Cybersecurity Internship

Task 1: Port Scanning with Nmap

Objective:

- To discover open ports on devices in my local network using Nmap and understand how attackers might use port scanning to identify vulnerabilities.

Tools Used:

- Nmap – for scanning open ports
- Wireshark – for monitoring packets during the scan
- OS – Kali Linux

Steps Performed:

1. Identified Local IP Range:
   - Used **ifconfig** for Linux to find my local subnet.
   - **netdiscover** command can also be used to find IP address.
2. Performed TCP SYN Scan with Nmap:
   - **sudo nmap –sS –sV 192.168.171.131/24**
   - This will scan all devices on your network and list open TCP ports and their services with service version**.**
3. Saved Scan Results:
   - You can save results in text or HTML in
   - Sudo nmap **-sS –sV 192.168.171.131/24 –oX scanfile.html**
   - Scanfile.html is the file name
4. Monitored the scan using **Wireshark** to observe SYN/SYN-ACK traffic.

Findings:

- Number of active devices found: 5
- Open ports detected on some devices:
  - 192.168.171.2
    -Open Port: 53
  - 192.168.171.130 (most ports open , 22 ports open in total)
    -Open Ports: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

- Devices with No Open Ports:
  - 192.168.171.1 – All 1000 ports filtered
  - 192.168.171.131 – All 1000 ports closed
  - 192.168.171.254 – All 1000 ports filtered