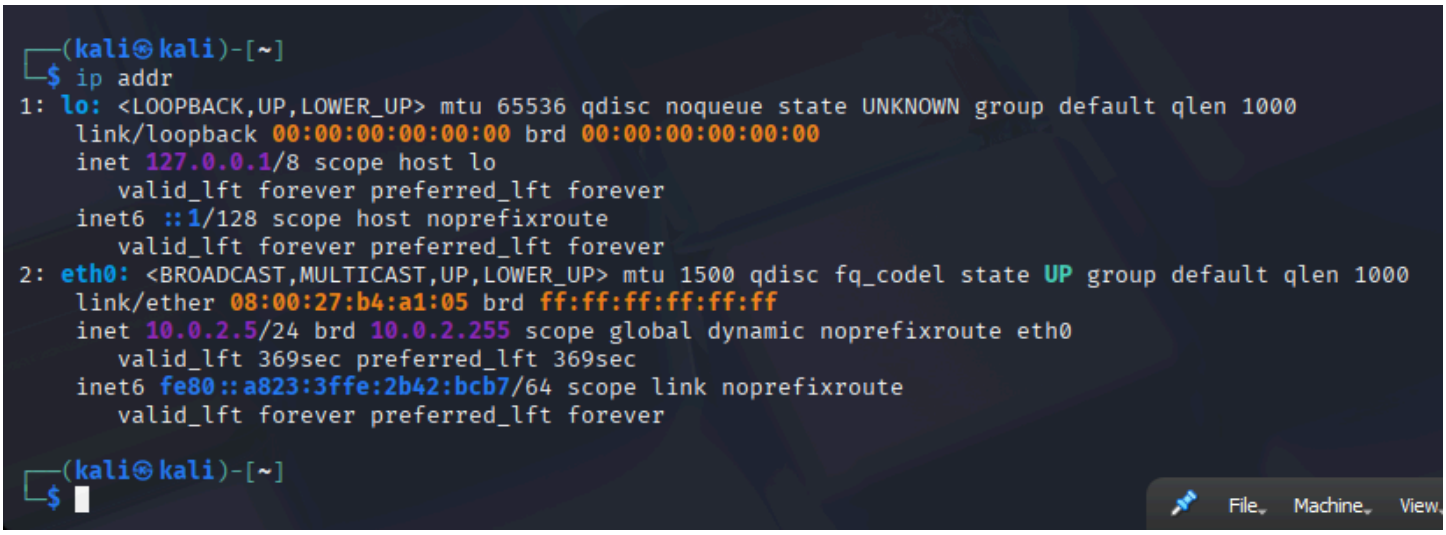
ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-1:

1) 1.Install Nmap from official website.

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

2.Find your local IP range



Here I can find my ip address as 10.0.2.5 with the subnet /24. Now I am scanning this in the nmap using the command sudo nmap -sn 10.0.2.5/24 to perform ping scan without a port scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 10.0.2.5/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 11:43 IST
Nmap scan report for 10.0.2.1
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00017s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00064s latency).
MAC Address: 08:00:27:C8:A0:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 4.62 seconds

