ISC.SSCP.v2023-01-01.q803

Exam Code:	SSCP
Exam Name:	System Security Certified Practitioner (SSCP)
Certification Provider:	ISC
Free Question Number:	803
Version:	v2023-01-01
# of views:	12895
# of Questions views:	8030
https://www.freeqas.com/qa/ISC/SSCP/ISC.SSCP.v2023-01-01.q803.html	

NEW QUESTION: 1
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers does NOT have which of the following characteristics?
A. Standard model for network communications
B. Used to gain information from network devices such as count of packets received and routing tables
C. Enables dissimilar networks to communicate
D. Defines 7 protocol layers (a.k.a. protocol stack)
Answer: (SHOW ANSWER)
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers and Characteristics Standard model for network communications enables dissimilar networks to communicate, Defines 7 protocol layers (a.k.a. protocol stack) Each layer on one workstation communicates with its respective layer on another workstation using protocols (i.e. agreed-upon communication formats) "Mapping" each protocol to the model is useful for comparing protocols.
Mnemonics: Please Do Not Throw Sausage Pizza Away (bottom to top layer)
All People Seem To Need Data Processing (top to bottom layer).
Source: STEINER, Kurt, Telecommunications and Network Security, Version 1, May 2002, CISSP Open Study Group (Domain Leader: skottikus), Page 12.

NEW QUESTION: 2
How should a risk be HANDLED when the cost of the countermeasure OUTWEIGHS the cost of the risk?
A. Reject the risk
B. Perform another risk analysis
C. Accept the risk
D. Reduce the risk
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery

Explanation/Reference:
Which means the company understands the level of risk it is faced.
The following answers are incorrect because :
Reject the risk is incorrect as it means ignoring the risk which is dangerous.
Perform another risk analysis is also incorrect as the existing risk analysis has already shown the results.
Reduce the risk is incorrect is applicable after implementing the countermeasures.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 39

NEW QUESTION: 3
Transport Layer Security (TLS) is a two-layered socket layer security protocol that contains the TLS Record Protocol and the::
A. Transport Layer Security (TLS) Internet Protocol.
B. Transport Layer Security (TLS) Data Protocol.
C. Transport Layer Security (TLS) Link Protocol.
D. Transport Layer Security (TLS) Handshake Protocol.
Answer: (SHOW ANSWER)
Section: Network and Telecommunications

NEW QUESTION: 4
Which of the following phases of a system development life-cycle is most concerned with maintaining proper authentication of users and processes to ensure appropriate access control decisions?
A. Development/acquisition
B. Implementation
C. Operation/Maintenance
D. Initiation
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The operation phase of an IT system is concerned with user authentication.
Authentication is the process where a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action, thereby ensuring that security is not compromised by an untrusted source.
It is essential that adequate authentication be achieved in order to implement security policies and achieve security goals. Additionally, level of trust is always an issue when dealing with cross-domain interactions. The solution is to establish an authentication policy and apply it to cross-domain interactions as required.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 15).

NEW QUESTION: 5

Which of the following addresses a portion of the primary memory by specifying the actual address of the memory location?

A. direct addressing

B. Indirect addressing

C. implied addressing

D. indexed addressing

Answer: A (LEAVE A REPLY)

Absolute/Direct

+------+-----+-------------------------------------+ | load | reg | address | +------+-----

+-------------------------------------+

(Effective address = address as given in instruction)

This requires space in an instruction for quite a large address. It is often available on CISC machines which have variable-length instructions, such as x86.

Some RISC machines have a special Load Upper Literal instruction which places a 16-bit constant in the top half of a register. An OR literal instruction can be used to insert a 16-bit constant in the lower half of that register, so that a full 32-bit address can then be used via the register-indirect addressing mode, which itself is provided as "base-plus-offset" with an offset of 0.

http://en.wikipedia.org/wiki/Addressing_mode (Very good coverage of the subject)

also see:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 186.

also see:

http://www.comsci.us/ic/notes/am.html

NEW QUESTION: 6

CORRECT TEXT

A type of virus that resides in a Word or Excel document is called a _____ virus?

Answer:

NEW QUESTION: 7

Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered. There are two basic IDS analysis methods that exists. Which of the basic method is more prone to false positive?

A. Pattern Matching (also called signature analysis)

B. Anomaly Detection

C. Host-based intrusion detection

D. Network-based intrusion detection

Answer: (SHOW ANSWER)

Explanation/Reference:

Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered.
There are two basic IDS analysis methods:
1. Pattern Matching (also called signature analysis), and
2. Anomaly detection

PATTERN MATCHING

Some of the first IDS products used signature analysis as their detection method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the data stream) to produce an alert if that pattern was detected. If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS.

ANOMALY DETECTION

Alternately, anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host. Anomalies may include but are not limited to:

Multiple failed log-on attempts
Users logging in at strange hours
Unexplained changes to system clocks
Unusual error messages
Unexplained system shutdowns or restarts
Attempts to access restricted files

An anomaly-based IDS tends to produce more data because anything outside of the expected behavior is reported. Thus, they tend to report more false positives as expected behavior patterns change. An advantage to anomaly-based IDS is that, because they are based on behavior identification and not specific patterns of traffic, they are often able to detect new attacks that may be overlooked by a signature- based system. Often information from an anomaly-based IDS may be used to create a pattern for a signature-based IDS.

Host Based Intrusion Detection (HIDS)

HIDS is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.

Network Based Intrustion Detection (NIDS)

NIDS are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network.

Below you have other ways that instrusion detection can be performed:

Stateful Matching Intrusion Detection

Stateful matching takes pattern matching to the next level. It scans for attack signatures in the context of a stream of traffic or overall system behavior rather than the individual packets or discrete system activities.

For example, an attacker may use a tool that sends a volley of valid packets to a targeted system. Because all the packets are valid, pattern matching is nearly useless. However, the fact that a large volume of the packets was seen may, itself, represent a known or potential attack pattern. To evade attack, then, the attacker may send the packets from multiple locations with long wait periods between each transmission to either confuse the signature detection system or exhaust its session timing window. If the IDS service is tuned to record and analyze traffic over a long period of time it may detect such an attack.

Because stateful matching also uses signatures, it too must be updated regularly and, thus, has some of the same limitations as pattern matching.

Statistical Anomaly-Based Intrusion Detection

The statistical anomaly-based IDS analyzes event data by comparing it to typical, known, or predicted traffic profiles in an effort to find potential security breaches. It attempts to identify suspicious behavior by analyzing event data and identifying patterns of entries that deviate from a predicted norm. This type of detection method can be very effective and, at a very high level, begins to take on characteristics seen in IPS by establishing an expected baseline of behavior and acting on divergence from that baseline.

However, there are some potential issues that may surface with a statistical IDS. Tuning the IDS can be challenging and, if not performed regularly, the system will be prone to false positives. Also, the definition of normal traffic can be open to interpretation and does not preclude an attacker from using normal activities to penetrate systems. Additionally, in a large, complex, dynamic corporate environment, it can be difficult, if not impossible, to clearly define "normal" traffic. The value of statistical analysis is that the system has the potential to detect previously unknown attacks. This is a huge departure from the limitation of matching previously known signatures. Therefore, when combined with signature matching technology, the statistical anomaly-based IDS can be very effective.

Protocol Anomaly-Based Intrusion Detection

A protocol anomaly-based IDS identifies any unacceptable deviation from expected behavior based on known network protocols. For example, if the IDS is monitoring an HTTP session and the traffic contains attributes that deviate from established HTTP session protocol standards, the IDS may view that as a malicious attempt to manipulate the protocol, penetrate a firewall, or exploit a vulnerability. The value of this method is directly related to the use of well-known or well-defined protocols within an environment. If an organization primarily uses well-known protocols (such as HTTP, FTP, or telnet) this can be an effective method of performing intrusion detection. In the face of custom or nonstandard protocols, however, the system will have more difficulty or be completely unable to determine the proper packet format.

Interestingly, this type of method is prone to the same challenges faced by signature-based IDSs. For example, specific protocol analysis modules may have to be added or customized to deal with unique or new protocols or unusual use of standard protocols. Nevertheless, having an IDS that is intimately aware of valid protocol use can be very powerful when an organization employs standard implementations of common protocols.

Traffic Anomaly-Based Intrusion
Detection A traffic anomaly-based IDS identifies any unacceptable deviation from expected behavior based on actual traffic structure. When a session is established between systems, there is typically an expected pattern and behavior to the traffic transmitted in that session. That traffic can be compared to expected traffic conduct based on the understandings of traditional system interaction for that type of connection.
Like the other types of anomaly-based IDS, traffic anomaly-based IDS relies on the ability to establish "normal" patterns of traffic and expected modes of behavior in systems, networks, and applications. In a highly dynamic environment it may be difficult, if not impossible, to clearly define these parameters.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3664-3686). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3711-3734). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3694-3711). Auerbach Publications. Kindle Edition.

NEW QUESTION: 8
Under United States law, an investigator's notebook may be used in court in which of the following scenarios?
A. When the investigator is unwilling to testify.
B. When other forms of physical evidence are not available.
C. To refresh the investigators memory while testifying.
D. If the defense has no objections.
Answer: C (LEAVE A REPLY)
An investigator's notebook cannot be used as evidence is court. It can only be used by the investigator to refresh his memory during a proceeding, but cannot be submitted as evidence in any form.
The following answers are incorrect:
When the investigator is unwilling to testify. Is incorrect because the notebook cannot be submitted as evidence in any form.
When other forms of physical evidence are not available. Is incorrect because the notebook cannot be submitted as evidence in any form.
If the defense has no objections. Is incorrect because the notebook cannot be submitted as evidence in any form.

NEW QUESTION: 9
Which of the following does not address Database Management Systems (DBMS) Security?
A. Perturbation
B. Cell suppression

C. Padded cells
D. Partitioning
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Padded cells complement Intrusion Detection Systems (IDSs) and are not related to DBMS security. Padded cells are simulated environments to which IDSs seamlessly transfer detected attackers and are designed to convince an attacker that the attack is going according to the plan. Cell suppression is a technique used against inference attacks by not revealing information in the case where a statistical query produces a very small result set. Perturbation also addresses inference attacks but involves making minor modifications to the results to a query. Partitioning involves splitting a database into two or more physical or logical parts; especially relevant for multilevel secure databases.
Source: LaROSA, Jeanette (domain leader), Application and System Development Security CISSP Open Study Guide, version 3.0, January 2002.

NEW QUESTION: 10
In what way could Java applets pose a security threat?
A. Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing SSL and S-HTTP
B. Java interpreters do not provide the ability to limit system access that an applet could have on a client system.
C. Executables from the Internet may attempt an intentional attack when they are downloaded on a client system.
D. Java does not check the bytecode at runtime or provide other safety mechanisms for program isolation from the client system.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 11
What is NOT an authentication method within IKE and IPsec?
A. CHAP
B. Pre shared key
C. certificate based authentication
D. Public key authentication
Answer: (SHOW ANSWER)
CHAP is not used within IPSEC or IKE. CHAP is an authentication scheme
used by Point to Point Protocol (PPP) servers to validate the identity of remote clients.
CHAP periodically verifies the identity of the client by using a three-way handshake. This
happens at the time of establishing the initial link (LCP), and may happen again at any time
afterwards. The verification is based on a shared secret (such as the client user's

password).
After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.
The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.
The following were incorrect answers:
Pre Shared Keys
In cryptography, a pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. To build a key from shared secret, the key derivation function should be used. Such systems almost always use symmetric key cryptographic algorithms. The term PSK is used in WiFi encryption such as WEP or WPA, where both the wireless access points (AP) and all clients share the same key.
The characteristics of this secret or key are determined by the system which uses it; some system designs require that such keys be in a particular format. It can be a password like 'bret13i', a passphrase like 'Idaho hung gear id gene', or a hexadecimal string like '65E4 E556 8622 EEE1'. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems.
Certificat Based Authentication
The most common form of trusted authentication between parties in the wide world of Web commerce is the exchange of certificates. A certificate is a digital document that at a minimum includes a Distinguished Name (DN) and an associated public key.
The certificate is digitally signed by a trusted third party known as the Certificate Authority (CA). The CA vouches for the authenticity of the certificate holder. Each principal in the transaction presents certificate as its credentials. The recipient then validates the certificate's signature against its cache of known and trusted CA certificates. A "personal certificate" identifies an end user in a transaction; a "server certificate" identifies the service provider.
Generally, certificate formats follow the X.509 Version 3 standard. X.509 is part of the Open Systems Interconnect
(OSI) X.500 specification.
Public Key Authentication
Public key authentication is an alternative means of identifying yourself to a login server, instead of typing a password. It is more secure and more flexible, but more difficult to set up.
In conventional password authentication, you prove you are who you claim to be by proving

that you know the correct password. The only way to prove you know the password is to tell the server what you think the password is. This means that if the server has been hacked, or spoofed an attacker can learn your password.
Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have a copy of that private key; but anybody who has your public key can verify that a particular signature is genuine.
So you generate a key pair on your own computer, and you copy the public key to the server. Then, when the server asks you to prove who you are, you can generate a signature using your private key. The server can verify that signature (since it has your public key) and allow you to log in. Now if the server is hacked or spoofed, the attacker does not gain your private key or password; they only gain one signature. And signatures cannot be re-used, so they have gained nothing.
There is a problem with this: if your private key is stored unprotected on your own computer, then anybody who gains access to your computer will be able to generate signatures as if they were you. So they will be able to log in to your server under your account. For this reason, your private key is usually encrypted when it is stored on your local machine, using a passphrase of your choice. In order to generate a signature, you must decrypt the key, so you have to type your passphrase.
References:
RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E.
Internet Cryptography, 1997, Addison-Wesley Pub Co.; HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 467.
http://en.wikipedia.org/wiki/Pre-shared_key
http://www.home.umk.pl/~mgw/LDAP/RS.C4.JUN.97.pdf
http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html#S8.1

NEW QUESTION: 12
CORRECT TEXT
Public keys are used for _____ messages and private keys are used for _____ messages.
Answer:
depcrypting

NEW QUESTION: 13
A prolonged complete loss of electric power is a:
A. brownout
B. blackout

C. surge
D. fault
Answer: B (LEAVE A REPLY)
Explanation/Reference:
A prolonged power outage is a blackout.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 14
Which of the following can best be defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs?
A. A known-plaintext attack
B. A known-algorithm attack
C. A chosen-ciphertext attack
D. A chosen-plaintext attack
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
RFC2828 (Internet Security Glossary) defines a known-plaintext attack as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs (although the analyst may also have other clues, such as the knowing the cryptographic algorithm). A chosen-ciphertext attack is defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of plaintext that corresponds to ciphertext selected (i.e., dictated) by the analyst. A chosen-plaintext attack is a cryptanalysis technique in which the analyst tries to determine the key from knowledge of ciphertext that corresponds to plaintext selected (i.e., dictated) by the analyst. The other choice is a distracter.
The following are incorrect answers:
A chosen-plaintext attacks
The attacker has the plaintext and ciphertext, but can choose the plaintext that gets encrypted to see the corresponding ciphertext. This gives her more power and possibly a deeper understanding of the way the encryption process works so she can gather more information about the key being used. Once the key is discovered, other messages encrypted with that key can be decrypted.
A chosen-ciphertext attack
In chosen-ciphertext attacks, the attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext. Again, the goal is to figure out the key. This is a harder attack to carry out compared to the previously mentioned attacks, and the attacker may need to have control of the system that contains the cryptosystem.
A known-algorithm attack
Knowing the algorithm does not give you much advantage without knowing the key. This is a bogus detractor.
The algorithm should be public, which is the Kerckhoffs's Principle . The only secret should be the key.

Reference(s) used for this question:
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 866). McGraw-Hill. Kindle Edition.
and
Kerckhoffs's Principle

NEW QUESTION: 15
Notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects is part of:
A. Incident Evaluation
B. Incident Recognition
C. Incident Protection
D. Incident Response
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
These are core functions of the incident response process.
"Incident Evaluation" is incorrect. Evaluation of the extent and cause of the incident is a component of the incident response process.
"Incident Recognition" is incorrect. Recognition that an incident has occurred is the precursor to the initiation of the incident response process.
"Incident Protection" is incorrect. This is an almost-right-sounding nonsense answer to distract the unwary.
References
CBK, pp. 698 - 703

NEW QUESTION: 16
When we encrypt or decrypt data there is a basic operation involving ones and zeros where they are compared in a process that looks something like this:
0101 0001 Plain text
0111 0011 Key stream
0010 0010 Output
What is this cryptographic operation called?
A. Exclusive-OR
B. Bit Swapping
C. Logical-NOR
D. Decryption
Answer: A (LEAVE A REPLY)

When we encrypt data we are basically taking the plaintext information and applying some key material or keystream and conducting something called an XOR or Exclusive-OR operation.
The symbol used for XOR is the following: This is a type of cipher known as a stream cipher.
The operation looks like this: 0101 0001 Plain text 0111 0011 Key stream 0010 0010 Output (ciphertext)
As you can see, it's not simple addition and the XOR Operation uses something called a truth table that explains why 0+1=1 and 1+1=0.
The rules are simples, if both bits are the same the result is zero, if both bits are not the same the result is one.
The following answers are incorrect:
-Bit Swapping: Incorrect. This isn't a known cryptographic operations.
-Logical NOR: Sorry, this isn't correct but is where only 0+0=1. All other combinations of 1+1, 1+0 equals 0. More on NOR here.
-Decryption: Sorry, this is the opposite of the process of encryption or, the process of applying the keystream to the plaintext to get the resulting encrypted text.
The following reference(s) was used to create this question:
For more details on XOR and all other questions of cryptography. Subscribe to our holistic Security+ CBT tutorial at http://www.cccure.tv and http://en.wikipedia.org/wiki/Exclusive-or and http://en.wikipedia.org/wiki/Stream_cipher

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 17
The Orange Book states that "Hardware and software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB [Trusted Computing Base]." This statement is the formal requirement for:
A. Security Testing.
B. Design Verification.
C. System Integrity.
D. System Architecture Specification.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
This is a requirement starting as low as C1 within the TCSEC rating.
The Orange book requires the following for System Integrity Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

NOTE FROM CLEMENT:
This is a question that confuses a lot of people because most people take for granted that the orange book with its associated Bell LaPadula model has nothing to do with integrity. However you have to be careful about the context in which the word integrity is being used. You can have Data Integrity and you can have System Integrity which are two completely different things.
Yes, the Orange Book does not specifically address the Integrity requirements, however it has to run on top of systems that must meet some integrity requirements.
This is part of what they call operational assurance which is defined as a level of confidence of a trusted system's architecture and implementation that enforces the system's security policy. It includes:
System architecture
Covert channel analysis
System integrity
Trusted recovery
DATA INTEGRITY
Data Integrity is very different from System Integrity. When you have integrity of the data, there are three goals:
1. Prevent authorized users from making unauthorized modifications
2. Preven unauthorized users from making modifications
3. Maintaining internal and external consistancy of the data
Bell LaPadula which is based on the Orange Book address does not address Integrity, it addresses only Confidentiality.
Biba address only the first goal of integrity.
Clark-Wilson addresses the three goals of integrity.
In the case of this question, there is a system integrity requirement within the TCB. As mentioned above here is an extract of the requirements: Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.
The following answers are incorrect:
Security Testing. Is incorrect because Security Testing has no set of requirements in the Orange book.
Design Verification. Is incorrect because the Orange book's requirements for Design Verification include: A formal model of the security policy must be clearly identified and documented, including a mathematical proof that the model is consistent with its axioms and is sufficient to support the security policy.
System Architecture Specification. Is incorrect because there are no requirements for System Architecture Specification in the Orange book.
The following reference(s) were used for this question:
Trusted Computer Security Evaluation Criteria (TCSEC), DoD 5200.28-STD, page 15, 18, 25, 31, 40, 50.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page 392-397, for users with the Kindle Version see Kindle Locations 28504-28505.
and
DOD TCSEC - http://www.cerberussystems.com/INFOSEC/stds/d520028.htm

NEW QUESTION: 18
In which layer of the OSI Model are connection-oriented protocols located in the TCP/IP suite of protocols?
A. Transport layer
B. Application layer
C. Physical layer
D. Network layer
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Connection-oriented protocols such as TCP provides reliability.
It is the responsibility of such protocols in the transport layer to ensure every byte is accounted for. The network layer does not provide reliability. It only privides the best route to get the traffic to the final destination address.
For your exam you should know the information below about OSI model:
The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.
The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.
OSI Model

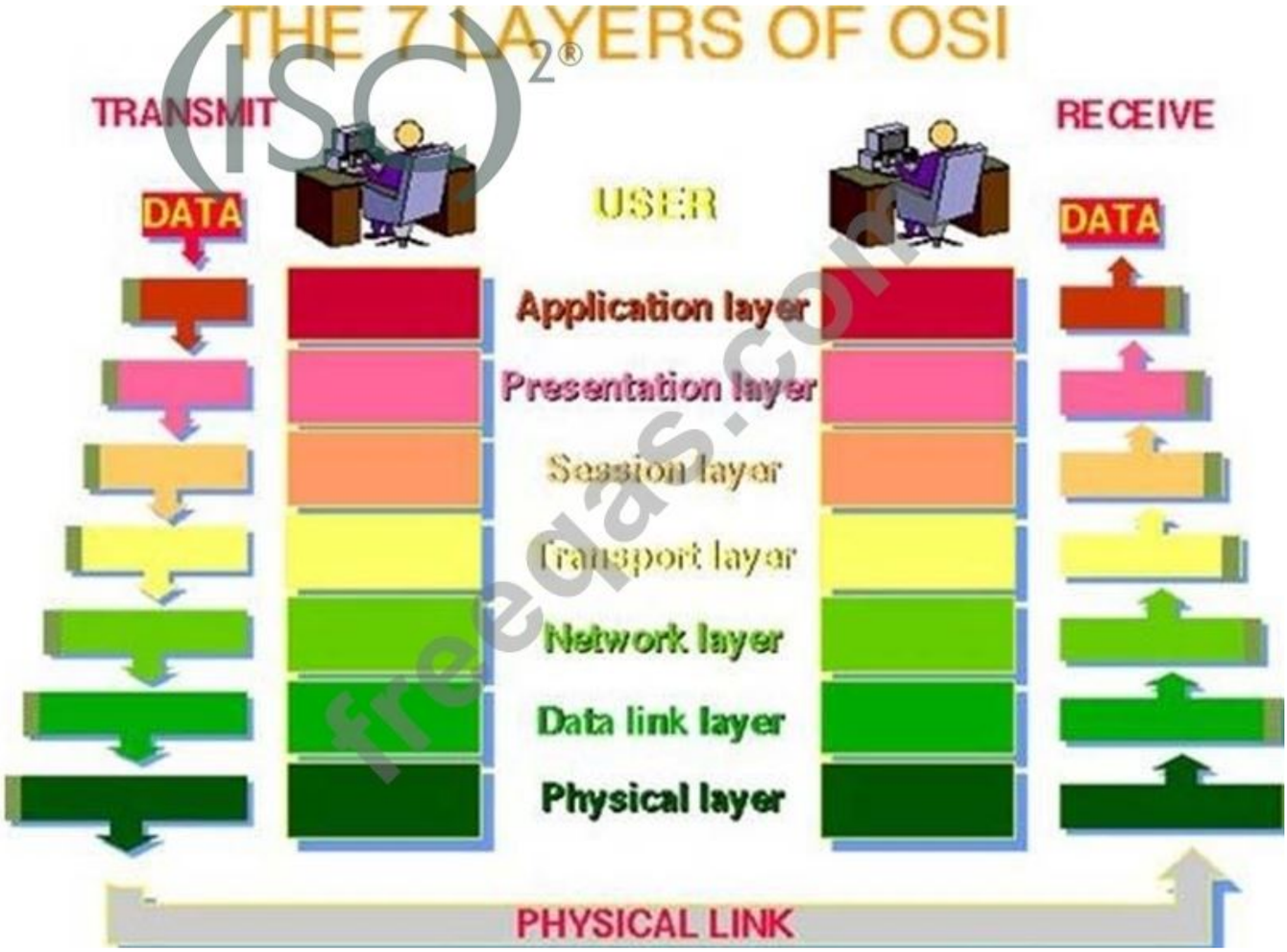


Image source: http://www.petri.co.il/images/osi_model.JPG

PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts

How the receiving station delimits a frame

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
Frame delimiting: creates and recognizes frame boundaries.
Frame error checking: checks received frames for integrity.
Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:
Routing: routes frames among networks.
Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.
This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).
In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.
The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.
The transport layer provides:
Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).
Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.
The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.
End-to-end layers
Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.
SESSION LAYER
The session layer allows session establishment between processes running on different stations. It provides:
Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.
PRESENTATION LAYER
The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.
The presentation layer provides:
Character code translation: for example, ASCII to EBCDIC.
Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
Data compression: reduces the number of bits that need to be transmitted on the network.
Data encryption: encrypt data for security purposes. For example, password encryption.
APPLICATION LAYER
The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication

Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals
The following were incorrect answers:
Application Layer - The application layer serves as the window for users and application processes to access network services.
Network layer - The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.
Physical Layer - The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 260
and
Official ISC2 guide to CISSP CBK 3rd Edition Page number 287
and
http://en.wikipedia.org/wiki/Tcp_protocol

NEW QUESTION: 19
Which one of the following represents an ALE calculation?
A. single loss expectancy x annualized rate of occurrence.
B. gross loss expectancy x loss frequency.
C. actual replacement cost - proceeds of salvage.
D. asset value x loss expectancy.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
Single Loss Expectancy (SLE) is the dollar amount that would be lost if there was a loss of an asset.
Annualized Rate of Occurrence (ARO) is an estimated possibility of a threat to an asset taking place in one year (for example if there is a change of a flood occuring once in 10 years the ARO would be .1, and if there was a chance of a flood occuring once in 100 years then the ARO would be .01).
The following answers are incorrect:
gross loss expectancy x loss frequency. Is incorrect because this is a distractor.
actual replacement cost - proceeds of salvage. Is incorrect because this is a distractor.
asset value x loss expectancy. Is incorrect because this is a distractor.

NEW QUESTION: 20
Degaussing is used to clear data from all of the following medias except:

A. Floppy Disks
B. Read-Only Media
C. Video Tapes
D. Magnetic Hard Disks
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Atoms and Data
Shon Harris says: "A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes"
The latest ISC2 book says:
"Degaussing can also be a form of media destruction. High-power degaussers are so strong in some cases that they can literally bend and warp the platters in a hard drive. Shredding and burning are effective destruction methods for non-rigid magnetic media. Indeed, some shredders are capable of shredding some rigid media such as an optical disk. This may be an effective alternative for any optical media containing nonsensitive information due to the residue size remaining after feeding the disk into the machine. However, the residue size might be too large for media containing sensitive information. Alternatively, grinding and pulverizing are acceptable choices for rigid and solid-state media. Specialized devices are available for grinding the face of optical media that either sufficiently scratches the surface to render the media unreadable or actually grinds off the data layer of the disk. Several services also exist which will collect drives, destroy them on site if requested and provide certification of completion. It will be the responsibility of the security professional to help, select, and maintain the most appropriate solutions for media cleansing and disposal."
Degaussing is achieved by passing the magnetic media through a powerful magnet field to rearrange the metallic particles, completely removing any resemblance of the previously recorded signal (from the "all about degaussers link below). Therefore, degaussing will work on any electronic based media such as floppy disks, or hard disks - all of these are examples of electronic storage. However, "read-only media" includes items such as paper printouts and CD-ROM wich do not store data in an electronic form or is not magnetic storage. Passing them through a magnet field has no effect on them.
Not all clearing/ purging methods are applicable to all media- for example, optical media is not susceptible to degaussing, and overwriting may not be effective against Flash devices. The degree to which information may be recoverable by a sufficiently motivated and capable adversary must not be underestimated or guessed at in ignorance. For the highest-value commercial data, and for all data regulated by government or military classification rules, read and follow the rules and standards.
I will admit that this is a bit of a trick question. Determining the difference between "read-only media" and "read-only memory" is difficult for the question taker. However, I believe it is representative of the type of question you might one day see on an exam.
The other answers are incorrect because:
Floppy Disks, Magnetic Tapes, and Magnetic Hard Disks are all examples of magnetic storage, and therefore are erased by degaussing.

A videotape is a recording of images and sounds on to magnetic tape as opposed to film stock used in filmmaking or random access digital media. Videotapes are also used for storing scientific or medical data, such as the data produced by an electrocardiogram. In most cases, a helical scan video head rotates against the moving tape to record the data in two dimensions, because video signals have a very high bandwidth, and static heads would require extremely high tape speeds. Videotape is used in both video tape recorders (VTRs) or, more commonly and more recently, videocassette recorder (VCR) and camcorders. A Tape use a linear method of storing information and since nearly all video recordings made nowadays are digital direct to disk recording (DDR), videotape is expected to gradually lose importance as non-linear/random-access methods of storing digital video data become more common.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 25627-25630). McGraw-Hill. Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Operations (Kindle Locations 580-588). . Kindle Edition.
All About Degaussers and Erasure of Magnetic Media:
http://www.degausser.co.uk/degauss/degabout.htm
http://www.degaussing.net/
http://www.cerberussystems.com/INFOSEC/stds/ncsctg25.htm

NEW QUESTION: 21
Which layer of the DoD TCP/IP Model ensures error-free delivery and packet sequencing?
A. Internet layer
B. Network access layer
C. Host-to-host
D. Application layer
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
This layer of the DoD Model is also sometimes called Transport in some books but the proper name is Host-to- Host as per the RFC document.
The host-to-host layer provides for reliable end-to-end communications, ensures the data's error-free delivery, handles the data's packet sequencing, and maintains the data's integrity.
It is comparable to the transport layer of the OSI model.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/Internet_protocol_suite
and
http://technet.microsoft.com/en-us/library/cc786900%28v=ws.10%29.aspx
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 85).

NEW QUESTION: 22
What is the maximum length of cable that can be used for a twisted-pair, Category 5 10Base-T cable?
A. 80 meters
B. 100 meters
C. 185 meters
D. 500 meters
Answer: B (LEAVE A REPLY)
As a signal travels though a medium, it attenuates (loses strength) and at some point will become indistinguishable from noise. To assure trouble-free communication, maximum cable lengths are set between nodes to assure that attenuation will not cause a problem. The maximum CAT-5 UTP cable length between two nodes for 10BASE-T is 100M.
The following answers are incorrect:
80 meters. It is only a distracter.
185 meters. Is incorrect because it is the maximum length for 10Base-2 500 meters. Is incorrect because it is the maximum length for 10Base-5

NEW QUESTION: 23
Which backup method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup?
A. differential backup method
B. full backup method
C. incremental backup method
D. tape backup method.
Answer: A (LEAVE A REPLY)
The Differential Backup Method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup. Archive Bits
Unless you've done a lot of backups in your time you've probably never heard of an Archive Bit. An archive bit is, essentially, a tag that is attached to every file. In actuality, it is a binary digit that is set on or off in the file, but that's crummy technical jargon that doesn't really tell us anything. For the sake of our discussion, just think of it as the flag on a mail box. If the flag is up, it means the file has been changed. If it's down, then the file is unchanged.
Archive bits let the backup software know what needs to be backed up. The differential and incremental backup types rely on the archive bit to direct them. Backup Types
Full or Normal The "Full" or "normal" backup type is the most standard. This is the backup type that you would use if you wanted to backup every file in a given folder or drive. It backs up everything you direct it to regardless of what the archive bit says. It also resets all archive bits (puts the flags down). Most backup software, including the built-in Windows backup software, lets you select down to the individual file that you want backed up. You can also choose to backup things like the "system state".

Incremental When you schedule an incremental backup, you are in essence instructing the software to only backup files that have been changed, or files that have their flag up. After the incremental backup of that file has occured, that flag will go back down. If you perform a normal backup on Monday, then an incremental backup on Wednesday, the only files that will be backed up are those that have changed since Monday. If on Thursday someone deletes a file by accident, in order to get it back you will have to restore the full backup from Monday, followed by the Incremental backup from Wednesday.
Differential Differential backups are similar to incremental backups in that they only backup files with their archive bit, or flag, up. However, when a differential backup occurs it does not reset those archive bits which means, if the following day, another differential backup occurs, it will back up that file again regardless of whether that file has been changed or not.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.
And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (pages 617-619). And:
http://www.brighthub.com/computing/windows-platform/articles/24531.aspx

NEW QUESTION: 24
What can be defined as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate?
A. A public-key certificate
B. An attribute certificate
C. A digital certificate
D. A descriptive certificate
Answer: B (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
The Internet Security Glossary (RFC2828) defines an attribute certificate as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate. A public-key certificate binds a subject name to a public key value, along with information needed to perform certain cryptographic functions. Other attributes of a subject, such as a security clearance, may be certified in a separate kind of digital certificate, called an attribute certificate. A subject may have multiple attribute certificates associated with its name or with each of its public-key certificates.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 25
While using IPsec, the ESP and AH protocols both provides integrity services. However when using AH, some special attention needs to be paid if one of the peers uses NAT for address translation service. Which of the items below would affects the use of AH and it´s Integrity Check Value (ICV) the most?
A. Key session exchange

B. Packet Header Source or Destination address
C. VPN cryptographic key size
D. Crypotographic algorithm used
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
It may seem odd to have two different protocols that provide overlapping functionality.
AH provides authentication and integrity, and ESP can provide those two functions and confidentiality.
Why even bother with AH then?
In most cases, the reason has to do with whether the environment is using network address translation (NAT).
IPSec will generate an integrity check value (ICV), which is really the same thing as a MAC value, over a portion of the packet. Remember that the sender and receiver generate their own values. In IPSec, it is called an ICV value. The receiver compares her ICV value with the one sent by the sender. If the values match, the receiver can be assured the packet has not been modified during transmission. If the values are different, the packet has been altered and the receiver discards the packet.
The AH protocol calculates this ICV over the data payload, transport, and network headers. If the packet then goes through a NAT device, the NAT device changes the IP address of the packet. That is its job. This means a portion of the data (network header) that was included to calculate the ICV value has now changed, and the receiver will generate an ICV value that is different from the one sent with the packet, which means the packet will be discarded automatically.
The ESP protocol follows similar steps, except it does not include the network header portion when calculating its ICV value. When the NAT device changes the IP address, it will not affect the receiver's ICV value because it does not include the network header when calculating the ICV.
Here is a tutorial on IPSEC from the Shon Harris Blog:
The Internet Protocol Security (IPSec) protocol suite provides a method of setting up a secure channel for protected data exchange between two devices. The devices that share this secure channel can be two servers, two routers, a workstation and a server, or two gateways between different networks. IPSec is a widely accepted standard for providing network layer protection. It can be more flexible and less expensive than end- to end and link encryption methods.
IPSec has strong encryption and authentication methods, and although it can be used to enable tunneled communication between two computers, it is usually employed to establish virtual private networks (VPNs) among networks across the Internet.
IPSec is not a strict protocol that dictates the type of algorithm, keys, and authentication method to use. Rather, it is an open, modular framework that provides a lot of flexibility for companies when they choose to use this type of technology. IPSec uses two basic security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH is the authenticating protocol, and ESP is an authenticating and encrypting protocol that uses cryptographic mechanisms to provide source authentication, confidentiality, and message integrity.
IPSec can work in one of two modes: transport mode, in which the payload of the message is protected, and tunnel mode, in which the payload and the routing and header information are protected. ESP in

transport mode encrypts the actual message information so it cannot be sniffed and uncovered by an unauthorized entity. Tunnel mode provides a higher level of protection by also protecting the header and trailer data an attacker may find useful. Figure 8-26 shows the high-level view of the steps of setting up an IPSec connection.

Each device will have at least one security association (SA) for each VPN it uses. The SA, which is critical to the IPSec architecture, is a record of the configurations the device needs to support an IPSec connection.

When two devices complete their handshaking process, which means they have agreed upon a long list of parameters they will use to communicate, these data must be recorded and stored somewhere, which is in the SA.

The SA can contain the authentication and encryption keys, the agreed-upon algorithms, the key lifetime, and the source IP address. When a device receives a packet via the IPSec protocol, it is the SA that tells the device what to do with the packet. So if device B receives a packet from device C via IPSec, device B will look to the corresponding SA to tell it how to decrypt the packet, how to properly authenticate the source of the packet, which key to use, and how to reply to the message if necessary.

SAs are directional, so a device will have one SA for outbound traffic and a different SA for inbound traffic for each individual communication channel. If a device is connecting to three devices, it will have at least six SAs, one for each inbound and outbound connection per remote device. So how can a device keep all of these SAs organized and ensure that the right SA is invoked for the right connection? With the mighty secu rity parameter index (SPI), that's how. Each device has an SPI that keeps track of the different SAs and tells the device which one is appropriate to invoke for the different packets it receives. The SPI value is in the header of an IPSec packet, and the device reads this value to tell it which SA to consult.

IPSec can authenticate the sending devices of the packet by using MAC (covered in the earlier section, "The One-Way Hash"). The ESP protocol can provide authentication, integrity, and confidentiality if the devices are configured for this type of functionality.

So if a company just needs to make sure it knows the source of the sender and must be assured of the integrity of the packets, it would choose to use AH. If the company would like to use these services and also have confidentiality, it would use the ESP protocol because it provides encryption functionality. In most cases, the reason ESP is employed is because the company must set up a secure VPN connection.

It may seem odd to have two different protocols that provide overlapping functionality. AH provides authentication and integrity, and ESP can provide those two functions and confidentiality. Why even bother with AH then? In most cases, the reason has to do with whether the environment is using network address translation (NAT). IPSec will generate an integrity check value (ICV), which is really the same thing as a MAC value, over a portion of the packet. Remember that the sender and receiver generate their own values. In IPSec, it is called an ICV value. The receiver compares her ICV value with the one sent by the sender. If the values match, the receiver can be assured the packet has not been modified during transmission. If the values are different, the packet has been altered and the receiver discards the packet.

The AH protocol calculates this ICV over the data payload, transport, and network headers. If the packet then goes through a NAT device, the NAT device changes the IP address of the packet. That is its job. This means a portion of the data (network header) that was included to calculate the ICV value has now changed, and the receiver will generate an ICV value that is different from the one sent with the packet, which means the packet will be discarded automatically.
The ESP protocol follows similar steps, except it does not include the network header portion when calculating its ICV value. When the NAT device changes the IP address, it will not affect the receiver's ICV value because it does not include the network header when calculating the ICV.
Because IPSec is a framework, it does not dictate which hashing and encryption algorithms are to be used or how keys are to be exchanged between devices. Key management can be handled manually or automated by a key management protocol. The de facto standard for IPSec is to use Internet Key Exchange (IKE), which is a combination of the ISAKMP and OAKLEY protocols. The Internet Security Association and Key Management Protocol (ISAKMP) is a key exchange architecture that is independent of the type of keying mechanisms used.
Basically, ISAKMP provides the framework of what can be negotiated to set up an IPSec connection (algorithms, protocols, modes, keys). The OAKLEY protocol is the one that carries out the negotiation process.
You can think of ISAKMP as providing the playing field (the infrastructure) and OAKLEY as the guy running up and down the playing field (carrying out the steps of the negotiation).
IPSec is very complex with all of its components and possible configurations. This complexity is what provides for a great degree of flexibility, because a company has many different configuration choices to achieve just the right level of protection. If this is all new to you and still confusing, please review one or more of the following references to help fill in the gray areas.
The following answers are incorrect:
The other options are distractors.
The following reference(s) were/was used to create this question:
Shon Harris, CISSP All-in-One Exam Guide- fiveth edition, page 759
and
https://neodean.wordpress.com/tag/security-protocol/

NEW QUESTION: 26
Which of the following protocols is designed to send individual messages securely?
A. Kerberos
B. Secure Electronic Transaction (SET).
C. Secure Sockets Layer (SSL).
D. Secure HTTP (S-HTTP).
Answer: D (LEAVE A REPLY)
Explanation/Reference:
An early standard for encrypting HTTP documents, Secure HTTP (S-HTTP) is designed to send individual messages securely. SSL is designed to establish a secure connection between two computers.

SET was originated by VISA and MasterCard as an Internet credit card protocol using digital signatures. Kerberos is an authentication system.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 89.

NEW QUESTION: 27
Which of the following statements pertaining to software testing approaches is correct?
A. A bottom-up approach allows interface errors to be detected earlier.
B. A top-down approach allows errors in critical modules to be detected earlier.
C. The test plan and results should be retained as part of the system's permanent documentation.
D. Black box testing is predicated on a close examination of procedural detail.
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
A bottom-up approach to testing begins testing of atomic units, such as programs or modules, and works upwards until a complete system testing has taken place. It allows errors in critical modules to be found early.
A top-down approach allows for early detection of interface errors and raises confidence in the system, as programmers and users actually see a working system. White box testing is predicated on a close examination of procedural detail. Black box testing examines some aspect of the system with little regard for the internal logical structure of the software.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).
Top Down Testing: An approach to integration testing where the component at the top of the component hierarchy is tested first, with lower level components being simulated by stubs. Tested components are then used to test lower level components. The process is repeated until the lowest level components have been tested.
Bottom Up Testing: An approach to integration testing where the lowest level components are tested first, then used to facilitate the testing of higher level components. The process is repeated until the component at the top of the hierarchy is tested.
Black Box Testing: Testing based on an analysis of the specification of a piece of software without reference to its internal workings. The goal is to test how well the component conforms to the published requirements for the component.

NEW QUESTION: 28
Which of the following protocols operates at the session layer (layer 5)?
A. RPC
B. IGMP
C. LPD
D. SPX

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Remotre Procedure Call (RPC) is the only of the above choices to operate at the session layer (layer 5). All of the other answers were wrong.

LPD operates at layer 7

SPX operates at layer 4

IGMP operates at layer 3.

Reference:

WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

NEW QUESTION: 29

Which of the following would best classify as a management control?

A. Review of security controls

B. Personnel security

C. Physical and environmental protection

D. Documentation

Answer: A (LEAVE A REPLY)

Section: Security Operation Adimnistration

Explanation/Reference:

Management controls focus on the management of the IT security system and the management of risk for a system.

They are techniques and concerns that are normally addressed by management.

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system, thus considered management controls.

SECURITY CONTROLS: The management, operational, and technical controls (i.e.,safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

SECURITY CONTROL BASELINE: The set of minimum security controls defined for a low-impact, moderate- impact,or high-impact information system.

The following are incorrect answers:

Personnel security, physical and environmental protection and documentation are forms of operational controls.

Reference(s) used for this question:

http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf and FIPS PUB 200 at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

NEW QUESTION: 30

Secure Shell (SSH-2) supports authentication, compression, confidentiality, and integrity, SSH is commonly used as a secure alternative to all of the following protocols below except:

A. telnet

B. rlogin
C. RSH
D. HTTPS
Answer: (SHOW ANSWER)
HTTPS is used for secure web transactions and is not commonly replaced by SSH.
Users often want to log on to a remote computer. Unfortunately, most early implementations to meet that need were designed for a trusted network. Protocols/programs, such as TELNET, RSH, and rlogin, transmit unencrypted over the network, which allows traffic to be easily intercepted. Secure shell (SSH) was designed as an alternative to the above insecure protocols and allows users to securely access resources on remote computers over an encrypted tunnel. SSH's services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel. Many users protect less secure traffic of protocols, such as X Windows and VNC (virtual network computing), by forwarding them through a SSH tunnel. The SSH tunnel protects the integrity of communication, preventing session hijacking and other man-in-the-middle attacks. Another advantage of SSH over its predecessors is that it supports strong authentication. There are several alternatives for SSH clients to authenticate to a SSH server, including passwords and digital certificates. Keep in mind that authenticating with a password is still a significant improvement over the other protocols because the password is transmitted encrypted.
The following were wrong answers:
telnet is an incorrect choice. SSH is commonly used as an more secure alternative to telnet. In fact Telnet should not longer be used today.
rlogin is and incorrect choice. SSH is commonly used as a more secure alternative to rlogin.
RSH is an incorrect choice. SSH is commonly used as a more secure alternative to RSH.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7077-7088). Auerbach Publications. Kindle Edition.

NEW QUESTION: 31
Which of the following is implemented through scripts or smart agents that replays the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services?
A. Single Sign-On
B. Dynamic Sign-On
C. Smart cards
D. Kerberos
Answer: (SHOW ANSWER)
SSO can be implemented by using scripts that replay the users multiple log-ins against authentication servers to verify a user's identity and to permit access to system services.

Single Sign on was the best answer in this case because it would include Kerberos.
When you have two good answers within the 4 choices presented you must select the BEST one. The high level choice is always the best. When one choice would include the other one that would be the best as well.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 40.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 32
Why do buffer overflows happen? What is the main cause?
A. Because buffers can only hold so much data
B. Because of improper parameter checking within the application
C. Because they are an easy weakness to exploit
D. Because of insufficient system memory
Answer: (SHOW ANSWER)
Explanation/Reference:
Buffer Overflow attack takes advantage of improper parameter checking within the application. This is the classic form of buffer overflow and occurs because the programmer accepts whatever input the user supplies without checking to make sure that the length of the input is less than the size of the buffer in the program.
The buffer overflow problem is one of the oldest and most common problems in software development and programming, dating back to the introduction of interactive computing. It can result when a program fills up the assigned buffer of memory with more data than its buffer can hold. When the program begins to write beyond the end of the buffer, the program's execution path can be changed, or data can be written into areas used by the operating system itself. This can lead to the insertion of malicious code that can be used to gain administrative privileges on the program or system.
As explained by Gaurab, it can become very complex. At the time of input even if you are checking the length of the input, it has to be check against the buffer size. Consider a case where entry point of data is stored in Buffer1 of Application1 and then you copy it to Buffer2 within Application2 later on, if you are just checking the length of data against Buffer1, it will not ensure that it will not cause a buffer overflow in Buffer2 of Application2.
A bit of reassurance from the ISC2 book about level of Coding Knowledge needed for the exam:

It should be noted that the CISSP is not required to be an expert programmer or know the inner workings of developing application software code, like the FORTRAN programming language, or how to develop Web applet code using Java. It is not even necessary that the CISSP know detailed security-specific coding practices such as the major divisions of buffer overflow exploits or the reason for preferring str(n) cpy to strcpy in the C language (although all such knowledge is, of course, helpful). Because the CISSP may be the person responsible for ensuring that security is included in such developments, the CISSP should know the basic procedures and concepts involved during the design and development of software programming. That is, in order for the CISSP to monitor the software development process and verify that security is included, the CISSP must understand the fundamental concepts of programming developments and the security strengths and weaknesses of various application development processes.
The following are incorrect answers:
"Because buffers can only hold so much data" is incorrect. This is certainly true but is not the best answer because the finite size of the buffer is not the problem -- the problem is that the programmer did not check the size of the input before moving it into the buffer.
"Because they are an easy weakness to exploit" is incorrect. This answer is sometimes true but is not the best answer because the root cause of the buffer overflow is that the programmer did not check the size of the user input.
"Because of insufficient system memory" is incorrect. This is irrelevant to the occurrence of a buffer overflow.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 13319-13323). Auerbach Publications. Kindle Edition.

NEW QUESTION: 33
Crackers today are MOST often motivated by their desire to:
A. Help the community in securing their networks.
B. Seeing how far their skills will take them.
C. Getting recognition for their actions.
D. Gaining Money or Financial Gains.
Answer: D (LEAVE A REPLY)
A few years ago the best choice for this question would have been seeing how far their skills can take them. Today this has changed greatly, most crimes committed are financially motivated.
Profit is the most widespread motive behind all cybercrimes and, indeed, most crimes-everyone wants to make money. Hacking for money or for free services includes a smorgasbord of crimes such as embezzlement, corporate espionage and being a "hacker for hire". Scams are easier to undertake but the likelihood of success is much lower. Money-seekers come from any lifestyle but those with persuasive skills make better con artists in the same way as those who are exceptionally tech-savvy make better "hacks for hire".
"White hats" are the security specialists (as opposed to Black Hats) interested in helping the community in securing their networks. They will test systems and network with the owner authorization.

A Black Hat is someone who uses his skills for offensive purpose. They do not seek authorization before they attempt to comprise the security mechanisms in place.
"Grey Hats" are people who sometimes work as a White hat and other times they will work as a "Black Hat", they have not made up their mind yet as to which side they prefer to be.
The following are incorrect answers:
All the other choices could be possible reasons but the best one today is really for financial gains.
References used for this question:
http://library.thinkquest.org/04oct/00460/crimeMotives.html and
http://www.informit.com/articles/article.aspx?p=1160835 and http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C506938FE8BB53%7Dhtcb006.pdf

NEW QUESTION: 34
Another example of Computer Incident Response Team (CIRT) activities is:
A. Management of the netware logs, including collection, retention, review, and analysis of data
B. Management of the network logs, including collection and analysis of data
C. Management of the network logs, including review and analysis of data
D. Management of the network logs, including collection, retention, review, and analysis of data
Answer: D (LEAVE A REPLY)
Additional examples of CIRT activities are:
Management of the network logs, including collection, retention, review, and analysis of data
Management of the resolution of an incident, management of the remediation of a vulnerability, and post-event reporting to the appropriate parties. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 64.

NEW QUESTION: 35
What security control provides a method to insure that a transaction did or did not occur?
A. Identification
B. Accountability
C. Nonrepudiation
D. Verification
E. Access control
Answer: (SHOW ANSWER)
Nonrepudiation serves to validate whether or not a claimed event or action occurred in order to resolve disputes about the validity of the event. Nonrepudiation is vital in electronic commerce because it protects both the seller and the consumer from fraudulent behavior by the other party.

NEW QUESTION: 36
An area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability can be defined as:
A. Netware availability
B. Network availability

C. Network acceptability
D. Network accountability
Answer: B (LEAVE A REPLY)
Network availability can be defined as an area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 64.

NEW QUESTION: 37
Unshielded Twisted Pair (UTP) cables comes in several categories. The categories are based on:
A. The level of performance
B. How thick the shielding is.
C. The length of the cable
D. The diameter of the copper.
Answer: A (LEAVE A REPLY)
TIA/EIA-568 is a set of telecommunications standards from the Telecommunications Industry Association, an offshoot of the EIA. The standards address commercial building cabling for telecom products and services.
The standard is currently (2009) at revision C, replacing the 2001 revision B, the 1995 revision A, and the initial issue of 1991, which are now obsolete.
Perhaps the best known features of TIA/EIA-568 are the pin/pair assignments for eight-conductor 100-ohm balanced twisted pair cabling. These assignments are named T568A and T568B, and are frequently referred to (erroneously) as TIA/EIA-568A and TIA/EIA568B. An IEC standard ISO/IEC 11801 provides similar standards for network cables.
The standard defines categories of unshielded twisted pair cable systems, with different levels of performance in signal bandwidth, attenuation, and cross-talk. Generally increasing category numbers correspond with a cable system suitable for higher rates of data transmission. Category 3 cable was suitable for telephone circuits and data rates up to 16 million bits per second. Category 5 cable, with more restrictions on attenuation and cross talk, has a bandwidth of 100 MHz. The 1995 edition of the standard defined categories 3, 4, and 5. Categories 1 and 2 were excluded from the standard since these categories were only used for voice circuits, not for data.
Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs. It was invented by Alexander Graham Bell.
SOME OF THE LIMITATION OF UTP UTP has several drawbacks. Because it does not have shielding like shielded twisted-pair cables, UTP is susceptible to interference from external electrical sources, which could reduce the integrity of the signal. Also, to intercept transmitted data, an intruder can install a tap on the cable or monitor the radiation from the wire. Thus, UTP may not be a good choice when transmitting very sensitive data or when installed in an environment with much electromagnetic interference (EMI) or radio frequency interference (RFI). Despite its drawbacks, UTP is the most common

cable type. UTP is inexpensive, can be easily bent during installation, and, in most cases, the risk from the above drawbacks is not enough to justify more expensive cables.
Resource(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6507-6511). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/TIA/EIA-568#cite_note-7 http://en.wikipedia.org/wiki/Twisted_pair AIOv3 Telecommunication and Networking Security (page 455)

NEW QUESTION: 38
Total risk is defined as:
A. Threats * Vulnerability * Asset Control Gap = Total Risk
B. Threats * Vulnerability * Asset Replacement Cost = Total Risk
C. Threats * Estimated Downtime * Asset Value = Total Risk
D. Total Risk = Asset Value * Exposure
E. Threats * Vulnerability * Asset Value = Total Risk
Answer: (SHOW ANSWER)
(Threats * Vulnerability * Asset Value = Total Risk) is the formula used to calculate risk.

NEW QUESTION: 39
A confidential number used as an authentication factor to verify a user's identity is called a:
A. PIN
B. User ID
C. Password
D. Challenge
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
PIN Stands for Personal Identification Number, as the name states it is a combination of numbers.
The following answers are incorrect:
User ID This is incorrect because a Userid is not required to be a number and a Userid is only used to establish identity not verify it.
Password. This is incorrect because a password is not required to be a number, it could be any combination of characters.
Challenge. This is incorrect because a challenge is not defined as a number, it could be anything.

NEW QUESTION: 40
One purpose of a security awareness program is to modify:
A. employee's attitudes and behaviors towards enterprise's security posture
B. management's approach towards enterprise's security posture
C. attitudes of employees with sensitive data
D. corporate attitudes about safeguarding data

Answer: A (LEAVE A REPLY)

Explanation/Reference:

security awareness training is to modify employees behaviour and attitude towards towards enterprise's security posture.

Security-awareness training is performed to modify employees' behavior and attitude toward security. This can best be achieved through a formalized process of security-awareness training.

It is used to increase the overall awareness of security throughout the company. It is targeted to every single employee and not only to one group of users.

Unfortunately you cannot apply a patch to a human being, the only thing you can do is to educate employees and make them more aware of security issues and threats. Never underestimate human stupidity.

Reference(s) used for this question:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

also see:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 130). McGraw-Hill. Kindle Edition.

NEW QUESTION: 41

Which of the following statements pertaining to protection rings is false?

A. They provide strict boundaries and definitions on what the processes that work within each ring can access.

B. Programs operating in inner rings are usually referred to as existing in a privileged mode.

C. They support the CIA triad requirements of multitasking operating systems.

D. They provide users with a direct access to peripherals

Answer: (SHOW ANSWER)

Explanation/Reference:

In computer science, hierarchical protection domains, often called protection rings, are mechanisms to protect data and functionality from faults (fault tolerance) and malicious behaviour (computer security). This approach is diametrically opposite to that of capability-based security.

Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level.

Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.

Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be

prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.
"They provide strict boundaries and definitions on what the processes that work within each ring can access" is incorrect. This is in fact one of the characteristics of a ring protection system.
"Programs operating in inner rings are usually referred to as existing in a privileged mode" is incorrect. This is in fact one of the characteristics of a ring protection system.
"They support the CIA triad requirements of multitasking operating systems" is incorrect. This is in fact one of the characteristics of a ring protection system.
Reference(s) used for this question:
CBK, pp. 310-311
AIO3, pp. 253-256
AIOv4 Security Architecture and Design (pages 308 - 310)
AIOv5 Security Architecture and Design (pages 309 - 312)

NEW QUESTION: 42
Brute force attacks against encryption keys have increased in potency because of increased computing power. Which of the following is often considered a good protection against the brute force cryptography attack?
A. The use of good key generators.
B. The use of session keys.
C. Nothing can defend you against a brute force crypto key attack.
D. Algorithms that are immune to brute force key attacks.
Answer: B (LEAVE A REPLY)
If we assume a crytpo-system with a large key (and therefore a large key space) a brute force attack will likely take a good deal of time - anywhere from several hours to several years depending on a number of variables. If you use a session key for each message you encrypt, then the brute force attack provides the attacker with only the key for that one message. So, if you are encrypting 10 messages a day, each with a different session key, but it takes me a month to break each session key then I am fighting a loosing battle.
The other answers are not correct because:
"The use of good key generators" is not correct because a brute force key attack will eventually run through all possible combinations of key. Therefore, any key will eventually be broken in this manner given enough time.
"Nothing can defend you against a brute force crypto key attack" is incorrect, and not the best answer listed. While it is technically true that any key will eventually be broken by a brute force attack, the question remains "how long will it take?". In other words, if you encrypt something today but I can't read it for 10,000 years, will you still care? If the key is changed every session does it matter if it can be broken after the session has ended? Of the answers listed here, session keys are "often considered a good protection against the brute force cryptography attack" as the question asks.

"Algorithms that are immune to brute force key attacks" is incorrect because there currently are no such algorithms.
References:
Official ISC2 Guide page: 259
All in One Third Edition page: 623

NEW QUESTION: 43
Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?
A. Degaussing
B. Parity Bit Manipulation
C. Zeroization
D. Buffer overflow
Answer: A (LEAVE A REPLY)
A "Degausser (Otherwise known as a Bulk Eraser) has the main function of reducing to near zero the magnetic flux stored in the magnetized medium. Flux density is measured in Gauss or Tesla. The operation is speedier than overwriting and done in one short operation. This is achieved by subjecting the subject in bulk to a series of fields of alternating polarity and gradually decreasing strength.
The following answers are incorrect:Parity Bit Manipulation. Parity has to do with disk lerror detection, not data removal. A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the infromation that was sent.
Zeroization. Zeroization involves overwrting data to sanitize it. It is time-consuming and not foolproof. The potential of restoration of data does exist with this method. Buffer overflow. This is a detractor. Although many Operating Systems use a disk buffer to temporarily hold data read from disk, its primary purpose has no connection to data removal. An overflow goes outside the constraints defined for the buffer and is a method used by an attacker to attempt access to a system.
The following reference(s) were/was used to create this question:
Shon Harris AIO v3. pg 908 Reference: What is degaussing.

NEW QUESTION: 44
Which type of attack involves impersonating a user or a system?
A. Smurfing attack
B. Spoofing attack
C. Spamming attack
D. Sniffing attack
Answer: B (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
A spoofing attack is when an attempt is made to gain access to a computer system by posing as an authorized user or system. Spamming refers to sending out or posting junk advertising and unsolicited

mail. A smurf attack is a type of denial-of-service attack using PING and a spoofed address. Sniffing refers to observing packets passing on a network.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
77).

NEW QUESTION: 45
Which of the following was developed by the National Computer Security Center (NCSC) for the US Department of Defense ?
A. TCSEC
B. ITSEC
C. DIACAP
D. NIACAP
E. Explanation:
The
Answer: A (LEAVE A REPLY)
; The TCSEC, frequently referred to as the Orange
Book, is the centerpiece of the DoD Rainbow Series publications.
Initially issued by the National Computer Security Center (NCSC) an arm of the National Security Agency in 1983 and then updated in 1985, TCSEC was replaced with the development of the Common Criteria international standard originally published in 2005.
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 197-199.
Wikepedia
http://en.wikipedia.org/wiki/TCSEC

NEW QUESTION: 46
The session layer provides a logical persistent connection between peer hosts. Which of the following is one of the modes used in the session layer to establish this connection?
A. Full duplex
B. Synchronous
C. Asynchronous
D. Half simplex
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
Layer 5 of the OSI model is the Session Layer. This layer provides a logical persistent connection between peer hosts. A session is analogous to a conversation that is necessary for applications to exchange information.

The session layer is responsible for establishing, managing, and closing end-to-end connections, called sessions, between applications located at different network endpoints. Dialogue control management provided by the session layer includes full-duplex, half-duplex, and simplex communications. Session layer management also helps to ensure that multiple streams of data stay synchronized with each other, as in the case of multimedia applications like video conferencing, and assists with the prevention of application related data errors.
The session layer is responsible for creating, maintaining, and tearing down the session.
Three modes are offered:
(Full) Duplex: Both hosts can exchange information simultaneously, independent of each other.
Half Duplex: Hosts can exchange information, but only one host at a time.
Simplex: Only one host can send information to its peer. Information travels in one direction only.
Another aspect of performance that is worthy of some attention is the mode of operation of the network or connection. Obviously, whenever we connect together device A and device B, there must be some way for A to send to B and B to send to A. Many people don't realize, however, that networking technologies can differ in terms of how these two directions of communication are handled. Depending on how the network is set up, and the characteristics of the technologies used, performance may be improved through the selection of performance-enhancing modes.
Basic Communication Modes of Operation
Let's begin with a look at the three basic modes of operation that can exist for any network connection, communications channel, or interface.
Simplex Operation
In simplex operation, a network cable or communications channel can only send information in one direction; it's a "one-way street". This may seem counter-intuitive: what's the point of communications that only travel in one direction? In fact, there are at least two different places where simplex operation is encountered in modern networking.
The first is when two distinct channels are used for communication: one transmits from A to B and the other from B to A. This is surprisingly common, even though not always obvious. For example, most if not all fiber optic communication is simplex, using one strand to send data in each direction. But this may not be obvious if the pair of fiber strands are combined into one cable.
Simplex operation is also used in special types of technologies, especially ones that are asymmetric. For example, one type of satellite Internet access sends data over the satellite only for downloads, while a regular dial-up modem is used for upload to the service provider. In this case, both the satellite link and the dial-up connection are operating in a simplex mode.
Half-Duplex Operation
Technologies that employ half-duplex operation are capable of sending information in both directions between two nodes, but only one direction or the other can be utilized at a time. This is a fairly common mode of operation when there is only a single network medium (cable, radio frequency and so forth) between devices.
While this term is often used to describe the behavior of a pair of devices, it can more generally refer to any number of connected devices that take turns transmitting. For example, in conventional Ethernet networks, any device can transmit, but only one may do so at a time. For this reason, regular

(unswitched) Ethernet networks are often said to be "half-duplex", even though it may seem strange to describe a LAN that way.
Full-Duplex Operation
In full-duplex operation, a connection between two devices is capable of sending data in both directions simultaneously. Full-duplex channels can be constructed either as a pair of simplex links (as described above) or using one channel designed to permit bidirectional simultaneous transmissions. A full-duplex link can only connect two devices, so many such links are required if multiple devices are to be connected together.
Note that the term "full-duplex" is somewhat redundant; "duplex" would suffice, but everyone still says "full- duplex" (likely, to differentiate this mode from half-duplex).
For a listing of protocols associated with Layer 5 of the OSI model, see below:
ADSP - AppleTalk Data Stream Protocol
ASP - AppleTalk Session Protocol
H.245 - Call Control Protocol for Multimedia Communication
ISO-SP
OSI session-layer protocol (X.225, ISO 8327)
iSNS - Internet Storage Name Service
The following are incorrect answers:
Synchronous and Asynchronous are not session layer modes.
Half simplex does not exist. By definition, simplex means that information travels one way only, so half-simplex is a oxymoron.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 5603-5636). Auerbach Publications. Kindle Edition.
and
http://www.tcpipguide.com/free/t_SimplexFullDuplexandHalfDuplexOperation.htm and
http://www.wisegeek.com/what-is-a-session-layer.htm

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 47
Who of the following is responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data?
A. Business and functional managers
B. IT Security practitioners

C. System and information owners
D. Chief information officer
Answer: (SHOW ANSWER)
The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. IT security practitioners are responsible for proper implementation of security requirements in their IT systems. Source: STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 6).

NEW QUESTION: 48
Which of the following OSI layers provides routing and related services?
A. Network Layer
B. Presentation Layer
C. Session Layer
D. Physical Layer
Answer: A (LEAVE A REPLY)
The Network Layer performs network routing functions.
The following answers are incorrect:
Presentation Layer. Is incorrect because the Presentation Layer transforms the data to provide a standard interface for the Application layer.
Session Layer. Is incorrect because the Session Layer controls the dialogues/connections (sessions) between computers.
Physical Layer. is incorrect because the Physical Layer defines all the electrical and physical specifications for devices.

NEW QUESTION: 49
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?
A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
C. They both involve rewriting the media.
D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.
Answer: B (LEAVE A REPLY)
The removal of information from a storage medium is called sanitization.
Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack).
There are three general methods of purging media: overwriting, degaussing, and

destruction.
There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.
Reference(s) use for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 26).
and
A guide to understanding Data Remanence in Automated Information Systems

NEW QUESTION: 50
Which protocol is used to send email?
A. File Transfer Protocol (FTP).
B. Post Office Protocol (POP).
C. Network File System (NFS).
D. Simple Mail Transfer Protocol (SMTP).
Answer: D (LEAVE A REPLY)
Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. POP is a protocol used to retrieve e-mail from a mail server. NFS is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture. FTP is the protocol that is used to facilitate file transfer between two machines.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

NEW QUESTION: 51
Related to information security, the prevention of the intentional or unintentional unauthorized disclosure of contents is which of the following?
A. Confidentiality
B. Integrity
C. Availability
D. capability
Answer: (SHOW ANSWER)
Confidentiality is the prevention of the intentional or unintentional
unauthorized disclosure of contents.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the

Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 60.

NEW QUESTION: 52
Which of the following is a not a preventative control?
A. Deny programmer access to production data.
B. Require change requests to include information about dates, descriptions, cost analysis and anticipated effects.
C. Run a source comparison program between control and current source periodically.
D. Establish procedures for emergency changes.
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Running the source comparison program between control and current source periodically allows detection, not prevention, of unauthorized changes in the production environment. Other options are preventive controls.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

NEW QUESTION: 53
Who should DECIDE how a company should approach security and what security measures should be implemented?
A. Senior management
B. Data owner
C. Auditor
D. The information security specialist
Answer: A (LEAVE A REPLY)
They are responsible for security of the organization and the protection of its assets.
The following answers are incorrect because :
Data owner is incorrect as data owners should not decide as to what security measures should be applied.
Auditor is also incorrect as auditor cannot decide as to what security measures should be applied.
The information security specialist is also incorrect as they may have the technical knowledge of how security measures should be implemented and configured , but they
should not be in a position of deciding what measures should be applied.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 51.

NEW QUESTION: 54
Virus scanning and content inspection of SMIME encrypted e-mail without doing any further processing is:
A. Not possible

B. Only possible with key recovery scheme of all user keys
C. It is possible only if X509 Version 3 certificates are used
D. It is possible only by "brute force" decryption
Answer: A (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
Content security measures presumes that the content is available in cleartext on the central mail server. Encrypted emails have to be decrypted before it can be filtered (e.g. to detect viruses), so you need the decryption key on the central "crypto mail server".
There are several ways for such key management, e.g. by message or key recovery methods. However, that would certainly require further processing in order to achieve such goal.

NEW QUESTION: 55
Who is responsible for providing reports to the senior management on the effectiveness of the security controls?
A. Information systems security professionals
B. Data owners
C. Data custodians
D. Information systems auditors
Answer: D (LEAVE A REPLY)
IT auditors determine whether systems are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction and other requirements" and "provide top company management with an independent view of the controls that have been designed and their effectiveness."
"Information systems security professionals" is incorrect. Security professionals develop the security policies and supporting baselines, etc.
"Data owners" is incorrect. Data owners have overall responsibility for information assets and assign the appropriate classification for the asset as well as ensure that the asset is protected with the proper controls.
"Data custodians" is incorrect. Data custodians care for an information asset on behalf of the data owner.
References:
CBK, pp. 38 - 42. AIO3. pp. 99 - 104

NEW QUESTION: 56
Which of the following encryption methods is known to be unbreakable?
A. Symmetric ciphers.
B. DES codebooks.
C. One-time pads.
D. Elliptic Curve Cryptography.
Answer: (SHOW ANSWER)
Section: Cryptography

Explanation/Reference:
A One-Time Pad uses a keystream string of bits that is generated completely at random that is used only once.
Because it is used only once it is considered unbreakable.
The following answers are incorrect:
Symmetric ciphers. This is incorrect because a Symmetric Cipher is created by substitution and transposition.
They can and have been broken
DES codebooks. This is incorrect because Data Encryption Standard (DES) has been broken, it was replaced by Advanced Encryption Standard (AES).
Elliptic Curve Cryptography. This is incorrect because Elliptic Curve Cryptography or ECC is typically used on wireless devices such as cellular phones that have small processors. Because of the lack of processing power the keys used at often small. The smaller the key, the easier it is considered to be breakable. Also, the technology has not been around long enough or tested thourough enough to be considered truly unbreakable.

NEW QUESTION: 57
Which of the following is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length?
A. Fiber Optic cable
B. Coaxial cable
C. Twisted Pair cable
D. Axial cable
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Fiber Optic cable is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length (up to two kilometers in some cases).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

NEW QUESTION: 58
BIA - Business Impact Analysis deals strictly with financial assessment of a loss in relation to business operations?
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
Configuration Management controls what?
A. Auditing of changes to the Trusted Computing Base.

B. Control of changes to the Trusted Computing Base.
C. Changes in the configuration access to the Trusted Computing Base.
D. Auditing and controlling any changes to the Trusted Computing Base.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
All of these are components of Configuration Management.
The following answers are incorrect:
Auditing of changes to the Trusted Computing Base. Is incorrect because it refers only to auditing the changes, but nothing about controlling them.
Control of changes to the Trusted Computing Base. Is incorrect because it refers only to controlling the changes, but nothing about ensuring the changes will not lead to a weakness or fault in the system.
Changes in the configuration access to the Trusted Computing Base. Is incorrect because this does not refer to controlling the changes or ensuring the changes will not lead to a weakness or fault in the system.

NEW QUESTION: 60
Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?
A. Bridge
B. Repeater
C. Router
D. Gateway
Answer: D (LEAVE A REPLY)
A gateway is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.
Important Note:
For the purpose of the exam, you have to remember that a gateway is not synonymous to the term firewall.
The second thing you must remembers is the fact that a gateway act as a translation device.
It could be used to translate from IPX to TCP/IP for example. It could be used to convert different types of applications protocols and allow them to communicate together. A gateway could be at any of the OSI layers but usually tend to be higher up in the stack.
For your exam you should know the information below:
Repeaters
A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel. Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes

extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal. A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

Repeater

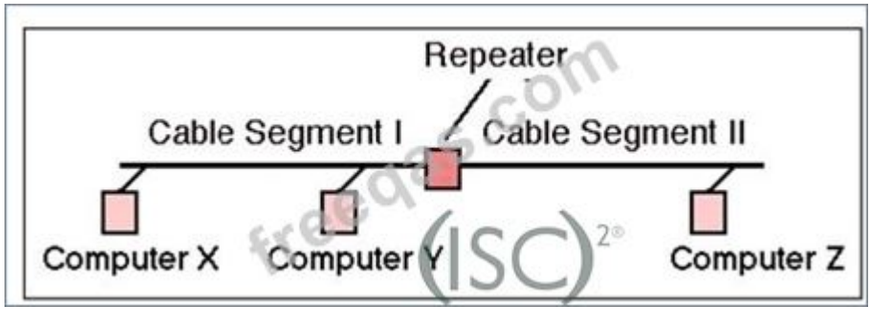


Image Reference- http://www.erg.abdn.ac.uk/~gorry/course/images/repeater.gif

Bridges A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge C:\Users\MCS\Desktop\1.jpg

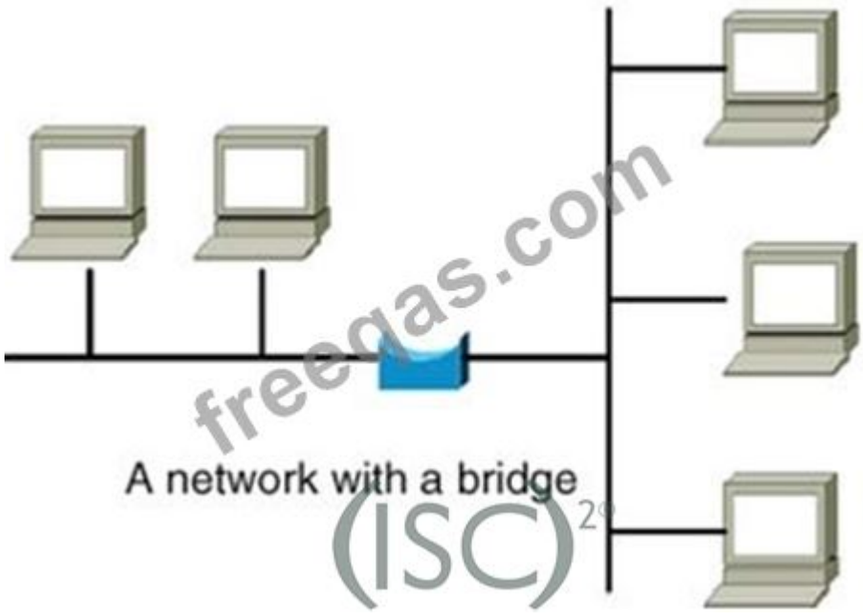


Image Reference- http://www.oreillynet.com/network/2001/01/30/graphics/bridge.jpg

Routers Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when

necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch

Image Reference- http://www.computer-networking-success.com/images/router-switch.jpg

Switches Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

Gateways Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server C:\Users\MCS\Desktop\1.jpg

Image Referencehttp://static.howtoforge.com/images/screenshots/556af08d5e43aa768260f9e589dc547f3024.jpg
The following answers are incorrect:
Repeater - A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.
Bridges - A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.
Routers - Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary.
Following reference(s) were/was used to create this question: CISA review manual 2014 Page number 263 Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and 230

NEW QUESTION: 61
What kind of Encryption technology does SSL utilize?
A. Secret or Symmetric key
B. Hybrid (both Symmetric and Asymmetric)

C. Public Key
D. Private key
Answer: (SHOW ANSWER)
SSL use public-key cryptography to secure session key, while the session key (secret key) is used to secure the whole session taking place between both parties communicating with each other.
The SSL protocol was originally developed by Netscape. Version 1.0 was never publicly released; version 2.0 was released in February 1995 but "contained a number of security flaws which ultimately led to the design of SSL version 3.0." SSL version 3.0, released in 1996, was a complete redesign of the protocol produced by Paul Kocher working with Netscape engineers Phil Karlton and Alan Freier.
All of the other answers are incorrect

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 62
This type of supporting evidence is used to help prove an idea or a point, however It cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. What is the name of this type of evidence?
A. Circumstantial evidence
B. Corroborative evidence
C. Opinion evidence
D. Secondary evidence
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
This type of supporting evidence is used to help prove an idea or a point, however It cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. Corrobative evidence takes many forms.
In a rape case for example, this could consist of torn clothing, soiled bed sheets, 911 emergency calls tapes, and prompt complaint witnesses.
There are many types of evidence that exist. Below you have explanations of some of the most common types:
Physical Evidence
Physical evidence is any evidence introduced in a trial in the form of a physical object, intended to prove a fact in issue based on its demonstrable physical characteristics. Physical evidence can conceivably include all or part of any object.

In a murder trial for example (or a civil trial for assault), the physical evidence might include DNA left by the attacker on the victim's body, the body itself, the weapon used, pieces of carpet spattered with blood, or casts of footprints or tire prints found at the scene of the crime.

Real Evidence

Real evidence is a type of physical evidence and consists of objects that were involved in a case or actually played a part in the incident or transaction in question.

Examples include the written contract, the defective part or defective product, the murder weapon, the gloves used by an alleged murderer. Trace evidence, such as fingerprints and firearm residue, is a species of real evidence. Real evidence is usually reported upon by an expert witness with appropriate qualifications to give an opinion. This normally means a forensic scientist or one qualified in forensic engineering.

Admission of real evidence requires authentication, a showing of relevance, and a showing that the object is in

"the same or substantially the same condition" now as it was on the relevant date. An object of real evidence is authenticated through the senses of witnesses or by circumstantial evidence called chain of custody.

Documentary

Documentary evidence is any evidence introduced at a trial in the form of documents. Although this term is most widely understood to mean writings on paper (such as an invoice, a contract or a will), the term actually include any media by which information can be preserved. Photographs, tape recordings, films, and printed emails are all forms of documentary evidence.

Documentary versus physical evidence

A piece of evidence is not documentary evidence if it is presented for some purpose other than the examination of the contents of the document. For example, if a blood-spattered letter is introduced solely to show that the defendant stabbed the author of the letter from behind as it was being written, then the evidence is physical evidence, not documentary evidence. However, a film of the murder taking place would be documentary evidence (just as a written description of the event from an eyewitness). If the content of that same letter is then introduced to show the motive for the murder, then the evidence would be both physical and documentary.

Documentary Evidence Authentication

Documentary evidence is subject to specific forms of authentication, usually through the testimony of an eyewitness to the execution of the document, or to the testimony of a witness able to identify the handwriting of the purported author. Documentary evidence is also subject to the best evidence rule, which requires that the original document be produced unless there is a good reason not to do so.

The role of the expert witness

Where physical evidence is of a complexity that makes it difficult for the average person to understand its significance, an expert witness may be called to explain to the jury the proper interpretation of the evidence at hand.

Digital Evidence or Electronic Evidence

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files.

While many courts in the United States have applied the Federal Rules of Evidence to digital evidence in the same way as more traditional documents, courts have noted very important differences. As compared to the more traditional evidence, courts have noted that digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive, and more readily available. As such, some courts have sometimes treated digital evidence differently for purposes of authentication, hearsay, the best evidence rule, and privilege. In December 2006, strict new rules were enacted within the Federal Rules of Civil Procedure requiring the preservation and disclosure of electronically stored evidence.

Demonstrative Evidence

Demonstrative evidence is evidence in the form of a representation of an object. This is, as opposed to, real evidence, testimony, or other forms of evidence used at trial.

Examples of demonstrative evidence include photos, x-rays, videotapes, movies, sound recordings, diagrams, forensic animation, maps, drawings, graphs, animation, simulations, and models. It is useful for assisting a finder of fact (fact-finder) in establishing context among the facts presented in a case. To be admissible, a demonstrative exhibit must "fairly and accurately" represent the real object at the relevant time.

Chain of custody

Chain of custody refers to the chronological documentation, and/or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.

The idea behind recoding the chain of custody is to establish that the alleged evidence is fact related to the alleged crime - rather than, for example, having been planted fraudulently to make someone appear guilty.

Establishing the chain of custody is especially important when the evidence consists of fungible goods. In practice, this most often applies to illegal drugs which have been seized by law enforcement personnel. In such cases, the defendant at times disclaims any knowledge of possession of the controlled substance in question.

Accordingly, the chain of custody documentation and testimony is presented by the prosecution to establish that the substance in evidence was in fact in the possession of the defendant.

An identifiable person must always have the physical custody of a piece of evidence. In practice, this means that a police officer or detective will take charge of a piece of evidence, document its collection, and hand it over to an evidence clerk for storage in a secure place. These transactions, and every succeeding transaction between the collection of the evidence and its appearance in court, should be completely documented chronologically in order to withstand legal challenges to the authenticity of the

evidence. Documentation should include the conditions under which the evidence is gathered, the identity of all evidence handlers, duration of evidence custody, security conditions while handling or storing the evidence, and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).
Example
An example of "Chain of Custody" would be the recovery of a bloody knife at a murder scene:
Officer Andrew collects the knife and places it into a container, then gives it to forensics technician Bill.
Forensics technician Bill takes the knife to the lab and collects fingerprints and other evidence from the knife.
Bill then gives the knife and all evidence gathered from the knife to evidence clerk Charlene. Charlene then stores the evidence until it is needed, documenting everyone who has accessed the original evidence (the knife, and original copies of the lifted fingerprints).
The Chain of Custody requires that from the moment the evidence is collected, every transfer of evidence from person to person be documented and that it be provable that nobody else could have accessed that evidence.
It is best to keep the number of transfers as low as possible.
In the courtroom, if the defendant questions the Chain of Custody of the evidence it can be proven that the knife in the evidence room is the same knife found at the crime scene. However, if there are discrepancies and it cannot be proven who had the knife at a particular point in time, then the Chain of Custody is broken and the defendant can ask to have the resulting evidence declared inadmissible.
"Chain of custody" is also used in most chemical sampling situations to maintain the integrity of the sample by providing documentation of the control, transfer, and analysis of samples. Chain of custody is especially important in environmental work where sampling can identify the existence of contamination and can be used to identify the responsible party.
REFERENCES:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 23173-23185). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Documentary_evidence
http://en.wikipedia.org/wiki/Physical_evidence
http://en.wikipedia.org/wiki/Digital_evidence
http://en.wikipedia.org/wiki/Demonstrative_evidence
http://en.wikipedia.org/wiki/Real_evidence
http://en.wikipedia.org/wiki/Chain_of_custody

NEW QUESTION: 63
During which phase of an IT system life cycle are security requirements developed?
A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation
Answer: C (LEAVE A REPLY)

The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems.
The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:
This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:
Conduct the risk assessment and use the results to supplement the baseline security controls;
Analyze security requirements;
Perform functional and security testing;
Prepare initial documents for system certification and accreditation; and
Design security architecture.
Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.
Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:
Project initiation Functional design analysis and planning System design specifications Software development Installation Maintenance support Revision and replacement
According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase.
SDLC POSITIONING FROM NIST 800-64

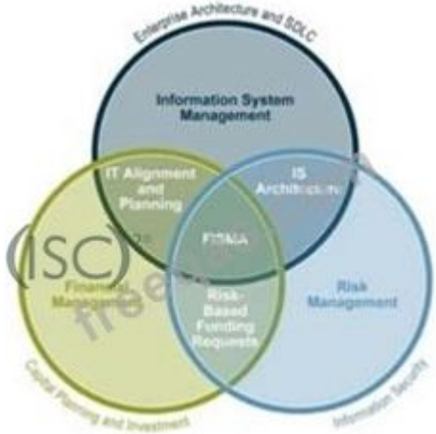


FIGURE 2-1. POSITIONING SECURITY CONSIDERATIONS

SDLC Positioning in the enterprise Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of

information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency's vital business operations, their supporting assets, and existing interdependencies and relationships.

With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program's cost-effective performance as well as articulate its business impact and value to the agency.

SDLC OVERVIEW FROM NIST 800-64 SDLC Overview from NIST 800-64 Revision 2

NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at:

http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf

DISCUSSION:

Different sources present slightly different info as far as the phases names are concerned. People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.

NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice.

Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:

The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.

At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage. By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.
NIST says: NIST`s Information Technology Laboratory recently issued Special Publication (SP) 80064, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.
I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956 and NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64Revision2.pdf and http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlcsystem-development

NEW QUESTION: 64
In an online transaction processing system (OLTP), which of the following actions should be taken when erroneous or invalid transactions are detected?
A. The transactions should be dropped from processing.
B. The transactions should be processed after the program makes adjustments.
C. The transactions should be written to a report and reviewed.
D. The transactions should be corrected and reprocessed.
Answer: C (LEAVE A REPLY)
In an online transaction processing system (OLTP) all transactions are recorded as they occur. When erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.
As explained in the ISC2 OIG: OLTP is designed to record all of the business transactions of an organization as they occur. It is a data processing system facilitating and managing transaction-oriented applications. These are characterized as a system used by many concurrent users who are actively adding and modifying data to effectively change real-time data.
OLTP environments are frequently found in the finance, telecommunications, insurance, retail, transportation, and travel industries. For example, airline ticket agents enter data in the database in real-time by creating and modifying travel reservations, and these are increasingly joined by users directly making their own reservations and purchasing tickets through airline company Web sites as well as discount travel Web site portals. Therefore, millions of people may be accessing the same flight database every day, and dozens of people may be looking at a specific flight at the same time.
The security concerns for OLTP systems are concurrency and atomicity.
Concurrency controls ensure that two users cannot simultaneously change the same data, or that one user cannot make changes before another user is finished with it. In an airline ticket system, it is critical for an agent processing a reservation to complete the transaction, especially if it is the last seat available on the plane.

Atomicity ensures that all of the steps involved in the transaction complete successfully. If one step should fail, then the other steps should not be able to complete. Again, in an airline ticketing system, if the agent does not enter a name into the name data field correctly, the transaction should not be able to complete.

OLTP systems should act as a monitoring system and detect when individual processes abort, automatically restart an aborted process, back out of a transaction if necessary, allow distribution of multiple copies of application servers across machines, and perform dynamic load balancing.

A security feature uses transaction logs to record information on a transaction before it is processed, and then mark it as processed after it is done. If the system fails during the transaction, the transaction can be recovered by reviewing the transaction logs.

Checkpoint restart is the process of using the transaction logs to restart the machine by running through the log to the last checkpoint or good transaction. All transactions following the last checkpoint are applied before allowing users to access the data again.

Wikipedia has nice coverage on what is OLTP:

Online transaction processing, or OLTP, refers to a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval transaction processing. The term is somewhat ambiguous; some understand a "transaction" in the context of computer or database transactions, while others (such as the Transaction Processing Performance Council) define it in terms of business or commercial transactions. OLTP has also been used to refer to processing in which the system responds immediately to user requests. An automatic teller machine (ATM) for a bank is an example of a commercial transaction processing application.

The technology is used in a number of industries, including banking, airlines, mailorder, supermarkets, and manufacturing. Applications include electronic banking, order processing, employee time clock systems, e-commerce, and eTrading.

There are two security concerns for OLTP system: Concurrency and Atomicity

ATOMICITY

In database systems, atomicity (or atomicness) is one of the ACID transaction properties. In an atomic transaction, a series of database operations either all occur, or nothing occurs. A guarantee of atomicity prevents updates to the database occurring only partially, which can cause greater problems than rejecting the whole series outright.

The etymology of the phrase originates in the Classical Greek concept of a fundamental and indivisible component; see atom.

An example of atomicity is ordering an airline ticket where two actions are required: payment, and a seat reservation. The potential passenger must either:

both pay for and reserve a seat; OR

neither pay for nor reserve a seat.

The booking system does not consider it acceptable for a customer to pay for a ticket without securing the seat, nor to reserve the seat without payment succeeding.

CONCURRENCY

Database concurrency controls ensure that transactions occur in an ordered fashion.
The main job of these controls is to protect transactions issued by different users/applications from the effects of each other. They must preserve the four characteristics of database transactions ACID test: Atomicity, Consistency, Isolation, and Durability. Read http://en.wikipedia.org/wiki/ACID for more details on the ACID test.
Thus concurrency control is an essential element for correctness in any system where two database transactions or more, executed with time overlap, can access the same data, e.g., virtually in any general-purpose database system. A well established concurrency control theory exists for database systems: serializability theory, which allows to effectively design and analyze concurrency control methods and mechanisms.
Concurrency is not an issue in itself, it is the lack of proper concurrency controls that makes it a serious issue.
The following answers are incorrect:
The transactions should be dropped from processing. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.
The transactions should be processed after the program makes adjustments. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.
The transactions should be corrected and reprocessed. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.
References:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12749-12768). Auerbach Publications. Kindle Edition. and
http://en.wikipedia.org/wiki/Online_transaction_processing and
http://databases.about.com/od/administration/g/concurrency.htm

NEW QUESTION: 65
Which of the following would be true about Static password tokens?
A. The owner identity is authenticated by the token
B. The owner will never be authenticated by the token.
C. The owner will authenticate himself to the system.
D. The token does not authenticates the token owner but the system.
Answer: A (LEAVE A REPLY)
Password Tokens Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a dynamic system the user will often have to log themselves in.
Static Password Tokens: The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated

by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room.
Synchronous Dynamic Password Tokens:
This system is a lot more complex then the static token password. The synchronous dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring. Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have troubles authenticating themselves to the system.
Asynchronous Dynamic Password Tokens:
The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principal as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the companies VPN (Virtual private Network).
Challenge Response Tokens:
This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals. The user inputs this challenge string into their token device and the device will respond by generating a challenge response. The user then types this response into the system and if it is correct they are authenticated.
Reference(s) used for this question:
http://www.informit.com/guides/content.aspx?g=security&seqNum=146
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION: 66
In the statement below, fill in the blank:
Law enforcement agencies must get a warrant to search and seize an individual's property, as stated in the
_____ Amendment.
A. First.
B. Second.
C. Third.
D. Fourth.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
The Fourth Amendment does not apply to a seizure or an arrest by private citizens.
Search and seizure activities can get tricky depending on what is being searched for and where.

For example, American citizens are protected by the Fourth Amendment against unlawful search and seizure, so law enforcement agencies must have probable cause and request a search warrant from a judge or court before conducting such a search.
The actual search can only take place in the areas outlined by the warrant. The Fourth Amendment does not apply to actions by private citizens unless they are acting as police agents. So, for example, if Kristy's boss warned all employees that the management could remove files from their computers at any time, and her boss was not a police officer or acting as a police agent, she could not successfully claim that her Fourth Amendment rights were violated. Kristy's boss may have violated some specific privacy laws, but he did not violate Kristy's Fourth Amendment rights.
In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction.
This is referred to as exigent circumstances, and a judge will later decide whether the seizure was proper and legal before allowing the evidence to be admitted. For example, if a police officer had a search warrant that allowed him to search a suspect's living room but no other rooms, and then he saw the suspect dumping cocaine down the toilet, the police officer could seize the cocaine even though it was in a room not covered under his search warrant. After evidence is gathered, the chain of custody needs to be enacted and enforced to make sure the evidence's integrity is not compromised.
All other choices were only detractors.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1057). McGraw-Hill. Kindle Edition.

NEW QUESTION: 67
Which of the following statements pertaining to Secure Sockets Layer (SSL) is false?
A. The SSL protocol was developed by Netscape to secure Internet client-server transactions.
B. The SSL protocol's primary use is to authenticate the client to the server using public key cryptography and digital certificates.
C. Web pages using the SSL protocol start with HTTPS
D. SSL can be used with applications such as Telnet, FTP and email protocols.
Answer: B (LEAVE A REPLY)
All of these statements pertaining to SSL are true except that it is primary use is to authenticate the client to the server using public key cryptography and digital certificates. It is the opposite, Its primary use is to authenticate the server to the client.
The following reference(s) were used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 170).

NEW QUESTION: 68

In the statement below, fill in the blank:
Law enforcement agencies must get a warrant to search and seize an individual's property, as stated in the
_____ Amendment.
A. First.
B. Second.
C. Third.
D. Fourth.
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The Fourth Amendment does not apply to a seizure or an arrest by private citizens.
Search and seizure activities can get tricky depending on what is being searched for and where.
For example, American citizens are protected by the Fourth Amendment against unlawful search and seizure, so law enforcement agencies must have probable cause and request a search warrant from a judge or court before conducting such a search.
The actual search can only take place in the areas outlined by the warrant. The Fourth Amendment does not apply to actions by private citizens unless they are acting as police agents. So, for example, if Kristy's boss warned all employees that the management could remove files from their computers at any time, and her boss was not a police officer or acting as a police agent, she could not successfully claim that her Fourth Amendment rights were violated. Kristy's boss may have violated some specific privacy laws, but he did not violate Kristy's Fourth Amendment rights.
In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction. This is referred to as exigent circumstances, and a judge will later decide whether the seizure was proper and legal before allowing the evidence to be admitted. For example, if a police officer had a search warrant that allowed him to search a suspect's living room but no other rooms, and then he saw the suspect dumping cocaine down the toilet, the police officer could seize the cocaine even though it was in a room not covered under his search warrant. After evidence is gathered, the chain of custody needs to be enacted and enforced to make sure the evidence's integrity is not compromised.
All other choices were only detractors.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1057). McGraw-Hill. Kindle Edition.

NEW QUESTION: 69
Which of the following encryption algorithms does not deal with discrete logarithms?
A. El Gamal
B. Diffie-Hellman
C. RSA

D. Elliptic Curve

Answer: (SHOW ANSWER)

Explanation/Reference:

The security of the RSA system is based on the assumption that factoring the product into two original large prime numbers is difficult

Source:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 159).

Shon Harris, CISSP All-in-One Examine Guide, Third Edition, McGraw-Hill Companies, August 2005, Chapter 8: Cryptography, Page 636 - 639

NEW QUESTION: 70

Which of the following rules is least likely to support the concept of least privilege?

A. The number of administrative accounts should be kept to a minimum.

B. Administrators should use regular accounts when performing routine operations like reading mail.

C. Permissions on tools that are likely to be used by hackers should be as restrictive as possible.

D. Only data to and from critical systems and applications should be allowed through the firewall.

Answer: (SHOW ANSWER)

Only data to and from critical systems and applications should be allowed through the firewall is a detractor. Critical systems or applications do not necessarily need to have traffic go through a firewall. Even if they did, only the minimum required services should be allowed. Systems that are not deemed critical may also need to have traffic go through the firewall.

Least privilege is a basic tenet of computer security that means users should be given only those rights required to do their jobs or tasks. Least privilege is ensuring that you have the minimum privileges necessary to do a task. An admin NOT using his admin account to check email is a clear example of this.

Reference(s) used for this question:

National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 9.

NEW QUESTION: 71

Which of the following would be the best reason for separating the test and development environments?

A. To restrict access to systems under test.

B. To control the stability of the test environment.

C. To segregate user and development staff.

D. To secure access to systems under development.

Answer: B (LEAVE A REPLY)

Explanation/Reference:

The test environment must be controlled and stable in order to ensure that development projects are tested in a realistic environment which, as far as possible, mirrors the live environment.

Reference(s) used for this question:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

NEW QUESTION: 72
What enables users to validate each other's certificate when they are certified under different certification hierarchies?
A. Cross-certification
B. Multiple certificates
C. Redundant certification authorities
D. Root certification authorities
Answer: (SHOW ANSWER)
Cross-certification is the act or process by which two CAs each certifiy a public key of the other, issuing a public-key certificate to that other CA, enabling users that are certified under different certification hierarchies to validate each other's certificate. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 73
A momentary high voltage is a:
A. spike
B. blackout
C. surge
D. fault
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Too much voltage for a short period of time is a spike.
Too much voltage for a long period of time is a surge.
Not enough voltage for a short period of time is a sag or dip
Not enough voltage for a long period of time is brownout
A short power interruption is a fault
A long power interruption is a blackout
You MUST know all of the power issues above for the purpose of the exam.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 74
In an organization, an Information Technology security function should:
A. Be a function within the information systems function of an organization.
B. Report directly to a specialized business unit such as legal, corporate security or insurance.
C. Be lead by a Chief Security Officer and report directly to the CEO.

D. Be independent but report to the Information Systems function.
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
In order to offer more independence and get more attention from management, an IT security function should be independent from IT and report directly to the CEO. Having it report to a specialized business unit (e.g.
legal) is not recommended as it promotes a low technology view of the function and leads people to believe that it is someone else's problem.
Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

NEW QUESTION: 75
Why is infrared generally considered to be more secure to eavesdropping than multidirectional radio transmissions?
A. Because infrared eavesdropping requires more sophisticated equipment.
B. Because infrared operates only over short distances.
C. Because infrared requires direct line-of-sight paths.
D. Because infrared operates at extra-low frequencies (ELF).
Answer: C (LEAVE A REPLY)
Infrared is generally considered to be more secure to eavesdropping than multidirectional radio transmissions because infrared requires direct line-of-sight paths. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 173).

NEW QUESTION: 76
Which of the following is true related to network sniffing?
A. Sniffers allow an attacker to monitor data passing across a network.
B. Sniffers alter the source address of a computer to disguise and exploit weak authentication methods.
C. Sniffers take over network connections.
D. Sniffers send IP fragments to a system that overlap with each other.
Answer: A (LEAVE A REPLY)
The following answers are incorrect: Sniffers alter the source address of a computer to disguise and exploit weak authentication methods. IP Spoofing is a network-based attack, which involves altering the source address of a computer to disguise the attacker and exploit weak authentication methods.
Sniffers take over network connections. Session Hijacking tools allow an attacker to take over network connections, kicking off the legitimate user or sharing a login.
Sniffers send IP fragments to a system that overlap with each other. Malformed Packet attacks are a type of DoS attack that involves one or two packets that are formatted in an unexpected way. Many vendor product implementations do not take into account all variations of user entries or packet types. If software handles such errors poorly, the system may crash when it receives such packets. A classic example of this type of attack involves sending IP fragments to a system that overlap with each other (the fragment

offset values are incorrectly set. Some unpatched Windows and Linux systems will crash when the encounter such packets.
The following reference(s) were/was used to create this question:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, Auerbach, NY, NY 2001, Chapter 22, Hacker Tools and Techniques by Ed Skoudis. ISC2 OIG, 2007 p. 137-138, 419

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 77
Which software development model is actually a meta-model that incorporates a number of the software development models?
A. The Waterfall model
B. The modified Waterfall model
C. The Spiral model
D. The Critical Path Model (CPM)
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The spiral model is actually a meta-model that incorporates a number of the software development models.
This model depicts a spiral that incorporates the various phases of software development. The model states that each cycle of the spiral involves the same series of steps for each part of the project. CPM refers to the Critical Path Methodology.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 246).

