Day 11: Ethical Hacking and Its Phases

Date: 8/07/25

Summary:
Today's session introduced us to the concept of **Ethical Hacking**, which is one of the core practices in the field of cybersecurity. We learned how ethical hacking helps in identifying vulnerabilities in systems before malicious hackers can exploit them. The session also covered the **phases of ethical hacking**, each of which is essential for performing a structured and legal penetration test.

Key Concepts Covered:

1. **What is Ethical Hacking?**
    - Ethical hacking refers to the **authorized and legal** attempt to gain access to computer systems, applications, or data to identify vulnerabilities and weaknesses.
    - Also known as **White Hat Hacking**.
    - Done with the permission of the system owner for the purpose of improving security.
2. **Types of Hackers:**
    - **White Hat Hackers –** Ethical hackers working for security.
    - **Black Hat Hackers –** Malicious hackers with illegal intent.
    - **Grey Hat Hackers –** Hackers who may violate laws but not for personal gain.
3. **Need for Ethical Hacking:**
    - To identify and fix security vulnerabilities.
    - To strengthen system defense against real cyberattacks.
    - To prevent data breaches and improve organizational trust.

🛠️ The 5 Phases of Ethical Hacking:

1. **Reconnaissance (Footprinting):**
    - The initial phase of gathering information about the target.
    - Types: **Active** (direct interaction), **Passive** (no direct contact).

    - Tools: Nmap, Whois, Maltego.

2. **Scanning:**
    - Identifying live hosts, open ports, and services.
    - Detecting vulnerabilities.
    - Tools: Nmap, Nessus, OpenVAS.
3. **Gaining Access:**
    - Exploiting the vulnerabilities found in the scanning phase.
    - Tools: Metasploit, SQLmap, Hydra.
4. **Maintaining Access:**
    - Ensuring persistent connection to the target system for future access.
    - Tools: Netcat, Backdoors, Reverse Shells.
5. **Clearing Tracks:**
    - Erasing logs and traces to avoid detection.
    - In **ethical hacking**, this phase is used to simulate real-world attack scenarios safely and is followed by reporting.

Hands-on/Activity:

- We were shown a live demonstration of the **Reconnaissance** and **Scanning** phases using **Nmap** and **Whois lookup**.
- Discussed a case study where an ethical hacker helped a company prevent a large-scale data breach.