CCOA Cyber Analyst Prep

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 505 questions
+ unlimited timed mock exams + mistake book

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

What you unlock: all 505 questions • unlimited timed mock exams • mistake book • instant explanations

Also on iOS & Android — and watch the full Q&A walkthrough on YouTube @CertsQuizPrep

Practice Questions

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

1. Which phase of the Cyber Kill Chain involves an attacker gathering information about the target organization?

A. Exploitation
B. Installation
C. Command and Control
D. Reconnaissance

2. What technique do threat actors commonly use to maintain persistence after gaining initial access to a system?

A. Initial exploitation only
B. Immediate data exfiltration
C. Creating backdoors
D. Performing reconnaissance

3. Which of the following best describes a watering hole attack?

A. Using social engineering to obtain credentials directly from users
B. Compromising websites frequently visited by the target to deliver malware
C. Sending mass phishing emails to many potential victims
D. Attacking water utility infrastructure systems

4. What is the primary purpose of lateral movement in an attack sequence?

A. To gain access to additional systems within the network after initial compromise
B. To establish the initial foothold in a network
C. To exfiltrate data from the network
D. To remove evidence of the attack

5. Which of the following frameworks categorizes adversary tactics and techniques to help organizations understand attack methodologies?

A. ISO 27001
B. NIST CSF
C. OWASP Top 10
D. MITRE ATT&CK

6. What type of malware delivery vector involves exploiting vulnerabilities in legitimate websites to infect visitors?

A. Malvertising
B. USB baiting
C. Drive-by download
D. Spear phishing

7. Which technique involves an attacker using a compromised email account to trick recipients into believing an email is legitimate?

A. SQL Injection
B. Business Email Compromise
C. DNS Cache Poisoning
D. ARP Spoofing

8. What is the primary goal of a threat actor's exfiltration procedures?

A. To transfer stolen data out of the target network while avoiding detection
B. To install additional malware on the network
C. To damage systems and make them inoperable
D. To recruit insiders for future attacks

9. Which attack technique involves capturing authentication credentials as they pass between client and server?

A. Brute force attack
B. SQL injection
C. Zero-day exploit
D. Man-in-the-Middle attack

10. What technique do attackers use to evade detection by modifying their malware's signature or behavior?

A. Social engineering
B. Brute force attacks
C. Polymorphic malware
D. Port scanning

11. Which of the following is a common method for threat actors to escalate privileges after gaining initial access?

A. Implementing network segmentation
B. Exploiting unpatched vulnerabilities
C. Installing anti-virus software
D. Enabling multi-factor authentication

12. What technique involves hackers using legitimate administrative tools to conduct malicious activities?

A. Living off the land
B. Social engineering
C. Brute force attacks
D. DNS tunneling

13. Which of the following best describes a supply chain attack?

A. Directly attacking an organization's network perimeter
B. Conducting DDoS attacks against cloud service providers
C. Exploiting vulnerabilities in public-facing web applications
D. Compromising a trusted vendor to distribute malware through legitimate software updates

14. What is the purpose of data staging in the exfiltration process?

A. To permanently delete the original data
B. To modify system logs to hide evidence
C. To collect and prepare stolen data in a central location before transferring it out of the network
D. To encrypt the stolen data

15. Which threat actor capability allows attackers to maintain control over compromised systems?

A. Social engineering
B. Command and Control infrastructure
C. Vulnerability scanning
D. Password cracking

16. What technique do attackers use to hide communication with their command and control servers?

A. DNS tunneling
B. Network segmentation
C. Intrusion prevention
D. Firewall implementation

17. Which attack vector involves manipulating a user into taking actions that benefit the attacker?

A. SQL injection
B. Buffer overflow
C. Cross-site scripting
D. Social engineering

18. What is the primary purpose of credential dumping in an attack sequence?

A. To identify vulnerabilities in applications
B. To encrypt sensitive data on the system
C. To extract stored credentials from a compromised system for use in lateral movement
D. To create new administrative accounts

19. Which technique involves attackers maintaining long-term, stealthy access to a target network?

A. Crypto-jacking
B. Advanced Persistent Threat (APT)
C. Distributed Denial of Service (DDoS)
D. Ransomware attack

20. What technique do attackers use to identify potential entry points into a target network?

A. Port scanning
B. Data exfiltration
C. Lateral movement
D. Privilege escalation

21. Which incident response phase involves restoring systems to normal operations and ensuring no residual threats remain?

