GETCERTKEY

GETCERTKEY
100% guarantee you pass IT cert exam!

http://www.getcertkey.com

No help, Full refund!

Exam : **312-50v13**

Title : Certified Ethical Hacker Exam (CEHv13)

Vendor : ECCouncil

Version : DEMO

NO.1 As a cybersecurity professional at XYZ Corporation, you are tasked with investigating anomalies in system logs that suggest potential unauthorized activity. System administrators have detected repeated failed login attempts on a critical server, followed by a sudden surge in outbound data traffic. These indicators suggest a possible compromise. Given the sensitive nature of the system and the sophistication of the threat, what should be your initial course of action?

A. Conduct real-time monitoring of the server, analyze logs for abnormal patterns, and identify the nature of the activity to formulate immediate countermeasures.

B. Conduct a comprehensive audit of all outbound traffic and analyze destination IP addresses to map the attacker's network.

C. Immediately reset all server credentials and instruct all users to change their passwords.

D. Immediately disconnect the affected server from the network to prevent further data exfiltration.

Answer: A

Explanation:

The Certified Ethical Hacker (CEH) Incident Response lifecycle begins with Identification, followed by containment, eradication, recovery, and lessons learned. CEH documentation stresses that understanding the scope and nature of an incident is critical before taking disruptive action.

Option A is the correct initial response because it focuses on real-time monitoring and log analysis, which are essential during the identification phase. CEH materials emphasize analyzing logs, authentication failures, and traffic anomalies to confirm whether an incident has occurred and determine the attacker's techniques, persistence level, and impact.

Option B, while valuable, is more appropriate after initial identification. Conducting deep outbound traffic audits without first understanding the attack vector can delay containment decisions.

Option C is premature. CEH warns that changing credentials too early may alert the attacker and cause them to escalate or destroy evidence.

Option D represents a containment strategy, not an initial response. CEH guidelines advise against immediately disconnecting systems unless there is confirmed active data exfiltration that cannot be otherwise controlled, as this may disrupt business operations and erase volatile forensic evidence.

Therefore, the CEH-approved approach is to monitor, analyze, and identify the incident before moving to containment and eradication.

NO.2 Maya Patel from SecureHorizon Consulting is investigating a breach at Dallas General Hospital in Texas after a nurse misplaced a smartphone containing patient management software. Although the device remained active on the network, administrators had no way to identify its physical whereabouts, delaying incident response and allowing sensitive medical records to be exposed for hours. Which mobile security guideline would have most directly reduced the impact of this incident?

A. Install device tracking software that allows the device to be located remotely

B. Register devices with a remote locate and wipe facility

C. Use anti-virus and data loss prevention (DLP) solutions

D. Utilize a secure VPN connection while accessing public Wi-Fi networks

Answer: B

NO.3 During a penetration test at Lone Star Healthcare in Austin, ethical hacker Liam evaluates the hospital ' s perimeter defenses by generating controlled traffic flows through the firewall. He uses a tool that can create and replay diverse traffic patterns to test how well the firewall enforces its rules against both legitimate and malicious traffic types. This allows him to demonstrate whether the

device properly identifies evasion attempts under simulated attack conditions.
Which tool is Liam most likely using in this test?
A. Metasploit
B. Traffic IQ Professional
C. Colasoft Packet Builder
D. Nmap
Answer: B

NO.4 In Denver, Colorado, ethical hacker Rachel Nguyen is conducting a network security assessment for Apex Logistics, a transportation firm with a complex internal network. During her test, Rachel observes a client- server communication and injects specially crafted packets into the exchange, disrupting the client's session.
As a result, the server continues interacting with Rachel's system while the legitimate client's connection becomes unresponsive. She uses this setup in a controlled environment to demonstrate vulnerabilities to the company's IT team.
What network-level session hijacking technique is Rachel employing in this assessment?
A. Blind hijacking
B. UDP hijacking
C. RST hijacking
D. TCP/IP hijacking
Answer: C
Explanation:
RST hijacking is a TCP session hijacking technique emphasized in CEH materials under network attacks against established communications. In TCP, a Reset flag packet is used to abruptly tear down a connection. If an attacker can observe the session and determine the correct parameters such as IP addresses, ports, and an in- window sequence number, they can forge a TCP RST packet that appears to come from one endpoint. This can force the victim side to drop the session, making the legitimate client suddenly lose responsiveness.
The key clue in the scenario is that Rachel "observes a client-server communication" and then injects crafted packets that disrupt the client while the server continues to communicate with Rachel's system. That behavior matches the practical use of RST hijacking in demonstrations: terminate or desynchronize the victim endpoint while keeping the server-side session usable long enough for the attacker to inject traffic with valid sequence and acknowledgment values. In a switched LAN, this is often paired with sniffing or traffic visibility to reliably craft the reset packet and subsequent injected packets.
Blind hijacking is different because the attacker cannot see the traffic and must guess sequence numbers, which contradicts the "observes communication" detail. UDP hijacking is not applicable because UDP is connectionless and does not use session state or RST flags. "TCP/IP hijacking" is a broad category, but the question asks for the specific technique used to disrupt the client via crafted packets, which is best identified as RST hijacking.

NO.5 A Nessus scan reports a CVSS 9.0 SSH vulnerability allowing remote code execution. What should be immediately prioritized?
A. Apply the vendor patch and reboot during maintenance
B. Dismiss it as a false positive if unverified

C. Reroute SSH traffic to another server

D. Isolate the server, audit it, and apply patches

Answer: D

Explanation:

CEH v13 states that vulnerabilities with a CVSS score # 9.0 are critical and require immediate containment.

When remote code execution is possible, the system may already be compromised.

The recommended response is to isolate the affected system, preventing lateral movement, then perform a forensic audit before applying patches. Immediate patching without isolation may alert attackers or destroy evidence.

Thus, option D aligns with CEH incident response best practices.

NO.6 You are performing a security audit for a regional hospital in Dallas, Texas. While monitoring the network, you discover that an unknown actor has been silently capturing clear-text credentials and analyzing unencrypted traffic flowing across the internal Wi-Fi network. No modifications have been made to the data, and the attack remained undetected until your assessment. Based on this activity, what type of attack is most likely being conducted?

A. Passive attack

B. Distribution attack

C. Close-in attack

D. Insider attack

Answer: A

Explanation:

The correct answer is A. Passive attack because the activity described involves monitoring and capturing information without altering data, system resources, or communications. In CEH-aligned information security concepts, passive attacks are defined by the attacker's goal of eavesdropping-observing traffic to collect intelligence such as usernames/passwords, session identifiers, network patterns, or sensitive content-while making minimal changes that would trigger detection. The scenario explicitly states that the actor is "silently capturing clear-text credentials" and "analyzing unencrypted traffic," and that "no modifications have been made to the data." These are signature indicators of passive attacks such as packet sniffing and traffic analysis.

On an internal Wi-Fi network, passive attacks are particularly effective when encryption is weak or absent, or when users access services that transmit credentials in clear text. An attacker can capture packets and reconstruct sensitive information, especially where legacy protocols or misconfigurations exist. Because passive attackers do not need to inject or modify packets, they often avoid generating anomalies such as retransmissions, spoofed responses, or unexpected routing changes-helping them remain undetected, consistent with the prompt.

