CompTIA Security+ SY0-701

Practice Questions

Date of Issue: 2024

By ExamNav

The CompTIA Security+ certification (SY0-701) is an updated, globally recognized credential that validates the fundamental skills and knowledge required to perform core security functions and pursue a career in IT security. This course is designed to prepare participants for the CompTIA Security+ (SY0-701) exam, focusing on the latest cybersecurity concepts, techniques, and best practices. It encompasses an in-depth understanding of various domains essential for securing organizations and mitigating risks.

---

1. Which of the following is an example of a cryptographic attack that relies on finding two different inputs that produce the same hash value?

- A) Dictionary attack
- B) Brute force attack
- C) Birthday attack
- D) Rainbow table attack

Answer: C) Birthday attack
Explanation: A birthday attack exploits the mathematics behind the birthday paradox in probability theory. It aims to find two different inputs that produce the same hash value, which is a type of collision attack.

2. Which protocol is primarily used for securing communication between email servers?

- A) HTTPS
- B) TLS
- C) S/MIME
- D) STARTTLS

Answer: D) STARTTLS
Explanation: STARTTLS is an email protocol command used to upgrade a plain text connection to

an encrypted (TLS or SSL) connection, commonly used for securing communication between email servers.

3. What type of malware is specifically designed to provide unauthorized access to or control of a device without being detected by antivirus programs?

- A) Virus
- B) Trojan
- C) Rootkit
- D) Worm

Answer: C) Rootkit
Explanation: A rootkit is a type of malware designed to gain unauthorized access to a computer system and remain hidden from security software.

4. Which type of attack involves an attacker intercepting communication between two parties and altering the communication without their knowledge?

- A) Replay attack
- B) Man-in-the-middle attack
- C) Phishing attack
- D) Denial of Service (DoS) attack

Answer: B) Man-in-the-middle attack
Explanation: A Man-in-the-Middle (MITM) attack occurs when an attacker secretly intercepts and potentially alters communication between two parties who believe they are directly communicating with each other.

5. Which of the following access control models grants or denies access based on roles assigned to users?

- A) Mandatory Access Control (MAC)
- B) Discretionary Access Control (DAC)
- C) Role-Based Access Control (RBAC)
- D) Attribute-Based Access Control (ABAC)

Answer: C) Role-Based Access Control (RBAC)
Explanation: RBAC is an access control model that grants or denies access based on the roles assigned to users within an organization.

6. Which type of vulnerability allows attackers to execute arbitrary commands on a host operating system through a vulnerable application?

- A) Cross-Site Scripting (XSS)
- B) SQL Injection
- C) Command Injection
- D) Buffer Overflow

Answer: C) Command Injection
Explanation: Command Injection is a vulnerability that allows attackers to execute arbitrary commands on a host operating system through a vulnerable application.

7. Which of the following is a primary function of a SIEM system in cybersecurity?

- A) Intrusion Prevention
- B) Log Aggregation and Analysis
- C) Data Encryption
- D) Vulnerability Scanning

Answer: B) Log Aggregation and Analysis
Explanation: SIEM (Security Information and Event Management) systems are primarily used for log aggregation, monitoring, and analyzing security events and incidents.

8. What is the purpose of the Security Assertion Markup Language (SAML)?

- A) To encrypt network traffic
- B) To provide secure user authentication
- C) To perform data backups
- D) To establish secure VPN connections

Answer: B) To provide secure user authentication
Explanation: SAML (Security Assertion Markup Language) is an XML-based framework used for exchanging authentication and authorization data between security domains, typically used in Single Sign-On (SSO) scenarios.

9. Which type of backup method only saves files that have changed since the last full backup?

- A) Full backup
- B) Differential backup
- C) Incremental backup
- D) Snapshot

Answer: B) Differential backup
Explanation: A differential backup saves files that have changed since the last full backup. Unlike an incremental backup, it does not reset the archive bit.

