Experiment No. – 8				
Date of Performance:				
Date of Submission:				
Program Execution/ formation/ correction/ ethical practices (06)	Timely Submission (01)	Viva (03)	Experiment Total (10)	Sign with Date

Experiment No. 8
IDS and firewalls

8.1Aim: Study the behaviour of protections such as IDS and firewalls when altering headers in network packets.

8.2 Course Outcome: Identify various web application and Network vulnerability scanning techniques and defence methodologies.

8.3 Learning Objectives: Study of IDS and firewall using Wireshark.

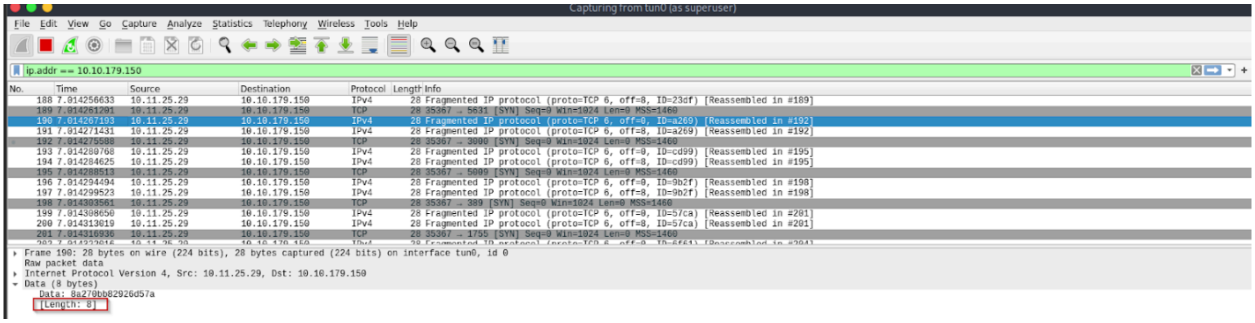
8.4 Requirement: Kali Linux

8.5 Related Theory:

1. By Fragmenting the packets with 8 bit data:

Fragment packets, optionally with given MTU. If the firewall, or the IDS/IPS, does not reassemble the packet, it will most likely let it pass. Consequently, the target system will reassemble and process it.

Command: nmap -sS -Pn -f -F 10.10.179.150


Capturing from tun0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.10.179.150

```
No.   Time          Source        Destination     Protocol Length Info
  188 7.014256633   10.11.25.29   10.10.179.150   IPv4     28 Fragmented IP protocol (proto=TCP 6, off=8, ID=23df) [Reassembled in #189]
  189 7.014261201   10.11.25.29   10.10.179.150   TCP      28 35367 → 5631 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  190 7.014267193   10.11.25.29   10.10.179.150   IPv4     28 Fragmented IP protocol (proto=TCP 6, off=0, ID=a269) [Reassembled in #192]
  191 7.014271431   10.11.25.29   10.10.179.150   IPv4     28 Fragmented IP protocol (proto=TCP 6, off=8, ID=a269) [Reassembled in #192]
  192 7.014275588   10.11.25.29   10.10.179.150   TCP      28 35367 → 3000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  193 7.014280768   10.11.25.29   10.10.179.150   IPv4     28 Fragmented IP protocol (proto=TCP 6, off=0, ID=cd99) [Reassembled in #195]
  194 7.014284625   10.11.25.29   10.10.179.150   IPv4     28 Fragmented IP protocol (proto=TCP 6, off=8, ID=cd99) [Reassembled in #195]
  195 7.014288513   10.11.25.29   10.10.179.150   TCP      28 35367 → 5009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  196 7.014294494   10.11.25.29   10.10.179.150   IPv4     28 Fragmented IP protocol (proto=TCP 6, off=0, ID=9b2f) [Reassembled in #198]
  197 7.014299523   10.11.25.29   10.10.179.150   IPv4     28 Fragmented IP protocol (proto=TCP 6, off=8, ID=9b2f) [Reassembled in #198]
  198 7.014303561   10.11.25.29   10.10.179.150   TCP      28 35367 → 389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  199 7.014308650   10.11.25.29   10.10.179.150   IPv4     28 Fragmented IP protocol (proto=TCP 6, off=0, ID=57ca) [Reassembled in #201]
  200 7.014313019   10.11.25.29   10.10.179.150   IPv4     28 Fragmented IP protocol (proto=TCP 6, off=8, ID=57ca) [Reassembled in #201]
  201 7.014316936   10.11.25.29   10.10.179.150   TCP      28 35367 → 1755 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

▸ Frame 190: 28 bytes on wire (224 bits), 28 bytes captured (224 bits) on interface tun0, id 0
  Raw packet data
▸ Internet Protocol Version 4, Src: 10.11.25.29, Dst: 10.10.179.150
▾ Data (8 bytes)
    Data: 8a270bb82926d57a
    [Length: 8]
```

Figure 8.1 Wireshark to capture packets

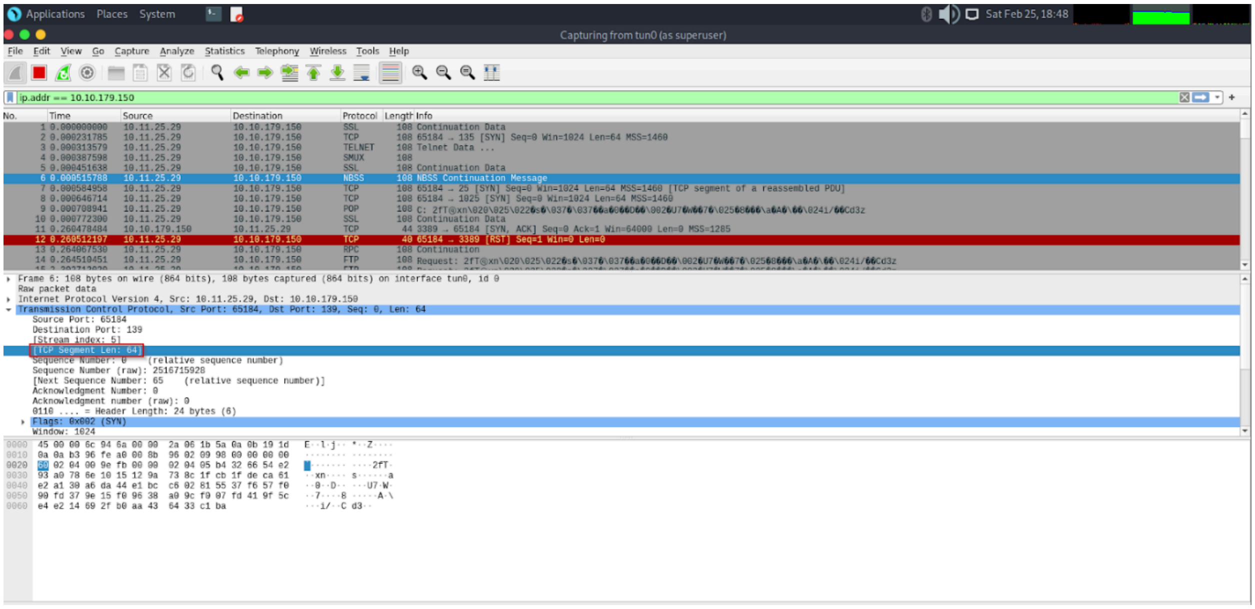
If you want to limit the IP data to 8 bytes, the 24 bytes of the TCP header will be divided across 3 IP packets

2. Generate ip packets with specific length.

In some instances, you might find out that the size of the packets is triggering the firewall or the IDS/IPS to detect and block you. If you ever find yourself in such a situation, you can make your port scanning more evasive by setting a specific length. You can set the length of data carried within the IP packet using --data-length VALUE. Again, remember that the length should be a multiple of 8.

If you run the following Nmap scan nmap -sS -Pn --data-length 64 -F 10.10.179.150, each TCP segment will be padded with random data till its length is 64 bytes. In the screenshot below, we can see that each TCP segment has a length of 64 bytes.

Command:


Applications Places System
Sat Feb 25, 18:48
Capturing from tun0 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.10.179.150