┌──(kali㉿kali)-[~]
└─$
```

3.Run: nmap -sS 10.0.2.5/24 to perform TCP SYN scan.

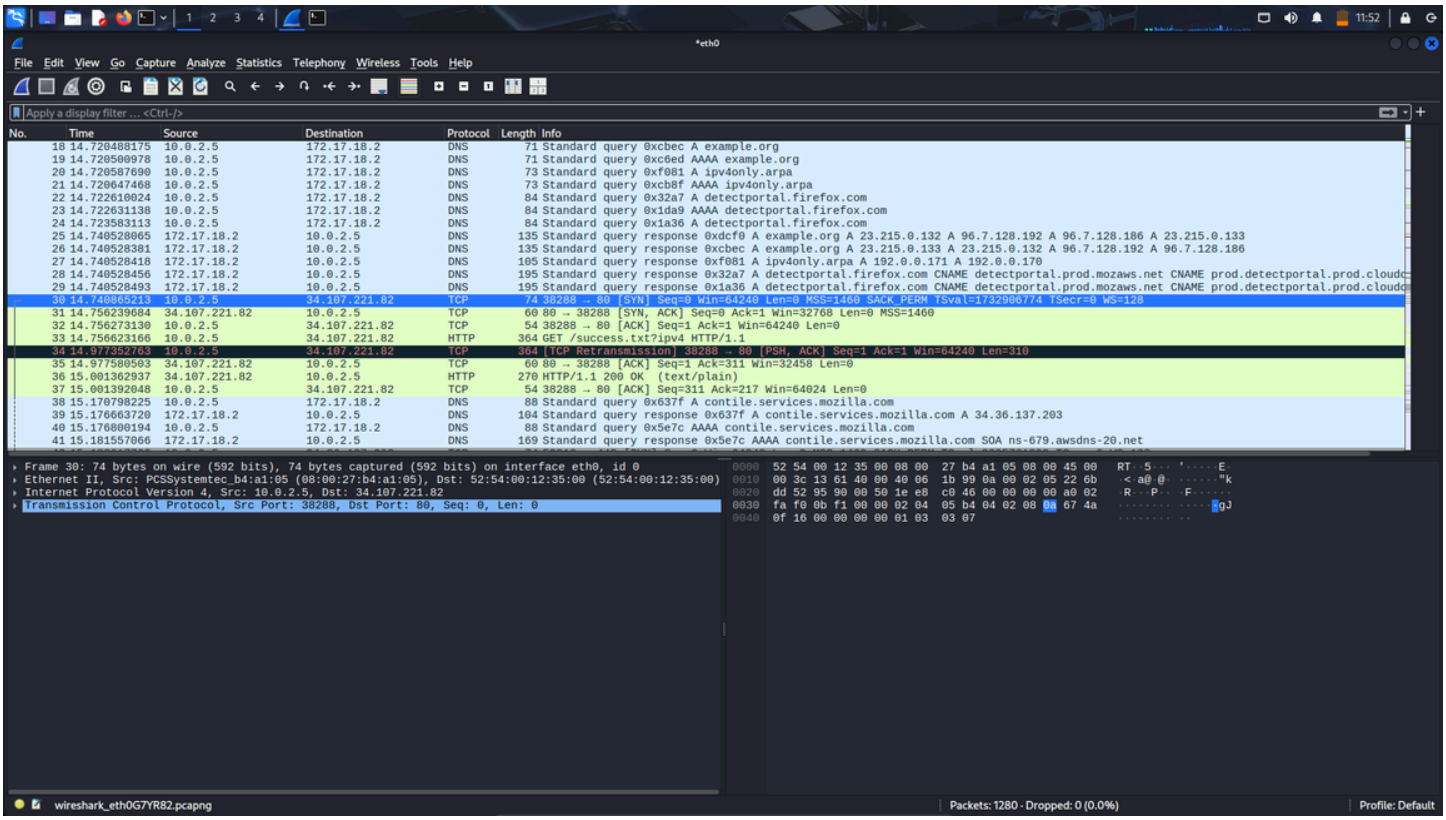
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 10.0.2.5/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 11:46 IST
Nmap scan report for 10.0.2.1
Host is up (0.00073s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.00056s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:C8:A0:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.5
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.0.2.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.57 seconds

┌──(kali㉿kali)-[~]
└─$
```

4.Note down IP addresses and open ports found.

