Name: Pankaj Parihar

Roll No.: 74

Batch: T21

Assignment – 7

Aim: To study packet sniffer tools like Wireshark and TCPDUMP.

Theory:

Wireshark

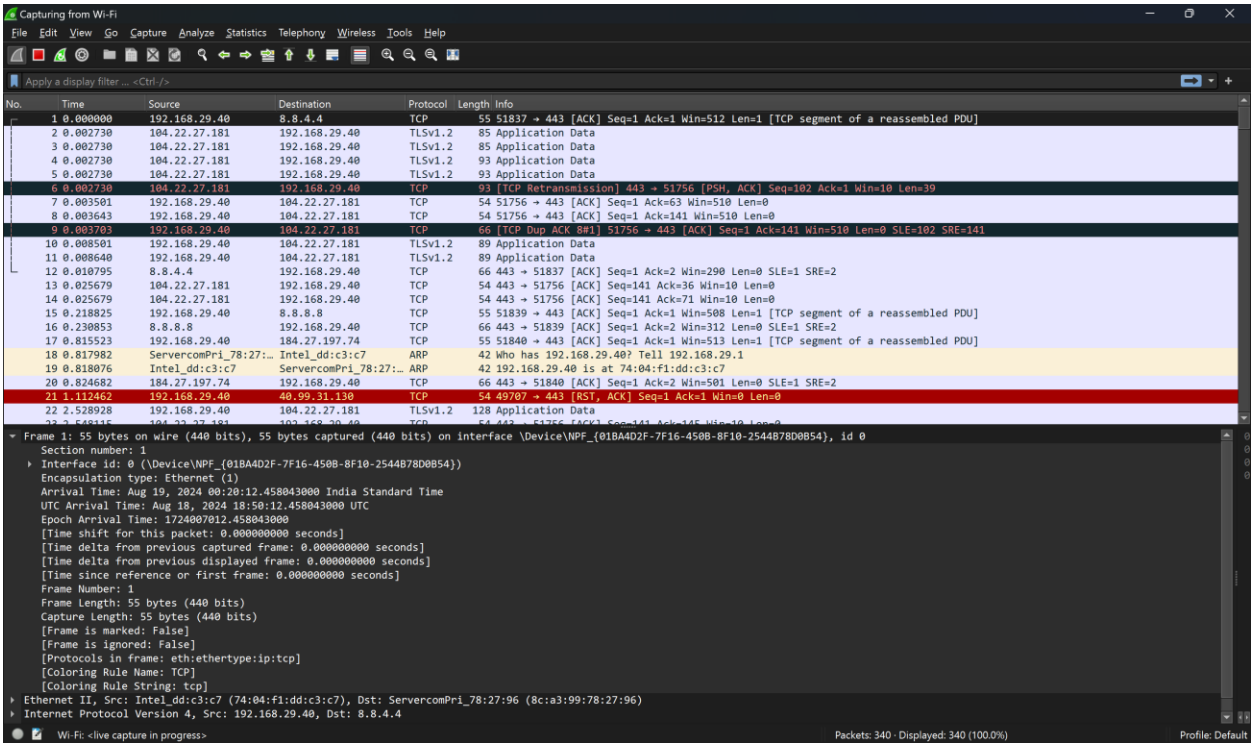
1. **Purpose**: Wireshark is a network protocol analyzer that captures and interacts with live network traffic. It provides a graphical interface to analyze packet data.
2. **Features**:
    - **User Interface**: Wireshark has a graphical user interface (GUI) that displays network data in a detailed and organized manner.
    - **Packet Analysis**: It offers extensive protocol decoding and analysis capabilities, allowing users to inspect packets at various layers of the OSI model.
    - **Filtering**: Supports powerful display and capture filters to focus on specific network traffic.
    - **Visualization**: Provides graphical representations of network traffic, including statistics, flow diagrams, and more.
3. **Use Cases**:
    - **Network Troubleshooting**: Helps diagnose network issues by providing detailed insights into network traffic and protocol behavior.
    - **Security Analysis**: Useful for identifying and analyzing security vulnerabilities and attacks.
    - **Protocol Development**: Assists in developing and testing new network protocols.

tcpdump

1. **Purpose**: tcpdump is a command-line network packet analyzer that captures and displays network traffic.
2. **Features**:
    - **Command-Line Interface**: Operates through the command line, making it suitable for scripting and remote administration.
    - **Packet Capture**: Captures packets in real-time and saves them to files for later analysis.
    - **Filtering**: Uses BPF (Berkeley Packet Filter) syntax for specifying which packets to capture or ignore.
    - **Output**: Provides raw packet data and basic decoding, but lacks advanced graphical analysis features.
3. **Use Cases**:
    - **Quick Analysis**: Ideal for quick, real-time network diagnostics and capturing packets from the command line.
    - **Scripting and Automation**: Useful for automating network capture tasks and integrating with other tools.
    - **Remote Debugging**: Can be used on remote systems where a GUI might not be available.

