EC-COUNCIL.312-38.v2022-10-06.q121

Exam Code:	312-38
Exam Name:	EC-Council Certified Network Defender CND
Certification Provider:	EC-COUNCIL
Free Question Number:	121
Version:	v2022-10-06
# of views:	2270
# of Questions views:	1210
https://www.freeqas.com/qa/EC-COUNCIL/312-38/EC-COUNCIL.312-38.v2022-10-06.q121.html	

NEW QUESTION: 1
Phishing-like attempts that present users a fake usage bill of the cloud provider is an example of a:
A. Cloud to user attack surface
B. User to service attack surface
C. Cloud to service attack surface
D. User to cloud attack surface
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
Sam wants to implement a network-based IDS in the network. Sam finds out the one IDS solution which works is based on patterns matching. Which type of network-based IDS is Sam implementing?
A. Anomaly-based IDS
B. Stateful protocol analysis
C. Behavior-based IDS
D. Signature-based IDS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
With which of the following forms of acknowledgment can the sender be informed by the data receiver about all segments that have arrived successfully?
A. Block Acknowledgment
B. Negative Acknowledgment
C. Cumulative Acknowledgment
D. Selective Acknowledgment

Answer: (SHOW ANSWER)
Selective Acknowledgment (SACK) is one of the forms of acknowledgment. With selective acknowledgments, the sender can be informed by a data receiver about all segments that have arrived successfully, so the sender retransmits only those segments that have actually been lost. The selective acknowledgment extension uses two TCP options: The first is an enabling option, "SACK-permitted", which may be sent in a SYN segment to indicate that the SACK option can be used once the connection is established. The other is the SACK option itself, which can be sent over an established connection once permission has been given by "SACK-permitted". Answer option A is incorrect. Block Acknowledgment (BA) was initially defined in IEEE 802.11e as an optional scheme to improve the MAC efficiency. IEEE 802.11n capable devices are also referred to as High Throughput (HT) devices.Instead of transmitting an individual ACK for every MPDU, multiple MPDUs can be acknowledged together using a single BA frame. Block Ack (BA) contains bitmap size of 64*16 bits. Each bit of this bitmap represents the status (success/failure) of an MPDU. Answer option B is incorrect. With Negative Acknowledgment, the receiver explicitly notifies the sender which packets, messages, or segments were received incorrectly that may need to be retransmitted. Answer option C is incorrect. With Cumulative Acknowledgment, the receiver acknowledges that it has correctly received a packet, message, or segment in a stream which implicitly informs the sender that the previous packets were received correctly. TCP uses cumulative acknowledgment with its TCP sliding window.

NEW QUESTION: 4
Which of the following are provided by digital signatures?
A. Identification and validation
B. Authentication and identification
C. Integrity and validation
D. Security and integrity
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 5
Which of the following is a Cisco product that performs VPN and firewall functions?
A. IP Packet Filtering Firewall
B. Circuit-Level Gateway
C. Application Level Firewall
D. PIX Firewall
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6

Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify
OPSEC indicators that could reveal critical information and then compare those indicators with the adversary's
intelligence collection capabilities identified in the previous action?
A. Analysis of Threats
B. Application of Appropriate OPSEC Measures
C. Identification of Critical Information
D. Analysis of Vulnerabilities
E. Assessment of Risk
Answer: (SHOW ANSWER)
OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive
information and preserve essential secrecy.
The OPSEC process has five steps, which are as follows:
1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary,
which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to
protect all classified or sensitive unclassified information.
2.Analysis of Threats: This step includes the research and analysis of intelligence, counter-intelligence, and
open source information to identify likely adversaries to a planned operation.
3.Analysis of Vulnerabilities: It includes examining each aspect of the planned operation to identify OPSEC
indicators that could reveal critical information and then comparing those indicators with the adversary's
intelligence collection capabilities identified in the previous action.
4.Assessment of Risk: Firstly, planners analyze the vulnerabilities identified in the previous action and identify
possible OPSEC measures for each vulnerability. Secondly, specific OPSEC measures are selected for
execution based upon a risk assessment done by the commander and staff.
5.Application of Appropriate OPSEC Measures: The command implements the OPSEC measures selected in
the assessment of risk action or, in the case of planned future operations and activities, includes the measures
in specific OPSEC plans.

NEW QUESTION: 7

Attacks are classified into which of the following? Each correct answer represents a complete solution. Choose all that apply.

A. Active attack

B. Session hijacking

C. Passive attack

D. Replay attack

Answer: A,C (LEAVE A REPLY)

An attack is an action against an information system or network that attempts to violate the system's security policy. Attacks can be broadly classified as being either active or passive. 1.Active attacks modify the target system or message, i.e. they violate the integrity of the system or message. 2.Passive attacks violate confidentiality without affecting the state of the system. An example of such an attack is the electronic eavesdropping on network transmissions to release message contents or to gather unprotected passwords.

Answer options B and D are incorrect. Session hijacking and replay attacks come under the category of active attacks.

NEW QUESTION: 8

Which of the following offer "always-on" Internet service for connecting to your ISP? Each correct answer represents a complete solution. Choose all that apply.

A. analog modem

B. digital modem

C. DSL

D. cable modem

Answer: C,D (LEAVE A REPLY)

Explanation

NEW QUESTION: 9

The _____ protocol works in the network layer and is responsible for handling the error codes during the delivery of packets. This protocol is also responsible for providing communication in the TCP/IP stack.

A. DHCP

B. ICMP

C. RARP

D. ARP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 10

A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It

provides an attacker unauthorized access to a computer. Which of the following tools can an attacker use to
perform war dialing? Each correct answer represents a complete solution. Choose all that apply.
A. ToneLoc
B. Wingate
C. THC-Scan
D. NetStumbler
Answer: A,C (LEAVE A REPLY)
THC-Scan and ToneLoc are tools used for war dialing. A war dialer is a tool that is used to scan thousands of
telephone numbers to detect vulnerable modems. It provides the attacker unauthorized access to a computer.
Answer option D is incorrect. NetStumbler is a Windows-based tool that is used for the detection of wireless
LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. It detects wireless networks and marks their
relative position with a GPS. It uses an 802.11 Probe Request
that has been sent to the broadcast destination address.
Answer option B is incorrect. Wingate is a proxy server.

NEW QUESTION: 11
Which of the following statements are true about a wireless network?
Each correct answer represents a complete solution. Choose all that apply.
A. Data can be shared easily between wireless devices.
B. It provides mobility to users to access a network.
C. Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC, etc.
D. It is easy to connect.
Answer: A,B,C,D (LEAVE A REPLY)
The advantages of a wireless network are as follows:
It provides mobility to users to access a network.
It is easy to connect.
The initial cost to set up a wireless network is low as compared to that of manual cable network. Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC, etc. Data can be shared easily between the wireless devices.

NEW QUESTION: 12
The IR team and the network administrator have successfully handled a malware incident on the network. The team is now preparing countermeasure guideline to avoid a future occurrence of the malware incident.

Which of the following countermeasure(s) should be added to deal with future malware incidents? (Select all that apply)

A. Install antivirus software

B. Complying with the company's security policies

C. Implementing strong authentication schemes

D. Implementing a strong password policy

Answer: A (LEAVE A REPLY)

NEW QUESTION: 13

Which of the following flags is set when a closed port responds to an Xmas tree scan?

A. RST

B. FIN

C. PUSH

D. ACK

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14

Which of the following security models enable strict identity verification for every user or device attempting to access the network resources?

1. Zero-trust network model
2. Castle-and-Moat model

A. None

B. Both 1 and 2

C. 1 only

D. 2 only

Answer: C (LEAVE A REPLY)

NEW QUESTION: 15

How is application whitelisting different from application blacklisting?

A. It allows execution of untrusted applications in an isolated environment

B. It allows execution of trusted applications in a unified environment

C. It rejects all applications other than the allowed applications

D. It allows all applications other than the undesirable applications

Answer: (SHOW ANSWER)

NEW QUESTION: 16

Which of the following TCP commands are used to allocate a receiving buffer associated with the specified
connection?

A. Send

B. Close

C. None
D. Receive
E. Interrupt
Answer: D (LEAVE A REPLY)
The Receive command is used to allocate a receiving buffer associated with the specified connection. An error
is returned if no OPEN precedes this command or the calling process is not authorized to use this connection.
Answer option A is incorrect. The Send command causes the data contained in the indicated user buffer to be
sent to the indicated connection.
Answer option C is incorrect. The Abort command causes all pending SENDs and RECEIVES to be aborted.
Answer option B is incorrect. The Close command causes the connection specified to be closed.

