Cisco.100-160.v2026-03-09.q128

Exam Code:	100-160
Exam Name:	Cisco Certified Support Technician (CCST) Cybersecurity
Certification Provider:	Cisco
Free Question Number:	128
Version:	v2026-03-09
# of views:	138
# of Questions views:	1280
https://www.freeqas.com/qa/Cisco/100-160/Cisco.100-160.v2026-03-09.q128.html	

NEW QUESTION: 1
Which of the following is a limitation of vulnerability databases?
A. They may not include vulnerabilities discovered by malicious actors.
B. They require minimal human effort for maintaining and updating.
C. They provide real-time information on emerging threats.
D. They cover all known vulnerabilities in every software and hardware.
Answer: A (LEAVE A REPLY)
Vulnerability databases are an essential resource for cybersecurity professionals to stay informed about known vulnerabilities. However, these databases primarily rely on information shared by vendors, security researchers, and ethical hackers. Malicious actors, who may discover vulnerabilities independently, may not disclose them in such databases. Therefore, it is crucial to adopt a well-rounded approach to vulnerability management and consider potential undisclosed vulnerabilities.

NEW QUESTION: 2
What is one of the main objectives of documenting cybersecurity incidents?
A. To create a historical record of incidents for legal purposes
B. To assign blame to individuals responsible for the incident
C. To minimize the impact of cyber attacks
D. To divert attention from the incident
Answer: C (LEAVE A REPLY)
Documenting cybersecurity incidents helps organizations understand the nature, extent, and impact of the incident. By documenting incidents, organizations can analyze trends, develop strategies to prevent future incidents, and minimize the impact of cyber attacks.

NEW QUESTION: 3
What is the purpose of a firewall in a network security system?

A. To prevent unauthorized access to or from private networks
B. To scan and filter network traffic for potential threats
C. To encrypt data transmitted over the network
D. To provide secure remote access to the network
Answer: A (LEAVE A REPLY)
Option 1: Correct. A firewall is designed to prevent unauthorized access to or from private networks by monitoring and controlling network traffic based on predetermined security rules.
Option 2: Incorrect. While a firewall can scan and filter network traffic for potential threats, this is not its primary purpose.
Option 3: Incorrect. While encryption may be a feature of some firewalls, it is not the primary purpose of a firewall in a network security system.
Option 4: Incorrect. While a secure remote access solution may include a firewall, this is not the primary purpose of a firewall in a network security system.

NEW QUESTION: 4
What is a common outcome of the policy development phase in cybersecurity planning?
A. Implementation of technical controls
B. Creation of incident response plans
C. Identification of security vulnerabilities
D. Development of security awareness training programs
Answer: D (LEAVE A REPLY)
The policy development phase in cybersecurity planning involves creating and documenting the policies and procedures that guide the organization's cybersecurity practices. It often includes the development of security awareness training programs to educate employees about their roles and responsibilities in maintaining cybersecurity and to promote good security practices throughout the organization.

NEW QUESTION: 5
What does the term "ad hoc" mean in the context of cybersecurity?
A. A security assessment conducted by external auditors.
B. A security incident response plan that is predefined and well-documented.
C. A method of threat detection through continuous monitoring and analysis.
D. A temporary or improvised solution in response to a specific situation or problem.
Answer: D (LEAVE A REPLY)
In cybersecurity, "ad hoc" refers to a temporary or improvised solution that is implemented to address a specific cybersecurity situation or problem. It is often done in situations where there is no predefined process or security control in place. Ad hoc solutions may not be scalable or sustainable in the long run, but they can be useful in urgent or unexpected situations to mitigate threats or vulnerabilities temporarily.

NEW QUESTION: 6

Which of the following features of the Cisco Identity Services Engine (ISE) allows network administrators to define policies for controlling access to network resources based on user identities and user or group attributes?

A. Network Access Profiles

B. Identity Firewall

C. Profiling

D. TrustSec

Answer: C (LEAVE A REPLY)

Option 1: Network Access Profiles: Network Access Profiles in Cisco ISE define the behavior of network devices when they are accessed by authenticated users. They are a set of policies that determine how network resources are allocated to users or user groups, and what level of access they have.

Option 2: Identity Firewall: Cisco ISE's Identity Firewall feature enables network administrators to apply firewall policies based on user identities. It allows for granular control over network access and can enforce allow, deny, or redirect actions based on user attributes.

Option 3: Profiling: This is the correct answer. Cisco ISE's Profiling feature is used to dynamically classify endpoints connecting to the network based on their characteristics, such as their MAC addresses, IP addresses, and DHCP options. This information is then used to enforce access policies.

Option 4: TrustSe TrustSec is a Cisco security solution that provides secure access control across the network infrastructure. While TrustSec is related to identity and access management, it is not a feature of Cisco ISE specifically.

NEW QUESTION: 7

What is an insider threat?

A. A threat posed by an individual with authorized access to an organization's systems and data.

B. A vulnerability in an organization's network infrastructure.

C. The accidental disclosure of sensitive information.

D. A security breach caused by an external attacker.

Answer: (SHOW ANSWER)

Insider threats refer to risks and vulnerabilities that arise from individuals who have authorized access to an organization's systems, networks, or data. These individuals may intentionally or unintentionally cause harm, such as stealing confidential information, sabotaging systems, or disclosing sensitive data to unauthorized entities.

NEW QUESTION: 8

Which technology allows on-demand access to shared pools of configurable computing resources over a network?

A. Virtualization

B. Cloud

C. Proxy

D. DMZ

Answer: B (LEAVE A REPLY)

Cloud computing refers to the delivery of on-demand computing resources, including servers, storage, databases, networking, software, and analytics, over the internet. It provides organizations with the ability to access and use shared pools of configurable computing resources quickly and easily, without the need for extensive upfront infrastructure investments. Cloud computing offers scalability, cost-efficiency, and flexibility, making it an essential component of modern IT environments.

NEW QUESTION: 9

Which command-line tool is commonly used to test network connectivity and measure response time?

A. netstat

B. nslookup

C. tcpdump

D. ping

Answer: D (LEAVE A REPLY)

The correct command-line tool for testing network connectivity and measuring response time is ping. It sends ICMP echo request packets to a specified network device or IP address and waits for the corresponding echo reply, helping to verify if a host is reachable and measure packet latency. However, it is important to note that although ping can provide some basic network testing, it does not capture traffic or packet contents like tcpdump.

NEW QUESTION: 10

What are botnets?

A. An attack that manipulates individuals into revealing sensitive information or performing certain actions.

B. A network of compromised computers controlled by a central entity to carry out malicious activities.

C. A form of cyber attack that attempts to gain unauthorized access to a network.

D. A software program that is designed to damage, disrupt, or gain unauthorized access to a computer system.

Answer: B (LEAVE A REPLY)

Botnets are networks of compromised computers that are controlled by a central entity, often referred to as a botmaster. These compromised computers, also known as bots or zombies, are typically infected with malware and can be used to carry out various malicious activities, such as launching DDoS attacks, sending spam emails, or stealing sensitive information.

NEW QUESTION: 11

Which protocol is used for communication between web browsers and web servers?

A. ICMP

B. TCP
C. UDP
D. HTTP
Answer: (SHOW ANSWER)
HTTP (Hypertext Transfer Protocol) is the protocol used for communication between web browsers (client) and web servers. It allows for the exchange of hypertext, which includes text, images, and other resources, over the Internet. HTTP operates on top of TCP, ensuring reliable delivery of data.

NEW QUESTION: 12
What is a denial of service (DoS) attack?
A. A technique used by attackers to obtain sensitive information through deception.
B. A software program that is designed to damage, disrupt, or gain unauthorized access to a computer system.
C. A form of cyber attack that attempts to gain unauthorized access to a network.
D. An attack that overwhelms a target system with a flood of traffic or requests, rendering it inaccessible to legitimate users.
Answer: D (LEAVE A REPLY)
A denial of service (DoS) attack is a type of cyber attack that aims to make a target system or network unavailable to its intended users by overwhelming it with a flood of traffic or requests. This effectively denies legitimate users access to the system.

NEW QUESTION: 13
Which of the following is an example of a data security principle?
A. Least Privilege
B. Session Management
C. ARP Spoofing
D. Ciphertext
Answer: A (LEAVE A REPLY)
Option 1: Correct. Least Privilege is a data security principle that limits the access rights of individuals to only what is necessary for them to perform their job functions.
Option 2: Incorrect. Session Management is a security practice related to handling user sessions, but it is not specifically a data security principle.
Option 3: Incorrect. ARP Spoofing is a network attack technique, not a data security principle.
Option 4: Incorrect. Ciphertext refers to encrypted data, but it is not a data security principle.

NEW QUESTION: 14
Which component of network security architecture is designed to separate the internal network from the external network?
A. Cloud
B. DMZ

C. Proxy
D. Virtualization
Answer: B (LEAVE A REPLY)
A DMZ, or demilitarized zone, is a network segment that is used to separate the internal network from the external network. It acts as a buffer zone between the organization's network and the internet, providing an additional layer of security. By placing servers, such as web servers or email servers, in the DMZ, organizations can ensure that external traffic is filtered and scrutinized before reaching the internal network.

NEW QUESTION: 15
What does hardening mean in the context of cybersecurity?
A. Removing all vulnerabilities from a system or network
B. Implementing cybersecurity policies and regulations
C. Creating a backup of critical data and configurations
D. Making a system more resistant to threats and attacks
Answer: (SHOW ANSWER)
Hardening refers to the process of securing a system by reducing its vulnerability to potential threats and attacks. It involves implementing security best practices, such as disabling unnecessary services, applying patches and updates, configuring access controls, strengthening passwords, and employing additional security measures like firewalls or intrusion detection systems. Hardening helps ensure systems are less susceptible to exploitation.

NEW QUESTION: 16
Which of the following log file entries is typically associated with a Distributed Denial of Service (DDoS) attack?
A. "High CPU utilization on server at 15:20:05."
B. "Web server responding slowly to client requests at 14:10:15."
C. "Spike in network traffic volume at 12:45:10."
D. "Unusual number of concurrent sessions established at 09:30:00."
Answer: C (LEAVE A REPLY)
In a Distributed Denial of Service (DDoS) attack, the attacker overwhelms the target system or network with a massive volume of traffic from multiple sources. This excessive traffic causes the targeted system to become inaccessible to legitimate users. Therefore, a sudden and significant spike in network traffic volume is a typical indicator of a DDoS attack. Additionally, other log entries may also be present, such as increased resource utilization or slow response times, as mentioned in the other options, but the spike in network traffic volume is the most indicative of a DDoS attack.

NEW QUESTION: 17
Which aspect of the Diamond Model represents the "Infrastructure" used by threat actors?
A. Adversary
B. Victim
C. Capability
D. Campaign
Answer: (SHOW ANSWER)
The Diamond Model is a tool used for analyzing cyber threat intelligence. It consists of four components: Adversary, Victim, Infrastructure, and Capability. The Infrastructure aspect refers to the resources and infrastructure utilized by the threat actors, including networks, servers, and tools.

