COMPTIA SECURITY+ SY0-701

PRACTICE QUESTIONS AND ANSWERS

SkillWeed

CONTENTS

Question 1:
What is the purpose of a phishing attack?

A) To gain unauthorized access to systems

B) To trick users into revealing sensitive information

C) To flood a network with traffic

D) To execute malicious code remotely

Answer:

B) To trick users into revealing sensitive information

Explanation: Phishing uses deceptive communication to manipulate users into divulging credentials or other data.

Question 2:
Which type of malware locks users out of their systems until a ransom is paid?

A) Spyware

B) Ransomware

C) Worm

D) Adware

Answer:

B) Ransomware

Explanation: Ransomware encrypts files and demands payment to restore access.

Question 3:
Which attack exploits vulnerabilities in poorly sanitized user input fields?

A) SQL Injection

B) Man-in-the-Middle

C) DNS Spoofing

D) XSS

Answer:

A) SQL Injection

Explanation: SQL Injection involves injecting malicious SQL queries into user input fields to manipulate databases.

Question 4:
What is a common advantage of using cloud-based infrastructure?

A) Fixed pricing

B) Scalability

C) Complete control over hardware

D) Improved latency

Answer:

B) Scalability

Explanation: Cloud infrastructure allows organizations to scale resources up or down based on demand.

Question 5:
What does a hypervisor enable in a virtualization environment?

A) Execution of virtual machines

B) Enforcement of least privilege

C) Improved data encryption

D) Data backup

Answer:

A) Execution of virtual machines

Explanation: Hypervisors are software or hardware that create and manage virtual machines.

Question 6:
What is the main benefit of implementing endpoint detection and response (EDR)?

A) Encrypting all data in transit

B) Preventing phishing attacks

C) Identifying and responding to endpoint threats

D) Managing user authentication

Answer:

C) Identifying and responding to endpoint threats

Explanation: EDR solutions monitor endpoints for threats and provide automated responses.

Question 7:
Which protocol is used for encrypted remote server access?

A) Telnet

B) SSH

C) FTP

D) HTTP

Answer:

B) SSH

Explanation: Secure Shell (SSH) encrypts remote administrative access to servers.

Question 8:
What is the purpose of network segmentation?

A) To enhance encryption

B) To isolate sensitive systems

C) To increase bandwidth

D) To improve scalability

Answer:

B) To isolate sensitive systems

Explanation: Network segmentation limits access to sensitive data and reduces the impact of potential breaches.

Question 9:
Which step comes after containment in the incident response process?

A) Eradication

B) Recovery

C) Identification

D) Reporting

Answer:

A) Eradication

Explanation: Eradication involves removing the root cause of the incident after containment.

Question 10:
What tool is used to detect unauthorized changes to system files?

A) SIEM

B) IDS

C) File Integrity Monitor (FIM)

D) Vulnerability Scanner

Answer:

C) File Integrity Monitor (FIM)

Explanation: FIM tools identify changes to system files, indicating potential compromise.

Question 11:
Which type of data is most volatile and should be collected first during an investigation?

A) Hard drive data

B) Network logs

C) RAM

D) Email archives

Answer:

C) RAM

Explanation: RAM is volatile and lost upon shutdown, so it should be captured first during forensic investigations.

Question 12:
What framework is widely used for assessing and improving cybersecurity posture?

A) PCI DSS

B) HIPAA

C) NIST CSF

D) GDPR

Answer:

C) NIST CSF

Explanation: The NIST Cybersecurity Framework provides guidelines for improving cybersecurity.

Question 13:
Which compliance regulation applies to credit card transactions?

A) PCI DSS

B) GDPR

C) FISMA

D) SOX

Answer:

A) PCI DSS

Explanation: Payment Card Industry Data Security Standard (PCI DSS) governs the security of card transactions.

Question 14:
What is the primary goal of a risk assessment?

A) To eliminate all risks

B) To prioritize and mitigate risks

C) To identify threats

D) To create a disaster recovery plan

Answer:

B) To prioritize and mitigate risks

Explanation: Risk assessments help organizations evaluate and address potential risks to operations.

Question 21:
What is the main objective of a brute force attack?

A) Inject malicious code

B) Guess passwords through repeated attempts

C) Redirect users to malicious websites

D) Exploit a software vulnerability

Answer:

B) Guess passwords through repeated attempts

Explanation: Brute force attacks systematically try all possible combinations to guess passwords.

Question 22:
Which of the following is a characteristic of spear phishing?