Output:

Wireshark:



TCPDUMP

1. tcpdump -D

```
lab1003@lab1003-OptiPlex-3020:~$ tcpdump -D
1.enp2s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
6.usbmon1 (USB bus number 1)
7.usbmon2 (USB bus number 2)
8.usbmon3 (USB bus number 3)
9.usbmon4 (USB bus number 4)
lab1003@lab1003-OptiPlex-3020:~$
```

2. sudo tcpdump -n

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -n
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:09:48.443472 ARP, Request who-has 192.168.0.123 tell 192.168.0.174, length 46
15:09:48.753495 ARP, Request who-has 192.168.0.13 tell 192.168.0.9, length 46
15:09:48.826150 IP6 fe80::df48:273b:146c:210.5353 > ff02::fb.5353: 0 PTR (QM)? _scanner._tcp.local. (37)
15:09:48.826185 IP 192.168.0.213.5353 > 224.0.0.251.5353: 0 PTR (QM)? _scanner._tcp.local. (37)
15:09:48.889280 IP 192.168.0.43.62249 > 239.255.255.250.1900: UDP, length 175
15:09:48.944652 ARP, Request who-has 192.168.0.198 tell 192.168.0.174, length 46
15:09:49.298754 ARP, Request who-has 192.168.0.197 tell 192.168.0.80, length 46
15:09:49.444240 ARP, Request who-has 192.168.0.123 tell 192.168.0.174, length 46
15:09:49.737676 ARP, Request who-has 192.168.0.13 tell 192.168.0.9, length 46
15:09:49.827723 IP6 fe80::df48:273b:146c:210.5353 > ff02::fb.5353: 0 PTR (QM)? _scanner._tcp.local. (37)
15:09:49.827747 IP 192.168.0.213.5353 > 224.0.0.251.5353: 0 PTR (QM)? _scanner._tcp.local. (37)
15:09:49.887947 ARP, Request who-has 192.168.0.199 tell 192.168.0.112, length 46
15:09:49.904743 IP 192.168.0.43.62249 > 239.255.255.250.1900: UDP, length 175
15:09:49.945946 ARP, Request who-has 192.168.0.198 tell 192.168.0.174, length 46
15:09:49.955180 IP6 fe80::468f:63c4:550f:d809.546 > ff02::1:2.547: dhcp6 solicit
15:09:49.980368 ARP, Request who-has 169.254.25.253 tell 0.0.0.0, length 46
15:09:49.980389 ARP, Request who-has 192.168.0.196 tell 0.0.0.0, length 46
```

3. sudo tcpdump -v -n

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -v -n
[sudo] password for lab1003:
tcpdump: listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:11:37.742348 IP (tos 0x0, ttl 1, id 43739, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.182.51145 > 239.255.255.250.1900: UDP, length 175
15:11:37.751716 IP (tos 0x0, ttl 128, id 43603, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.0.155.52125 > 192.168.0.33.7680: Flags [S], cksum 0x21e3 (correct), seq 3815965470, win 64240, options [mss 1460,nop,wscale 8,nop,n
op,sackOK], length 0
15:11:37.764287 IP (tos 0x0, ttl 1, id 57579, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.26.56615 > 239.255.255.250.1900: UDP, length 175
15:11:37.842000 IP6 (flowlabel 0xa7728, hlim 1, next-header UDP (17) payload length: 94) fe80::468f:63c4:550f:d809.546 > ff02::1:2.547: [udp su
m ok] dhcp6 solicit (xid=d11c90 (elapsed-time 301) (client-ID hwaddr/time type 1 time 706809801 489ebd9e7339) (IA_NA IAID:122199741 T1:0 T2:0)
(Client-FQDN) (vendor-class) (option-request vendor-specific-info DNS-server DNS-search-list Client-FQDN))
15:11:37.921709 IP (tos 0x0, ttl 128, id 60344, offset 0, flags [none], proto UDP (17), length 96)
    169.254.25.253.137 > 169.254.255.255.137: UDP, length 68
15:11:37.926830 IP (tos 0x0, ttl 1, id 54412, offset 0, flags [none], proto UDP (17), length 203)
    192.168.0.65.51108 > 239.255.255.250.1900: UDP, length 175
15:11:38.001456 IP6 (hlim 255, next-header ICMPv6 (58) payload length: 16) fe80::468f:63c4:550f:d809 > ff02::2: [icmp6 sum ok] ICMP6, router so
licitation, length 16
```

