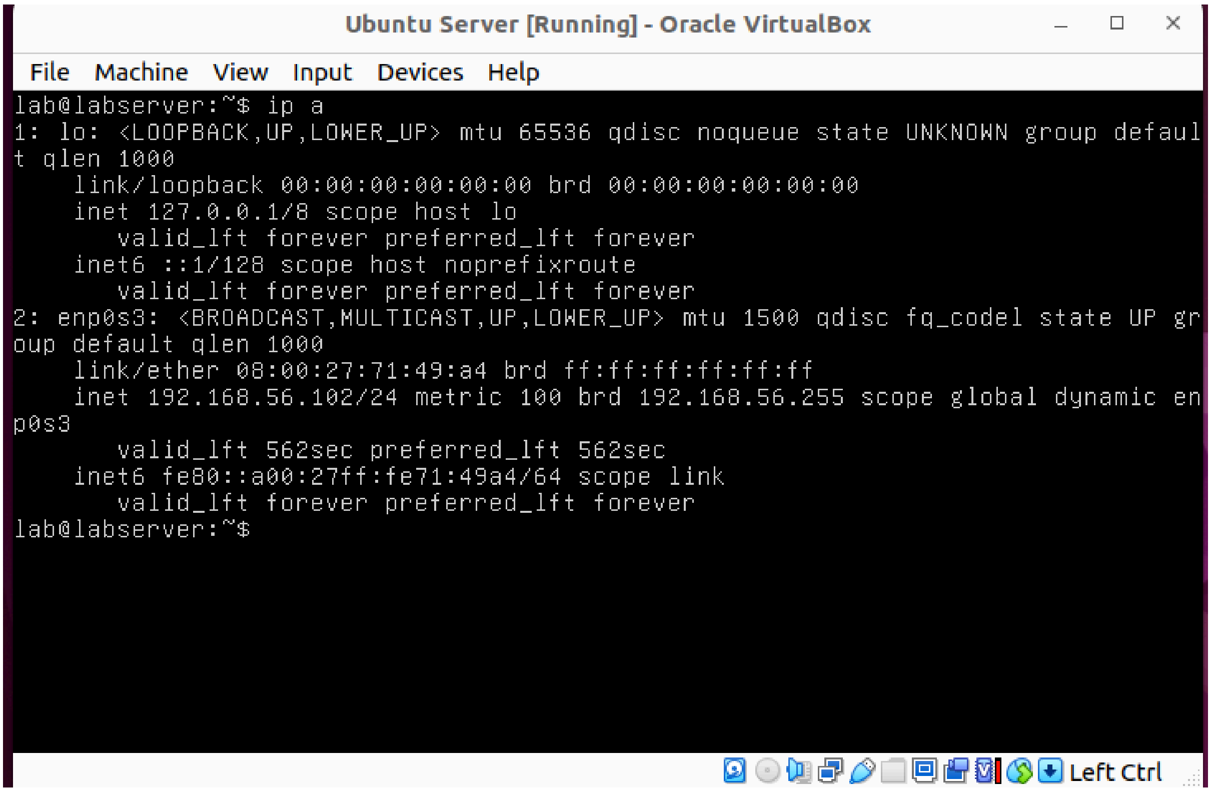
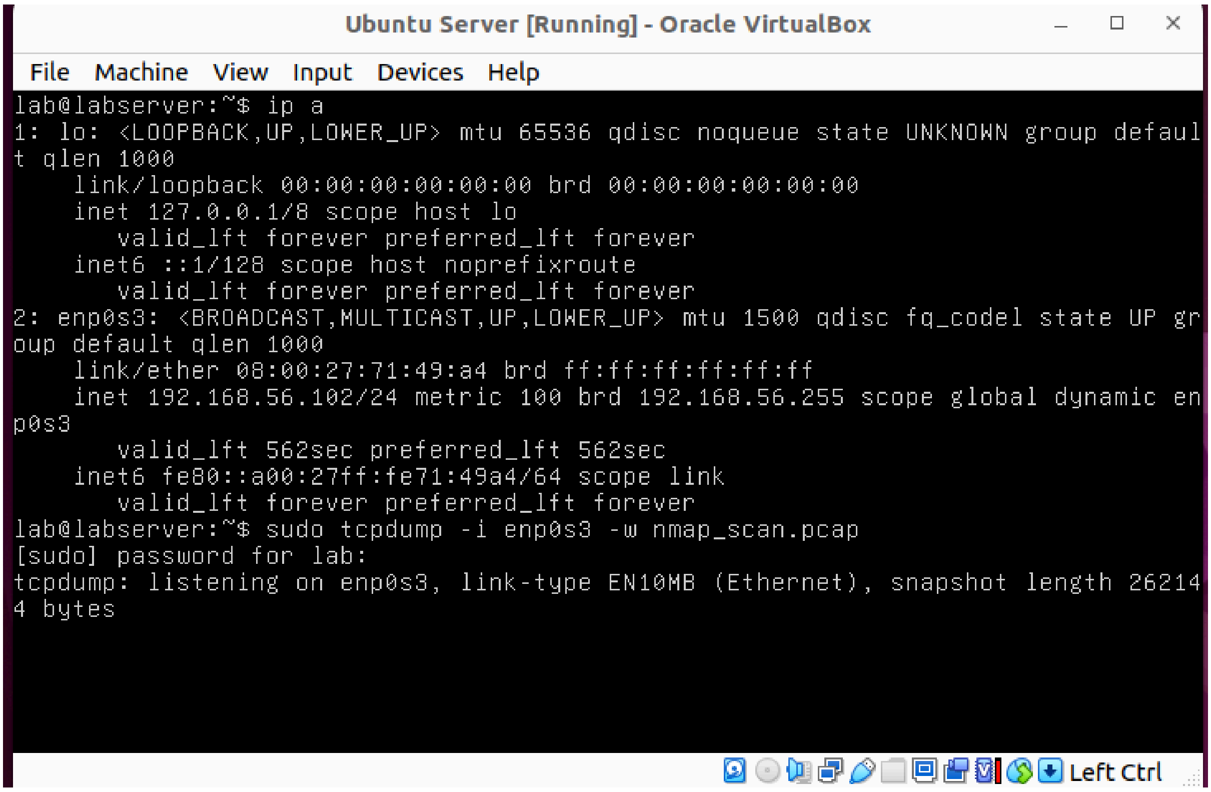
Recom & Traffic Analysis


Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Left Ctrl

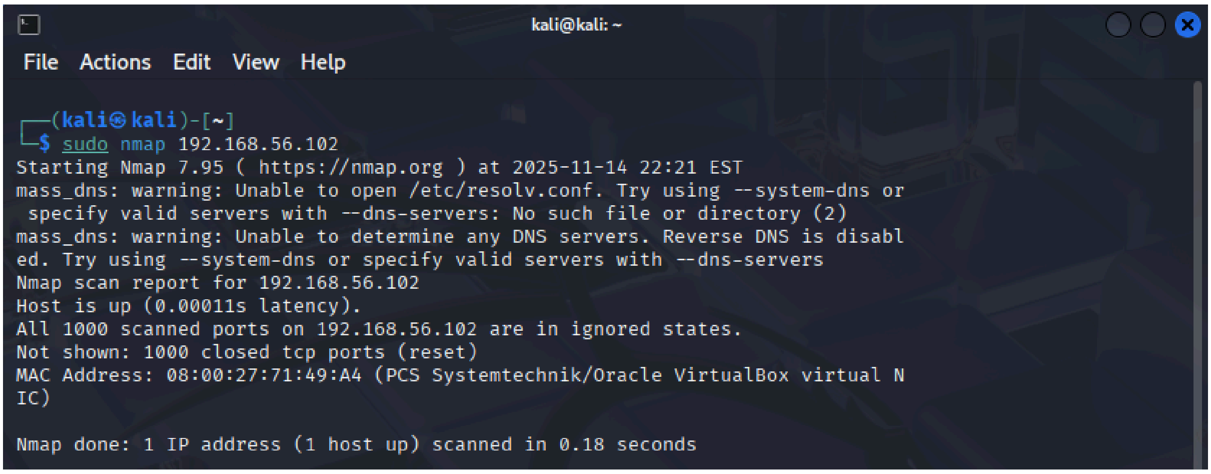
```
lab@labserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:71:49:a4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 metric 100 brd 192.168.56.255 scope global dynamic en
p0s3
       valid_lft 562sec preferred_lft 562sec
    inet6 fe80::a00:27ff:fe71:49a4/64 scope link
       valid_lft forever preferred_lft forever
lab@labserver:~$
```

Since I found the interface, which is enp0s3, I started tcpdump.