NEW QUESTION: 78
Which common backup method is the fastest on a daily basis?
A. Full backup method
B. Incremental backup method
C. Fast backup method
D. Differential backup method
Answer: B (LEAVE A REPLY)

Section: Risk, Response and Recovery
Explanation/Reference:
The incremental backup method only copies files that have been recently changed or added. Only files with their archive bit set are backed up. This method is fast and uses less tape space but has some inherent vulnerabilities, one being that all incremental backups need to be available and restored from the date of the last full backup to the desired date should a restore be needed.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
69).

NEW QUESTION: 79
Network cabling comes in three flavors, they are:
A. twisted pair, coaxial, and fiber optic.
B. tagged pair, coaxial, and fiber optic.
C. trusted pair, coaxial, and fiber optic.
D. twisted pair, control, and fiber optic.
Answer: (SHOW ANSWER)
Explanation/Reference:
Network cabling comes in three flavors: twisted pair, coaxial, and fiber optic.
Twisted pair
Twisted pair cabling is a form of wiring in which two wires (the forward and return conductors of a single circuit) are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources. This type of cable is used for home and corporate Ethernet networks. Twisted pair cables consist of two insulated copper wires. There are three types of twisted pair cables: Shielded, Unshielded and Foil
Fiber Optic cable
An optical fiber cable consists of a center glass core surrounded by several layers of protective material. The outer insulating jacket is made of Teflon or PVC to prevent interference. It is expensive but has higher bandwidth and can transmit data over longer distances.
Coaxial cable
Coaxial lines confine the electromagnetic wave to area inside the cable, between the center conductor and the shield. The transmission of energy in the line occurs totally through the dielectric inside the cable between the conductors. Coaxial lines can therefore be bent and twisted (subject to limits) without negative effects, and they can be strapped to conductive supports without inducing unwanted currents in them and though.
The most common use for coaxial cables is for television and other signals with bandwidth of multiple megahertz. Although in most homes coaxial cables have been installed for transmission of TV signals, new technologies (such as the ITU-T G.hn standard) open the possibility of using home coaxial cable for high- speed home networking applications (Ethernet over coax).

See the following page for more details: http://fcit.usf.edu/network/chap4/chap4.htm Reference used for this question:
KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 101.
and
Wikipedia at http://en.wikipedia.org/wiki/Networking_cables

NEW QUESTION: 80
Which of the following would constitute the best example of a password to use for access to a system by a network administrator?
A. holiday
B. Christmas12
C. Jenny
D. GyN19Za!
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
GyN19Za! would be the the best answer because it contains a mixture of upper and lower case characters, alphabetic and numeric characters, and a special character making it less vulnerable to password attacks.
All of the other answers are incorrect because they are vulnerable to brute force or dictionary attacks. Passwords should not be common words or names. The addition of a number to the end of a common word only marginally strengthens it because a common password attack would also check combinations of words:
Christmas23
Christmas123
etc...

NEW QUESTION: 81
What does the simple security (ss) property mean in the Bell-LaPadula model?
A. No read up
B. No write down
C. No read down
D. No write up
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The ss (simple security) property of the Bell-LaPadula access control model states that reading of information by a subject at a lower sensitivity level from an object at a higher sensitivity level is not permitted (no read up).

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 202).

NEW QUESTION: 82
Prior to a live disaster test also called a Full Interruption test, which of the following is most important?
A. Restore all files in preparation for the test.
B. Document expected findings.
C. Arrange physical security for the test site.
D. Conduct of a successful Parallel Test
Answer: D (LEAVE A REPLY)
A live disaster test or Full interruption test is an actual simulation of the Disaster Recovery Plan. All operations are shut down and brought back online at the alternate site. This test poses the biggest threat to an organization and should not be performed until a successful Parallell Test has been conducted.
1.A Checklist test would be conducted where each of the key players will get a copy of the plan and they read it to make sure it has been properly developed for the specific needs of their departments.
2.A Structure Walk Through would be conducted next. This is when all key players meet together in a room and they walk through the test together to identify shortcoming and dependencies between department.
3.A simulation test would be next. In this case you go through a disaster scenario up to the point where you would move to the alternate site. You do not move to the alternate site and you learn from your mistakes and you improve the plan. It is the right time to find shortcomings.
4.A Parallell Test would be done. You go through a disaster scenario. You move to the alternate site and you process from both sites simultaneously.
5.A full interruption test would be conducted. You move to the alternate site and you resume processing at the alternate site.
The following answers are incorrect:
Restore all files in preparation for the test. Is incorrect because you would restore the files at the alternate site as part of the test not in preparation for the test.
Document expected findings. Is incorrect because it is not the best answer. Documenting the expected findings won't help if you have not performed tests prior to a Full interruption test or live disaster test.
Arrange physical security for the test site. Is incorrect because it is not the best answer. why physical security for the test site is important if you have not performed a successful structured walk-through prior to performing a Full interruption test or live disaster test you might have some unexpected and disasterous results.

NEW QUESTION: 83
Only law enforcement personnel are qualified to do computer forensic investigations.
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 84
Which of the following type of cryptography is used when both parties use the same key to communicate securely with each other?
A. Symmetric Key Cryptography
B. PKI - Public Key Infrastructure
C. Diffie-Hellman
D. DSS - Digital Signature Standard
Answer: (SHOW ANSWER)
Explanation/Reference:
Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext (sender) and decryption of ciphertext (receiver). The keys may be identical, in practice, they represent a shared secret between two or more parties that can be used to maintain a private information link.
This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. This is also known as secret key encryption. In symmetric key cryptography, each end of the conversation must have the same key or they cannot decrypt the message sent to them by the other party.
Symmetric key crypto is very fast but more difficult to manage due to the need to distribute the key in a secure means to all parts needing to decrypt the data. There is no key management built within Symmetric crypto.
PKI provides CIA - Confidentiality (Through encryption) Integrity (By guaranteeing that the message hasn't change in transit) and Authentication (Non-repudiation). Symmetric key crypto provides mostly Confidentiality.
The following answers are incorrect:
- PKI - Public Key Infrastructure: This is the opposite of symmetric key crypto. Each side in PKI has their own private key and public key. What one key encrypt the other one can decrypt. You make use of the receiver public key to communicate securely with a remote user. The receiver will use their matching private key to decrypt the data.
- Diffie-Hellman: Sorry, this is an asymmetric key technique. It is used for key agreement over an insecure network such as the Internet. It allows two parties who has never met to negotiate a secret key over an insecure network while preventing Man-In-The-Middle (MITM) attacks.
- DSS - Digital Signature Standard: Sorry, this is an asymmetric key technique.
The following reference(s) was used to create this question:
To learn more about this Qs and 100% of the Security+ CBK, subscribe to our Holistic Computer Based Tutorial (CBT) on our Learning Management System at: http://www.cccure.tv and http://en.wikipedia.org/wiki/Symmetric-key_algorithm

NEW QUESTION: 85
Which of the following results in the most devastating business interruptions?
A. Loss of Hardware/Software
B. Loss of Data

C. Loss of Communication Links
D. Loss of Applications
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Source: Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.
All of the others can be replaced or repaired. Data that is lost and was not backed up, cannot be restored.

NEW QUESTION: 86
Penetration testing involves three steps. Identify the three steps below:
(Choose three)
A. War Driving
B. Network reconnaissance
C. Network Penetration
D. System Control
E. Denial of system services
F. Network scanning
Answer: (SHOW ANSWER)
Penetration tests are intrusive and should always have the written approval of management. The steps include: reconnaissance, penetration, and control.

NEW QUESTION: 87
What is the name of the protocol use to set up and manage Security Associations (SA) for
IP Security (IPSec)?
A. Internet Key Exchange (IKE)
B. Secure Key Exchange Mechanism
C. Oakley
D. Internet Security Association and Key Management Protocol
Answer: A (LEAVE A REPLY)
The Key management for IPSec is called the Internet Key Exchange (IKE)
Note: IKE underwent a series of improvements establishing IKEv2 with RFC 4306. The basis of this answer is IKEv2.
The IKE protocol is a hybrid of three other protocols: ISAKMP (Internet Security Association and Key Management Protocol), Oakley and SKEME. ISAKMP provides a framework for authentication and key exchange, but does not define them (neither authentication nor key exchange). The Oakley protocol describes a series of modes for key exchange and the SKEME protocol defines key exchange techniques.
IKE-Internet Key Exchange. A hybrid protocol that implements Oakley and Skeme key exchanges inside the ISAKMP framework. IKE can be used with other protocols, but its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations. IKE is implemented in accordance with RFC 2409, The Internet Key Exchange.

The Internet Key Exchange (IKE) security protocol is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and the SKEME key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and SKEME are security protocols implemented by IKE.)

IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual preconfiguration. Specifically, IKE provides these benefits:

Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.

Allows you to specify a lifetime for the IPSec security association.

Allows encryption keys to change during IPSec sessions.

Allows IPSec to provide anti-replay services.

Permits certification authority (CA) support for a manageable, scalable IPSec implementation.

Allows dynamic authentication of peers.

About ISAKMP The Internet Security Association and Key Management Protocol (ISAKMP) is a framework that defines the phases for establishing a secure relationship and support for negotiation of security attributes, it does not establish sessions keys by itself, it is used along with the Oakley session key establishment protocol. The Secure Key Exchange Mechanism (SKEME) describes a secure exchange mechanism and Oakley defines the modes of operation needed to establish a secure connection.

ISAKMP provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. Alone, it does not establish session keys. However it can be used with various session key establishment protocols, such as Oakley, to provide a complete solution to Internet key management. About Oakley The Oakley protocol uses a hybrid Diffie-Hellman technique to establish session keys on Internet hosts and routers. Oakley provides the important security property of Perfect Forward Secrecy (PFS) and is based on cryptographic techniques that have survived substantial public scrutiny. Oakley can be used by itself, if no attribute negotiation is needed, or Oakley can be used in conjunction with ISAKMP. When ISAKMP is used with Oakley, key escrow is not feasible.

The ISAKMP and Oakley protocols have been combined into a hybrid protocol. The resolution of ISAKMP with Oakley uses the framework of ISAKMP to support a subset of Oakley key exchange modes. This new key exchange protocol provides optional PFS, full security association attribute negotiation, and authentication methods that provide both repudiation and non-repudiation. Implementations of this protocol can be used to establish VPNs and also allow for users from remote sites (who may have a dynamically allocated IP address) access to a secure network.

About IPSec The IETF's IPSec Working Group develops standards for IP-layer security mechanisms for both IPv4 and IPv6. The group also is developing generic key management protocols for use on the Internet. For more information, refer to the IP Security and Encryption Overview.

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. It acts at the network level and implements the following

standards:
IPSec
Internet Key Exchange (IKE)
Data Encryption Standard (DES)
MD5 (HMAC variant)
SHA (HMAC variant)
Authentication Header (AH)
Encapsulating Security Payload (ESP)
IPSec services provide a robust security solution that is standards-based. IPSec also provides data authentication and anti-replay services in addition to data confidentiality services.
For more information regarding IPSec, refer to the chapter "Configuring IPSec Network Security."
About SKEME
SKEME constitutes a compact protocol that supports a variety of realistic scenarios and security models over Internet. It provides clear tradeoffs between security and performance as required by the different scenarios without incurring in unnecessary system complexity. The protocol supports key exchange based on public key, key distribution centers, or manual installation, and provides for fast and secure key refreshment. In addition, SKEME selectively provides perfect forward secrecy, allows for replaceability and negotiation of the underlying cryptographic primitives, and addresses privacy issues as anonymity and repudiatability
SKEME's basic mode is based on the use of public keys and a Diffie-Hellman shared secret generation.
However, SKEME is not restricted to the use of public keys, but also allows the use of a pre-shared key. This key can be obtained by manual distribution or by the intermediary of a key distribution center (KDC) such as Kerberos.
In short, SKEME contains four distinct modes:
Basic mode, which provides a key exchange based on public keys and ensures PFS thanks to Diffie-Hellman.
A key exchange based on the use of public keys, but without Diffie-Hellman.
A key exchange based on the use of a pre-shared key and on Diffie-Hellman.
A mechanism of fast rekeying based only on symmetrical algorithms.
In addition, SKEME is composed of three phases: SHARE, EXCH and AUTH.
During the SHARE phase, the peers exchange half-keys, encrypted with their respective public keys. These two half-keys are used to compute a secret key K. If anonymity is wanted, the identities of the two peers are also encrypted. If a shared secret already exists, this phase is skipped.
The exchange phase (EXCH) is used, depending on the selected mode, to exchange either Diffie-Hellman public values or nonces. The Diffie-Hellman shared secret will only be computed after the end of the exchanges.

The public values or nonces are authenticated during the authentication phase (AUTH), using the secret key established during the SHARE phase.
The messages from these three phases do not necessarily follow the order described above; in actual practice they are combined to minimize the number of exchanged messages.
References used for this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 172).
http://tools.ietf.org/html/rfc4306
http://tools.ietf.org/html/rfc4301
http://en.wikipedia.org/wiki/Internet_Key_Exchange
CISCO ISAKMP and OAKLEY information
CISCO Configuring Internet Key Exchange Protocol
http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.en

NEW QUESTION: 88
Similar to Secure Shell (SSH-2), Secure Sockets Layer (SSL) uses symmetric encryption for encrypting the bulk of the data being sent over the session and it uses asymmetric or public key cryptography for:
A. Peer Authentication
B. Peer Identification
C. Server Authentication
D. Name Resolution
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
SSL provides for Peer Authentication. Though peer authentication is possible, authentication of the client is seldom used in practice when connecting to public e-commerce web sites. Once authentication is complete, confidentiality is assured over the session by the use of symmetric encryption in the interests of better performance.
The following answers were all incorrect:
"Peer identification" is incorrect. The desired attribute is assurance of the identity of the communicating parties provided by authentication and NOT identification. Identification is only who you claim to be. Authentication is proving who you claim to be.
"Server authentication" is incorrect. While server authentication only is common practice, the protocol provides for peer authentication (i.e., authentication of both client and server). This answer was not complete.
"Name resolution" is incorrect. Name resolution is commonly provided by the Domain Name System (DNS) not SSL.
Reference(s) used for this question:
CBK, pp. 496 - 497.

NEW QUESTION: 89
The DES algorithm is an example of what type of cryptography?
A. Secret Key
B. Two-key
C. Asymmetric Key
D. Public Key
Answer: A (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
DES is also known as a Symmetric Key or Secret Key algorithm.
DES is a Symmetric Key algorithm, meaning the same key is used for encryption and decryption.
For the exam remember that:
DES key Sequence is 8 Bytes or 64 bits (8 x 8 = 64 bits)
DES has an Effective key length of only 56 Bits. 8 of the Bits are used for parity purpose only.
DES has a total key length of 64 Bits.
The following answers are incorrect:
Two-key This is incorrect because DES uses the same key for encryption and decryption.
Asymmetric Key This is incorrect because DES is a Symmetric Key algorithm using the same key for encryption and decryption and an Asymmetric Key algorithm uses both a Public Key and a Private Key.
Public Key. This is incorrect because Public Key or algorithm Asymmetric Key does not use the same key is used for encryption and decryption.
References used for this question:
http://en.wikipedia.org/wiki/Data_Encryption_Standard

NEW QUESTION: 90
What security model is dependent on security labels?
A. Discretionary access control
B. Label-based access control
C. Mandatory access control
D. Non-discretionary access control
Answer: (SHOW ANSWER)
With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and the classification or sensitivity of the object.
Label-based access control is not defined. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION: 91
Most access violations are:
A. Accidental

B. Caused by internal hackers
C. Caused by external hackers
D. Related to Internet
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 192).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 92
Which of the following best defines add-on security?
A. Physical security complementing logical security measures.
B. Protection mechanisms implemented as an integral part of an information system.
C. Layer security.
D. Protection mechanisms implemented after an information system has become operational.
Answer: D (LEAVE A REPLY)
The Internet Security Glossary (RFC2828) defines add-on security as "The
retrofitting of protection mechanisms, implemented by hardware or software, after the
[automatic data processing] system has become operational."
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 93
What is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility?
A. DS-0
B. DS-1
C. DS-2
D. DS-3
Answer: B (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:

Digital Signal level 1 (DS-1) is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility. DS-0 is the framing specification used in transmitting digital signals over a single 64 Kbps channel over a T1 facility. DS-3 is the framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility. DS-2 is not a defined framing specification.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
114).

NEW QUESTION: 94
A periodic review of user account management should not determine:
A. Conformity with the concept of least privilege.
B. Whether active accounts are still being used.
C. Strength of user-chosen passwords.
D. Whether management authorizations are up-to-date.
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.
Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.
The strength of user passwords is beyond the scope of a simple user account management review, since it requires specific tools to try and crack the password file/database through either a dictionary or brute-force attack in order to check the strength of passwords.
Reference(s) used for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 28).

NEW QUESTION: 95
Which of the following best ensures accountability of users for the actions taken within a system or domain?
A. Identification
B. Authentication
C. Authorization
D. Credentials
Answer: (SHOW ANSWER)
Section: Access Control

Explanation/Reference:
Details:
The only way to ensure accountability is if the subject is uniquely identified and authenticated. Identification alone does not provide proof the user is who they claim to be. After showing proper credentials, a user is authorized access to resources.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 126).

NEW QUESTION: 96
A Business Continuity Plan should be tested:
A. Once a month.
B. At least twice a year.
C. At least once a year.
D. At least once every two years.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
It is recommended that testing does not exceed established frequency limits. For a plan to be effective, all components of the BCP should be tested at least once a year. Also, if there is a major change in the operations of the organization, the plan should be revised and tested not more than three months after the change becomes operational.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 165).

NEW QUESTION: 97
The most important component of antivirus software is the _____?
A. Definitions
B. Console
C. Engine
D. Heuristics
E. Desktop
Answer: C (LEAVE A REPLY)

NEW QUESTION: 98
Packet Filtering Firewalls can also enable access for:
A. only authorized application port or service numbers.
B. only unauthorized application port or service numbers.
C. only authorized application port or ex-service numbers.
D. only authorized application port or service integers.
Answer: (SHOW ANSWER)

Firewall rules can be used to enable access for traffic to specific ports or services. "Service numbers" is rather stilted English but you may encounter these types of wordings on the actual exam -- don't let them confuse you.
"Only unauthorized application port or service numbers" is incorrect. Unauthorized ports/services would be blocked in a properly installed firewall rather than permitting access.
"Only authorized application port or ex-service numbers" is incorrect. "Ex-service" numbers is a nonsense term meant to distract you.
"Only authorized application port or service integers." While service numbers are in fact integers, the more usual (and therefore better) answer is either service or "service number."
References
CBK, p. 464 AIO3, pp. 482 - 484

NEW QUESTION: 99
A Security Kernel is defined as a strict implementation of a reference monitor mechanism responsible for enforcing a security policy. To be secure, the kernel must meet three basic conditions, what are they?
A. Confidentiality, Integrity, and Availability
B. Policy, mechanism, and assurance
C. Isolation, layering, and abstraction
D. Completeness, Isolation, and Verifiability
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
A security kernel is responsible for enforcing a security policy. It is a strict implementation of a reference monitor mechanism. The architecture of a kernel operating system is typically layered, and the kernel should be at the lowest and most primitive level.
It is a small portion of the operating system through which all references to information and all changes to authorizations must pass. In theory, the kernel implements access control and information flow control between implemented objects according to the security policy.
To be secure, the kernel must meet three basic conditions:
completeness (all accesses to information must go through the kernel),
isolation (the kernel itself must be protected from any type of unauthorized access), and verifiability (the kernel must be proven to meet design specifications).
The reference monitor, as noted previously, is an abstraction, but there may be a reference validator, which usually runs inside the security kernel and is responsible for performing security access checks on objects, manipulating privileges, and generating any resulting security audit messages.
A term associated with security kernels and the reference monitor is the trusted computing base (TCB). The TCB is the portion of a computer system that contains all elements of the system responsible for supporting the security policy and the isolation of objects. The security capabilities of products for use in the TCB can be verified through various evaluation criteria, such as the earlier Trusted Computer System Evaluation Criteria (TCSEC) and the current Common Criteria standard.

Many of these security terms-reference monitor, security kernel, TCB-are defined loosely by vendors for purposes of marketing literature. Thus, it is necessary for security professionals to read the small print and between the lines to fully understand what the vendor is offering in regard to security features.
TIP FOR THE EXAM:
The terms Security Kernel and Reference monitor are synonymous but at different levels.
As it was explained by Diego:
While the Reference monitor is the concept, the Security kernel is the implementation of such concept (via hardware, software and firmware means).
The two terms are the same thing, but on different levels: one is conceptual, one is "technical" The following are incorrect answers:
Confidentiality, Integrity, and Availability
Policy, mechanism, and assurance
Isolation, layering, and abstraction
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 13858-13875). Auerbach Publications. Kindle Edition.

NEW QUESTION: 100
What is Kerberos?
A. A three-headed dog from the egyptian mythology.
B. A trusted third-party authentication protocol.
C. A security model.
D. A remote authentication dial in user server.
Answer: B (LEAVE A REPLY)
Is correct because that is exactly what Kerberos is.
The following answers are incorrect:
A three-headed dog from Egyptian mythology. Is incorrect because we are dealing with Information Security and not the Egyptian mythology but the Greek Mythology.
A security model. Is incorrect because Kerberos is an authentication protocol and not just a security model.
A remote authentication dial in user server. Is incorrect because Kerberos is not a remote authentication dial in user server that would be called RADIUS.

NEW QUESTION: 101
Which of the following statements is most accurate regarding a digital signature?
A. It is a method used to encrypt confidential data.
B. It is the art of transferring handwritten signature to electronic media.
C. It allows the recipient of data to prove the source and integrity of data.
D. It can be used as a signature system and a cryptosystem.
Answer: (SHOW ANSWER)
Explanation/Reference:

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 102
Which of the following is an advantage of a qualitative over a quantitative risk analysis?
A. It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
B. It provides specific quantifiable measurements of the magnitude of the impacts.
C. It makes a cost-benefit analysis of recommended controls easier.
D. It can easily be automated.
Answer: A (LEAVE A REPLY)
The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. It does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-analysis of any recommended controls difficult. Since it involves a consensus of export and some guesswork based on the experience of Subject Matter Experts (SME's), it can not be easily automated.
Reference used for this question:
STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 23).

NEW QUESTION: 103
Which Network Address Translation (NAT) is the most convenient and secure solution?
A. Hiding Network Address Translation
B. Port Address Translation
C. Dedicated Address Translation
D. Static Address Translation
Answer: B (LEAVE A REPLY)
Static network address translation offers the most flexibility, but it is not normally practical given the shortage of IP version 4 addresses. Hiding network address translation is was an interim step in the development of network address translation technology, and is seldom used because port address translation offers additional features above and beyond those present in hiding network address translation while maintaining the same basic design and engineering considerations. PAT is often the most convenient and secure solution.
Source: WACK, John et al., NIST Special publication 800-41, Guidelines on Firewalls and Firewall Policy, January 2002 (page 18).

NEW QUESTION: 104
The scope and focus of the Business continuity plan development depends most on:
A. Directives of Senior Management
B. Business Impact Analysis (BIA)
C. Scope and Plan Initiation
D. Skills of BCP committee

Answer: B (LEAVE A REPLY)

SearchStorage.com Definitions mentions "As part of a disaster recovery plan, BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on.

A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance.

Where possible, impact is expressed monetarily for purposes of comparison. For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence."

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 278.

NEW QUESTION: 105

A prolonged complete loss of electric power is a:

A. brownout

B. blackout

C. surge

D. fault

Answer: (SHOW ANSWER)

Section: Risk, Response and Recovery

Explanation/Reference:

A prolonged power outage is a blackout.

From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 106

Which of the following statements regarding an off-site information processing facility is TRUE?

A. It should have the same amount of physical access restrictions as the primary processing site.

B. It should be located in proximity to the originating site so that it can quickly be made operational.

C. It should be easily identified from the outside so in the event of an emergency it can be easily found.

D. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Answer: A (LEAVE A REPLY)

It is very important that the offsite has the same restrictions in order to avoide misuse.

The following answers are incorrect because:

It should be located in proximity to the originating site so that it can quickly be made operational is incorrect as the offsite is also subject to the same disaster as of the primary site.

It should be easily identified from the outside so in the event of an emergency it can be easily found is also incorrect as it should not be easily identified to prevent intentional sabotage. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive is also incorrect as it should be like its primary site.

Reference : Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 265).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 107
Which of the following are NT Audit events? (Choose all that apply)
A. Use of User Rights
B. Security Policy Change
C. All of choices are correct
D. Logon and Logoff
E. Registry Tracking
Answer: (SHOW ANSWER)

NEW QUESTION: 108
What does the simple integrity axiom mean in the Biba model?
A. No write down
B. No read down
C. No read up
D. No write up
Answer: B (LEAVE A REPLY)
The simple integrity axiom of the Biba access control model states that a subject at one level of integrity is not permitted to observe an object of a lower integrity (no read down). Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

NEW QUESTION: 109
Asynchronous Communication transfers data by sending:
A. bits of data sequentially
B. bits of data sequentially in irregular timing patterns
C. bits of data in sync with a heartbeat or clock
D. bits of data simultaneously
Answer: B (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:

Asynchronous Communication transfers data by sending bits of data in irregular timing patterns.
In asynchronous transmission each character is transmitted separately, that is one character at a time. The character is preceded by a start bit, which tells the receiving end where the character coding begins, and is followed by a stop bit, which tells the receiver where the character coding ends. There will be intervals of ideal time on the channel shown as gaps. Thus there can be gaps between two adjacent characters in the asynchronous communication scheme. In this scheme, the bits within the character frame (including start, parity and stop bits) are sent at the baud rate.
The START BIT and STOP BIT including gaps allow the receiving and sending computers to synchronise the data transmission. Asynchronous communication is used when slow speed peripherals communicate with the computer. The main disadvantage of asynchronous communication is slow speed transmission. Asynchronous communication however, does not require the complex and costly hardware equipments as is required for synchronous transmission.
Asynchronous communication is transmission of data without the use of an external clock signal. Any timing required to recover data from the communication symbols is encoded within the symbols. The most significant aspect of asynchronous communications is variable bit rate, or that the transmitter and receiver clock generators do not have to be exactly synchronized.
The asynchronous communication technique is a physical layer transmission technique which is most widely used for personal computers providing connectivity to printers, modems, fax machines, etc.
An asynchronous link communicates data as a series of characters of fixed size and format. Each character is preceded by a start bit and followed by 1-2 stop bits.
Parity is often added to provide some limited protection against errors occurring on the link.
The use of independent transmit and receive clocks constrains transmission to relatively short characters (<8 bits) and moderate data rates (< 64 kbps, but typically lower).
The asynchronous transmitter delimits each character by a start sequence and a stop sequence. The start bit (0), data (usually 8 bits plus parity) and stop bit(s) (1) are transmitted using a shift register clocked at the nominal data rate.
When asynchronous transmission is used to support packet data links (e.g. IP), then special characters have to be used ("framing") to indicate the start and end of each frame transmitted.
One character (none as an escape character) is reserved to mark any occurrence of the special characters within the frame. In this way the receiver is able to identify which characters are part of the frame and which are part of the "framing".
Packet communication over asynchronous links is used by some users to get access to a network using a modem.
Most Wide Area Networks use synchronous links and a more sophisticated link protocol Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.
and
http://en.wikipedia.org/wiki/Asynchronous_communication
and
http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/async.html
and

http://www.ligaturesoft.com/data_communications/async-data-transmission.html

NEW QUESTION: 110
What is the PRIMARY goal of incident handling?
A. Successfully retrieve all evidence that can be used to prosecute
B. Improve the company's ability to be prepared for threats and disasters
C. Improve the company's disaster recovery plan
D. Contain and repair any damage caused by an event.
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
This is the PRIMARY goal of an incident handling process.
The other answers are incorrect because :
Successfully retrieve all evidence that can be used to prosecute is more often used in identifying weaknesses than in prosecuting.
Improve the company's ability to be prepared for threats and disasters is more appropriate for a disaster recovery plan.
Improve the company's disaster recovery plan is also more appropriate for disaster recovery plan.
Reference : Shon Harris AIO v3 , Chapter - 10 : Law, Investigation, and Ethics , Page : 727-728

NEW QUESTION: 111
The type of discretionary access control (DAC) that is based on an individual's identity is also called:
A. Identity-based Access control
B. Rule-based Access control
C. Non-Discretionary Access Control
D. Lattice-based Access control
Answer: A (LEAVE A REPLY)
Explanation/Reference:
An identity-based access control is a type of Discretionary Access Control (DAC) that is based on an individual's identity.
DAC is good for low level security environment. The owner of the file decides who has access to the file. If a user creates a file, he is the owner of that file. An identifier for this user is placed in the file header and/ or in an access control matrix within the operating system.
Ownership might also be granted to a specific individual. For example, a manager for a certain department might be made the owner of the files and resources within her department. A system that uses discretionary access control (DAC) enables the owner of the resource to specify which subjects can access specific resources.
This model is called discretionary because the control of access is based on the discretion of the owner. Many times department managers, or business unit managers , are the owners of the data within their specific department. Being the owner, they can specify who should have access and who should not.
Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 220). McGraw-Hill . Kindle Edition.

NEW QUESTION: 112
If an operating system permits shared resources such as memory to be used sequentially by multiple users/application or subjects without a refresh of the objects/memory area, what security problem is MOST likely to exist?
A. Disclosure of residual data.
B. Unauthorized obtaining of a privileged execution state.
C. Data leakage through covert channels.
D. Denial of service through a deadly embrace.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Allowing objects to be used sequentially by multiple users without a refresh of the objects can lead to disclosure of residual data. It is important that steps be taken to eliminate the chance for the disclosure of residual data.
Object reuse refers to the allocation or reallocation of system resources to a user or, more appropriately, to an application or process. Applications and services on a computer system may create or use objects in memory and in storage to perform programmatic functions. In some cases, it is necessary to share these resources between various system applications. However, some objects may be employed by an application to perform privileged tasks on behalf of an authorized user or upstream application. If object usage is not controlled or the data in those objects is not erased after use, they may become available to unauthorized users or processes.
Disclosure of residual data and Unauthorized obtaining of a privileged execution state are both a problem with shared memory and resources. Not clearing the heap/stack can result in residual data and may also allow the user to step on somebody's session if the security token/identify was maintained in that space. This is generally more malicious and intentional than accidental though. The MOST common issue would be Disclosure of residual data.
The following answers are incorrect:
Unauthorized obtaining of a privileged execution state. Is incorrect because this is not a problem with Object Reuse.
Data leakage through covert channels. Is incorrect because it is not the best answer. A covert channel is a communication path. Data leakage would not be a problem created by Object Reuse. In computer security, a covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. The term, originated in 1973 by Lampson is defined as "(channels) not intended for information transfer at all, such as the service program's effect on system load." to distinguish it from Legitimate channels that are subjected to access controls by COMPUSEC.
Denial of service through a deadly embrace. Is incorrect because it is only a detractor.
References:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4174-4179). Auerbach Publications. Kindle Edition.
and
https://www.fas.org/irp/nsa/rainbow/tg018.htm
and
http://en.wikipedia.org/wiki/Covert_channel

NEW QUESTION: 113
What is it called when a computer uses more than one CPU in parallel to execute instructions?
A. Multiprocessing
B. Multitasking
C. Multithreading
D. Parallel running
Answer: A (LEAVE A REPLY)
A system with multiple processors is called a multiprocessing system.
Multitasking is incorrect. Multitasking involves sharing the processor amoung all ready processes. Though it appears to the user that multiple processes are executing at the same time, only one process is running at any point in time.
Multithreading is incorrect. The developer can structure a program as a collection of independent threads to achieve better concurrency. For example, one thread of a program might be performing a calculation while another is waiting for additional input from the user.
"Parallel running" is incorrect. This is not a real term and is just a distraction.
References:
CBK, pp. 315-316 AIO3, pp. 234 - 239

NEW QUESTION: 114
What type of attack involves IP spoofing, ICMP ECHO and a bounce site?
A. IP spoofing attack
B. Teardrop attack
C. SYN attack
D. Smurf attack
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
A smurf attack occurs when an attacker sends a spoofed (IP spoofing) PING (ICMP ECHO) packet to the broadcast address of a large network (the bounce site). The modified packet containing the address of the target system, all devices on its local network respond with a ICMP REPLY to the target system, which is then saturated with those replies. An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A teardrop attack consists of modifying the length and

fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
76).

NEW QUESTION: 115
Which of the following NAT firewall translation modes offers no protection from hacking attacks to an internal host using this functionality?
A. Network redundancy translation
B. Load balancing translation
C. Dynamic translation
D. Static translation
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Static translation (also called port forwarding), assigns a fixed address to a specific internal network resource (usually a server).
Static NAT is required to make internal hosts available for connection from external hosts.
It merely replaces port information on a one-to-one basis. This affords no protection to statistically translated hosts: hacking attacks will be just as efficiently translated as any other valid connection attempt.
NOTE FROM CLEMENT:
Hiding Nat or Overloaded Nat is when you have a group of users behind a unique public IP address. This will provide you with some security through obscurity where an attacker scanning your network would see the unique IP address on the outside of the gateway but could not tell if there is one user, ten users, or hundreds of users behind that IP.
NAT was NEVER built as a security mechanism.
In the case of Static NAT used for some of your servers for example, your web server private IP is map to a valid external public IP on a one on one basis, your SMTP server private IP is mapped to a static public IP, and so on.
If an attacker scan the IP address range on the external side of the gateway he would discover every single one of your servers or any other hosts using static natting. Ports that are open, services that are listening, and all of this info could be gathered just as if the server was in fact using a public IP. It does not provide this security through obscurity mentioned above.
All of the other answer are incorrect.
Reference used for this question:
STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 7: Network Address Translation.

NEW QUESTION: 116
Compared to RSA, which of the following is true of Elliptic Curve Cryptography(ECC)?
A. It has been mathematically proved to be more secure.
B. It has been mathematically proved to be less secure.
C. It is believed to require longer key for equivalent security.
D. It is believed to require shorter keys for equivalent security.
Answer: D (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
The following answers are incorrect: It has been mathematically proved to be less secure. ECC has not been proved to be more or less secure than RSA. Since ECC is newer than RSA, it is considered riskier by some, but that is just a general assessment, not based on mathematical arguments.
It has been mathematically proved to be more secure. ECC has not been proved to be more or less secure than RSA. Since ECC is newer than RSA, it is considered riskier by some, but that is just a general assessment, not based on mathematical arguments.
It is believed to require longer key for equivalent security. On the contrary, it is believed to require shorter keys for equivalent security of RSA.
Shon Harris, AIO v5 pg719 states:
"In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter that what RSA requires" The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p. 258
Shon Harris, AIO v5 pg719

NEW QUESTION: 117
A Security Reference Monitor relates to which DoD security standard?
A. D1
B. C2
C. LC3
D. L2TP
E. None of the items listed
Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
Which of the following offers advantages such as the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access?
A. Smart cards
B. Single Sign-On (SSO)
C. Symmetric Ciphers
D. Public Key Infrastructure (PKI)

Answer: (SHOW ANSWER)

Section: Access Control

Explanation/Reference:

The advantages of SSO include having the ability to use stronger passwords, easier administration as far as changing or deleting the passwords, minimize the risks of orphan accounts, and requiring less time to access resources.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

NEW QUESTION: 119

Which of the following describes a computer processing architecture in which a language compiler or pre-processor breaks program instructions down into basic operations that can be performed by the processor at the same time?

A. Very-Long Instruction-Word Processor (VLIW)

B. Complex-Instruction-Set-Computer (CISC)

C. Reduced-Instruction-Set-Computer (RISC)

D. Super Scalar Processor Architecture (SCPA)

Answer: (SHOW ANSWER)

Very long instruction word (VLIW) describes a computer processing architecture in which a language compiler or pre-processor breaks program instruction down into basic operations that can be performed by the processor in parallel (that is, at the same time). These operations are put into a very long instruction word which the processor can then take apart without further analysis, handing each operation to an appropriate functional unit.

The following answer are incorrect:

The term "CISC" (complex instruction set computer or computing) refers to computers designed with a full set of computer instructions that were intended to provide needed capabilities in the most efficient way. Later, it was discovered that, by reducing the full set to only the most frequently used instructions, the computer would get more work done in a shorter amount of time for most applications. Intel's Pentium microprocessors are CISC microprocessors.

The PowerPC microprocessor, used in IBM's RISC System/6000 workstation and Macintosh computers, is a RISC microprocessor. RISC takes each of the longer, more complex instructions from a CISC design and reduces it to multiple instructions that are shorter and faster to process. RISC technology has been a staple of mobile devices for decades, but it is now finally poised to take on a serious role in data center servers and server virtualization. The latest RISC processors support virtualization and will change the way computing resources scale to meet workload demands.

A superscalar CPU architecture implements a form of parallelism called instruction level parallelism within a single processor. It therefore allows faster CPU throughput than would otherwise be possible at a given clock rate. A superscalar processor executes more than one instruction during a clock cycle by simultaneously dispatching multiple instructions to redundant functional units on the processor. Each functional unit is not a separate CPU core but an execution resource within a single CPU such as an arithmetic logic unit, a bit shifter, or a multiplier.

Reference(s) Used for this question:
http://whatis.techtarget.com/definition/0,,sid9_gci214395,00.html and http://searchcio-midmarket.techtarget.com/definition/CISC and http://en.wikipedia.org/wiki/Superscalar

NEW QUESTION: 120
What is the most secure way to dispose of information on a CD-ROM?
A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
First you have to realize that the question is specifically talking about a CDROM. The information stored on a CDROM is not in electro magnetic format, so a degausser woud be inneffective.
You cannot sanitize a CDROM but you might be able to sanitize a RW/CDROM. A CDROM is a write once device and cannot be overwritten like a hard disk or other magnetic device.
Physical Damage would not be enough as information could still be extracted in a lab from the undamaged portion of the media or even from the pieces after the physical damage has been done.
Physical Destruction using a shredder, your microwave oven, melting it, would be very effective and the best choice for a non magnetic media such as a CDROM.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 121
Which of the following backup method must be made regardless of whether Differential or Incremental methods are used?
A. Full Backup Method.
B. Incremental backup method.
C. Supplemental backup method.
D. Tape backup method.
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
A Full Backup must be made regardless of whether Differential or Incremental methods are used.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.
And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9:
Disaster Recovery and Business continuity (pages 617-619).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 122
Which of the following will a Business Impact Analysis NOT identify?
A. Areas that would suffer the greatest financial or operational loss in the event of a disaster.
B. Systems critical to the survival of the enterprise.
C. The names of individuals to be contacted during a disaster.
D. The outage time that can be tolerated by the enterprise as a result of a disaster.
Answer: (SHOW ANSWER)
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 123
An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):
A. active attack
B. outside attack
C. inside attack
D. passive attack
Answer: (SHOW ANSWER)
An inside attack is an attack initiated by an entity inside the security perimeter, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization whereas an outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system. An active attack attempts to alter system resources to affect their operation and a passive attack attempts to learn or make use of the information from the system but does not affect system resources. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 124
The term "principle of least privilege" is best as:
A. A separation of command, program and interface functions
B. Active monitoring with network base intrusion detection systems and host based intrusion detection systems
C. The process of granting each user the lowest clearance and access needed to accomplish their task
D. Implementation of mandatory access control
Answer: C (LEAVE A REPLY)
The principle of least privilege is used in part to limit the damage resulting from accidents, errors, or unauthorized use of system resources.

NEW QUESTION: 125
Which of the following statements pertaining to software testing is incorrect?
A. Unit testing should be addressed and considered when the modules are being designed.
B. Test data should be part of the specifications.
C. Testing should be performed with live data to cover all possible situations.
D. Test data generators can be used to systematically generate random test data that can be used to test programs.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Live or actual field data is not recommended for use in the testing procedures because both data types may not cover out of range situations and the correct outputs of the test are unknown. Live data would not be the best data to use because of the lack of anomalies and also because of the risk of exposure to your live data.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 251).

NEW QUESTION: 126
Which of the following statements pertaining to quantitative risk analysis is false?
A. Portion of it can be automated
B. It involves complex calculations
C. It requires a high volume of information
D. It requires little experience to apply
Answer: (SHOW ANSWER)
Assigning the values for the inputs to a purely quantitative risk assessment requires both a lot of time and significant experience on the part of the assessors. The most experienced employees or representatives from each of the departments would be involved in the process. It is NOT an easy task if you wish to come up with accurate values.
"It can be automated" is incorrect. There are a number of tools on the market that automate the process of conducting a quantitative risk assessment.
"It involves complex calculations" is incorrect. The calculations are simple for basic scenarios but could become fairly complex for large cases. The formulas have to be applied correctly.
"It requires a high volume of information" is incorrect. Large amounts of information are required in order to develop reasonable and defensible values for the inputs to the quantitative risk assessment.
References:
CBK, pp. 60-61 AIO3, p. 73, 78 The Cissp Prep Guide - Mastering The Ten Domains Of Computer Security - 2001, page 24

NEW QUESTION: 127
Which of the following Kerberos components holds all users' and services' cryptographic keys?

A. The Key Distribution Service
B. The Authentication Service
C. The Key Distribution Center
D. The Key Granting Service
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The Key Distribution Center (KDC) holds all users' and services' cryptographic keys. It provides authentication services, as well as key distribution functionality. The Authentication Service is the part of the KDC that authenticates a principal. The Key Distribution Service and Key Granting Service are distracters and are not defined Kerberos components.
Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

NEW QUESTION: 128
The scope and focus of the Business continuity plan development depends most on:
A. Directives of Senior Management
B. Business Impact Analysis (BIA)
C. Scope and Plan Initiation
D. Skills of BCP committee
Answer: B (LEAVE A REPLY)
Explanation/Reference:
SearchStorage.com Definitions mentions "As part of a disaster recovery plan, BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on.
A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance.
Where possible, impact is expressed monetarily for purposes of comparison. For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 278.

NEW QUESTION: 129
The Internet service that converts www.soundbodyworks.com to 216.230.195.151 is known as
A. GOPHER
B. SMTP
C. DNS
D. FTP
E. HTTP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 130
In order to be able to successfully prosecute an intruder:
A. A point of contact should be designated to be responsible for communicating with law enforcement and other external agencies.
B. A proper chain of custody of evidence has to be preserved.
C. Collection of evidence has to be done following predefined procedures.
D. Whenever possible, analyze a replica of the compromised resource, not the original, thereby avoiding inadvertently tamping with evidence.
Answer: (SHOW ANSWER)
If you intend on prosecuting an intruder, evidence has to be collected in a lawful manner and, most importantly, protected through a secure chain-of-custody procedure that tracks who has been involved in handling the evidence and where it has been stored. All other choices are all important points, but not the best answer, since no prosecution is possible without a proper, provable chain of custody of evidence.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 282-285).

NEW QUESTION: 131
What is called a system that is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it?
A. A fail safe system
B. A fail soft system
C. A fault-tolerant system
D. A failover system
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
A fault-tolerant system is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it. In a fail-safe system, program execution is terminated, and the system is protected from being compromised when a hardware or software failure occurs and is detected. In a fail-soft system, when a hardware or software failure occurs and is detected, selected, non-critical processing is terminated. The term failover refers to switching to a duplicate "hot" backup component in real-time when a hardware or software failure occurs, enabling processing to continue.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 196).

NEW QUESTION: 132
A periodic review of user account management should not determine:
A. Conformity with the concept of least privilege.
B. Whether active accounts are still being used.
C. Strength of user-chosen passwords.

D. Whether management authorizations are up-to-date.

Answer: C (LEAVE A REPLY)

Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.

The strength of user passwords is beyond the scope of a simple user account management review, since it requires specific tools to try and crack the password file/database through either a dictionary or brute-force attack in order to check the strength of passwords.

Reference(s) used for this question:

SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 28).

NEW QUESTION: 133

Which of the following items is NOT a benefit of cold sites?

A. No resource contention with other organisation

B. Quick Recovery

C. A secondary location is available to reconstruct the environment

D. Low Cost

Answer: (SHOW ANSWER)

Section: Risk, Response and Recovery

Explanation/Reference:

A cold site is a permanent location that provide you with your own space that you can move into in case of a disaster or catastrophe. It is one of the cheapest solution available as a rental place but it is also the one that would take the most time to recover. A cold site usually takes one to two weeks for recoverey.

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. The plan should include a trategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:

Dedicated site owned or operated by the organization. Also called redundant or alternate sites;

Reciprocal agreement or memorandum of agreement with an internal or external entity; and

Commercially leased facility.

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites. Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types.

Progressing from basic to advanced, the sites are described below:

Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.
ƒWarm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.
Hot Sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.
As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each organization should evaluate its core requirements in order to establish the most effective solution.
Two examples of variations to the site types are:
ƒMobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.
ƒMirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.
There are obvious cost and ready-time differences among the options. In these examples, the mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain, although they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours, but the time necessary for equipment installation and setup can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel and/or equipment there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the organization's primary site.
The following reference(s) were used for this question:
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

NEW QUESTION: 134
What can be defined as an instance of two different keys generating the same ciphertext from the same plaintext?
A. Key collision
B. Key clustering
C. Hashing
D. Ciphertext collision
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Key clustering happens when a plaintext message generates identical ciphertext messages using the same transformation algorithm, but with different keys.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 130).

NEW QUESTION: 135
The Orange Book states that "Hardware and software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB [Trusted Computing Base]." This statement is the formal requirement for:
A. Security Testing.
B. Design Verification.
C. System Integrity.
D. System Architecture Specification.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
This is a requirement starting as low as C1 within the TCSEC rating.
The Orange book requires the following for System Integrity Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.
NOTE FROM CLEMENT:
This is a question that confuses a lot of people because most people take for granted that the orange book with its associated Bell LaPadula model has nothing to do with integrity. However you have to be careful about the context in which the word integrity is being used. You can have Data Integrity and you can have System Integrity which are two completely different things.
Yes, the Orange Book does not specifically address the Integrity requirements, however it has to run on top of systems that must meet some integrity requirements.
This is part of what they call operational assurance which is defined as a level of confidence of a trusted system's architecture and implementation that enforces the system's security policy. It includes:
System architecture
Covert channel analysis
System integrity
Trusted recovery
DATA INTEGRITY
Data Integrity is very different from System Integrity. When you have integrity of the data, there are three goals:
1. Prevent authorized users from making unauthorized modifications
2. Preven unauthorized users from making modifications
3. Maintaining internal and external consistancy of the data
Bell LaPadula which is based on the Orange Book address does not address Integrity, it addresses only Confidentiality.
Biba address only the first goal of integrity.
Clark-Wilson addresses the three goals of integrity.
In the case of this question, there is a system integrity requirement within the TCB. As mentioned above here is an extract of the requirements: Hardware and/or software features shall be provided that can be

used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.
The following answers are incorrect:
Security Testing. Is incorrect because Security Testing has no set of requirements in the Orange book.
Design Verification. Is incorrect because the Orange book's requirements for Design Verification include: A formal model of the security policy must be clearly identified and documented, including a mathematical proof that the model is consistent with its axioms and is sufficient to support the security policy.
System Architecture Specification. Is incorrect because there are no requirements for System Architecture Specification in the Orange book.
The following reference(s) were used for this question:
Trusted Computer Security Evaluation Criteria (TCSEC), DoD 5200.28-STD, page 15, 18, 25, 31, 40, 50.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page
392-397, for users with the Kindle Version see Kindle Locations 28504-28505.
and
DOD TCSEC - http://www.cerberussystems.com/INFOSEC/stds/d520028.htm

NEW QUESTION: 136
IT security measures should:
A. Be complex
B. Be tailored to meet organizational security goals.
C. Make sure that every asset of the organization is well protected.
D. Not be developed in a layered fashion.
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
In general, IT security measures are tailored according to an organization's unique needs. While numerous factors, such as the overriding mission requirements, and guidance, are to be considered, the fundamental issue is the protection of the mission or business from IT security-related, negative impacts. Because IT security needs are not uniform, system designers and security practitioners should consider the level of trust when connecting to other external networks and internal sub-domains. Recognizing the uniqueness of each system allows a layered security strategy to be used - implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas.
The more complex the mechanism, the more likely it may possess exploitable flaws. Simple mechanisms tend to have fewer exploitable flaws and require less maintenance. Further, because configuration management issues are simplified, updating or replacing a simple mechanism becomes a less intensive process.
Security designs should consider a layered approach to address or protect against a specific threat or to reduce a vulnerability. For example, the use of a packet-filtering router in conjunction with an application

gateway and an intrusion detection system combine to increase the work-factor an attacker must expend to successfully attack the system. Adding good password controls and adequate user training improves the system's security posture even more.
The need for layered protections is especially important when commercial-off-the-shelf (COTS) products are used. Practical experience has shown that the current state-of-the-art for security quality in COTS products does not provide a high degree of protection against sophisticated attacks. It is possible to help mitigate this situation by placing several controls in series, requiring additional work by attackers to accomplish their goals.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (pages 9-10).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 137
The preliminary steps to security planning include all of the following EXCEPT which of the following?
A. Establish objectives.
B. List planning assumptions.
C. Establish a security audit function.
D. Determine alternate courses of action
Answer: C (LEAVE A REPLY)
The keyword within the question is: preliminary
This means that you are starting your effort, you cannot audit if your infrastructure is not even in place.
Reference used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 138
Which of the following is not a logical control when implementing logical access security?
A. access profiles.
B. userids.
C. employee badges.
D. passwords.
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:

Employee badges are considered Physical so would not be a logical control.
The following answers are incorrect:
userids. Is incorrect because userids are a type of logical control.
access profiles. Is incorrect because access profiles are a type of logical control.
passwords. Is incorrect because passwords are a type of logical control.

NEW QUESTION: 139
Some Unix systems use a very simple cipher called _____.
A. DES
B. SOT14
C. Block
D. ROT13
E. Stream
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?
A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
C. They both involve rewriting the media.
D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack). There are three general methods of purging media: overwriting, degaussing, and destruction.
There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.
Reference(s) use for this question:

SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 26).
and
A guide to understanding Data Remanence in Automated Information Systems

NEW QUESTION: 141
Access Control techniques do not include which of the following choices?
A. Relevant Access Controls
B. Discretionary Access Control
C. Mandatory Access Control
D. Lattice Based Access Control
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Access Control Techniques
Discretionary Access Control
Mandatory Access Control
Lattice Based Access Control
Rule-Based Access Control
Role-Based Access Control
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

NEW QUESTION: 142
Which of the following offers confidentiality to an e-mail message?
A. The sender encrypting it with its private key.
B. The sender encrypting it with its public key.
C. The sender encrypting it with the receiver's public key.
D. The sender encrypting it with the receiver's private key.
Answer: C (LEAVE A REPLY)
An e-mail message's confidentiality is protected when encrypted with the receiver's public key, because he is the only one able to decrypt the message. The sender is not supposed to have the receiver's private key. By encrypting a message with its private key, anybody possessing the corresponding public key would be able to read the message. By encrypting the message with its public key, not even the receiver would be able to read the message.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 517).

NEW QUESTION: 143

Which of the following can be defined as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client?

A. IMAP4

B. SMTP

C. MIME

D. PEM

Answer: (SHOW ANSWER)

Section: Network and Telecommunications

Explanation/Reference:

RFC 2828 (Internet Security Glossary) defines the Internet Message Access Protocol, version 4 (IMAP4) as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client.

IMAP4 has mechanisms for optionally authenticating a client to a server and providing other security services.

MIME is the MultiPurpose Internet Mail Extension. MIME extends the format of Internet mail to allow non-US- ASCII textual messages, non-textual messages, multipart message bodies, and non-US-ASCII information in message headers.

Simple Mail Transfer Protocol (SMTP) is a TCP-based, application-layer, Internet Standard protocol for moving electronic mail messages from one computer to another.

Privacy Enhanced Mail (PEM) is an Internet protocol to provide data confidentiality, data integrity, and data origin authentication for electronic mail.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 144

Who should direct short-term recovery actions immediately following a disaster?

A. Chief Information Officer.

B. Chief Operating Officer.

C. Disaster Recovery Manager.

D. Chief Executive Officer.

Answer: (SHOW ANSWER)

Section: Risk, Response and Recovery

Explanation/Reference:

The Disaster Recovery Manager should also be a member of the team that assisted in the development of the Disaster Recovery Plan. Senior-level management need to support the process but would not be involved with the initial process.

The following answers are incorrect:

Chief Information Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.

Chief Operating Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.
Chief Executive Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.

NEW QUESTION: 145
What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?
A. A
B. D
C. E
D. F
Answer: B (LEAVE A REPLY)
D or "minimal protection" is reserved for systems that were evaluated under the TCSEC but did not meet the requirements for a higher trust level.
A is incorrect. A or "Verified Protectection" is the highest trust level under the TCSEC. E is incorrect. The trust levels are A - D so "E" is not a valid trust level.
F is incorrect. The trust levels are A - D so "F" is not a valid trust level.
CBK, pp. 329 - 330 AIO3, pp. 302 - 306

NEW QUESTION: 146
The typical computer fraudsters are usually persons with which of the following characteristics?
A. They have had previous contact with law enforcement
B. They conspire with others
C. They hold a position of trust
D. They deviate from the accepted norms of society
Answer: C (LEAVE A REPLY)
Explanation/Reference:
These people, as employees, are trusted to perform their duties honestly and not take advantage of the trust placed in them.
The following answers are incorrect:
They have had previous contact with law enforcement. Is incorrect because most often it is a person that holds a position of trust and this answer implies they have a criminal background. This type of individual is typically not in a position of trust within an organization.
They conspire with others. Is incorrect because they typically work alone, often as a form of retribution over a percieved injustice done to them.
They deviate from the accepted norms of society. Is incorrect because while the nature of fraudsters deviate from the norm, the fraudsters often hold a position of trust within the organization.

NEW QUESTION: 147
Which of the following are REGISTERED PORTS as defined by IANA ?
A. Ports 128 to 255
B. Ports 1024 to 49151
C. Ports 1025 to 65535
D. Ports 1024 to 32767
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Ports 1024 to 49151 has been defined as REGISTERED PORTS by IANA.
A registered port is a network port (a sub-address defined within the Internet Protocol, in the range 1-65535) assigned by the Internet Assigned Numbers Authority (IANA) (or by Internet Corporation for Assigned Names and Numbers (ICANN) before March 21, 2001) for use with a certain protocol or application.
Ports with numbers lower than those of the registered ports are called well known ports; ports with numbers greater than those of the registered ports are called dynamic and/or private ports.
Ports 0-1023 - well known ports
Ports 1024-49151 - Registered port: vendors use for applications
Ports >49151 - dynamic / private ports
The other answers are not correct
Reference(s) used for this question:
http://en.wikipedia.org/wiki/Registered_port

NEW QUESTION: 148
Who should DECIDE how a company should approach security and what security measures should be implemented?
A. Senior management
B. Data owner
C. Auditor
D. The information security specialist
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
They are responsible for security of the organization and the protection of its assets.
The following answers are incorrect because :
Data owner is incorrect as data owners should not decide as to what security measures should be applied.
Auditor is also incorrect as auditor cannot decide as to what security measures should be applied.
The information security specialist is also incorrect as they may have the technical knowledge of how security measures should be implemented and configured , but they should not be in a position of deciding what measures should be applied.

Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 51.

NEW QUESTION: 149
Which of the following is NOT a defined ISO basic task related to network management?
A. Fault management
B. Accounting resources
C. Security management
D. Communications management
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
ISO has defined five basic tasks related to network management :
Fault management: Detects the devices that present some kind of fault.
Configuration management: Allows users to know, define and change remotely the configuration of any device.
Accounting resources: Holds the records of the resource usage in the WAN.
Performance management: Monitors usage levels and sets alarms when a threshold has been surpassed.
Security management: Detects suspicious traffic or users and generates alarms accordingly.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 137).

NEW QUESTION: 150
Cable modems are less secure than DSL connections because cable modems are shared with other subscribers?
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 151
According to private sector data classification levels, how would salary levels and medical information be classified?
A. Public.
B. Internal Use Only.
C. Restricted.
D. Confidential.
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Typically there are three to four levels of information classification used by most organizations:

Confidential: Information that, if released or disclosed outside of the organization, would create severe problems for the organization. For example, information that provides a competitive advantage is important to the technical or financial success (like trade secrets, intellectual property, or research designs), or protects the privacy of individuals would be considered confidential. Information may include payroll information, health records, credit information, formulas, technical designs, restricted regulatory information, senior management internal correspondence, or business strategies or plans. These may also be called top secret, privileged, personal, sensitive, or highly confidential. In other words this information is ok within a defined group in the company such as marketing or sales, but is not suited for release to anyone else in the company without permission.
The following answers are incorrect:
Public: Information that may be disclosed to the general public without concern for harming the company, employees, or business partners. No special protections are required, and information in this category is sometimes referred to as unclassified. For example, information that is posted to a company's public Internet site, publicly released announcements, marketing materials, cafeteria menus, and any internal documents that would not present harm to the company if they were disclosed would be classified as public. While there is little concern for confidentiality, integrity and availability should be considered.
Internal Use Only: Information that could be disclosed within the company, but could harm the company if disclosed externally. Information such as customer lists, vendor pricing, organizational policies, standards and procedures, and internal organization announcements would need baseline security protections, but do not rise to the level of protection as confidential information. In other words, the information may be used freely within the company but any unapproved use outside the company can pose a chance of harm.
Restricted: Information that requires the utmost protection or, if discovered by unauthorized personnel, would cause irreparable harm to the organization would have the highest level of classification. There may be very few pieces of information like this within an organization, but data classified at this level requires all the access control and protection mechanisms available to the organization. Even when information classified at this level exists, there will be few copies of it Reference(s) Used for this question: Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 952-976). Auerbach Publications. Kindle Edition.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 152
Configuration Management controls what?
A. Auditing of changes to the Trusted Computing Base.

B. Control of changes to the Trusted Computing Base.
C. Changes in the configuration access to the Trusted Computing Base.
D. Auditing and controlling any changes to the Trusted Computing Base.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
All of these are components of Configuration Management.
The following answers are incorrect:
Auditing of changes to the Trusted Computing Base. Is incorrect because it refers only to auditing the changes, but nothing about controlling them.
Control of changes to the Trusted Computing Base. Is incorrect because it refers only to controlling the changes, but nothing about ensuring the changes will not lead to a weakness or fault in the system.
Changes in the configuration access to the Trusted Computing Base. Is incorrect because this does not refer to controlling the changes or ensuring the changes will not lead to a weakness or fault in the system.

NEW QUESTION: 153
Which one of the following authentication mechanisms creates a problem for mobile users?
A. Mechanisms based on IP addresses
B. Mechanism with reusable passwords
C. one-time password mechanism.
D. challenge response mechanism.
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Anything based on a fixed IP address would be a problem for mobile users because their location and its associated IP address can change from one time to the next. Many providers will assign a new IP every time the device would be restarted. For example an insurance adjuster using a laptop to file claims online. He goes to a different client each time and the address changes every time he connects to the ISP.
NOTE FROM CLEMENT:
The term MOBILE in this case is synonymous with Road Warriors where a user is contantly traveling and changing location. With smartphone today that may not be an issue but it would be an issue for laptops or WIFI tablets. Within a carrier network the IP will tend to be the same and would change rarely. So this question is more applicable to devices that are not cellular devices but in some cases this issue could affect cellular devices as well.
The following answers are incorrect:
mechanism with reusable password. This is incorrect because reusable password mechanism would not present a problem for mobile users. They are the least secure and change only at specific interval.
one-time password mechanism. This is incorrect because a one-time password mechanism would not present a problem for mobile users. Many are based on a clock and not on the IP address of the user.

challenge response mechanism. This is incorrect because challenge response mechanism would not present a problem for mobile users.

NEW QUESTION: 154
Java is not:
A. Object-oriented.
B. Distributed.
C. Architecture Specific.
D. Multithreaded.
Answer: C (LEAVE A REPLY)
JAVA was developed so that the same program could be executed on multiple hardware and operating system platforms, it is not Architecture Specific.
The following answers are incorrect:
Object-oriented. Is not correct because JAVA is object-oriented. It should use the object-oriented programming methodology.
Distributed. Is incorrect because JAVA was developed to be able to be distrubuted, run on multiple computer systems over a network.
Multithreaded. Is incorrect because JAVA is multi-threaded that is calls to subroutines as is the case with object-oriented programming.
A virus is a program that can replicate itself on a system but not necessarily spread itself by network connections.

NEW QUESTION: 155
Why should batch files and scripts be stored in a protected area?
A. Because of the least privilege concept.
B. Because they cannot be accessed by operators.
C. Because they may contain credentials.
D. Because of the need-to-know concept.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully. Operators might need access to batch files and scripts. The least privilege concept requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.
Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

NEW QUESTION: 156
Countermeasures have three main objectives, what are they? (Choose all that apply)

A. Detect
B. Trace
C. Prevent
D. Retaliate
E. Recover
Answer: A,C,E (LEAVE A REPLY)

NEW QUESTION: 157
Within the context of the CBK, which of the following provides a MINIMUM level of security ACCEPTABLE for an environment ?
A. A baseline
B. A standard
C. A procedure
D. A guideline
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Baselines provide the minimum level of security necessary throughout the organization.
Standards specify how hardware and software products should be used throughout the organization.
Procedures are detailed step-by-step instruction on how to achieve certain tasks.
Guidelines are recommendation actions and operational guides to personnel when a specific standard does not apply.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 3:
Security Management Practices (page 94).

NEW QUESTION: 158
What refers to legitimate users accessing networked services that would normally be restricted to them?
A. Spoofing
B. Piggybacking
C. Eavesdropping
D. Logon abuse
Answer: (SHOW ANSWER)
Unauthorized access of restricted network services by the circumvention of security access controls is known as logon abuse. This type of abuse refers to users who may be internal to the network but access resources they would not normally be allowed. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 74).

NEW QUESTION: 159

What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?

A. Biometrics

B. Micrometrics

C. Macrometrics

D. MicroBiometrics

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

NEW QUESTION: 160

What can be defined as: It confirms that users' needs have been met by the supplied solution ?

A. Accreditation

B. Certification

C. Assurance

D. Acceptance

Answer: (SHOW ANSWER)

Acceptance confirms that users' needs have been met by the supplied solution. Verification and Validation informs Acceptance by establishing the evidence - set against acceptance criteria - to determine if the solution meets the users' needs. Acceptance should also explicitly address any integration or interoperability requirements involving other equipment or systems. To enable acceptance every user and system requirement must have a 'testable' characteristic.

Accreditation is the formal acceptance of security, adequacy, authorization for operation and acceptance of existing risk. Accreditation is the formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.

Certification is the formal testing of security safeguards and assurance is the degree of confidence that the implemented security measures work as intended. The certification is a Comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified ecurity requirements.

Assurance is the descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the Security Targets (ST) and Protection Profiles (PP), respectively.

Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 4, August 1999.

and Official ISC2 Guide to the CISSP CBK, Second Edition, on page 211. and
http://www.aof.mod.uk/aofcontent/tactical/randa/content/randaintroduction.htm

NEW QUESTION: 161
Which of the following computer design approaches is based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle?
A. Pipelining
B. Reduced Instruction Set Computers (RISC)
C. Complex Instruction Set Computers (CISC)
D. Scalar processors
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation
Explanation/Reference:
Complex Instruction Set Computer (CISC) uses instructions that perform many operations per instruction. It was based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle.
Therefore, by packing more operations into an instruction, the number of fetches could be reduced. Pipelining involves overlapping the steps of different instructions to increase the performance in a computer. Reduced Instruction Set Computers (RISC) involve simpler instructions that require fewer clock cycles to execute. Scalar processors are processors that execute one instruction at a time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 188).

NEW QUESTION: 162
Which of the following choices describe a Challenge-response tokens generation?
A. A workstation or system that generates a random challenge string that the user enters into the token when prompted along with the proper PIN.
B. A workstation or system that generates a random login id that the user enters when prompted along with the proper PIN.
C. A special hardware device that is used to generate ramdom text in a cryptography system.
D. The authentication mechanism in the workstation or system does not determine if the owner should be authenticated.
Answer: A (LEAVE A REPLY)
Challenge-response tokens are:
-A workstation or system generates a random challenge string and the owner enters the string into the token along with the proper PIN.
-
The token generates a response that is then entered into the workstation or system.
-

The authentication mechanism in the workstation or system then determines if the owner should be authenticated.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 136-137).

NEW QUESTION: 163
What can a packet filtering firewall also be called?
A. a scanning router
B. a shielding router
C. a sniffing router
D. a screening router
Answer: (SHOW ANSWER)
Explanation/Reference:
While neither CBK nor AIO3 use the term "screening router," they both discuss how the packet filtering capabilities of a router can be used to block traffic much like a packet filtering firewall. Krutz and Vine use this term on p. 90.
"A scanning router" is incorrect. This is a nonsense term to distract you.
"A shielding router" is incorrect. This is a nonsense term to distract you.
"A sniffing router" is incorrect. This is a nonsense term to distract you.
References:
CBK, p. 433
AIO3, pp.484 - 485

NEW QUESTION: 164
Which of the following enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks?
A. Risk assessment
B. Residual risks
C. Security controls
D. Business units
Answer: A (LEAVE A REPLY)
The risk assessment is critical because it enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks. The risk management process includes the risk assessment and determination of suitable technical, management, and operational security controls based on the level of threat the risk imposes. Business units should be included in this process. Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 7).

NEW QUESTION: 165
What is called an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets?
A. SYN Flood attack
B. Smurf attack
C. Ping of Death attack
D. Denial of Service (DOS) attack
Answer: B (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Although it may cause a denial of service to the victim's system, this type of attack is a Smurf attack. A SYN Flood attack uses up all of a system's resources by setting up a number of bogus communication sockets on the victim's system. A Ping of Death attack is done by sending IP packets that exceed the maximum legal length (65535 octets).
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11:
Application and System Development (page 789).

NEW QUESTION: 166
Which of the following is true of network security?
A. A firewall is a not a necessity in today's connected world.
B. A firewall is a necessity in today's connected world.
C. A whitewall is a necessity in today's connected world.
D. A black firewall is a necessity in today's connected world.
Answer: B (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Commercial firewalls are a dime-a-dozen in todays world. Black firewall and whitewall are just distracters.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 167
Which TCSEC level is labeled Controlled Access Protection?
A. C1
B. C2

C. C3

D. B1

Answer: (SHOW ANSWER)

C2 is labeled Controlled Access Protection.

The TCSEC defines four divisions: D, C, B and A where division A has the highest security.

Each division represents a significant difference in the trust an individual or organization can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1.

Each division and class expands or modifies as indicated the requirements of the immediately prior division or class. D - Minimal protection

Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division

C - Discretionary protection

C1 - Discretionary Security Protection Identification and authentication Separation of users and data Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis Required System Documentation and user manuals C2 - Controlled Access Protection More finely grained DAC Individual accountability through login procedures Audit trails Object reuse Resource isolation

B - Mandatory protection

B1 - Labeled Security Protection Informal statement of the security policy model Data sensitivity labels Mandatory Access Control (MAC) over selected subjects and objects Label exportation capabilities All discovered flaws must be removed or otherwise mitigated Design specifications and verification B2 - Structured Protection Security policy model clearly defined and formally documented DAC and MAC enforcement extended to all subjects and objects Covert storage channels are analyzed for occurrence and bandwidth Carefully structured into protection-critical and non-protection-critical elements Design and implementation enable more comprehensive testing and review Authentication mechanisms are strengthened Trusted facility management is provided with administrator and operator segregation Strict configuration management controls are imposed B3 - Security Domains Satisfies reference monitor requirements Structured to exclude code not essential to security policy enforcement Significant system engineering directed toward minimizing complexity Security administrator role defined Audit security-relevant events Automated imminent intrusion detection, notification, and response Trusted system recovery procedures Covert timing channels are analyzed for occurrence and bandwidth An example of such a system is the XTS-300, a precursor to the XTS-400

A - Verified protection

A1 - Verified Design Functionally identical to B3 Formal design and verification techniques including a formal top-level specification Formal management and distribution procedures An example of such a system is Honeywell's Secure Communications Processor SCOMP, a precursor to the XTS-400 Beyond A1 System Architecture demonstrates that the requirements of self-protection and completeness for reference monitors have been implemented in the Trusted Computing Base (TCB). Security Testing automatically generates test-case from the formal top-level specification or formal lower-level specifications. Formal Specification and Verification is where the TCB is verified down to the source code

level, using formal verification methods where feasible. Trusted Design Environment is where the TCB is designed in a trusted facility with only trusted (cleared) personnel.
The following are incorrect answers:
C1 is Discretionary security
C3 does not exists, it is only a detractor
B1 is called Labeled Security Protection.
Reference(s) used for this question:
HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.
and
AIOv4 Security Architecture and Design (pages 357 - 361)
AIOv5 Security Architecture and Design (pages 358 - 362)

NEW QUESTION: 168
Which of the following exemplifies proper separation of duties?
A. Operators are not permitted modify the system time.
B. Programmers are permitted to use the system console.
C. Console operators are permitted to mount tapes and disks.
D. Tape operators are permitted to use the system console.
Answer: (SHOW ANSWER)
This is an example of Separation of Duties because operators are prevented from modifying the system time which could lead to fraud. Tasks of this nature should be performed by they system administrators. AIO defines Separation of Duties as a security principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.
The following answers are incorrect: Programmers are permitted to use the system console. Is incorrect because programmers should not be permitted to use the system console, this task should be performed by operators. Allowing programmers access to the system console could allow fraud to occur so this is not an example of Separation of Duties..
Console operators are permitted to mount tapes and disks. Is incorrect because operators should be able to mount tapes and disks so this is not an example of Separation of Duties.
Tape operators are permitted to use the system console. Is incorrect because operators should be able to use the system console so this is not an example of Separation of Duties.
References:
OIG CBK Access Control (page 98 - 101)
AIOv3 Access Control (page 182)

NEW QUESTION: 169
What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?
A. Authentication
B. Identification
C. Authorization

D. Confidentiality

Answer: B (LEAVE A REPLY)

Section: Access Control

Explanation/Reference:

Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system.

Identification is nothing more than claiming you are somebody. You identify yourself when you speak to someone on the phone that you don't know, and they ask you who they're speaking to. When you say, "I'm Jason.", you've just identified yourself.

In the information security world, this is analogous to entering a username. It's not analogous to entering a password. Entering a password is a method for verifying that you are who you identified yourself as.

NOTE: The word "professing" used above means: "to say that you are, do, or feel something when other people doubt what you say". This is exactly what happen when you provide your identifier (identification), you claim to be someone but the system cannot take your word for it, you must further Authenticate to the system to prove who you claim to be.

The following are incorrect answers:

Authentication: is how one proves that they are who they say they are. When you claim to be Jane Smith by logging into a computer system as "jsmith", it's most likely going to ask you for a password. You've claimed to be that person by entering the name into the username field (that's the identification part), but now you have to prove that you are really that person.

Many systems use a password for this, which is based on "something you know", i.e. a secret between you and the system.

Another form of authentication is presenting something you have, such as a driver's license, an RSA token, or a smart card.

You can also authenticate via something you are. This is the foundation for biometrics. When you do this, you first identify yourself and then submit a thumb print, a retina scan, or another form of bio-based authentication.

Once you've successfully authenticated, you have now done two things: you've claimed to be someone, and you've proven that you are that person. The only thing that's left is for the system to determine what you're allowed to do.

Authorization: is what takes place after a person has been both identified and authenticated; it's the step determines what a person can then do on the system.

An example in people terms would be someone knocking on your door at night. You say, "Who is it?", and wait for a response. They say, "It's John." in order to identify themselves. You ask them to back up into the light so you can see them through the peephole. They do so, and you authenticate them based on what they look like (biometric). At that point you decide they can come inside the house.

If they had said they were someone you didn't want in your house (identification), and you then verified that it was that person (authentication), the authorization phase would not include access to the inside of the house.

Confidentiality: Is one part of the CIA triad. It prevents sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. A good example is a credit card number

while shopping online, the merchant needs it to clear the transaction but you do not want your informaiton exposed over the network, you would use a secure link such as SSL, TLS, or some tunneling tool to protect the information from prying eyes between point A and point B. Data encryption is a common method of ensuring confidentiality.
The other parts of the CIA triad are listed below:
Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.
Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. If an unexpected change occurs, a backup copy must be available to restore the affected data to its correct state.
Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, providing a certain measure of redundancy and failover, providing adequate communications bandwidth and preventing the occurrence of bottlenecks, implementing emergency backup power systems, keeping current with all necessary system upgrades, and guarding against malicious actions such as denial-of- service (DoS) attacks.
Reference used for this question:
http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
http://www.danielmiessler.com/blog/security-identification-authentication-and-authorization
http://www.merriam-webster.com/dictionary/profess
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 170
Rule-Based Access Control (RuBAC) access is determined by rules. Such rules would fit within what category of access control ?
A. Discretionary Access Control (DAC)
B. Mandatory Access control (MAC)
C. Non-Discretionary Access Control (NDAC)
D. Lattice-based Access control
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Rule-based access control is a type of non-discretionary access control because this access is determined by rules and the subject does not decide what those rules will be, the rules are uniformly applied to ALL of the users or subjects.
In general, all access control policies other than DAC are grouped in the category of non-discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action.

Both Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC) fall within Non Discretionary Access Control (NDAC). If it is not DAC or MAC then it is most likely NDAC.

IT IS NOT ALWAYS BLACK OR WHITE

The different access control models are not totally exclusive of each others. MAC is making use of Rules to be implemented. However with MAC you have requirements above and beyond having simple access rules. The subject would get formal approval from management, the subject must have the proper security clearance, objects must have labels/sensitivity levels attached to them, subjects must have the proper security clearance. If all of this is in place then you have MAC.

BELOW YOU HAVE A DESCRIPTION OF THE DIFFERENT CATEGORIES:

MAC = Mandatory Access Control

Under a mandatory access control environment, the system or security administrator will define what permissions subjects have on objects. The administrator does not dictate user's access but simply configure the proper level of access as dictated by the Data Owner.

The MAC system will look at the Security Clearance of the subject and compare it with the object sensitivity level or classification level. This is what is called the dominance relationship.

The subject must DOMINATE the object sensitivity level. Which means that the subject must have a security clearance equal or higher than the object he is attempting to access.

MAC also introduce the concept of labels. Every objects will have a label attached to them indicating the classification of the object as well as categories that are used to impose the need to know (NTK) principle.

Even thou a user has a security clearance of Secret it does not mean he would be able to access any Secret documents within the system. He would be allowed to access only Secret document for which he has a Need To Know, formal approval, and object where the user belong to one of the categories attached to the object.

If there is no clearance and no labels then IT IS NOT Mandatory Access Control.

Many of the other models can mimic MAC but none of them have labels and a dominance relationship so they are NOT in the MAC category.

NISTR-7316 Says:

Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the "simple security rule," or "no read up." Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the "*-property" (pronounced "star property") or "no write down." The *-property is required to maintain system security in an automated environment. A variation on this rule called the "strict *-property" requires that information can be written at, but not above, the subject's clearance level. Multilevel security models such as the Bell-La Padula Confidentiality and Biba Integrity models are used to formally specify this kind of MAC policy.

DAC = Discretionary Access Control

DAC is also known as: Identity Based access control system.

The owner of an object is define as the person who created the object. As such the owner has the discretion to grant access to other users on the network. Access will be granted based solely on the identity of those users.
Such system is good for low level of security. One of the major problem is the fact that a user who has access to someone's else file can further share the file with other users without the knowledge or permission of the owner of the file. Very quickly this could become the wild wild west as there is no control on the dissimination of the information.
RBAC = Role Based Access Control
RBAC is a form of Non-Discretionary access control.
Role Based access control usually maps directly with the different types of jobs performed by employees within a company.
For example there might be 5 security administrator within your company. Instead of creating each of their profile one by one, you would simply create a role and assign the administrators to the role. Once an administrator has been assigned to a role, he will IMPLICITLY inherit the permissions of that role.
RBAC is great tool for environment where there is a a large rotation of employees on a daily basis such as a very large help desk for example.
RBAC or RuBAC = Rule Based Access Control
RuBAC is a form of Non-Discretionary access control.
A good example of a Rule Based access control device would be a Firewall. A single set of rules is imposed to all users attempting to connect through the firewall.
NOTE FROM CLEMENT:
Lot of people tend to confuse MAC and Rule Based Access Control.
Mandatory Access Control must make use of LABELS. If there is only rules and no label, it cannot be Mandatory Access Control. This is why they call it Non Discretionary Access control (NDAC).
There are even books out there that are WRONG on this subject. Books are sometimes opiniated and not strictly based on facts.
In MAC subjects must have clearance to access sensitive objects. Objects have labels that contain the classification to indicate the sensitivity of the object and the label also has categories to enforce the need to know.
Today the best example of rule based access control would be a firewall. All rules are imposed globally to any user attempting to connect through the device. This is NOT the case with MAC.
I strongly recommend you read carefully the following document:
NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf It is one of the best Access Control Study document to prepare for the exam. Usually I tell people not to worry about the hundreds of NIST documents and other reference. This document is an exception. Take some time to read it.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.
and
NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf and
Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Locations 651-

652). Elsevier Science (reference). Kindle Edition.

NEW QUESTION: 171
What is called the type of access control where there are pairs of elements that have the least upper bound of values and greatest lower bound of values?
A. Mandatory model
B. Discretionary model
C. Lattice model
D. Rule model
Answer: C (LEAVE A REPLY)
Explanation/Reference:
In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 172
Which of the following choice is NOT normally part of the questions that would be asked in regards to an organization's information security policy?
A. Who is involved in establishing the security policy?
B. Where is the organization's security policy defined?
C. What are the actions that need to be performed in case of a disaster?
D. Who is responsible for monitoring compliance to the organization's security policy?
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Actions to be performed in case of a disaster are not normally part of an information security policy but part of a Disaster Recovery Plan (DRP).
Only personnel implicated in the plan should have a copy of the Disaster Recovery Plan whereas everyone should be aware of the contents of the organization's information security policy.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 398).

NEW QUESTION: 173
An alternative to using passwords for authentication in logical or technical access control is:
A. manage without passwords
B. biometrics
C. not there
D. use of them for physical access control
Answer: B (LEAVE A REPLY)

An alternative to using passwords for authentication in logical or technical access control is biometrics. Biometrics are based on the Type 3 authentication mechanism-something you are. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION: 174
An application layer firewall is also called a:
A. Proxy
B. A Presentation Layer Gateway.
C. A Session Layer Gateway.
D. A Transport Layer Gateway.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
An application layer firewall can also be called a proxy.
"A presentation layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.
"A session layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.
"A transport layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.
References:
CBK, p. 467
AIO3, pp. 486 - 490, 960

NEW QUESTION: 175
Which of the following questions is less likely to help in assessing an organization's contingency planning controls?
A. Is damaged media stored and/or destroyed?
B. Are the backup storage site and alternate site geographically far enough from the primary site?
C. Is there an up-to-date copy of the plan stored securely off-site?
D. Is the location of stored backups identified?
Answer: A (LEAVE A REPLY)
Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small.
Handling of damaged media is an operational task related to regular production and is not specific to contingency planning. Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-27 to A-28).

NEW QUESTION: 176
Which of the following is true related to network sniffing?
A. Sniffers allow an attacker to monitor data passing across a network.
B. Sniffers alter the source address of a computer to disguise and exploit weak authentication methods.
C. Sniffers take over network connections.
D. Sniffers send IP fragments to a system that overlap with each other.
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The following answers are incorrect: Sniffers alter the source address of a computer to disguise and exploit weak authentication methods. IP Spoofing is a network-based attack, which involves altering the source address of a computer to disguise the attacker and exploit weak authentication methods.
Sniffers take over network connections. Session Hijacking tools allow an attacker to take over network connections, kicking off the legitimate user or sharing a login.
Sniffers send IP fragments to a system that overlap with each other. Malformed Packet attacks are a type of DoS attack that involves one or two packets that are formatted in an unexpected way. Many vendor product implementations do not take into account all variations of user entries or packet types. If software handles such errors poorly, the system may crash when it receives such packets. A classic example of this type of attack involves sending IP fragments to a system that overlap with each other (the fragment offset values are incorrectly set. Some unpatched Windows and Linux systems will crash when the encounter such packets.
The following reference(s) were/was used to create this question:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, Auerbach, NY, NY 2001, Chapter 22, Hacker Tools and Techniques by Ed Skoudis. ISC2 OIG, 2007 p. 137-138, 419

NEW QUESTION: 177
Which of the following is used to interrupt the opportunity to use or perform collusion to subvert operation for fraudulent purposes?
A. Key escrow
B. Rotation of duties
C. Principle of need-to-know
D. Principle of least privilege
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation
Explanation/Reference:
Job rotations reduce the risk of collusion of activities between individuals. Companies with individuals working with sensitive information or systems where there might be the opportunity for personal gain through collusion can benefit by integrating job rotation with segregation of duties. Rotating the position

may uncover activities that the individual is performing outside of the normal operating procedures, highlighting errors or fraudulent behavior.
Rotation of duties is a method of reducing the risk associated with a subject performing a (sensitive) task by limiting the amount of time the subject is assigned to perform the task before being moved to a different task.
The following are incorrect answers:
Key escrow is related to the protection of keys in storage by splitting the key in pieces that will be controlled by different departments. Key escrow is the process of ensuring a third party maintains a copy of a private key or key needed to decrypt information. Key escrow also should be considered mandatory for most organization's use of cryptography as encrypted information belongs to the organization and not the individual; however often an individual's key is used to encrypt the information.
Separation of duties is a basic control that prevents or detects errors and irregularities by assigning responsibility for different parts of critical tasks to separate individuals, thus limiting the effect a single person can have on a system. One individual should not have the capability to execute all of the steps of a particular process. This is especially important in critical business areas, where individuals may have greater access and capability to modify, delete, or add data to the system. Failure to separate duties could result in individuals embezzling money from the company without the involvement of others.
The need-to-know principle specifies that a person must not only be cleared to access classified or other sensitive information, but have requirement for such information to carry out assigned job duties.
Ordinary or limited user accounts are what most users are assigned. They should be restricted only to those privileges that are strictly required, following the principle of least privilege. Access should be limited to specific objects following the principle of need-to-know.
The principle of least privilege requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. Least privilege refers to granting users only the accesses that are required to perform their job functions. Some employees will require greater access than others based upon their job functions. For example, an individual performing data entry on a mainframe system may have no need for Internet access or the ability to run reports regarding the information that they are entering into the system. Conversely, a supervisor may have the need to run reports, but should not be provided the capability to change information in the database.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10628-10631). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10635-10638). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10693-10697). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 16338-16341). Auerbach Publications. Kindle Edition.

NEW QUESTION: 178
Which of the following is NOT a VPN communications protocol standard?
A. Point-to-point tunnelling protocol (PPTP)
B. Challenge Handshake Authentication Protocol (CHAP)
C. Layer 2 tunnelling protocol (L2TP)
D. IP Security
Answer: B (LEAVE A REPLY)
Explanation/Reference:
CHAP is an authentication mechanism for point-to-point protocol connections that encrypt the user's password. It is a protocol that uses a three-way handshake. The server sends the client a challenge, which includes a random value (a nonce) to thwart replay attacks. The client responds with a MD5 hash of the nonce and the password. The authentication is successful if the client's response is the one that the server expected.
The VPN communication protocol standards listed above are PPTP, L2TP and IPSec.
PPTP and L2TP operate at the data link layer (layer 2) of the OSI model and enable only a single point-to- point connection per session.
The following are incorrect answers:
PPTP uses native PPP authentication and encryption services. Point-to-Point Tunneling Protocol (PPTP) is a VPN protocol that runs over other protocols. PPTP relies on generic routing encapsulation (GRE) to build the tunnel between the endpoints. After the user authenticates, typically with Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2), a Point-to-Point Protocol (PPP) session creates a tunnel using GRE.
L2TP is a combination of PPTP and the earlier Layer 2 Forwarding protocol (L2F). Layer 2 Tunneling Protocol (L2TP) is a hybrid of Cisco's Layer 2 Forwarding (L2F) and Microsoft's PPTP. It allows callers over a serial line using PPP to connect over the Internet to a remote network. A dial-up user connects to his ISP's L2TP access concentrator (LAC) with a PPP connection. The LAC encapsulates the PPP packets into L2TP and forwards it to the remote network's layer 2 network server (LNS). At this point, the LNS authenticates the dial-up user. If authentication is successful, the dial-up user will have access to the remote network.
IPSec operates at the network layer (layer 3) and enables multiple simultaneous tunnels. IP Security (IPSec) is a suite of protocols for communicating securely with IP by providing mechanisms for authenticating and encryption. Implementation of IPSec is mandatory in IPv6, and many organizations are using it over IPv4. Further, IPSec can be implemented in two modes, one that is appropriate for end-to-end protection and one that safeguards traffic between networks.
Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7067-7071). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6987-6990). Auerbach Publications. Kindle Edition.

NEW QUESTION: 179
Which access control model is also called Non Discretionary Access Control (NDAC)?
A. Lattice based access control
B. Mandatory access control
C. Role-based access control
D. Label-based access control
Answer: C (LEAVE A REPLY)
Explanation/Reference:
RBAC is sometimes also called non-discretionary access control (NDAC) (as Ferraiolo says "to distinguish it from the policy-based specifics of MAC"). Another model that fits within the NDAC category is Rule- Based Access Control (RuBAC or RBAC). Most of the CISSP books use the same acronym for both models but NIST tend to use a lowercase "u" in between R and B to differentiate the two models. You can certainly mimic MAC using RBAC but true MAC makes use of Labels which contains the sensitivity of the objects and the categories they belong to. No labels means MAC is not being used.
One of the most fundamental data access control decisions an organization must make is the amount of control it will give system and data owners to specify the level of access users of that data will have. In every organization there is a balancing point between the access controls enforced by organization and system policy and the ability for information owners to determine who can have access based on specific business requirements. The process of translating that balance into a workable access control model can be defined by three general access frameworks:
Discretionary access control
Mandatory access control
Nondiscretionary access control
A role-based access control (RBAC) model bases the access control authorizations on the roles (or functions) that the user is assigned within an organization. The determination of what roles have access to a resource can be governed by the owner of the data, as with DACs, or applied based on policy, as with MACs.
Access control decisions are based on job function, previously defined and governed by policy, and each role (job function) will have its own access capabilities. Objects associated with a role will inherit privileges assigned to that role. This is also true for groups of users, allowing administrators to simplify access control strategies by assigning users to groups and groups to roles.
There are several approaches to RBAC. As with many system controls, there are variations on how they can be applied within a computer system.
There are four basic RBAC architectures:
1. Non-RBAC: Non-RBAC is simply a user-granted access to data or an application by traditional mapping, such as with ACLs. There are no formal "roles" associated with the mappings, other than any identified by the particular user.
2. Limited RBAC: Limited RBAC is achieved when users are mapped to roles within a single application rather than through an organization-wide role structure. Users in a limited RBAC system are also able to access non-RBAC-based applications or data. For example, a user may be assigned to multiple roles

within several applications and, in addition, have direct access to another application or system independent of his or her assigned role. The key attribute of limited RBAC is that the role for that user is defined within an application and not necessarily based on the user's organizational job function.
3. Hybrid RBAC: Hybrid RBAC introduces the use of a role that is applied to multiple applications or systems based on a user's specific role within the organization. That role is then applied to applications or systems that subscribe to the organization's role-based model. However, as the term "hybrid" suggests, there are instances where the subject may also be assigned to roles defined solely within specific applications, complimenting (or, perhaps, contradicting) the larger, more encompassing organizational role used by other systems.
4. Full RBAC: Full RBAC systems are controlled by roles defined by the organization's policy and access control infrastructure and then applied to applications and systems across the enterprise. The applications, systems, and associated data apply permissions based on that enterprise definition, and not one defined by a specific application or system.
Be careful not to try to make MAC and DAC opposites of each other -- they are two different access control strategies with RBAC being a third strategy that was defined later to address some of the limitations of MAC and DAC.
The other answers are not correct because:
Mandatory access control is incorrect because though it is by definition not discretionary, it is not called "non-discretionary access control." MAC makes use of label to indicate the sensitivity of the object and it also makes use of categories to implement the need to know.
Label-based access control is incorrect because this is not a name for a type of access control but simply a bogus detractor.
Lattice based access control is not adequate either. A lattice is a series of levels and a subject will be granted an upper and lower bound within the series of levels. These levels could be sensitivity levels or they could be confidentiality levels or they could be integrity levels.
Reference(s) used for this question:
All in One, third edition, page 165.
Ferraiolo, D., Kuhn, D. & Chandramouli, R. (2003). Role-Based Access Control, p. 18.
Ferraiolo, D., Kuhn, D. (1992). Role-Based Access Controls. http://csrc.nist.gov/rbac/Role_Based_Access_Control-1992.html
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 1557-1584). Auerbach Publications. Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 1474-1477). Auerbach Publications. Kindle Edition.

NEW QUESTION: 180
Which expert system operating mode allows determining if a given hypothesis is valid?
A. Blackboard
B. Lateral chaining
C. Forward chaining
D. Backward chaining

Answer: D (LEAVE A REPLY)
Backward-chaining mode - the expert system backtracks to determine if a given hypothesis is valid. Backward-chaining is generally used when there are a large number of possible solutions relative to the number of inputs.
Incorrect answers are:
In a forward-chaining mode, the expert system acquires information and comes to a conclusion based on that information. Forward-chaining is the reasoning approach that can be used when there is a small number of solutions relative to the number of inputs.
Blackboard is an expert system-reasoning methodology in which a solution is generated by the use of a virtual blackboard, wherein information or potential solutions are placed on the blackboard by a plurality of individuals or expert knowledge sources. As more information is placed on the blackboard in an iterative process, a solution is generated.
Lateral-chaining mode - No such expert system mode.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 259).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Expert Systems (page 354).

NEW QUESTION: 181
What are the three FUNDAMENTAL principles of security?
A. Accountability, confidentiality and integrity
B. Confidentiality, integrity and availability
C. Integrity, availability and accountability
D. Availability, accountability and confidentiality
Answer: B (LEAVE A REPLY)
The following answers are incorrect because:
Accountability, confidentiality and integrity is not the correct answer as Accountability is not one of the fundamental principle of security.
Integrity, availability and accountability is not the correct answer as Accountability is not one of the fundamental principle of security.
Availability, accountability and confidentiality is not the correct answer as Accountability is not one of the fundamental objective of security.
References : Shon Harris AIO v3 , Chapter - 3: Security Management Practices , Pages : 49-52

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine

here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 182
The ability to identify and audit a user and his / her actions is known as _____.
A. Forensics
B. Accessibility
C. Auditing
D. Accountability
E. Journaling
Answer: D (LEAVE A REPLY)

NEW QUESTION: 183
Which of the following control pairing places emphasis on "soft" mechanisms that support the access control objectives?
A. Preventive/Technical Pairing
B. Preventive/Administrative Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing
Answer: B (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Soft Control is another way of referring to Administrative control.
Technical and Physical controls are NOT soft control, so any choice listing them was not the best answer.
Preventative/Technical is incorrect because although access control can be technical control, it is commonly not referred to as a "soft" control Preventative/Administrative is correct because access controls are preventative in nature. it is always best to prevent a negative event, however there are times where controls might fail and you cannot prevent everything.
Administrative controls are roles, responsibilities, policies, etc which are usually paper based. In the administrative category you would find audit, monitoring, and security awareness as well.
Preventative/Physical pairing is incorrect because Access controls with an emphasis on "soft" mechanisms conflict with the basic concept of physical controls, physical controls are usually tangible objects such as fences, gates, door locks, sensors, etc...
Detective/Administrative Pairing is incorrect because access control is a preventative control used to control access, not to detect violations to access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 184
The Clipper Chip utilizes which concept in public key cryptography?

A. Substitution
B. Key Escrow
C. An undefined algorithm
D. Super strong encryption
Answer: B (LEAVE A REPLY)
The Clipper chip is a chipset that was developed and promoted by the U.S. Government as an encryption device to be adopted by telecommunications companies for voice transmission. It was announced in 1993 and by 1996 was entirely defunct.
The heart of the concept was key escrow. In the factory, any new telephone or other device with a Clipper chip would be given a "cryptographic key", that would then be provided to the government in "escrow". If government agencies "established their authority" to listen to a communication, then the password would be given to those government agencies, who could then decrypt all data transmitted by that particular telephone.
The CISSP Prep Guide states, "The idea is to divide the key into two parts, and to escrow two portions of the key with two separate 'trusted' organizations. Then, law enforcement officals, after obtaining a court order, can retreive the two pieces of the key from the organizations and decrypt the message."
References:
http://en.wikipedia.org/wiki/Clipper_Chip and Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 166.

NEW QUESTION: 185
To be admissible in court, computer evidence must be which of the following?
A. Relevant
B. Decrypted
C. Edited
D. Incriminating
Answer: A (LEAVE A REPLY)
Before any evidence can be admissible in court, the evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence. This holds true for computer evidence as well.
While there are no absolute means to ensure that evidence will be allowed and helpful in a court of law, information security professionals should understand the basic rules of evidence. Evidence should be relevant, authentic, accurate, complete, and convincing. Evidence gathering should emphasize these criteria.
As stated in CISSP for Dummies:
Because computer-generated evidence can sometimes be easily manipulated, altered , or tampered with, and because it's not easily and commonly understood, this type of evidence is usually considered suspect in a court of law. In order to be admissible, evidence must be
Relevant: It must tend to prove or disprove facts that are relevant and material to the case.
Reliable: It must be reasonably proven that what is presented as evidence is what was originally collected and that the evidence itself is reliable. This is accomplished, in part, through proper evidence

handling and the chain of custody. (We discuss this in the upcoming section "Chain of custody and the evidence life cycle.")
Legally permissible: It must be obtained through legal means. Evidence that's not legally permissible may include evidence obtained through the following means:
Illegal search and seizure: Law enforcement personnel must obtain a prior court order; however, non-law enforcement personnel, such as a supervisor or system administrator, may be able to conduct an authorized search under some circumstances.
Illegal wiretaps or phone taps: Anyone conducting wiretaps or phone taps must obtain a prior court order.
Entrapment or enticement: Entrapment encourages someone to commit a crime that the individual may have had no intention of committing. Conversely, enticement lures someone toward certain evidence (a honey pot, if you will) after that individual has already committed a crime. Enticement is not necessarily illegal but does raise certain ethical arguments and may not be admissible in court.
Coercion: Coerced testimony or confessions are not legally permissible.
Unauthorized or improper monitoring: Active monitoring must be properly authorized and conducted in a standard manner; users must be notified that they may be subject to monitoring.
The following answers are incorrect:
decrypted. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence.
edited. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence. Edited evidence violates the rules of evidence.
incriminating. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence.
Reference(s) used for this question:
CISSP STudy Guide (Conrad, Misenar, Feldman) Elsevier. 2012. Page 423
and Mc Graw Hill, Shon Harris CISSP All In One (AIO), 6th Edition , Pages 1051-1056 and CISSP for Dummies , Peter Gregory

NEW QUESTION: 186
Examples of types of physical access controls include all EXCEPT which of the following?
A. badges
B. locks
C. guards
D. passwords
Answer: (SHOW ANSWER)
Explanation/Reference:
Passwords are considered a Preventive/Technical (logical) control.
The following answers are incorrect:
badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.
locks Locks are a Preventative Physical control and has no Technical association.

guards Guards are a Preventative Physical control and has no Technical association.
The following reference(s) were/was used to create this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 35).

