GSDC
Global Skill Development Council

ETHICAL HACKING MCQ PRACTICE QUESTION BANK

www.gsdcouncil.org

Q1. Which of the following best defines ethical hacking?

- A) Hacking into systems for personal financial gain
- B) Authorized testing of systems to identify vulnerabilities before malicious attackers do
- C) Monitoring network traffic without the system owner's knowledge
- D) Testing systems without notifying the target organization

✅ **Answer: B** — Ethical hacking is authorized testing to find vulnerabilities.

Q2. A hacker discovers a vulnerability in a company's website and reports it without exploiting it, but without any prior authorization to test the system. What type of hacker are they?

- A) White Hat
- B) Black Hat
- C) Grey Hat
- D) Red Hat

✅ **Answer: C — Grey Hat** — They acted without authorization but did not exploit the issue.

Q3. What is the correct sequence of the 5 phases of ethical hacking?

- A) Scanning → Reconnaissance → Gaining Access → Maintaining Access → Covering Tracks
- B) Reconnaissance → Gaining Access → Scanning → Maintaining Access → Covering Tracks
- C) Reconnaissance → Scanning → Gaining Access → Maintaining Access → Covering Tracks
- D) Scanning → Gaining Access → Reconnaissance → Covering Tracks → Maintaining Access

✅ **Answer: C** — The phases begin with reconnaissance and then move to scanning.

Q4. Which of the following is the most fundamental requirement before beginning any ethical hacking engagement?

- A) A vulnerability scanner and network mapping tool
- B) Written authorization from the system owner defining scope and rules of engagement
- C) Knowledge of the target organization's technology stack
- D) A secure VPN connection to mask the tester's identity

✅ **Answer: B — Written authorization** — Written authorization is required before any testing begins.

Q5. Which phase of ethical hacking involves gathering information without directly interacting with the target system?

- A) Active Reconnaissance
- B) Scanning
- C) Passive Reconnaissance
- D) Enumeration

✅ **Answer: C** — It collects information from public sources without touching the target.

Q6. A penetration tester is given full knowledge of the target system's architecture, source code, and credentials before beginning the test. What type of penetration test is this?

- A) Black Box
- B) Grey Box
- C) White Box
- D) Red Team

✅ **Answer: C** — White box testing gives the tester complete prior knowledge.

Q7. What is the primary difference between a vulnerability scan and a penetration test?

- A) A vulnerability scan is illegal without authorization; a penetration test is not
- B) A vulnerability scan identifies potential weaknesses; a penetration test actively exploits them to confirm they are real vulnerabilities
- C) Penetration tests are automated; vulnerability scans require manual effort
- D) Vulnerability scans are performed externally; penetration tests are always internal

✅ **Answer: B** — Scans find weaknesses; penetration tests try to exploit them.

Q8. Which of the following best describes "scope creep" in ethical hacking?

- A) Discovering more vulnerabilities than expected during a test
- B) Testing systems or using techniques not covered by the written authorization
- C) Extending the duration of a penetration test without additional billing
- D) Broadening the test based on vulnerabilities discovered in the initial phase

✅ **Answer: B** — Scope creep means testing beyond the authorized boundaries.

Q9. What is Google Dorking?

- A) Using Google's internal admin tools to access private data
- B) Using advanced Google search operators to find sensitive information publicly exposed on the internet
- C) Installing malware through Google's advertising network
- D) Bypassing Google's reCAPTCHA using automated tools

✅ **Answer: B** — Uses search operators to find publicly exposed sensitive info.

Q10. What information does a WHOIS lookup provide during reconnaissance?

- A) The internal network topology of the target organization
- B) Encrypted passwords used by the target's web application
- C) Domain registration details including owner, registrar, and contact information
- D) A list of all users on the target system

✅ **Answer: C** — Provides domain registration details and contact info.

Q11. Which scanning technique sends a SYN packet and waits for a response without completing the three-way TCP handshake?

- A) Full Connect Scan
- B) UDP Scan
- C) SYN Scan (Half-Open Scan)
- D) XMAS Scan

✅ **Answer: C — SYN Scan (Half-Open Scan)** — Sends SYN packets without completing the handshake.

Q12. What does banner grabbing reveal to an ethical hacker during the scanning phase?

- A) The target user's login credentials
- B) Service and software version information running on open ports
- C) The encryption key used by the target system
- D) The physical location of the target server

✅ **Answer: B** — Reveals service names and version information on open ports.

Q13. What is the purpose of OS fingerprinting during a penetration test?

- A) To obtain a physical copy of the target's operating system files
- B) To identify the operating system running on a target to find version-specific vulnerabilities
- C) To decrypt files on the target operating system
- D) To bypass operating system login screens

✅ **Answer: B** — Identifies the target OS to help find version-specific vulnerabilities.