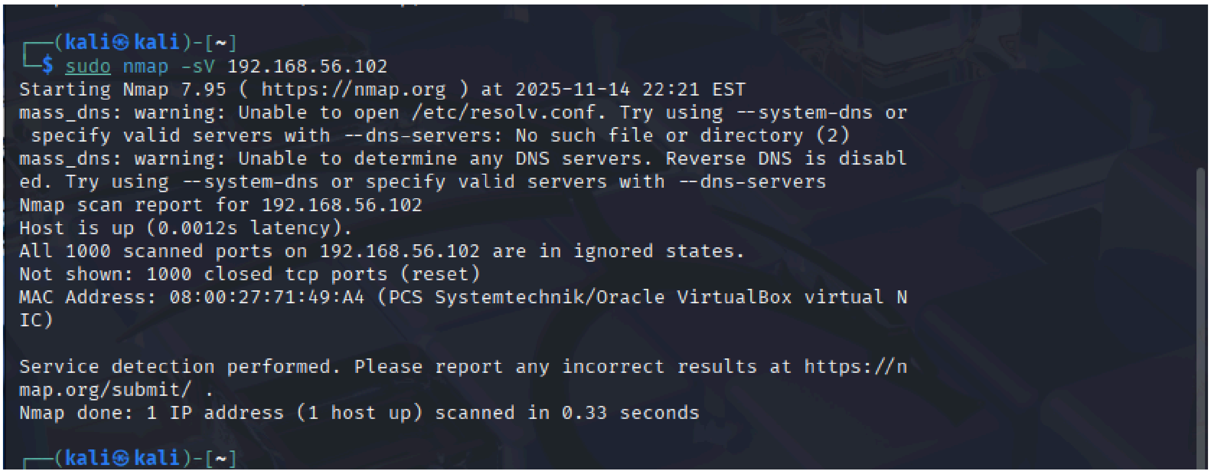

Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Left Ctrl

```
lab@labserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:71:49:a4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 metric 100 brd 192.168.56.255 scope global dynamic en
p0s3
       valid_lft 562sec preferred_lft 562sec
    inet6 fe80::a00:27ff:fe71:49a4/64 scope link
       valid_lft forever preferred_lft forever
lab@labserver:~$ sudo tcpdump -i enp0s3 -w nmap_scan.pcap
[sudo] password for lab:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 26214
4 bytes
```

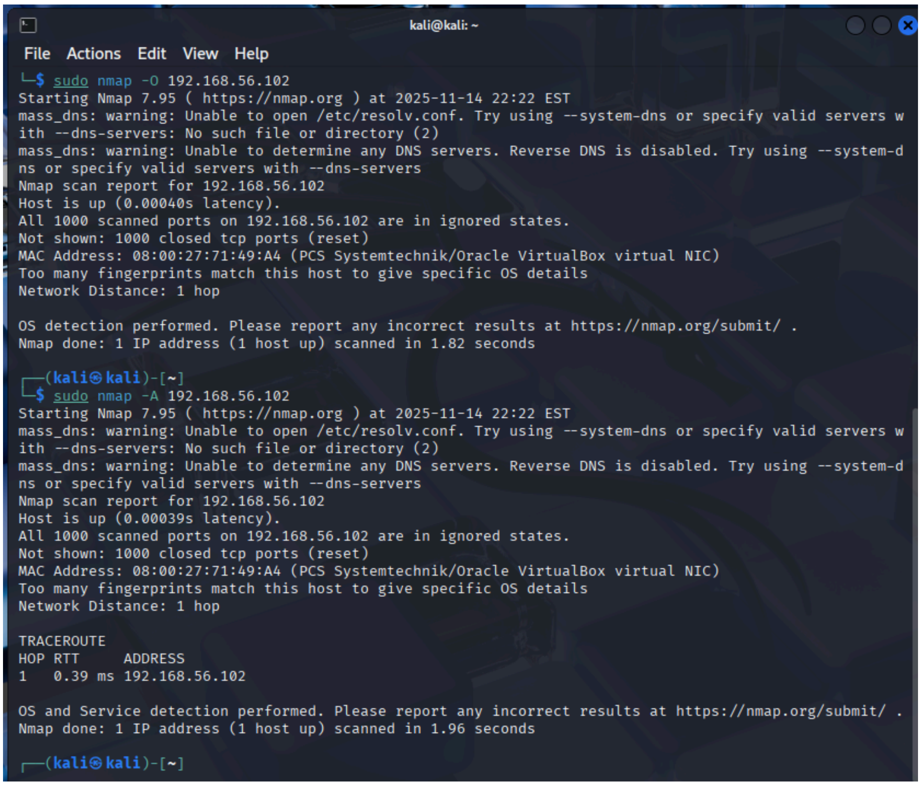
From Kali, I ran nmap scans, which are basic scan, version detection, os detection, and full aggressive scan.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 22:21 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
 specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:71:49:A4 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