NEW QUESTION: 187
Within the realm of IT security, which of the following combinations best defines risk?
A. Threat coupled with a breach
B. Threat coupled with a vulnerability
C. Vulnerability coupled with an attack
D. Threat coupled with a breach of security
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
The Answer: Threat coupled with a vulnerability. Threats are circumstances or actions with the ability to harm a system. They can destroy or modify data or result an a DoS. Threats by themselves are not acted upon unless there is a vulnerability that can be taken advantage of. Risk enters the equation when a vulnerability (Flaw or weakness) exists in policies, procedures, personnel management, hardware, software or facilities and can be exploited by a threat agent. Vulnerabilities do not cause harm, but they leave the system open to harm. The combination of a threat with a vulnerability increases the risk to the system of an intrusion.
The following answers are incorrect:
Threat coupled with a breach. A threat is the potential that a particular threat-source will take advantage of a vulnerability. Breaches get around security. It does not matter if a breach is discovered or not, it has still occured and is not a risk of something occuring. A breach would quite often be termed as an incident or intrusion.
Vulnerability coupled with an attack. Vulnerabilities are weaknesses (flaws) in policies, procedures, personnel management, hardware, software or factilities that may result in a harmful intrusion to an IT system. An attack takes advantage of the flaw or vulnerability. Attacks are explicit attempts to violate security, and are more than risk as they are active.
Threat coupled with a breach of security. This is a detractor. Although a threat agent may take advantage of (Breach) vulnerabilities or flaws in systems security. A threat coupled with a breach of security is more than a risk as this is active.
The following reference(s) may be used to research the Qs in this question:
ISC2 OIG, 2007 p. 66-67
Shon Harris AIO v3 p. 71-72

NEW QUESTION: 188
A business continuity plan should list and prioritize the services that need to be brought back after a disaster strikes. Which of the following services is more likely to be of primary concern in the context of what your Disaster Recovery Plan would include?

A. Marketing/Public relations
B. Data/Telecomm/IS facilities
C. IS Operations
D. Facilities security
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
The main concern when recovering after a disaster is data, telecomm and IS facilities. Other services, in descending priority order are: IS operations, IS support services, market structure, marketing/public relations, customer service & systems support, market regulation/surveillance, listing, application development, accounting services, facilities, human resources, facilities security, legal and Office of the Secretary, national sales.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 129).

NEW QUESTION: 189
What can be defined as an event that could cause harm to the information systems?
A. A risk
B. A threat
C. A vulnerability
D. A weakness
Answer: (SHOW ANSWER)
Explanation/Reference:
A threat is an event or activity that has the potential to cause harm to the information systems. A risk is the probability that a threat will materialize. A vulnerability, or weakness, is a lack of a safeguard, which may be exploited by a threat, causing harm to the information systems.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 1: Access Control Systems (page 32).

NEW QUESTION: 190
Which of the following are the steps usually followed in the development of documents such as security policy, standards and procedures?
A. design, development, publication, coding, and testing.
B. design, evaluation, approval, publication, and implementation.
C. initiation, evaluation, development, approval, publication, implementation, and maintenance.
D. feasibility, development, approval, implementation, and integration.
Answer: (SHOW ANSWER)
The common steps used the the development of security policy are initiation of the project, evaluation, development, approval, publication, implementation, and maintenance. The other choices listed are the phases of the software development life cycle and not the step used to develop ducuments such as Policies, Standards, etc...

Reference: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.

NEW QUESTION: 191
You have been tasked to develop an effective information classification program. Which one of the following steps should be performed first?
A. Establish procedures for periodically reviewing the classification and ownership
B. Specify the security controls required for each classification level
C. Identify the data custodian who will be responsible for maintaining the security level of data
D. Specify the criteria that will determine how data is classified
Answer: D (LEAVE A REPLY)
Explanation/Reference:
According to the AIO 3rd edition, these are the necessary steps for a proper classification program:
1. Define classification levels.
2. Specify the criteria that will determine how data is classified.
3. Have the data owner indicate the classification of the data she is responsible for.
4. Identify the data custodian who will be responsible for maintaining data and its security level.
5. Indicate the security controls, or protection mechanisms, that are required for each classification level.
6. Document any exceptions to the previous classification issues.
7. Indicate the methods that can be used to transfer custody of the information to a different data owner.
8. Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian.
9. Indicate termination procedures for declassifying the data.
10. Integrate these issues into the security-awareness program so that all employees understand how to handle data at different classification levels.
Domain: Information security and risk management
Reference: AIO 3rd edition page 50

NEW QUESTION: 192
In which of the following security models is the subject's clearance compared to the object's classification such that specific rules can be applied to control how the subject-to-object interactions take place?
A. Bell-LaPadula model
B. Biba model
C. Access Matrix model
D. Take-Grant model
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The Bell-LAPadula model is also called a multilevel security system because users with different clearances use the system and the system processes data with different classifications. Developed by the US Military in the 1970s.

A security model maps the abstract goals of the policy to information system terms by specifying explicit data structures and techniques necessary to enforce the security policy. A security model is usually represented in mathematics and analytical ideas, which are mapped to system specifications and then developed by programmers through programming code. So we have a policy that encompasses security goals, such as
"each subject must be authenticated and authorized before accessing an object." The security model takes this requirement and provides the necessary mathematical formulas, relationships, and logic structure to be followed to accomplish this goal.
A system that employs the Bell-LaPadula model is called a multilevel security system because users with different clearances use the system, and the system processes data at different classification levels. The level at which information is classified determines the handling procedures that should be used. The Bell-LaPadula model is a state machine model that enforces the confidentiality aspects of access control. A matrix and security levels are used to determine if subjects can access different objects. The subject's clearance is compared to the object's classification and then specific rules are applied to control how subject-to-object subject-to-object interactions can take place.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 369). McGraw-Hill. Kindle Edition.

NEW QUESTION: 193
How would nonrepudiation be best classified as?
A. A preventive control
B. A logical control
C. A corrective control
D. A compensating control
Answer: (SHOW ANSWER)
Explanation/Reference:
Systems accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Because the mechanisms implemented in nonrepudiation prevent the ability to successfully repudiate an action, it can be considered as a preventive control.
Source: STONEBURNER, Gary, NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security, National Institute of Standards and Technology, December 2001, page 7.

NEW QUESTION: 194
L2TP is considered to be a less secure protocol than PPTP.
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 195

What can be best defined as the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment?

A. Risk management

B. Risk analysis

C. Threat analysis

D. Due diligence

Answer: (SHOW ANSWER)

Explanation/Reference:

Threat analysis is the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

The following answers are incorrect:

Risk analysis is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.

Risk analysis is synonymous with risk assessment and part of risk management, which is the ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost- effective controls to achieve and maintain an acceptable level or risk.

Due Diligence is identifying possible risks that could affect a company based on best practices and standards.

Reference(s) used for this question:

STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page B-3).

NEW QUESTION: 196

FTP, TFTP, SNMP, and SMTP are provided at what level of the Open Systems Interconnect (OSI) Reference Model?

A. Application

B. Network

C. Presentation

D. Transport

Answer: A (LEAVE A REPLY)

Section: Network and Telecommunications

Explanation/Reference:

The Answer: Application. The Layer 7 Application Layer of the Open Systems Interconnect (OSI) Reference Model is a service for applications and Operating Systems data transmission, for example FTP, TFTP, SNMP, and SMTP.

The following answers are incorrect:

Network. The Network layer moves information between hosts that are not physically connected. It deals with routing of information. IP is a protocol that is used in Network Layer. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 3 Network Layer in the OSI Reference Model.

Presentation. The Presentation Layer is concerned with the formatting of data into a standard presentation such as ASCII. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 6 Presentation Layer in the OSI Reference Model.
Transport. The Transport Layer creates an end-to-end transportation between peer hosts. The transmission can be connectionless and unreliable such as UDP, or connection-oriented and ensure error-free delivery such as TCP. FTP, TFTP, SNMP, and SMTP do not reside at the Layer 4 Transportation Layer in the OSI Reference Model.
The following reference(s) were/was used to create this question: Reference: OSI/ISO.
Shon Harris AIO v.3 p. 420-421
ISC2 OIG, 2997 p.412-413

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 197
Which of the following would provide the BEST stress testing environment taking under consideration and avoiding possible data exposure and leaks of sensitive data?
A. Test environment using test data.
B. Test environment using sanitized live workloads data.
C. Production environment using test data.
D. Production environment using sanitized live workloads data.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
The best way to properly verify an application or system during a stress test would be to expose it to "live" data that has been sanitized to avoid exposing any sensitive information or Personally Identifiable Data (PII) while in a testing environment. Fabricated test data may not be as varied, complex or computationally demanding as "live" data. A production environment should never be used to test a product, as a production environment is one where the application or system is being put to commercial or operational use. It is a best practice to perform testing in a non-production environment.
Stress testing is carried out to ensure a system can cope with production workloads, but as it may be tested to destruction, a test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment. If only test data is used, there is no certainty that the system was adequately stress tested.
Incorrect answers:
Test environment using test data. This is incorrect because live data is typically more useful during stress testing

Production environment using test data. This is incorrect because the production environment should not be used for testing.
Production environment using live workloads. This is incorrect because the production environment should not be used for testing.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).
And:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 251.
And:

NEW QUESTION: 198
Which of the following statements pertaining to IPSec is incorrect?
A. IPSec can help in protecting networks from some of the IP network attacks.
B. IPSec provides confidentiality and integrity to information transferred over IP networks through transport layer encryption and authentication.
C. IPSec protects against man-in-the-middle attacks.
D. IPSec protects against spoofing.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
IPSec provides confidentiality and integrity to information transferred over IP networks through network (not transport) layer encryption and authentication. All other statements are correct.
Source: TIPTON, Harold F & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 6, Extranet Access Control Issues (page 110).

NEW QUESTION: 199
A _____ is a program that poses as a useful or legitimate program, but turns out to be malicious code.
A. Trojan Horse
B. Worm
C. Polymorphic Virus
D. Logic Bomb
Answer: A (LEAVE A REPLY)

NEW QUESTION: 200
Which of the following forms of authentication would most likely apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier?
A. Dynamic authentication
B. Continuous authentication
C. Encrypted authentication

D. Robust authentication

Answer: (SHOW ANSWER)

Continuous authentication is a type of authentication that provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect. Robust authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, but does not provide protection against active attacks. Encrypted authentication is a distracter. Source: GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 34).

NEW QUESTION: 201

A code, as is pertains to cryptography:

A. Is a generic term for encryption.

B. Is specific to substitution ciphers.

C. Deals with linguistic units.

D. Is specific to transposition ciphers.

Answer: C (LEAVE A REPLY)

Historically, a code refers to a cryptosystem that deals with linguistic units: words, phrases, sentences, and so forth. Codes are only useful for specialized circumstances where the message to transmit has an already defined equivalent ciphertext word. Source: DUPUIS, Cl?ment, CISSP Open Study Guide on domain 5, cryptography, April
1999.

NEW QUESTION: 202

Which of the following statements relating to the Bell-LaPadula security model is FALSE (assuming the Strong Star property is not being used) ?

A. A subject is not allowed to read up.

B. The property restriction can be escaped by temporarily downgrading a high level subject.

C. A subject is not allowed to read down.

D. It is restricted to confidentiality.

Answer: C (LEAVE A REPLY)

Explanation/Reference:

It is not a property of Bell LaPadula model.

The other answers are incorrect because:

A subject is not allowed to read up is a property of the 'simple security rule' of Bell LaPadula model.

The property restriction can be escaped by temporarily downgrading a high level subject can be escaped by temporarily downgrading a high level subject or by identifying a set of trusted objects which are permitted to violate the property as long as it is not in the middle of an operation.
It is restricted to confidentiality as it is a state machine model that enforces the confidentiality aspects of access control.
Reference: Shon Harris AIO v3 , Chapter-5 : Security Models and Architecture , Page:279-282

NEW QUESTION: 203
Which of the following is a LAN transmission method?
A. Broadcast
B. Carrier-sense multiple access with collision detection (CSMA/CD)
C. Token ring
D. Fiber Distributed Data Interface (FDDI)
Answer: (SHOW ANSWER)
Explanation/Reference:
LAN transmission methods refer to the way packets are sent on the network and are either unicast, multicast or broadcast.
CSMA/CD is a common LAN media access method.
Token ring is a LAN Topology.
LAN transmission protocols are the rules for communicating between computers on a LAN.
Common LAN transmission protocols are: polling and token-passing.
A LAN topology defines the manner in which the network devices are organized to facilitate communications.
Common LAN topologies are: bus, ring, star or meshed.
LAN transmission methods refer to the way packets are sent on the network and are either unicast, multicast or broadcast.
LAN media access methods control the use of a network (physical and data link layers). They can be Ethernet, ARCnet, Token ring and FDDI.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
103).
HERE IS A NICE OVERVIEW FROM CISCO:
LAN Transmission Methods
LAN data transmissions fall into three classifications: unicast, multicast, and broadcast.
In each type of transmission, a single packet is sent to one or more nodes.
In a unicast transmission, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.
A multicast transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The

packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.
A broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network.
LAN Topologies
LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star. A bus topology is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations. Of the three
most widely used LAN implementations, Ethernet/IEEE 802.3 networks-including 100BaseT-implement a bus topology
Sources:
KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 104).
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introlan.htm

NEW QUESTION: 204
You work in a police department forensics lab where you examine computers for evidence of crimes. Your work is vital to the success of the prosecution of criminals.
One day you receive a laptop and are part of a two man team responsible for examining it together. However, it is lunch time and after receiving the laptop you leave it on your desk and you both head out to lunch.
What critical step in forensic evidence have you forgotten?
A. Chain of custody
B. Locking the laptop in your desk
C. Making a disk image for examination
D. Cracking the admin password with chntpw
Answer: (SHOW ANSWER)
When evidence from a crime is to be used in the prosecution of a criminal it is critical that you follow the law when handling that evidence. Part of that process is called chain of custody and is when you maintain proactive and documented control over ALL evidence involved in a crime.
Failure to do this can lead to the dismissal of charges against a criminal because if the evidence is compromised because you failed to maintain of chain of custody.
A chain of custody is chronological documentation for evidence in a particular case, and is especially important with electronic evidence due to the possibility of fraudulent data alteration, deletion, or creation.
A fully detailed chain of custody report is necessary to prove the physical custody of a piece of evidence and show all parties that had access to said evidence at any given time.

Evidence must be protected from the time it is collected until the time it is presented in court.
The following answers are incorrect:
-Locking the laptop in your desk: Even this wouldn't assure that the defense team would try to challenge chain of custody handling. It's usually easy to break into a desk drawer and evidence should be stored in approved safes or other storage facility.
-Making a disk image for examination: This is a key part of system forensics where we make a disk image of the evidence system and study that as opposed to studying the real disk drive. That could lead to loss of evidence. However if the original evidence is not secured than the chain of custoday has not been maintained properly.
-Cracking the admin password with chntpw: This isn't correct. Your first mistake was to compromise the chain of custody of the laptop. The chntpw program is a Linux utility to (re)set the password of any user that has a valid (local) account on a Windows system, by modifying the crypted password in the registry's SAM file. You do not need to know the old password to set a new one. It works offline which means you must have physical access (i.e., you have to shutdown your computer and boot off a linux floppy disk). The bootdisk includes stuff to access NTFS partitions and scripts to glue the whole thing together. This utility works with SYSKEY and includes the option to turn it off. A bootdisk image is provided on their website at http://freecode.com/projects/chntpw .
The following reference(s) was used to create this question:
For more details and to cover 100% of the exam questions, subscribe to our holistic Security+ 2014 CBT Tutorial at: http://www.cccure.tv/ and http://en.wikipedia.org/wiki/Chain_of_custody and http://www.datarecovery.com/forensic_chain_of_custody.asp

NEW QUESTION: 205
Which of the following would be the best reason for separating the test and development environments?
A. To restrict access to systems under test.
B. To control the stability of the test environment.
C. To segregate user and development staff.
D. To secure access to systems under development.
Answer: (SHOW ANSWER)
The test environment must be controlled and stable in order to ensure that
development projects are tested in a realistic environment which, as far as possible, mirrors
the live environment.
Reference(s) used for this question:
Information Systems Audit and Control Association, Certified Information Systems Auditor
2002 review manual, chapter 6: Business Application System Development, Acquisition,
Implementation and Maintenance (page 309).

NEW QUESTION: 206
_____ attacks capitalize on programming errors and can allow the originator to gain additional privileges on a machine.
A. SYN Flood

B. Distributed Denial of Service
C. Buffer Overflow
D. Coordinated
E. Denial of Service
Answer: C (LEAVE A REPLY)

NEW QUESTION: 207
The type of discretionary access control (DAC) that is based on an individual's identity is also called:
A. Identity-based Access control
B. Rule-based Access control
C. Non-Discretionary Access Control
D. Lattice-based Access control
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
An identity-based access control is a type of Discretionary Access Control (DAC) that is based on an individual's identity.
DAC is good for low level security environment. The owner of the file decides who has access to the file. If a user creates a file, he is the owner of that file. An identifier for this user is placed in the file header and/or in an access control matrix within the operating system.
Ownership might also be granted to a specific individual. For example, a manager for a certain department might be made the owner of the files and resources within her department. A system that uses discretionary access control (DAC) enables the owner of the resource to specify which subjects can access specific resources.
This model is called discretionary because the control of access is based on the discretion of the owner. Many times department managers, or business unit managers , are the owners of the data within their specific department. Being the owner, they can specify who should have access and who should not.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 220). McGraw-Hill . Kindle Edition.

NEW QUESTION: 208
Today, privacy violations are almost as serious as security violations?
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 209
SATAN stands for _____
A. Scavanger Administrator Tool for Analyzing Networks
B. Storage Administration Tool for Analyzing Networks

C. Simple Administration Tool for Analyzing Networks
D. System Administrator Tool for Analyzing Networks
E. SANS Administrator Tool for Analyzing Networks
F. Security Administrator Tool for Analyzing Networks
Answer: (SHOW ANSWER)
: . SATAN (an acronym standing for Security Administrator Tool for Analyzing Networks) is a testing and reporting tool that gathers information from networks, such as type of machine and security flaws that may be on these machines. SATAN was developed by Dan Farmer of Silicon Graphics with a purpose of scanning thousands of host computers on the Internet for security vulnerabilities. Availability: anonymous ftp at ftp.cerias.purdue.edu

NEW QUESTION: 210
Which of the following access control models requires security clearance for subjects?
A. Identity-based access control
B. Role-based access control
C. Discretionary access control
D. Mandatory access control
Answer: (SHOW ANSWER)
Explanation/Reference:
With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance. Identity-based access control is a type of discretionary access control. A role-based access control is a type of non-discretionary access control. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION: 211
What is called an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets?
A. SYN Flood attack
B. Smurf attack
C. Ping of Death attack
D. Denial of Service (DOS) attack
Answer: (SHOW ANSWER)
Although it may cause a denial of service to the victim's system, this type of attack is a Smurf attack. A SYN Flood attack uses up all of a system's resources by setting up a number of bogus communication sockets on the victim's system. A Ping of Death attack is done by sending IP packets that exceed the maximum legal length (65535 octets). Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 789).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 212

This type of supporting evidence is used to help prove an idea or a point, however It cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. What is the name of this type of evidence?

A. Circumstantial evidence

B. Corroborative evidence

C. Opinion evidence

D. Secondary evidence

Answer: B (LEAVE A REPLY)

Explanation/Reference:

This type of supporting evidence is used to help prove an idea or a point, however It cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. Corrobative evidence takes many forms.

In a rape case for example, this could consist of torn clothing, soiled bed sheets, 911 emergency calls tapes, and

prompt complaint witnesses.

There are many types of evidence that exist. Below you have explanations of some of the most common types:

Physical Evidence

Physical evidence is any evidence introduced in a trial in the form of a physical object, intended to prove a fact in issue based on its demonstrable physical characteristics. Physical evidence can conceivably include all or part of any object.

In a murder trial for example (or a civil trial for assault), the physical evidence might include DNA left by the attacker on the victim's body, the body itself, the weapon used, pieces of carpet spattered with blood, or casts of footprints or tire prints found at the scene of the crime.

Real Evidence

Real evidence is a type of physical evidence and consists of objects that were involved in a case or actually played a part in the incident or transaction in question.

Examples include the written contract, the defective part or defective product, the murder weapon, the gloves used by an alleged murderer. Trace evidence, such as fingerprints and firearm residue, is a species of real evidence. Real evidence is usually reported upon by an expert witness with appropriate qualifications to give an opinion. This normally means a forensic scientist or one qualified in forensic engineering.

Admission of real evidence requires authentication, a showing of relevance, and a showing that the object is in "the same or substantially the same condition" now as it was on the relevant date. An object of real evidence is authenticated through the senses of witnesses or by circumstantial evidence called chain of custody.

Documentary

Documentary evidence is any evidence introduced at a trial in the form of documents. Although this term is most widely understood to mean writings on paper (such as an invoice, a contract or a will), the term actually include any media by which information can be preserved. Photographs, tape recordings, films, and printed emails are all forms of documentary evidence.

Documentary versus physical evidence

A piece of evidence is not documentary evidence if it is presented for some purpose other than the examination of the contents of the document. For example, if a blood-spattered letter is introduced solely to show that the defendant stabbed the author of the letter from behind as it was being written, then the evidence is physical evidence, not documentary evidence. However, a film of the murder taking place would be documentary evidence (just as a written description of the event from an eyewitness). If the content of that same letter is then introduced to show the motive for the murder, then the evidence would be both physical and documentary.

Documentary Evidence Authentication

Documentary evidence is subject to specific forms of authentication, usually through the testimony of an eyewitness to the execution of the document, or to the testimony of a witness able to identify the handwriting of the purported author. Documentary evidence is also subject to the best evidence rule, which requires that the original document be produced unless there is a good reason not to do so.

The role of the expert witness

Where physical evidence is of a complexity that makes it difficult for the average person to understand its significance, an expert witness may be called to explain to the jury the proper interpretation of the evidence at hand.

Digital Evidence or Electronic Evidence

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files.

While many courts in the United States have applied the Federal Rules of Evidence to digital evidence in the same way as more traditional documents, courts have noted very important differences. As compared to the more traditional evidence, courts have noted that digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive, and more readily available. As such, some courts have sometimes treated digital evidence differently for purposes of authentication, hearsay, the best evidence rule, and privilege. In December 2006, strict new

rules were enacted within the Federal Rules of Civil Procedure requiring the preservation and disclosure of electronically stored evidence.

Demonstrative Evidence

Demonstrative evidence is evidence in the form of a representation of an object. This is, as opposed to, real evidence, testimony, or other forms of evidence used at trial.

Examples of demonstrative evidence include photos, x-rays, videotapes, movies, sound recordings, diagrams, forensic animation, maps, drawings, graphs, animation, simulations, and models. It is useful for assisting a finder of fact (fact-finder) in establishing context among the facts presented in a case. To be admissible, a demonstrative exhibit must "fairly and accurately" represent the real object at the relevant time.

Chain of custody

Chain of custody refers to the chronological documentation, and/or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.

The idea behind recoding the chain of custody is to establish that the alleged evidence is fact related to the alleged crime - rather than, for example, having been planted fraudulently to make someone appear guilty.

Establishing the chain of custody is especially important when the evidence consists of fungible goods. In practice, this most often applies to illegal drugs which have been seized by law enforcement personnel. In such cases, the defendant at times disclaims any knowledge of possession of the controlled substance in question.

Accordingly, the chain of custody documentation and testimony is presented by the prosecution to establish that the substance in evidence was in fact in the possession of the defendant.

An identifiable person must always have the physical custody of a piece of evidence. In practice, this means that a police officer or detective will take charge of a piece of evidence, document its collection, and hand it over to an evidence clerk for storage in a secure place. These transactions, and every succeeding transaction between the collection of the evidence and its appearance in court, should be completely documented chronologically in order to withstand legal challenges to the authenticity of the evidence.

Documentation should include the conditions under which the evidence is gathered, the identity of all evidence handlers, duration of evidence custody, security conditions while handling or storing the evidence, and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).

Example

An example of "Chain of Custody" would be the recovery of a bloody knife at a murder scene:

Officer Andrew collects the knife and places it into a container, then gives it to forensics technician Bill. Forensics technician Bill takes the knife to the lab and collects fingerprints and other evidence from the knife. Bill then gives the knife and all evidence gathered from the knife to evidence clerk Charlene.

Charlene then stores the evidence until it is needed, documenting everyone who has accessed the original evidence (the knife, and original copies of the lifted fingerprints).
The Chain of Custody requires that from the moment the evidence is collected, every transfer of evidence from person to person be documented and that it be provable that nobody else could have accessed that evidence. It is best to keep the number of transfers as low as possible.
In the courtroom, if the defendant questions the Chain of Custody of the evidence it can be proven that the knife in the evidence room is the same knife found at the crime scene. However, if there are discrepancies and it cannot be proven who had the knife at a particular point in time, then the Chain of Custody is broken and the defendant can ask to have the resulting evidence declared inadmissible.
"Chain of custody" is also used in most chemical sampling situations to maintain the integrity of the sample by providing documentation of the control, transfer, and analysis of samples. Chain of custody is especially important in environmental work where sampling can identify the existence of contamination and can be used to identify the responsible party.
REFERENCES:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 23173-23185). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Documentary_evidence
http://en.wikipedia.org/wiki/Physical_evidence
http://en.wikipedia.org/wiki/Digital_evidence
http://en.wikipedia.org/wiki/Demonstrative_evidence
http://en.wikipedia.org/wiki/Real_evidence
http://en.wikipedia.org/wiki/Chain_of_custody

NEW QUESTION: 213
In a stateful inspection firewall, data packets are captured by an inspection engine that is operating at the:
A. Network or Transport Layer.
B. Application Layer.
C. Inspection Layer.
D. Data Link Layer.
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Most stateful packet inspection firewalls work at the network or transport layers. For the TCP/IP protcol, this allows the firewall to make decisions both on IP addresses, protocols and TCP/UDP port numbers
Application layer is incorrect. This is too high in the OSI stack for this type of firewall.
Inspection layer is incorrect. There is no such layer in the OSI stack.
"Data link layer" is incorrect. This is too low in the OSI stack for this type of firewall.
References:
CBK, p. 466
AIO3, pp. 485 - 486

NEW QUESTION: 214
Which of the following statements pertaining to using Kerberos without any extension is false?
A. A client can be impersonated by password-guessing.
B. Kerberos is mostly a third-party authentication protocol.
C. Kerberos uses public key cryptography.
D. Kerberos provides robust authentication.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Kerberos is a trusted, credential-based, third-party authentication protocol that uses symmetric (secret) key cryptography to provide robust authentication to clients accessing services on a network.
Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.
Here is a nice overview of HOW Kerberos is implement as described in RFC 4556:
1. Introduction
The Kerberos V5 protocol [RFC4120] involves use of a trusted third party known as the Key Distribution Center (KDC) to negotiate shared
session keys between clients and services and provide mutual authentication between them.
The corner-stones of Kerberos V5 are the Ticket and the Authenticator. A Ticket encapsulates a symmetric key (the ticket session key) in an envelope (a public message) intended for a specific service. The contents of the Ticket are encrypted with a symmetric key shared between the service principal and the issuing KDC. The encrypted part of the Ticket contains the client principal name, among other items.
An Authenticator is a record that can be shown to have been recently generated using the ticket session key in the associated Ticket. The ticket session key is known by the client who requested the ticket. The contents of the Authenticator are encrypted with the associated ticket session key. The encrypted part of an Authenticator contains a timestamp and the client principal name, among other items.
As shown in Figure 1, below, the Kerberos V5 protocol consists of the following message exchanges between the client and the KDC, and the
client and the application service:
The Authentication Service (AS) Exchange
The client obtains an "initial" ticket from the Kerberos authentication server (AS), typically a Ticket Granting Ticket (TGT). The AS-REQ message and the AS-REP message are the request and the reply message, respectively, between the client and the AS.
The Ticket Granting Service (TGS) Exchange
The client subsequently uses the TGT to authenticate and request a service ticket for a particular service, from the Kerberos ticket-granting server (TGS). The TGS-REQ message and the TGS-REP message are the request and the reply message respectively between the client and the TGS.
The Client/Server Authentication Protocol (AP) Exchange
The client then makes a request with an AP-REQ message, consisting of a service ticket and an authenticator that certifies the client's possession of the ticket session key. The server may optionally reply with an AP-REP message. AP exchanges typically negotiate session-specific symmetric keys.

Usually, the AS and TGS are integrated in a single device also known as the KDC.

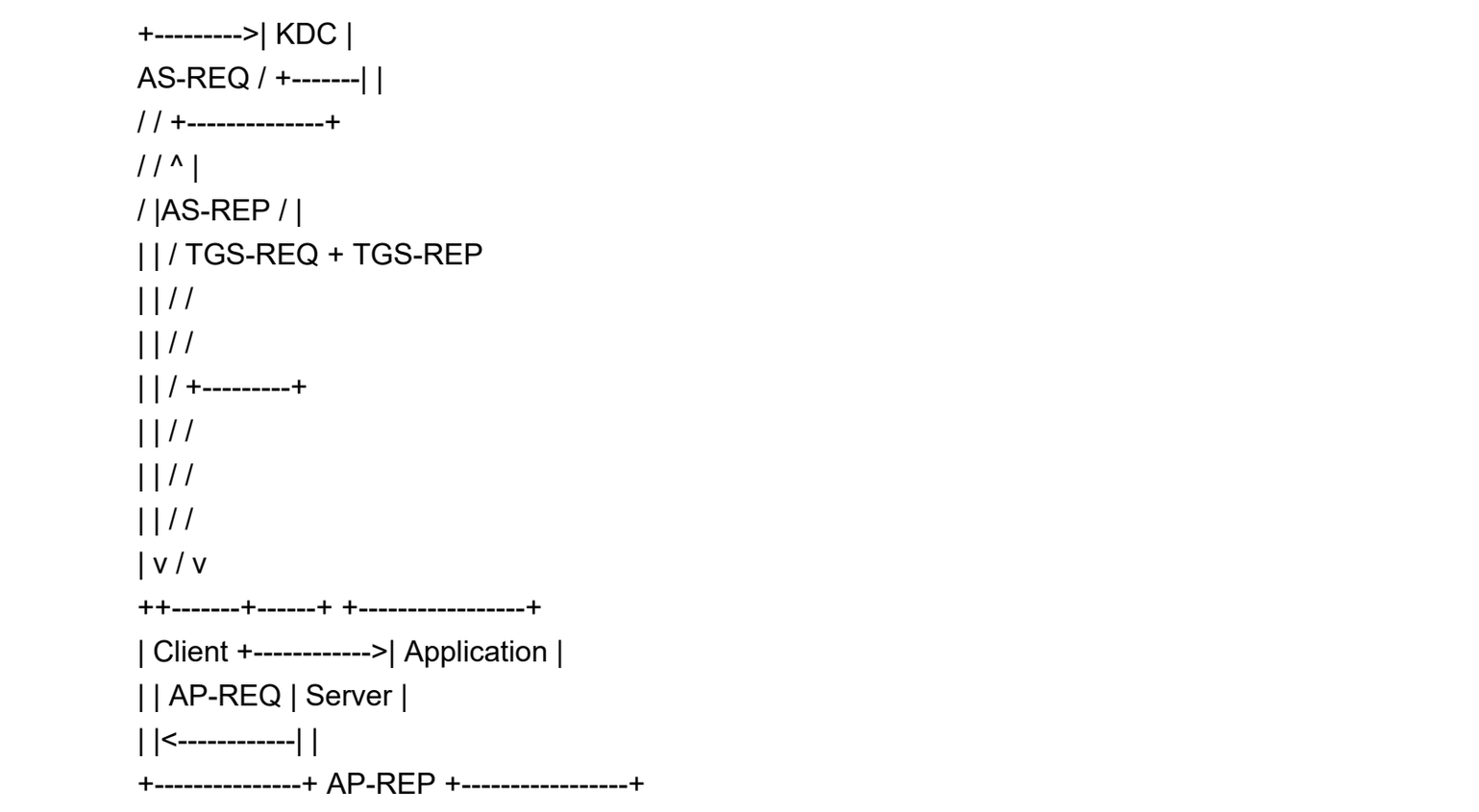


Figure 1: The Message Exchanges in the Kerberos V5 Protocol

In the AS exchange, the KDC reply contains the ticket session key, among other items, that is encrypted using a key (the AS reply key)
shared between the client and the KDC. The AS reply key is typically derived from the client's password for human users. Therefore, for
human users, the attack resistance strength of the Kerberos protocol is no stronger than the strength of their passwords.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 40).

And

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 147-151).

and

http://www.ietf.org/rfc/rfc4556.txt

NEW QUESTION: 215

If an organization were to monitor their employees' e-mail, it should not:

A. Monitor only a limited number of employees.

B. Inform all employees that e-mail is being monitored.

C. Explain who can read the e-mail and how long it is backed up.

D. Explain what is considered an acceptable use of the e-mail system.

Answer: A (LEAVE A REPLY)
Monitoring has to be conducted is a lawful manner and applied in a
consistent fashion; thus should be applied uniformly to all employees, not only to a small
number.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law,
Investigation, and Ethics (page 304).

NEW QUESTION: 216
Which of the following mechanisms was created to overcome the problem of collisions that occur on wired networks when traffic is simultaneously transmitted from different nodes?
A. Carrier sense multiple access with collision detection (CSMA/CD)
B. Token-passing
C. Carrier sense multiple access with collision avoidance (CSMA/CA)
D. Polling
Answer: (SHOW ANSWER)

NEW QUESTION: 217
Which of the following was developed by the National Computer Security Center (NCSC) for the US Department of Defense ?
A. TCSEC
B. ITSEC
C. DIACAP
D. NIACAP
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The Answer: TCSEC; The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications.
Initially issued by the National Computer Security Center (NCSC) an arm of the National Security Agency in
1983 and then updated in 1985, TCSEC was replaced with the development of the Common Criteria international standard originally published in 2005.
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 197-199.
Wikepedia
http://en.wikipedia.org/wiki/TCSEC

NEW QUESTION: 218

Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?

A. B

B. A

C. C

D. D

Answer: (SHOW ANSWER)

B level is the first Mandatory Access Control Level.

First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.

Reference used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17920-17926). Auerbach Publications. Kindle Edition.

and

THE source for all TCSEC "level" questions:

http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt (paragraph 3 for this one)

NEW QUESTION: 219

The viewing of recorded events after the fact using a closed-circuit TV camera is considered a

A. Preventative control.

B. Detective control

C. Compensating control

D. Corrective control

Answer: (SHOW ANSWER)

Explanation/Reference:

Detective security controls are like a burglar alarm. They detect and report an unauthorized or undesired event (or an attempted undesired event). Detective security controls are invoked after the undesirable event has occurred. Example detective security controls are log monitoring and review, system audit, file integrity checkers, and motion detection.

Visual surveillance or recording devices such as closed circuit television are used in conjunction with guards in order to enhance their surveillance ability and to record events for future analysis or prosecution.

When events are monitored, it is considered preventative whereas recording of events is considered detective in nature.
Below you have explanations of other types of security controls from a nice guide produce by James Purcell (see reference below):
Preventive security controls are put into place to prevent intentional or unintentional disclosure, alteration, or destruction (D.A.D.) of sensitive information. Some example preventive controls follow:
Policy - Unauthorized network connections are prohibited.
Firewall - Blocks unauthorized network connections.
Locked wiring closet - Prevents unauthorized equipment from being physically plugged into a network switch.
Notice in the preceding examples that preventive controls crossed administrative, technical, and physical categories discussed previously. The same is true for any of the controls discussed in this section.
Corrective security controls are used to respond to and fix a security incident. Corrective security controls also limit or reduce further damage from an attack. Examples follow:
Procedure to clean a virus from an infected system
A guard checking and locking a door left unlocked by a careless employee Updating firewall rules to block an attacking IP address
Note that in many cases the corrective security control is triggered by a detective security control.
Recovery security controls are those controls that put a system back into production after an incident. Most Disaster Recovery activities fall into this category. For example, after a disk failure, data is restored from a backup tape.
Directive security controls are the equivalent of administrative controls. Directive controls direct that some action be taken to protect sensitive organizational information. The directive can be in the form of a policy, procedure, or guideline.
Deterrent security controls are controls that discourage security violations. For instance, "Unauthorized Access Prohibited" signage may deter a trespasser from entering an area. The presence of security cameras might deter an employee from stealing equipment. A policy that states access to servers is monitored could deter unauthorized access.
Compensating security controls are controls that provide an alternative to normal controls that cannot be used for some reason. For instance, a certain server cannot have antivirus software installed because it interferes with a critical application. A compensating control would be to increase monitoring of that server or isolate that server on its own network segment.
Note that there is a third popular taxonomy developed by NIST and described in NIST Special Publication
800-53, "Recommended Security Controls for Federal Information Systems." NIST categorizes security controls into 3 classes and then further categorizes the controls within the classes into 17 families. Within each security control family are dozens of specific controls. The NIST taxonomy is not covered on the CISSP exam but is one the CISSP should be aware of if you are employed within the US federal workforce.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 340).

and
CISSP Study Guide By Eric Conrad, Seth Misenar, Joshua Feldman, page 50-52 and
Security Control Types and Operational Security, James E. Purcell, http://www.giac.org/cissp-papers/207.pdf

NEW QUESTION: 220
Which of the following would be used to detect and correct errors so that integrity and confidentiality of transactions over networks may be maintained while preventing unauthorize interception of the traffic?
A. Information security
B. Server security
C. Client security
D. Communications security
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Communications security is the discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients. In the United States Department of Defense culture, it is often referred to by the abbreviation COMSEC. The field includes cryptosecurity, transmission security, emission security, traffic-flow security and physical security of COMSEC equipment.
All of the other answers are incorrect answers:
Information security
Information security would be the overall program but communications security is the more specific and better answer. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.
These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.
Server security
While server security plays a part in the overall information security program, communications security is a better answer when talking about data over the network and preventing interception. See publication 800-
123 listed in the reference below to learn more.
Client security

While client security plays a part in the overall information security program, communications security is a better answer. Securing the client would not prevent interception of data or capture of data over the network. Today people referred to this as endpoint security.
References:
http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
and
https://en.wikipedia.org/wiki/Information_security
and
https://en.wikipedia.org/wiki/Communications_security

NEW QUESTION: 221
In order to be able to successfully prosecute an intruder:
A. A point of contact should be designated to be responsible for communicating with law enforcement and other external agencies.
B. A proper chain of custody of evidence has to be preserved.
C. Collection of evidence has to be done following predefined procedures.
D. Whenever possible, analyze a replica of the compromised resource, not the original, thereby avoiding inadvertently tamping with evidence.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
If you intend on prosecuting an intruder, evidence has to be collected in a lawful manner and, most importantly, protected through a secure chain-of-custody procedure that tracks who has been involved in handling the evidence and where it has been stored. All other choices are all important points, but not the best answer, since no prosecution is possible without a proper, provable chain of custody of evidence.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 282-285).

NEW QUESTION: 222
A contingency plan should address:
A. Potential risks.
B. Residual risks.
C. Identified risks.
D. All answers are correct.
Answer: (SHOW ANSWER)
Explanation/Reference:
Because it is rarely possible or cost effective to eliminate all risks, an attempt is made to reduce risks to an acceptable level through the risk assessment process. This process allows, from a set of potential risks (whether likely or not), to come up with a set of identified, possible risks.

The implementation of security controls allows reducing the identified risks to a smaller set of residual risks. Because these residual risks represent the complete set of situations that could affect system performance, the scope of the contingency plan may be reduced to address only this decreased risk set. As a result, the contingency plan can be narrowly focused, conserving resources while ensuring an effective system recovery capability.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 7).

NEW QUESTION: 223
Within the OSI model, at what layer are some of the SLIP, CSLIP, PPP control functions provided?
A. Data Link
B. Transport
C. Presentation
D. Application
Answer: (SHOW ANSWER)
RFC 1661 - The Point-to-Point Protocol (PPP) specifies that the Point-to-
Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams
over point-to-point links. PPP is comprised of three main components:
1 A method for encapsulating multi-protocol datagrams.
2 A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link
connection.
3 A family of Network Control Protocols (NCPs) for establishing and configuring different
network-layer protocols.

NEW QUESTION: 224
In response to Access-request from a client such as a Network Access Server (NAS), which of the following is not one of the response from a RADIUS Server?
A. Access-Accept
B. Access-Reject
C. Access-Granted
D. Access-Challenge
Answer: (SHOW ANSWER)
In response to an access-request from a client, a RADIUS server returns one of three authentication responses: access-accept, access-reject, or access-challenge, the latter being a request for additional authentication information such as a one-time password from a token or a callback identifier. Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 36.

NEW QUESTION: 225

In discretionary access environments, which of the following entities is authorized to grant information access to other people?

A. Manager

B. Group Leader

C. Security Manager

D. Data Owner

Answer: D (LEAVE A REPLY)

In Discretionary Access Control (DAC) environments, the user who creates a file is also considered the owner and has full control over the file including the ability to set permissions for that file.

The following answers are incorrect:

manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

group leader. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

security manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.

IMPORTANT NOTE: The term Data Owner is also used within Classifications as well. Under the subject of classification the Data Owner is a person from management who has been entrusted with a data set that belongs to the company. For example it could be the Chief Financial Officer (CFO) who is entrusted with all of the financial data for a company. As such the CFO would determine the classification of the financial data and who can access as well. The Data Owner would then tell the Data Custodian (a technical person) what the classification and need to know is on the specific set of data.

The term Data Owner under DAC simply means whoever created the file and as the creator of the file the owner has full access and can grant access to other subjects based on their identity.

NEW QUESTION: 226

Which of the following is used to interrupt the opportunity to use or perform collusion to subvert operation for fraudulent purposes?

A. Key escrow

B. Rotation of duties

C. Principle of need-to-know

D. Principle of least privilege

Answer: B (LEAVE A REPLY)

Job rotations reduce the risk of collusion of activities between individuals. Companies with individuals working with sensitive information or systems where there might be the opportunity for personal gain through collusion can benefit by integrating job rotation with segregation of duties. Rotating the position may uncover activities that the individual is performing outside of the normal operating procedures, highlighting errors or fraudulent behavior.

Rotation of duties is a method of reducing the risk associated with a subject performing a (sensitive) task by limiting the amount of time the subject is assigned to perform the task before being moved to a different task.

The following are incorrect answers: Key escrow is related to the protection of keys in storage by splitting the key in pieces that will be controlled by different departments. Key escrow is the process of ensuring a third party maintains a copy of a private key or key needed to decrypt information. Key escrow also should be considered mandatory for most organization's use of cryptography as encrypted information belongs to the organization and not the individual; however often an individual's key is used to encrypt the information.
Separation of duties is a basic control that prevents or detects errors and irregularities by assigning responsibility for different parts of critical tasks to separate individuals, thus limiting the effect a single person can have on a system. One individual should not have the capability to execute all of the steps of a particular process. This is especially important in critical business areas, where individuals may have greater access and capability to modify, delete, or add data to the system. Failure to separate duties could result in individuals embezzling money from the company without the involvement of others.
The need-to-know principle specifies that a person must not only be cleared to access classified or other sensitive information, but have requirement for such information to carry out assigned job duties.
Ordinary or limited user accounts are what most users are assigned. They should be restricted only to those privileges that are strictly required, following the principle of least privilege. Access should be limited to specific objects following the principle of need-to-know.
The principle of least privilege requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. Least privilege refers to granting users only the accesses that are required to perform their job functions. Some employees will require greater access than others based upon their job functions. For example, an individual performing data entry on a mainframe system may have no need for Internet access or the ability to run reports regarding the information that they are entering into the system. Conversely, a supervisor may have the need to run reports, but should not be provided the capability to change information in the database.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10628-10631). Auerbach Publications. Kindle Edition. and Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10635-10638). Auerbach Publications. Kindle Edition. and Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10693-10697). Auerbach Publications. Kindle Edition. and Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 16338-16341). Auerbach Publications. Kindle Edition.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine

here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 227
Which of the following statements pertaining to the maintenance of an IT contingency plan is incorrect?
A. The plan should be reviewed at least once a year for accuracy and completeness.
B. The Contingency Planning Coordinator should make sure that every employee gets an up-to-date copy of the plan.
C. Strict version control should be maintained.
D. Copies of the plan should be provided to recovery personnel for storage offline at home and office.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Because the contingency plan contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled. Not all employees would obtain a copy, but only those involved in the execution of the plan.
All other statements are correct.
NOTE FROM CLEMENT:
I have received multiple emails stating the explanations contradict the correct answer. It seems many people have a hard time with negative question. In this case the Incorrect choice (the one that is not true) is the correct choice. Be very carefull of such questions, you will get some on the real exam as well.
Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication
800-34, Contingency Planning Guide for Information Technology Systems

NEW QUESTION: 228
Which of the following is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance
processes?
A. The Software Capability Maturity Model (CMM)
B. The Spiral Model
C. The Waterfall Model
D. Expert Systems Model
Answer: (SHOW ANSWER)
The Capability Maturity Model (CMM) is a service mark owned by Carnegie Mellon University (CMU) and refers to a development model elicited from actual data. The data was collected from organizations that contracted with the U.S. Department of Defense, who funded the research, and became the foundation from which CMU created the Software Engineering Institute (SEI). Like any model, it is an abstraction of an existing system.

The Capability Maturity Model (CMM) is a methodology used to develop and refine an organization's software development process. The model describes a five-level evolutionary path of increasingly organized and systematically more mature processes. CMM was developed and is promoted by the Software Engineering Institute (SEI), a research and development center sponsored by the U.S. Department of Defense (DoD). SEI was founded in 1984 to address software engineering issues and, in a broad sense, to advance software engineering methodologies. More specifically, SEI was established to optimize the process of developing, acquiring, and maintaining heavily software-reliant systems for the DoD. Because the processes involved are equally applicable to the software industry as a whole, SEI advocates industry-wide adoption of the CMM.

The CMM is similar to ISO 9001, one of the ISO 9000 series of standards specified by the International Organization for Standardization (ISO). The ISO 9000 standards specify an effective quality system for manufacturing and service industries; ISO 9001 deals specifically with software development and maintenance. The main difference between the two systems lies in their respective purposes: ISO 9001 specifies a minimal acceptable quality level for software processes, while the CMM establishes a framework for continuous process improvement and is more explicit than the ISO standard in defining the means to be employed to that end. CMM's Five Maturity Levels of Software Processes

At the initial level, processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated. At the repeatable level, basic project management techniques are established, and successes could be repeated, because the requisite processes would have been made

established, defined, and documented.

At the defined level, an organization has developed its own standard software process through greater attention to documentation, standardization, and integration.

At the managed level, an organization monitors and controls its own processes through data collection and analysis.

At the optimizing level, processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

When it is applied to an existing organization's software development processes, it allows an effective approach toward improving them. Eventually it became clear that the model could be applied to other processes. This gave rise to a more general concept that is applied to business processes and to developing people.

CMM is superseded by CMMI

The CMM model proved useful to many organizations, but its application in software development has sometimes been problematic. Applying multiple models that are not integrated within and across an organization could be costly in terms of training, appraisals, and improvement activities. The Capability Maturity Model Integration (CMMI) project was formed to sort out the problem of using multiple CMMs.

For software development processes, the CMM has been superseded by Capability Maturity Model Integration (CMMI), though the CMM continues to be a general theoretical

process capability model used in the public domain.
CMM is adapted to processes other than software development
The CMM was originally intended as a tool to evaluate the ability of government contractors to perform a contracted software project. Though it comes from the area of software development, it can be, has been, and continues to be widely applied as a general model of the maturity of processes (e.g., IT Service Management processes) in IS/IT (and other) organizations.
Source:
http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci930057,00.html
and
http://en.wikipedia.org/wiki/Capability_Maturity_Model

NEW QUESTION: 229
In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?
A. Both client and server
B. The client's browser
C. The web server
D. The merchant's Certificate Server
Answer: (SHOW ANSWER)
Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant's public key and sent to the server. The fact that the master secret is generated by the client's browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, page 569.

NEW QUESTION: 230
Which of the following is most concerned with personnel security?
A. Management controls
B. Operational controls
C. Technical controls
D. Human resources controls
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:

Many important issues in computer security involve human users, designers, implementers, and managers.
A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. Since operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems), personnel security is considered a form of operational control.
Operational controls are put in place to improve security of a particular system (or group of systems). They often require specialized expertise and often rely upon management activities as well as technical controls.
Implementing dual control and making sure that you have more than one person that can perform a task would fall into this category as well.
Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.
Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access of misuse, facilitate detection of security violations, and support security requirements for applications and data.
Reference use for this question:
NIST SP 800-53 Revision 4 http://dx.doi.org/10.6028/NIST.SP.800-53r4
You can get it as a word document by clicking HERE
NIST SP 800-53 Revision 4 has superseded the document below:
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Page A-18).

NEW QUESTION: 231
Which of the following was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN?
A. DHCP
B. BootP
C. DNS
D. ARP
Answer: (SHOW ANSWER)
Explanation/Reference:
BootP was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN. Over time, it has expanded to allow centralized configuration of many aspects of a host's identity and behavior on the network. Note that DHCP, more complex, has replaced BootP over time.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4: Sockets and Services from a Security Viewpoint.

NEW QUESTION: 232

Which of the following Intrusion Detection Systems (IDS) uses a database of attacks, known system vulnerabilities, monitoring current attempts to exploit those vulnerabilities, and then triggers an alarm if an attempt is found?

A. Knowledge-Based ID System

B. Application-Based ID System

C. Host-Based ID System

D. Network-Based ID System

Answer: A (LEAVE A REPLY)

Knowledge-based Intrusion Detection Systems use a database of previous attacks and known system vulnerabilities to look for current attempts to exploit their vulnerabilities, and trigger an alarm if an attempt is found. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

Application-Based ID System - "a subset of HIDS that analyze what's going on in an application using the transaction log files of the application." Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87

Host-Based ID System - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host." Source: Official ISC2 Guide to the CISSP CBK - p.

Network-Based ID System - "a network device, or dedicated system attached to teh network, that monitors traffic traversing teh network segment for which it is integrated." Source: Official ISC2 Guide to the CISSP CBK - p. 196

NEW QUESTION: 233

Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT) by ensuring the message comes from its claimed originator and that it has not been altered in transmission?

A. Secure Electronic Transaction (SET)

B. Message Authentication Code (MAC)

C. Cyclic Redundancy Check (CRC)

D. Secure Hash Standard (SHS)

Answer: B (LEAVE A REPLY)

In order to protect against fraud in electronic fund transfers (EFT), the Message Authentication Code (MAC), ANSI X9.9, was developed. The MAC is a check value, which is derived from the contents of the message itself, that is sensitive to the bit changes in a message. It is similar to a Cyclic Redundancy Check (CRC).

The aim of message authentication in computer and communication systems is to verify that he message comes from its claimed originator and that it has not been altered in transmission. It is particularly needed for EFT Electronic Funds Transfer). The protection mechanism is generation of a Message Authentication Code (MAC), attached to the message, which can be recalculated by the receiver and will reveal any alteration in transit. One standard method is described in (ANSI, X9.9). Message authentication mechanisms an also be used to achieve non-repudiation of messages.

The Secure Electronic Transaction (SET) was developed by a consortium including MasterCard and VISA as a means of preventing fraud from occurring during electronic payment.
The Secure Hash Standard (SHS), NIST FIPS 180, available at http://www.itl.nist.gov/fipspubs/fip180-1.htm, specifies the Secure Hash Algorithm (SHA-1).
Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 170)
also see:
http://luizfirmino.blogspot.com/2011/04/message-authentication-code-mac.html
and
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.22.2312&rep=rep1&type=pdf

NEW QUESTION: 234
Wiretapping is an example of a passive network attack?
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 235
Which of the following cannot be undertaken in conjunction or while computer incident handling is ongoing?
A. System development activity
B. Help-desk function
C. System Imaging
D. Risk management process
Answer: A (LEAVE A REPLY)
If Incident Handling is underway an incident has potentially been identified. At that point all use of the system should stop because the system can no longer be trusted and any changes could contaminate the evidence. This would include all System Development Activity.
Every organization should have plans and procedures in place that deals with Incident Handling. Employees should be instructed what steps are to be taken as soon as an incident occurs and how to report it. It is important that all parties involved are aware of these steps to protect not only any possible evidence but also to prevent any additional harm.
It is quite possible that the fraudster has planted malicous code that could cause destruction or even a Trojan Horse with a back door into the system. As soon as an incident has been identified the system can no longer be trusted and all use of the system should cease.
Shon Harris in her latest book mentions: Although we commonly use the terms "event" and "incident" interchangeably, there are subtle differences between the two. An event is a negative occurrence that can be observed, verified, and documented, whereas an incident is a series of events that negatively affects the company and/ or impacts its security posture. This is why we call reacting to these issues

"incident response" (or "incident handling"), because something is negatively affecting the company and causing a security breach.

Many types of incidents (virus, insider attack, terrorist attacks, and so on) exist, and sometimes it is just human error. Indeed, many incident response individuals have received a frantic call in the middle of the night because a system is acting "weird." The reasons could be that a deployed patch broke something, someone misconfigured a device, or the administrator just learned a new scripting language and rolled out some code that caused mayhem and confusion.

When a company endures a computer crime, it should leave the environment and evidence unaltered and contact whomever has been delegated to investigate these types of situations. Someone who is unfamiliar with the proper process of collecting data and evidence from a crime scene could instead destroy that evidence, and thus all hope of prosecuting individuals, and achieving a conviction would be lost.

Companies should have procedures for many issues in computer security such as enforcement procedures, disaster recovery and continuity procedures, and backup procedures. It is also necessary to have a procedure for dealing with computer incidents because they have become an increasingly important issue of today's information security departments. This is a direct result of attacks against networks and information systems increasing annually. Even though we don't have specific numbers due to a lack of universal reporting and reporting in general, it is clear that the volume of attacks is increasing. Just think about all the spam, phishing scams, malware, distributed denial-of-service, and other attacks you see on your own network and hear about in the news. Unfortunately, many companies are at a loss as to who to call or what to do right after they have been the victim of a cybercrime. Therefore, all companies should have an incident response policy that indicates who has the authority to initiate an incident response, with supporting procedures set up before an incident takes place.

This policy should be managed by the legal department and security department. They need to work together to make sure the technical security issues are covered and the legal issues that surround criminal activities are properly dealt with. The incident response policy should be clear and concise. For example, it should indicate if systems can be taken offline to try to save evidence or if systems have to continue functioning at the risk of destroying evidence. Each system and functionality should have a priority assigned to it. For instance, if the file server is infected, it should be removed from the network, but not shut down. However, if the mail server is infected, it should not be removed from the network or shut
down because of the priority the company attributes to the mail server over the file server. Tradeoffs and decisions will have to be made, but it is better to think through these issues before the situation occurs, because better logic is usually possible before a crisis, when there's less emotion and chaos.

The Australian Computer Emergency Response Team's General Guidelines for Computer Forensics:

Keep the handling and corruption of original data to a minimum.

Document all actions and explain changes.

Follow the Five Rules for Evidence (Admissible, Authentic, Complete, Accurate, Convincing).

Bring in more experienced help when handling and/ or analyzing the evidence is beyond your knowledge, skills, or abilities.
Adhere to your organization's security policy and obtain written permission to conduct a forensics investigation.
Capture as accurate an image of the system(s) as possible while working quickly.
Be ready to testify in a court of law.
Make certain your actions are repeatable.
Prioritize your actions, beginning with volatile and proceeding to persistent evidence.
Do not run any programs on the system(s) that are potential evidence.
Act ethically and in good faith while conducting a forensics investigation, and do not attempt to do any harm.
The following answers are incorrect:
help-desk function. Is incorrect because during an incident, employees need to be able to communicate with a central source. It is most likely that would be the help-desk. Also the help-desk would need to be able to communicate with the employees to keep them informed.
system imaging. Is incorrect because once an incident has occured you should perform a capture of evidence starting with the most volatile data and imaging would be doen using bit for bit copy of storage medias to protect the evidence.
risk management process. Is incorrect because incident handling is part of risk management, and should continue.
Reference(s) used for this question: Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21468-21476). McGraw-Hill. Kindle Edition. and Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21096-21121). McGraw-Hill. Kindle Edition. and NIST Computer Security incident handling http://csrc.nist.gov/publications/nistpubs/80012/800-12-html/chapter12.html

NEW QUESTION: 236
Which of the following is most appropriate to notify an internal user that session monitoring is being conducted?
A. Logon Banners
B. Wall poster
C. Employee Handbook
D. Written agreement
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
This is a tricky question, the keyword in the question is Internal users.
There are two possible answers based on how the question is presented, this question could either apply to internal users or ANY anonymous/external users.
Internal users should always have a written agreement first, then logon banners serve as a constant reminder.

Banners at the log-on time should be used to notify external users of any monitoring that is being conducted. A good banner will give you a better legal stand and also makes it obvious the user was warned about who should access the system, who is authorized and unauthorized, and if it is an unauthorized user then he is fully aware of trespassing. Anonymous/External users, such as those logging into a web site, ftp server or even a mail server; their only notification system is the use of a logon banner.
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 50.
and
Shon Harris, CISSP All-in-one, 5th edition, pg 873

NEW QUESTION: 237
Which access control model achieves data integrity through well-formed transactions and separation of duties?
A. Clark-Wilson model
B. Biba model
C. Non-interference model
D. Sutherland model
Answer: A (LEAVE A REPLY)
The Clark-Wilson model differs from other models that are subject- and object- oriented by introducing a third access element programs resulting in what is called an access triple, which prevents unauthorized users from modifying data or programs. The Biba model uses objects and subjects and addresses integrity based on a hierarchical lattice of integrity levels. The non-interference model is related to the information flow model with restrictions on the information flow. The Sutherland model approaches integrity by focusing on the problem of inference. Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 12). And: KRAUSE, Micki & TIPTON, Harold F., Handbook of Information Security Management, CRC Press, 1997, Domain 1: Access Control.

NEW QUESTION: 238
Which of the following is NOT a transaction redundancy implementation?
A. on-site mirroring
B. Electronic Vaulting
C. Remote Journaling
D. Database Shadowing
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Three concepts are used to create a level of fault tolerance and redundancy in transaction processing. They are Electronic vaulting, remote journaling and database shadowing provide redundancy at the transaction level.

Electronic vaulting is accomplished by backing up system data over a network. The backup location is usually at a separate geographical location known as the vault site. Vaulting can be used as a mirror or a backup mechanism using the standard incremental or differential backup cycle. Changes to the host system are sent to the vault server in real-time when the backup method is implemented as a mirror. If vaulting updates are recorded in real-time, then it will be necessary to perform regular backups at the off-site location to provide recovery services due to inadvertent or malicious alterations to user or system data.
Journaling or Remote Journaling is another technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location. The journal provides sufficient detail for the transaction to be replayed on the remote system. This provides for database recovery in the event that the database becomes corrupted or unavailable.
There are also additional redundancy options available within application and database software platforms.
For example, database shadowing may be used where a database management system updates records in multiple locations. This technique updates an entire copy of the database at a remote location.
Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20403-20407). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20375-20377). Auerbach Publications. Kindle Edition.

NEW QUESTION: 239
It is a violation of the "separation of duties" principle when which of the following individuals access the software on systems implementing security?
A. security administrator
B. security analyst
C. systems auditor
D. systems programmer
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Reason: The security administrator, security analysis, and the system auditor need access to portions of the security systems to accomplish their jobs. The system programmer does not need access to the working (AKA: Production) security systems.
Programmers should not be allowed to have ongoing direct access to computers running production systems (systems used by the organization to operate its business). To maintain system integrity, any changes they make to production systems should be tracked by the organization's change management control system.

Because the security administrator's job is to perform security functions, the performance of non-security tasks must be strictly limited. This separation of duties reduces the likelihood of loss that results from users abusing their authority by taking actions outside of their assigned functional responsibilities.
References:
OFFICIAL (ISC)2® GUIDE TO THE CISSP® EXAM (2003), Hansche, S., Berti, J., Hare, H., Auerbach Publication, FL, Chapter 5 - Operations Security, section 5.3,"Security Technology and Tools," Personnel section (page 32).
KRUTZ, R. & VINES, R. The CISSP Prep Guide: Gold Edition (2003), Wiley Publishing Inc., Chapter 6: Operations Security, Separations of Duties (page 303).

NEW QUESTION: 240
A momentary power outage is a:
A. spike
B. blackout
C. surge
D. fault
Answer: D (LEAVE A REPLY)
A momentary power outage is a fault.
Power Excess
Spike --> Too much voltage for a short period of time.
Surge --> Too much voltage for a long period of time.
Power Loss
Fault --> A momentary power outage.
Blackout --> A long power interruption.
Power Degradation
Sag or Dip --> A momentary low voltage.
Brownout --> A prolonged power supply that is below normal voltage.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.
and
https://en.wikipedia.org/wiki/Power_quality

NEW QUESTION: 241
A channel within a computer system or network that is designed for the authorized transfer of information is identified as a(n)?
A. Covert channel
B. Overt channel
C. Opened channel
D. Closed channel
Answer: B (LEAVE A REPLY)

Explanation/Reference:
An overt channel is a path within a computer system or network that is designed for the authorized transfer of data. The opposite would be a covert channel which is an unauthorized path.
A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way. Receiving information in this manner clearly violates the system's security policy.
All of the other choices are bogus detractors.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 219.
and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 380
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 378). McGraw-Hill. Kindle Edition.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 242
Which of the following access control models introduces user security clearance and data classification?
A. Role-based access control
B. Discretionary access control
C. Non-discretionary access control
D. Mandatory access control
Answer: (SHOW ANSWER)
Explanation/Reference:
The mandatory access control model is based on a security label system. Users are given a security clearance and data is classified. The classification is stored in the security labels of the resources. Classification labels specify the level of trust a user must have to access a certain file.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter
4: Access Control (Page 154).

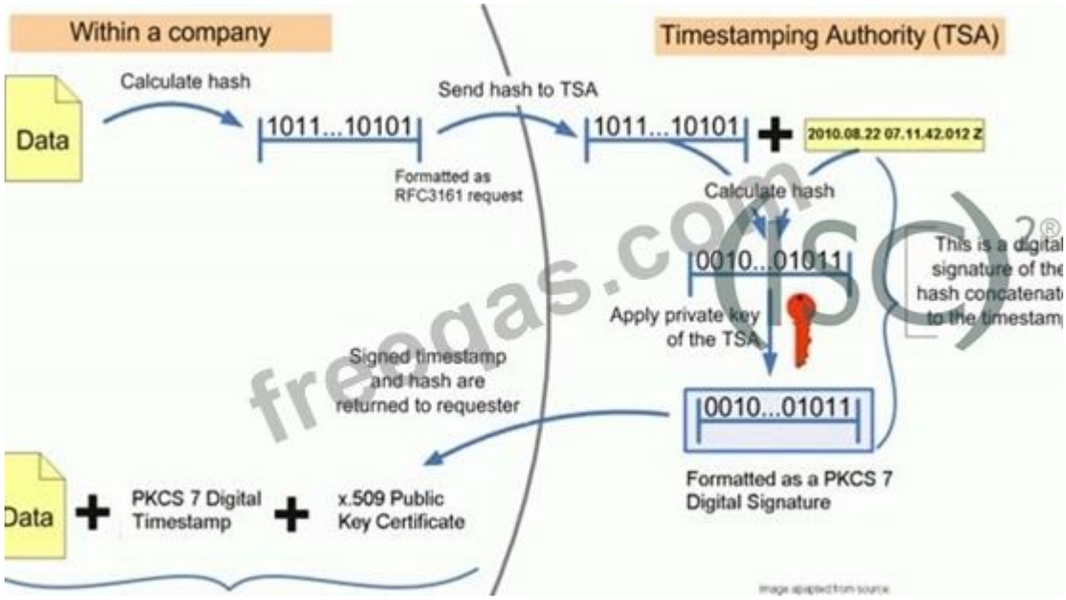
NEW QUESTION: 243
Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?
A. OAKLEY
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. IPsec Key exchange (IKE)
Answer: B (LEAVE A REPLY)
RFC 2828 (Internet Security Glossary) defines the Internet Security Association and Key Management Protocol (ISAKMP) as an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.
Let's clear up some confusion here first. Internet Key Exchange (IKE) is a hybrid protocol, it consists of 3 "protocols"
ISAKMP: It's not a key exchange protocol per se, it's a framework on which key exchange protocols operate. ISAKMP is part of IKE. IKE establishs the shared security policy and authenticated keys. ISAKMP is the protocol that specifies the mechanics of the key exchange.
Oakley: Describes the "modes" of key exchange (e.g. perfect forward secrecy for keys, identity protection, and authentication). Oakley describes a series of key exchanges and services.
SKEME: Provides support for public-key-based key exchange, key distribution centres, and manual installation, it also outlines methods of secure and fast key refreshment.
So yes, IPSec does use IKE, but ISAKMP is part of IKE.
The questions did not ask for the actual key negotiation being done but only for the "exchange of key generation and authentication data" being done. Under Oakly it would be Diffie Hellman (DH) that would be used for the actual key nogotiation.
The following are incorrect answers:
Simple Key-management for Internet Protocols (SKIP) is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.
OAKLEY is a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP.
IPsec Key Exchange (IKE) is an Internet, IPsec, key-establishment protocol [R2409] (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.
Reference used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 244

Single Sign-on (SSO) is characterized by which of the following advantages?
A. Convenience
B. Convenience and centralized administration
C. Convenience and centralized data administration
D. Convenience and centralized network administration
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Convenience -Using single sign-on users have to type their passwords only once when they first log in to access all the network resources; and Centralized Administration as some single sign-on systems are built around a unified server administration system. This allows a single administrator to add and delete accounts across the entire network from one user interface.
The following answers are incorrect:
Convenience - alone this is not the correct answer.
Centralized Data or Network Administration - these are thrown in to mislead the student. Neither are a benefit to SSO, as these specifically should not be allowed with just an SSO.
References: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, page 35.
TIPTON, Harold F. & HENRY, Kevin, Official (ISC)2 Guide to the CISSP CBK, 2007, page 180.

NEW QUESTION: 245
What is used to bind a document to its creation at a particular time?
A. Network Time Protocol (NTP)
B. Digital Signature
C. Digital Timestamp
D. Certification Authority (CA)
Answer: C (LEAVE A REPLY)
While a digital signature binds a document to the possessor of a particular key, a digital timestamp binds a document to its creation at a particular time.
Trusted timestamping is the process of securely keeping track of the creation and modification time of a document. Security here means that no one - not even the owner of the document - should be able to change it once it has been recorded provided that the timestamper's integrity is never compromised.
The administrative aspect involves setting up a publicly available, trusted timestamp management infrastructure to collect, process and renew timestamps or to make use of a commercially available time stamping service.
A modern example of using a Digital Timestamp is the case of an industrial research organization that may later need to prove, for patent purposes, that they made a particular discovery on a particular date; since magnetic media can be altered easily, this may be a nontrivial issue. One possible solution is for a researcher to compute and record in a hardcopy laboratory notebook a cryptographic hash of the relevant data file. In the future, should there be a need to prove the version of this file retrieved from a backup tape has not been altered, the hash function could be recomputed and compared with the hash value recorded in that paper notebook.

According to the RFC 3161 standard, a trusted timestamp is a timestamp issued by a trusted third party (TTP) acting as a Time Stamping Authority (TSA). It is used to prove the existence of certain data before a certain point (e.g. contracts, research data, medical records,...) without the possibility that the owner can backdate the timestamps. Multiple TSAs can be used to increase reliability and reduce vulnerability. The newer ANSI ASC X9.95 Standard for trusted timestamps augments the RFC 3161 standard with data-level security requirements to ensure data integrity against a reliable time source that is provable to any third party. This standard has been applied to authenticating digitally signed data for regulatory compliance, financial transactions, and legal evidence.



Digital TimeStamp

The following are incorrect answers:

Network Time Protocol (NTP) is used to achieve high accuracy time synchronization for computers across a network.

A Certification Authority (CA) is the entity responsible for the issuance of digital certificates.

A Digital Signature provides integrity and authentication but does not bind a document to a specific time it was created.

Reference used for this question:

http://en.m.wikipedia.org/wiki/File:Trusted_timestamping.gif

and

http://en.wikipedia.org/wiki/Trusted_timestamping

NEW QUESTION: 246

Which of the following are WELL KNOWN PORTS assigned by the IANA?

A. Ports 0 to 255

B. Ports 0 to 1024

C. Ports 0 to 1023

D. Ports 0 to 127

Answer: (SHOW ANSWER)

The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports. The range for assigned "Well Known" ports managed by the IANA (Internet Assigned Numbers Authority) is 0-1023.
Source: iana.org: port assignments.

NEW QUESTION: 247
How is Annualized Loss Expectancy (ALE) derived from a threat?
A. ARO x (SLE - EF)
B. SLE x ARO
C. SLE/EF
D. AV x EF
Answer: B (LEAVE A REPLY)
Three steps are undertaken in a quantitative risk assessment:
Initial management approval
Construction of a risk assessment team, and
The review of information currently available within the organization.
There are a few formulas that you MUST understand for the exam. See them below:
SLE (Single Loss Expectancy)
Single loss expectancy (SLE) must be calculated to provide an estimate of loss. SLE is defined as the difference between the original value and the remaining value of an asset after a single exploit.
The formula for calculating SLE is as follows: SLE = asset value (in $) x exposure factor (loss due to successful threat exploit, as a %)
Losses can include lack of availability of data assets due to data loss, theft, alteration, or denial of service (perhaps due to business continuity or security issues).
ALE (Annualized Loss Expectancy)
Next, the organization would calculate the annualized rate of occurrence (ARO).
This is done to provide an accurate calculation of annualized loss expectancy (ALE).
ARO is an estimate of how often a threat will be successful in exploiting a vulnerability over the period of a year.
When this is completed, the organization calculates the annualized loss expectancy (ALE).
The ALE is a product of the yearly estimate for the exploit (ARO) and the loss in value of an asset after an SLE.
The calculation follows ALE = SLE x ARO
Note that this calculation can be adjusted for geographical distances using the local annual frequency estimate (LAFE) or the standard annual frequency estimate (SAFE). Given that there is now a value for SLE, it is possible to determine what the organization should spend, if anything, to apply a countermeasure for the risk in question.
Remember that no countermeasure should be greater in cost than the risk it mitigates, transfers, or avoids.
Countermeasure cost per year is easy and straightforward to calculate. It is simply the cost

of the countermeasure divided by the years of its life (i.e., use within the organization).
Finally, the organization is able to compare the cost of the risk versus the cost of the countermeasure and make some objective decisions regarding its countermeasure selection.
The following were incorrect answers:
All of the other choices were incorrect.
The following reference(s) were used for this quesiton:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10048-10069). Auerbach Publications. Kindle Edition.

NEW QUESTION: 248
Which of the following items is NOT a benefit of cold sites?
A. No resource contention with other organisation
B. Quick Recovery
C. A secondary location is available to reconstruct the environment
D. Low Cost
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
A cold site is a permanent location that provide you with your own space that you can move into in case of a disaster or catastrophe. It is one of the cheapest solution available as a rental place but it is also the one that would take the most time to recover. A cold site usually takes one to two weeks for recoverey.
Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. The plan should include a trategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:
Dedicated site owned or operated by the organization. Also called redundant or alternate sites;
Reciprocal agreement or memorandum of agreement with an internal or external entity; and
Commercially leased facility.
Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites. Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types.
Progressing from basic to advanced, the sites are described below:
Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.
fWarm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.

Hot Sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.
As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each organization should evaluate its core requirements in order to establish the most effective solution.
Two examples of variations to the site types are:
fMobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.
fMirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.
There are obvious cost and ready-time differences among the options. In these examples, the mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain, although they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours, but the time necessary for equipment installation and setup can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel and/or equipment there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the organization's primary site.
The following reference(s) were used for this question:
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

NEW QUESTION: 249
Which must bear the primary responsibility for determining the level of protection needed for information systems resources?
A. IS security specialists
B. Senior Management
C. Senior security analysts
D. systems Auditors
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
If there is no support by senior management to implement, execute, and enforce security policies and procedure, then they won't work. Senior management must be involved in this because they have an obligation to the organization to protect the assests . The requirement here is for management to show "due diligence" in establishing an effective compliance, or security program. It is senior management that could face legal repercussions if they do not have sufficient controls in place.
The following answers are incorrect:
IS security specialists. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.

Senior security analysts. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.
systems auditors. Is incorrect because it is not the best answer, system auditors are responsible that the controls in place are effective. Senior management bears the primary responsibility for determining the level of protection needed.

NEW QUESTION: 250
Which protocol is NOT implemented in the Network layer of the OSI Protocol Stack?
A. hyper text transport protocol
B. Open Shortest Path First
C. Internet Protocol
D. Routing Information Protocol
Answer: A (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
Open Shortest Path First, Internet Protocol, and Routing Information Protocol are all protocols implemented in the Network Layer.
Domain: Telecommunications and Network Security
References: AIO 3rd edition. Page 429
Official Guide to the CISSP CBK. Page 411

NEW QUESTION: 251
Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?
A. Extensible Authentication Protocol
B. Challenge Handshake Authentication Protocol
C. Remote Authentication Dial-In User Service
D. Multilevel Authentication Protocol.
Answer: (SHOW ANSWER)
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines the Extensible Authentication Protocol as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge- response, and arbitrary dialog sequences. It is intended for use primarily by a host or router that connects to a PPP network server via switched circuits or dial-up lines. The Remote Authentication Dial-In User Service (RADIUS) is defined as an Internet protocol for carrying dial-in user's authentication information and configuration information between a shared, centralized authentication server and a network access server that needs to authenticate the users of its network access ports. The other option is a distracter.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 252
What is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity?
A. Polyinstantiation
B. Inference
C. Aggregation
D. Data mining
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Aggregation is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity.
The incorrect answers are:
Polyinstantiation is the development of a detailed version of an object from another object using different values in the new object.
Inference is the ability of users to infer or deduce information about data at sensitivity levels for which they do not have access privilege.
Data mining refers to searching through a data warehouse for data correlations.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 261).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Database Security Issues (page 358).

NEW QUESTION: 253
Which of the following pairings uses technology to enforce access control policies?
A. Preventive/Administrative
B. Preventive/Technical
C. Preventive/Physical
D. Detective/Administrative
Answer: B (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The preventive/technical pairing uses technology to enforce access control policies.
TECHNICAL CONTROLS
Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.
Preventive Technical Controls
Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:

Access control software.
Antivirus software.
Library control systems.
Passwords.
Smart cards.
Encryption.
Dial-up access control and callback systems.
Preventive Physical Controls
Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media) and to help protect against natural disasters. Examples of these controls include:
Backup files and documentation.
Fences.
Security guards.
Badge systems.
Double door systems.
Locks and keys.
Backup power.
Biometric access controls.
Site selection.
Fire extinguishers.
Preventive Administrative Controls
Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:
Security awareness and technical training.
Separation of duties.
Procedures for recruiting and terminating employees.
Security policies and procedures.
Supervision.
Disaster recovery, contingency, and emergency plans.
User registration for computer access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 254
Which of the following is a disadvantage of a statistical anomaly-based intrusion detection system?
A. it may truly detect a non-attack event that had caused a momentary anomaly in the system.
B. it may falsely detect a non-attack event that had caused a momentary anomaly in the system.
C. it may correctly detect a non-attack event that had caused a momentary anomaly in the system.
D. it may loosely detect a non-attack event that had caused a momentary anomaly in the system.

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Some disadvantages of a statistical anomaly-based ID are that it will not detect an attack that does not significantly change the system operating characteristics, or it may falsely detect a non-attack event that had caused a momentary anomaly in the system.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

NEW QUESTION: 255

Which security model uses division of operations into different parts and requires different users to perform each part?

A. Bell-LaPadula model

B. Biba model

C. Clark-Wilson model

D. Non-interference model

Answer: (SHOW ANSWER)

Explanation/Reference:

The Clark-Wilson model uses separation of duties, which divides an operation into different parts and requires different users to perform each part. This prevents authorized users from making unauthorized modifications to data, thereby protecting its integrity.

The Clark-Wilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.

The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent.

An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules.

The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction.

A well-formed transaction is a series of operations that transition a system from one consistent state to another consistent state.

In this model the integrity policy addresses the integrity of the transactions.

The principle of separation of duty requires that the certifier of a transaction and the implementer be different entities.

The model contains a number of basic constructs that represent both data items and processes that operate on those data items. The key data type in the Clark-Wilson model is a Constrained Data Item (CDI). An Integrity Verification Procedure (IVP) ensures that all CDIs in the system are valid at a certain state. Transactions that enforce the integrity policy are represented by Transformation Procedures (TPs). A TP takes as input a CDI or Unconstrained Data Item (UDI) and produces a CDI. A TP must transition the system from one valid state to another valid state. UDIs represent system input (such as that

provided by a user or adversary). A TP must guarantee (via certification) that it transforms all possible values of a UDI to a "safe" CDI.
In general, preservation of data integrity has three goals:
Prevent data modification by unauthorized parties
Prevent unauthorized data modification by authorized parties
Maintain internal and external consistency (i.e. data reflects the real world) Clark-Wilson addresses all three rules but BIBA addresses only the first rule of intergrity.
References:
HARRIS, Shon, All-In-One CISSP Certification Fifth Edition, McGraw-Hill/Osborne, Chapter 5: Security Architecture and Design (Page 341-344).
and
http://en.wikipedia.org/wiki/Clark-Wilson_model

NEW QUESTION: 256
What is the main characteristic of a multi-homed host?
A. It is placed between two routers or firewalls.
B. It allows IP routing.
C. It has multiple network interfaces, each connected to separate networks.
D. It operates at multiple layers.
Answer: C (LEAVE A REPLY)
The main characteristic of a multi-homed host is that is has multiple network interfaces, each connected to logically and physically separate networks. IP routing should be disabled to prevent the firewall from routing packets directly from one interface to the other.
Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 2 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 257
Which of the following is NOT a characteristic of a host-based intrusion detection system?
A. A HIDS does not consume large amounts of system resources
B. A HIDS can analyse system logs, processes and resources
C. A HIDS looks for unauthorized changes to the system
D. A HIDS can notify system administrators when unusual events are identified
Answer: A (LEAVE A REPLY)

A HIDS does not consume large amounts of system resources is the correct choice. HIDS can consume inordinate amounts of CPU and system resources in order to function effectively, especially during an event.
All the other answers are characteristics of HIDSes
A HIDS can:
scrutinize event logs, critical system files, and other auditable system resources; look for unauthorized change or suspicious patterns of behavior or activity can send alerts when unusual events are discovered
Reference:
Official guide to the CISSP CBK. Pages 197 to 198.

NEW QUESTION: 258
Crime Prevention Through Environmental Design (CPTED) is a discipline that:
A. Outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior.
B. Outlines how the proper design of the logical environment can reduce crime by directly affecting human behavior.
C. Outlines how the proper design of the detective control environment can reduce crime by directly affecting human behavior.
D. Outlines how the proper design of the administrative control environment can reduce crime by directly affecting human behavior.
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Crime Prevention Through Environmental Design (CPTED) is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. It provides guidance about lost and crime prevention through proper facility contruction and environmental components and procedures.
CPTED concepts were developed in the 1960s. They have been expanded upon and have matured as our environments and crime types have evolved. CPTED has been used not just to develop corporate physical security programs, but also for large-scale activities such as development of neighborhoods, towns, and cities.
It addresses landscaping, entrances, facility and neighborhood layouts, lighting, road placement, and traffic circulation patterns. It looks at microenvironments, such as offices and rest-rooms, and macroenvironments, like campuses and cities.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 435). McGraw-Hill. Kindle Edition.
and
CPTED Guide Book

NEW QUESTION: 259
Countermeasures address security concerns in which of the following categories?
A. Information
B. Operations
C. Computer
D. All of the listed categories
E. Communication
F. Physical
Answer: A (LEAVE A REPLY)

NEW QUESTION: 260
Which of the following does NOT use token-passing?
A. ARCnet
B. FDDI
C. Token-ring
D. IEEE 802.3
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
IEEE 802.3 specifies the standard for Ethernet and uses CSMA/CD, not token-passing.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
104).

NEW QUESTION: 261
What can be defined as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity?
A. A digital envelope
B. A cryptographic hash
C. A Message Authentication Code
D. A digital signature
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines a digital signature as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.
The steps to create a Digital Signature are very simple:
1. You create a Message Digest of the message you wish to send
2. You encrypt the message digest using your Private Key which is the action of Signing

3. You send the Message along with the Digital Signature to the recipient To validate the Digital Signature the recipient will make use of the sender Public Key. Here are the steps:
1. The receiver will decrypt the Digital Signature using the sender Publick Key producing a clear text message digest.
2. The receiver will produce his own message digest of the message received.
3. At this point the receiver will compare the two message digest (the one sent and the one produce by the receiver), if the two matches, it proves the authenticity of the message and it confirms that the message was not modified in transit validating the integrity as well. Digital Signatures provides for Authenticity and Integrity only. There is no confidentiality in place, if you wish to get confidentiality it would be needed for the sender to encrypt everything with the receiver public key as a last step before sending the message.
A Digital Envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient. In simple term it is a type of security that uses two layers of encryption to protect a message. First, the message itself is encoded using symmetric encryption, and then the key to decode the message is encrypted using public-key encryption. This technique overcomes one of the problems of public-key encryption, which is that it is slower than symmetric encryption. Because only the key is protected with public-key encryption, there is very little overhead.
A cryptographic hash is the result of a cryptographic hash function such as MD5, SHA-1, or SHA-2. A hash value also called a Message Digest is like a fingerprint of a message. It is used to proves integrity and ensure the message was not changed either in transit or in storage.
A Message Authentication Code (MAC) refers to an ANSI standard for a checksum that is computed with a keyed hash that is based on DES or it can also be produced without using DES by concataning the Secret Key at the end of the message (simply adding it at the end of the message) being sent and then producing a Message digest of the Message+Secret Key together. The MAC is then attached and sent along with the message but the Secret Key is NEVER sent in clear text over the network.
In cryptography, HMAC (Hash-based Message Authentication Code), is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key.
As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output length in bits and on the size and quality of the cryptographic key.
There is more than one type of MAC: Meet CBC-MAC
In cryptography, a Cipher Block Chaining Message Authentication Code, abbreviated CBC-MAC, is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the previous block. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher.
References:

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
http://www.webopedia.com/TERM/D/digital_envelope.html
and
http://en.wikipedia.org/wiki/CBC-MAC

NEW QUESTION: 262
Which of the following specifically addresses cyber attacks against an organization's IT systems?
A. Continuity of support plan
B. Business continuity plan
C. Incident response plan
D. Continuity of operations plan
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
The incident response plan focuses on information security responses to incidents affecting systems and/or networks. It establishes procedures to address cyber attacks against an organization's IT systems. These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware or software. The continuity of support plan is the same as an IT contingency plan.
It addresses IT system disruptions and establishes procedures for recovering a major application or general support system. It is not business process focused. The business continuity plan addresses business processes and provides procedures for sustaining essential business operations while recovering from a significant disruption. The continuity of operations plan addresses the subset of an organization's missions that are deemed most critical and procedures to sustain these functions at an alternate site for up to 30 days.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page
8).

NEW QUESTION: 263
What is a packet sniffer?
A. It tracks network connections to off-site locations.
B. It monitors network traffic for illegal packets.
C. It scans network segments for cabling faults.
D. It captures network traffic for later analysis.
Answer: D (LEAVE A REPLY)
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 264
Which of the following would best describe secondary evidence?
A. Oral testimony by a non-expert witness
B. Oral testimony by an expert witness
C. A copy of a piece of evidence
D. Evidence that proves a specific act
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
Secondary evidence is defined as a copy of evidence or oral description of its contents. It is considered not as reliable as best evidence. Evidence that proves or disproves a specific act through oral testimony based on information gathered through he witness's five senses is considered direct evidence. The fact that testimony is given by an expert only affects the witness's ability to offer an opinion instead of only testifying of the facts.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 310).

NEW QUESTION: 265
Which of the following are the two MOST common implementations of Intrusion Detection Systems?
A. Server-based and Host-based.
B. Network-based and Guest-based.
C. Network-based and Client-based.
D. Network-based and Host-based.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
The two most common implementations of Intrusion Detection are Network-based and Host-based.
IDS can be implemented as a network device, such as a router, switch, firewall, or dedicated device monitoring traffic, typically referred to as network IDS (NIDS).
The" (IDS) "technology can also be incorporated into a host system (HIDS) to monitor a single system for undesirable activities. "
A network intrusion detection system (NIDS) is a network device .... that monitors traffic traversing the network segment for which it is integrated." Remember that NIDS are usually passive in nature.
HIDS is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3649-3652). Auerbach Publications. Kindle Edition.

NEW QUESTION: 266
Which of the following is an advantage that UDP has over TCP?
A. UDP is connection-oriented whereas TCP is not.
B. UDP is more reliable than TCP.
C. UDP is faster than TCP.
D. UDP makes a better effort to deliver packets.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
UDP is a scaled-down version of TCP. It is used like TCP, but only offers a "best effort" delivery. It is connectionless, does not offer error correction, does not sequence the packet segments, and less reliable than TCP but because of its lower overhead, it provides a faster transmission than TCP.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
86).

NEW QUESTION: 267
Which of the following statements pertaining to protection rings is false?
A. They provide strict boundaries and definitions on what the processes that work within each ring can access.
B. Programs operating in inner rings are usually referred to as existing in a privileged mode.
C. They support the CIA triad requirements of multitasking operating systems.
D. They provide users with a direct access to peripherals
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
In computer science, hierarchical protection domains, often called protection rings, are mechanisms to protect data and functionality from faults (fault tolerance) and malicious behaviour (computer security). This approach is diametrically opposite to that of capability-based security.
Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level.
Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.
Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources

intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.
"They provide strict boundaries and definitions on what the processes that work within each ring can access" is incorrect. This is in fact one of the characteristics of a ring protection system.
"Programs operating in inner rings are usually referred to as existing in a privileged mode" is incorrect. This is in fact one of the characteristics of a ring protection system.
"They support the CIA triad requirements of multitasking operating systems" is incorrect. This is in fact one of the characteristics of a ring protection system.
Reference(s) used for this question:
CBK, pp. 310-311
AIO3, pp. 253-256
AIOv4 Security Architecture and Design (pages 308 - 310)
AIOv5 Security Architecture and Design (pages 309 - 312)

NEW QUESTION: 268
Which expert system operating mode allows determining if a given hypothesis is valid?
A. Blackboard
B. Lateral chaining
C. Forward chaining
D. Backward chaining
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Backward-chaining mode - the expert system backtracks to determine if a given hypothesis is valid. Backward-chaining is generally used when there are a large number of possible solutions relative to the number of inputs.
Incorrect answers are:
In a forward-chaining mode, the expert system acquires information and comes to a conclusion based on that information. Forward-chaining is the reasoning approach that can be used when there is a small number of solutions relative to the number of inputs.
Blackboard is an expert system-reasoning methodology in which a solution is generated by the use of a virtual blackboard, wherein information or potential solutions are placed on the blackboard by a plurality of individuals or expert knowledge sources. As more information is placed on the blackboard in an iterative process, a solution is generated.
Lateral-chaining mode - No such expert system mode.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 259).

KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Expert Systems (page 354).

NEW QUESTION: 269
The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated up to?
A. Illiminated at nine feet high with at least three foot-candles
B. Illiminated at eight feet high with at least three foot-candles
C. Illiminated at eight feet high with at least two foot-candles
D. Illuminated at nine feet high with at least two foot-candles
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated eight feet high with at least two foot-candles.
It can also be referred to as illuminating to a height of eight feet, with a BRIGHTNESS of two foot-candles.
One footcandle ≈ 10.764 lux. The footcandle (or lumen per square foot) is a non-SI unit of illuminance. Like the BTU, it is obsolete but it is still in fairly common use in the United States, particularly in construction-related engineering and in building codes. Because lux and footcandles are different units of the same quantity, it is perfectly valid to convert footcandles to lux and vice versa.
The name "footcandle" conveys "the illuminance cast on a surface by a one-candela source one foot away." As natural as this sounds, this style of name is now frowned upon, because the dimensional formula for the unit is not foot * candela, but lumens per square foot.
Some sources do however note that the "lux" can be thought of as a "metre-candle" (i.e. the illuminance cast on a surface by a one-candela source one meter away). A source that is farther away casts less illumination than one that is close, so one lux is less illuminance than one footcandle. Since illuminance follows the inverse- square law, and since one foot = 0.3048 m, one lux = 0.30482 footcandle ≈ 1/10.764 footcandle.
TIPS FROM CLEMENT:
Illuminance (light level) - The amount of light, measured in foot-candles (US unit), that falls n a surface, either horizontal or vertical.
Parking lots lighting needs to be an average of 2 foot candles; uniformity of not more than 3:1, no area less than 1 fc.
All illuminance measurements are to be made on the horizontal plane with a certified light meter calibrated to NIST standards using traceable light sources.
The CISSP Exam Cram 2 from Michael Gregg says:
Lighting is a commonly used form of perimeter protection.
Some studies have found that up to 80% of criminal acts at businesses and shopping centers happen in adjacent parking lots. Therefore, it's easy to see why lighting can be such an important concern.
Outside lighting discourages prowlers and thieves.

The National Institute of Standards and Technologies (NIST) states that, for effective perimeter control, buildings should be illuminated 8 feet high, with 2-foot candle power.
Reference used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 325.
and
Shon's AIO v5 pg 459
and
http://en.wikipedia.org/wiki/Foot-candle

NEW QUESTION: 270
Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?
A. B
B. A
C. C
D. D
Answer: A (LEAVE A REPLY)
Explanation/Reference:
B level is the first Mandatory Access Control Level.
First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.
Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17920-17926). Auerbach Publications. Kindle Edition.
and
THE source for all TCSEC "level" questions: http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt (paragraph 3 for this one)

NEW QUESTION: 271
A channel within a computer system or network that is designed for the authorized transfer of information is identified as a(n)?
A. Covert channel
B. Overt channel
C. Opened channel

D. Closed channel

Answer: B (LEAVE A REPLY)

An overt channel is a path within a computer system or network that is designed for the authorized transfer of data. The opposite would be a covert channel which is an unauthorized path.

A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way. Receiving information in this manner clearly violates the system's security policy.

All of the other choices are bogus detractors.

Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 219. and Shon Harris, CISSP All In One (AIO), 6th Edition , page 380 and Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 378). McGraw-Hill. Kindle Edition.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 272

This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

A. Checkpoint level

B. Ceiling level

C. Clipping level

D. Threshold level

Answer: C (LEAVE A REPLY)

Section: Access Control

Explanation/Reference:

Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established. The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium- sized installations. Organizations with large-scale computing facilities often track all violations

and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).
If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred. Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch the perpetrator. In addition, business protection and preservation are strengthened.
The following answers are incorrect:
All of the other choices presented were simply detractors.
The following reference(s) were used for this question:
Handbook of Information Security Management

NEW QUESTION: 273
Which of the following questions is less likely to help in assessing identification and authentication controls?
A. Is a current list maintained and approved of authorized users and their access?
B. Are passwords changed at least every ninety days or earlier if needed?
C. Are inactive user identifications disabled after a specified period of time?
D. Is there a process for reporting incidents?
Answer: (SHOW ANSWER)
Explanation/Reference:
Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. Reporting incidents is more related to incident response capability (operational control) than to identification and authentication (technical control).
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-30 to A-32).

NEW QUESTION: 274
Which of the following prevents, detects, and corrects errors so that the integrity, availability, and confidentiality of transactions over networks may be maintained?
A. Communications security management and techniques
B. Information security management and techniques
C. Client security management and techniques
D. Server security management and techniques
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:

Communications security and techniques are the best area for addressing this objective.
"Information security management and techniques" is incorrect. While the overall information security program would include this objective, communications security is the more specific and better answer.
"Client security management and techniques" is incorrect. While client security plays a part in this overall objective, communications security is the more specific and better answer.
"Server security management and techniques" is incorrect. While server security plays a part in this overall objective, communications security is the more specific and better answer.
References:
CBK, p. 408

NEW QUESTION: 275
What is a common problem when using vibration detection devices for perimeter control?
A. They are vulnerable to non-adversarial disturbances.
B. They can be defeated by electronic means.
C. Signal amplitude is affected by weather conditions.
D. They must be buried below the frost line.
Answer: (SHOW ANSWER)
Vibration sensors are similar and are also implemented to detect forced entry. Financial institutions may choose to implement these types of sensors on exterior walls, where bank robbers may attempt to drive a vehicle through. They are also commonly used around the ceiling and flooring of vaults to detect someone trying to make an unauthorized bank withdrawal.
Such sensors are proned to false positive. If there is a large truck with heavy equipment driving by it may trigger the sensor. The same with a storm with thunder and lighting, it may trigger the alarm even thou there are no adversarial threat or disturbance.
The following are incorrect answers:
All of the other choices are incorrect.
Reference used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (pp. 495-496). McGraw-Hill . Kindle Edition.

NEW QUESTION: 276
Which of the following protects Kerberos against replay attacks?
A. Tokens
B. Passwords
C. Cryptography
D. Time stamps
Answer: (SHOW ANSWER)
A replay attack refers to the recording and retransmission of packets on the network. Kerberos uses time stamps, which protect against this type of attack.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 581).

NEW QUESTION: 277
Which of the following is an advantage that UDP has over TCP?
A. UDP is connection-oriented whereas TCP is not.
B. UDP is more reliable than TCP.
C. UDP is faster than TCP.
D. UDP makes a better effort to deliver packets.
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
UDP is a scaled-down version of TCP. It is used like TCP, but only offers a "best effort" delivery. It is connectionless, does not offer error correction, does not sequence the packet segments, and less reliable than TCP but because of its lower overhead, it provides a faster transmission than TCP.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
86).

NEW QUESTION: 278
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:
A. through access control mechanisms that require identification and authentication and through the audit function.
B. through logical or technical controls involving the restriction of access to systems and the protection of information.
C. through logical or technical controls but not involving the restriction of access to systems and the protection of information.
D. through access control mechanisms that do not require identification and authentication and do not operate through the audit function.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 279
Which of the following best describes the purpose of debugging programs?

A. To generate random data that can be used to test programs before implementing them.
B. To ensure that program coding flaws are detected and corrected.
C. To protect, during the programming phase, valid changes from being overwritten by other changes.
D. To compare source code versions before transferring to the test environment
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Debugging provides the basis for the programmer to correct the logic errors in a program under development before it goes into production.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 298).

NEW QUESTION: 280
Which of the following statements is NOT true of IPSec Transport mode?
A. It is required for gateways providing access to internal systems
B. Set-up when end-point is host or communications terminates at end-points
C. If used in gateway-to-host communication, gateway must act as host
D. When ESP is used for the security protocol, the hash is only applied to the upper layer protocols contained in the packet
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Source: TIPTON, Harold F & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

NEW QUESTION: 281
A security evaluation report and an accreditation statement are produced in which of the following phases of the system development life cycle?
A. project initiation and planning phase
B. system design specification phase
C. development & documentation phase
D. acceptance phase
Answer: D (LEAVE A REPLY)
Explanation/Reference:
"acceptance phase". Note the question asks about an "evaluation report" - which details how the system evaluated, and an "accreditation statement" which describes the level the system is allowed to operate at. Because those two activities are a part of testing and testing is a part of the acceptance phase, the only answer above that can be correct is "acceptance phase".
The other answers are not correct because:
The "project initiation and planning phase" is just the idea phase. Nothing has been developed yet to be evaluated, tested, accredited, etc.

