TRAINING DAY 2 REPORT:

- ## More Terms Used in Hacking

Today, I learned some more **important hacking terms**:

1. *Threat*
   A **potential cause of harm** to a system or data, such as a hacker, malware, or insider attack.
2. *Risk*
   The **likelihood that a threat will exploit a vulnerability**, causing damage or loss.
3. *Asset*
   Anything **valuable to an organization**, like data, hardware, software, or reputation, that needs protection.
4. *Bug*
   A **flaw or error in software code** that can cause unintended behavior or vulnerabilities.
5. *InfoSec* (Information Security)
   The practice of **protecting information systems and data** from unauthorized access, use, or destruction.
6. *Penetration Testing*
   Also called **pen testing**, it's an authorized attempt to **find and exploit vulnerabilities** in systems to improve security.
7. *Vulnerability Assessment*
   A process of **identifying, quantifying, and prioritizing vulnerabilities** in systems or networks.
8. *Cyber Espionage*
   The act of **stealing sensitive or confidential information** through digital means, usually for political or economic gain.
9. *Exploit*
   A **method or tool used to take advantage of a vulnerability** in a system.

10. *Script Kiddie*
    A person who uses existing **hacking tools or scripts without understanding how they work**, usually for fun or mischief.

11. *Zero-Day*
    A **newly discovered vulnerability** with no official fix or patch, exploited before developers can respond — known as a **zero-day attack**.

- # Cybercrime & Its Types

What is Cybercrime?

Cybercrime refers to **illegal activities committed using computers, networks, or the internet**, either as the main tool or target of the crime

Types of Cybercrime:

1. *Computer Fraud*
   Using computers to **deceive people or organizations for financial or personal gain**, such as fake websites or scams.
2. *Privacy Violation*
   Illegally **accessing or disclosing someone's private data**, like emails, photos, or personal documents.
3. *Identity Theft*
   Stealing someone's **personal information** (name, address, credit card details) to impersonate them or commit fraud.
4. *Sharing Copyrighted Files/Information*
   Illegally **distributing copyrighted software, movies, music, or documents** without the owner's permission — also called **piracy**.
5. *Electronic Funds Transfer (EFT) Fraud*
   Manipulating **electronic money transfers** to steal funds from bank accounts or financial institutions.
6. *Electronic Money Laundering*
   Using online transactions or cryptocurrencies to **hide or "clean" illegal money**.
7. *ATM Fraud*
   Using **skimming devices, stolen cards, or fake PIN pads** to steal money from ATMs or bank accounts.

8. *Denial of Service (DoS) Attacks*
   Flooding a website or server with massive traffic to **make it unavailable to users**, disrupting services.

9. *Spam*
Sending **unwanted, bulk emails or messages**, often containing ads, scams, or malware links.

- # History of Hacking

- how it started and evolved over time.

➢ **Early Days (1960s – 1970s)**

The term **"hacker"** originally referred to **clever programmers and engineers** at places like MIT who loved exploring and modifying computer systems creatively.
Hacking was about **innovation and pushing limits**, not malicious activity.

➢ **Phone Phreaking (1970s)**
Hackers called **phone phreakers** explored telephone networks to make **free long-distance calls** by manipulating tones.
Famous phreakers included **John Draper ("Captain Crunch")**.

➢ **Emergence of Computer Hacking (1980s)**
Personal computers became popular, and hacking shifted towards **breaking into computer systems**.
In 1983, the movie **WarGames** introduced hacking to the public, showing a teen accidentally accessing a military computer.
The **1986 U.S. Computer Fraud and Abuse Act (CFAA)** was passed to criminalize unauthorized computer access.

➢ **Rise of Cybercrime (1990s)**
The internet expanded, and hackers began exploiting **websites, networks, and email systems** for personal or financial gain.
Hacker groups like **L0pht** and **Cult of the Dead Cow** emerged, sharing exploits and tools.

➢ **2000s – Modern Hacking Era**
Cybercrime became **organized**, with attacks targeting governments, banks, and corporations.

➢ **Today’s Hacking Landscape**
Hacking now includes **state-sponsored attacks, hacktivism, and large-scale cyber espionage**.
Ethical hacking has also grown, with companies hiring **white hat hackers** to find vulnerabilities.

Over time, hacking evolved from curiosity and exploration to a mix of **ethical and malicious activities**, making cybersecurity more important than ever.

- # What is Hacking?

Hacking is the activity of **identifying weaknesses in a computer system or network to exploit the security and gain unauthorized access to personal or business data**.

- Hacking is the process used by an attacker to take control of a targetsystem without the owner’s permission.

- Mostly, hacking is used for criminal activities such as data theft, financial fraud, or spreading malware.

- There is no ethics in malicious hacking, as it violates privacy, security, and trust.

- # Who is a Hacker?

A **hacker** is a person who uses their **skills and knowledge to gain unauthorized access to software, computers, or networks**, often by exploiting vulnerabilities.

- Uses their own tools and techniques to break or bypass security measures.

- Is NOT always bad — hackers can be ethical (white hat) or malicious (black hat).
- A hacker **can go to prison if caught doing illegal hacking**, or **earn millions** if working legally as an ethical hacker.
- Hacking is **one of the most risky professions**, with high stakes whether working ethically or illegally.
- Hackers need **deep knowledge of computer systems, networking, programming, and security techniques**.

- # Types of Hackers

- *White Hat Hackers*
  Also called **ethical hackers**, they use their skills **legally to find and fix security vulnerabilities**. They help organizations strengthen security.

- *Black Hat Hackers*
  These are **malicious hackers** who break into systems illegally for personal gain, like stealing data, committing fraud, or spreading malware.

- *Grey Hat Hackers*
  They fall **between white and black hats** — they hack without permission but may not have malicious intent. For example, they might find a bug and report it, but still break laws in the process.

- *Script Kiddies*
  Inexperienced hackers who use **ready-made tools or scripts** without understanding how they work. They often hack for fun or to cause mischief.

- *Hacktivists*
  Hackers who use their skills to **promote political, social, or ideological causes**, for example, defacing websites to protest against governments or organizations.

- **Phreaker**
  A **phreaker** is a person who **manipulates or hacks telephone networks to make free calls or explore telecom systems**. The term comes from combining **"phone"** and **"hacker."**

• Ethical Hacking & Ethical Hackers

What is Ethical Hacking?

Ethical Hacking is the practice of **legally and systematically testing computer systems, networks, or applications for security vulnerabilities**, so they can be identified and fixed before malicious hackers exploit them.

- Ethical hacking is **authorized** by the system owner.
- It follows a **defined scope and rules of engagement** agreed upon with the organization.
- The main goal is to **protect the confidentiality, integrity, and availability** of data and systems.

Who is an Ethical Hacker?

An **Ethical Hacker**, also called a **white hat hacker**, is a **cybersecurity professional who uses hacking skills for defensive purposes**.

- They **find security weaknesses** in systems and report them to the owner.

- They use the **same tools and techniques as malicious hackers**, but in a legal and ethical manner.

- Ethical hackers often work as **penetration testers, security analysts, or consultants**.
- They help organizations comply with **security standards and regulations**.