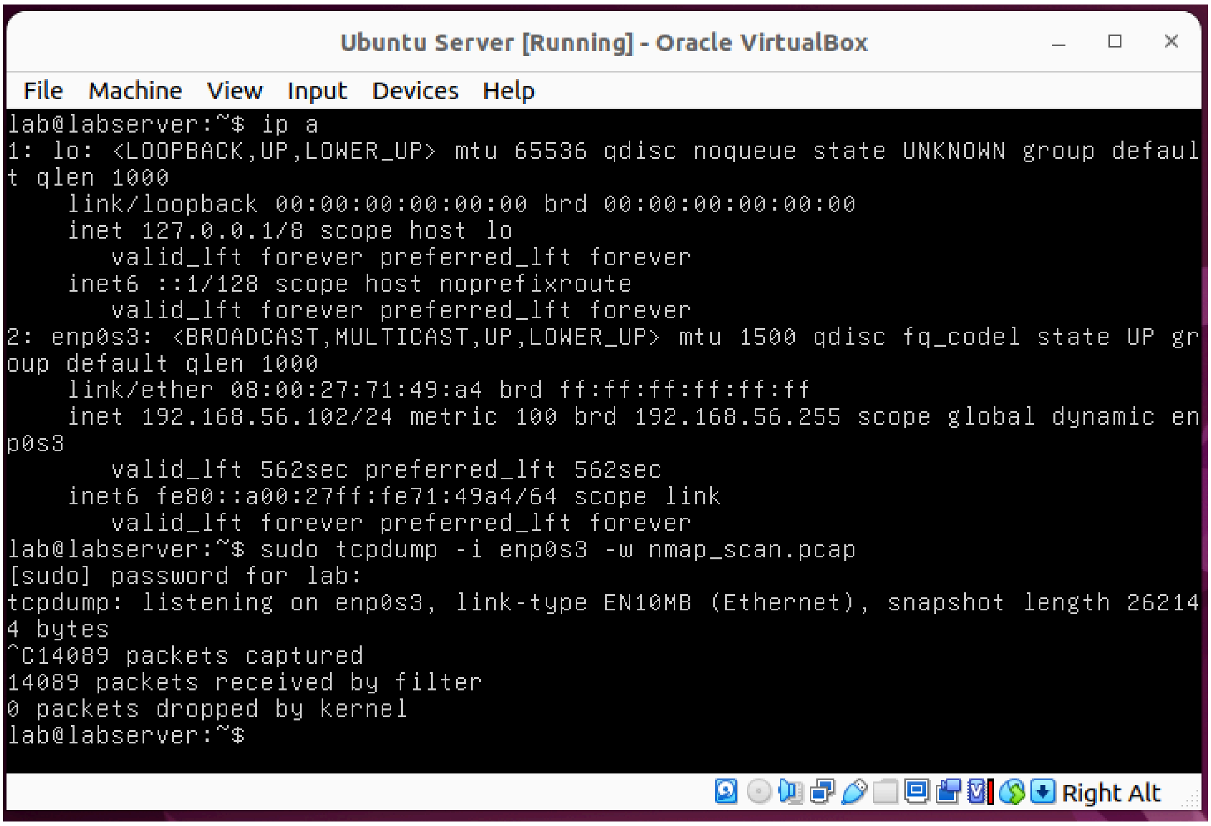


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 22:21 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
 specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:71:49:A4 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

┌──(kali㉿kali)-[~]
```



```
└─$ sudo nmap -O 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 22:22 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers w
ith --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-d
ns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00040s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:71:49:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 22:22 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers w
ith --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-d
ns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00039s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:71:49:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.39 ms 192.168.56.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.96 seconds