A) Targeting a large group of random users

B) Using a malicious website to distribute malware

C) Crafting a message to target a specific individual or group

D) Leveraging compromised email accounts for spam

Answer:

C) Crafting a message to target a specific individual or group

Explanation: Spear phishing focuses on specific targets using personalized messages.

Question 23:
What type of attack involves overwhelming a system with a flood of traffic?

A) DNS Spoofing

B) Denial-of-Service (DoS)

C) Man-in-the-Middle

D) Cross-Site Scripting

Answer:

B) Denial-of-Service (DoS)

Explanation: DoS attacks disrupt services by overloading the target with excessive traffic.

Question 24:
Which security control ensures users can only access resources they are authorized for?

A) Role-Based Access Control (RBAC)

B) Data Loss Prevention (DLP)

C) Network Segmentation

D) Firewall Rules

Answer:

A) Role-Based Access Control (RBAC)

Explanation: RBAC restricts resource access based on user roles and permissions.

Question 25:
What is the purpose of applying defense in depth?

A) To simplify security management

B) To create multiple layers of security

C) To eliminate all security vulnerabilities

D) To implement a single control for efficiency

Answer:

B) To create multiple layers of security

Explanation: Defense in depth uses overlapping security controls to mitigate risks.

Question 26:
Which of the following authentication factors is considered 'something you have'?

A) Password

B) Security Token

C) Fingerprint

D) PIN

Answer:

B) Security Token

Explanation: 'Something you have' refers to physical items like security tokens used for authentication.

Question 27:
What technology isolates workloads and ensures they are securely separated?

A) Virtualization

B) Containerization

C) Encryption

D) Proxy Server

Answer:

B) Containerization

Explanation: Containerization isolates applications using lightweight, portable environments.

Question 28:
Which of the following actions is part of the 'containment' phase in incident response?

A) Identifying affected systems

B) Removing malicious files from servers

C) Isolating impacted systems to prevent spread

D) Restoring data from backups

Answer:

C) Isolating impacted systems to prevent spread

Explanation: Containment involves preventing the incident from spreading to other systems.

Question 29:
What is the primary benefit of using Security Information and Event Management (SIEM) tools?

A) Preventing attacks

B) Real-time monitoring and correlation of security events

C) Encrypting sensitive information

D) Identifying vulnerabilities

Answer:

B) Real-time monitoring and correlation of security events

Explanation: SIEM tools aggregate and analyze security events to detect and respond to threats.

Question 51:
What type of attack exploits human psychology to gain unauthorized access to systems?

A) Phishing

B) Social Engineering

C) Malware Injection

D) Privilege Escalation

Answer:

B) Social Engineering

Explanation: Social engineering manipulates individuals to divulge confidential information or grant access.

Question 52:
Which type of malware modifies the operating system to avoid detection?

A) Rootkit

B) Ransomware

C) Spyware

D) Worm

Answer:

A) Rootkit

Explanation: Rootkits are stealthy malware designed to remain hidden by modifying the operating system.

Question 53:
What is the primary purpose of a logic bomb?

A) Encrypt sensitive data

B) Cause harm when specific conditions are met

C) Exploit software vulnerabilities

D) Replicate across systems

Answer:

B) Cause harm when specific conditions are met

Explanation: Logic bombs execute malicious actions only when certain triggers are activated.

Question 54:
What is the purpose of network segmentation in securing sensitive data?

A) Enhance performance

B) Isolate critical systems

C) Reduce network costs

D) Increase redundancy

Answer:

B) Isolate critical systems

Explanation: Network segmentation isolates critical systems to reduce attack surfaces and limit damage.

Question 55:
What architectural model limits the trust given to devices or users inside a network?

A) Perimeter Security

B) Zero Trust

C) Layered Security

D) Flat Network

Answer:

B) Zero Trust

Explanation: Zero Trust ensures no implicit trust, requiring verification for every access request.

Question 56:
Which technology is used to distribute and balance traffic across multiple servers?

A) Virtualization

B) Load Balancer

C) Firewall

D) Proxy Server

Answer:

B) Load Balancer

Explanation: Load balancers evenly distribute incoming traffic to improve availability and performance.

Question 57:
Which type of access control is based on predefined roles within an organization?

A) Rule-Based Access Control

B) Role-Based Access Control

C) Discretionary Access Control

D) Mandatory Access Control

Answer:

B) Role-Based Access Control

Explanation: RBAC assigns permissions to users based on their job roles.

Question 58:
What protocol is typically used for secure email communication?

A) IMAP

B) POP3

C) S/MIME

D) HTTP

Answer:

C) S/MIME

Explanation: S/MIME provides encryption and digital signatures for secure email communication.