Q14. What is enumeration in the context of ethical hacking?

- A) Counting the number of systems on a network
- B) Extracting specific details from a target — user accounts, network shares, services — to prepare for exploitation
- C) Documenting vulnerabilities discovered during scanning
- D) Scanning a network for open wireless access points

✅ **Answer: B** — Gathers actionable details like usernames, shares, and services.

Q15. Which of the following is an example of active reconnaissance?

- A) Reading the target organization's annual report
- B) Searching LinkedIn for employees at the target company
- C) Performing a port scan on the target's IP address range
- D) Looking up the target's domain registration in WHOIS

✅ **Answer: C** — Port scanning directly interacts with the target system.

Q16. What does DNS enumeration reveal that is useful for an ethical hacker?

- A) The encryption algorithms used by the target's web server
- B) Subdomains, mail servers, and other DNS records that reveal the target's infrastructure
- C) Physical network cable topology
- D) User account password policies

✅ **Answer: B** — Reveals subdomains and records that expose infrastructure.

Q17. What is a buffer overflow attack?

- A) Sending too many login attempts to lock out an account
- B) Sending more data to a program than it can handle, overwriting memory
- C) Overloading a web server with too many HTTP requests
- D) Filling a database with duplicate records to slow down queries

✅ **Answer: B** — It sends excess data that can overwrite memory and run code.

Q18. What is the primary goal of the "Maintaining Access" phase of ethical hacking?

- A) Continuing to extract data from the target system
- B) Testing whether sustained unauthorized access would be detected
- C) Keeping the target system running to avoid detection
- D) Maintaining documentation of all discovered vulnerabilities

✅ **Answer: B** — It checks whether persistence would be detected over time.

Q19. What is a rootkit?

- A) A tool used to scan for open ports on a network
- B) Software that allows administrators to manage root-level system access
- C) Malware designed to hide itself and other malicious software
- D) A legitimate tool for managing system startup processes

✅ **Answer: C** — It hides malicious software and helps maintain privileged access.

Q20. What distinguishes a Trojan from a virus?

- A) A Trojan self-replicates; a virus does not
- B) A Trojan disguises itself as legitimate software; a virus attaches to files and self-replicates
- C) A Trojan targets networks; a virus targets individual files
- D) A Trojan is always detected by antivirus; a virus evades detection

✅ **Answer: B** — A Trojan pretends to be legit; a virus spreads by copying itself.

Q21. Which password attack method tries every possible combination of characters until the correct password is found?

- A) Dictionary Attack
- B) Rainbow Table Attack
- C) Brute Force Attack
- D) Credential Stuffing

✅ **Answer: C — Brute Force Attack** — Tries every possible password combination.

Q22. What is credential stuffing?

- A) Adding extra characters to a password to make it longer before hashing
- B) Using lists of username and password pairs from previous data breaches to attempt login to other services
- C) Stuffing multiple credentials into a single login request to bypass rate limiting
- D) Encoding credentials in base64 to evade security filters

✅ **Answer: B** — Uses leaked credentials from one breach on other sites.

Q23. What is privilege escalation in the context of system hacking?

- A) Requesting additional permissions from a system administrator
- B) Gaining higher-level access rights than were initially obtained — such as moving from a regular user to an administrator
- C) Escalating a security incident to management
- D) Increasing the severity rating of a discovered vulnerability

✅ **Answer: B** — Gaining higher permissions than initially granted.

Q24. A penetration tester installs a backdoor on a system after gaining access. What is the legitimate purpose of this action during an ethical hacking engagement?

- A) To give the tester remote access for personal use after the engagement
- B) To test whether the organization's monitoring and detection systems would identify and remove the backdoor
- C) To ensure the tester can return if the vulnerability is patched before the report is written
- D) To demonstrate that the tester has administrator privileges

✅ **Answer: B** — Tests whether monitoring can detect the backdoor.

Q25. What is a Man-in-the-Middle (MITM) attack?

- A) An attack where the attacker physically sits between two servers in a data center
- B) An attack where the attacker secretly intercepts and potentially alters communication between two parties who believe they are communicating directly with each other
- C) An attack where a middleman is bribed to share confidential data
- D) An attack targeting the middle tier of a three-tier application architecture

✅ **Answer: B** — The attacker intercepts or alters communication between two parties without their knowledge.

Q26. What is ARP poisoning and why is it dangerous?

- A) Corrupting DNS records to redirect users to malicious websites
- B) Sending forged ARP messages to associate the attacker's MAC address with a legitimate IP address, enabling interception of network traffic
- C) Poisoning a web application's session management system
- D) Injecting malicious code into ARP-compliant routers

✅ **Answer: B** — Fake ARP replies redirect traffic to the attacker's device.

Q27. What is a SQL injection attack?

