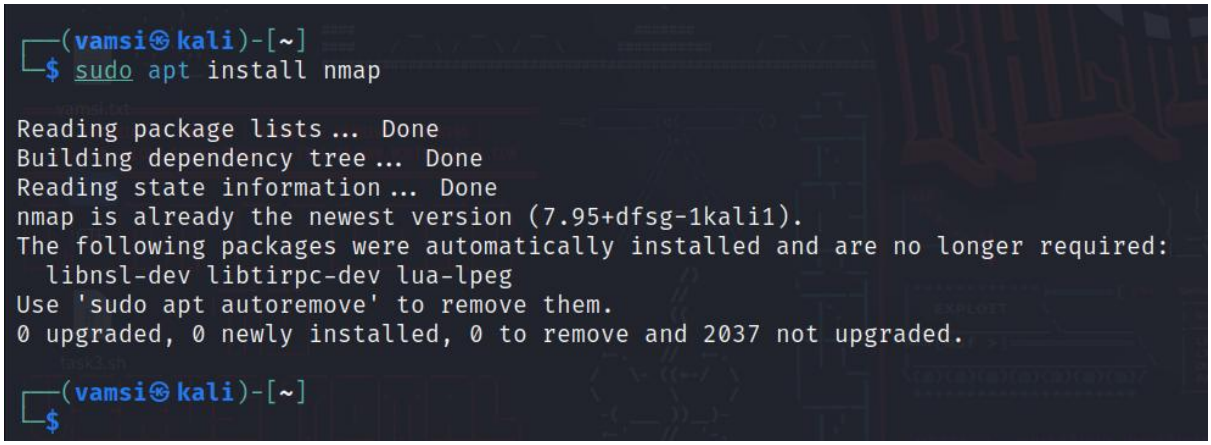
ELEVATE LABS CYBER SECURITY INTERNSHIP

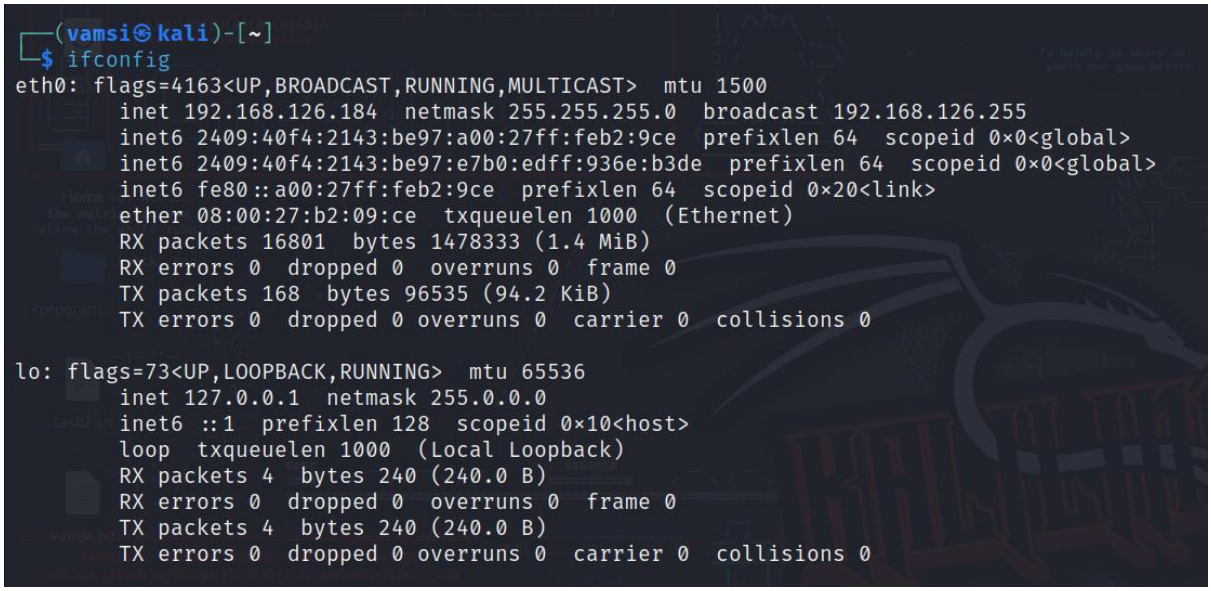
1) Install Nmap from official website.



This command is used to install nmap.

This command is used to check the version of nmap.

2) Find your local IP range (e.g., 192.168.1.0/24).



