SSCP Security Exam Prep

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 1509 questions
+ unlimited timed mock exams + mistake book

Practice on the web: https://certs.theorypractice.app/sscp
$2.99 / week · $6.99 / month · cancel anytime

What you unlock: all 1509 questions • unlimited timed mock exams • mistake book • instant explanations

Study offline on the free app — search your exam on the App Store or Google Play

Practice Questions

Try all 30 first, then check the answer key at the back.

1. In the context of incident response, reviewing an organization's data handling policies may be necessary to ensure that information is:

A. confidential.
B. secure.
C. available.
D. protected.

2. At which stage in the incident response process does evidence collection occur?

A. Containment
B. Preparation
C. Identification
D. Evidence Gathering

3. Which characteristic of virtualization technology may make it difficult for cybersecurity teams to trace and mitigate an attack?

A. Isolation
B. Scalability
C. Compatibility
D. Performance

4. Which of the following attributes is NOT necessary for a thorough incident report?

A. Accurate
B. Subjective
C. Comprehensive
D. Verifiable

5. Which type of disaster recovery site is the most cost-effective to set up?

A. Warm site
B. Hot site
C. Cold site
D. Inactive site

6. In the context of business continuity planning, which risk treatment strategy demands the HIGHEST risk tolerance?

A. Mitigate
B. Transfer
C. Accept
D. Avoid

7. Which of the following risk management frameworks was developed by the National Institute of Standards and Technology (NIST)?

A. NIST RMF
B. ISO 27005
C. COBIT
D. ITIL

8. Which type of analysis ensures that existing mitigation strategies remain effective when a new threat is identified?

A. Initial risk assessment
B. Risk re-assessment
C. Risk aversion
D. Threat validation

9. Which of the following is NOT a phase in the NIST Risk Management Framework (RMF)?

A. Prepare
B. Continuous improvement
C. Select
D. Monitor

10. How many phases are included in the NIST Risk Management Framework?

A. 5
B. 3
C. 4
D. 6

11. Which type of access control is ideal for an organization that requires strict enforcement of security policies and minimal user discretion over permissions?

A. DAC
B. MAC
C. RBAC
D. ABAC

12. Which of the following statements is NOT true about OAuth tokens?

A. They contain information about user permissions.
B. They can be used for API access control.
C. They are used to store passwords.
D. They are issued by an authorization server.

13. Which of the following is NOT a fundamental role of an Identity and Access Management (IAM) system?

A. Authentication
B. Monitoring bandwidth usage
C. Authorization
D. Access provisioning

14. Which type of monitoring system is MOST effective at identifying insider threats based on anomalous user behavior?

A. User Behavior Analytics (UBA)
B. Antivirus Software
C. Firewall
D. Encryption

15. Which access control model is MOST effective for a financial institution needing to comply with stringent regulatory requirements for transaction monitoring and auditing?

A. MAC
B. DAC
C. RBAC
D. ABAC

16. At what level of access control would requiring a multi-factor authentication (MFA) using both a password and a biometric scan fall under when providing remote access to a sensitive system?

A. Level 0
B. Level 1
C. Level 3
D. Level 2

17. Which of the following access models restricts access modes based on defined policies and dynamically considers the current state of the system and related historical information?

A. Graham-Denning
B. Clark-Wilson
C. Gogun-Meseguer
D. Brewer and Nash

18. SSL/TLS's trust model is BEST described as which of the following?

A. Network of trust
B. Web of trust
C. Chain of trust
D. Hierarchy of trust

19. In the context of information security, which of the following terms is the MOST comprehensive?

A. Information Security
B. Cybersecurity
C. Information Assurance
D. All terms are equally comprehensive.

20. In the context of the CIA triad, which of the following principles ensures that data remains unaltered during storage or transit?

A. Non-Repudiation
B. Confidentiality
C. Availability
D. Integrity

21. When a courier service provides a delivery option that requires the recipient to sign upon receipt, what type of security control is being implemented?

A. Nonrepudiation
B. Confidentiality
C. Privacy
D. Integrity

22. Which of the following IP address types might indicate a security issue if observed frequently on an internal network?

