C|EH Prep

Certified | Ethical Hacker

Prepared by Youssef Mohamed



Explain Information Security Concepts

CypherPanther

EC-COUNCIL

(International Council of E-Commerce Consultants**)** is a globally recognized organization specializing in **cybersecurity**. Founded in 2001 in the United States,

Penetration Tester

Security Analyst



Vulnerability Analyst

Cybersecurity Consultant

it is renowned for offering industry-recognized certifications in **ethical hacking**, **network security**, and **incident response**.

Some of its popular certifications:

- **C**ertified **E**thical **H**acker **(CEH)**
  - Focuses on ethical hacking techniques to test the security of systems and networks.

- **C**ertified **N**etwork **D**efender **(CND)**
  - Specializes in securing and protecting networks from threats and attacks.

- **C**ertified **I**ncident **H**andler **(ECIH)**
  - Focuses on incident handling, response, and containment.



- **L**icensed **P**enetration **T**ester **(LPT)**
  - An advanced certification for professional penetration testing.

- **C**ertified **C**hief **I**nformation **S**ecurity **O**fficer **(CCISO)**
  - Designed for senior-level professionals to develop leadership in cybersecurity strategies.

CEH Exam Information

Item	Details
Exam Title	Certified Ethical Hacker (CEH)
Exam Code	312-50
Availability / Delivery	EC-Council Exam Portal (EC-Council) and VUE (Pearson VUE)
Duration	4 Hours
Number of Questions	125
Passing Score	See EC-Council FAQ for the current passing score (may vary by exam version)

confidentiality, integrity, availability,authenticity and Non-repudiation

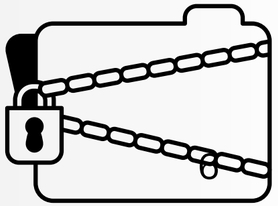
confidentiality :

- **Meaning:**
  - Ensures that information is only accessible to those who are authorized.

- **Threats:**
  - Data leakage, eavesdropping/sniffing, insider misuse, weak encryption.

- **Controls:**
  - Encryption (AES-256 for storage, TLS 1.2/1.3 for transmission).
  - Access control (RBAC, least privilege).
  - Multi-Factor Authentication (MFA).
  - Data Loss Prevention (DLP) tools.

- **Example:**
  - Payroll data is stored encrypted and only HR staff can access it with MFA.



Integrity:

- **Meaning:**
  - Protects data from unauthorized or accidental modification; ensures accuracy and trustworthiness.

- **Threats:**
  - Unauthorized changes, database corruption, Man-in-the-Middle attacks, software tampering.

- **Controls:**
  - Cryptographic hashes (SHA-256, SHA-3).
  - Digital signatures.
  - File Integrity Monitoring (FIM).
  - Verified backups with checksum comparison.

- **Example:**
  - A downloaded software package is verified with its vendor’s digital signature before installation.



Availability:

- **Meaning:**
  - Systems and data must be accessible to authorized users when needed.

- **Threats:**
  - DDoS attacks, ransomware, hardware failure, natural disasters, misconfigurations.

- **Controls:**
  - High-Availability (HA) setups with redundancy.
  - Load balancing and auto-scaling.
  - Disaster Recovery (DR) and Business Continuity Plans.
  - Regular tested backups.

- **Example:**
  - A banking system remains online during a server crash thanks to failover and replication



Authenticity:

- **Meaning:**
  - Ensures that data, communications, or entities are genuine and not impersonated.

- **Threats:**
  - Phishing, identity spoofing, fake certificates, DNS hijacking.

- **Controls:**
  - PKI and digital certificates.
  - Mutual TLS (mTLS).
  - Strong user authentication (password + MFA).
  - Signed tokens (JWT).



- **Example:**
  - When you visit a website with HTTPS, the digital certificate proves the server is authentic.

Non-Repudiation:

- **Meaning:**
  - Provides proof that someone performed an action (e.g., sent a message, approved a transaction) and prevents them from later denying it.

- **Threats:**
  - Disputes over transactions, denial of responsibility, altered logs.

- **Controls:**
  - Digital signatures with private/public key pairs.
  - Trusted timestamping services.
  - Tamper-evident logs and audit trails.



- **Example:**
  - An electronically signed contract with a timestamp ensures the signer cannot deny having signed it.