The "system design specification phase" is essentially where the initiation and planning phase is fleshed out. For example, in the initiation and planning phase, we might decide we want the system to have authentication. In the design specification phase, we decide that that authentication will be accomplished via username/password. But there is still nothing actually developed at this point to evaluate or accredit. The "development & documentation phase" is where the system is created and documented. Part of the documentation includes specific evaluation and accreditation criteria. That is the criteria that will be used to evaluate and accredit the system during the "acceptance phase".
In other words - you cannot evaluate or accredit a system that has not been created yet. Of the four answers listed, only the acceptance phase is dealing with an existing system. The others deal with planning and creating the system, but the actual system isn't there yet.
Reference:
Official ISC2 Guide Page: 558 - 559
All in One Third Edition page: 832 - 833 (recommended reading)

NEW QUESTION: 282
Making sure that only those who are supposed to access the data can access is which of the following?
A. confidentiality.
B. capability.
C. integrity.
D. availability.
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate, domain definition. Confidentiality is making sure that only those who are supposed to access the data can access it.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 283
Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer
7 of the ISO/OSI Model?
A. Bridge
B. Repeater
C. Router
D. Gateway
Answer: D (LEAVE A REPLY)
Explanation/Reference:
A gateway is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.

Important Note:
For the purpose of the exam, you have to remember that a gateway is not synonymous to the term firewall.
The second thing you must remembers is the fact that a gateway act as a translation device.
It could be used to translate from IPX to TCP/IP for example. It could be used to convert different types of applications protocols and allow them to communicate together. A gateway could be at any of the OSI layers but usually tend to be higher up in the stack.
For your exam you should know the information below:
Repeaters
A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.
Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.
A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.
Repeater

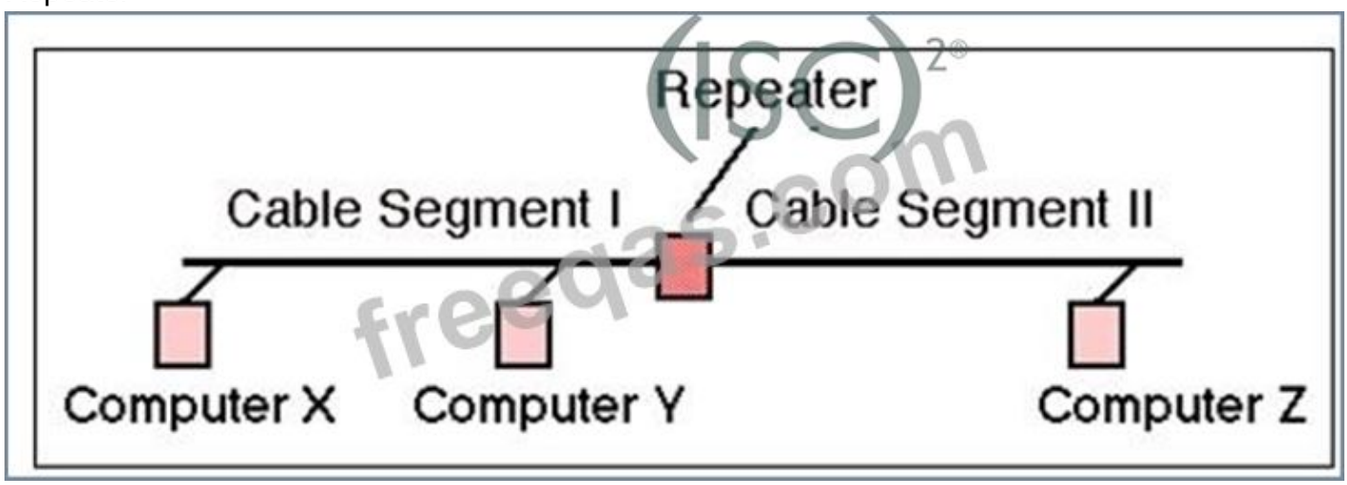


Image Reference- http://www.erg.abdn.ac.uk/~gorry/course/images/repeater.gif Bridges
A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.
Bridge

Image Reference- http://www.oreillynet.com/network/2001/01/30/graphics/bridge.jpg Routers
Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.
Router and Switch

Image Reference- http://www.computer-networking-success.com/images/router-switch.jpg Switches
Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.
Gateways

Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol
packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.
Gateway Server

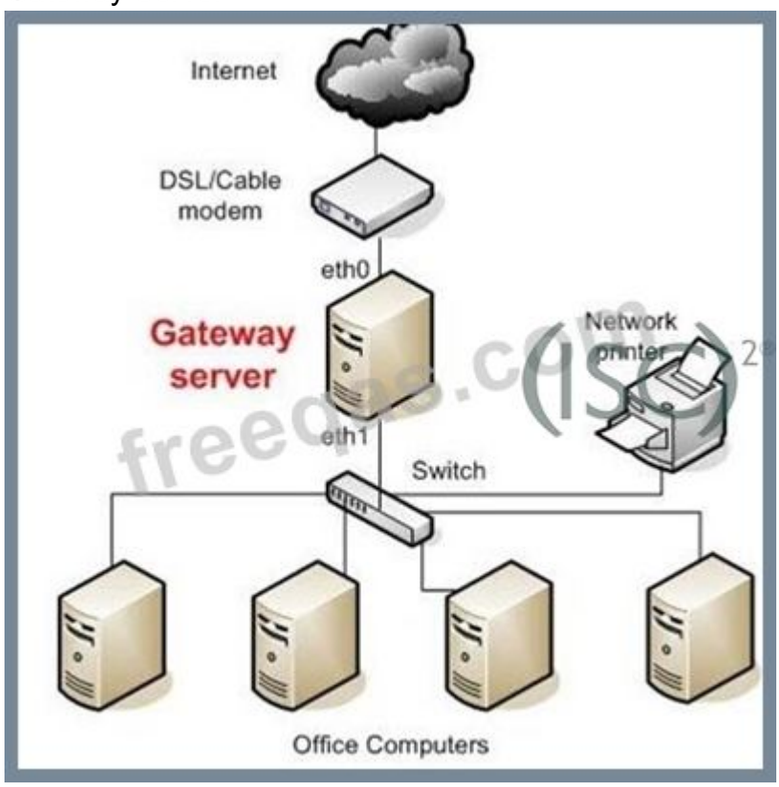


Image Reference-
http://static.howtoforge.com/images/screenshots/556af08d5e43aa768260f9e589dc547f-3024.jpg
The following answers are incorrect:
Repeater - A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.
Bridges - A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.
Routers - Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.)

A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 263
Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and 230

NEW QUESTION: 284
Which must bear the primary responsibility for determining the level of protection needed for information systems resources?
A. IS security specialists
B. Senior Management
C. Senior security analysts
D. systems Auditors
Answer: B (LEAVE A REPLY)
Explanation/Reference:
If there is no support by senior management to implement, execute, and enforce security policies and procedure, then they won't work. Senior management must be involved in this because they have an obligation to the organization to protect the assests . The requirement here is for management to show "due diligence" in establishing an effective compliance, or security program. It is senior management that could face legal repercussions if they do not have sufficient controls in place.
The following answers are incorrect:
IS security specialists. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.
Senior security analysts. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.
systems auditors. Is incorrect because it is not the best answer, system auditors are responsible that the controls in place are effective. Senior management bears the primary responsibility for determining the level of protection needed.

NEW QUESTION: 285
What IDS approach relies on a database of known attacks?
A. Signature-based intrusion detection
B. Statistical anomaly-based intrusion detection
C. Behavior-based intrusion detection
D. Network-based intrusion detection
Answer: A (LEAVE A REPLY)
A weakness of the signature-based (or knowledge-based) intrusion detection approach is that only attack signatures that are stored in a database are detected. Network-based intrusion detection can either be signature-based or statistical anomaly-
based (also called behavior-based).

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 49).

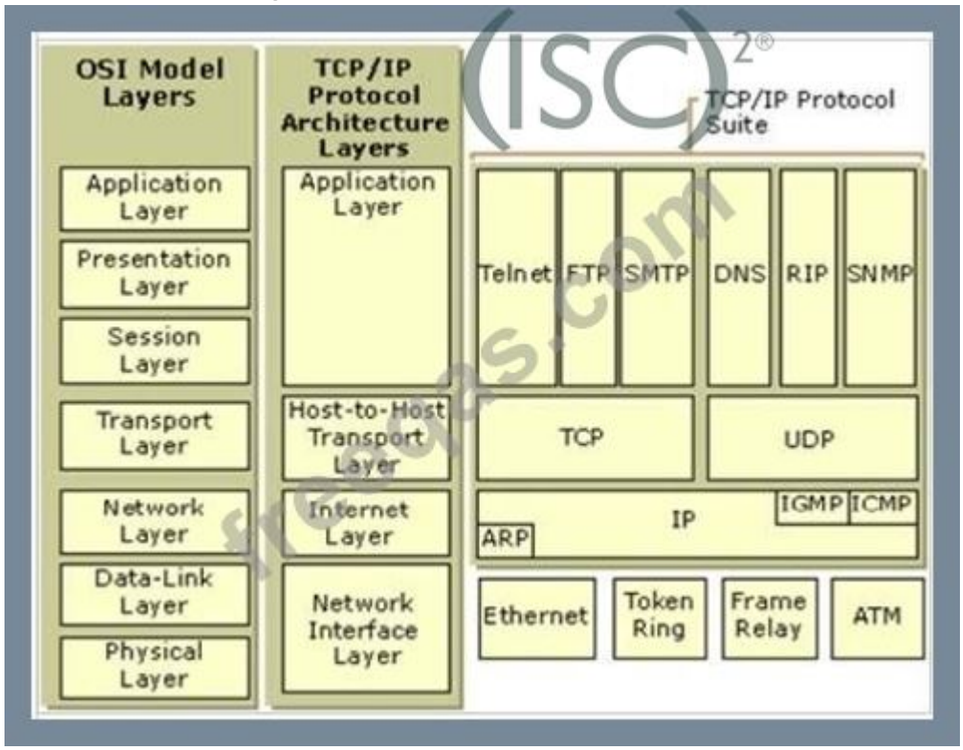
NEW QUESTION: 286
Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?
A. SESAME
B. RADIUS
C. KryptoKnight
D. TACACS+
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Secure European System for Applications in a Multi-vendor Environment (SESAME) was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support.
Reference:
TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 184.
ISC OIG Second Edition, Access Controls, Page 111

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 287
Which of the following protocols is not implemented at the Internet layer of the TCP/IP protocol model?
A. User datagram protocol (UDP)
B. Internet protocol (IP)
C. Internet Group Management Protocol (IGMP)
D. Internet control message protocol (ICMP)
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The User Datagram Protocol (UDP) is implemented at the host-to-host transport layer, not at the internet layer.
Protocol at what layer?

Ensure you are familiar with both the OSI model and the DoD TCP/IP model as well. You need to know how to contrast the two side by side and what are the names being used on both side. Below you have a graphic showing the two and how things maps between the two as well as some of the most common protcolos found at each of the layers:

Protocols at what layers of the DoD TCP/IP model



Graphic from http://technet.microsoft.com/en-us/library/cc958821.aspx

The following are incorrect answers:

All of the other protocols sit at the Internet Layer of the TCP/IP model.

NOTE:

Some reference are calling the Transport layer on the DoD model Host-to-Host.

Reference(s) used for this question:

Shon Harris, CISSP All In One (AIO), 6th edition , Telecommunication and Network Security, Page 518,534 and KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 85).

and

Microsoft Technet at http://technet.microsoft.com/en-us/library/cc958821.aspx

NEW QUESTION: 288

Identifying specific attempts to penetrate systems is the function of the _____.

A. Firewall

B. Vulnerability Scanner

C. Router

D. CERT - Computer Emergency Response Team

E. Intrusion Detection System

Answer: (SHOW ANSWER)

NEW QUESTION: 289
Which backup type run at regular intervals would take the least time to complete?
A. Full Backup
B. Differential Backup
C. Incremental Backup
D. Disk Mirroring
Answer: C (LEAVE A REPLY)
Incremental backups only backup changed data (changes archive bit to not backup again if not changed).
Although the incremental backup is fastest to backup, it is usually more time consuming for the restore process.
In some cases, the window available for backup may not be long enough to backup all the data on the system during each backup. In that case, differential or incremental backups may be more appropriate.
In an incremental backup, only the files that changed since the last backup will be backed up.
In a differential backup, only the files that changed since the last full backup will be backed up.
In general, differentials require more space than incremental backups while incremental backups are faster to perform. On the other hand, restoring data from incremental backups requires more time than differential backups. To restore from incremental backups, the last full backup and all of the incremental backups performed are combined. In contrast, restoring from a differential backup requires only the last full backup and the latest differential.
The following are incorrect answers:
Differential backups backup all data since the last full backup (does not reset archive bit)
Full backups backup all selected data, regardless of archive bit, and resets the archive bit.
Disk mirroring is not considered as a backup type.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20385-20390). Auerbach Publications. Kindle Edition.
and
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 618).

NEW QUESTION: 290
Guards are appropriate whenever the function required by the security program involves which of the following?

A. The use of discriminating judgment
B. The use of physical force
C. The operation of access control devices
D. The need to detect unauthorized access
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The Answer: The use of discriminating judgment, a guard can make the determinations that hardware or other automated security devices cannot make due to its ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment. Guards are better at making value decisions at times of incidents. They are appropriate whenever immediate, discriminating judgment is required by the security entity.
The following answers are incorrect:
The use of physical force This is not the best answer. A guard provides discriminating judgment, and the ability to discern the need for physical force.
The operation of access control devices A guard is often uninvolved in the operations of an automated access control device such as a biometric reader, a smart lock, mantrap, etc.
The need to detect unauthorized access The primary function of a guard is not to detect unauthorized access, but to prevent unauthorized physical access attempts and may deter social engineering attempts.
The following reference(s) were/was used to create this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 339).
Source: ISC2 Offical Guide to the CBK page 288-289.

NEW QUESTION: 291
Which of the following statements pertaining to PPTP (Point-to-Point Tunneling Protocol) is incorrect?
A. PPTP allow the tunnelling of any protocols that can be carried within PPP.
B. PPTP does not provide strong encryption.
C. PPTP does not support any token-based authentication method for users.
D. PPTP is derived from L2TP.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
PPTP is an encapsulation protocol based on PPP that works at OSI layer 2 (Data Link) and that enables a single point-to-point connection, usually between a client and a server.
While PPTP depends on IP to establish its connection.
As currently implemented, PPTP encapsulates PPP packets using a modified version of the generic routing encapsulation (GRE) protocol, which gives PPTP to the flexibility of handling protocols other than IP, such as IPX and NETBEUI over IP networks.
PPTP does have some limitations:

It does not provide strong encryption for protecting data, nor does it support any token-based methods for authenticating users.
L2TP is derived from L2F and PPTP, not the opposite.

NEW QUESTION: 292
Making sure that the data has not been changed unintentionally, due to an accident or malice is:
A. Integrity.
B. Confidentiality.
C. Availability.
D. Auditability.
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Integrity refers to the protection of information from unauthorized modification or deletion.
Confidentiality is incorrect. Confidentiality refers to the protection of information from unauthorized disclosure.
Availability is incorrect. Availability refers to the assurance that information and services will be available to authorized users in accordance with the service level objective.
Auditability is incorrect. Auditability refers to the ability to trace an action to the identity that performed it and identify the date and time at which it occurred.
References:
CBK, pp. 5 - 6
AIO3, pp. 56 - 57

NEW QUESTION: 293
What type of software can be used to prevent, detect (and possibly correct) malicious activities on a system?
A. Antivirus
B. All methods listed
C. Personal Firewall
D. IDS - host based
Answer: (SHOW ANSWER)

NEW QUESTION: 294
If you the text listed below at the beginning or end of an email message, what would it be anindication of?
mQGiBDfJY1ERBADd1lBX8WlbSHj2uDt6YbMVl4Da3O1yG0exQnEwU3sKQARzspNB zB2BF
+ngFiy1+RSfDjfbpwz6vLHo6zQZkT2vKOfDu1e4/LqiuOLpd/6rOrmH/Mvk
A. A software error
B. A PGP Signed message
C. A virus
D. A worm

Answer: B (LEAVE A REPLY)

NEW QUESTION: 295
What do the ILOVEYOU and Melissa virus attacks have in common?
A. They are both denial-of-service (DOS) attacks.
B. They have nothing in common.
C. They are both masquerading attacks.
D. They are both social engineering attacks.
Answer: (SHOW ANSWER)
While a masquerading attack can be considered a type of social engineering,
the Melissa and ILOVEYOU viruses are examples of masquerading attacks, even if it may
cause some kind of denial of service due to the web server being flooded with messages.
In this case, the receiver confidently opens a message coming from a trusted individual,
only to find that the message was sent using the trusted party's identity.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-
Hill/Osborne, 2002, Chapter 10: Law, Investigation, and Ethics (page 650).

NEW QUESTION: 296
Which access model is most appropriate for companies with a high employee turnover?
A. Role-based access control
B. Mandatory access control
C. Lattice-based access control
D. Discretionary access control
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
The underlying problem for a company with a lot of turnover is assuring that new employees are assigned the correct access permissions and that those permissions are removed when they leave the company.
Selecting the best answer requires one to think about the access control options in the context of a company with a lot of flux in the employee population. RBAC simplifies the task of assigning permissions because the permissions are assigned to roles which do not change based on who belongs to them. As employees join the company, it is simply a matter of assigning them to the appropriate roles and their permissions derive from their assigned role. They will implicitely inherit the permissions of the role or roles they have been assigned to.
When they leave the company or change jobs, their role assignment is revoked/changed appropriately.
Mandatory access control is incorrect. While controlling access based on the clearence level of employees and the sensitivity of obects is a better choice than some of the other incorrect answers, it is not the best choice when RBAC is an option and you are looking for the best solution for a high number of employees constantly leaving or joining the company.

Lattice-based access control is incorrect. The lattice is really a mathematical concept that is used in formally modeling information flow (Bell-Lapadula, Biba, etc). In the context of the question, an abstract model of information flow is not an appropriate choice. CBK, pp. 324-325.
Discretionary access control is incorrect. When an employee joins or leaves the company, the object owner must grant or revoke access for that employee on all the objects they own. Problems would also arise when the owner of an object leaves the company. The complexity of assuring that the permissions are added and removed correctly makes this the least desirable solution in this situation.
References
Alll in One, third edition page 165
RBAC is discussed on pp. 189 through 191 of the ISC(2) guide.

NEW QUESTION: 297
What can be defined as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire?
A. Certificate revocation list
B. Certificate revocation tree
C. Authority revocation list
D. Untrusted certificate list
Answer: C (LEAVE A REPLY)
Explanation/Reference:
The Internet Security Glossary (RFC2828) defines the Authority Revocation List (ARL) as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire.
Do not to confuse with an ARL with a Certificate Revocation List (CRL). A certificate revocation list is a mechanism for distributing notices of certificate revocations. The question specifically mentions "issued to CAs" which makes ARL a better answer than CRL.
http://rfclibrary.hosting.com/rfc/rfc2828/rfc2828-29.asp
$ certificate revocation list (CRL)
(I) A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were
scheduled to expire. (See: certificate expiration, X.509 certificate revocation list.)
http://rfclibrary.hosting.com/rfc/rfc2828/rfc2828-17.asp
$ authority revocation list (ARL)
(I) A data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire. (See: certificate expiration, X.509 authority revocation list.)
In a few words: We use CRL's for end-user cert revocation and ARL's for CA cert revocation - both can be placed in distribution points.

NEW QUESTION: 298
Which of the following best defines add-on security?

A. Physical security complementing logical security measures.
B. Protection mechanisms implemented as an integral part of an information system.
C. Layer security.
D. Protection mechanisms implemented after an information system has become operational.
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The Internet Security Glossary (RFC2828) defines add-on security as "The retrofitting of protection mechanisms, implemented by hardware or software, after the [automatic data processing] system has become operational." Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 299
Which of the following algorithms does NOT provide hashing?
A. SHA-1
B. MD2
C. RC4
D. MD5
Answer: C (LEAVE A REPLY)
As it is an algorithm used for encryption and does not provide hashing
functions , it is also commonly implemented ' Stream Ciphers '.
The other answers are incorrect because :
SHA-1 was designed by NIST and NSA to be used with the Digital Signature Standard
(DSS). SHA was designed to be used in digital signatures and was developed when a
more secure hashing algorithm was required for U.S. government applications.
MD2 is a one-way hash function designed by Ron Rivest that creates a 128-bit message
digest value. It is not necessarily any weaker than the other algorithms in the "MD" family,
but it is much slower.
MD5 was also created by Ron Rivest and is the newer version of MD4. It still produces a
128-bit hash, but the algorithm is more complex, which makes it harder to break.
Reference : Shon Harris , AIO v3 , Chapter - 8 : Cryptography , Page : 644 - 645

NEW QUESTION: 300
A 'Pseudo flaw' is which of the following?
A. An apparent loophole deliberately implanted in an operating system program as a trap for intruders.
B. An omission when generating Psuedo-code.
C. Used for testing for bounds violations in application programming.
D. A normally generated page fault causing the system to halt.
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:

A Pseudo flaw is something that looks like it is vulnerable to attack, but really acts as an alarm or triggers automatic actions when an intruder attempts to exploit the flaw.
The following answers are incorrect:
An omission when generating Psuedo-code. Is incorrect because it is a distractor.
Used for testing for bounds violations in application programming. Is incorrect, this is a testing methodology.
A normally generated page fault causing the system to halt. This is incorrect because it is distractor.

NEW QUESTION: 301
Which of the following best defines source routing?
A. The packets hold the forwarding information so they don't need to let bridges and routers decide what is the best route or way to get to the destination.
B. The packets hold source information in a fashion that source address cannot be forged.
C. The packets are encapsulated to conceal source information.
D. The packets hold information about redundant paths in order to provide a higher reliability.
Answer: A (LEAVE A REPLY)
With source routing, the packets hold the forwarding information so that they can find their way to the destination themselves without bridges and routers dictating their paths.
In computer networking, source routing allows a sender of a packet to specify the route the packet takes through the network.
With source routing the entire path to the destination is known to the sender and is included when sending data. Source routing differs from most other routing in that the source makes most or all of the routing decisions for each router along the way.
Source:
WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#2 Telecommunications and Network Security (page 5)
Wikipedia at http://en.wikipedia.org/wiki/Dynamic_Source_Routing

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 302
What is the PRIMARY use of a password?
A. Allow access to files.
B. Identify the user.
C. Authenticate the user.

D. Segregate various user's accesses.
Answer: (SHOW ANSWER)
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 303
What is called the access protection system that limits connections by calling back the number of a previously authorized location?
A. Sendback systems
B. Callback forward systems
C. Callback systems
D. Sendback forward systems
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The Answer: Call back Systems; Callback systems provide access protection by calling back the number of a previously authorized location, but this control can be compromised by call forwarding.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

NEW QUESTION: 304
Which of the following backup methods is most appropriate for off-site archiving?
A. Incremental backup method
B. Off-site backup method
C. Full backup method
D. Differential backup method
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The full backup makes a complete backup of every file on the system every time it is run. Since a single backup set is needed to perform a full restore, it is appropriate for off-site archiving.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
69).

NEW QUESTION: 305
How many bits is the effective length of the key of the Data Encryption Standard algorithm?
A. 168
B. 128
C. 56
D. 64

Answer: (SHOW ANSWER)
The correct answer is "56". This is actually a bit of a trick question, since the actual key length is 64 bits. However, every eighth bit is ignored because it is used for parity. This makes the "effective length of the key" that the question actually asks for 56 bits.
The other answers are not correct because:
168 - This is the number of effective bits in Triple DES (56 times 3).
128 - Many encryption algorithms use 128 bit key, but not DES. Note that you may see 128 bit encryption referred to as "military strength encryption" because many military systems use key of this length.
64 - This is the actual length of a DES encryption key, but not the "effective length" of the DES key.
Reference:
Official ISC2 Guide page: 238
All in One Third Edition page: 622

NEW QUESTION: 306
Which of the following would be an example of the best password?
A. golf001
B. Elizabeth
C. T1me4g0lF
D. password
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
The best passwords are those that are both easy to remember and hard to crack using a dictionary attack. The best way to create passwords that fulfil both criteria is to use two small unrelated words or phonemes, ideally with upper and lower case characters, a special character, and/or a number. Shouldn't be used: common names, DOB, spouse, phone numbers, words found in dictionaries or system defaults.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 1.

NEW QUESTION: 307
Which of the following is the primary reason why a user would choose a dial-up modem connection to the Internet when they have a faster, secure Internet connection through the organization's network?
A. To access web sites that blocked by the organization's proxy server.
B. To set up public services using the organization's resources.
C. To check their personal e-mail.
D. To circumvent the organization's security policy.
Answer: D (LEAVE A REPLY)
All the choices above represent examples of circumventing the organization's security policy, which is the primary reason why a user would be using a dial-up Internet connection when a secure connection is available through the

organization's network.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000,
Chapter 1: Understanding Firewalls.

NEW QUESTION: 308
Under the principle of culpable negligence, executives can be held liable for losses that result from computer system breaches if:
A. The company is not a multi-national company.
B. They have not exercised due care protecting computing resources.
C. They have failed to properly insure computer resources against loss.
D. The company does not prosecute the hacker that caused the breach.
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Culpable negligence is defined as: Recklessly acting without reasonable caution and putting another person at risk of injury or death (or failing to do something with the same consequences) Where a suspected security breach has been caused (through wilful intent or culpable negligence) disciplinary action may be sought in line with the appropriate misconduct guidelines for internal employees.
By not exercising Due Care and taking the proper actions, the executives would be liable for losses a company has suffered.
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
http://www.thefreedictionary.com/culpable+negligence

NEW QUESTION: 309
A Packet Filtering Firewall system is considered a:
A. first generation firewall.
B. second generation firewall.
C. third generation firewall.
D. fourth generation firewall.
Answer: A (LEAVE A REPLY)
The first types of firewalls were packet filtering firewalls. It is the most basic firewall making access decisions based on ACL's. It will filter traffic based on source IP and port as well as destination IP and port. It does not understand the context of the communication and inspects every single packet one by one without understanding the context of the connection.
"Second generation firewall" is incorrect. The second generation of firewall were Proxy based firewalls. Under proxy based firewall you have Application Level Proxy and also the Circuit-level proxy firewall. The application level proxy is very smart and understand the inner structure of the protocol itself. The Circui-Level Proxy is a generic proxy that allow you to proxy protocols for which you do not have an Application

Level Proxy. This is better than allowing a direct connection to the net. Today a great example of this would be the SOCKS protocol.
"Third generation firewall" is incorrect. The third generation firewall is the Stateful Inspection firewall. This type of firewall makes use of a state table to maintain the context of connections being established.
"Fourth generation firewall" is incorrect. The fourth generation firewall is the dynamic packet filtering firewall.
References:
CBK, p. 464 AIO3, pp. 482 - 484
Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm for a general discussion of the different generations.

NEW QUESTION: 310
To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:
A. Access Rules
B. Access Matrix
C. Identification controls
D. Access terminal
Answer: (SHOW ANSWER)
Explanation/Reference:
Controlling access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up access rules.
These rules can be classified into three access control models: Mandatory, Discretionary, and Non-Discretionary.
An access matrix is one of the means used to implement access control.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 311
Which of the following tasks is NOT usually part of a Business Impact Analysis (BIA)?
A. Calculate the risk for each different business function.
B. Identify the company's critical business functions.
C. Calculate how long these functions can survive without these resources.
D. Develop a mission statement.
Answer: (SHOW ANSWER)
Explanation/Reference:
The Business Impact Analysis is critical for the development of a business continuity plan (BCP). It identifies risks, critical processes and resources needed in case of recovery and quantifies the impact a

disaster will have upon the organization. The development of a mission statement is normally performed before the BIA.
A BIA (business impact analysis) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions ; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level.
BIA Steps
The more detailed and granular steps of a BIA are outlined here:
1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Location 21076). Auerbach Publications. Kindle Edition.
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 905-910). McGraw-Hill. Kindle Edition.

NEW QUESTION: 312
Which of the following should NOT be performed by an operator?
A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry
D. Controlling job flow
E. Section: Security Operation Adimnistration
Explanation/Reference:
Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.
System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system's security policy. As such, use of these privileges should be monitored through audit logs.
Some of the privileges and responsibilities assigned to operators include:

Implementing the initial program load: This is used to start the operating system. The boot process or initial program load of a system is a critical time for ensuring system security. Interruptions to this process may reduce the integrity of the system or cause the system to crash, precluding its availability.
Monitoring execution of the system: Operators respond to various events, to include errors, interruptions, and job completion messages.
Volume mounting: This allows the desired application access to the system and its data.
Controlling job flow: Operators can initiate, pause, or terminate programs. This may allow an operator to affect the scheduling of jobs. Controlling job flow involves the manipulation of configuration information needed by the system. Operators with the ability to control a job or application can cause output to be altered or diverted, which can threaten the confidentiality.
Bypass label processing: This allows the operator to bypass security label information to run foreign tapes (foreign tapes are those from a different data center that would not be using the same label format that the system could run). This privilege should be strictly controlled to prevent unauthorized access.
Renaming and relabeling resources: This is sometimes necessary in the mainframe environment to allow programs to properly execute. Use of this privilege should be monitored, as it can allow the unauthorized viewing of sensitive information.
Reassignment of ports and lines: Operators are allowed to reassign ports or lines. If misused, reassignment can cause program errors, such as sending sensitive output to an unsecured location. Furthermore, an incidental port may be opened, subjecting the system to an attack through the creation of a new entry point into the system.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 19367-19395). Auerbach Publications. Kindle Edition.
129
Which of the following should be performed by an operator?
A. Changing profiles
B. Approving changes
C. Adding and removal of users
D. Installing system software
Answer: C (LEAVE A REPLY)
Of the listed tasks, installing system software is the only task that should normally be performed by an operator in a properly segregated environment.
Source: MOSHER, Richard & ROTHKE, Ben, CISSP CBK Review presentation on domain 7.

NEW QUESTION: 313
Which of the following specifically addresses cyber attacks against an organization's IT systems?
A. Continuity of support plan
B. Business continuity plan
C. Incident response plan
D. Continuity of operations plan
Answer: (SHOW ANSWER)

Section: Risk, Response and Recovery
Explanation/Reference:
The incident response plan focuses on information security responses to incidents affecting systems and/or networks. It establishes procedures to address cyber attacks against an organization's IT systems. These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware or software. The continuity of support plan is the same as an IT contingency plan.
It addresses IT system disruptions and establishes procedures for recovering a major application or general support system. It is not business process focused. The business continuity plan addresses business processes and provides procedures for sustaining essential business operations while recovering from a significant disruption. The continuity of operations plan addresses the subset of an organization's missions that are deemed most critical and procedures to sustain these functions at an alternate site for up to 30 days.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page
8).

NEW QUESTION: 314
Which of the following firewall rules found on a firewall installed between an organization's internal network and the Internet would present the greatest danger to the internal network?
A. Permit all traffic between local hosts.
B. Permit all inbound ssh traffic.
C. Permit all inbound tcp connections.
D. Permit all syslog traffic to log-server.abc.org.
Answer: C (LEAVE A REPLY)
Any opening of an internal network to the Internet is susceptible of creating a new vulnerability.
Of the given rules, the one that permits all inbound tcp connections is the less likely to be used since it amounts to almost having no firewall at all, tcp being widely used on the Internet.
Reference(s) used for this question:
ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 409).

NEW QUESTION: 315
Which of the following is NOT a characteristic or shortcoming of packet filtering gateways?
A. The source and destination addresses, protocols, and ports contained in the IP packet header are the only information that is available to the router in making a decision whether or not to permit traffic access to an internal network.
B. They don't protect against IP or DNS address spoofing.
C. They do not support strong user authentication.

D. They are appropriate for medium-risk environment.

Answer: D (LEAVE A REPLY)

Section: Network and Telecommunications

Explanation/Reference:

Packet filtering firewalls use routers with packet filtering rules to grant or deny access based on source address, destination address, and port.

They offer minimum security but at a very low cost, and can be an appropriate choice for a low-risk environment.

Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 60).

NEW QUESTION: 316

Which of the following is the MOST important aspect relating to employee termination?

A. The details of employee have been removed from active payroll files.

B. Company property provided to the employee has been returned.

C. User ID and passwords of the employee have been deleted.

D. The appropriate company staff are notified about the termination.

Answer: D (LEAVE A REPLY)

Even though Logical access to information by a terminated employee is possible if the ID and password of the terminated employee has not been deleted this is only one part of the termination procedures. If user ID is not disabled or deleted, it could be possible for the employee without physical access to visit the companies networks remotely and gain access to the information.

Please note that this can also be seen in a different way: the most important thing to do could also be to inform others of the person's termination, because even if user ID's and passwords are deleted, a terminated individual could simply socially engineer their way back in by calling an individual he/she used to work with and ask them for access. He could intrude on the facility or use other weaknesses to gain access to information after he has been terminated.

By notifying the appropriate company staff about the termination, they would in turn intitiate account termination, ask the employee to return company property, and all credentials would be withdrawn for the individual concerned. This answer is more complete than simply disabling account.

It seems harsh and cold when this actually takes place , but too many companies have been hurt by vengeful employees who have lashed out at the company when their positions were revoked for one reason or another. If an employee is disgruntled in any way, or the termination is unfriendly, that employee's accounts should be disabled right away, and all passwords on all systems changed.

For your exam you should know the information below:

Employee Termination Processes Employees join and leave organizations every day. The reasons vary widely, due to retirement,reduction in force, layoffs, termination with or without cause, relocation to another city, careeropportunities with other employers, or involuntary transfers. Terminations may be friendly or unfriendly and will need different levels of care as a result.

Friendly Terminations Regular termination is when there is little or no evidence or reason to believe that the termination is not agreeable to both the company and the employee. A standard set of procedures,

typically maintained by the human resources department, governs the dismissal of the terminated employee to ensure that company property is returned, and all access is removed. These procedures may include exit interviews and return of keys, identification cards, badges, tokens, and cryptographic keys. Other property, such as laptops, cable locks, credit cards, and phone cards, are also collected. The user manager notifies the security department of the termination to ensure that access is revoked for all platforms and facilities. Some facilities choose to immediately delete the accounts, while others choose to disable the accounts for a policy defined period, for example, 30 days, to account for changes or extensions in the final termination date. The termination process should include a conversation with the departing associate about their continued responsibility for confidentiality of information.
Unfriendly Terminations Unfriendly terminations may occur when the individual is fired, involuntarily transferred, laid off,or when the organization has reason to believe that the individual has the means and intention to potentially cause harm to the system. Individuals with technical skills and higher levels of access, such as the systems administrators, computer programmers, database administrators, or any individual with elevated privileges, may present higher risk to the environment. These individuals could alter files, plant logic bombs to create system file damage at a future date, or remove sensitive information. Other disgruntled users could enter erroneous data into the system that may not be discovered for several months. In these situations, immediate termination of systems access is warranted at the time of termination or prior to notifying the employee of the termination. Managing the people aspect of security, from pre-employment to postemployment, is critical to ensure that trustworthy, competent resources are employed to further the business objectives that will protect company information. Each of these actions contributes to preventive, detective, or corrective personnel controls.
The following answers are incorrect:
The other options are less important.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 99
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 129). McGraw-Hill. Kindle Edition.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 317
Which of the following would assist the most in Host Based intrusion detection?
A. audit trails.
B. access control lists.
C. security clearances

D. host-based authentication

Answer: (SHOW ANSWER)

Section: Analysis and Monitoring

Explanation/Reference:

To assist in Intrusion Detection you would review audit logs for access violations.

The following answers are incorrect:

access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.

security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.

host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

NEW QUESTION: 318

Which of the following would be true about Static password tokens?

A. The owner identity is authenticated by the token

B. The owner will never be authenticated by the token.

C. The owner will authenticate himself to the system.

D. The token does not authenticates the token owner but the system.

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Password Tokens

Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a dynamic system the user will often have to log themselves in.

Static Password Tokens:

The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room.

Synchronous Dynamic Password Tokens:

This system is a lot more complex then the static token password. The synchronous dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring. Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have troubles authenticating themselves to the system.

Asynchronous Dynamic Password Tokens:

The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principal as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the companies VPN (Virtual private Network).
Challenge Response Tokens:
This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals. The user inputs this challenge string into their token device and the device will respond by generating a challenge response. The user then types this response into the system and if it is correct they are authenticated.
Reference(s) used for this question:
http://www.informit.com/guides/content.aspx?g=security&seqNum=146
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION: 319
The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?
A. integrity and confidentiality.
B. confidentiality and availability.
C. integrity and availability.
D. none of the above.
Answer: C (LEAVE A REPLY)
TCSEC focused on confidentiality while ITSEC added integrity and availability as security goals.
The following answers are incorrect:
integrity and confidentiality. Is incorrect because TCSEC addressed confidentiality. confidentiality and availability. Is incorrect because TCSEC addressed confidentiality. none of the above. Is incorrect because ITSEC added integrity and availability as security goals.

NEW QUESTION: 320
A prolonged complete loss of electric power is a:
A. brownout
B. blackout
C. surge
D. fault
Answer: (SHOW ANSWER)
A prolonged power outage is a blackout.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 321

Which of the following does NOT concern itself with key management?
A. Internet Security Association Key Management Protocol (ISAKMP)
B. Diffie-Hellman (DH)
C. Cryptology (CRYPTO)
D. Key Exchange Algorithm (KEA)
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
Cryptology is the science that includes both cryptography and cryptanalysis and is not directly concerned with key management. Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis.
The following are all concerned with Key Management which makes them the wrong choices:
Internet Security Association Key Management Protocol (ISAKMP) is a key management protocol used by IPSec. ISAKMP (Internet Security Association and Key Management Protocol) is a protocol defined by RFC
2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange. The actual key exchange is done by the Oakley Key Determination Protocol which is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm.
Diffie-Hellman and one variation of the Diffie-Hellman algorithm called the Key Exchange Algorithm (KEA) are also key exchange protocols. Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. Diffie-Hellman key exchange (D-H) is a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
Reference(s) used for this question:
Mike Meyers CISSP Certification Passport, by Shon Harris and Mike Meyers, page 228.
It is highlighted as an EXAM TIP. Which tells you that it is a must know for the purpose of the exam.
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Chapter 8:
Cryptography (page 713-715).
and
https://en.wikipedia.org/wiki/ISAKMP
and
http://searchsecurity.techtarget.com/definition/cryptology

NEW QUESTION: 322

Which protocol makes USE of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?

A. SSH (Secure Shell)

B. S/MIME (Secure MIME)

C. SET (Secure Electronic Transaction)

D. SSL (Secure Sockets Layer)

Answer: C (LEAVE A REPLY)

As protocol was introduced by Visa and Mastercard to allow for more credit card transaction possibilities. It is comprised of three different pieces of software, running on the customer's PC (an electronic wallet), on the merchant's Web server and on the payment server of the merchant's bank. The credit card information is sent by the customer to the merchant's Web server, but it does not open it and instead digitally signs it and sends it to its bank's payment server for processing.

The following answers are incorrect because :

SSH (Secure Shell) is incorrect as it functions as a type of tunneling mechanism that provides terminal like access to remote computers.

S/MIME is incorrect as it is a standard for encrypting and digitally signing electronic mail and for providing secure data transmissions.

SSL is incorrect as it uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication.

Reference : Shon Harris AIO v3 , Chapter-8: Cryptography , Page : 667-669

NEW QUESTION: 323

Proxies works by transferring a copy of each accepted data packet from one network to another, thereby masking the:

A. data's payload

B. data's details

C. data's owner

D. data's origin

Answer: D (LEAVE A REPLY)

Explanation/Reference:

The application firewall (proxy) relays the traffic from a trusted host running a specific application to an untrusted server. It will appear to the untrusted server as if the request originated from the proxy server.

"Data's payload" is incorrect. Only the origin is changed.

"Data's details" is incorrect. Only the origin is changed.

"Data's owner" is incorrect. Only the origin is changed.

References:

CBK, p. 467

AIO3, pp. 486 - 490

NEW QUESTION: 324

The Trusted Computer Security Evaluation Criteria book (TCSEC) defines two types of assurance. What are they? (Choose two)

A. Life cycle assurance

B. Quality assurance

C. System architecture assurance

D. OS hardening methods and assurance

E. Operational assurance

Answer: A,E (LEAVE A REPLY)

Life cycle assurance ensures that a trusted computer base (TCB) is designed and developed with controlled standards that act to enforce protection at each stage in the system's life cycle. Operational assurance are concerned with the basic features and architecture of a system.

NEW QUESTION: 325

Which of the following is best defined as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it?

A. Aggregation

B. Inference

C. Clustering

D. Collision

Answer: A (LEAVE A REPLY)

Explanation/Reference:

The Internet Security Glossary (RFC2828) defines aggregation as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 326

Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys. This protocol establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis?

A. Internet Security Association and Key Management Protocol (ISAKMP)

B. Simple Key-management for Internet Protocols (SKIP)

C. Diffie-Hellman Key Distribution Protocol

D. IPsec Key exchange (IKE)

Answer: (SHOW ANSWER)

Explanation/Reference:

RFC 2828 (Internet Security Glossary) defines Simple Key Management for Internet Protocols (SKIP) as: A key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

SKIP is an hybrid Key distribution protocol similar to SSL, except that it establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-

session basis. Therefore, no connection setup overhead exists and new keys values are not continually generated.
SKIP uses the knowledge of its own secret key or private component and the destination's public component to calculate a unique key that can only be used between them.
IKE stand for Internet Key Exchange, it makes use of ISAKMP and OAKLEY internally.
Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication and a Diffie-Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.
The following are incorrect answers:
ISAKMP is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.
IKE is an Internet, IPsec, key-establishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.
IPsec Key exchange (IKE) is only a detracto.
Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol

NEW QUESTION: 327
Who should measure the effectiveness of Information System security related controls in an organization?
A. The local security specialist
B. The business manager
C. The systems auditor
D. The central security manager
Answer: (SHOW ANSWER)
Explanation/Reference:
It is the systems auditor that should lead the effort to ensure that the security controls are in place and effective. The audit would verify that the controls comply with polices, procedures, laws, and regulations where applicable. The findings would provide these to senior management.
The following answers are incorrect:
the local security specialist. Is incorrect because an independent review should take place by a third party.
The security specialist might offer mitigation strategies but it is the auditor that would ensure the effectiveness of the controls

the business manager. Is incorrect because the business manager would be responsible that the controls are in place, but it is the auditor that would ensure the effectiveness of the controls.
the central security manager. Is incorrect because the central security manager would be responsible for implementing the controls, but it is the auditor that is responsibe for ensuring their effectiveness.

NEW QUESTION: 328
All hosts on an IP network have a logical ID called a(n):
A. IP address.
B. MAC address.
C. TCP address.
D. Datagram address.
Answer: (SHOW ANSWER)
Explanation/Reference:
All hosts on a network have a logical ID that is called an IP address. An IP address is a numeric identifier that is assigned to each machine on an IP network. It designates the location of a device on a network. A MAC address is typically called a hardware address because it is "burned" into the NIC card. TCP address and Datagram address are imposter answers.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

NEW QUESTION: 329
How do you distinguish between a bridge and a router?
A. A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to.
B. "Bridge" and "router" are synonyms for equipment used to join two networks.
C. The bridge is a specific type of router used to connect a LAN to the global Internet.
D. The bridge connects multiple networks at the data link layer, while router connects multiple networks at the network layer.
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
A bridge operates at the Data Link Layer and a router operates at the Network Layer.
The following answers are incorrect:
A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to. Is incorrect because both forward packets this is not distinctive enough.
"Bridge" and "router" are synonyms for equipment used to join two networks. Is incorrect because the two are unique and operate at different layers of the OSI model.
The bridge is a specific type of router used to connect a LAN to the global Internet. Is incorrect because a bridge does not connect a LAN to the global internet, but connects networks together creating a LAN.

NEW QUESTION: 330

What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?

A. Biometrics

B. Micrometrics

C. Macrometrics

D. MicroBiometrics

Answer: A (LEAVE A REPLY)

Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

NEW QUESTION: 331

What is the primary reason why some sites choose not to implement Trivial File Transfer Protocol (TFTP)?

A. It is too complex to manage user access restrictions under TFTP

B. Due to the inherent security risks

C. It does not offer high level encryption like FTP

D. It cannot support the Lightwight Directory Access Protocol (LDAP)

Answer: B (LEAVE A REPLY)

Section: Network and Telecommunications

Explanation/Reference:

Some sites choose not to implement Trivial File Transfer Protocol (TFTP) due to the inherent security risks.

TFTP is a UDP-based file transfer program that provides no security. There is no user authentication. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 332

Devices that supply power when the commercial utility power system fails are called which of the following?

A. power conditioners

B. uninterruptible power supplies

C. power filters
D. power dividers
Answer: B (LEAVE A REPLY)
From Shon Harris AIO Fifth Edition:
Protecting power can be done in three ways: through UPSs, power line conditioners, and backup sources.
UPSs use battery packs that range in size and capacity. A UPS can be online or standby.
Online UPS systems use AC line voltage to charge a bank of batteries. When in use, the UPS has an inverter that changes the DC output from the batteries into the required AC form and that regulates the voltage as it powers computer devices.
Online UPS systems have the normal primary power passing through them day in and day out. They constantly provide power from their own inverters, even when the electric power is in proper use. Since the environment's electricity passes through this type of UPS all the time, the UPS device is able to quickly detect when a power failure takes place. An online UPS can provide the necessary electricity and picks up the load after a power failure much more quickly than a standby UPS.
Standby UPS devices stay inactive until a power line fails. The system has sensors that detect a power failure, and the load is switched to the battery pack. The switch to the battery pack is what causes the small delay in electricity being provided. So an online UPS picks up the load much more quickly than a standby UPS, but costs more of course.

NEW QUESTION: 333
Which of the following pairings uses technology to enforce access control policies?
A. Preventive/Administrative
B. Preventive/Technical
C. Preventive/Physical
D. Detective/Administrative
Answer: B (LEAVE A REPLY)
Explanation/Reference:
The preventive/technical pairing uses technology to enforce access control policies.
TECHNICAL CONTROLS
Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.
Preventive Technical Controls
Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:
Access control software.
Antivirus software.
Library control systems.
Passwords.
Smart cards.

Encryption.
Dial-up access control and callback systems.
Preventive Physical Controls
Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media) and to help protect against natural disasters. Examples of these controls include:
Backup files and documentation.
Fences.
Security guards.
Badge systems.
Double door systems.
Locks and keys.
Backup power.
Biometric access controls.
Site selection.
Fire extinguishers.
Preventive Administrative Controls
Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:
Security awareness and technical training.
Separation of duties.
Procedures for recruiting and terminating employees.
Security policies and procedures.
Supervision.
Disaster recovery, contingency, and emergency plans.
User registration for computer access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

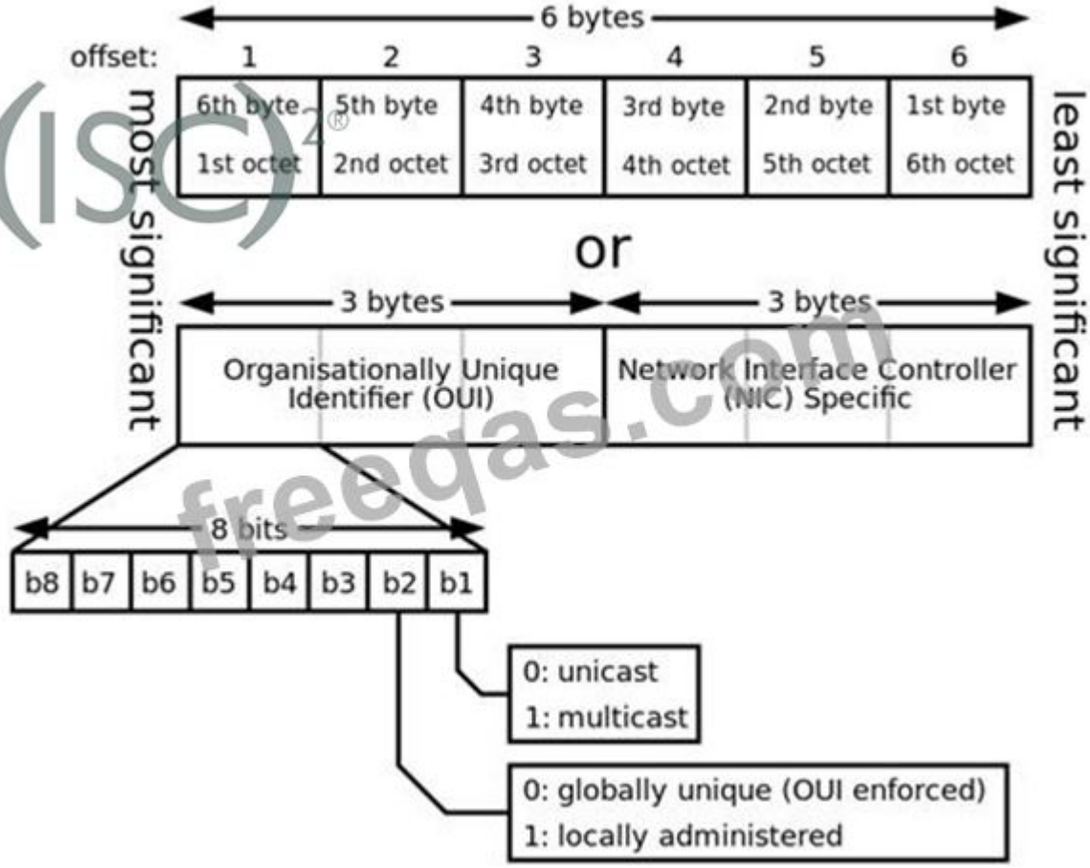
NEW QUESTION: 334
Which of the following types of Intrusion Detection Systems uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host?
A. Network-based ID systems.
B. Anomaly Detection.
C. Host-based ID systems.
D. Signature Analysis.
Answer: B (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:

There are two basic IDS analysis methods: pattern matching (also called signature analysis) and anomaly detection.
Anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host. Anomalies may include but are not limited to:
Multiple failed log-on attempts
Users logging in at strange hours
Unexplained changes to system clocks
Unusual error messages
The following are incorrect answers:
Network-based ID Systems (NIDS) are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network.
Host-based ID Systems (HIDS) is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.
Signature Analysis Some of the first IDS products used signature analysis as their detection method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the data stream) to produce an alert if that pattern was detected. For example, an attacker manipulating an FTP server may use a tool that sends a specially constructed packet. If that particular packet pattern is known, it can be represented in the form of a signature that IDS can then compare to incoming packets. Pattern-based IDS will have a database of hundreds, if not thousands, of signatures that are compared to traffic streams. As new attack signatures are produced, the system is updated, much like antivirus solutions. There are drawbacks to pattern-based IDS. Most importantly, signatures can only exist for known attacks. If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS. Additionally, if an attacker knows that the IDS is present, he or she can alter his or her methods to avoid detection. Changing packets and data streams, even slightly, from known signatures can cause an IDS to miss the attack. As with some antivirus systems, the IDS is only as good as the latest signature database on the system.
For additional information on Intrusion Detection Systems - http://en.wikipedia.org/wiki/Intrusion_detection_system Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3623-3625, 3649-3654, 3666-3686). Auerbach Publications. Kindle Edition.

NEW QUESTION: 335
Making sure that the data is accessible when and where it is needed is which of the following?

A. confidentiality
B. integrity
C. acceptability
D. availability
Answer: (SHOW ANSWER)
Explanation/Reference:
Availability is making sure that the data is accessible when and where it is needed.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 336
How many bits of a MAC address uniquely identify a vendor, as provided by the IEEE?
A. 6 bits
B. 12 bits
C. 16 bits
D. 24 bits
Answer: D (LEAVE A REPLY)
Explanation/Reference:
The MAC address is 48 bits long, 24 of which identify the vendor, as provided by the IEEE. The other 24 bits are provided by the vendor.
A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.
MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This is can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address. An example is many SOHO routers, where the ISP grants access to only one MAC address (used previously to inserting the router) so the router must use that MAC address on its Internet-facing NIC. Therefore the router administrator configures a MAC address to override the burned-in one.
A network node may have multiple NICs and each must have one unique MAC address per NIC.
See diagram below from Wikipedia showing the format of a MAC address. :
MAC Address format



Reference(s) used for this question:
http://en.wikipedia.org/wiki/MAC_address

NEW QUESTION: 337
Packet Filtering Firewalls can also enable access for:
A. only authorized application port or service numbers.
B. only unauthorized application port or service numbers.
C. only authorized application port or ex-service numbers.
D. only authorized application port or service integers.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Firewall rules can be used to enable access for traffic to specific ports or services. "Service numbers" is rather stilted English but you may encounter these types of wordings on the actual exam -- don't let them confuse you.
"Only unauthorized application port or service numbers" is incorrect. Unauthorized ports/services would be blocked in a properly installed firewall rather than permitting access.
"Only authorized application port or ex-service numbers" is incorrect. "Ex-service" numbers is a nonsense term meant to distract you.
"Only authorized application port or service integers." While service numbers are in fact integers, the more usual (and therefore better) answer is either service or "service number." References

CBK, p. 464
AIO3, pp. 482 - 484

NEW QUESTION: 338
Which of the following steps should be one of the first step performed in a Business Impact Analysis (BIA)?
A. Identify all CRITICAL business units within the organization.
B. Evaluate the impact of disruptive events.
C. Estimate the Recovery Time Objectives (RTO).
D. Identify and Prioritize Critical Organization Functions
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Project Initiation and Management
This is the first step in building the Business Continuity program is project initiation and management. During this phase, the following activities will occur:
Obtain senior management support to go forward with the project
Define a project scope, the objectives to be achieved, and the planning assumptions Estimate the project resources needed to be successful, both human resources and financial resources Define a timeline and major deliverables of the project In this phase, the program will be managed like a project, and a project manager should be assigned to the BC and DR domain.
The next step in the planning process is to have the planning team perform a BIA. The BIA will help the company decide what needs to be recovered, and how quickly. Mission functions are typically designated with terms such as critical, essential, supporting and nonessential to help determine the appropriate prioritization.
One of the first steps of a BIA is to Identify and Prioritize Critical Organization Functions. All organizational functions and the technology that supports them need to be classified based on their recovery priority.
Recovery time frames for organization operations are driven by the consequences of not performing the function. The consequences may be the result of organization lost during the down period; contractual commitments not met resulting in fines or lawsuits, lost goodwill with customers.
All other answers are incorrect.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 21073-21075). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20697-20710). Auerbach Publications. Kindle Edition.

NEW QUESTION: 339
The Telecommunications Security Domain of information security is also concerned with the prevention and detection of the misuse or abuse of systems, which poses a threat to the tenets of:

A. Confidentiality, Integrity, and Entity (C.I.E.).
B. Confidentiality, Integrity, and Authenticity (C.I.A.).
C. Confidentiality, Integrity, and Availability (C.I.A.).
D. Confidentiality, Integrity, and Liability (C.I.L.).
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The CIA acronym stands for Confidentiality, Integrity and Availability.
"Confidentiality, Integrity and Entity (CIE)" is incorrect. "Entity" is not part of the telecommunications domain definition.
"Confidentiality, Integrity and Authenticity (CIA)" is incorrect. While authenticity is included in the telecommunications domain, CIA is the acronym for confidentiality, integrity and availability.
"Confidentiality, Integrity, and Liability (CIL)" is incorrect. Liability is not part of the telecommunications domain definition.
References:
CBK, pp. 407 - 408

NEW QUESTION: 340
In biometric identification systems, the parts of the body conveniently available for identification are:
A. neck and mouth
B. hands, face, and eyes
C. feet and hair
D. voice and neck
Answer: B (LEAVE A REPLY)
Today implementation of fast, accurate, reliable, and user-acceptable biometric identification systems are already under way. Because most identity authentication takes place when a people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are hands, face, and eyes. From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

NEW QUESTION: 341
Upon which of the following ISO/OSI layers does network address translation operate?
A. Transport layer
B. Session layer
C. Data link layer
D. Network layer
Answer: (SHOW ANSWER)
Explanation/Reference:
Network address translation (NAT) is concerned with IP address translation between two networks and operates at the network layer (layer 3).

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter
3: Telecommunications and Network Security (page 440).

NEW QUESTION: 342
What is defined as the manner in which the network devices are organized to facilitate communications?
A. LAN transmission methods
B. LAN topologies
C. LAN transmission protocols
D. LAN media access methods
Answer: B (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
A network topology defines the manner in which the network devices are organized to facilitate communications. Common LAN technologies are:
bus
ring
star
meshed
LAN transmission methods refer to the way packets are sent on the network and are:
unicast
multicast
broadcast
LAN transmission protocols are the rules for communicating between computers on a LAN. Common LAN transmission protocols are:
CSMA/CD
polling
token-passing
LAN media access methods control the use of a network (physical and data link layers). They can be:
Ethernet
ARCnet
Token ring
FDDI
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
105).

NEW QUESTION: 343
Which of the following computer crime is MORE often associated with INSIDERS?
A. IP spoofing

B. Password sniffing
C. Data diddling
D. Denial of service (DOS)
Answer: C (LEAVE A REPLY)
Explanation/Reference:
It refers to the alteration of the existing data , most often seen before it is entered into an application.This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed.
The other answers are incorrect because :
IP Spoofing is not correct as the questions asks about the crime associated with the insiders. Spoofing is generally accomplished from the outside.
Password sniffing is also not the BEST answer as it requires a lot of technical knowledge in understanding the encryption and decryption process.
Denial of service (DOS) is also incorrect as most Denial of service attacks occur over the internet.
Reference : Shon Harris , AIO v3 , Chapter-10 : Law , Investigation & Ethics , Page : 758-760.

NEW QUESTION: 344
How many rounds are used by DES?
A. 16
B. 32
C. 64
D. 48
Answer: (SHOW ANSWER)
DES is a block encryption algorithm using 56-bit keys and 64-bit blocks that are divided in half and each character is encrypted one at a time. The characters are put through 16 rounds of transposition and substitution functions. Triple DES uses 48 rounds. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 3).

NEW QUESTION: 345
Which of the following type of traffic can easily be filtered with a stateful packet filter by enforcing the context or state of the request?
A. ICMP
B. TCP
C. UDP
D. IP
Answer: B (LEAVE A REPLY)
Explanation/Reference:
The question is explict in asking *easily*. With TCP connection establishment there is a distinct state or sequence that can be expected. Consult the references for further details.

ICMP, IP and UDP don't have any concept of a session; i.e. each packet or datagram is handled individually, with no reference to the contents of the previous one. With no sessions, these protocols usually cannot be filtered on the state of the session.
Some newer firewalls, however, simulate the concept of state for these protocols, and filter out unexpected packets based upon normal usage. Although these are commonly treated like normal stateful filters, they are more complex to program, and hence more prone to errors.
A stateful packet filter or stateful inspection inspects each packet and only allows known connection states through. So, if a SYN/ACK packet was recieved and there was not a prior SYN packet sent it would filter that packet and not let it in. The correct sequence of steps are known and if the sequence or state is incorrect then it is dropped.
The incorrect answers are:
ICMP. ICMP is basically stateless so you could not easily filter them based on the state or sequence.
UDP. UDP has no real state so you could only partially filter them based on the state or sequence. The question was explicit in asking easily. While it is possible, UDP is not the best answer.
IP. IP would refer to the Internet Protocol and as such is stateless so you would not be able to filter it out easily.
The following reference(s) were used for this question:
http://www.nwo.net/ipf/ipf-howto.pdf

NEW QUESTION: 346
It is a violation of the "separation of duties" principle when which of the following individuals access the software on systems implementing security?
A. security administrator
B. security analyst
C. systems auditor
D. systems programmer
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Reason: The security administrator, security analysis, and the system auditor need access to portions of the security systems to accomplish their jobs. The system programmer does not need access to the working (AKA: Production) security systems.
Programmers should not be allowed to have ongoing direct access to computers running production systems (systems used by the organization to operate its business). To maintain system integrity, any changes they make to production systems should be tracked by the organization's change management control system.
Because the security administrator's job is to perform security functions, the performance of non-security tasks must be strictly limited. This separation of duties reduces the likelihood of loss that results from users abusing their authority by taking actions outside of their assigned functional responsibilities.
References:

OFFICIAL (ISC)2 GUIDE TO THE CISSP EXAM (2003), Hansche, S., Berti, J., Hare, H., Auerbach Publication, FL, Chapter 5 - Operations Security, section 5.3,"Security Technology and Tools," Personnel section (page 32).
KRUTZ, R. & VINES, R. The CISSP Prep Guide: Gold Edition (2003), Wiley Publishing Inc., Chapter 6: Operations Security, Separations of Duties (page 303).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 347
Which of the following steps is NOT one of the eight detailed steps of a Business Impact Assessment (BIA):
A. Notifying senior management of the start of the assessment.
B. Creating data gathering techniques.
C. Identifying critical business functions.
D. Calculating the risk for each different business function.
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Source: HARRIS, S., CISSP All- In-One Exam Guide, 3rd. Edition, 2005, Chapter 9, Page 701.
There have been much discussion about the steps of the BIA and I struggled with this before deciding to scrape the question about "the four steps," and re-write the question using the AIO for a reference. This question should be easy.... if you know all eight steps.
The eight detailed and granular steps of the BIA are:
1. Select Individuals to interview for the data gathering.
2. Create data gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources that these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and the threats to these functions.
7. Calculate risk for each of the different business functions.
8. Document findings and report them to management.
Shon goes on to cover each step in Chapter 9.

NEW QUESTION: 348

Which of the following is the act of performing tests and evaluations to test a system's security level to see if it complies with the design specifications and security requirements?

A. Validation

B. Verification

C. Assessment

D. Accuracy

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Verification vs. Validation:

Verification determines if the product accurately represents and meets the specifications. A product can be developed that does not match the original specifications. This step ensures that the specifications are properly met.

Validation determines if the product provides the necessary solution intended real-world problem. In large projects, it is easy to lose sight of overall goal. This exercise ensures that the main goal of the project is met.

From DITSCAP:

6.3.2. Phase 2, Verification. The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (i)), there is a corresponding set of security activities, enclosure 3, that shall verify compliance with the security requirements and evaluate vulnerabilities.

6.3.3. Phase 3, Validation. The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.

You must also be familiar with Verification and Validation for the purpose of the exam. A simple definition for Verification would be whether or not the developers followed the design specifications along with the security requirements. A simple definition for Validation would be whether or not the final product meets the end user needs and can be use for a specific purpose.

Wikipedia has an informal description that is currently written as: Validation can be expressed by the query "Are you building the right thing?" and Verification by "Are you building it right?

NOTE:

DITSCAP was replaced by DIACAP some time ago (2007). While DITSCAP had defined both a verification and a validation phase, the DIACAP only has a validation phase. It may not make a difference in the answer for the exam; however, DIACAP is the cornerstone policy of DOD C&A and IA efforts today.

Be familiar with both terms just in case all of a sudden the exam becomes updated with the new term.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1106). McGraw-Hill. Kindle Edition.

http://iase.disa.mil/ditscap/DITSCAP.html

https://en.wikipedia.org/wiki/Verification_and_validation

For the definition of "validation" in DIACAP, Click Here

Further sources for the phases in DIACAP, Click Here

NEW QUESTION: 349
Sensitivity labels are an example of what application control type?
A. Preventive security controls
B. Detective security controls
C. Compensating administrative controls
D. Preventive accuracy controls
Answer: A (LEAVE A REPLY)
Sensitivity labels are a preventive security application controls, such as are firewalls, reference monitors, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments.
The incorrect answers are:
Detective security controls - Intrusion detection systems (IDS), monitoring activities, and audit trails.
Compensating administrative controls - There no such application control.
Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 264). KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Application Controls, Figure 7.1 (page 360).

NEW QUESTION: 350
In the process of gathering evidence from a computer attack, a system administrator took a series of actions which are listed below. Can you identify which one of these actions has compromised the whole evidence collection process?
A. Using a write blocker
B. Made a full-disk image
C. Created a message digest for log files
D. Displayed the contents of a folder
Answer: D (LEAVE A REPLY)
Displaying the directory contents of a folder can alter the last access time on each listed file.
Using a write blocker is wrong because using a write blocker ensure that you cannot modify the data on the host and it prevent the host from writing to its hard drives.
Made a full-disk image is wrong because making a full-disk image can preserve all data on a hard disk, including deleted files and file fragments.
Created a message digest for log files is wrong because creating a message digest for log files. A message digest is a cryptographic checksum that can demonstrate that the integrity of a file has not been compromised (e.g. changes to the content of a log file)
Domain: LEGAL, REGULATIONS, COMPLIANCE AND INVESTIGATIONS

References: AIO 3rd Edition, page 783-784 NIST 800-61 Computer Security Incident Handling guide page 3-18 to 3-20

NEW QUESTION: 351
At what stage of the applications development process should the security department become involved?
A. Prior to the implementation
B. Prior to systems testing
C. During unit testing
D. During requirements development
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 352
Which of the following embodies all the detailed actions that personnel are required to follow?
A. Standards
B. Guidelines
C. Procedures
D. Baselines
Answer: (SHOW ANSWER)
Procedures are step-by-step instructions in support of of the policies, standards, guidelines and baselines. The procedure indicates how the policy will be implemented and who does what to accomplish the tasks."
Standards is incorrect. Standards are a "Mandatory statement of minimum requirements that support some part of a policy, the standards in this case is your own company standards and not standards such as the ISO standards"
Guidelines is incorrect. "Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions."
Baselines is incorrect. Baselines "are a minimum acceptable level of security. This minimum is implemented using specific rules necessary to implement the security controls in support of the policy and standards." For example, requiring a password of at leat 8 character would be an example. Requiring all users to have a minimun of an antivirus, a personal firewall, and an anti spyware tool could be another example.
References:
CBK, pp. 12 - 16. Note especially the discussion of the "hammer policy" on pp. 16-17 for the differences between policy, standard, guideline and procedure.
AIO3, pp. 88-93.

NEW QUESTION: 353
What is the difference between Access Control Lists (ACLs) and Capability Tables?

A. Access control lists are related/attached to a subject whereas capability tables are related/attached to an object.
B. Access control lists are related/attached to an object whereas capability tables are related/attached to a subject.
C. Capability tables are used for objects whereas access control lists are used for users.
D. They are basically the same.
Answer: (SHOW ANSWER)
Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's posession of a capability (or ticket) for the object. It is a row within the matrix.
To put it another way, A capabiltiy table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.
CLEMENT NOTE:
If we wish to express this very simply:
Capabilities are attached to a subject and it describe what access the subject has to each of the objects on the row that matches with the subject within the matrix. It is a row within the matrix. ACL's are attached to objects, it describe who has access to the object and what type of access they have. It is a column within the matrix.
The following are incorrect answers:
"Access control lists are subject-based whereas capability tables are object-based" is incorrect.
"Capability tables are used for objects whereas access control lists are used for users" is incorrect.
"They are basically the same" is incorrect. References used for this question:
CBK, pp. 191 - 192 AIO3 p. 169

NEW QUESTION: 354
Which of the following models does NOT include data integrity or conflict of interest?
A. Biba
B. Clark-Wilson
C. Bell-LaPadula
D. Brewer-Nash
Answer: (SHOW ANSWER)
Explanation/Reference:
Bell LaPadula model (Bell 1975): The granularity of objects and subjects is not predefined, but the model prescribes simple access rights. Based on simple access restrictions the Bell LaPadula model enforces a discretionary access control policy enhanced with mandatory rules. Applications with rigid confidentiality requirements and without strong integrity requirements may properly be modeled.
These simple rights combined with the mandatory rules of the policy considerably restrict the spectrum of applications which can be appropriately modeled.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
Also check:

Proceedings of the IFIP TC11 12th International Conference on Information Security, Samos (Greece), May 1996, On Security Models.

NEW QUESTION: 355
Which of the following networking devices allows the connection of two or more homogeneous LANs in a simple way where they forward the traffic based on the MAC address ?
A. Gateways
B. Routers
C. Bridges
D. Firewalls
Answer: C (LEAVE A REPLY)
Bridges are simple, protocol-dependent networking devices that are used to connect two or more homogeneous LANs to form an extended LAN.
A bridge does not change the contents of the frame being transmitted but acts as a relay.
A gateway is designed to reduce the problems of interfacing any combination of local networks that employ different level protocols or local and long-haul networks.
A router connects two networks or network segments and may use IP to route messages.
Firewalls are methods of protecting a network against security threats from other systems or networks by centralizing and controlling access to the protected network segment.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7: Telecommunications and Network Security (page 397).

NEW QUESTION: 356
In addition to the accuracy of the biometric systems, there are other factors that must also be considered:
A. These factors include the enrollment time and the throughput rate, but not acceptability.
B. These factors do not include the enrollment time, the throughput rate, and acceptability.
C. These factors include the enrollment time, the throughput rate, and acceptability.
D. These factors include the enrollment time, but not the throughput rate, neither the acceptability.
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
In addition to the accuracy of the biometric systems, there are other factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability.
Enrollment time is the time it takes to initially "register" with a system by providing samples of the biometric characteristic to be evaluated. An acceptable enrollment time is around two minutes.
For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases.
In finger-scan technology, a full fingerprint is not stored-the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template.

Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37 & 38.

NEW QUESTION: 357
What is NOT true with pre shared key authentication within IKE / IPsec protocol?
A. Pre shared key authentication is normally based on simple passwords
B. Needs a Public Key Infrastructure (PKI) to work
C. IKE is used to setup Security Associations
D. IKE builds upon the Oakley protocol and the ISAKMP protocol.
Answer: (SHOW ANSWER)
Explanation/Reference:
Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication which are either pre-shared or distributed using DNS (preferably with DNSSEC) and a Diffie-Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.
Internet Key Exchange (IKE) Internet key exchange allows communicating partners to prove their identity to each other and establish a secure communication channel, and is applied as an authentication component of IPSec.
IKE uses two phases:
Phase 1: In this phase, the partners authenticate with each other, using one of the following:
Shared Secret: A key that is exchanged by humans via telephone, fax, encrypted e-mail, etc.
Public Key Encryption: Digital certificates are exchanged.
Revised mode of Public Key Encryption: To reduce the overhead of public key encryption, a nonce (a Cryptographic function that refers to a number or bit string used only once, in security engineering) is encrypted with the communicating partner's public key, and the peer's identity is encrypted with symmetric encryption using the nonce as the key. Next, IKE establishes a temporary security association and secure tunnel to protect the rest of the key exchange. Phase 2: The peers' security associations are established, using the secure tunnel and temporary SA created at the end of phase 1.
The following reference(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7032-7048). Auerbach Publications. Kindle Edition.
and
RFC 2409 at http://tools.ietf.org/html/rfc2409
and
http://en.wikipedia.org/wiki/Internet_Key_Exchange

NEW QUESTION: 358
Which of the following is NOT an advantage that TACACS+ has over TACACS?

A. Event logging
B. Use of two-factor password authentication
C. User has the ability to change his password
D. Ability for security tokens to be resynchronized
Answer: A (LEAVE A REPLY)
Although TACACS+ provides better audit trails, event logging is a service that is provided with TACACS.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 121).

NEW QUESTION: 359
Which of the following is related to physical security and is not considered a technical control?
A. Access control Mechanisms
B. Intrusion Detection Systems
C. Firewalls
D. Locks
Answer: (SHOW ANSWER)
All of the above are considered technical controls except for locks, which are physical controls.
Administrative, Technical, and Physical Security Controls
Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. For example, policy might dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information. Requiring that information be classified and the process to classify and review information classifications is another example of an administrative control. The organization security awareness program is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.
Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the C.I.A. of sensitive information. Examples include logical access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems.
Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control. From the GIAC.ORG website

NEW QUESTION: 360

Which of the following exemplifies proper separation of duties?
A. Operators are not permitted modify the system time.
B. Programmers are permitted to use the system console.
C. Console operators are permitted to mount tapes and disks.
D. Tape operators are permitted to use the system console.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
This is an example of Separation of Duties because operators are prevented from modifying the system time which could lead to fraud. Tasks of this nature should be performed by they system administrators. AIO defines Separation of Duties as a security principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.
The following answers are incorrect:
Programmers are permitted to use the system console. Is incorrect because programmers should not be permitted to use the system console, this task should be performed by operators. Allowing programmers access to the system console could allow fraud to occur so this is not an example of Separation of Duties..
Console operators are permitted to mount tapes and disks. Is incorrect because operators should be able to mount tapes and disks so this is not an example of Separation of Duties.
Tape operators are permitted to use the system console. Is incorrect because operators should be able to use the system console so this is not an example of Separation of Duties.
References:
OIG CBK Access Control (page 98 - 101)
AIOv3 Access Control (page 182)

NEW QUESTION: 361
What system allows a user to provide one ID and password per work session and then is automatically logged-on to all the required applications?
A. Tickets
B. SSO
C. Challenge Response
D. Token-based authentication
E. Biometrics
Answer: B (LEAVE A REPLY)
Single Sign-On (SSO) overcomes the problems of having to log on multiple times to access different network resources.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine

here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 362
Domain Name Service is a distributed database system that is used to map:
A. Domain Name to IP addresses.
B. MAC addresses to domain names.
C. MAC Address to IP addresses.
D. IP addresses to MAC Addresses.
Answer: A (LEAVE A REPLY)
The Domain Name Service is a distributed database system that is used to map domain names to IP addresses and IP addresses to domain names.
The Domain Name System is maintained by a distributed database system, which uses the client-server model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root nameservers, the servers to query when looking up (resolving) a TLD.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100. and
https://en.wikipedia.org/wiki/Domain_Name_System

NEW QUESTION: 363
Secure Shell (SSH) is a strong method of performing:
A. client authentication
B. server authentication
C. host authentication
D. guest authentication
Answer: A (LEAVE A REPLY)
Secure shell (SSH) was designed as an alternative to some of the insecure protocols and allows users to securely access resources on remote computers over an encrypted tunnel. The Secure Shell Protocol (SSH) is a protocol for secure remote login and other secure network services over an insecure network. The SSH authentication protocol runs on top of the SSH transport layer protocol and provides a single authenticated tunnel for the SSH connection protocol.
SSH's services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel. Many users protect less secure traffic of protocols, such as X Windows and VNC (virtual network computing), by forwarding them through a SSH tunnel.
The SSH tunnel protects the integrity of communication, preventing session hijacking and other man-in-the-middle attacks. Another advantage of SSH over its predecessors is that it supports strong

authentication. There are several alternatives for SSH clients to authenticate to a SSH server, including passwords and digital certificates.
Keep in mind that authenticating with a password is still a significant improvement over the other protocols because the password is transmitted encrypted.
There are two incompatible versions of the protocol, SSH-1 and SSH-2, though many servers support both. SSH-2 has improved integrity checks (SSH-1 is vulnerable to an insertion attack due to weak CRC-32 integrity checking) and supports local extensions and additional types of digital certificates such as Open PGP. SSH was originally designed for UNIX, but there are now implementations for other operating systems, including Windows, Macintosh, and OpenVMS.
Is SSH 3.0 the same as SSH3? The short answer is: NO SSH 3.0 refers to version 3 of SSH Communications SSH2 protocol implementation and it could also refer to OpenSSH Version 3.0 of its SSH2 software. The "3" refers to the software release version not the protocol version. As of this writing (July 2013), there is no SSH3 protocol.
"Server authentication" is incorrect. Though many SSH clients allow pre-caching of server/host keys, this is a minimal form of server/host authentication.
"Host authentication" is incorrect. Though many SSH clients allow pre-caching of server/host keys, this is a minimal form of server/host authentication.
"Guest authentication" is incorrect. The general idea of "guest" is that it is unauthenticated access.
Reference(s) used for this question:
http://www.ietf.org/rfc/rfc4252.txt Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7080-7088). Auerbach Publications. Kindle Edition.

NEW QUESTION: 364
What is the main problem of the renewal of a root CA certificate?
A. It requires key recovery of all end user keys
B. It requires the authentic distribution of the new root CA certificate to all PKI participants
C. It requires the collection of the old root CA certificates from all the users
D. It requires issuance of the new root CA certificate
Answer: B (LEAVE A REPLY)
The main task here is the authentic distribution of the new root CA certificate as new trust anchor to all the PKI participants (e.g. the users).
In some of the rollover-scenarios there is no automatic way, often explicit assignment of trust from each user is needed, which could be very costly.
Other methods make use of the old root CA certificate for automatic trust establishment (see PKIX-reference), but these solutions works only well for scenarios with currently valid root CA certificates (and not for emergency cases e.g. compromise of the current root CA certificate).
The rollover of the root CA certificate is a specific and delicate problem and therefore are often ignored during PKI deployment.

Reference: Camphausen, I.; Petersen, H.; Stark, C.: Konzepte zum Root CA Zertifikatswechsel, conference Enterprise Security 2002, March 26-27, 2002, Paderborn; RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

NEW QUESTION: 365
Which of the following best defines a Computer Security Incident Response Team (CSIRT)?
A. An organization that provides a secure channel for receiving reports about suspected security incidents.
B. An organization that ensures that security incidents are reported to the authorities.
C. An organization that coordinates and supports the response to security incidents.
D. An organization that disseminates incident-related information to its constituency and other involved parties.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines a Computer Security Incident Response Team (CSIRT) as an organization that coordinates and supports the response to security incidents that involves sites within a defined constituency. This is the proper definition for the CSIRT. To be considered a CSIRT, an organization must provide a secure channel for receiving reports about suspected security incidents, provide assistance to members of its constituency in handling the incidents and disseminate incident-related information to its constituency and other involved parties. Security-related incidents do not necessarily have to be reported to the authorities.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 366
If your property Insurance has Actual Cash Valuation (ACV) clause, your damaged property will be compensated based on:
A. Value of item on the date of loss
B. Replacement with a new item for the old one regardless of condition of lost item
C. Value of item one month before the loss
D. Value of item on the date of loss plus 10 percent
Answer: A (LEAVE A REPLY)
This is called the Actual Cash Value (ACV) or Actual Cost Valuation (ACV)
All of the other answers were only detractors. Below you have an explanation of the different types of valuation you could use. It is VERY important for you to validate with your insurer which one applies to you as you could have some very surprising finding the day you have a disaster that takes place.
Replacement Cost Property replacement cost insurance promises to replace old with new. Generally, replacement of a building must be done on the same premises and used for the same purpose, using materials comparable to the quality of the materials in the damaged or destroyed property.
There are some other limitations to this promise. For example, the cost of repairs or replacement for buildings doesn't include the increased cost associated with building codes or other laws controlling how buildings must be built today. An endorsement adding coverage for the operation of Building Codes and

the increased costs associated with complying with them is available separately - usually for additional premium. In addition, some insurance underwriters will only cover certain property on a depreciated value (actual cash value - ACV) basis even when attached to the building. This includes awnings and floor coverings, appliances for refrigerating, ventilating, cooking, dishwashing, and laundering. Depreciated value also applies to outdoor equipment or furniture.

Actual Cash Value (ACV) The ACV is the default valuation clause for commercial property insurance. It is also known as depreciated value, but this is not the same as accounting depreciated value. The actual cash value is determined by first calculating the replacement value of the property. The next step involves estimating the amount to be subtracted, which reflects the building's age, wear, and tear. This amount deducted from the replacement value is known as depreciation. The amount of depreciation is reduced by inflation (increased cost of replacing the property); regular maintenance; and repair (new roofs, new electrical systems, etc.) because these factors reduce the effective age of the buildings.

The amount of depreciation applicable is somewhat subjective and certainly subject to negotiation. In fact, there is often disagreement and a degree of uncertainty over the amount of depreciation applicable to a particular building.

Given this reality, property owners should not leave the determination of depreciation to chance or wait until suffering a property loss to be concerned about it. Every three to five years, property owners should obtain a professional appraisal of the replacement value and depreciated value of the buildings.

The ACV valuation is an option for directors to consider when certain buildings are in need of repair, or budget constraints prevent insuring all of your facilities on a replacement cost basis. There are other valuation options for property owners to consider as well.

Functional Replacement Cost This valuation method has been available for some time but has not been widely used. It is beginning to show up on property insurance policies imposed by underwriters with concerns about older, buildings. It can also be used for buildings, which are functionally obsolete. This method provides for the replacement of a building with similar property that performs the same function, using less costly material. The endorsement includes coverage for building codes automatically. In the event of a loss, the insurance company pays the smallest of four payment options.

1.In the event of a total loss, the insurer could pay the limit of insurance on the building or the cost to replace the building on the same (or different) site with a payment that is "functionally equivalent."

2.In the event of a partial loss, the insurance company could pay the cost to repair or replace the damaged portion in the same architectural style with less costly material (if available).

3.The insurance company could also pay the amount actually spent to demolish the undamaged portion of the building and clear the site if necessary.

4.The fourth payment option is to pay the amount actually spent to repair, or replace the building using less costly materials, if available (Hillman and McCracken 1997).

Unlike the replacement cost valuation method, which excluded certain fixtures and personal property used to service the premises, this endorsement provides functional replacement cost coverage for these items (awnings, floor coverings, appliances, etc.) (Hillman nd McCracken 1997).

As in the standard replacement cost value option, the insured can elect not to repair or replace the property. Under these circumstances the company pays the smallest of the following:

1.The Limit of Liability

2.The "market value" (not including the value of the land) at the time of the loss. The endorsement defines "market value" as the price which the property might be expected to realize if ffered for sale in fair market."
3.A modified form of ACV (the amount to repair or replace on he same site with less costly material and in the same architectural tyle, less depreciation) (Hillman and McCracken 1997).
Agreed Value or Agreed Amount Agreed value or agreed amount is not a valuation method. Instead, his term refers to a waiver of the coinsurance clause in the property insurance policy. Availability of this coverage feature varies among insurers but, it is usually available only when the underwriter has proof (an independent appraisal, or compliance with an insurance company valuation model) of the value of your property. When do I get paid?
Generally, the insurance company will not pay a replacement cost settlement until the property that was damaged or destroyed is actually repaired or replaced as soon as reasonably possible after the loss. Under no circumstances will the insurance company pay more than your limit of insurance or more than the actual amount you spend to repair or replace the damaged property if this amount is less than the limit of insurance.
Replacement cost insurance terms give the insured the option of settling the loss on an ACV basis. This option may be exercised if you don't plan to replace the building or if you are faced with a significant coinsurance penalty on a replacement cost settlement.
References:
http://www.schirickinsurance.com/resources/value2005.pdf and TIPTON, Harold F. & KRAUSE, MICKI Information Security Management Handbook, 4th Edition, Volume 1 Property Insurance overview, Page 587.

NEW QUESTION: 367
What is called the probability that a threat to an information system will materialize?
A. Threat
B. Risk
C. Vulnerability
D. Hole
Answer: (SHOW ANSWER)
Explanation/Reference:
Risk: The potential for harm or loss to an information system or network; the probability that a threat will materialize.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

NEW QUESTION: 368
The absence of a safeguard, or a weakness in a system that may possibly be exploited is called a(n)?
A. Threat
B. Exposure
C. Vulnerability

D. Risk

Answer: C (LEAVE A REPLY)

Explanation/Reference:

A vulnerability is a weakness in a system that can be exploited by a threat.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 237.

NEW QUESTION: 369

What is the effective key size of DES?

A. 56 bits

B. 64 bits

C. 128 bits

D. 1024 bits

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Data Encryption Standard (DES) is a symmetric key algorithm. Originally developed by IBM, under project name Lucifer, this 128-bit algorithm was accepted by the NIST in 1974, but the total key size was reduced to 64 bits, 56 of which make up the effective key, plus and extra 8 bits for parity. It somehow became a national cryptographic standard in 1977, and an American National Standard Institute (ANSI) standard in

1978. DES was later replaced by the Advanced Encryption Standard (AES) by the NIST.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter

8: Cryptography (page 525).

NEW QUESTION: 370

In biometrics, the "one-to-one" search used to verify claim to an identity made by a person is considered:

A. Authentication

B. Identification

C. Auditing

D. Authorization

Answer: A (LEAVE A REPLY)

Biometric devices can be use for either IDENTIFICATION or AUTHENTICATION ONE TO ONE is for AUTHENTICATION This means that you as a user would provide some biometric credential such as your fingerprint. Then they will compare the template that you have provided with the one stored in the Database. If the two are exactly the same that prove that you are who you pretend to be.

ONE TO MANY is for IDENTIFICATION A good example of this would be within airport. Many airports today have facial recognition cameras, as you walk through the airport it will take a picture of your face and then compare the template (your face) with a database full of templates and see if there is a match between your template and the ones stored in the Database. This is for IDENTIFICATION of a person.

Some additional clarification or comments that might be helpful are: Biometrics establish authentication using specific information and comparing results to expected data. It does not perform well for identification purposes such as scanning for a person's face in a moving crowd for example.
Identification methods could include: username, user ID, account number, PIN, certificate, token, smart card, biometric device or badge.
Auditing is a process of logging or tracking what was done after the identity and authentication process is completed.
Authorization is the rights the subject is given and is performed after the identity is established.
Reference OIG (2007) p148, 167
Authentication in biometrics is a "one-to-one" search to verify claim to an identity made by a person.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION: 371
What can be defined as an instance of two different keys generating the same ciphertext from the same plaintext?
A. Key collision
B. Key clustering
C. Hashing
D. Ciphertext collision
Answer: B (LEAVE A REPLY)
Key clustering happens when a plaintext message generates identical ciphertext messages using the same transformation algorithm, but with different keys.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 130).

NEW QUESTION: 372
What would be the Annualized Rate of Occurrence (ARO) of the threat "user input error", in the case where a company employs 100 data entry clerks and every one of them makes one input error each month?
A. 100
B. 120
C. 1
D. 1200
Answer: D (LEAVE A REPLY)
If every one of the 100 clerks makes 1 error 12 times per year, it makes a total of 1200 errors. The Annnualized Rate of Occurence (ARO) is a value that represents the estimated frequency in which a threat is expected to occur. The range can be from 0.0 to a large number. Having an average of 1200 errors per year means an ARO of 1200

NEW QUESTION: 373
Which of the following statements pertaining to link encryption is false?
A. It encrypts all the data along a specific communication path.
B. It provides protection against packet sniffers and eavesdroppers.
C. Information stays encrypted from one end of its journey to the other.
D. User information, header, trailers, addresses and routing data that are part of the packets are encrypted.
Answer: (SHOW ANSWER)
When using link encryption, packets have to be decrypted at each hop and encrypted again.
Information staying encrypted from one end of its journey to the other is a characteristic of end-to-end encryption, not link encryption.
Link Encryption vs. End-to-End Encryption
Link encryption encrypts the entire packet, including headers and trailers, and has to be decrypted at each hop.
End-to-end encryption does not encrypt the IP Protocol headers, and therefore does not need to be decrypted at each hop.
Reference: All in one, Page 735 & Glossary
and
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

NEW QUESTION: 374
Which of the following outlined how senior management are responsible for the computer and information security decisions that they make and what actually took place within their organizations?
A. The Computer Security Act of 1987.
B. The Federal Sentencing Guidelines of 1991.
C. The Economic Espionage Act of 1996.
D. The Computer Fraud and Abuse Act of 1986.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
In 1991, U.S. Federal Sentencing Guidelines were developed to provide judges with courses of action in dealing with white collar crimes. These guidelines provided ways that companies and law enforcement should prevent, detect and report computer crimes. It also outlined how senior management are responsible for the computer and information security decisions that they make and what actually took place within their organizations.

NEW QUESTION: 375
Which of the following are not Remote Access concerns?
A. Justification for remote access
B. Auditing of activities
C. Regular review of access privileges

D. Access badges
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Access badges are more relevant to physical security rather than remote access.
"Justification for remote access" is incorrect. Justification for remote access is a relevant concern.
"Auditing of activities" is incorrect. Auditing of activites is an imporant aspect to assure that malicious or unauthorized activities are not occuring.
"Regular review of access privileges" is incorrect. Regular review of remote accept privileges is an important management responsibility.
References:
AIO3, pp. 547 - 548

NEW QUESTION: 376
Which of the following focuses on sustaining an organization's business functions during and after a disruption?
A. Business continuity plan
B. Business recovery plan
C. Continuity of operations plan
D. Disaster recovery plan
Answer: A (LEAVE A REPLY)
Explanation/Reference:
A business continuity plan (BCP) focuses on sustaining an organization's business functions during and after a disruption. Information systems are considered in the BCP only in terms of their support to the larger business processes. The business recovery plan (BRP) addresses the restoration of business processes after an emergency. The BRP is similar to the BCP, but it typically lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. The continuity of operations plan (COOP) focuses on restoring an organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. The disaster recovery plan (DRP) applies to major, usually catastrophic events that deny access to the normal facility for an extended period.
A DRP is narrower in scope than an IT contingency plan in that it does not address minor disruptions that do not require relocation.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 8).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated**

and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 377
Another type of access control is lattice-based access control. In this type of control a lattice model is applied. How is this type of access control concept applied?
A. The pair of elements is the subject and object, and the subject has an upper bound equal or higher than the upper bound of the object being accessed.
B. The pair of elements is the subject and object, and the subject has an upper bound lower then the upper bound of the object being accessed.
C. The pair of elements is the subject and object, and the subject has no special upper or lower bound needed within the lattice.
D. The pair of elements is the subject and object, and the subject has no access rights in relation to an object.
Answer: A (LEAVE A REPLY)
To apply this concept to access control, the pair of elements is the subject and object, and the subject has to have an upper bound equal or higher than the object being accessed.
WIKIPEDIA has a great explanation as well:
In computer security, lattice-based access control (LBAC) is a complex access control based on the interaction between any combination of objects (such as resources, computers, and applications) and subjects (such as individuals, groups or organizations). In this type of label-based mandatory access control model, a lattice is used to define the levels of security that an object may have and that a subject may have access to. The subject is only allowed to access an object if the security level of the subject is greater than or equal to that of the object.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34. and http://en.wikipedia.org/wiki/Lattice-based_access_control

NEW QUESTION: 378
Which of the following would be MOST important to guarantee that the computer evidence will be admissible in court?
A. It must prove a fact that is immaterial to the case.
B. Its reliability must be proven.
C. The process for producing it must be documented and repeatable.
D. The chain of custody of the evidence must show who collected, secured, controlled, handled, transported the evidence, and that it was not tampered with.
Answer: D (LEAVE A REPLY)
Explanation/Reference:

It has to be material, relevant and reliable, and the chain of custody must be maintained, it is unlikely that it will be admissible in court if it has been tampered with.
The following answers are incorrect:
It must prove a fact that is immaterial to the case. Is incorrect because evidence must be relevant. If it is immaterial then it is not relevant.
Its reliability must be proven. Is incorrect because it is not the best answer. While evidence must be relevant if the chain of custody cannot be verified, then the evidence could lose it's credibility because there is no proof that the evidence was not tampered with. So, the correct answer above is the BEST answer.
The process for producing it must be documented and repeatable. Is incorrect because just because the process is documented and repeatable does not mean that it will be the same. This amounts to Corroborative Evidence that may help to support a case.

NEW QUESTION: 379
Which of the following would best classify as a management control?
A. Review of security controls
B. Personnel security
C. Physical and environmental protection
D. Documentation
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Management controls focus on the management of the IT security system and the management of risk for a system.
They are techniques and concerns that are normally addressed by management.
Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system, thus considered management controls.
SECURITY CONTROLS: The management, operational, and technical controls (i.e.,safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
SECURITY CONTROL BASELINE: The set of minimum security controls defined for a low-impact, moderate-impact,or high-impact information system.
The following are incorrect answers:
Personnel security, physical and environmental protection and documentation are forms of operational controls.
Reference(s) used for this question:
http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf and
FIPS PUB 200 at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

NEW QUESTION: 380
Who is responsible for providing reports to the senior management on the effectiveness of the security controls?

A. Information systems security professionals
B. Data owners
C. Data custodians
D. Information systems auditors
Answer: D (LEAVE A REPLY)
Explanation/Reference:
IT auditors determine whether systems are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction and other requirements" and "provide top company management with an independent view of the controls that have been designed and their effectiveness."
"Information systems security professionals" is incorrect. Security professionals develop the security policies and supporting baselines, etc.
"Data owners" is incorrect. Data owners have overall responsibility for information assets and assign the appropriate classification for the asset as well as ensure that the asset is protected with the proper controls.
"Data custodians" is incorrect. Data custodians care for an information asset on behalf of the data owner.
References:
CBK, pp. 38 - 42.
AIO3. pp. 99 - 104

NEW QUESTION: 381
Which OSI/ISO layer is responsible for determining the best route for data to be transferred?
A. Session layer
B. Physical layer
C. Network layer
D. Transport layer
Answer: C (LEAVE A REPLY)
Explanation/Reference:
The main responsibility of the network layer is to insert information into the packet's header so that it can be properly routed. The protocols at the network layer must determine the best path for the packet to take.
The following answers are incorrect:
Session layer. The session layer is responsible for establishing a connection between two applications.
Physical layer. The physical layer if responsible for converting electronic impulses into bits and vice-versa.
Transport layer. The transport layer is responsible for data transmission and error detection.
The following reference(s) were/was used to create this question:
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, v3, chapter 7:
Telecommunications and Network Security (page 422-428).
ISC2 Official ISC2 Guide to the CBK (OIG) 2007, p. 409-412

NEW QUESTION: 382
A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:
A. Mandatory Access Control
B. Discretionary Access Control
C. Non-Discretionary Access Control
D. Rule-based Access control
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
A central authority determines what subjects can have access to certain objects based on the organizational security policy.
The key focal point of this question is the 'central authority' that determines access rights.
Cecilia one of the quiz user has sent me feedback informing me that NIST defines MAC as: "MAC Policy means that Access Control Policy Decisions are made by a CENTRAL AUTHORITY. Which seems to indicate there could be two good answers to this question.
However if you read the NISTR document mentioned in the references below, it is also mentioned that: MAC is the most mentioned NDAC policy. So MAC is a form of NDAC policy.
Within the same document it is also mentioned: "In general, all access control policies other than DAC are grouped in the category of non- discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action." Under NDAC you have two choices:
Rule Based Access control and Role Base Access Control
MAC is implemented using RULES which makes it fall under RBAC which is a form of NDAC. It is a subset of NDAC.
This question is representative of what you can expect on the real exam where you have more than once choice that seems to be right. However, you have to look closely if one of the choices would be higher level or if one of the choice falls under one of the other choice. In this case NDAC is a better choice because MAC is falling under NDAC through the use of Rule Based Access Control.
The following are incorrect answers:
MANDATORY ACCESS CONTROL
In Mandatory Access Control the labels of the object and the clearance of the subject determines access rights, not a central authority. Although a central authority (Better known as the Data Owner) assigns the label to the object, the system does the determination of access rights automatically by comparing the Object label with the Subject clearance. The subject clearance MUST dominate (be equal or higher) than the object being accessed.
The need for a MAC mechanism arises when the security policy of a system dictates that:
1. Protection decisions must not be decided by the object owner.

2. The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object owner).

Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the "simple security rule," or "no read up." Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the "*-property" (pronounced "star property") or "no write down." The *- property is required to maintain system security in an automated environment.

DISCRETIONARY ACCESS CONTROL

In Discretionary Access Control the rights are determined by many different entities, each of the persons who have created files and they are the owner of that file, not one central authority.

DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. For example, it is generally used to limit a user's access to a file; it is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file.

DAC policy tends to be very flexible and is widely used in the commercial and government sectors. However, DAC is known to be inherently weak for two reasons:

First, granting read access is transitive; for example, when Ann grants Bob read access to a file, nothing stops Bob from copying the contents of Ann's file to an object that Bob controls. Bob may now grant any other user access to the copy of Ann's file without Ann's knowledge.

