Day 42

Topic: Network Scanning using Nmap

Objective: To discover active hosts and open ports on a network using Nmap (Network Mapper).

Theoretical Concepts:
Scanning is the first active touch on the target network. We focused on **Nmap**, the king of scanners. We learned about the TCP 3-way handshake and how Nmap manipulates it (e.g., SYN Scan vs. Connect Scan). We discussed port states: Open, Closed, and Filtered (blocked by firewall).

Practical Work:
We ran various Nmap scans against our lab target (Metasploitable): *nmap -sP*: Ping sweep to find live hosts. *nmap -sS*: Stealth scan (SYN scan). *nmap -sV*: Version detection to find what software version is running on the ports. *nmap -O*: OS detection. We analyzed the output to identify potential entry points.

Tools Used: Nmap, Zenmap (GUI).

Outcome: Proficient in mapping a network topology and identifying open services.