NEW QUESTION: 18
Which approach to risk management involves accepting the potential risk and not taking any specific action to mitigate it?
A. Risk acceptance.
B. Risk mitigation.
C. Risk transfer.
D. Risk avoidance.
Answer: (SHOW ANSWER)
Risk acceptance is an approach to risk management wherein the potential risk is acknowledged, and a conscious decision is made not to take any specific action to mitigate it. This approach is usually taken when the potential risk is deemed acceptable or when the cost of mitigating the risk outweighs the potential impact.

NEW QUESTION: 19
Which of the following updates is responsible for updating the software embedded within hardware devices?
A. Application updates
B. Firmware updates
C. Windows Update
D. Device drivers
Answer: B (LEAVE A REPLY)

Firmware updates are specific to hardware devices and involve updating the software that is embedded within those devices. Firmware updates can improve the device's functionality, address security vulnerabilities, and fix bugs. It is crucial to regularly check for and apply firmware updates to ensure devices are operating optimally and securely.

NEW QUESTION: 20
What is one benefit of regularly updating documentation in the context of cybersecurity?
A. Decreasing accountability and traceability of incidents
B. Increasing the risk of unauthorized access to the documentation
C. Creating confusion among users accessing the documentation
D. Increasing the likelihood of compliance with industry regulations
Answer: D (LEAVE A REPLY)
Regularly updating documentation helps organizations stay current with industry regulations and best practices. By aligning documentation with compliance requirements, organizations can ensure they are meeting the necessary standards and reduce the risk of potential penalties or legal issues.

NEW QUESTION: 21
You work for a hospital that stores electronic protected health information (ePHI) in an online portal. Authorized employees can use their mobile devices to access patient ePHI.
You need to ensure that employees' mobile devices comply with HIPAA regulations.
Which safeguard should you develop and implement?
A. An ownership policy for employees' mobile devices
B. A contingency plan
C. A policy that requires multi-factor authentication to use the mobile device
D. A policy to govern how ePHI is removed from mobile devices
Answer: D (LEAVE A REPLY)
The CCST Cybersecurity Study Guide notes that HIPAA (Health Insurance Portability and Accountability Act) requires that ePHI be protected both in storage and when devices are decommissioned or repurposed. This includes implementing data removal policies for mobile devices.
"HIPAA requires procedures for the removal of electronic protected health information (ePHI) from devices before disposal, reuse, or reassignment." (CCST Cybersecurity, Essential Security Principles, Regulatory Compliance section, Cisco Networking Academy)

NEW QUESTION: 22
What is the main difference between a public and a private network?
A. Public networks are secured, while private networks are not
B. Private networks are more expensive to set up than public networks
C. Public networks use public IP addresses, while private networks use private IP addresses
D. Private networks are accessible to the general public, while public networks are not

Answer: (SHOW ANSWER)
The main difference between a public network and a private network lies in the IP addressing scheme. Public networks use public IP addresses, provided by ISPs, to route traffic over the internet. Private networks, on the other hand, use private IP addresses, typically reserved IP ranges (e.g., 192.168.x.x or 10.x.x.x), for local communication within a network.

NEW QUESTION: 23
What is the primary purpose of malware remediation?
A. To remove or neutralize malware infections
B. To prevent malware infections
C. To create a backup of infected systems
D. To detect malware threats
Answer: A (LEAVE A REPLY)
Malware remediation aims to remove or neutralize malware infections from compromised systems. It involves various techniques, such as scanning and cleaning the infected files, removing malicious software, and repairing damages caused by the malware. The goal is to restore the system's integrity, security, and functionality by eliminating the presence and impact of malware.

NEW QUESTION: 24
Which of the following options is an example of a cybersecurity news and subscription service?
A. VPN (Virtual Private Network)
B. Email filtering software
C. SIEM (Security Information and Event Management) system
D. Firewall
Answer: C (LEAVE A REPLY)
A SIEM system is an example of a cybersecurity news and subscription service. It collects and analyzes security event data from various sources and provides real-time alerts and reports to enhance threat detection and management. It provides valuable insights into the cybersecurity landscape, including news and updates related to security incidents, vulnerabilities, and emerging threats.

NEW QUESTION: 25
Which of the following is an example of a passive vulnerability identification technique?
A. Penetration testing
B. Intrusion detection system (IDS)
C. Vulnerability scanning
D. Incident response
Answer: C (LEAVE A REPLY)

Vulnerability scanning is a passive technique used to identify vulnerabilities in a system or network. It involves the use of automated tools that scan the system for known vulnerabilities without actively exploiting them.

NEW QUESTION: 26
Which of the following is a data protection technique that involves the transformation of data into a format that is unreadable to unauthorized users?
A. Authentication
B. Encryption
C. Firewall
D. Intrusion Detection System
Answer: B (LEAVE A REPLY)
Option 1: Incorrect. Authentication refers to the process of verifying the identity of a user or system.
Option 2: Correct. Encryption is a data protection technique that transforms data into a format that is unreadable to unauthorized users. It provides confidentiality and ensures that even if the data is intercepted, it cannot be easily understood.
Option 3: Incorrect. A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on predetermined security rules.
Option 4: Incorrect. An Intrusion Detection System (IDS) is a security tool that monitors network traffic for suspicious activity or violations of security policies.

NEW QUESTION: 27
What should you create to prevent spoofing of the internal network?
A. A NAT rule
B. An ACL
C. A record in the host file
D. A DNS record
Answer: B (LEAVE A REPLY)
The CCST Cybersecurity Study Guide states that Access Control Lists (ACLs) can be used to filter traffic based on IP addresses and block packets that appear to originate from the internal network but arrive from external interfaces (IP spoofing).
"ACLs can prevent spoofing by dropping traffic from external sources that claim to have an internal source address. Configuring ACLs on the perimeter firewall or router is a common countermeasure for IP spoofing." (CCST Cybersecurity, Basic Network Security Concepts, ACLs and Traffic Filtering section, Cisco Networking Academy) A (NAT rule) changes IP addresses but does not inherently prevent spoofing.
B (ACL) is correct because it can enforce anti-spoofing filters.
C (host file) only affects name resolution locally.
D (DNS record) is for domain mapping, not spoofing prevention.

NEW QUESTION: 28
What type of security technique involves setting up a decoy system or network to lure and trap potential attackers?
A. Honeypot
B. Virtualization
C. DMZ
D. Proxy
Answer: A (LEAVE A REPLY)
A honeypot is a security technique that involves setting up a decoy system or network to attract potential attackers. The purpose of a honeypot is to gather information about attackers' tactics, techniques, and intentions, allowing organizations to learn more about the threats they face and improve their defenses.
By monitoring the activities within a honeypot, organizations can gain valuable insights into emerging attack methods and enhance their overall cybersecurity strategy.

NEW QUESTION: 29
Which of the following best describes asset management in the context of cybersecurity?
A. Identifying and protecting valuable resources
B. Monitoring user activity
C. Tracking software licenses
D. Managing network infrastructure
Answer: A (LEAVE A REPLY)
Asset management in a cybersecurity context involves identifying and protecting valuable resources within an organization. This includes identifying critical systems, data, and information that need to be protected from unauthorized access, modification, or destruction.

NEW QUESTION: 30
Which of the following updates improve the functionality and security of installed software?
A. Device drivers
B. Firmware updates
C. Application updates
D. Windows Update
Answer: C (LEAVE A REPLY)
Application updates refer to updates released by software vendors to improve the functionality, fix bugs, and address security vulnerabilities in their applications. Regularly updating applications is crucial to ensure that the latest security patches and enhancements are applied, reducing the risk of exploitation by attackers.

NEW QUESTION: 31
Which regulation is aimed at protecting the privacy and security of personally identifiable information (PII) within the European Union?

A. HIPAA
B. PCI DSS
C. GDPR
D. BYOD
Answer: C (LEAVE A REPLY)
The General Data Protection Regulation (GDPR) is a regulation that aims to protect the privacy and security of personally identifiable information (PII) of individuals within the European Union (EU). It provides guidelines and requirements for data processing, consent, transparency, and breach notification, among other aspects.

NEW QUESTION: 32
Which security feature provides network segmentation by creating virtual networks?
A. VLANs
B. VLANs
C. Intrusion Prevention System (IPS)
D. Virtual Private Network (VPN)
Answer: (SHOW ANSWER)
Option 1: Correct, VLANs (Virtual Local Area Networks) provide network segmentation by creating virtual networks, allowing different groups of devices to be logically separated on the same physical network.
Option 2: Incorrect, Firewalls are designed to monitor and filter network traffic based on predetermined security rules, but they do not provide network segmentation by creating virtual networks.
Option 3: Incorrect, An Intrusion Prevention System (IPS) is a security appliance or software that monitors network traffic for suspicious activity and takes action to prevent potential threats, but it does not provide network segmentation by creating virtual networks.
Option 4: Incorrect, A Virtual Private Network (VPN) is a secure tunnel between two or more devices, typically used to connect remote sites or allow remote users to access the private network. It does not provide network segmentation by creating virtual networks.

NEW QUESTION: 33
What is the main purpose of a disaster recovery plan?

A. Recovering data after a disaster
B. Preventing disasters from occurring
C. Minimizing the impact of disasters
D. Identifying potential threats and vulnerabilities
Answer: A (LEAVE A REPLY)
The primary purpose of a disaster recovery plan is to ensure that data, systems, and operations can be restored in a timely manner following a disaster. It focuses on recovering critical resources and minimizing downtime to resume normal business operations as quickly as possible.

NEW QUESTION: 34
During an incident response, the security team needs to isolate a compromised server from the rest of the network but still allow forensic analysis. Which action should they take?
A. Power off the server immediately.
B. Disconnect the server from the network and connect it to an isolated forensic network.
C. Delete suspicious files from the server.
D. Reset all user passwords on the server.
Answer: B (LEAVE A REPLY)
The CCST Cybersecurity course notes that isolation is a key part of the containment phase of incident response. The goal is to prevent the compromised system from communicating with the attacker or spreading malware, while preserving it for analysis.
"Containment often involves removing an affected system from the production network and connecting it to a controlled forensic environment to preserve evidence and prevent further compromise." (CCST Cybersecurity, Incident Handling, Containment Procedures section, Cisco Networking Academy)

NEW QUESTION: 35
What is the purpose of Security Information and Event Management (SIEM) systems?
A. To analyze network traffic and detect potential security threats.
B. To centrally collect, store, and analyze logs from various systems to detect and respond to security incidents.
C. To encrypt sensitive data to protect it from unauthorized access.
D. To authenticate and authorize users to access network resources.
Answer: B (LEAVE A REPLY)
Option 1: This option is incorrect. While SIEM systems may perform analysis of network traffic, their primary purpose is not network traffic analysis, but rather log collection and analysis for security incident detection and response.
Option 2: This option is correct. SIEM systems are designed to centrally collect, store, and analyze logs from various systems to detect and respond to security incidents. They provide real-time monitoring, correlation, and analysis of security events, allowing organizations to identify potential threats and take appropriate actions.

Option 3: This option is incorrect. Encryption of sensitive data is not the purpose of SIEM systems. While encryption is an important security measure, SIEM systems focus on log management and analysis rather than encryption.
Option 4: This option is incorrect. User authentication and authorization are not within the scope of SIEM systems. SIEM systems focus on log collection and analysis for security incident detection and response, rather than user access control.