Second, DAC policy is vulnerable to Trojan horse attacks. Because programs inherit the identity of the invoking user, Bob may, for example, write a program for Ann that, on the surface, performs some useful function, while at the same time destroys the contents of Ann's files. When investigating the problem, the audit files would indicate that Ann destroyed her own files. Thus, formally, the drawbacks of DAC are as follows:

Discretionary Access Control (DAC) Information can be copied from one object to another; therefore, there is no real assurance on the flow of information in a system.

No restrictions apply to the usage of information when the user has received it.

The privileges for accessing objects are decided by the owner of the object, rather than through a system-wide policy that reflects the organization's security requirements.

ACLs and owner/group/other access control mechanisms are by far the most common mechanism for implementing DAC policies. Other mechanisms, even though not designed with DAC in mind, may have the capabilities to implement a DAC policy.

RULE BASED ACCESS CONTROL

In Rule-based Access Control a central authority could in fact determine what subjects can have access when assigning the rules for access. However, the rules actually determine the access and so this is not the most correct answer.

RuBAC (as opposed to RBAC, role-based access control) allow users to access systems and information based on pre determined and configured rules. It is important to note that there is no commonly understood definition or formally defined standard for rule-based access control as there is for DAC, MAC, and RBAC.

"Rule-based access" is a generic term applied to systems that allow some form of organization-defined rules, and therefore rule-based access control encompasses a broad range of systems. RuBAC may in fact be combined with other models, particularly RBAC or DAC. A RuBAC system intercepts every access request and compares the rules with the rights of the user to make an access decision. Most of the rule-based access control relies on a security label system, which dynamically composes a set of rules defined by a security policy. Security labels are attached to all objects, including files, directories, and devices. Sometime roles to subjects (based on their attributes) are assigned as well. RuBAC meets the business needs as well as the technical needs of controlling service access. It allows business rules to be applied to access control-for example, customers who have overdue balances may be denied service access. As a mechanism for MAC, rules of RuBAC cannot be changed by users. The rules can be established by any attributes of a system related to the users such as domain, host, protocol, network, or IP addresses. For example, suppose that a user wants to access an object in another network on the other side of a router. The router employs RuBAC with the rule composed by the network addresses, domain, and protocol to decide whether or not the user can be granted access. If employees change their roles within the organization, their existing authentication credentials remain in effect and do not need to be re configured. Using rules in conjunction with roles adds greater flexibility because rules can be applied to people as well as to devices. Rule-based access control can be combined with role-based access control, such that the role of a user is one of the attributes in rule setting.
Some provisions of access control systems have rule- based policy engines in addition to a role-based policy engine and certain implemented dynamic policies [Des03]. For example, suppose that two of the primary types of software users are product engineers and quality engineers. Both groups usually have access to the same data, but they have different roles to perform in relation to the data and the application's function. In addition, individuals within each group have different job responsibilities that may be identified using several types of attributes such as developing programs and testing areas. Thus, the access decisions can be made in real time by a scripted policy that regulates the access between the groups of product engineers and quality engineers, and each individual within these groups. Rules can either replace or complement role-based access control. However, the creation of rules and security policies is also a complex process, so each organization will need to strike the appropriate balance.
References used for this question:
http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf
and
AIO v3 p162-167 and OIG (2007) p.186-191
also
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 383
Which of the following was not designed to be a proprietary encryption algorithm?
A. RC2
B. RC4
C. Blowfish

D. Skipjack

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Blowfish is a symmetric block cipher with variable-length key (32 to 448 bits) designed in 1993 by Bruce Schneier as an unpatented, license-free, royalty-free replacement for DES or IDEA. See attributes below:

Block cipher: 64-bit block

Variable key length: 32 bits to 448 bits

Designed by Bruce Schneier

Much faster than DES and IDEA

Unpatented and royalty-free

No license required

Free source code available

Rivest Cipher #2 (RC2) is a proprietary, variable-key-length block cipher invented by Ron Rivest for RSA Data Security, Inc.

Rivest Cipher #4 (RC4) is a proprietary, variable-key-length stream cipher invented by Ron Rivest for RSA Data Security, Inc.

The Skipjack algorithm is a Type II block cipher [NIST] with a block size of 64 bits and a key size of 80 bits that was developed by NSA and formerly classified at the U.S. Department of Defense "Secret" level. The NSA announced on June 23, 1998, that Skipjack had been declassified.

References:

RSA Laboratories

http://www.rsa.com/rsalabs/node.asp?id=2250

RFC 2828 - Internet Security Glossary

http://www.faqs.org/rfcs/rfc2828.html

NEW QUESTION: 384

Which of the following media is MOST resistant to EMI interference?

A. microwave

B. fiber optic

C. twisted pair

D. coaxial cable

Answer: B (LEAVE A REPLY)

Explanation/Reference:

A fiber optic cable is a physical medium that is capable of conducting modulated light trasmission. Fiber optic cable carries signals as light waves, thus creating higher trasmission speeds and greater distances due to less attenuation. This type of cabling is more difficult to tap than other cabling and is most resistant to interference, especially EMI.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
103).

NEW QUESTION: 385
What can be described as an imaginary line that separates the trusted components of the TCB from those elements that are NOT trusted?
A. The security kernel
B. The reference monitor
C. The security perimeter
D. The reference perimeter
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The security perimeter is the imaginary line that separates the trusted components of the kernel and the Trusted Computing Base (TCB) from those elements that are not trusted. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. The security kernel can be software, firmware or hardware components in a trusted system and is the actual instantiation of the reference monitor. The reference perimeter is not defined and is a distracter.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 386
Which of the following is NOT part of the Kerberos authentication protocol?
A. Symmetric key cryptography
B. Authentication service (AS)
C. Principals
D. Public Key
Answer: D (LEAVE A REPLY)
There is no such component within kerberos environment. Kerberos uses
only symmetric encryption and does not make use of any public key component.
The other answers are incorrect because :
Symmetric key cryptography is a part of Kerberos as the KDC holds all the users' and
services' secret keys.
Authentication service (AS) : KDC (Key Distribution Center) provides an authentication
service
Principals : Key Distribution Center provides services to principals , which can be users ,
applications or network services.
References: Shon Harris , AIO v3 , Chapter - 4: Access Control , Pages : 152-155.

NEW QUESTION: 387
Which SSL version offers client-side authentication?
A. SSL v1
B. SSL v2

C. SSL v3
D. SSL v4
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Secure Sockets Layer (SSL) is the technology used in most Web-based applications. SSL version 2.0 supports strong authentication of the web server, but the authentication of the client side only comes with version 3.0. SSL v4 is not a defined standard.
Source: TIPTON, Harold F & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 54).

NEW QUESTION: 388
Which of the following is NOT a fundamental component of an alarm in an intrusion detection system?
A. Communications
B. Enunciator
C. Sensor
D. Response
Answer: D (LEAVE A REPLY)
Response is the correct choice. A response would essentially be the action that is taken once an alarm has been produced by an IDS, but is not a fundamental component of the alarm.
The following are incorrect answers:
Communications is the component of an alarm that delivers alerts through a variety of channels such as email, pagers, instant messages and so on.
An Enunciator is the component of an alarm that uses business logic to compose the content and format of an alert and determine the recipients of that alert.
A sensor is a fundamental component of IDS alarms. A sensor detects an event and produces an appropriate notification.
Domain: Access Control
Reference:
Official guide to the CISSP CBK. page 203.

NEW QUESTION: 389
Which of the following would BEST be defined as an absence or weakness of safeguard that could be exploited?
A. A threat
B. A vulnerability
C. A risk
D. An exposure
Answer: B (LEAVE A REPLY)
It is a software , hardware or procedural weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment. A vulnerability characterizes the absence or weakness of a safeguard that could be

exploited. This vulnerability may be a service running on a server, unpatched applications or operating system software etc.
The following answers are incorrect because: Threat: A threat is defined as a potential danger to information or systems. The threat is someone or something will identify a specific vulnerability and use it against the company or individual. The entity that takes advantage of a vulnerability is referred to as a 'Threat Agent'. A threat agent could be an intruder accessing the network through a port on the firewall , a process accessing data that violates the security policy. Risk:A risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. If a firewall has several ports open , there is a higher likelihood that an intruder will use one to access the network in an unauthorized method.
Exposure: An exposure is an instance of being exposed to losses from a threat agent.
REFERENCES: SHON HARRIS , ALL IN ONE THIRD EDITION : Chapter 3 : Security Management Practices , Pages: 57-59

NEW QUESTION: 390
Which of the following is given the responsibility of the maintenance and protection of the data?
A. Data owner
B. Data custodian
C. User
D. Security administrator
Answer: B (LEAVE A REPLY)
It is usually responsible for maintaining and protecting the data.
The following answers are incorrect:
Data owner is usually a member of management , in charge of a specific business unit and is ultimately responsible for the protection and use of the information.
User is any individual who routinely uses the data for work-related tasks.
Security administrator's tasks include creating new system user accounts , implementing new security software.
References : Shon Harris AIO v3 , Chapter - 3: Security Management Practices , Pages : 99 - 103

NEW QUESTION: 391
Which of the following protects a password from eavesdroppers and supports the encryption of communication?
A. Challenge Handshake Authentication Protocol (CHAP)
B. Challenge Handshake Identification Protocol (CHIP)
C. Challenge Handshake Encryption Protocol (CHEP)
D. Challenge Handshake Substitution Protocol (CHSP)
Answer: A (LEAVE A REPLY)

CHAP: A protocol that uses a three way hanbdshake The server sends the client a challenge which includes a random value(a nonce) to thwart replay attacks. The client responds with the MD5 hash of the nonce and the password.
The authentication is successful if the client's response is the one that the server expected.
Reference: Page 450, OIG 2007.
CHAP protects the password from eavesdroppers and supports the encryption of communication.
Reference: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 44.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 392
A business continuity plan is an example of which of the following?
A. Corrective control
B. Detective control
C. Preventive control
D. Compensating control
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Business Continuity Plans are designed to minimize the damage done by the event, and facilitate rapid restoration of the organization to its full operational capacity. They are for use "after the fact", thus are examples of corrective controls.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 273).
and
Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Location 8069). Elsevier Science (reference). Kindle Edition.
and

NEW QUESTION: 393
CORRECT TEXT
_____ is responsible for creating security policies and for communicating those policies to system users.

Answer:

NEW QUESTION: 394
When an outgoing request is made on a port number greater than 1023, this type of firewall creates an ACL to allow the incoming reply on that port to pass:
A. packet filtering
B. CIrcuit level proxy
C. Dynamic packet filtering
D. Application level proxy
Answer: C (LEAVE A REPLY)
Explanation/Reference:
The dynamic packet filtering firewall is able to create ACL's on the fly to allow replies on dynamic ports (higher than 1023).
Packet filtering is incorrect. The packet filtering firewall usually requires that the dynamic ports be left open as a group in order to handle this situiation.
Circuit level proxy is incorrect. The circuit level proxy builds a conduit between the trusted and untrusted hosts and does not work by dynamically creating ACL's.
Application level proxy is incorrect. The application level proxy "proxies" for the trusted host in its communications with the untrusted host. It does not dynamically create ACL's to control traffic.

NEW QUESTION: 395
Which of the following is NOT a compensating measure for access violations?
A. Backups
B. Business continuity planning
C. Insurance
D. Security awareness
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Security awareness is a preventive measure, not a compensating measure for access violations.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 50).

NEW QUESTION: 396
Which of the following choices describe a Challenge-response tokens generation?
A. A workstation or system that generates a random challenge string that the user enters into the token when prompted along with the proper PIN.
B. A workstation or system that generates a random login id that the user enters when prompted along with the proper PIN.
C. A special hardware device that is used to generate ramdom text in a cryptography system.

D. The authentication mechanism in the workstation or system does not determine if the owner should be authenticated.

Answer: A (LEAVE A REPLY)

Section: Access Control

Explanation/Reference:

Challenge-response tokens are:

- A workstation or system generates a random challenge string and the owner enters the string into the token along with the proper PIN.
- The token generates a response that is then entered into the workstation or system.
- The authentication mechanism in the workstation or system then determines if the owner should be authenticated.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4:

Access Control (pages 136-137).

NEW QUESTION: 397

Which of the following is NOT a valid reason to use external penetration service firms rather than corporate resources?

A. They are more cost-effective

B. They offer a lack of corporate bias

C. They use highly talented ex-hackers

D. They ensure a more complete reporting

Answer: C (LEAVE A REPLY)

Section: Analysis and Monitoring

Explanation/Reference:

Two points are important to consider when it comes to ethical hacking: integrity and independence.

By not using an ethical hacking firm that hires or subcontracts to ex-hackers of others who have criminal records, an entire subset of risks can be avoided by an organization. Also, it is not cost-effective for a single firm to fund the effort of the ongoing research and development, systems development, and maintenance that is needed to operate state-of-the-art proprietary and open source testing tools and techniques.

External penetration firms are more effective than internal penetration testers because they are not influenced by any previous system security decisions, knowledge of the current system environment, or future system security plans. Moreover, an employee performing penetration testing might be reluctant to fully report security gaps.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Appendix F: The Case for Ethical Hacking (page 517).

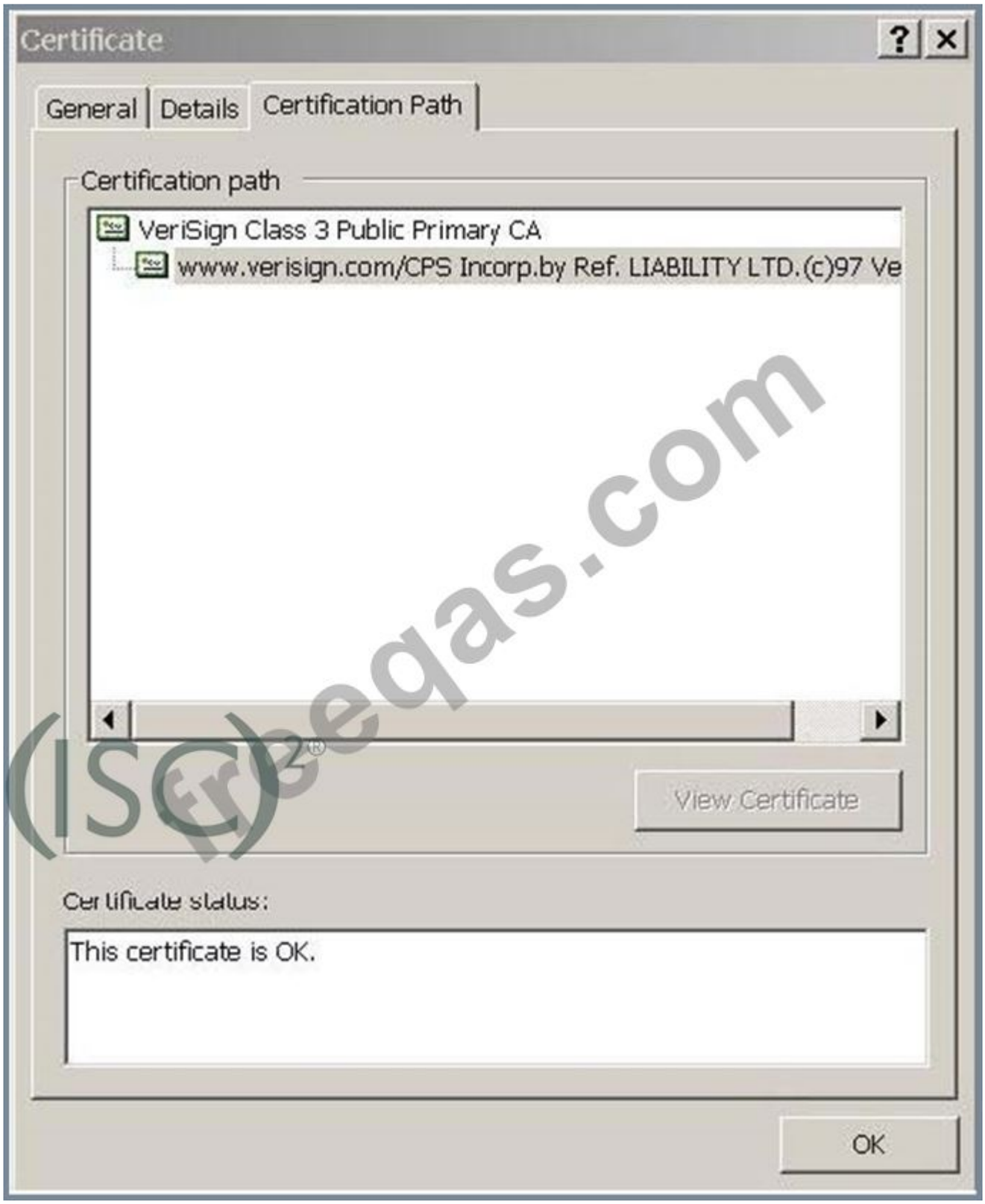
NEW QUESTION: 398

Smart cards are an example of which type of control?
A. Detective control
B. Administrative control
C. Technical control
D. Physical control
Answer: (SHOW ANSWER)
Explanation/Reference:
Logical or technical controls involve the restriction of access to systems and the protection of information. Smart cards and encryption are examples of these types of control.
Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
Many types of technical controls enable a user to access a system and the resources within that system. A technical control may be a username and password combination, a Kerberos implementation, biometrics, public key infrastructure (PKI), RADIUS, TACACS +, or authentication using a smart card through a reader connected to a system. These technologies verify the user is who he says he is by using different types of authentication methods. Once a user is properly authenticated, he can be authorized and allowed access to network resources.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 245). McGraw-Hill. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 32).

NEW QUESTION: 399
What layer of the OSI/ISO model does Point-to-point tunnelling protocol (PPTP) work at?
A. Data link layer
B. Transport layer
C. Session layer
D. Network layer
Answer: A (LEAVE A REPLY)
Explanation/Reference:
PPTP operates at the data link layer (layer 2) of the OSI model and uses native PPP authentication and encryption services. Designed for individual client to server connections, it enables only a single point-to-point connection per session.

PPTP - Point-to-Point Tunneling Protocol - extends the Point to Point Protocol (PPP) standard for traditional dial-up networking. PPTP is best suited for the remote access applications of VPNs, but it also supports LAN internetworking.
PPTP operates at Layer 2 of the OSI model.
Using PPTP
PPTP packages data within PPP packets, then encapsulates the PPP packets within IP packets (datagrams) for transmission through an Internet-based VPN tunnel. PPTP supports data encryption and compression of these packets. PPTP also uses a form of General Routing Encapsulation (GRE) to get data to and from its final destination.
Reference(s) used for this question:
KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 95).
and
http://compnetworking.about.com/od/vpn/l/aa030103a.htm
and
http://technet.microsoft.com/en-us/library/cc768084.aspx

NEW QUESTION: 400
Which of the following would best describe certificate path validation?
A. Verification of the validity of all certificates of the certificate chain to the root certificate
B. Verification of the integrity of the associated root certificate
C. Verification of the integrity of the concerned private key
D. Verification of the revocation status of the concerned certificate
Answer: A (LEAVE A REPLY)
With the advent of public key cryptography (PKI), it is now possible to communicate securely with untrusted parties over the Internet without prior arrangement. One of the necessities arising from such communication is the ability to accurately verify someone's identity (i.e. whether the person you are communicating with is indeed the person who he/she claims to be). In order to be able to perform identity check for a given entity, there should be a fool-proof method of "binding" the entity's public key to its unique domain name (DN).
A X.509 digital certificate issued by a well known certificate authority (CA), like Verisign, Entrust, Thawte, etc., provides a way of positively identifying the entity by placing trust on the CA to have performed the necessary verifications. A X.509 certificate is a cryptographically sealed data object that contains the entity's unique DN, public key, serial number, validity period, and possibly other extensions.
The Windows Operating System offers a Certificate Viewer utility which allows you to double-click on any certificate and review its attributes in a human-readable format. For instance, the "General" tab in the Certificate Viewer Window (see below) shows who the certificate was issued to as well as the certificate's issuer, validation period and usage functions.



Certification Path graphic

Certification Path graphic The "Certification Path" tab contains the hierarchy for the chain of certificates. It allows you to select the certificate issuer or a subordinate certificate and then click on "View Certificate" to open the certificate in the Certificate Viewer.

Each end-user certificate is signed by its issuer, a trusted CA, by taking a hash value (MD5 or SHA-1) of ASN.1 DER (Distinguished Encoding Rule) encoded object and then encrypting the resulting hash with

the issuer's private key (CA's Private Key) which is a digital signature. The encrypted data is stored in the "signatureValue" attribute of the entity's (CA) public certificate.
Once the certificate is signed by the issuer, a party who wishes to communicate with this entity can then take the entity's public certificate and find out who the issuer of the certificate is. Once the issuer's of the certificate (CA) is identified, it would be possible to decrypt the value of the "signatureValue" attribute in the entity's certificate using the issuer's public key to retrieve the hash value. This hash value will be compared with the independently calculated hash on the entity's certificate. If the two hash values match, then the information contained within the certificate must not have been altered and, therefore, one must trust that the CA has done enough background check to ensure that all details in the entity's certificate are accurate.
The process of cryptographically checking the signatures of all certificates in the certificate chain is called "key chaining". An additional check that is essential to key chaining is verifying that the value of the "subjectKeyIdentifier" extension in one certificate matches the same in the subsequent certificate.
Similarly, the process of comparing the subject field of the issuer certificate to the issuer field of the subordinate certificate is called "name chaining". In this process, these values must match for each pair of adjacent certificates in the certification path in order to guarantee that the path represents unbroken chain of entities relating directly to one another and that it has no missing links.
The two steps above are the steps to validate the Certification Path by ensuring the validity of all certificates of the certificate chain to the root certificate as described in the two paragraphs above.
Reference(s) used for this question:
FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 262.
and
https://www.tibcommunity.com/docs/DOC-2197

NEW QUESTION: 401
Which of the following is true about link encryption?
A. Each entity has a common key with the destination node.
B. Encrypted messages are only decrypted by the final node.
C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.
D. Only secure nodes are used in this type of transmission.
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:

In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain.
Thus, a node receives the encrypted message from its predecessor, decrypts it, and then re-encrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the transmission path is compromised.
Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption.
Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers.
In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 845-846). McGraw-Hill.
And:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 132).

NEW QUESTION: 402
What is the greatest danger from DHCP?
A. An intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients.
B. Having multiple clients on the same LAN having the same IP address.
C. Having the wrong router used as the default gateway.
D. Having the organization's mail server unreachable.
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The greatest danger from BootP or DHCP (Dynamic Host Control Protocol) is from an intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients. Other choices are possible consequences of DHCP impersonation.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4: Sockets and Services from a Security Viewpoint.

NEW QUESTION: 403
Which approach to a security program ensures people responsible for protecting the company's assets are DRIVING the program?

A. The Delphi approach
B. The top-down approach
C. The bottom-up approach
D. The technology approach
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
A security program should use a top-down approach, meaning that the initiation, support, and direction come from top management; work their way through middle management; and then reach staff members.
In contrast, a bottom-up approach refers to a situation in which staff members (usually IT) try to develop a security program without getting proper management support and direction. A bottom-up approach is commonly less effective, not broad enough to address all security risks, and doomed to fail.
A top-down approach makes sure the people actually responsible for protecting the company's assets (senior management) are driving the program.
The following are incorrect answers:
The Delphi approach is incorrect as this is for a brainstorming technique.
The bottom-up approach is also incorrect as this approach would be if the IT department tried to develop a security program without proper support from upper management.
The technology approach is also incorrect as it does not fit into the category of best answer.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 63). McGraw-Hill. Kindle Edition.

NEW QUESTION: 404
ICMP and IGMP belong to which layer of the OSI model?
A. Datagram Layer.
B. Network Layer.
C. Transport Layer.
D. Data Link Layer.
Answer: (SHOW ANSWER)
The network layer contains the Internet Protocol (IP), the Internet Control Message Protocol (ICMP), and the Internet Group Management Protocol (IGMP)
The following answers are incorrect:
Datagram Layer. Is incorrect as a distractor as there is no Datagram Layer.
Transport Layer. Is incorrect because it is used to data between applications and uses the
TCP and UDP protocols.
Data Link Layer. Is incorrect because this layer deals with addressing hardware.

NEW QUESTION: 405
How often should a Business Continuity Plan be reviewed?

A. At least once a month
B. At least every six months
C. At least once a year
D. At least Quarterly
Answer: C (LEAVE A REPLY)
As stated in SP 800-34 Rev. 1: To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies.
As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency (at least once a year for the purpose of the exam) or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews.
Remember, there could be two good answers as specified above. Either once a year or whenever significant changes occur to the plan. You will of course get only one of the two presented within you exam.
Reference(s) used for this question: NIST SP 800-34 Revision 1
Topic 4, Risk, Response and Recovery

NEW QUESTION: 406
Which of the following are not Remote Access concerns?
A. Justification for remote access
B. Auditing of activities
C. Regular review of access privileges
D. Access badges
Answer: (SHOW ANSWER)
Explanation/Reference:
Access badges are more relevant to physical security rather than remote access.
"Justification for remote access" is incorrect. Justification for remote access is a relevant concern.
"Auditing of activities" is incorrect. Auditing of activites is an imporant aspect to assure that malicious or unauthorized activities are not occuring.
"Regular review of access privileges" is incorrect. Regular review of remote accept privileges is an important management responsibility.
References:
AIO3, pp. 547 - 548

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine

here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 407
Which of the following are NOT a countermeasure to traffic analysis?
A. Padding messages.
B. Eavesdropping.
C. Sending noise.
D. Faraday Cage
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Eavesdropping is not a countermeasure, it is a type of attack where you are collecting traffic and attempting to see what is being send between entities communicating with each other.
The following answers are incorrect:
Padding Messages. Is incorrect because it is considered a countermeasure you make messages uniform size, padding can be used to counter this kind of attack, in which decoy traffic is sent out over the network to disguise patterns and make it more difficult to uncover patterns.
Sending Noise. Is incorrect because it is considered a countermeasure, tansmitting non-informational data elements to disguise real data.
Faraday Cage Is incorrect because it is a tool used to prevent emanation of electromagnetic waves. It is a very effective tool to prevent traffic analysis.

NEW QUESTION: 408
Which of the following is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length?
A. Fiber Optic cable
B. Coaxial cable
C. Twisted Pair cable
D. Axial cable
Answer: (SHOW ANSWER)
Fiber Optic cable is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length (up to two kilometers in some cases). Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

NEW QUESTION: 409
Which of the following access control techniques best gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure?
A. Access control lists
B. Discretionary access control

C. Role-based access control
D. Non-mandatory access control
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Role-based access control (RBAC) gives the security officers the ability to specify and enforce enterprise- specific security policies in a way that maps naturally to an organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are given to users in that role. An access control list (ACL) is a table that tells a system which access rights each user has to a particular system object.
With discretionary access control, administration is decentralized and owners of resources control other users' access. Non-mandatory access control is not a defined access control technique.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 9).

NEW QUESTION: 410
How would an IP spoofing attack be best classified?
A. Session hijacking attack
B. Passive attack
C. Fragmentation attack
D. Sniffing attack
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
IP spoofing is used to convince a system that it is communicating with a known entity that gives an intruder access. IP spoofing attacks is a common session hijacking attack.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
77).

NEW QUESTION: 411
Passfilt.dll enforces which of the following? (Choose all that apply)
A. 6 character minimum password length
B. Each password must have a combination of upper case, lower case, numbers and special characters
C. 90 day password change
D. 8 character minimum password length
Answer: (SHOW ANSWER)

NEW QUESTION: 412
Which OSI/ISO layers are TCP and UDP implemented at?

A. Application layer
B. Presentation layer
C. Session layer
D. Transport layer
Answer: D (LEAVE A REPLY)
Explanation/Reference:
TCP and UDP are implemented at the transport layer (layer 4).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
82).

NEW QUESTION: 413
Each data packet is assigned the IP address of the sender and the IP address of the:
A. recipient.
B. host.
C. node.
D. network.
Answer: A (LEAVE A REPLY)
Each data packet is assigned the IP address of the sender and the IP address of the recipient. The term network refers to the part of the IP address that identifies each network. The terms host and node refer to the parts of the IP address that identify a specific machine on a network.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

NEW QUESTION: 414
What does the (star) integrity axiom mean in the Biba model?
A. No read up
B. No write down
C. No read down
D. No write up
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
The (star) integrity axiom of the Biba access control model states that an object at one level of integrity is not permitted to modify an object of a higher level of integrity (no write up).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

NEW QUESTION: 415
An alternative to using passwords for authentication in logical or technical access control is:

A. manage without passwords
B. biometrics
C. not there
D. use of them for physical access control
Answer: B (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
An alternative to using passwords for authentication in logical or technical access control is biometrics. Biometrics are based on the Type 3 authentication mechanism-something you are.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION: 416
Preservation of confidentiality within information systems requires that the information is not disclosed to:
A. Authorized person
B. Unauthorized persons or processes.
C. Unauthorized persons.
D. Authorized persons and processes
Answer: (SHOW ANSWER)
Explanation/Reference:
Confidentiality assures that the information is not disclosed to unauthorized persons or processes.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

NEW QUESTION: 417
Which of the following is a not a preventative control?
A. Deny programmer access to production data.
B. Require change requests to include information about dates, descriptions, cost analysis and anticipated effects.
C. Run a source comparison program between control and current source periodically.
D. Establish procedures for emergency changes.
Answer: (SHOW ANSWER)
Running the source comparison program between control and current source periodically allows detection, not prevention, of unauthorized changes in the production environment. Other options are preventive controls.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

NEW QUESTION: 418
Related to information security, availability is the opposite of which of the following?

A. delegation
B. distribution
C. documentation
D. destruction
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Availability is the opposite of "destruction."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 419
What can be best defined as the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment?
A. Risk management
B. Risk analysis
C. Threat analysis
D. Due diligence
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Threat analysis is the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
The following answers are incorrect:
Risk analysis is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.
Risk analysis is synonymous with risk assessment and part of risk management, which is the ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level or risk.
Due Diligence is identifying possible risks that could affect a company based on best practices and standards.
Reference(s) used for this question:
STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication
800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June
2001 (page B-3).

NEW QUESTION: 420
Which of the following would be the best criterion to consider in determining the classification of an information asset?

A. Value
B. Age
C. Useful life
D. Personal association
Answer: A (LEAVE A REPLY)
Information classification should be based on the value of the information to the organization and its sensitivity (reflection of how much damage would accrue due to disclosure).
Age is incorrect. While age might be a consideration in some cases, the guiding principles should be value and sensitivity.
Useful life. While useful lifetime is relevant to how long data protections should be applied, the classification is based on information value and sensitivity.
Personal association is incorrect. Information classification decisions should be based on value of the information and its sensitiviry.
References
CBK, pp. 101 - 102.

NEW QUESTION: 421
In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?
A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-Ciphertext attack
D. Plaintext-only attack
Answer: B (LEAVE A REPLY)
Explanation/Reference:
In a ciphertext-only attack, the attacker has the ciphertext of several messages encrypted with the same encryption algorithm. Its goal is to discover the plaintext of the messages by figuring out the key used in the encryption process. In a known-plaintext attack, the attacker has the plaintext and the ciphertext of one or more messages. In a chosen-ciphertext attack, the attacker can chose the ciphertext to be decrypted and has access to the resulting plaintext.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter
8: Cryptography (page 578).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine

here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 422
Related to information security, the guarantee that the message sent is the message received with the assurance that the message was not intentionally or unintentionally altered is an example of which of the following?
A. integrity
B. confidentiality
C. availability
D. identity
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Integrity is the guarantee that the message sent is the message received, and that the message was not intentionally or unintentionally altered.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 60.

NEW QUESTION: 423
Which of the following statements pertaining to packet switching is incorrect?
A. Most data sent today uses digital signals over network employing packet switching.
B. Messages are divided into packets.
C. All packets from a message travel through the same route.
D. Each network node or point examines each packet for routing.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
When using packet switching, messages are broken down into packets. Source and destination address are added to each packet so that when passing through a network node, they can be examined and eventually rerouted through different paths as conditions change. All message packets may travel different paths and not arrive in the same order as sent. Packets need to be collected and reassembled into the original message at destination.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 424
Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?
A. 192.168.42.5
B. 192.166.42.5
C. 192.175.42.5
D. 192.1.42.5

Answer: A (LEAVE A REPLY)

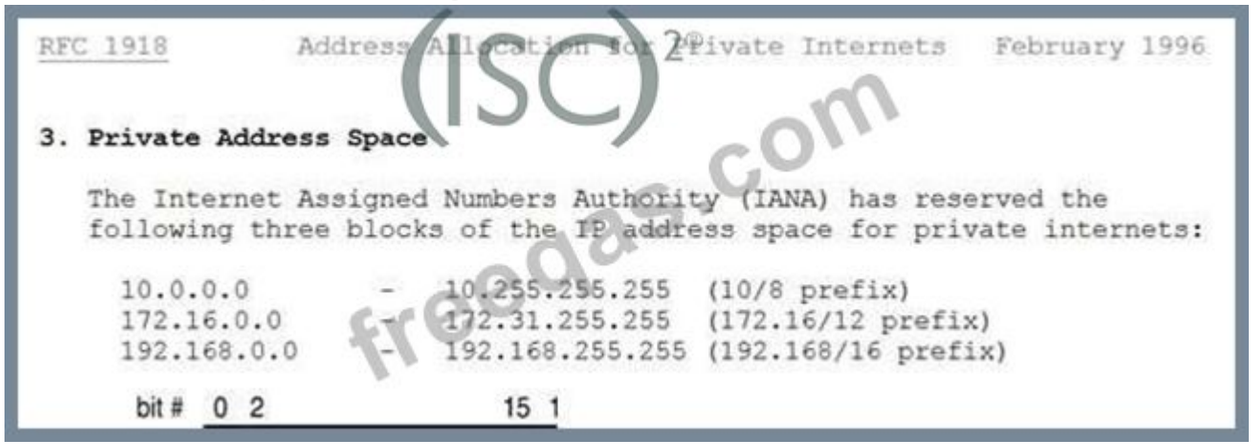
Section: Network and Telecommunications

Explanation/Reference:

This is a valid Class C reserved address. For Class C, the reserved addresses are 192.168.0.0 - 192.168.255.255.

The private IP address ranges are defined within RFC 1918:

RFC 1918 private ip address range



The following answers are incorrect:

192.166.42.5 Is incorrect because it is not a Class C reserved address.

192.175.42.5 Is incorrect because it is not a Class C reserved address.

192.1.42.5 Is incorrect because it is not a Class C reserved address.

NEW QUESTION: 425

Which of the following security models does NOT concern itself with the flow of data?

A. The information flow model

B. The Biba model

C. The Bell-LaPadula model

D. The noninterference model

Answer: (SHOW ANSWER)

Explanation/Reference:

The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.

The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned with confidentiality and bases access control decsions on the classfication of objects and the clearences of subjects.

The information flow model is incorrect. The information flow models have a similar framework to the Bell- LaPadula model and control how information may flow between objects based on security classes.

The Biba model is incorrect. The Biba model is concerned with integrity and is a complement to the Bell-LaPadula model in that higher levels of integrity are more trusted than lower levels. Access control us based on these integrity levels to assure that read/write operations do not decrease an object's integrity.

References:
CBK, pp 325 - 326
AIO3, pp. 290 - 291

NEW QUESTION: 426
Which of the following rules is least likely to support the concept of least privilege?
A. The number of administrative accounts should be kept to a minimum.
B. Administrators should use regular accounts when performing routine operations like reading mail.
C. Permissions on tools that are likely to be used by hackers should be as restrictive as possible.
D. Only data to and from critical systems and applications should be allowed through the firewall.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Only data to and from critical systems and applications should be allowed through the firewall is a detractor. Critical systems or applications do not necessarily need to have traffic go through a firewall. Even if they did, only the minimum required services should be allowed. Systems that are not deemed critical may also need to have traffic go through the firewall.
Least privilege is a basic tenet of computer security that means users should be given only those rights required to do their jobs or tasks. Least privilege is ensuring that you have the minimum privileges necessary to do a task. An admin NOT using his admin account to check email is a clear example of this.
Reference(s) used for this question:
National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 9.

NEW QUESTION: 427
Which of the following issues is not addressed by digital signatures?
A. nonrepudiation
B. authentication
C. data integrity
D. denial-of-service
Answer: D (LEAVE A REPLY)
A digital signature directly addresses both confidentiality and integrity of the CIA triad. It does not directly address availability, which is what denial-of-service attacks.
The other answers are not correct because:
"nonrepudiation" is not correct because a digital signature can provide for nonrepudiation.
"authentication" is not correct because a digital signature can be used as an authentication mechanism
"data integrity" is not correct because a digital signature does verify data integrity (as part of nonrepudiation)
References:
Official ISC2 Guide page: 227 & 265 All in One Third Edition page: 648

NEW QUESTION: 428

Brute force attacks against encryption keys have increased in potency because of increased computing power.
Which of the following is often considered a good protection against the brute force cryptography attack?
A. The use of good key generators.
B. The use of session keys.
C. Nothing can defend you against a brute force crypto key attack.
D. Algorithms that are immune to brute force key attacks.
Answer: B (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
If we assume a crytpo-system with a large key (and therefore a large key space) a brute force attack will likely take a good deal of time - anywhere from several hours to several years depending on a number of variables. If you use a session key for each message you encrypt, then the brute force attack provides the attacker with only the key for that one message. So, if you are encrypting 10 messages a day, each with a different session key, but it takes me a month to break each session key then I am fighting a loosing battle.
The other answers are not correct because:
"The use of good key generators" is not correct because a brute force key attack will eventually run through all possible combinations of key. Therefore, any key will eventually be broken in this manner given enough time.
"Nothing can defend you against a brute force crypto key attack" is incorrect, and not the best answer listed.
While it is technically true that any key will eventually be broken by a brute force attack, the question remains
"how long will it take?". In other words, if you encrypt something today but I can't read it for 10,000 years, will you still care? If the key is changed every session does it matter if it can be broken after the session has ended? Of the answers listed here, session keys are "often considered a good protection against the brute force cryptography attack" as the question asks.
"Algorithms that are immune to brute force key attacks" is incorrect because there currently are no such algorithms.
References:
Official ISC2 Guide page: 259
All in One Third Edition page: 623

NEW QUESTION: 429
Which of the following centralized access control mechanisms is the least appropriate for mobile workers accessing the corporate network over analog lines?
A. TACACS
B. Call-back
C. CHAP
D. RADIUS

Answer: B (LEAVE A REPLY)
Explanation/Reference:
Call-back allows for a distant user connecting into a system to be called back at a number already listed in a database of trusted users. The disadvantage of this system is that the user must be at a fixed location whose phone number is known to the authentication server. Being mobile workers, users are accessing the system from multiple locations, making call-back inappropriate for them.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 44).

NEW QUESTION: 430
What is called a sequence of characters that is usually longer than the allotted number for a password?
A. passphrase
B. cognitive phrase
C. anticipated phrase
D. Real phrase
Answer: A (LEAVE A REPLY)
Explanation/Reference:
A passphrase is a sequence of characters that is usually longer than the allotted number for a password.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, page 37.

NEW QUESTION: 431
Which of the following does not apply to system-generated passwords?
A. Passwords are harder to remember for users.
B. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
C. Passwords are more vulnerable to brute force and dictionary attacks.
D. Passwords are harder to guess for attackers.
Answer: (SHOW ANSWER)
Explanation/Reference:
Users tend to choose easier to remember passwords. System-generated passwords can provide stronger, harder to guess passwords. Since they are based on rules provided by the administrator, they can include combinations of uppercase/lowercase letters, numbers and special characters, making them less vulnerable to brute force and dictionary attacks. One danger is that they are also harder to remember for users, who will tend to write them down, making them more vulnerable to anyone having access to the user's desk. Another danger with system-generated passwords is that if the password-generating algorithm gets to be known, the entire system is in jeopardy.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 64).

NEW QUESTION: 432

Which one of the following statements about the advantages and disadvantages of network-based Intrusion detection systems is true

A. Network-based IDSs are not vulnerable to attacks.

B. Network-based IDSs are well suited for modern switch-based networks.

C. Most network-based IDSs can automatically indicate whether or not an attack was successful.

D. The deployment of network-based IDSs has little impact upon an existing network.

Answer: D (LEAVE A REPLY)

Section: Analysis and Monitoring

Explanation/Reference:

Network-based IDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a network. Thus, it is usually easy to retrofit a network to include network-based IDSs with minimal effort.

Network-based IDSs are not vulnerable to attacks is not true, even thou network-based IDSs can be made very secure against attack and even made invisible to many attackers they still have to read the packets and sometimes a well crafted packet might exploit or kill your capture engine.

Network-based IDSs are well suited for modern switch-based networks is not true as most switches do not provide universal monitoring ports and this limits the monitoring range of a network-based IDS sensor to a single host. Even when switches provide such monitoring ports, often the single port cannot mirror all traffic traversing the switch.

Most network-based IDSs can automatically indicate whether or not an attack was successful is not true as most network-based IDSs cannot tell whether or not an attack was successful; they can only discern that an attack was initiated. This means that after a network-based IDS detects an attack, administrators must manually investigate each attacked host to determine whether it was indeed penetrated.

Reference:

NIST special publication 800-31 Intrusion Detection System pages 15-16

Official guide to the CISSP CBK. Pages 196 to 197

NEW QUESTION: 433

Which of the following is less likely to be used today in creating a Virtual Private Network?

A. L2TP

B. PPTP

C. IPSec

D. L2F

Answer: D (LEAVE A REPLY)

Explanation/Reference:

L2F (Layer 2 Forwarding) provides no authentication or encryption. It is a Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

At one point L2F was merged with PPTP to produce L2TP to be used on networks and not only on dial up links.

IPSec is now considered the best VPN solution for IP environments.

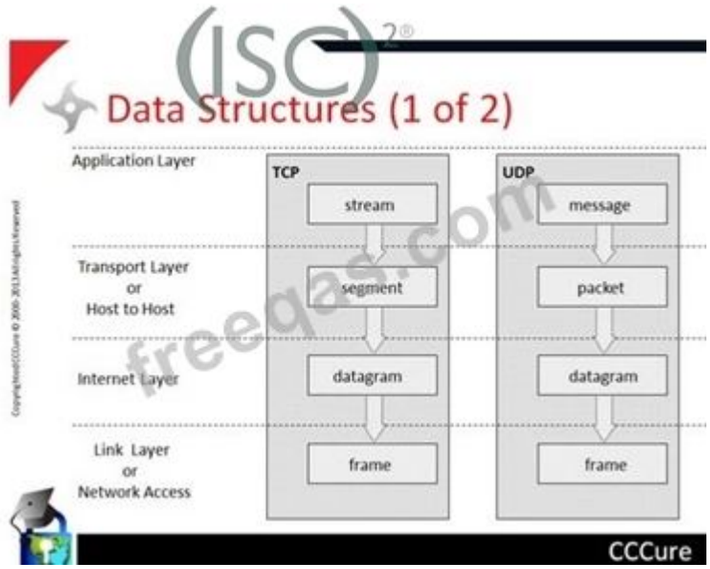
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter
8: Cryptography (page 507).

NEW QUESTION: 434
For maximum security design, what type of fence is most effective and cost-effective method (Foot are being used as measurement unit below)?
A. 3' to 4' high
B. 6' to 7' high
C. 8' high and above with strands of barbed wire
D. Double fencing
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The most commonly used fence is the chain linked fence and it is the most affordable. The standard is a six- foot high fence with two-inch mesh square openings. The material should consist of nine-gauge vinyl or galvanized metal. Nine-gauge is a typical fence material installed in residential areas.
Additionally, it is recommended to place barbed wire strands angled out from the top of the fence at a 45° angle and away from the protected area with three strands running across the top. This will provide for a seven-foot fence. There are several variations of the use of "top guards" using V-shaped barbed wire or the use of concertina wire as an enhancement, which has been a replacement for more traditional three strand barbed wire "top guards." The fence should be fastened to ridged metal posts set in concrete every six feet with additional bracing at the corners and gate openings. The bottom of the fence should be stabilized against intruders crawling under by attaching posts along the bottom to keep the fence from being pushed or pulled up from the bottom. If the soil is sandy, the bottom edge of the fence should be installed below ground level.
For maximum security design, the use of double fencing with rolls of concertina wire positioned between the two fences is the most effective deterrent and cost-efficient method. In this design, an intruder is required to use an extensive array of ladders and equipment to breach the fences.
Most fencing is largely a psychological deterrent and a boundary marker rather than a barrier, because in most cases such fences can be rather easily penetrated unless added security measures are taken to enhance the security of the fence. Sensors attached to the fence to provide electronic monitoring of cutting or scaling the fence can be used.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 24416-24431). Auerbach Publications. Kindle Edition.

NEW QUESTION: 435
Communications devices must operate:
A. at different speeds to communicate.
B. at the same speed to communicate.

C. at varying speeds to interact.
D. at high speed to interact.
Answer: B (LEAVE A REPLY)
Communications devices must operate at the same speed to communicate.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.

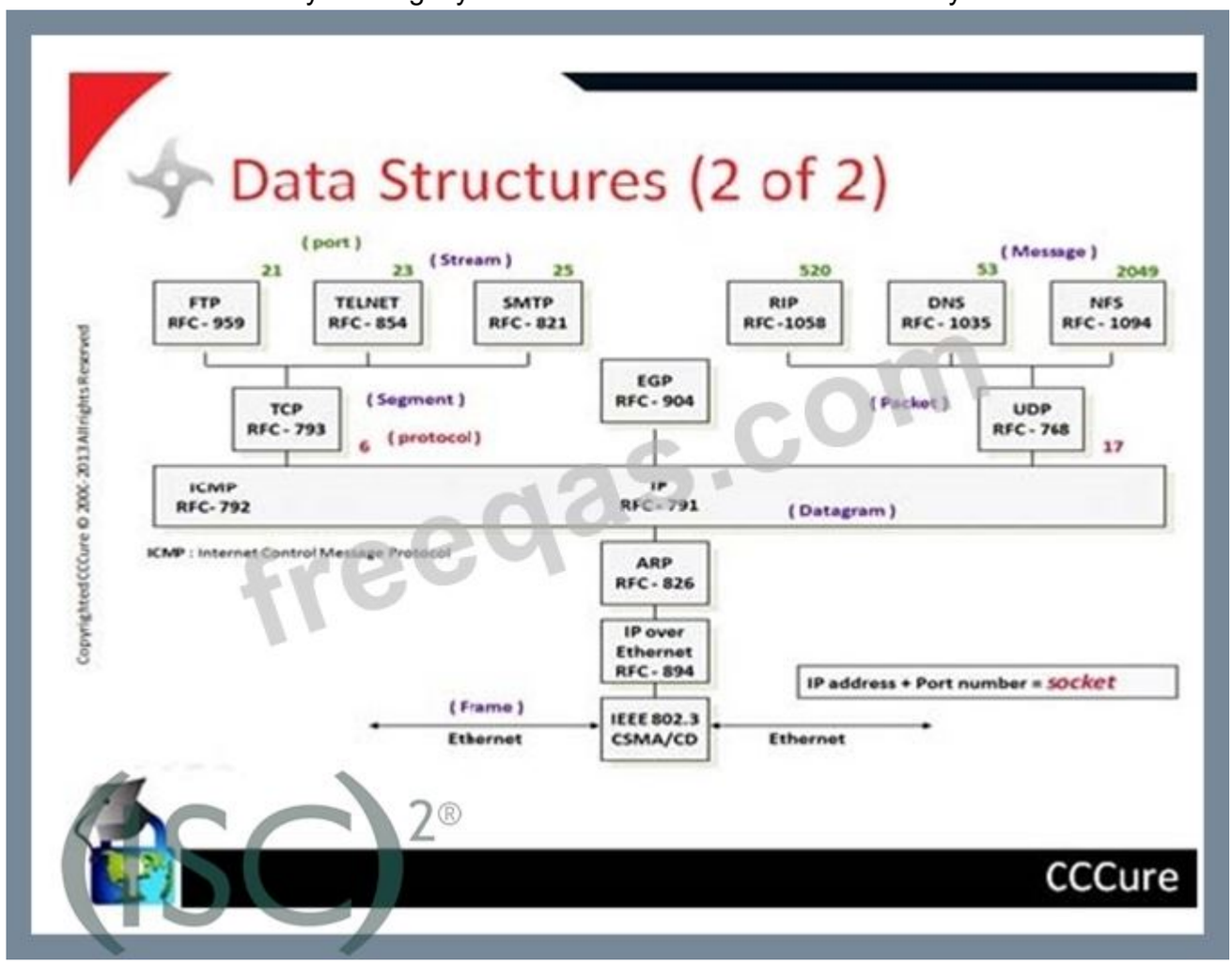
NEW QUESTION: 436
What is the proper term to refer to a single unit of Ethernet data at the link layer of the DoD TCP model ?
A. Ethernet Segment.
B. Ethernet Datagram.
C. Ethernet Frame.
D. Ethernet Packet.
Answer: (SHOW ANSWER)
Ethernet is frame based network technology. See below a few definitions from RFC 1122:
SEGMENT A segment is the unit of end-to-end transmission in the TCP protocol. A segment consists of a TCP header followed by application data. A segment is transmitted by encapsulation inside an IP datagram.
PACKET A packet is the unit of data passed across the interface between the internet layer and the link layer. It includes an IP header and data. A packet may be a complete IP datagram or a fragment of an IP datagram.
FRAME A frame is the unit of transmission in a link layer protocol, and consists of a link-layer header followed by a packet.
The following answers are incorrect:
Ethernet segment. Is incorrect because Ethernet segment is a distractor, TCP segment would be the correct terminology. Ethernet is a frame based network technology,
Ethernet datagram. Is incorrect because Ethernet datagram is a distractor, IP datagram would be the correct terminology. Ethernet is a frame based network technology
Ethernet packet. Is incorrect because Ethernet packet is a distractor, a Packet is a group of information so would not be a "single unit". Ethernet is a frame based network technology.
Look at the diagrams below that were extracted from my Security+ Computer Based Tutorial. TCP/IP Data Structures



IMPORTANT NOTE:

The names used on the diagram above are from RFC 1122 which describe the DOD Model.

Vendors and Books may use slightly different names or even number of layers.



TCP/IP Data Structure The following Reference(s) were used for this question:

Wikipedia http://en.wikipedia.org/wiki/Ethernet

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 437
Which of the following is best defined as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it?
A. Aggregation
B. Inference
C. Clustering
D. Collision
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
The Internet Security Glossary (RFC2828) defines aggregation as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 438
DES - Data Encryption standard has a 128 bit key and is very difficult to break.
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 439
A server cluster looks like a:
A. single server from the user's point of view
B. dual server from the user's point of view
C. triple server from the user's point of view
D. quardle server from the user's point of view
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The cluster looks like a single server from the user's point of view.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 67.

NEW QUESTION: 440
Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT) by ensuring the message comes from its claimed originator and that it has not been altered in transmission?
A. Secure Electronic Transaction (SET)
B. Message Authentication Code (MAC)
C. Cyclic Redundancy Check (CRC)
D. Secure Hash Standard (SHS)
Answer: B (LEAVE A REPLY)
Explanation/Reference:
In order to protect against fraud in electronic fund transfers (EFT), the Message Authentication Code (MAC), ANSI X9.9, was developed. The MAC is a check value, which is derived from the contents of the message itself, that is sensitive to the bit changes in a message. It is similar to a Cyclic Redundancy Check (CRC).
The aim of message authentication in computer and communication systems is to verify that he message comes from its claimed originator and that it has not been altered in transmission. It is particularly needed for EFT Electronic Funds Transfer). The protection mechanism is generation of a Message Authentication Code (MAC), attached to the message, which can be recalculated by the receiver and will reveal any alteration in transit. One standard method is described in (ANSI, X9.9). Message authentication mechanisms an also be used to achieve non-repudiation of messages.
The Secure Electronic Transaction (SET) was developed by a consortium including MasterCard and VISA as a means of preventing fraud from occurring during electronic payment.
The Secure Hash Standard (SHS), NIST FIPS 180, available at http://www.itl.nist.gov/fipspubs/fip180-1.htm, specifies the Secure Hash Algorithm (SHA-1).
Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 170)
also see:
http://luizfirmino.blogspot.com/2011/04/message-authentication-code-mac.html and
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.22.2312&rep=rep1&type=pdf

NEW QUESTION: 441
What layer of the ISO/OSI model do routers normally operate at?
A. Data link layer
B. Session layer
C. Transport layer
D. Network layer
Answer: D (LEAVE A REPLY)
Explanation/Reference:

Routers are switching devices that operate at the network layer (layer 3) by examining network addresses.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
111).

NEW QUESTION: 442
Which of the following is required in order to provide accountability?
A. Authentication
B. Integrity
C. Confidentiality
D. Audit trails
Answer: D (LEAVE A REPLY)
Accountability can actually be seen in two different ways:
1) Although audit trails are also needed for accountability, no user can be accountable for their actions unless properly authenticated.
2) Accountability is another facet of access control. Individuals on a system are responsible for their actions. This accountability property enables system activities to be traced to the proper individuals. Accountability is supported by audit trails that record events on the
system and network. Audit trails can be used for intrusion detection and for the
reconstruction of past events. Monitoring individual activities, such as keystroke monitoring, should be accomplished in accordance with the company policy and appropriate laws. Banners at the log-on time should notify the user of any monitoring that is being conducted. The point is that unless you employ an appropriate auditing mechanism, you don't have accountability. Authorization only gives a user certain permissions on the network. Accountability is far more complex because it also includes intrusion detection, unauthorized actions by both unauthorized users and authorized users, and system faults. The audit trail provides the proof that unauthorized modifications by both authorized and unauthorized users took place. No proof, No accountability.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 50.
The Shon Harris AIO book, 4th Edition, on Page 243 also states:
Auditing Capabilities ensures users are accountable for their actions, verify that the secutiy policies are enforced,
and can be used as investigation tools. Accountability is tracked by recording user, system, and application activities.
This recording is done through auditing functions and mechanisms within an operating sytem or application.
Audit trail contain information about operating System activities, application events, and user actions.

NEW QUESTION: 443
Which of the following statements pertaining to a Criticality Survey is incorrect?
A. It is implemented to gather input from all personnel that is going to be part of the recovery teams.
B. The purpose of the survey must be clearly stated.
C. Management's approval should be obtained before distributing the survey.
D. Its intent is to find out what services and systems are critical to keeping the organization in business.
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The Criticality Survey is implemented through a standard questionnaire to gather input from the most knowledgeable people. Not all personnel that is going to be part of recovery teams is necessarily able to help in identifying critical functions of the organization.
The intent of such a survey is to identify the services and systems that are critical to the organization.
Having a clearly stated purpose for the survey helps in avoiding misinterpretations.
Management's approval of the survey should be obtained before distributing it.
Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

NEW QUESTION: 444
Which of the following embodies all the detailed actions that personnel are required to follow?
A. Standards
B. Guidelines
C. Procedures
D. Baselines
Answer: (SHOW ANSWER)
Explanation/Reference:
Procedures are step-by-step instructions in support of of the policies, standards, guidelines and baselines.
The procedure indicates how the policy will be implemented and who does what to accomplish the tasks." Standards is incorrect. Standards are a "Mandatory statement of minimum requirements that support some part of a policy, the standards in this case is your own company standards and not standards such as the ISO standards"
Guidelines is incorrect. "Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions."
Baselines is incorrect. Baselines "are a minimum acceptable level of security. This minimum is implemented using specific rules necessary to implement the security controls in support of the policy and standards." For example, requiring a password of at leat 8 character would be an example.
Requiring all users to have a minimun of an antivirus, a personal firewall, and an anti spyware tool could be another example.
References:

CBK, pp. 12 - 16. Note especially the discussion of the "hammer policy" on pp. 16-17 for the differences between policy, standard, guideline and procedure.
AIO3, pp. 88-93.

NEW QUESTION: 445
Name three types of firewalls _____, _____, and _____ (Choose three)
A. Stateful Inspection
B. Microsoft Proxy
C. SonicWall
D. Application Proxy
E. Packet Filtering
F. Raptor Firewall
Answer: A,D,E (LEAVE A REPLY)

NEW QUESTION: 446
A timely review of system access audit records would be an example of which of the basic security functions?
A. avoidance
B. deterrence
C. prevention
D. detection
Answer: D (LEAVE A REPLY)
Explanation/Reference:
By reviewing system logs you can detect events that have occured.
The following answers are incorrect:
avoidance. This is incorrect, avoidance is a distractor. By reviewing system logs you have not avoided anything.
deterrence. This is incorrect because system logs are a history of past events. You cannot deter something that has already occurred.
prevention. This is incorrect because system logs are a history of past events. You cannot prevent something that has already occurred.

NEW QUESTION: 447
Which of the following is the BEST way to detect software license violations?
A. Implementing a corporate policy on copyright infringements and software use.
B. Requiring that all PCs be diskless workstations.
C. Installing metering software on the LAN so applications can be accessed through the metered software.
D. Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.
Answer: (SHOW ANSWER)

Explanation/Reference:
The best way to prevent and detect software license violations is to regularly scan used PCs, either from the LAN or directly, to ensure that unauthorized copies of software have not been loaded on the PC.
Other options are not detective.
A corporate policy is not necessarily enforced and followed by all employees.
Software can be installed from other means than floppies or CD-ROMs (from a LAN or even downloaded from the Internet) and software metering only concerns applications that are registered.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 108).

NEW QUESTION: 448
Which of the following statements pertaining to the maintenance of an IT contingency plan is incorrect?
A. The plan should be reviewed at least once a year for accuracy and completeness.
B. The Contingency Planning Coordinator should make sure that every employee gets an up-to-date copy of the plan.
C. Strict version control should be maintained.
D. Copies of the plan should be provided to recovery personnel for storage offline at home and office.
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
Because the contingency plan contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled. Not all employees would obtain a copy, but only those involved in the execution of the plan.
All other statements are correct.
NOTE FROM CLEMENT:
I have received multiple emails stating the explanations contradict the correct answer. It seems many people have a hard time with negative question. In this case the Incorrect choice (the one that is not true) is the correct choice. Be very carefull of such questions, you will get some on the real exam as well.
Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication
800-34, Contingency Planning Guide for Information Technology Systems

NEW QUESTION: 449
Which of the following is not a responsibility of an information (data) owner?
A. Determine what level of classification the information requires.
B. Periodically review the classification assignments against business needs.
C. Delegate the responsibility of data protection to data custodians.
D. Running regular backups and periodically testing the validity of the backup data.
Answer: D (LEAVE A REPLY)

Section: Security Operation Adimnistration
Explanation/Reference:
This responsibility would be delegated to a data custodian rather than being performed directly by the information owner.
"Determine what level of classification the information requires" is incorrect. This is one of the major responsibilities of an information owner.
"Periodically review the classification assignments against business needs" is incorrect. This is one of the major responsibilities of an information owner.
"Delegates responsibility of maintenance of the data protection mechanisms to the data custodian" is incorrect.
This is a responsibility of the information owner.
References:
CBK p. 105.
AIO3, p. 53-54, 960

NEW QUESTION: 450
Which of the following protocols operates at the session layer (layer 5)?
A. RPC
B. IGMP
C. LPD
D. SPX
Answer: (SHOW ANSWER)
Remotre Procedure Call (RPC) is the only of the above choices to operate at the session layer (layer 5).
All of the other answers were wrong.
LPD operates at layer 7 SPX operates at layer 4 IGMP operates at layer 3.
Reference:
WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

NEW QUESTION: 451
Password management falls into which control category?
A. Compensating
B. Detective
C. Preventive
D. Technical
Answer: C (LEAVE A REPLY)
Password management is an example of preventive control. Proper passwords prevent unauthorized users from accessing a system.
There are literally hundreds of different access approaches, control methods, and technologies, both in the physical world and in the virtual electronic world. Each method addresses a different type of access control or a specific access need.

For example, access control solutions may incorporate identification and authentication mechanisms, filters, rules, rights, logging and monitoring, policy, and a plethora of other controls. However, despite the diversity of access control methods, all access control systems can be categorized into seven primary categories.
The seven main categories of access control are:
1.Directive: Controls designed to specify acceptable rules of behavior within an organization
2.Deterrent: Controls designed to discourage people from violating security directives
3.Preventive: Controls implemented to prevent a security incident or information breach
4.Compensating: Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
5.Detective: Controls designed to signal a warning when a security control has been breached
6.Corrective: Controls implemented to remedy circumstance, mitigate damage, or restore controls
7.Recovery: Controls implemented to restore conditions to normal after a security incident
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1156-1176). Auerbach Publications. Kindle Edition.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 452
What is called a password that is the same for each log-on session?
A. "one-time password"
B. "two-time password"
C. static password
D. dynamic password
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 453
What is the following paragraph an example of? <<ATTN: This system is for the use of authorized persons only. If you use this system without authority, or if you abuse your authority, then you are subject to having all of your activities on this system monitored and recorded by system personnel. >>

A. Welcome Banner
B. Access Control Banner
C. Warning Banner
D. Audit Trail Banner
Answer: C (LEAVE A REPLY)

NEW QUESTION: 454
A Business Continuity Plan should be tested:
A. Once a month.
B. At least twice a year.
C. At least once a year.
D. At least once every two years.
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
It is recommended that testing does not exceed established frequency limits. For a plan to be effective, all components of the BCP should be tested at least once a year. Also, if there is a major change in the operations of the organization, the plan should be revised and tested not more than three months after the change becomes operational.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 165).

NEW QUESTION: 455
Which of the following is the FIRST step in protecting data's confidentiality?
A. Install a firewall
B. Implement encryption
C. Identify which information is sensitive
D. Review all user access rights
Answer: C (LEAVE A REPLY)
In order to protect the confidentiality of the data.
The following answers are incorrect because :
Install a firewall is incorrect as this would come after the information has been identified for sensitivity levels.
Implement encryption is also incorrect as this is one of the mechanisms to protect the data once it has been identified.
Review all user access rights is also incorrect as this is also a protection mechanism for the identified information.
Reference : Shon Harris AIO v3 , Chapter-4 : Access Control , Page : 126

NEW QUESTION: 456

Because ordinary cable introduces a toxic hazard in the event of fire, special cabling is required in a separate area provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. This area is referred to as the:

A. smoke boundry area

B. fire detection area

C. Plenum area

D. Intergen area

Answer: C (LEAVE A REPLY)

Explanation/Reference:

In building construction, a plenum (pronounced PLEH-nuhm, from Latin meaning full) is a separate space provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. A plenum may also be under a raised floor. In buildings with computer installations, the plenum space is often used to house connecting communication cables. Because ordinary cable introduces a toxic hazard in the event of fire, special plenum cabling is required in plenum areas.

Source: http://searchdatacenter.techtarget.com/sDefinition/0,,sid80_gci213716,00.html

NEW QUESTION: 457

Which of the following is considered the MOST secure?

A. Confidential

B. Public

C. Private

D. Sensitive

Answer: D (LEAVE A REPLY)

The order of classification from highest to lowest is: Sensitive, Confidential, Private, and Public. Review NIST Special Publication 800-26 for more details about information classifications.

NEW QUESTION: 458

From a security standpoint, the product development life cycle consists of which of the following?

A. Code Review

B. System Test Review

C. Functional Design Review

D. All of the items listed

E. Certification

F. Accreditation

Answer: D (LEAVE A REPLY)

NEW QUESTION: 459

Why should batch files and scripts be stored in a protected area?

A. Because of the least privilege concept.

B. Because they cannot be accessed by operators.
C. Because they may contain credentials.
D. Because of the need-to-know concept.
Answer: C (LEAVE A REPLY)
Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully. Operators might need access to batch files and scripts. The least privilege concept requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services. Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

NEW QUESTION: 460
Which of the following would assist the most in Host Based intrusion detection?
A. audit trails.
B. access control lists.
C. security clearances
D. host-based authentication
Answer: A (LEAVE A REPLY)
To assist in Intrusion Detection you would review audit logs for access violations.
The following answers are incorrect:
access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.
security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.
host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

NEW QUESTION: 461
What does the simple integrity axiom mean in the Biba model?
A. No write down
B. No read down
C. No read up
D. No write up
Answer: (SHOW ANSWER)
Explanation/Reference:
The simple integrity axiom of the Biba access control model states that a subject at one level of integrity is not permitted to observe an object of a lower integrity (no read down).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

NEW QUESTION: 462
Which of the following would be LESS likely to prevent an employee from reporting an incident?
A. They are afraid of being pulled into something they don't want to be involved with.
B. The process of reporting incidents is centralized.
C. They are afraid of being accused of something they didn't do.
D. They are unaware of the company's security policies and procedures.
Answer: (SHOW ANSWER)
Explanation/Reference:
The reporting process should be centralized else employees won't bother.
The other answers are incorrect because :
They are afraid of being pulled into something they don't want to be involved with is incorrect as most of the employees fear of this and this would prevent them to report an incident.
They are afraid of being accused of something they didn't do is also incorrect as this also prevents them to report an incident.
They are unaware of the company's security policies and procedures is also incorrect as mentioned above.
Reference : Shon Harris AIO v3 , Ch-10 : Laws , Investigatio & Ethics , Page : 675.

NEW QUESTION: 463
How would nonrepudiation be best classified as?
A. A preventive control
B. A logical control
C. A corrective control
D. A compensating control
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Systems accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Because the mechanisms implemented in nonrepudiation prevent the ability to successfully repudiate an action, it can be considered as a preventive control.
Source: STONEBURNER, Gary, NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security, National Institute of Standards and Technology, December 2001, page 7.

NEW QUESTION: 464
Which of the following best defines a Computer Security Incident Response Team (CSIRT)?
A. An organization that provides a secure channel for receiving reports about suspected security incidents.
B. An organization that ensures that security incidents are reported to the authorities.
C. An organization that coordinates and supports the response to security incidents.

D. An organization that disseminates incident-related information to its constituency and other involved parties.

Answer: C (LEAVE A REPLY)

RFC 2828 (Internet Security Glossary) defines a Computer Security Incident Response Team (CSIRT) as an organization that coordinates and supports the response to security incidents that involves sites within a defined constituency. This is the proper definition for the CSIRT. To be considered a CSIRT, an organization must provide a secure channel for receiving reports about suspected security incidents, provide assistance to
members of its constituency in handling the incidents and disseminate incident-related information to its constituency and other involved parties. Security-related incidents do not necessarily have to be reported to the authorities.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 465

Which of the following are NOT a countermeasure to traffic analysis?

A. Padding messages.

B. Eavesdropping.

C. Sending noise.

D. Faraday Cage

Answer: (SHOW ANSWER)

Explanation/Reference:

Eavesdropping is not a countermeasure, it is a type of attack where you are collecting traffic and attempting to see what is being send between entities communicating with each other.

The following answers are incorrect:

Padding Messages. Is incorrect because it is considered a countermeasure you make messages uniform size, padding can be used to counter this kind of attack, in which decoy traffic is sent out over the network to disguise patterns and make it more difficult to uncover patterns.

Sending Noise. Is incorrect because it is considered a countermeasure, tansmitting non-informational data elements to disguise real data.

Faraday Cage Is incorrect because it is a tool used to prevent emanation of electromagnetic waves. It is a very effective tool to prevent traffic analysis.

NEW QUESTION: 466

Which backup method does not reset the archive bit on files that are backed up?

A. Full backup method

B. Incremental backup method

C. Differential backup method

D. Additive backup method

Answer: (SHOW ANSWER)

The differential backup method only copies files that have changed since the last full backup was performed. It is additive in the fact that it does not reset the archive bit so all changed or added files are

backed up in every differential backup until the next full backup. The "additive backup method" is not a common backup method. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 467
Virus scanning and content inspection of SMIME encrypted e-mail without doing any further processing is:
A. Not possible
B. Only possible with key recovery scheme of all user keys
C. It is possible only if X509 Version 3 certificates are used
D. It is possible only by "brute force" decryption
Answer: A (LEAVE A REPLY)
Section: Malicious Code
Explanation/Reference:
Content security measures presumes that the content is available in cleartext on the central mail server. Encrypted emails have to be decrypted before it can be filtered (e.g. to detect viruses), so you need the decryption key on the central "crypto mail server".
There are several ways for such key management, e.g. by message or key recovery methods. However, that would certainly require further processing in order to achieve such goal.

NEW QUESTION: 468
How often should tests and disaster recovery drills be performed?
A. At least once a quarter
B. At least once every 6 months
C. At least once a year
D. At least once every 2 years
Answer: C (LEAVE A REPLY)
Tests and disaster recovery drills should be performed at least once a year. The company should have no confidence in an untested plan. Since systems and processes can change, frequent testing will aid in ensuring a plan will succeed. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 621).

NEW QUESTION: 469
Which of the following is NOT a type of motion detector?
A. Photoelectric sensor
B. Passive infrared sensors
C. Microwave Sensor.
D. Ultrasonic Sensor.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
A photoelectric sensor does not "directly" sense motion there is a narrow beam that won't set off the sensor unless the beam is broken. Photoelectric sensors, along with dry contact switches, are a type of perimeter intrusion detector.
All of the other answers are valid types of motion detectors types.
The content below on the different types of sensors is from Wikepedia:
Indoor Sensors
These types of sensors are designed for indoor use. Outdoor use would not be advised due to false alarm vulnerability and weather durability.Passive infrared detectors

Passive Infrared Sensor
The passive infrared detector (PIR) is one of the most common detectors found in household and small business environments because it offers affordable and reliable functionality. The term passive means the detector is able to function without the need to generate and radiate its own energy (unlike ultrasonic and microwave volumetric intrusion detectors that are "active" in operation). PIRs are able to distinguish if an infrared emitting object is present by first learning the ambient temperature of the monitored space and then detecting a change in the temperature caused by the presence of an object. Using the principle of differentiation, which is a check of presence or nonpresence, PIRs verify if an intruder or object is actually there. Creating individual zones of detection where each zone comprises one or more layers can achieve differentiation. Between the zones there are areas of no sensitivity (dead zones) that are used by the sensor for comparison.
Ultrasonic detectors
Using frequencies between 15 kHz and 75 kHz, these active detectors transmit ultrasonic sound waves that are inaudible to humans. The Doppler shift principle is the underlying method of operation, in which a change in frequency is detected due to object motion. This is caused when a moving object changes the

frequency of sound waves around it. Two conditions must occur to successfully detect a Doppler shift event:

There must be motion of an object either towards or away from the receiver.

The motion of the object must cause a change in the ultrasonic frequency to the receiver relative to the transmitting frequency.

The ultrasonic detector operates by the transmitter emitting an ultrasonic signal into the area to be protected. The sound waves are reflected by solid objects (such as the surrounding floor, walls and ceiling) and then detected by the receiver. Because ultrasonic waves are transmitted through air, then hard- surfaced objects tend to reflect most of the ultrasonic energy, while soft surfaces tend to absorb most energy.

When the surfaces are stationary, the frequency of the waves detected by the receiver will be equal to the transmitted frequency. However, a change in frequency will occur as a result of the Doppler principle, when a person or object is moving towards or away from the detector. Such an event initiates an alarm signal. This technology is considered obsolete by many alarm professionals, and is not actively installed.

Microwave detectors

This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing (monostatic) for indoor applications, and separate housings (bistatic) for outdoor applications. To reduce false alarms this type of detector is usually combined with a passive infrared detector or "Dualtec" alarm.

Microwave detectors respond to a Doppler shift in the frequency of the reflected energy, by a phase shift, or by a sudden reduction of the level of received energy. Any of these effects may indicate motion of an intruder.

Photo-electric beams

Photoelectric beam systems detect the presence of an intruder by transmitting visible or infrared light beams across an area, where these beams may be obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. However, if an intruder is aware of the technology's presence, it can be avoided. The technology can be an effective long-range detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier.

Systems are available for both internal and external applications. To prevent a clandestine attack using a secondary light source being used to hold the detector in a 'sealed' condition whilst an intruder passes through, most systems use and detect a modulated light source.

Glass break detectors

The glass break detector may be used for internal perimeter building protection. When glass breaks it generates sound in a wide band of frequencies. These can range from infrasonic, which is below 20 hertz (Hz) and can not be heard by the human ear, through the audio band from 20 Hz to 20 kHz which humans can hear, right up to ultrasonic, which is above 20 kHz and again cannot be heard. Glass break acoustic detectors are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking. Seismic glass break detectors are different in that they are installed on the glass pane.

When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic interlayer. Seismic glass break detectors "feel" these shock frequencies and in turn generate an alarm condition.
The more primitive detection method involves gluing a thin strip of conducting foil on the inside of the glass and putting low-power electrical current through it. Breaking the glass is practically guaranteed to tear the foil and break the circuit.
Smoke, heat, and carbon monoxide detectors

Heat Detection System
Most systems may also be equipped with smoke, heat, and/or carbon monoxide detectors. These are also known as 24 hour zones (which are on at all times). Smoke detectors and heat detectors protect from the risk of fire and carbon monoxide detectors protect from the risk of carbon monoxide. Although an intruder alarm panel may also have these detectors connected, it may not meet all the local fire code requirements of a fire alarm system.
Other types of volumetric sensors could be:
Active Infrared
Passive Infrared/Microware combined
Radar
Accoustical Sensor/Audio
Vibration Sensor (seismic)
Air Turbulence

NEW QUESTION: 470
Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer in a network. Within which OSI/ISO layer is RPC implemented?
A. Session layer
B. Transport layer
C. Data link layer
D. Network layer
Answer: (SHOW ANSWER)

Section: Network and Telecommunications
Explanation/Reference:
The Answer: Session layer, which establishes, maintains and manages sessions and synchronization of data flow. Session layer protocols control application-to-application communications, which is what an RPC call is.
The following answers are incorrect:
Transport layer: The Transport layer handles computer-to computer communications, rather than application- to-application communications like RPC.
Data link Layer: The Data Link layer protocols can be divided into either Logical Link Control (LLC) or Media Access Control (MAC) sublayers. Protocols like SLIP, PPP, RARP and L2TP are at this layer. An application- to-application protocol like RPC would not be addressed at this layer.
Network layer: The Network Layer is mostly concerned with routing and addressing of information, not application-to-application communication calls such as an RPC call.
The following reference(s) were/was used to create this question:
The Remote Procedure Call (RPC) protocol is implemented at the Session layer, which establishes, maintains and manages sessions as well as synchronization of the data flow.
Source: Jason Robinett's CISSP Cram Sheet: domain2.
Source: Shon Harris AIO v3 pg. 423

NEW QUESTION: 471
What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?
A. Central station alarm
B. Proprietary alarm
C. A remote station alarm
D. An auxiliary station alarm
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Auxiliary station alarms automatically cause an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters. They are usually Municipal Fire Alarm Boxes are installed at your business or building, they are wired directly into the fire station.
Central station alarms are operated by private security organizations. It is very similar to a proprietary alarm system (see below). However, the biggest difference is the monitoring and receiving of alarm is done off site at a central location manned by non staff members. It is a third party.
Proprietary alarms are similar to central stations alarms except that monitoring is performed directly on the protected property. This type of alarm is usually use to protect large industrials or commercial buildings.
Each of the buildings in the same vincinity has their own alarm system, they are all wired together at a central location within one of the building acting as a common receiving point. This point is usually far

away from the other building so it is not under the same danger. It is usually man 24 hours a day by a trained team who knows how to react under different conditions.
A remote station alarm is a direct connection between the signal-initiating device at the protected property and the signal-receiving device located at a remote station, such as the fire station or usually a monitoring service. This is the most popular type of implementation and the owner of the premise must pay a monthly monitoring fee. This is what most people use in their home where they get a company like ADT to receive the alarms on their behalf.
A remote system differs from an auxiliary system in that it does not use the municipal fire of police alarm circuits.
Reference(s) used for this question:
ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 11: Physical Security (page 211).
and
Great presentation J.T.A. Stone on SlideShare

NEW QUESTION: 472
A security evaluation report and an accreditation statement are produced in which of the following phases of the system development life cycle?
A. project initiation and planning phase
B. system design specification phase
C. development & documentation phase
D. acceptance phase
Answer: (SHOW ANSWER)
The answer: "acceptance phase". Note the question asks about an "evaluation report" - which details how the system evaluated, and an "accreditation statement" which describes the level the system is allowed to operate at. Because those two activities are a part of testing and testing is a part of the acceptance phase, the only answer above that can be correct is "acceptance phase".
The other answers are not correct because:
The "project initiation and planning phase" is just the idea phase. Nothing has been developed yet to be evaluated, tested, accredited, etc.
The "system design specification phase" is essentially where the initiation and planning phase is fleshed out. For example, in the initiation and planning phase, we might decide we want the system to have authentication. In the design specification phase, we decide that that authentication will be accomplished via username/password. But there is still nothing actually developed at this point to evaluate or accredit.
The "development & documentation phase" is where the system is created and documented. Part of the documentation includes specific evaluation and accreditation criteria. That is the criteria that will be used to evaluate and accredit the system during the "acceptance phase".
In other words - you cannot evaluate or accredit a system that has not been created yet. Of the four answers listed, only the acceptance phase is dealing with an existing system. The others deal with planning and creating the system, but the actual system isn't there yet.
Reference:
Official ISC2 Guide Page: 558 - 559

All in One Third Edition page: 832 - 833 (recommended reading)

NEW QUESTION: 473
Which of the following should be emphasized during the Business Impact Analysis (BIA) considering that the BIA focus is on business processes?
A. Composition
B. Priorities
C. Dependencies
D. Service levels
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The Business Impact Analysis (BIA) identifies time-critical aspects of the critical business processes, and determines their maximum tolerable downtime. The BIA helps to Identify organization functions, the capabilities of each organization unit to handle outages, and the priority and sequence of functions and applications to be recovered, identify resources required for recovery of those areas and interdependencies In performing the Business Impact Analysis (BIA) it is very important to consider what the dependencies are.
You cannot bring a system up if it depends on another system to be operational. You need to look at not only internal dependencies but external as well. You might not be able to get the raw materials for your business so dependencies are very important aspect of a BIA.
The BIA committee will not truly understand all business processes, the steps that must take place, or the resources and supplies these processes require. So the committee must gather this information from the people who do know- department managers and specific employees throughout the organization.
The committee starts by identifying the people who will be part of the BIA data-gathering sessions. The committee needs to identify how it will collect the data from the selected employees, be it through surveys, interviews, or workshops. Next, the team needs to collect the information by actually conducting surveys, interviews, and workshops. Data points obtained as part of the information gathering will be used later during analysis. It is important that the team members ask about how different tasks- whether processes, transactions, or services, along with any relevant dependencies- get accomplished within the organization.
The following answers are incorrect:
composition This is incorrect because it is not the best answer. While the make up of business may be important, if you have not determined the dependencies first you may not be able to bring the critical business processes to a ready state or have the materials on hand that are needed.
priorities This is incorrect because it is not the best answer. While the priorities of processes are important, if you have not determined the dependencies first you may not be able to bring the critical business processes to a ready state or have the materials on hand that are needed.
service levels This is incorrect because it is not the best answer. Service levels are not as important as dependencies.
Reference(s) used for this question:

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Business Continuity and Disaster Recovery Planning (Kindle Locations 188-191). . Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 18562-18568). McGraw-Hill. Kindle Edition.

NEW QUESTION: 474
What type of attack involves IP spoofing, ICMP ECHO and a bounce site?
A. IP spoofing attack
B. Teardrop attack
C. SYN attack
D. Smurf attack
Answer: D (LEAVE A REPLY)
A smurf attack occurs when an attacker sends a spoofed (IP spoofing) PING (ICMP ECHO) packet to the broadcast address of a large network (the bounce site). The modified packet containing the address of the target system, all devices on its local network respond with a ICMP REPLY to the target system, which is then saturated with those replies. An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A teardrop attack consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 76).

NEW QUESTION: 475
What is the Biba security model concerned with?
A. Confidentiality
B. Reliability
C. Availability
D. Integrity
Answer: D (LEAVE A REPLY)
Explanation/Reference:
The Biba security model addresses the integrity of data being threatened when subjects at lower security levels are able to write to objects at higher security levels and when subjects can read data at lower levels.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter
5: Security Models and Architecture (Page 244).

NEW QUESTION: 476
External consistency ensures that the data stored in the database is:
A. in-consistent with the real world.
B. remains consistant when sent from one system to another.
C. consistent with the logical world.
D. consistent with the real world.
Answer: D (LEAVE A REPLY)
External consistency ensures that the data stored in the database is
consistent with the real world.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, page 33.

NEW QUESTION: 477
Which of the following forms of authentication would most likely apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier?
A. Dynamic authentication
B. Continuous authentication
C. Encrypted authentication
D. Robust authentication
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Continuous authentication is a type of authentication that provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect. Robust authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, but does not provide protection against active attacks. Encrypted authentication is a distracter.
Source: GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 34).

NEW QUESTION: 478
You are running a packet sniffer on a network and see a packet containing a long string of "0x90 0x90 0x90
0x90...." in the middle of it traveling to an x86-based machine as a target. This could be indicative of what activity being attempted?
A. Over-subscription of the traffic on a backbone.
B. A source quench packet.

C. A FIN scan.
D. A buffer overflow attack.
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
A series of the same control characters, hexadecimal code, imbedded in the string is usually an indicator of a buffer overflow attack.
The Intel x86 processors use the hexadecimal number 90 to represent NOP (no operation). Many buffer overflow attacks use long strings of control characters and this is representative of that type of attack.
A buffer overflow takes place when too much data are accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed. So, the purpose of a buffer overflow may be either to make a mess, by shoving arbitrary data into various memory segments, or to accomplish a specific task, by pushing into the memory segment a carefully crafted set of data that will accomplish a specific task. This task could be to open a command shell with administrative privilege or execute malicious code.
Common threats to system availability, integrity, and confidentiality include hardware failure, misuse of system privileges, buffer overflows and other memory attacks, denial of service, reverse engineering, and system hacking.
Since many vulnerabilities result from insecure design and most threats are well known, it is the responsibility of the security architect to ensure that their designs are addressing security requirements appropriately while also ensuring that the system can continue to perform its intended function.
The following answers are incorrect:
Over-subscription of the traffic on a backbone. Is incorrect because if there was Over-subscription of the traffic on a backbone, that would typically result in not being able to send or receive any packets, more commonly known as Denial of Service or DoS.
A source quench packet. This is incorrect because a source quench packet is an ICMP message that contains the internet header plus 64 bits of the original datagram.
A FIN scan. This is incorrect because a FIN scan is when a packet with the FIN flag set is sent to a specific port and the results are then analyzed.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page
332, for people using the Kindle edition you will find it at Kindle Locations 7310-7315.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Architecture and Design (Kindle Locations 1403-1407). . Kindle Edition.
Wikipedia http://en.wikipedia.org/wiki/Port_scanner
ICMP http://security.maruhn.com/iptables-tutorial/x1078.html
Wikipedia http://en.wikipedia.org/wiki/Buffer_overflow

NEW QUESTION: 479

Corporate networks are safer if an end user connects through a VPN connection?
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 480
What does the simple security (ss) property mean in the Bell-LaPadula model?
A. No read up
B. No write down
C. No read down
D. No write up
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The ss (simple security) property of the Bell-LaPadula access control model states that reading of information by a subject at a lower sensitivity level from an object at a higher sensitivity level is not permitted (no read up).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 202).

NEW QUESTION: 481
Which of the following methods of providing telecommunications continuity involves the use of an alternative media?
A. Alternative routing
B. Diverse routing
C. Long haul network diversity
D. Last mile circuit protection
Answer: A (LEAVE A REPLY)
Alternative routing is a method of routing information via an alternate medium such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be unavailable. Diverse routing routes traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and therefore subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. This type of access is time-consuming and costly. Long haul network diversity is a diverse long-distance network utilizing T1 circuits among the major long-distance carriers. It ensures long-distance access should any one carrier experience a network failure. Last mile circuit protection is a redundant combination of local carrier T1s microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing is also utilized. Source: Information Systems Audit and Control Association, Certified

Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 259).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 482
Single Sign-on (SSO) is characterized by which of the following advantages?
A. Convenience
B. Convenience and centralized administration
C. Convenience and centralized data administration
D. Convenience and centralized network administration
Answer: B (LEAVE A REPLY)
Convenience -Using single sign-on users have to type their passwords only once when they first log in to access all the network resources; and Centralized Administration as some single sign-on systems are built around a unified server administration system. This allows a single administrator to add and delete accounts across the entire network from one user interface.
The following answers are incorrect:
Convenience - alone this is not the correct answer.
Centralized Data or Network Administration - these are thrown in to mislead the student. Neither are a benefit to SSO, as these specifically should not be allowed with just an SSO.
References: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, page 35. TIPTON, Harold F. & HENRY, Kevin, Official (ISC)2 Guide to the CISSP CBK, 2007, page
180.

NEW QUESTION: 483
Step-by-step instructions used to satisfy control requirements is called a:
A. policy
B. standard
C. guideline
D. procedure
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 484
In a hierarchical PKI the highest CA is regularly called Root CA, it is also referred to by which one of the following term?
A. Subordinate CA
B. Top Level CA
C. Big CA
D. Master CA
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Reference: Arsenault, Turner, Internet X.509 Public Key Infrastructure: Roadmap, Chapter "Terminology".
Also note that sometimes other terms such as Certification Authority Anchor (CAA) might be used within some government organization, Top level CA is another common term to indicate the top level CA, Top Level Anchor could also be used.

NEW QUESTION: 485
Of the following, which is NOT a risk assessment system?
A. Analysis of Networked Systems Security Risks (ANSSR)
B. Aggregated Countermeasures Effectiveness (ACE) Model
C. Information Security Protection Assessment Model (ISPAM)
D. Dollar-based OPSEC Risk Analysis (DORA)
Answer: (SHOW ANSWER)

NEW QUESTION: 486
Examples of types of physical access controls include all EXCEPT which of the following?
A. badges
B. locks
C. guards
D. passwords
Answer: D (LEAVE A REPLY)
Passwords are considered a Preventive/Technical (logical) control.
The following answers are incorrect:
badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.
locks Locks are a Preventative Physical control and has no Technical association. guards Guards are a Preventative Physical control and has no Technical association.
The following reference(s) were/was used to create this question: Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 35).

NEW QUESTION: 487
CORRECT TEXT
_____ is a vendor neutral authorization and authentication protocol used by Windows 2000.
Answer:

NEW QUESTION: 488
When first analyzing an intrusion that has just been detected and confirming that it is a true positive, which of the following actions should be done as a first step if you wish to prosecute the attacker in court?
A. Back up the compromised systems.
B. Identify the attacks used to gain access.
C. Capture and record system information.
D. Isolate the compromised systems.
Answer: C (LEAVE A REPLY)
When an intrusion has been detected and confirmed, if you wish to prosecute the attacker in court, the following actions should be performed in the following order:
Capture and record system information and evidence that may be lost, modified, or not captured during the execution of a backup procedure. Start with the most volative memory areas first.
Make at least two full backups of the compromised systems, using hardware-write-protectable or write-once media. A first backup may be used to re-install the compromised system for further analysis and the second one should be preserved in a secure location to preserve the chain of custody of evidence.
Isolate the compromised systems.
Search for signs of intrusions on other systems.
Examine logs in order to gather more information and better identify other systems to which the intruder might have gained access.
Search through logs of compromised systems for information that would reveal the kind of attacks used to gain access.
Identify what the intruder did, for example by analyzing various log files, comparing checksums of known, trusted files to those on the compromised machine and by using other intrusion analysis tools.
Regardless of the exact steps being followed, if you wish to prosecute in a court of law it means you MUST capture the evidence as a first step before it could be lost or contaminated. You always start with the most volatile evidence first.
NOTE:
I have received feedback saying that some other steps may be done such as Disconnecting the system from the network or shutting down the system. This is true. However, those are not choices listed within the 4 choices attached to this question, you MUST avoid changing the question. You must stick to the four choices presented and pick

which one is the best out of the four presented.
In real life, Forensic is not always black or white. There are many shades of grey. In real life you would have to consult your system policy (if you have one), get your Computer Incident team involved, and talk to your forensic expert and then decide what is the best course of action.
Reference(s) Used for this question:
http://www.newyorkcomputerforensics.com/learn/forensics_process.php
and
ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 273-277).

NEW QUESTION: 489
In response to Access-request from a client such as a Network Access Server (NAS), which of the following is not one of the response from a RADIUS Server?
A. Access-Accept
B. Access-Reject
C. Access-Granted
D. Access-Challenge
Answer: C (LEAVE A REPLY)
Explanation/Reference:
In response to an access-request from a client, a RADIUS server returns one of three authentication responses: access-accept, access-reject, or access-challenge, the latter being a request for additional authentication information such as a one-time password from a token or a callback identifier.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 36.

NEW QUESTION: 490
In which of the following phases of system development life cycle (SDLC) is contingency planning most important?
A. Initiation
B. Development/acquisition
C. Implementation
D. Operation/maintenance
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Contingency planning requirements should be considered at every phase of SDLC, but most importantly when a new IT system is being conceived. In the initiation phase, system requirements are identified and matched to their related operational processes, allowing determination of the system's appropriate recovery priority.

Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page
12).
and
The Official ISC2 Guide to the CBK, Second Edition, Application Security, page 180-185

NEW QUESTION: 491
Which of the following phases of a system development life-cycle is most concerned with establishing a good security policy as the foundation for design?
A. Development/acquisition
B. Implementation
C. Initiation
D. Maintenance
Answer: C (LEAVE A REPLY)
Explanation/Reference:
A security policy is an important document to develop while designing an information system. The security policy begins with the organization's basic commitment to information security formulated as a general policy statement.
The policy is then applied to all aspects of the system design or security solution. The policy identifies security goals (e.g., confidentiality, integrity, availability, accountability, and assurance) the system should support, and these goals guide the procedures, standards and controls used in the IT security architecture design.
The policy also should require definition of critical assets, the perceived threat, and security-related roles and responsibilities.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 6).

NEW QUESTION: 492
Why is traffic across a packet switched network difficult to monitor?
A. Packets are link encrypted by the carrier
B. Government regulations forbids monitoring
C. Packets can take multiple paths when transmitted
D. The network factor is too high
Answer: C (LEAVE A REPLY)
Explanation/Reference:
With a packet switched network, packets are difficult to monitor because they can be transmitted using different paths.
A packet-switched network is a digital communications network that groups all transmitted data, irrespective of content, type, or structure into suitably sized blocks, called packets. The network over

which packets are transmitted is a shared network which routes each packet independently from all others and allocates transmission resources as needed.
The principal goals of packet switching are to optimize utilization of available link capacity, minimize response times and increase the robustness of communication. When traversing network adapters, switches and other network nodes, packets are buffered and queued, resulting in variable delay and throughput, depending on the traffic load in the network.
Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies. In contrast, normal telephone service is based on a circuit-switching technology, in which a dedicated line is allocated for transmission between two parties. Circuit-switching is ideal when data must be transmitted quickly and must arrive in the same order in which it's sent. This is the case with most real-time data, such as live audio and video. Packet switching is more efficient and robust for data that can withstand some delays in transmission, such as e-mail messages and Web pages.
All of the other answer are wrong
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
https://en.wikipedia.org/wiki/Packet-switched_network
and
http://www.webopedia.com/TERM/P/packet_switching.html

NEW QUESTION: 493
Which of the following is not a disadvantage of symmetric cryptography when compared with Asymmetric Ciphers?
A. Provides Limited security services
B. Has no built in Key distribution
C. Speed
D. Large number of keys are needed
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Symmetric cryptography ciphers are generally fast and hard to break. So speed is one of the key advantage of Symmetric ciphers and NOT a disadvantage. Symmetric Ciphers uses simple encryption steps such as XOR, substitution, permutation, shifting columns, shifting rows, etc... Such steps does not required a large amount of processing power compare to the complex mathematical problem used within Asymmetric Ciphers.
Some of the weaknesses of Symmetric Ciphers are:
The lack of automated key distribution. Usually an Asymmetric cipher would be use to protect the symmetric key if it needs to be communicated to another entity securely over a public network. In the good old day this was done manually where it was distributed using the Floppy Net sometimes called the Sneaker Net (you run to someone's office to give them the key).

As far as the total number of keys are required to communicate securely between a large group of users, it does not scale very well. 10 users would require 45 keys for them to communicate securely with each other. If you have 1000 users then you would need almost half a million key to communicate secure.
On Asymmetric ciphers there is only 2000 keys required for 1000 users. The formula to calculate the total number of keys required for a group of users who wishes to communicate securely with each others using Symmetric encryption is Total Number of Users (N) * Total Number of users minus one Divided by 2 or N (N-1)/2
Symmetric Ciphers are limited when it comes to security services, they cannot provide all of the security services provided by Asymmetric ciphers. Symmetric ciphers provides mostly confidentiality but can also provide integrity and authentication if a Message Authentication Code (MAC) is used and could also provide user authentication if Kerberos is used for example. Symmetric Ciphers cannot provide Digital Signature and Non-Repudiation.
Reference used for theis question:
WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

NEW QUESTION: 494
What is called the percentage at which the False Rejection Rate equals the False Acceptance Rate?
A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. Failure to enroll rate (FTE or FER)
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The percentage at which the False Rejection Rate equals the False Acceptance Rate is called the Crossover Error Rate (CER). Another name for the CER is the Equal Error Rate (EER), any of the two terms could be used.
Equal error rate or crossover error rate (EER or CER)
It is the rate at which both accept and reject errors are equal. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.
The other choices were all wrong answers:
The following are used as performance metrics for biometric systems:
false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. This is when an impostor would be accepted by the system.
False reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected. This is when a valid company employee would be rejected by the system.

Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.
and
https://en.wikipedia.org/wiki/Biometrics

NEW QUESTION: 495
What is one disadvantage of content-dependent protection of information?
A. It increases processing overhead.
B. It requires additional password entry.
C. It exposes the system to data locking.
D. It limits the user's individual address space.
Answer: A (LEAVE A REPLY)
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 496
Which of the following Intrusion Detection Systems (IDS) uses a database of attacks, known system vulnerabilities, monitoring current attempts to exploit those vulnerabilities, and then triggers an alarm if an attempt is found?
A. Knowledge-Based ID System
B. Application-Based ID System
C. Host-Based ID System
D. Network-Based ID System
Answer: A (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
Knowledge-based Intrusion Detection Systems use a database of previous attacks and known system vulnerabilities to look for current attempts to exploit their vulnerabilities, and trigger an alarm if an attempt is found.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.
Application-Based ID System - "a subset of HIDS that analyze what's going on in an application using the transaction log files of the application." Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87 Host-Based ID System - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host." Source: Official ISC2 Guide to the CISSP CBK - p. 197 Network-Based ID System - "a network device, or dedicated system attached to teh network, that monitors traffic traversing teh network segment for which it is integrated." Source: Official ISC2 Guide to the CISSP CBK - p. 196

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 497
Which layer of the DoD TCP/IP Model ensures error-free delivery and packet sequencing?
A. Internet layer
B. Network access layer
C. Host-to-host
D. Application layer
Answer: (SHOW ANSWER)
This layer of the DoD Model is also sometimes called Transport in some books but the proper name is Host-to-Host as per the RFC document.
The host-to-host layer provides for reliable end-to-end communications, ensures the data's error-free delivery, handles the data's packet sequencing, and maintains the data's integrity.
It is comparable to the transport layer of the OSI model.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/Internet_protocol_suite and http://technet.microsoft.com/en-us/library/cc786900%28v=ws.10%29.aspx and KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 85).

