Certified Ethical Hacker (CEH) Lab Report

Hands-on Ethical Hacking and Cybersecurity Exercises

EC-COUNCIL C|EH v13

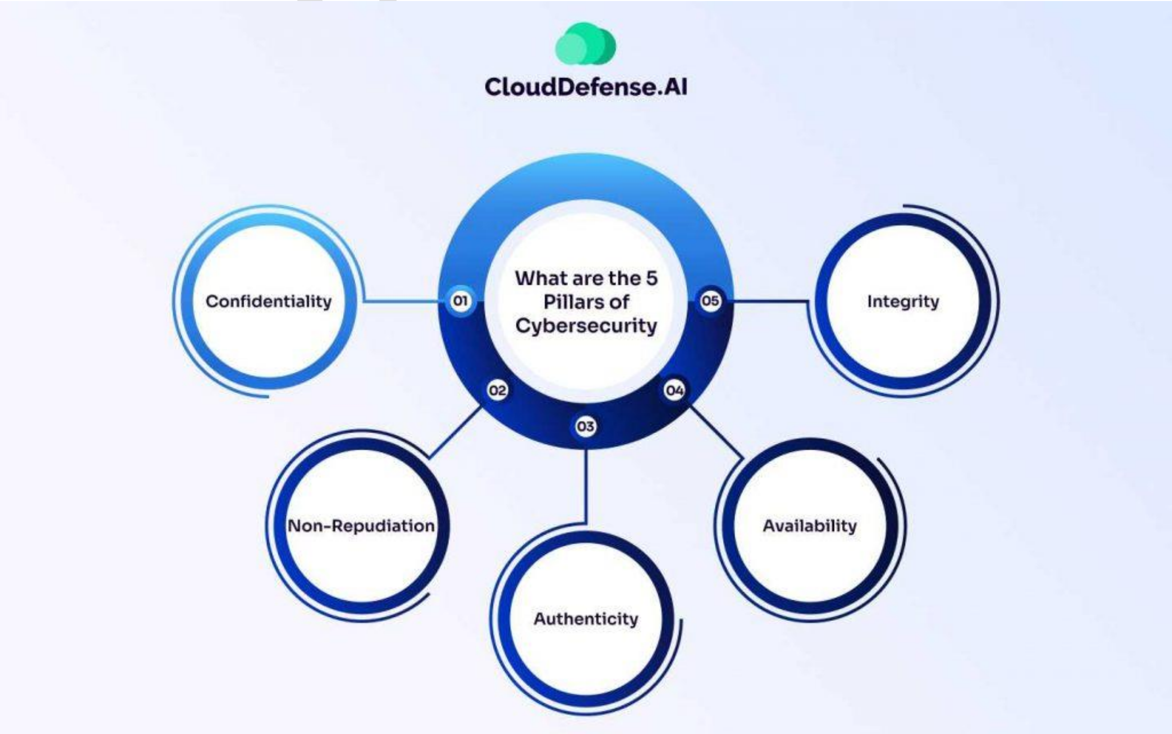
Lab Report demonstrating a understanding and execution of a scientific experiment, This Lab Report is a product created within the guidelines of Sysap (EC-Council) Official Curriculum to show mastery of specific skills and Knowledge.

Name: Omkar Hundekari
Course: CEH Practical Training
Subject: Cybersecurity
Date: 18th August 2025

Introduction to Ethical Hacking

Information security Concept

Information security programs are designed to uphold the principles of CIA Triad: Confidentiality, Integrity, and Availability by implementing a range of security controls. This involves understanding different types of threats and developing strategies to protect against attacks while ensuring authorized users can access the information they need.



The CIA Triad

This is the foundational principle for information security, balancing the three core goals:

- **Confidentiality**:
  - Protecting sensitive information from unauthorized disclosure or access. This is achieved through methods like encryption and access control lists.
- **Integrity**:
  - Maintaining the accuracy, completeness, and reliability of data by preventing unauthorized modification or deletion. Tools like audit trails and file permissions help ensure data integrity.
- **Availability**:
  - Ensuring that information and systems are accessible and usable by authorized users when they are needed. This involves disaster recovery plans and business continuity strategies.
- **Authentication**:
  - The process of verifying the identity of a user or device to ensure they are who they claim to be.
- **Non-repudiation:**

The assurance that a party involved in a transaction or action cannot later deny their participation.

✚Information security Goals, Motives and objectives

- **Goals**

  Information security's overarching goals are the Confidentiality, Integrity, and Availability (the CIA Triad) of information and digital assets.

- **Motives**

  Are for pursuing these goals include protecting sensitive data, complying with regulations, managing risks, and ensuring business continuity.

- **Objectives**

  Are the specific, measurable actions taken to achieve these goals, such as implementing access controls, conducting risk assessments, or training employees on security best practices.

✚Tactics, Techniques and Procedures (TTP)

Are the behavioral patterns and methods used by threat actors in cybersecurity to conduct attacks.