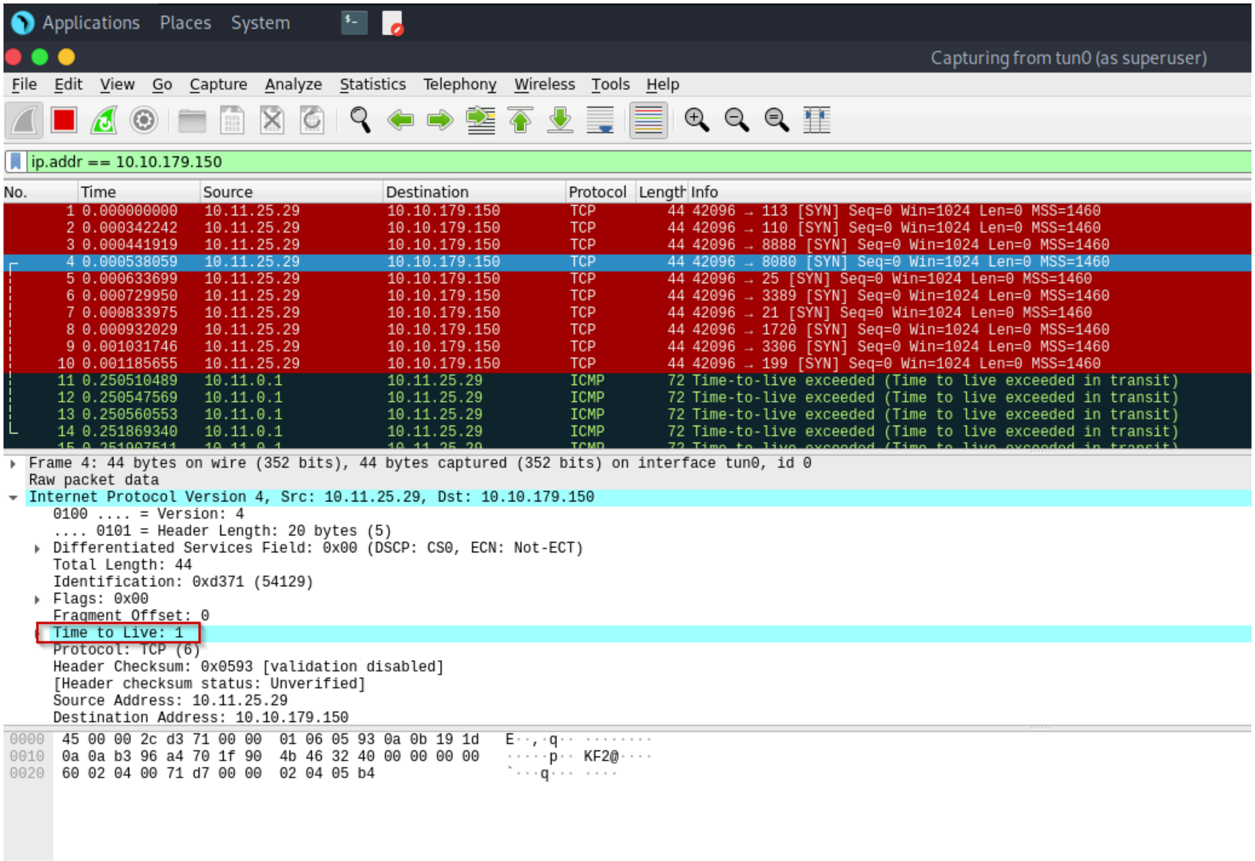
```
No.   Time          Source          Destination     Protocol Length Info
    1 0.000000000   10.11.25.29     10.10.179.150   SSL      108 Continuation Data
    2 0.000231785   10.11.25.29     10.10.179.150   TCP      108 65184 → 135 [SYN] Seq=0 Win=1024 Len=64 MSS=1460
    3 0.000313579   10.11.25.29     10.10.179.150   TELNET   108 Telnet Data ...
    4 0.000387598   10.11.25.29     10.10.179.150   SMUX     108
    5 0.000451638   10.11.25.29     10.10.179.150   SSL      108 Continuation Data
    6 0.000515788   10.11.25.29     10.10.179.150   NBSS     108 NBSS Continuation Message
    7 0.000584958   10.11.25.29     10.10.179.150   TCP      108 65184 → 25 [SYN] Seq=0 Win=1024 Len=64 MSS=1460 [TCP segment of a reassembled PDU]
    8 0.000646714   10.11.25.29     10.10.179.150   TCP      108 65184 → 1025 [SYN] Seq=0 Win=1024 Len=64 MSS=1460
    9 0.000708941   10.11.25.29     10.10.179.150   POP      108 C: 2fT@xn\020\025\022�s�\037�\037��a�0��D��\002�U7�W��7�\025�8���\a�A�\��\024i/��Cd3z
   10 0.000772300   10.11.25.29     10.10.179.150   SSL      108 Continuation Data
   11 0.260478484   10.10.179.150   10.11.25.29     TCP       44 3389 → 65184 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1285
   12 0.260512197   10.11.25.29     10.10.179.150   TCP       40 65184 → 3389 [RST] Seq=1 Win=0 Len=0
   13 0.264067530   10.11.25.29     10.10.179.150   RPC      108 Continuation
   14 0.264510451   10.11.25.29     10.10.179.150   FTP      108 Request: 2fT@xn\020\025\022�s�\037�\037��a�0��D��\002�U7�W��7�\025�8���\a�A�\��\024i/��Cd3z

▸ Frame 6: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface tun0, id 0
  Raw packet data
▸ Internet Protocol Version 4, Src: 10.11.25.29, Dst: 10.10.179.150
▾ Transmission Control Protocol, Src Port: 65184, Dst Port: 139, Seq: 0, Len: 64
    Source Port: 65184
    Destination Port: 139
    [Stream index: 5]
    [TCP Segment Len: 64]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2516715928
    [Next Sequence Number: 65    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0110 .... = Header Length: 24 bytes (6)
  ▸ Flags: 0x002 (SYN)
    Window: 1024

0000  45 00 00 6c 94 6a 00 00  2a 06 1b 5a 0a 0b 19 1d   E··l·j·· *··Z····
0010  0a 0a b3 96 fe a0 00 8b  96 02 09 98 00 00 00 00   ········ ········
0020  60 02 04 00 9e fb 00 00  02 04 05 b4 32 66 54 e2   `······· ····2fT·
0030  93 a0 78 6e 10 15 12 9a  73 8c 1f cb 1f de ca 61   ··xn···· s······a
0040  e2 a1 30 a6 da 44 e1 bc  c6 02 81 55 37 f6 57 f0   ··0··D·· ···U7·W·
0050  90 fd 37 9e 15 f0 96 38  a0 9c f0 07 fd 41 9f 5c   ··7····8 ·····A·\
0060  e4 e2 14 69 2f b0 aa 43  64 33 c1 ba               ···i/··C d3··
```

Figure 8.2 Wireshark to generate ip packets with specific length

By manipulating TTL value

Nmap gives you further control over the different fields in the IP header. One of the fields you can control is the Time-to-Live (TTL). Nmap options include --ttl VALUE to set the TTL to a custom value. This option might be useful if you think the default TTL exposes your port scan activities.

Command: nmap -sS -Pn --ttl 81 -F 10.10.179.150.



ip.addr == 10.10.179.150

```
No.   Time         Source        Destination    Protocol Length Info
    1 0.000000000  10.11.25.29   10.10.179.150  TCP      44 42096 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    2 0.000342242  10.11.25.29   10.10.179.150  TCP      44 42096 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    3 0.000441919  10.11.25.29   10.10.179.150  TCP      44 42096 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    4 0.000538059  10.11.25.29   10.10.179.150  TCP      44 42096 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    5 0.000633699  10.11.25.29   10.10.179.150  TCP      44 42096 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    6 0.000729950  10.11.25.29   10.10.179.150  TCP      44 42096 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    7 0.000833975  10.11.25.29   10.10.179.150  TCP      44 42096 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    8 0.000932029  10.11.25.29   10.10.179.150  TCP      44 42096 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    9 0.001031746  10.11.25.29   10.10.179.150  TCP      44 42096 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   10 0.001185655  10.11.25.29   10.10.179.150  TCP      44 42096 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   11 0.250510489  10.11.0.1     10.11.25.29    ICMP     72 Time-to-live exceeded (Time to live exceeded in transit)
   12 0.250547569  10.11.0.1     10.11.25.29    ICMP     72 Time-to-live exceeded (Time to live exceeded in transit)
   13 0.250560553  10.11.0.1     10.11.25.29    ICMP     72 Time-to-live exceeded (Time to live exceeded in transit)
   14 0.251869340  10.11.0.1     10.11.25.29    ICMP     72 Time-to-live exceeded (Time to live exceeded in transit)
   15 0.251907511  10.11.0.1     10.11.25.29    ICMP     72 Time-to-live exceeded (Time to live exceeded in transit)
```

```
▸ Frame 4: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface tun0, id 0
  Raw packet data
▾ Internet Protocol Version 4, Src: 10.11.25.29, Dst: 10.10.179.150
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 44
    Identification: 0xd371 (54129)
  ▸ Flags: 0x00
    Fragment Offset: 0
    Time to Live: 1
    Protocol: TCP (6)
    Header Checksum: 0x0593 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.11.25.29
    Destination Address: 10.10.179.150
```

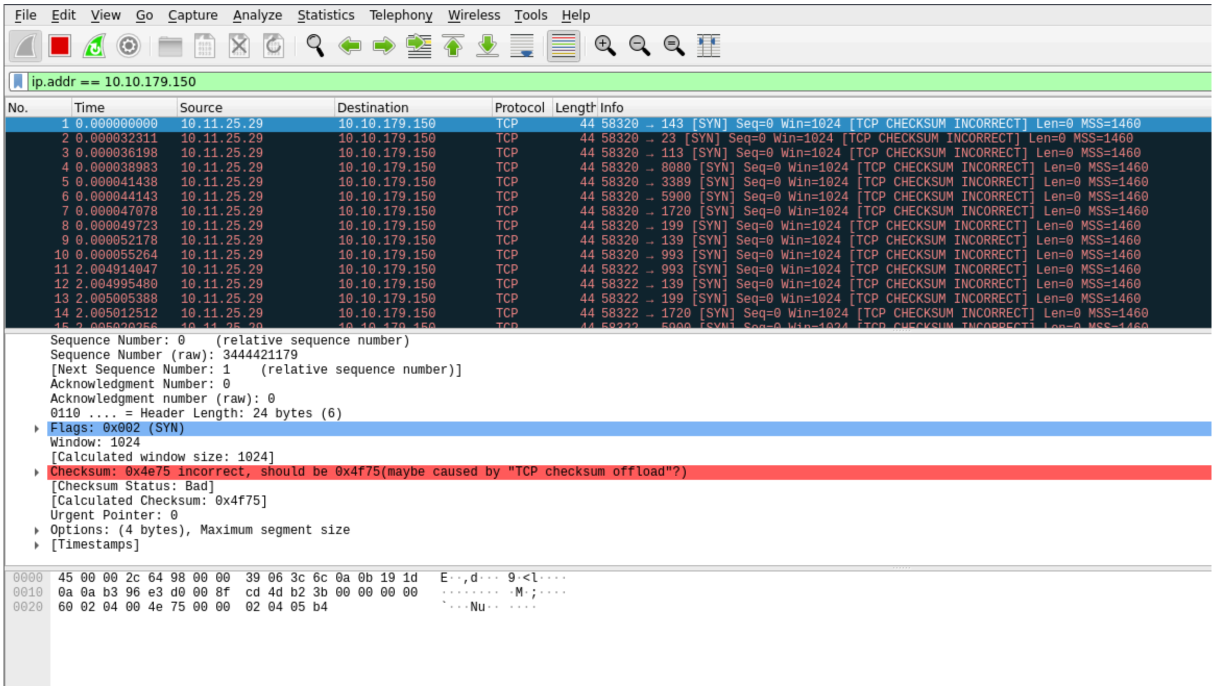
```
0000  45 00 00 2c d3 71 00 00  01 06 05 93 0a 0b 19 1d   E··,·q·· ········
0010  0a 0a b3 96 a4 70 1f 90  4b 46 32 40 00 00 00 00   ·····p·· KF2@····
0020  60 02 04 00 71 d7 00 00  02 04 05 b4               `···q··· ····
```