┌──(kali㉿kali)-[~]
```

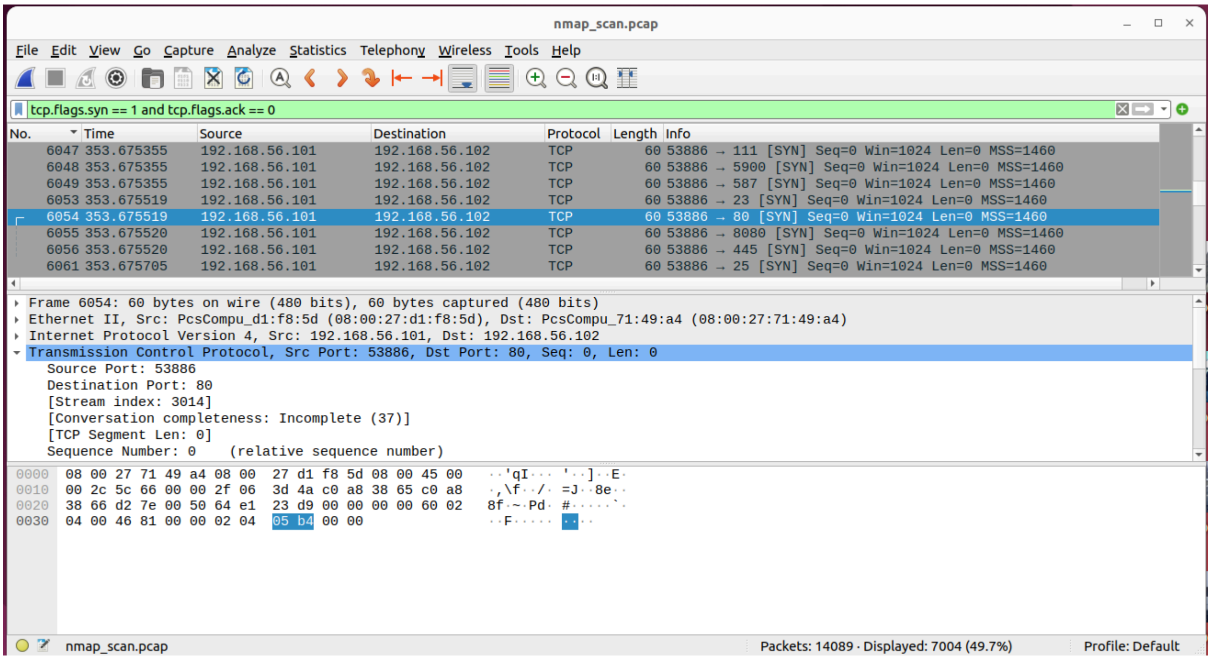
The ubuntu server successfully captured 14089 packets.



Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Alt