Question 59:
Which encryption method uses a single key for both encryption and decryption?

A) Asymmetric Encryption

B) Symmetric Encryption

C) Hashing

D) Public Key Infrastructure

Answer:

B) Symmetric Encryption

Explanation: Symmetric encryption uses the same key for encrypting and decrypting data.

Question 60:
What is the first action taken when responding to a cybersecurity incident?

A) Containment

B) Eradication

C) Recovery

D) Identification

Answer:

D) Identification

Explanation: Identifying the scope and nature of the incident is the initial step in incident response.

Question 61:
Which tool captures and analyzes network traffic for security monitoring?

A) Nessus

B) Wireshark

C) Splunk

D) Metasploit

Answer:

B) Wireshark

Explanation: Wireshark is a packet analyzer used to capture and inspect network traffic.

Question 62:
What is the purpose of log aggregation in a SIEM solution?

A) Encrypt logs

B) Centralize and analyze logs from multiple sources

C) Block malicious traffic

D) Facilitate user authentication

Answer:

B) Centralize and analyze logs from multiple sources

Explanation: Log aggregation consolidates logs for correlation and security event analysis.

Question 63:
Which regulation enforces the protection of EU citizens' personal data?

A) HIPAA

B) GDPR

C) CCPA

D) FISMA

Answer:

B) GDPR

Explanation: The General Data Protection Regulation (GDPR) ensures privacy for EU citizens' personal data.

Question 64:
What is the primary goal of a vulnerability assessment?

A) Exploit known vulnerabilities

B) Detect and prioritize vulnerabilities

C) Replace outdated software

D) Train employees on security practices

Answer:

B) Detect and prioritize vulnerabilities

Explanation: Vulnerability assessments identify and rank weaknesses for remediation.

Question 65:
Which framework is most commonly used for improving cybersecurity practices?

A) COBIT

B) ISO 27001

C) NIST CSF

D) ITIL

Answer:

C) NIST CSF

Explanation: The NIST Cybersecurity Framework provides guidelines to improve cybersecurity posture.

Question 81:
What is a characteristic of ransomware?

A) It replicates itself across systems

B) It locks or encrypts user data for a ransom

C) It captures keystrokes without user knowledge

D) It creates backdoors for remote access

Answer:

B) It locks or encrypts user data for a ransom

Explanation: Ransomware encrypts data and demands payment to restore access.

Question 82:
Which attack type exploits an authenticated user's session ID?

A) Cross-Site Scripting (XSS)

B) Replay Attack

C) Session Hijacking

D) Phishing

Answer:

C) Session Hijacking

Explanation: Session hijacking involves stealing an active session ID to impersonate a user.

Question 83:
What type of threat actor is typically motivated by financial gain?

A) Hacktivist

B) Insider

C) Cybercriminal

D) Nation-State

Answer:

C) Cybercriminal

Explanation: Cybercriminals aim to profit from malicious activities, such as theft or fraud.

Question 84:
What is the purpose of an Intrusion Detection System (IDS)?

A) Block malicious traffic

B) Encrypt sensitive data

C) Monitor and alert on suspicious activity

D) Perform vulnerability scans

Answer:

C) Monitor and alert on suspicious activity

Explanation: IDS monitors network traffic for anomalies and sends alerts when threats are detected.

Question 85:
Which of the following is a key characteristic of Infrastructure as Code (IaC)?

A) Manual network configuration

B) Automated provisioning and management

C) Lack of scalability

D) Physical infrastructure management

Answer:

B) Automated provisioning and management

Explanation: IaC uses scripts to automate infrastructure setup, ensuring consistency and scalability.

Question 86:
What is the role of a demilitarized zone (DMZ) in network security?

A) Encrypt all network traffic

B) Host public-facing services while isolating internal systems

C) Monitor network traffic for threats

D) Block unauthorized access to the network

Answer:

B) Host public-facing services while isolating internal systems

Explanation: A DMZ provides a secure buffer zone for public-facing servers.

Question 87:
Which type of encryption is used in HTTPS to secure web communications?

A) AES

B) RSA

C) DES

D) MD5

Answer:

B) RSA

Explanation: RSA is an asymmetric encryption algorithm used in HTTPS to secure connections.

Question 88:
What is the purpose of a digital signature?

A) Encrypts the entire message

B) Verifies the authenticity and integrity of a message

C) Provides anonymous communication

D) Encrypts user credentials

Answer:

B) Verifies the authenticity and integrity of a message

Explanation: Digital signatures ensure that a message has not been tampered with and verify its origin.

Question 89:
What type of authentication uses physical characteristics such as fingerprints?