NEW QUESTION: 498
What is the length of an MD5 message digest?
A. 128 bits
B. 160 bits
C. 256 bits
D. varies depending upon the message size.
Answer: A (LEAVE A REPLY)
A hash algorithm (alternatively, hash "function") takes binary data, called the message, and produces a condensed representation, called the message digest. A cryptographic hash algorithm is a hash algorithm that is designed to achieve certain security properties. The Federal Information Processing Standard 180-3, Secure Hash Standard, specifies five cryptographic hash algorithms - SHA-1, SHA-224, SHA-256, SHA384, and SHA-512 for federal use in the US; the standard was also widely adopted by the information technology industry and commercial companies.

The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. Specified in RFC 1321, MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash is typically expressed as a 32-digit hexadecimal number.
However, it has since been shown that MD5 is not collision resistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property. In 1996, a flaw was found with the design of MD5, and while it was not a clearly fatal weakness, cryptographers began recommending the use of other algorithms, such as SHA1 - which has since been found also to be vulnerable. In 2004, more serious flaws were discovered in MD5, making further use of the algorithm for security purposes questionable specifically, a group of researchers described how to create a pair of files that share the same MD5 checksum. Further advances were made in breaking MD5 in 2005, 2006, and 2007. In December 2008, a group of researchers used this technique to fake SSL certificate validity, and US-CERT now says that MD5 "should be considered cryptographically broken and unsuitable for further use." and most U.S. government applications now require the SHA-2 family of hash functions.
NIST CRYPTOGRAPHIC HASH PROJECT NIST announced a public competition in a Federal Register Notice on November 2, 2007 to develop a new cryptographic hash algorithm, called SHA-3, for standardization. The competition was NIST's response to advances made in the cryptanalysis of hash algorithms.
NIST received sixty-four entries from cryptographers around the world by October 31, 2008, and selected fifty-one first-round candidates in December 2008, fourteen second-round candidates in July 2009, and five finalists - BLAKE, Grostl, JH, Keccak and Skein, in December 2010 to advance to the third and final round of the competition.
Throughout the competition, the cryptographic community has provided an enormous amount of feedback. Most of the comments were sent to NIST and a public hash forum; in addition, many of the cryptanalysis and performance studies were published as papers in major cryptographic conferences or leading cryptographic journals. NIST also hosted a SHA-3 candidate conference in each round to obtain public feedback. Based on the public comments and internal review of the candidates, NIST announced Keccak as the winner of the SHA-3 Cryptographic Hash Algorithm Competition on October 2, 2012, and ended the five-year competition.
Reference:
Tipton, Harold, et. al., Officical (ISC)2 Guide to the CISSP CBK, 2007 edition, page 261.
and
https://secure.wikimedia.org/wikipedia/en/wiki/Md5
and http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

NEW QUESTION: 499
What would BEST define risk management?
A. The process of eliminating the risk
B. The process of assessing the risks
C. The process of reducing risk to an acceptable level

D. The process of transferring risk

Answer: C (LEAVE A REPLY)

Section: Risk, Response and Recovery

Explanation/Reference:

This is the basic process of risk management.

Risk is the possibility of damage happening and the ramifications of such damage should it occur. Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree.

The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Proper risk management requires a strong commitment from senior management, a documented process that supports the organization's mission, an information risk management (IRM) policy and a delegated IRM team.

Once you've identified your company's acceptable level of risk, you need to develop an information risk management policy.

The IRM policy should be a subset of the organization's overall risk management policy (risks to a company include more than just information security issues) and should be mapped to the organizational security policies, which lay out the acceptable risk and the role of security as a whole in the organization. The IRM policy is focused on risk management while the security policy is very high-level and addresses all aspects of security. The IRM policy should address the following items:

Objectives of IRM team

Level of risk the company will accept and what is considered an acceptable risk (as defined in the previous article) Formal processes of risk identification Connection between the IRM policy and the organization's strategic planning processes Responsibilities that fall under IRM and the roles that are to fulfill them Mapping of risk to internal controls Approach for changing staff behaviors and resource allocation in response to risk analysis Mapping of risks to performance targets and budgets Key indicators to monitor the effectiveness of controls Shon Harris provides a 10,000-foot view of the risk management process below:

A big question that companies have to deal with is, "What is enough security?" This can be restated as, "What is our acceptable risk level?" These two questions have an inverse relationship. You can't know what constitutes enough security unless you know your necessary baseline risk level.

To set an enterprise-wide acceptable risk level for a company, a few things need to be investigated and understood. A company must understand its federal and state legal requirements, its regulatory requirements, its business drivers and objectives, and it must carry out a risk and threat analysis. (I will dig deeper into formalized risk analysis processes in a later article, but for now we will take a broad approach.) The result of these findings is then used to define the company's acceptable risk level, which is then outlined in security policies, standards, guidelines and procedures.

Although there are different methodologies for enterprise risk management, the core components of any risk analysis is made up of the following:
Identify company assets
Assign a value to each asset
Identify each asset's vulnerabilities and associated threats
Calculate the risk for the identified assets
Once these steps are finished, then the risk analysis team can identify the necessary countermeasures to mitigate the calculated risks, carry out cost/benefit analysis for these countermeasures and report to senior management their findings.
When we look at information security, there are several types of risk a corporation needs to be aware of and address properly. The following items touch on the major categories:
Physical damage Fire, water, vandalism, power loss, and natural disasters Human interaction Accidental or intentional action or inaction that can disrupt productivity Equipment malfunction Failure of systems and peripheral devices Inside and outside attacks Hacking, cracking, and attacking Misuse of data Sharing trade secrets, fraud, espionage, and theft Loss of data Intentional or unintentional loss of information through destructive means Application error Computation errors, input errors, and buffer overflows The following answers are incorrect:
The process of eliminating the risk is not the best answer as risk cannot be totally eliminated.
The process of assessing the risks is also not the best answer.
The process of transferring risk is also not the best answer and is one of the ways of handling a risk after a risk analysis has been performed.
References:
Shon Harris , AIO v3 , Chapter 3: Security Management Practices , Page: 66-68 and
http://searchsecurity.techtarget.com/tip/Understanding-risk

NEW QUESTION: 500
Which type of password provides maximum security because a new password is required for each new log-on?
A. One-time or dynamic password
B. Congnitive password
C. Static password
D. Passphrase
Answer: (SHOW ANSWER)
"one-time password" provides maximum security because a new password is
required for each new log-on.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 501
The Crossover Error Rate (CER) is a good measure of performance for:
A. Biometrics

B. Tokens
C. Kerberos
D. A fingerprint scan
E. Discretionary access control
Answer: A (LEAVE A REPLY)
The CER is one of the three main performance measurements used in biometrics.

NEW QUESTION: 502
Notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects is part of:
A. Incident Evaluation
B. Incident Recognition
C. Incident Protection
D. Incident Response
Answer: D (LEAVE A REPLY)
Explanation/Reference:
These are core functions of the incident response process.
"Incident Evaluation" is incorrect. Evaluation of the extent and cause of the incident is a component of the incident response process.
"Incident Recognition" is incorrect. Recognition that an incident has occurred is the precursor to the initiation of the incident response process.
"Incident Protection" is incorrect. This is an almost-right-sounding nonsense answer to distract the unwary.
References
CBK, pp. 698 - 703

NEW QUESTION: 503
Which of the following control pairing places emphasis on "soft" mechanisms that support the access control objectives?
A. Preventive/Technical Pairing
B. Preventive/Administrative Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing
Answer: B (LEAVE A REPLY)
Soft Control is another way of referring to Administrative control.
Technical and Physical controls are NOT soft control, so any choice listing them was not the best answer.
Preventative/Technical is incorrect because although access control can be technical control, it is commonly not referred to as a "soft" control
Preventative/Administrative is correct because access controls are preventative in nature. it is always best to prevent a negative event, however there are times where controls might

fail and you cannot prevent everything. Administrative controls are roles, responsibilities, policies, etc which are usually paper based. In the administrative category you would find audit, monitoring, and security awareness as well.
Preventative/Physical pairing is incorrect because Access controls with an emphasis on "soft" mechanisms conflict with the basic concept of physical controls, physical controls are usually tangible objects such as fences, gates, door locks, sensors, etc...
Detective/Administrative Pairing is incorrect because access control is a preventative control used to control access, not to detect violations to access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 504
Which of the following choice is NOT normally part of the questions that would be asked in regards to an organization's information security policy?
A. Who is involved in establishing the security policy?
B. Where is the organization's security policy defined?
C. What are the actions that need to be performed in case of a disaster?
D. Who is responsible for monitoring compliance to the organization's security policy?
Answer: C (LEAVE A REPLY)
Actions to be performed in case of a disaster are not normally part of an information security policy but part of a Disaster Recovery Plan (DRP).
Only personnel implicated in the plan should have a copy of the Disaster Recovery Plan whereas everyone should be aware of the contents of the organization's information security policy.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 398).

NEW QUESTION: 505
Another example of Computer Incident Response Team (CIRT) activities is:
A. Management of the netware logs, including collection, retention, review, and analysis of data
B. Management of the network logs, including collection and analysis of data
C. Management of the network logs, including review and analysis of data
D. Management of the network logs, including collection, retention, review, and analysis of data
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Additional examples of CIRT activities are:
Management of the network logs, including collection, retention, review, and analysis of data
Management of the resolution of an incident, management of the remediation of a vulnerability, and post-event reporting to the appropriate parties.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 64.

NEW QUESTION: 506
Which of the following statements pertaining to VPN protocol standards is false?
A. L2TP is a combination of PPTP and L2F.
B. L2TP and PPTP were designed for single point-to-point client to server communication.
C. L2TP operates at the network layer.
D. PPTP uses native PPP authentication and encryption services.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
L2TP and PPTP were both designed for individual client to server connections; they enable only a single point-to-point connection per session. Dial-up VPNs use L2TP often. Both L2TP and PPTP operate at the data link layer (layer 2) of the OSI model. PPTP uses native PPP authentication and encryption services and L2TP is a combination of PPTP and Layer 2 Forwarding protocol (L2F).
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
95).

NEW QUESTION: 507
Memory management in TCSEC levels B3 and A1 operating systems may utilize "data hiding". What does this mean?
A. System functions are layered, and none of the functions in a given layer can access data outside that layer.
B. Auditing processes and their memory addresses cannot be accessed by user processes.
C. Only security processes are allowed to write to ring zero memory.
D. It is a form of strong encryption cipher.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Data Hiding is protecting data so that it is only available to higher levels this is done and is also performed by layering, when the software in each layer maintains its own global data and does not directly reference data outside its layers.
The following answers are incorrect:
Auditing processes and their memory addresses cannot be accessed by user processes. Is incorrect because this does not offer data hiding.
Only security processes are allowed to write to ring zero memory. This is incorrect, the security kernel would be responsible for this.
It is a form of strong encryption cipher. Is incorrect because this does not conform to the definition of data hiding.

NEW QUESTION: 508
Which of the following is not a logical control when implementing logical access security?
A. access profiles.
B. userids.
C. employee badges.
D. passwords.
Answer: C (LEAVE A REPLY)
Employee badges are considered Physical so would not be a logical control.
The following answers are incorrect:
userids. Is incorrect because userids are a type of logical control. access profiles. Is incorrect because access profiles are a type of logical control. passwords. Is incorrect because passwords are a type of logical control.

NEW QUESTION: 509
Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are some of the examples of:
A. Administrative controls
B. Logical controls
C. Technical controls
D. Physical controls
Answer: D (LEAVE A REPLY)
Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are all examples of Physical Security.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 510
Which of the following phases of a system development life-cycle is most concerned with maintaining proper authentication of users and processes to ensure appropriate access control decisions?
A. Development/acquisition
B. Implementation
C. Operation/Maintenance
D. Initiation
Answer: C (LEAVE A REPLY)
The operation phase of an IT system is concerned with user authentication.

Authentication is the process where a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action, thereby ensuring that security is not compromised by an untrusted source.
It is essential that adequate authentication be achieved in order to implement security policies and achieve security goals. Additionally, level of trust is always an issue when dealing with cross-domain interactions. The solution is to establish an authentication policy and apply it to cross-domain interactions as required.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 15).

NEW QUESTION: 511
You work in a police department forensics lab where you examine computers for evidence of crimes. Your work is vital to the success of the prosecution of criminals.
One day you receive a laptop and are part of a two man team responsible for examining it together. However, it is lunch time and after receiving the laptop you leave it on your desk and you both head out to lunch.
What critical step in forensic evidence have you forgotten?
A. Chain of custody
B. Locking the laptop in your desk
C. Making a disk image for examination
D. Cracking the admin password with chntpw
Answer: A (LEAVE A REPLY)
Explanation/Reference:
When evidence from a crime is to be used in the prosecution of a criminal it is critical that you follow the law when handling that evidence. Part of that process is called chain of custody and is when you maintain proactive and documented control over ALL evidence involved in a crime.
Failure to do this can lead to the dismissal of charges against a criminal because if the evidence is compromised because you failed to maintain of chain of custody.
A chain of custody is chronological documentation for evidence in a particular case, and is especially important with electronic evidence due to the possibility of fraudulent data alteration, deletion, or creation.
A fully detailed chain of custody report is necessary to prove the physical custody of a piece of evidence and show all parties that had access to said evidence at any given time.
Evidence must be protected from the time it is collected until the time it is presented in court.
The following answers are incorrect:
- Locking the laptop in your desk: Even this wouldn't assure that the defense team would try to challenge chain of custody handling. It's usually easy to break into a desk drawer and evidence should be stored in approved safes or other storage facility.
- Making a disk image for examination: This is a key part of system forensics where we make a disk image of the evidence system and study that as opposed to studying the real disk drive. That could lead

to loss of evidence. However if the original evidence is not secured than the chain of custoday has not been maintained properly.
- Cracking the admin password with chntpw: This isn't correct. Your first mistake was to compromise the chain of custody of the laptop. The chntpw program is a Linux utility to (re)set the password of any user that has a valid (local) account on a Windows system, by modifying the crypted password in the registry's SAM file. You do not need to know the old password to set a new one. It works offline which means you must have physical access (i.e., you have to shutdown your computer and boot off a linux floppy disk). The bootdisk includes stuff to access NTFS partitions and scripts to glue the whole thing together. This utility works with SYSKEY and includes the option to turn it off. A bootdisk image is provided on their website at
http://freecode.com/projects/chntpw .
The following reference(s) was used to create this question:
For more details and to cover 100% of the exam Qs, subscribe to our holistic Security+ 2014 CBT Tutorial at: http://www.cccure.tv/
and
http://en.wikipedia.org/wiki/Chain_of_custody
and
http://www.datarecovery.com/forensic_chain_of_custody.asp

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 512
Which of the following is a device that is used to regenerate or replicate the received signals?
A. Bridge
B. Router
C. Repeater
D. Brouter
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Repeaters offer the simplest form of connectivity. They regenerate received electrical signals at their original strength between cable segments. Bridges are devices used to connect similar or dissimilar LANs together to form an extended LAN. Routers provide packet routing between network segments. Brouter are devices that combine router and bridge functionality.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter

7: Telecommunications and Network Security (page 397).

NEW QUESTION: 513
Organizations should not view disaster recovery as which of the following?
A. Committed expense.
B. Discretionary expense.
C. Enforcement of legal statutes.
D. Compliance with regulations.
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
Disaster Recovery should never be considered a discretionary expense. It is far too important a task. In order to maintain the continuity of the business Disaster Recovery should be a commitment of and by the organization.
A discretionary fixed cost has a short future planning horizon-under a year. These types of costs arise from annual decisions of management to spend in specific fixed cost areas, such as marketing and research. DR would be an ongoing long term committment not a short term effort only.
A committed fixed cost has a long future planning horizon- more than on year. These types of costs relate to a company's investment in assets such as facilities and equipment. Once such costs have been incurred, the company is required to make future payments.
The following answers are incorrect:
committed expense. Is incorrect because Disaster Recovery should be a committed expense.
enforcement of legal statutes. Is incorrect because Disaster Recovery can include enforcement of legal statutes. Many organizations have legal requirements toward Disaster Recovery.
compliance with regulations. Is incorrect because Disaster Recovery often means compliance with regulations.
Many financial institutions have regulations requiring Disaster Recovery Plans and Procedures.

NEW QUESTION: 514
Secure Shell (SSH) is a strong method of performing:
A. client authentication
B. server authentication
C. host authentication
D. guest authentication
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Secure shell (SSH) was designed as an alternative to some of the insecure protocols and allows users to securely access resources on remote computers over an encrypted tunnel. The Secure Shell Protocol (SSH) is a protocol for secure remote login and other secure network services over an insecure network.

The SSH authentication protocol runs on top of the SSH transport layer protocol and provides a single authenticated tunnel for the SSH connection protocol.
SSH's services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel. Many users protect less secure traffic of protocols, such as X Windows and VNC (virtual network computing), by forwarding them through a SSH tunnel.
The SSH tunnel protects the integrity of communication, preventing session hijacking and other man-in-the- middle attacks. Another advantage of SSH over its predecessors is that it supports strong authentication.
There are several alternatives for SSH clients to authenticate to a SSH server, including passwords and digital certificates.
Keep in mind that authenticating with a password is still a significant improvement over the other protocols because the password is transmitted encrypted.
There are two incompatible versions of the protocol, SSH-1 and SSH-2, though many servers support both.
SSH-2 has improved integrity checks (SSH-1 is vulnerable to an insertion attack due to weak CRC-32 integrity checking) and supports local extensions and additional types of digital certificates such as Open PGP. SSH was originally designed for UNIX, but there are now implementations for other operating systems, including Windows, Macintosh, and OpenVMS.
Is SSH 3.0 the same as SSH3?
The short answer is: NO SSH 3.0 refers to version 3 of SSH Communications SSH2 protocol implementation and it could also refer to OpenSSH Version 3.0 of its SSH2 software. The "3" refers to the software release version not the protocol version. As of this writing (July 2013), there is no SSH3 protocol.
"Server authentication" is incorrect. Though many SSH clients allow pre-caching of server/host keys, this is a minimal form of server/host authentication.
"Host authentication" is incorrect. Though many SSH clients allow pre-caching of server/host keys, this is a minimal form of server/host authentication.
"Guest authentication" is incorrect. The general idea of "guest" is that it is unauthenticated access.
Reference(s) used for this question:
http://www.ietf.org/rfc/rfc4252.txt
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7080-7088). Auerbach Publications. Kindle Edition.

NEW QUESTION: 515
Attributes that characterize an attack are stored for reference using which of the following Intrusion Detection System (IDS) ?
A. signature-based IDS
B. statistical anomaly-based IDS
C. event-based IDS
D. inferent-based IDS

Answer: A (LEAVE A REPLY)
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

NEW QUESTION: 516
Who should direct short-term recovery actions immediately following a disaster?
A. Chief Information Officer.
B. Chief Operating Officer.
C. Disaster Recovery Manager.
D. Chief Executive Officer.
Answer: C (LEAVE A REPLY)
The Disaster Recovery Manager should also be a member of the team that assisted in the development of the Disaster Recovery Plan. Senior-level management need to support the process but would not be involved with the initial process.
The following answers are incorrect:
Chief Information Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.
Chief Operating Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.
Chief Executive Officer. Is incorrect because the Senior-level management are the ones to authorize the recovery plan and process but during the initial recovery process they will most likely be heavily involved in other matters.

NEW QUESTION: 517
What is the greatest danger from DHCP?
A. An intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients.
B. Having multiple clients on the same LAN having the same IP address.
C. Having the wrong router used as the default gateway.
D. Having the organization's mail server unreachable.
Answer: A (LEAVE A REPLY)
The greatest danger from BootP or DHCP (Dynamic Host Control Protocol)
is from an intruder on the network impersonating a DHCP server and thereby
misconfiguring the DHCP clients. Other choices are possible consequences of DHCP
impersonation.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000,
Chapter 4: Sockets and Services from a Security Viewpoint.

NEW QUESTION: 518

Organizations should not view disaster recovery as which of the following?
A. Committed expense.
B. Discretionary expense.
C. Enforcement of legal statutes.
D. Compliance with regulations.
Answer: (SHOW ANSWER)
Explanation/Reference:
Disaster Recovery should never be considered a discretionary expense. It is far too important a task. In order to maintain the continuity of the business Disaster Recovery should be a commitment of and by the organization.
A discretionary fixed cost has a short future planning horizon-under a year. These types of costs arise from annual decisions of management to spend in specific fixed cost areas, such as marketing and research. DR would be an ongoing long term committment not a short term effort only.
A committed fixed cost has a long future planning horizon- more than on year. These types of costs relate to a company's investment in assets such as facilities and equipment. Once such costs have been incurred, the company is required to make future payments.
The following answers are incorrect:
committed expense. Is incorrect because Disaster Recovery should be a committed expense.
enforcement of legal statutes. Is incorrect because Disaster Recovery can include enforcement of legal statutes. Many organizations have legal requirements toward Disaster Recovery.
compliance with regulations. Is incorrect because Disaster Recovery often means compliance with regulations. Many financial institutions have regulations requiring Disaster Recovery Plans and Procedures.

NEW QUESTION: 519
Application Layer Firewalls operate at the:
A. OSI protocol Layer seven, the Application Layer.
B. OSI protocol Layer six, the Presentation Layer.
C. OSI protocol Layer five, the Session Layer.
D. OSI protocol Layer four, the Transport Layer.
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Since the application layer firewall makes decisions based on application-layer information in the packet, it operates at the application layer of the OSI stack.
"OSI protocol layer 6, the presentation layer" is incorrect. The application layer firewall must have access to the application layer information in the packet and therefore operates at the application layer.
"OSI protocol layer 5, the session layer" is incorrect. The application layer firewall must have access to the application layer information in the packet and therefore operates at the application layer.
"OSI protocol layer 4, the transport layer" is incorrect. The application layer firewall must have access to the application layer information in the packet and therefore operates at the application layer.

References:
CBK, p. 467
AIO3, pp.488 - 490

NEW QUESTION: 520
What is called an attack in which an attacker floods a system with connection requests but does not respond when the target system replies to those requests?
A. Ping of death attack
B. SYN attack
C. Smurf attack
D. Buffer overflow attack
Answer: B (LEAVE A REPLY)
A SYN attack occurs when an attacker floods the target system's small "inprocess" queue with connection requests, but it does not respond when the target system replies to those requests. This causes the target system to "time out" while waiting for the proper response, which makes the system crash or become unusable. A buffer overflow attack occurs when a process receives much more data than expected. One common buffer overflow attack is the ping of death, where an attacker sends IP packets that exceed the maximum legal length (65535 octets). A smurf attack is an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 76).

NEW QUESTION: 521
Single Sign-on (SSO) is characterized by which of the following advantages?
A. Convenience
B. Convenience and centralized administration
C. Convenience and centralized data administration
D. Convenience and centralized network administration
Answer: B (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Convenience -Using single sign-on users have to type their passwords only once when they first log in to access all the network resources; and Centralized Administration as some single sign-on systems are built around a unified server administration system. This allows a single administrator to add and delete accounts across the entire network from one user interface.
The following answers are incorrect:
Convenience - alone this is not the correct answer.
Centralized Data or Network Administration - these are thrown in to mislead the student. Neither are a benefit to SSO, as these specifically should not be allowed with just an SSO.

References: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, page 35.
TIPTON, Harold F. & HENRY, Kevin, Official (ISC)2 Guide to the CISSP CBK, 2007, page 180.

NEW QUESTION: 522
What is the main focus of the Bell-LaPadula security model?
A. Accountability
B. Integrity
C. Confidentiality
D. Availability
Answer: C (LEAVE A REPLY)
The Bell-LaPadula model is a formal model dealing with confidentiality.
The Bell-LaPadula Model (abbreviated BLP) is a state machine model used for enforcing access control in government and military applications. It was developed by David Elliott Bell and Leonard J. LaPadula, subsequent to strong guidance from Roger R. Schell to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policy. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g."Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").
The Bell-LaPadula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. In this formal model, the entities in an information system are divided into subjects and objects.
The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system satisfies the security objectives of the model. The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions.
A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.
The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:
The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).
The -property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The -property is also known as the Confinement property. The Discretionary Security Property - use of an access matrix to specify the discretionary access control.
The following are incorrect answers:

Accountability is incorrect. Accountability requires that actions be traceable to the user that performed them and is not addressed by the Bell-LaPadula model.
Integrity is incorrect. Integrity is addressed in the Biba model rather than Bell-Lapadula.
Availability is incorrect. Availability is concerned with assuring that data/services are available to authorized users as specified in service level objectives and is not addressed by the Bell-Lapadula model.
References:
CBK, pp. 325-326
AIO3, pp. 279 - 284
AIOv4 Security Architecture and Design (pages 333 - 336)
AIOv5 Security Architecture and Design (pages 336 - 338)
Wikipedia at https://en.wikipedia.org/wiki/Bell-La_Padula_model

NEW QUESTION: 523
What are the two most critical aspects of risk analysis? (Choose two)
A. Identifying threats
B. Identifying vulnerabilities
C. Identifying resources
D. Identifying assets
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 524
Which of the following countermeasures would be the most appropriate to prevent possible intrusion or damage from wardialing attacks?
A. Monitoring and auditing for such activity
B. Require user authentication
C. Making sure only necessary phone numbers are made public
D. Using completely different numbers for voice and data accesses
Answer: B (LEAVE A REPLY)
Knowlege of modem numbers is a poor access control method as an attacker can discover modem numbers by dialing all numbers in a range. Requiring user authentication before remote access is granted will help in avoiding unauthorized access over a modem line.
"Monitoring and auditing for such activity" is incorrect. While monitoring and auditing can assist in detecting a wardialing attack, they do not defend against a successful wardialing attack.
"Making sure that only necessary phone numbers are made public" is incorrect. Since a wardialing attack blindly calls all numbers in a range, whether certain numbers in the range are public or not is irrelevant.
"Using completely different numbers for voice and data accesses" is incorrect. Using different number ranges for voice and data access might help prevent an attacker from stumbling across the data lines while wardialing the public voice number range but this is not an adequate countermeaure.
References: CBK, p. 214 AIO3, p. 534-535

NEW QUESTION: 525
In which of the following model are Subjects and Objects identified and the permissions applied to each subject/object combination are specified. Such a model can be used to quickly summarize what permissions a subject has for various system objects.
A. Access Control Matrix model
B. Take-Grant model
C. Bell-LaPadula model
D. Biba model
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects. Matrices are data structures that programmers implement as table lookups that will be used and enforced by the operating system.
This type of access control is usually an attribute of DAC models. The access rights can be assigned directly to the subjects (capabilities) or to the objects (ACLs).
Capability Table
A capability table specifies the access rights a certain subject possesses pertaining to specific objects. A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.
Access control lists (ACLs)
ACLs are used in several operating systems, applications, and router configurations. They are lists of subjects that are authorized to access a specific object, and they define what level of authorization is granted.
Authorization can be specific to an individual, group, or role. ACLs map values from the access control matrix to the object.
Whereas a capability corresponds to a row in the access control matrix, the ACL corresponds to a column of the matrix.
NOTE: Ensure you are familiar with the terms Capability and ACLs for the purpose of the exam.
Resource(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5264-5267). McGraw- Hill. Kindle Edition.
or
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Page 229 and Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1923-1925). Auerbach Publications. Kindle Edition.

NEW QUESTION: 526
Access Control techniques do not include which of the following?
A. Rule-Based Access Controls
B. Role-Based Access Control

C. Mandatory Access Control
D. Random Number Based Access Control
Answer: D (LEAVE A REPLY)
Access Control Techniques Discretionary Access Control Mandatory Access Control Lattice Based Access Control Rule-Based Access Control Role-Based Access Control Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 527
The Data Encryption Standard (DES) encryption algorithm has which of the following characteristics?
A. 64 bits of data input results in 56 bits of encrypted output
B. 128 bit key with 8 bits used for parity
C. 64 bit blocks with a 64 bit total key length
D. 56 bits of data input results in 56 bits of encrypted output
Answer: C (LEAVE A REPLY)
DES works with 64 bit blocks of text using a 64 bit key (with 8 bits used for parity, so the effective key length is 56 bits).
Some people are getting the Key Size and the Block Size mixed up. The block size is usually a specific length. For example DES uses block size of 64 bits which results in 64
bits of encrypted data for each block. AES uses a block size of 128 bits, the block size on AES can only be 128 as per the published standard FIPS-197.
A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte1. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it.
IN CONTRAST WITH AES
The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits. Other input, output and Cipher Key lengths are not permitted by this standard.

The Advanced Encryption Standard (AES) specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in the AES standard.
The AES algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256".
The other answers are not correct because:
"64 bits of data input results in 56 bits of encrypted output" is incorrect because while DES does work with 64 bit block input, it results in 64 bit blocks of encrypted output.
"128 bit key with 8 bits used for parity" is incorrect because DES does not ever use a 128 bit key.
"56 bits of data input results in 56 bits of encrypted output" is incorrect because DES always works with 64 bit blocks of input/output, not 56 bits.
Reference(s) used for this question:
Official ISC2 Guide to the CISSP CBK, Second Edition, page: 336-343
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

NEW QUESTION: 528
Which of the following is the simplest type of firewall ?
A. Stateful packet filtering firewall
B. Packet filtering firewall
C. Dual-homed host firewall
D. Application gateway
Answer: B (LEAVE A REPLY)
A static packet filtering firewall is the simplest and least expensive type of firewalls, offering minimum security provisions to a low-risk computing environment.
A static packet filter firewall examines both the source and destination addresses of the incoming data packet and applies ACL's to them. They operates at either the Network or Transport layer. They are known as the First generation of firewall.
Older firewalls that were only packet filters were essentially routing devices that provided access control functionality for host addresses and communication sessions. These devices, also known as stateless inspection firewalls, do not keep track of the state of each flow of traffic that passes though the firewall; this means, for example, that they cannot associate multiple requests within a single session to each other. Packet filtering is at the core of most modern firewalls, but there are few firewalls sold today that only do stateless packet filtering. Unlike more advanced filters, packet filters are not concerned about the content of packets. Their access control functionality is governed by a set of directives referred to as a ruleset. Packet filtering capabilities are built into most operating systems and devices capable of routing; the most common example of a pure packet filtering device

is a network router that employs access control lists.
There are many types of Firewall:
Application Level Firewalls - Often called a Proxy Server. It works by transferring a copy of each accepted data packet from one network to another. They are known as the Second generation of firewalls.
An application-proxy gateway is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality. These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them. Each successful connection attempt actually results in the creation of two separate connections-one between the client and the proxy server, and another between the proxy server and the true destination. The proxy is meant to be transparent to the two hosts-from their perspectives there is a direct connection. Because external hosts only communicate with the proxy agent, internal IP addresses are not visible to the outside world. The proxy agent interfaces directly with the firewall ruleset to determine whether a given instance of network traffic should be allowed to transit the firewall.
Stateful Inspection Firewall - Packets are captured by the inspection engine operating at the network layer and then analyzed at all layers. They are known as the Third generation of firewalls.
Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each connection in a state table. While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information.
Web Application Firewalls - The HTTP protocol used in web servers has been exploited by attackers in many ways, such as to place malicious software on the computer of someone browsing the web, or to fool a person into revealing private information that they might not have otherwise. Many of these exploits can be detected by specialized application firewalls called web application firewalls that reside in front of the web server. Web application firewalls are a relatively new technology, as compared to other firewall technologies, and the type of threats that they mitigate are still changing frequently. Because they are put in front of web servers to prevent attacks on the server, they are often considered to be very different than traditional firewalls.
Host-Based Firewalls and Personal Firewalls - Host-based firewalls for servers and personal firewalls for desktop and laptop personal computers (PC) provide an additional layer of security against network-based attacks. These firewalls are software-based, residing on the hosts they are protecting-each monitors and controls the incoming and outgoing network traffic for a single host. They can provide more granular protection than network firewalls to meet the needs of specific hosts.
Host-based firewalls are available as part of server operating systems such as Linux, Windows, Solaris, BSD, and Mac OS X Server, and they can also be installed as third-party add-ons. Configuring a host-based firewall to allow only necessary traffic to the server provides protection against malicious activity from all hosts, including those on the same

subnet or on other internal subnets not separated by a network firewall. Limiting outgoing traffic from a server may also be helpful in preventing certain malware that infects a host from spreading to other hosts.11 Host-based firewalls usually perform logging, and can often be configured to perform address-based and application-based access controls
Dynamic Packet Filtering - Makes informed decisions on the ACL's to apply. They are known as the Fourth generation of firewalls.
Kernel Proxy - Very specialized architecture that provides modular kernel-based, multi-layer evaluation and runs in the NT executive space. They are known as the Fifth generation of firewalls.
The following were incorrect answers:
All of the other types of firewalls listed are more complex than the Packet Filtering Firewall.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th Edition, Telecommunications and Network Security, Page 630.
and
NIST Guidelines on Firewalls and Firewalls policies, Special Publication 800-4 Revision 1

NEW QUESTION: 529
In non-discretionary access control using Role Based Access Control (RBAC), a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on:
A. The societies role in the organization
B. The individual's role in the organization
C. The group-dynamics as they relate to the individual's role in the organization
D. The group-dynamics as they relate to the master-slave role in the organization
Answer: (SHOW ANSWER)
In Non-Discretionary Access Control, when Role Based Access Control is being used, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual's role in the organization.
Reference(S) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 530
Which of the following is not a one-way hashing algorithm?
A. MD2
B. RC4
C. SHA-1
D. HAVAL
Answer: B (LEAVE A REPLY)

RC4 was designed by Ron Rivest of RSA Security in 1987. While it is officially termed "Rivest Cipher 4", the RC acronym is alternatively understood to stand for "Ron's Code" (see also RC2, RC5 and RC6). RC4 was initially a trade secret, but in September 1994 a description of it was anonymously posted to the Cypherpunks mailing list. It was soon posted on the sci.crypt newsgroup, and from there to many sites on the Internet. The leaked code was confirmed to be genuine as its output was found to match that of proprietary software using licensed RC4. Because the algorithm is known, it is no longer a trade secret. The name RC4 is trademarked, so RC4 is often referred to as ARCFOUR or ARC4 (meaning alleged RC4) to avoid trademark problems. RSA Security has never officially released the algorithm; Rivest has, however, linked to the English Wikipedia article on RC4 in his own course notes. RC4 has become part of some commonly used encryption protocols and standards, including WEP and WPA for wireless cards and TLS.

The main factors in RC4's success over such a wide range of applications are its speed and simplicity: efficient implementations in both software and hardware are very easy to develop.

The following answer were not correct choices:

SHA-1 is a one-way hashing algorithms. SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard. SHA stands for "secure hash algorithm". The three SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, and SHA-2. SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used security applications and protocols. In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although no successful attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved alternatives. A new hash standard, SHA-3, is currently under development - an ongoing NIST hash function competition is scheduled to end with the selection of a winning function in 2012.

SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.

MD2 is a one-way hashing algorithms. The MD2 Message-Digest Algorithm is a cryptographic hash function developed by Ronald Rivest in 1989. The algorithm is optimized for 8-bit computers. MD2 is specified in RFC 1319. Although MD2 is no longer considered secure, even as of 2010 it remains in use in public key infrastructures as part of certificates generated with MD2 and RSA.

Haval is a one-way hashing algorithms. HAVAL is a cryptographic hash function. Unlike MD5, but like most modern cryptographic hash functions, HAVAL can produce hashes of

different lengths. HAVAL can produce hashes in lengths of 128 bits, 160 bits, 192 bits, 224 bits, and 256 bits. HAVAL also allows users to specify the number of rounds (3, 4, or 5) to be used to generate the hash.
The following reference(s) were used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000. and
https://en.wikipedia.org/wiki/HAVAL and https://en.wikipedia.org/wiki/MD2_%28cryptography%29 and https://en.wikipedia.org/wiki/SHA-1

NEW QUESTION: 531
What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?
A. Accountability controls
B. Mandatory access controls
C. Assurance procedures
D. Administrative controls
Answer: C (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
Controls provide accountability for individuals accessing information. Assurance procedures ensure that access control mechanisms correctly implement the security policy for the entire life cycle of an information system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION: 532
Which of the following computer crime is MORE often associated with INSIDERS?
A. IP spoofing
B. Password sniffing
C. Data diddling
D. Denial of service (DOS)
Answer: C (LEAVE A REPLY)
Section: Malicious Code
Explanation/Reference:
It refers to the alteration of the existing data , most often seen before it is entered into an application.This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed.
The other answers are incorrect because :
IP Spoofing is not correct as the questions asks about the crime associated with the insiders. Spoofing is generally accomplished from the outside.

Password sniffing is also not the BEST answer as it requires a lot of technical knowledge in understanding the encryption and decryption process.
Denial of service (DOS) is also incorrect as most Denial of service attacks occur over the internet.
Reference : Shon Harris , AIO v3 , Chapter-10 : Law , Investigation & Ethics , Page : 758-760.

NEW QUESTION: 533
Which of the following types of Intrusion Detection Systems uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host?
A. Network-based ID systems.
B. Anomaly Detection.
C. Host-based ID systems.
D. Signature Analysis.
Answer: B (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation
Explanation/Reference:
There are two basic IDS analysis methods: pattern matching (also called signature analysis) and anomaly detection.
Anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host. Anomalies may include but are not limited to:
Multiple failed log-on attempts
Users logging in at strange hours
Unexplained changes to system clocks
Unusual error messages
The following are incorrect answers:
Network-based ID Systems (NIDS) are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network.
Host-based ID Systems (HIDS) is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.
Signature Analysis Some of the first IDS products used signature analysis as their detection method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the data stream) to produce an alert if that pattern was detected. For example, an attacker manipulating an

FTP server may use a tool that sends a specially constructed packet. If that particular packet pattern is known, it can be represented in the form of a signature that IDS can then compare to incoming packets. Pattern-based IDS will have a database of hundreds, if not thousands, of signatures that are compared to traffic streams. As new attack signatures are produced, the system is updated, much like antivirus solutions. There are drawbacks to pattern-based IDS. Most importantly, signatures can only exist for known attacks. If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS. Additionally, if an attacker knows that the IDS is present, he or she can alter his or her methods to avoid detection. Changing packets and data streams, even slightly, from known signatures can cause an IDS to miss the attack. As with some antivirus systems, the IDS is only as good as the latest signature database on the system.
For additional information on Intrusion Detection Systems - http://en.wikipedia.org/wiki/Intrusion_detection_system Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3623-3625, 3649-3654, 3666-3686). Auerbach Publications. Kindle Edition.

NEW QUESTION: 534
What can be defined as a momentary low voltage?
A. Spike
B. Sag
C. Fault
D. Brownout
Answer: (SHOW ANSWER)
A sag is a momentary low voltage. A spike is a momentary high voltage. A fault is a momentary power out and a brownout is a prolonged power supply that is below normal voltage. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 6: Physical security (page 299)

NEW QUESTION: 535
Which of the following backup methods is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets?
A. full backup method.
B. incremental backup method.
C. differential backup method.
D. tape backup method.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
The Full Backup Method is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

NEW QUESTION: 536
Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient's "public" key in order to get confidentiality of the data being sent. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:
A. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.
B. The channels through which the information flows are secure.
C. The recipient's identity can be positively verified by the sender.
D. The sender of the message is the only other person with access to the recipient's private key.
Answer: (SHOW ANSWER)
Through the use of Public Key Infrastructure (PKI) the recipient's identity can be positively verified by the sender.
The sender of the message knows he is using a Public Key that belongs to a specific user. He can validate through the Certification Authority (CA) that a public key is in fact the valid public key of the receiver and the receiver is really who he claims to be. By using the public key of the recipient, only the recipient using the matching private key will be able to decrypt the message. When you wish to achieve confidentiality, you encrypt the message with the recipient public key.
If the sender would wish to prove to the recipient that he is really who he claims to be then the sender would apply a digital signature on the message before encrypting it with the public key of the receiver. This would provide Confidentiality and Authenticity of the message.
A PKI (Public Key Infrastructure) enables users of an insecure public network, such as the Internet, to securely and privately exchange data through the use of public key-pairs that are obtained and shared through a trusted authority, usually referred to as a Certificate Authority.
The PKI provides for digital certificates that can vouch for the identity of individuals or organizations, and for directory services that can store, and when necessary, revoke those
digital certificates. A PKI is the underlying technology that addresses the issue of trust in a normally untrusted environment.
The following answers are incorrect:
The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use. Is incorrect because through the use of Public Key Infrastructure (PKI), the parties do not have to have a mutual agreement. They have a trusted 3rd party Certificate Authority to perform the verification of the sender.
The channels through which the information flows are secure. Is incorrect because the use of Public Key Infrastructure (PKI) does nothing to secure the channels.
The sender of the message is the only other person with access to the recipient's private key. Is incorrect because the sender does not have access to the recipient's private key though Public Key Infrastructure (PKI).
Reference(s) used for this question:
OIG CBK Cryptography (pages 253 - 254)

NEW QUESTION: 537
Which backup method copies only files that have changed since the last full backup, but does not clear the archive bit?
A. Differential backup method.
B. Full backup method.
C. Incremental backup method.
D. Tape backup method.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
One of the key item to understand regarding backup is the archive bit. The archive bit is used to determine what files have been backuped already. The archive bit is set if a file is modified or a new file is created, this indicates to the backup program that it has to be saved on the next backup. When a full backup is performed the archive bit will be cleared indicating that the files were backup. This allows backup programs to do an incremental or differential backup that only backs up the changes to the filesystem since the last time the bit was cleared
Full Backup (or Reference Backup)
A Full backup will backup all the files and folders on the drive every time you run the full backup. The archive bit is cleared on all files indicating they were all backuped.
Advantages:
All files from the selected drives and folders are backed up to one backup set.
In the event you need to restore files, they are easily restored from the single backup set.
Disadvantages:
A full backup is more time consuming than other backup options.
Full backups require more disk, tape, or network drive space.
Incremental Backup
An incremental backup provides a backup of files that have changed or are new since the last incremental backup.
For the first incremental backup, all files in the file set are backed up (just as in a full backup). If you use the same file set to perform a incremental backup later, only the files that have changed are backed up. If you use the same file set for a third backup, only the files that have changed since the second backup are backed up, and so on.
Incremental backup will clear the archive bit.
Advantages:
Backup time is faster than full backups.
Incremental backups require less disk, tape, or network drive space.
You can keep several versions of the same files on different backup sets.
Disadvantages:
In order to restore all the files, you must have all of the incremental backups available.
It may take longer to restore a specific file since you must search more than one backup set to find the latest version of a file.

Differential Backup
A differential backup provides a backup of files that have changed since a full backup was performed. A differential backup typically saves only the files that are different or new since the last full backup. Together, a full backup and a differential backup include all the files on your computer, changed and unchanged.
Differential backup do not clear the archive bits.
Advantages:
Differential backups require even less disk, tape, or network drive space than incremental backups.
Backup time is faster than full or incremental backups.
Disadvantages:
Restoring all your files may take considerably longer since you may have to restore both the last differential and full backup.
Restoring an individual file may take longer since you have to locate the file on either the differential or full backup.
For more info see: http://support.microsoft.com/kb/136621
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

NEW QUESTION: 538
What is the most secure way to dispose of information on a CD-ROM?
A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction
Answer: (SHOW ANSWER)
Explanation/Reference:
First you have to realize that the question is specifically talking about a CDROM. The information stored on a CDROM is not in electro magnetic format, so a degausser woud be inneffective.
You cannot sanitize a CDROM but you might be able to sanitize a RW/CDROM. A CDROM is a write once device and cannot be overwritten like a hard disk or other magnetic device.
Physical Damage would not be enough as information could still be extracted in a lab from the undamaged portion of the media or even from the pieces after the physical damage has been done.
Physical Destruction using a shredder, your microwave oven, melting it, would be very effective and the best choice for a non magnetic media such as a CDROM.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 539
Physically securing backup tapes from unauthorized access is obviously a security concern and is considered a function of the:
A. Operations Security Domain.
B. Operations Security Domain Analysis.

C. Telecommunications and Network Security Domain.
D. Business Continuity Planning and Disater Recovery Planning.
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Physically securing the tapes from unauthorized access is obviously a security concern and is considered a function of the Operations Security Domain.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

NEW QUESTION: 540
What type of cable is used with 100Base-TX Fast Ethernet?
A. Fiber-optic cable
B. Category 3 or 4 unshielded twisted-pair (UTP).
C. Category 5 unshielded twisted-pair (UTP).
D. RG-58 cable.
Answer: C (LEAVE A REPLY)
This is the type of cabling recommended for 100Base-TX networks.
Fiber-optic cable is incorrect. Incorrect media type for 100Base-TX -- 100Base-FX would denote fiber optic cabling.
"Category 3 or 4 unshielded twisted-pair (UTP)" is incorrect. These types are not recommended for 100Mbps operation.
RG-58 cable is incorrect. Incorrect media type for 100Base-TX.
References CBK, p. 428 AIO3, p. 455

NEW QUESTION: 541
In the context of Biometric authentication, what is a quick way to compare the accuracy of devices. In general, the device that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?
A. the CER is used.
B. the FRR is used
C. the FAR is used
D. the FER is used
Answer: (SHOW ANSWER)
Explanation/Reference:
equal error rate or crossover error rate (EER or CER): the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.
In the context of Biometric Authentication almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in

an airport metal detector, the system becomes increasingly selective and has a higher False Reject Rate (FRR).
Conversely, if the sensitivity is decreased, the False Acceptance Rate (FAR) will increase.
Thus, to have a valid measure of the system performance, the CrossOver Error Rate (CER) is used.
The following are used as performance metrics for biometric systems:
false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, then he is treated as genuine that increase the FAR and hence performance also depends upon the selection of threshold value.
false reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
template capacity: the maximum number of sets of data which can be stored in the system.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.
and
Wikipedia at: https://en.wikipedia.org/wiki/Biometrics

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 542
What is called an event or activity that has the potential to cause harm to the information systems or networks?
A. Vulnerability
B. Threat agent
C. Weakness
D. Threat
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery

Explanation/Reference:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

NEW QUESTION: 543
A proxy is considered a:
A. first generation firewall.
B. third generation firewall.
C. second generation firewall.
D. fourth generation firewall.
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The proxy (application layer firewall, circuit level proxy, or application proxy) is a second generation firewall
"First generation firewall" incorrect. A packet filtering firewall is a first generation firewall.
"Third generation firewall" is incorrect. Stateful Firewall are considered third generation firewalls
"Fourth generation firewall" is incorrect. Dynamic packet filtering firewalls are fourth generation firewalls
References:
CBK, p. 464
AIO3, pp. 482 - 484
Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/ scf4ch3.htm for a general discussion of the different generations.

NEW QUESTION: 544
Which of the following is used to monitor network traffic or to monitor host audit logs in real time to determine violations of system security policy that have taken place?
A. Intrusion Detection System
B. Compliance Validation System
C. Intrusion Management System (IMS)
D. Compliance Monitoring System
Answer: A (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
An Intrusion Detection System (IDS) is a system that is used to monitor network traffic or to monitor host audit logs in order to determine if any violations of an organization's system security policy have taken place.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

NEW QUESTION: 545
The Reference Validation Mechanism that ensures the authorized access relationships between subjects and objects is implementing which of the following concept:
A. The reference monitor.
B. Discretionary Access Control.
C. The Security Kernel.
D. Mandatory Access Control.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
The reference monitor concept is an abstract machine that ensures that all subjects have the necessary access rights before accessing objects. Therefore, the kernel will mediates all accesses to objects by subjects and will do so by validating through the reference monitor concept.
The kernel does not decide whether or not the access will be granted, it will be the Reference Monitor which is a subset of the kernel that will say YES or NO.
All access requests will be intercepted by the Kernel, validated through the reference monitor, and then access will either be denied or granted according to the request and the subject privileges within the system.
1. The reference monitor must be small enough to be full tested and valided
2. The Kernel must MEDIATE all access request from subjects to objects
3. The processes implementing the reference monitor must be protected
4. The reference monitor must be tamperproof
The following answers are incorrect:
The security kernel is the mechanism that actually enforces the rules of the reference monitor concept.
The other answers are distractors.
Shon Harris, All In One, 5th Edition, Security Architecture and Design, Page 330 also see http://en.wikipedia.org/wiki/Reference_monitor

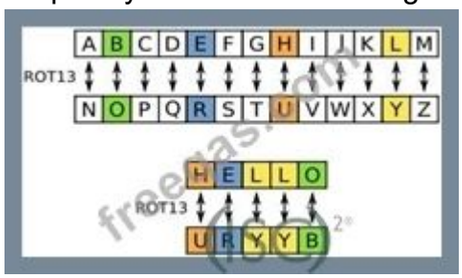
NEW QUESTION: 546
What is the name for a substitution cipher that shifts the alphabet by 13 places?
A. Caesar cipher
B. Polyalphabetic cipher
C. ROT13 cipher
D. Transposition cipher
Answer: C (LEAVE A REPLY)
Explanation/Reference:
An extremely simple example of conventional cryptography is a substitution cipher.
A substitution cipher substitutes one piece of information for another. This is most frequently done by offsetting letters of the alphabet. Two examples are Captain Midnight's Secret Decoder Ring, which you may have owned when you were a kid, and Julius Caesar's cipher. In both cases, the algorithm is to

offset the alphabet and the key is the number of characters to offset it. So the offset could be one, two, or any number you wish. ROT-13 is an example where it is shifted 13 spaces. The Ceaser Cipher is another example where it is shifted 3 letters to the left.

ROT13 ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple letter substitution cipher that replaces a letter with the letter 13 letters after it in the alphabet. ROT13 is an example of the Caesar cipher, developed in ancient Rome.

In the basic Latin alphabet, ROT13 is its own inverse; that is, to undo ROT13, the same algorithm is applied, so the same action can be used for encoding and decoding. The algorithm provides virtually no cryptographic security, and is often cited as a canonical example of weak encryption.

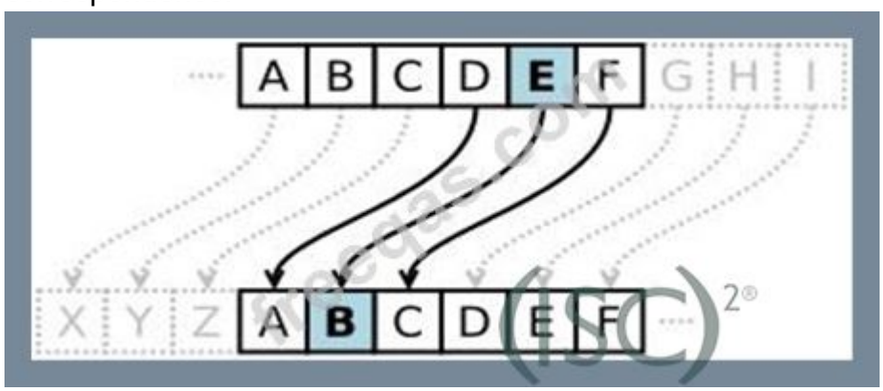
ROT13 is used in online forums as a means of hiding spoilers, puzzle solutions, and offensive materials from the casual glance. ROT13 has been described as the "Usenet equivalent of a magazine printing the answer to a quiz upside down". ROT13 has inspired a variety of letter and word games on-line, and is frequently mentioned in newsgroup conversations. See diagram Below:



Rot 13 Cipher

The following are incorrect:

The Caesar cipher is a simple substitution cipher that involves shifting the alphabet three positions to the right. In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.



Caesar Cipher

Polyalphabetic cipher refers to using multiple alphabets at a time. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Viginere Cipher

Transposition cipher is a different type of cipher. In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed. See the reference below for multiple examples of Transpositio Ciphers.

An exemple of Transposition cipher could be columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the word ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the keyword ZEBRAS and the message WE ARE DISCOVERED. FLEE AT ONCE. In a regular columnar transposition, we write this into the grid as Follows:

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

Transposition Cipher

Providing five nulls (QKJEU) at the end. The ciphertext is then read off as:

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE
Reference(s) used for this question:
http://en.wikipedia.org/wiki/ROT13
http://en.wikipedia.org/wiki/Caesar_cipher
http://en.wikipedia.org/wiki/Polyalphabetic_cipher
http://en.wikipedia.org/wiki/Transposition_cipher

NEW QUESTION: 547
Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?
A. SESAME
B. RADIUS
C. KryptoKnight
D. TACACS+
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Secure European System for Applications in a Multi-vendor Environment (SESAME) was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support.
Reference:
TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 184.
ISC OIG Second Edition, Access Controls, Page 111

NEW QUESTION: 548
Which of the following is NOT a factor related to Access Control?
A. integrity
B. authenticity
C. confidentiality
D. availability
Answer: B (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
These factors cover the integrity, confidentiality, and availability components of information system security.
Integrity is important in access control as it relates to ensuring only authorized subjects can make changes to objects.
Authenticity is different from authentication. Authenticity pertains to something being authentic, not necessarily having a direct correlation to access control.
Confidentiality is pertinent to access control in that the access to sensitive information is controlled to protect confidentiality.

vailability is protected by access controls in that if an attacket attempts to disrupt availability they would first need access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

NEW QUESTION: 549
Related to information security, confidentiality is the opposite of which of the following?
A. closure
B. disclosure
C. disposal
D. disaster
Answer: (SHOW ANSWER)
Explanation/Reference:
Confidentiality is the opposite of disclosure.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 550
Which security model is based on the military classification of data and people with clearances?
A. Brewer-Nash model
B. Clark-Wilson model
C. Bell-LaPadula model
D. Biba model
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
The Bell-LaPadula model is a confidentiality model for information security based on the military classification of data, on people with clearances and data with a classification or sensitivity model. The Biba, Clark-Wilson and Brewer-Nash models are concerned with integrity.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 551
Which of the following logical access exposures INVOLVES CHANGING data before, or as it is entered into the computer?
A. Data diddling
B. Salami techniques
C. Trojan horses
D. Viruses
Answer: A (LEAVE A REPLY)

It involves changing data before , or as it is entered into the computer or in other words , it refers to the alteration of the existing data.
The other answers are incorrect because :
Salami techniques : A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed.
Trojan horses: A Trojan Horse is a program that is disguised as another program. Viruses:A Virus is a small application , or a string of code , that infects applications.
Reference: Shon Harris , AIO v3
Chapter - 11: Application and System Development, Page : 875-880
Chapter - 10: Law, Investigation and Ethics , Page : 758-759

NEW QUESTION: 552
During which phase of an IT system life cycle are security requirements developed?
A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation
Answer: (SHOW ANSWER)
Explanation/Reference:
The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems.
The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:
This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:
* Conduct the risk assessment and use the results to supplement the baseline security controls;
* Analyze security requirements;
* Perform functional and security testing;
* Prepare initial documents for system certification and accreditation; and
* Design security architecture.
Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.
Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:
Project initiation
Functional design analysis and planning
System design specifications
Software development
Installation
Maintenance support

Revision and replacement

According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase.

SDLC POSITIONING FROM NIST 800-64

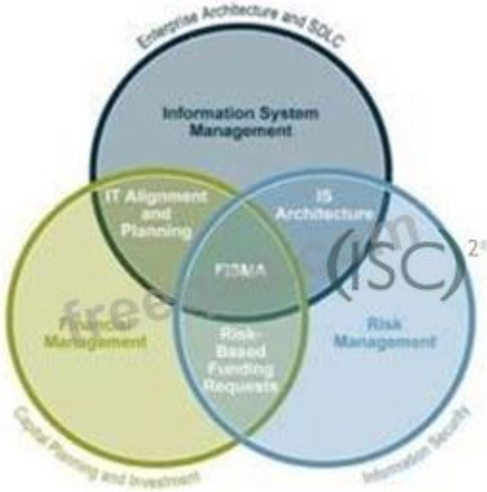


FIGURE 2-1. POSITIONING SECURITY CONSIDERATIONS

SDLC Positioning in the enterprise

Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency's vital business operations, their supporting assets, and existing interdependencies and relationships.

With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program's cost-effective performance as well as articulate its business impact and value to the agency.

SDLC OVERVIEW FROM NIST 800-64

SDLC Overview from NIST 800-64 Revision 2

NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at: http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf DISCUSSION:
Different sources present slightly different info as far as the phases names are concerned.
People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.
NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice.
Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:
The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.
At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.
By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.
NIST says:
NIST`s Information Technology Laboratory recently issued Special Publication (SP) 800-64, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.
I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956 and

NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf and
http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlc-system-development

NEW QUESTION: 553
Tripwire is a _____
A. Port Scanner
B. Polymorphic virus
C. Log analyzer
D. File Integrity Checker
E. Digital Certificate Company
Answer: D (LEAVE A REPLY)

NEW QUESTION: 554
Which of the following is used in database information security to hide information?
A. Inheritance
B. Polyinstantiation
C. Polymorphism
D. Delegation
Answer: (SHOW ANSWER)
Explanation/Reference:
Polyinstantiation enables a relation to contain multiple tuples with the same primary keys with each instance distinguished by a security level. When this information is inserted into a database, lower-level subjects need to be restricted from this information. Instead of just restricting access, another set of data is created to fool the lower-level subjects into thinking that the information actually means something else.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter
11: Application and System Development (page 727).

NEW QUESTION: 555
Which of the following layers provides end-to-end data transfer service?
A. Network Layer.
B. Data Link Layer.
C. Transport Layer.
D. Presentation Layer.
Answer: C (LEAVE A REPLY)
It is the Transport Layer that is responsible for reliable end-to-end data transfer between end systems.
The following answers are incorrect:

Network Layer. Is incorrect because the Network Layer is the OSI layer that is responsible for routing, switching, and subnetwork access across the entire OSI environment.
Data Link Layer. Is incorrect because the Data Link Layer is the serial communications path between nodes or devices without any intermediate switching nodes.
Presentation Layer. Is incorrect because the Presentation Layer is the OSI layer that determines how application information is represented (i.e., encoded) while in transit between two end systems.

NEW QUESTION: 556
During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?
A. Measurement of accuracy
B. Elapsed time for completion of critical tasks
C. Quantitatively measuring the results of the test
D. Evaluation of the observed test results
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
It is important to have ways to measure the success of the plan and tests against the stated objectives. Therefore, results must be quantitatively gauged as opposed to an evaluation based only on observation. Quantitatively measuring the results of the test involves a generic statement measuring all the activities performed during BCP, which gives the best assurance of an effective plan. Although choices A and B are also quantitative, they relate to specific areas, or an analysis of results from one viewpoint, namely the accuracy of the results and the elapsed time.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 5: Disaster Recovery and Business Continuity (page 269).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 557
Related to information security, integrity is the opposite of which of the following?
A. abstraction
B. alteration
C. accreditation
D. application
Answer: B (LEAVE A REPLY)

Section: Security Operation Adimnistration
Explanation/Reference:
Integrity is the opposite of "alteration."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 558
When considering an IT System Development Life-cycle, security should be:
A. Mostly considered during the initiation phase.
B. Mostly considered during the development phase.
C. Treated as an integral part of the overall system design.
D. Added once the design is completed.
Answer: (SHOW ANSWER)
Security must be considered in information system design. Experience has
shown it is very difficult to implement security measures properly and successfully after a system has been developed, so it should be integrated fully into the system life-cycle process. This includes establishing security policies, understanding the resulting security requirements, participating in the evaluation of security products, and finally in the engineering, design, implementation, and disposal of the system.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 7).

NEW QUESTION: 559
All following observations about IPSec are correct except:
A. Default Hashing protocols are HMAC-MD5 or HMAC-SHA-1
B. Default Encryption protocol is Cipher Block Chaining mode DES, but other algorithms like ECC (Elliptic curve cryptosystem) can be used
C. Support two communication modes - Tunnel mode and Transport mode
D. Works only with Secret Key Cryptography
Answer: (SHOW ANSWER)
Explanation/Reference:
Source: TIPTON, Harold F & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

NEW QUESTION: 560
Which of the following would best define a digital envelope?
A. A message that is encrypted and signed with a digital certificate.
B. A message that is signed with a secret key and encrypted with the sender's private key.
C. A message encrypted with a secret key attached with the message. The secret key is encrypted with the public key of the receiver.

D. A message that is encrypted with the recipient's public key and signed with the sender's private key.
Answer: C (LEAVE A REPLY)
A digital envelope for a recipient is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.
It consists of a hybrid encryption scheme in sealing a message, by encrypting the data and sending both it and a protected form of the key to the intended recipient, so that one else can open the message.
In PKCS #7, it means first encrypting the data using a symmetric encryption algorithm and a secret key, and then encrypting the secret key using an asymmetric encryption algorithm and the public key of the intended recipient.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 561
What is RAD?
A. A development methodology
B. A project management technique
C. A measure of system complexity
D. Risk-assessment diagramming
Answer: A (LEAVE A REPLY)
RAD stands for Rapid Application Development.
RAD is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.
RAD is a programming system that enables programmers to quickly build working programs.
In general, RAD systems provide a number of tools to help build graphical user interfaces that would normally take a large development effort.
Two of the most popular RAD systems for Windows are Visual Basic and Delphi. Historically, RAD systems have tended to emphasize reducing development time, sometimes at the expense of generating in-efficient executable code. Nowadays, though, many RAD systems produce extremely faster code that is optimized.
Conversely, many traditional programming environments now come with a number of visual tools to aid development. Therefore, the line between RAD systems and other development environments has become blurred.
Reference:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 307)
http://www.webopedia.com

NEW QUESTION: 562
Which of the following is NOT a compensating measure for access violations?
A. Backups
B. Business continuity planning

C. Insurance
D. Security awareness
Answer: D (LEAVE A REPLY)
Security awareness is a preventive measure, not a compensating measure for access violations. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 50).

NEW QUESTION: 563
Which of the following does NOT use token-passing?
A. ARCnet
B. FDDI
C. Token-ring
D. IEEE 802.3
Answer: D (LEAVE A REPLY)
Explanation/Reference:
IEEE 802.3 specifies the standard for Ethernet and uses CSMA/CD, not token-passing.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
104).

NEW QUESTION: 564
What mechanism does a system use to compare the security labels of a subject and an object?
A. Validation Module.
B. Reference Monitor.
C. Clearance Check.
D. Security Module.
Answer: B (LEAVE A REPLY)
Because the Reference Monitor is responsible for access control to the objects by the subjects it compares the security labels of a subject and an object.
According to the OIG: The reference monitor is an access control concept referring to an abstract machine that mediates all accesses to objects by subjects based on information in an access control database. The reference monitor must mediate all access, be protected from modification, be verifiable as correct, and must always be invoked. The reference monitor, in accordance with the security policy, controls the checks that are made in the access control database.
The following are incorrect:
Validation Module. A Validation Module is typically found in application source code and is used to validate data being inputted.
Clearance Check. Is a distractor, there is no such thing other than what someone would do when checking if someone is authorized to access a secure facility.

Security Module. Is typically a general purpose module that prerforms a variety of security related functions.
References:
OIG CBK, Security Architecture and Design (page 324)
AIO, 4th Edition, Security Architecture and Design, pp 328-328.
Wikipedia - http://en.wikipedia.org/wiki/Reference_monitor

NEW QUESTION: 565
Guards are appropriate whenever the function required by the security program involves which of the following?
A. The use of discriminating judgment
B. The use of physical force
C. The operation of access control devices
D. The need to detect unauthorized access
Answer: A (LEAVE A REPLY)
The use of discriminating judgment, a guard can make the determinations that hardware or other automated security devices cannot make due to its ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment. Guards are better at making value decisions at times of incidents. They are appropriate whenever immediate, discriminating judgment is required by the security entity.
The following answers are incorrect:
The use of physical force This is not the best answer. A guard provides discriminating judgment, and the ability to discern the need for physical force.
The operation of access control devices A guard is often uninvolved in the operations of an automated access control device such as a biometric reader, a smart lock, mantrap, etc.
The need to detect unauthorized access The primary function of a guard is not to detect unauthorized access, but to prevent unauthorized physical access attempts and may deter social engineering attempts.
The following reference(s) were/was used to create this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 339).
Source: ISC2 Offical Guide to the CBK page 288-289.

NEW QUESTION: 566
Which of the following is less likely to accompany a contingency plan, either within the plan itself or in the form of an appendix?
A. Contact information for all personnel.
B. Vendor contact information, including offsite storage and alternate site.

C. Equipment and system requirements lists of the hardware, software, firmware and other resources required to support system operations.
D. The Business Impact Analysis.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Why is this the correct answer? Simply because it is WRONG, you would have contact information for your emergency personnel within the plan but NOT for ALL of your personnel. Be careful of words such as ALL.
According to NIST's Special publication 800-34, contingency plan appendices provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the given system. Contact information for recovery team personnel (not all personnel) and for vendor should be included, as well as detailed system requirements to allow for supporting of system operations. The Business Impact Analysis (BIA) should also be included as an appendix for reference should the plan be activated.
Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

NEW QUESTION: 567
_____ is the most famous Unix password cracking tool.
A. CRACK
B. SNIFF
C. JOLT
D. ROOT
E. NMAP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 568
Which of the following concerning the Rijndael block cipher algorithm is false?
A. The design of Rijndael was strongly influenced by the design of the block cipher Square.
B. A total of 25 combinations of key length and block length are possible
C. Both block size and key length can be extended to multiples of 64 bits.
D. The cipher has a variable block length and key length.
Answer: (SHOW ANSWER)
The answer above is the correct answer because it is FALSE. Rijndael does
not support multiples of 64 bits but multiples of 32 bits in the range of 128 bits to 256 bits.
Key length could be 128, 160, 192, 224, and 256.
Both block length and key length can be extended very easily to multiples of 32 bits. For a
total combination of 25 different block and key size that are possible.
The Rijndael Cipher
Rijndael is a block cipher, designed by Joan Daemen and Vincent Rijmen as a candidate

algorithm for the Advanced Encryption Standard (AES) in the United States of America.
The cipher has a variable block length and key length.
Rijndael can be implemented very efficiently on a wide range of processors and in hardware.
The design of Rijndael was strongly influenced by the design of the block cipher Square.
The Advanced Encryption Standard (AES)
The Advanced Encryption Standard (AES) keys are defined to be either 128, 192, or 256 bits in accordance with the requirements of the AES.
The number of rounds, or iterations of the main algorithm, can vary from 10 to 14 within the Advanced Encryption Standard (AES) and is dependent on the block size and key length. 128 bits keys uses 10 rounds or encryptions, 192 bits keys uses 12 rounds of encryption, and 256 bits keys uses 14 rounds of encryption.
The low number of rounds has been one of the main criticisms of Rijndael, but if this ever becomes a problem the number of rounds can easily be increased at little extra cost performance wise by increasing the block size and key length.
Range of key and block lengths in Rijndael and AES Rijndael and AES differ only in the range of supported values for the block length and cipher key length.
For Rijndael, the block length and the key length can be independently specified to any multiple of 32 bits, with a minimum of 128 bits, and a maximum of 256 bits. The support for block and key lengths 160 and 224 bits was introduced in Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999 available at http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
AES fixes the block length to 128 bits, and supports key lengths of 128, 192 or 256 bits only.
Reference used for this question:
The Rijndael Page and http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf and FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.

NEW QUESTION: 569
Which of the following describes the major disadvantage of many Single Sign-On (SSO) implementations?
A. Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
B. The initial logon process is cumbersome to discourage potential intruders.
C. Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
D. Once a user obtains access to the system through the initial log-on, he has to logout from all other systems
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:

Single Sign-On is a distrubuted Access Control methodology where an individual only has to authenticate once and would have access to all primary and secondary network domains. The individual would not be required to re-authenticate when they needed additional resources. The security issue that this creates is if a fraudster is able to compromise those credential they too would have access to all the resources that account has access to.
All the other answers are incorrect as they are distractors.

NEW QUESTION: 570
Which of the following is related to physical security and is not considered a technical control?
A. Access control Mechanisms
B. Intrusion Detection Systems
C. Firewalls
D. Locks
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
All of the above are considered technical controls except for locks, which are physical controls.
Administrative, Technical, and Physical Security Controls
Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. For example, policy might dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information. Requiring that information be classified and the process to classify and review information classifications is another example of an administrative control. The organization security awareness program is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.
Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the C.I.A. of sensitive information. Examples include logical access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems.
Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control.
From the GIAC.ORG website

NEW QUESTION: 571

The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?

A. integrity and confidentiality.

B. confidentiality and availability.

C. integrity and availability.

D. none of the above.

Answer: C (LEAVE A REPLY)

Explanation/Reference:

TCSEC focused on confidentiality while ITSEC added integrity and availability as security goals.

The following answers are incorrect:

integrity and confidentiality. Is incorrect because TCSEC addressed confidentiality.

confidentiality and availability. Is incorrect because TCSEC addressed confidentiality.

none of the above. Is incorrect because ITSEC added integrity and availability as security goals.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 572

In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

A. Both client and server

B. The client's browser

C. The web server

D. The merchant's Certificate Server

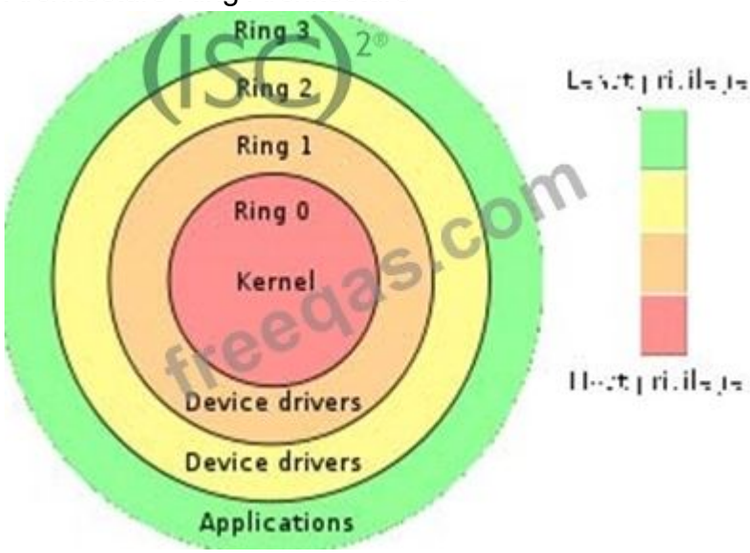
Answer: B (LEAVE A REPLY)

Section: Cryptography

Explanation/Reference:

Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant's public key and sent to the server. The fact that the master secret is generated by the client's browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client.

Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112). Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, page 569.

NEW QUESTION: 573
An Architecture where there are more than two execution domains or privilege levels is called:
A. Ring Architecture.
B. Ring Layering
C. Network Environment.
D. Security Models
Answer: A (LEAVE A REPLY)
In computer science, hierarchical protection domains, often called protection rings, are a mechanism to protect data and functionality from faults (fault tolerance) and malicious behavior (computer security). This approach is diametrically opposite to that of capability-based security.
Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level. Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.
Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring. Ring Architecture Ring Architecture


All of the other answers are incorrect because they are detractors.
References:

OIG CBK Security Architecture and Models (page 311) and https://en.wikipedia.org/wiki/Ring_%28computer_security%29

NEW QUESTION: 574
What is the effective key size of DES?
A. 56 bits
B. 64 bits
C. 128 bits
D. 1024 bits
Answer: A (LEAVE A REPLY)
Data Encryption Standard (DES) is a symmetric key algorithm. Originally developed by IBM, under project name Lucifer, this 128-bit algorithm was accepted by the NIST in 1974, but the total key size was reduced to 64 bits, 56 of which make up the effective key, plus and extra 8 bits for parity. It somehow became a national cryptographic standard in 1977, and an American National Standard Institute (ANSI) standard in 1978. DES was later replaced by the Advanced Encryption Standard (AES) by the NIST.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 525).

NEW QUESTION: 575
Passwords can be required to change monthly, quarterly, or at other intervals:
A. depending on the criticality of the information needing protection
B. depending on the criticality of the information needing protection and the password's frequency of use
C. depending on the password's frequency of use
D. not depending on the criticality of the information needing protection but depending on the password's frequency of use
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Passwords can be compromised and must be protected. In the ideal case, a password should only be used once. The changing of passwords can also fall between these two extremes. Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password's frequency of use. Obviously, the more times a password is used, the more chance there is of it being compromised.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36 & 37.

NEW QUESTION: 576
Which of the following are valid modes of operation? (Choose all that apply)
A. Multilevel mode
B. Restricted mode
C. Dedicated mode
D. Allowed mode

E. Access Mode

Answer: A,C (LEAVE A REPLY)

The four modes of operation include: dedicated mode, system-high mode, compartmented mode, and multilevel mode.

NEW QUESTION: 577

Secure Sockets Layer (SSL) uses a Message Authentication Code (MAC) for what purpose?

A. message non-repudiation.

B. message confidentiality.

C. message interleave checking.

D. message integrity.

Answer: (SHOW ANSWER)

A keyed hash also called a MAC (message authentication code) is used for integrity protection and authenticity.

In cryptography, a message authentication code (MAC) is a generated value used to authenticate a message. A MAC can be generated by HMAC or CBC-MAC methods. The MAC protects both a message's integrity (by ensuring that a different MAC will be produced if the message has changed) as well as its authenticity, because only someone who knows the secret key could have modified the message.

MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages.

HMAC When using HMAC the symmetric key of the sender would be concatenated (added at the end) with the message. The result of this process (message + secret key) would be put through a hashing algorithm, and the result would be a MAC value. This MAC value is then appended to the message being sent. If an enemy were to intercept this message and modify it, he would not have the necessary symmetric key to create a valid MAC value. The receiver would detect the tampering because the MAC value would not be valid on the receiving side.

CBC-MAC If a CBC-MAC is being used, the message is encrypted with a symmetric block cipher in CBC mode, and the output of the final block of ciphertext is used as the MAC. The sender does not send the encrypted version of the message, but instead sends the plaintext version and the MAC attached to the message. The receiver receives the plaintext message and encrypts it with the same symmetric block cipher in CBC mode and calculates an independent MAC value. The receiver compares the new MAC value with the MAC value sent with the message. This method does not use a hashing algorithm as does HMAC.

Cipher-Based Message Authentication Code (CMAC) Some security issues with CBC-MAC were found and they created Cipher-Based Message Authentication Code (CMAC) as a replacement. CMAC provides the same type of data origin authentication and integrity as CBC-MAC, but is more secure

mathematically. CMAC is a variation of CBC-MAC. It is approved to work with AES and Triple DES. HMAC, CBC-
MAC, and CMAC work higher in the network stack and can identify not only transmission errors (accidental), but also more nefarious modifications, as in an attacker messing with a message for her own benefit. This means all of these technologies can identify intentional, unauthorized modifications and accidental changes- three in one.
The following are all incorrect answers:
"Message non-repudiation" is incorrect.
Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
To repudiate means to deny. For many years, authorities have sought to make repudiation impossible in some situations. You might send registered mail, for example, so the recipient cannot deny that a letter was delivered. Similarly, a legal document typically requires witnesses to signing so that the person who signs cannot deny having done so.
On the Internet, a digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.
"Message confidentiality" is incorrect. The Message confidentiality is protected by encryption not by hashing algorithms.
"Message interleave checking" is incorrect. This is a nonsense term included as a distractor.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw-Hill. Kindle Edition.
and
http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
and
http://searchsecurity.techtarget.com/definition/nonrepudiation
and
https://en.wikipedia.org/wiki/Message_authentication_code

NEW QUESTION: 578
What algorithm has been selected as the AES algorithm, replacing the DES algorithm?
A. RC6
B. Twofish
C. Rijndael
D. Blowfish
Answer: (SHOW ANSWER)

On October 2, 2000, NIST announced the selection of the Rijndael Block Cipher, developed by the Belgian cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen, as the proposed AES algorithm. Twofish and RC6 were also candidates. Blowfish is also a symmetric algorithm but wasn't a finalist for a replacement for DES.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 152).

NEW QUESTION: 579
Which of the following are additional access control objectives?
A. Consistency and utility
B. Reliability and utility
C. Usefulness and utility
D. Convenience and utility
Answer: B (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Availability assures that a system's authorized users have timely and uninterrupted access to the information in the system. The additional access control objectives are reliability and utility. These and other related objectives flow from the organizational security policy. This policy is a high-level statement of management intent regarding the control of access to information and the personnel who are authorized to receive that information. Three things that must be considered for the planning and implementation of access control mechanisms are the threats to the system, the system's vulnerability to these threats, and the risk that the threat may materialize Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.

NEW QUESTION: 580
Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?
A. The Take-Grant model
B. The Biba integrity model
C. The Clark Wilson integrity model
D. The Bell-LaPadula integrity model
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation
Explanation/Reference:
The Clark Wilson integrity model addresses the three following integrity goals: 1) data is protected from modification by unauthorized users; 2) data is protected from unauthorized modification by authorized users; and 3) data is internally and externally consistent. It also defines a Constrained Data Item (CDI),

an Integrity Verification Procedure (IVP), a Transformation Procedure (TP) and an Unconstrained Data item. The Bell- LaPadula and Take-Grant models are not integrity models.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 205).

NEW QUESTION: 581
Attributable data should be:
A. always traced to individuals responsible for observing and recording the data
B. sometimes traced to individuals responsible for observing and recording the data
C. never traced to individuals responsible for observing and recording the data
D. often traced to individuals responsible for observing and recording the data
Answer: A (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
As per FDA data should be attributable, original, accurate, contemporaneous and legible. In an automated system attributability could be achieved by a computer system designed to identify individuals responsible for any input.
Source: U.S. Department of Health and Human Services, Food and Drug Administration, Guidance for Industry
- Computerized Systems Used in Clinical Trials, April 1999, page 1.

NEW QUESTION: 582
What is the name of the first mathematical model of a multi-level security policy used to define the concept of a secure state, the modes of access, and rules for granting access?
A. Clark and Wilson Model
B. Harrison-Ruzzo-Ullman Model
C. Rivest and Shamir Model
D. Bell-LaPadula Model
Answer: (SHOW ANSWER)
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 583
Which ISO/OSI layer establishes the communications link between individual devices over a physical link or channel?
A. Transport layer
B. Network layer
C. Data link layer
D. Physical layer
Answer: C (LEAVE A REPLY)

The data link layer (layer 2) establishes the communications link between individual devices over a physical link or channel. It also ensures that messages are delivered to the proper device and translates the messages from layers above into bits for the physical layer (layer 1) to transmit. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 83).

NEW QUESTION: 584
Which of the following enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks?
A. Risk assessment
B. Residual risks
C. Security controls
D. Business units
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The risk assessment is critical because it enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks. The risk management process includes the risk assessment and determination of suitable technical, management, and operational security controls based on the level of threat the risk imposes. Business units should be included in this process.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 7).

NEW QUESTION: 585
Which of the following standards concerns digital certificates?
A. X.400
B. X.25
C. X.509
D. X.75
Answer: C (LEAVE A REPLY)
X.509 is used in digital certificates. X.400 is used in e-mail as a message handling protocol. X.25 is a standard for the network and data link levels of a communication network and X.75 is a standard defining ways of connecting two X.25 networks. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 164).

NEW QUESTION: 586
Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?
A. Using a TACACS+ server.

B. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
C. Setting modem ring count to at least 5.
D. Only attaching modems to non-networked hosts.
Answer: B (LEAVE A REPLY)
Containing the dial-up problem is conceptually easy: by installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall, any access to internal resources through the RAS can be filtered as would any other connection coming from the Internet.
The use of a TACACS+ Server by itself cannot eliminate hacking.
Setting a modem ring count to 5 may help in defeating war-dialing hackers who look for modem by dialing long series of numbers.
Attaching modems only to non-networked hosts is not practical and would not prevent these hosts from being hacked.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2: Hackers.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 587
What can be defined as: It confirms that users' needs have been met by the supplied solution ?
A. Accreditation
B. Certification
C. Assurance
D. Acceptance
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Acceptance confirms that users' needs have been met by the supplied solution. Verification and Validation informs Acceptance by establishing the evidence - set against acceptance criteria - to determine if the solution meets the users' needs. Acceptance should also explicitly address any integration or interoperability requirements involving other equipment or systems. To enable acceptance every user and system requirement must have a 'testable' characteristic.
Accreditation is the formal acceptance of security, adequacy, authorization for operation and acceptance of existing risk. Accreditation is the formal declaration by a Designated Approving Authority (DAA) that an

IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.
Certification is the formal testing of security safeguards and assurance is the degree of confidence that the implemented security measures work as intended. The certification is a Comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified ecurity requirements.
Assurance is the descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the Security Targets (ST) and Protection Profiles (PP), respectively.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 4, August 1999.
and
Official ISC2 Guide to the CISSP CBK, Second Edition, on page 211.
and
http://www.aof.mod.uk/aofcontent/tactical/randa/content/randaintroduction.htm

NEW QUESTION: 588
Which of the following is less likely to be included in the change control sub-phase of the maintenance phase of a software product?
A. Estimating the cost of the changes requested
B. Recreating and analyzing the problem
C. Determining the interface that is presented to the user
D. Establishing the priorities of requests
Answer: D (LEAVE A REPLY)
Change control sub-phase includes Recreating and analyzing the problem,
Determining the interface that is presented to the user, and Establishing the priorities of requests.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).

NEW QUESTION: 589
Why would a memory dump be admissible as evidence in court?
A. Because it is used to demonstrate the truth of the contents.
B. Because it is used to identify the state of the system.
C. Because the state of the memory cannot be used as evidence.
D. Because of the exclusionary rule.
Answer: B (LEAVE A REPLY)

A memory dump can be admitted as evidence if it acts merely as a statement of fact. A system dump is not considered hearsay because it is used to identify the state of the system, not the truth of the contents. The exclusionary rule mentions that evidence must be gathered legally or it can't be used. This choice is a distracter.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 187).

NEW QUESTION: 590
What is the goal of the Maintenance phase in a common development process of a security policy?
A. to review the document on the specified review date
B. publication within the organization
C. to write a proposal to management that states the objectives of the policy
D. to present the document to an approving body
Answer: A (LEAVE A REPLY)
Explanation/Reference:
"publication within the organization" is the goal of the Publication Phase "write a proposal to management that states the objectives of the policy" is part of Initial and Evaluation Phase "Present the document to an approving body" is part of Approval Phase.
Reference: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.
Also: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 286).

NEW QUESTION: 591
Which of the following best ensures accountability of users for the actions taken within a system or domain?
A. Identification
B. Authentication
C. Authorization
D. Credentials
Answer: (SHOW ANSWER)
Details:
The only way to ensure accountability is if the subject is uniquely identified and authenticated. Identification alone does not provide proof the user is who they claim to be.
After showing proper credentials, a user is authorized access to resources.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 126).

NEW QUESTION: 592

Which of the following is a device that is used to regenerate or replicate the received signals?

A. Bridge

B. Router

C. Repeater

D. Brouter

Answer: (SHOW ANSWER)

Repeaters offer the simplest form of connectivity. They regenerate received electrical signals at their original strength between cable segments. Bridges are devices used to connect similar or dissimilar LANs together to form an extended LAN. Routers provide packet routing between network segments. Brouter are devices that combine router and bridge functionality. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7: Telecommunications and Network Security (page 397).

NEW QUESTION: 593

What can be described as a measure of the magnitude of loss or impact on the value of an asset?

A. Probability

B. Exposure factor

C. Vulnerability

D. Threat

Answer: (SHOW ANSWER)

Explanation/Reference:

The exposure factor is a measure of the magnitude of loss or impact on the value of an asset.

The probability is the chance or likelihood, in a finite sample, that an event will occur or that a specific loss value may be attained should the event occur.

A vulnerability is the absence or weakness of a risk-reducing safeguard.

A threat is event, the occurrence of which could have an undesired impact.

Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 3, August 1999.

NEW QUESTION: 594

In the CIA triad, what does the letter A stand for?

A. Auditability

B. Accountability

C. Availability

D. Authentication

Answer: (SHOW ANSWER)

Explanation/Reference:

The CIA triad stands for Confidentiality, Integrity and Availability.

NEW QUESTION: 595

Which of the following was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN?

A. DHCP

B. BootP

C. DNS

D. ARP

Answer: B (LEAVE A REPLY)

BootP was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN. Over time, it has expanded to allow centralized configuration of many aspects of a host's identity and behavior on the network. Note that DHCP, more complex, has replaced BootP over time. Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4: Sockets and Services from a Security Viewpoint.

NEW QUESTION: 596

What does the (star) integrity axiom mean in the Biba model?

A. No read up

B. No write down

C. No read down

D. No write up

Answer: D (LEAVE A REPLY)

The (star) integrity axiom of the Biba access control model states that an object at one level of integrity is not permitted to modify an object of a higher level of integrity (no write up). Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

NEW QUESTION: 597

Which of the following is true of network security?

A. A firewall is a not a necessity in today's connected world.

B. A firewall is a necessity in today's connected world.

C. A whitewall is a necessity in today's connected world.

D. A black firewall is a necessity in today's connected world.

Answer: B (LEAVE A REPLY)

Commercial firewalls are a dime-a-dozen in todays world. Black firewall and whitewall are just distracters.

NEW QUESTION: 598

Which of the following is used to find the Media Access Control address (MAC) that matches with a known Internet Protocol (IP) address?

A. Address Resolution Protocol (ARP).

B. Reverse Address Resolution Protocol (RARP).

C. Internet Control Message protocol (ICMP).

D. User Datagram Protocol (UDP).

Answer: (SHOW ANSWER)
ARP is used to find the Media Access Control address (MAC) that matches with a known Internet Protocol (IP) address.
The Address Resolution Protocol (ARP) is a computer networking protocol for determining a network host's link layer or hardware address when only its Internet Layer (IP) or Network Layer address is known
Reverse Address Resolution Protocol (RARP) is used to find the IP address that matches an Ethernet address.
ICMP is a management protocol and messaging service provider for IP (e.g. PING).
UDP runs over IP. It is a best effort protocol that offers no reliability. UDS is used for application such as streaming media, voice over IP, the DNS protocol, as well as the Simple Network Management Protocol (SNMP).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.
also see:
http://en.wikipedia.org/wiki/Address_resolution_protocol

NEW QUESTION: 599
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?
A. Limiting the local access of operations personnel
B. Job rotation of operations personnel
C. Management monitoring of audit logs
D. Enforcing regular password changes
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.
Management monitoring of audit logs is a detective control and it would not prevent collusion.
Changing passwords regularly would not prevent such attack.
This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 600
Which of the following is most appropriate to notify an external user that session monitoring is being conducted?
A. Logon Banners
B. Wall poster

C. Employee Handbook
D. Written agreement
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Banners at the log-on time should be used to notify external users of any monitoring that is being conducted. A good banner will give you a better legal stand and also makes it obvious the user was warned about who should access the system and if it is an unauthorized user then he is fully aware of trespassing.
This is a tricky question, the keyword in the question is External user.
There are two possible answers based on how the question is presented, this question could either apply to internal users or ANY anonymous user.
Internal users should always have a written agreement first, then logon banners serve as a constant reminder.
Anonymous users, such as those logging into a web site, ftp server or even a mail server; their only notification system is the use of a logon banner.
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 50.
and
Shon Harris, CISSP All-in-one, 5th edition, pg 873

NEW QUESTION: 601
Which of the following is NOT a proper component of Media Viability Controls?
A. Storage
B. Writing
C. Handling
D. Marking
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Media Viability Controls include marking, handling and storage.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 231.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine

here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 602
Which element must computer evidence have to be admissible in court?
A. It must be relevant.
B. It must be annotated.
C. It must be printed.
D. It must contain source code.
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 603
Knowledge-based Intrusion Detection Systems (IDS) are more common than:
A. Network-based IDS
B. Host-based IDS
C. Behavior-based IDS
D. Application-Based IDS
Answer: (SHOW ANSWER)
Explanation/Reference:
Knowledge-based IDS are more common than behavior-based ID systems.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 63.
Application-Based IDS - "a subset of HIDS that analyze what's going on in an application using the transaction log files of the application." Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87
Host-Based IDS - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host." Source: Official ISC2 Guide to the CISSP CBK - p. 197
Network-Based IDS - "a network device, or dedicated system attached to the network, that monitors traffic traversing the network segment for which it is integrated." Source: Official ISC2 Guide to the CISSP CBK - p. 196
CISSP for dummies a book that we recommend for a quick overview of the 10 domains has nice and concise coverage of the subject:
Intrusion detection is defined as real-time monitoring and analysis of network activity and data for potential vulnerabilities and attacks in progress. One major limitation of current intrusion detection system (IDS) technologies is the requirement to filter false alarms lest the operator (system or security administrator) be overwhelmed with data. IDSes are classified in many different ways, including active and passive, network- based and host-based, and knowledge-based and behavior-based:

Active and passive IDS

An active IDS (now more commonly known as an intrusion prevention system - IPS) is a system that's configured to automatically block suspected attacks in progress without any intervention required by an operator. IPS has the advantage of providing real-time corrective action in response to an attack but has many disadvantages as well. An IPS must be placed in-line along a network boundary; thus, the IPS itself is susceptible to attack. Also, if false alarms and legitimate traffic haven't been properly identified and filtered, authorized users and applications may be improperly denied access. Finally, the IPS itself may be used to effect a Denial of Service (DoS) attack by intentionally flooding the system with alarms that cause it to block connections until no connections or bandwidth are available.

A passive IDS is a system that's configured only to monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. It isn't capable of performing any protective or corrective functions on its own. The major advantages of passive IDSes are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.

Network-based and host-based IDS

A network-based IDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

A host-based IDS requires small programs (or agents) to be installed on individual systems to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host-based IDS can only monitor the individual host systems on which the agents are installed; it doesn't monitor the entire network.

Knowledge-based and behavior-based IDS

A knowledge-based (or signature-based) IDS references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge-based IDS is currently more common than behavior-based IDS.

Advantages of knowledge-based systems include the following:

It has lower false alarm rates than behavior-based IDS.

Alarms are more standardized and more easily understood than behavior-based IDS.

Disadvantages of knowledge-based systems include these:

Signature database must be continually updated and maintained.

New, unique, or original attacks may not be detected or may be improperly classified.

A behavior-based (or statistical anomaly-based) IDS references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.

Advantages of behavior-based systems include that they

Dynamically adapt to new, unique, or original attacks.

Are less dependent on identifying specific operating system vulnerabilities.

Disadvantages of behavior-based systems include

Higher false alarm rates than knowledge-based IDSes.

Usage patterns that may change often and may not be static enough to implement an effective behavior-based IDS.

NEW QUESTION: 604
Which of the following is the BEST way to detect software license violations?
A. Implementing a corporate policy on copyright infringements and software use.
B. Requiring that all PCs be diskless workstations.
C. Installing metering software on the LAN so applications can be accessed through the metered software.
D. Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.
Answer: D (LEAVE A REPLY)
The best way to prevent and detect software license violations is to regularly scan used PCs, either from the LAN or directly, to ensure that unauthorized copies of software have not been loaded on the PC. Other options are not detective.
A corporate policy is not necessarily enforced and followed by all employees.
Software can be installed from other means than floppies or CD-ROMs (from a LAN or even downloaded from the Internet) and software metering only concerns applications that are registered. Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 108).

NEW QUESTION: 605
Heuristic scanning in antivirus software is designed to catch 100% of all known and unknownvirus technologies.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 606
The standard of _____ states that a certain level of integrity and information protection levels will be maintained.
A. Due Diligence
B. Due Care
C. Due Process
D. BSO 1799
Answer: B (LEAVE A REPLY)

NEW QUESTION: 607
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:
A. through access control mechanisms that require identification and authentication and through the audit function.

B. through logical or technical controls involving the restriction of access to systems and the protection of information.
C. through logical or technical controls but not involving the restriction of access to systems and the protection of information.
D. through access control mechanisms that do not require identification and authentication and do not operate through the audit function.
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 608
_____ states that users should only be given enough access to accomplish their jobs.
A. Due Diligence
B. Concept of Least Privilege
C. Separation of Duties
D. All of the listed items are correct
Answer: (SHOW ANSWER)

NEW QUESTION: 609
Which of the following access control models introduces user security clearance and data classification?
A. Role-based access control
B. Discretionary access control
C. Non-discretionary access control
D. Mandatory access control
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The mandatory access control model is based on a security label system. Users are given a security clearance and data is classified. The classification is stored in the security labels of the resources. Classification labels specify the level of trust a user must have to access a certain file.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4:
Access Control (Page 154).

NEW QUESTION: 610
What is the main problem of the renewal of a root CA certificate?
A. It requires key recovery of all end user keys
B. It requires the authentic distribution of the new root CA certificate to all PKI participants
C. It requires the collection of the old root CA certificates from all the users
D. It requires issuance of the new root CA certificate
Answer: B (LEAVE A REPLY)
Explanation/Reference:
The main task here is the authentic distribution of the new root CA certificate as new trust anchor to all the PKI participants (e.g. the users).
In some of the rollover-scenarios there is no automatic way, often explicit assignment of trust from each user is needed, which could be very costly.
Other methods make use of the old root CA certificate for automatic trust establishment (see PKIX-reference), but these solutions works only well for scenarios with currently valid root CA certificates (and not for emergency cases e.g. compromise of the current root CA certificate).
The rollover of the root CA certificate is a specific and delicate problem and therefore are often ignored during PKI deployment.
Reference: Camphausen, I.; Petersen, H.; Stark, C.: Konzepte zum Root CA Zertifikatswechsel, conference Enterprise Security 2002, March 26-27, 2002, Paderborn; RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

NEW QUESTION: 611
In non-discretionary access control using Role Based Access Control (RBAC), a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on:
A. The societies role in the organization
B. The individual's role in the organization
C. The group-dynamics as they relate to the individual's role in the organization
D. The group-dynamics as they relate to the master-slave role in the organization
Answer: B (LEAVE A REPLY)
Explanation/Reference:
In Non-Discretionary Access Control, when Role Based Access Control is being used, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual's role in the organization.
Reference(S) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 612
In addition to the accuracy of the biometric systems, there are other factors that must also be considered:
A. These factors include the enrollment time and the throughput rate, but not acceptability.

B. These factors do not include the enrollment time, the throughput rate, and acceptability.
C. These factors include the enrollment time, the throughput rate, and acceptability.
D. These factors include the enrollment time, but not the throughput rate, neither the acceptability.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
In addition to the accuracy of the biometric systems, there are other factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability.
Enrollment time is the time it takes to initially "register" with a system by providing samples of the biometric characteristic to be evaluated. An acceptable enrollment time is around two minutes.
For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases.
In finger-scan technology, a full fingerprint is not stored-the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template.
Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37 & 38.

NEW QUESTION: 613
Which of the following is a device that is used to regenerate or replicate the received signals?
A. Bridge
B. Router
C. Repeater
D. Brouter
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Repeaters offer the simplest form of connectivity. They regenerate received electrical signals at their original strength between cable segments. Bridges are devices used to connect similar or dissimilar LANs together to form an extended LAN. Routers provide packet routing between network segments. Brouter are devices that combine router and bridge functionality.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7:
Telecommunications and Network Security (page 397).

NEW QUESTION: 614
Which of the following describes the major disadvantage of many Single Sign-On (SSO) implementations?

A. Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
B. The initial logon process is cumbersome to discourage potential intruders.
C. Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
D. Once a user obtains access to the system through the initial log-on, he has to logout from all other systems
Answer: A (LEAVE A REPLY)
Single Sign-On is a distrubuted Access Control methodology where an individual only has to authenticate once and would have access to all primary and secondary network domains. The individual would not be required to re-authenticate when they needed additional resources. The security issue that this creates is if a fraudster is able to compromise those credential they too would have access to all the resources that account has access to.
All the other answers are incorrect as they are distractors.

NEW QUESTION: 615
Devices that supply power when the commercial utility power system fails are called which of the following?
A. power conditioners
B. uninterruptible power supplies
C. power filters
D. power dividers
Answer: B (LEAVE A REPLY)
Explanation/Reference:
From Shon Harris AIO Fifth Edition:
Protecting power can be done in three ways: through UPSs, power line conditioners, and backup sources.
UPSs use battery packs that range in size and capacity. A UPS can be online or standby.
Online UPS systems use AC line voltage to charge a bank of batteries. When in use, the UPS has an inverter that changes the DC output from the batteries into the required AC form and that regulates the voltage as it powers computer devices.
Online UPS systems have the normal primary power passing through them day in and day out. They constantly provide power from their own inverters, even when the electric power is in proper use. Since the environment's electricity passes through this type of UPS all the time, the UPS device is able to quickly detect when a power failure takes place. An online UPS can provide the necessary electricity and picks up the load after a power failure much more quickly than a standby UPS.
Standby UPS devices stay inactive until a power line fails. The system has sensors that detect a power failure, and the load is switched to the battery pack. The switch to the battery pack is what causes the small delay in electricity being provided.
So an online UPS picks up the load much more quickly than a standby UPS, but costs more of course.