NEW QUESTION: 36
What is the purpose of Tactics in the context of cybersecurity?
A. To track the impact of a cyberattack on the integrity of data
B. To identify specific cyber threat actors
C. To categorize the methods and strategies employed by cyber threat actors
D. To determine the motive behind a cyberattack
Answer: (SHOW ANSWER)
Tactics in cybersecurity refer to the methods and strategies used by cyber threat actors to achieve their objectives. Understanding and categorizing these tactics help organizations assess their vulnerability to specific attacks and develop appropriate defense measures.

NEW QUESTION: 37
What is the main purpose of two-factor authentication (2FA)?
A. To provide multiple backup copies of critical data.
B. To ensure the confidentiality of data transmitted over a network.
C. To identify and classify potential security threats.
D. To prevent unauthorized access by requiring two different types of credentials.
Answer: D (LEAVE A REPLY)
Two-factor authentication (2FA) is a security measure that adds an extra layer of protection to the authentication process. It requires users to provide two different types of credentials, usually something they know (e.g., a password) and something they possess (e.g., a unique code generated by a mobile app), making it more difficult for unauthorized individuals to gain access to systems or accounts.

NEW QUESTION: 38
What logging mechanism is commonly used to track and record security-related events and activities in an organization?
A. System and application logs
B. Event Viewer
C. Syslog
D. Audit logs
Answer: D (LEAVE A REPLY)
Audit logs are specifically designed to track and record security-related events and activities in an organization. They capture information about user actions, system changes, and resource access

attempts, providing a detailed record for forensic analysis, compliance auditing, and security investigation purposes.

NEW QUESTION: 39
What is the role of a firewall in secure access technologies?
A. To authenticate users
B. To encrypt data
C. To prevent unauthorized access
D. To monitor network traffic
Answer: (SHOW ANSWER)
A firewall is a network security device that is used to filter incoming and outgoing network traffic based on predetermined security rules. Its primary role is to prevent unauthorized access to a network or system by blocking potentially harmful or malicious traffic.

NEW QUESTION: 40
What is a common security threat in which an attacker attempts to overwhelm a targeted system by flooding it with Internet traffic?
A. Ransomware
B. Distributed Denial of Service (DDoS) attack
C. Phishing
D. SQL injection
Answer: B (LEAVE A REPLY)
Option 1: Ransomware is a type of malicious software that encrypts a victim's files and demands a ransom in exchange for the decryption key. While it can cause damage to systems, it is not specifically designed to overwhelm a system with Internet traffic.
Option 2: Correct. A Distributed Denial of Service (DDoS) attack is a common security threat in which an attacker attempts to overwhelm a targeted system by flooding it with Internet traffic. This can result in a loss of service availability for legitimate users.
Option 3: Phishing is a type of social engineering attack in which an attacker masquerades as a trustworthy entity to trick individuals into providing sensitive information. It does not involve overwhelming a system with Internet traffic.
Option 4: SQL injection is a type of web application attack in which an attacker manipulates a SQL query to gain unauthorized access to a database. It does not involve overwhelming a system with Internet traffic.

NEW QUESTION: 41
What is an attack vector in cybersecurity?
A. The method used by an attacker to gain unauthorized access
B. A vulnerability in a system that can be exploited
C. The path or means through which an attacker can exploit vulnerabilities
D. The likelihood of a cyber attack taking place

Answer: C (LEAVE A REPLY)
An attack vector refers to the pathway or means by which an attacker can carry out a successful exploit or gain unauthorized access to a system. It can be a network protocol, software vulnerability, social engineering technique, malicious email attachment, or any other method that allows an attacker to exploit vulnerabilities. Understanding attack vectors is crucial for implementing effective defenses and mitigating risks.

NEW QUESTION: 42
How do threat actors launch ransomware attacks on organizations?
A. They implant malware to collect data from the corporation's financial system.
B. They deface an organization's public-facing website.
C. They lock data and deny access to the data until they receive money.
D. They secretly spy on employees and collect employees' personal information.
Answer: C (LEAVE A REPLY)
The CCST Cybersecurity course describes ransomware as a form of malicious software that encrypts or locks access to an organization's data, demanding payment for its release. "Ransomware is a type of malware that denies access to data by encrypting it and demands payment from the victim to restore access. Threat actors may deliver ransomware through phishing emails, malicious downloads, or exploiting vulnerabilities in exposed systems." (CCST Cybersecurity, Essential Security Principles, Malware Types and Threats section, Cisco Networking Academy) A describes spyware or information-stealing malware.
B is website defacement, which is vandalism, not ransomware.
C is correct: locking/encrypting data and demanding payment is the defining behavior of ransomware.
D is more aligned with insider threat or espionage activities.

NEW QUESTION: 43
What is a social engineering attack?
A. An attack that targets physical infrastructure
B. An attack that attempts to overload a network with excessive traffic
C. An attack that intercepts wireless network packets
D. An attack that manipulates people to obtain sensitive information
Answer: (SHOW ANSWER)
A social engineering attack is a type of attack that manipulates people to obtain sensitive information or perform actions that could compromise security. This could include techniques such as impersonating trustworthy entities, phishing, baiting, or tailgating. Social engineering attacks exploit human psychology and trust to deceive individuals into revealing confidential details or granting unauthorized access. It is important to be aware of such tactics and exercise caution when dealing with requests for sensitive information.

NEW QUESTION: 44

Which of the following is a characteristic of a denial-of-service (DoS) attack?
A. An attacker attempts to gain unauthorized access to a system.
B. An attacker steals or alters sensitive data.
C. An attacker floods a system with excessive requests, rendering it unable to function properly.
D. An attacker intercepts and modifies network traffic.
Answer: C (LEAVE A REPLY)
A denial-of-service (DoS) attack is a type of cyber attack where an attacker floods a system with an excessive amount of requests, overwhelming its resources and causing it to crash or become unresponsive.

NEW QUESTION: 45
Which of the following features help to secure a wireless SoHo network from unauthorized access?
A. Default admin credentials
B. SSID broadcast
C. MAC filtering
D. Weak encryption
Answer: C (LEAVE A REPLY)

NEW QUESTION: 46
Which of the following best defines "Techniques, Tactics, and Procedures (TTP)" in the context of cybersecurity investigations?
A. A framework for analyzing network traffic.
B. A pattern of behavior adopted by threat actors.
C. A set of guidelines for securing network devices.
D. An organized digital evidence collection process.
Answer: (SHOW ANSWER)
Techniques, Tactics, and Procedures (TTP) refer to the methods and strategies used by threat actors in cyber-attacks. TTPs encompass various aspects such as the tools and techniques employed, the patterns of behavior exhibited, and the procedures followed by attackers during their malicious activities. By understanding TTPs, cybersecurity professionals can better identify and defend against threats.

NEW QUESTION: 47
What is the main motivation for attackers to conduct cyber attacks?
A. Knowledge
B. Financial gain
C. Curiosity
D. Revenge
Answer: (SHOW ANSWER)
The primary motivation for many cyber attackers is financial gain. By conducting cyber attacks, attackers may aim to steal sensitive information, such as credit card details or personal data, which they can then use or sell for financial profit.

NEW QUESTION: 48
Which protocol is used for broadcasting and resolving MAC addresses to IP addresses?
A. ICMP
B. TCP
C. ARP
D. UDP
Answer: C (LEAVE A REPLY)
ARP (Address Resolution Protocol) is used for broadcasting and resolving MAC (Media Access Control) addresses to IP addresses within a local network. It helps devices determine the MAC address associated with a given IP address, enabling proper communication on the network. ARP operates at the data link layer of the OSI model.

NEW QUESTION: 49
Which of the following best defines a vulnerability assessment in the context of cybersecurity?
A. A process that determines the level of risk associated with a cybersecurity incident.
B. A process that identifies potential cybersecurity threats in an organization.
C. A process that mitigates the impact of cybersecurity incidents on an organization.
D. A process that identifies potential security flaws or weaknesses in a system.
Answer: D (LEAVE A REPLY)
A vulnerability assessment is a systematic process that identifies potential security flaws or weaknesses in a system, network, or application. It focuses on identifying vulnerabilities that could be exploited by attackers. It involves scanning and testing for known vulnerabilities and vulnerabilities resulting from misconfigurations or poor security practices. The assessment provides valuable information for organizations to prioritize their efforts in remediating identified vulnerabilities and improving their overall security posture.

NEW QUESTION: 50
Which macOS security feature encrypts the entire macOS volume?
A. FileVault
B. Gatekeeper
C. System Integrity Protection (SIP)
D. XProtect
Answer: A (LEAVE A REPLY)
The CCST Cybersecurity Study Guide highlights FileVault as the macOS full-disk encryption tool. "FileVault is macOS's built-in full-disk encryption feature. It encrypts the contents of the entire startup disk to help prevent unauthorized access to the information stored on the drive, even if the device is lost or stolen." (CCST Cybersecurity, Endpoint Security Concepts, Disk Encryption section, Cisco Networking Academy) A is correct: FileVault provides complete volume encryption.
B (Gatekeeper) controls app installation by verifying code signatures.
C (System Integrity Protection) protects system files from modification.
D (XProtect) is macOS's built-in malware detection system.

NEW QUESTION: 51
Your home network seems to have slowed down considerably. You look at the home router GUI and notice that an unknown host is attached to the network.
What should you do to prevent this specific host from attaching to the network again?
A. Create an IP access control list.
B. Implement MAC address filtering.
C. Block the host IP address.
D. Change the network SSID.
Answer: B (LEAVE A REPLY)
The CCST Cybersecurity course explains that MAC address filtering is a network access control method that allows only approved device hardware addresses to connect. While not foolproof against spoofing, it can block a specific device from reconnecting to a small home network. "MAC address filtering restricts network access to devices whose unique hardware addresses are explicitly allowed. This can be used to block known unauthorized devices from reconnecting." (CCST Cybersecurity, Basic Network Security Concepts, Wireless Security Controls section, Cisco Networking Academy) A is incorrect: IP ACLs are better for controlling traffic types, not blocking specific devices at the router level.
B is correct: It prevents the device's hardware address from reconnecting.
C is temporary since the host can get a new IP via DHCP.
D may hide the network but will not stop a determined attacker who can still detect it.

NEW QUESTION: 52
Which of the following strategies is recommended for managing communication proactively after an event?
A. Regularly backing up data

B. Conducting a forensic analysis
C. Implementing multi-factor authentication
D. Keeping antivirus software up to date
Answer: B (LEAVE A REPLY)
Conducting a forensic analysis is a recommended strategy for managing communication proactively after an event. When a security incident occurs, it is essential to investigate the nature of the incident, determine its impact, and identify the root cause. Conducting a forensic analysis helps uncover valuable information such as the method of attack, affected systems, and potential weaknesses that can be addressed to prevent similar incidents in the future. This proactive approach facilitates the development of a more robust security posture.

NEW QUESTION: 53
What regulation is specifically designed to ensure the security of payment card data processed by organizations?
A. GDPR
B. BYOD
C. PCI DSS
D. HIPAA
Answer: C (LEAVE A REPLY)
The Payment Card Industry Data Security Standard (PCI DSS) is a regulation that focuses on ensuring the security of payment card data processed by organizations. It provides a set of security requirements that organizations handling payment card data must follow to protect against fraud and data breaches.