A) Multi-Factor Authentication

B) Biometric Authentication

C) Token-Based Authentication

D) Role-Based Authentication

Answer:

B) Biometric Authentication

Explanation: Biometric authentication relies on unique physical traits for user verification.

Question 90:
Which action is part of the recovery phase of incident response?

A) Restoring systems to operational status

B) Isolating infected machines

C) Analyzing logs for anomalies

D) Removing malware from endpoints

Answer:

A) Restoring systems to operational status

Explanation: Recovery involves bringing systems back to normal operation after an incident.

Question 91:
What type of evidence should be collected first in a forensic investigation?

A) Volatile memory

B) Hard disk data

C) Archived logs

D) Network backups

Answer:

A) Volatile memory

Explanation: Volatile data, such as RAM, is collected first because it is lost when the system is powered off.

Question 92:
What is the function of a packet sniffer?

A) To encrypt traffic

B) To capture and analyze network traffic

C) To block malicious IP addresses

D) To detect malware

Answer:

B) To capture and analyze network traffic

Explanation: Packet sniffers like Wireshark analyze network packets for troubleshooting and security monitoring.

Question 93:
Which framework is commonly used for risk management?

A) COBIT

B) NIST 800-37

C) PCI DSS

D) GDPR

Answer:

B) NIST 800-37

Explanation: NIST 800-37 provides a risk management framework for federal information systems.

Question 94:
What is the primary purpose of a data privacy impact assessment (DPIA)?

A) Ensure compliance with GDPR

B) Detect vulnerabilities in applications

C) Analyze potential risks to personal data

D) Conduct penetration testing

Answer:

C) Analyze potential risks to personal data

Explanation: A DPIA identifies and mitigates privacy risks associated with data processing activities.

Question 95:
What is required under the General Data Protection Regulation (GDPR) for data breaches?

A) Immediate system shutdown

B) Notification to affected individuals and authorities

C) Public disclosure of breach details

D) Replacement of compromised hardware

Answer:

B) Notification to affected individuals and authorities

Explanation: GDPR mandates breach notifications within 72 hours of detection.

Question 111:
What is the purpose of an advanced persistent threat (APT)?

A) Conducting short-term attacks for financial gain

B) Gaining and maintaining long-term access to a target system

C) Randomly targeting multiple organizations

D) Disrupting services without a specific goal

Answer:

B) Gaining and maintaining long-term access to a target system

Explanation: APTs focus on persistent access to a target system to extract data or disrupt operations over time.

Question 112:
Which attack involves sending fraudulent text messages to trick users?

A) Phishing

B) Smishing

C) Vishing

D) Spear Phishing

Answer:

B) Smishing

Explanation: Smishing uses SMS messages to deceive users into revealing sensitive information.

Question 113:
What is the main goal of a Distributed Denial-of-Service (DDoS) attack?

A) Stealing sensitive data

B) Overwhelming a network or service to make it unavailable

C) Gaining unauthorized access

D) Exploiting a software vulnerability

Answer:

B) Overwhelming a network or service to make it unavailable

Explanation: DDoS attacks flood the target system with traffic to render it unusable.

Question 114:
What is the primary benefit of using a software-defined network (SDN)?

A) Increased hardware redundancy

B) Centralized management and dynamic configuration

C) Improved physical security

D) Automatic data encryption

Answer:

B) Centralized management and dynamic configuration

Explanation: SDN separates the control plane from the data plane, enabling centralized control of network traffic.

Question 115:
What is a key principle of secure system design?

A) Least Privilege

B) Default Permit

C) Implicit Trust

D) No Auditing

Answer:

A) Least Privilege

Explanation: Least privilege ensures that users and systems have the minimum access required for their tasks.

Question 116:
Which of the following protects the integrity of data during transmission?

A) Encryption

B) Hashing

C) Firewall

D) Multi-Factor Authentication

Answer:

B) Hashing

Explanation: Hashing verifies data integrity by comparing hash values before and after transmission.

Question 117:
Which wireless authentication protocol is commonly used with WPA3?

A) EAP-TLS

B) PAP

C) CHAP

D) RADIUS

Answer:

A) EAP-TLS

Explanation: EAP-TLS provides strong authentication for wireless networks, often used with WPA3.

Question 118:
What type of encryption is commonly used for securing web traffic?

A) Symmetric Encryption

B) Asymmetric Encryption

C) SSL/TLS

D) Hashing

Answer:

C) SSL/TLS

Explanation: SSL/TLS protocols secure web traffic by encrypting data in transit.

Question 119:
What is the main purpose of endpoint detection and response (EDR) solutions?

