Eccouncil

312-50v13

Certified Ethical Hacker Exam (CEH v13 AI)

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**



Latest Version: 6.0

Question: 1

Which advanced session hijacking technique is hardest to detect and mitigate in a remote-access environment?

A. Session sidejacking over public Wi-Fi
B. ARP spoofing on local networks
C. Brute-force session guessing
D. Cookie poisoning

Answer: B

Explanation:
ARP spoofing–based session hijacking is identified in CEH v13 Web Application and Network Attacks as one of the most stealthy and difficult-to-detect session compromise techniques, especially within internal or VPN-connected networks.
In ARP spoofing, attackers poison ARP caches to position themselves as a man-in-the-middle (MitM). Once in place, they can silently intercept, modify, or replay session data—even when encryption is used—by redirecting traffic transparently between endpoints.
Option A (sidejacking) is mitigated by HTTPS. Option C (session guessing) is noisy and detectable. Option D (cookie poisoning) relies on weak validation and is easier to detect via integrity checks.
CEH v13 highlights ARP spoofing as particularly dangerous because:
It exploits trusted local network behavior
It does not require breaking encryption directly
It is often invisible to users and applications
Therefore, Option B is the most challenging to detect and mitigate and is the correct answer.

Question: 2

During a red team engagement against a multinational financial services organization, an ethical hacker conducts network reconnaissance against externally accessible systems. Instead of sending scan traffic directly from the originating assessment machine, the tester routes all reconnaissance packets through an intermediary external system before they reach the target network.
When the organization's security team reviews monitoring data, the activity appears to originate from infrastructure unrelated to the tester's actual geographic or organizational location.
From a reconnaissance methodology perspective, what is the primary objective of using this intermediary system?

A. To Establish Persistent Access within the Target Network
B. To Bypass Authentication Controls Protecting Internal Applications
C. To Conceal the Origin of Reconnaissance Activity and Reduce Attribution Risk
D. To Spoof Packet Source Addresses at the IP Layer

Answer: C

Explanation:
The correct answer is C. To Conceal the Origin of Reconnaissance Activity and Reduce Attribution Risk. The tester is routing reconnaissance traffic through an intermediary external system so that monitoring logs show the intermediary as the apparent source. The primary objective is operational concealment: making it harder for defenders to attribute the activity to the tester's real machine, organization, or location.
CEH-aligned firewall-evasion material describes bypassing through external systems and related techniques used to make traffic appear to come from another host or pathway rather than the original source .
Option A is incorrect because routing reconnaissance through an intermediary does not by itself establish persistence inside the target network.
Option B is incorrect because the scenario does not describe bypassing application authentication controls.
Option D is incorrect because IP spoofing changes source IP information at the packet level, while the scenario describes routing through an intermediary system that actually forwards the traffic.
Option C is correct because the intermediary system is used to hide the true origin of reconnaissance activity.
Therefore, the best answer is C. To Conceal the Origin of Reconnaissance Activity and Reduce Attribution Risk.

Question: 3

During an internal security assessment of a medium-sized enterprise network, a security analyst notices an unusual spike in ARP traffic. Closer inspection reveals that one particular MAC address is associated with multiple IP addresses across different subnets. The ARP packets were unsolicited replies rather than requests, and several employees from different departments have reported intermittent connection drops, failed logins, and broken intranet sessions. The analyst suspects an intentional interference on the local network segment. What is the most likely cause of this abnormal behavior?

A. ARP poisoning causing routing inconsistencies
B. DHCP snooping improperly configured
C. Legitimate ARP table refresh on all clients
D. Port security restricting all outbound MAC responses

Answer: A

Explanation:
CEH v13 explains that ARP poisoning (also known as ARP spoofing) occurs when an attacker sends forged ARP replies across the network to associate their MAC address with multiple IP addresses, tricking hosts into sending traffic through the attacker's machine. This results in routing inconsistencies, intermittent connectivity, failed logins, and degraded intranet performance—exactly the symptoms described. ARP poisoning typically involves unsolicited ARP replies, which overwrite legitimate ARP cache entries. CEH emphasizes that ARP-based attacks are common on LANs because ARP lacks

authentication, allowing attackers to impersonate gateways or key hosts. DHCP snooping misconfigurations (Option B) affect IP allocation, not ARP mappings. Legitimate ARP refreshes (Option C) are request-based and do not involve flooding unsolicited replies. Port security restrictions (Option D) block MAC anomalies, not create them. Therefore, ARP poisoning is the correct root cause.