A. Identification
B. Preparation
C. Eradication
D. Recovery

22. What is the primary purpose of an incident response playbook?

A. To automatically remediate all security incidents
B. To satisfy compliance requirements only
C. To provide standardized procedures for handling specific types of incidents
D. To replace the need for skilled incident responders

23. During incident triage, which of the following is the MOST important factor to assess first?

A. Legal implications
B. Scope and impact of the incident
C. Identity of the threat actor
D. Cost of remediation

24. Which of the following is NOT typically part of the containment phase of incident response?

A. Performing root cause analysis
B. Isolating affected systems
C. Blocking malicious IP addresses
D. Disabling compromised accounts

25. Which document typically defines roles, responsibilities, and procedures for responding to security incidents?

A. Business Continuity Plan
B. Disaster Recovery Plan
C. Security Policy
D. Incident Response Plan

26. What is the purpose of maintaining a chain of custody during incident response?

A. To assign blame to responsible employees
B. To meet compliance requirements only
C. To ensure evidence integrity and admissibility in legal proceedings
D. To track the cost of the incident response effort

27. Which tool is BEST suited for collecting and analyzing log data from multiple sources during incident investigation?

A. Network sniffer
B. SIEM (Security Information and Event Management)
C. Firewall
D. Antivirus software

28. During which phase of incident response should system backups be created before making changes?

A. Containment
B. Preparation
C. Recovery
D. Eradication

29. What is an Indicator of Compromise (IoC)?

A. A measure of how severely an incident has impacted operations
B. A rating system for categorizing incident severity
C. A tool used to identify vulnerabilities before they're exploited
D. Forensic evidence suggesting a security breach has occurred

30. Which of the following is a key component of post-incident analysis?

A. Terminating responsible employees
B. Migrating to new systems
C. Conducting lessons learned sessions
D. Deploying new security tools

Answer Key & Explanations

1. D — Reconnaissance
Reconnaissance is the first phase of the Cyber Kill Chain where attackers collect information about their targets through various methods such as scanning networks, social engineering, or open-source intelligence gathering.

2. C — Creating backdoors
Creating backdoors is a common persistence technique that allows attackers to maintain access to compromised systems even if their initial access point is discovered and remediated.

3. B — Compromising websites frequently visited by the target to deliver malware
A watering hole attack involves compromising websites that target victims are known to visit, rather than attacking them directly. This allows attackers to infect specific groups of users who trust these legitimate websites.

4. A — To gain access to additional systems within the network after initial compromise
After gaining initial access, attackers use lateral movement to expand their control by moving from one compromised system to others within the network, searching for valuable assets or higher privileges.

5. D — MITRE ATT&CK
MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations, providing a framework for understanding how threat actors operate.

6. C — Drive-by download
Drive-by downloads occur when users visit compromised websites that contain malicious code that automatically downloads and executes without the user's knowledge or consent by exploiting browser or plugin vulnerabilities.

7. B — Business Email Compromise
Business Email Compromise (BEC) involves attackers compromising or spoofing business email accounts to conduct unauthorized transfers of funds, steal data, or gain access to other systems by exploiting established trust relationships.

8. A — To transfer stolen data out of the target network while avoiding detection
The primary goal of exfiltration is to transfer stolen data out of the target network to an attacker-controlled location while avoiding detection by security systems.

9. D — Man-in-the-Middle attack
Man-in-the-Middle attacks involve intercepting network traffic between two parties, allowing attackers to eavesdrop and capture sensitive information like credentials without either party knowing.