Components of TTPs

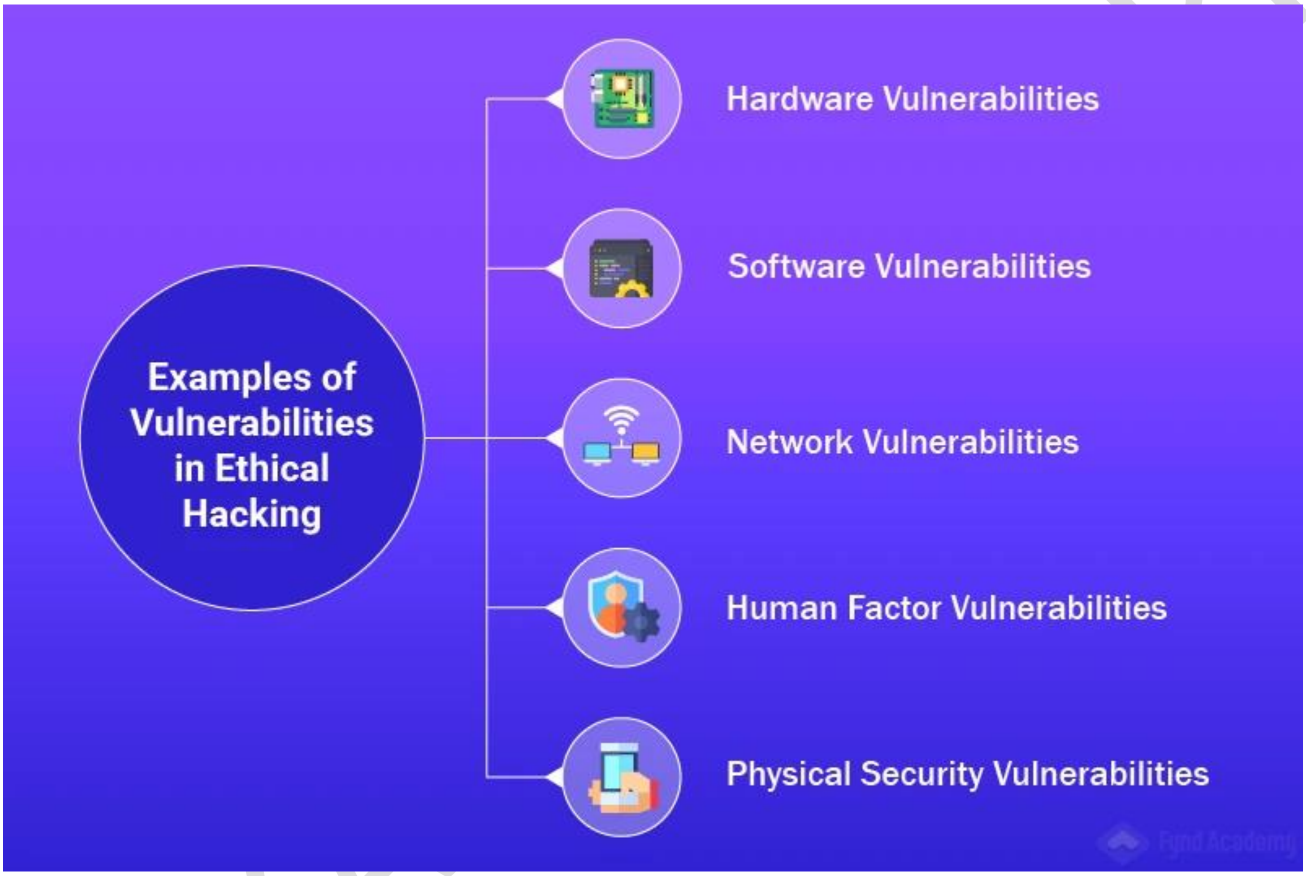
- **Tactics:**
  These are the overarching objectives or goals of the attacker, representing the "what" of the attack.
  Example: Gaining initial access to a network.

- **Techniques:**
  These are the specific methods or approaches an attacker uses to achieve a tactical goal.
  Example: Using phishing emails to gain credentials or port scanning to find vulnerabilities.

- **Procedures:**
  These are the detailed, step-by-step actions and specific tools used to execute a technique.
  Example: The exact sequence of emails sent, the specific links included, or the particular scanners and command-line tools used in a reconnaissance phase.

Vulnerability

Is a weakness in a computer system, its security procedures, or its design that a real hacker could exploit to gain unauthorized access or cause harm. Examples of vulnerabilities in ethical hacking include technical weaknesses like SQL injection, unpatched software, and misconfigurations; human vulnerabilities such as phishing susceptibility and weak passwords; and systemic issues like broken access control and insufficient logging.



Examples of Vulnerabilities in Ethical Hacking
Hardware Vulnerabilities
Software Vulnerabilities
Network Vulnerabilities
Human Factor Vulnerabilities
Physical Security Vulnerabilities

Classification of Attacks

- Here is a breakdown of each attack type:
- Active vs. Passive Attacks
- **Passive Attacks**:

  Focus on observation and monitoring to gather information, such as eavesdropping on traffic or analyzing network patterns. These attacks do not change data or system resources, making them difficult to detect.

- **Active Attacks**:
  Involve direct interaction with the target system to modify or damage data, disrupt services, or gain unauthorized access. Examples include denial-of-service (DoS) attacks and data breaches.

- **Close-in Attacks**:
- Definition:
  Attacks performed when the attacker is in close physical proximity to the target system or within the same local network.
- **Methods:**
  This can involve actions like shoulder surfing to view credentials or using physical keyloggers to capture user inputs.
- **insider Attacks**:
- **Definition:**
  Attacks launched by someone with legitimate, authorized access to the target system, such as an employee or contractor.
- **Motivation:**
  Can be accidental, due to negligence or mistakes, or malicious, with the intent to steal information or cause harm for personal gain.

- Distribution Attacks:
- **Definition:**
  Occur when malicious users or vendors alter hardware or software before it reaches the end-user or during transit.
- **Examples:**
  Creating a software backdoor at the source or spreading malware through infected applications are common types of distribution attacks.

Examples of Passive and Active Attacks

- Passive Attacks:
  Definition:

The attacker monitors and collects information from network communications without disrupting the network or altering the data.

- **Goal:**
  To learn about the system and gather sensitive information, such as passwords, messages, or other data.
- **Characteristics:**
  - Silent and non-intrusive.
  - Does not change the system or network operations.
  - Focuses on information acquisition.
  - Difficult to detect because they don't leave obvious traces.

Examples:

- **Foot Printing**

This method involves gathering information without directly interacting with the target system. Examples include:

- **Eavesdropping/Wiretapping**: An attacker intercepts network traffic to listen in on communications, like a conversation, to collect sensitive information.