NEW QUESTION: 17
To provide optimum security while enabling safe/necessary services, blocking known dangerous services, and making employees accountable for their online activity, what Internet Access policy would Brian, the network administrator, have to choose?
A. Paranoid policy
B. Permissive policy
C. Promiscuous policy
D. Prudent policy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
Which BC/DR activity includes action taken toward resuming all services that are dependent on business-critical applications?
A. Recovery
B. Resumption
C. Response

D. Restoration
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines. What are the other f unction(s) of the device? (Select all that apply)
A. Enables input/output (I/O) operations
B. Assigns user addresses
C. Manages security keys
D. Provides access memory, achieving high efficiency
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 20
Which of the following is a process of transformation where the old system can no longer be maintained?
A. Crisis
B. Risk
C. Disaster
D. Threat
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
The IP addresses reserved for experimental purposes belong to which of the following classes?
A. Class C
B. Class A
C. Class E
D. Class D
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
Which of the following layers refers to the higher-level protocols used by most applications for network communication?
A. Internet layer
B. Transport layer
C. Application layer
D. Link layer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 23
CORRECT TEXT

Fill in the blank with the appropriate term._____is a codename referring to investigations and studies of compromising emission (CE).

Answer:

TEMPEST

Explanation:

TEMPEST is a codename referring to investigations and studies of compromising emission (CE). Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment. Tempest stands for Transient ElectroMagnetic Pulse Emanations Standard according to Certified Information Systems Security Professional training. TEMPEST was the name of a U.S. government project to study the effects of electric or electromagnetic radiation emanations from electronic equipment.

NEW QUESTION: 24

Timothy works as a network administrator in a multinational organization. He decides to implement a dedicated network for sharing storage resources. He uses a_____as it seperates the storage units from the servers and the user network.

A. NAS

B. SAN

C. SAS

D. SCSA

Answer: B (LEAVE A REPLY)

NEW QUESTION: 25

Which of the following TCP commands are used to allocate a receiving buffer associated with the specified connection?

A. Send

B. Close

C. None

D. Receive

E. Interrupt

Answer: D (LEAVE A REPLY)

The Receive command is used to allocate a receiving buffer associated with the specified connection. An error is returned if no OPEN precedes this command or the calling process is not authorized to use this connection.

Answer option A is incorrect. The Send command causes the data contained in the indicated user buffer to be sent to the indicated connection.

Answer option C is incorrect. The Abort command causes all pending SENDs and RECEIVES to be aborted.

Answer option B is incorrect. The Close command causes the connection specified to be closed.

NEW QUESTION: 26
Which of the following is a computer network that covers a broad area?
A. PAN
B. SAN
C. WAN
D. CAN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
Which of the following provide an "always on" Internet access service when connecting to an ISP? Each correct answer represents a complete solution. (Choose two.)
A. Digital modem
B. Cable modem
C. Analog modem
D. DSL
Answer: (SHOW ANSWER)
DSL and Cable modems are used in remote-access WAN technology for connecting to the Internet. Both provide an "always on" Internet access service.
Answer options C and A are incorrect. Analog and Digital modems are not always in 'ON' mode when connecting to an ISP. Analog modems transmit analog voice signals, while Digital modems transmit digital signals over a link.

NEW QUESTION: 28
Which of the following is a symmetric 64-bit block cipher that can support key lengths up to 448 bits?
A. IDEA
B. HAVAL
C. XOR
D. BLOWFISH
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
Which of the following statements are true about security risks? Each correct answer represents a complete solution. (Choose three.)
A. They are considered an indicator of threats coupled with vulnerability.
B. They can be removed completely by taking proper actions.
C. They can be analyzed and measured by the risk analysis process.

D. They can be mitigated by reviewing and taking responsible actions based on possible risks.

Answer: A,C,D (LEAVE A REPLY)

In information security, security risks are considered an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. These risks can be analyzed and measured by the risk analysis process.

Answer option B is incorrect. Security risks can never be removed completely but can be mitigated by taking proper actions.

NEW QUESTION: 30

Which of the following ranges of addresses can be used in the first octet of a Class C network address?

A. 128-191

B. 0-127

C. 224-255

D. 192-223

Answer: D (LEAVE A REPLY)

NEW QUESTION: 31

CORRECT TEXT

Fill in the blank with the appropriate term. A _____is a block of data that a Web server stores on the client computer.

Answer:

cookie

Explanation:

Cookie is a block of data, which a Web server stores on the client computer. If no expiration date is set for the cookie, it expires when the browser closes. If the expiration date is set for a future date, the cookie will be stored on the client's disk after the session ends. If the expiration date is set for a past date, the cookie is deleted.

Topic 2, Volume B

NEW QUESTION: 32
Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?
A. Spoofing
B. Smurf
C. Session hijacking
D. Phishing
Answer: C (LEAVE A REPLY)
Session hijacking refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to Web developers, as the HTTP cookies used to maintain a session on many Web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer (see HTTP cookie theft).TCP session hijacking is when a hacker takes over a TCP session between two machines. Since most authentication only occurs at the start of a TCP session, this allows the hacker to gain access to a machine. Answer option A is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected. Answer option B is incorrect. Smurf is an attack that generates significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages. In such attacks, a perpetrator sends a large amount of ICMP echo request (ping) traffic to IP broadcast addresses, all of which have a spoofed source IP address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all hosts, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, which multiplies the traffic by the number of hosts responding. Answer option D is incorrect. Phishing is a type of scam that entices a user to disclose personal information such as social security number, bank account details, or credit card number. An example of phishing attack is a fraudulent e-mail that appears to come from a user's bank asking to change his online banking password. When the user clicks the link available on the e-mail, it directs him to a phishing site which replicates the original bank site. The phishing site lures the user to provide his personal information.

NEW QUESTION: 33

A newly joined network administrator wants to assess the organization against possible risk. He notices the organization doesn't have a_____identified which helps measure how risky an activity is.

A. Risk Matrix

B. Key Risk Indicator

C. Risk Severity

D. Risk levels

Answer: B (LEAVE A REPLY)

NEW QUESTION: 34

You work as the network administrator for uCertify Inc. The company has planned to add the support for IPv6 addressing. The initial phase deployment of IPv6 requires support from some IPv6-only devices. These devices need to access servers that support only IPv4. Which of the following tools would be suitable to use?

A. Multipoint tunnels

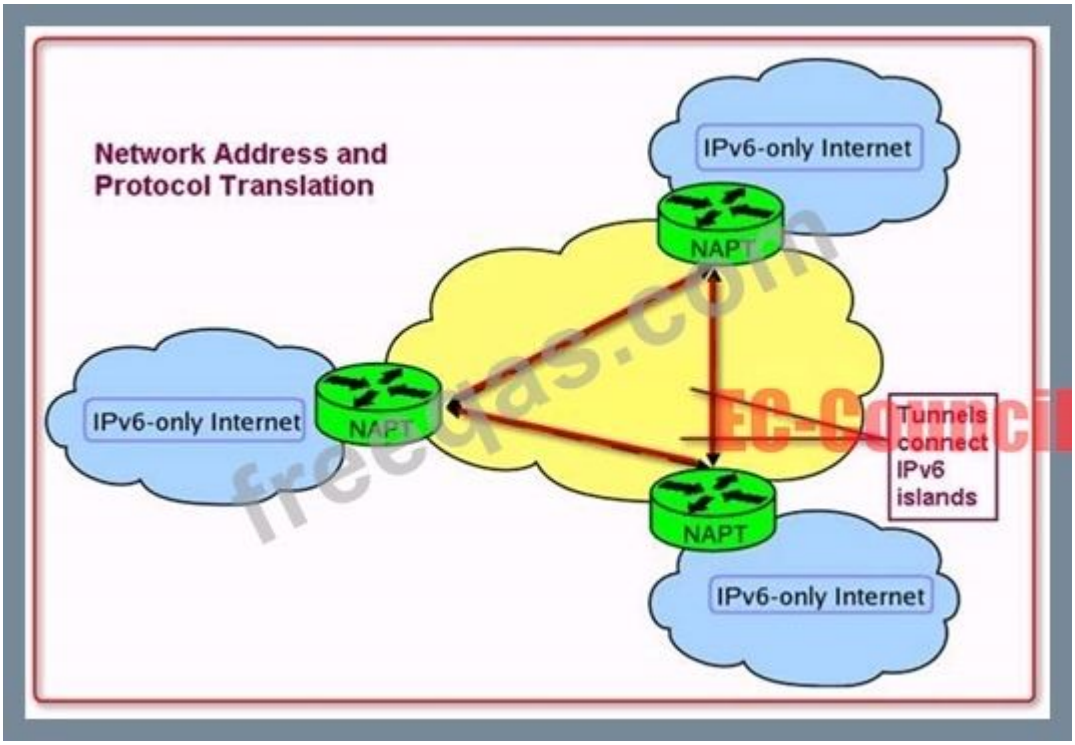
B. NAT-PT

C. Point-to-point tunnels

D. Native IPv6

Answer: B (LEAVE A REPLY)

NAT-PT (Network address translation-Protocol Translation) is useful when an IPv4-only host needs to communicate with an IPv4-only host. NAT-PT (Network Address Translation-Protocol Translation) is an implementation of RFC 2766 as specified by the IETF. NAT-PT was designed so that it can be run on low-end, commodity hardware. NAT-PT runs in user space, capturing and translating packets between the IPv6 and IPv4 networks (and vice-versa). NAT-PT uses the Address Resolution Protocol (ARP) and Neighbor Discovery (ND) on the IPv4 and IPv6 network systems, respectively.