Question: 4

You are an ethical hacker at Nexus Cybersecurity, contracted to perform a penetration test for BlueRidge Retail, a US-based e-commerce company in Atlanta, Georgia. While testing their online store's product search page, you attempt to inject a malicious query into the URL to extract customer data. The application is protected by a web application firewall WAF that blocks standard SQL injection attempts. To bypass this, you modify your input to split the query into multiple parts, ensuring the malicious instructions are not detected as a single signature. For example, you craft the URL as products.php?id=1+UNION+SE+LECT+1,2, which successfully retrieves unauthorized data. Based on the observed behavior, which SQL injection evasion technique are you employing?

A. Hex Encoding
B. String Concatenation
C. In-line Comment
D. Null Byte

Answer: B

Explanation:
String concatenation is the best match because the technique described is breaking a recognizable SQL keyword or payload into separate pieces so a signature-based WAF rule does not see the full malicious token in one continuous pattern. In CEH-aligned web application testing, many WAF detections rely on matching known strings such as UNION SELECT, OR 1=1, and other classic patterns. If an attacker can cause the database parser to interpret the same meaning while the input appears different at the inspection layer, the WAF may fail to match its rule and the payload can reach the backend.
The prompt explicitly says you "split the query into multiple parts" to avoid detection as "a single signature." That is the core idea of concatenation-based evasion: represent the same instruction through separated fragments that are recombined or tolerated by the SQL parser, depending on the database and application behavior. This differs from in-line comments, which would typically insert comment markers inside keywords to break signatures while preserving parsing, and differs from hex encoding, which replaces characters or strings with hexadecimal representations. A null byte technique is usually associated with string-termination tricks in older contexts and does not align with splitting SQL keywords for WAF bypass.
Defensively, CEH guidance emphasizes that relying on WAF signatures alone is insufficient. Strong prevention requires parameterized queries, strict server-side input validation, least-privilege database accounts, and monitoring for anomalous query patterns and error behaviors even when obvious signatures are not present.

Question: 5

Which of the following is the primary goal of ethical hacking?

A. To disrupt services by launching denial-of-service attacks
B. To identify and fix security vulnerabilities in a system
C. To steal sensitive information from a company ' s network
D. To spread malware to compromise multiple systems

Answer: B

Explanation:
Ethical hacking, as defined throughout CEH courseware, is the authorized and legitimate process of identifying vulnerabilities, weaknesses, and misconfigurations in information systems. The primary objective is to strengthen security by discovering issues before malicious actors can exploit them. Ethical hackers follow strict legal guidelines, obtain written permission, and operate within a defined scope to ensure their activities contribute positively to the organization's security posture. Unlike malicious hacking, the intent is not to steal data, cause harm, or disrupt operations. Ethical hackers use the same tools, techniques, and methodologies that attackers use, but with the purpose of remediation and risk reduction. CEH emphasizes that ethical hacking supports defense-in-depth strategies by enabling organizations to harden their environments and proactively mitigate threats. Therefore, identifying and fixing vulnerabilities is the central mission of ethical hacking.

Question: 6

An ethical hacker audits a hospital's wireless network secured with WPA using TKIP and successfully performs packet injection and decryption attacks. Which WPA vulnerability most likely enabled this?

A. Use of weak Initialization Vectors (IVs)
B. Dependence on weak passwords
C. Lack of AES-based encryption
D. Predictable Group Temporal Key (GTK)

Answer: C

Explanation:
CEH documentation explains that WPA-TKIP was a transitional security protocol and does not use AES encryption, relying instead on RC4-based mechanisms.
The lack of AES-based encryption makes WPA-TKIP vulnerable to injection and replay attacks.
Option C is correct.
Options A applies to WEP.
Option B affects authentication, not TKIP weakness.
Option D is not the primary TKIP flaw.
CEH recommends WPA2/WPA3 with AES.

Question: 7

A regional e-commerce company in Dallas, Texas operates an Apache-based web server to manage product catalogs and promotional campaigns. During an authorized assessment, a security consultant

analyzes how the platform processes a referral parameter embedded in product-sharing links. While reviewing responses through an intercepting proxy, he observes that values supplied in the referral parameter are incorporated into metadata returned to the browser. By introducing carefully crafted delimiter characters into the parameter, he notices that the structure of the server's outbound response changes in an unexpected manner. Further testing shows that the manipulated input causes the server to generate multiple logically distinct response segments within what should have been a single transaction. When the crafted link is accessed through a standard browser, the client interprets the injected portion as a separate directive, resulting in redirection behavior influenced by the attacker-controlled input. Identify the web server attack technique being demonstrated in this scenario.