Why the other options do not fit: Distribution attack is not the standard classification for this behavior and does not specifically describe silent observation of traffic. Close-in attack refers to attacks that depend on physical proximity (e.g., shoulder surfing, physical tapping, local interception near the target). While Wi-Fi sniffing can require proximity, the defining characteristic in the question is the non-invasive observation with no data modification-i.e., passive attack. Insider attack relates to the attacker's identity/role (a trusted internal person), which is not established here; the scenario only describes behavior, not who the actor is.

Therefore, the described credential capture and traffic analysis without modification most clearly

indicates a passive attack.

NO.7 Bob, a seasoned security analyst at XYZ Aerospace, was investigating a series of misaligned transaction timestamps coming from one of the data archival systems. Suspecting that the server might be syncing with an unstable time source, Bob decided to extract a detailed list of all peer servers associated with the target machine, including metrics such as delay, offset, and jitter, to determine whether the issue stemmed from time synchronization drift.
Which of the following commands should Bob use to retrieve this information?
A. ntptrace [-n] [-m maxhosts] [servername/IP_address]
B. ntpq -p [host]
C. ntpdc [-n] [-s] [-c command] [host] [...]
D. ntpq [-n] [-l] [-c command] [host] [...]
Answer: B
Explanation:
The command that best matches Bob's goal is ntpq -p. In CEH-aligned coverage of network services and operational troubleshooting, NTP is highlighted as a critical dependency because inaccurate time can break authentication, distort logs, and cause incorrect transaction ordering. When investigating suspected time drift, the most useful first step is to view the active NTP associations and their quality metrics. The ntpq utility queries an NTP daemon and reports peer status and performance data. Specifically, ntpq -p displays a peer table that includes each configured or discovered time source along with fields such as delay, offset, and jitter.
These values help determine whether the server is locked to a stable source or being influenced by a poor or rogue time server. Offset indicates how far the local clock differs from the peer, delay reflects network latency to the peer, and jitter shows the variability in timing measurements, all of which are directly mentioned in the question.
Option A, ntptrace, is used to trace the chain of NTP servers back to a reference clock and is useful for understanding hierarchy, but it does not provide the detailed delay, offset, and jitter peer metrics in the same way. Option C, ntpdc, is an older monitoring tool that can query NTP, but CEH references more commonly emphasize ntpq for peer statistics and associations. Option D is a generic ntpq invocation with interactive command support, but the -p option is the explicit mode that outputs the peer list with the required metrics.

NO.8 A competing technology firm begins releasing products that closely mirror the design, pricing strategy, and feature roadmap of ApexDynamics Inc. An internal review reveals that detailed information about ApexDynamics ' s upcoming initiatives had been gradually collected through publicly available sources and external disclosures before product launch. Which footprinting-related threat does this scenario best represent?
A. Corporate Espionage
B. Business Loss
C. Information Leakage
D. Social Engineering
Answer: A
Explanation:
The best answer is Corporate Espionage. CEH reconnaissance coverage explains that footprinting can be used not only for technical attack preparation but also for competitive intelligence gathering

against organizations.
In this scenario, a rival company appears to have derived meaningful strategic information about product design, pricing, and roadmap decisions from publicly available data and external disclosures before launch.
The resulting harm is not just accidental exposure in the abstract; it is the use of collected intelligence to gain a business advantage over the target organization. That makes corporate espionage the most accurate classification. Information leakage is certainly part of the pathway, because some information had to be exposed or inferable from public sources, but the threat asked for is the footprinting-related consequence represented by the competitor's behavior. Business loss describes an impact, not the threat category itself.
Social engineering would require manipulative interaction with people, which is not stated here. CEH materials note that careless public disclosures, metadata, career postings, partner information, and strategic announcements can all support footprinting by competitors or adversaries. When such data is systematically collected to mirror or undermine business strategy, the activity is best described as corporate espionage.

NO.9 You are a cybersecurity consultant at FortiSec, advising DesertTech Innovations in Phoenix, Arizona. The company wants to modernize its Wi-Fi so that even if an attacker obtains a captured handshake or a weak passphrase, they cannot perform offline dictionary attacks or recover session keys; management also wants stronger, per-session encryption and protection for IoT devices without relying on a single shared password.
Which wireless security measure should DesertTech implement to meet these goals?
A. MAC Address Filtering
B. Use 802.1X Authentication
C. Upgrade to WPA3
D. Disable TKIP
Answer: C
Explanation:
The requirements map most directly to WPA3, because WPA3-Personal replaces the legacy WPA2-PSK handshake with SAE (Simultaneous Authentication of Equals). SAE is designed to resist offline dictionary attacks: even if an attacker captures the handshake, they cannot simply take it offline and test password guesses at high speed the way they can with WPA2-PSK handshakes. This directly addresses management's concern that a captured handshake plus a weak passphrase could enable offline cracking and eventual session key recovery.
WPA3 also strengthens per-session protection by improving how keys are established and by supporting stronger cryptographic defaults. In enterprise contexts, WPA3 aligns with stronger authentication and encryption suites, and in IoT scenarios it supports modern onboarding and improved security posture compared to older WPA2/TKIP-era configurations. The "per-session encryption" and "stronger protection" goals are consistent with WPA3's modern design focus.
Why the other options are less suitable:
MAC address filtering (A) is not a security control against credential capture or offline attacks; MACs are easily spoofed and do not provide cryptographic protection.
802.1X authentication (B) (WPA2/WPA3-Enterprise) is very strong and removes reliance on a single shared PSK by using per-user/device credentials and dynamic keys. However, the question's key requirement explicitly calls out preventing offline dictionary attacks even if a handshake is captured-this is most directly the hallmark improvement of WPA3-Personal (SAE). (In practice, WPA3-

Enterprise with 802.1X is also excellent, but "upgrade to WPA3" is the single best match to the stated offline dictionary concern.) Disabling TKIP (D) is good hygiene (prefer AES/CCMP), but it does not prevent WPA2-PSK handshake capture and offline cracking if PSK is used.
Therefore, the best measure to meet the stated modernization goals is C. Upgrade to WPA3.