- **Traffic Analysis**: An attacker analyzes the patterns of network data flow to deduce sensitive information, even if the data itself is encrypted.

- **Port Scanning**: An attacker probes a system to find open ports, which are then used to identify potential weaknesses without directly interacting with the services.

Active Attacks

- **Definition:**

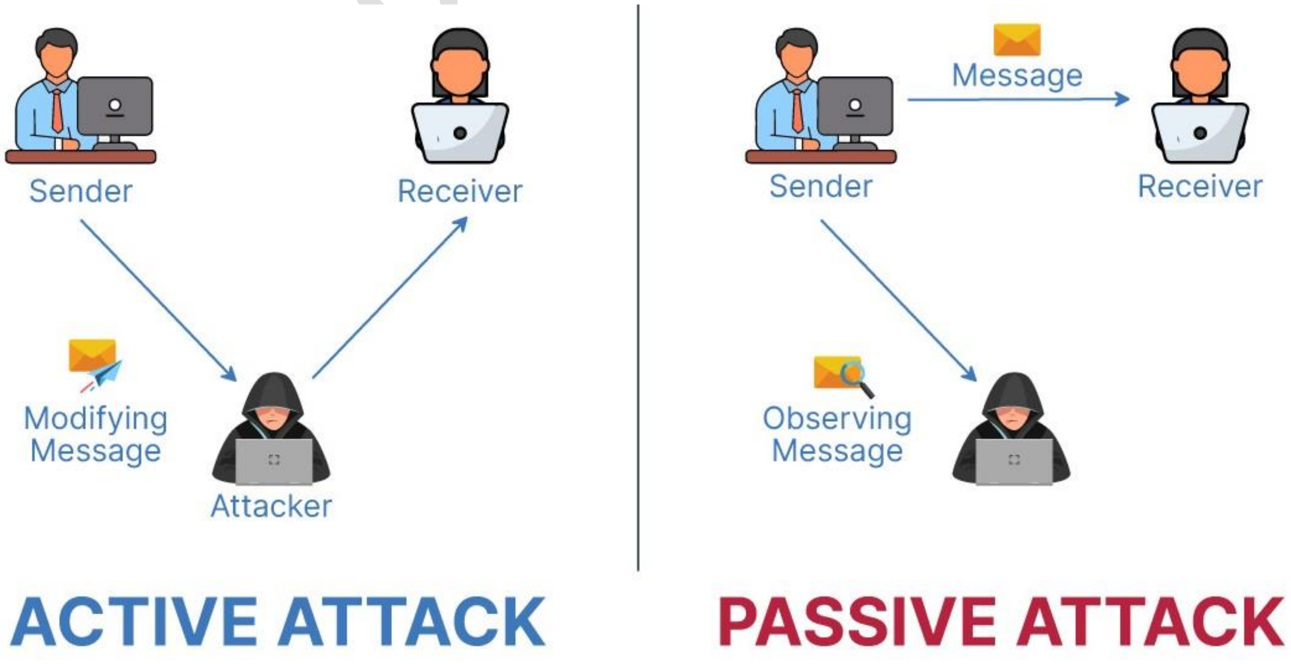
The attacker actively interferes with a system or network by modifying, disrupting, or destroying data, services, or network operations.

- **Goal:**

To gain unauthorized access, alter data, or make systems unusable.

- **Characteristics:**
    - Involves direct interaction with the target.
    - Modifies or disrupts the system's services or integrity.
    - Easier to detect because they cause direct and often immediate changes.
- **Examples:**

- **Malware/Virus Attacks**: An attacker injects malicious software into a system to steal data or cause damage.
- **Denial of Service (DoS) Attack**: The attacker overloads a system with excessive traffic to prevent legitimate users from accessing it.
- **Masquerade Attacks**: An attacker pretends to be a trusted user by using forged or stolen credentials to gain unauthorized access.
- **Session Hijacking**: An attacker intercepts an active session between two parties and takes over the communication.



✚ Information Warfare

Offensive information warfare is the active use of information and communication technologies (ICT) to disrupt, destroy, corrupt, or exploit an opponent's information systems, data, or control mechanisms to gain a strategic advantage. This includes tactics like disinformation campaigns to manipulate enemy perceptions, cyberattacks to disable infrastructure, data theft to acquire sensitive intelligence, and psychological operations to demoralize an adversary. The goal is to achieve information superiority by influencing decision-makers through the opponent's vulnerable information channels.

Here's a breakdown of the types of attacks mentioned:

Web Application Attacks

These attacks target vulnerabilities in web applications to gain unauthorized access, steal data, or disrupt services.

- **SQL Injection (SQLi)**:

Malicious SQL queries are injected into application databases to manipulate data.

- **Cross-Site Scripting (XSS)**:

Malicious scripts are injected into webpages to be executed by unsuspecting users.

- Credential Stuffing:

Attackers use stolen username and password combinations from previous breaches to gain access to other accounts.

- **Broken Access Control/Privilege Escalation**:

Attackers exploit weaknesses to gain higher-level privileges within an application or system.

- Denial-of-Service (DoS)/Distributed DoS (DDoS):

Overloading a web server with excessive requests to make it unavailable to legitimate users.

Web Server Attacks

These are attacks specifically targeting the server infrastructure that hosts web applications.

- Server-Side Request Forgery (SSRF): Exploiting a server to send requests to internal systems that are not intended to be exposed.
- Security Misconfigurations: Attackers exploit default, weak, or improperly configured server settings.

Malware Attacks

Involve the use of harmful software to damage systems or steal information.

- Viruses, **Worms, and Spyware**: Software designed to infect systems, replicate, and steal sensitive data.
- Ransomware: Malware that encrypts a victim's files and demands a ransom payment for their decryption.

