Day 13 – Topic: Footprinting, Scanning, and Grabbing
Date: 10/07/25

🧠 What We Learned Today:

Today in our cybersecurity session, sir taught us about the **initial phases of ethical hacking** which include:

---

1. 🔍 Footprinting

Footprinting is the **first step in the information gathering phase** of hacking. It is about collecting data about a target system or organization to find ways to attack it.

- **Types of Footprinting:**
    - **Passive Footprinting:** Gathering information without direct interaction (e.g., social media, WHOIS, websites).
    - **Active Footprinting:** Directly engaging with the target (e.g., pinging, traceroute).
- **Tools/Methods used:**
    - WHOIS lookup
    - DNS Interrogation
    - Google Dorking
    - Social Engineering

---

2. 📡 Scanning

Scanning is the process of identifying **live hosts, open ports, and services** running on a system.

- **Types of Scanning:**
    - **Port Scanning:** Finding open ports using tools like Nmap.
    - **Network Scanning:** Identifying live hosts and IP addresses.
    - **Vulnerability Scanning:** Detecting vulnerabilities in the system.
- **Tools Used:**
    - Nmap
    - Angry IP Scanner
    - Advanced IP Scanner

---

3. 🧾 Enumeration (Grabbing)

Enumeration is a more detailed scanning phase where we extract **specific information like usernames, shares, services** from the system.

- **Common Enumeration Targets:**
  - Network resources
  - Usernames and groups
  - SNMP, SMB, LDAP info
- **Tools Used:**
  - Netcat
  - SNMPwalk
  - Enum4linux

💡 Key Takeaways:

- Footprinting helps identify what information is publicly available.
- Scanning helps map out network structure and open services.
- Enumeration digs deeper to get actual system data like users and services.

🧪 Practical Task:

Sir also demonstrated some scanning tools on Kali Linux like:

- Using nmap for port and OS detection.