NO.10 During a red team engagement at a manufacturing company in Dallas, penetration tester Tyler gains access to a Windows workstation. Later in the exercise, he reviews his exfiltrated logs and finds detailed records of employee logins, email drafts, and sensitive data entered into desktop applications. The collection occurred without requiring browser injection or physical device access, and no kernel drivers were installed.
Which type of keylogger did Tyler most likely deploy?
A. JavaScript Keylogger
B. Hardware Keylogger
C. Kernel Keylogger
D. Application Keylogger
Answer: D
Explanation:
The correct answer is D. Application Keylogger because the scenario describes keystroke capture from desktop applications on a Windows workstation without installing kernel drivers and without requiring physical access or browser-level script injection. In CEH-aligned keylogger classifications, an application (user-mode) keylogger operates at the application layer by using user-space techniques such as hooking common Windows APIs (for example, keyboard input functions and message-handling routines) to intercept keystrokes as they are processed by applications. This enables logging of credentials typed into local programs, draft emails written in desktop clients, and sensitive text entered into business tools-exactly the outcome Tyler observed.
The question provides two strong eliminators. First, it states no kernel drivers were installed, which rules out kernel keyloggers that capture input at the kernel level (often requiring driver installation and deeper OS integration). Second, it states the attack did not require browser injection, which rules out a JavaScript keylogger (typically implemented by injecting script into a web page/application to capture form inputs within a browser session). It also explicitly notes that there was no physical device access, which rules out a hardware keylogger (a physical device placed between keyboard and computer or embedded in a keyboard) that requires in-person installation.
Application keyloggers are frequently used in post-exploitation because they can be deployed quickly with standard user-level privileges (though higher privileges may expand coverage), can target a broad range of applications, and can run covertly. From a defense perspective, monitoring for suspicious API hooking behavior, unusual process injection, abnormal input-capture patterns, and endpoint controls that detect credential access techniques are common countermeasures.
Therefore, given the constraints and the observed logging of desktop application input, the most likely keylogger type is an application keylogger.

NO.11 During a security compliance audit at Nexus Tech Solutions in Boston, Massachusetts, the ethical hacking team launches a controlled social engineering exercise to assess help desk vulnerabilities. Ethical hacker Rachel Kim calls the company ' s help desk, posing as a stressed employee named Laura Bennett from the marketing department. Rachel claims her laptop is running slowly and offers to share her login credentials if the help desk can provide a quick fix to meet a tight project deadline. The call is designed to test whether help desk staff follow proper verification

protocols or fall for the offer of credentials in exchange for assistance.
What social engineering technique is Rachel employing in this exercise?
A. Shoulder Surfing
B. Vishing
C. Impersonation
D. Quid Pro Quo
Answer: C
Explanation:
This scenario best illustrates impersonation. In CEH-aligned social engineering concepts, impersonation occurs when an attacker assumes the identity of a legitimate person, such as an employee, contractor, executive, or vendor, to exploit trust and bypass established procedures. Rachel explicitly "poses as a stressed employee named Laura Bennett" and uses a believable workplace pretext such as a slow laptop and a tight deadline. This is a classic pressure-and-urgency tactic used to lower skepticism and push the target into breaking policy, such as skipping identity verification or accepting unsafe troubleshooting steps.
Although the interaction happens over the phone, the defining technique being tested is not merely the communication channel but the identity deception. Vishing is phone-based phishing, and while the call could be described as vishing in a broad sense, the prompt emphasizes the assumed identity and the help desk's verification controls, which is the hallmark of impersonation. Quid pro quo typically involves offering a benefit or service in exchange for information; here, the core mechanic is Rachel's false identity and her attempt to get the help desk to accept credential sharing as part of support. Shoulder surfing is unrelated because it involves physically observing someone's screen or keystrokes.
CEH best practices to mitigate impersonation include strict caller verification, callback procedures to known numbers, ticket validation, prohibiting password sharing, requiring multi-factor authentication resets via approved workflows, and training help desk staff to recognize urgency-based manipulation and escalate suspicious requests.

NO.12 At Norwest Freight Services, a rotating audit team is asked to evaluate host exposure across multiple departments following a suspected misconfiguration incident. Simon, a junior analyst working from a trusted subnet, initiates a network-wide scan using the default configuration profile of his assessment tool. The tool completes quickly but returns only partial insights such as open service ports and version banners while deeper registry settings, user policies, and missing patches remain unreported. Midway through the report review, Simon notices that system login prompts were never triggered during scanning, and no credential failures were logged in the SIEM.
Which type of vulnerability scan BEST explains the behavior observed in Simon's assessment?
A. Unauthenticated Scanning
B. Authenticated Scanning
C. Internal Scan
D. Credentialed Scanning
Answer: A
Explanation:
The behavior described is most consistent with an unauthenticated scan. In CEH-aligned vulnerability assessment methodology, unauthenticated scanning evaluates systems from the perspective of an external or non-privileged entity. The scanner can typically identify network-reachable services, open

ports, service banners, protocol fingerprints, and sometimes known vulnerabilities inferred from versions or exposed configurations. However, it cannot reliably inspect host-internal posture such as registry settings, local security policies, installed patch levels, missing hotfixes, detailed configuration baselines, or user and group policy settings because those require authenticated access to query the operating system and installed software inventory directly.
The prompt explicitly states that the results were limited to "open service ports and version banners" and that
"deeper registry settings, user policies, and missing patches remain unreported." That limitation is a hallmark of unauthenticated scanning. The additional clue that "system login prompts were never triggered" and "no credential failures were logged in the SIEM" further confirms that the scanner never attempted to authenticate to endpoints using accounts, SSH/WinRM/WMI, SMB, or agent-based credential checks. If the scan were authenticated or credentialed, you would expect authentication attempts, potential login prompts on some services, and often audit logs or SIEM events reflecting successful or failed logons.
Option C, internal scan, only describes where the scan originates, not whether credentials were used. Options B and D imply authentication and host-level interrogation, which contradicts the observed lack of credential activity and missing patch/policy visibility. Therefore, unauthenticated scanning best explains the outcome.

NO.13 In the crisp mountain air of Denver, Colorado, ethical hacker Lila Chen investigates the security framework of MedVault, a US-based healthcare platform used by regional clinics to manage patient data. During her assessment, Lila manipulates session parameters while navigating the patient portal's dashboard. Her tests reveal a critical flaw: the system allows users to access sensitive medical records not associated with their own account, enabling unauthorized changes to private health data. Upon deeper inspection, Lila determines that the issue stems from the application allowing users to perform actions beyond their assigned roles rather than failures in encryption, unsafe object handling, or server configuration.
Which OWASP Top 10 2021 vulnerability is Lila most likely exploiting in MedVault's web application?

A. Security Misconfiguration

B. Insecure Deserialization

C. Cryptographic Failures

D. Broken Access Control

Answer: D

Explanation:
Broken Access Control is the correct choice because the scenario describes a user being able to access and modify resources that should be restricted to other users or roles. In CEH-aligned web testing, access control flaws occur when an application fails to enforce authorization checks consistently on the server side.
Manipulating session parameters and then retrieving "sensitive medical records not associated with their own account" is a classic indicator of an authorization bypass, often seen as insecure direct object references, parameter tampering, or horizontal and vertical privilege escalation. Horizontal escalation is when one user accesses another user's data at the same privilege level, while vertical escalation is when a user performs actions reserved for higher-privileged roles. The prompt explicitly states users can perform actions beyond assigned roles, which is the definition of broken authorization enforcement.
The other options do not align with the described root cause. Cryptographic Failures focuses on weak

or missing encryption and does not explain why authenticated users can reach unauthorized records. Insecure Deserialization involves unsafe deserialization leading to remote code execution or data tampering via serialized objects, which is not indicated here. Security Misconfiguration is broader and can contribute to exposure, but the scenario emphasizes role and resource permission bypass rather than mis-set server headers, default accounts, or exposed admin interfaces.
Mitigation in CEH best practices includes enforcing server-side authorization on every request, using deny-by- default policies, validating that the authenticated user is allowed to access the specific record identifier, implementing robust role-based access control, logging access denials, and adding automated tests to prevent IDOR and privilege escalation regressions.