NAT-Protocol Translation can be used to translate both the source and destination IP addresses. Answer option D is incorrect. Native IPv6 is of use when the IPv6 deployment is pervasive, with heavy traffic loads. Answer option C is incorrect. Point-to-point tunnels work well when IPv6 is needed only in a subset of sites. These point-to-point tunnels act as virtual point-to-point serial link. These are
useful when the traffic is of very high volume.
Answer option A is incorrect. The multipoint tunnels are used for IPv6 deployment even when IPv6
is needed in a subset of sites and is suitable when the traffic is infrequent and of less predictable
volume.

NEW QUESTION: 35
Which of the following creates passwords for individual administrator accounts and stores them in Windows AD?
A. SRM
B. LAPS
C. SAM
D. LSASS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the

interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts. Which of the following attacks is being used by Eve?

A. Replay

B. Fire walking

C. Cross site scripting

D. Session fixation

Answer: A (LEAVE A REPLY)

Eve is using Replay attack. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Session tokens can be used to avoid replay attacks. Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Mallory has captured this value and tries to use it on another session; Bob sends a different session token, and when Mallory replies with the captured value it will be different from Bob's computation. Answer option C is incorrect. In the cross site scripting attack, an attacker tricks the user's computer into running code, which is treated as trustworthy because it appears to belong to the server, allowing the attacker to obtain a copy of the cookie or perform other operations. Answer option B is incorrect. Firewalking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. Answer option D is incorrect. In session fixation, an attacker sets a user's session id to one known to him, for example by sending the user an email with a link that contains a particular session id. The attacker now only has to wait until the user logs in.

NEW QUESTION: 37

According to the company's security policy, all access to any network resources must use Windows Active Directory Authentication. A Linux server was recently installed to run virtual servers and it is not using Windows Authentication. What needs to happen to force this server to use Windows Authentication?

A. Edit the PAM file to enforce Windows Authentication

B. Edit the shadow file.

C. Remove the /var/bin/localauth.conf file.

D. Edit the ADLIN file.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
Which of the following is a software tool used in passive attacks for capturing network traffic?
A. Sniffer
B. Intrusion detection system
C. Intrusion prevention system
D. Warchalking
Answer: (SHOW ANSWER)
A sniffer is a software tool that is used to capture any network traffic. Since a sniffer changes the NIC of the LAN card into promiscuous mode, the NIC begins to record incoming and outgoing data traffic across the network. A sniffer attack is a passive attack because the attacker does not directly connect with the target host.
This attack is most often used to grab logins and passwords from network traffic. Tools such as Ethereal, Snort, Windump, EtherPeek, Dsniff are some good examples of sniffers. These tools provide many facilities to users such as graphical user interface, traffic statistics graph, multiple sessions tracking, etc.
Answer option C is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass.
Answer option B is incorrect. An IDS (Intrusion Detection System) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
Answer option D is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

NEW QUESTION: 39
Identify the network topology where each computer acts as a repeater and the data passes from one computer to the other in a single direction until it reaches the destination.
A. Ring
B. Bus
C. Star
D. Mesh
Answer: A (LEAVE A REPLY)

NEW QUESTION: 40
Which of the following are the six different phases of the Incident handling process? Each correct answer represents a complete solution. Choose all that apply.
A. Containment
B. Identification
C. Post mortem review
D. Preparation
E. Lessons learned
F. Recovery
G. Eradication
Answer: (SHOW ANSWER)
Following are the six different phases of the Incident handling process: 1.Preparation: Preparation is the first step in the incident handling process. It includes processes like backing up copies of all key data on a regular basis, monitoring and updating software on a regular basis, and creating and implementing a documented security policy. To apply this step a documented security policy is formulated that outlines the responses to various incidents, as a reliable set of instructions during the time of an incident. The following list contains items that the incident handler should maintain in the preparation phase i.e. before an incident occurs: Establish applicable policies Build relationships with key players Build response kit Create incident checklists Establish communication plan Perform threat modeling Build an incident response team Practice the demo incidents 2.Identification: The Identification phase of the Incident handling process is the stage at which the Incident handler evaluates the critical level of an incident for an enterprise or system. It is an important stage where the distinction between an event and an incident is determined, measured and tested. 3.Containment: The Containment phase of the Incident handling process supports and builds up the incident combating process. It helps in ensuring the stability of the system and also confirms that the incident does not get any worse. 4.Eradication: The Eradication phase of the Incident handling process involves the cleaning-up of the identified harmful incidents from the system. It includes the analyzing of the information that has been gathered for determining how the attack was committed. To prevent the incident from happening again, it is vital to recognize how it was conceded out so that a prevention technique is applied. 5.Recovery: Recovery is the fifth step of the incident handling process. In this phase, the Incident Handler places the system back into the working environment. In the recovery phase the Incident Handler also works with the questions to validate that the system recovery is successful. This involves testing the system to make sure that all the processes and functions are working normal. The Incident Handler also monitors the system to make sure that the systems are not compromised again. It looks for additional signs of attack. 6.Lessons learned: Lessons learned is the sixth and the final step of incident handling process. The Incident Handler utilizes the knowledge and experience he learned during the handling of the incident to enhance and

improve the incident-handling process. This is the most ignorant step of all incident handling processes. Many times the Incident Handlers are relieved to have systems back to normal and get busy trying to catch up other unfinished work. The Incident Handler should make documents related to the incident or look for ways to improve the process.
Answer option C is incorrect. The post mortem review is one of the phases of the Incident response process.

NEW QUESTION: 41
Which of the following is an attack on a website that changes the visual appearance of the site and seriously
damages the trust and reputation of the website?
A. Website defacement
B. Zero-day attack
C. Spoofing
D. Buffer overflow
Answer: (SHOW ANSWER)
Website defacement is an attack on a website that changes the visual appearance of the site. These are
typically the work of system crackers, who break into a Web server and replace the hosted website with one of
their own. Sometimes, the Defacer makes fun of the system administrator for failing to maintain server
security. Most times, the defacement is harmless; however, it can sometimes be used as a distraction to cover
up more sinister actions such as uploading malware.
A high-profile website defacement was carried out on the website of the company SCO Group following its
assertion that Linux contained stolen code. The title of the page was changed from Red Hat vs. SCO to SCO
vs. World with various satirical content.
Answer option D is incorrect. Buffer overflow is a condition in which an application receives more data than it is
configured to accept. This usually occurs due to programming errors in the application. Buffer overflow can
terminate or crash the application.
Answer option B is incorrect. A zero-day attack, also known as zero-hour attack, is a computer threat that tries
to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor,
or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out

an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User
awareness training is the most effective technique to mitigate such attacks.
Answer option C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an
authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies
packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used
while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to
be misdirected.

NEW QUESTION: 42
Which of the following is a network analysis tool that sends packets with nontraditional IP stack parameters?
A. COPS
B. Nessus
C. HPing
D. SAINT
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
A local bank wants to protect their card holder dat
a. The bank should comply with the_____standard to ensure the security of card holder data.
A. SOAX
B. HIPAA
C. ISEC
D. PCI DSS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
Which of the following policies to help define what users can and should do to use the network and organization of computer equipment?
A. remote access policy
B. user policy
C. general policy
D. IT policy
E. None
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which of the following steps will NOT make a server fault tolerant? Each correct answer represents a complete solution. Choose two.
A. Adding a second power supply unit
B. Performing regular backup of the server
C. Adding one more same sized disk as mirror on the server
D. Implementing cluster servers facility
E. Encrypting confidential data stored on the server
Answer: B,E (LEAVE A REPLY)
Encrypting confidential data stored on the server and performing regular backup will not make the server fault tolerant. Fault tolerance is the ability to continue work when a hardware failure occurs on a system. A fault-tolerant system is designed from the ground up for reliability by building multiples of all critical components, such as CPUs, memories, disks and power supplies into the same computer. In the event one component fails, another takes over without skipping a beat. Answer options A, C, and D are incorrect. The following steps will make the server fault tolerant: Adding a second power supply unit Adding one more same sized disk as a mirror on the serverImplementing cluster servers facility

NEW QUESTION: 46
How can a WAF validate traffic before it reaches a web application?
A. It uses a role-based filtering technique
B. It uses a rule-based filtering technique
C. It uses an access-based filtering technique
D. It uses a sandboxing filtering technique
Answer: B (LEAVE A REPLY)

NEW QUESTION: 47
Which of the following tools is described below? It is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of its tools include arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. It is highly effective for sniffing both switched and shared

networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP,
etc.

