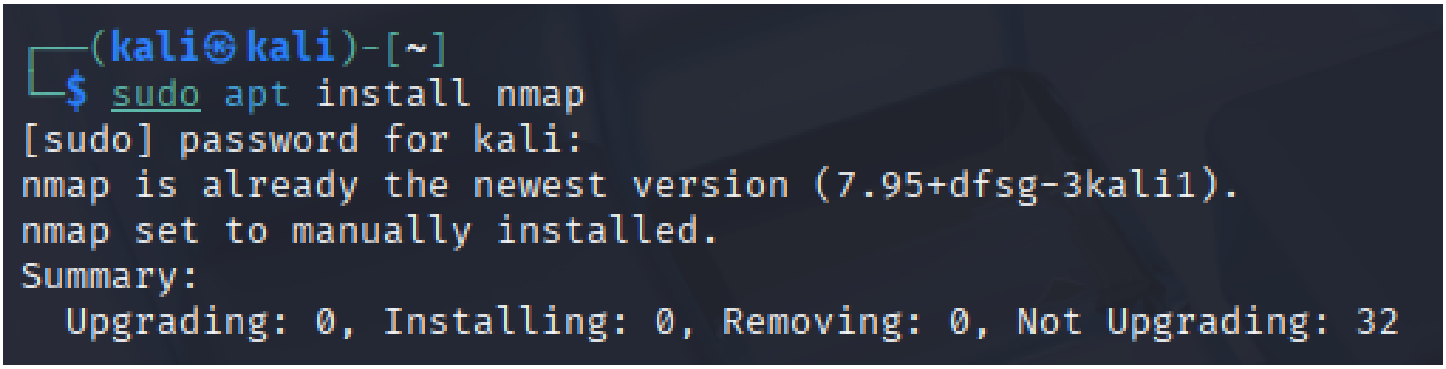
ELEVATE LABS CYBER SECURITY INTERNSHIP

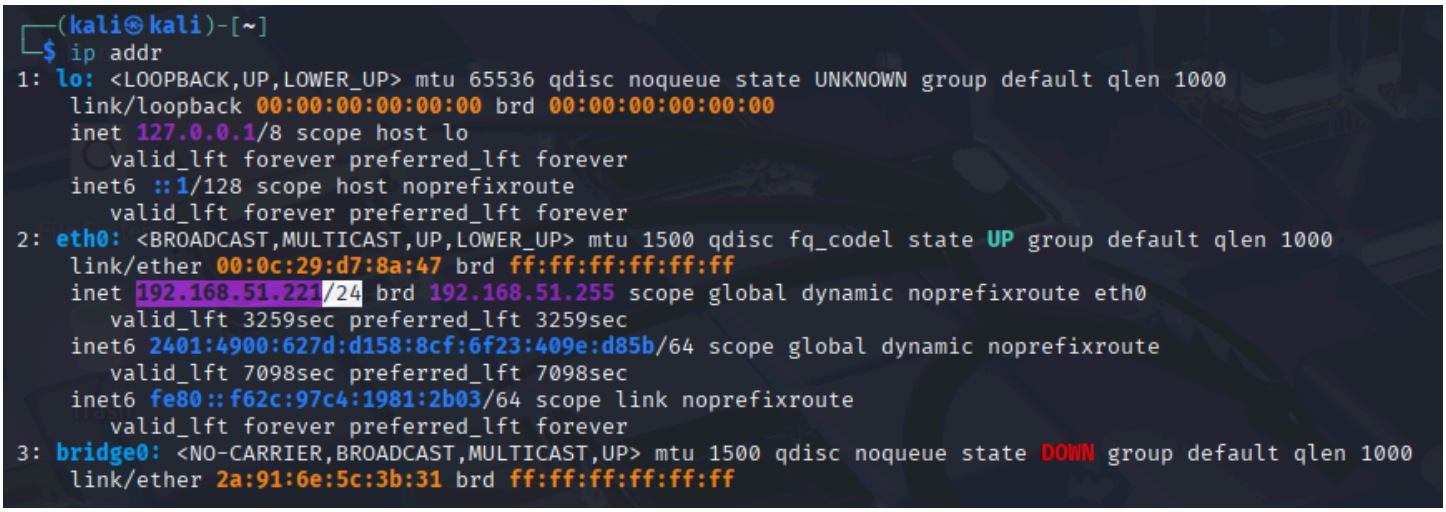
Task-1:

1. Install Nmap from official website.

Used the linux command `sudo apt install nmap` in my kali linux and downloaded `nmap`.