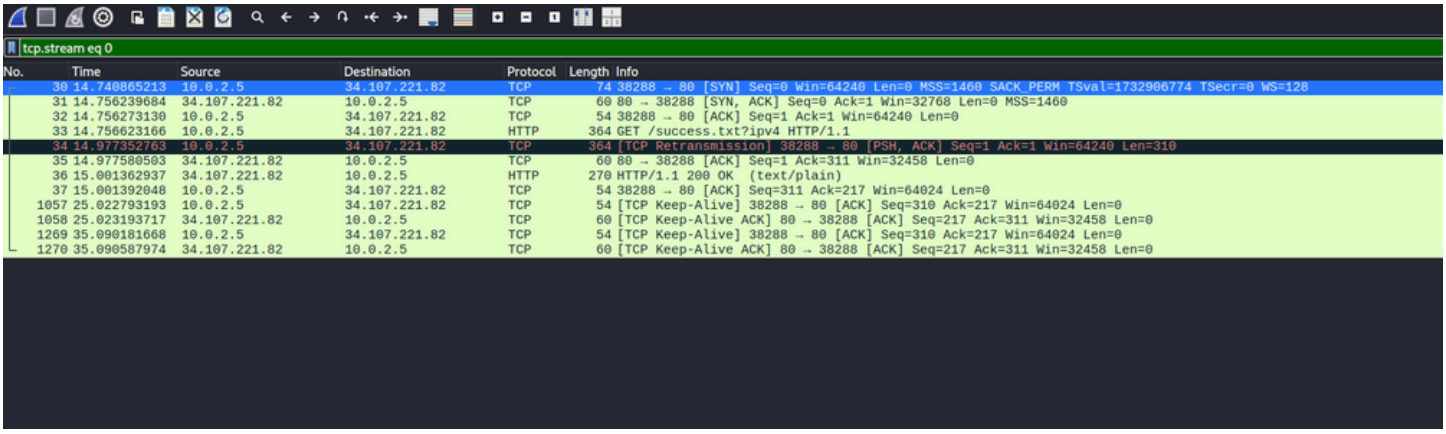
The IP addresses of the open ports found are 10.0.2.1 (1 open port) and 10.0.2.2 (3 open ports)

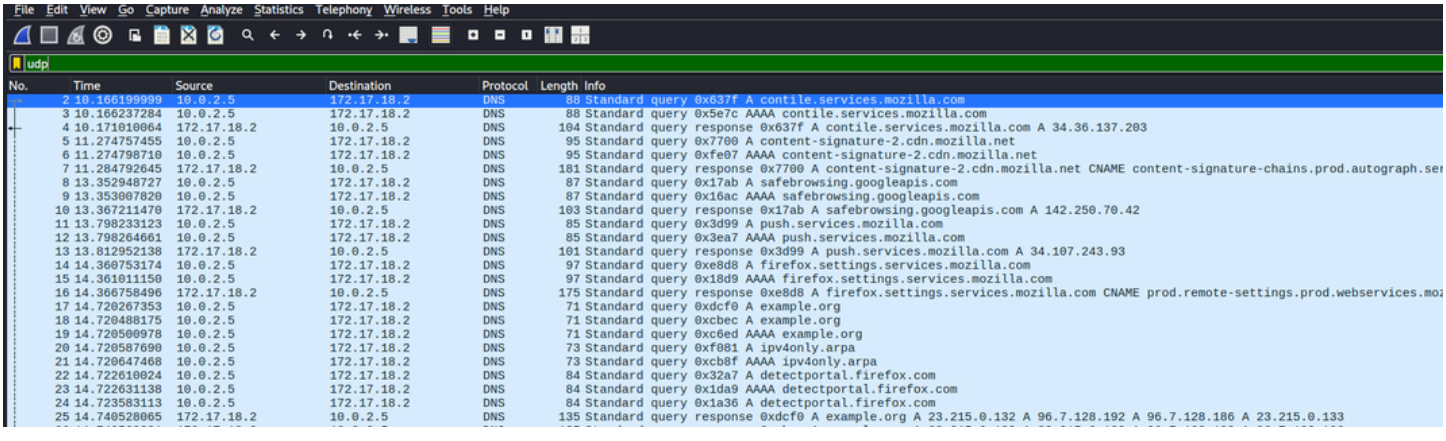
5.Optionally analyze packet capture with Wireshark.

Captured the live traffic through wireshark



Analysing the tarffic using some of the available filters.