A. Dsniff

B. Cain

C. Libnids

D. LIDS

Answer: A (LEAVE A REPLY)

Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff include dsniff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc. Answer option B is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks: Dictionary attack Brute force attack Rainbow attack Hybrid attack Answer options D and C are incorrect. These tools are port scan detection tools that are used in the Linux operating system.

NEW QUESTION: 48

Which of the following network monitoring techniques requires extra monitoring software or hardware?

A. Router based

B. Non-router based

C. Switch based

D. Hub based

Answer: B (LEAVE A REPLY)

NEW QUESTION: 49

Which of the following is a communication protocol multicasts messages and information of all the member IP multicast group?

A. ICMP

B. None

C. EGP

D. IGMP

E. BGP

Answer: D (LEAVE A REPLY)

NEW QUESTION: 50

How many layers are present in the TCP/IP model?
A. 5
B. 10
C. 7
D. 4
Answer: A (LEAVE A REPLY)

NEW QUESTION: 51
What is the range for private ports?
A. 1024 through 49151
B. 49152 through 65535
C. Above 65535
D. 0 through 1023
Answer: B (LEAVE A REPLY)

NEW QUESTION: 52
Which of the following is the primary international body for fostering cooperative standards for telecommunications equipment and systems?
A. ICANN
B. IEEE
C. NIST
D. CCITT
Answer: D (LEAVE A REPLY)
CCITT is the primary international body for fostering cooperative standards for telecommunications equipment and systems. It is now known as the ITU-T (for Telecommunication Standardization Sector of the International Telecommunications Union). The ITU-T mission is to ensure the efficient and timely production of standards covering all fields of telecommunications on a worldwide basis, as well as defining tariff and accounting principles for international telecommunication services.
Answer option A is incorrect. Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management.
Answer option B is incorrect. The Institute of Electrical and Electronic Engineers (IEEE) is a society of technical professionals. It promotes the development and application of electro-technology and allied sciences. IEEE develops communications and network standards, among other activities. The organization publishes number of journals, has many local chapters, and societies in specialized areas.
Answer option C is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a

measurement standards laboratory which is a non- regulatory agency of the United States Department of Commerce. The institute's official mission is as follows:
To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.
NIST had an operating budget for fiscal year 2007 (October 1, 2006-September 30, 2007) of about $843.3 million. NIST's 2009 budget was $992 million, but it also received $610 million as part of the American Recovery and Reinvestment Act. NIST employs about 2,900 scientists, engineers, technicians, and support and administrative personnel. About 1,800 NIST associates (guest researchers and engineers from American companies and foreign nations) complement the staff. In addition, NIST partners with 1,400 manufacturing specialists and staff at nearly 350 affiliated centers around the country.

NEW QUESTION: 53
Which of the following is the standard protocol that provides VPN security at the highest level?
A. PPP
B. P.M
C. None
D. IPSec
E. L2TP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 54
CORRECT TEXT
Fill in the blank with the appropriate term.
_____ is an enumeration technique used to glean information about computer systems on a network and the services running its open ports.
Answer:
Banner grabbing
Explanation:
Banner grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Administrators can use this to take inventory of the systems and services on their network. An intruder however can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits. Some examples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, which is included with most operating systems, and Netcat. For example, one could establish a connection to a target host running a Web service with netcat, then send a bad html

request in order to get information about the service on the host: [root@prober] nc www.targethost.com 80 HEAD / HTTP/1.1 HTTP/1.1 200 OK Date: Mon, 11 May 2009 22:10:40 EST Server: Apache/2.0.46 (Unix) (Red Hat/Linux) Last-Modified: Thu, 16 Apr 2009 11:20:14 PST ETag: "1986-69b-123a4bc6" Accept-Ranges: bytes Content-Length: 1110 Connection: close Content-Type: text/html The administrator can now catalog this system or an intruder now knows what version of Apache to look for exploits.

NEW QUESTION: 55
Which of the following protocols sends a jam signal when a collision is detected?
A. ALOHA
B. CSMA/CD
C. CSMA
D. CSMA/CA
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Which among the following filter is used to detect a SYN/FIN attack?
A. tcp.flags==0x004
B. tcp.flags==0x003
C. tcp.flags==0x001
D. tcp.flags==0x002
Answer: (SHOW ANSWER)

NEW QUESTION: 57
Which of the following honeypots provides an attacker access to the real operating system without any
restriction and collects a vast amount of information about the attacker?
A. High-interaction honeypot
B. Medium-interaction honeypot
C. Honeyd
D. Low-interaction honeypot
Answer: A (LEAVE A REPLY)
A high-interaction honeypot offers a vast amount of information about attackers. It provides an attacker access
to the real operating system without any restriction. A high-interaction honeypot is a powerful weapon that
provides opportunities to discover new tools, to identify new vulnerabilities in the operating system, and to learn
how blackhats communicate with one another.
Answer option D is incorrect. A low-interaction honeypot captures limited amounts of information that are

mainly transactional data and some limited interactive information. Because of simple design and basic
functionality, low-interaction honeypots are easy to install, deploy, maintain, and configure. A low-interaction
honeypot detects unauthorized scans or unauthorized connection attempts. A low-interaction honeypot is like a
one-way connection, as the honeypot provides services that are limited to listening ports. Its role is very
passive and does not alter any traffic. It generates logs or alerts when incoming packets match their patterns.
Answer option B is incorrect. A medium-interaction honeypot offers richer interaction capabilities than a low-
interaction honeypot, but does not provide any real underlying operating system target. Installing and
configuring a medium-interaction honeypot takes more time than a low-interaction honeypot. It is also more
complicated to deploy and maintain as compared to a low-interaction honeypot. A medium-interaction honeypot
captures a greater amount of information but comes with greater risk. Answer option C is incorrect. Honeyd is
an example of a low-interaction honeypot.

NEW QUESTION: 58
Which of the following fields in the IPv6 header replaces the TTL field in the IPv4 header?
A. Next header
B. Traffic class
C. Hop limit
D. Version
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 59
Which of the following is a distributed application architecture that partitions tasks or workloads between service providers and service requesters? Each correct answer represents a complete solution. Choose all that apply.
A. Client-server computing
B. Peer-to-peer (P2P) computing
C. Client-server networking
D. Peer-to-peer networking
Answer: A,C (LEAVE A REPLY)
Explanation/Reference:

Explanation:
Client-server networking is also known as client-server computing. It is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients.
Often clients and servers operate over a computer network on separate hardware. A server machine is a high- performance host that is running one or more server programs which share its resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.
Answer options D and B are incorrect. Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. Peer-to-peer networking (also known simply as peer networking) differs from client-server networking, where certain devices have the responsibility to provide or "serve" data, and other devices consume or otherwise act as "clients" of those servers.

NEW QUESTION: 60
You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company. The suspected employee is using an online e-mail system such as Hotmail or Yahoo. Which of the following folders on the local computer will you review to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.
A. History folder
B. Temporary Internet Folder
C. Cookies folder
D. Download folder
Answer: (SHOW ANSWER)
Online e-mail systems such as Hotmail and Yahoo leave files containing e-mail message information on the local computer. These files are stored in a number of folders, which are as follows:
Cookies folder
Temp folder
History folder
Cache folder
Temporary Internet Folder Forensic tools can recover these folders for the respective e-mail clients. When folders are retrieved, e-mail files can be accessed. If the data is not readable, various tools are available to decrypt the information such as a cookie reader used with cookies.
Answer option D is incorrect. Download folder does not contain any e-mail message information.

NEW QUESTION: 61
FILL BLANK
Fill in the blank with the appropriate term. A _____ is a set of tools that take Administrative control
of a computer system without authorization by the computer owners and/or legitimate managers.
Answer:
rootkit
Explanation:
A rootkit is a set of tools that take Administrative control of a computer system without authorization by the
computer owners and/or legitimate managers. A rootkit requires root access to be installed in the Linux
operating system, but once installed, the attacker can get root access at any time. Rootkits have the following
features:
They allow an attacker to run packet sniffers secretly to capture passwords.
They allow an attacker to set a Trojan into the operating system and thus open a backdoor for anytime access.
They allow an attacker to replace utility programs that can be used to detect the attacker's activity.
They provide utilities for installing Trojans with the same attributes as legitimate programs.