Man-in-the-Middle (MITM) Attacks

An attacker positions themselves between two communicating parties to eavesdrop, alter, or inject data into the communication channel.

- **Eavesdropping**:

Stealing sensitive information like login credentials or credit card numbers.

- **Data Manipulation**:

Intercepting and changing messages between parties without their knowledge.

- **Impersonation**:

Tricking users into sending information to the attacker, making it appear as a normal exchange.

System Hacking

The broad act of gaining unauthorized access to a computer system or network to steal data, disrupt operations, or achieve other illicit goals.

- Unauthorized Access: Gaining entry into a network or system without proper permission.
- Password Attacks/**Brute Force**: Attempts to guess passwords by trying many combinations until the correct one is found.

Defensive Information Warfare (IW-D) refers to all actions taken to protect against information attacks, which aim to disrupt, corrupt, or exploit information and information systems. It involves safeguarding data integrity, availability, and secrecy by defending against threats like deception, psyops, hacking, disinformation, and other forms of cyberattacks. The ultimate goals are to maintain a desired information state without outside interference, deter future attacks by raising their cost, and rapidly recover from any damage inflicted.

Here is a breakdown of each component:

1. Prevention

- **Goal:** To stop an attack from happening in the first place.
- **Strategies:** Implementing strong access controls, security patches, firewalls, encryption, and security awareness training to block unauthorized access and protect critical assets.

2. Deterrence

- **Goal:** To discourage potential attackers from attempting an information attack.
- **Strategies:** Demonstrating a robust defensive posture and potential retaliatory capabilities (offensive information warfare) to make the cost of an attack too high or impractical for adversaries.

3. Alerts

- **Goal:**

To notify relevant parties about potential threats or suspicious activities.

- **Strategies:**

Setting up alerts for unusual network traffic, failed login attempts, or other indicators of a potential security breach to enable a timely response.

4. Detection

- **Goal:**

To identify an attack that is currently in progress or has already occurred.

- **Strategies:**

Employing intrusion detection systems (IDS), network monitoring tools, and log analysis to identify malicious activities and gain visibility into network activity.

5. Emergency Preparedness

- **Goal:**

To plan and establish procedures for dealing with security incidents and potential large-scale attacks.

- **Strategies:**

Developing incident response plans, conducting regular drills and scenario analyses, and establishing communication plans to ensure a coordinated and effective response when an incident occurs.

6. Response

- **Goal:**

To mitigate the impact of a security incident and restore normal operations.

- **Strategies:**

Executing the incident response plan to isolate affected systems, eradicate the threat, recover data, and conduct a post-incident analysis to improve future defenses.

What is Hacking ?

Hacking, in simple terms, is getting unauthorized access to a computer, network, or digital device to steal information, cause harm, or gain control. A hacker is the person who performs the hack, often by exploiting weaknesses in security to gain access to systems or data without permission.

Types of Hackers and Their Motivations

- **Script Kiddies**
  - **Motivation:** A desire for attention, notoriety, or the thrill of causing disruption, rather than deep technical understanding or financial gain.
  - **Purpose:** To cause harm or chaos, often using pre-made hacking tools and scripts.
  - **Example:** An inexperienced user using a known vulnerability tool to take down a small website for attention.

- **White Hat Hackers (Ethical Hackers)**
  - **Motivation:** To identify and fix security vulnerabilities in systems, often for a client or organization.
  - **Purpose:** To strengthen security measures and defend against cyberattacks.
  - **Example:** A company hiring a white hat hacker to test its network's security.

- **Black Hat Hackers (Malicious Hackers)**
  - **Motivation:** Malicious intent, seeking financial profit, stealing information, or causing damage.
  - **Purpose:** To illegally exploit systems for their own gain.
  - **Example:** A hacker deploying ransomware to encrypt a victim's files and demand payment.

- **Gray Hat Hackers**
  - **Motivation:** A mix of both ethical and unethical intentions, sometimes operating without permission to expose issues.
  - **Purpose:** To explore systems and expose vulnerabilities, though their methods can be legally questionable.
  - **Example:** A hacker breaking into a system to find a flaw and then informing the owner, but without prior authorization.

- **Hacktivists**
  - **Motivation:** Political or social causes, aiming to promote a specific agenda or protest against an organization or government.
  - **Purpose:** To create a public statement or disrupt operations to raise awareness for a cause.
  - **Example:** A group hacking into a government's website to protest a policy.

- **State-Sponsored Hackers:**

  Individuals or groups employed by a government to conduct cyber espionage or attacks on behalf of their nation. Their goals are strategic, focusing on military, political, or economic advantages for their country.

(Don't)Motivations of Specific Hacker Types

- **Cyber Terrorists:**

Motivated by ideology, these hackers aim to cause fear, disruption, or significant damage to achieve political or social goals.

- **Corporate Spies:**

Driven by the pursuit of competitive advantage, these individuals or groups hack to steal business secrets, proprietary information, or other valuable data to benefit a rival company.