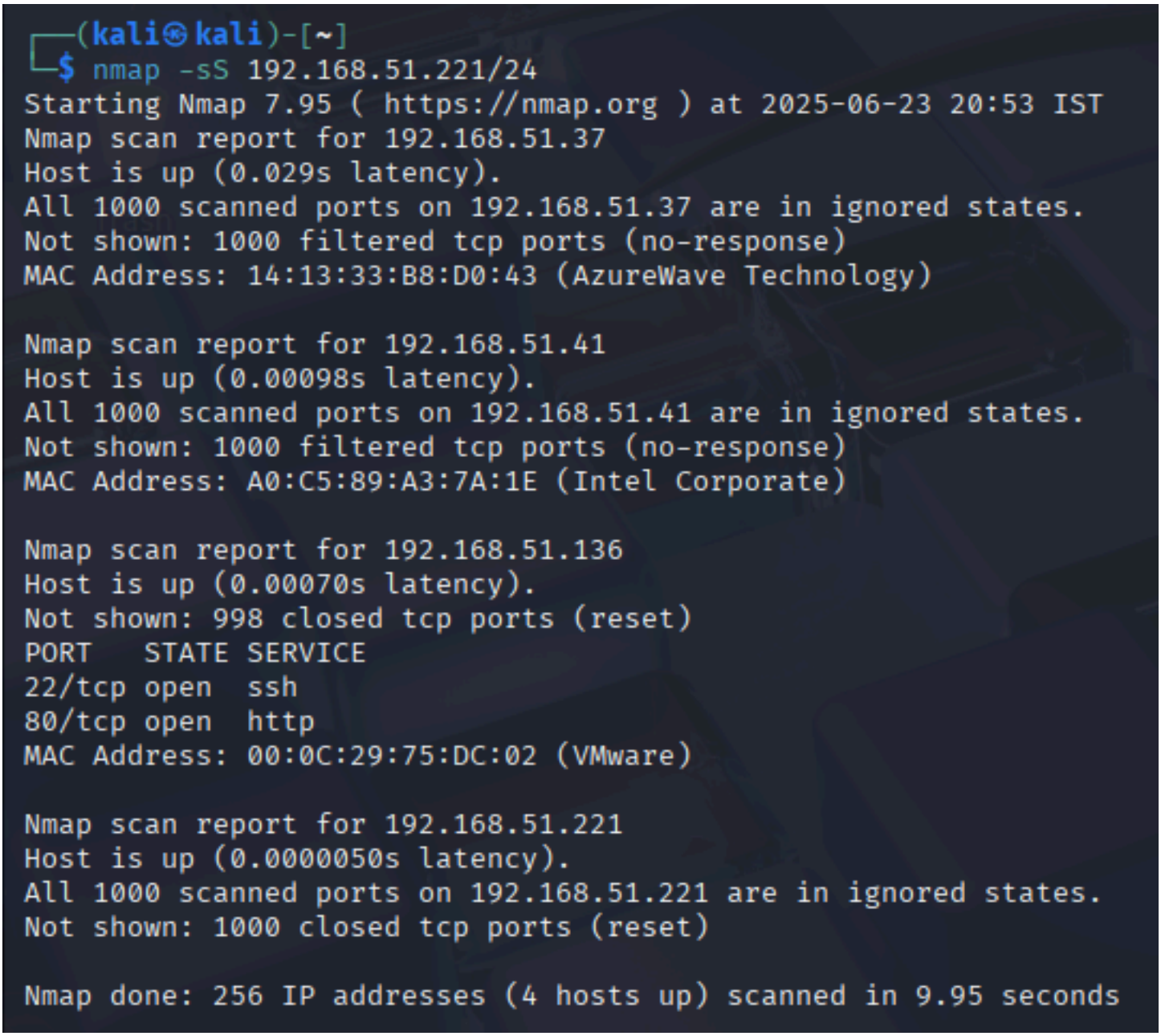


2. Find your local IP range



Here I can find my ip address as `192.168.51.222` with the subnet /24. Now I am scanning this in the nmap using the command `sudo nmap -sn 192.168.51.222/24` to perform ping scan without a port scan.