10. C — Polymorphic malware
Polymorphic malware continuously changes its code and signature to appear different each time it runs,

making it difficult for signature-based detection systems to identify it as malicious.

11. B — Exploiting unpatched vulnerabilities
Exploiting unpatched vulnerabilities is a common method for privilege escalation, as these security flaws can allow attackers to gain administrative or system-level access from a lower-privileged account.

12. A — Living off the land
Living off the land involves using legitimate system tools and features (like PowerShell, WMI, or PsExec) for malicious purposes, making attacks harder to detect since they leverage trusted system processes.

13. D — Compromising a trusted vendor to distribute malware through legitimate software updates
A supply chain attack compromises software vendors or suppliers to insert malicious code into legitimate software updates or products, allowing attackers to gain access to all organizations using those products.

14. C — To collect and prepare stolen data in a central location before transferring it out of the network
Data staging involves collecting and organizing stolen data in a central location within the victim's network before exfiltration, allowing attackers to efficiently transfer larger amounts of data and potentially avoid detection.

15. B — Command and Control infrastructure
Command and Control infrastructure enables attackers to remotely communicate with and control compromised systems, allowing them to issue commands, update malware, and manage their attack operations.

16. A — DNS tunneling
DNS tunneling encapsulates other protocols within DNS queries and responses to establish covert communication channels, making malicious traffic appear as legitimate DNS traffic to evade detection.

17. D — Social engineering
Social engineering manipulates users through psychological tactics rather than technical means, tricking them into performing actions or divulging confidential information that aids the attacker's objectives.

18. C — To extract stored credentials from a compromised system for use in lateral movement
Credential dumping extracts passwords, hashes, or authentication tokens from a system's memory or storage, allowing attackers to obtain valid credentials for lateral movement and privilege escalation.

19. B — Advanced Persistent Threat (APT)
Advanced Persistent Threats involve sophisticated attackers who establish a long-term presence within a target network, focusing on remaining undetected while slowly mapping the network and extracting valuable data over time.

20. A — Port scanning
Port scanning systematically probes network ports to discover available services, potential vulnerabilities, and open communication channels that could serve as entry points for attackers.

21. D — Recovery
The recovery phase focuses on bringing affected systems back to normal operation while ensuring they are free from compromise and residual threats.

22. C — To provide standardized procedures for handling specific types of incidents
Incident response playbooks provide standardized, documented procedures for handling specific types of security incidents, ensuring consistency and completeness in the response process.

23. B — Scope and impact of the incident
The scope and impact of an incident should be assessed first during triage to understand how widespread the incident is and what critical systems or data might be affected, which helps prioritize response efforts.

24. A — Performing root cause analysis
Root cause analysis is performed during the post-incident analysis phase, not during containment. Containment focuses on limiting the damage and preventing further spread of the incident.

25. D — Incident Response Plan
An Incident Response Plan (IRP) formally defines the roles, responsibilities, and procedures that should be followed when responding to security incidents.

26. C — To ensure evidence integrity and admissibility in legal proceedings
Chain of custody documentation ensures evidence integrity by tracking who handled evidence, when, and why, which is crucial if the incident leads to legal proceedings.

27. B — SIEM (Security Information and Event Management)
SIEM (Security Information and Event Management) systems are specifically designed to collect, correlate, and analyze log data from multiple sources, making them ideal for incident investigation.

28. A — Containment
Creating system backups before making changes is a critical step in the containment phase to preserve evidence and allow for recovery if containment actions have unintended consequences.

29. D — Forensic evidence suggesting a security breach has occurred
Indicators of Compromise are forensic artifacts or evidence that suggest a system security breach or intrusion has occurred, such as unusual outbound network traffic or unexpected registry changes.

30. C — Conducting lessons learned sessions
Lessons learned sessions identify what went well and what could be improved in the incident response process, helping to enhance future responses.

Ready to pass?

Unlock the full CCOA Cyber Analyst Prep bank, every explanation, and unlimited timed mock exams.

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

Watch the full video walkthrough on YouTube @CertsQuizPrep