- **Blue Hat Hackers:**

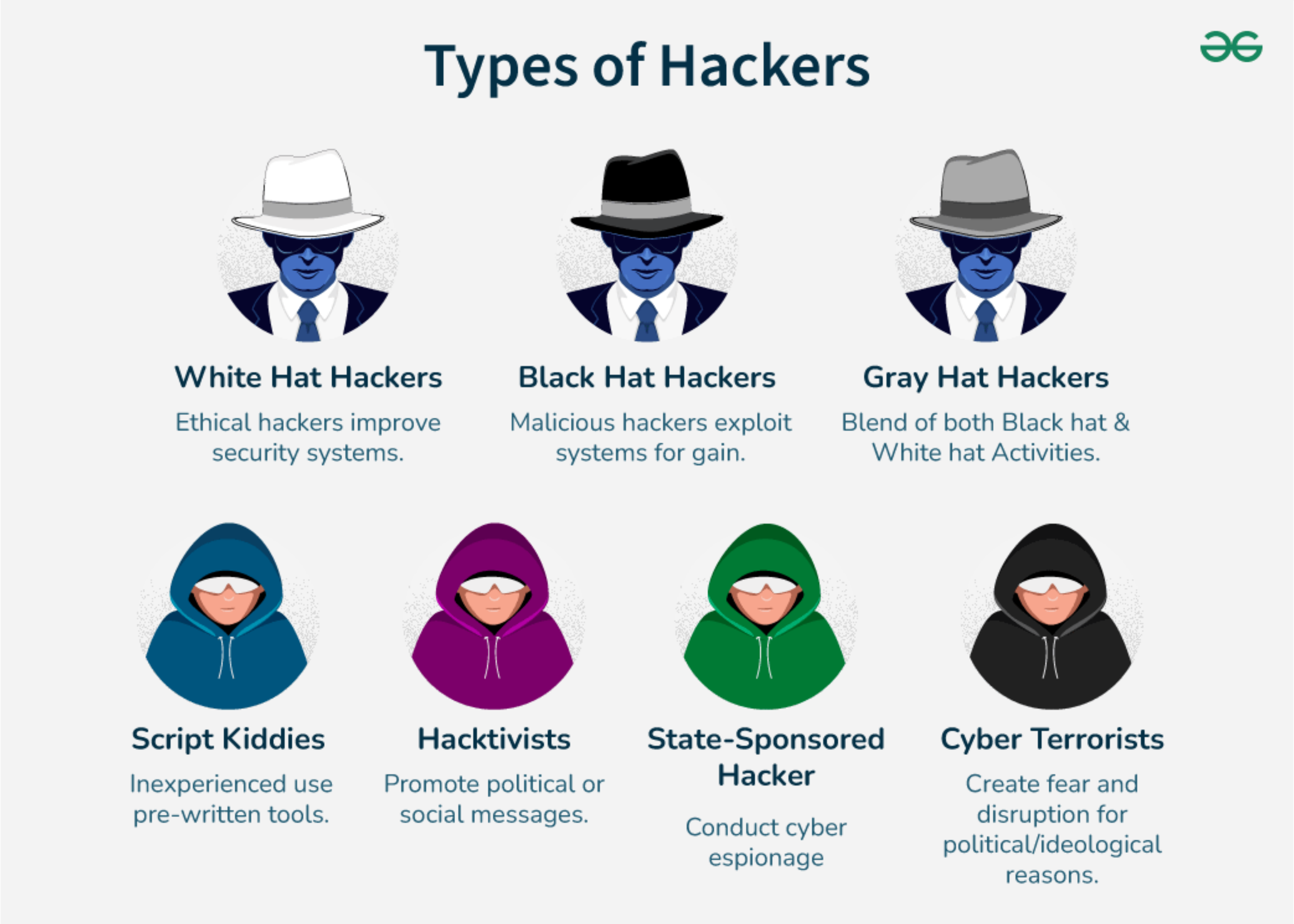
Unlike script kiddies, blue hat hackers aim to find flaws to resolve disputes or seek revenge, but a common definition involves testing software security before a company goes live with it.

- **Red Hat Hackers:**

Digital vigilantes who launch aggressive attacks to disrupt or destroy black hat hackers and their operations.

- **Green Hat Hackers**

Are **novice or beginner hackers** who are still in the learning phase. They are driven by curiosity and a desire to improve their hacking skills. Unlike script kiddies, who hack just for fun or mischief, green hats take hacking seriously and focus on gaining knowledge and experience. They usually lack expertise but are eager to grow, and their intent is generally not malicious.



Types of Hackers

White Hat Hackers
Ethical hackers improve security systems.

Black Hat Hackers
Malicious hackers exploit systems for gain.

Gray Hat Hackers
Blend of both Black hat & White hat Activities.

Script Kiddies
Inexperienced use pre-written tools.

Hacktivists
Promote political or social messages.

State-Sponsored Hacker
Conduct cyber espionage

Cyber Terrorists
Create fear and disruption for political/ideological reasons.

Ethical Hacking Concepts

Ethical hacking is like hiring a digital "burglar" to test your security. With permission, an ethical hacker, also known as a white-hat hacker, uses the same tools and methods as a criminal

hacker to find weak spots (vulnerabilities) in a computer system or network. Their goal isn't to steal or cause damage, but to report these security flaws to the owner so they can be fixed before a real bad-guy hacker (black-hat hacker) finds and exploits them.

Key Concepts

- **Authorization: Ethical hacking is always done with the owner's official permission, making it legal and professional.**

- **Vulnerabilities: These are the weaknesses or gaps in a system's security that a hacker could exploit.**
- **Penetration Testing (Pen Testing): This is the process of simulating an attack to find vulnerabilities.**
- **White-Hat Hackers: The good guys who are ethical hackers, trying to strengthen security.**
- **Black-Hat Hackers: The malicious hackers who exploit vulnerabilities for their own gain.**
- **Security Posture: The overall strength of an organization's security.**

Skills of Ethical Hacker

Ethical hacking requires strong technical skills in programming, networking, operating systems, and web technologies to identify vulnerabilities, alongside non-technical skills like problem-solving, critical thinking, effective communication, and strong ethical principles to report findings and propose solutions to organizations and non-technical stakeholders.

- **Technical Skills**

- **Programming and Scripting:**
- **Proficiency in languages like Python, Java, C/C++, and Bash helps in automating tasks, analyzing network traffic, creating custom tools, and understanding how exploits work to develop effective countermeasures.**

- **Networking:**
- **A thorough understanding of network principles is essential for analyzing network traffic, creating network maps, and identifying open ports and services using tools like Nmap.**

- **Operating Systems:**
- **Knowledge of different operating systems (e.g., Windows, Linux) allows ethical hackers to identify**

OS-specific vulnerabilities and exploit misconfigurations, according to the EC-Council.

