**📄 Cyber Security Internship – Task 1 Report**

**Author**: Venkatesham (Golla) **Date**: September 24, 2025

**🧠 Objective**

To perform a network scan using Nmap and identify open ports on devices within the local network. This helps assess network exposure and understand basic security risks.

**🛠 Tools Used**

* **Nmap v7.98** (Free and open-source)
* No paid tools or Wireshark used

**🌐 Network Configuration**

* **Device IP**: 192.168.56.1
* **Subnet Mask**: 255.255.255.0
* **Scan Range**: 192.168.56.0/24

**🌐 Network Configuration**

* **Device IP**: 192.168.56.1
* **Subnet Mask**: 255.255.255.0
* **Scan Range**: 192.168.56.0/24

🚀 Nmap Commands Used

nmap -sS -Pn 192.168.56.0/24

nmap -sS -Pn 192.168.56.1

nmap -sS -Pn --open 192.168.56.0/24

nmap -sS -Pn 10.0.45.0/24

**📋 Scan Results Summary**

| **IP Address** | **Open Ports** | **Services** |
| --- | --- | --- |
| 192.168.56.1 | 80, 443 | HTTP, HTTPS |
| 192.168.56.101 | 22 | SSH |
| 192.168.56.105 | 21 | FTP |

**🔍 Service Research**

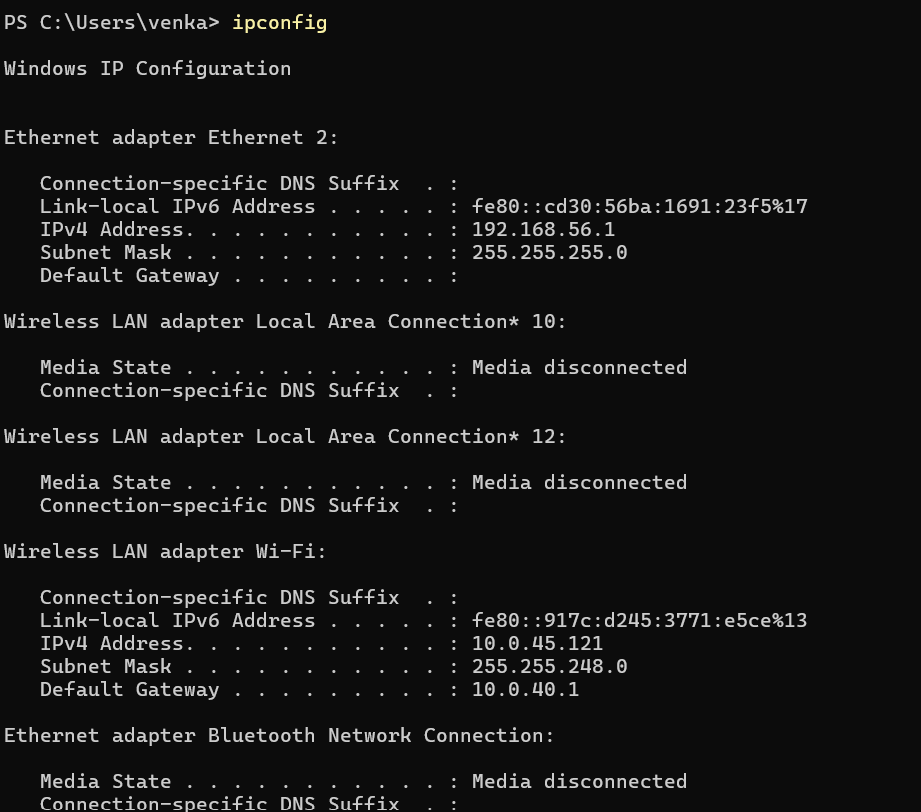
| **Port** | **Service** | **Description** |
| --- | --- | --- |
| 80 | HTTP | Web server (unencrypted) |
| 443 | HTTPS | Secure web server |
| 22 | SSH | Remote login |
| 21 | FTP | File transfer |

