# CEH v13 Module 1: Introduction to Ethical Hacking

## Practice Questions & Scenario-Based Mastery

### Question 1

A financial analyst notices that several transaction records in the database were subtly altered over the weekend, although no data was stolen. Which pillar of the CIA Triad has been specifically compromised in this scenario?

* A) Confidentiality
* B) Integrity
* C) Availability
* D) Non-Repudiation

Correct Answer: B) Integrity

Rationale: Integrity ensures that data remains accurate and hasn't been modified by unauthorized parties. Unauthorized modification is a direct breach of integrity.

### Question 2

An individual discovers a critical vulnerability in a popular social media app. Without obtaining prior permission, they exploit the vulnerability to prove it exists, then contact the company to demand a 'bug bounty' payment. How would EC-Council classify this hacker?

* A) White Hat
* B) Black Hat
* C) Grey Hat
* D) Suicide Hacker

Correct Answer: C) Grey Hat

Rationale: Grey hats operate in a legal middle ground. They often perform unauthorized research but lack the purely destructive intent of a Black Hat.

### Question 3

During a penetration test, a consultant uses 'Google Dorking' to find sensitive configuration files accidentally exposed on a client's web server. Which phase of the hacking methodology is the consultant currently in?

* A) Scanning
* B) Reconnaissance
* C) Gaining Access
* D) Maintaining Access

Correct Answer: B) Reconnaissance

Rationale: Gathering information about the target using public search engines is a form of passive reconnaissance.

### Question 4

An attacker successfully exploits a web server and immediately installs a hidden Netcat listener that triggers every time the system reboots. Which phase of the hacking methodology does this action represent?

* A) Scanning
* B) Gaining Access
* C) Maintaining Access
* D) Clearing Logs

Correct Answer: C) Maintaining Access

Rationale: Ensuring continued control over a compromised system through backdoors or persistent listeners is the hallmark of the "Maintaining Access" phase.

### Question 5

A retail company experiences a breach where thousands of customer credit card numbers are stolen from their database. Which regulatory standard will likely impose the most significant fines for this specific failure?

* A) HIPAA
* B) PCI-DSS
* C) SOX
* D) DMCA

Correct Answer: B) PCI-DSS

Rationale: The Payment Card Industry Data Security Standard is specifically designed to protect credit card data and transactions.

### Question 6

A group of hackers launches a massive DDoS attack against a government website to protest a new law. They do not use proxies to hide their IP addresses and state they are prepared to go to jail for their cause. Which type of hacker is this?

* A) State-Sponsored Hacker
* B) Script Kiddie
* C) Suicide Hacker
* D) White Hat

Correct Answer: C) Suicide Hacker

Rationale: Suicide hackers operate with the intent to cause damage regardless of whether they are captured or identified.

### Question 7

According to the Lockheed Martin Cyber Kill Chain, which stage involves the attacker creating a malicious payload, such as a PDF containing a Trojan, specifically for a target?

* A) Reconnaissance
* B) Weaponization
* C) Delivery
* D) Exploitation

Correct Answer: B) Weaponization

Rationale: Weaponization is the process of coupling an exploit with a backdoor into a deliverable payload.

### Question 8

A CEO signs an electronic contract using a digital signature. Later, she claims she never saw the document and that her signature was forged. The system proves the signature matches her private key. Which security concept prevents her from denying the action?

* A) Integrity
* B) Confidentiality
* C) Non-Repudiation
* D) Availability

Correct Answer: C) Non-Repudiation

Rationale: Non-repudiation ensures that a party cannot later deny the validity of an action or message they originated.

### Question 9

A hospital IT administrator discovers that an employee was selling patient medical histories to a local insurance broker. This breach is a primary violation of which US federal law?

* A) FISMA
* B) HIPAA
* C) GLBA
* D) COBIT

Correct Answer: B) HIPAA

Rationale: HIPAA (Health Insurance Portability and Accountability Act) sets strict standards for protecting sensitive patient health information.

### Question 10

An ethical hacker is hired to test a company's external network. During the test, he finds a vulnerability in a cloud server owned by a third-party partner of the client. He exploits it to show the client how their partner's weakness affects them. Why is this action unethical?

* A) He didn't find a significant enough bug.
* B) The hacker exceeded the defined scope of the engagement.
* C) Cloud servers cannot be legally tested by ethical hackers.
* D) Reporting a partner's vulnerability is a violation of HIPAA.