```
lab@labserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:71:49:a4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 metric 100 brd 192.168.56.255 scope global dynamic en
p0s3
       valid_lft 562sec preferred_lft 562sec
    inet6 fe80::a00:27ff:fe71:49a4/64 scope link
       valid_lft forever preferred_lft forever
lab@labserver:~$ sudo tcpdump -i enp0s3 -w nmap_scan.pcap
[sudo] password for lab:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 26214
4 bytes
^C14089 packets captured
14089 packets received by filter
0 packets dropped by kernel
lab@labserver:~$
```

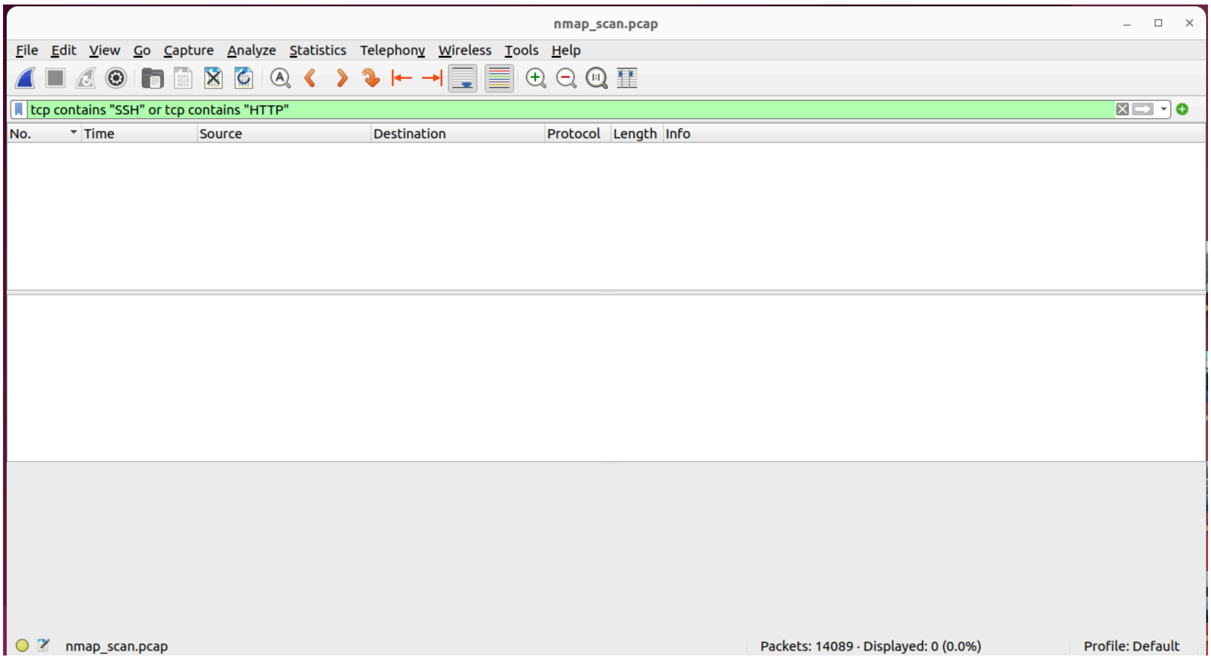
Then, I analyzed the nmap_scan.pcap file with wireshark.



nmap_scan.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.syn == 1 and tcp.flags.ack == 0

No.     Time        Source          Destination     Protocol Length Info
   6047 353.675355  192.168.56.101  192.168.56.102  TCP         60 53886 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   6048 353.675355  192.168.56.101  192.168.56.102  TCP         60 53886 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   6049 353.675355  192.168.56.101  192.168.56.102  TCP         60 53886 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   6053 353.675519  192.168.56.101  192.168.56.102  TCP         60 53886 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   6054 353.675519  192.168.56.101  192.168.56.102  TCP         60 53886 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   6055 353.675520  192.168.56.101  192.168.56.102  TCP         60 53886 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   6056 353.675520  192.168.56.101  192.168.56.102  TCP         60 53886 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   6061 353.675705  192.168.56.101  192.168.56.102  TCP         60 53886 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

 Frame 6054: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
 Ethernet II, Src: PcsCompu_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PcsCompu_71:49:a4 (08:00:27:71:49:a4)
 Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
 Transmission Control Protocol, Src Port: 53886, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 53886
    Destination Port: 80
    [Stream index: 3014]
    [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)

0000  08 00 27 71 49 a4 08 00  27 d1 f8 5d 08 00 45 00   ··'qI···  '··]··E·
0010  00 2c 5c 66 00 00 2f 06  3d 4a c0 a8 38 65 c0 a8   ·,\f··/·  =J··8e··
0020  38 66 d2 7e 00 50 64 e1  23 d9 00 00 00 00 60 02   8f·~·Pd·  #·····`·
0030  04 00 46 81 00 00 02 04  05 b4 00 00               ··F·····  ····

nmap_scan.pcap                Packets: 14089 · Displayed: 7004 (49.7%)      Profile: Default
```

I filtered SYN-only, so I could see the attacker’s half of the handshake attempt. It showed a SYN packet that initiated the first connection.

