TRAINING DAY 3 REPORT
2 JULY 2025

Understand Ethical Hacking, Ethical Hacker and Types of Hackers

Today, I learned some important concepts:

- ## What is Ethical Hacking?

Ethical hacking is the practice of legally and deliberately testing computer systems, networks, or applications to find security vulnerabilities before malicious hackers can exploit them. It is performed by trained professionals known as **ethical hackers** or **white hat hackers**, who have permission from the organization being tested. The goal of ethical hacking is to improve cyber security by identifying and fixing weaknesses.

- ## Who is a Ethical Hacker?

1. A **cyber security professional** who tests systems for vulnerabilities.

2. Works with **authorization** from the system owner.

3. Also known as a **white hat hacker**.

4. Identifies and reports **security weaknesses** before malicious hackers can exploit them.

5. Follows **legal and ethical standards**.

6. Helps improve the **security posture** of organizations.

- ## Who is a Hacker?

A hacker is a person with advanced knowledge of computers, networks, and programming who uses these skills to access or manipulate computer systems. Hackers may do this for ethical reasons (to improve security), malicious purposes (to steal or damage data), or curiosity.

- # Types Of Hackers

White Hat Hacker: A white hat hacker is an ethical cyber security expert who is authorized to test and assess computer systems, networks, or applications for security vulnerabilities. Their goal is to help organizations strengthen their defenses and prevent malicious attacks. White hat hackers follow legal and ethical guidelines and often work as penetration testers or security consultants.

Black Hat Hacker: A black hat hacker is a person who uses their technical skills to gain unauthorized access to computer systems, networks, or data for malicious purposes. Their activities often include stealing information, spreading malware, damaging systems, or committing fraud. Black hat hacking is illegal and harmful, and these hackers operate without permission or regard for the law.

Grey Hat Hacker: A grey hat hacker is someone who finds and exploits security vulnerabilities in computer systems **without permission**, but **without malicious intent**. They may inform the organization afterward or seek recognition or a reward, but their actions are still **unauthorized and potentially illegal**. Grey hat hackers fall between ethical (**white hat**) and malicious (**black hat**) hackers in terms of intent and behavior.

Script Kiddies: Script kiddies are beginners who use ready-made hacking tools without fully understanding how they work, usually to try to break into systems or cause trouble.

Hacktivist: A hacktivist is a hacker who uses their skills to promote political, social, or ideological causes by hacking into systems, defacing websites, or leaking information to raise awareness or protest.

Phreaker: A phreaker is someone who hacks into telephone systems to make free calls, manipulate phone networks, or explore how the phone system works. It's an early form of hacking focused on telecommunication systems.