Cyber Security Internship – Task 1 Report

NAME: DISHANYAA SHRII K M
DATE: 22/09/2025
TITLE: Scan Your Local Network for Open Ports

---

1. Objective

To discover open ports on devices in the local network using Nmap and optionally analyze network traffic with Wireshark. This helps understand network exposure and the risks associated with open services.

---

2. Tools Used

- **Nmap** (Network Mapper) – Free
- **Wireshark** (Optional) – Packet analyzer for observing network traffic

---

3. Key Concepts

- **Port Scanning:** Method to identify open ports on network devices.
- **TCP SYN Scan:** Nmap technique to quickly detect open TCP ports without completing the full handshake.
- **IP Ranges:** Group of IP addresses in a network (e.g., 192.168.1.0/24).
- **Open Ports:** Network entry points where services are listening.
- **Network Security Risks:** Open ports may expose services to attacks.

---

4. Steps Performed

Step 1: Installed Nmap on Kali Linux

```
sudo apt install nmap
```

Step 2: Identified local IP range

```
ip a
# Example output: 192.168.1.100/24
```

Step 3: Ran TCP SYN Scan

```
nmap -sS 192.168.1.0/24
```

Step 4: Noted open ports and IP addresses of devices in the local network. **Example Output:** | IP Address | Open Ports | Services | |----------------|-----------|----------------| | 192.168.1.1 | 80, 443 | HTTP, HTTPS | | 192.168.1.102 | 22 | SSH | | 192.168.1.150 | 139, 445 | SMB |

Step 5 (Optional): Captured packets with Wireshark for analysis. - Interface used: `wlan0` - Filter applied: `tcp` or `ip.addr == 192.168.1.102` - Observed SYN, SYN-ACK, and ACK packets for open ports.

Step 6: Researched common services running on discovered ports (HTTP, SSH, SMB, etc.)

Step 7: Identified potential security risks - Open SSH (22) without strong passwords may be brute-forced.
- SMB (139, 445) may be exploited if not patched.
- HTTP (80) may expose sensitive data if not secured.

Step 8: Saved scan results as files - `scan_results.txt`
- `scan_resultss.xml`
- `screenshot.png`

---

5. Observations

- Multiple devices with services exposed to the local network were discovered.
- Most common open ports: 22 (SSH), 80/443 (HTTP/HTTPS), 139/445 (SMB).
- Using Wireshark, the handshake patterns for TCP SYN scans were visible.

---

6. Outcome

- Gained hands-on experience in scanning local networks for open ports.
- Learned how to interpret Nmap scan results.
- Understood network service exposure and associated risks.
- Observed real-time packet exchanges using Wireshark.

---

7. Folder and Files Included

Folder Name: `/home/dishanyaa_shrii_k_m/task_1_elevate_labs`

Files: - `README.md`
- `scan_results.txt`

- `scan_resultss.xml`
- `screenshot.png`