

# ELEVATE LABS CYBER SECURITY INTERNSHIP

1) Install Nmap from official website.

```
(vamsi@kali)-[~]  
$ sudo apt install nmap  
  
Reading package lists ... Done  
Building dependency tree ... Done  
Reading state information ... Done  
nmap is already the newest version (7.95+dfsg-1kali1).  
The following packages were automatically installed and are no longer required:  
  libnsl-dev libtirpc-dev lua-lpeg  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 2037 not upgraded.  
  
(vamsi@kali)-[~]  
$
```

This command is used to install nmap.

```
(vamsi@kali)-[~]  
$ nmap --version  
  
Nmap version 7.95 ( https://nmap.org )  
Platform: x86_64-pc-linux-gnu  
Compiled with: liblua-5.4.7 openssl-3.3.2 libssh2-1.11.1 libz-1.3.1 libpcap-1.10.5 nmap-libdnet-1.12 ipv6  
Compiled without:  
Available nsock engines: epoll poll select  
  
(vamsi@kali)-[~]  
$
```

This command is used to check the version of nmap.

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

```
(vamsi@kali)-[~]  
$ ifconfig  
  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.126.184 netmask 255.255.255.0 broadcast 192.168.126.255  
    inet6 2409:40f4:2143:be97:a00:27ff:feb2:9ce prefixlen 64 scopeid 0x0<global>  
    inet6 2409:40f4:2143:be97:e7b0:edff:936e:b3de prefixlen 64 scopeid 0x0<global>  
    inet6 fe80::a00:27ff:feb2:9ce prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:b2:09:ce txqueuelen 1000 (Ethernet)  
    RX packets 16801 bytes 1478333 (1.4 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 168 bytes 96535 (94.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```

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)-[~]
$ 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

```

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.

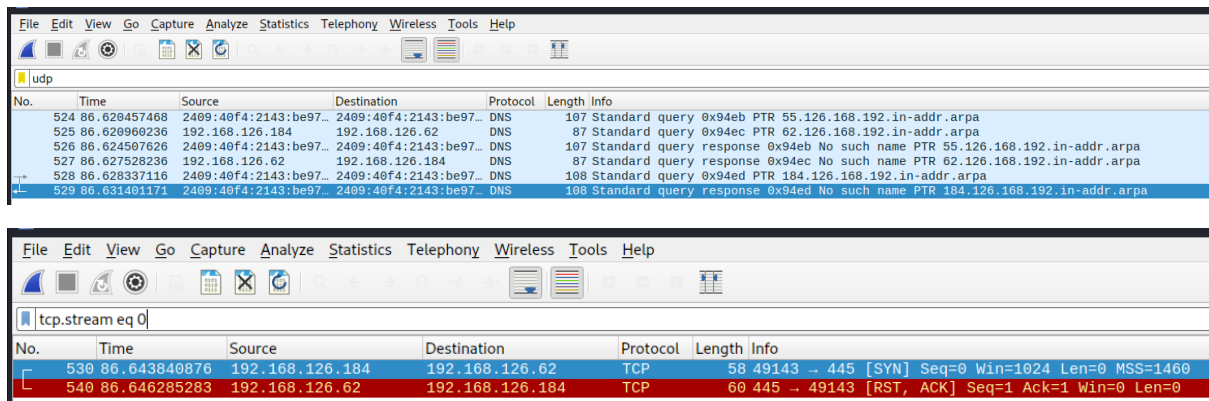
6646 is the open port for ip address 192.168.126.55 and 53 (DNS) is the open port for 192.168.126.62.

5) Optionaly analyze packet capture with Wireshark.

The screenshot shows a Wireshark packet capture on interface eth0. The packet list on the left shows multiple TCP SYN packets from 192.168.126.184 to 192.168.126.55. The packet details pane on the right shows the structure of a selected packet (Frame 4535), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol fields.

No.	Time	Source	Destination	Protocol	Length	Info
2942	88.757282289	192.168.126.184	192.168.126.55	TCP	58	49145 → 5981 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2943	88.757440915	192.168.126.184	192.168.126.55	TCP	58	49145 → 2557 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2944	88.757845495	192.168.126.184	192.168.126.55	TCP	58	49145 → 5357 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2945	88.760575946	192.168.126.184	192.168.126.55	TCP	58	49145 → 19101 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2946	88.760720147	192.168.126.184	192.168.126.55	TCP	58	49145 → 10617 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2947	88.760830930	192.168.126.184	192.168.126.55	TCP	58	49145 → 179 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2948	88.760954095	192.168.126.184	192.168.126.55	TCP	58	49145 → 34573 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2949	88.761069265	192.168.126.184	192.168.126.55	TCP	58	49145 → 40911 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2950	88.761185212	192.168.126.184	192.168.126.55	TCP	58	49145 → 1068 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2951	88.825750347	192.168.126.184	192.168.126.55	TCP	58	49145 → 6789 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2952	88.826221121	192.168.126.184	192.168.126.55	TCP	58	49145 → 16113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2953	88.826545637	192.168.126.184	192.168.126.55	TCP	58	49145 → 1287 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2954	88.826840442	192.168.126.184	192.168.126.55	TCP	58	49145 → 32773 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2955	88.827205907	192.168.126.184	192.168.126.55	TCP	58	49145 → 4045 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2956	88.827814752	192.168.126.184	192.168.126.55	TCP	58	49145 → 32783 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2957	88.831582397	192.168.126.184	192.168.126.55	TCP	58	49143 → 2875 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2958	88.831997448	192.168.126.184	192.168.126.55	TCP	58	49143 → 5859 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2959	88.834686336	192.168.126.184	192.168.126.55	TCP	58	49143 → 6881 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2960	88.835080769	192.168.126.184	192.168.126.55	TCP	58	49143 → 9877 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2961	88.835515135	192.168.126.184	192.168.126.55	TCP	58	49143 → 2170 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2962	88.836017061	192.168.126.184	192.168.126.55	TCP	58	49143 → 9850 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 4535: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0  
 Ethernet II, Src: PcsCompu, b2:09:ce (00:00:27:b2:09:ce), Dst: ce:2e:2b:18:2f:d5 (ce:2e:2b:18:2f:d5)  
 Internet Protocol Version 4, Src: 192.168.126.184, Dst: 192.168.126.62  
 Transmission Control Protocol, Src Port: 49152, Seq: 0, Len: 0



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

```
(vamsi@kali)-[~]  
$ nmap -sS 192.168.126.184/24 -oN scanned_results.txt  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 21:24 IST  
Nmap scan report for 192.168.126.55  
Host is up (0.0012s latency).  
All 1000 scanned ports on 192.168.126.55 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 14:D4:24:32:FC:FD (AzureWave Technology)  
  
Nmap scan report for 192.168.126.62  
Host is up (0.0073s 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 7.00 seconds  
  
(vamsi@kali)-[~]
```

Here this result is saved as scanned\_results.txt.