- A) Physically injecting a USB device into a database server
- B) Inserting malicious SQL code into user input fields to manipulate database queries
- C) Injecting SQL scripts into network packets to alter routing
- D) Using SQL commands to overflow a system's memory buffer

✅ **Answer: B** — Malicious input changes the database query to expose or alter data.

Q28. What is Cross-Site Scripting (XSS)?

- A) Running scripts across multiple servers simultaneously to increase processing power
- B) Injecting malicious scripts into web pages that are then executed by other users' browsers
- C) Cross-referencing scripts from different programming languages in one application
- D) Using scripts to bypass cross-origin resource sharing (CORS) policies

✅ **Answer: B** — Malicious scripts run in other users' browsers when they load the page.

Q29. What is a Denial of Service (DoS) attack and how does it differ from a DDoS attack?

- A) DoS targets data; DDoS targets the operating system
- B) DoS comes from a single source; DDoS comes from multiple distributed sources simultaneously
- C) DoS is legal; DDoS is illegal
- D) DoS is a physical attack; DDoS is a software attack

✅ **Answer: B** — DoS comes from one source; DDoS comes from many sources at once.

Q30. What layer of the OSI model does a SYN flood attack target?

- A) Layer 7 — Application
- B) Layer 3 — Network
- C) Layer 2 — Data Link
- D) Layer 4 — Transport

✅ **Answer: D** — SYN floods target TCP at the Transport layer.

Q31. According to the OWASP Top 10, which vulnerability type involves users accessing data or functions they should not be permitted to?

- A) Injection
- B) Cryptographic Failures
- C) Broken Access Control
- D) Security Misconfiguration

✅ **Answer: C** — Broken Access Control lets users access unauthorized data or actions.

Q32. What is a session hijacking attack?

- A) Stealing a user's physical session token card
- B) Taking over an authenticated user session by stealing or predicting their session token
- C) Hijacking the server's session management software
- D) Intercepting session data during the login process before authentication is complete

✅ **Answer: B** — Session hijacking steals a valid session token to impersonate a user.

Q33. Which type of malware encrypts the victim's files and demands payment for the decryption key?

- A) Spyware
- B) Adware
- C) Ransomware
- D) Rootkit

✅ **Answer: C — Ransomware** — It encrypts files and demands payment for the key.

Q34. A worm differs from a virus primarily because:

- A) A worm targets hardware; a virus targets software
- B) A worm self-replicates across networks without needing to attach to a host file; a virus attaches to existing files
- C) A worm is always more destructive than a virus
- D) A worm can only spread through email; a virus spreads through all channels

✅ **Answer: B** — Worms spread on their own; viruses need a host file.

Q35. What is pretexting in social engineering?

- A) Sending a deceptive text message to a target to steal credentials
- B) Creating a fabricated scenario or false identity to manipulate a target into revealing information
- C) Placing malware on a website frequently visited by the target
- D) Sending a pre-authorized test phishing email to employees

✅ **Answer: B** — It uses a false identity or scenario to trick the target.

Q36. What is a watering hole attack?

- A) Flooding a victim's network with traffic to cause a DoS condition
- B) Compromising a website frequently visited by the target group and waiting for them to visit it
- C) Physically accessing water-cooled data center equipment to install hardware keyloggers
- D) Using excessive authentication failures to lock out target accounts

✅ **Answer: B** — It compromises a trusted site the target group visits.

Q37. Which wireless security protocol is considered most secure and is currently recommended as the industry standard?

- A) WEP
- B) WPA
- C) WPA2
- D) WPA3

✅ **Answer: D — WPA3** — WPA3 is the current Wi-Fi security standard.

Q38. What is an Evil Twin attack in the context of wireless security?

- A) Running two identical malware programs simultaneously to double processing power
- B) Creating a rogue wireless access point with the same name (SSID) as a legitimate network to intercept victim traffic
- C) Duplicating a victim's MAC address to bypass MAC filtering
- D) Cloning an employee's RFID badge to gain physical access

✅ **Answer: B** — A fake AP mimics a real network to intercept traffic.

Q39. What does the term "zero-day vulnerability" mean?

- A) A vulnerability that has existed for zero days — discovered on the day of disclosure
- B) A vulnerability that takes zero effort to exploit
- C) A vulnerability for which no patch or fix exists because it has not yet been publicly disclosed
- D) A vulnerability that affects systems with zero existing security controls

✅ **Answer: C** — It is undisclosed and has no patch yet.

Q40. A spear phishing attack differs from a standard phishing attack because:

- A) Spear phishing uses social media; standard phishing uses email
- B) Spear phishing is a highly targeted attack on a specific individual using personalized information; phishing is broadly sent to many recipients
- C) Spear phishing only targets financial institutions; phishing targets any organization
- D) Spear phishing uses malicious attachments; phishing uses malicious links

✅ **Answer: B** — Spear phishing targets one person with personalized deception.