NEW QUESTION: 62
Which among the following is used to limit the number of cmdlets or administrative privileges of administrator, user, or service accounts?
A. User Account Control (UAC)
B. Credential Guard
C. Windows Security Identifier (SID)
D. Just Enough Administration (EA)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 63
Which of the following are the common security problems involved in communications and email?
Each correct answer represents a complete solution. Choose all that apply.
A. False message
B. Message digest
C. Message replay
D. Message repudiation
E. Message modification
F. Eavesdropping
G. Identity theft
Answer: A,C,D,E,F,G (LEAVE A REPLY)
Following are the common security problems involved in communications and email:
Eavesdropping: It is the act of secretly listening to private information through telephone lines, e-
mail, instant messaging, and any other method of communication considered private.
Identity theft: It is the act of obtaining someone's username and password to access his/her email
servers for reading email and sending false email messages. These credentials can be obtained
by eavesdropping on SMTP, POP, IMAP, or Webmail connections.
Message modification: The person who has system administrator permission on any of the SMTP
servers can visit anyone's message and can delete or change the message before it continues on
to its destination. The recipient has no way of telling that the email message has been altered.
False message: It the act of constructing messages that appear to be sent by someone else.
Message replay: In a message replay, messages are modified, saved, and re-sent later.
Message repudiation: In message repudiation, normal email messages can be forged. There is no
way for the receiver to prove that someone had sent him/her a particular message. This means
that even if someone has sent a message, he/she can successfully deny it.
Answer option B is incorrect. A message digest is a number that is created algorithmically from a
file and represents that file uniquely.

NEW QUESTION: 64

Which of the following protocols is a method of implementing virtual private networks?
A. IRDP
B. PPTP
C. OSPF
D. DHCP
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which of the following UTP cables supports transmission up to 20MHz?
A. Category 1
B. Category 5e
C. Category 2
D. Category 4
Answer: (SHOW ANSWER)

NEW QUESTION: 66
Justine has been tasked by her supervisor to ensure that the company's physical security is on the same level as their logical security measures. She installs video cameras at all entrances and exits and installs badge access points for all doors. The last item she wants to install is a method to prevent unauthorized people piggybacking employees. What should she install to prevent piggybacking?
A. Justine needs to install a biometrics station at each entrance
B. Justine will need to install a revolving security door
C. She should install a Thompson Trapdoor.
D. She should install a mantrap
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which of the following are valid steps to secure routers? Each correct answer represents a complete solution.
Choose all that apply.
A. Keep routers updated with the latest security updates.
B. Configure access list entries to prevent unauthorized connections and routing.
C. Use a password that is easy to remember the router's administrative console.
D. Use a complex password of the router management console.
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Which of the following is an IPSec protocol that can be used alone in combination with Authentication Header (AH)?
A. L2TP

B. PPTP
C. PPP
D. ESP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
CORRECT TEXT
Fill in the blank with the appropriate term. The _____layer establishes, manages, and terminates the connections between the local and remote application.
Answer:
session
Explanation:
The session layer of the OSI/RM controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session check pointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls.

NEW QUESTION: 70
Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?
A. Disaster Recovery Plan
B. Business Continuity Plan
C. Contingency Plan
D. Continuity of Operations Plan
Answer: B (LEAVE A REPLY)
BCP is a strategy to minimize the consequence of the instability and to allow for the continuation of business processes. The goal of BCP is to minimize the effects of a disruptive event on a company, and is formed to avoid interruptions to normal business activity. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer option C is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process

and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer option A is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity. Answer option D is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

NEW QUESTION: 71
Which of the following is also known as slag code?
A. Logic bomb
B. Worm
C. Trojan
D. IRC bot
Answer: A (LEAVE A REPLY)

NEW QUESTION: 72
Which of the following is a software tool used in passive attacks for capturing network traffic?
A. Sniffer
B. Intrusion detection system
C. Intrusion prevention system
D. Warchalking
Answer: A (LEAVE A REPLY)
A sniffer is a software tool that is used to capture any network traffic. Since a sniffer changes the NIC of the LAN card into promiscuous mode, the NIC begins to record incoming and outgoing data traffic across the network. A sniffer attack is a passive attack because the attacker does not directly connect with the target host. This attack is most often used to grab logins and passwords from network traffic. Tools such as Ethereal, Snort, Windump, EtherPeek, Dsniff are some good examples of sniffers. These tools provide many facilities to users such as graphical user interface, traffic statistics graph, multiple sessions tracking, etc. Answer option C is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those

activities. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass. Answer option B is incorrect. An IDS (Intrusion Detection System) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. Answer option D is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

NEW QUESTION: 73
Which of the following tool is used for passive attacks to capture network traffic?
A. Intrusion prevention system
B. Intrusion detection system
C. Sniffer
D. None
E. warchalking
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
How is an "attack" represented?
A. Motive (goal) + method + vulnerability
B. Asset + Threat + Vulnerability
C. Motive (goal) + method
D. Asset + Threat
Answer: C (LEAVE A REPLY)

NEW QUESTION: 75
Which of the following is a standard-based protocol that provides the highest level of VPN security?
A. L2TP
B. IP
C. PPP
D. IPSec
Answer: D (LEAVE A REPLY)
Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and

password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP). Answer option B is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide. Answer option C is incorrect. Point-to-Point Protocol (PPP) is a remote access protocol commonly used to connect to the Internet. It supports compression and encryption and can be used to connect to a variety of networks. It can connect to a network running on the IPX, TCP/IP, or NetBEUI protocol. It supports multi-protocol and dynamic IP assignments. It is the default protocol for the Microsoft Dial-Up adapter. Answer option A is incorrect. Layer 2 Tunneling Protocol (L2TP) is a more secure version of Point-to-Point Tunneling Protocol (PPTP). It provides tunneling, address assignment, and authentication. It allows the transfer of Point-to-Point Protocol (PPP) traffic between different networks.L2TP combines with IPSec to provide tunneling and security for Internet Protocol (IP), Internetwork Packet Exchange (IPX), and other protocol packets across IP networks.

NEW QUESTION: 76
Which of the following is a physical security device designed to entrap a person on purpose?
A. War Chalking
B. Trap
C. Mantrap
D. War Flying
Answer: C (LEAVE A REPLY)

NEW QUESTION: 77

Which of the following router configuration modes to change the terminal settings temporarily, perform basic tests, and lists the system information?
A. user EXEC
B. None
C. UI Config
D. Global Config
E. the privileged EXEC
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
Which of the following layers of the OSI model provides interhost communication?
A. Session layer
B. Network layer
C. Application layer
D. Transport layer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 79
Which of the following TCP/IP state transitions represents no connection state at all?
A. Closed
B. Fin-wait-1
C. Closing
D. Close-wait
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80
Which of the following is the primary international body for fostering cooperative standards for telecommunications equipment and systems?
A. ICANN
B. IEEE
C. NIST
D. CCITT
Answer: D (LEAVE A REPLY)
CCITT is the primary international body for fostering cooperative standards for telecommunications equipment and systems. It is now known as the ITU-T (for Telecommunication Standardization Sector of the International Telecommunications Union). The ITU-T mission is to ensure the efficient and timely production of standards covering all fields of telecommunications on a worldwide basis, as well as defining tariff and accounting principles for international telecommunication services. Answer option A is incorrect. Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that oversees the allocation of IP addresses, management of the DNS

infrastructure, protocol parameter assignment, and root server system management. Answer option B is incorrect. The Institute of Electrical and Electronic Engineers (IEEE) is a society of technical professionals. It promotes the development and application of electrotechnology and allied sciences. IEEE develops communications and network standards, among other activities. The organization publishes number of journals, has many local chapters, and societies in specialized areas. Answer option C is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is as follows: To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. NIST had an operating budget for fiscal year 2007 (October 1, 2006-September 30, 2007) of about $843.3 million. NIST's 2009 budget was $992 million, but it also received $610 million as part of the American Recovery and Reinvestment Act. NIST employs about 2,900 scientists, engineers, technicians, and support and administrative personnel. About 1,800 NIST associates (guest researchers and engineers from American companies and foreign nations) complement the staff. In addition, NIST partners with 1,400 manufacturing specialists and staff at nearly 350 affiliated centers around the country.

NEW QUESTION: 81
Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts. Which of the following attacks is being used by Eve?
A. Replay
B. Fire walking
C. Cross site scripting
D. Session fixation
Answer: (SHOW ANSWER)
Explanation
Explanation:
Eve is using Replay attack. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Session tokens can be used to avoid replay attacks. Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the

session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Mallory has captured this value and tries to use it on another session; Bob sends a different session token, and when Mallory replies with the captured value it will be different from Bob's computation.
Answer option C is incorrect. In the cross site scripting attack, an attacker tricks the user's computer into running code, which is treated as trustworthy because it appears to belong to the server, allowing the attacker to obtain a copy of the cookie or perform other operations.
Answer option B is incorrect. Firewalking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.
Answer option D is incorrect. In session fixation, an attacker sets a user's session id to one known to him, for example by sending the user an email with a link that contains a particular session id. The attacker now only has to wait until the user logs in.