Figure 8.3 Manipulate TTL value

Send packets with bogus Tcp/Udp checksums.

Asks Nmap to use an invalid TCP, UDP or SCTP checksum for packets sent to target hosts. Since virtually all host IP stacks properly drop these packets, any responses received are likely coming from a firewall or IDS that didn't bother to verify the checksum

Command: nmap -sS -Pn --badsum -F 10.10.179.150


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 10.10.179.150
```

```
No.  Time          Source        Destination    Protocol Length Info
   1 0.000000000  10.11.25.29  10.10.179.150  TCP      44 58320 → 143 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
   2 0.000032311  10.11.25.29  10.10.179.150  TCP      44 58320 → 23 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
   3 0.000036198  10.11.25.29  10.10.179.150  TCP      44 58320 → 113 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
   4 0.000038983  10.11.25.29  10.10.179.150  TCP      44 58320 → 8080 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
   5 0.000041438  10.11.25.29  10.10.179.150  TCP      44 58320 → 3389 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
   6 0.000044143  10.11.25.29  10.10.179.150  TCP      44 58320 → 5900 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
   7 0.000047078  10.11.25.29  10.10.179.150  TCP      44 58320 → 1720 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
   8 0.000049723  10.11.25.29  10.10.179.150  TCP      44 58320 → 199 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
   9 0.000052178  10.11.25.29  10.10.179.150  TCP      44 58320 → 139 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
  10 0.000055264  10.11.25.29  10.10.179.150  TCP      44 58320 → 993 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
  11 2.004914047  10.11.25.29  10.10.179.150  TCP      44 58322 → 993 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
  12 2.004995480  10.11.25.29  10.10.179.150  TCP      44 58322 → 139 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
  13 2.005005388  10.11.25.29  10.10.179.150  TCP      44 58322 → 199 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
  14 2.005012512  10.11.25.29  10.10.179.150  TCP      44 58322 → 1720 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
  15 2.005020256  10.11.25.29  10.10.179.150  TCP      44 58322 → 5900 [SYN] Seq=0 Win=1024 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
```

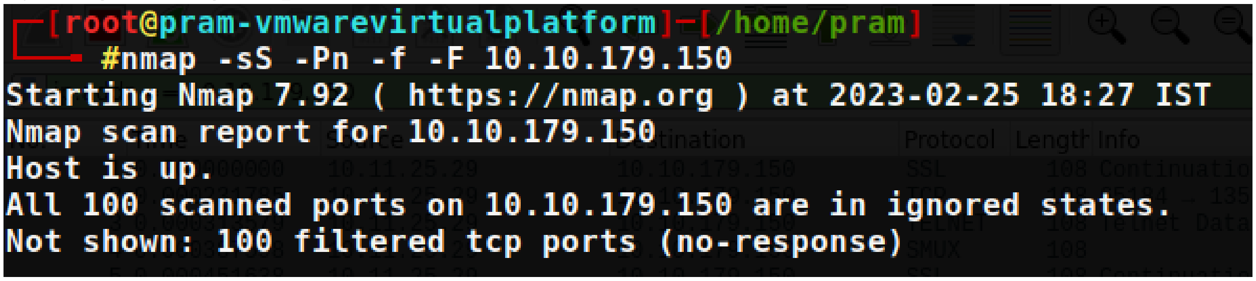
```
      Sequence Number: 0    (relative sequence number)
      Sequence Number (raw): 3444421179
      [Next Sequence Number: 1    (relative sequence number)]
      Acknowledgment Number: 0
      Acknowledgment number (raw): 0
      0110 .... = Header Length: 24 bytes (6)
    ▸ Flags: 0x002 (SYN)
      Window: 1024
      [Calculated window size: 1024]
    ▸ Checksum: 0x4e75 incorrect, should be 0x4f75(maybe caused by "TCP checksum offload"?)
      [Checksum Status: Bad]
      [Calculated Checksum: 0x4f75]
      Urgent Pointer: 0
    ▸ Options: (4 bytes), Maximum segment size
    ▸ [Timestamps]
```

```
0000  45 00 00 2c 64 98 00 00  39 06 3c 6c 0a 0b 19 1d   E··,d···  9·<l····
0010  0a 0a b3 96 e3 d0 00 8f  cd 4d b2 3b 00 00 00 00   ········  ·M·;····
0020  60 02 04 00 4e 75 00 00  02 04 05 b4               `···Nu··  ····
```

Figure 8.4 Send packets with bogus Tcp/Udp checksums

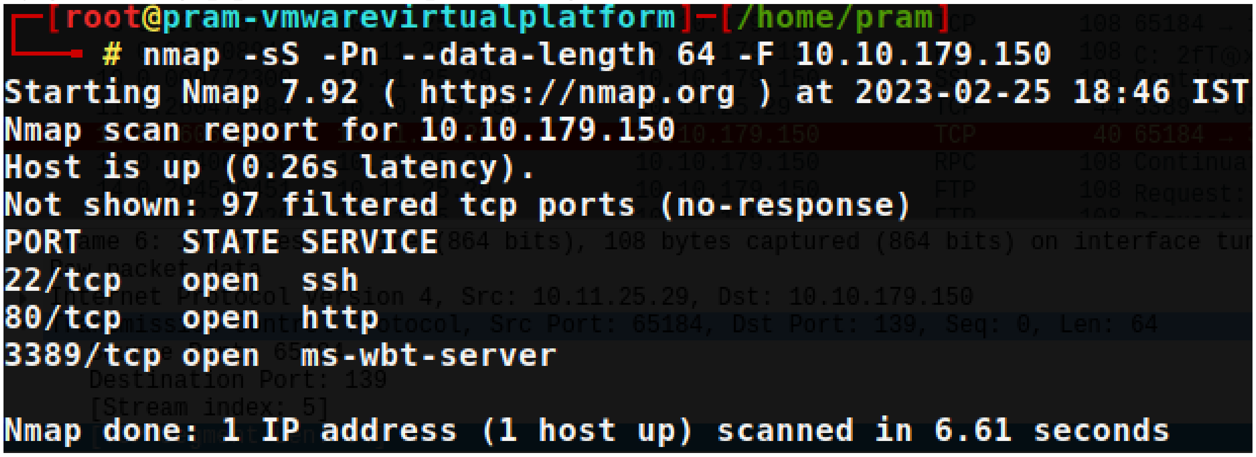
Results:

By Fragmenting the packets with 8 bit data:



```
┌─[root@pram-vmwarevirtualplatform]─[/home/pram]
└──╼ #nmap -sS -Pn -f -F 10.10.179.150
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 18:27 IST
Nmap scan report for 10.10.179.150
Host is up.
All 100 scanned ports on 10.10.179.150 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
```

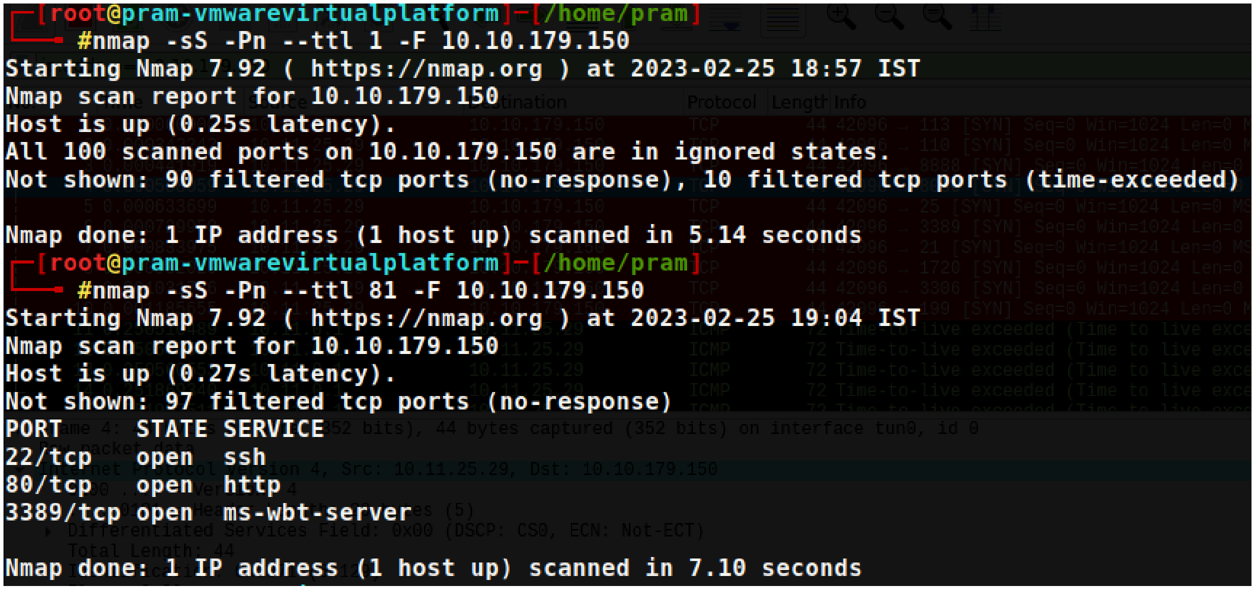
By generating ip packets with specific length.