Q41. What is the primary difference between symmetric and asymmetric encryption?

- A) Symmetric encryption is stronger; asymmetric encryption is faster
- B) Symmetric encryption uses the same key to encrypt and decrypt; asymmetric uses a public key to encrypt and a private key to decrypt
- C) Symmetric encryption is used for files; asymmetric is used for network traffic
- D) Symmetric encryption is one-way; asymmetric encryption is two-way

✅ **Answer: B** — Symmetric uses one shared key; asymmetric uses a public/private key pair.

Q42. What is the purpose of a cryptographic salt?

- A) To add flavor to an encryption algorithm to make it harder to reverse
- B) To add random data to a password before hashing so that identical passwords produce different hash values, preventing rainbow table attacks
- C) To encrypt a hash to add a second layer of protection
- D) To extend the length of an encryption key to meet minimum security requirements

✅ **Answer: B** — A salt makes identical passwords hash differently and helps defeat rainbow tables.

Q43. What is a rainbow table attack?

- A) An attack that cycles through all colors of the visible light spectrum to crack optical security systems
- B) An attack using precomputed tables of hash values to reverse password hashes rapidly
- C) A multi-stage attack that progresses through different attack types in sequence
- D) An attack that targets graphical user interfaces to bypass visual CAPTCHAs

✅ **Answer: B** — It uses precomputed hash tables to look up passwords quickly.

Q44. In digital forensics, what is the "chain of custody"?

- A) The sequence of commands executed during a penetration test
- B) A documented record of who handled evidence, when, and how — ensuring evidence integrity for legal proceedings
- C) The hierarchy of authority in an incident response team
- D) The sequence of events in a cyberattack reconstructed from log files

✅ **Answer: B** — It records who handled evidence to preserve its integrity.

Q45. What is steganography?

- A) Writing malware in a way that hides its true purpose
- B) The practice of hiding information within other non-secret data or files — such as hiding a message inside an image
- C) Using strong encryption to make data unreadable
- D) Hiding network traffic by disguising it as normal web traffic

✅ **Answer: B** — It hides a message inside ordinary-looking data.

Q46. What does the Computer Fraud and Abuse Act (CFAA) primarily govern?

- A) Regulations for computer hardware manufacturers in the United States
- B) Federal criminal penalties for unauthorized access to computer systems in the United States
- C) Data protection requirements for companies handling consumer financial data
- D) Licensing requirements for cybersecurity professionals

✅ **Answer: B** — It covers unauthorized access to computer systems.

Q47. What is the primary purpose of covering tracks during an ethical hacking engagement?

- A) To protect the ethical hacker's identity from the target organization
- B) To avoid triggering security alerts that would end the engagement prematurely
- C) To test whether the organization's logging, monitoring, and detection systems would identify an attacker attempting to erase evidence of their presence
- D) To comply with legal requirements for penetration testers

✅ **Answer: C** — It tests whether defenders can detect log tampering.

Q48. An ethical hacker discovers a critical vulnerability in a system that is outside the defined testing scope. What is the correct course of action?

- A) Test the vulnerability to understand its full impact and include it in the report
- B) Ignore the vulnerability as it is outside scope
- C) Report the potential vulnerability through proper channels without testing it
- D) Patch the vulnerability immediately to protect the organization

✅ **Answer: C** — Report it without testing or exploiting it.

Q49. What is the purpose of a penetration test report's executive summary?

- A) To provide technical details of every vulnerability found for the security team
- B) To document the tools and techniques used during the engagement
- C) To communicate the business risk and key findings to non-technical stakeholders in plain language
- D) To provide legal documentation of the testing authorization

✅ **Answer: C** — It gives business leaders a plain-language summary of the key risks and findings.

Q50. What does CVE stand for and why is it important in ethical hacking?

- A) Critical Vulnerability Exposure — a severity rating system for vulnerabilities
- B) Common Vulnerabilities and Exposures — a standardized identifier for publicly known security vulnerabilities
- C) Cyber Vulnerability Evaluation — an assessment framework for penetration testers
- D) Computer Vulnerability Encyclopedia — a comprehensive database of all known exploits

✅ **Answer: B — Common Vulnerabilities and Exposures** — It is a standard ID used to reference known vulnerabilities consistently.

End of Question Bank — This completes all 50 exam-style MCQs for the **GSDC Certified Ethical Hacking Foundation** certification. Review any questions where you selected an incorrect answer, paying particular attention to the explanations which highlight the key distinctions tested in the exam.

GSDC
Global Skill Development Council

CERTIFIED ETHICAL HACKING FOUNDATION (CEHF)

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING OBJECTIVE

- Gain insights into autonomous decision-making processes
- Apply knowledge using ready-to-implement templates
- Demonstrate ability to work with Agentic AI models
- Validate your skills wit

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org