Cyber Security Internship – Task 1 Report

\*\*Name:\*\* Naveen Kumar

\*\*Date of Scan:\*\* May 26, 2025

\*\*Task:\*\* Scan Local Network for Open Ports

\*\*Tool Used:\*\* Nmap

\*\*Command Used:\*\* nmap -sS 192.168.184.0/24

# Scan Summary

|  |  |  |
| --- | --- | --- |
| IP Address | Open Ports | Services |
| 192.168.184.234 | 135, 139, 445 | MSRPC, NetBIOS-SSN, Microsoft-DS (SMB) |

# Risk Analysis

- \*\*Port 135 (MSRPC):\*\* Often used for remote procedure calls; may be vulnerable if exposed to untrusted networks.  
- \*\*Port 139 (NetBIOS-SSN):\*\* Common for Windows file sharing; can be a security risk if exposed.  
- \*\*Port 445 (SMB):\*\* Vulnerable to attacks like WannaCry ransomware if unpatched or exposed.

# Conclusion

The scan identified 2 active hosts in the local network. The device at 192.168.184.234 has ports related to Windows file sharing and remote procedure services open. These ports can be risky if the device is not properly secured. It's recommended to ensure firewall rules are in place and unnecessary services are disabled to reduce attack surface.