NO.14 As part of an annual security awareness program at BrightPath Consulting in Denver, Colorado, the cybersecurity team conducts an ethical hacking experiment to test employee vigilance against physical social engineering threats. During a simulated attack, ethical hacker Liam Carter strategically places a USB drive labeled "Confidential 2025 Budget Plans" in the company's parking lot, designed to look like it was accidentally dropped. The USB is programmed to install a harmless tracking script when plugged into a workstation, alerting the security team. Sarah, a project coordinator, finds the USB and considers plugging it into her office laptop to identify its owner.
What social engineering technique is being tested in this experiment?
A. Phishing
B. Hoax
C. Pretexting
D. Baiting
Answer: D
Explanation:
The scenario clearly describes baiting, a physical social engineering technique covered in CEH under human- based attacks. Baiting involves enticing a victim with something appealing or intriguing, such as free software, confidential documents, or valuable information, in order to trick them into compromising security.
In this case, the USB drive is deliberately labeled "Confidential 2025 Budget Plans," which is designed to trigger curiosity and urgency. The attacker relies on human psychology, specifically curiosity and perceived importance, to motivate the target to plug the device into a company system.
Unlike phishing, which typically occurs through email or electronic communication, baiting often involves physical media such as USB drives left in public areas like parking lots or lobbies. CEH materials highlight that attackers may preload such devices with malware that executes automatically when inserted, granting access to the internal network. Even though this experiment uses a harmless tracking script, the methodology mirrors real-world attacks where malicious payloads could establish backdoors, exfiltrate data, or deploy ransomware.
Hoaxes spread false warnings to create panic but do not necessarily require interaction with physical devices.
Pretexting involves fabricating a scenario or identity to elicit information directly from a target through conversation or interaction. The use of a strategically placed USB labeled with enticing information fits the definition of baiting precisely. This test reinforces the importance of policies prohibiting unknown removable media usage and promoting employee awareness training.

NO.15 An IoT traffic light shows anomalous traffic to an external IP and has an open port. What should be your next step?

A. Attempt reverse connections
B. Isolate the device and investigate firmware
C. Modify firewall rules only
D. Conduct full network penetration testing
Answer: B
Explanation:
CEH v13 emphasizes that IoT and smart city environments are highly sensitive and safety-critical. When an IoT device shows anomalous outbound traffic and unauthorized open ports, this strongly indicates device compromise.
The correct immediate response is to isolate the affected device to prevent lateral movement and protect public safety. CEH v13 further stresses the importance of firmware analysis, as IoT malware often resides at the firmware level to maintain persistence.
Attempting reverse connections (Option A) is risky and may violate operational safety. Firewall changes alone (Option C) do not address an already compromised device. A full penetration test (Option D) is appropriate later but not as an immediate containment step.
Therefore, Option B aligns with CEH v13 incident handling best practices for IoT and OT environments.

NO.16 A penetration tester finds malware that spreads across a network without user interaction, replicating itself from one machine to another. What type of malware is this?
A. Keylogger
B. Ransomware
C. Virus
D. Worm
Answer: D
Explanation:
Comprehensive Explanation from CEH v13 Courseware:
CEH v13 describes worms as standalone malicious programs capable of self-replication without requiring user assistance. Unlike viruses, which need a host file and are triggered typically by user actions, worms propagate autonomously by scanning networks, exploiting vulnerabilities, or copying themselves to accessible machines. Worms are known for causing rapid, widespread damage by consuming bandwidth, degrading system performance, and creating backdoors for attackers. Classic examples such as Conficker, WannaCry, and SQL Slammer reinforce the destructive potential of automated propagation. CEH stresses that worms often use network shares, open ports, or unpatched vulnerabilities to move laterally. In contrast, keyloggers harvest keystrokes, ransomware encrypts data and demands payment, and viruses require user involvement to spread. The behavior in the scenario-automatic replication across the network-is the defining characteristic of worm activity according to CEH's malware taxonomy.

NO.17 A financial technology firm in Atlanta, Georgia launches an internal investigation after multiple employees report that a popular messaging application on their Android devices has begun displaying excessive advertisements and behaving unpredictably. Security analysts discover that users had installed a utility application from a third-party marketplace weeks earlier. Further examination shows that this application silently replaced certain legitimate apps already present on the device. The compromised applications were then used to generate large volumes of advertisements and

collect user data for external transmission. Based on the observed behavior, what malware is most consistent with this incident?

A. Mamo

B. Pegasus

C. Agent Smith

D. GoldPickaxe

Answer: C

Explanation:

The behavior described most closely matches Agent Smith, an Android malware family known for replacing or hijacking legitimate applications and monetizing that access through ad fraud and data abuse. The strongest clues are the installation from a third-party marketplace, the silent replacement of already installed apps, and the use of those altered applications to push excessive advertisements while collecting information. In CEH mobile platform discussions, third-party app ecosystems are repeatedly identified as high-risk distribution paths for malicious or trojanized software because the apps may avoid the stricter vetting associated with official marketplaces. Pegasus is generally associated with advanced spyware capabilities and covert surveillance, not ad-fraud-driven replacement of popular apps. GoldPickaxe is tied to more targeted mobile credential and identity theft campaigns, while Mamo is not the fitting malware profile here. This question is testing recognition of a well-known Android malware pattern: malicious code embedded in an apparently useful application that later abuses the trust and visibility of legitimate apps already on the phone. CEH mobile security principles stress that unofficial app sources significantly increase the risk of this kind of compromise.

NO.18 You are a cybersecurity analyst at a global banking corporation and suspect a backdoor attack due to abnormal outbound traffic during non-working hours, unexplained reboots, and modified system files. Which combination of measures would be most effective to accurately identify and neutralize the backdoor while ensuring system integrity?

A. Review firewall logs, analyze traffic, and immediately reboot systems

B. Monitor system and file activity, apply anomaly detection, and use advanced anti-malware tools

C. Enforce strong passwords, MFA, and regular vulnerability assessments

D. Apply ACLs, patch systems, and audit user privileges

Answer: B

Explanation:

According to CEH v13 Security Operations and Incident Response, backdoors are stealth mechanisms that allow attackers persistent access. Indicators such as unexplained outbound traffic, unauthorized file modifications, and irregular reboots strongly suggest post-compromise persistence mechanisms. CEH v13 recommends a behavioral and host-based detection approach for backdoor identification. Continuous monitoring of system and file activity helps detect unauthorized binaries, registry changes, and scheduled tasks. Anomaly detection identifies deviations from normal system behavior, which is critical for uncovering hidden backdoors that evade signature-based detection. Additionally, advanced anti-malware tools with heuristic and memory analysis capabilities are essential to identify sophisticated backdoors that traditional antivirus may miss. These tools can detect rootkits, fileless persistence, and covert communication channels.