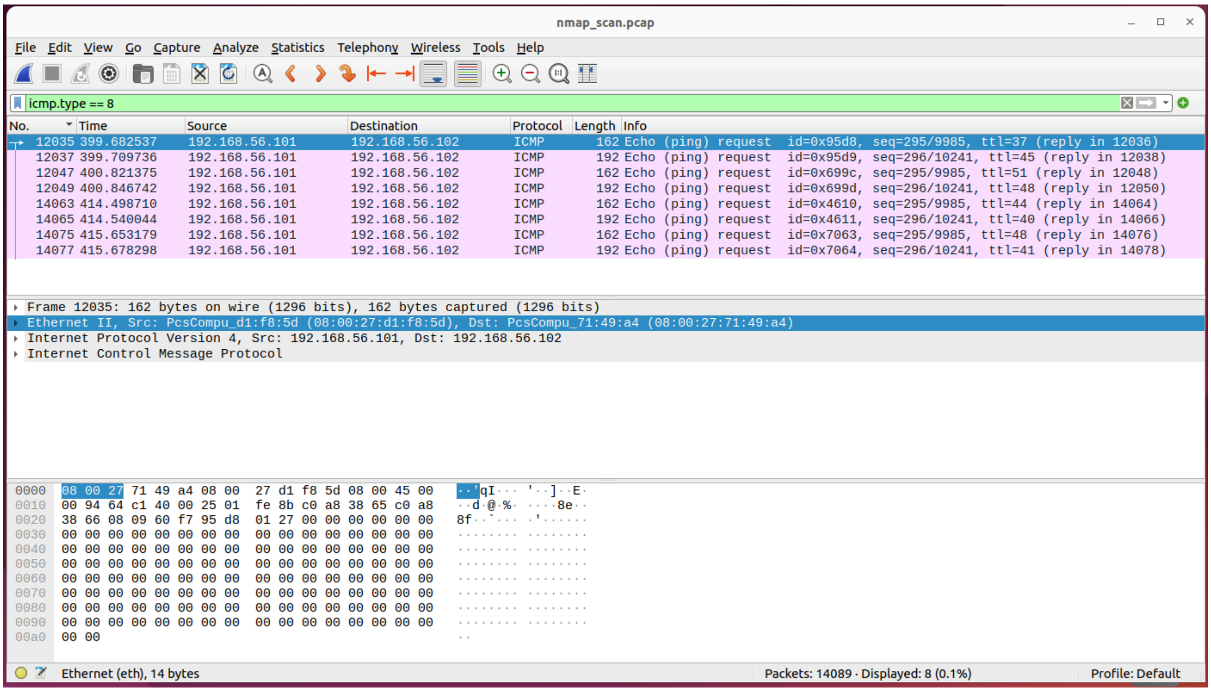

nmap_scan.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp contains "SSH" or tcp contains "HTTP"
```

```
No.      Time       Source       Destination       Protocol  Length  Info
```

```
nmap_scan.pcap                                   Packets: 14089 · Displayed: 0 (0.0%)      Profile: Default
```

I checked port 22 and 80 because Nmap aggressive scans tried to send probes containing HTTP/SSH signatures. But, since there were no services running, and port 22 and 80 were closed, there was nothing on the result.


nmap_scan.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
icmp.type == 8
```

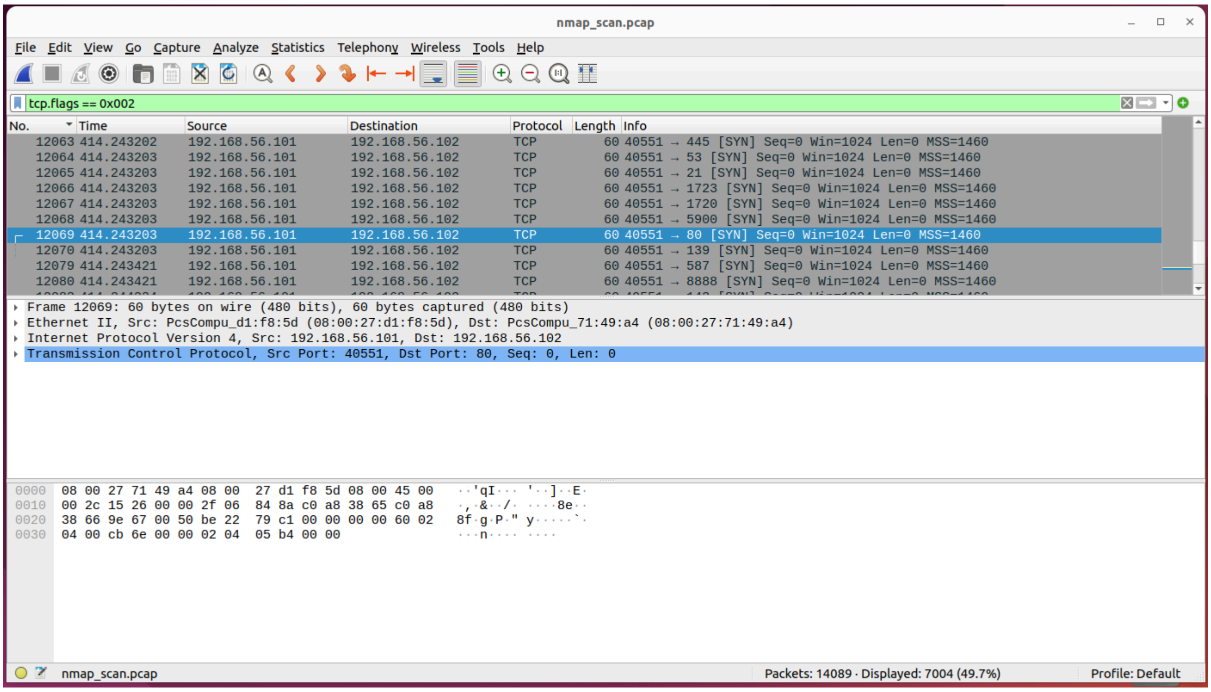
```
No.     Time        Source          Destination     Protocol  Length Info
12035 399.682537    192.168.56.101  192.168.56.102  ICMP      162 Echo (ping) request  id=0x95d8, seq=295/9985, ttl=37 (reply in 12036)
12037 399.709736    192.168.56.101  192.168.56.102  ICMP      192 Echo (ping) request  id=0x95d9, seq=296/10241, ttl=45 (reply in 12038)
12047 400.821375    192.168.56.101  192.168.56.102  ICMP      162 Echo (ping) request  id=0x699c, seq=295/9985, ttl=51 (reply in 12048)
12049 400.846742    192.168.56.101  192.168.56.102  ICMP      192 Echo (ping) request  id=0x699d, seq=296/10241, ttl=48 (reply in 12050)
14063 414.498710    192.168.56.101  192.168.56.102  ICMP      162 Echo (ping) request  id=0x4610, seq=295/9985, ttl=44 (reply in 14064)
14065 414.540044    192.168.56.101  192.168.56.102  ICMP      192 Echo (ping) request  id=0x4611, seq=296/10241, ttl=40 (reply in 14066)
14075 415.653179    192.168.56.101  192.168.56.102  ICMP      162 Echo (ping) request  id=0x7063, seq=295/9985, ttl=48 (reply in 14076)
14077 415.678298    192.168.56.101  192.168.56.102  ICMP      192 Echo (ping) request  id=0x7064, seq=296/10241, ttl=41 (reply in 14078)
```

```
› Frame 12035: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
› Ethernet II, Src: PcsCompu_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PcsCompu_71:49:a4 (08:00:27:71:49:a4)
› Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
› Internet Control Message Protocol
```

```
0000  08 00 27 71 49 a4 08 00  27 d1 f8 5d 08 00 45 00   ··'qI···  '··]··E·
0010  00 94 64 c1 40 00 25 01  fe 8b c0 a8 38 65 c0 a8   ··d·@·%·  ····8e··
0020  38 66 08 09 60 f7 95 d8  01 27 00 00 00 00 00 00   8f··`···  ·'······
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
00a0  00 00                                              ··
```

```
Ethernet (eth), 14 bytes                         Packets: 14089 · Displayed: 8 (0.1%)      Profile: Default
```