NEW QUESTION: 54
Which of the following is an example of a source of evidence (artifact) in a cybersecurity investigation?
A. Firewall logs recording network traffic.
B. Configuration files of network devices.
C. Security policy documents.
D. Training materials for security awareness.
Answer: A (LEAVE A REPLY)
In a cybersecurity investigation, evidence or artifacts play a crucial role in determining the nature of an incident. Firewall logs recording network traffic can provide valuable information regarding communication between systems, including IP addresses, ports, protocols, and timestamps. Analyzing these logs can help identify potential threats or suspicious activities within a network.

NEW QUESTION: 55
What is the purpose of conducting assessments of IT systems in the context of information security and change management?
A. All of the above

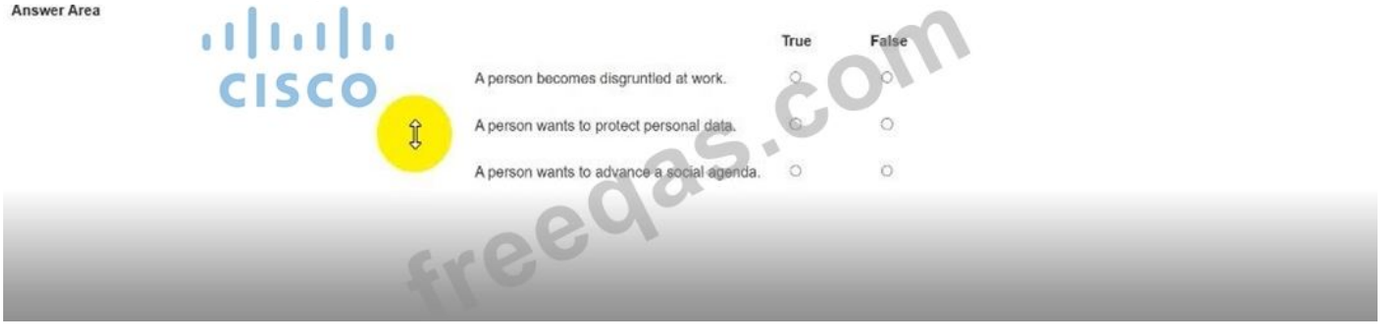
B. To assess the potential impact of changes on overall system performance
C. To identify any vulnerabilities or weaknesses in the system
D. To determine the level of compliance with regulatory requirements
Answer: (SHOW ANSWER)
Assessments of IT systems in the context of information security and change management serve multiple purposes. Firstly, they help identify any vulnerabilities or weaknesses in the system, enabling organizations to take necessary measures to strengthen security and protect against potential threats. Secondly, these assessments assist in determining the level of compliance with regulatory requirements, ensuring that the system meets necessary standards. Lastly, they help assess the potential impact of changes on overall system performance, allowing organizations to make informed decisions and minimize any disruptions. Therefore, all the options mentioned in the

NEW QUESTION: 56
What is smishing?
A. A form of social engineering attack that uses SMS or text messages to trick victims into revealing sensitive information.
B. A physical attack where an unauthorized person gains entry to a restricted area by following closely behind an authorized person.
C. A type of phishing attack that targets specific individuals or organizations.
D. A cyber attack where an attacker manipulates and deceives an individual to reveal sensitive information.
Answer: (SHOW ANSWER)
Smishing, short for SMS phishing, is a social engineering attack that utilizes SMS or text messages to deceive individuals into disclosing sensitive information or performing certain actions. These messages often mimic legitimate sources, such as banks or service providers, and typically contain links or phone numbers that, when accessed or called, lead to malicious activities. Smishing takes advantage of the ubiquity of mobile devices and users' tendency to trust text messages.

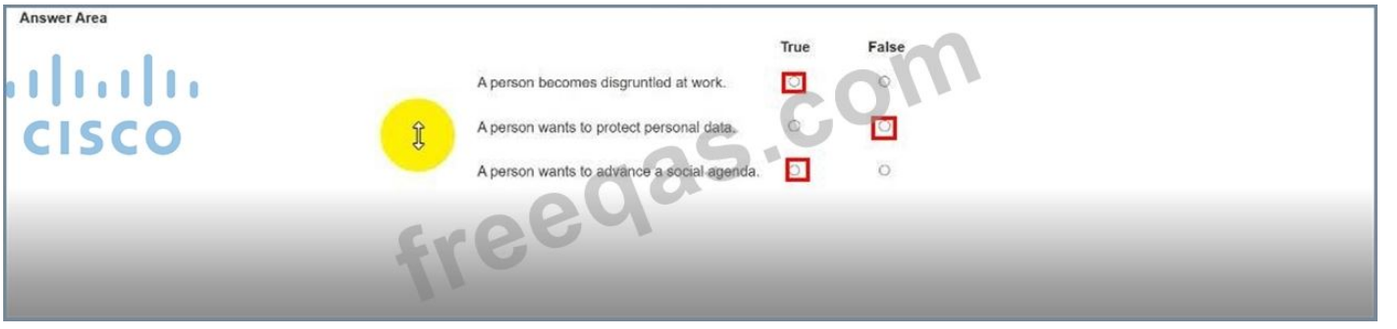
NEW QUESTION: 57
You are going to perform a penetration test on a company LAN. As part of your preparation, you access the company's websites, view webpage source code, and run internet searches to uncover domain information. You also use social media to gather details about the company and its employees.
Which type of reconnaissance activities are you performing?
A. Passive
B. Active
C. Offline
D. Invasive
Answer: A (LEAVE A REPLY)

The CCST Cybersecurity Study Guide explains that reconnaissance is the process of collecting information about a target before attempting exploitation.
"Passive reconnaissance is conducted without directly engaging with the target systems. Examples include reviewing public websites, examining HTML source code, querying public DNS records, and using social media to gather information. Since no packets are sent directly to the target system, it reduces the risk of detection." (CCST Cybersecurity, Vulnerability Assessment and Risk Management, Reconnaissance Techniques section, Cisco Networking Academy)
Passive (A) is correct because all actions described - viewing public pages, searching online, and checking social media - involve no direct interaction that could alert the target.
Active (B) would involve direct probing, like port scans or vulnerability scans.
Offline (C) is not an official reconnaissance classification in this context.
Invasive (D) is a general term and not used as a standard reconnaissance category in CCST material.

NEW QUESTION: 58
For each statement, select True if it is a common motivation to commit cyber attacks or False if it is not.
Note: You will receive partial credit for each correct selection.



Answer:



NEW QUESTION: 59
What does NAT stand for in networking?
A. Network Address Transmission
B. Network Access Technology
C. Network Address Translation
D. Network Address Terminal
Answer: C (LEAVE A REPLY)

NAT stands for Network Address Translation. It is a process used in networking to translate private IP addresses into public IP addresses, enabling devices with private addresses to communicate with devices on public networks like the internet.

NEW QUESTION: 60
Which endpoint security mechanism is used to secure data transmitted between the endpoint and the network?
A. Firewall
B. Antivirus
C. Encryption
D. Intrusion Detection System (IDS)
Answer: (SHOW ANSWER)
Encryption is the mechanism used to secure data transmitted between the endpoint and the network. By encrypting the data, it becomes unreadable to unauthorized parties, ensuring the confidentiality and integrity of the information being transmitted. Encryption transforms the data into a ciphertext, which can only be decrypted back into its original form using the proper encryption key. This helps protect sensitive and confidential data from interception and unauthorized access during transmission over the network.

NEW QUESTION: 61
Which of the following features help to secure a wireless SoHo network from unauthorized access?
A. Default admin credentials
B. Weak encryption
C. MAC filtering
D. SSID broadcast
Answer: (SHOW ANSWER)
MAC filtering is a feature that allows a network administrator to specify which devices can connect to the wireless network based on their MAC (Media Access Control) addresses. By enabling MAC filtering, only devices with authorized MAC addresses will be allowed to connect, thereby enhancing network security. SSID (Service Set Identifier) broadcast refers to the network name being broadcasted, and hiding it doesn't provide significant security improvement. Default admin credentials should always be changed to prevent unauthorized access, making option C a weak answer choice. Weak encryption, such as WEP or TKIP, provides little security and should be avoided.

NEW QUESTION: 62
What are anomalies in the context of cybersecurity?
A. Security vulnerabilities in computer networks
B. External threats that aim to breach an organization's defenses
C. Unusual behaviors or patterns that deviate from the norm
D. Malware that infects a system and causes it to malfunction
Answer: (SHOW ANSWER)
Anomalies in the context of cybersecurity refer to unusual behaviors or patterns that deviate from the norm. These anomalies can indicate potential security breaches, malicious activities, or abnormal system behaviors. By detecting and analyzing anomalies, cybersecurity professionals can identify potential threats and take appropriate actions to mitigate them. Anomaly detection is an important aspect of cybersecurity to ensure the overall safety and protection of computer systems and networks.

NEW QUESTION: 63
Which of the following is an element of an incident response plan?
A. Installing antivirus software
B. Conducting regular backups
C. Developing security policies
D. Identifying vulnerabilities
Answer: C (LEAVE A REPLY)
An incident response plan outlines the steps and procedures to be followed when a cybersecurity incident occurs. One of the elements of an incident response plan is developing security policies. These policies serve as a framework for managing and responding to security incidents.

NEW QUESTION: 64
What is a digital certificate used for in the context of cybersecurity?
A. Encrypting data
B. Verifying the identity of an entity
C. Creating a secure tunnel
D. Decrypting data
Answer: B (LEAVE A REPLY)
A digital certificate is an electronic document used to prove the authenticity and identity of an entity, such as a person, organization, or device, in an online environment. It is issued and digitally signed by a trusted third party known as a certification authority (CA). Digital certificates

are commonly used in cybersecurity for purposes such as authentication, ensuring secure communication, and establishing trust between entities.

NEW QUESTION: 65
Which technology actively inspects incoming and outgoing network traffic and takes immediate action to prevent security threats?
A. Firewall
B. IPS
C. Server
D. IDS
Answer: B (LEAVE A REPLY)
An Intrusion Prevention System (IPS) is a technology that actively inspects network traffic, both incoming and outgoing, and takes immediate action to prevent security threats. It not only identifies potential threats but also actively blocks or mitigates them in real-time.

NEW QUESTION: 66
Which protocol is responsible for resolving IP addresses to domain names?
A. DNS
B. HTTP
C. UDP
D. TCP
Answer: (SHOW ANSWER)
DNS (Domain Name System) is responsible for resolving IP (Internet Protocol) addresses to domain names. It translates human-readable domain names, such as www.example.com, into IP addresses, which are numerical identifiers used to locate and identify devices on a network.

NEW QUESTION: 67
Why is it important to maintain the chain of custody when handling digital evidence?
A. To accelerate the analysis of the evidence.
B. To prevent unauthorized access or tampering.
C. To ensure the evidence is stored securely.
D. To recover lost or deleted data from the evidence.
Answer: B (LEAVE A REPLY)
Maintaining the chain of custody is crucial to ensure the integrity and admissibility of digital evidence in a legal case. It helps establish that the evidence has not been tampered with or accessed by unauthorized individuals, which ensures its reliability and credibility. By maintaining a strict chain of custody, any potential challenges to the evidence's validity can be effectively addressed by demonstrating that it has been handled in a controlled and secure manner.