```
┌─[root@pram-vmwarevirtualplatform]─[/home/pram]
└──╼ # nmap -sS -Pn --data-length 64 -F 10.10.179.150
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 18:46 IST
Nmap scan report for 10.10.179.150
Host is up (0.26s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 6.61 seconds
```

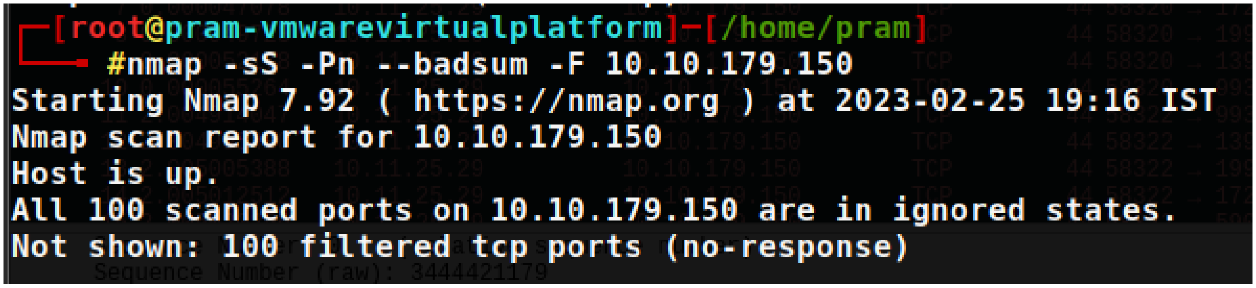
Figure 8.5 Results

By manipulating the TTL value.



```
┌─[root@pram-vmwarevirtualplatform]─[/home/pram]
└──╼ #nmap -sS -Pn --ttl 1 -F 10.10.179.150
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 18:57 IST
Nmap scan report for 10.10.179.150
Host is up (0.25s latency).
All 100 scanned ports on 10.10.179.150 are in ignored states.
Not shown: 90 filtered tcp ports (no-response), 10 filtered tcp ports (time-exceeded)

Nmap done: 1 IP address (1 host up) scanned in 5.14 seconds
┌─[root@pram-vmwarevirtualplatform]─[/home/pram]
└──╼ #nmap -sS -Pn --ttl 81 -F 10.10.179.150
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 19:04 IST
Nmap scan report for 10.10.179.150
Host is up (0.27s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 7.10 seconds
```

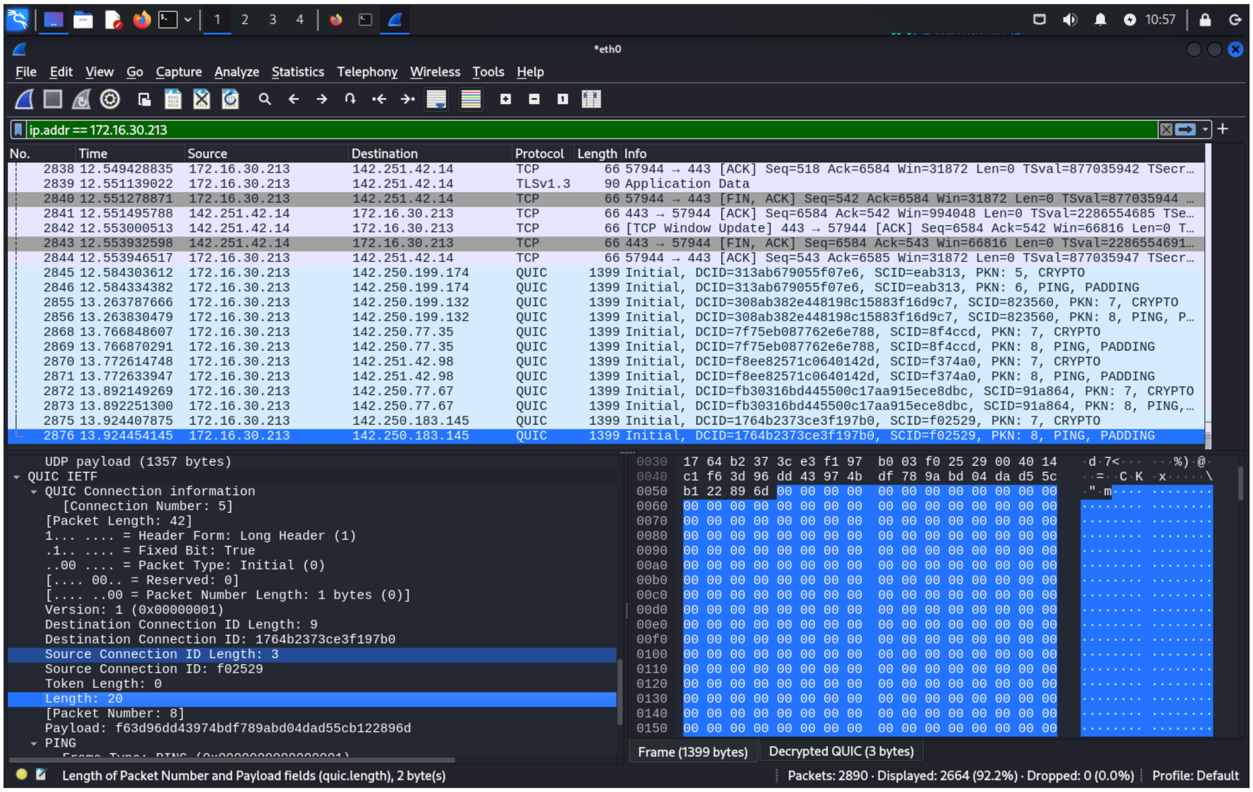
By sending packets with bogus TCP/UDP checksums.



```
┌─[root@pram-vmwarevirtualplatform]─[/home/pram]
└──╼ #nmap -sS -Pn --badsum -F 10.10.179.150
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-25 19:16 IST
Nmap scan report for 10.10.179.150
Host is up.
All 100 scanned ports on 10.10.179.150 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
```

Figure 8.6 Results

8.6 Simulated output:

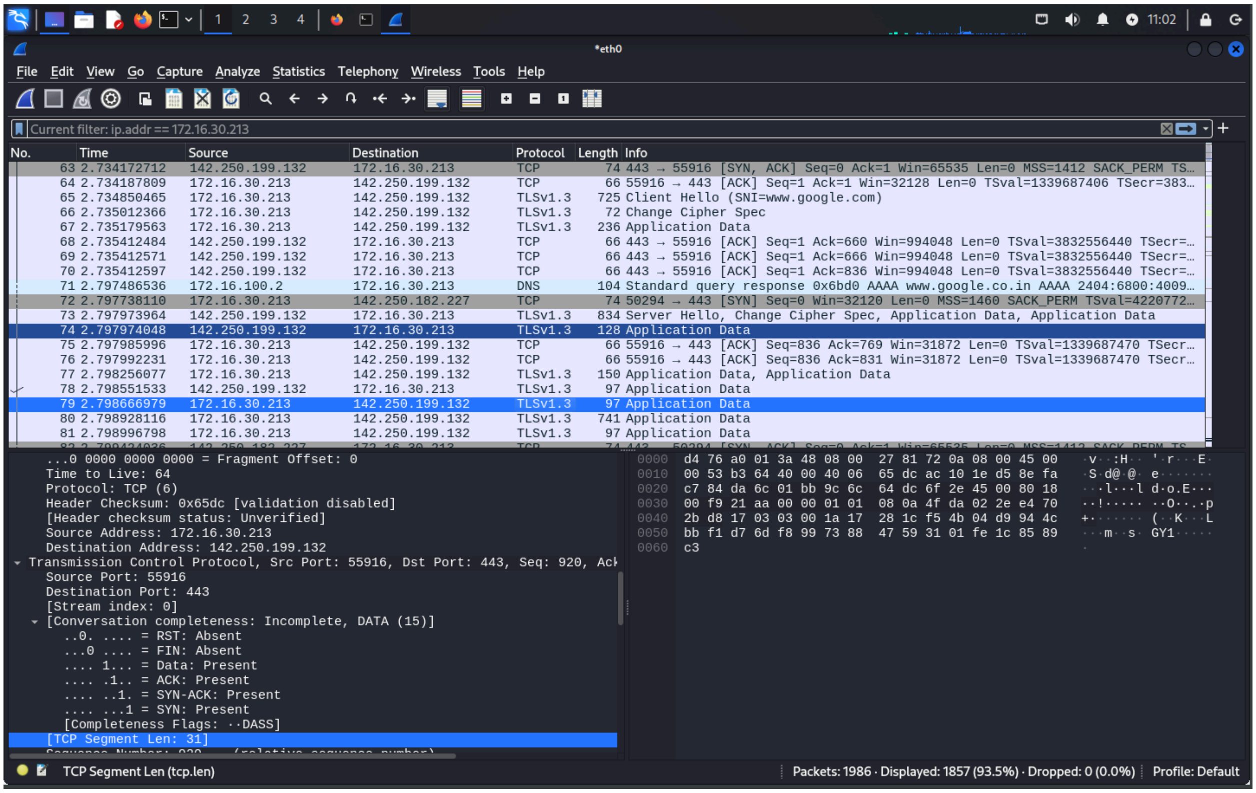