A. 10.x.x.x
B. 192.168.x.x
C. 169.254.x.x
D. 172.16.x.x

23. Which of the following protocols does NOT run over UDP?

A. TFTP
B. DNS
C. SNMP
D. FTP

24. Which of the following is NOT a core component of network segmentation?

A. Virtual LANs (VLANs)
B. Firewalls
C. Decryption
D. Access Control Lists (ACLs)

25. Which type of wireless attack might be used to inject malicious data packets into a Wi-Fi network?

A. Man-in-the-middle
B. Packet injection
C. War driving
D. Signal jamming

26. Which of the following standards defines a security protocol for wireless networks?

A. IEEE 802.11i
B. IEEE 802.3
C. IEEE 802.16
D. IEEE 802.15

27. Which of the following network intrusion detection techniques is specifically designed for detecting attacks based on predefined patterns?

A. Heuristic-Based Detection
B. Anomaly-Based Detection
C. Signature-Based Detection
D. Behavior-Based Detection

28. Which of the following does NOT specify disallowed traffic on a network?

A. Blocklisting
B. Allowlisting
C. Disallowed IP ranges
D. Negative control

29. Which type of network attack can propagate without requiring any user interaction?

A. Worm
B. Virus
C. Spyware
D. Adware

30. Which of the following mechanisms is BEST suited to identifying an attacker attempting to exfiltrate sensitive data from a compromised system?

A. Endpoint Behavioral Modeling
B. User Behavioral Modeling
C. Access Control
D. Security Logs

Answer Key & Explanations

1. D — protected.
Answer: protected. Information needs to be: - Secure - Confidential - Available - Protected Reviewing policies helps ensure data handling practices align with legal requirements and industry standards to provide comprehensive data protection.

2. D — Evidence Gathering
Answer: Evidence Gathering The incident response process includes the following stages: Preparation: Developing and implementing an incident response capability. Identification: Detecting and acknowledging the occurrence of an incident. Evidence Gathering: Collecting relevant data and securing evidence. Containment: Mitigating the spread and damage from the incident. Eradication: Removing the incident's cause and affected components. Recovery: Restoring normal operations and confirming system functionality. Lessons Learned: Documenting and analyzing the incident response to improve future preparedness.

3. A — Isolation
Answer: Isolation Certain attributes of virtualization technology that can complicate cybersecurity efforts include: Isolation: Virtual machines are often designed to be isolated from each other for security purposes. This isolation can make it challenging to trace the origin or path of an attack within a virtualized environment. Scalability: While virtualization allows for rapid scaling of resources, tracking and managing security across a swiftly changing environment can be complex. Compatibility: Differences in hypervisors and virtual machine configurations can create compatibility issues that hinder unified security protocols. Performance: The abstraction layers in virtualization can sometimes obscure performance issues that may be indicative of malicious activities.

4. B — Subjective
Answer: Subjective An effective incident report needs to be: Attribute Accurate Comprehensive Verifiable Timely Clear Although it is important to document observations during an incident, the report itself should be based on factual, objective information rather than subjective opinions. Including subjective data can lead to bias and may undermine the reliability of the report.

5. C — Cold site
Answer: Cold site Hot sites are fully operational environments where all critical systems and processes are kept in sync with the primary site. These are the most expensive to maintain. Cold sites, on the other hand, are physical locations that only provide the infrastructure without any current data or systems running. They are the least costly to set up because they involve minimal upkeep. Warm sites offer a compromise, providing some infrastructure and data synchronization, making them moderately expensive. The term inactive site is not a recognized category in disaster recovery terminology.

6. C — Accept
Correct answer: Accept The risk treatment strategies in the context of business continuity planning are typically as follows: Strategy Description **Accept** Acknowledge the risk and do nothing about it, which requires the highest risk tolerance. **Transfer** Assign responsibility for a risk to another party, such as an

insurance provider. **Mitigate** Take steps to reduce or eliminate the risk, such as implementing redundant systems or improving access controls. **Avoid** Cease the activity or disuse the system that introduces the risk.

7. A — NIST RMF
Answer: NIST RMF The NIST Risk Management Framework (RMF) is a comprehensive, flexible, risk-based approach developed by the National Institute of Standards and Technology for integrating security and risk management activities into the system development lifecycle. This helps organizations meet federal requirements for securing information systems. ISO 27005 is an international standard that provides guidelines for information security risk management. COBIT (Control Objectives for Information and Related Technologies) is a framework created by ISACA for IT management and governance. ITIL (Information Technology Infrastructure Library) focuses on aligning IT services with the needs of the business.

8. B — Risk re-assessment
Risk re-assessment ensures that existing mitigation strategies are still effective when new threats are identified. Initial risk assessment is performed before mitigation strategies are applied. Risk aversion and threat validation are not standard terms in this context.