NEW QUESTION: 68
Which of the following is true regarding the incident response process?

A. It is a reactive process that is only initiated after an incident has occurred.
B. It is a proactive process that focuses on preventing incidents from occurring.
C. It is an iterative process that involves continuous improvement based on lessons learned.
D. It is a one-time process that is only performed when an organization first establishes its security program.
Answer: C (LEAVE A REPLY)
Option 1: Incorrect. The incident response process can be both proactive and reactive. While it does involve reacting to incidents that have already occurred, it also includes proactive measures to prevent incidents from happening again in the future.
Option 2: Incorrect. While incident response can involve proactive measures to prevent incidents, it is not solely focused on prevention. It also includes reacting to incidents that have already occurred.
Option 3: Correct. The incident response process is an iterative process that involves continuous improvement based on lessons learned. Organizations should regularly review and update their incident response plans to ensure they are effective and up to date.
Option 4: Incorrect. The incident response process is not a one-time process. It should be an ongoing and continuous process to address security incidents as they occur and to improve the incident response capabilities of the organization.

NEW QUESTION: 69
Which of the following options is not an example of a subscription service in cybersecurity?
A. Anti-malware software
B. Intrusion detection system (IDS) signatures updates
C. Threat intelligence feeds
D. Vulnerability scanning tools
Answer: A (LEAVE A REPLY)
Anti-malware software is not typically considered a subscription service in cybersecurity. It is a security tool that detects, prevents, and removes malware from systems, but it is usually purchased as a one-time product rather than a subscription. On the other hand, threat intelligence feeds, vulnerability scanning tools, and IDS signatures updates are examples of subscription services that provide regular updates and information to enhance security against evolving threats.

NEW QUESTION: 70
The company web server collects information through a form. The form is accessed by using port 80. The form content is transferred to an encrypted database for storage. You are investigating a complaint that the form content has been compromised.
What is the cause of the security breach?
A. The database was compromised.
B. The data was transferred to the database using a nonsecure protocol.
C. The website was accessed using HTTP, which is an unencrypted protocol.

D. The web browser used to access the site was not updated to the latest version.
Answer: C (LEAVE A REPLY)
The CCST Cybersecurity Study Guide explains that HTTP (port 80) transmits data in cleartext, making it susceptible to interception. Even if data is stored securely in an encrypted database, sensitive information can be compromised during transmission if HTTPS (port 443) is not used. "When HTTP is used instead of HTTPS, all form inputs and transmitted data are sent in plaintext over the network, where they can be intercepted by attackers." (CCST Cybersecurity, Basic Network Security Concepts, Secure Protocols section, Cisco Networking Academy)

NEW QUESTION: 71
What term refers to the process of creating a virtual version of a device or resource, such as a server or a network?
A. Virtualization
B. DMZ
C. Cloud
D. Proxy
Answer: A (LEAVE A REPLY)
Virtualization is the process of creating a virtual version of a device or resource, such as a server or a network, by abstracting the underlying physical infrastructure. It allows multiple virtual instances to be created and run on a single physical server, enabling organizations to maximize resource utilization, increase flexibility, and simplify management. Virtualization is widely used in data centers to optimize efficiency and reduce costs. -

NEW QUESTION: 72
Which compliance framework is specifically related to protecting the personal data and privacy of European Union (EU) citizens?
A. HIPAA
B. GDPR
C. PCI-DSS
D. FERPA
Answer: (SHOW ANSWER)
The General Data Protection Regulation (GDPR) is a compliance framework implemented by the European Union to protect the personal data and privacy of EU citizens. It focuses on the collection, processing, and storage of personal data, and it applies to any organization that handles EU citizens' data, regardless of its location.

NEW QUESTION: 73
Which of the following services or protocols can be used to ensure the security and compliance of an organization's network?
A. NTP (Network Time Protocol)
B. SNMP (Simple Network Management Protocol)

C. DHCP (Dynamic Host Configuration Protocol)
D. DNS (Domain Name System)
Answer: (SHOW ANSWER)
Option 1: NTP is a protocol used to synchronize the clocks of computers in a network. While it is important for maintaining accurate time, it does not directly contribute to network security and compliance. This makes it an incorrect answer.
Option 2: SNMP is a protocol used for managing and monitoring network devices. It allows for centralized monitoring, troubleshooting, and configuration of devices. SNMP can play a crucial role in security and compliance by providing real-time information about network devices and their behaviors. This makes it a correct answer.
Option 3: DHCP is a protocol used to assign IP addresses and network configuration parameters to devices on a network. While DHCP is essential for network connectivity, it does not directly contribute to security and compliance. This makes it an incorrect answer.
Option 4: DNS is a protocol used to translate domain names into IP addresses. While DNS is critical for internet connectivity, it does not directly contribute to security and compliance. This makes it an incorrect answer.

NEW QUESTION: 74
What is a key principle of securing data in the cloud?
A. Implementing strong physical security measures
B. Encrypting data at rest and in transit
C. Using complex passwords for all cloud users
D. Limiting access to the cloud from specific IP addresses
Answer: B (LEAVE A REPLY)
Option 1: Incorrect. Implementing strong physical security measures is important, but it is not the key principle of securing data in the cloud.
Option 2: Correct. Encrypting data at rest and in transit is a key principle of securing data in the cloud. This ensures that even if the data is compromised, it cannot be accessed without the decryption key.
Option 3: Incorrect. Using complex passwords is a good security practice, but it is not the key principle of securing data in the cloud.
Option 4: Incorrect. Limiting access to the cloud from specific IP addresses is a security measure, but it is not the key principle of securing data in the cloud.

NEW QUESTION: 75
Which of the following is an example of a detective control?
A. Security information and event management (SIEM) system
B. Access control list (ACL)
C. Patch management
D. Encryption
Answer: A (LEAVE A REPLY)

A SIEM system is a detective control that collects and analyzes security event logs from various sources to identify and detect potential security incidents. It provides real-time monitoring and alerts for suspicious activities, enabling organizations to identify and respond to security events effectively.

NEW QUESTION: 76
What type of encryption is used to secure data that is stored on a hard drive or other storage media?
A. File-based encryption
B. Hash encryption
C. Symmetric encryption
D. Public Key Infrastructure (PKI)
Answer: (SHOW ANSWER)
Symmetric encryption is a type of encryption where the same key is used for both the encryption and decryption processes. It is commonly employed to secure data at rest, such as on a hard drive or other storage media. With symmetric encryption, the key must be kept secret to ensure the confidentiality of the encrypted data.

NEW QUESTION: 77
You are collecting data after a suspected intrusion on the local LAN.
You need to capture incoming IP packets to a file for an investigator to analyze.
Which two tools should you use? (Choose 2.)
A. Wireshark
B. tcpdump
C. Nmap
D. netstat
Answer: A,B (LEAVE A REPLY)
The CCST Cybersecurity Study Guide specifies that both Wireshark and tcpdump are packet capture tools that can record network traffic to a file for later analysis.
"Wireshark provides a graphical interface for packet capture and analysis. Tcpdump is a command-line tool that captures packets for detailed offline review." (CCST Cybersecurity,

Incident Handling, Network Traffic Analysis section, Cisco Networking Academy) A is correct: Wireshark is widely used for packet capture and analysis.
B is correct: tcpdump is a CLI-based packet capture tool.
C (Nmap) is for network scanning, not packet capture.
D (netstat) displays network connections and ports but does not capture packets.

NEW QUESTION: 78
Which logging mechanism is used in Linux and Unix-based systems to store system and application logs?
A. System and application logs
B. Syslog
C. Event Viewer
D. Audit logs
Answer: (SHOW ANSWER)
Syslog is a standard logging protocol that is commonly used in Linux and Unix-based systems to store and forward system and application logs. It allows administrators to collect logs from multiple devices and applications and store them in a centralized location for analysis, troubleshooting, and compliance purposes.

NEW QUESTION: 79
Which of the following elements are part of cybersecurity incident response?
A. Prevention, Monitoring, Compliance, Remediation
B. Assessment, Authorization, Authentication, Accounting
C. Identification, Recovery, Mitigation, Restoration
D. Detection, Analysis, Containment, Eradication
Answer: D (LEAVE A REPLY)
Cybersecurity incident response involves several key elements, including detection, analysis, containment, and eradication. Detection refers to the identification and recognition of a potential cybersecurity incident. Analysis involves examining the incident to understand its nature, impact, and cause. Containment entails taking immediate action to minimize further damage and prevent the incident from spreading. Eradication involves completely removing the threat or vulnerability from the system or network in order to eliminate the possibility of a recurring incident. These elements are crucial for an effective incident response strategy.

NEW QUESTION: 80
Which of the following is a preventive control that can help in reducing the risk of future incidents?
A. Creating secure backups of critical data
B. Implementing strong access controls and authentication mechanisms
C. Regularly updating antivirus signatures
D. Conducting periodic employee training on incident response
Answer: (SHOW ANSWER)

Implementing strong access controls and authentication mechanisms is a preventive control that can help reduce the risk of future incidents. By ensuring that only authorized individuals have access to systems and data, the likelihood of unauthorized access or malicious activity is minimized. While regularly updating antivirus signatures, conducting employee training, and creating secure backups are also important preventive measures, the focus here is on access controls and authentication mechanisms.

NEW QUESTION: 81
What is the primary goal of a threat actor in a cyber attack?
A. To exploit vulnerabilities in a system
B. To gain unauthorized access to a network
C. To cause damage or disruption to a target
D. To identify and mitigate security risks
Answer: (SHOW ANSWER)
The primary goal of a threat actor in a cyber attack is typically to cause damage, disruption, or gain some form of unauthorized advantage. They may aim to steal sensitive data, encrypt files for ransom, disrupt services, or compromise the integrity of a system. Understanding the motivations of threat actors helps in building effective defense strategies.

NEW QUESTION: 82
Which two basic metrics should be taken into consideration when assigning a severity to a vulnerability during an assessment? (Choose 2.)
A. The likelihood that an adversary can and will exploit the vulnerability
B. The impacts that an exploit of the vulnerability will have on the organization
C. The time involved in choosing replacement software to replace older systems
D. The age of the hardware running the software that contains the vulnerability
Answer: A,B (LEAVE A REPLY)
The CCST Cybersecurity course describes that risk scoring for vulnerabilities often involves likelihood and impact - similar to the CVSS (Common Vulnerability Scoring System) model. "When prioritizing vulnerabilities, assess both the likelihood of exploitation and the potential impact to the organization. Likelihood measures how easy or probable it is for an adversary to exploit the weakness, while impact measures the consequences to confidentiality, integrity, and availability if exploitation occurs." (CCST Cybersecurity, Vulnerability Assessment and Risk Management, Risk Assessment and Prioritization section, Cisco Networking Academy) A is correct: Likelihood is a fundamental part of severity assessment.
B is correct: Impact determines how damaging an exploit would be.
C is incorrect: Time to choose replacement software is an operational consideration, not a severity metric.
D is incorrect: Hardware age may influence performance but does not directly define vulnerability severity.