3. Run: nmap -sS 192.168.51.222/24 to perform TCP SYN scan

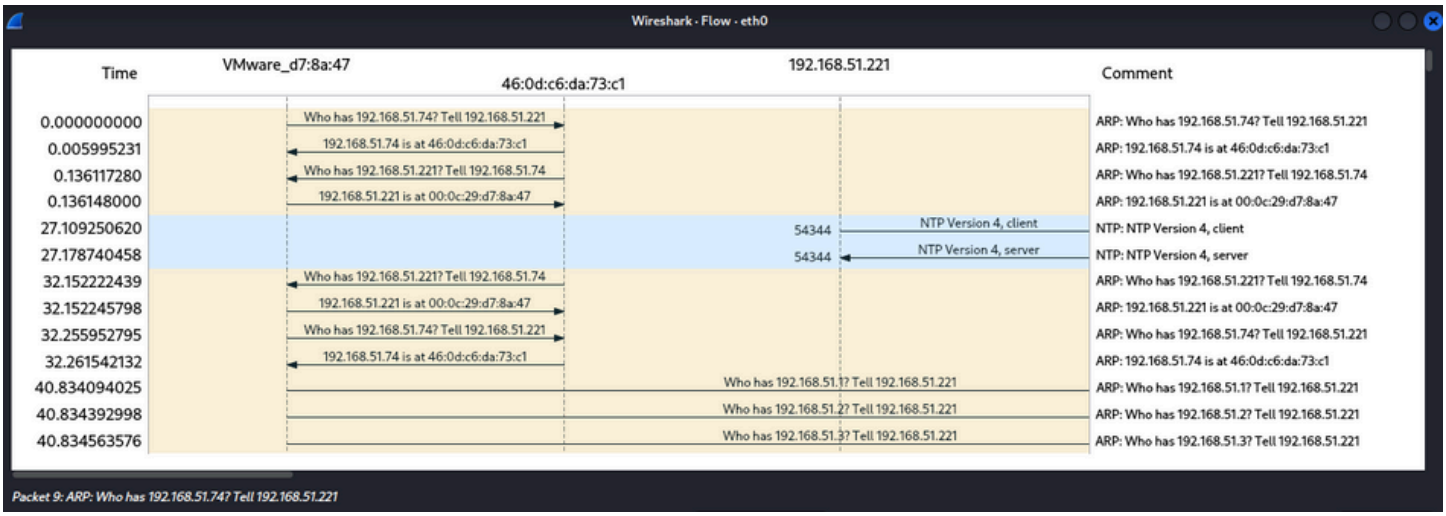


4. Note down IP addresses and open ports found.

The IP addresses of the open ports found are 192.168.51.136 (2 open ports).

5. Optionally analyze packet capture with Wireshark.

Captured the live trac through wireshark



6. Research common services running on those ports.

Port	Service	Purpose
22/tcp	ssh	Provides secure command-line access and remote login over an encrypted connection.
80/tcp	http	Facilitates the transfer of web pages and resources over the internet.

7. Identify potential security risks from open ports.

Port	Service	Potential Security Risks
22/tcp	SSH	• Brute-force attacks on login credentials. • If weak or default passwords are used, attackers may gain remote access. • Unpatched SSH versions can have vulnerabilities.
80/tcp	HTTP	• Unencrypted data transmission, making it vulnerable to eavesdropping or Man-in-the-Middle (MitM) attacks. • May expose web server software to exploits if outdated. • Susceptible to web attacks like XSS, SQL injection, etc. if web apps are misconfigured.

8. Save scan results as a text or HTML file.