Module 01

Introduction to Ethical Hacking - CEH v13

1. What is Ethical Hacking?

Ethical hacking involves legally breaking into systems and networks to test their security. Ethical hackers, also known as white-hat hackers, help organizations identify vulnerabilities before malicious hackers can exploit them.

2. Key Terminologies

- **Threat**: A potential danger that can exploit a vulnerability.
- **Vulnerability**: A weakness in a system, application, or network.
- **Exploit**: Code or technique used to take advantage of a vulnerability.
- **Risk**: The potential impact of a threat exploiting a vulnerability.
- **Payload**: Malicious code executed after a system is exploited.

3. Types of Hackers

- **White Hat Hackers**: Ethical hackers who perform security testing legally.
- **Black Hat Hackers**: Malicious hackers who exploit systems for personal gain.
- **Gray Hat Hackers**: Hackers who sometimes act legally and sometimes illegally.

4. Five Phases of Ethical Hacking

1. **Reconnaissance** – Gathering information about the target.
2. **Scanning** – Identifying live systems, open ports, and services.
3. **Gaining Access** – Exploiting vulnerabilities to enter the system.
4. **Maintaining Access** – Installing backdoors for persistent access.
5. **Covering Tracks** – Hiding activities to avoid detection.

5. Ethical Hacking vs. Penetration Testing

- **Ethical Hacking**: Broad practice of testing security.
- **Penetration Testing**: A structured and controlled security assessment.

6. Cybersecurity Laws and Compliance

Ethical hackers must follow legal frameworks such as:

- **GDPR (General Data Protection Regulation)**
- **HIPAA (Health Insurance Portability and Accountability Act)**
- **ISO 27001 (Information Security Management Standard)**
- **Computer Fraud and Abuse Act (CFAA)**

7. Common Attack Vectors

- **Phishing**: Social engineering attack to steal credentials.
- **Malware**: Viruses, worms, trojans, and ransomware.
- **Denial of Service (DoS)**: Overloading a system to make it unavailable.
- **SQL Injection**: Injecting malicious SQL queries to manipulate databases.
- **Man-in-the-Middle (MITM) Attack**: Intercepting communication between two parties.

8. Ethical Hacking Tools

Some commonly used tools in ethical hacking include:

- **Nmap** – Network scanning tool.
- **Wireshark** – Packet sniffing tool.
- **Metasploit** – Penetration testing framework.
- **Burp Suite** – Web application security testing tool.
- **Kali Linux** – A popular OS for ethical hacking.

9. Ethical Hacking Certifications

Apart from CEH, other certifications include:

- **OSCP (Offensive Security Certified Professional)**
- **GPEN (GIAC Penetration Tester)**
- **CISSP (Certified Information Systems Security Professional)**

10. Countermeasures Against Hacking

- **Regularly updating software & patches**
- **Using strong passwords & multi-factor authentication**
- **Implementing intrusion detection/prevention systems (IDS/IPS)**
- **Security awareness training for employees**
- **Conducting frequent penetration tests & vulnerability assessments**

Module 02

Footprinting and Reconnaissance - CEH v13

1. Introduction to Footprinting and Reconnaissance

Footprinting and reconnaissance are the first steps in ethical hacking. They involve gathering information about a target system, network, or organization to identify potential vulnerabilities.

Objectives of Footprinting and Reconnaissance:

- Gather publicly available information about a target.
- Identify the network and system architecture.