9. B — Continuous improvement
Answer: Continuous improvement The NIST Risk Management Framework (RMF) consists of six steps: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. Continuous improvement is not one of the phases in the RMF.

10. D — 6
Answer: 6 The NIST Risk Management Framework (RMF) consists of 6 phases, which include: Categorize, Select, Implement, Assess, Authorize, and Monitor.

11. B — MAC
Answer: MAC Mandatory Access Control (MAC) centrally manages control over files, applications, directories, etc., and denies users the ability to manage access to their own assets. Discretionary Access Control (DAC) is the access control model built into most operating systems and allows the owner of an asset to manage privileges associated with it. Role-Based Access Control (RBAC) assigns access and permissions based upon an entity's role within the organization, making it easier to implement least privilege and separation of duties. Attribute-Based Access Control (ABAC) assigns sets of attributes to each entity. Access control rules are implemented using Boolean logic that describes the combinations of attributes needed to access a resource or perform a particular action.

12. C — They are used to store passwords.
Answer: They are used to store passwords. OAuth tokens are used to grant access to resources without sharing credentials. They do not store passwords but rather act as a means to verify user identity and permissions.

13. B — Monitoring bandwidth usage
Answer: Monitoring bandwidth usage Identity and Access Management (IAM) systems primarily focus on managing digital identities and determining access rights for individuals within an organization. The core roles of IAM include: IAM Role Description **Authentication** Verifying the identity of a user. **Authorization** Determining the access permissions a user has once authenticated. **Access provisioning** Assigning and managing user permissions effectively. Monitoring bandwidth usage is a function more relevant to network

management and not a primary role of IAM systems.

14. A — User Behavior Analytics (UBA)
User Behavior Analytics (UBA) involves tracking user behaviors and looking for deviations from the norm, which can help to detect potential insider threats. For example, unusual access patterns or data downloads could indicate malicious activities.

15. A — MAC
Correct answer: MAC Mandatory Access Control (MAC) centrally manages control over assets and does not allow users to manage access permissions themselves. This ensures compliance with strict regulatory requirements by controlling all access rules centrally. Discretionary Access Control (DAC) allows owners of resources to manage permissions, which can lead to inconsistent enforcement of policies. Role-Based Access Control (RBAC) grants permissions based on roles within the organization, which can improve the implementation of the least privilege but might not meet the high-security and audit requirements as effectively as MAC. Attribute-Based Access Control (ABAC) provides fine-grained access control through attributes but may be complex to manage and enforce regulatory compliance uniformly in highly sensitive environments.

16. D — Level 2
The access control levels for remote access to sensitive systems are as follows: Access Control Level Description Level 1 Basic authentication such as a username and password. Level 2 Enhanced authentication including multi-factor authentication (e.g., password & biometric scan). Level 3 Strictest control involving physical tokens or smart cards in combination with other factors. Level 0 No access control implemented. Requiring multi-factor authentication (MFA) using both a password and a biometric scan corresponds to Level 2. Level 2 access controls provide a higher assurance by validating the user's identity using multiple factors, thereby enhancing security.

17. D — Brewer and Nash
Answer: Brewer and Nash The Brewer and Nash (Chinese Wall) access model dynamically considers a subject's current state and historical information to make access decisions, preventing conflicts of interest. The Clark-Wilson model focuses on ensuring that information is accessed by authorized users and in an authorized manner. The Gogun-Meseguer model defines security domains to prevent interference between groups, but it does not consider historical information. The Graham-Denning model is concerned with controlling the rights to create, delete, read, or write objects and subjects.

18. D — Hierarchy of trust
Answer: Hierarchy of trust In a hierarchy of trust, an anchor node delegates its authority and trust to other nodes. PKI (Public Key Infrastructure) systems, including SSL/TLS, are designed as hierarchies of trust with the root CA (Certificate Authority) as the anchor node. A chain of trust exists between a root CA and a particular end entity. In a web of trust, no anchor nodes exist, and chains of trust are created via peer-to-peer relationships. The term 'network of trust' is a fabricated term.

19. C — Information Assurance
Answer: Information Assurance Information Assurance is an umbrella term that encompasses the protection and defense of information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Cybersecurity focuses on defending against cyber threats, while Information Security primarily deals with the protection of information assets. Therefore, Information Assurance is the most comprehensive.