4. sudo tcpdump -n -e

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -n -e
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:13:40.303701 a4:ae:12:84:80:4d > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.14 tell 192.168.0.191, leng
th 46
15:13:40.325675 a4:ae:12:84:80:86 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.13 tell 192.168.0.140, leng
th 46
15:13:40.456432 20:88:10:84:96:a0 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.100 tell 192.168.0.118, len
gth 46
15:13:40.648507 ac:15:a2:b9:9e:29 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.165 tell 192.168.0.1, lengt
h 46
15:13:40.804854 a4:ae:12:84:80:4d > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.36 tell 192.168.0.191, leng
th 46
15:13:40.804871 a4:ae:12:84:80:4d > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.73 tell 192.168.0.191, leng
th 46
15:13:40.804872 a4:ae:12:84:80:4d > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.33 tell 192.168.0.191, leng
th 46
15:13:40.816442 04:0e:3c:19:2b:7b > 33:33:00:01:00:02, ethertype IPv6 (0x86dd), length 157: fe80::e184:c8cb:ee17:97a.546 > ff02::1:2.547: dhcp6
 solicit
15:13:40.918319 a4:ae:12:84:83:65 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.13 tell 192.168.0.195, leng
th 46
15:13:41.021201 20:88:10:84:96:a0 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Request who-has 192.168.0.100 tell 192.168.0.118, len
gth 46
```

5. sudo tcpdump –n tcp

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -n tcp
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:15:41.092902 IP 31.13.79.53.443 > 192.168.0.177.35516: Flags [P.], seq 909398290:909399608, ack 1139319493, win 2038, options [nop,nop,TS val 399922323 ecr 3692291971], length 1318
15:15:41.092957 IP 192.168.0.177.35516 > 31.13.79.53.443: Flags [.], ack 1318, win 2720, options [nop,nop,TS val 3692302852 ecr 399922323], length 0
15:15:41.214140 IP 192.168.0.177.35516 > 31.13.79.53.443: Flags [P.], seq 1:99, ack 1318, win 2728, options [nop,nop,TS val 3692302973 ecr 399922323], length 98
15:15:41.217167 IP 31.13.79.53.443 > 192.168.0.177.35516: Flags [.], ack 99, win 2038, options [nop,nop,TS val 399922448 ecr 3692302973], length 0
15:15:42.039633 IP 192.168.0.196.59250 > 192.168.0.33.7680: Flags [S], seq 352470751, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
15:15:42.419135 IP 192.168.0.177.35516 > 31.13.79.53.443: Flags [P.], seq 99:197, ack 1318, win 2728, options [nop,nop,TS val 3692304178 ecr 399922448], length 98
15:15:42.420911 IP 31.13.79.53.443 > 192.168.0.177.35516: Flags [.], ack 197, win 2038, options [nop,nop,TS val 399923651 ecr 3692304178], length 0
```

6. sudo tcpdump -n icmp

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -n icmp
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:18:08.288767 IP 192.168.0.177 > 192.168.0.1: ICMP 192.168.0.177 udp port 137 unreachable, length 86
15:18:08.300641 IP 192.168.0.177 > 192.168.0.1: ICMP 192.168.0.177 udp port 137 unreachable, length 86
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

7. sudo tcpdump -n src 172.16.92.1

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -n src 172.16.92.1
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

8. sudo tcpdump -n dst 172.16.92.1

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -n dst 172.16.92.1
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