NEW QUESTION: 616
Frame relay uses a public switched network to provide:
A. Local Area Network (LAN) connectivity.
B. Metropolitan Area Network (MAN) connectivity.
C. Wide Area Network (WAN) connectivity.
D. World Area Network (WAN) connectivity.
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Frame relay uses a public switched network to provide Wide Area Network (WAN) connectivity.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 73.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 617
CORRECT TEXT
Attackers have been known to search through company trash bins in order to collect potentially useful information. This method of attack is known as _____.
Answer:
diving

NEW QUESTION: 618
Which of the following describes the major disadvantage of many Single Sign-On (SSO) implementations?
A. Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
B. The initial logon process is cumbersome to discourage potential intruders.
C. Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
D. Once a user obtains access to the system through the initial log-on, he has to logout from all other systems
Answer: A (LEAVE A REPLY)
Explanation/Reference:

Single Sign-On is a distrubuted Access Control methodology where an individual only has to authenticate once and would have access to all primary and secondary network domains. The individual would not be required to re-authenticate when they needed additional resources. The security issue that this creates is if a fraudster is able to compromise those credential they too would have access to all the resources that account has access to.
All the other answers are incorrect as they are distractors.

NEW QUESTION: 619
Which of the following would be used to implement Mandatory Access Control (MAC)?
A. Clark-Wilson Access Control
B. Role-based access control
C. Lattice-based access control
D. User dictated access control
Answer: (SHOW ANSWER)
The lattice is a mechanism use to implement Mandatory Access Control (MAC)
Under Mandatory Access Control (MAC) you have: Mandatory Access Control
Under Non Discretionary Access Control (NDAC) you have: Rule-Based Access Control Role-Based Access Control
Under Discretionary Access Control (DAC) you have: Discretionary Access Control
The Lattice Based Access Control is a type of access control used to implement other access control method. A lattice is an ordered list of elements that has a least upper bound and a most lower bound. The lattice can be used for MAC, DAC, Integrity level, File Permission, and more
For example in the case of MAC, if we look at common government classifications, we have the following:
TOP SECRET SECRET ----------I am the user at secret CONFIDENTIAL SENSITIVE BUT UNCLASSIFIED UNCLASSIFIED
If you look at the diagram above where I am a user at SECRET it means that I can access document at lower classification but not document at TOP SECRET. The lattice is a list of ORDERED ELEMENT, in this case the ordered elements are classification levels. My least upper bound is SECRET and my most lower bound is UNCLASSIFIED.
However the lattice could also be used for Integrity Levels such as:
VERY HIGH HIGH MEDIUM ----------I am a user, process, application at the medium level LOW VERY LOW In the case of of Integrity levels you have to think about TRUST. Of course if I take for example the the VISTA operating system which is based on Biba then Integrity Levels would be used. As a user having access to the system I cannot tell a process running with administrative privilege what to do. Else any users on the system could take control of the system by getting highly privilege process to do things on their behalf. So no read down would be allowed in this case and this is an example of the Biba model.
Last but not least the lattice could be use for file permissions:
RWX RW ---------User at this level R
If I am a user with READ and WRITE (RW) access privilege then I cannot execute the file because I do not have execute permission which is the X under linux and UNIX.

Many people confuse the Lattice Model and many books says MAC = LATTICE, however the lattice can be use for other purposes.
There is also Role Based Access Control (RBAC) that exists out there. It COULD be used to simulate MAC but it is not MAC as it does not make use of Label on objects indicating sensitivity and categories. MAC also require a clearance that dominates the object.
You can get more info about RBAC at:http://csrc.nist.gov/groups/SNS/rbac/faq.html#03
Also note that many book uses the same acronym for Role Based Access Control and Rule Based Access Control which is RBAC, this can be confusing.
The proper way of writing the acronym for Rule Based Access Control is RuBAC, unfortunately it is not commonly used.
References:
There is a great article on technet that talks about the lattice in VISTA:
http://blogs.technet.com/b/steriley/archive/2006/07/21/442870.aspx
also see: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33). and
http://www.microsoft-watch.com/content/vista/gaging_vistas_integrity.html

NEW QUESTION: 620
Which of the following statements pertaining to firewalls is incorrect?
A. Firewalls create bottlenecks between the internal and external network.
B. Firewalls allow for centralization of security services in machines optimized and dedicated to the task.
C. Firewalls protect a network at all layers of the OSI models.
D. Firewalls are used to create security checkpoints at the boundaries of private networks.
Answer: (SHOW ANSWER)
Firewalls can protect a network at multiple layers of the OSI models, however most of the firewalls do not have the ability to monitor the payload of the packets and see if an application level attack is taking place.
Today there are a new breed of firewall called Unified Threat Managers or UTM. They are a collection of products on a single computer and not necessarily a typical firewall. A UTM can address all of the layers but typically a firewall cannot.
Firewalls are security checkpoints at the boundaries of internal networks through which every packet must pass and be inspected, hence they create bottlenecks between the internal and external networks. But since external connections are relatively slow compared to modern computers, the latency caused by this bottleneck can almost be transparent.
By implementing the concept of border security, they centralize security services in machines optimized and dedicated to the task, thus relieving the other hosts on the network from that function.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.

NEW QUESTION: 621
Another name for a VPN is a:

A. tunnel
B. one-time password
C. pipeline
D. bypass
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 622
The Terminal Access Controller Access Control System (TACACS) employs which of the following?
A. a user ID and static password for network access
B. a user ID and dynamic password for network access
C. a user ID and symmetric password for network access
D. a user ID and asymmetric password for network access
Answer: (SHOW ANSWER)
Explanation/Reference:
For networked applications, the Terminal Access Controller Access Control System (TACACS) employs a user ID and a static password for network access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 44.

NEW QUESTION: 623
The type of discretionary access control (DAC) that is based on an individual's identity is also called:
A. Identity-based Access control
B. Rule-based Access control
C. Non-Discretionary Access Control
D. Lattice-based Access control
Answer: (SHOW ANSWER)
An identity-based access control is a type of Discretionary Access Control
(DAC) that is based on an individual's identity.
DAC is good for low level security environment. The owner of the file decides who has access to the file.
If a user creates a file, he is the owner of that file. An identifier for this user is placed in the file header and/or in an access control matrix within the operating system.
Ownership might also be granted to a specific individual. For example, a manager for a certain department might be made the owner of the files and resources within her department. A system that uses discretionary access control (DAC) enables the owner of the resource to specify which subjects can access specific resources.
This model is called discretionary because the control of access is based on the discretion of the owner. Many times department managers, or business unit managers , are the

owners of the data within their specific department. Being the owner, they can specify who should have access and who should not.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 220). McGraw-Hill . Kindle Edition.

NEW QUESTION: 624
What key size is used by the Clipper Chip?
A. 40 bits
B. 56 bits
C. 64 bits
D. 80 bits
Answer: D (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
The Clipper Chip is a NSA designed tamperproof chip for encrypting data and it uses the SkipJack algorithm.
Each Clipper Chip has a unique serial number and a copy of the unit key is stored in the database under this serial number. The sending Clipper Chip generates and sends a Law Enforcement Access Field (LEAF) value included in the transmitted message. It is based on a 80-bit key and a 16-bit checksum.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 1).

NEW QUESTION: 625
All following observations about IPSec are correct except:
A. Default Hashing protocols are HMAC-MD5 or HMAC-SHA-1
B. Default Encryption protocol is Cipher Block Chaining mode DES, but other algorithms like ECC (Elliptic curve cryptosystem) can be used
C. Support two communication modes - Tunnel mode and Transport mode
D. Works only with Secret Key Cryptography
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

NEW QUESTION: 626
The information security staff's participation in which of the following system development life cycle phases provides maximum benefit to the organization?
A. project initiation and planning phase
B. system design specifications phase
C. development and documentation phase

D. in parallel with every phase throughout the project
Answer: D (LEAVE A REPLY)
Explanation/Reference:
The other answers are not correct because:
You are always looking for the "best" answer. While each of the answers listed here could be considered correct in that each of them require input from the security staff, the best answer is for that input to happen at all phases of the project.
Reference:
Official ISC2 Guide page: 556
All in One Third Edition page: 832 - 833

NEW QUESTION: 627
Which auditing practice relates to the controlling of hardware, software, firmware, and documentation to insure it has not been improperly modified?
A. System Control
B. Configuration Control
C. Consequence Assessment
D. Certification / Accreditation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 628
Which of the following is best defined as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in a system?
A. Fail proof
B. Fail soft
C. Fail safe
D. Fail Over
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
NOTE: This question is referring to a system which is Logical/Technical, so it is in the context of a system that you must choose the right answer. This is very important to read the question carefully and to identify the context whether it is in the Physical world or in the Technical/Logical world.
RFC 2828 (Internet Security Glossary) defines fail safe as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system.
A secure state means in the Logical/Technical world that no access would be granted or no packets would be allowed to flow through the system inspecting the packets such as a firewall for example.
If the question would have made reference to a building or something specific to the Physical world then the answer would have been different. In the Physical World everything becomes open and full access would be granted. See the valid choices below for the Physical context.

Fail-safe in the physical security world is when doors are unlocked automatically in case of emergency. Used in environment where humans work around. As human safety is prime concern during Fire or other hazards.
The following were all wrong choices:
Fail-secure in the physical security world is when doors are locked automatically in case of emergency. Can be in an area like Cash Locker Room provided there should be alternative manually operated exit door in case of emergency.
Fail soft is selective termination of affected non-essential system functions and processes when a failure occurs or is detected in the system.
Fail Over is a redundancy mechanism and does not apply to this question.
There is a great post within the CCCure Forums on this specific Q:
saintrockz who is a long term contributor to the forums did outstanding research and you have the results below. The CCCure forum is a gold mine where thousands of Qs related to the CBK have been discussed.
According to the Official ISC2 Study Guide (OIG):
Fault Tolerance is defined as built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults. It means a system can operate in the presence of hardware component failures. A single component failure in a fault-tolerant system will not cause a system interruption because the alternate component will take over the task transparently. As the cost of components continues to drop, and the demand for system availability increases, many non-fault-tolerant systems have redundancy built-in at the subsystem level. As a result, many non-fault-tolerant systems can tolerate hardware faults - consequently, the line between a fault-tolerant system and a non-fault-tolerant system becomes increasingly blurred.
According to Common Criteria:
Fail Secure - Failure with preservation of secure state, which requires that the TSF (TOE security functions) preserve a secure state in the face of the identified failures.
Acc. to The CISSP Prep Guide, Gold Ed.:
Fail over - When one system/application fails, operations will automatically switch to the backup system.
Fail safe - Pertaining to the automatic protection of programs and/or processing systems to maintain safety when a hardware or software failure is detected in a system.
Fail secure - The system preserves a secure state during and after identified failures occur.
Fail soft - Pertaining to the selective termination of affected non-essential processing when a hardware or software failure is detected in a system.
Acc. to CISSP for Dummies:
Fail closed - A control failure that results all accesses blocked.
Fail open - A control failure that results in all accesses permitted.
Failover - A failure mode where, if a hardware or software failure is detected, the system automatically transfers processing to a hot backup component, such as a clustered server.
Fail-safe - A failure mode where, if a hardware or software failure is detected, program execution is terminated, and the system is protected from compromise.

Fail-soft (or resilient) - A failure mode where, if a hardware or software failure is detected, certain, noncritical processing is terminated, and the computer or network continues to function in a degraded mode.
Fault-tolerant - A system that continues to operate following failure of a computer or network component.
It's good to differentiate this concept in Physical Security as well:
Fail-safe
* Door defaults to being unlocked
* Dictated by fire codes
Fail-secure
* Door defaults to being locked
Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 629
When a possible intrusion into your organization's information system has been detected, which of the following actions should be performed first?
A. Eliminate all means of intruder access.
B. Contain the intrusion.
C. Determine to what extent systems and data are compromised.
D. Communicate with relevant parties.
Answer: C (LEAVE A REPLY)
Once an intrusion into your organization's information system has been detected, the first action that needs to be performed is determining to what extent systems and data are compromised (if they really are), and then take action.
This is the good old saying: "Do not cry wolf until you know there is a wolf for sure" Sometimes it smells like a wolf, it looks like a wolf, but it may not be a wolf. Technical problems or bad hardware might cause problems that looks like an intrusion even thou it might not be. You must make sure that a crime has in fact been committed before implementing your reaction plan.
Information, as collected and interpreted through analysis, is key to your decisions and actions while executing response procedures. This first analysis will provide information such as what attacks were used, what systems and data were accessed by the intruder, what the intruder did after obtaining access and what the intruder is currently doing (if the intrusion has not been contained).
The next step is to communicate with relevant parties who need to be made aware of the intrusion in a timely manner so they can fulfil their responsibilities.
Step three is concerned with collecting and protecting all information about the compromised systems and causes of the intrusion. It must be carefully collected, labelled, catalogued, and securely stored.
Containing the intrusion, where tactical actions are performed to stop the intruder's access, limit the extent of the intrusion, and prevent the intruder from causing further damage, comes next.
Since it is more a long-term goal, eliminating all means of intruder access can only be achieved last, by implementing an ongoing security improvement process.
Reference used for this question:

ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 271-289).

NEW QUESTION: 630
What size is an MD5 message digest (hash)?
A. 128 bits
B. 160 bits
C. 256 bits
D. 128 bytes
Answer: A (LEAVE A REPLY)
Explanation/Reference:
MD5 is a one-way hash function producing a 128-bit message digest from the input message, through 4 rounds of transformation. MD5 is specified as an Internet Standard (RFC1312).
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 631
The standard server port number for HTTP is which of the following?
A. 81
B. 80
C. 8080
D. 8180
Answer: B (LEAVE A REPLY)
HTTP is Port 80.
Reference: MAIWALD, Eric, Network Security: A Beginner's Guide, McGraw-Hill/Osborne Media, 2001, page 135.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 632
Which of the following BEST describes a function relying on a shared secret key that is used along with a hashing algorithm to verify the integrity of the communication content as well as the sender?
A. Message Authentication Code - MAC
B. PAM - Pluggable Authentication Module
C. NAM - Negative Acknowledgement Message

D. Digital Signature Certificate

Answer: A (LEAVE A REPLY)

Section: Cryptography

Explanation/Reference:

The purpose of a message authentication code - MAC is to verify both the source and message integrity without the need for additional processes.

A MAC algorithm, sometimes called a keyed (cryptographic) hash function (however, cryptographic hash function is only one of the possible ways to generate MACs), accepts as input a secret key and an arbitrary- length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

MACs differ from digital signatures as MAC values are both generated and verified using the same secret key.

This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key:

any user who can verify a MAC is also capable of generating MACs for other messages.

In contrast, a digital signature is generated using the private key of a key pair, which is asymmetric encryption.

Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation.

The following answers are incorrect:

PAM - Pluggable Authentication Module: This isn't the right answer. There is no known message authentication function called a PAM. However, a pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes and commonly used within the Linux Operating System.

NAM - Negative Acknowledgement Message: This isn't the right answer. There is no known message authentication function called a NAM. The proper term for a negative acknowledgement is NAK, it is a signal used in digital communications to ensure that data is received with a minimum of errors.

Digital Signature Certificate: This isn't right. As it is explained and contrasted in the explanations provided above.

The following reference(s) was used to create this question:

The CCCure Computer Based Tutorial for Security+, you can subscribe at http://www.cccure.tv and http://en.wikipedia.org/wiki/Message_authentication_code

NEW QUESTION: 633

Which layer of the TCP/IP protocol stack corresponds to the ISO/OSI Network layer (layer 3)?

A. Host-to-host layer

B. Internet layer

C. Network access layer

D. Session layer

Answer: B (LEAVE A REPLY)

The Internet layer in the TCP/IP protocol stack corresponds to the network layer (layer 3) in the OSI/ISO model. The host-to-host layer corresponds to the transport layer (layer 4) in the OSI/ISO model. The Network access layer corresponds to the data link and physical layers (layers 2 and 1) in the OSI/ISO model. The session layer is not defined in the TCP/IP protocol stack.

Source: WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

NEW QUESTION: 634

Which of the following would best describe the difference between white-box testing and black-box testing?

A. White-box testing is performed by an independent programmer team.

B. Black-box testing uses the bottom-up approach.

C. White-box testing examines the program internal logical structure.

D. Black-box testing involves the business units

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Black-box testing observes the system external behavior, while white-box testing is a detailed exam of a logical path, checking the possible conditions.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).

NEW QUESTION: 635

In the statement below, fill in the blank:

Law enforcement agencies must get a warrant to search and seize an individual's property, as stated in the

_____ Amendment.

A. First.

B. Second.

C. Third.

D. Fourth.

Answer: D (LEAVE A REPLY)

Section: Risk, Response and Recovery

Explanation

Explanation/Reference:

The Fourth Amendment does not apply to a seizure or an arrest by private citizens.

Search and seizure activities can get tricky depending on what is being searched for and where.

For example, American citizens are protected by the Fourth Amendment against unlawful search and seizure, so law enforcement agencies must have probable cause and request a search warrant from a judge or court before conducting such a search.
The actual search can only take place in the areas outlined by the warrant. The Fourth Amendment does not apply to actions by private citizens unless they are acting as police agents. So, for example, if Kristy's boss warned all employees that the management could remove files from their computers at any time, and her boss was not a police officer or acting as a police agent, she could not successfully claim that her Fourth Amendment rights were violated. Kristy's boss may have violated some specific privacy laws, but he did not violate Kristy's Fourth Amendment rights.
In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction. This is referred to as exigent circumstances, and a judge will later decide whether the seizure was proper and legal before allowing the evidence to be admitted. For example, if a police officer had a search warrant that allowed him to search a suspect's living room but no other rooms, and then he saw the suspect dumping cocaine down the toilet, the police officer could seize the cocaine even though it was in a room not covered under his search warrant. After evidence is gathered, the chain of custody needs to be enacted and enforced to make sure the evidence's integrity is not compromised.
All other choices were only detractors.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1057). McGraw-Hill. Kindle Edition.

NEW QUESTION: 636
Which of the following is not a security goal for remote access?
A. Reliable authentication of users and systems
B. Protection of confidential data
C. Easy to manage access control to systems and network resources
D. Automated login for remote users
Answer: D (LEAVE A REPLY)
Explanation/Reference:
An automated login function for remote users would imply a weak authentication, thus certainly not a security goal.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition, volume 2, 2001, CRC Press, Chapter 5: An Introduction to Secure Remote Access (page 100).

NEW QUESTION: 637
Why is Network File System (NFS) used?
A. It enables two different types of file systems to interoperate.
B. It enables two different types of file systems to share Sun applications.
C. It enables two different types of file systems to use IP/IPX.

D. It enables two different types of file systems to emulate each other.

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Network File System (NFS) is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture.

Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

NEW QUESTION: 638

Insiders have a clear advantage in committing computer crime. Which two of the following do they possess? (Choose two)

A. Advantage

B. Motive

C. Outside connections

D. Means

E. Opportunity

F. Tools

Answer: D,E (LEAVE A REPLY)

Insiders possess the means and opportunity to commit a computer crime. All that is lacking is a motive.

NEW QUESTION: 639

Which of the following is NOT a common integrity goal?

A. Prevent unauthorized users from making modifications.

B. Maintain internal and external consistency.

C. Prevent authorized users from making improper modifications.

D. Prevent paths that could lead to inappropriate disclosure.

Answer: (SHOW ANSWER)

Explanation/Reference:

Inappropriate disclosure is a confidentiality, not an integrity goal.

All of the other choices above are integrity goals addressed by the Clark-Wilson integrity model.

The Clark-Wilson model is an integrity model that addresses all three integrity goals:

1. prevent unauthorized users from making modifications,

2. prevent authorized users from making improper modifications, and

3. maintain internal and external consistency through auditing.

NOTE: Biba address only the first goal of integrity above

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw-Hill. Kindle Edition.

NEW QUESTION: 640

What setup should an administrator use for regularly testing the strength of user passwords?

A. A networked workstation so that the live password database can easily be accessed by the cracking program.
B. A networked workstation so the password database can easily be copied locally and processed by the cracking program.
C. A standalone workstation on which the password database is copied and processed by the cracking program.
D. A password-cracking program is unethical; therefore it should not be used.
Answer: (SHOW ANSWER)
Explanation/Reference:
Poor password selection is frequently a major security problem for any system's security. Administrators should obtain and use password-guessing programs frequently to identify those users having easily guessed passwords.
Because password-cracking programs are very CPU intensive and can slow the system on which it is running, it is a good idea to transfer the encrypted passwords to a standalone (not networked) workstation.
Also, by doing the work on a non-networked machine, any results found will not be accessible by anyone unless they have physical access to that system.
Out of the four choice presented above this is the best choice.
However, in real life you would have strong password policies that enforce complexity requirements and does not let the user choose a simple or short password that can be easily cracked or guessed. That would be the best choice if it was one of the choice presented.
Another issue with password cracking is one of privacy. Many password cracking tools can avoid this by only showing the password was cracked and not showing what the password actually is. It is masking the password being used from the person doing the cracking.
Source: National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 8.

NEW QUESTION: 641
What is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept?
A. The reference monitor
B. Protection rings
C. A security kernel
D. A protection domain
Answer: C (LEAVE A REPLY)
Explanation/Reference:
A security kernel is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept. A reference monitor is a system component that enforces access controls on an object. A protection domain consists of the execution and memory space assigned to each process. The use of protection rings is a scheme that supports multiple protection domains.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 194).

NEW QUESTION: 642
Good security is built on which of the following concept?
A. The concept of a pass-through device that only allows certain traffic in and out
B. The Concept of defense in depth
C. The Concept of Preventative controls
D. The Concept of Defensive Controls
Answer: (SHOW ANSWER)
Explanation/Reference:
This the best of the four answers as a defense that depends on multiple layers is superior to one where all protection is embedded in a single layer (e.g., a firewall). Defense in depth would include all categories of controls.
The Following answers are incorrect:
"Concept of a pass through device that only allows certain traffic in and out" is incorrect. This is one definition of a firewall which can be a component of a defense in depth strategy in combination with other measures.
"Concept of preventative controls" is incorrect. This is a component of a defense in depth strategy but the core concept is that there must be multiple layers of defenses.
"Concept of defensive controls" is incorrect. This is a component of a defense in depth strategy but the core concept is that there must be multiple layers of defenses.
References:
http://en.wikipedia.org/wiki/Defense_in_depth_(computing)
http://www.nsa.gov/snac/support/defenseindepth.pdf

NEW QUESTION: 643
Which of the following is not a one-way hashing algorithm?
A. MD2
B. RC4
C. SHA-1
D. HAVAL
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
RC4 was designed by Ron Rivest of RSA Security in 1987. While it is officially termed "Rivest Cipher 4", the RC acronym is alternatively understood to stand for "Ron's Code" (see also RC2, RC5 and RC6). RC4 was initially a trade secret, but in September 1994 a description of it was anonymously posted to the Cypherpunks mailing list. It was soon posted on the sci.crypt newsgroup, and from there to many sites on the Internet. The leaked code was confirmed to be genuine as its output was found to match that of proprietary software using licensed RC4. Because the algorithm is known, it is no longer a trade secret.

The name RC4 is trademarked, so RC4 is often referred to as ARCFOUR or ARC4 (meaning alleged RC4) to avoid trademark problems. RSA Security has never officially released the algorithm; Rivest has, however, linked to the English Wikipedia article on RC4 in his own course notes. RC4 has become part of some commonly used encryption protocols and standards, including WEP and WPA for wireless cards and TLS.
The main factors in RC4's success over such a wide range of applications are its speed and simplicity: efficient implementations in both software and hardware are very easy to develop.
The following answer were not correct choices:
SHA-1 is a one-way hashing algorithms. SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard. SHA stands for "secure hash algorithm".
The three SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, and SHA-2. SHA-
1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.
SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used security applications and protocols. In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable.
Although no successful attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved alternatives. A new hash standard, SHA-3, is currently under development - an ongoing NIST hash function competition is scheduled to end with the selection of a winning function in 2012.
SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.
MD2 is a one-way hashing algorithms. The MD2 Message-Digest Algorithm is a cryptographic hash function developed by Ronald Rivest in 1989. The algorithm is optimized for 8-bit computers. MD2 is specified in RFC
1319. Although MD2 is no longer considered secure, even as of 2010 it remains in use in public key infrastructures as part of certificates generated with MD2 and RSA.
Haval is a one-way hashing algorithms. HAVAL is a cryptographic hash function. Unlike MD5, but like most modern cryptographic hash functions, HAVAL can produce hashes of different lengths. HAVAL can produce hashes in lengths of 128 bits, 160 bits, 192 bits, 224 bits, and 256 bits. HAVAL also allows users to specify the number of rounds (3, 4, or 5) to be used to generate the hash.
The following reference(s) were used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
https://en.wikipedia.org/wiki/HAVAL
and
https://en.wikipedia.org/wiki/MD2_%28cryptography%29

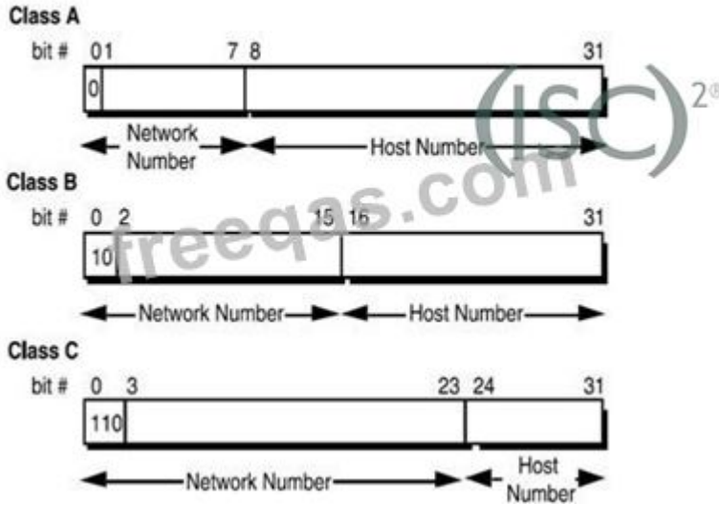
and
https://en.wikipedia.org/wiki/SHA-1

NEW QUESTION: 644
Which of the following is NOT a technical control?
A. Password and resource management
B. Identification and authentication methods
C. Monitoring for physical intrusion
D. Intrusion Detection Systems
Answer: (SHOW ANSWER)
Explanation/Reference:
It is considered to be a 'Physical Control'
There are three broad categories of access control: administrative, technical, and physical. Each category has different access control mechanisms that can be carried out manually or automatically. All of these access control mechanisms should work in concert with each other to protect an infrastructure and its data.
Each category of access control has several components that fall within it, a partial list is shown here. Not all controls fall into a single category, many of the controls will be in two or more categories. Below you have an example with backups where it is in all three categories:
Administrative Controls
Policy and procedures
- A backup policy would be in place
Personnel controls
Supervisory structure
Security-awareness training
Testing
Physical Controls
Network segregation
Perimeter security
Computer controls
Work area separation
Data backups (actual storage of the media, i:e Offsite Storage Facility) Cabling
Technical Controls
System access
Network architecture
Network access
Encryption and protocols
Control zone
Auditing
Backup (Actual software doing the backups)
The following answers are incorrect :

Password and resource management is considered to be a logical or technical control.
Identification and authentication methods is considered to be a logical or technical control.
Intrusion Detection Systems is considered to be a logical or technical control.
Reference : Shon Harris , AIO v3 , Chapter - 4 : Access Control , Page : 180 - 185

NEW QUESTION: 645
In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class B network?
A. The first bit of the IP address would be set to zero.
B. The first bit of the IP address would be set to one and the second bit set to zero.
C. The first two bits of the IP address would be set to one, and the third bit set to zero.
D. The first three bits of the IP address would be set to one.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Each Class B network address has a 16-bit network prefix, with the two highest order bits set to 1-0.
The following answers are incorrect:
The first bit of the IP address would be set to zero. Is incorrect because, this would be a Class A network address.
The first two bits of the IP address would be set to one, and the third bit set to zero. Is incorrect because, this would be a Class C network address.
The first three bits of the IP address would be set to one. Is incorrect because, this is a distractor. Class D
& E have the first three bits set to 1. Class D the 4th bit is 0 and for Class E the 4th bit to 1.
Classless Internet Domain Routing (CIDR)
High Order bits are shown in bold below.
For Class A, the addresses are 0.0.0.0 - 127.255.255.255
The lowest Class A address is represented in binary as 00000000.00000000.0000000.00000000 For Class B networks, the addresses are 128.0.0.0 - 191.255.255.255.
The lowest Class B address is represented in binary as 10000000.00000000.00000000.00000000 For Class C, the addresses are 192.0.0.0 - 223.255.255.255
The lowest Class C address is represented in binary as 11000000.00000000.00000000.00000000 For Class D, the addresses are 224.0.0.0 - 239.255.255.255 (Multicast)
The lowest Class D address is represented in binary as 11100000.00000000.00000000.00000000 For Class E, the addresses are 240.0.0.0 - 255.255.255.255 (Reserved for future usage) The lowest Class E address is represented in binary as 11110000.00000000.00000000.00000000 Classful IP Address Format

FIGURE 4. Principle Classful IP Address Formats



References:
3Com http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf
AIOv3 Telecommunications and Networking Security (page 438)

NEW QUESTION: 646
In which of the following phases of system development life cycle (SDLC) is contingency planning most important?
A. Initiation
B. Development/acquisition
C. Implementation
D. Operation/maintenance
Answer: (SHOW ANSWER)
Contingency planning requirements should be considered at every phase of SDLC, but most importantly when a new IT system is being conceived. In the initiation phase, system requirements are identified and matched to their related operational processes, allowing determination of the system's appropriate recovery priority.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 12). and The Official ISC2 Guide to the CBK, Second Edition, Application Security, page 180-185

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine

here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 647
Which type of encryption is considered to be unbreakable if the stream is truly random and is as large as the plaintext and never reused in whole or part?
A. One Time Pad (OTP)
B. One time Cryptopad (OTC)
C. Cryptanalysis
D. Pretty Good Privacy (PGP)
Answer: A (LEAVE A REPLY)
Explanation/Reference:
OTP or One Time Pad is considered unbreakable if the key is truly random and is as large as the plaintext and never reused in whole or part AND kept secret.
In cryptography, a one-time pad is a system in which a key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using the matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected.
With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. One-time pads have sometimes been used when the both parties started out at the same physical location and then separated, each with knowledge of the keys in the one-time pad.
The key used in a one-time pad is called a secret key because if it is revealed, the messages encrypted with it can easily be deciphered.
One-time pads figured prominently in secret message transmission and espionage before and during World War II and in the Cold War era. On the Internet, the difficulty of securely controlling secret keys led to the invention of public key cryptography.
The biggest challenge with OTP was to get the pad security to the person or entity you wanted to communicate with. It had to be done in person or using a trusted courrier or custodian. It certainly did not scale up very well and it would not be usable for large quantity of data that needs to be encrypted as we often time have today.
The following answers are incorrect:
- One time Cryptopad: Almost but this isn't correct. Cryptopad isn't a valid term in cryptography.
- Cryptanalysis: Sorry, incorrect. Cryptanalysis is the process of analyzing information in an effort to breach the cryptographic security systems.
- PGP - Pretty Good Privacy: PGP, written by Phil Zimmermann is a data encryption and decryption program that provides cryptographic privacy and authentication for data. Still isn't the right answer though.
Read more here about PGP.
The following reference(s) was used to create this question:

To get more info on this Qs or any Qs of Security+, subscribe to the CCCure Holistic Security+ CBT available at: http://www.cccure.tv
and
http://users.telenet.be/d.rijmenants/en/otp.htm
and
http://en.wikipedia.org/wiki/One-time_pad
and
http://searchsecurity.techtarget.com/definition/one-time-pad

NEW QUESTION: 648
What is defined as the rules for communicating between computers on a Local Area Network (LAN)?
A. LAN Media Access methods
B. LAN topologies
C. LAN transmission methods
D. Contention Access Control
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Media contention occurs when two or more network devices have data to send at the same time. Because multiple devices cannot talk on the network simultaneously, some type of method must be used to allow one device access to the network media at a time.
This is done in two main ways: carrier sense multiple access collision detect (CSMA/CD) and token passing.
In networks using CSMA/CD technology such as Ethernet, network devices contend for the network media.
When a device has data to send, it first listens to see if any other device is currently using the network. If not, it starts sending its data. After finishing its transmission, it listens again to see if a collision occurred. A collision occurs when two devices send data simultaneously. When a collision happens, each device waits a random length of time before resending its data. In most cases, a collision will not occur again between the two devices. Because of this type of network contention, the busier a network becomes, the more collisions occur.
This is why performance of Ethernet degrades rapidly as the number of devices on a single network increases.
In token-passing networks such as Token Ring and FDDI, a special network frame called a token is passed around the network from device to device. When a device has data to send, it must wait until it has the token and then sends its data. When the data transmission is complete, the token is released so that other devices may use the network media. The main advantage of token-passing networks is that they are deterministic. In other words, it is easy to calculate the maximum time that will pass before a device has the opportunity to send data. This explains the popularity of token-passing networks in some real-time environments such as factories, where machinery must be capable of communicating at a determinable interval.

For CSMA/CD networks, switches segment the network into multiple collision domains. This reduces the number of devices per network segment that must contend for the media. By creating smaller collision domains, the performance of a network can be increased significantly without requiring addressing changes.
The following are incorrect answers:
LAN topologies: Think of a topology as a network's virtual shape or structure. This shape does not necessarily correspond to the actual physical layout of the devices on the network. For example, the computers on a home LAN may be arranged in a circle in a family room, but it would be highly unlikely to find a ring topology there.
Common topologies are: bus, ring, star or meshed. See THIS LINK for more information.
LAN transmission methods: refer to the way packets are sent on the network and are either unicast, multicast or broadcast. See THIS LINK for more information.
Contention Access Control: This is a bogus detractor.
Contention is a real term but Contention Access Control is just made up. Contention methods is very closely related to Media Access Control methods. In communication networks, contention is a media access method that is used to share a broadcast medium. In contention, any computer in the network can transmit data at any time (first come-first served). This system breaks down when two computers attempt to transmit at the same time. This is a case of collision. To avoid collision, carrier sensing mechanism is used. Here each computer listens to the network before attempting to transmit. If the network is busy, it waits until network quiets down. In carrier detection, computers continue to listen to the network as they transmit. If computer detects another signal that interferes with the signal it is sending, it stops transmitting. Both computers then wait for random amount of time and attempt to transmit. Contention methods are most popular media access control method on LANs.
Reference(s) used for this question:
http://docwiki.cisco.com/wiki/Introduction_to_LAN_Protocols#LAN_Media-Access_Methods
http://en.wikipedia.org/wiki/Contention_%28telecommunications%29

NEW QUESTION: 649
Which of the following is BEST defined as a physical control?
A. Monitoring of system activity
B. Fencing
C. Identification and authentication methods
D. Logical access control mechanisms
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.
The following answers are incorrect answers:
Monitoring of system activity is considered to be administrative control.
Identification and authentication methods are considered to be a technical control.

Logical access control mechanisms is also considered to be a technical control.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 1280-1282). McGraw- Hill. Kindle Edition.

NEW QUESTION: 650
What is called the verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time?
A. Authentication
B. Identification
C. Integrity
D. Confidentiality
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 651
Which type of control is concerned with avoiding occurrences of risks?
A. Deterrent controls
B. Detective controls
C. Preventive controls
D. Compensating controls
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Preventive controls are concerned with avoiding occurrences of risks while deterrent controls are concerned with discouraging violations. Detecting controls identify occurrences and compensating controls are alternative controls, used to compensate weaknesses in other controls. Supervision is an example of compensating control.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 652
Which of the following describes a logical form of separation used by secure computing systems?
A. Processes use different levels of security for input and output devices.
B. Processes are constrained so that each cannot access objects outside its permitted domain.
C. Processes conceal data and computations to inhibit access by outside processes.
D. Processes are granted access based on granularity of controlled objects.

Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 653
Which of the following are the steps usually followed in the development of documents such as security policy, standards and procedures?
A. design, development, publication, coding, and testing.
B. design, evaluation, approval, publication, and implementation.
C. initiation, evaluation, development, approval, publication, implementation, and maintenance.
D. feasibility, development, approval, implementation, and integration.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
The common steps used the the development of security policy are initiation of the project, evaluation, development, approval, publication, implementation, and maintenance. The other choices listed are the phases of the software development life cycle and not the step used to develop ducuments such as Policies, Standards, etc...
Reference: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.

NEW QUESTION: 654
Which of the following would be the best criterion to consider in determining the classification of an information asset?
A. Value
B. Age
C. Useful life
D. Personal association
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Information classification should be based on the value of the information to the organization and its sensitivity (reflection of how much damage would accrue due to disclosure).
Age is incorrect. While age might be a consideration in some cases, the guiding principles should be value and sensitivity.
Useful life. While useful lifetime is relevant to how long data protections should be applied, the classification is based on information value and sensitivity.
Personal association is incorrect. Information classification decisions should be based on value of the information and its sensitiviry.
References
CBK, pp. 101 - 102.

NEW QUESTION: 655
Digital Certificates use which protocol?
A. X.509
B. None of the above
C. X.500
D. X.525
E. X.511
F. X.400
Answer: (SHOW ANSWER)

NEW QUESTION: 656
Which of the following packets should NOT be dropped at a firewall protecting an organization's internal network?
A. Inbound packets with Source Routing option set
B. Router information exchange protocols
C. Inbound packets with an internal address as the source IP address
D. Outbound packets with an external destination IP address
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Normal outbound traffic has an internal source IP address and an external destination IP address.
Traffic with an internal source IP address should only come from an internal interface. Such packets coming from an external interface should be dropped.
Packets with the source-routing option enabled usually indicates a network intrusion attempt.
Router information exchange protocols like RIP and OSPF should be dropped to avoid having internal routing equipment being reconfigured by external agents.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 10: The Perfect Firewall.

NEW QUESTION: 657
Sensitivity labels are an example of what application control type?
A. Preventive security controls
B. Detective security controls
C. Compensating administrative controls
D. Preventive accuracy controls
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:

Sensitivity labels are a preventive security application controls, such as are firewalls, reference monitors, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments.
The incorrect answers are:
Detective security controls - Intrusion detection systems (IDS), monitoring activities, and audit trails.
Compensating administrative controls - There no such application control.
Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 264).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter
7: Application Controls, Figure 7.1 (page 360).

NEW QUESTION: 658
The Computer Security Policy Model the Orange Book is based on is which of the following?
A. Bell-LaPadula
B. Data Encryption Standard
C. Kerberos
D. Tempest
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The Computer Security Policy Model Orange Book is based is the Bell-LaPadula Model. Orange Book Glossary.
The Data Encryption Standard (DES) is a cryptographic algorithm. National Information Security Glossary.
TEMPEST is related to limiting the electromagnetic emanations from electronic equipment.
Reference: U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here).

NEW QUESTION: 659
Which protocol is used to send email?
A. File Transfer Protocol (FTP).
B. Post Office Protocol (POP).
C. Network File System (NFS).
D. Simple Mail Transfer Protocol (SMTP).
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:

Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. POP is a protocol used to retrieve e-mail from a mail server. NFS is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture. FTP is the protocol that is used to facilitate file transfer between two machines.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

NEW QUESTION: 660
What is the MOST critical piece to disaster recovery and continuity planning?
A. Security policy
B. Management support
C. Availability of backup information processing facilities
D. Staff training
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The keyword is ' MOST CRITICAL ' and the correct answer is ' Management Support ' as the management must be convinced of its necessity and that's why a business case must be made. The decision of how a company should recover from any disaster is purely a business decision and should be treated as so.
The other answers are incorrect because :
Security policy is incorrect as it is not the MOST CRITICAL piece.
Availability of backup information processing facilities is incorrect as this comes once the organization has BCP Plans in place and for a BCP Plan , management support must be there.
Staff training comes after the plans are in place with the support from management.
Reference : Shon Harris , AIO v3 , Chapter-9: Business Continuity Planning , Page : 697.

NEW QUESTION: 661
When packets are captured and converted to hexadecimal, _____ represents the ICMP protocol in the IP header.
A. 06
B. 17
C. 16
D. All of the above
E. 01
F. 25
Answer: E (LEAVE A REPLY)

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 662
What can be defined as an abstract machine that mediates all access to objects by subjects to ensure that subjects have the necessary access rights and to protect objects from unauthorized access?
A. The Reference Monitor
B. The Security Kernel
C. The Trusted Computing Base
D. The Security Domain
Answer: (SHOW ANSWER)
Explanation/Reference:
The reference monitor refers to abstract machine that mediates all access to objects by subjects.
This question is asking for the concept that governs access by subjects to objects, thus the reference monitor is the best answer. While the security kernel is similar in nature, it is what actually enforces the concepts outlined in the reference monitor.
In operating systems architecture a reference monitor concept defines a set of design requirements on a reference validation mechanism, which enforces an access control policy over subjects' (e.g., processes and users) ability to perform operations (e.g., read and write) on objects (e.g., files and sockets) on a system. The properties of a reference monitor are:
The reference validation mechanism must always be invoked (complete mediation). Without this property, it is possible for an attacker to bypass the mechanism and violate the security policy.
The reference validation mechanism must be tamperproof (tamperproof). Without this property, an attacker can undermine the mechanism itself so that the security policy is not correctly enforced.
The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured (verifiable). Without this property, the mechanism might be flawed in such a way that the policy is not enforced.
For example, Windows 3.x and 9x operating systems were not built with a reference monitor, whereas the Windows NT line, which also includes Windows 2000 and Windows XP, was designed to contain a reference monitor, although it is not clear that its properties (tamperproof, etc.) have ever been independently verified, or what level of computer security it was intended to provide.
The claim is that a reference validation mechanism that satisfies the reference monitor concept will correctly enforce a system's access control policy, as it must be invoked to mediate all security-sensitive operations, must not be tampered, and has undergone complete analysis and testing to verify correctness.

The abstract model of a reference monitor has been widely applied to any type of system that needs to enforce access control, and is considered to express the necessary and sufficient properties for any system making this security claim.
According to Ross Anderson, the reference monitor concept was introduced by James Anderson in an influential 1972 paper.
Systems evaluated at B3 and above by the Trusted Computer System Evaluation Criteria (TCSEC) must enforce the reference monitor concept.
The reference monitor, as defined in AIO V5 (Harris) is: "an access control concept that refers to an abstract machine that mediates all access to objects by subjects."
The security kernel, as defined in AIO V5 (Harris) is: "the hardware, firmware, and software elements of a trusted computing based (TCB) that implement the reference monitor concept. The kernel must mediate all access between subjects and objects, be protected from modification, and be verifiable as correct."
The trusted computing based (TCB), as defined in AIO V5 (Harris) is: "all of the protection mechanisms within a computer system (software, hardware, and firmware) that are responsible for enforcing a security policy."
The security domain, "builds upon the definition of domain (a set of resources available to a subject) by adding the fact that resources withing this logical structure (domain) are working under the same security policy and managed by the same group."
The following answers are incorrect:
"The security kernel" is incorrect. One of the places a reference monitor could be implemented is in the security kernel but this is not the best answer.
"The trusted computing base" is incorrect. The reference monitor is an important concept in the TCB but this is not the best answer.
"The security domain is incorrect." The reference monitor is an important concept in the security domain but this is not the best answer.
Reference(s) used for this question:
Official ISC2 Guide to the CBK, page 324
AIO Version 3, pp. 272 - 274
AIOv4 Security Architecture and Design (pages 327 - 328)
AIOv5 Security Architecture and Design (pages 330 - 331)
Wikipedia article at https://en.wikipedia.org/wiki/Reference_monitor

NEW QUESTION: 663
Name three SSO types? (Choose three)
A. KryptoKnight
B. Kerberos
C. Clipper
D. SESAME
E. DES
Answer: A,B,D (LEAVE A REPLY)
Single Sign-On (SSO) options include: KryptoKnight , Kerberos, and SESAME.

NEW QUESTION: 664
Which access control type has a central authority that determine to what objects the subjects have access to and it is based on role or on the organizational security policy?
A. Mandatory Access Control
B. Discretionary Access Control
C. Non-Discretionary Access Control
D. Rule-based Access control
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Non Discretionary Access Control include Role Based Access Control (RBAC) and Rule Based Access Control (RBAC or RuBAC). RABC being a subset of NDAC, it was easy to eliminate RBAC as it was covered under NDAC already.
Some people think that RBAC is synonymous with NDAC but RuBAC would also fall into this category.
Discretionary Access control is for environment with very low level of security. There is no control on the dissemination of the information. A user who has access to a file can copy the file or further share it with other users.
Rule Based Access Control is when you have ONE set of rules applied uniformly to all users. A good example would be a firewall at the edge of your network. A single rule based is applied against any packets received from the internet.
Mandatory Access Control is a very rigid type of access control. The subject must dominate the object and the subject must have a Need To Know to access the information. Objects have labels that indicate the sensitivity (classification) and there is also categories to enforce the Need To Know (NTK).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 665
How many rounds are used by DES?
A. 16
B. 32
C. 64
D. 48
Answer: A (LEAVE A REPLY)
Explanation/Reference:
DES is a block encryption algorithm using 56-bit keys and 64-bit blocks that are divided in half and each character is encrypted one at a time. The characters are put through 16 rounds of transposition and substitution functions. Triple DES uses 48 rounds.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 3).

NEW QUESTION: 666

Identification and authentication are the keystones of most access control systems. Identification establishes:

A. User accountability for the actions on the system.

B. Top management accountability for the actions on the system.

C. EDP department accountability for the actions of users on the system.

D. Authentication for actions on the system

Answer: (SHOW ANSWER)

Explanation/Reference:

Identification and authentication are the keystones of most access control systems. Identification establishes user accountability for the actions on the system.

The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Once a person has been identified through the user ID or a similar value, she must be authenticated, which means she must prove she is who she says she is. Three general factors can be used for authentication:

something a person knows, something a person has, and something a person is. They are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic.

For a user to be able to access a resource, he first must prove he is who he claims to be, has the necessary credentials, and has been given the necessary rights or privileges to perform the actions he is requesting. Once these steps are completed successfully, the user can access and use network resources; however, it is necessary to track the user's activities and enforce accountability for his actions.

Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase, cryptographic key, personal identification number (PIN), anatomical attribute, or token.

These two credential items are compared to information that has been previously stored for this subject. If these credentials match the stored information, the subject is authenticated. But we are not done yet.

Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions. The system will look at some type of access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.

Although identification, authentication, authorization, and accountability have close and complementary definitions, each has distinct functions that fulfill a specific requirement in the process of access control. A user may be properly identified and authenticated to the network, but he may not have the authorization to access the files on the file server. On the other hand, a user may be authorized to

access the files on the file server, but until she is properly identified and authenticated, those resources are out of reach.
Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Access Control ((ISC)2 Press) (Kindle Locations 889-892). Auerbach Publications. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3875-3878). McGraw-Hill. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3833-3848). McGraw-Hill. Kindle Edition.
and
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 667
Which of the following offers advantages such as the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access?
A. Smart cards
B. Single Sign-On (SSO)
C. Symmetric Ciphers
D. Public Key Infrastructure (PKI)
Answer: (SHOW ANSWER)
Explanation/Reference:
The advantages of SSO include having the ability to use stronger passwords, easier administration as far as changing or deleting the passwords, minimize the risks of orphan accounts, and requiring less time to access resources.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

NEW QUESTION: 668
Why would a memory dump be admissible as evidence in court?
A. Because it is used to demonstrate the truth of the contents.
B. Because it is used to identify the state of the system.
C. Because the state of the memory cannot be used as evidence.
D. Because of the exclusionary rule.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
A memory dump can be admitted as evidence if it acts merely as a statement of fact. A system dump is not considered hearsay because it is used to identify the state of the system, not the truth of the

contents. The exclusionary rule mentions that evidence must be gathered legally or it can't be used. This choice is a distracter.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 187).

NEW QUESTION: 669
Buffer overflow and boundary condition errors are subsets of which of the following?
A. Race condition errors.
B. Access validation errors.
C. Exceptional condition handling errors.
D. Input validation errors.
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
In an input validation error, the input received by a system is not properly checked, resulting in a vulnerability that can be exploited by sending a certain input sequence. There are two important types of input validation errors: buffer overflows (input received is longer than expected input length) and boundary condition error (where an input received causes the system to exceed an assumed boundary).
A race condition occurs when there is a delay between the time when a system checks to see if an operation is allowed by the security model and the time when the system actually performs the operation.
In an access validation error, the system is vulnerable because the access control mechanism is faulty.
In an exceptional condition handling error, the system somehow becomes vulnerable due to an exceptional condition that has arisen.
Source: DUPUIS, Clement, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 105).

NEW QUESTION: 670
Which backup method usually resets the archive bit on the files after they have been backed up?
A. Incremental backup method.
B. Differential backup method.
C. Partial backup method.
D. Tape backup method.
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The incremental backup method usually resets the archive bit on the files after they have been backed up.
An Incremental Backup will backup all the files that have changed since the last Full Backup (the first time it is run after a full backup was previously completed) or after an Incremental Backup (for the second backup and subsequent backups) and sets the archive bit to 0. This type of backup take less time during the backup phase but it will take more time to restore.

The other answers are all incorrect choices.
The following backup types also exists:
Full Backup - All data are backed up. The archive bit is cleared, which means that it is set to 0.
Differential Backup - Backup the files that have been modified since the last Full Backup. The archive bit does not change. Take more time while the backup phase is performed and take less time to restore.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

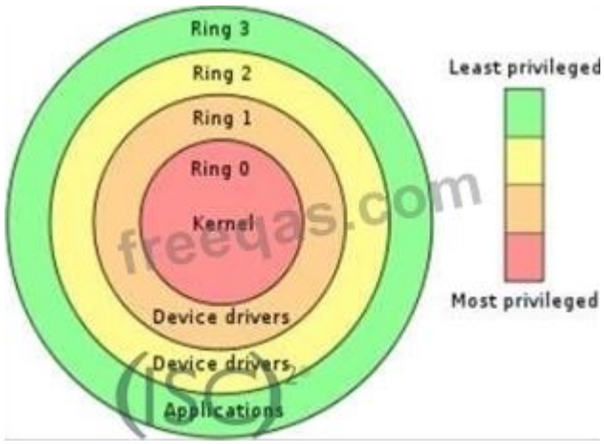
NEW QUESTION: 671
Which protocol is used to send email?
A. File Transfer Protocol (FTP).
B. Post Office Protocol (POP).
C. Network File System (NFS).
D. Simple Mail Transfer Protocol (SMTP).
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. POP is a protocol used to retrieve e-mail from a mail server. NFS is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture. FTP is the protocol that is used to facilitate file transfer between two machines.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

NEW QUESTION: 672
Within the legal domain what rule is concerned with the legality of how the evidence was gathered ?
A. Exclusionary rule
B. Best evidence rule
C. Hearsay rule
D. Investigation rule
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The exclusionary rule mentions that evidence must be gathered legally or it can't be used.
The principle based on federal Constitutional Law that evidence illegally seized by law enforcement officers in violation of a suspect's right to be free from unreasonable searches and seizures cannot be used against the suspect in a criminal prosecution.
The exclusionary rule is designed to exclude evidence obtained in violation of a criminal defendant's Fourth Amendment rights. The Fourth Amendment protects against unreasonable searches and seizures by law enforcement personnel. If the search of a criminal suspect is unreasonable, the evidence obtained in the search will be excluded from trial.

The exclusionary rule is a court-made rule. This means that it was created not in statutes passed by legislative bodies but rather by the U.S. Supreme Court. The exclusionary rule applies in federal courts by virtue of the Fourth Amendment. The Court has ruled that it applies in state courts although the due process clause of the Fourteenth Amendment.(The Bill of Rights-the first ten amendments- applies to actions by the federal government. The Fourteenth Amendment, the Court has held, makes most of the protections in the Bill of Rights applicable to actions by the states.) The exclusionary rule has been in existence since the early 1900s. Before the rule was fashioned, any evidence was admissible in a criminal trial if the judge found the evidence to be relevant. The manner in which the evidence had been seized was not an issue. This began to change in 1914, when the U.S.
Supreme Court devised a way to enforce the Fourth Amendment. In Weeks v. United States, 232 U.S. 383, 34 S. Ct. 341, 58 L. Ed. 652 (1914), a federal agent had conducted a warrantless search for evidence of gambling at the home of Fremont Weeks. The evidence seized in the search was used at trial, and Weeks was convicted. On appeal, the Court held that the Fourth Amendment barred the use of evidence secured through a warrantless search. Weeks's conviction was reversed, and thus was born the exclusionary rule.
The best evidence rule concerns limiting potential for alteration. The best evidence rule is a common law rule of evidence which can be traced back at least as far as the 18th century. In Omychund v Barker (1745) 1 Atk, 21, 49; 26 ER 15, 33, Lord Harwicke stated that no evidence was admissible unless it was "the best that the nature of the case will allow". The general rule is that secondary evidence, such as a copy or facsimile, will be not admissible if an original document exists, and is not unavailable due to destruction or other circumstances indicating unavailability.
The rationale for the best evidence rule can be understood from the context in which it arose: in the eighteenth century a copy was usually made by hand by a clerk (or even a litigant). The best evidence rule was predicated on the assumption that, if the original was not produced, there was a significant chance of error or fraud in relying on such a copy.
The hearsay rule concerns computer-generated evidence, which is considered second-hand evidence. Hearsay is information gathered by one person from another concerning some event, condition, or thing of which the first person had no direct experience. When submitted as evidence, such statements are called hearsay evidence. As a legal term, "hearsay" can also have the narrower meaning of the use of such information as evidence to prove the truth of what is asserted. Such use of "hearsay evidence" in court is generally not allowed. This prohibition is called the hearsay rule.
For example, a witness says "Susan told me Tom was in town". Since the witness did not see Tom in town, the statement would be hearsay evidence to the fact that Tom was in town, and not admissible. However, it would be admissible as evidence that Susan said Tom was in town, and on the issue of her knowledge of whether he was in town.
Hearsay evidence has many exception rules. For the purpose of the exam you must be familiar with the business records exception rule to the Hearsay Evidence. The business records created during the ordinary course of business are considered reliable and can usually be brought in under this exception if the proper foundation is laid when the records are introduced into evidence. Depending on which jurisdiction the case is in, either the records custodian or someone with knowledge of the records must lay a foundation for the records. Logs that are collected as part of a document business process being

carried at regular interval would fall under this exception. They could be presented in court and not be considered Hearsay.
Investigation rule is a detractor.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 9.
and
The FREE Online Law Dictionary at: http://legal-dictionary.thefreedictionary.com/Exclusionary+Rule and Wikipedia has a nice article on this subject at: http://en.wikipedia.org/wiki/Exclusionary_rule and http://en.wikipedia.org/wiki/Hearsay_in_United_States_law#Hearsay_exceptions

NEW QUESTION: 673
An Architecture where there are more than two execution domains or privilege levels is called:
A. Ring Architecture.
B. Ring Layering
C. Network Environment.
D. Security Models
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
In computer science, hierarchical protection domains, often called protection rings, are a mechanism to protect data and functionality from faults (fault tolerance) and malicious behavior (computer security). This approach is diametrically opposite to that of capability-based security.
Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level. Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.
Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.
Ring Architecture



All of the other answers are incorrect because they are detractors.
References:
OIG CBK Security Architecture and Models (page 311)
and
https://en.wikipedia.org/wiki/Ring_%28computer_security%29

NEW QUESTION: 674
Which of the following floors would be most appropriate to locate information processing facilities in a 6-stories building?
A. Basement
B. Ground floor
C. Third floor
D. Sixth floor
Answer: (SHOW ANSWER)
You data center should be located in the middle of the facility or the core of a building to provide protection from natural disasters or bombs and provide easier access to emergency crewmembers if necessary. By being at the core of the facility the external wall would act as a secondary layer of protection as well.
Information processing facilities should not be located on the top floors of buildings in case of a fire or flooding coming from the roof. Many crimes and theft have also been conducted by simply cutting a large hole on the roof.
They should not be in the basement because of flooding where water has a natural tendancy to flow down :-) Even a little amount of water would affect your operation considering the quantity of electrical cabling sitting directly on the cement floor under under your raise floor.
The data center should not be located on the first floor due to the presence of the main entrance where people are coming in and out. You have a lot of high traffic areas such as the elevators, the loading docks, cafeteria, coffee shopt, etc.. Really a bad location for a data center.
So it was easy to come up with the answer by using the process of elimination where the top, the bottom, and the basement are all bad choices. That left you with only one possible answer which is the third floor.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 5th Edition, Page
425.

NEW QUESTION: 675
Which of the following is not appropriate in addressing object reuse?
A. Degaussing magnetic tapes when they're no longer needed.
B. Deleting files on disk before reusing the space.
C. Clearing memory blocks before they are allocated to a program or data.
D. Clearing buffered pages, documents, or screens from the local memory of a terminal or printer.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Object reuse requirements, applying to systems rated TCSEC C2 and above, are used to protect files, memory, and other objects in a trusted system from being accidentally accessed by users who are not authorized to access them. Deleting files on disk merely erases file headers in a directory structure. It does not clear data from the disk surface, thus making files still recoverable. All other options involve clearing used space, preventing any unauthorized access.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 119).

NEW QUESTION: 676
What is the main concern with single sign-on?
A. Maximum unauthorized access would be possible if a password is disclosed.
B. The security administrator's workload would increase.
C. The users' password would be too hard to remember.
D. User access rights would be increased.
Answer: (SHOW ANSWER)
Explanation/Reference:
A major concern with Single Sign-On (SSO) is that if a user's ID and password are compromised, the intruder would have access to all the systems that the user was authorized for.
The following answers are incorrect:
The security administrator's workload would increase. Is incorrect because the security administrator's workload would decrease and not increase. The admin would not be responsible for maintaining multiple user accounts just the one.
The users' password would be too hard to remember. Is incorrect because the users would have less passwords to remember.
User access rights would be increased. Is incorrect because the user access rights would not be any different than if they had to log into systems manually.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine

here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 677

If your property Insurance has Replacement Cost Valuation (RCV) clause your damaged property will be compensated:

A. Based on the value of item on the date of loss

B. Based on new, comparable, or identical item for old regardless of condition of lost item

C. Based on value of item one month before the loss

D. Based on the value listed on the Ebay auction web site

Answer: B (LEAVE A REPLY)

Section: Risk, Response and Recovery

Explanation/Reference:

RCV is the maximum amount your insurance company will pay you for damage to covered property before deducting for depreciation. The RCV payment is based on the current cost to replace your property with new, identical or comparable property.

The other choices were detractor:

Application and definition of the insurance terms Replacement Cost Value (RCV), Actual Cash Value (ACV) and depreciation can be confusing. It's important that you understand the terms to help settle your claim fairly.

An easy way to understand RCV and ACV is to think in terms of "new" and "used." Replacement cost is the item's current price, new. "What will it cost when I replace it?" Actual cash is the item's used price, old. "How much money is it worth since I used it for five years?" Hold Back Most policies only pay the Actual Cash Value upfront, and then they pay you the "held back" depreciation after you incur the expense to repair or replace your personal property items.

NOTE: You must remember to send documentation to the insurance company proving you've incurred the additional expense you will be reimbursed.

Actual Cash Value (ACV)

ACV is the amount your insurance company will pay you for damage to covered property after deducting for depreciation. ACV is the replacement cost of a new item, minus depreciation. If stated as a simple equation, ACV could be defined as follows: ACV=RCV-Depreciation Unfortunately, ACV is not always as easy to agree upon as a simple math equation. The ACV can also be calculated as the price a willing buyer would pay for your used item.

Depreciation

Depreciation (sometimes called "hold back") is defined as the "loss in value from all causes, including age, and wear and tear." Although the definition seems to be clear, in our experience, value" as a real-world application is clearly subjective and varies widely. We have seen the same adjuster apply NO depreciation (100 percent value) on one claim and 40 percent depreciation almost half value) on an almost identical claim.

This shows that the process of applying depreciation is subjective and clearly negotiable.

Excessive Depreciation

When the insurance company depreciates more than they should, it is called "Excessive depreciation." Although not ethical, it is very common. Note any items that have excessive depreciation and write a letter to your insurance company.
References:
http://carehelp.org/downloads/category/1-insurance-handouts.html?download=17%3Ahandout08-rcv-and-acv and
http://www.schirickinsurance.com/resources/value2005.pdf
and
TIPTON, Harold F. & KRAUSE, MICKI, information Security Management Handbook, 4th Edition, Volume 1 Property Insurance overview, Page 587.

NEW QUESTION: 678
Virus scanning and content inspection of SMIME encrypted e-mail without doing any further processing is:
A. Not possible
B. Only possible with key recovery scheme of all user keys
C. It is possible only if X509 Version 3 certificates are used
D. It is possible only by "brute force" decryption
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Content security measures presumes that the content is available in cleartext on the central mail server. Encrypted emails have to be decrypted before it can be filtered (e.g. to detect viruses), so you need the decryption key on the central "crypto mail server".
There are several ways for such key management, e.g. by message or key recovery methods. However, that would certainly require further processing in order to achieve such goal.

NEW QUESTION: 679
What is it called when a computer uses more than one CPU in parallel to execute instructions?
A. Multiprocessing
B. Multitasking
C. Multithreading
D. Parallel running
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
A system with multiple processors is called a multiprocessing system.
Multitasking is incorrect. Multitasking involves sharing the processor amoung all ready processes. Though it appears to the user that multiple processes are executing at the same time, only one process is running at any point in time.

Multithreading is incorrect. The developer can structure a program as a collection of independent threads to achieve better concurrency. For example, one thread of a program might be performing a calculation while another is waiting for additional input from the user.
"Parallel running" is incorrect. This is not a real term and is just a distraction.
References:
CBK, pp. 315-316
AIO3, pp. 234 - 239

NEW QUESTION: 680
Which cable technology refers to the CAT3 and CAT5 categories?
A. Coaxial cables
B. Fiber Optic cables
C. Axial cables
D. Twisted Pair cables
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Twisted Pair cables currently have two categories in common usage. CAT3 and CAT5.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

NEW QUESTION: 681
Which of the following attacks could capture network user passwords?
A. Data diddling
B. Sniffing
C. IP Spoofing
D. Smurfing
Answer: B (LEAVE A REPLY)
A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.
Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.
A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.
Another method for sniffing is to use a network tap-a device that literally splits a network transmission into two identical streams; one going to the original network destination and

the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.
The packets captured by sniffer are decoded and then displayed by the sniffer. Therfore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).
Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.
The following answers are incorrect:
Data diddling involves changing data before, as it is enterred into a computer, or after it is extracted.
Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.
Smurfing would refer to the smurf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.
The following reference(s) were/was used to create this question:
CISA Review manual 2014 Page number 321 Official ISC2 Guide to the CISSP 3rd edition Page Number 153

NEW QUESTION: 682
Which of the following services relies on UDP?
A. FTP
B. Telnet
C. DNS
D. SMTP
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
DNS relies on connectionless UDP whereas services like FTP, Telnet and SMTP rely on TCP.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

NEW QUESTION: 683
What is called the percentage at which the False Rejection Rate equals the False Acceptance Rate?
A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. Failure to enroll rate (FTE or FER)
Answer: (SHOW ANSWER)
Explanation/Reference:

The percentage at which the False Rejection Rate equals the False Acceptance Rate is called the Crossover Error Rate (CER). Another name for the CER is the Equal Error Rate (EER), any of the two terms could be used.
Equal error rate or crossover error rate (EER or CER)
It is the rate at which both accept and reject errors are equal. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.
The other choices were all wrong answers:
The following are used as performance metrics for biometric systems:
false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. This is when an impostor would be accepted by the system.
False reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected. This is when a valid company employee would be rejected by the system.
Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.
and
https://en.wikipedia.org/wiki/Biometrics

NEW QUESTION: 684
Which of the following phases of a software development life cycle normally addresses Due Care and Due Diligence?
A. Implementation
B. System feasibility
C. Product design
D. Software plans and requirements
Answer: (SHOW ANSWER)
The software plans and requirements phase addresses threats, vulnerabilities, security requirements, reasonable care, due diligence, legal liabilities, cost/benefit analysis, level of protection desired, test plans.
Implementation is incorrect because it deals with Installing security software, running the system, acceptance testing, security software testing, and complete documentation certification and accreditation (where necessary).
System Feasibility is incorrect because it deals with information security policy, standards, legal issues, and the early validation of concepts.
Product design is incorrect because it deals with incorporating security specifications,

adjusting test plans and data,
determining access controls, design documentation, evaluating encryption options, and verification.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Security Life Cycle Components, Figure 7.5 (page 346).

NEW QUESTION: 685
Frame relay uses a public switched network to provide:
A. Local Area Network (LAN) connectivity.
B. Metropolitan Area Network (MAN) connectivity.
C. Wide Area Network (WAN) connectivity.
D. World Area Network (WAN) connectivity.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Frame relay uses a public switched network to provide Wide Area Network (WAN) connectivity.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 73.

NEW QUESTION: 686
An effective information security policy should not have which of the following characteristic?
A. Include separation of duties
B. Be designed with a short- to mid-term focus
C. Be understandable and supported by all stakeholders
D. Specify areas of responsibility and authority
Answer: (SHOW ANSWER)
Explanation/Reference:
An effective information security policy should be designed with a long-term focus. All other characteristics apply.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 397).

NEW QUESTION: 687
Which of the following is BEST defined as a physical control?
A. Monitoring of system activity
B. Fencing
C. Identification and authentication methods
D. Logical access control mechanisms

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

The following answers are incorrect answers:

Monitoring of system activity is considered to be administrative control.

Identification and authentication methods are considered to be a technical control.

Logical access control mechanisms is also considered to be a technical control.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 1280-1282). McGraw-Hill. Kindle Edition.

NEW QUESTION: 688

A trusted system does NOT involve which of the following?

A. Enforcement of a security policy.

B. Sufficiency and effectiveness of mechanisms to be able to enforce a security policy.

C. Assurance that the security policy can be enforced in an efficient and reliable manner.

D. Independently-verifiable evidence that the security policy-enforcing mechanisms are sufficient and effective.

Answer: (SHOW ANSWER)

A trusted system is one that meets its intended security requirements. It involves sufficiency and effectiveness, not necessarily efficiency, in enforcing a security policy. Put succinctly, trusted systems have (1) policy, (2) mechanism, and (3) assurance. Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 689

The basic language of modems and dial-up remote access systems is:

A. Asynchronous Communication.

B. Synchronous Communication.

C. Asynchronous Interaction.

D. Synchronous Interaction.

Answer: A (LEAVE A REPLY)

Asynchronous Communication is the basic language of modems and dial-up remote access systems. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.

NEW QUESTION: 690

The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as "_____," RSA is quite feasible for computer use.

A. computing in Galois fields

B. computing in Gladden fields
C. computing in Gallipoli fields
D. computing in Galbraith fields
Answer: (SHOW ANSWER)
Explanation/Reference:
The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as computing in Galois fields, RSA is quite feasible for computer use.
Source: FITES, Philip E., KRATZ, Martin P., Information Systems Security: A Practitioner's Reference, 1993, Van Nostrand Reinhold, page 44.

NEW QUESTION: 691
Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?
A. Extensible Authentication Protocol
B. Challenge Handshake Authentication Protocol
C. Remote Authentication Dial-In User Service
D. Multilevel Authentication Protocol.
Answer: (SHOW ANSWER)
RFC 2828 (Internet Security Glossary) defines the Extensible Authentication Protocol as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences. It is intended for use primarily by a host or router that connects to a PPP network server via switched circuits or dial-up lines. The Remote Authentication Dial-In User Service (RADIUS) is defined as an Internet protocol for carrying dial-in user's authentication information and configuration information between a shared, centralized authentication server and a network access server that needs to authenticate the users of its network access ports. The other option is a distracter. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 692
What type of cable is used with 100Base-TX Fast Ethernet?
A. Fiber-optic cable
B. Category 3 or 4 unshielded twisted-pair (UTP).

C. Category 5 unshielded twisted-pair (UTP).
D. RG-58 cable.
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
This is the type of cabling recommended for 100Base-TX networks.
Fiber-optic cable is incorrect. Incorrect media type for 100Base-TX -- 100Base-FX would denote fiber optic cabling.
"Category 3 or 4 unshielded twisted-pair (UTP)" is incorrect. These types are not recommended for 100Mbps operation.
RG-58 cable is incorrect. Incorrect media type for 100Base-TX.
References
CBK, p. 428
AIO3, p. 455

NEW QUESTION: 693
In a hierarchical PKI the highest CA is regularly called Root CA, it is also referred to by which one of the following term?
A. Subordinate CA
B. Top Level CA
C. Big CA
D. Master CA
Answer: B (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference: Arsenault, Turner, Internet X.509 Public Key Infrastructure: Roadmap, Chapter "Terminology".
Also note that sometimes other terms such as Certification Authority Anchor (CAA) might be used within some government organization, Top level CA is another common term to indicate the top level CA, Top Level Anchor could also be used.

NEW QUESTION: 694
After a company is out of an emergency state, what should be moved back to the original site first?
A. Executives
B. Least critical components
C. IT support staff
D. Most critical components
Answer: (SHOW ANSWER)
This will expose any weaknesses in the plan and ensure the primary site has been properly repaired before moving back. Moving critical assets first may induce a second disaster if the primary site has not been repaired properly.

The first group to go back would test items such as connectivity, HVAC, power, water, improper procedures, and/or steps that has been overlooked or not done properly. By moving these first, and fixing any problems identified, the critical operations of the company are not negatively affected.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 621).

NEW QUESTION: 695
Which of the following is NOT part of the Kerberos authentication protocol?
A. Symmetric key cryptography
B. Authentication service (AS)
C. Principals
D. Public Key
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
There is no such component within kerberos environment. Kerberos uses only symmetric encryption and does not make use of any public key component.
The other answers are incorrect because :
Symmetric key cryptography is a part of Kerberos as the KDC holds all the users' and services' secret keys.
Authentication service (AS) : KDC (Key Distribution Center) provides an authentication service
Principals : Key Distribution Center provides services to principals , which can be users , applications or network services.
References: Shon Harris , AIO v3 , Chapter - 4: Access Control , Pages : 152-155.

NEW QUESTION: 696
Which of the following rules appearing in an Internet firewall policy is inappropriate?
A. Source routing shall be disabled on all firewalls and external routers.
B. Firewalls shall be configured to transparently allow all outbound and inbound services.
C. Firewalls should fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a firewall has failed.
D. Firewalls shall not accept traffic on its external interfaces that appear to be coming from internal network addresses.
Answer: B (LEAVE A REPLY)
Unless approved by the Network Services manager, all in-bound services shall be intercepted and processed by the firewall. Allowing unrestricted services inbound and outbound is certainly NOT recommended and very dangerous.
Pay close attention to the keyword: all
All of the other choices presented are recommended practices for a firewall policy.
Reference(s) used for this question:

GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 78).

NEW QUESTION: 697
Which of the following is more suitable for a hardware implementation?
A. Stream ciphers
B. Block ciphers
C. Cipher block chaining
D. Electronic code book
Answer: (SHOW ANSWER)
A stream cipher treats the message as a stream of bits or bytes and performs mathematical functions on them individually. The key is a random value input into the stream cipher, which it uses to ensure the randomness of the keystream data. They are more suitable for hardware implementations, because they encrypt and decrypt one bit at a time. They are intensive because each bit must be manipulated, which works better at the silicon level. Block ciphers operate a the block level, dividing the message into blocks of bits. Cipher Block chaining (CBC) and Electronic Code Book (ECB) are operation modes of DES, a block encryption algorithm. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

NEW QUESTION: 698
In a hierarchical PKI the highest CA is regularly called Root CA, it is also referred to by which one of the following term?
A. Subordinate CA
B. Top Level CA
C. Big CA
D. Master CA
Answer: B (LEAVE A REPLY)
Reference: Arsenault, Turner, Internet X.509 Public Key Infrastructure: Roadmap, Chapter "Terminology".
Also note that sometimes other terms such as Certification Authority Anchor (CAA) might be used within some government organization, Top level CA is another common term to indicate the top level CA, Top Level Anchor could also be used.

NEW QUESTION: 699
Related to information security, availability is the opposite of which of the following?
A. delegation
B. distribution
C. documentation
D. destruction
Answer: D (LEAVE A REPLY)
Availability is the opposite of "destruction."

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 700
What can be defined as an abstract machine that mediates all access to objects by subjects to ensure that subjects have the necessary access rights and to protect objects from unauthorized access?
A. The Reference Monitor
B. The Security Kernel
C. The Trusted Computing Base
D. The Security Domain
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The reference monitor refers to abstract machine that mediates all access to objects by subjects.
This question is asking for the concept that governs access by subjects to objects, thus the reference monitor is the best answer. While the security kernel is similar in nature, it is what actually enforces the concepts outlined in the reference monitor.
In operating systems architecture a reference monitor concept defines a set of design requirements on a reference validation mechanism, which enforces an access control policy over subjects' (e.g., processes and users) ability to perform operations (e.g., read and write) on objects (e.g., files and sockets) on a system. The properties of a reference monitor are:
The reference validation mechanism must always be invoked (complete mediation). Without this property, it is possible for an attacker to bypass the mechanism and violate the security policy.
The reference validation mechanism must be tamperproof (tamperproof). Without this property, an attacker can undermine the mechanism itself so that the security policy is not correctly enforced.
The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured (verifiable). Without this property, the mechanism might be flawed in such a way that the policy is not enforced.
For example, Windows 3.x and 9x operating systems were not built with a reference monitor, whereas the Windows NT line, which also includes Windows 2000 and Windows XP, was designed to contain a reference monitor, although it is not clear that its properties (tamperproof, etc.) have ever been independently verified, or what level of computer security it was intended to provide.
The claim is that a reference validation mechanism that satisfies the reference monitor concept will correctly enforce a system's access control policy, as it must be invoked to mediate all security-sensitive operations, must not be tampered, and has undergone complete analysis and testing to verify correctness. The abstract model of a reference monitor has been widely applied to any type of system that needs to enforce access control, and is considered to express the necessary and sufficient properties for any system making this security claim.
According to Ross Anderson, the reference monitor concept was introduced by James Anderson in an influential 1972 paper.

Systems evaluated at B3 and above by the Trusted Computer System Evaluation Criteria (TCSEC) must enforce the reference monitor concept.
The reference monitor, as defined in AIO V5 (Harris) is: "an access control concept that refers to an abstract machine that mediates all access to objects by subjects." The security kernel, as defined in AIO V5 (Harris) is: "the hardware, firmware, and software elements of a trusted computing based (TCB) that implement the reference monitor concept. The kernel must mediate all access between subjects and objects, be protected from modification, and be verifiable as correct." The trusted computing based (TCB), as defined in AIO V5 (Harris) is: "all of the protection mechanisms within a computer system (software, hardware, and firmware) that are responsible for enforcing a security policy." The security domain, "builds upon the definition of domain (a set of resources available to a subject) by adding the fact that resources withing this logical structure (domain) are working under the same security policy and managed by the same group." The following answers are incorrect:
"The security kernel" is incorrect. One of the places a reference monitor could be implemented is in the security kernel but this is not the best answer.
"The trusted computing base" is incorrect. The reference monitor is an important concept in the TCB but this is not the best answer.
"The security domain is incorrect." The reference monitor is an important concept in the security domain but this is not the best answer.
Reference(s) used for this question:
Official ISC2 Guide to the CBK, page 324
AIO Version 3, pp. 272 - 274
AIOv4 Security Architecture and Design (pages 327 - 328)
AIOv5 Security Architecture and Design (pages 330 - 331)
Wikipedia article at https://en.wikipedia.org/wiki/Reference_monitor

NEW QUESTION: 701
Unclassified, Private, Confidential, Secret, Top Secret, and Internal Use Only are levels of
A. Security Classification
B. Data Classification
C. Object Classification
D. Change Control Classification
Answer: (SHOW ANSWER)

NEW QUESTION: 702
Which of the following answers is described as a random value used in cryptographic algorithms to ensure that patterns are not created during the encryption process?
A. IV - Initialization Vector
B. Stream Cipher
C. OTP - One Time Pad
D. Ciphertext
Answer: A (LEAVE A REPLY)

Explanation/Reference:
The basic power in cryptography is randomness. This uncertainty is why encrypted data is unusable to someone without the key to decrypt.
Initialization Vectors are a used with encryption keys to add an extra layer of randomness to encrypted data. If no IV is used the attacker can possibly break the keyspace because of patterns resulting in the encryption process. Implementation such as DES in Code Book Mode (CBC) would allow frequency analysis attack to take place.
In cryptography, an initialization vector (IV) or starting variable (SV)is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by so-called modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.
It is define by TechTarget as:
An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.
The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the ciphertext.
The following answers are incorrect:
- Stream Cipher: This isn't correct. A stream cipher is a symmetric key cipher where plaintext digits are combined with pseudorandom key stream to product cipher text.
- OTP - One Time Pad: This isn't correct but OTP is made up of random values used as key material. (Encryption key) It is considered by most to be unbreakable but must be changed with a new key after it is used which makes it impractical for common use.
- Ciphertext: Sorry, incorrect answer. Ciphertext is basically text that has been encrypted with key material (Encryption key)
The following reference(s) was used to create this question:
For more details on this TOPIC and other Qs of the Security+ CBK, subscribe to our Holistic Computer Based Tutorial (CBT) at http://www.cccure.tv
and
whatis.techtarget.com/definition/initialization-vector-IV
and
en.wikipedia.org/wiki/Initialization_vector

NEW QUESTION: 703

All of the following can be considered essential business functions that should be identified when creating a Business Impact Analysis (BIA) except one. Which of the following would not be considered an essential element of the BIA but an important TOPIC to include within the BCP plan:

A. IT Network Support

B. Accounting

C. Public Relations

D. Purchasing

Answer: C (LEAVE A REPLY)

Public Relations, although important to a company, is not listed as an essential business function that should be identified and have loss criteria developed for. All other entries are considered essential and should be identified and have loss criteria developed.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 598).

NEW QUESTION: 704

In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

A. Both client and server

B. The client's browser

C. The web server

D. The merchant's Certificate Server

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant's public key and sent to the server. The fact that the master secret is generated by the client's browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client.

Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112). Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, page 569.

NEW QUESTION: 705

How can an individual/person best be identified or authenticated to prevent local masquarading attacks?

A. UserId and password

B. Smart card and PIN code

C. Two-factor authentication

D. Biometrics

Answer: (SHOW ANSWER)

The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric identification). Physical attributes cannot be shared, borrowed, or duplicated. They ensure that you do identify the person, however they are not perfect and they would have to be supplemented by another factor.

Some people are getting thrown off by the term Masquarade. In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. Spoofing is another term used to describe this type of attack as well.

A UserId only provides for identification.

A password is a weak authentication mechanism since passwords can be disclosed, shared, written down, and more.

A smart card can be stolen and its corresponding PIN code can be guessed by an intruder. A smartcard can be borrowed by a friend of yours and you would have no clue as to who is really logging in using that smart card.

Any form of two-factor authentication not involving biometrics cannot be as reliable as a biometric system to identify the person.

Biometric identifying verification systems control people. If the person with the correct hand, eye, face, signature, or voice is not present, the identification and verification cannot take place and the desired action (i.e., portal passage, data, or resource access) does not occur.

As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be accomplished by people, not cards and

information, because unauthorized persons can (and do) obtain the cards and information.

Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost.

NOTE FROM CLEMENT:

This question has been generating lots of interest. The keyword in the question is:

Individual (the person) and also the authenticated portion as well.

I totally agree with you that Two Factors or Strong Authentication would be the strongest means of authentication. However the question is not asking what is the strongest mean of authentication, it is asking what is the best way to identify the user (individual) behind the technology. When answering questions do not make assumptions to facts not presented in the question or answers.

Nothing can beat Biometrics in such case. You cannot lend your fingerprint and pin to

someone else, you cannot borrow one of my eye balls to defeat the Iris or Retina scan. This is why it is the best method to authenticate the user.
I think the reference is playing with semantics and that makes it a bit confusing. I have improved the question to make it a lot clearer and I have also improve the explanations attached with the question.
The reference mentioned above refers to authenticating the identity for access. So the distinction is being made that there is identity and there is authentication. In the case of physical security the enrollment process is where the identity of the user would be validated and then the biometrics features provided by the user would authenticate the user on a one to one matching basis (for authentication) with the reference contained in the database of biometrics templates. In the case of system access, the user might have to provide a username, a pin, a passphrase, a smart card, and then provide his biometric attributes.
Biometric can also be used for Identification purpose where you do a one to many match. You take a facial scan of someone within an airport and you attempt to match it with a large database of known criminal and terrorists. This is how you could use biometric for Identification.
There are always THREE means of authentication, they are:
Something you know (Type 1) Something you have (Type 2) Something you are (Type 3)
Reference(s) used for this question:
TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1) , 2000, CRC Press, Chapter 1, Biometric Identification (page 7). and Search Security at http://searchsecurity.techtarget.com/definition/masquerade

NEW QUESTION: 706
Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are some of the examples of:
A. Administrative controls
B. Logical controls
C. Technical controls
D. Physical controls
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are all examples of Physical Security.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 707
Which one of the following factors is NOT one on which Authentication is based?
A. Type 1. Something you know, such as a PIN or password
B. Type 2. Something you have, such as an ATM card or smart card
C. Type 3. Something you are (based upon one or more intrinsic physical or behavioral traits), such as a fingerprint or retina scan
D. Type 4. Something you are, such as a system administrator or security administrator
Answer: D (LEAVE A REPLY)
Authentication is based on the following three factor types:
Type 1. Something you know, such as a PIN or password
Type 2. Something you have, such as an ATM card or smart card
Type 3. Something you are (Unique physical characteristic), such as a fingerprint or retina scan
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 132-133).

NEW QUESTION: 708
What can be defined as a batch process dumping backup data through communications lines to a server at an alternate location?
A. Remote journaling
B. Electronic vaulting
C. Data clustering
D. Database shadowing
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Electronic vaulting refers to the transfer of backup data to an off-site location. This is primarily a batch process of dumping backup data through communications lines to a server at an alternate location. Electronic vaulting is accomplished by backing up system data over a network. The backup location is usually at a separate geographical location known as the vault site. Vaulting can be used as a mirror or a backup mechanism using the standard incremental or differential backup cycle. Changes to the host

system are sent to the vault server in real-time when the backup method is implemented as a mirror. If vaulting updates are recorded in real-time, then it will be necessary to perform regular backups at the off-site location to provide recovery services due to inadvertent or malicious alterations to user or system data.
The following are incorrect answers:
Remote journaling refers to the parallel processing of transactions to an alternate site (as opposed to a batch dump process). Journaling is a technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location. The journal provides sufficient detail for the transaction to be replayed on the remote system. This provides for database recovery in the event that the database becomes corrupted or unavailable.
Database shadowing uses the live processing of remote journaling, but creates even more redundancy by duplicating the database sets to multiple servers. There are also additional redundancy options available within application and database software platforms. For example, database shadowing may be used where a database management system updates records in multiple locations. This technique updates an entire copy of the database at a remote location.
Data clustering refers to the classification of data into groups (clusters). Clustering may also be used, although it should not be confused with redundancy. In clustering, two or more "partners" are joined into the cluster and may all provide service at the same time. For example, in an active-active pair, both systems may provide services at any time. In the case of a failure, the remaining partners may continue to provide service but at a decreased capacity.
The following resource(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20403-20407 and 20411-20414 and 20375-20377 and 20280-20283). Auerbach Publications. Kindle Edition.

NEW QUESTION: 709
The Diffie-Hellman algorithm is primarily used to provide which of the following?
A. Confidentiality
B. Key Agreement
C. Integrity
D. Non-repudiation
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Diffie and Hellman describe a means for two parties to agree upon a shared secret in such a way that the secret will be unavailable to eavesdroppers. This secret may then be converted into cryptographic keying material for other (symmetric) algorithms. A large number of minor variants of this process exist. See RFC
2631 Diffie-Hellman Key Agreement Method for more details.
In 1976, Diffie and Hellman were the first to introduce the notion of public key cryptography, requiring a system allowing the exchange of secret keys over non-secure channels. The Diffie-Hellman algorithm is

used for key exchange between two parties communicating with each other, it cannot be used for encrypting and decrypting messages, or digital signature.
Diffie and Hellman sought to address the issue of having to exchange keys via courier and other unsecure means. Their efforts were the FIRST asymmetric key agreement algorithm. Since the Diffie-Hellman algorithm cannot be used for encrypting and decrypting it cannot provide confidentiality nor integrity. This algorithm also does not provide for digital signature functionality and thus non-repudiation is not a choice.
NOTE: The DH algorithm is susceptible to man-in-the-middle attacks.
KEY AGREEMENT VERSUS KEY EXCHANGE
A key exchange can be done multiple way. It can be done in person, I can generate a key and then encrypt the key to get it securely to you by encrypting it with your public key. A Key Agreement protocol is done over a public medium such as the internet using a mathematical formula to come out with a common value on both sides of the communication link, without the ennemy being able to know what the common agreement is.
The following answers were incorrect:
All of the other choices were not correct choices
Reference(s) used for this question:
Shon Harris, CISSP All In One (AIO), 6th edition . Chapter 7, Cryptography, Page 812.
http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
http://www.google.com/patents?vid=4200770

NEW QUESTION: 710
The standard server port number for HTTP is which of the following?
A. 81
B. 80
C. 8080
D. 8180
Answer: B (LEAVE A REPLY)
Explanation/Reference:
HTTP is Port 80.
Reference: MAIWALD, Eric, Network Security: A Beginner's Guide, McGraw-Hill/Osborne Media, 2001, page 135.

NEW QUESTION: 711
The controls that usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists are associated with:
A. Preventive/physical
B. Detective/technical
C. Detective/physical
D. Detective/administrative
Answer: (SHOW ANSWER)

Section: Access Control
Explanation/Reference:
Detective/physical controls usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 712
Which of the following types of Intrusion Detection Systems uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host?
A. Network-based ID systems.
B. Anomaly Detection.
C. Host-based ID systems.
D. Signature Analysis.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
There are two basic IDS analysis methods: pattern matching (also called signature analysis) and anomaly detection.
Anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host. Anomalies may include but are not limited to:
Multiple failed log-on attempts
Users logging in at strange hours
Unexplained changes to system clocks
Unusual error messages
The following are incorrect answers:
Network-based ID Systems (NIDS) are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network.
Host-based ID Systems (HIDS) is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.
Signature Analysis Some of the first IDS products used signature analysis as their detection method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the data stream) to produce an alert if that pattern was detected. For example, an attacker manipulating an

FTP server may use a tool that sends a specially constructed packet. If that particular packet pattern is known, it can be represented in the form of a signature that IDS can then compare to incoming packets. Pattern- based IDS will have a database of hundreds, if not thousands, of signatures that are compared to traffic streams. As new attack signatures are produced, the system is updated, much like antivirus solutions.

There are drawbacks to pattern-based IDS. Most importantly, signatures can only exist for known attacks.

If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS. Additionally, if an attacker knows that the IDS is present, he or she can alter his or her methods to avoid detection. Changing packets and data streams, even slightly, from known signatures can cause an IDS to miss the attack. As with some antivirus systems, the IDS is only as good as the latest signature database on the system.

For additional information on Intrusion Detection Systems - http://en.wikipedia.org/wiki/Intrusion_detection_system

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3623-3625, 3649-3654, 3666-3686). Auerbach Publications. Kindle Edition.

NEW QUESTION: 713

What is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept?

A. The reference monitor

B. Protection rings

C. A security kernel

D. A protection domain

Answer: C (LEAVE A REPLY)

A security kernel is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept. A reference monitor is a system component that enforces access controls on an object. A protection domain consists of the execution and memory space assigned to each process. The use of protection rings is a scheme that supports multiple protection domains.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 194).

NEW QUESTION: 714

If an employee's computer has been used by a fraudulent employee to commit a crime, the hard disk may be seized as evidence and once the investigation is complete it would follow the normal steps of the Evidence Life Cycle. In such case, the Evidence life cycle would not include which of the following steps listed below?

A. Acquisition collection and identification

B. Analysis

C. Storage, preservation, and transportation
D. Destruction
Answer: D (LEAVE A REPLY)
Unless the evidence is illegal then it should be returned to owner, not destroyed.
The Evidence Life Cycle starts with the discovery and collection of the evidence. It progresses through the following series of states until it is finally returned to the victim or owner:
Acquisition collection and identification
Analysis
Storage, preservation, and transportation
Presented in court
Returned to victim (owner)
The Second edition of the ISC2 book says on page 529-530:
Identifying evidence: Correctly identifying the crime scene, evidence, and potential containers of evidence. Collecting or acquiring evidence: Adhering to the criminalistic principles and ensuring that the contamination and the destruction of the scene are kept to a minimum. Using sound, repeatable, collection techniques that allow for the demonstration of the accuracy and integrity of evidence, or copies of evidence. Examining or analyzing the evidence: Using sound scientific methods to determine the characteristics of the evidence, conducting comparison for individuation of evidence, and conducting event reconstruction. Presentation of findings: Interpreting the output from the examination and analysis based on findings of fact and articulating these in a format appropriate for the intended audience (e.g., court brief, executive memo, report).
Note on returning the evidence to the Owner/Victim
The final destination of most types of evidence is back with its original owner. Some types of evidence, such as drugs or drug paraphernalia (i.e., contraband), are destroyed after the trial.
Any evidence gathered during a search, although maintained by law enforcement, is legally under the control of the courts. And although a seized item may be yours and may even have your name on it, it might not be returned to you unless the suspect signs a release or after a hearing by the court.
Unfortunately, many victims do not want to go to trial; they just want to get their property back.
Many investigations merely need the information on a disk to prove or disprove a fact in question; thus, there is no need to seize the entire system. Once a schematic of the system is drawn or photographed, the hard disk can be removed and then transported to a forensic lab for copying.
Mirror copies of the suspect disk are obtained using forensic software and then one of those copies can be returned to the victim so that business operations can resume.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 309). and The Official Study Book, Second Edition, Page 529-230

NEW QUESTION: 715
A timely review of system access audit records would be an example of which of the basic security functions?

A. avoidance
B. deterrence
C. prevention
D. detection
Answer: D (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
By reviewing system logs you can detect events that have occured.
The following answers are incorrect:
avoidance. This is incorrect, avoidance is a distractor. By reviewing system logs you have not avoided anything.
deterrence. This is incorrect because system logs are a history of past events. You cannot deter something that has already occurred.
prevention. This is incorrect because system logs are a history of past events. You cannot prevent something that has already occurred.

NEW QUESTION: 716
Which of the following best describes what would be expected at a "hot site"?
A. Computers, climate control, cables and peripherals
B. Computers and peripherals
C. Computers and dedicated climate control systems.
D. Dedicated climate control systems
Answer: A (LEAVE A REPLY)
A Hot Site contains everything needed to become operational in the shortest amount of time.
The following answers are incorrect:
Computers and peripherals. Is incorrect because no mention is made of cables. You would not be fully operational without those.
Computers and dedicated climate control systems. Is incorrect because no mention is made of peripherals. You would not be fully operational without those.
Dedicated climate control systems. Is incorrect because no mentionis made of computers, cables and peripherals. You would not be fully operational without those.
According to the OIG, a hot site is defined as a fully configured site with complete customer required hardware and software provided by the service provider. A hot site in the context of the CBK is always a RENTAL place. If you have your own site fully equipped that you make use of in case of disaster that would be called a redundant site or an alternate site.
Wikipedia: "A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data."
References:
OIG CBK, Business Continuity and Disaster Recovery Planning (pages 367 - 368)
AIO, 3rd Edition, Business Continuity Planning (pages 709 - 714)
AIO, 4th Edition, Business Continuity Planning , p 790.

Wikipedia - http://en.wikipedia.org/wiki/Hot_site#Hot_Sites

NEW QUESTION: 717
Which type of attack would a competitive intelligence attack best classify as?
A. Business attack
B. Intelligence attack
C. Financial attack
D. Grudge attack
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Business attacks concern information loss through competitive intelligence gathering and computer-related attacks. These attacks can be very costly due the loss of trade secrets and reputation.
Intelligence attacks are aimed at sensitive military and law enforcement files containing military data and investigation reports.
Financial attacks are concerned with frauds to banks and large corporations.
Grudge attacks are targeted at individuals and companies who have done something that the attacker doesn't like.
The CISSP for Dummies book has nice coverage of the different types of attacks, here is an extract:
Terrorism Attacks
Terrorism exists at many levels on the Internet. In April 2001, during a period of tense relations between China and the U.S. (resulting from the crash landing of a U.S. Navy reconnaissance plane on Hainan Island), Chinese hackers (cyberterrorists) launched a major effort to disrupt critical U.S. infrastructure, which included U.S.
government and military systems.
Following the terrorist attacks against the U.S. on September 11, 2001, the general public became painfully aware of the extent of terrorism on the Internet. Terrorist organizations and cells are using online capabilities to coordinate attacks, transfer funds, harm international commerce, disrupt critical systems, disseminate propaganda, and gain useful information about developing techniques and instruments of terror, including nuclear , biological, and chemical weapons.
Military and intelligence attacks
Military and intelligence attacks are perpetrated by criminals, traitors, or foreign intelligence agents seeking classified law enforcement or military information. Such attacks may also be carried out by governments during times of war and conflict.
Financial attacks
Banks, large corporations, and e-commerce sites are the targets of financial attacks, all of which are motivated by greed. Financial attacks may seek to steal or embezzle funds, gain access to online financial information, extort individuals or businesses, or obtain the personal credit card numbers of customers.
Business attacks

Businesses are becoming the targets of more and more computer and Internet attacks. These attacks include competitive intelligence gathering, denial of service, and other computer- related attacks. Businesses are often targeted for several reasons including Lack of expertise: Despite heightened security awareness, a shortage of qualified security professionals still exists, particularly in private enterprise.

Lack of resources: Businesses often lack the resources to prevent, or even detect, attacks against their systems.

Lack of reporting or prosecution : Because of public relations concerns and the inability to prosecute computer criminals due to either a lack of evidence or a lack of properly handled evidence, the majority of business attacks still go unreported.

The cost to businesses can be significant, including loss of trade secrets or proprietary information, loss of revenue, and loss of reputation.

Grudge attacks

Grudge attacks are targeted at individuals or businesses and are motivated by a desire to take revenge against a person or organization. A disgruntled employee, for example, may steal trade secrets, delete valuable data, or plant a logic bomb in a critical system or application.

Fortunately, these attacks (at least in the case of a disgruntled employee) can be easier to prevent or prosecute than many other types of attacks because:

The attacker is often known to the victim.

The attack has a visible impact that produces a viable evidence trail.

Most businesses (already sensitive to the possibility of wrongful termination suits) have well-established termination procedures

"Fun" attacks

"Fun" attacks are perpetrated by thrill seekers and script kiddies who are motivated by curiosity or excitement.

Although these attackers may not intend to do any harm or use any of the information that they access, they're still dangerous and their activities are still illegal.

These attacks can also be relatively easy to detect and prosecute. Because the perpetrators are often script kiddies or otherwise inexperienced hackers, they may not know how to cover their tracks effectively.

