

EC Council

312-50

Certified Ethical Hacker Exam

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.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/312-50>

Latest Version: 23.5

Question: 1

A financial services firm is experiencing a sophisticated DoS attack on their DNS servers using DNS amplification and on their web servers using HTTP floods. Traditional firewall rules and IDS are failing to mitigate the attack effectively. To protect their infrastructure without impacting legitimate users, which advanced mitigation strategy should the firm implement?

- A. Increase server capacity and implement simple rate limiting
- B. Block all incoming traffic from suspicious IP ranges using access control lists
- C. Deploy a Web Application Firewall (WAF) to filter HTTP traffic
- D. Utilize a cloud-based DDoS protection service with traffic scrubbing capabilities

Answer: D

Explanation:

Cloud-based DDoS mitigation services provide upstream traffic scrubbing, detecting and filtering high-volume attacks such as DNS amplification and HTTP floods before the traffic reaches the victim's network. These services use distributed infrastructures capable of handling multi-vector attacks that surpass the capacity of traditional on-premises firewalls and IDS. Traffic scrubbing centers distinguish legitimate traffic from malicious traffic, allowing normal operations to continue without service disruption.

Question: 2

A penetration tester is assessing a web application that does not properly sanitize user input in the search field. The tester suspects the application is vulnerable to a SQL injection attack. Which approach should the tester take to confirm the vulnerability?

- A. Use directory traversal in the search field to access sensitive files on the server
- B. Input a SQL query such as 1 OR 1=1 — into the search field to check for SQL injection
- C. Perform a brute-force attack on the login page to identify weak passwords
- D. Inject JavaScript into the search field to perform a Cross-Site Scripting (XSS) attack

Answer: B

Explanation:

SQL injection is one of the most common and dangerous vulnerabilities covered in CEH training. It occurs when an application accepts unsanitized input and directly passes it to a backend SQL query. To confirm the presence of SQL injection, the tester must insert a payload that alters the

logic of the SQL query executed by the application. A classic test payload such as “1 OR 1=1 —” is widely used because it forces the database to return all rows instead of filtering based on the intended search value. This verifies whether the input field is being concatenated directly into a SQL command. The CEH methodology emphasizes starting with simple, non-destructive boolean-based payloads to safely evaluate the vulnerability without causing harm to the database or impacting server availability. Since directory traversal, brute-force login attempts, and XSS attacks target entirely different weaknesses, they are not appropriate for confirming SQL injection. The selected option aligns with proper CEH testing methodology for identifying insecure input handling and improper query construction.

Question: 3

A penetration tester is assessing the security of a corporate wireless network that uses WPA2-Enterprise encryption with RADIUS authentication. The tester wants to perform a man-in-the-middle attack by tricking wireless clients into connecting to a rogue access point. What is the most effective method to achieve this?

- A. Set up a fake access point with the same SSID and use a de-authentication attack
- B. Use a brute-force attack to crack the WPA2 encryption directly
- C. Perform a dictionary attack on the RADIUS server to retrieve credentials
- D. Execute a Cross-Site Scripting (XSS) attack on the wireless controller's login page

Answer: A

Explanation:

WPA2-Enterprise networks authenticate clients through 802.1X using a RADIUS server. A common attack method described in CEH training is to create an evil-twin access point broadcasting the same SSID as the legitimate one. Combined with de-authentication frames, clients are forced off the real AP and automatically reconnect to the stronger rogue AP. This allows the attacker to capture authentication exchanges for later misuse, including credential harvesting or EAP-based downgrade attacks.

Question: 4

A security analyst is tasked with gathering detailed information about an organization's network infrastructure without making any direct contact that could be logged or trigger alarms. Which method should the analyst use to obtain this information covertly?

- A. Examine leaked documents or data dumps related to the organization
- B. Use network mapping tools to scan the organization's IP range
- C. Initiate social engineering attacks to elicit information from employees
- D. Perform a DNS brute-force attack to discover subdomains

Answer: A

Explanation:

Passive reconnaissance focuses on collecting intelligence without interacting with the target's systems. CEH materials emphasize reviewing publicly available information, including leaked documents, breach data, reports, or exposed metadata, as this yields internal network structure details while generating no detectable traffic. This method avoids triggering monitoring systems and aligns with stealth requirements for covert intelligence gathering.

Question: 5

A penetration tester is assessing a company's HR department for vulnerability to social engineering attacks using knowledge of recruitment and onboarding processes. What is the most effective technique to obtain network access credentials without raising suspicion?

- A. Develop a fake social media profile to connect with HR employees and request sensitive information
- B. Create a convincing fake onboarding portal that mimics the company's internal systems
- C. Send a generic phishing email with a link to a fake HR policy document
- D. Conduct a phone call posing as a new employee to request password resets

Answer: B

Explanation:

Social engineering attacks that target business processes are especially effective when they mimic legitimate workflows. CEH learning materials emphasize that attackers often exploit trust relationships and organizational procedures rather than attempting broad or generic phishing methods. In the context of HR operations, onboarding portals are highly trusted and frequently accessed by new employees who expect to enter personal information, submit documents, and receive initial network credentials. By creating a fake onboarding portal that closely resembles the organization's internal system, an attacker can collect credentials without triggering suspicion because the action being requested appears normal and expected. This method leverages procedural familiarity, brand consistency, and the implied authority of HR communications, making it far more effective than generic phishing emails or unsolicited social media messages. Phone calls, while sometimes useful, involve real-time interaction and increase the chance of detection. The fake portal, however, seamlessly integrates into existing processes, making it the most effective and lowest-profile approach for acquiring network credentials.

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/>