A) Encrypt endpoint communications

B) Detect and respond to threats on endpoints

C) Provide secure remote access

D) Monitor web traffic

Answer:

B) Detect and respond to threats on endpoints

Explanation: EDR tools focus on monitoring and mitigating security threats at the endpoint level.

Question 120:
Which type of analysis involves examining malicious code in a controlled environment?

A) Dynamic Analysis

B) Static Analysis

C) Forensic Analysis

D) Vulnerability Scanning

Answer:

A) Dynamic Analysis

Explanation: Dynamic analysis executes code in a sandbox environment to observe its behavior.

Question 121:
What is the primary role of a SIEM in security operations?

A) Encrypt network traffic

B) Collect and correlate log data from multiple sources

C) Perform penetration testing

D) Provide secure remote access

Answer:

B) Collect and correlate log data from multiple sources

Explanation: SIEM solutions aggregate and analyze log data to detect and respond to security incidents.

Question 122:
What is the purpose of chain of custody in forensic investigations?

A) To ensure the evidence is admissible in court

B) To identify the source of malware

C) To mitigate vulnerabilities

D) To recover lost data

Answer:

A) To ensure the evidence is admissible in court

Explanation: Chain of custody documents the handling of evidence to maintain its integrity.

Question 123:
What is the main focus of ISO/IEC 27001?

A) Physical security

B) Risk management for information security

C) Cybersecurity for critical infrastructure

D) Privacy for individuals

Answer:

B) Risk management for information security

Explanation: ISO/IEC 27001 provides a framework for establishing, implementing, and maintaining an information security management system (ISMS).

Question 124:
Which regulation is focused on protecting healthcare information in the United States?

A) GDPR

B) HIPAA

C) SOX

D) CCPA

Answer:

B) HIPAA

Explanation: The Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of sensitive healthcare information.

Question 125:
What is the goal of penetration testing?

A) To implement security controls

B) To identify and exploit vulnerabilities

C) To provide employee security training

D) To block malicious IP addresses

Answer:

B) To identify and exploit vulnerabilities

Explanation: Penetration testing simulates attacks to identify and remediate security weaknesses.

Question 141:
What type of attack involves sending spoofed ARP messages to link an attacker's MAC address to the IP address of a legitimate user?

A) ARP Poisoning

B) DNS Spoofing

C) Smishing

D) IP Spoofing

Answer:

A) ARP Poisoning

Explanation: ARP Poisoning tricks a network into associating the attacker's MAC address with a legitimate IP, intercepting traffic.

Question 142:
Which of the following is a method used to exfiltrate data from an organization?

A) Data Encryption

B) DNS Tunneling

C) Firewall Rules

D) Zero Trust Architecture

Answer:

B) DNS Tunneling

Explanation: DNS Tunneling encodes data within DNS requests to secretly send it out of a network.

Question 143:
What is a key characteristic of spyware?

A) Encrypting user files

B) Monitoring user activity and collecting information

C) Replicating itself across networks

D) Demanding a ransom

Answer:

B) Monitoring user activity and collecting information

Explanation: Spyware secretly collects information about user activity, often without their consent.

Question 144:
Which of the following is an example of physical security control?

A) Firewall

B) Security Guard

C) Encryption

D) VPN

Answer:

B) Security Guard

Explanation: Physical security controls like guards protect physical access to resources.

Question 145:
What is the primary function of an Intrusion Prevention System (IPS)?

A) Alert administrators to threats

B) Block malicious traffic in real-time

C) Scan systems for vulnerabilities

D) Encrypt sensitive data

Answer:

B) Block malicious traffic in real-time

Explanation: IPS actively blocks detected threats to prevent damage or compromise.

Question 146:
What type of design ensures that sensitive data is only visible to authorized personnel?

A) Network Segmentation

B) Data Masking

C) Zero Trust

D) SIEM

Answer:

B) Data Masking

Explanation: Data masking conceals sensitive information, allowing access only to authorized users.

Question 147:
Which protocol is commonly used for secure file transfer over the internet?

A) HTTP

B) SFTP

C) Telnet

D) FTP

Answer:

B) SFTP

Explanation: SFTP (Secure File Transfer Protocol) encrypts file transfers to ensure confidentiality.

Question 148:
What is the purpose of multi-factor authentication?

A) To encrypt sensitive data

B) To add additional layers of identity verification

C) To simplify access control

D) To monitor user activity

Answer:

B) To add additional layers of identity verification

Explanation: MFA increases security by requiring multiple verification methods for access.

Question 149:
Which of the following is a form of asymmetric encryption?