- Web Technologies:
- For web application hacking, familiarity with HTML, CSS, JavaScript, and various web frameworks is necessary to detect web vulnerabilities such as SQL injections, XSS, and IDOR.

- Vulnerability Scanning:
- Ethical hackers use tools like Nessus for vulnerability scanning and tools like Angry IP Scanner to find weaknesses in systems and applications, notes the EC-Council.

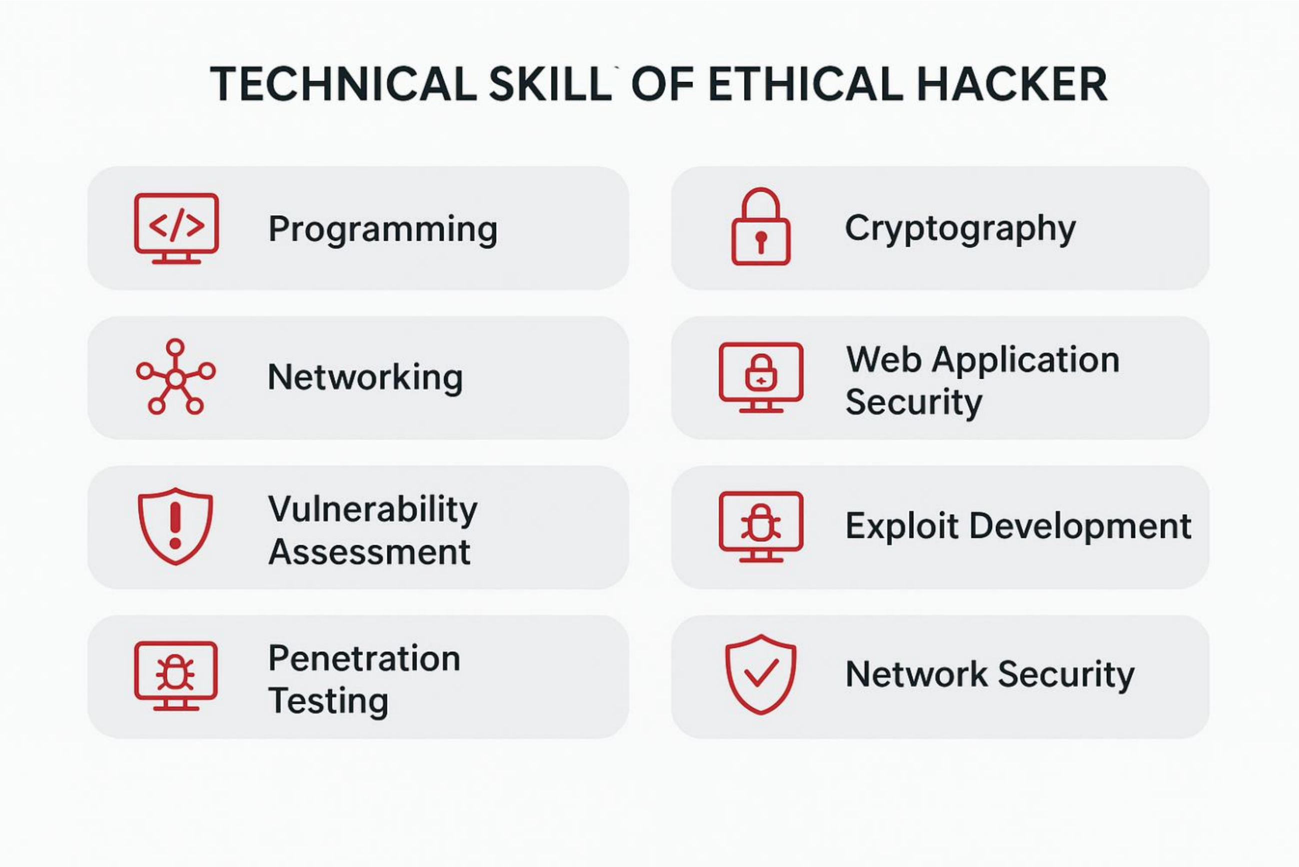
- Information Security Principles:
- A solid foundation in information security principles is necessary to understand how to effectively secure systems and networks.
- Non-Technical Skills.

- Problem-Solving and Analytical Thinking:
- The ability to think critically and creatively to quickly identify vulnerabilities, understand their impact, and devise innovative exploitation techniques is crucial.

- Communication:
- Ethical hackers must be able to clearly communicate their findings, vulnerabilities, and suggested fixes to both technical and non-technical audiences, including managers and executives.

- Ethical Conduct:
- Ethical hackers must have a strong ethical framework and adhere to legal and professional standards, ensuring they have written permission to perform tests and that all findings are reported to the system owner.

- Curiosity and Eagerness to Learn:
- The cyber threat landscape is constantly evolving, requiring ethical hackers to continuously learn about new technologies and attack methods to stay ahead of malicious actors.



TECHNICAL SKILL OF ETHICAL HACKER

Programming

Cryptography

Networking

Web Application Security

Vulnerability Assessment

Exploit Development

Penetration Testing

Network Security

- Non-Technical Skills:

Non-technical skills crucial for an ethical hacker include communication, to explain findings to diverse audiences; problem-solving and analytical thinking, to identify complex vulnerabilities; continuous learning, to stay ahead of evolving threats; attention to detail, to spot subtle security flaws; a strong ethical mindset, for professional conduct; and the ability to perform risk assessment, to prioritize security efforts.

Cognitive & Problem-Solving Skills

- Analytical Thinking:

The capacity to deconstruct systems, understand how they function, and identify potential weaknesses.