The other options are preventative but not investigative. Immediate reboots may destroy volatile evidence, while password policies and ACLs do not detect existing compromises. Therefore, option B

provides the most effective and CEH-aligned response.

NO.19 A technology consulting firm in Portland, Oregon began experiencing repeated topology recalculations across its switching infrastructure. Shortly after a newly connected device came online in a conference room, spanning-tree convergence events were triggered across multiple distribution switches. Engineers determined that the access-layer interface connected to that device was influencing path-selection decisions, introducing a more favorable bridge priority value into the environment and affecting the established hierarchy. To preserve the intended switching structure and prevent unauthorized devices from altering root selection decisions, which control should be employed?

A. Configuring Loop Guard on non-designated ports

B. Activating UDLD (Unidirectional Link Detection) on uplinks

C. Applying Root Guard on designated interfaces

D. Enabling BPDU Guard on edge ports

Answer: D

Explanation:

The best answer is BPDU Guard on edge ports. CEH network defense material explains that BPDU Guard is used on access or edge ports where end-user devices are expected, not switches. If a device connected to such a port begins sending Bridge Protocol Data Units, the switch treats that as an abnormal condition and can shut the port down or place it in an error-disabled state. This prevents unauthorized or misconfigured devices from participating in spanning-tree and influencing root bridge election or topology decisions. That matches the scenario, where a newly connected device introduced a more favorable bridge priority and triggered spanning- tree recalculations. Root Guard is also related to protecting spanning-tree hierarchy, but it is typically applied where you want to prevent a downstream switch from becoming root while still allowing BPDU participation under controlled conditions. CEH exam framing usually expects BPDU Guard when the threat originates from an end-host-facing access port in a conference room or office edge location. Because the goal is to stop unauthorized edge-connected devices from affecting spanning-tree at all, enabling BPDU Guard on edge ports is the most appropriate control.

NO.20 During a red team assessment at New England Insurance in Boston, ethical hacker Daniel sends a series of spoofed TCP packets carrying the reset flag to a server hosting client applications. As a result, several active sessions between employees and the server are abruptly terminated, causing temporary disruption of legitimate work. Daniel uses this demonstration to highlight how attackers can forcibly tear down sessions without completing a full hijack.

Which type of network-level session hijacking technique is Daniel simulating?

A. UDP Hijacking

B. RST Hijacking

C. Blind Hijacking

D. TCP/IP Hijacking

Answer: B

Explanation:

The technique described is RST hijacking because the attacker sends spoofed TCP packets with the RST (reset) flag to forcibly terminate established TCP sessions. In TCP, an RST packet is used to immediately abort a connection. If an attacker can craft packets that appear to belong to an existing

session (matching the 4- tuple and using plausible sequence/acknowledgment values), the receiving endpoint may accept the reset and tear down the connection. This creates disruption-sessions drop, users are disconnected, and applications experience errors-without the attacker needing to fully take over the session or inject meaningful application data.
The scenario matches this exactly: "spoofed TCP packets carrying the reset flag," followed by "active sessions...abruptly terminated." That is the hallmark outcome of RST-based session disruption. It is often used as a demonstration of how fragile sessions can be when attackers can spoof traffic within a path (or on the same network segment) and when defensive controls do not validate or protect sessions adequately.
Why the other options are incorrect:
UDP hijacking (A) doesn't apply because UDP is connectionless and has no RST flag or session teardown mechanism like TCP.
Blind hijacking (C) refers to injecting traffic without seeing responses (guessing sequence numbers), but the specific mechanism asked here is the reset-flag termination; "blind" could be a property of how it's done, not the named technique.
TCP/IP hijacking (D) is a broader category that includes multiple methods of taking over or manipulating TCP sessions. The question is specifically about using RST packets to kill sessions, which is most precisely called RST hijacking.
Therefore, the correct answer is B. RST Hijacking.

NO.21 A major financial institution is experiencing persistent DoS attacks against online banking, disrupting transactions. Which sophisticated DoS technique poses the greatest challenge to detect and mitigate effectively, potentially jeopardizing service availability?
A. A synchronized Layer 3 Smurf attack flooding routers with ICMP echo requests
B. A distributed SQL injection attack against online banking database servers causing resource exhaustion
C. A zero-day buffer overflow exploit against the web server causing service unavailability via RCE
D. A coordinated UDP flood targeting authoritative DNS servers to disrupt domain resolution
Answer: B
Explanation:
CEH emphasizes that application-layer DoS attacks are often the most difficult to detect and mitigate because they can mimic legitimate user behavior while exhausting backend resources. A distributed SQL injection- driven DoS (Option B) can be especially challenging: attackers send requests that appear valid at the HTTP level, but the injected or crafted parameters force the application/database to execute expensive queries (heavy joins, sleep/delay functions, or costly operations). When distributed across many sources, the traffic can look like normal customer usage-successful TCP handshakes, valid HTTP requests, and realistic user- agent patterns-while still causing database connection pool exhaustion, CPU spikes, lock contention, and degraded response times.
Option A (Smurf) and Option D (UDP/DNS flooding) are more volumetric/network-layer patterns and are typically mitigated with upstream DDoS scrubbing, rate limiting, and filtering, and are more readily detectable via traffic anomalies. Option C (zero-day RCE) is severe, but it is not primarily a "DoS technique" in CEH classification; it's an exploitation scenario that may lead to service outage, but the detection
/mitigation path centers on exploit prevention, EDR, patching, and containment rather than DoS controls. In CEH terms, Option B aligns best with a sophisticated, scenario-like DoS that blends into normal app activity.

CEH mitigation approaches for application-layer DoS include WAF rules, input validation/parameterization (preventing SQLi), query cost controls, rate limiting by behavior, caching, database hardening, and anomaly detection at the application and database tiers.

NO.22 A web server was compromised through DNS hijacking. What would most effectively prevent this in the future?

A. Changing IP addresses

B. Regular patching

C. Implementing DNSSEC

D. Using LAMP architecture

Answer: C

Explanation:

DNS hijacking occurs when attackers manipulate DNS responses to redirect traffic to malicious servers. CEH v13 clearly identifies DNSSEC (Domain Name System Security Extensions) as the primary defense against such attacks.

DNSSEC adds cryptographic signatures to DNS records, enabling clients to verify authenticity and integrity of DNS responses. Without DNSSEC, attackers can spoof DNS responses even if servers are fully patched.

Changing IP addresses and using LAMP do not address DNS trust. Patching is essential but does not prevent DNS spoofing.

CEH v13 explicitly recommends DNSSEC for preventing cache poisoning and DNS hijacking attacks, making Option C the correct answer.

NO.23 During an external assessment of a regional retail company ' s digital infrastructure, security analyst Joe is assigned to map internal services without active intrusion. While testing the behavior of a publicly exposed resolution system, he discovers that a secondary system responds unusually to structured queries. When he issues a specific request format, the server replies with a full list of internal mappings, including subdomains, mail hosts, and system aliases without requiring credentials or triggering alerts.

Which technique was most likely used to obtain this information?