Ifconfig command is used to find the ip address.

```
┌──(vamsi㉿kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b2:09:ce brd ff:ff:ff:ff:ff:ff
    inet 192.168.126.184/24 brd 192.168.126.255 scope global dynamic noprefixroute eth0
       valid_lft 3248sec preferred_lft 3248sec
    inet6 2409:40f4:2143:be97:e7b0:edff:936e:b3de/64 scope global temporary dynamic
       valid_lft 6852sec preferred_lft 6852sec
    inet6 2409:40f4:2143:be97:a00:27ff:feb2:9ce/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 6852sec preferred_lft 6852sec
    inet6 fe80::a00:27ff:feb2:9ce/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(vamsi㉿kali)-[~]
```

Here,we can see the subnet range.

```
┌──(vamsi㉿kali)-[~]
└─$ sudo nmap -sn 192.168.126.184/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 21:10 IST
Nmap scan report for 192.168.126.55
Host is up (0.00077s latency).
MAC Address: 14:D4:24:32:FC:FD (AzureWave Technology)
Nmap scan report for 192.168.126.62
Host is up (0.011s latency).
MAC Address: CE:2E:2B:18:2F:D5 (Unknown)
Nmap scan report for 192.168.126.184
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.66 seconds

┌──(vamsi㉿kali)-[~]
└─$
```

```
┌──(vamsi㉿kali)-[~]
└─$ ipcalc 192.168.126.184/24
Address:   192.168.126.184      11000000.10101000.01111110. 10111000
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
⇒
Network:   192.168.126.0/24     11000000.10101000.01111110. 00000000
HostMin:   192.168.126.1        11000000.10101000.01111110. 00000001
HostMax:   192.168.126.254      11000000.10101000.01111110. 11111110
Broadcast: 192.168.126.255      11000000.10101000.01111110. 11111111
Hosts/Net: 254                   Class C, Private Internet

┌──(vamsi㉿kali)-[~]
```

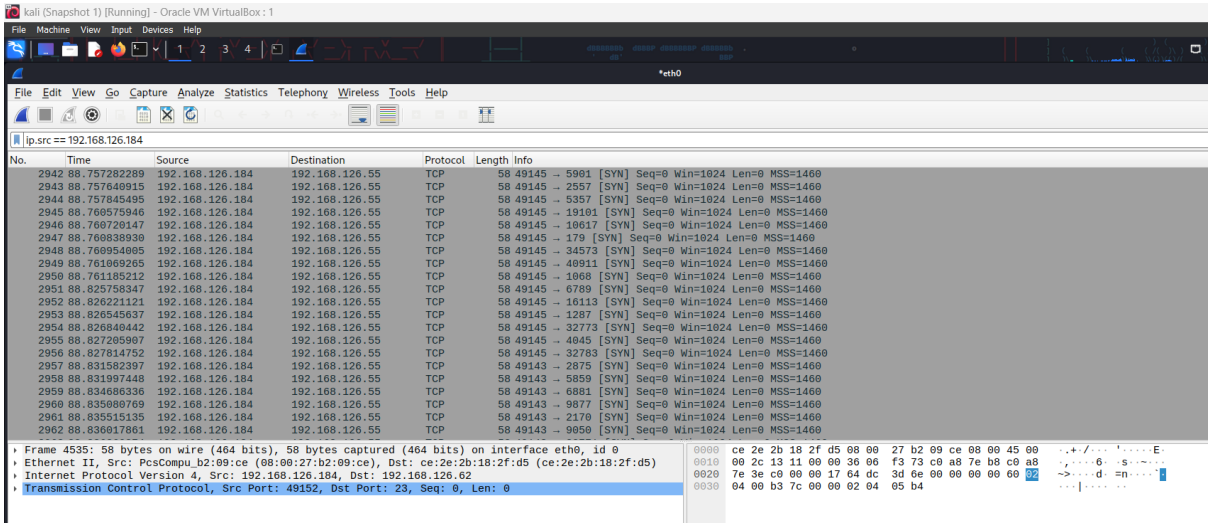
3)Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.

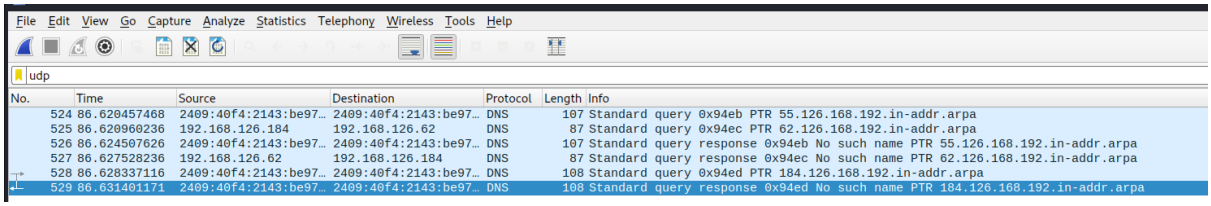
```
┌──(vamsi㉿kali)-[~]
└─$ nmap -sS 192.168.126.184/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 21:11 IST
Nmap scan report for 192.168.126.55
Host is up (0.0029s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
6646/tcp open  unknown
MAC Address: 14:D4:24:32:FC:FD (AzureWave Technology)

Nmap scan report for 192.168.126.62
Host is up (0.014s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: CE:2E:2B:18:2F:D5 (Unknown)

Nmap scan report for 192.168.126.184
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.126.184 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 87.65 seconds

┌──(vamsi㉿kali)-[~]
└─$
```

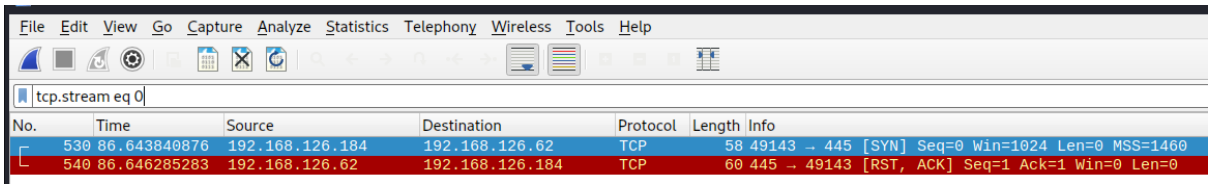
4) Note down IP addresses and open ports found.