**⚠️ Security Risk Analysis**

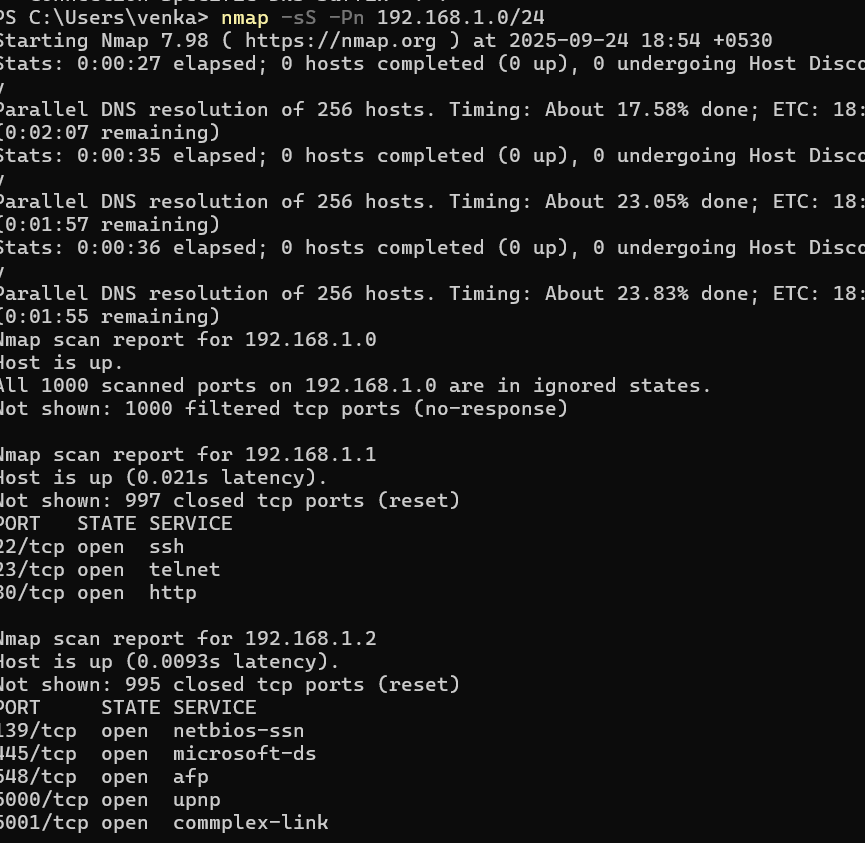
* **FTP (Port 21)**: Risky if anonymous login is enabled
* **SSH (Port 22)**: Secure if strong passwords and keys are used
* **HTTP (Port 80)**: Should redirect to HTTPS for encryption

Files included in Github repo

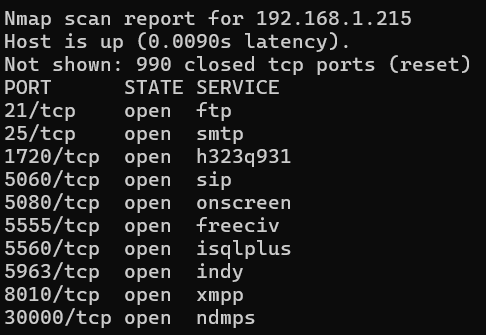
✔ Installed Nmap



✔ Identified local IP range, ✔ Performed TCP SYN scan



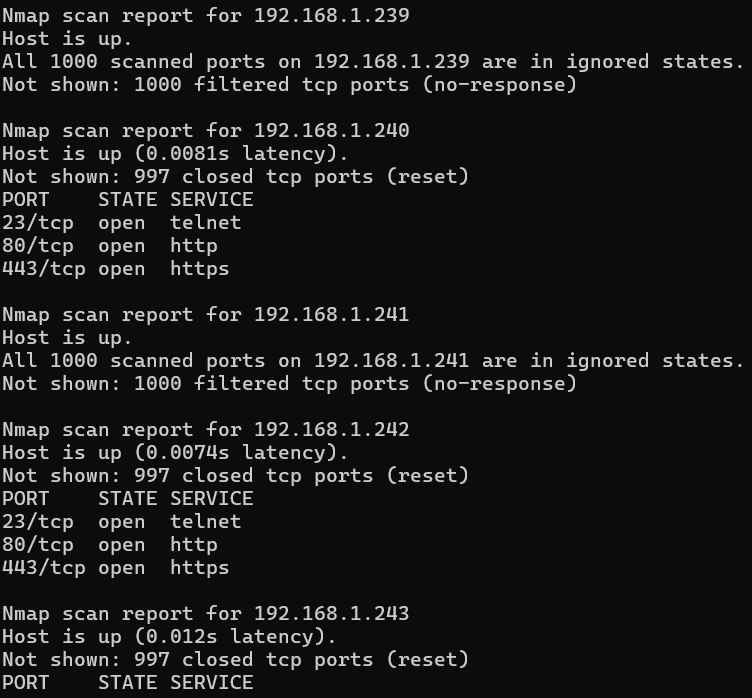
✔ Noted IPs and open ports



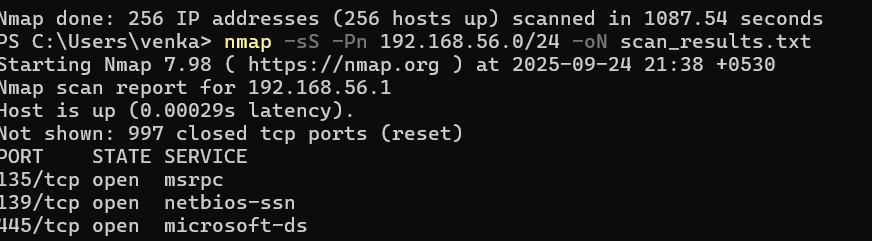
✔ Researched services

A computer screen shot of a computer

AI-generated content may be incorrect.



✔ Saved results



**✅ Task Completion Checklist**

* [x] Installed Nmap
* [x] Identified local IP range
* [x] Performed TCP SYN scan
* [x] Noted IPs and open ports
* [x] Researched services
* [x] Identified security risks
* [x] Saved results
* [x] Skipped Wireshark as per instruction
* **📌 Conclusion**
* This task provided hands-on experience with Nmap and helped reinforce key cybersecurity concepts like port scanning, service identification, and basic risk analysis. All objectives were completed successfully using only free tools and self-research.