NEW QUESTION: 83
Which encryption method uses a single key to both encrypt and decrypt data?
A. SSL/TLS
B. Symmetric encryption
C. Hashing
D. Asymmetric encryption
Answer: B (LEAVE A REPLY)
Symmetric encryption uses a single key to both encrypt and decrypt data. This means that the same key is used by both the sender and the receiver to secure the communication. It is faster and less computationally intensive than asymmetric encryption.

NEW QUESTION: 84
Which of the following tools is commonly used to detect intrusions on a network?
A. Microsoft Office Suite
B. Snort
C. Apache Tomcat
D. Wireshark
Answer: B (LEAVE A REPLY)
Snort is a widely used tool for network intrusion detection and prevention. It is an open-source network security solution that employs a combination of signature-based and anomaly-based detection techniques. Snort can analyze network traffic in real-time, identify suspicious patterns or behavior, and raise alerts in case of potential intrusions or security breaches.

NEW QUESTION: 85
Which of the following network technologies is commonly used to connect devices within a local area network (LAN)?
A. Wi-Fi
B. Ethernet
C. DSL
D. VPN
Answer: (SHOW ANSWER)
Ethernet is a widely used network technology for connecting devices within a local area network (LAN). It provides a physical and data link layer protocol for wired connections, allowing devices to communicate over a LAN using Ethernet cables. Ethernet has various speeds and standards, including Ethernet over twisted pair (such as Cat 5e or Cat 6 cables), fiber optic cables, and other mediums.

NEW QUESTION: 86
What is a common vulnerability in cloud-based systems?
A. Inadequate access controls
B. Outdated antivirus software

C. Weak passwords
D. Lack of network segmentation
Answer: (SHOW ANSWER)
Option 1: Correct: Inadequate access controls can leave cloud-based systems vulnerable to unauthorized access and data breaches.
Option 2: Incorrect: Outdated antivirus software is a concern for individual devices but not specific to cloud-based systems.
Option 3: Incorrect: Weak passwords can be a vulnerability but not a common one in cloud-based systems, which usually have password policies in place.
Option 4: Incorrect: Lack of network segmentation can be a vulnerability, but it is not as common as inadequate access controls.

NEW QUESTION: 87
Which of the following is a principle of data security?
A. Encryption
B. Firewall
C. Intrusion Detection System
D. Data Masking
Answer: A (LEAVE A REPLY)
Option 1: Correct. Encryption is a principle of data security that involves converting data into a form that is unreadable by unauthorized users. This helps protect the confidentiality of data.
Option 2: Incorrect. A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on predetermined security rules. While it plays a role in data security, it is not a principle of data security.
Option 3: Incorrect. An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports. While it plays a role in data security, it is not a principle of data security.
Option 4: Incorrect. Data masking is a technique that replaces sensitive data with fictitious data to protect the privacy of data. While it plays a role in data security, it is not a principle of data security.

NEW QUESTION: 88
Which of the following is a common authentication protocol used in wireless networks?
A. FTP
B. WPA
C. SSH
D. SMTP
Answer: B (LEAVE A REPLY)
WPA (Wi-Fi Protected Access) is a widely used authentication protocol for securing wireless networks. It provides stronger security than the older WEP (Wired Equivalent Privacy) protocol by utilizing encryption algorithms and dynamic key generation. WPA offers better protection against

unauthorized access and helps ensure the confidentiality and integrity of wireless communications.

NEW QUESTION: 89
Which of the following updates is responsible for ensuring proper communication between hardware devices and the operating system?
A. Device drivers
B. Windows Update
C. Application updates
D. Firmware updates
Answer: (SHOW ANSWER)
Device drivers are software programs that facilitate communication between hardware devices (such as printers, graphics cards, or network adapters) and the operating system. Updating device drivers is important as it can enhance compatibility, performance, and resolve known issues or security vulnerabilities.

NEW QUESTION: 90
Which protocol uses encryption for secure remote access to network resources?
A. Point-to-Point Protocol (PPP)
B. Wireless Equivalent Privacy (WEP)
C. Internet Protocol Security (IPSec)
D. Secure Shell (SSH)
Answer: (SHOW ANSWER)
Secure Shell (SSH) is a cryptographic network protocol that provides secure remote access and control of network resources. It employs encryption to protect data exchanged between the client and the server, ensuring the confidentiality and integrity of the communication. SSH is commonly used for remote administration and secure file transfers.

NEW QUESTION: 91
What is the main purpose of port scanning in cybersecurity?
A. To gather information about potential targets on the internet
B. To exploit vulnerabilities in the target system
C. To identify open ports and services running on a target system
D. To detect intrusions and prevent unauthorized access
Answer: C (LEAVE A REPLY)
Port scanning is a technique used to identify open ports and services running on a target system. By scanning the ports, a cybersecurity professional can gather valuable information about the target, such as the services and protocols in use, which can help in identifying potential vulnerabilities and securing the system.

NEW QUESTION: 92
Which of the following is a network security device that operates at the session layer of the OSI model?
A. Firewall
B. Intrusion Detection System (IDS)
C. Intrusion Prevention System (IPS)
D. SSL/TLS
Answer: B (LEAVE A REPLY)
Option 1: Incorrect. A firewall operates at the network layer (layer of the OSI model, not the session layer (layer 5).
Option 2: Correct. An Intrusion Prevention System (IPS) operates at the session layer (layer 5) of the OSI model. It monitors network traffic in real-time and can block or prevent malicious activities.
Option 3: Incorrect. An Intrusion Detection System (IDS) operates at the network layer (layer of the OSI model, not the session layer (layer 5).
Option 4: Incorrect. SSL/TLS is a cryptographic protocol that operates at the transport layer (layer of the OSI model, not the session layer (layer 5).

NEW QUESTION: 93
Which of the following is a hardware or software-based network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on predefined security rules?
A. NAC
B. Firewall
C. VPN
D. ACL
Answer: B (LEAVE A REPLY)
A firewall is a hardware or software-based network security device that acts as a barrier between internal and external networks. It monitors network traffic and applies predefined rules to determine whether to allow or block specific traffic. Firewalls are commonly used to protect network infrastructure and prevent unauthorized access by filtering out potentially harmful or suspicious traffic.

NEW QUESTION: 94
Which encryption type is commonly used to secure WiFi networks?
A. Data Encryption Standard (DES)
B. Triple Data Encryption Algorithm (Triple DES)
C. Advanced Encryption Algorithm (AES)
D. RSA (Rivest-Shamir-Adleman)
Answer: (SHOW ANSWER)
The CCST Cybersecurity Study Guide specifies that AES (Advanced Encryption Standard) is the encryption method used in modern WiFi security protocols like WPA2 and WPA3.
"WPA2 and WPA3 use the Advanced Encryption Standard (AES) for securing wireless traffic. AES provides strong symmetric encryption, replacing outdated methods like WEP and TKIP." (CCST Cybersecurity, Basic Network Security Concepts, Wireless Security section, Cisco Networking Academy) A (DES) is outdated and insecure.
B (Triple DES) is older and slower, rarely used in WiFi.
C is correct: AES is the industry standard for WiFi security.
D (RSA) is asymmetric encryption used in key exchange, not bulk WiFi encryption.

NEW QUESTION: 95
Which of the following is an integral part of the CIA triad in cybersecurity?
A. Data loss prevention (DLP)
B. Two-factor authentication (2FA)
C. Intrusion Detection System (IDS)
D. Firewall
Answer: B (LEAVE A REPLY)
The CIA triad in cybersecurity stands for confidentiality, integrity, and availability. Two-factor authentication (2FA) ensures confidentiality by adding an extra layer of security, requiring users to provide two forms of authentication before gaining access. It helps protect against unauthorized access and adds an additional level of assurance for ensuring data confidentiality.

NEW QUESTION: 96
What is an Advanced Persistent Threat (APT)?
A. A vulnerability in network communication protocols.
B. A cyberattack that compromises multiple devices simultaneously.
C. A sophisticated and targeted attack that aims to gain unauthorized access and maintain persistence over a long period.
D. A type of malware that spreads rapidly through a network.
Answer: (SHOW ANSWER)
Advanced Persistent Threats (APTs) are stealthy and prolonged attacks targeted at specific organizations or entities. APTs typically employ sophisticated techniques, including social engineering and zero-day exploits. The primary objectives of APTs are to gain unauthorized

access, maintain persistence within the target network or system, and conduct reconnaissance or exfiltrate sensitive data without being detected for an extended period of time.

NEW QUESTION: 97
Which of the following best describes the role of automated threat intelligence in a cybersecurity system?
A. All of the above
B. It provides advanced analytics for proactive threat mitigation
C. It enables real-time monitoring of threat landscapes
D. It automates the detection and response to security incidents
Answer: (SHOW ANSWER)
Automated threat intelligence plays a multifaceted role in a cybersecurity system. Firstly, it enables real-time monitoring of threat landscapes by continuously collecting and analyzing data from various sources. This allows organizations to stay updated on emerging threats and trends. Secondly, it automates the detection and response to security incidents by leveraging machine learning algorithms and predefined rules. Finally, automated threat intelligence provides advanced analytics for proactive threat mitigation, helping organizations anticipate and prevent potential security breaches.

NEW QUESTION: 98
What is the primary purpose of a cybersecurity risk assessment?
A. To identify vulnerabilities in information systems
B. To determine the likelihood of a cybersecurity incident occurring
C. To prioritize security controls and mitigation strategies
D. To quantify the potential impact of a cybersecurity incident
Answer: C (LEAVE A REPLY)
A cybersecurity risk assessment is conducted to identify and assess potential risks to the organization's information systems. This assessment helps in prioritizing security controls and mitigation strategies based on the likelihood and potential impact of each risk. It enables organizations to allocate resources effectively and address the most critical risks first.

NEW QUESTION: 99
You need to transfer configuration files to a router across an unsecured network.
Which protocol should you use to encrypt the files in transit?
A. Telnet
B. HTTP
C. TFTP
D. SSH
Answer: D (LEAVE A REPLY)

The CCST Cybersecurity Study Guide highlights that SSH (Secure Shell) provides encrypted communication for secure remote access and file transfer (using SCP or SFTP) over unsecured networks. This ensures confidentiality and integrity of the files in transit.
"SSH encrypts all data exchanged between client and server, protecting credentials and file contents from interception. It is the preferred protocol for secure device management and file transfers across untrusted networks." (CCST Cybersecurity, Basic Network Security Concepts, Secure Remote Management section, Cisco Networking Academy) A (Telnet) transmits data in plaintext.
B (HTTP) is unencrypted web traffic.
C (TFTP) is a simple, insecure file transfer protocol without encryption.
D is correct: SSH secures configuration file transfers across insecure networks.

NEW QUESTION: 100
Which of the following best describes the concept of data integrity in cybersecurity?
A. Ensuring data is available for authorized users when needed
B. Encrypting data to prevent unauthorized modifications
C. Protecting data from unauthorized access or disclosure
D. Ensuring data is accurate, consistent, and trustworthy
Answer: D (LEAVE A REPLY)
Data integrity in cybersecurity refers to the assurance that data is accurate, consistent, and trustworthy throughout its lifecycle. It involves maintaining the correctness and reliability of data, preventing unauthorized modifications or tampering. Ensuring data integrity is crucial for maintaining the reliability and credibility of information within a system or network.