A) AES

B) RSA

C) 3DES

D) MD5

Answer:

B) RSA

Explanation: RSA is a widely used asymmetric encryption algorithm for secure communication.

Question 150:
What type of data is considered most volatile in a forensic investigation?

A) Hard Drive Data

B) RAM

C) Backup Tapes

D) Archived Logs

Answer:

B) RAM

Explanation: RAM is volatile memory that is lost when a system is powered off, making it a priority during investigations.

Question 151:
Which step in the incident response process involves removing malware or compromised components?

A) Identification

B) Containment

C) Eradication

D) Recovery

Answer:

C) Eradication

Explanation: Eradication removes the root cause of an incident to prevent further compromise.

Question 152:
What type of backup retains only the changes made since the last backup?

A) Full Backup

B) Incremental Backup

C) Differential Backup

D) Snapshot

Answer:

B) Incremental Backup

Explanation: Incremental backups store only the data changed since the previous backup, saving time and storage.

Question 153:
Which compliance standard focuses on protecting payment card information?

A) GDPR

B) PCI DSS

C) HIPAA

D) SOX

Answer:

B) PCI DSS

Explanation: The Payment Card Industry Data Security Standard (PCI DSS) ensures secure handling of credit card information.

Question 154:
What is the primary goal of risk management?

A) To eliminate all risks

B) To prioritize and mitigate risks

C) To increase system performance

D) To create audit logs

Answer:

B) To prioritize and mitigate risks

Explanation: Risk management identifies and addresses potential threats to minimize their impact.

Question 155:
Which framework is widely used for managing information security in organizations?

A) ITIL

B) NIST CSF

C) GDPR

D) FISMA

Answer:

B) NIST CSF

Explanation: The NIST Cybersecurity Framework provides guidelines to improve organizational security posture.

Question 180:
Which of the following describes a waterhole attack?

A) An attack that exploits vulnerabilities in a system

B) A targeted attack where malicious content is planted on frequently visited websites

C) An attack that floods a system with traffic

D) An attack that manipulates DNS queries

Answer:

B) A targeted attack where malicious content is planted on frequently visited websites

Explanation: Waterhole attacks target websites that are likely to be visited by specific victims.

Question 181:
What is a characteristic of polymorphic malware?

A) It self-replicates across systems

B) It changes its code to evade detection

C) It creates backdoors for remote access

D) It encrypts user files for ransom

Answer:

B) It changes its code to evade detection

Explanation: Polymorphic malware modifies its code to bypass signature-based detection methods.

Question 182:
Which attack exploits web applications by inserting malicious SQL statements?

A) Cross-Site Scripting (XSS)

B) Command Injection

C) SQL Injection

D) Buffer Overflow

Answer:

C) SQL Injection

Explanation: SQL Injection allows attackers to manipulate a database by injecting malicious SQL code.

Question 183:
What is the primary benefit of implementing network segmentation?

A) Reduced network latency

B) Enhanced security by isolating sensitive systems

C) Increased bandwidth

D) Simplified access control

Answer:

B) Enhanced security by isolating sensitive systems

Explanation: Network segmentation isolates critical assets, reducing the impact of breaches.

Question 184:
What is a core principle of zero trust architecture?

A) Implicit trust for all internal users

B) Always assume a breach and verify every access request

C) No encryption for internal traffic

D) Allow unrestricted access to external networks

Answer:

B) Always assume a breach and verify every access request

Explanation: Zero trust requires continuous verification for all access, regardless of origin.

Question 185:
Which security feature is commonly used to restrict access to resources based on the time of day?

A) Network Segmentation

B) Mandatory Access Control

C) Time-Based Access Control

D) Role-Based Access Control

Answer:

C) Time-Based Access Control

Explanation: Time-based access control enforces restrictions based on specific time periods.

Question 186:
What is the purpose of Secure Boot in modern systems?

A) Encrypt all system data

B) Verify the integrity of the operating system during startup

C) Prevent user account lockouts

D) Enable multi-factor authentication

Answer:

B) Verify the integrity of the operating system during startup

Explanation: Secure Boot ensures that only trusted OS components load during the boot process.

Question 187:
Which of the following is a symmetric encryption algorithm?

A) RSA

B) ECC

C) AES

D) DSA

Answer:

C) AES

Explanation: AES is a symmetric encryption algorithm used for securing data.

Question 188:
What is the role of Transport Layer Security (TLS) in secure communications?

A) Encrypts data in storage

B) Provides end-to-end encryption for data in transit

C) Protects against SQL Injection attacks

D) Blocks malicious IP addresses

Answer:

B) Provides end-to-end encryption for data in transit

Explanation: TLS ensures secure communication over the internet by encrypting data in transit.