```
ip.addr == 172.16.30.213

No.  Time         Source          Destination      Protocol Length Info
2838 12.549428835 172.16.30.213   142.251.42.14    TCP        66 57944 → 443 [ACK] Seq=518 Ack=6584 Win=31872 Len=0 TSval=877035942 TSecr…
2839 12.551139022 172.16.30.213   142.251.42.14    TLSv1.3    90 Application Data
2840 12.551278871 172.16.30.213   142.251.42.14    TCP        66 57944 → 443 [FIN, ACK] Seq=542 Ack=6584 Win=31872 Len=0 TSval=877035944 …
2841 12.551495788 142.251.42.14   172.16.30.213    TCP        66 443 → 57944 [ACK] Seq=6584 Ack=542 Win=994048 Len=0 TSval=2286554685 TSe…
2842 12.553000513 142.251.42.14   172.16.30.213    TCP        66 [TCP Window Update] 443 → 57944 [ACK] Seq=6584 Ack=542 Win=66816 Len=0 T…
2843 12.553932598 142.251.42.14   172.16.30.213    TCP        66 443 → 57944 [FIN, ACK] Seq=6584 Ack=543 Win=66816 Len=0 TSval=2286554691…
2844 12.553946517 172.16.30.213   142.251.42.14    TCP        66 57944 → 443 [ACK] Seq=543 Ack=6585 Win=31872 Len=0 TSval=877035947 TSecr…
2845 12.584303612 172.16.30.213   142.250.199.174  QUIC     1399 Initial, DCID=313ab679055f07e6, SCID=eab313, PKN: 5, CRYPTO
2846 12.584334382 172.16.30.213   142.250.199.174  QUIC     1399 Initial, DCID=313ab679055f07e6, SCID=eab313, PKN: 6, PING, PADDING
2855 13.263787666 172.16.30.213   142.250.199.132  QUIC     1399 Initial, DCID=308ab382e448198c15883f16d9c7, SCID=823560, PKN: 7, CRYPTO
2856 13.263830479 172.16.30.213   142.250.199.132  QUIC     1399 Initial, DCID=308ab382e448198c15883f16d9c7, SCID=823560, PKN: 8, PING, P…
2868 13.766848607 172.16.30.213   142.250.77.35    QUIC     1399 Initial, DCID=7f75eb087762e6e788, SCID=8f4ccd, PKN: 7, CRYPTO
2869 13.766870291 172.16.30.213   142.250.77.35    QUIC     1399 Initial, DCID=7f75eb087762e6e788, SCID=8f4ccd, PKN: 8, PING, PADDING
2870 13.772614748 172.16.30.213   142.251.42.98    QUIC     1399 Initial, DCID=f8ee82571c0640142d, SCID=f374a0, PKN: 7, CRYPTO
2871 13.772633947 172.16.30.213   142.251.42.98    QUIC     1399 Initial, DCID=f8ee82571c0640142d, SCID=f374a0, PKN: 8, PING, PADDING
2872 13.892149269 172.16.30.213   142.250.77.67    QUIC     1399 Initial, DCID=fb30316bd445500c17aa915ece8dbc, SCID=91a864, PKN: 7, CRYPTO
2873 13.892251300 172.16.30.213   142.250.77.67    QUIC     1399 Initial, DCID=fb30316bd445500c17aa915ece8dbc, SCID=91a864, PKN: 8, PING,…
2875 13.924407875 172.16.30.213   142.250.183.145  QUIC     1399 Initial, DCID=1764b2373ce3f197b0, SCID=f02529, PKN: 7, CRYPTO
2876 13.924454145 172.16.30.213   142.250.183.145  QUIC     1399 Initial, DCID=1764b2373ce3f197b0, SCID=f02529, PKN: 8, PING, PADDING
```

```
    UDP payload (1357 bytes)
  QUIC IETF
    QUIC Connection information
        [Connection Number: 5]
      [Packet Length: 42]
      1... .... = Header Form: Long Header (1)
      .1.. .... = Fixed Bit: True
      ..00 .... = Packet Type: Initial (0)
      [.... 00.. = Reserved: 0]
      [.... ..00 = Packet Number Length: 1 bytes (0)]
      Version: 1 (0x00000001)
      Destination Connection ID Length: 9
      Destination Connection ID: 1764b2373ce3f197b0
      Source Connection ID Length: 3
      Source Connection ID: f02529
      Token Length: 0
      Length: 20
      [Packet Number: 8]
      Payload: f63d96dd43974bdf789abd04dad55cb122896d
    PING
```

```
0030  17 64 b2 37 3c e3 f1 97  b0 03 f0 25 29 00 40 14   ·d·7<··· ···%)·@·
0040  c1 f6 3d 96 dd 43 97 4b  df 78 9a bd 04 da d5 5c   ··=··C·K ·x·····\
0050  b1 22 89 6d 00 00 00 00  00 00 00 00 00 00 00 00   ·"·m···· ········
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 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

```
Length of Packet Number and Payload fields (quic.length), 2 byte(s)
Packets: 2890 · Displayed: 2664 (92.2%) · Dropped: 0 (0.0%)   Profile: Default
```

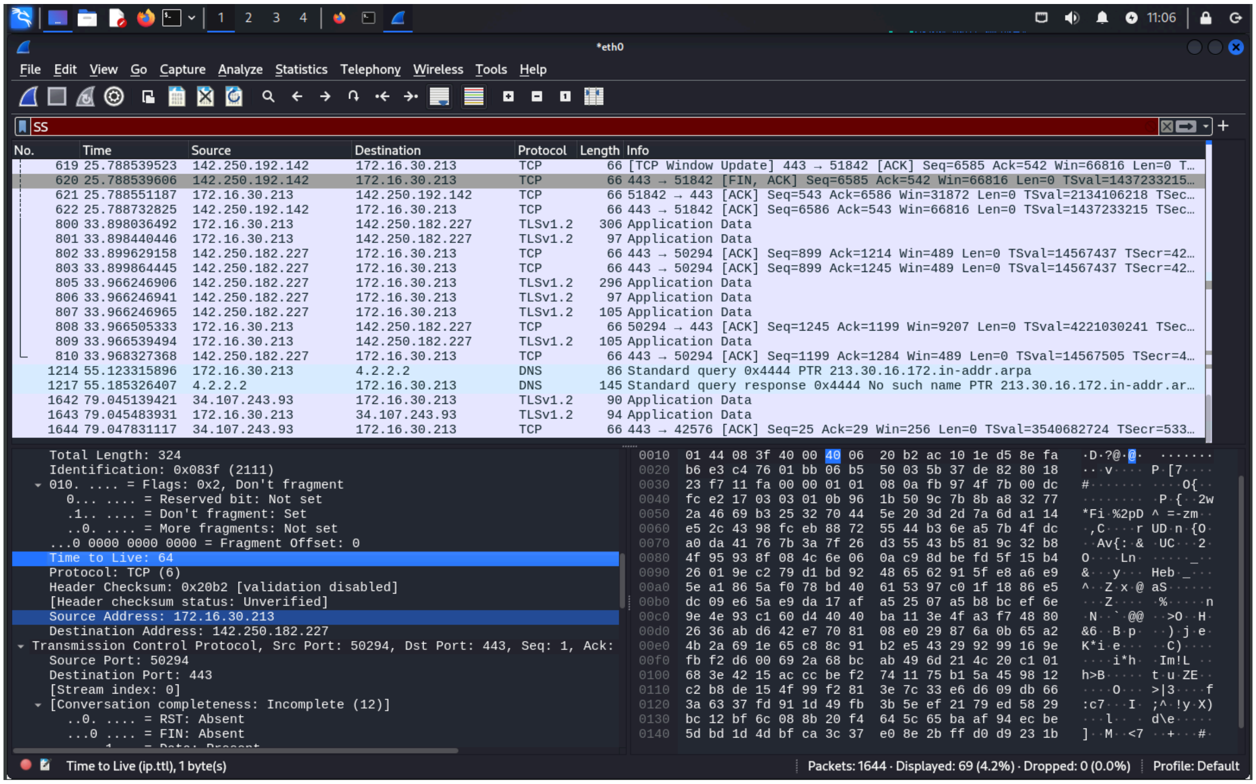


```
Current filter: ip.addr == 172.16.30.213

No. Time        Source          Destination     Protocol Length Info
 63 2.734172712 142.250.199.132 172.16.30.213   TCP        74 443 → 55916 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TS…
 64 2.734187809 172.16.30.213   142.250.199.132 TCP        66 55916 → 443 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1339687406 TSecr=383…
 65 2.734850465 172.16.30.213   142.250.199.132 TLSv1.3   725 Client Hello (SNI=www.google.com)
 66 2.735012366 172.16.30.213   142.250.199.132 TLSv1.3    72 Change Cipher Spec
 67 2.735179563 172.16.30.213   142.250.199.132 TLSv1.3   236 Application Data
 68 2.735412484 142.250.199.132 172.16.30.213   TCP        66 443 → 55916 [ACK] Seq=1 Ack=660 Win=994048 Len=0 TSval=3832556440 TSecr=…
 69 2.735412571 142.250.199.132 172.16.30.213   TCP        66 443 → 55916 [ACK] Seq=1 Ack=666 Win=994048 Len=0 TSval=3832556440 TSecr=…
 70 2.735412597 142.250.199.132 172.16.30.213   TCP        66 443 → 55916 [ACK] Seq=1 Ack=836 Win=994048 Len=0 TSval=3832556440 TSecr=…
 71 2.797486536 172.16.100.2    172.16.30.213   DNS       104 Standard query response 0x6bd0 AAAA www.google.co.in AAAA 2404:6800:4009…
 72 2.797738110 172.16.30.213   142.250.182.227 TCP        74 50294 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=4220772…
 73 2.797973964 142.250.199.132 172.16.30.213   TLSv1.3   834 Server Hello, Change Cipher Spec, Application Data, Application Data
 74 2.797974048 142.250.199.132 172.16.30.213   TLSv1.3   128 Application Data
 75 2.797985996 172.16.30.213   142.250.199.132 TCP        66 55916 → 443 [ACK] Seq=836 Ack=769 Win=31872 Len=0 TSval=1339687470 TSecr…
 76 2.797992231 172.16.30.213   142.250.199.132 TCP        66 55916 → 443 [ACK] Seq=836 Ack=831 Win=31872 Len=0 TSval=1339687470 TSecr…
 77 2.798256077 172.16.30.213   142.250.199.132 TLSv1.3   150 Application Data, Application Data
 78 2.798551533 142.250.199.132 172.16.30.213   TLSv1.3    97 Application Data
 79 2.798666979 172.16.30.213   142.250.199.132 TLSv1.3    97 Application Data
 80 2.798928116 172.16.30.213   142.250.199.132 TLSv1.3   741 Application Data
 81 2.798996798 172.16.30.213   142.250.199.132 TLSv1.3    97 Application Data
```

```
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x65dc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.30.213
    Destination Address: 142.250.199.132
  Transmission Control Protocol, Src Port: 55916, Dst Port: 443, Seq: 920, Ack
    Source Port: 55916
    Destination Port: 443
    [Stream index: 0]
    [Conversation completeness: Incomplete, DATA (15)]
      ..0. .... = RST: Absent
      ...0 .... = FIN: Absent
      .... 1... = Data: Present
      .... .1.. = ACK: Present
      .... ..1. = SYN-ACK: Present
      .... ...1 = SYN: Present
      [Completeness Flags: ··DASS]
    [TCP Segment Len: 31]
```

```
0000  d4 76 a0 01 3a 48 08 00  27 81 72 0a 08 00 45 00   ·v··:H·· '·r···E·
0010  00 53 b3 64 40 00 40 06  65 dc ac 10 1e d5 8e fa   ·S·d@·@· e·······
0020  c7 84 da 6c 01 bb 9c 6c  64 dc 6f 2e 45 00 80 18   ···l···l d·o.E···
0030  00 f9 21 aa 00 00 01 01  08 0a 4f da 02 2e e4 70   ··!····· ··O···.p
0040  2b d8 17 03 03 00 1a 17  28 1c f5 4b 04 d9 94 4c   +······· (··K···L
0050  bb f1 d7 6d f8 99 73 88  47 59 31 01 fe 1c 85 89   ···m··s· GY1·····
0060  c3                                                 ·
```

```
TCP Segment Len (tcp.len)
Packets: 1986 · Displayed: 1857 (93.5%) · Dropped: 0 (0.0%)   Profile: Default
```