20. D — Integrity
Answer: Integrity The CIA triad stands for: - Confidentiality: Limiting who has access to data - Integrity: Ensuring that data remains unaltered and is accurate during storage or transit. - Availability: Ensuring that data is available in a timely manner and usable format - Non-Repudiation: Preventing someone from denying that they took an action

21. A — Nonrepudiation
Nonrepudiation is ensured when the recipient signs upon receiving a package from a courier service, making it infeasible for the recipient to deny having received it.

22. C — 169.254.x.x
The correct answer is 169.254.x.x. This range is used for Automatic Private IP Addressing (APIPA), which means the device could not obtain an IP address from the DHCP server, indicating a possible network configuration or connectivity issue. The ranges 192.168.x.x, 10.x.x.x, and 172.16.x.x are private IP address ranges typically used in corporate networks.

23. D — FTP
Answer: FTP FTP is a protocol that runs over TCP, which ensures reliable data transfer. DNS, SNMP, and TFTP are protocols that run over UDP, which is a lighterweight protocol.

24. C — Decryption
Answer: Decryption. Network segmentation primarily involves components such as firewalls, Virtual LANs (VLANs), and Access Control Lists (ACLs) to control and manage network traffic, but not decryption.

25. B — Packet injection
Answer: Packet injection. Packet injection involves inserting malicious packets into a Wi-Fi network. Man-in-the-middle attacks intercept and potentially alter the communication between two parties. War driving involves searching for Wi-Fi networks while driving around. Signal jamming disrupts wireless communication by overwhelming the network with noise or other signals.

26. A — IEEE 802.11i
Answer: IEEE 802.11i IEEE 802.11i is a standard that defines a security protocol for wireless networks, commonly known as WPA2, which provides robust security mechanisms for wireless communication. IEEE 802.3 is an Ethernet standard that governs wired LAN technologies. IEEE 802.16, also known as WiMAX, defines wireless broadband standards. IEEE 802.15 focuses on wireless personal area networks (WPANs).

27. C — Signature-Based Detection
Answer: Signature-Based Detection Network Intrusion Detection Systems (NIDS) can utilize various methods to identify potential attacks, including: Technique Description Signature-Based Detection Uses predefined patterns or rules to identify known threats. Anomaly-Based Detection Establishes a baseline of normal network behavior and identifies deviations that may indicate attacks. Heuristic-Based Detection Uses algorithms to detect suspicious activity by examining behaviors and assessing their potential threats. Behavior-Based Detection Monitors the behavior of system components to identify actions that deviate from expected norms.

28. B — Allowlisting
Answer: Allowlisting Negative control or blocklisting specifies what should be blocked, creating a "default deny" policy. Examples of common negative controls include: 1. IP blocklists 2. Disallowed URLs 3. Malware

signatures Positive control or allowlisting specifies what should be allowed through, creating a "default deny" policy by assuming all other traffic is disallowed unless stated otherwise. Examples of common positive controls include: 1. Network allowlists 2. IP whitelists 3. Application control lists

29. A — Worm
Answer: Worm Worms are capable of spreading themselves across networks without any user interaction. Viruses typically require some kind of user action to propagate, such as opening an infected file. Spyware is used to gather information from a user's system without their knowledge, often requiring some form of user action for initial infection. Adware generates revenue by displaying ads to users, often requiring user action to install the software that displays these ads.

30. C — Access Control
Answer: Access Control Malicious activity on a system could be detected in a few different ways, such as: User Behavioral Modeling: User behavioral modeling attempts to identify what is "normal" for a user. Based on this definition of "normal," it can identify potential attacks as deviations from "normal" behavior. For example, unusual data transfer activities (especially without authorization) may indicate a compromised account. Endpoint Behavioral Modeling: Endpoints also have "normal" and "abnormal" behavior that can be used to detect attacks. For example, a program generating large amounts of outbound traffic could be a sign of an exfiltration event. Access Control: Attackers commonly attempt to abuse the access of a compromised account and potentially exfiltrate sensitive data without authorization. Access control systems can alert on anomalous or unauthorized data transfer attempts that point to a compromised account. Security Logs: Endpoints, security solutions, and other tools will generate log files that record important events that occurred on the system. This could include events that point to data exfiltration attempts or other security events. Exfiltration of sensitive data commonly involves abusing an account's permissions or compromising new accounts to gain access to valuable information. Access control systems can help to detect and prevent these exfiltration attempts.

Ready to pass?

Unlock the full SSCP Security Exam Prep bank, every explanation, and unlimited timed mock exams.

Scan to start practising
https://certs.theorypractice.app/sscp

Also on iOS & Android — search your exam name on the App Store or Google Play