Correct Answer: B) The hacker exceeded the defined scope of the engagement.

Rationale: Ethical hackers must strictly adhere to the boundaries (IPs, domains) defined in the written "Rules of Engagement."

### Question 11

A security operations center (SOC) team is analyzing an ongoing intrusion. They use a matrix to identify that the attacker used 'PowerShell' for execution and 'Registry Run Keys' for persistence. Which framework are they utilizing?

* A) Cyber Kill Chain
* B) MITRE ATT&CK
* C) OSSTMM
* D) NIST 800-53

Correct Answer: B) MITRE ATT&CK

Rationale: MITRE ATT&CK is a comprehensive matrix used to categorize and track specific adversary tactics and techniques.

### Question 12

After extracting sensitive files, an attacker runs a script to delete the Windows Security Event Log and modifies the timestamps of the malicious files to match system files. What is the primary purpose of this phase?

* A) Gaining Access
* B) Reconnaissance
* C) Clearing Logs
* D) Enumeration

Correct Answer: C) Clearing Logs

Rationale: This phase involves hiding "digital footprints" to evade detection and hinder forensic analysis.

### Question 13

A public company’s internal auditor discovers that the IT department hasn't been keeping logs of who accesses the financial database for over a year. This lack of accountability is a violation of which law?

* A) DMCA
* B) SOX
* C) GDPR
* D) PCI-DSS

Correct Answer: B) SOX

Rationale: The Sarbanes-Oxley Act requires public companies to maintain strict internal controls and audit trails for financial data.

### Question 14

A high school student downloads a tool that automatically scans for vulnerabilities in WordPress sites and attempts to exploit them using a pre-written list of payloads. The student doesn't understand the underlying code. How is this student classified?

* A) Ethical Hacker
* B) Script Kiddie
* C) Hacktivist
* D) Black Hat

Correct Answer: B) Script Kiddie

Rationale: Script kiddies rely on automated tools and scripts written by others because they lack the skill to create their own.

### Question 15

A US-based e-commerce site realizes they have a large customer base in France and Germany. They must now ensure their data handling policies comply with which specific privacy framework?

* A) FISMA
* B) SOX
* C) GDPR
* D) HIPAA

Correct Answer: C) GDPR

Rationale: The General Data Protection Regulation applies to any organization processing the personal data of EU residents.

### Question 16

A company implements Multi-Factor Authentication (MFA) requiring a password, a fingerprint, and a one-time code sent via SMS. Which security concept is primarily strengthened by these multiple layers?

* A) Availability
* B) Authenticity
* C) Non-Repudiation
* D) Confidentiality

Correct Answer: B) Authenticity

Rationale: Authenticity verifies that a user is who they claim to be; MFA significantly raises the level of proof required.

### Question 17

An intelligence agency launches a cyberattack against a rival nation's power grid to disable it during a military conflict. How is this type of activity classified?

* A) Defensive Information Warfare
* B) Offensive Information Warfare
* C) Ethical Hacking
* D) Social Engineering

Correct Answer: B) Offensive Information Warfare

Rationale: Offensive Information Warfare involves attacking an opponent's information assets or infrastructure for competitive/military advantage.

### Question 18

A penetration tester is gathering information about a target. He performs a 'WHOIS' search and looks at the target's public job postings on LinkedIn. What type of reconnaissance is he performing?

* A) Active Reconnaissance
* B) Passive Reconnaissance
* C) Enumeration
* D) Gaining Access

Correct Answer: B) Passive Reconnaissance

Rationale: Gathering information without directly interacting with the target's network (using public records) is passive reconnaissance.

### Question 19

An attacker uses a known buffer overflow vulnerability in an unpatched server to execute a remote shell and gain a command prompt. Which phase of the hacking methodology has just been completed?

* A) Scanning
* B) Gaining Access
* C) Maintaining Access
* D) Clearing Logs

Correct Answer: B) Gaining Access

Rationale: Gaining access occurs when an attacker exploits a vulnerability to bypass security and enter a system.

### Question 20

In the Lockheed Martin Cyber Kill Chain, an attacker successfully exfiltrates 5GB of sensitive corporate data to an external server. Which stage does this represent?

* A) Command and Control (C2)
* B) Installation
* C) Actions on Objectives
* D) Delivery

Correct Answer: C) Actions on Objectives

Rationale: This final stage is where the attacker achieves their ultimate goal, such as data theft or destruction.