Detailed comparison between Hash and Encryption

Hash:

- **Function:**
  - Used to generate a fixed-length hash value from any amount of data.
- **Usage:**
  - Widely used for data **integrity** verification and digital signature generation.
- **Retrieval:**
  - Original data cannot be retrieved from the hash value; hashing is a (**one-way function**)
- **Processing Speed:**
  - Hashing operations are typically faster than encryption operations.
- **Use Cases:**
  - Data integrity verification.
  - Secure storage of passwords (with the addition of salt)

Encryption :

- **Function:**
  - Used to transform data into an unreadable form using a key, and the original data can be recovered using the appropriate key.
- **Usage:**
  - Used to secure data and protect it from unauthorized access. (**confidentiality**)



- **Retrieval:**
  - The original data can be retrieved using the correct key (**Two-way function**)
- **Processing Speed:**
  - Usually slower than hashing due to additional operations related to encryption and key verification
- **Use Cases:**
  - Protection of sensitive data.
  - Securing online communications (HTTPS).
  - Establishing secure communication channels.

Attacker Equation

Attack = Motive (Goal) + Method (TTP) + Vulnerability

This is a logical model, not a strict arithmetic formula. All three components must be present (to some degree) for an attacker to succeed. The strength or likelihood of success increases as each component becomes stronger/more available.

Motive (Goal)

- **Meaning:**
  - the attacker's why — what they want to achieve.

- **What determines motive:**
  - money, political objectives, corporate espionage, revenge, fame, discovery, or simply curiosity. Different motives cause different attacker profiles and investment levels (e.g., a nation-state vs. a script kiddie).

- **Indicators of motive:**
  - targeting of specific departments (finance, R&D), timing (around a corporate event), customized social-engineering lures.

- **Defender actions:**
  - perform threat profiling — ask "who would want this asset and why?" — and prioritize protection of crown- jewels accordingly.

Method — TTP (Tactics, Techniques, Procedures)

- **Tactic (big picture):** the attack stage or objective — e.g., Initial Access, Persistence, Privilege Escalation, Lateral Movement, Data Collection, Exfiltration, Impact.
  - **Use:** helps design high-level playbooks (e.g., “Initial Access playbook”).

- **Technique (how, generally):** a category of behavior used to fulfill a tactic — e.g., phishing, exploiting a public-facing app, credential stuffing, using scheduled tasks for persistence, DNS tunneling for exfiltration.
  - **Use:** informs controls (email security, web app hardening, MFA).

- **Procedure (exact steps):** attacker-specific, low-level actions and artifacts — the exact chain of steps, tools, filenames, command patterns, C2 behavior or timing that an actor uses.
  - **Use:** yields high-fidelity indicators (IOCs) for fast detection and blocking.

- **Why the distinction matters:**
  - If you know tactics, you prepare playbooks and monitoring categories.
  - If you know techniques, you add controls that stop broad classes of attacks.
  - If you know procedures, you can hunt, block, and attribute using precise indicators.

- **Defender actions:**

map likely adversaries → map their common TTPs (MITRE ATT&CK is a useful taxonomy) → build detections and controls at each level.

Vulnerability (Weakness)

- **Meaning:**
  - a weakness in people, processes, or technology that the method can exploit.

- **Types:**
  - software bugs, misconfiguration, excessive privileges, weak authentication, exposed services, human error (phishing-prone users).

- **How it fits the equation:**
  - without a usable vulnerability, even a motivated attacker with a method cannot achieve the objective.

- **Defender actions:**
  - asset inventory → vulnerability scanning → patching/prioritization → hardening → least privilege → user training.

Classification of attacks

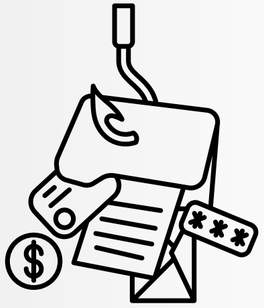
Passive Attacks:

- These involve monitoring systems or networks to gather information without altering them.
- **Example:** Intercepting network traffic to capture data (e.g., passwords or emails).



Active Attacks

- These involve actions to disrupt, modify, or damage systems or data.
- **Example:** Injecting malicious code, altering communication, or performing DoS attacks.



Close-in Attacks

- These require physical proximity to the target system or network.
- **Example:** Gaining access to a system by being near its hardware (e.g., plugging a malicious USB).



Insider Attacks

- Carried out by individuals with legitimate access to an organization's systems or data.
- **Example:** Employees stealing sensitive information or sabotaging systems.