NEW QUESTION: 101
Which of the following best describes a vulnerability in the context of cybersecurity?
A. A tool used to test the security of a network or system.
B. A security feature implemented to protect a network or system.
C. A method used to attack a network or system.
D. A weakness in a network or system that can be exploited by attackers.
Answer: D (LEAVE A REPLY)
A vulnerability refers to a weakness in a network or system that can be exploited by attackers. It can be a flaw or an oversight in the design, implementation, or configuration of a system, which may allow unauthorized access, data leakage, or other malicious activities.

NEW QUESTION: 102
Which of the following is a feature of cloud computing?
A. On-premises hosting
B. Hardware provisioning
C. Data encryption
D. Physical server maintenance

Answer: (SHOW ANSWER)

Option 1: Incorrect. On-premises hosting refers to hosting applications and data on local servers within an organization's physical infrastructure. It is not a feature of cloud computing.

Option 2: Incorrect. Hardware provisioning is the process of setting up and configuring the physical infrastructure required to run applications and store data. While this is an important aspect of cloud computing, it is not a specific feature of cloud computing.

Option 3: Correct. Data encryption is a feature of cloud computing that ensures the security and confidentiality of data stored and transmitted within the cloud. It protects sensitive information from unauthorized access.

Option 4: Incorrect. Physical server maintenance involves activities such as hardware repairs, upgrades, and maintenance tasks associated with physical servers. While these tasks are necessary for managing an on-premises infrastructure, they are not specific features of cloud computing.

NEW QUESTION: 103

Which of the following best describes network security?

A. Ensuring high availability and performance of the network

B. Securing physical access to network devices

C. Protecting data from unauthorized access or modifications

D. Preventing network configuration errors

Answer: (SHOW ANSWER)

Network security is the practice of protecting data in a network from unauthorized access, modifications, or attacks. It involves implementing various security measures such as access control, encryption, firewalls, and intrusion prevention systems.

NEW QUESTION: 104

A threat actor sets up a rogue access point (AP) at a local cafe. The rogue AP captures traffic and then forwards the traffic to the cafe AP.

Which type of attack does this scenario describe?

A. Man-in-the-middle

B. Reconnaissance

C. Ransomware

D. DDoS

Answer: (SHOW ANSWER)

The CCST Cybersecurity Study Guide describes a man-in-the-middle (MITM) attack as an attack where the adversary secretly intercepts and possibly alters communications between two parties, making them believe they are communicating directly. A rogue AP configured to pass traffic through itself before sending it on is a classic wireless MITM method.

"In a MITM attack, the attacker places themselves between the sender and receiver, intercepting and possibly altering data in transit. Rogue access points can facilitate MITM attacks in wireless environments." (CCST Cybersecurity, Basic Network Security Concepts, Wireless Threats

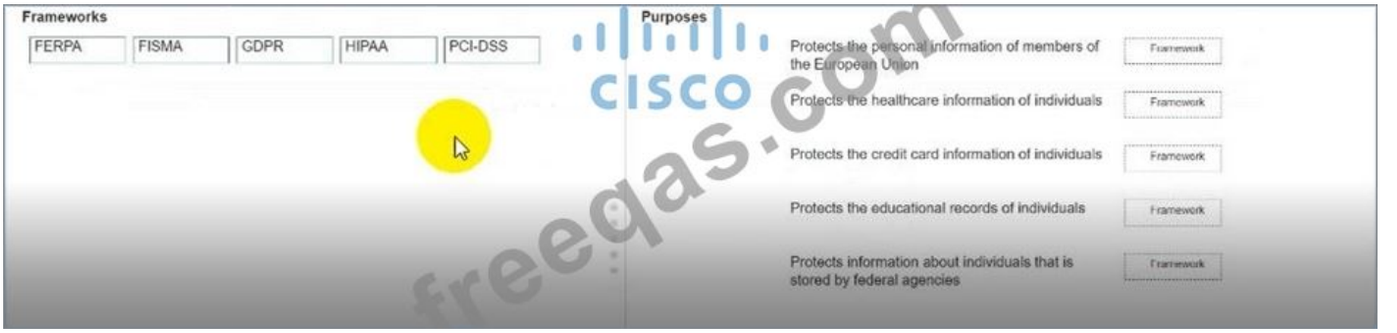
section, Cisco Networking Academy) A is incorrect: Reconnaissance is information gathering, not active interception.
B is correct: This is a wireless MITM attack.
C is incorrect: DDoS aims to overwhelm a service, not intercept data.
D is incorrect: Ransomware encrypts data for extortion.

NEW QUESTION: 105
What is ransomware?
A. A technique used by attackers to obtain sensitive information through deception.
B. A software program that is designed to damage, disrupt, or gain unauthorized access to a computer system.
C. Malicious software that encrypts files on a victim's computer and demands ransom for their release.
D. A form of cyber attack that attempts to gain unauthorized access to a network.
Answer: C (LEAVE A REPLY)
Ransomware is a type of malware that encrypts files on a victim's computer or network and then demands a ransom payment in exchange for the decryption key. It is a form of extortion and can cause significant damage and disruption to individuals and organizations.

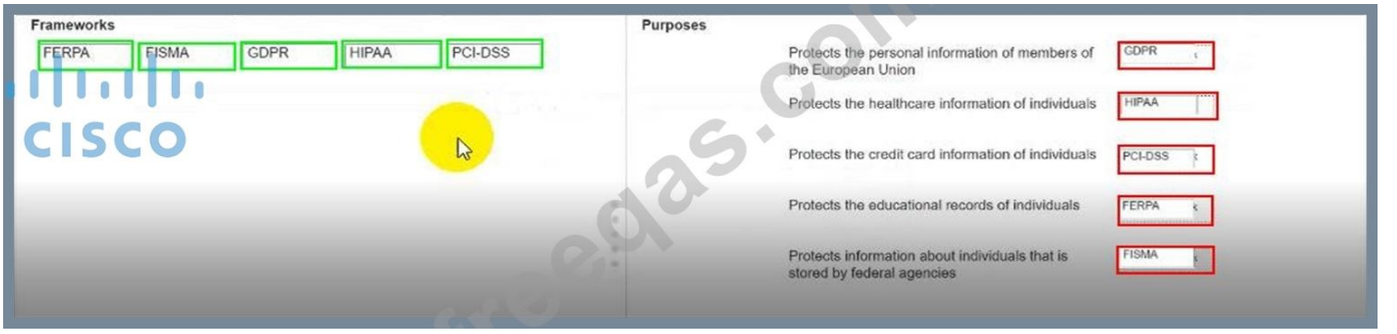
NEW QUESTION: 106
Which notation is used by IPv6?
A. Decimal notation
B. Octal notation
C. Hexadecimal notation
D. Binary notation
Answer: C (LEAVE A REPLY)
IPv6 addresses are expressed using hexadecimal notation. It consists of eight groups of four hexadecimal digits separated by colons, e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Hexadecimal digits range from 0 to 9 and A to F.

NEW QUESTION: 107
Move each framework from the list on the left to the correct purpose on the right.

Note: You will receive partial credit for each correct answer.



Answer:



NEW QUESTION: 108

Which of the following is a primary purpose of software inventory in a cybersecurity program?

A. Monitoring user access and permissions

B. Identifying vulnerabilities and patch requirements

C. Analyzing network traffic for potential threats

D. Ensuring compliance with software licensing agreements

Answer: B (LEAVE A REPLY)

Software inventory is an essential component of a cybersecurity program as it helps in identifying the software applications installed on devices within the network. By maintaining an accurate software inventory, organizations can identify vulnerabilities and track patch requirements to keep their systems secure and up to date.

NEW QUESTION: 109

What is the purpose of performing a vulnerability scan?

A. To encrypt sensitive data transmission

B. To assess the performance and latency of network devices

C. To identify any exploitable weaknesses in a system or network

D. To detect and block malicious network traffic

Answer: (SHOW ANSWER)

Vulnerability scanning is conducted to identify potential weaknesses or security flaws in a system or network that could be exploited by attackers. By conducting regular vulnerability scans, organizations can proactively discover and address vulnerabilities before they are exploited, ensuring the overall security and integrity of their systems. This helps in preventing unauthorized access, data breaches, and potential damage to the network infrastructure.

NEW QUESTION: 110
Which of the following best describes the purpose of the MITRE ATT&CK; Matrix?
A. To map vulnerabilities and exposures in computer systems
B. To analyze the impact of cyber threats on critical infrastructure
C. To track the global distribution of cyber threat actors
D. To provide a standardized way to categorize cyber threat tactics and techniques
Answer: D (LEAVE A REPLY)
The MITRE ATT&CK; Matrix provides a comprehensive framework that categorizes various tactics, techniques, and procedures (TTPs) used by cyber threat actors. It enables organizations to understand how different attackers operate and helps in developing effective cybersecurity defenses and detection mechanisms.

NEW QUESTION: 111
You are planning to work from home. Your company requires that you connect to the company network through a VPN.
Which three critical functions do VPNs provide to remote workers? (Choose 3.)
A. WAN management
B. Authorization of users
C. Integrity of data
D. Authentication of users
E. Confidentiality of information
F. Password management
Answer: C,D,E (LEAVE A REPLY)
The CCST Cybersecurity material states that a Virtual Private Network (VPN) provides secure communication over an untrusted network, typically by ensuring:
Authentication → verifying the identity of the user/device
Confidentiality → encrypting the data so it cannot be read by unauthorized parties Integrity → ensuring that transmitted data has not been altered in transit
"VPNs secure remote access by authenticating users, encrypting data for confidentiality, and ensuring integrity through cryptographic checks." (CCST Cybersecurity, Basic Network Security Concepts, VPNs section, Cisco Networking Academy) A is incorrect: WAN management is a network administration function, not a VPN feature.
B is incorrect: Authorization is related but not a primary VPN security function.
C is correct: Integrity is preserved through cryptographic hashing.
D is correct: Authentication verifies user identity.
E is correct: Confidentiality is provided via encryption.
F is incorrect: Password management is separate from VPN functions.

NEW QUESTION: 112
Which of the following helps to ensure the confidentiality of data in computer operations?

A. Data integrity controls
B. Access control lists (ACLs)
C. Intrusion Detection System (IDS)
D. Antivirus software
Answer: (SHOW ANSWER)
Access control lists (ACLs) are a security mechanism used in computer operations to enforce and manage access permissions for users and resources. ACLs enable organizations to control who can access specific data or resources, helping to ensure the confidentiality of sensitive information.

NEW QUESTION: 113
What is the purpose of implementing a firewall in a network?
A. To scan and remove malware from network traffic
B. To prevent unauthorized physical access to network devices
C. To control and filter network traffic based on predetermined security policies
D. To monitor network performance and troubleshoot issues
Answer: C (LEAVE A REPLY)
A firewall is a network security device that acts as a barrier between internal and external networks. Its main purpose is to control and filter network traffic based on predetermined security policies. It examines packets entering or leaving the network and either allows or blocks them based on the configured rules.