A. LDAP Enumeration

B. NTP Enumeration

C. DNS Zone Transfer Enumeration

D. NetBIOS Enumeration

Answer: C

Explanation:

The described behavior matches DNS Zone Transfer Enumeration. In CEH reconnaissance, DNS enumeration aims to discover hosts and services by querying DNS records. A zone transfer is a special DNS operation intended for legitimate replication between an authoritative primary DNS server and its secondary DNS servers. When misconfigured, a DNS server may allow an unauthorized requester to perform a zone transfer, returning the entire DNS zone database. This can reveal extensive internal naming information such as subdomains, hostnames, mail exchangers, service records, and aliases, exactly like the "full list of internal mappings, including subdomains, mail hosts, and system aliases" described in the question. The clue

"secondary system responds unusually" is especially telling, because secondary DNS servers are

commonly the ones configured for replication and may be mistakenly left open to transfers from any host.
The other options do not fit the output. LDAP enumeration targets directory services and would not yield DNS-style mappings unless you already had directory access and queries. NTP enumeration relates to time synchronization services and can reveal time/server details, not comprehensive host/subdomain lists.
NetBIOS enumeration focuses on Windows networking (names, shares, workgroups) typically on internal networks and would not produce a DNS zone's record set.
CEH-recommended mitigations include restricting zone transfers to authorized secondary server IPs only, using TSIG keys for authenticated transfers, minimizing publicly exposed DNS data, splitting internal and external DNS (split-horizon), and continuously auditing DNS configurations to prevent inadvertent information leakage.

NO.24 A future-focused security audit discusses risks where attackers collect encrypted data now, anticipating that they can decrypt it later with quantum computers. What is this threat known as?
A. Saving data today for future quantum decryption
B. Replaying intercepted quantum messages
C. Breaking RSA using quantum algorithms
D. Flipping qubit values to corrupt the output
Answer: A
Explanation:
In CEH v13 Cryptography, this threat is formally referred to as "Harvest Now, Decrypt Later" (HNDL). It describes a long-term cryptographic risk where adversaries intercept and store encrypted communications today, even though they cannot decrypt them with current computational capabilities. The expectation is that future quantum computers will be powerful enough to break widely used public-key cryptographic algorithms.
CEH v13 emphasizes that quantum algorithms such as Shor's Algorithm can theoretically break RSA, DSA, and ECC by efficiently solving integer factorization and discrete logarithm problems. However, the defining feature of this threat is not the act of breaking encryption itself, but rather the strategic collection and storage of encrypted data in advance.
Option C is incomplete because it focuses only on the cryptographic mechanism rather than the threat model.
Options B and D are unrelated to the scenario described and refer to quantum communication integrity issues, not long-term cryptographic exposure.
CEH v13 highlights that sensitive data with long confidentiality lifetimes-such as government records, financial data, healthcare information, and intellectual property-is especially vulnerable to this threat. As a result, organizations are encouraged to adopt quantum-resistant (post-quantum) cryptographic algorithms proactively.
Thus, Option A accurately describes the threat model and aligns with CEH v13's treatment of future cryptographic risks.

NO.25 A penetration tester is attacking a wireless network running WPA3 encryption. Since WPA3 handshake protections prevent offline brute-force cracking, what is the most effective approach?
A. Downgrade the connection to WPA2 and capture the handshake to crack the key
B. Execute a dictionary attack on the WPA3 handshake using common passwords

C. Perform a brute-force attack directly on the WPA3 handshake

D. Perform a SQL injection attack on the router ' s login page

Answer: A

Explanation:

CEH v13 explains that WPA3 introduces SAE (Simultaneous Authentication of Equals), which resists traditional offline dictionary and brute-force attacks by removing crackable handshake material. Because WPA3 prevents attackers from capturing a reusable handshake, the most practical offensive method is to force a downgrade attack, tricking clients into associating using WPA2 instead of WPA3. Once the victim reconnects under WPA2-PSK, the attacker captures the standard 4-way handshake, which can then be cracked offline using dictionary or GPU-accelerated brute-force methods. CEH discusses downgrade attacks as a significant real-world threat when mixed-mode configurations are enabled or when access points fail to enforce strict WPA3-only operation. Options B and C are ineffective because WPA3 handshake materials cannot be brute-forced offline. Option D is unrelated to Wi-Fi encryption. Downgrading to WPA2 is the most effective and widely documented attack path.

NO.26 Systems are communicating with unknown external entities, raising concerns about exfiltration or malware.

Which strategy most directly identifies and mitigates the risk?

A. Aggressive zero-trust shutdown

B. Deep forensic analysis

C. Behavioral analytics profiling normal interactions

D. Employee awareness training

Answer: C

Explanation:

CEH v13 highlights behavioral analytics as one of the most effective techniques for identifying ambiguous or stealthy threats such as data exfiltration, command-and-control traffic, and insider abuse. When interactions appear suspicious but not definitively malicious, behavioral profiling provides the most direct visibility.

Behavioral analytics tools establish a baseline of normal system and network behavior, including typical communication patterns, data transfer volumes, destinations, and timing. Deviations from this baseline trigger alerts, allowing analysts to detect previously unknown threats without relying on signatures.

Option C is the most appropriate because it both identifies anomalies and supports continuous mitigation. A full zero-trust shutdown (Option A) is disruptive. Forensics (Option B) is reactive and better suited after confirmation of compromise. Training (Option D) does not address system-level interactions.

CEH v13 emphasizes that modern attacks often blend into normal traffic, making behavioral analysis essential. Therefore, Option C is the correct answer.

NO.27 Lily, a network security analyst at a regional healthcare provider, is preparing defenses ahead of a scheduled external vulnerability assessment. During internal simulation drills, she observes that scanners are successfully identifying open ports and service banners across critical systems. Tasked with reducing exposure to such reconnaissance efforts, Lily is instructed to apply measures that specifically hinder port scanning activity without disrupting legitimate traffic.

Which of the following actions should Lily implement?

A. Block unwanted services running on the ports and update the service versions
B. Use a custom rule set to lock down the network, block unwanted ports at the firewall, and filter specific ports
C. Configure firewall and IDS rules to detect and block probes
D. Block inbound ICMP message types and all outbound ICMP type 3 unreachable messages
Answer: C
C: Configuring firewall and IDS rules to detect and block probes is the most direct and CEH-aligned countermeasure for hindering port scanning while preserving legitimate traffic. Port scans typically generate recognizable patterns such as many connection attempts across multiple ports in a short time window, repeated SYN packets, abnormal TCP flag combinations, or sequential targeting of hosts and ports. An IDS or IPS can detect these behaviors using thresholds and signatures and then alert or actively block the scanning source through shunning, dynamic ACL updates, or automated firewall integration. This approach focuses on stopping the reconnaissance activity itself, rather than only addressing the symptoms after exposure has already occurred.Option B is partially valid because blocking unwanted ports at the firewall reduces the attack surface, but it is primarily hardening and exposure reduction. It does not necessarily hinder scanning behavior, and overly broad filtering can unintentionally block legitimate services if not carefully scoped. Option A improves security by removing unnecessary services and patching, but scanning can still occur and banners may still be collected from required services. Option D is not appropriate because blocking ICMP type 3 unreachable messages can interfere with normal network operations, troubleshooting, and path MTU discovery, and it does not reliably stop modern scanning techniques that use TCP-based probing.
Therefore, the best action specifically aimed at disrupting port scanning activity with minimal impact on legitimate traffic is tuning firewall and IDS controls to detect and block scan probes.

