

# TRAINING DAY 7 REPORT

8 JULY 2025

## Understand Phases of ethical hacking and penetration testing cybersecurity vs ethical hacking and laws

Today, I learned some important concept

### Phases of Ethical Hacking

Footprinting : **Footprinting** is the **first step in the reconnaissance phase** of ethical hacking. It involves **gathering information** about a target system, network, or organization to understand its structure and potential vulnerabilities—**without engaging directly with the target** (in passive methods).

Ethical hacking, also known as penetration testing or white-hat hacking, involves simulating cyberattacks to identify vulnerabilities and help secure systems. The process typically follows **five key phases**:

#### 1. Reconnaissance (Information Gathering)

- **Goal:** Collect as much information as possible about the target system or network.
- **Types:**
  - **Passive Reconnaissance:** Using publicly available data (e.g., WHOIS, DNS records, social media).
  - **Active Reconnaissance:** Directly interacting with the target (e.g., pinging, port scanning).
- **Tools:** Nmap, Maltego, Google Dorking, Recon-ng

#### 2. Scanning

- **Goal:** Identify open ports, services, and potential vulnerabilities.
- **Types:**
  - **Network Scanning:** Discover active devices and IP addresses.
  - **Port Scanning:** Identify open ports and running services.
  - **Vulnerability Scanning:** Look for known weaknesses in systems.
- **Tools:** Nmap, Nessus, OpenVAS, Nikto

#### 3. Gaining Access

- **Goal:** Exploit vulnerabilities to gain unauthorized access.
- **Techniques:**
  - Exploiting software bugs
  - Brute-force attacks
  - SQL injection, buffer overflows
- **Tools:** Metasploit, SQLmap, Hydra

#### 4. Maintaining Access

- **Goal:** Establish a persistent presence in the system.
- **Methods:**
  - Installing backdoors or rootkits
  - Creating new user accounts
- **Purpose:** Observe how long an attacker could remain undetected.
- **Tools:** Netcat, Meterpreter

#### 5. Covering Tracks

- **Goal:** Hide traces of the attack to avoid detection.
- **Techniques:**
  - Clearing logs
  - Modifying timestamps
  - Deleting temporary files

## Penetration Testing

**Penetration Testing** is a **simulated cyberattack** carried out by ethical hackers to identify, exploit, and report vulnerabilities in a system, network, or application—**before malicious hackers do**. It helps organizations **evaluate the security of their IT infrastructure** and uncover weaknesses that could be exploited in real-world attacks.

## Phases of Penetration Testing

### 1. Planning and Preparation

- **Objective:** Define the scope, objectives, and rules of engagement.
- **Activities:**
  - Decide what systems will be tested (IP ranges, applications, etc.)
  - Identify goals (e.g., test resilience, meet compliance)

- Establish permissions and legal agreements
- Determine testing type: Black-box, White-box, or Gray-box

## 2. Reconnaissance (Information Gathering)

- **Objective:** Collect information about the target to plan attacks.
- **Types:**
  - **Passive Recon:** No direct interaction (e.g., WHOIS, Google Dorking)
  - **Active Recon:** Direct interaction (e.g., ping, DNS interrogation)
- **Tools:** Nslookup, Nmap, Maltego, Shodan

## 3. Scanning and Enumeration

- **Objective:** Identify live systems, open ports, services, and vulnerabilities.
- **Activities:**
  - Network scanning
  - Port and service identification
  - Banner grabbing
  - Vulnerability scanning
- **Tools:** Nmap, Nessus, Nikto, OpenVAS

## 4. Gaining Access (Exploitation)

- **Objective:** Exploit discovered vulnerabilities to gain unauthorized access.
- **Techniques:**
  - SQL Injection
  - Password cracking
  - Buffer overflows
  - Web app exploits
- **Tools:** Metasploit, Hydra, SQLmap

## 5. Maintaining Access

- **Objective:** Determine whether a persistent presence can be established.
- **Why It Matters:** Simulates real attackers staying hidden over time.
- **Methods:**
  - Installing backdoors
  - Creating admin accounts
  - Using remote access tools

## 6. Covering Tracks (Optional in Ethical Testing)

- **Objective:** Erase evidence of the attack (only demonstrated in reports).
- **Techniques:**
  - Clearing logs
  - Modifying timestamps
  - Disabling monitoring tools

## Cybersecurity vs. Ethical Hacking

Aspect	Cybersecurity	Ethical Hacking
<b>Definition</b>	Practice of protecting systems, networks, and data	Simulating attacks to find and fix vulnerabilities
<b>Approach</b>	Defensive (prevention-focused)	Offensive (attack-focused for testing)
<b>Purpose</b>	Stop threats, enforce policies, ensure security	Identify security holes by mimicking real attackers
<b>Scope</b>	Broad: includes risk management, policies, tools, etc.	Narrow: focuses on penetration testing and vulnerability research
<b>Legality</b>	Always legal	Legal only with permission (white-hat)
<b>Roles</b>	Security Analyst, Engineer, SOC Analyst	Ethical Hacker, Penetration Tester, Red Team Expert
<b>Tools Used</b>	Firewalls, antivirus, SIEM, IDS/IPS	Metasploit, Burp Suite, Nmap, Wireshark

## Ethical Laws and Policies

**Ethical hacking** involves testing systems for vulnerabilities with permission, but it must follow strict **laws and ethical guidelines**. Ethical hackers must obtain **written authorization**, respect **confidentiality**, avoid causing damage, and act within the scope of the test. Laws like the **Computer Fraud and Abuse Act (CFAA)** in the U.S., **GDPR** in the EU, and **IT Act 2000** in India govern these practices. Ethical hackers are also expected to follow codes of conduct from certifications like **CEH** and **OSCP**, ensuring they act legally, responsibly, and transparently.

## Information Technology (IT) Act, 2000

The **Information Technology Act, 2000** is **India's primary law** dealing with **cybercrime and electronic commerce**. It was enacted to provide legal recognition to electronic transactions and to combat cybercrime in the growing digital space.

## **Key Objectives of the IT Act, 2000**

- Legal recognition of **electronic documents and digital signatures**
- Define and penalize **cybercrimes** like hacking, identity theft, and data breaches
- Provide rules for **electronic governance**
- Protect **data privacy and security**

## **Important Cybercrime Sections**

<b>Section</b>	<b>Offense</b>	<b>Penalty</b>
<b>Sec 43</b>	Unauthorized access, downloading, or damaging data	Fine up to ₹1 crore
<b>Sec 66</b>	Hacking with malicious intent	Up to 3 years in prison + fine
<b>Sec 66C</b>	Identity theft using passwords or digital signatures	Up to 3 years + ₹1 lakh fine
<b>Sec 66D</b>	Cheating using impersonation (e.g. phishing)	Up to 3 years + ₹1 lakh fine
<b>Sec 67</b>	Publishing obscene content online	Up to 5 years + fine (can vary)