- Problem-Solving:

The ability to think creatively and develop solutions to complex security challenges, often anticipating threats before they manifest.

- Attention to Detail:

The meticulous nature required to find hidden vulnerabilities within systems and logs, a process that often demands patience.

Interpersonal & Communication Skills

- Communication Skills:

The essential ability to clearly and effectively convey complex technical information, security risks, and findings in reports and presentations to both technical and non-technical stakeholders.

- Teamwork:

The skill to collaborate with different teams, including developers and management, to address security issues and implement solutions.

Professional & Mindset Skills

- Ethical Mindset:

A strong moral compass and a deep understanding of ethical and legal boundaries, which is crucial for working with sensitive information and maintaining trust.

- **Continuous Learning:**

A commitment to staying updated with the latest cybersecurity trends, emerging threats, technologies, and attack vectors to remain effective.

- **Risk Assessment & Compliance:**

The understanding of security frameworks and policies to assess risks, implement security measures, and ensure compliance with regulations like GDPR.

NON-TECHNICAL SKILLS OF ETHICAL HACKER
Communication
Ethics
Critical Thinking
Teamwork
Problem-Solving
Adaptability

AI driven Ethical Hacking

AI-driven ethical hacking uses artificial intelligence and machine learning to automate vulnerability detection, perform more effective penetration tests, and analyze threat intelligence at scale. By automating tasks like vulnerability scanning and simulating attacks, AI enhances the speed and accuracy of security assessments, helping ethical hackers identify weaknesses before malicious actors can exploit them. Key applications include automated vulnerability discovery, AI-powered penetration testing, advanced threat intelligence, and the detection of sophisticated phishing attacks.

Myth: AI will Replace Ethical Hackers

One of the most persistent AI myths vs reality debates is whether AI will replace cybersecurity professionals. In truth, AI complements human capabilities rather than replacing them. It automates repetitive tasks, enabling security teams to focus on more complex strategic functions.

ChatGPT- Powered AI tools for Ethical Hackers

AI tools for ethical hacking are like a security expert's superpower. They use artificial intelligence to automate, speed up, and improve the process of finding and fixing vulnerabilities in a system. Instead of replacing human hackers, these tools act as an intelligent assistant, making security testing faster and smarter.

Examples of ChatGPT-Powered AI Tools for Ethical Hackers

ShellGPT – A command-line AI assistant that generates and explains Linux/Windows commands for automation, reconnaissance, and security tasks.

AutoGPT – An autonomous AI agent that performs multi-step operations like scanning, analysis, and reporting without constant user input.

WormGPT – A malicious GPT variant used by cybercriminals to create phishing emails, malware, and social engineering attacks.

ChatGPT with DAN Prompt – A jailbreak prompt ("Do Anything Now") used to bypass ChatGPT's restrictions; studied in CEH as an example of AI misuse.

FreedomGPT – An uncensored AI model that runs locally without safety filters; often cited as a security risk if misused.

FraudGPT – A black-hat GPT variant promoted in underground forums for generating scams, phishing kits, and fraudulent schemes.

ChaosGPT – A concept AI agent variant demonstrating destructive goals; highlights the risks of uncontrolled autonomous AI.

PoisonGPT – An AI model deliberately poisoned with backdoors or misinformation, showing threats in AI supply chain and model security

HackerGPT – AI assistant designed for security learners and penetration testers; explains exploits and generates payloads but may be misused if not ethically controlled.

Bug Bounty GPT – AI assistant for bug bounty hunters; helps with reconnaissance, vulnerability discovery, and report drafting for responsible disclosure.

GPT White Hack – AI model designed to assist ethical hackers; focuses on penetration testing, defense strategies, and secure coding practices.

CybGPT – Cybersecurity-focused GPT assistant that helps in threat intelligence, vulnerability analysis, and cyber defense training.

Bug Hunter GPT – AI tool for bug bounty hunters; automates recon, payload testing, and helps draft responsible disclosure reports.

Hacking APIs GPT – Specialized GPT that helps security researchers test, exploit, and secure APIs by generating attack vectors and defense methods.

H4ck GPT – A hacker-oriented GPT model often discussed in underground forums; used for generating exploits or scripts (⚠ misuse risk).

Hacker News GPT – GPT variant trained on cybersecurity news and blogs; provides updates on latest exploits, breaches, and patches.

Ethical Hacker GPT – AI assistant built for CEH-style training; explains attacks, suggests countermeasures, and helps in learning hacking legally.

Gp(en)T(ester) – A penetration testing–focused GPT tool that integrates scanning, exploitation guidance, and report generation for pentesters.

✚CEH Ethical Hacking Framework:

- **Reconnaissance (Information Gathering)**

- First step: collect as much information as possible about the target.
- Techniques: OSINT, footprinting, scanning, Google Dorks, social engineering.
- Goal: build a profile of the target system or network.
- **Vulnerability Scanning**

- Automated process to identify weaknesses in systems, networks, and applications.
- Purpose: detect misconfigurations, outdated software, missing patches, and known vulnerabilities.
- Types of scans:
  - Network Scanning → open ports, services.
  - Web App Scanning → SQL injection, XSS.
  - Database Scanning → weak authentication, privilege flaws.
  - Host Scanning → OS misconfigurations.
  - Cloud/Container Scanning → insecure IAM, storage.

- Common tools: Nessus, OpenVAS, QualysGuard, Nikto, Acunetix.
- Process: Define scope → Run scan → Validate results → Report → Remediate.
- Difference from Penetration Testing: Scanning finds flaws; Pentesting exploits flaws.