Also, because no real harm is normally done nor intended against the system, it may be tempting (although ill advised) for a business to prosecute the individual and put a positive public relations spin on the incident.

You've seen the film at 11: "We quickly detected the attack, prevented any harm to our network, and prosecuted the responsible individual; our security is unbreakable !" Such action, however, will likely motivate others to launch a more serious and concerted grudge attack against the business.

Many computer criminals in this category only seek notoriety. Although it's one thing to brag to a small circle of friends about defacing a public Web site, the wily hacker who appears on CNN reaches the next level of hacker celebrity-dom. These twisted individuals want to be caught to revel in their 15 minutes of fame.

References:

ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 187) and CISSP Professional Study Guide by James Michael Stewart, Ed Tittel, Mike Chapple, page 607-609 and CISSP for Dummies, Miller L. H. and Gregory P. H. ISBN: 0470537914, page 309-311

NEW QUESTION: 718
Which of the following control pairings include: organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?
A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The Answer: Preventive/Administrative Pairing: These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 719
Valuable paper insurance coverage does not cover damage to which of the following?
A. Inscribed, printed and Written documents
B. Manuscripts
C. Records
D. Money and Securities
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
All businesses are driven by records. Even in today's electronic society businesses generate mountains of critical documents everyday. Invoices, client lists, calendars, contracts, files, medical records, and innumerable other records are generated every day.
Stop and ask yourself what happens if your business lost those documents today.
Valuable papers business insurance coverage provides coverage to your business in case of a loss of vital records. Over the years policy language has evolved to include a number of different types of records.

Generally, the policy will cover "written, printed, or otherwise inscribed documents and records, including books, maps, films, drawings, abstracts, deeds, mortgages, and manuscripts." But, read the policy coverage carefully. The policy language typically "does not mean "money" or "securities," converted data,programs or instructions used in your data processing operations, including the materials on which the data is recorded." The coverage is often included as a part of property insurance or as part of a small business owner policy. For example, a small business owner policy includes in many cases valuable papers coverage up to $25,000.

It is important to realize what the coverage actually entails and, even more critical, to analyze your business to determine what it would cost to replace records.

The coverage pays for the loss of vital papers and the cost to replace the records up to the limit of the insurance and after application of any deductible. For example, the insurer will pay to have waterlogged papers dried and reproduced (remember, fires are put out by water and the fire department does not stop to remove your book keeping records). The insurer may cover temporary storage or the cost of moving records to avoid a loss.

For some businesses, losing customer lists, some business records, and contracts, can mean the expense and trouble of having to recreate those documents, but is relatively easy and a low level risk and loss. Larger businesses and especially professionals (lawyers, accountants, doctors) are in an entirely separate category and the cost of replacement of documents is much higher. Consider, in analyzing your business and potential risk, what it would actually cost to reproduce your critical business records. Would you need to hire temporary personnel? How many hours of productivity would go into replacing the records? Would you need to obtain originals? Would original work need to be recreated (for example, home inspectors, surveyors, cartographers)?

Often when a business owner considers the actual cost related to the reproduction of records, the owner quickly realizes that their business insurance policy limits for valuable papers coverage is woefully inadequate.

Insurers (and your insurance professional)will often suggest higher coverages for valuable papers. The extra premium is often worth the cost and should be considered.

Finally, most policies will require records to be protected. You need to review your declarations pages and speak with your insurer to determine what is required. Some insurers may offer discounted coverage if there is a document retention and back up plan in place and followed. There are professional organizations that can assist your business in designing a records management policy to lower the risk (and your premiums). For example, ARMA International has been around since 1955 and its members consist of some of the top document retention and storage companies.

Reference(s) used for this question:

http://businessinsure.about.com/od/propertyinsurance/f/vpcov.htm

NEW QUESTION: 720

In a known plaintext attack, the cryptanalyst has knowledge of which of the following?

A. the ciphertext and the key

B. the plaintext and the secret key

C. both the plaintext and the associated ciphertext of several messages

D. the plaintext and the algorithm

Answer: C (LEAVE A REPLY)

Explanation/Reference:

In a known plaintext attack, the attacker has the plaintext and ciphertext of one or more messages. The goal is to discover the key used to encrypt the messages so that other messages can be deciphered and read.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 3rd Ed., chapter 8: Cryptography (page 676). Also check out: Handbook of Applied Cryptography 4th Edition by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone.

NEW QUESTION: 721

Which of the following statements pertaining to the Bell-LaPadula is TRUE if you are NOT making use of the strong star property?

A. It allows "read up."

B. It addresses covert channels.

C. It addresses management of access controls.

D. It allows "write up."

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Bell-LaPadula Confidentiality Model10 The Bell-LaPadula model is perhaps the most well-known and significant security model, in addition to being one of the oldest models used in the creation of modern secure computing systems. Like the Trusted Computer System Evaluation Criteria (or TCSEC), it was inspired by early U.S. Department of Defense security policies and the need to prove that confidentiality could be maintained. In other words, its primary goal is to prevent disclosure as the model system moves from one state (one point in time) to another.

When the strong star property is not being used it means that both the property and the Simple Security Property rules would be applied.

The Star (*) property rule of the Bell-LaPadula model says that subjects cannot write down, this would compromise the confidentiality of the information if someone at the secret layer would write the object down to a confidential container for example.

The Simple Security Property rule states that the subject cannot read up which means that a subject at the secret layer would not be able to access objects at Top Secret for example.

You must remember: The model tells you about are NOT allowed to do. Anything else would be allowed. For example within the Bell LaPadula model you would be allowed to write up as it does not compromise the security of the information. In fact it would upgrade it to the point that you could lock yourself out of your own information if you have only a secret security clearance.

The following are incorrect answers because they are all FALSE:

"It allows read up" is incorrect. The "simple security" property forbids read up.

"It addresses covert channels" is incorrect. Covert channels are not addressed by the Bell-LaPadula model.

"It addresses management of access controls" is incorrect. Management of access controls are beyond the scope of the Bell-LaPadula model.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17595-17600). Auerbach Publications. Kindle Edition.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 722
Which of the following is most appropriate to notify an internal user that session monitoring is being conducted?
A. Logon Banners
B. Wall poster
C. Employee Handbook
D. Written agreement
Answer: D (LEAVE A REPLY)
Explanation/Reference:
This is a tricky question, the keyword in the question is Internal users.
There are two possible answers based on how the question is presented, this question could either apply to internal users or ANY anonymous/external users.
Internal users should always have a written agreement first, then logon banners serve as a constant reminder.
Banners at the log-on time should be used to notify external users of any monitoring that is being conducted. A good banner will give you a better legal stand and also makes it obvious the user was warned about who should access the system, who is authorized and unauthorized, and if it is an unauthorized user then he is fully aware of trespassing. Anonymous/External users, such as those logging into a web site, ftp server or even a mail server; their only notification system is the use of a logon banner.
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 50.
and
Shon Harris, CISSP All-in-one, 5th edition, pg 873

NEW QUESTION: 723

Which of the following transmission media would NOT be affected by cross talk or interference?

A. Copper cable

B. Radio System

C. Satellite radiolink

D. Fiber optic cables

Answer: (SHOW ANSWER)

Only fiber optic cables are not affected by crosstalk or interference.

For your exam you should know the information about transmission media:

Copper Cable Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data. Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Image Source http://i00.i.aliimg.com/photo/v0/570456138/FRLS_HR_PVC_Copper_Cable.jpg

Coaxial cable Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable are expensive and does not support many LAN's. It supports data and video Coaxial Cable

Image Source - http://www.tlc-direct.co.uk/Images/Products/size_3/CARG59.JPG

Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Radio System

Radio systems are used for short distance,cheap and easy to tap.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Fiber Optics

Image Source - http://aboveinfranet.com/wp-content/uploads/2014/04/fiber-optic-cablesabove-infranet-solutions.jpg

Microwave radio system Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimetre; these are called microwaves. Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System

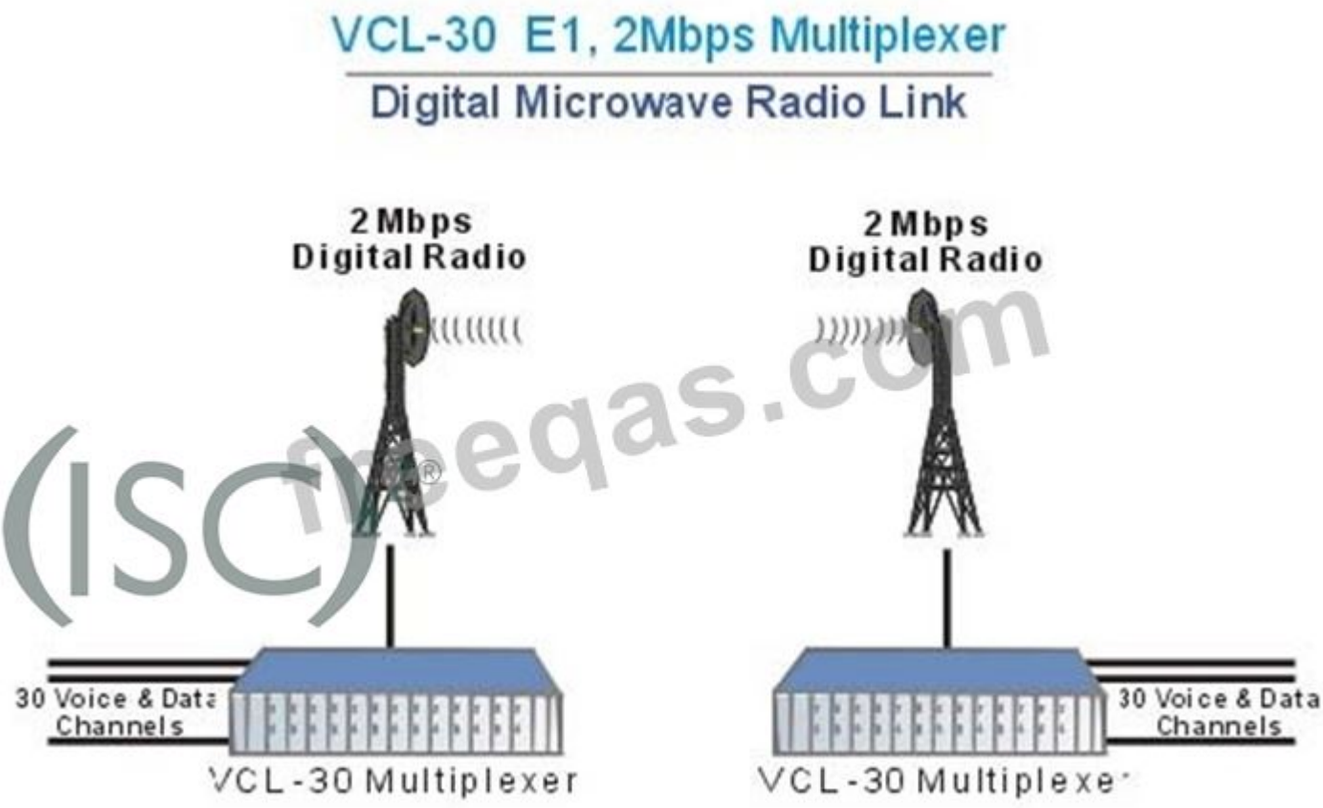


Image Source http://www.valiantcom.com/images/applications/e1_digital_microwave_radio.gif
Satellite Radio Link Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.
Satellite radio link uses transponder to send information and easy to tap.
The following answers are incorrect:
Copper Cable - Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Radio System - Radio systems are used for short distance,cheap and easy to tap.
Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 265 &
Official ISC2 guide to CISSP CBK 3rd Edition Page number 233

NEW QUESTION: 724
A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:
A. concern that the laser beam may cause eye damage
B. the iris pattern changes as a person grows older.
C. there is a relatively high rate of false accepts.
D. the optical unit must be positioned so that the sun does not shine into the aperture.

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Because the optical unit utilizes a camera and infrared light to create the images, sun light can impact the aperture so it must not be positioned in direct light of any type. Because the subject does not need to have direct contact with the optical reader, direct light can impact the reader.

An Iris recognition is a form of biometrics that is based on the uniqueness of a subject's iris. A camera like device records the patterns of the iris creating what is known as Iriscode.

It is the unique patterns of the iris that allow it to be one of the most accurate forms of biometric identification of an individual. Unlike other types of biometics, the iris rarely changes over time. Fingerprints can change over time due to scaring and manual labor, voice patterns can change due to a variety of causes, hand geometry can also change as well. But barring surgery or an accident it is not usual for an iris to change. The subject has a high-resoulution image taken of their iris and this is then converted to Iriscode. The current standard for the Iriscode was developed by John Daugman. When the subject attempts to be authenticated an infrared light is used to capture the iris image and this image is then compared to the Iriscode. If there is a match the subject's identity is confirmed. The subject does not need to have direct contact with the optical reader so it is a less invasive means of authentication then retinal scanning would be.

Reference(s) used for this question:

AIO, 3rd edition, Access Control, p 134.

AIO, 4th edition, Access Control, p 182.

Wikipedia - http://en.wikipedia.org/wiki/Iris_recognition

The following answers are incorrect:

concern that the laser beam may cause eye damage. The optical readers do not use laser so, concern that the laser beam may cause eye damage is not an issue.

the iris pattern changes as a person grows older. The question asked about the physical installation of the scanner, so this was not the best answer. If the question would have been about long term problems then it could have been the best choice. Recent research has shown that Irises actually do change over time: http://www.nature.com/news/ageing-eyes-hinder-biometric-scans-1.10722 there is a relatively high rate of false accepts. Since the advent of the Iriscode there is a very low rate of false accepts, in fact the algorithm used has never had a false match. This all depends on the quality of the equipment used but because of the uniqueness of the iris even when comparing identical twins, iris patterns are unique.

NEW QUESTION: 725

What works as an E-mail message transfer agent?

A. SMTP

B. SNMP

C. S-RPC

D. S/MIME

Answer: A (LEAVE A REPLY)

Section: Network and Telecommunications

Explanation/Reference:

SMTP (Simple Mail Transfer Protocol) works as a message transfer agent.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 821.

NEW QUESTION: 726
What is the highest amount a company should spend annually on countermeasures for protecting an asset valued at $1,000,000 from a threat that has an annualized rate of occurrence (ARO) of once every five years and an exposure factor (EF) of 30%?
A. $300,000
B. $150,000
C. $60,000
D. $1,500
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The cost of a countermeasure should not be greater in cost than the risk it mitigates (ALE). For a quantitative risk assessment, the equation is ALE = ARO x SLE where the SLE is calculated as the product of asset value x exposure factor. An event that happen once every five years would have an ARO of .2 (1 divided by 5).
SLE = Asset Value (AV) x Exposure Fact (EF)
SLE = 1,000,000 x .30 = 300,000
ALE = SLE x Annualized Rate of Occurance (ARO)
ALE = 300,000 x .2 = 60,000
Know your acronyms:
ALE -- Annual loss expectancy
ARO -- Annual rate of occurrence
SLE -- Single loss expectancy
The following are incorrect answers:
$300,000 is incorrect. See the explanation of the correct answer for the correct calculation.
$150,000 is incorrect. See the explanation of the correct answer for the correct calculation.
$1,500 is incorrect. See the explanation of the correct answer for the correct calculation.
Reference(s) used for this question:
Mc Graw Hill, Shon Harris, CISSP All In One (AIO) book, Sixth Edition , Pages 87-88 and Official ISC2 Guide to the CISSP Exam, (OIG), Pages 60-61

NEW QUESTION: 727
Which of the following virus types changes some of its characteristics as it spreads?
A. Boot Sector
B. Parasitic
C. Stealth
D. Polymorphic

Answer: D (LEAVE A REPLY)
A Polymorphic virus produces varied but operational copies of itself in hopes of evading anti-virus software.
The following answers are incorrect:
boot sector. Is incorrect because it is not the best answer. A boot sector virus attacks the boot sector of a drive. It describes the type of attack of the virus and not the characteristics of its composition.
parasitic. Is incorrect because it is not the best answer. A parasitic virus attaches itself to other files but does not change its characteristics.
stealth. Is incorrect because it is not the best answer. A stealth virus attempts to hide changes of the affected files but not itself.

NEW QUESTION: 728
Which of the following are required for Life-Cycle Assurance?
A. System Architecture and Design specification.
B. Security Testing and Covert Channel Analysis.
C. Security Testing and Trusted distribution.
D. Configuration Management and Trusted Facility Management.
Answer: (SHOW ANSWER)
Explanation/Reference:
Security testing and trusted distribution are required for Life-Cycle Assurance.
The following answers are incorrect:
System Architecture and Design specification. Is incorrect because System Architecture is not requried for Life-Cycle Assurance.
Security Testing and Covert Channel Analysis. Is incorrect because Covert Channel Analysis is not requried for Life-Cycle Assurance.
Configuration Management and Trusted Facility Management. Is incorrect because Trusted Facility Management. is not requried for Life-Cycle Assurance.

NEW QUESTION: 729
Which of the following is NOT a task normally performed by a Computer Incident Response Team (CIRT)?
A. Develop an information security policy.
B. Coordinate the distribution of information pertaining to the incident to the appropriate parties.
C. Mitigate risk to the enterprise.
D. Assemble teams to investigate the potential vulnerabilities.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Writing a corporate security policy is normally a task of upper management in an organization. Other tasks would usually be performed by a Computer Incident Response Team.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
64).

NEW QUESTION: 730
At which layer of ISO/OSI does the fiber optics work?
A. Network layer
B. Transport layer
C. Data link layer
D. Physical layer
Answer: D (LEAVE A REPLY)
Physical
layer The Physical layer is responsible for the transmission of the data through the physical medium. This includes such things as cables. Fiber optics is a cabling mechanism which works at Physical layer of OSI model
All of the other answers are incorrect.
The following reference(s) were/was used to create this question: Shon Harris all in one - Chapter 7 (Cabling)

NEW QUESTION: 731
The control of communications test equipment should be clearly addressed by security policy for which of the following reasons?
A. Test equipment is easily damaged.
B. Test equipment can be used to browse information passing on a network.
C. Test equipment is difficult to replace if lost or stolen.
D. Test equipment must always be available for the maintenance personnel.
Answer: (SHOW ANSWER)
Explanation/Reference:
Test equipment must be secured. There are equipment and other tools that if in the wrong hands could be used to "sniff" network traffic and also be used to commit fraud. The storage and use of this equipment should be detailed in the security policy for this reason.
The following answers are incorrect:
Test equipment is easily damaged. Is incorrect because it is not the best answer, and from a security point of view not relevent.
Test equipment is difficult to replace if lost or stolen. Is incorrect because it is not the best answer, and from a security point of view not relevent.
Test equipment must always be available for the maintenance personnel. Is incorrect because it is not the best answer, and from a security point of view not relevent.
References:
OIG CBK Operations Security (pages 642 - 643)

NEW QUESTION: 732
What are called user interfaces that limit the functions that can be selected by a user?
A. Constrained user interfaces
B. Limited user interfaces
C. Mini user interfaces
D. Unlimited user interfaces
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Constrained user interfaces limit the functions that can be selected by a user.
Another method for controlling access is by restricting users to specific functions based on their role in the system. This is typically implemented by limiting available menus, data views, encryption, or by physically constraining the user interfaces.
This is common on devices such as an automated teller machine (ATM). The advantage of a constrained user interface is that it limits potential avenues of attack and system failure by restricting the processing options that are available to the user.
On an ATM machine, if a user does not have a checking account with the bank he or she will not be shown the "Withdraw money from checking" option. Likewise, an information system might have an "Add/Remove Users" menu option for administrators, but if a normal, non-administrative user logs in he or she will not even see that menu option. By not even identifying potential options for non-qualifying users, the system limits the potentially harmful execution of unauthorized system or application commands.
Many database management systems have the concept of "views." A database view is an extract of the data stored in the database that is filtered based on predefined user or system criteria. This permits multiple users to access the same database while only having the ability to access data they need (or are allowed to have) and not data for another user. The use of database views is another example of a constrained user interface.
The following were incorrect answers:
All of the other choices presented were bogus answers.
The following reference(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1989-2002). Auerbach Publications. Kindle Edition.

NEW QUESTION: 733
Another type of access control is lattice-based access control. In this type of control a lattice model is applied. How is this type of access control concept applied?
A. The pair of elements is the subject and object, and the subject has an upper bound equal or higher than the upper bound of the object being accessed.
B. The pair of elements is the subject and object, and the subject has an upper bound lower then the upper bound of the object being accessed.

C. The pair of elements is the subject and object, and the subject has no special upper or lower bound needed within the lattice.
D. The pair of elements is the subject and object, and the subject has no access rights in relation to an object.
Answer: (SHOW ANSWER)
Explanation/Reference:
To apply this concept to access control, the pair of elements is the subject and object, and the subject has to have an upper bound equal or higher than the object being accessed.
WIKIPEDIA has a great explanation as well:
In computer security, lattice-based access control (LBAC) is a complex access control based on the interaction between any combination of objects (such as resources, computers, and applications) and subjects (such as individuals, groups or organizations).
In this type of label-based mandatory access control model, a lattice is used to define the levels of security that an object may have and that a subject may have access to. The subject is only allowed to access an object if the security level of the subject is greater than or equal to that of the object.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.
and
http://en.wikipedia.org/wiki/Lattice-based_access_control

NEW QUESTION: 734
What is the essential difference between a self-audit and an independent audit?
A. Tools used
B. Results
C. Objectivity
D. Competence
Answer: (SHOW ANSWER)
To maintain operational assurance, organizations use two basic methods: system audits and monitoring. Monitoring refers to an ongoing activity whereas audits are one-time or periodic events and can be either internal or external. The essential difference between a self-audit and an independent audit is objectivity, thus indirectly affecting the results of the audit. Internal and external auditors should have the same level of competence and can use the same tools.
Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 25).

NEW QUESTION: 735
Which of the following is often the greatest challenge of distributed computing solutions?
A. scalability
B. security

C. heterogeneity
D. usability
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The correct answer to this "security". It is a major factor in deciding if a centralized or decentralized environment is more appropriate.
Example: In a centralized computing environment, you have a central server and workstations (often "dumb terminals") access applications, data, and everything else from that central servers. Therefore, the vast majority of your security resides on a centrally managed server. In a decentralized (or distributed) environment, you have a collection of PC's each with their own operating systems to maintain, their own software to maintain, local data storage requiring protection and backup. You may also have PDA's and "smart phones", data watches, USB devices of all types able to store data... the list gets longer all the time.
It is entirely possible to reach a reasonable and acceptable level of security in a distributed environment. But doing so is significantly more difficult, requiring more effort, more money, and more time.
The other answers are not correct because:
scalability - A distributed computing environment is almost infinitely scalable. Much more so than a centralized environment. This is therefore a bad answer.
heterogeneity - Having products and systems from multiple vendors in a distributed environment is significantly easier than in a centralized environment. This would not be a "challenge of distributed computing solutions" and so is not a good answer.
usability - This is potentially a challenge in either environment, but whether or not this is a problem has very little to do with whether it is a centralized or distributed environment. Therefore, this would not be a good answer.
Reference:
Official ISC2 Guide page: 313-314
All in One Third Edition page: (unavailable at this time)

NEW QUESTION: 736
Which layer of the TCP/IP protocol model would best correspond to the OSI/ISO model's network layer?
A. Network access layer
B. Application layer
C. Host-to-host transport layer
D. Internet layer
Answer: D (LEAVE A REPLY)
The Internet layer corresponds to the OSI's network layer. It handles the
routing of packets among multiple networks.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3:
Telecommunications and Network Security (page 85).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 737
Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?
A. Extensible Authentication Protocol
B. Challenge Handshake Authentication Protocol
C. Remote Authentication Dial-In User Service
D. Multilevel Authentication Protocol.
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines the Extensible Authentication Protocol as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge- response, and arbitrary dialog sequences. It is intended for use primarily by a host or router that connects to a PPP network server via switched circuits or dial-up lines. The Remote Authentication Dial-In User Service (RADIUS) is defined as an Internet protocol for carrying dial-in user's authentication information and configuration information between a shared, centralized authentication server and a network access server that needs to authenticate the users of its network access ports. The other option is a distracter.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 738
What prevents a process from accessing another process' data?
A. Memory segmentation
B. Process isolation
C. The reference monitor
D. Data hiding
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Process isolation is where each process has its own distinct address space for its application code and data. In this way, it is possible to prevent each process from accessing another process' data. This

prevents data leakage, or modification to the data while it is in memory. Memory segmentation is a virtual memory management mechanism. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. Data hiding, also known as information hiding, is a mechanism that makes information available at one processing level is not available at another level.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 739
What can be defined as secret communications where the very existence of the message is hidden?
A. Clustering
B. Steganography
C. Cryptology
D. Vernam cipher
Answer: B (LEAVE A REPLY)
Steganography is a secret communication where the very existence of the message is hidden. For example, in a digital image, the least significant bit of each word can be used to comprise a message without causing any significant change in the image. Key clustering is a situation in which a plaintext message generates identical ciphertext messages using the same transformation algorithm but with different keys. Cryptology encompasses cryptography and cryptanalysis. The Vernam Cipher, also called a one-time pad, is an encryption scheme using a random key of the same size as the message and is used only once. It is said to be unbreakable, even with infinite resources.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 134).

NEW QUESTION: 740
If an organization were to monitor their employees' e-mail, it should not:
A. Monitor only a limited number of employees.
B. Inform all employees that e-mail is being monitored.
C. Explain who can read the e-mail and how long it is backed up.
D. Explain what is considered an acceptable use of the e-mail system.
Answer: (SHOW ANSWER)
Explanation/Reference:
Monitoring has to be conducted is a lawful manner and applied in a consistent fashion; thus should be applied uniformly to all employees, not only to a small number.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 304).

NEW QUESTION: 741
What can be defined as secret communications where the very existence of the message is hidden?
A. Clustering
B. Steganography

C. Cryptology
D. Vernam cipher
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Steganography is a secret communication where the very existence of the message is hidden. For example, in a digital image, the least significant bit of each word can be used to comprise a message without causing any significant change in the image. Key clustering is a situation in which a plaintext message generates identical ciphertext messages using the same transformation algorithm but with different keys. Cryptology encompasses cryptography and cryptanalysis. The Vernam Cipher, also called a one-time pad, is an encryption scheme using a random key of the same size as the message and is used only once. It is said to be unbreakable, even with infinite resources.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 134).

NEW QUESTION: 742
Which of the following describes a computer processing architecture in which a language compiler or pre- processor breaks program instructions down into basic operations that can be performed by the processor at the same time?
A. Very-Long Instruction-Word Processor (VLIW)
B. Complex-Instruction-Set-Computer (CISC)
C. Reduced-Instruction-Set-Computer (RISC)
D. Super Scalar Processor Architecture (SCPA)
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Very long instruction word (VLIW) describes a computer processing architecture in which a language compiler or pre-processor breaks program instruction down into basic operations that can be performed by the processor in parallel (that is, at the same time). These operations are put into a very long instruction word which the processor can then take apart without further analysis, handing each operation to an appropriate functional unit.
The following answer are incorrect:
The term "CISC" (complex instruction set computer or computing) refers to computers designed with a full set of computer instructions that were intended to provide needed capabilities in the most efficient way.
Later, it was discovered that, by reducing the full set to only the most frequently used instructions, the computer would get more work done in a shorter amount of time for most applications. Intel's Pentium microprocessors are CISC microprocessors.
The PowerPC microprocessor, used in IBM's RISC System/6000 workstation and Macintosh computers, is a RISC microprocessor. RISC takes each of the longer, more complex instructions from a CISC design and reduces it to multiple instructions that are shorter and faster to process. RISC technology has been a staple of mobile devices for decades, but it is now finally poised to take on a serious role in data center

servers and server virtualization. The latest RISC processors support virtualization and will change the way computing resources scale to meet workload demands.
A superscalar CPU architecture implements a form of parallelism called instruction level parallelism within a single processor. It therefore allows faster CPU throughput than would otherwise be possible at a given clock rate. A superscalar processor executes more than one instruction during a clock cycle by simultaneously dispatching multiple instructions to redundant functional units on the processor. Each functional unit is not a separate CPU core but an execution resource within a single CPU such as an arithmetic logic unit, a bit shifter, or a multiplier.
Reference(s) Used for this question:
http://whatis.techtarget.com/definition/0,,sid9_gci214395,00.html
and
http://searchcio-midmarket.techtarget.com/definition/CISC
and
http://en.wikipedia.org/wiki/Superscalar

NEW QUESTION: 743
Which of the following is used in database information security to hide information?
A. Inheritance
B. Polyinstantiation
C. Polymorphism
D. Delegation
Answer: B (LEAVE A REPLY)
Polyinstantiation enables a relation to contain multiple tuples with the same primary keys with each instance distinguished by a security level. When this information is inserted into a database, lower-level subjects need to be restricted from this information. Instead of just restricting access, another set of data is created to fool the lower-level subjects into thinking that the information actually means something else. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 727).

NEW QUESTION: 744
What is the Maximum Tolerable Downtime (MTD)?
A. Maximum elapsed time required to complete recovery of application data
B. Minimum elapsed time required to complete recovery of application data
C. Maximum elapsed time required to move back to primary site after a major disruption
D. It is maximum delay businesses can tolerate and still remain viable
Answer: D (LEAVE A REPLY)
The Maximum Tolerable Downtime (MTD) is the maximum length of time a BUSINESS FUNCTION can endure without being restored, beyond which the BUSINESS is no longer viable
NIST SAYS: The ISCP Coordinator should analyze the supported mission/business processes and with the process owners, leadership and business managers determine the acceptable downtime if a given

process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.
Maximum Tolerable Downtime (MTD). The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on selection of an appropriate recovery method, and the depth of detail which will be required when developing recovery procedures, including their scope and content.
Other BCP and DRP terms you must be familiar with are:
Recovery Time Objective (RTO). RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.
Recovery Point Objective (RPO). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process. Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 276. and
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov112010.pdf

NEW QUESTION: 745
Which of the following tape formats can be used to backup data systems in addition to its original intended audio uses?
A. Digital Video Tape (DVT).
B. Digital Analog Tape (DAT).
C. Digital Voice Tape (DVT).
D. Digital Audio Tape (DAT).
Answer: D (LEAVE A REPLY)
Digital Audio Tape (DAT) can be used to backup data systems in addition to its original intended audio uses.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 70.

NEW QUESTION: 746

Which access control model enables the OWNER of the resource to specify what subjects can access specific resources based on their identity?

A. Discretionary Access Control

B. Mandatory Access Control

C. Sensitive Access Control

D. Role-based Access Control

Answer: (SHOW ANSWER)

Data owners decide who has access to resources based only on the identity of the person accessing the resource.

The following answers are incorrect :

Mandatory Access Control : users and data owners do not have as much freedom to determine who can access files. The operating system makes the final decision and can override the users' wishes and access decisions are based on security labels.

Sensitive Access Control : There is no such access control in the context of the above question.

Role-based Access Control : uses a centrally administered set of controls to determine how subjects and objects interact , also called as non discretionary access control.

In a mandatory access control (MAC) model, users and data owners do not have as much freedom to determine who can access files. The operating system makes the final decision and can override the users' wishes. This model is much more structured and strict and is based on a security label system. Users are given a security clearance (secret, top secret, confidential, and so on), and data is classified in the same way. The clearance and classification data is stored in the security labels, which are bound to the specific subjects and objects. When the system makes a decision about fulfilling a request to access an object, it is based on the clearance of the subject, the classification of the object, and the security policy of the system. The rules for how subjects access objects are made by the security officer, configured by the administrator, enforced by the operating system, and supported by security technologies

Reference : Shon Harris , AIO v3 , Chapter-4 : Access Control , Page : 163-165

NEW QUESTION: 747

Which of the following is the best reason for the use of an automated risk analysis tool?

A. Much of the data gathered during the review cannot be reused for subsequent analysis.

B. Automated methodologies require minimal training and knowledge of risk analysis.

C. Most software tools have user interfaces that are easy to use and does not require any training.

D. Information gathering would be minimized and expedited due to the amount of information already built into the tool.

Answer: (SHOW ANSWER)

Section: Risk, Response and Recovery

Explanation/Reference:

The use of tools simplifies this process. Not only do they usually have a database of assests, threats, and vulnerabilities but they also speed up the entire process.
Using Automated tools for performing a risk assessment can reduce the time it takes to perform them and can simplify the process as well. The better types of these tools include a well-researched threat population and associated statistics. Using one of these tools virtually ensures that no relevant threat is overlooked, and associated risks are accepted as a consequence of the threat being overlooked.
In most situations, the assessor will turn to the use of a variety of automated tools to assist in the vulnerability assessment process. These tools contain extensive databases of specific known vulnerabilities as well as the ability to analyze system and network configuration information to predict where a particular system might be vulnerable to different types of attacks. There are many different types of tools currently available to address a wide variety of vulnerability assessment needs. Some tools will examine a system from the viewpoint of the network, seeking to determine if a system can be compromised by a remote attacker exploiting available services on a particular host system. These tools will test for open ports listening for connections, known vulnerabilities in common services, and known operating system exploits.
Michael Gregg says:
Automated tools are available that minimize the effort of the manual process. These programs enable users to rerun the analysis with different parameters to answer "what-ifs." They perform calculations quickly and can be used to estimate future expected losses easier than performing the calculations manually.
Shon Harris in her latest book says:
The gathered data can be reused, greatly reducing the time required to perform subsequent analyses. The risk analysis team can also print reports and comprehensive graphs to present to management.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4655-4661). Auerbach Publications. Kindle Edition.
and
CISSP Exam Cram 2 by Michael Gregg
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 2333-2335). McGraw- Hill. Kindle Edition.
The following answers are incorrect:
Much of the data gathered during the review cannot be reused for subsequent analysis. Is incorrect because the data can be reused for later analysis.
Automated methodologies require minimal training and knowledge of risk analysis. Is incorrect because it is not the best answer. While a minimal amount of training and knowledge is needed, the analysis should still be performed by skilled professionals.
Most software tools have user interfaces that are easy to use and does not require any training. Is incorrect because it is not the best answer. While many of the user interfaces are easy to use it is better if the tool already has information built into it. There is always a training curve when any product is being used for the first time.

NEW QUESTION: 748
Which of the following is not a DES mode of operation?
A. Cipher block chaining
B. Electronic code book
C. Input feedback
D. Cipher feedback
Answer: C (LEAVE A REPLY)
Output feedback (OFB) is a DES mode of operation, not input feedback.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 149).

NEW QUESTION: 749
What is the main goal of a risk management program?
A. None of the above
B. To develop a disaster recovery plan
C. To help managers find the correct cost balance between risks and countermeasures
D. To calculate ALE formulas
E. To evaluate appropriate risk mitigation scenarios
Answer: C (LEAVE A REPLY)

NEW QUESTION: 750
Secure Shell (SSH-2) provides all the following services except:
A. secure remote login
B. command execution
C. port forwarding
D. user authentication
Answer: D (LEAVE A REPLY)
This is one of the tricky negative question. You have to pay close attention to the word EXCEPT within the question.
The SSH transport layer is a secure, low level transport protocol. It provides strong encryption, cryptographic host authentication, and integrity protection.
Authentication in this protocol level is host-based; this protocol does not perform user authentication. A higher level protocol for user authentication can be designed on top of this protocol.
The protocol has been designed to be simple and flexible to allow parameter negotiation, and to minimize the number of round-trips. The key exchange method, public key algorithm, symmetric encryption algorithm, message authentication algorithm, and hash algorithm are all negotiated. It is expected that in most environments, only 2 round-trips will be needed for full key exchange, server authentication, service request, and acceptance notification of service request. The worst case is 3 round-trips.

The following are incorrect answers:
"Remote log-on" is incorrect. SSH does provide remote log-on.
"Command execution" is incorrect. SSH does provide command execution.
"Port forwarding" is incorrect. SSH does provide port forwarding. SSH also has a wonderful feature called SSH Port Forwarding, sometimes called SSH Tunneling, which allows you to establish a secure SSH session and then tunnel arbitrary TCP connections through it. Tunnels can be created at any time, with almost no effort and no programming, which makes them very appealing. See the article below in the reference to take a look at SSH Port Forwarding in detail, as it is a very useful but often misunderstood technology. SSH Port Forwarding can be used for secure communications in a myriad of different ways.
You can see a nice tutorial on the PUTTY web site on how to use PUTTY to do port forwarding at:
http://www.cs.uu.nl/technical/services/ssh/putty/puttyfw.html
Reference(s) used for this question:
RFC 4253 at https://www.ietf.org/rfc/rfc4253.txt
and
SSH Port Forwarding by Symantec

NEW QUESTION: 751
Secure Sockets Layer (SSL) uses a Message Authentication Code (MAC) for what purpose?
A. message non-repudiation.
B. message confidentiality.
C. message interleave checking.
D. message integrity.
Answer: D (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
A keyed hash also called a MAC (message authentication code) is used for integrity protection and authenticity.
In cryptography, a message authentication code (MAC) is a generated value used to authenticate a message.
A MAC can be generated by HMAC or CBC-MAC methods. The MAC protects both a message's integrity (by ensuring that a different MAC will be produced if the message has changed) as well as its authenticity, because only someone who knows the secret key could have modified the message.
MACs differ from digital signatures as MAC values are both generated and verified using the same secret key.
This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key:
any user who can verify a MAC is also capable of generating MACs for other messages.

HMAC

When using HMAC the symmetric key of the sender would be concatenated (added at the end) with the message. The result of this process (message + secret key) would be put through a hashing algorithm, and the result would be a MAC value. This MAC value is then appended to the message being sent. If an enemy were to intercept this message and modify it, he would not have the necessary symmetric key to create a valid MAC value. The receiver would detect the tampering because the MAC value would not be valid on the receiving side.

CBC-MAC

If a CBC-MAC is being used, the message is encrypted with a symmetric block cipher in CBC mode, and the output of the final block of ciphertext is used as the MAC. The sender does not send the encrypted version of the message, but instead sends the plaintext version and the MAC attached to the message. The receiver receives the plaintext message and encrypts it with the same symmetric block cipher in CBC mode and calculates an independent MAC value. The receiver compares the new MAC value with the MAC value sent with the message. This method does not use a hashing algorithm as does HMAC.

Cipher-Based Message Authentication Code (CMAC)

Some security issues with CBC-MAC were found and they created Cipher-Based Message Authentication Code (CMAC) as a replacement. CMAC provides the same type of data origin authentication and integrity as CBC-MAC, but is more secure mathematically. CMAC is a variation of CBC-MAC. It is approved to work with AES and Triple DES. HMAC, CBC-MAC, and CMAC work higher in the network stack and can identify not only transmission errors (accidental), but also more nefarious modifications, as in an attacker messing with a message for her own benefit. This means all of these technologies can identify intentional, unauthorized modifications and accidental changes- three in one.

The following are all incorrect answers:

"Message non-repudiation" is incorrect.

Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

To repudiate means to deny. For many years, authorities have sought to make repudiation impossible in some situations. You might send registered mail, for example, so the recipient cannot deny that a letter was delivered. Similarly, a legal document typically requires witnesses to signing so that the person who signs cannot deny having done so.

On the Internet, a digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.

"Message confidentiality" is incorrect. The Message confidentiality is protected by encryption not by hashing algorithms.

"Message interleave checking" is incorrect. This is a nonsense term included as a distractor.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw-Hill. Kindle Edition.

and
http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
and
http://searchsecurity.techtarget.com/definition/nonrepudiation
and
https://en.wikipedia.org/wiki/Message_authentication_code

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 752
Related to information security, integrity is the opposite of which of the following?
A. abstraction
B. alteration
C. accreditation
D. application
Answer: B (LEAVE A REPLY)
Integrity is the opposite of "alteration."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 753
CORRECT TEXT
_____ is a major component of an overall risk management program.
Answer:
assessment

NEW QUESTION: 754
The IDEA algorithm (used in PGP) is _____ bits long.
A. 168
B. 56
C. 158
D. 128
Answer: D (LEAVE A REPLY)

NEW QUESTION: 755

Which of the following protocols is not implemented at the Internet layer of the TCP/IP protocol model?

A. User datagram protocol (UDP)

B. Internet protocol (IP)

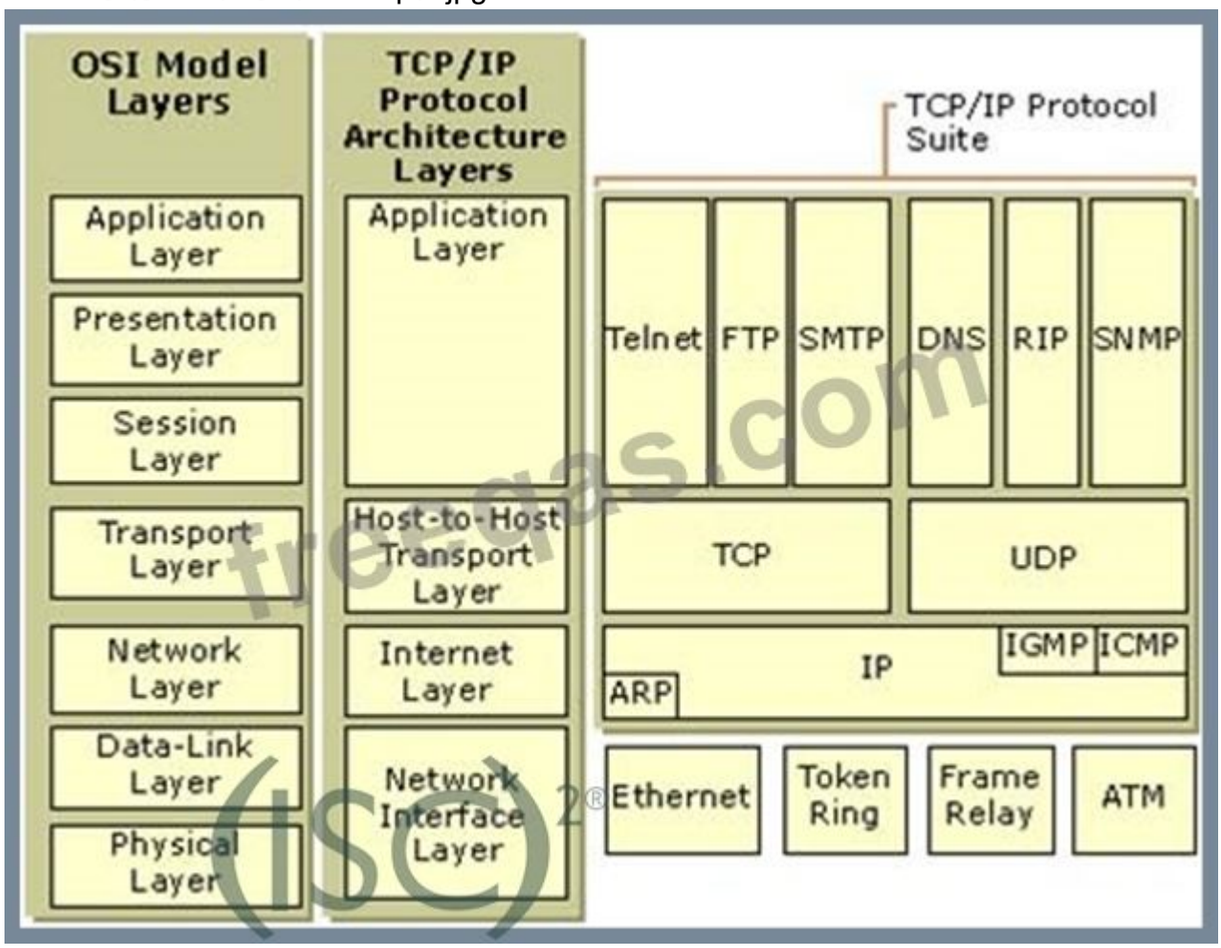
C. Internet Group Management Protocol (IGMP)

D. Internet control message protocol (ICMP)

Answer: A (LEAVE A REPLY)

The User Datagram Protocol (UDP) is implemented at the host-to-host transport layer, not at the internet layer.

Protocol at what layer? Ensure you are familiar with both the OSI model and the DoD TCP/IP model as well. You need to know how to contrast the two side by side and what are the names being used on both side. Below you have a graphic showing the two and how things maps between the two as well as some of the most common protcolos found at each of the layers: Protocols at what layers of the DoD TCP/IP model C:\Users\MCS\Desktop\1.jpg



Graphic from http://technet.microsoft.com/en-us/library/cc958821.aspx

The following are incorrect answers:

All of the other protocols sit at the Internet Layer of the TCP/IP model.

NOTE:

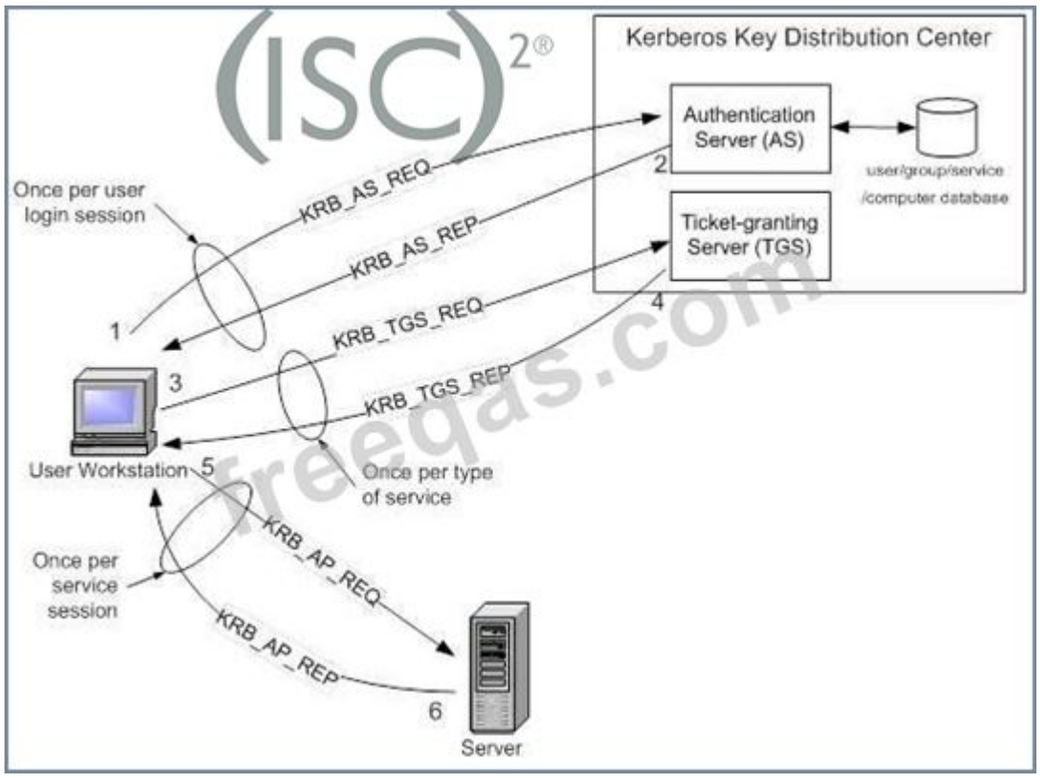
Some reference are calling the Transport layer on the DoD model Host-to-Host.

Reference(s) used for this question:

Shon Harris, CISSP All In One (AIO), 6th edition , Telecommunication and Network

Security, Page 518,534
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 85).
and
Microsoft Technet at http://technet.microsoft.com/en-us/library/cc958821.aspx

NEW QUESTION: 756
Which of the following is NOT true of the Kerberos protocol?
A. Only a single login is required per session.
B. The initial authentication steps are done using public key algorithm.
C. The KDC is aware of all systems in the network and is trusted by all of them
D. It performs mutual authentication
Answer: B (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It has the following characteristics:
It is secure: it never sends a password unless it is encrypted.
Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.
The concept depends on a trusted third party - a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.
It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.
Kerberos introduces the concept of a Ticket-Granting Server/Service (TGS). A client that wishes to use a service has to receive a ticket from the TGS - a ticket is a time-limited cryptographic message - giving it access to the server. Kerberos also requires an Authentication Server (AS) to verify clients. The two servers combined make up a KDC.
Within the Windows environment, Active Directory performs the functions of the KDC. The following figure shows the sequence of events required for a client to gain access to a service using Kerberos authentication.
Each step is shown with the Kerberos message associated with it, as defined in RFC 4120 "The Kerberos Network Authorization Service (V5)".



Kerberos Authentication Step by Step

Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT).

Step 2: The Authorization Server verifies the user's access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user's password and sends a message back to the user workstation.

The workstation prompts the user for a password and uses the password to decrypt the incoming message.

When decryption succeeds, the user will be able to use the TGT to request a service ticket.

Step 3: When the user wants access to a service, the workstation client application sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.

Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key - one encrypted with the client password, and one encrypted by the service password.

Step 5: The client application now sends a service request to the server containing the ticket received in Step

4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.

Step 6: If mutual authentication is required, then the server will reply with a server authentication message.

The Kerberos server knows "secrets" (encrypted passwords) for all clients and servers under its control, or it is in contact with other secure servers that have this information. These "secrets" are used to encrypt all of the messages shown in the figure above.
To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Since the clocks of two computers are often out of synch, administrators can establish a policy to establish the maximum acceptable difference to Kerberos between a client's clock and server's clock. If the difference between a client's clock and the server's clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic. The maximum difference is usually set to five minutes.
Note that if a client application wishes to use a service that is "Kerberized" (the service is configured to perform Kerberos authentication), the client must also be Kerberized so that it expects to support the necessary message responses.
For more information about Kerberos, see http://web.mit.edu/kerberos/www/.
References:
Introduction to Kerberos Authentication from Intel
and
http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/#1.3.5.3
and
http://www.ietf.org/rfc/rfc4120.txt

NEW QUESTION: 757
There are 6 types of security control practices. _____ controls are management policies, procedures, and guidelines that usually effect the entire system. These types of controls deal with system auditing and usability.
A. Corrective
B. Combination
C. Recovery
D. Detective
E. Preventive
F. Directive
Answer: F (LEAVE A REPLY)

NEW QUESTION: 758
Which of the following best corresponds to the type of memory addressing where the address location that is specified in the program instruction contains the address of the final desired location?
A. Direct addressing
B. Indirect addressing
C. Indexed addressing
D. Program addressing

Answer: B (LEAVE A REPLY)
Explanation/Reference:
Indirect addressing is when the address location that is specified in the program instruction contains the address of the final desired location. Direct addressing is when a portion of primary memory is accessed by specifying the actual address of the memory location. Indexed addressing is when the contents of the address defined in the program's instruction is added to that of an index register. Program addressing is not a defined memory addressing mode.
Source: WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 2).

NEW QUESTION: 759
Which of the following technologies is a target of XSS or CSS (Cross-Site Scripting) attacks?
A. Web Applications
B. Intrusion Detection Systems
C. Firewalls
D. DNS Servers
Answer: A (LEAVE A REPLY)
Explanation/Reference:
XSS or Cross-Site Scripting is a threat to web applications where malicious code is placed on a website that attacks the use using their existing authenticated session status.
Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.
An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.
Mitigation:
Configure your IPS - Intrusion Prevention System to detect and suppress this traffic.
Input Validation on the web application to normalize inputted data.
Set web apps to bind session cookies to the IP Address of the legitimate user and only permit that IP Address to use that cookie.
See the XSS (Cross Site Scripting) Prevention Cheat Sheet
See the Abridged XSS Prevention Cheat Sheet
See the DOM based XSS Prevention Cheat Sheet
See the OWASP Development Guide article on Phishing.
See the OWASP Development Guide article on Data Validation.
The following answers are incorrect:

Intrusion Detection Systems: Sorry. IDS Systems aren't usually the target of XSS attacks but a properly-configured IDS/IPS can "detect and report on malicious string and suppress the TCP connection in an attempt to mitigate the threat.
Firewalls: Sorry. Firewalls aren't usually the target of XSS attacks.
DNS Servers: Same as above, DNS Servers aren't usually targeted in XSS attacks but they play a key role in the domain name resolution in the XSS attack process.
The following reference(s) was used to create this question:
CCCure Holistic Security+ CBT and Curriculum
and
https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

NEW QUESTION: 760
What is the RESULT of a hash algorithm being applied to a message ?
A. A digital signature
B. A ciphertext
C. A message digest
D. A plaintext
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
As when a hash algorithm is applied on a message , it produces a message digest.
The other answers are incorrect because :
A digital signature is a hash value that has been encrypted with a sender's private key.
A ciphertext is a message that appears to be unreadable.
A plaintext is a readable data.
Reference : Shon Harris , AIO v3 , Chapter-8 : Cryptography , Page : 593-594 , 640 , 648

NEW QUESTION: 761
Which of the following LAN topologies offers the highest availability?
A. Bus topology
B. Tree topology
C. Full mesh topology
D. Partial mesh topology
Answer: C (LEAVE A REPLY)
In a full mesh topology, all network nodes are individually connected with
each other, providing the highest availability. A partial mesh topology can sometimes be
used to offer some redundancy.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3:
Telecommunications and Network Security (page 106).

NEW QUESTION: 762
Which of the following choices describe a condition when RAM and Secondary storage are used together?
A. Primary storage
B. Secondary storage
C. Virtual storage
D. Real storage
Answer: (SHOW ANSWER)
Explanation/Reference:
Virtual storage a service provided by the operating system where it uses a combination of RAM and disk storage to simulate a much larger address space than is actually present. Infrequently used portions of memory are paged out by being written to secondary storage and paged back in when required by a running program.
Most OS's have the ability to simulate having more main memory than is physically available in the system.
This is done by storing part of the data on secondary storage, such as a disk. This can be considered a virtual page. If the data requested by the system is not currently in main memory, a page fault is taken. This condition triggers the OS handler. If the virtual address is a valid one, the OS will locate the physical page, put the right information in that page, update the translation table, and then try the request again. Some other page might be swapped out to make room. Each process may have its own separate virtual address space along with its own mappings and protections.
The following are incorrect answers:
Primary storage is incorrect. Primary storage refers to the combination of RAM, cache and the processor registers. Primary Storage The data waits for processing by the processors, it sits in a staging area called primary storage. Whether implemented as memory, cache, or registers (part of the CPU), and regardless of its location, primary storage stores data that has a high probability of being requested by the CPU, so it is usually faster than long-term, secondary storage. The location where data is stored is denoted by its physical memory address. This memory register identifier remains constant and is independent of the value stored there. Some examples of primary storage devices include random-access memory (RAM), synchronous dynamic random-access memory (SDRAM), and read-only memory (ROM). RAM is volatile, that is, when the system shuts down, it flushes the data in RAM although recent research has shown that data may still be retrievable. Contrast this
Secondary storage is incorrect. Secondary storage holds data not currently being used by the CPU and is used when data must be stored for an extended period of time using high-capacity, nonvolatile storage.
Secondary storage includes disk, floppies, CD's, tape, etc. While secondary storage includes basically anything different from primary storage, virtual memory's use of secondary storage is usually confined to high-speed disk storage.
Real storage is incorrect. Real storage is another word for primary storage and distinguishes physical memory from virtual memory.
Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17164-17171). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17196-17201). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17186-17187). Auerbach Publications. Kindle Edition.

NEW QUESTION: 763
Which of the following is NOT a true statement regarding the implementaton of the 3DES modes?
A. DES-EEE1 uses one key
B. DES-EEE2 uses two keys
C. DES-EEE3 uses three keys
D. DES-EDE2 uses two keys
Answer: A (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
There is no DES mode call DES-EEE1. It does not exist.
The following are the correct modes for triple-DES (3DES):
DES-EEE3 uses three keys for encryption and the data is encrypted, encrypted, encrypted; DES-EDE3 uses three keys and encrypts, decrypts and encrypts data.
DES-EEE2 and DES-EDE2 are the same as the previous modes, but the first and third operations use the same key.
Reference(s) used for this question:
Shon Harris, CISSP All In One (AIO) book, 6th edition , page 808
and
Official ISC2 Guide to the CISSP CBK, 2nd Edition (2010) , page 344-345

NEW QUESTION: 764
PGP & PEM are programs that allow users to send encrypted messages to each other. What form of encryption do these programs use?
A. DES
B. All of the above
C. 3DES
D. RSA
E. Blowfish
F. 3RSA
Answer: D (LEAVE A REPLY)

NEW QUESTION: 765
Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any

specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?

A. OAKLEY

B. Internet Security Association and Key Management Protocol (ISAKMP)

C. Simple Key-management for Internet Protocols (SKIP)

D. IPsec Key exchange (IKE)

Answer: B (LEAVE A REPLY)

Section: Cryptography

Explanation/Reference:

RFC 2828 (Internet Security Glossary) defines the Internet Security Association and Key Management Protocol (ISAKMP) as an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.

Let's clear up some confusion here first. Internet Key Exchange (IKE) is a hybrid protocol, it consists of 3 "protocols"

ISAKMP: It's not a key exchange protocol per se, it's a framework on which key exchange protocols operate.

ISAKMP is part of IKE. IKE establishs the shared security policy and authenticated keys. ISAKMP is the protocol that specifies the mechanics of the key exchange.

Oakley: Describes the "modes" of key exchange (e.g. perfect forward secrecy for keys, identity protection, and authentication). Oakley describes a series of key exchanges and services.

SKEME: Provides support for public-key-based key exchange, key distribution centres, and manual installation, it also outlines methods of secure and fast key refreshment.

So yes, IPSec does use IKE, but ISAKMP is part of IKE.

The questions did not ask for the actual key negotiation being done but only for the "exchange of key generation and authentication data" being done. Under Oakly it would be Diffie Hellman (DH) that would be used for the actual key nogotiation.

The following are incorrect answers:

Simple Key-management for Internet Protocols (SKIP) is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

OAKLEY is a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie- Hellman algorithm and designed to be a compatible component of ISAKMP.

IPsec Key Exchange (IKE) is an Internet, IPsec, key-establishment protocol [R2409] (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.

Reference used for this question:

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 766

When should a post-mortem review meeting be held after an intrusion has been properly taken care of?

A. Within the first three months after the investigation of the intrusion is completed.
B. Within the first week after prosecution of intruders have taken place, whether successful or not.
C. Within the first month after the investigation of the intrusion is completed.
D. Within the first week of completing the investigation of the intrusion.
Answer: (SHOW ANSWER)
A post-mortem review meeting should be held with all involved parties within three to five working days of completing the investigation of the intrusion. Otherwise, participants are likely to forget critical information. Even if it enabled an organization to validate the correctness of its chain of custody of evidence, it would not make sense to wait until prosecution is complete because it would take too much time and many cases of intrusion never get to court anyway.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (page 297).

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 767
Which access control model was proposed for enforcing access control in government and military applications?
A. Bell-LaPadula model
B. Biba model
C. Sutherland model
D. Brewer-Nash model
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The Bell-LaPadula model, mostly concerned with confidentiality, was proposed for enforcing access control in government and military applications. It supports mandatory access control by determining the access rights from the security levels associated with subjects and objects. It also supports discretionary access control by checking access rights from an access matrix. The Biba model, introduced in 1977, the Sutherland model, published in 1986, and the Brewer-Nash model, published in 1989, are concerned with integrity.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 11).

NEW QUESTION: 768

Logical or technical controls involve the restriction of access to systems and the protection of information. Which of the following statements pertaining to these types of controls is correct?
A. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks but do not include a review of vacation history, and also do not include increased supervision.
B. Examples of these types of controls do not include encryption, smart cards, access lists, and transmission protocols.
C. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.
D. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.
Answer: C (LEAVE A REPLY)
Logical or technical controls involve the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 769
You are running a packet sniffer on a network and see a packet containing a long string of "0x90 0x90 0x90 0x90...." in the middle of it traveling to an x86-based machine as a target. This could be indicative of what activity being attempted?
A. Over-subscription of the traffic on a backbone.
B. A source quench packet.
C. A FIN scan.
D. A buffer overflow attack.
Answer: (SHOW ANSWER)
A series of the same control characters, hexadecimal code, imbedded in the string is usually an indicator of a buffer overflow attack.
The Intel x86 processors use the hexadecimal number 90 to represent NOP (no operation). Many buffer overflow attacks use long strings of control characters and this is representative of that type of attack.
A buffer overflow takes place when too much data are accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed. So, the purpose of a buffer overflow may be either to make a mess, by shoving arbitrary data into various memory segments, or to accomplish a specific task, by pushing into the memory segment a carefully crafted set of data that will accomplish a specific task. This task could be to open a command shell with administrative privilege or execute malicious code.
Common threats to system availability, integrity, and confidentiality include hardware

failure, misuse of system privileges, buffer overflows and other memory attacks, denial of service, reverse engineering, and system hacking.
Since many vulnerabilities result from insecure design and most threats are well known, it is the responsibility of the security architect to ensure that their designs are addressing security requirements appropriately while also ensuring that the system can continue to perform its intended function.
The following answers are incorrect:
Over-subscription of the traffic on a backbone. Is incorrect because if there was Over-subscription of the traffic on a backbone, that would typically result in not being able to send or receive any packets, more commonly known as Denial of Service or DoS.
A source quench packet. This is incorrect because a source quench packet is an ICMP message that contains the internet header plus 64 bits of the original datagram.
A FIN scan. This is incorrect because a FIN scan is when a packet with the FIN flag set is sent to a specific port and the results are then analyzed.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page 332, for people using the Kindle edition you will find it at Kindle Locations 7310-7315.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Architecture and Design (Kindle Locations 1403-1407). . Kindle Edition.
Wikipedia http://en.wikipedia.org/wiki/Port_scanner
ICMP http://security.maruhn.com/iptables-tutorial/x1078.html
Wikipedia http://en.wikipedia.org/wiki/Buffer_overflow

NEW QUESTION: 770
Which of the following tools is less likely to be used by a hacker?
A. l0phtcrack
B. Tripwire
C. OphCrack
D. John the Ripper
Answer: B (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
Tripwire is an integrity checking product, triggering alarms when important files (e.g. system or configuration files) are modified.
This is a tool that is not likely to be used by hackers, other than for studying its workings in order to circumvent it.
Other programs are password-cracking programs and are likely to be used by security administrators as well as by hackers. More info regarding Tripwire available on the Tripwire, Inc. Web Site.
NOTE:

The biggest competitor to the commercial version of Tripwire is the freeware version of Tripwire. You can get the Open Source version of Tripwire at the following URL: http://sourceforge.net/projects/tripwire/

NEW QUESTION: 771
Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?
A. OAKLEY
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. IPsec Key exchange (IKE)
Answer: B (LEAVE A REPLY)
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines the Internet Security Association and Key Management Protocol (ISAKMP) as an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.
Let's clear up some confusion here first. Internet Key Exchange (IKE) is a hybrid protocol, it consists of 3 "protocols"
ISAKMP: It's not a key exchange protocol per se, it's a framework on which key exchange protocols operate. ISAKMP is part of IKE. IKE establishs the shared security policy and authenticated keys. ISAKMP is the protocol that specifies the mechanics of the key exchange.
Oakley: Describes the "modes" of key exchange (e.g. perfect forward secrecy for keys, identity protection, and authentication). Oakley describes a series of key exchanges and services.
SKEME: Provides support for public-key-based key exchange, key distribution centres, and manual installation, it also outlines methods of secure and fast key refreshment.
So yes, IPSec does use IKE, but ISAKMP is part of IKE.
The questions did not ask for the actual key negotiation being done but only for the "exchange of key generation and authentication data" being done. Under Oakly it would be Diffie Hellman (DH) that would be used for the actual key nogotiation.
The following are incorrect answers:
Simple Key-management for Internet Protocols (SKIP) is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.
OAKLEY is a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie- Hellman algorithm and designed to be a compatible component of ISAKMP.
IPsec Key Exchange (IKE) is an Internet, IPsec, key-establishment protocol [R2409] (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.
Reference used for this question:

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 772
Which of the following is a CHARACTERISTIC of a decision support system (DSS) in regards to Threats and Risks Analysis?
A. DSS is aimed at solving highly structured problems.
B. DSS emphasizes flexibility in the decision making approach of users.
C. DSS supports only structured decision-making tasks.
D. DSS combines the use of models with non-traditional data access and retrieval functions.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
DSS emphasizes flexibility in the decision-making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions and supports semi-structured decision-making tasks.
DSS is sometimes referred to as the Delphi Method or Delphi Technique:
The Delphi technique is a group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result of a particular threat will be. This avoids a group of individuals feeling pressured to go along with others' thought processes and enables them to participate in an independent and anonymous way. Each member of the group provides his or her opinion of a certain threat and turns it in to the team that is performing the analysis. The results are compiled and distributed to the group members, who then write down their comments anonymously and return them to the analysis group. The comments are compiled and redistributed for more comments until a consensus is formed. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree verbally.
Here is the ISC2 book coverage of the subject:
One of the methods that uses consensus relative to valuation of information is the consensus/modified Delphi method. Participants in the valuation exercise are asked to comment anonymously on the task being discussed. This information is collected and disseminated to a participant other than the original author. This participant comments upon the observations of the original author. The information gathered is discussed in a public forum and the best course is agreed upon by the group (consensus).
EXAM TIP:
The DSS is what some of the books are referring to as the Delphi Method or Delphi Technique. Be familiar with both terms for the purpose of the exam.
The other answers are incorrect:
'DSS is aimed at solving highly structured problems' is incorrect because it is aimed at solving less structured problems.
'DSS supports only structured decision-making tasks' is also incorrect as it supports semi-structured decision-making tasks.
'DSS combines the use of models with non-traditional data access and retrieval functions' is also incorrect as it combines the use of models and analytic techniques with traditional data access and retrieval functions.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 91). McGraw-Hill. Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Information Security Governance and Risk Management ((ISC)2 Press) (Kindle Locations 1424-1426). Auerbach Publications. Kindle Edition.

NEW QUESTION: 773
In SSL/TLS protocol, what kind of authentication is supported when you establish a secure session between a client and a server?
A. Peer-to-peer authentication
B. Only server authentication (optional)
C. Server authentication (mandatory) and client authentication (optional)
D. Role based authentication scheme
Answer: C (LEAVE A REPLY)
Explanation/Reference:
RESCORLA, Eric, SSL and TLS: Designing and Building Secure Systems, 2000, Addison Wesley Professional; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 774
Address Resolution Protocol (ARP) interrogates the network by sending out a?
A. broadcast.
B. multicast.
C. unicast.
D. semicast.
Answer: (SHOW ANSWER)
Explanation/Reference:
ARP interrogates the network by sending out a broadcast seeking a network node that has a specific IP address, and asks it to reply with its hardware address. A broadcast message is sent to everyone whether or not the message was requested. A traditional unicast is a "one-to-one" or "narrowcast" message. A multicast is a "one-to-many" message that is traditionally only sent to those machine that requested the information. Semicast is an imposter answer.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

NEW QUESTION: 775
Which of the following statements pertaining to stream ciphers is correct?
A. A stream cipher is a type of asymmetric encryption algorithm.
B. A stream cipher generates what is called a keystream.
C. A stream cipher is slower than a block cipher.

D. A stream cipher is not appropriate for hardware-based encryption.

Answer: (SHOW ANSWER)

A stream cipher is a type of symmetric encryption algorithm that operates on continuous streams of plain text and is appropriate for hardware-based encryption.

Stream ciphers can be designed to be exceptionally fast, much faster than any block cipher. A stream cipher generates what is called a keystream (a sequence of bits used as a key).

Stream ciphers can be viewed as approximating the action of a proven unbreakable cipher, the one-time pad (OTP), sometimes known as the Vernam cipher. A one-time pad uses a keystream of completely random digits. The keystream is combined with the plaintext digits one at a time to form the ciphertext. This system was proved to be secure by Claude Shannon in 1949. However, the keystream must be (at least) the same length as the plaintext, and generated completely at random. This makes the system very cumbersome to implement in practice, and as a result the one-time pad has not been widely used, except for the most critical applications.

A stream cipher makes use of a much smaller and more convenient key - 128 bits, for example. Based on this key, it generates a pseudorandom keystream which can be combined with the plaintext digits in a similar fashion to the one-time pad. However, this comes at a cost: because the keystream is now pseudorandom, and not truly random, the proof of security associated with the one-time pad no longer holds: it is quite possible for a stream cipher to be completely insecure if it is not implemented properly as we have seen with the Wired Equivalent Privacy (WEP) protocol.

Encryption is accomplished by combining the keystream with the plaintext, usually with the bitwise XOR operation.

Source: DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.

More details can be obtained on Stream Ciphers in RSA Security's FAQ on Stream Ciphers.

NEW QUESTION: 776

In SSL/TLS protocol, what kind of authentication is supported when you establish a secure session between a client and a server?

A. Peer-to-peer authentication

B. Only server authentication (optional)

C. Server authentication (mandatory) and client authentication (optional)

D. Role based authentication scheme

Answer: C (LEAVE A REPLY)

RESCORLA, Eric, SSL and TLS: Designing and Building Secure Systems, 2000, Addison Wesley Professional; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 777

Kerberos is vulnerable to replay in which of the following circumstances?

A. When a private key is compromised within an allotted time window.

B. When a public key is compromised within an allotted time window.
C. When a ticket is compromised within an allotted time window.
D. When the KSD is compromised within an allotted time window.
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Replay can be accomplished on Kerberos if the compromised tickets are used within an allotted time window.
The security depends on careful implementation:enforcing limited lifetimes for authentication credentials minimizes the threat of of replayed credentials, the KDC must be physically secured, and it should be hardened, not permitting any non-kerberos activities.
Reference:
Official ISC2 Guide to the CISSP, 2007 Edition, page 184
also see:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

NEW QUESTION: 778
To protect and/or restore lost, corrupted, or deleted information, thereby preserving the data integrity and availability is the purpose of:
A. Remote journaling.
B. Database shadowing.
C. A tape backup method.
D. Mirroring.
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
The purpose of a tape backup method is to protect and/or restore lost, corrupted, or deleted information, thereby preserving the data integrity and ensuring availability.
All other choices could suffer from corruption and it might not be possible to restore the data without proper backups being done.
This is a tricky question, if the information is lost, corrupted, or deleted only a good backup could be use to restore the information. Any synchronization mechanism would update the mirror copy and the data could not be recovered.
With backups there could be a large gap where your latest data may not be available. You would have to look at your Recovery Point Objective and see if this is acceptable for your company recovery objectives.
The following are incorrect answers:
Mirroring will preserve integrity and restore points in all cases of drive failure. However, if you have corrupted data on the primary set of drives you may get corrupted data on the secondary set as well.

Remote Journaling provides Continuous or periodic synchronized recording of transaction data at a remote location as a backup strategy. (http://www.businessdictionary.com/definition/remote-journaling.html) With journaling there might be a gap of time between the data updates being send in batch at regular interval. So some of the data could be lost.
Database shadowing is synonymous with Mirroring but it only applies to databases, but not to information and data as a whole.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 68.

NEW QUESTION: 779
The change control process:
A. Should allow for quick changes without the burden on paperwork or formal committee review
B. Every incorporated required change does not need to be traceable to an approved change request
C. Should be a well defined in that it provides stakeholders with a formal mechanism for proposing changes in requirements
D. The change control process should not let you track the status of all proposed changes
E. Should allow for design or implementation work to be performed without approval
Answer: C (LEAVE A REPLY)
While the change control process is not intended to be an obstacle or roadblock to making changes, it should provide stakeholders a formal mechanism for proposing and controlling change.

NEW QUESTION: 780
In biometrics, the "one-to-one" search used to verify claim to an identity made by a person is considered:
A. Authentication
B. Identification
C. Auditing
D. Authorization
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Biometric devices can be use for either IDENTIFICATION or AUTHENTICATION ONE TO ONE is for AUTHENTICATION This means that you as a user would provide some biometric credential such as your fingerprint. Then they will compare the template that you have provided with the one stored in the Database. If the two are exactly the same that prove that you are who you pretend to be.
ONE TO MANY is for IDENTIFICATION
A good example of this would be within airport. Many airports today have facial recognition cameras, as you walk through the airport it will take a picture of your face and then compare the template (your face) with a database full of templates and see if there is a match between your template and the ones stored in the Database. This is for IDENTIFICATION of a person.

Some additional clarification or comments that might be helpful are: Biometrics establish authentication using specific information and comparing results to expected data. It does not perform well for identification purposes such as scanning for a person's face in a moving crowd for example.
Identification methods could include: username, user ID, account number, PIN, certificate, token, smart card, biometric device or badge.
Auditing is a process of logging or tracking what was done after the identity and authentication process is completed.
Authorization is the rights the subject is given and is performed after the identity is established.
Reference OIG (2007) p148, 167
Authentication in biometrics is a "one-to-one" search to verify claim to an identity made by a person.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION: 781
The major objective of system configuration management is which of the following?
A. system maintenance.
B. system stability.
C. system operations.
D. system tracking.
Answer: (SHOW ANSWER)
Explanation/Reference:
A major objective with Configuration Management is stability. The changes to the system are controlled so that they don't lead to weaknesses or faults in th system.
The following answers are incorrect:
system maintenance. Is incorrect because it is not the best answer. Configuration Management does control the changes to the system but it is not as important as the overall stability of the system.
system operations. Is incorrect because it is not the best answer, the overall stability of the system is much more important.
system tracking. Is incorrect because while tracking changes is important, it is not the best answer. The overall stability of the system is much more important.

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 782
For which areas of the enterprise are business continuity plans required?

A. All areas of the enterprise.
B. The financial and information processing areas of the enterprise.
C. The operating areas of the enterprise.
D. The marketing, finance, and information processing areas.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 783
Which of the following control pairings include: organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?
A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Preventive/Administrative Pairing: These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 784
Which of the following best describes signature-based detection?
A. Compare source code, looking for events or sets of events that could cause damage to a system or network.
B. Compare system activity for the behaviour patterns of new attacks.
C. Compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack.
D. Compare network nodes looking for objects or sets of objects that match a predefined pattern of objects that may describe a known attack.
Answer: (SHOW ANSWER)
Explanation/Reference:
Misuse detectors compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection." The most common

form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to detect groups of attacks.
Reference:
Old Document:
BACE, Rebecca & MELL, Peter, NIST Special Publication 800-31 on Intrusion Detection Systems, Page 16.
The publication above has been replaced by 800-94 on page 2-4
The Updated URL is: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

NEW QUESTION: 785
Which virus category has the capability of changing its own code, making it harder to detect by anti-virus software?
A. Stealth viruses
B. Polymorphic viruses
C. Trojan horses
D. Logic bombs
Answer: B (LEAVE A REPLY)
A polymorphic virus has the capability of changing its own code, enabling it to have many different variants, making it harder to detect by anti-virus software. The particularity of a stealth virus is that it tries to hide its presence after infecting a system. A Trojan horse is a set of unauthorized instructions that are added to or replacing a legitimate program. A logic bomb is a set of instructions that is initiated when a specific event occurs. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 786).

NEW QUESTION: 786
A momentary high voltage is a:
A. spike
B. blackout
C. surge
D. fault
Answer: (SHOW ANSWER)
Too much voltage for a short period of time is a spike. Too much voltage for a long period of time is a surge. Not enough voltage for a short period of time is a sag or dip Not enough voltage for a long period of time is brownout A short power interruption is a fault A long power interruption is a blackout You MUST know all of the power issues above for the purpose of the exam.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 787

In non-discretionary access control using Role Based Access Control (RBAC), a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on:

A. The societies role in the organization

B. The individual's role in the organization

C. The group-dynamics as they relate to the individual's role in the organization

D. The group-dynamics as they relate to the master-slave role in the organization

Answer: B (LEAVE A REPLY)

Section: Access Control

Explanation/Reference:

In Non-Discretionary Access Control, when Role Based Access Control is being used, a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual's role in the organization.

Reference(S) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 788

Which of these virus incidents did not occur in 1999? (Choose all that apply)

A. ILoveYou

B. Michelangelo

C. AnnaKournikova

D. Melissa

E. None of the above - they all happened in 1999

F. Chernobyl

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 789

Which of the following teams should NOT be included in an organization's contingency plan?

A. Damage assessment team

B. Hardware salvage team

C. Tiger team

D. Legal affairs team

Answer: C (LEAVE A REPLY)

According to NIST's Special publication 800-34, a capable recovery strategy will require some or all of the following functional groups: Senior management official, management team, damage assessment team, operating system administration team, systems software team, server recovery team, LAN/WAN recovery team, database recovery team, network operations recovery team, telecommunications team, hardware salvage team, alternate site recovery coordination team, original site restoration/salvage coordination team, test team, administrative support team, transportation and relocation team, media relations team, legal affairs team, physical/personal security team, procurements team. Ideally, these

teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. A tiger team, originally a U.S. military jargon term, defines a team (of sneakers) whose purpose is to penetrate security, and thus test security measures. Used today for teams performing ethical hacking.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 23).

NEW QUESTION: 790
Guards are appropriate whenever the function required by the security program involves which of the following?
A. The use of discriminating judgment
B. The use of physical force
C. The operation of access control devices
D. The need to detect unauthorized access
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The use of discriminating judgment, a guard can make the determinations that hardware or other automated security devices cannot make due to its ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment. Guards are better at making value decisions at times of incidents. They are appropriate whenever immediate, discriminating judgment is required by the security entity.
The following answers are incorrect:
The use of physical force This is not the best answer. A guard provides discriminating judgment, and the ability to discern the need for physical force.
The operation of access control devices A guard is often uninvolved in the operations of an automated access control device such as a biometric reader, a smart lock, mantrap, etc.
The need to detect unauthorized access The primary function of a guard is not to detect unauthorized access, but to prevent unauthorized physical access attempts and may deter social engineering attempts.
The following reference(s) were/was used to create this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 339).
Source: ISC2 Offical Guide to the CBK page 288-289.

NEW QUESTION: 791
Which of the following can be defined as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client?
A. IMAP4
B. SMTP

C. MIME
D. PEM
Answer: A (LEAVE A REPLY)
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines the Internet Message Access Protocol, version 4 (IMAP4) as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client.
IMAP4 has mechanisms for optionally authenticating a client to a server and providing other security services.
MIME is the MultiPurpose Internet Mail Extension. MIME extends the format of Internet mail to allow non-US-ASCII textual messages, non-textual messages, multipart message bodies, and non-US-ASCII information in message headers.
Simple Mail Transfer Protocol (SMTP) is a TCP-based, application-layer, Internet Standard protocol for moving electronic mail messages from one computer to another.
Privacy Enhanced Mail (PEM) is an Internet protocol to provide data confidentiality, data integrity, and data origin authentication for electronic mail.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 792
What protocol is used to match an IP address to the appropriate hardware address of the packet's destination so it can be sent?
A. Routing tables
B. Address resolution protocol (ARP)
C. Reverse address resolution protocol (RARP)
D. Internet Control Message Protocol (ICMP)
Answer: B (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation
Explanation/Reference:
The Address Resolution Protocol (ARP) is used to match an IP address to an Ethernet address so the packet can be sent to the appropriate node.
Shon Harris in her book says:
MAC and IP addresses must be properly mapped so they can be correctly resolved. This happens through the Address Resolution Protocol (ARP). When the data link layer receives a frame, the network layer has already attached the destination IP address to it, but the data link layer cannot understand the IP address and thus invokes ARP for help.
ARP broadcasts a frame requesting the MAC address that corresponds with the destination IP address. Each computer on the subnet receives this broadcast frame, and all but the computer that has the requested IP address ignore it.
The computer that has the destination IP address responds with its MAC address. Now ARP knows what hardware address corresponds with that specific IP address. The data link layer takes the frame, adds

the hardware address to it, and passes it on to the physical layer, which enables the frame to hit the wire and go to the destination computer.
ARP maps the hardware address and associated IP address and stores this mapping in its table for a predefined amount of time. This caching is done so that when another frame destined for the same IP address needs to hit the wire, ARP does not need to broadcast its request again. It just looks in its table for this information.
Man-In-The-Middle attack
Because ARP does not require authentication, an attacker could place bogus entries into the ARP cache of a remote host (gratuitous ARP replies) to carry out attacks, such as a man-in-the-middle attacks. This attack is called ARP poisoning.
The following answers were incorrect:
RARP is used to match an Ethernet address to an IP address.
ICMP is a management protocol whose function is to send message between network devices.
Routing tables are used by routers to choose the appropriate interface to route packets.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Chapter 6 Telecommunications and Network Security, Pages 580-581 or on the Kindle edition look around Locations 12298-12306. McGraw-Hill.
Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK , Third Edition: Telecommunications and Network Security, Page 342.

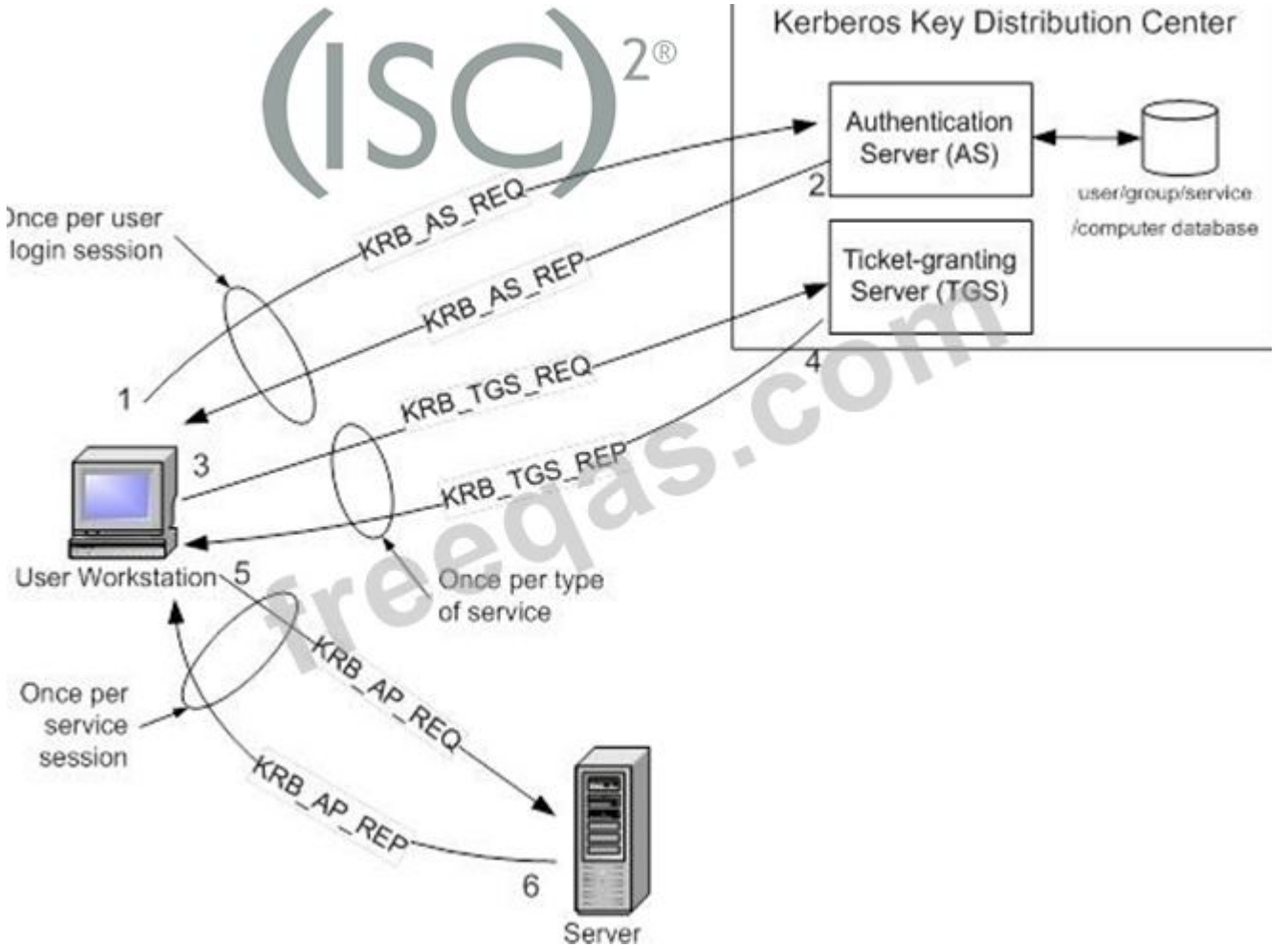
NEW QUESTION: 793
After a company is out of an emergency state, what should be moved back to the original site first?
A. Executives
B. Least critical components
C. IT support staff
D. Most critical components
Answer: B (LEAVE A REPLY)
Explanation/Reference:
This will expose any weaknesses in the plan and ensure the primary site has been properly repaired before moving back. Moving critical assets first may induce a second disaster if the primary site has not been repaired properly.
The first group to go back would test items such as connectivity, HVAC, power, water, improper procedures, and/or steps that has been overlooked or not done properly. By moving these first, and fixing any problems identified, the critical operations of the company are not negatively affected.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter
9: Disaster Recovery and Business continuity (page 621).

NEW QUESTION: 794
An effective information security policy should not have which of the following characteristic?
A. Include separation of duties
B. Be designed with a short- to mid-term focus
C. Be understandable and supported by all stakeholders
D. Specify areas of responsibility and authority
Answer: B (LEAVE A REPLY)
An effective information security policy should be designed with a long-term
focus. All other characteristics apply.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices,
Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 397).

NEW QUESTION: 795
A salami attack refers to what type of activity?
A. Setting a program to attack a website at11:59 am on New Year's Eve
B. Embedding or hiding data inside of a legitimate communication - a picture, etc.
C. Hijacking a session and stealing passwords
D. Committing computer crimes in such small doses that they almost go unnoticed
Answer: D (LEAVE A REPLY)

NEW QUESTION: 796
Which of the following is NOT true of the Kerberos protocol?
A. Only a single login is required per session.
B. The initial authentication steps are done using public key algorithm.
C. The KDC is aware of all systems in the network and is trusted by all of them
D. It performs mutual authentication
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/ server applications by using secret-key cryptography. It has the following characteristics:
It is secure: it never sends a password unless it is encrypted.
Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.
The concept depends on a trusted third party - a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.
It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.
Kerberos introduces the concept of a Ticket-Granting Server/Service (TGS). A client that wishes to use a service has to receive a ticket from the TGS - a ticket is a time-limited cryptographic message - giving it access to the server. Kerberos also requires an Authentication Server (AS) to verify clients. The two servers combined make up a KDC.

Within the Windows environment, Active Directory performs the functions of the KDC. The following figure shows the sequence of events required for a client to gain access to a service using Kerberos authentication. Each step is shown with the Kerberos message associated with it, as defined in RFC 4120
"The Kerberos Network Authorization Service (V5)".



Kerberos Authentication Step by Step
Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT).
Step 2: The Authorization Server verifies the user's access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user's password and sends a message back to the user workstation.
The workstation prompts the user for a password and uses the password to decrypt the incoming message. When decryption succeeds, the user will be able to use the TGT to request a service ticket.
Step 3: When the user wants access to a service, the workstation client application sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.
Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned

message contains two copies of a server session key - one encrypted with the client password, and one encrypted by the service password.
Step 5: The client application now sends a service request to the server containing the ticket received in Step 4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.
Step 6: If mutual authentication is required, then the server will reply with a server authentication message.
The Kerberos server knows "secrets" (encrypted passwords) for all clients and servers under its control, or it is in contact with other secure servers that have this information. These "secrets" are used to encrypt all of the messages shown in the figure above.
To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Since the clocks of two computers are often out of synch, administrators can establish a policy to establish the maximum acceptable difference to Kerberos between a client's clock and server's clock. If the difference between a client's clock and the server's clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic. The maximum difference is usually set to five minutes.
Note that if a client application wishes to use a service that is "Kerberized" (the service is configured to perform Kerberos authentication), the client must also be Kerberized so that it expects to support the necessary message responses.
For more information about Kerberos, see http://web.mit.edu/kerberos/www/.
References:
Introduction to Kerberos Authentication from Intel
and
http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/#1.3.5.3
and
http://www.ietf.org/rfc/rfc4120.txt

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

NEW QUESTION: 797
You are running a packet sniffer on a network and see a packet containing a long string of "0x90 0x90

0x90 0x90...." in the middle of it traveling to an x86-based machine as a target. This could be indicative of what activity being attempted?

A. Over-subscription of the traffic on a backbone.

B. A source quench packet.

C. A FIN scan.

D. A buffer overflow attack.

Answer: D (LEAVE A REPLY)

Explanation/Reference:

A series of the same control characters, hexadecimal code, imbedded in the string is usually an indicator of a buffer overflow attack.

The Intel x86 processors use the hexadecimal number 90 to represent NOP (no operation). Many buffer overflow attacks use long strings of control characters and this is representative of that type of attack.

A buffer overflow takes place when too much data are accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed. So, the purpose of a buffer overflow may be either to make a mess, by shoving arbitrary data into various memory segments, or to accomplish a specific task, by pushing into the memory segment a carefully crafted set of data that will accomplish a specific task. This task could be to open a command shell with administrative privilege or execute malicious code.

Common threats to system availability, integrity, and confidentiality include hardware failure, misuse of system privileges, buffer overflows and other memory attacks, denial of service, reverse engineering, and system hacking.

Since many vulnerabilities result from insecure design and most threats are well known, it is the responsibility of the security architect to ensure that their designs are addressing security requirements appropriately while also ensuring that the system can continue to perform its intended function.

The following answers are incorrect:

Over-subscription of the traffic on a backbone. Is incorrect because if there was Over-subscription of the traffic on a backbone, that would typically result in not being able to send or receive any packets, more commonly known as Denial of Service or DoS.

A source quench packet. This is incorrect because a source quench packet is an ICMP message that contains the internet header plus 64 bits of the original datagram.

A FIN scan. This is incorrect because a FIN scan is when a packet with the FIN flag set is sent to a specific port and the results are then analyzed.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page 332, for people using the Kindle edition you will find it at Kindle Locations 7310-7315.

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Architecture and Design (Kindle Locations 1403-1407). . Kindle Edition.

Wikipedia http://en.wikipedia.org/wiki/Port_scanner

ICMP http://security.maruhn.com/iptables-tutorial/x1078.html

Wikipedia http://en.wikipedia.org/wiki/Buffer_overflow

NEW QUESTION: 798
Which of the following is a method of multiplexing data where a communication channel is divided into an arbitrary number of variable bit-rate digital channels or data streams. This method allocates bandwidth dynamically to physical channels having information to transmit?
A. Time-division multiplexing
B. Asynchronous time-division multiplexing
C. Statistical multiplexing
D. Frequency division multiplexing
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Statistical multiplexing is a type of communication link sharing, very similar to dynamic bandwidth allocation (DBA). In statistical multiplexing, a communication channel is divided into an arbitrary number of variable bit- rate digital channels or data streams. The link sharing is adapted to the instantaneous traffic demands of the data streams that are transferred over each channel. This is an alternative to creating a fixed sharing of a link, such as in general time division multiplexing (TDM) and frequency division multiplexing (FDM). When performed correctly, statistical multiplexing can provide a link utilization improvement, called the statistical multiplexing gain.
Generally, the methods for multiplexing data include the following :
Time-division multiplexing (TDM): information from each data channel is allocated bandwidth based on pre- assigned time slots, regardless of whether there is data to transmit. Time-division multiplexing is used primarily for digital signals, but may be applied in analog multiplexing in which two or more signals or bit streams are transferred appearing simultaneously as sub-channels in one communication channel, but are physically taking turns on the channel. The time domain is divided into several recurrent time slots of fixed length, one for each sub-channel. A sample byte or data block of sub-channel 1 is transmitted during time slot
1, sub-channel 2 during time slot 2, etc. One TDM frame consists of one time slot per sub-channel plus a synchronization channel and sometimes error correction channel before the synchronization. After the last sub- channel, error correction, and synchronization, the cycle starts all over again with a new frame, starting with the second sample, byte or data block from sub-channel 1, etc.
Asynchronous time-division multiplexing (ATDM): information from data channels is allocated bandwidth as needed, via dynamically assigned time slots. ATM provides functionality that is similar to both circuit switching and packet switching networks: ATM uses asynchronous time-division multiplexing, and encodes data into small, fixed-sized packets (ISO-OSI frames) called cells. This differs from approaches such as the Internet Protocol or Ethernet that use variable sized packets and frames. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.
These virtual circuits may be "permanent", i.e. dedicated connections that are usually preconfigured by the service provider, or "switched", i.e. set up on a per-call basis using signalling and disconnected when the call is terminated.

Frequency division multiplexing (FDM): information from each data channel is allocated bandwidth based on the signal frequency of the traffic. In telecommunications, frequency-division multiplexing (FDM) is a technique by which the total bandwidth available in a communication medium is divided into a series of non-overlapping frequency sub-bands, each of which is used to carry a separate signal. This allows a single transmission medium such as the radio spectrum, a cable or optical fiber to be shared by many signals.
Reference used for this question:
http://en.wikipedia.org/wiki/Statistical_multiplexing
and
http://en.wikipedia.org/wiki/Frequency_division_multiplexing
and
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 114).

NEW QUESTION: 799
Which of the following statements pertaining to block ciphers is incorrect?
A. It operates on fixed-size blocks of plaintext.
B. It is more suitable for software than hardware implementations.
C. Plain text is encrypted with a public key and decrypted with a private key.
D. Some Block ciphers can operate internally as a stream.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Block ciphers do not use public cryptography (private and public keys).
Block ciphers is a type of symmetric-key encryption algorithm that transforms a fixed-size block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length. They are appropriate for software implementations and can operate internally as a stream. See more info below about DES in Output Feedback Mode (OFB), which makes use internally of a stream cipher.
The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location.
This property allows many error correcting codes to function normally even when applied before encryption.
Reference(s) used for this question:
Wikipedia on Block Cipher mode at: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation and http://www.itl.nist.gov/fipspubs/fip81.htm

NEW QUESTION: 800
Proxies works by transferring a copy of each accepted data packet from one network to another, thereby masking the:
A. data's payload

B. data's details
C. data's owner
D. data's origin
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
The application firewall (proxy) relays the traffic from a trusted host running a specific application to an untrusted server. It will appear to the untrusted server as if the request originated from the proxy server.
"Data's payload" is incorrect. Only the origin is changed.
"Data's details" is incorrect. Only the origin is changed.
"Data's owner" is incorrect. Only the origin is changed.
References:
CBK, p. 467
AIO3, pp. 486 - 490

NEW QUESTION: 801
Which of the following control pairings include: organizational policies and procedures, preemployment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?
A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing
Answer: A (LEAVE A REPLY)
Preventive
/Administrative Pairing: These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 802
The three classic ways of authenticating yourself to the computer security software are by something you know, by something you have, and by something:
A. you need.
B. non-trivial
C. you are.
D. you can get.
Answer: (SHOW ANSWER)

Section: Access Control
Explanation/Reference:
This is more commonly known as biometrics and is one of the most accurate ways to authenticate an individual.
The rest of the answers are incorrect because they not one of the three recognized forms for Authentication.

NEW QUESTION: 803
What is the maximum length of cable that can be used for a twisted-pair, Category 5 10Base-T cable?
A. 80 meters
B. 100 meters
C. 185 meters
D. 500 meters
Answer: B (LEAVE A REPLY)
Explanation/Reference:
As a signal travels though a medium, it attenuates (loses strength) and at some point will become indistinguishable from noise. To assure trouble-free communication, maximum cable lengths are set between nodes to assure that attenuation will not cause a problem. The maximum CAT-5 UTP cable length between two nodes for 10BASE-T is 100M.
The following answers are incorrect:
80 meters. It is only a distracter.
185 meters. Is incorrect because it is the maximum length for 10Base-2
500 meters. Is incorrect because it is the maximum length for 10Base-5

Valid SSCP Dumps shared by PrepPdf.com for Helping Passing SSCP Exam! PrepPdf.com now offer the **newest SSCP exam dumps**, the PrepPdf.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com SSCP dumps with Test Engine here: https://www.preppdf.com/ISC/SSCP-prepaway-exam-dumps.html (**1338** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)