NEW QUESTION: 82
Which of the following tools examines a system for a number of known weaknesses and alerts the administrator?
A. COPS
B. SAINT
C. Nessus
D. SATAN
Answer: A (LEAVE A REPLY)

NEW QUESTION: 83
Which of the following steps will NOT make a server fault tolerant? Each correct answer represents a complete
solution. (Choose two.)
A. Adding a second power supply unit
B. Performing regular backup of the server
C. Adding one more same sized disk as mirror on the server
D. Implementing cluster servers' facility
E. Encrypting confidential data stored on the server
Answer: B,E (LEAVE A REPLY)
Encrypting confidential data stored on the server and performing regular backup will not make the server fault
tolerant.
Fault tolerance is the ability to continue work when a hardware failure occurs on a system. A fault-tolerant

system is designed from the ground up for reliability by building multiples of all critical components, such as
CPUs, memories, disks and power supplies into the same computer. In the event one component fails, another
takes over without skipping a beat.
Answer options A, C, and D are incorrect. The following steps will make the server fault tolerant:
Adding a second power supply unit
Adding one more same sized disk as a mirror on the server implementing cluster servers facility

NEW QUESTION: 84
Which of the following is a term to describe the use of inert gases and chemical agents to extinguish a fire?
A. Fire suppression system
B. Fire sprinkler
C. Gaseous fire suppression
D. Fire alarm system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 85
Which of the following OSI layers establishes, manages, and terminates the connections between the local and remote applications?
A. Data Link layer
B. Network layer
C. Application layer
D. Session layer
Answer: (SHOW ANSWER)
The session layer of the OSI/RM controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls. Answer option C is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data

transfer. Answer option A is incorrect. The Data Link Layer is Layer 2 of the seven-layer OSI model of computer networking. It corresponds to or is part of the link layer of the TCP/IP reference model. The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC, and ADCCP for point-to-point (dual-node) connections. Answer option B is incorrect. The network layer controls the operation of subnet, deciding which physical path the data should take, based on network conditions, priority of service, and other factors. Routers work on the Network layer of the OSI stack.

NEW QUESTION: 86
Which of the following layers of TCP/IP model is used to move packets between the Internet Layer interfaces of two different hosts on the same link?
A. Application layer
B. Internet layer
C. Link layer
D. Transport Layer
E. None
Answer: C (LEAVE A REPLY)
The Link Layer of TCP/IP model is the networking scope of the local network connection to which a host is attached. This is the lowest component layer of the Internet protocols, as TCP/IP is designed to be hardware independent. As a result, TCP/IP has been implemented on top of virtually any hardware networking technology in existence. The Link Layer is used to move packets between the Internet Layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets.
Answer option B is incorrect. The Internet Layer of the TCP/IP model solves the problem of sending packets across one or more networks. Internetworking requires sending data from the source network to the destination network. This process is called routing. IP can carry data for a number of different upper layer protocols.
Answer option D is incorrect. The Transport Layer of TCP/IP model is responsible for end-to-end message transfer capabilities independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers). End to end message transmission or connecting applications at the transport layer can be categorized as either connection-oriented, implemented in Transmission Control Protocol (TCP), or connectionless, implemented in User Datagram Protocol (UDP).

Answer option is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer.

NEW QUESTION: 87
Which of the following incident handling stage removes the root cause of the incident?
A. Eradication
B. Recovery
C. Containment
D. Detection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 88
Network security is the specialist area, which consists of the provisions and policies adopted by the Network
Administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer
network and network-accessible resources. For which of the following reasons is network security needed?
Each correct answer represents a complete solution. Choose all that apply.
A. To protect information from loss and deliver it to its destination properly
B. To protect information from unwanted editing, accidentally or intentionally by unauthorized users
C. To protect private information on the Internet
D. To prevent a user from sending a message to another user with the name of a third person
Answer: A,B,C,D (LEAVE A REPLY)
Network security is needed for the following reasons:
To protect private information on the Internet
To protect information from unwanted editing, accidentally or intentionally by unauthorized users
To protect information from loss and deliver it to its destination properly
To prevent a user from sending a message to another user with the name of a third person

NEW QUESTION: 89
Which of the following statements are TRUE about Demilitarized zone (DMZ)? Each correct answer represents
a complete solution. Choose all that apply.

A. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network
like the Internet.
B. Demilitarized zone is a physical or logical sub-network that contains and exposes external services of an
organization to a larger un-trusted network.
C. The purpose of a DMZ is to add an additional layer of security to the Local Area Network of an
organization.
D. Hosts in the DMZ have full connectivity to specific hosts in the internal network.
Answer: A,B,C (LEAVE A REPLY)
A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of
an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of
security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in
the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in
the internal network, though communication with other hosts in the DMZ and to the external network is allowed.
This allows hosts in the DMZ to provide services to both the internal and external networks, while an
intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ
configuration, most computers on the LAN run behind a firewall connected to a public network such as the
Internet.

NEW QUESTION: 90
Which of the following techniques uses a modem in order to automatically scan a list of telephone numbers?
A. War driving
B. War dialing
C. Warchalking
D. Warkitting
Answer: B (LEAVE A REPLY)
War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, BBS systems, and fax machines. Hackers use the resulting lists for various purposes, hobbyists

for exploration, and crackers (hackers that specialize in computer security) for password guessing.
Answer option C is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.
Answer option A is incorrect. War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, one needs a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car.
Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.
Answer option D is incorrect. Warkitting is a combination of wardriving and rootkitting. In a warkitting attack, a hacker replaces the firmware of an attacked router. This allows them to control all traffic for the victim, and could even permit them to disable SSL by replacing HTML content as it is being downloaded. Warkitting was identified by Tsow, Jakobsson, Yang, and Wetzel in 2006. Their discovery indicated that 10% of the wireless routers were susceptible to WAPjacking (malicious configuring of the firmware settings, but making no modification on the firmware itself) and 4.4% of wireless routers were vulnerable to WAPkitting (subverting the router firmware). Their analysis showed that the volume of credential theft possible through Warkitting exceeded the estimates of credential theft due to phishing.

NEW QUESTION: 91
Adam works as a Professional Penetration Tester. A project has been assigned to him to test the vulnerabilities of the CISCO Router of Umbrella Inc. Adam finds out that HTTP Configuration Arbitrary Administrative Access Vulnerability exists in the router. By applying different password cracking tools, Adam gains access to the router. He analyzes the router config file and notices the following lines:
logging buffered errors
logging history critical
logging trap warnings
logging 10.0.1.103
By analyzing the above lines, Adam concludes that this router is logging at log level 4 to the syslog server 10.0.1.103. He decides to change the log level from 4 to 0.
Which of the following is the most likely reason of changing the log level?
A. Changing the log level from 4 to 0 will result in the logging of only emergencies. This way the modification in the router is not sent to the syslog server.
B. By changing the log level, Adam can easily perform a SQL injection attack.

C. Changing the log level grants access to the router as an Administrator.
D. Changing the log level from 4 to 0 will result in the termination of logging. This way the modification in the router is not sent to the syslog server.
Answer: A (LEAVE A REPLY)
The Router Log Level directive is used by the sys log server to specify the level of severity of the log. This directive is used to control the types of errors that are sent to the error log by constraining the severity level. Eight different levels are present in the Log Level directive, which are shown below in order of their descending significance: Number Level Description 0emergEmergencies - system is unusable 1alertAction must be taken immediately 2critCritical Conditions 3errorError conditions 4warnWarning conditions 5notice Normal but significant condition 6infoInformational 7debug Debug-level messages Note: When a certain level is specified, the messages from all other levels of higher significance will also be reported. For example, when Log Level crit is specified, then messages with log levels of alert and emerg will also be reported.

NEW QUESTION: 92
Emmanuel works as a Windows system administrator at an MNC. He uses PowerShell to enforce the script execution policy. He wants to allow the execution of the scripts that are signed by a trusted publisher. Which of the following script execution policy setting this?
A. RemoteSigned
B. AllSigned
C. Restricted
D. Unrestricted
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
Consider a scenario consisting of a tree network. The root Node N is connected to two man nodes N1 and N2.
N1 is connected to N11 and N12. N2 is connected to N21 and N22. What will happen if any one of the main nodes fail?
A. Does not cause any disturbance to the child nodes or its tranmission
B. Failure of the main node will affect all related child nodes connected to the main node

C. Failure of the main node affects all other child nodes at the same level irrespective of the main node.
D. Affects the root node only
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
Which of the following policies helps in defining what users can and should do to use network and organization's computer equipment?
A. General policy
B. Remote access policy
C. IT policy
D. User policy
Answer: (SHOW ANSWER)
A user policy helps in defining what users can and should do to use network and organization's computer equipment. It also defines what limitations are put on users for maintaining the network secure such as whether users can install programs on their workstations, types of programs users are using, and how users can access data. Answer option C is incorrect. IT policy includes general policies for the IT department. These policies are intended to keep the network secure and stable. It includes the following: Virus incident and security incident Backup policy Client update policies Server configuration, patch update, and modification policies (security) Firewall policies Dmz policy, email retention, and auto forwarded email policy Answer option A is incorrect. It defines the high level program policy and business continuity plan. Answer option B is incorrect. Remote access policy is a document that outlines and defines acceptable methods of remotely connecting to the internal network.