Question 189:
What is the purpose of a jump server in a secure network?

A) To store encryption keys

B) To facilitate secure administrative access to sensitive systems

C) To act as a firewall for external traffic

D) To analyze network packets

Answer:

B) To facilitate secure administrative access to sensitive systems

Explanation: Jump servers provide secure access to critical resources by acting as a controlled gateway.

Question 190:
Which tool is commonly used for automated penetration testing?

A) Nessus

B) Wireshark

C) Metasploit

D) Splunk

Answer:

C) Metasploit

Explanation: Metasploit is an automated penetration testing framework for identifying vulnerabilities.

Question 191:
What is the role of a root cause analysis in incident response?

A) Identifying and addressing the underlying cause of an incident

B) Monitoring system performance

C) Blocking future phishing attempts

D) Generating compliance reports

Answer:

A) Identifying and addressing the underlying cause of an incident

Explanation: Root cause analysis determines the primary factor that caused an incident.

Question 192:
Which regulation requires organizations to protect personal data of EU citizens?

A) PCI DSS

B) HIPAA

C) GDPR

D) SOX

Answer:

C) GDPR

Explanation: The General Data Protection Regulation (GDPR) mandates the protection of EU citizens' personal data.

Question 193:
What is a key benefit of conducting regular vulnerability assessments?

A) Ensures 100% system security

B) Identifies and prioritizes security weaknesses

C) Simplifies incident response processes

D) Reduces encryption overhead

Answer:

B) Identifies and prioritizes security weaknesses

Explanation: Vulnerability assessments highlight system flaws that need remediation.

Question 194:
What is the primary goal of an information security audit?

A) Detect system vulnerabilities

B) Ensure compliance with security policies and regulations

C) Block unauthorized access

D) Recover lost data

Answer:

B) Ensure compliance with security policies and regulations

Explanation: Information security audits assess adherence to established security standards.

Question 215:
What type of attack is carried out by overwhelming a network resource with more requests than it can handle?

A) Man-in-the-Middle

B) Denial-of-Service (DoS)

C) Cross-Site Scripting (XSS)

D) Replay Attack

Answer:

B) Denial-of-Service (DoS)

Explanation: DoS attacks overload a target with excessive requests, rendering it unavailable to legitimate users.

Question 216:
Which attack involves redirecting a user from a legitimate website to a malicious one?

A) DNS Poisoning

B) SQL Injection

C) Phishing

D) Credential Stuffing

Answer:

A) DNS Poisoning

Explanation: DNS Poisoning manipulates DNS records to redirect users to malicious sites.

Question 217:
What is the primary goal of a phishing attack?

A) Disrupt network services

B) Steal sensitive information by tricking users

C) Exploit software vulnerabilities

D) Gain unauthorized remote access

Answer:

B) Steal sensitive information by tricking users

Explanation: Phishing tricks users into providing sensitive information like passwords or financial data.

Question 218:
What is the purpose of a honeypot in network security?

A) To isolate critical systems

B) To lure attackers and study their behavior

C) To encrypt sensitive data

D) To block malware

Answer:

B) To lure attackers and study their behavior

Explanation: Honeypots attract malicious actors, helping organizations understand and mitigate threats.

Question 219:
What is a core component of a Public Key Infrastructure (PKI)?

A) Firewall

B) Certificate Authority (CA)

C) VPN

D) Security Token

Answer:

B) Certificate Authority (CA)

Explanation: A CA is responsible for issuing and managing digital certificates in a PKI system.

Question 220:
Which principle ensures that no single individual has complete control over a critical task?

A) Least Privilege

B) Separation of Duties

C) Defense in Depth

D) Zero Trust

Answer:

B) Separation of Duties

Explanation: Separation of duties prevents misuse by dividing responsibilities among multiple individuals.

Question 221:
What type of authentication uses something you know and something you have?

A) Password-only Authentication

B) Two-Factor Authentication

C) Biometric Authentication

D) Token-Based Authentication

Answer:

B) Two-Factor Authentication

Explanation: Two-factor authentication combines two different types of credentials for secure access.

Question 222:
Which wireless encryption protocol is considered outdated and insecure?

A) WPA3

B) WPA2

C) WPA

D) WEP

Answer:

D) WEP

Explanation: Wired Equivalent Privacy (WEP) is weak and vulnerable to attacks.

Question 223:
What is the main purpose of a Virtual Private Network (VPN)?