9. sudo tcpdump -n port 80

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -n port 80
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:23:36.666790 IP 192.168.0.177.54890 > 185.125.190.96.80: Flags [S], seq 435535647, win 64240, options [mss 1460,sackOK,TS val 1928716699 ecr
 0,nop,wscale 7], length 0
15:23:36.799176 IP 185.125.190.96.80 > 192.168.0.177.54890: Flags [S.], seq 1032398175, ack 435535648, win 65160, options [mss 1440,sackOK,TS v
al 1173394848 ecr 1928716699,nop,wscale 7], length 0
15:23:36.799248 IP 192.168.0.177.54890 > 185.125.190.96.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 1928716831 ecr 1173394848], leng
th 0
15:23:36.799427 IP 192.168.0.177.54890 > 185.125.190.96.80: Flags [P.], seq 1:88, ack 1, win 502, options [nop,nop,TS val 1928716832 ecr 117339
4848], length 87: HTTP: GET / HTTP/1.1
15:23:36.931179 IP 185.125.190.96.80 > 192.168.0.177.54890: Flags [P.], seq 1:186, ack 88, win 509, options [nop,nop,TS val 1173394981 ecr 1928
716832], length 185: HTTP: HTTP/1.1 204 No Content
15:23:36.931204 IP 192.168.0.177.54890 > 185.125.190.96.80: Flags [.], ack 186, win 501, options [nop,nop,TS val 1928716963 ecr 1173394981], le
ngth 0
15:23:36.931293 IP 192.168.0.177.54890 > 185.125.190.96.80: Flags [F.], seq 88, ack 186, win 501, options [nop,nop,TS val 1928716963 ecr 117339
4981], length 0
15:23:36.931312 IP 185.125.190.96.80 > 192.168.0.177.54890: Flags [F.], seq 186, ack 88, win 509, options [nop,nop,TS val 1173394981 ecr 192871
6832], length 0
15:23:36.931318 IP 192.168.0.177.54890 > 185.125.190.96.80: Flags [.], ack 187, win 501, options [nop,nop,TS val 1928716964 ecr 1173394981], le
ngth 0
15:23:37.063018 IP 185.125.190.96.80 > 192.168.0.177.54890: Flags [.], ack 89, win 509, options [nop,nop,TS val 1173395112 ecr 1928716963], len
gth 0
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

10. sudo tcpdump port 80

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump port 80
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:53:15.745275 IP lab1003-OptiPlex-3020.59466 > 82.221.107.34.bc.googleusercontent.com.http: Flags [.], ack 197078827, win 501, options [nop,n
op,TS val 874295080 ecr 801145949], length 0
15:53:15.748129 IP 82.221.107.34.bc.googleusercontent.com.http > lab1003-OptiPlex-3020.59466: Flags [.], ack 1, win 261, options [nop,nop,TS va
l 801145952 ecr 874244004], length 0
15:53:16.002274 IP lab1003-OptiPlex-3020.59480 > 82.221.107.34.bc.googleusercontent.com.http: Flags [.], ack 570321776, win 501, options [nop,n
op,TS val 874295336 ecr 3108219291], length 0
15:53:16.004254 IP 82.221.107.34.bc.googleusercontent.com.http > lab1003-OptiPlex-3020.59480: Flags [.], ack 1, win 261, options [nop,nop,TS va
l 3108229529 ecr 874244271], length 0
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-OptiPlex-3020:~$
```

LibreOffice Writer

11. sudo tcpdump udp and src port 53

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump udp and src port 53
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:27:57.347928 IP _gateway.domain > lab1003-OptiPlex-3020.48636: 11455 1/0/1 A 31.13.79.53 (68)
15:27:57.348150 IP _gateway.domain > lab1003-OptiPlex-3020.45532: 49611 1/0/1 AAAA 2a03:2880:f22f:1c6:face:b00c:0:167 (80)
15:27:57.454023 IP _gateway.domain > lab1003-OptiPlex-3020.52250: 53668 NXDomain* 0/1/1 (114)
15:27:57.455729 IP _gateway.domain > lab1003-OptiPlex-3020.52250: 53668 NXDomain* 0/1/0 (103)
15:27:57.457182 IP _gateway.domain > lab1003-OptiPlex-3020.45894: 5139 NXDomain* 0/1/1 (112)
15:27:57.458887 IP _gateway.domain > lab1003-OptiPlex-3020.45894: 5139 NXDomain* 0/1/0 (101)
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
```

12. sudo tcpdump -n portrange 1-80

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -n portrange 1-80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:29:15.538722 IP 192.168.0.177.56815 > 192.168.0.1.53: 28384+ [1au] A? mmx-ds.cdn.whatsapp.net. (52)
15:29:15.538874 IP 192.168.0.177.48419 > 192.168.0.1.53: 1339+ [1au] AAAA? mmx-ds.cdn.whatsapp.net. (52)
15:29:15.540715 IP 192.168.0.1.53 > 192.168.0.177.56815: 28384 1/0/1 A 31.13.79.53 (68)
15:29:15.540893 IP 192.168.0.1.53 > 192.168.0.177.48419: 1339 1/0/1 AAAA 2a03:2880:f22f:1c6:face:b00c:0:167 (80)
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