NEW QUESTION: 95
Which of the following is NOT an AWS Shared Responsibility Model devised by AWS?
A. Shared Responsibility Model for Abstract Services
B. Shared Responsibility Model for Storage Services
C. Shared Responsibility Model for Infrastructure Services
D. Shared Responsibility Model for Container Services
Answer: B (LEAVE A REPLY)

NEW QUESTION: 96
Which of the following OSI layers is sometimes called the syntax layer?
A. Application layer
B. Physical layer
C. Data link layer
D. Presentation layer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 97
Which of the following procedures is 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, software, or data?
A. Cyber Incident Response Plan
B. Crisis Communication Plan
C. Disaster Recovery Plan
D. Occupant Emergency Plan
Answer: (SHOW ANSWER)
The Cyber Incident Response Plan is used to address cyber attacks against an organization's IT system
through various procedures. These procedures enable security personnel to identify, mitigate, and recover
from malicious computer incidents, such as denial-of-service attacks, unauthorized accessing of a system or
data, or unauthorized changes to system hardware, software, or data.
Answer option C is incorrect. A disaster recovery plan should contain data, hardware, and software that can be
critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business
should use backup and data recovery utilities to limit the loss of data.
Answer option D is incorrect. The Occupant Emergency Plan (OEP) is used to reduce the risk to personnel,
property, and other assets while minimizing work disorders in the event of an emergency. It is the response
procedure for occupants of a facility on the occurrence of a situation, which is posing a potential threat to the
health and safety of personnel, the environment, or property. OEPs are developed at the facility level, specific
to the geographic site and structural design of the building.
Answer option B is incorrect. The crisis communication plan can be broadly defined as the plan for the
exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public
relations profession that is designed to protect and defend an individual, company, or organization facing a
public challenge to its reputation. The aim of crisis communication plan is to assist organizations to achieve

continuity of critical business processes and information flows under crisis, disaster or event driven
circumstances.

NEW QUESTION: 98
During a security awareness program, management was explaining the various reasons which create threats to network security. Which could be a possible threat to network security?
A. Configuring automatic OS updates
B. Having a web server in the internal network
C. Implementing VPN
D. Patch management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
Which of the following protocols is used for inter-domain multicast routing and natively supports "source-specific multicast" (SSM)?
A. BGMP
B. DVMRP
C. OSPF
D. EIGRP
Answer: A (LEAVE A REPLY)
BGMP stands for border gateway multicast protocol. It is used for inter-domain multicast routing and natively supports "source-specific multicast" (SSM). In order to support "any-source multicast" (ASM), BGMP builds shared trees for active multicast groups. This allows domains to build source-specific, inter-domain, distribution branches where needed. BGMP uses TCP as its transport protocol, which helps in eliminating the need to implement message fragmentation, retransmission, acknowledgement, and sequencing.
Answer option B is incorrect. The Distance Vector Multicast Routing Protocol (DVMRP) is used to share information between routers to transport IP Multicast packets among networks. It uses a reverse path-flooding technique and is used as the basis for the Internet's multicast backbone (MBONE). In particular, DVMRP is notorious for poor network scaling, resulting from reflooding, particularly with versions that do not implement pruning. DVMRP's flat unicast routing mechanism also affects its capability to scale.
Answer option D is incorrect. EIGRP is a Cisco proprietary protocol. It is an enhanced version of IGRP. It has faster convergence due to use of triggered update and saving neighbor's routing table locally. It supports VLSM and routing summarization. As EIGRP is a distance vector protocol, it automatically summarizes routes across Class A, B, and C networks. It also supports multicast and incremental updates and provides routing for three routed protocols, i.e., IP, IPX, and AppleTalk.

Answer option C is incorrect. Open Shortest Path First (OSPF) is a routing protocol that is used in large networks. Internet Engineering Task Force (IETF) designates OSPF as one of the Interior Gateway Protocols. A host uses OSPF to obtain a change in the routing table and to immediately multicast updated information to all the other hosts in the network.

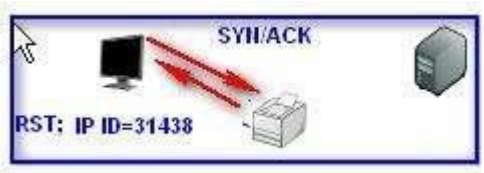
NEW QUESTION: 100
Which of the following is a network layer protocol used to obtain an IP address for a given hardware (MAC) address?
A. IP
B. PIM
C. RARP
D. ARP
Answer: (SHOW ANSWER)
Reverse Address Resolution Protocol (RARP) is a Network layer protocol used to obtain an IP address for a given hardware (MAC) address. RARP is sort of the reverse of an ARP. Common protocols that use RARP are BOOTP and DHCP.
Answer option D is incorrect. Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets.
Answer option B is incorrect. Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols, such as Border Gateway Protocol (BGP).
Answer option A is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.
IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide.

NEW QUESTION: 101

Which of the following steps are required in an idle scan of a closed port?
Each correct answer represents a part of the solution. Choose all that apply.
A. The attacker sends a SYN/ACK to the zombie.
B. The zombie's IP ID increases by only 1.
C. In response to the SYN, the target sends a RST.
D. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.
E. The zombie's IP ID increases by 2.
Answer: A,B,C,D (LEAVE A REPLY)
Following are the steps required in an idle scan of a closed port:
1.Probe the zombie's IP ID: The attacker sends a SYN/ACK to the zombie. The zombie, unaware of the SYN/ ACK, sends back a RST, thus disclosing its IP ID.

2.Forge a SYN packet from the zombie: In response to the SYN, the target sends a RST. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.

3.Probe the zombie's IP ID again: The zombie's IP ID has increased by only 1 since step 1. So the port is closed.



NEW QUESTION: 102
An employee of a medical service company clicked a malicious link in an email sent by an attacker. Suddenly, employees of the company are not able to access billing information or client record as it is encrypted. The attacker asked the company to pay money for gaining access to their dat a. Which type of malware attack is described above?
A. Trojan
B. Ransomware
C. Rootkits
D. Logic bomb

Answer: B (LEAVE A REPLY)

NEW QUESTION: 103
Which of the following provide an "always on" Internet access service when connecting to an ISP?Each correct answer represents a complete solution. Choose two.
A. Digital modem
B. Cable modem
C. Analog modem
D. DSL
Answer: (SHOW ANSWER)
DSL and Cable modems are used in remote-access WAN technology for connecting to the Internet. Both provide an "always on" Internet access service. Answer options C and A are incorrect. Analog and Digital modems are not always in 'ON' mode when connecting to an ISP. Analog modems transmit analog voice signals, while Digital modems transmit digital signals over a link.

NEW QUESTION: 104
Identify the password cracking attempt involving precomputed hash values stored as plaintext and using these to crack the password.
A. Dictionary
B. Hybrid
C. Bruteforce
D. Rainbow table
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following OSI layers establishes, manages, and terminates the connections between the local and
remote applications?
A. Data Link layer
B. Network layer
C. Application layer
D. Session layer
Answer: D (LEAVE A REPLY)
The session layer of the OSI/RM controls the dialogues (connections) between computers. It establishes,
manages and terminates the connections between the local and remote application. It provides for full-duplex,
half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart

procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of
the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used
in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application
environments that use remote procedure calls.
Answer option C is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used
by most applications for network communication. Examples of application layer protocols include the File
Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application
layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer
protocols to affect actual data transfer.
Answer option A is incorrect. The Data Link Layer is Layer 2 of the seven-layer OSI model of computer
networking. It corresponds to or is part of the link layer of the TCP/IP reference model. The Data Link Layer is
the protocol layer which transfers data between adjacent network nodes in a wide area network or between
nodes on the same local area network segment. The Data Link Layer provides the functional and procedural
means to transfer data between network entities and might provide the means to detect and possibly correct
errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area
networks (multi-node), the Point-to-Point Protocol (PPP), HDLC, and ADCCP for point-to-point (dual-node)
connections.
Answer option B is incorrect. The network layer controls the operation of subnet, deciding which physical path
the data should take, based on network conditions, priority of service, and other factors. Routers work on the
Network layer of the OSI stack.

NEW QUESTION: 106
Frank is a network technician working for a medium-sized law firm in Memphis. Frank and two other IT employees take care of all the technical needs for the firm. The firm's partners have asked that a secure wireless network be implemented in the office so employees can

move about freely without being tied to a network cable. While Frank and his colleagues are familiar with wired Ethernet technologies, 802.3, they are not familiar with how to setup wireless in a business environment. What IEEE standard should Frank and the other IT employees follow to become familiar with wireless?

A. 802.7 covers wireless standards and should be followed

B. Frank and the other IT employees should follow the 802.1 standard.

C. They should follow the 802.11 standard

D. The IEEE standard covering wireless is 802.9 and they should follow this.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 107

Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then compare those indicators with the adversary's intelligence collection capabilities identified in the previous action?