Distribution Attacks

- These involve tampering with hardware or software components before they are distributed.
- **Example:** Pre-installing malware on devices during manufacturing or supply chain attacks.





InfoWar is the use of information and communication technologies (ICT) to gain a competitive, political, military, or economic advantage over an opponent. It includes both defensive activities (protecting ICT assets) and offensive activities (attacking an opponent's ICT assets). In modern contexts it mixes traditional cyber operations, electronic warfare, psychological operations, and information operations.

Defensive Information Warfare

This is everything organizations do to protect their ICT assets and to reduce the impact of adversary operations. The slide breaks defensive efforts into phases or capabilities:

Prevention

- **Meaning:** measures to stop attacks before they occur.
- **Examples:** patch management, secure configurations, firewalls, strong authentication, network segmentation, secure SDLC.
- **Why it matters:** reduces the attack surface and the number of exploitable vulnerabilities.

Alerts

- **Meaning:** early-warning systems that notify defenders of suspicious events.
- **Examples:** IDS/IPS alerts, SIEM alerts, vendor threat feeds, honeypots, cloud security alerts.
- **Why it matters:** early detection shortens time-to-detect and enables faster containment.

Deterrence

- **Meaning:** measures that raise the attacker's cost/risk so they are less likely to attack.
- **Examples:** visible logging/monitoring, publicized legal or law-enforcement ties, strong incident response capability, cyber insurance, active threat hunting and attribution capabilities.
- **Why it matters:** some attackers avoid well-defended or easily-attributed targets.

Detection

- **Meaning:** continuous monitoring to identify successful or in-progress attacks.
- **Examples:** EDR telemetry, network flow analysis (NetFlow), log aggregation + analytics, anomaly detection, threat hunting.
- **Why it matters:** effective detection finds attacks that prevention missed.

Emergency Preparedness

- **Meaning:** planning and readiness for handling incidents at scale.
- **Examples:** incident response plans, defined RTO/RPO, table-top exercises, communication plans, backup & DR readiness.
- **Why it matters:** preparedness reduces downtime and business impact during major incidents.

Response

- **Meaning:** actions taken during and after an incident to contain, eradicate, recover and learn.
- **Examples:** isolate infected systems, forensic collection, patching exploited systems, restore from backups, post-incident reviews, legal/PR coordination.
- **Why it matters:** controls damage, supports prosecution/attribution and improves future defenses.

Offensive Information Warfare

This refers to actions that attack or manipulate an opponent's ICT assets to achieve objectives (political, economic, military, or disruptive). The slide lists common offensive categories:

Web Application Attacks

- **Examples:** SQL injection, Cross-Site Scripting (XSS), broken auth, insecure deserialization, SSRF.
- **Intent:** steal data, deface sites, pivot into back-end systems, or inject malicious content to target users.
- **Defender focus:** secure coding, WAFs, SAST/DAST, input validation, least privilege for DB accounts.

Web Server Attacks

- **Examples:** exploiting unpatched web server software (Apache/IIS/Nginx), misconfigurations, exploiting server modules, directory traversal, remote code execution.
- **Intent:** gain server shell, host phishing/malware, remove availability.
- **Defender focus:** patching OS and server software, hardening, HIPS, LFI/RCE mitigations.

Malware Attacks

- **Examples:** ransomware, banking trojans, backdoors, spyware. Techniques include initial delivery via phishing, drive-by download, or infected supply-chain.
- **Intent:** data theft, extortion, persistent espionage, system destruction.
- **Defender focus:** EDR, application allowlisting, backups (offline/immutable), network segmentation.

MITM (Man-in-the-Middle) Attacks

- **Examples:** session hijacking, SSL stripping, ARP spoofing, DNS spoofing, rogue Wi-Fi access points, TLS interception.
- **Intent:** intercept credentials, inject or modify traffic, sabotage communications.
- **Defender focus:** use strong TLS, HSTS, DNSSEC, mutual authentication where appropriate, secure Wi-Fi, certificate pinning.

System Hacking

- **Examples:** exploitation of OS vulnerabilities, privilege escalation, kernel exploits, credential dumping (LSASS), lateral movement (Pass-the-Hash).
- **Intent:** full control of hosts, pivot into network, long-term persistence.
- **Defender focus:** least privilege, PAM, endpoint protection, monitoring for suspicious process activity, patching, network segmentation..



CypherPanther

You can follow us here

Thank you