1 2 3 4
11:06
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

SS

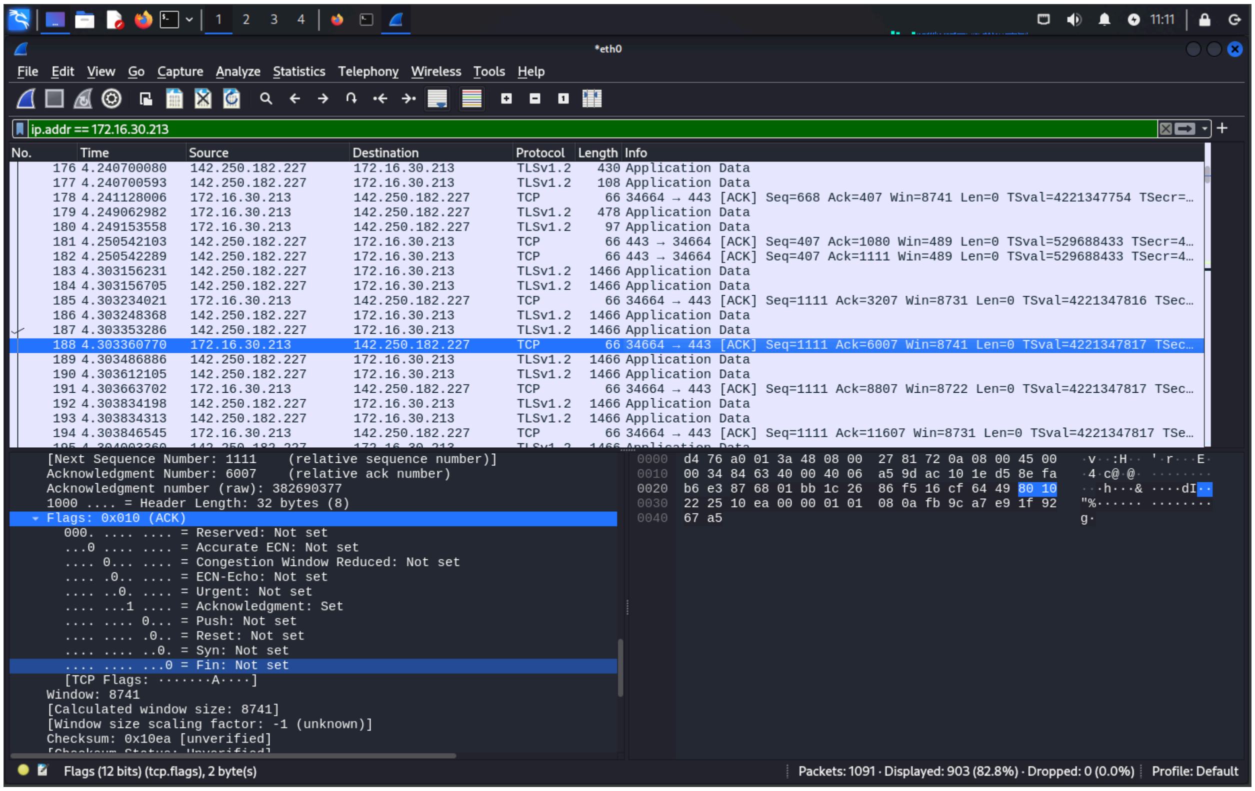
```
No.   Time          Source           Destination      Protocol Length Info
  619 25.788539523  142.250.192.142  172.16.30.213    TCP       66 [TCP Window Update] 443 → 51842 [ACK] Seq=6585 Ack=542 Win=66816 Len=0 T…
  620 25.788539606  142.250.192.142  172.16.30.213    TCP       66 443 → 51842 [FIN, ACK] Seq=6585 Ack=542 Win=66816 Len=0 TSval=1437233215…
  621 25.788551187  172.16.30.213    142.250.192.142  TCP       66 51842 → 443 [ACK] Seq=543 Ack=6586 Win=31872 Len=0 TSval=2134106218 TSec…
  622 25.788732825  142.250.192.142  172.16.30.213    TCP       66 443 → 51842 [ACK] Seq=6586 Ack=543 Win=66816 Len=0 TSval=1437233215 TSec…
  800 33.898036492  172.16.30.213    142.250.182.227  TLSv1.2  306 Application Data
  801 33.898440446  172.16.30.213    142.250.182.227  TLSv1.2   97 Application Data
  802 33.899629158  142.250.182.227  172.16.30.213    TCP       66 443 → 50294 [ACK] Seq=899 Ack=1214 Win=489 Len=0 TSval=14567437 TSecr=42…
  803 33.899864445  142.250.182.227  172.16.30.213    TCP       66 443 → 50294 [ACK] Seq=899 Ack=1245 Win=489 Len=0 TSval=14567437 TSecr=42…
  805 33.966246906  142.250.182.227  172.16.30.213    TLSv1.2  296 Application Data
  806 33.966246941  142.250.182.227  172.16.30.213    TLSv1.2   97 Application Data
  807 33.966246965  142.250.182.227  172.16.30.213    TLSv1.2  105 Application Data
  808 33.966505333  172.16.30.213    142.250.182.227  TCP       66 50294 → 443 [ACK] Seq=1245 Ack=1199 Win=9207 Len=0 TSval=4221030241 TSec…
  809 33.966539494  172.16.30.213    142.250.182.227  TLSv1.2  105 Application Data
  810 33.968327368  142.250.182.227  172.16.30.213    TCP       66 443 → 50294 [ACK] Seq=1199 Ack=1284 Win=489 Len=0 TSval=14567505 TSecr=4…
 1214 55.123315896  172.16.30.213    4.2.2.2          DNS       86 Standard query 0x4444 PTR 213.30.16.172.in-addr.arpa
 1217 55.185326407  4.2.2.2          172.16.30.213    DNS      145 Standard query response 0x4444 No such name PTR 213.30.16.172.in-addr.ar…
 1642 79.045139421  34.107.243.93    172.16.30.213    TLSv1.2   90 Application Data
 1643 79.045483931  172.16.30.213    34.107.243.93    TLSv1.2   94 Application Data
 1644 79.047831117  34.107.243.93    172.16.30.213    TCP       66 443 → 42576 [ACK] Seq=25 Ack=29 Win=256 Len=0 TSval=3540682724 TSecr=533…
```

```
    Total Length: 324
    Identification: 0x083f (2111)
  ▾ 010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x20b2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.30.213
    Destination Address: 142.250.182.227
▾ Transmission Control Protocol, Src Port: 50294, Dst Port: 443, Seq: 1, Ack:
    Source Port: 50294
    Destination Port: 443
    [Stream index: 0]
  ▾ [Conversation completeness: Incomplete (12)]
      ..0. .... = RST: Absent
      ...0 .... = FIN: Absent
```

```
0010  01 44 08 3f 40 00 40 06  20 b2 ac 10 1e d5 8e fa   ·D·?@·@·  ········
0020  b6 e3 c4 76 01 bb 06 b5  50 03 5b 37 de 82 80 18   ···v····  P·[7····
0030  23 f7 11 fa 00 00 01 01  08 0a fb 97 4f 7b 00 dc   #·······  ····O{··
0040  fc e2 17 03 03 01 0b 96  1b 50 9c 7b 8b a8 32 77   ········  ·P·{··2w
0050  2a 46 69 b3 25 32 70 44  5e 20 3d 2d 7a 6d a1 14   *Fi·%2pD  ^ =-zm··
0060  e5 2c 43 98 fc eb 88 72  55 44 b3 6e a5 7b 4f dc   ·,C····r  UD·n·{O·
0070  a0 da 41 76 7b 3a 7f 26  d3 55 43 b5 81 9c 32 b8   ··Av{:·&  ·UC···2·
0080  4f 95 93 8f 08 4c 6e 06  0a c9 8d be fd 5f 15 b4   O····Ln·  ·····_··
0090  26 01 9e c2 79 d1 bd 92  48 65 62 91 5f e8 a6 e9   &···y···  Heb·_···
00a0  5e a1 86 5a f0 78 bd 40  61 53 97 c0 1f 18 86 e5   ^··Z·x·@  aS······
00b0  dc 09 e6 5a e9 da 17 af  a5 25 07 a5 b8 bc ef 6e   ···Z····  ·%·····n
00c0  9e 4e 93 c1 60 d4 40 40  ba 11 3e 4f a3 f7 48 80   ·N··`·@@  ··>O··H·
00d0  26 36 ab d6 42 e7 70 81  08 e0 29 87 6a 0b 65 a2   &6··B·p·  ··)·j·e·
00e0  4b 2a 69 1e 65 c8 8c 91  b2 e5 43 29 92 99 16 9e   K*i·e···  ··C)····
00f0  fb f2 d6 00 69 2a 68 bc  ab 49 6d 21 4c 20 c1 01   ····i*h·  ·Im!L ··
0100  68 3e 42 15 ac cc be f2  74 11 75 b1 5a 45 98 12   h>B·····  t·u·ZE··
0110  c2 b8 de 15 4f 99 f2 81  3e 7c 33 e6 d6 09 db 66   ····O···  >|3····f
0120  3a 63 37 fd 91 1d 49 fb  3b 5e ef 21 79 ed 58 29   :c7···I·  ;^·!y·X)
0130  bc 12 bf 6c 08 8b 20 f4  64 5c 65 ba af 94 ec be   ···l·· ·  d\e·····
0140  5d bd 1d 4d bf ca 3c 37  e0 8e 2b ff d0 d9 23 1b   ]··M··<7  ··+···#·
```