NO.28 A penetration tester is tasked with uncovering historical content from a company's website, including previously exposed login portals or sensitive internal pages. Direct interaction with the live site is prohibited due to strict monitoring policies. To stay undetected, the tester decides to explore previously indexed snapshots of the organization's web content saved by external sources. Which approach would most effectively support this passive information-gathering objective?
A. Search with intext: " login " site:target.com to retrieve login data
B. Use the link: operator to find backlinks to login portals
C. Apply the cache: operator to view Google ' s stored versions of target pages
D. Use the intitle:login operator to list current login pages
Answer: C
Explanation:
Passive reconnaissance is emphasized throughout CEH as an essential method for gathering intelligence without alerting monitoring systems. When the tester cannot interact with the live site, they must rely entirely on third-party archives or cached content stored by search engines or internet archival services. Google's cache function provides previously stored versions of web pages exactly for this purpose. CEH explains that attackers frequently use cached content to retrieve outdated login portals, administrative pages, exposed directories, or other sensitive elements that may no longer appear on the live web server. Unlike operators such as intext or intitle, which query live indexed metadata, the cache operator retrieves historical snapshots without accessing the target website. The link operator identifies backlinks but does not provide historical page content. Only the cache

operator directly supports viewing previous versions of pages passively, aligning perfectly with the requirement to avoid detection while gathering intelligence on legacy web content.

NO.29 During an ethical hacking exercise, a security analyst is testing a web application that manages confidential information and suspects it may be vulnerable to SQL injection. Which payload would most likely reveal whether the application is vulnerable to time-based blind SQL injection?

A. UNION SELECT NULL, NULL, NULL--

B. ' OR ' 1 ' = ' 1 ' --

C. ' OR IF(1=1,SLEEP(5),0)--

D. AND UNION ALL SELECT ' admin ' , ' admin ' --

Answer: C

Explanation:

CEH's SQL Injection coverage distinguishes between classic (error-based), union-based, boolean-based blind, and time-based blind SQL injection. Time-based blind SQL injection is used when the application does not return database errors or query results to the attacker (no visible output), but the attacker can infer execution behavior by measuring response delays.

A time-based payload intentionally triggers a database delay function (for example, SLEEP(), WAITFOR DELAY, pg_sleep() depending on DBMS). If the injection is successful, the page response time increases predictably, confirming that attacker-controlled SQL is being executed.

Option C is the correct time-based blind probe because it uses conditional logic (IF(1=1, SLEEP(5), 0)) to cause a measurable delay only when the injected condition evaluates true. CEH teaches that this technique is particularly effective against hardened applications that suppress errors and sanitize outputs, because timing becomes the side-channel for confirmation.

Option A and Option D are UNION-based payload patterns intended to extract data via returned result sets, which time-based blind scenarios typically do not provide. Option B is a classic authentication-bypass

/boolean test; it can indicate injection but does not specifically validate time-based blind behavior when output is not observable.

CEH mitigation guidance includes parameterized queries, strict input validation, least-privilege DB accounts, WAF tuning, and centralized logging to detect anomalous query timing patterns.

NO.30 During an internal assessment, a penetration tester gains access to a hash dump containing NTLM password hashes from a compromised Windows system. To crack the passwords efficiently, the tester uses a high- performance CPU setup with Hashcat, attempting millions of password combinations per second. Which technique is being optimized in this scenario?

A. Spoof NetBIOS to impersonate a file server

B. Leverage hardware acceleration for cracking speed

C. Dump SAM contents for offline password retrieval

D. Exploit dictionary rules with appended symbols

Answer: B

Explanation:

Password cracking is a core component of the system hacking phase. CEH materials highlight that once password hashes are obtained, attackers often perform offline cracking to avoid detection and bypass account lockout policies. Tools like Hashcat make use of hardware acceleration-specifically, GPU or multi-core CPU computing-to significantly increase cracking throughput. Hardware

acceleration allows the system to perform thousands to millions of hash calculations simultaneously, dramatically improving cracking efficiency compared to traditional CPU-bound methods. While dumping SAM contents is part of credential extraction, it is not the optimization described in the scenario. Dictionary rules influence cracking strategy but not raw speed. NetBIOS spoofing is unrelated to password cracking. The emphasis here is on maximizing computational power to accelerate the hash-cracking process, aligning directly with CEH's explanation of hardware-accelerated offline cracking techniques.

NO.31 A Certified Ethical Hacker (CEH) is auditing a company's web server that employs virtual hosting. The server hosts multiple domains and uses a web proxy to maintain anonymity and prevent IP blocking. The CEH discovers that the server's document directory (containing critical HTML files) is named "certrcx" and stored in /admin/web. The server root (containing configuration, error, executable, and log files) is also identified. The CEH also notes that the server uses a virtual document tree for additional storage. Which action would most likely increase the security of the web server?

A. Moving the document root directory to a different disk

B. Regularly updating and patching the server software

C. Changing the server's IP address regularly

D. Implementing an open-source web server architecture such as LAMP

Answer: B

Explanation:

CEH guidance for web server hardening prioritizes controls that reduce exploitable conditions across the broadest set of threats. While obscuring paths (for example, unusual directory names like "certrcx" or storing content under "/admin/web") may slightly slow down casual discovery, CEH emphasizes that security through obscurity is not a reliable control. If an attacker can identify the server root, document root, and virtual directory structure (through misconfigurations, directory listing, error leakage, backup exposure, or known-path enumeration), then the real risk becomes unpatched vulnerabilities in the web server, modules, libraries, and underlying OS.

Regularly updating and patching the server software is the most direct, high-impact countermeasure because it closes known vulnerabilities attackers routinely exploit (RCE, privilege escalation, auth bypass, path traversal, request smuggling, etc.). CEH materials also stress that virtual hosting expands the attack surface (multiple sites, shared services, shared misconfigurations), making systematic patching and configuration management even more important.

Option A (moving the document root to a different disk) may help with organization and, in some cases, recovery planning, but it does not inherently reduce vulnerabilities. Option C (changing IPs) is not a security control; it may complicate blocking lists but doesn't fix the underlying weakness. Option D (using LAMP) is an architectural choice, not a security measure by itself-an open-source stack can still be insecure if misconfigured or unpatched.

Therefore, CEH-aligned best practice is regular patching and updates.

NO.32 In the bustling financial hub of Charlotte, North Carolina, ethical hacker Raj Patel is contracted by TrustBank, a regional US bank, to evaluate their online loan application portal. On April 22, 2025, Raj tests a feature allowing customers to upload structured financial documents for loan processing. By submitting a specially crafted document, he triggers a response that exposes internal server file paths and sensitive configuration data, including database connection strings. The issue arises from the portal ' s handling of external references in document parsing, not from response manipulation, authentication weaknesses, or undetected attack attempts. Raj compiles a detailed

report to assist TrustBank ' s security team in mitigating the vulnerability.
Which type of vulnerability is Raj most likely exploiting in TrustBank ' s online loan application portal?

