# Module 01: Introduction to Ethical Hacking

This module covers the fundamental concepts of information security, the different types of hackers, the phases of hacking, and the legal frameworks that govern ethical hacking activities.

## 1. Information Security Overview

At its core, security is about protecting assets. The industry uses several frameworks to define "security."

### The CIA Triad

The three pillars of security:

* **Confidentiality:** Ensuring that information is accessible only to those authorized to have access. (Encryption, access controls).
* **Integrity:** The trustworthiness of data over its entire lifecycle. Ensuring data hasn't been modified by unauthorized people. (Hashing, digital signatures).
* **Availability:** Ensuring that systems and data are available to authorized users when needed. (Redundancy, backups, DDoS protection).

### Extended Concepts

* **Authenticity:** Proving that a user or system is who they claim to be.
* **Non-Repudiation:** Ensuring that a sender cannot deny sending a message and the recipient cannot deny receiving it (Digital signatures).

## 2. Hacking Concepts

### Who is a Hacker?

In the CEH context, a hacker is someone who uses their skills to find and exploit vulnerabilities.

* **White Hat:** Ethical hackers. They have permission and work to improve security.
* **Black Hat:** Malicious hackers. They act without permission for personal gain or destruction.
* **Grey Hat:** Operates in a middle ground. Might find a vulnerability and disclose it without permission but without malicious intent.
* **Suicide Hacker:** Hackers who aim to cause massive damage without concern for getting caught or their own safety.
* **Script Kiddies:** Unskilled hackers who use existing tools and scripts created by others.
* **Hacktivist:** Hackers who hack for political or social causes.

### The 5 Phases of Hacking (EC-Council Methodology)

You must memorize these in order for the exam:

1. **Reconnaissance:** Gathering evidence (Footprinting). Can be passive (Google) or active (Nmap).
2. **Scanning:** Finding open ports, services, and vulnerabilities.
3. **Gaining Access:** Exploiting a vulnerability to enter the system (The "Hack").
4. **Maintaining Access:** Using backdoors or rootkits to stay in the system.
5. **Clearing Logs:** Removing evidence of the attack to avoid detection.

## 3. Information Warfare

Information Warfare (InfoWar) refers to the use of information and communication technologies to gain a competitive advantage over an opponent.

* **Defensive InfoWar:** Protecting your own information assets.
* **Offensive InfoWar:** Attacking an opponent's information assets.

## 4. Cyber Kill Chain & MITRE ATT&CK

### Cyber Kill Chain (Lockheed Martin)

A 7-step framework to understand the stages of a cyberattack:

1. Reconnaissance
2. Weaponization (Coupling a remote access trojan with an exploit)
3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Actions on Objectives

### MITRE ATT&CK Framework

A globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It provides a "Matrix" that security teams use to track what attackers do once they are inside a network.

## 5. Ethical Hacking Concepts

Ethical hacking is the **authorized** attempt to gain unauthorized access to a computer system, application, or data.

**Essential Requirements:**

* **Permission:** You must have a written contract (Rules of Engagement).
* **Scope:** You must stay within the boundaries defined in the contract.
* **Reporting:** You must report all findings to the client.
* **Confidentiality:** You must keep all client information secure.

## 6. Laws and Standards

The CEH exam frequently asks about specific laws and regulatory standards:

* **PCI-DSS:** Security standard for organizations that handle credit cards.
* **HIPAA:** Protects patient health information (USA).
* **GDPR:** Data protection and privacy in the European Union.
* **SOX (Sarbanes-Oxley):** Requirements for financial record keeping for corporations.
* **DMCA:** Digital Millennium Copyright Act (Intellectual property).
* **FISMA:** Federal Information Security Management Act (US Government systems).