A. Web Cache Poisoning Attack
B. Directory Traversal Attack
C. HTTP Response-Splitting Attack
D. Frontjacking Attack

Answer: C

Explanation:
The correct answer is HTTP Response-Splitting Attack. CEH web server coverage explains that HTTP response splitting occurs when attacker-controlled input is inserted into HTTP headers or response metadata in a way that allows the server to split one intended response into two separate responses or response segments. The question specifically describes crafted delimiter characters changing the structure of the outbound response and causing the browser to interpret the injected content as a separate directive, including attacker-influenced redirection. That is the classic behavior of response splitting. Directory traversal would involve unauthorized path navigation to restricted files or directories. Web cache poisoning focuses on corrupting cached responses so later users receive malicious or altered content, which is related conceptually but not the direct mechanism described here. CEH materials present HTTP response splitting as a means to an end, often used to trigger redirect behavior or facilitate secondary attacks by controlling the second response or header content. Because the attacker manipulates server output into multiple response components within a single transaction, HTTP Response-Splitting is the most precise answer.

Question: 8

You discover an unpatched Android permission-handling vulnerability on a device with fully updated antivirus software. What is the most effective exploitation approach that avoids antivirus detection?

A. Develop a custom exploit using obfuscation techniques
B. Use Metasploit to deploy a known payload
C. Install a rootkit to manipulate the device
D. Use SMS phishing to trick the user

Answer: A

Explanation:

The CEH Mobile Platform Security module explains that mobile antivirus solutions rely heavily on signatures and known exploit patterns. A custom exploit with obfuscation is far more likely to bypass detection.
CEH explicitly teaches that:
Zero-day or unpatched vulnerabilities
Custom, obfuscated payloads
Minimal use of known frameworks are the most effective for bypassing endpoint defenses during controlled testing.
Option A is correct.
Options B and C are easily detected.
Option D is social engineering, not a technical exploit.

Question: 9

A compromised endpoint communicates with C2 using DNS queries. What system-level indicator exists?

A. DNS anomalies
B. Memory leaks
C. CPU spikes
D. Disk usage

Answer: A

Explanation:
The correct answer is A, DNS anomalies. When a compromised endpoint uses DNS queries to communicate with a command-and-control server, the most relevant indicator is abnormal DNS behavior. In CEH-style incident detection, analysts correlate endpoint and network telemetry to identify suspicious communication patterns. DNS-based C2 may appear as repeated beaconing, unusually long domain names, excessive TXT queries, requests to newly registered or suspicious domains, high query volume, or DNS traffic that does not match normal baseline behavior. CEH materials discuss covert tunneling where commands can be hidden inside DNS name lookup query/reply traffic, making it appear like ordinary protocol traffic to network tools. IDS/monitoring concepts also emphasize anomaly detection by comparing activity against a baseline and investigating unusual behavior. Memory leaks, CPU spikes, and disk usage may occur in some malware cases, but they do not specifically indicate DNS-based C2. Therefore, the best indicator for this scenario is DNS anomalies.

Question: 10

A zero-day vulnerability is actively exploited in a critical web server, but no vendor patch is available. What should be the FIRST step to manage this risk?

A. Shut down the server
B. Apply a virtual patch using a WAF
C. Perform regular backups and prepare IR plans
D. Monitor for suspicious activity

Answer: B

Explanation:
According to CEH v13 Security Operations and Incident Response, zero-day vulnerabilities pose one of the highest operational risks because exploits exist before official remediation is available. When active exploitation is observed and no vendor patch exists, immediate compensating controls must be deployed.
The first and most effective action is implementing virtual patching, typically through a Web Application Firewall (WAF) or Intrusion Prevention System (IPS). CEH v13 defines virtual patching as a security measure that blocks exploitation attempts at the network or application layer without modifying the vulnerable software. This approach allows organizations to maintain service availability while reducing exposure.
Shutting down the server (Option A) may prevent exploitation but introduces unacceptable business disruption and is not recommended as a first response. Backups and incident response planning (Option C) are critical but do not actively prevent exploitation. Passive monitoring (Option D) allows attackers to continue exploiting the vulnerability unchecked.
CEH v13 emphasizes that virtual patching is the preferred first response for zero-day threats, especially when systems are mission-critical. It provides immediate risk reduction while allowing time for vendor patch development and controlled deployment.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/