Nmap Port Scanning Report

■ Cyber Security Internship – Task 1 Report

Task Name: Scan Your Local Network for Open Ports
Tool Used: Nmap
Optional Tool: Wireshark (Not used here)

Objective

Scan the local network to discover live devices and open TCP ports, to understand potential network exposure using Nmap.

Step – 1

Find network range: Used ipconfig to see IPv4 address (e.g. 192.168.1.2) and subnet mask (255.255.255.0), so the network is 192.168.1.0/24.

Step - 2: Discover Live Devices

Discover live devices:
nmap -sn 192.168.1.0/24
Identified hosts that responded, only those are scanned further.

Step - 3: Scan Open Ports

Command used: nmap -sS 192.168.1.0/24
Performs a TCP SYN scan to find open ports efficiently.

Live Devices (Hosts Up):

1. 192.168.1.1 - Host is up
2. 192.168.1.2 - Host is up
3. 192.168.1.3 - Host is up

Step - 4: Open Ports and Services

192.168.1.1

1. Port 53 is open (DNS): Router handles name lookup inside your network.
2. Port 80 is open (HTTP): Router admin page is accessible in plain text, not secure.
3. Port 443 is open (HTTPS): Secure, encrypted admin access.

192.168.1.2

1. Port 135 is open (RPC): Windows background service may expose system info if not patched.
2. Ports 139 & 445 are open (NetBIOS / SMB): Used for Windows file sharing, high risk if exposed. Attacks like WannaCry used these vulnerabilities.

192.168.1.3

1. No open TCP ports detected – no services running, low risk.

Conclusion

Ran a port scan on the network (192.168.1.0/24) and detected active services including DNS, router admin pages (HTTP/HTTPS). These services enable usage but can also expose risks if unneeded or unpatched; keeping unused ports closed and monitoring regularly helps maintain security.