6646 is the open port for ip address 192.168.126.55 and 53 (DNS)is the open port for 192.168.126.62.

5) Optiona ly analyze packet capture with Wireshark.







Here, I captured the live traffic using wireshark.

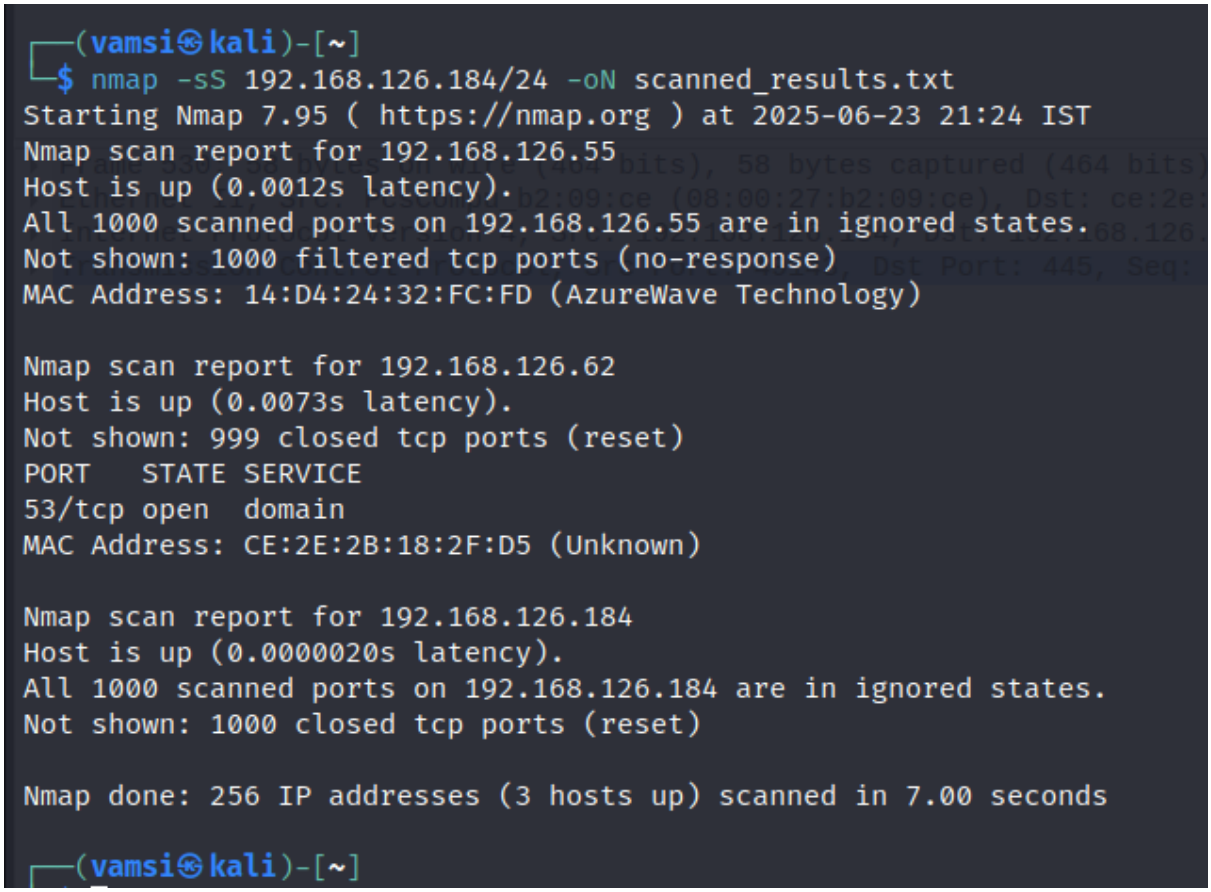
6) Research common services running on those ports.

IP Address	Open Port	Service Name	Description
192.168.126.55	6646	unknown	Port 6646 is not commonly used; could be a custom application or service.
192.168.126.62	53	domain	DNS (Domain Name System) – used for translating domain names to IP addresses.

7) .Identify potential security risks from open ports.

IP Address	Open Port	Service	Potential Risks
192.168.126.55	6646/tcp	Unknown	Unknown service – could be vulnerable or unnecessary; risk of exploitation.
192.168.126.62	53/tcp	DNS	DNS can be abused for DNS poisoning, DDoS amplification, or internal info leaks.

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



Here this result is saved as scanned_results.txt.