**Internship Report: Scanning Local Network for Open Ports**

**Date: 23/06/2025**

**Performed by: Aryanshu Saha**

**Internship Organization: Elevate Labs**

**Task Objective**

The purpose of this task is to discover open ports on devices within the local network to assess potential security risks and better understand network exposure. This helps in identifying vulnerable services and aids in securing networked systems.

**Tools Used**

* **Nmap** – A powerful network scanning tool for host discovery and port scanning.
* **Wireshark** *(Optional)* – For capturing and analyzing packet-level traffic.

**Methodology**

**Step 1: Install Nmap**

sudo apt update

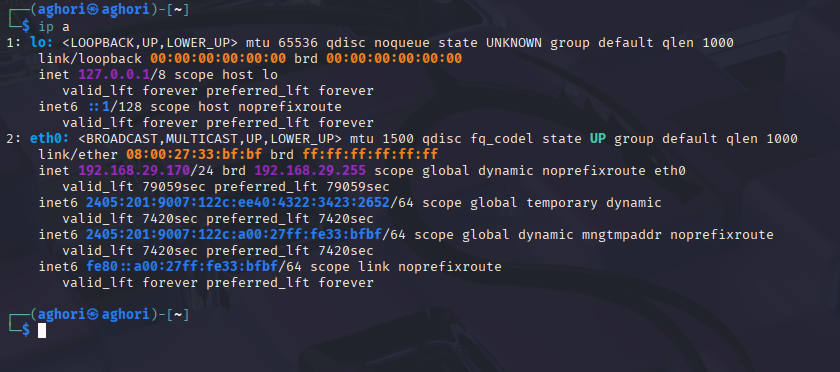
sudo apt install nmap

**Step 2: Identify Local IP Range**

ip a

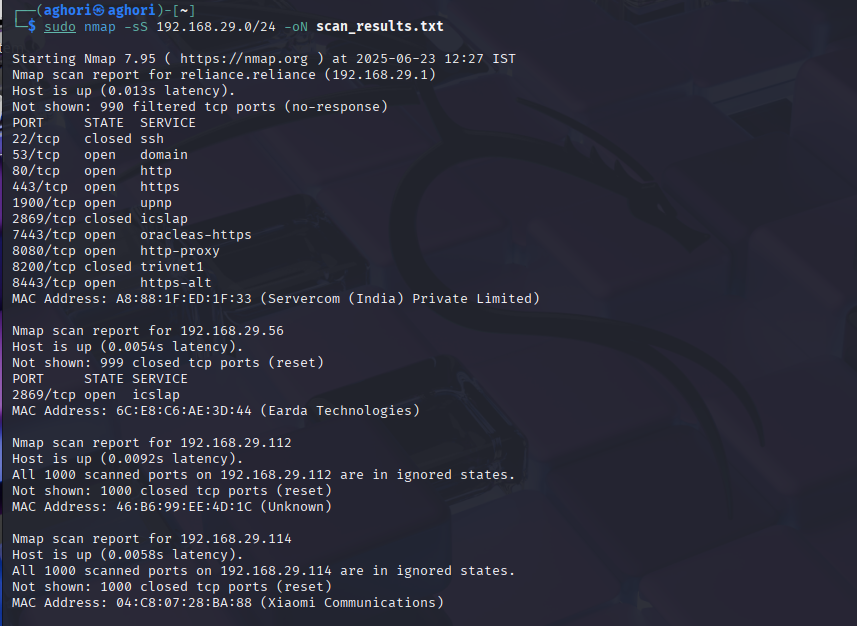
inet 192.168.29.170/24

Identified subnet: 192.168.29.0/24



**Step 3: Perform TCP SYN Scan**

sudo nmap -sS 192.168.29 -oN scan\_results.txt .0/24



This command:

* Conducts a **stealth SYN scan**
* Targets all 256 hosts in the /24 subnet
* Saves results in scan\_results.txt

**Optional Step 4: Capture Packets (Wireshark)**

* Interface: eth0 or wlan0
* Filter: tcp.port==80 (or relevant services)

**🔍 Findings**

**Example Output Summary:**

| **IP Address** | **Open Ports** | **Common Services** |
| --- | --- | --- |
| 192.168.1.1 | 80, 443 | HTTP, HTTPS (Router) |
| 192.168.1.100 | 22, 80 | SSH, Web Server (Linux) |
| 192.168.1.105 | 139, 445 | SMB (Windows Sharing) |

**🧠 Analysis**

* **Port 22 (SSH)**: Risk of brute-force attacks if not secured with key-based auth.
* **Port 445 (SMB)**: Often exploited in ransomware attacks; ensure it's patched.
* **Port 80/443**: Verify web servers are up-to-date and configured securely.

**📂 Report Files**

* scan\_results.txt – Raw scan data.
* network\_map.html *(optional)* – Visual layout if exported using Nmap GUI or third-party script.
* packets.pcap *(optional)* – Packet capture file analyzed with Wireshark.

**🛡️ Recommendations**

* Close unused ports.
* Enforce firewall rules (e.g., ufw, iptables).
* Ensure all services are updated and monitored.

**📚 References**

* Nmap Official Documentation
* Wireshark Filters Guide
* Kali Linux Toolset (2025.2 updates)