Daily Diary – Day 5: Cybersecurity Training

Date: 28/06/25

🔍 What We Learned Today

Today's session was centered around **Nmap (Network Mapper)**, a powerful and essential tool in cybersecurity for **network discovery and security auditing**. Sir explained both **theoretical concepts** and gave us a **live demonstration** on how to install and use Nmap in the **Windows operating system**.

🧠 Key Concepts Explained

1. **Introduction to Nmap:**
    - Nmap stands for **Network Mapper**.
    - It is an **open-source tool** used to discover hosts and services on a computer network.
    - Commonly used by **network administrators, ethical hackers, and security professionals**.
2. **Purpose and Applications:**
    - Scan large networks efficiently.
    - Identify live hosts, open ports, and running services.
    - Detect operating systems and hardware types.
    - Perform vulnerability scanning (when extended with scripts).
3. **Important Nmap Features:**
    - Host discovery (ping sweep).
    - Port scanning (TCP, UDP, etc.).
    - Service version detection.
    - OS detection.
    - Scriptable interaction with the target using **Nmap Scripting Engine (NSE)**.

🧑‍💻 Installation of Nmap on Windows:

Sir gave a step-by-step demo for installing Nmap on a Windows system:

1. **Downloading Nmap:**

    - Go to the official website: https://nmap.org/download.html.
    - Download the **Windows installer (.exe file)**.

2. **Installation Steps:**
    - Run the downloaded .exe file.
    - Follow the installation wizard.
    - Select the option to install **Nmap, Zenmap (GUI), Ncat, and Ndiff**.
    - Complete installation and verify by running nmap in the Command Prompt.
3. **Basic Commands Practiced:**
    - nmap <target IP> – Basic scan.
    - nmap -sP <subnet> – Ping sweep.
    - nmap -sS <target> – TCP SYN scan (stealth scan).
    - nmap -O <target> – OS detection.
    - nmap -sV <target> – Service version detection.

🧪 Hands-On Task Assigned

At the end of the session, Sir gave us a practical task:

- **Scan your own local network** using Nmap and list:
    - Number of active hosts.
    - Open ports on a specific IP.
    - OS and services running (if identifiable).

📚 Learning Outcome

By the end of today’s session, we understood:

- The **importance of network scanning** in identifying vulnerabilities.
- How to **safely install and use Nmap** on a Windows machine.
- The **basic usage of Nmap commands** for scanning and analyzing a network.

📝 Reflection

This was a very informative session as it introduced us to one of the **most used tools in cybersecurity**. We appreciated the hands-on approach and found the **command-line usage and Zenmap GUI** to be very insightful. We now feel confident in performing basic scans and look forward to deeper use of **Nmap Scripting Engine (NSE)** in upcoming sessions.