LOCAL NETWORK PORT SCANNING REPORT

Cyber Security Internship Task Submission

Prepared By: Muhammed Shan Yoosuf

Date: 20 February 2026

1. Objective

The objective of this task was to perform network reconnaissance by scanning the local network to identify active hosts and open ports. The goal was to understand service exposure and evaluate potential security risks associated with open ports.

2. Tools Used

- Nmap – TCP SYN Scan
- Wireshark – Packet Capture Analysis
- Windows Command Prompt

3. Methodology

The local IP range 192.168.1.0/24 was identified. A TCP SYN scan was performed using the following command:

```
nmap -sS 192.168.1.0/24 -oN nmap_scan.txt -oX nmap_scan.xml
```

4. Scan Results

Host IP	Open Port	Service	Risk Level
192.168.1.1	80	HTTP	Medium
192.168.1.5	22	SSH	Medium
192.168.1.10	443	HTTPS	Low
192.168.1.15	445	SMB	High
192.168.1.20	3389	RDP	High

5. Risk Analysis

- Open SSH ports may be vulnerable to brute-force attacks.
- Exposed HTTP services may reveal outdated applications.
- SMB and RDP ports are high-risk if not properly secured.
- Multiple open ports increase the network attack surface.

6. Security Recommendations

- Close unused ports and disable unnecessary services.

- Implement firewall rules to restrict external access.
- Use strong passwords and multi-factor authentication.
- Regularly update systems with security patches.

7. Conclusion

The network scan successfully identified multiple active hosts and open ports within the local network. The findings highlight the importance of continuous monitoring, proper port management, and implementing security best practices to reduce potential vulnerabilities.