A. Identification and Authentication Failures

B. HTTP Response Splitting

C. XML External Entity (XXE) Injection

D. Security Logging and Monitoring Failures

Answer: C

Explanation:
The vulnerability described is characteristic of XML External Entity (XXE) Injection. In CEH web application security coverage, XXE occurs when an application parses XML input without properly disabling external entity resolution. If the XML parser is configured insecurely, an attacker can define a malicious external entity that references local files or internal system resources. When the parser processes the XML document, it resolves the external entity and may return the contents of sensitive files in the server's response.
The scenario clearly states that the issue arises from "handling of external references in document parsing" and results in exposure of internal file paths and database connection strings. This aligns directly with XXE behavior, where attackers leverage external entity declarations to retrieve local files such as configuration files, environment settings, or system credentials. In some cases, XXE can also enable server-side request forgery by forcing the server to make internal network requests.
The other options do not match the described behavior. Identification and authentication failures relate to improper access controls, not document parsing. HTTP response splitting involves manipulating headers to inject malicious responses. Security logging and monitoring failures refer to detection gaps, not data exposure through parsing. CEH-recommended mitigation strategies include disabling DTD processing, turning off external entity resolution in XML parsers, validating input formats, implementing least privilege on file access, and using secure parsing libraries that prevent XXE exploitation.

NO.33 During a penetration test for a global e-commerce platform in Dallas, ethical hacker Maria simulates a large- scale DoS campaign. Instead of sending attack traffic directly, she forges requests to multiple open services across the internet. These services unknowingly reply to the victim system, multiplying the amount of traffic hitting the target. Within minutes, the victim ' s server is overwhelmed by a flood of responses, even though Maria ' s own machine generated only a small amount of traffic.
Which attack technique is Maria most likely demonstrating?

A. Smurf Attack

B. Distributed Reflection Denial-of-Service (DRDoS)

C. Botnet

D. NTP Amplification Attack

Answer: B

Explanation:
The correct answer is B. Distributed Reflection Denial-of-Service (DRDoS) because the scenario describes the two defining elements of DRDoS: reflection and amplification at scale using third-party systems. Maria
"forges requests" (i.e., spoofs the victim's IP address as the source) to "multiple open services across the internet." Those services then send their replies to the spoofed source-the victim-so the victim

receives a large volume of unsolicited responses. This is reflection: the attacker does not attack the victim directly; instead, the attacker reflects traffic off other servers. The "multiplying the amount of traffic" indicates amplification: many protocols/services respond with packets significantly larger than the request, so the attacker's small outbound traffic results in a much larger inbound flood against the target.
The mention of "multiple open services" and being overwhelmed by a "flood of responses" is classic DRDoS behavior. From a defender's perspective, DRDoS attacks are difficult because the traffic often appears to come from legitimate servers, and the victim is receiving replies to requests it never sent. Mitigations include source address validation (BCP 38 anti-spoofing), rate limiting, filtering/ACLs for abused UDP services, and upstream scrubbing/CDN or DDoS protection.
Why the other options are less accurate: Smurf is a specific reflection/amplification attack using ICMP to a broadcast address (now largely mitigated by disabling directed broadcasts). Botnet describes the attacker's infrastructure (many compromised machines) but not the reflection/amplification mechanism; a botnet can be used to launch many types of DDoS attacks. NTP amplification is one specific DRDoS variant using misconfigured NTP servers (UDP/123). The question describes the broader technique across "multiple open services" rather than naming NTP specifically, so the best match is the general category DRDoS.
Therefore, Maria is demonstrating a Distributed Reflection Denial-of-Service (DRDoS) attack.

NO.34 A penetration tester is conducting a security assessment for a client and needs to capture sensitive information transmitted across multiple VLANs without being detected by the organization ' s security monitoring systems. The network employs strict VLAN segmentation and port security measures. Which advanced sniffing technique should the tester use to discreetly intercept and analyze traffic across all VLANs?

A. Deploy a rogue DHCP server to redirect network traffic

B. Exploit a VLAN hopping vulnerability to access multiple VLANs

C. Implement switch port mirroring on all VLANs

D. Use ARP poisoning to perform a man-in-the-middle attack

Answer: B

Explanation:
VLAN hopping is an advanced attack technique described in CEH materials, used to bypass VLAN segmentation by exploiting switch misconfigurations or vulnerabilities. Two primary methods-switch spoofing and double tagging-allow attackers to gain access to traffic from VLANs they are not authorized to view. This technique enables the capture of inter-VLAN traffic without requiring administrative privileges or triggering security tools. Port mirroring requires administrative control and is not an attack method. Rogue DHCP servers target IP assignment, not VLAN segmentation. ARP poisoning is effective only within a single broadcast domain and cannot traverse VLAN boundaries. Because the objective is to silently access multiple VLANs despite enforced segmentation, VLAN hopping is the correct technique as per CEH's network perimeter attack methodology.

NO.35 Joe, a cybersecurity analyst at Norwest Freight Services, has been assigned to run a vulnerability scan across the organization ' s infrastructure. He is specifically tasked with detecting weaknesses such as missing patches, unnecessary services, weak encryption, and authentication flaws across multiple servers. His scan identifies open ports and active services throughout the environment, providing a clear map of potential entry points for attackers.
Which type of vulnerability scanning best matches Joe ' s assignment?

A. Network-based Scanning
B. External Scanning
C. Application Scanning
D. Host-based Scanning
Answer: A
Explanation:
Joe's assignment is best described as network-based vulnerability scanning because the scan is mapping open ports and active services across multiple servers and identifying weaknesses visible through network exposure, such as unnecessary services, weak encryption configurations on network services, and authentication-related flaws reachable over the network. Network-based scanning focuses on discovering and evaluating network-accessible entry points by probing hosts and services, enumerating versions
/configurations, and correlating findings to known weaknesses.
The scenario highlights that the scan "identifies open ports and active services throughout the environment," producing "a clear map of potential entry points." That is the core outcome of network-based scanning: a view of the organization's externally or internally reachable services, where each listening port represents a possible attack path. From there, scanners can detect issues like outdated service versions (implying missing patches), insecure protocols (e.g., weak TLS ciphers), default credentials, and exposed administrative interfaces.
Why the other options are less accurate:
External scanning (B) refers to a scan performed from outside the organization's perimeter. The scenario says he is scanning across organizational infrastructure and focuses on multiple servers; it doesn't specify "from the Internet," so "external" is not the best classification.
Application scanning (C) targets web applications or specific application-layer logic (e.g., SQLi, XSS, auth bypass). Joe's focus is broader infrastructure exposure and service/port mapping.
Host-based scanning (D) typically involves local, credentialed inspection on the host (patch inventory, local config files, registry) rather than primarily mapping ports/services across many systems. While host-based scanning is valuable, the described output is network entry-point mapping.
Therefore, the scan type that best matches Joe's task is A. Network-based Scanning.