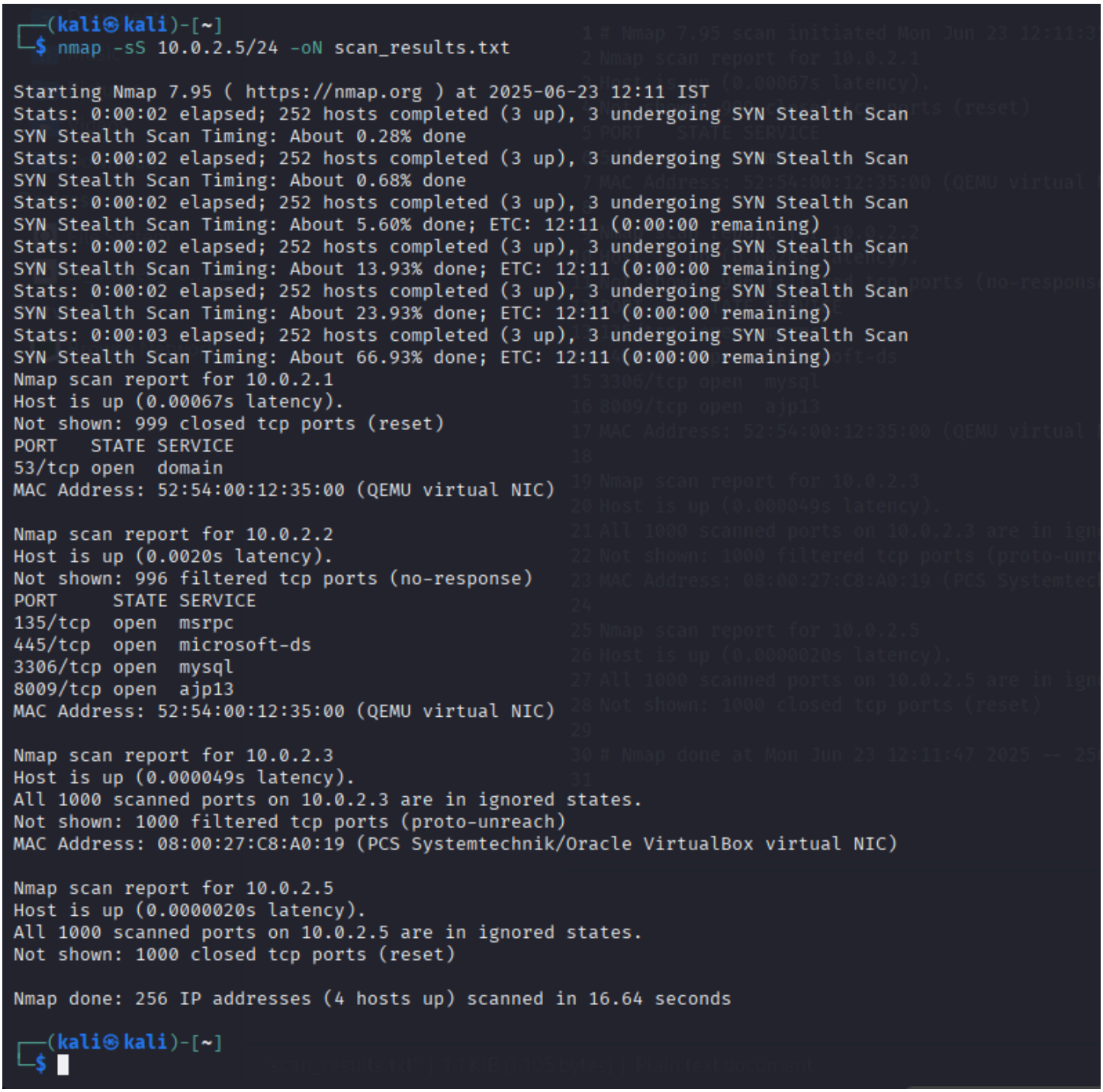
6.Research common services running on those ports.

Port	Service	Purpose
135/tcp	MSRPC	Enables communication between Windows applications and services over a network
445/tcp	Microsoft-DS (SMB)	Supports file sharing, printer sharing, and network resource access on Windows systems
3306/tcp	MySQL	Handles connections to MySQL databases for querying, updating, and managing data
53/tcp	DNS (TCP)	Resolves domain names to IP addresses and supports DNS zone transfers and large queries

7.Identify potential security risks from open ports.

Port	Service	Potential Security Risks
135/tcp	MSRPC	- Target of Windows vulnerabilities and exploits- Can be used for remote code execution or lateral movement
445/tcp	Microsoft-DS (SMB)	- Common in ransomware attacks (e.g., WannaCry)- Allows unauthorized file access or code execution
3306/tcp	MySQL	- Exposes database to brute-force or injection attacks- May leak sensitive data if not secured
53/tcp	DNS (TCP)	- Can be abused for DNS tunneling and data exfiltration- Vulnerable to spoofing or cache poisoning if misconfigured

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



Here this result is saved as scan_results.txt file.