A. Analysis of Threats

B. Application of Appropriate OPSEC Measures

C. Identification of Critical Information

D. Analysis of Vulnerabilities

E. Assessment of Risk

Answer: D (LEAVE A REPLY)

OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive information and preserve essential secrecy. The OPSEC process has five steps, which are as follows: 1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary, which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive unclassified information. 2.Analysis of Threats: This step includes the research and analysis of intelligence, counterintelligence, and open source information to identify likely adversaries to a planned operation. 3.Analysis of Vulnerabilities: It includes examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. 4.Assessment of Risk:

Firstly, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Secondly, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff. 5.Application of Appropriate OPSEC Measures: The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

NEW QUESTION: 108
Each of the following is a network layer protocol used for a particular (MAC) address to obtain an IP address?
A. RARP
B. P.M
C. ARP
D. PIM
E. None
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
Which of the following biometric devices is used to take impressions of the friction ridges of the skin on the underside of the tip of the fingers?
A. Facial recognition device
B. Iris camera
C. Voice recognition voiceprint
D. Fingerprint reader
Answer: D (LEAVE A REPLY)
A fingerprint reader is used to take impressions of the friction ridges of the skin on the underside of the tip of the fingers. Fingerprints help in identifying users and are unique and different to everyone and do not change over time. Even identical twins who share their DNA do not have the same fingerprints. Police and Government agencies have used these modes in order to identify humans for many years, but other agencies are starting to use biometric fingerprint readers for identification in many different applications. A fingerprint is created when the friction ridges of the skin come in contact with a surface that is receptive to a print by means of an agent to form the print like perspiration, oil, ink, grease, and many more. The agent is then transferred to the surface and leaves an impression which creates the fingerprint.
Answer option B is incorrect. An iris camera is used to perform recognition detection of a user's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. It is used to combine computer vision, pattern recognition, statistical inference, and optics.
Answer option A is incorrect. A facial recognition device helps in viewing an image or video of a person and compares it to one that is in the database. It performs facial recognition by

comparing the following: Structure, shape, and proportions of the face Distance between the eyes, nose, mouth, and jaw Upper outlines of the eye sockets The sides of the mouth Location of the nose and eyes The area surrounding the check bones. Answer option C is incorrect. A voice recognition voiceprint is a spectrogram, which is a graph that shows a sound's frequency on the vertical axis and time on the horizontal axis. Different speech sounds help in creating different shapes on the graph. Spectrograms also use color or shades of gray to represent the acoustical qualities of sound.

NEW QUESTION: 110
The SOC manager is reviewing logs in AlienVault USM to investigate an intrusion on the network. Which CND approach is being used?
A. Preventive
B. Reactive
C. Retrospective
D. Deterrent
Answer: C (LEAVE A REPLY)

NEW QUESTION: 111
Fred is a network technician working for Johnson Services, a temporary employment agency in Boston. Johnson Services has three remote offices in New England and the headquarters in Boston where Fred works.
The company relies on a number of customized applications to perform daily tasks and unfortunately these applications require users to be local administrators. Because of this, Fred's supervisor wants to implement tighter security measures in other areas to compensate for the inherent risks in making those users local admins. Fred's boss wants a solution that will be placed on all computers throughout the company and monitored by Fred. This solution will gather information on all network traffic to and from the local computers without actually affecting the traffic. What type of solution does Fred's boss want to implement?
A. Fred's boss wants a NIDS implementation.
B. Fred's boss wants to implement a HIPS solution.
C. Fred's boss wants to implement a HIDS solution.
D. Fred's boss wants Fred to monitor a NIPS system.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 112
Which of the following tools examines a system for a number of known weaknesses and alerts the
administrator?
A. COPS
B. Nessus

C. SATAN
D. SAINT
Answer: A (LEAVE A REPLY)

NEW QUESTION: 113
Adam, a malicious hacker, has just succeeded in stealing a secure cookie via a XSS attack. He is able to
replay the cookie even while the session is valid on the server. Which of the following is the most likely reason
of this cause?
A. No encryption is applied.
B. Two way encryption is applied.
C. Encryption is performed at the network layer (layer 1 encryption).
D. Encryption is performed at the application layer (single encryption key).
Answer: (SHOW ANSWER)
Single key encryption uses a single word or phrase as the key. The same key is used by the sender to encrypt
and the receiver to decrypt. Sender and receiver initially need to have a secure way of passing the key from
one to the other. With TLS or SSL this would not be possible. Symmetric encryption is a type of encryption that
uses a single key to encrypt and decrypt data. Symmetric encryption algorithms are faster than public key
encryption. Therefore, it is commonly used when a message sender needs to encrypt a large amount of data.
Data Encryption Standard (DES) uses the symmetric encryption key algorithm to encrypt data.

NEW QUESTION: 114
Larry is a network administrator working for a manufacturing company in Detroit. Larry is responsible for the entire company's network which consists of 300 workstations and 25 servers. After using a hosted email service for a year, the company wants to cut back on costs and bring the email control internal. Larry likes this idea because it will give him more control over email. Larry wants to purchase a server for email but he does not want the server to be on the internal network because this might cause security risks. He decides to place the email server on the outside of the company's internal firewall. There is another firewall connected directly to the Internet that will protect some traffic from accessing the email server; the server will essentially be place between the two firewalls. What logical area is Larry going to place the new email server into?
A. For security reasons, Larry is going to place the email server in the company's Logical Buffer Zone (LBZ).

B. He is going to place the server in a Demilitarized Zone (DMZ).
C. He will put the email server in an IPSec zone.
D. Larry is going to put the email server in a hot-server zone.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 115
Which of the following is designed to detect unwanted changes by observing the flame of the environment
associated with combustion?
A. Gaseous fire-extinguishing systems
B. None
C. Smoke alarm system
D. Fire extinguishing system
E. sprinkler
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?
A. Contingency Plan
B. Disaster Recovery Plan
C. Business Continuity Plan
D. Continuity Of Operations Plan
Answer: A (LEAVE A REPLY)
Contingency plan is prepared and documented for emergency response, backup operations, and recovery maintained by an activity as the element of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer option B is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.

Answer option D is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable. Answer option C is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.

NEW QUESTION: 117
Which of the following fields in the IPv6 header is decremented by 1 for each router that forwards the packet?
A. Flow label
B. Next header
C. Traffic class
D. Hop limit
Answer: D (LEAVE A REPLY)
The hop limit field in the IPv6 header is decremented by 1 for each router that forwards a packet.
The packet is discarded when the hop limit field reaches zero.
Answer option B is incorrect. Next header is an 8-bit field that specifies the next encapsulated
protocol.
Answer option A is incorrect. Flow label is a 20-bit field that is used for specifying special router
handling from source to destination for a sequence of packets.
Answer option C is incorrect. Traffic class is an 8-bit field that specifies the Internet traffic priority
delivery value.

NEW QUESTION: 118
Which of the following is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients? Each correct answer represents a complete solution. Choose all that apply.
A. Email spoofing
B. Junk mail
C. E-mail spam
D. Email jamming
Answer: B,C (LEAVE A REPLY)

E-mail spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. Answer option A is incorrect. Email spoofing is a fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Email spoofing is a technique commonly used in spam and phishing emails to hide the origin of the email message. By changing certain properties of the email, such as the From, Return-Path and Reply-To fields (which can be found in the message header), ill-intentioned users can make the email appear to be from someone other than the actual sender. The result is that, although the email appears to come from the address indicated in the From field (found in the email headers), it actually comes from another source. Answer option D is incorrect. Email jamming is the use of sensitive words in e-mails to jam the authorities that listen in on them by providing a form of a red herring and an intentional annoyance. In this attack, an attacker deliberately includes "sensitive" words and phrases in otherwise innocuous emails to ensure that these are picked up by the monitoring systems. As a result the senders of these emails will eventually be added to a "harmless" list and their emails will be no longer intercepted, hence it will allow them to regain some privacy.

NEW QUESTION: 119
Which of the following is a high-speed network that connects computers, printers, and other network devices together?
A. MAN
B. WAN
C. LAN
D. CAN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 120
Which of the following commands is used for port scanning?
A. nc -d
B. nc -v
C. nc -t
D. nc -z
Answer: D (LEAVE A REPLY)

NEW QUESTION: 121
Sophie has been working as a Windows network administrator at an MNC over the past 7 years. She wants to check whether SMB1 is enabled or disabled. Which of the following command allows Sophie to do so?
A. Get-WindowsOptionalFeatures -Online -FeatureName SMB1Protocol

B. Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
C. Get-WindowsOptionalFeatures -Online -FeatureNames SMB1Protocol
D. Get-WindowsOptionalFeature -Online -FeatureNames SMB1Protocol
Answer: B (LEAVE A REPLY)

Valid 312-38 Dumps shared by PrepPdf.com for Helping Passing 312-38 Exam! PrepPdf.com now offer the **newest 312-38 exam dumps**, the PrepPdf.com 312-38 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 312-38 dumps with Test Engine here: https://www.preppdf.com/EC-COUNCIL/312-38-prepaway-exam-dumps.html (**732** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)