Time to Live (ip.ttl), 1 byte(s)

Packets: 1644 · Displayed: 69 (4.2%) · Dropped: 0 (0.0%)   Profile: Default



1 2 3 4
11:11
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.16.30.213

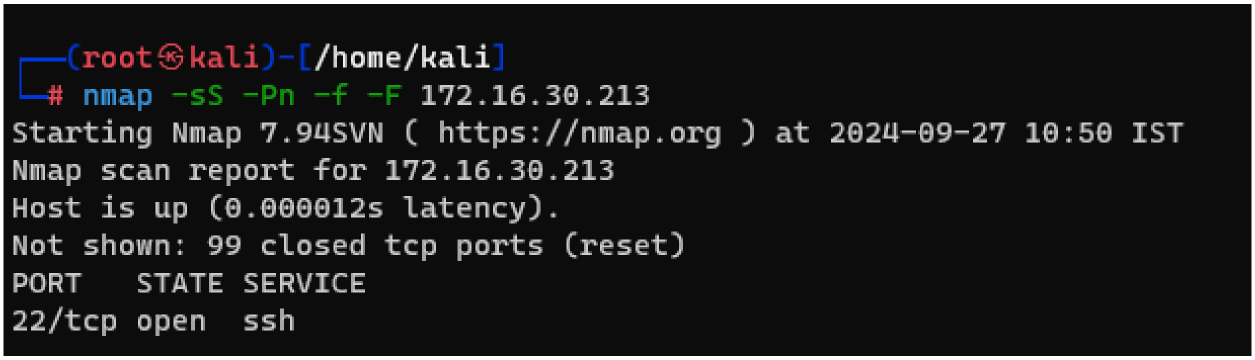
```
No.  Time         Source           Destination      Protocol Length Info
 176 4.240700080  142.250.182.227  172.16.30.213    TLSv1.2   430 Application Data
 177 4.240700593  142.250.182.227  172.16.30.213    TLSv1.2   108 Application Data
 178 4.241128006  172.16.30.213    142.250.182.227  TCP        66 34664 → 443 [ACK] Seq=668 Ack=407 Win=8741 Len=0 TSval=4221347754 TSecr=…
 179 4.249062982  172.16.30.213    142.250.182.227  TLSv1.2   478 Application Data
 180 4.249153558  172.16.30.213    142.250.182.227  TLSv1.2    97 Application Data
 181 4.250542103  142.250.182.227  172.16.30.213    TCP        66 443 → 34664 [ACK] Seq=407 Ack=1080 Win=489 Len=0 TSval=529688433 TSecr=4…
 182 4.250542289  142.250.182.227  172.16.30.213    TCP        66 443 → 34664 [ACK] Seq=407 Ack=1111 Win=489 Len=0 TSval=529688433 TSecr=4…
 183 4.303156231  142.250.182.227  172.16.30.213    TLSv1.2  1466 Application Data
 184 4.303156705  142.250.182.227  172.16.30.213    TLSv1.2  1466 Application Data
 185 4.303234021  172.16.30.213    142.250.182.227  TCP        66 34664 → 443 [ACK] Seq=1111 Ack=3207 Win=8731 Len=0 TSval=4221347816 TSec…
 186 4.303248368  142.250.182.227  172.16.30.213    TLSv1.2  1466 Application Data
 187 4.303353286  142.250.182.227  172.16.30.213    TLSv1.2  1466 Application Data
 188 4.303360770  172.16.30.213    142.250.182.227  TCP        66 34664 → 443 [ACK] Seq=1111 Ack=6007 Win=8741 Len=0 TSval=4221347817 TSec…
 189 4.303486886  142.250.182.227  172.16.30.213    TLSv1.2  1466 Application Data
 190 4.303612105  142.250.182.227  172.16.30.213    TLSv1.2  1466 Application Data
 191 4.303663702  172.16.30.213    142.250.182.227  TCP        66 34664 → 443 [ACK] Seq=1111 Ack=8807 Win=8722 Len=0 TSval=4221347817 TSec…
 192 4.303834198  142.250.182.227  172.16.30.213    TLSv1.2  1466 Application Data
 193 4.303834313  142.250.182.227  172.16.30.213    TLSv1.2  1466 Application Data
 194 4.303846545  172.16.30.213    142.250.182.227  TCP        66 34664 → 443 [ACK] Seq=1111 Ack=11607 Win=8731 Len=0 TSval=4221347817 TSe…
 195 4.304003360  142.250.182.227  172.16.30.213    TLSv1.2  1466 Application Data
```

```
    [Next Sequence Number: 1111    (relative sequence number)]
    Acknowledgment Number: 6007    (relative ack number)
    Acknowledgment number (raw): 382690377
    1000 .... = Header Length: 32 bytes (8)
  ▾ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A····]
    Window: 8741
    [Calculated window size: 8741]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x10ea [unverified]
```