10. In Public Key Infrastructure (PKI), what does the acronym CA stand for?

- A) Central Authority
- B) Certificate Authority
- C) Certification Agency
- D) Cybersecurity Authority

Answer: B) Certificate Authority
Explanation: CA stands for Certificate Authority, which is an entity responsible for issuing, managing, and revoking digital certificates in a PKI system.

11. What is the main purpose of a honeypot in a cybersecurity context?

- A) To detect malware
- B) To entice attackers and study their behavior
- C) To encrypt sensitive data
- D) To provide secure remote access

Answer: B) To entice attackers and study their behavior
Explanation: A honeypot is a decoy system used to attract attackers to study their tactics, techniques, and procedures (TTPs).

12. Which type of encryption uses the same key for both encryption and decryption?

- A) Asymmetric encryption
- B) Hashing
- C) Symmetric encryption
- D) One-time pad

Answer: C) Symmetric encryption
Explanation: Symmetric encryption uses the same key for both encryption and decryption, making it faster but requiring secure key distribution.

13. What is the primary function of a demilitarized zone (DMZ) in network security?

- A) To encrypt internal traffic
- B) To segment a network and reduce internal traffic
- C) To provide a buffer zone between internal and external networks
- D) To enforce security policies on internal traffic

Answer: C) To provide a buffer zone between internal and external networks
Explanation: A DMZ is a network area that acts as a buffer zone between a trusted internal network and an untrusted external network, such as the internet.

14. Which of the following is a technique used to prevent unauthorized users from identifying internal network structure?

- A) VLAN tagging
- B) Network Address Translation (NAT)
- C) VPN tunneling
- D) Port forwarding

Answer: B) Network Address Translation (NAT)
Explanation: NAT hides internal IP addresses from external networks, preventing unauthorized users from identifying internal network structure.

15. Which framework is commonly used for assessing cybersecurity readiness and managing risk in an organization?

- A) ISO 9001

- B) COBIT
- C) NIST Cybersecurity Framework
- D) ITIL

Answer: C) NIST Cybersecurity Framework
Explanation: The NIST Cybersecurity Framework provides guidelines for managing cybersecurity risk and improving an organization's cybersecurity posture.

16. Which of the following tools can be used to scan a network for open ports and services?

- A) Nessus
- B) Wireshark
- C) Nmap
- D) Metasploit

Answer: C) Nmap
Explanation: Nmap is a network scanning tool used to discover open ports and services on a network.

17. What is the primary goal of a DDoS (Distributed Denial of Service) attack?

- A) To steal sensitive information
- B) To gain unauthorized access
- C) To overwhelm a network or service and render it unavailable
- D) To execute malware on a target system

Answer: C) To overwhelm a network or service and render it unavailable
Explanation: A DDoS attack aims to overwhelm a target's network or service with traffic, causing it to become unavailable to legitimate users.

18. Which principle of cybersecurity refers to the practice of limiting access to only those resources and data a user needs to perform their job?

- A) Separation of duties
- B) Least Privilege
- C) Need-to-Know
- D) Defense-in-Depth

Answer: B) Least Privilege
Explanation: The principle of Least Privilege dictates that users should only have access to the resources they need to perform their jobs, minimizing potential damage in case of a breach.

19. What is a key advantage of using Multi-Factor Authentication (MFA) in an organization?

- A) It provides redundancy for authentication systems
- B) It ensures all employees use complex passwords
- C) It significantly reduces the risk of unauthorized access
- D) It allows for remote access without additional security measures

Answer: C) It significantly reduces the risk of unauthorized access
Explanation: MFA provides additional layers of security by requiring multiple forms of verification, significantly reducing the risk of unauthorized access.

20. Which of the following methods is used to securely erase data from a storage device?

- A) Formatting
- B) File deletion
- C) Degaussing
- D) Disk fragmentation

Answer: C) Degaussing
Explanation: Degaussing is a method that uses a magnetic field to erase data from storage devices, ensuring the data cannot be recovered.