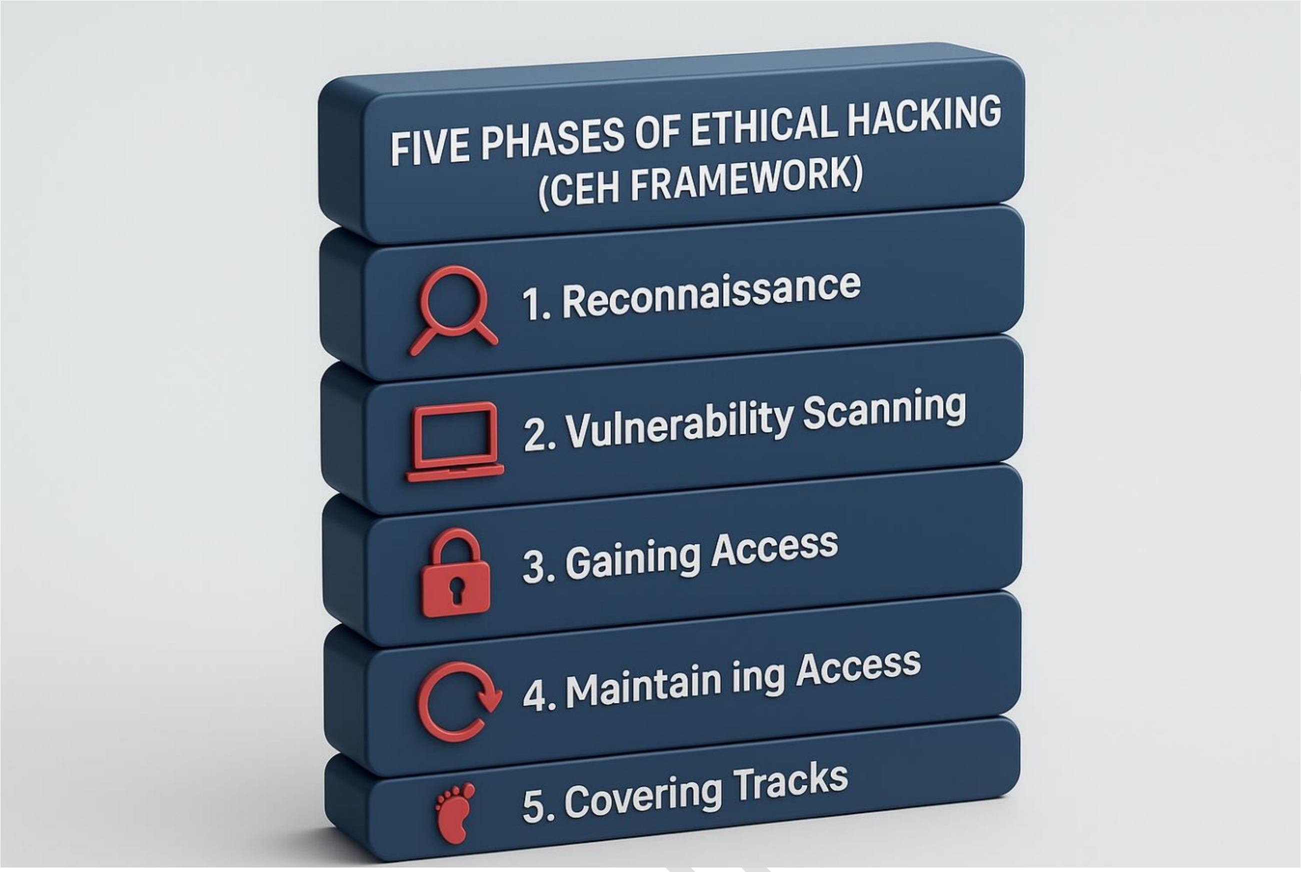
- **Gaining Access**

- Attempt to exploit vulnerabilities to get into the target system.
- Techniques: SQL injection, password cracking, malware, privilege escalation.
- Goal: establish control and prove exploitability (within scope).

- **Maintaining Access**

- Demonstrate persistence after initial compromise.
- Techniques: installing backdoors, rootkits, creating new accounts.
- Goal: simulate real-world attackers who maintain long-term access.

- **Covering Tracks**
- Process attackers use to hide evidence of hacking activity.
- Goal: avoid detection and maintain persistence.
- Common techniques:
  - Clearing logs (system, audit, event logs).
  - Modifying timestamps (timestomping).
  - Deleting malicious files/tools.
  - Disabling antivirus, monitoring, or logging.
  - Installing rootkits to hide processes.
  - Encrypting or obfuscating malicious traffic.
  - Creating hidden backdoors for re-entry.
- Ethical note: CEH professionals **do not erase tracks**, they document all actions.
- Defensive countermeasures: SIEM alerts, log monitoring, file integrity checks, IDS/IPS.



➢ ***Module Summary:***

Definition: Ethical hacking is the authorized practice of testing and evaluating security systems to identify and fix vulnerabilities before malicious attackers exploit them.

Need for Ethical Hacking:

- Rising cybercrime and advanced threats.

- Protection of sensitive data, networks, and applications.
- Ensures compliance with security standards and laws.

Key Terminologies:

- Threat, Vulnerability, Exploit, Attack Vector, Payload.
- Hacker classifications (Black Hat, White Hat, Grey Hat, Hacktivists, Script Kiddies, State-sponsored).

Scope of Ethical Hacking:

- Network security testing.
- Web application and database security.
- Cloud and IoT security.
- Social engineering defense.

Five Phases of Ethical Hacking:

1. Reconnaissance (Information Gathering).
2. Vulnerability Scanning & Enumeration.
3. Gaining Access.
4. Maintaining Access.

5. Covering Tracks.

Legal and Ethical Considerations:

- Performed with proper authorization (scope, agreement).
- Must follow responsible disclosure policies.
- Aligned with laws such as IT Act (India), GDPR, HIPAA, PCI-DSS.

Benefits of Ethical Hacking:

- Identifies weaknesses proactively.
- Strengthens defenses against cyberattacks.
- Builds trust and compliance for organizations.