Cyber Security Internship – Task 1 Report
Scan Your Local Network for Open Ports

Student Name: Dhanush Rao
Task: Network Port Scanning
Tool Used: Nmap
Objective: Learn to identify open ports and active devices in a local network to understand network exposure and basic reconnaissance techniques.

Procedure

1. Installed Nmap from the official website.
2. Identified the local IP address using the **ipconfig** command.
3. Determined the network range (example: 192.168.1.0/24).
4. Ran a TCP SYN scan using the command: **nmap -sS 192.168.1.0/24**.
5. Observed active devices and open ports.
6. Saved the scan results using: **nmap -sS 192.168.1.0/24 -oN scan-results.txt**.

Sample Scan Results

IP Address	Open Port	Service
192.168.1.1	80	HTTP
192.168.1.5	445	SMB
192.168.1.8	22	SSH

Security Risks of Open Ports

Open ports can expose services to unauthorized users. Attackers may exploit vulnerable services, gain unauthorized access, or perform further attacks on the network. Regular monitoring and proper firewall configuration help reduce these risks.

Conclusion

This task demonstrated how network scanning tools can identify active devices and open ports within a local network. Understanding these concepts helps improve awareness of network security and potential vulnerabilities.