icmp.type == 8 shows Nmap host-discovery pings, especially ICMP Echo Requests. Nmap always checks whether host is up using ICMP or ARP, so in here, the filter showed the ping request from 192.168.56.101 to 192.168.56.102, and the 192.168.56.102 replied with ICMP Echo Replies, meaning the target responded to the ping.


nmap_scan.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags == 0x002
```

```
No.     Time        Source          Destination     Protocol Length Info
  12063 414.243202  192.168.56.101  192.168.56.102  TCP        60 40551 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  12064 414.243203  192.168.56.101  192.168.56.102  TCP        60 40551 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  12065 414.243203  192.168.56.101  192.168.56.102  TCP        60 40551 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  12066 414.243203  192.168.56.101  192.168.56.102  TCP        60 40551 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  12067 414.243203  192.168.56.101  192.168.56.102  TCP        60 40551 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  12068 414.243203  192.168.56.101  192.168.56.102  TCP        60 40551 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  12069 414.243203  192.168.56.101  192.168.56.102  TCP        60 40551 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  12070 414.243203  192.168.56.101  192.168.56.102  TCP        60 40551 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  12079 414.243421  192.168.56.101  192.168.56.102  TCP        60 40551 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  12080 414.243421  192.168.56.101  192.168.56.102  TCP        60 40551 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
› Frame 12069: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
› Ethernet II, Src: PcsCompu_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PcsCompu_71:49:a4 (08:00:27:71:49:a4)
› Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102
› Transmission Control Protocol, Src Port: 40551, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  08 00 27 71 49 a4 08 00  27 d1 f8 5d 08 00 45 00   ··'qI··· '··]··E·
0010  00 2c 15 26 00 00 2f 06  84 8a c0 a8 38 65 c0 a8   ·,·&··/· ····8e··
0020  38 66 9e 67 00 50 be 22  79 c1 00 00 00 00 60 02   8f·g·P·" y·····`·
0030  04 00 cb 6e 00 00 02 04  05 b4 00 00               ···n···· ····
```

nmap_scan.pcap   Packets: 14089 · Displayed: 7004 (49.7%)   Profile: Default

Lastly, this showed all TCP SYN packets, which represented the very first step of the TCP handshake. By putting tcp.flags == 0x002, the result showed the packet that had only one SYN flag.

Readme.