NEW QUESTION: 114
Which of the following is an example of a natural disaster?
A. Malware attack
B. Data breach
C. Power outage
D. Server failure
Answer: C (LEAVE A REPLY)
A power outage is considered a natural disaster because it is caused by factors beyond human control, such as severe weather conditions or infrastructure failures. It can disrupt normal operations and impact the availability of systems and resources.

NEW QUESTION: 115
Which of the following is a best practice for managing security policies and procedures?
A. Implementing a regular review process for security policies
B. Relying solely on default security settings
C. Allowing users to create and manage their own security policies
D. Not documenting the security policies and procedures
Answer: A (LEAVE A REPLY)

Option 1: Correct: Implementing a regular review process for security policies ensures that they are up-to-date and aligned with the organization's current security needs.
Option 2: Incorrect: Relying solely on default security settings is not a best practice as default settings may not provide adequate protection and may not be appropriate for the organization's specific needs.
Option 3: Incorrect: Allowing users to create and manage their own security policies can lead to inconsistencies, lack of control, and potential security vulnerabilities.
Option 4: Incorrect: Not documenting the security policies and procedures makes it difficult to enforce and communicate these policies to employees.

NEW QUESTION: 116
Which of the following represents a technique used in Classless Inter-Domain Routing (CIDR)?
A. Variable-length subnet masks
B. Compressed MAC addresses
C. Binary notation for IP addresses
D. 32-bit IP addresses
Answer: (SHOW ANSWER)
Classless Inter-Domain Routing (CIDR) is a technique used to allocate and manage IP addresses more efficiently. It involves using variable-length subnet masks (VLSMs), which allow the network to have subnets of different sizes. VLSMs provide flexibility in allocating IP addresses by allowing the network administrator to choose the appropriate number of network and host bits based on the network requirements.

NEW QUESTION: 117
Which of the following is an example of a preventive control?
A. Incident response plan
B. User access log
C. Firewall
D. Intrusion detection system
Answer: C (LEAVE A REPLY)
A firewall is a preventive control that helps to protect a network by acting as a barrier between internal and external networks, monitoring and controlling incoming and outgoing traffic based on predetermined security rules. It prevents unauthorized access and defends against network-based attacks.

NEW QUESTION: 118
Which of the following operating systems includes a built-in antivirus software called Windows Defender?
A. Windows
B. macOS
C. Linux

D. Windows and macOS

Answer: A (LEAVE A REPLY)

Windows operating system includes a built-in antivirus software called Windows Defender. It provides real-time protection against various types of malware, including viruses, spyware, and ransomware. Windows Defender is automatically enabled and updated on Windows computers to help keep the system secure. Note: macOS and Linux operating systems have their own security features, but they do not include Windows Defender. macOS has a built-in security tool called XProtect, which provides some protection against malware, and Linux offers various security features such as SELinux (Security-Enhanced Linux) and AppArmor.

NEW QUESTION: 119

Which of the following is a recommended practice for securing a wireless SoHo network?

A. Disabling encryption for ease of use

B. Regularly updating the router's firmware

C. Sharing Wi-Fi passwords with neighbors

D. Using the default network name (SSID)

Answer: B (LEAVE A REPLY)

Regularly updating the router's firmware is a recommended practice for securing a wireless SoHo network. Router manufacturers often release firmware updates to address security vulnerabilities and improve performance. By installing the latest firmware updates, you can ensure that your router has the latest security patches. Disabling encryption (A) would make the network vulnerable to unauthorized access. Sharing Wi-Fi passwords with neighbors (C) may compromise security. Using the default network name (D) (SSID) can make it easier for attackers to identify and target your network.

NEW QUESTION: 120

Which of the following is an example of personally identifiable information (PII)?

A. Birthdate

B. Browser history

C. Employee ID number

D. IP address

Answer: A (LEAVE A REPLY)

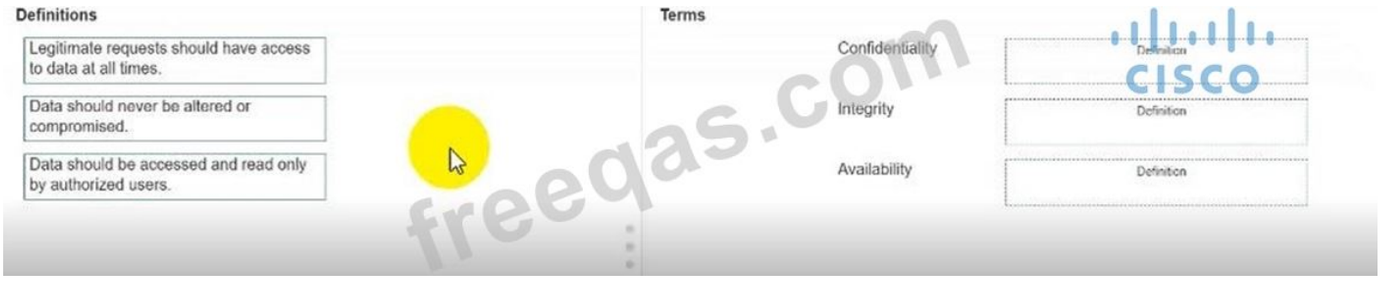
Personally identifiable information (PII) refers to any data that can be used to identify an individual.

Birthdate is considered PII as it can be used to pinpoint a specific person.

NEW QUESTION: 121

Move each definition from the list on the left to the correct CIA Triad term on the right.

Note: You will receive partial credit for each correct answer.



Answer:

NEW QUESTION: 122

You are reviewing your company's disaster recovery plan.

Which two daily data backup actions should the plan include? (Choose 2.)

A. Back up the data to removable media and store it off-site.

B. Back up each department's data to a separate local server.

C. Back up the data by using cloud services.

D. Back up the data by using RAID on a local external hard drive with a secondary power source.

Answer: A,C (LEAVE A REPLY)

The CCST Cybersecurity Study Guide emphasizes that backups should be stored off-site or in the cloud to ensure recovery even if the primary location is damaged or compromised.

"A comprehensive disaster recovery plan includes performing regular backups and ensuring copies are stored in locations not subject to the same physical risks as the primary site. Off-site storage and cloud-based backups provide resilience against local disasters." (CCST Cybersecurity, Essential Security Principles, Backup and Disaster Recovery section, Cisco Networking Academy) A is correct: Off-site removable media ensures recovery even if the main site is destroyed.

B is incorrect: Local-only backups are vulnerable to the same risks as production systems.

C is correct: Cloud services provide geographically separate storage with automated redundancy.

D is incorrect: RAID is for hardware fault tolerance, not a complete backup solution.

NEW QUESTION: 123
Which of the following is an example of a preventive control in computer operations?
A. Backup and recovery procedures
B. Firewall implementation
C. Incident response planning
D. Penetration testing
Answer: B (LEAVE A REPLY)
A firewall is a preventive control in computer operations that helps to protect the network by filtering incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between an internal network and external networks, such as the internet, to prevent unauthorized access and potential attacks.

NEW QUESTION: 124
Which wireless security protocol provides the strongest protection for a home or small business network?
A. WEP
B. WPA
C. WPA2 with AES
D. WPA3
Answer: D (LEAVE A REPLY)
The CCST Cybersecurity Study Guide explains that WPA3 is the most current and secure Wi-Fi Protected Access protocol, offering stronger encryption and better protection against brute-force attacks compared to earlier versions.
"WPA3 improves wireless security by using more robust encryption methods and protections against offline password guessing, making it the recommended protocol for securing modern Wi-Fi networks." (CCST Cybersecurity, Basic Network Security Concepts, Wireless Security Protocols section, Cisco Networking Academy)

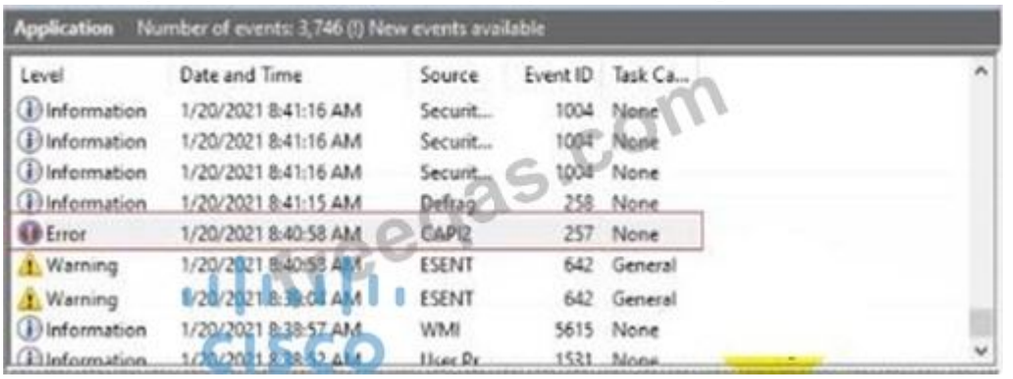
NEW QUESTION: 125
Why is updating documentation regularly important in the context of cybersecurity?
A. To facilitate effective incident response and investigation
B. To maintain accurate records of security incidents
C. All of the above
D. To ensure compliance with industry regulations
Answer: C (LEAVE A REPLY)
Updating documentation regularly is crucial in cybersecurity for multiple reasons. Firstly, it helps maintain accurate records of security incidents, which is essential for future reference and analysis. Secondly, updating documentation ensures compliance with industry regulations and standards, helping organizations avoid potential penalties and legal issues. Lastly, up-to-date

documentation facilitates effective incident response and investigation, enabling swift action and minimizing the impact of cybersecurity incidents.

NEW QUESTION: 126

You are reviewing the Application log on a Windows computer. You see an event with an error-level message as shown.

What can you determine about the application that generated the event message?



A. The application is currently running much slower than expected.

B. The application experienced a significant problem that caused it to fail.

C. The application recovered from an event without loss of functionality.

D. The application loaded and ran successfully without issues.

Answer: B (LEAVE A REPLY)

In the CCST Cybersecurity course, Windows Event Viewer Error events in the Application log indicate a severe problem that caused an application or component to fail. This usually requires investigation or repair.

"Error events indicate a significant problem such as a loss of functionality in an application or system component. Errors are often critical and need immediate attention." (CCST Cybersecurity, Incident Handling, Event Logging and Analysis section, Cisco Networking Academy) A is incorrect: Performance slowness would usually generate warnings, not errors.

B is correct: An "Error" level in Event Viewer means the application failed in some way.

C is incorrect: That describes an "Information" event, not an error.

D is incorrect: That also corresponds to an "Information" event.

NEW QUESTION: 127

What is the general motivation behind an Advanced Persistent Threat (APT)?

A. Publicity

B. Random disruption

C. Financial gain

D. Revenge

Answer: C (LEAVE A REPLY)

The general motivation behind an APT is often financial gain. Threat actors conducting APTs aim to gain unauthorized access to valuable information, such as financial data or intellectual property, with the intention of extracting monetary value from their targets.

NEW QUESTION: 128
Which command-line tool is commonly used to display active network connections?
A. ping
B. tcpdump
C. netstat
D. nslookup
Answer: C (LEAVE A REPLY)
The correct command-line tool to display active network connections is netstat. It allows you to view open ports, established connections, and other network statistics. It helps in verifying the security assessment information related to active connections.