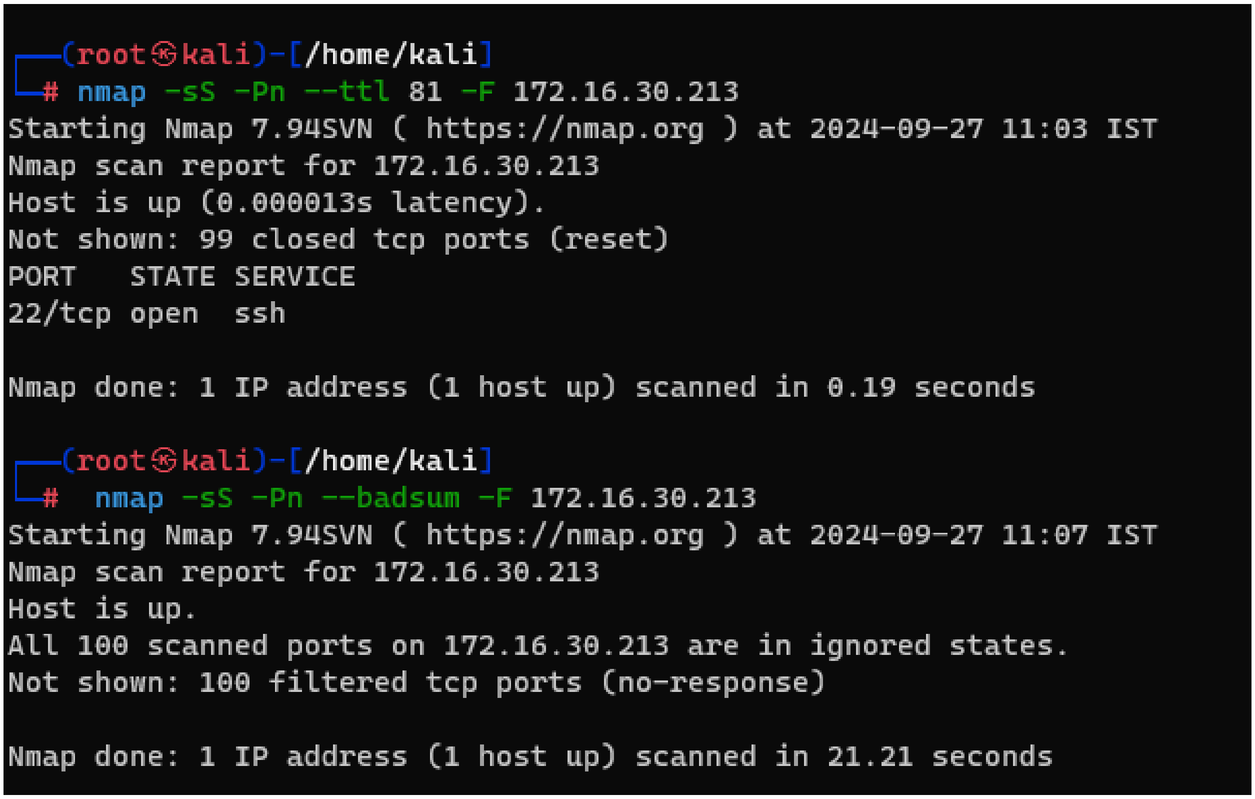
```
0000  d4 76 a0 01 3a 48 08 00  27 81 72 0a 08 00 45 00   ·v··:H··  '·r···E·
0010  00 34 84 63 40 00 40 06  a5 9d ac 10 1e d5 8e fa   ·4·c@·@·  ········
0020  b6 e3 87 68 01 bb 1c 26  86 f5 16 cf 64 49 80 10   ···h···&  ····dI··
0030  22 25 10 ea 00 00 01 01  08 0a fb 9c a7 e9 1f 92   "%······  ········
0040  67 a5                                              g·
```

Flags (12 bits) (tcp.flags), 2 byte(s)

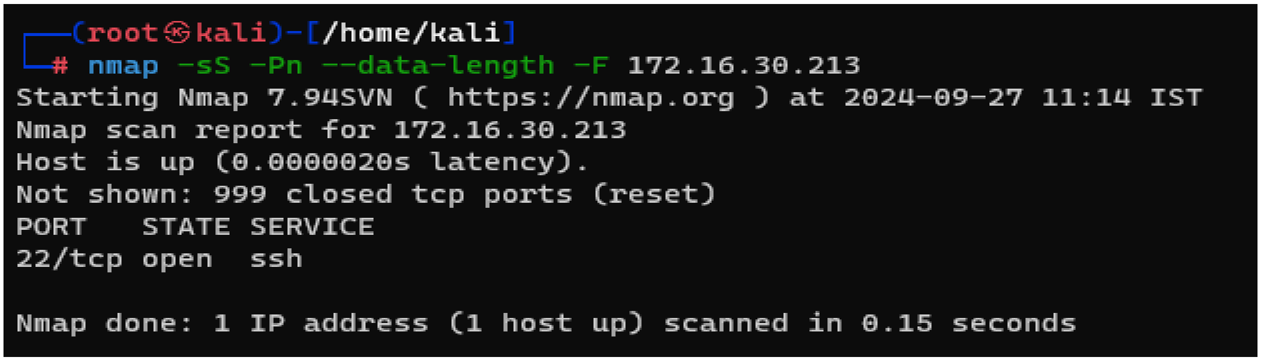
Packets: 1091 · Displayed: 903 (82.8%) · Dropped: 0 (0.0%)   Profile: Default



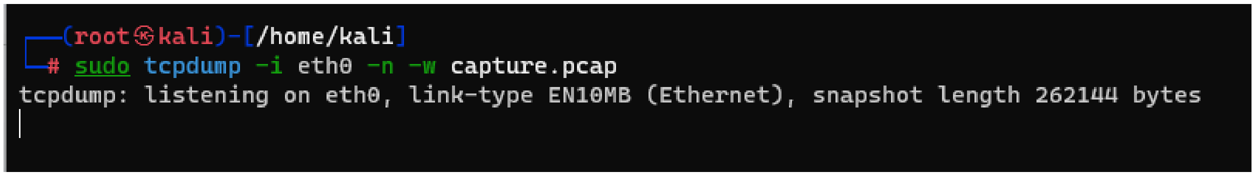
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -Pn -f -F 172.16.30.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 10:50 IST
Nmap scan report for 172.16.30.213
Host is up (0.000012s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
```



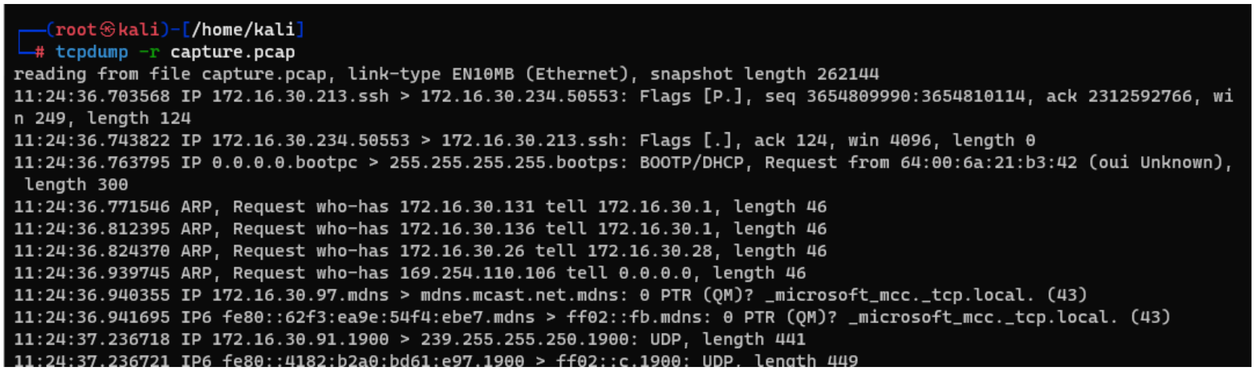
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -Pn --ttl 81 -F 172.16.30.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 11:03 IST
Nmap scan report for 172.16.30.213
Host is up (0.000013s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

┌──(root㉿kali)-[/home/kali]
└─#  nmap -sS -Pn --badsum -F 172.16.30.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 11:07 IST
Nmap scan report for 172.16.30.213
Host is up.
All 100 scanned ports on 172.16.30.213 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.21 seconds
```



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -Pn --data-length -F 172.16.30.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 11:14 IST
Nmap scan report for 172.16.30.213
Host is up (0.0000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```



```
┌──(root㉿kali)-[/home/kali]
└─# sudo tcpdump -i eth0 -n -w capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```



```
┌──(root㉿kali)-[/home/kali]
└─# tcpdump -r capture.pcap
reading from file capture.pcap, link-type EN10MB (Ethernet), snapshot length 262144
11:24:36.703568 IP 172.16.30.213.ssh > 172.16.30.234.50553: Flags [P.], seq 3654809990:3654810114, ack 2312592766, wi
n 249, length 124
11:24:36.743822 IP 172.16.30.234.50553 > 172.16.30.213.ssh: Flags [.], ack 124, win 4096, length 0
11:24:36.763795 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 64:00:6a:21:b3:42 (oui Unknown),
 length 300
11:24:36.771546 ARP, Request who-has 172.16.30.131 tell 172.16.30.1, length 46
11:24:36.812395 ARP, Request who-has 172.16.30.136 tell 172.16.30.1, length 46
11:24:36.824370 ARP, Request who-has 172.16.30.26 tell 172.16.30.28, length 46
11:24:36.939745 ARP, Request who-has 169.254.110.106 tell 0.0.0.0, length 46
11:24:36.940355 IP 172.16.30.97.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? _microsoft_mcc._tcp.local. (43)
11:24:36.941695 IP6 fe80::62f3:ea9e:54f4:ebe7.mdns > ff02::fb.mdns: 0 PTR (QM)? _microsoft_mcc._tcp.local. (43)
11:24:37.236718 IP 172.16.30.91.1900 > 239.255.255.250.1900: UDP, length 441
11:24:37.236721 IP6 fe80::4182:b2a0:bd61:e97.1900 > ff02::c.1900: UDP, length 449
```

8.7 Conclusion:

Hence we learned about IDS and firewalls and how to execute it in kali linux

8.8 Questions:

1. A **firewall** controls access to a network by blocking or permitting traffic based on security rules, while **Intrusion Detection System (IDS)** monitors and analyses network traffic for suspicious activities to detect potential threats.

2. Types of IDS are:
   - **Network-based IDS (NIDS)**
   - **Host-based IDS (HIDS)**
   - **Signature-based IDS**
   - **Anomaly-based IDS**
   - **Protocol-based IDS**

3. Types of firewall are:

- **Packet Filtering Firewall**
- **Stateful Inspection Firewall**
- **Proxy Firewall**
- **Next-Generation Firewall (NGFW)**
- **Web Application Firewall (WAF)**