A) To improve network speed

B) To provide secure communication over untrusted networks

C) To enforce access control policies

D) To store encryption keys

Answer:

B) To provide secure communication over untrusted networks

Explanation: VPNs create encrypted tunnels for secure remote communication.

Question 224:
What is a key objective during the containment phase of incident response?

A) Identify the root cause of the incident

B) Prevent further spread of the attack

C) Notify affected stakeholders

D) Restore normal operations

Answer:

B) Prevent further spread of the attack

Explanation: Containment focuses on isolating the threat to protect unaffected systems.

Question 225:
Which tool is most commonly used for network packet capture?

A) Nessus

B) Splunk

C) Wireshark

D) Metasploit

Answer:

C) Wireshark

Explanation: Wireshark is a popular tool for capturing and analyzing network packets.

Question 226:
What is the purpose of performing a post-incident review?

A) To identify vulnerabilities and prevent recurrence

B) To ensure evidence is preserved

C) To update disaster recovery plans

D) To encrypt sensitive data

Answer:

A) To identify vulnerabilities and prevent recurrence

Explanation: Post-incident reviews analyze incidents to strengthen security and prevent future issues.

Question 227:
What does the concept of 'due diligence' imply in cybersecurity?

A) Encrypting all network traffic

B) Taking reasonable steps to ensure compliance and security

C) Conducting penetration testing

D) Regularly updating software

Answer:

B) Taking reasonable steps to ensure compliance and security

Explanation: Due diligence involves implementing security measures to protect assets and comply with regulations.

Question 228:
Which compliance framework applies to the healthcare industry in the United States?

A) GDPR

B) HIPAA

C) PCI DSS

D) FISMA

Answer: B) HIPAA

Explanation: The Health Insurance Portability and Accountability Act (HIPAA) protects sensitive healthcare data.

Question 229:
What is the primary purpose of a risk assessment?

A) To eliminate all risks

B) To identify and prioritize potential threats

C) To encrypt sensitive information

D) To monitor network traffic

Answer:

B) To identify and prioritize potential threats

Explanation: Risk assessments evaluate potential threats to determine mitigation strategies.

Domain 1: Threats, Attacks, and Vulnerabilities General Threats

Question 230:
What is the primary goal of a Denial-of-Service (DoS) attack?

A) Steal user credentials

B) Disrupt system availability

C) Exploit system vulnerabilities

D) Encrypt user files

Answer:

B) Disrupt system availability

Explanation: DoS attacks aim to make resources unavailable by overwhelming them with traffic.

Question 231:
Which attack involves tricking users into revealing sensitive information?

A) Phishing

B) Man-in-the-middle

C) SQL injection

D) Credential stuffing

Answer:

A) Phishing

Explanation: Phishing is a social engineering technique used to obtain sensitive information like usernames and passwords.

Question 232:
Which type of malware disguises itself as legitimate software?

A) Rootkit

B) Worm

C) Trojan

D) Ransomware

Answer:

C) Trojan

Explanation: Trojans are malicious programs that appear legitimate but perform harmful actions.

Question 233:
What is the purpose of a buffer overflow attack?

A) To extract data from the system

B) To overload the memory of an application

C) To encrypt sensitive information

D) To redirect network traffic

Answer:

B) To overload the memory of an application

Explanation: Buffer overflows occur when a program writes more data to a buffer than it can hold, potentially leading to arbitrary code execution.

Question 234:
Which of the following is a characteristic of Advanced Persistent Threats (APTs)?

A) Short-term, high-impact attacks

B) Long-term, stealthy operations

C) Opportunistic attacks

D) Randomized malware campaigns

Answer:

B) Long-term, stealthy operations

Explanation: APTs are sophisticated, continuous attacks targeting specific organizations.

Domain 2: Architecture and Design Network Architecture

Question 235:
What is the primary purpose of a firewall?

A) Encrypt data

B) Block unauthorized access

C) Detect intrusions

D) Monitor user activity

Answer:

B) Block unauthorized access

Explanation: Firewalls enforce rules to block or allow traffic based on security policies.

Question 236:
Which design principle ensures that a system can withstand attacks and continue to operate?

A) Least privilege

B) Fault tolerance

C) Defense in depth

D) Secure by design

Answer:

B) Fault tolerance

Explanation: Fault tolerance ensures continued operation even when components fail.

Question 237:
What is the function of a VLAN in a network?

A) Securely connect remote users

B) Isolate traffic within the same physical network

C) Encrypt sensitive data

D) Provide network redundancy

Answer:

B) Isolate traffic within the same physical network

Explanation: VLANs create separate broadcast domains within the same network infrastructure.


SkillWeed