13. sudo tcpdump -n src port 443

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -n src port 443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:30:12.249372 IP 31.13.79.53.443 > 192.168.0.177.35516: Flags [.], ack 1139344921, win 2038, options [nop,nop,TS val 400793482 ecr 3693174007
], length 0
15:30:12.445060 IP 31.13.79.53.443 > 192.168.0.177.35516: Flags [P.], seq 0:71, ack 1, win 2038, options [nop,nop,TS val 400793677 ecr 36931740
07], length 71
15:30:13.853130 IP 31.13.79.53.443 > 192.168.0.177.35516: Flags [P.], seq 71:350, ack 1, win 2038, options [nop,nop,TS val 400795085 ecr 369317
4204], length 279
15:30:15.063189 IP 31.13.79.53.443 > 192.168.0.177.35516: Flags [P.], seq 350:480, ack 1, win 2038, options [nop,nop,TS val 400796294 ecr 36931
75612], length 130
15:30:15.133964 IP 31.13.79.53.443 > 192.168.0.177.35516: Flags [.], ack 101, win 2038, options [nop,nop,TS val 400796366 ecr 3693176891], leng
th 0
15:30:15.246110 IP 31.13.79.53.443 > 192.168.0.177.35516: Flags [P.], seq 480:574, ack 101, win 2038, options [nop,nop,TS val 400796478 ecr 369
3176891], length 94
15:30:15.267343 IP 31.13.79.53.443 > 192.168.0.177.35516: Flags [.], ack 174, win 2038, options [nop,nop,TS val 400796500 ecr 3693177024], leng
th 0
^Z
[1]+  Stopped                 sudo tcpdump -n src port 443
lab1003@lab1003-OptiPlex-3020:~$
```

14. sudo tcpdump port 80 -w capture_file

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump port 80 -w capture_file
tcpdump: listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C26 packets captured
26 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-OptiPlex-3020:~$
```

15. sudo tcpdump -r capture_file

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -r capture_file
reading from file capture_file, link-type EN10MB (Ethernet)
lab1003@lab1003-OptiPlex-3020:~$
```

16. sudo tcpdump -nnvvS src 10.5.2.3 and dst port 3389

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -nnvvS src 10.5.2.3 and dst port 3389
tcpdump: listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-OptiPlex-3020:~$
```

17. sudo tcpdump -nvX src net 192.168.0.0/16 and dst net 10.0.0.0/8 or 172.16.0.0/16

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump -nvX src net 192.168.0.0/16 and dst net 10.0.0.0/8 or 172.16.0.0/16
tcpdump: listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-OptiPlex-3020:~$
```

18. sudo tcpdump 'src 10.0.2.4 and (dst port 3389 or 22)'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo  tcpdump 'src 10.0.2.4 and (dst port 3389 or 22)'
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-OptiPlex-3020:~$
```

19. sudo tcpdump 'tcp[13] & 32!=0'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump 'tcp[13] & 32!=0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-OptiPlex-3020:~$
```

20. sudo tcpdump 'tcp[13] & 16!=0'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump 'tcp[13] & 16!=0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:45:34.095812 IP whatsapp-cdn-shv-02-bom1.fbcdn.net.https > lab1003-OptiPlex-3020.35516: Flags [P.], seq 909501984:909502171, ack 1139369874,
 win 2038, options [nop,nop,TS val 401715330 ecr 3694094936], length 187
15:45:34.095844 IP lab1003-OptiPlex-3020.35516 > whatsapp-cdn-shv-02-bom1.fbcdn.net.https: Flags [.], ack 187, win 2724, options [nop,nop,TS va
l 3694095855 ecr 401715330], length 0
15:45:34.100847 IP lab1003-OptiPlex-3020.35516 > whatsapp-cdn-shv-02-bom1.fbcdn.net.https: Flags [P.], seq 1:73, ack 187, win 2728, options [no
p,nop,TS val 3694095860 ecr 401715330], length 72
15:45:34.102916 IP whatsapp-cdn-shv-02-bom1.fbcdn.net.https > lab1003-OptiPlex-3020.35516: Flags [.], ack 73, win 2038, options [nop,nop,TS val
 401715337 ecr 3694095860], length 0
15:45:35.111171 IP lab1003-OptiPlex-3020.35516 > whatsapp-cdn-shv-02-bom1.fbcdn.net.https: Flags [P.], seq 73:145, ack 187, win 2728, options [
nop,nop,TS val 3694096870 ecr 401715337], length 72
15:45:35.114643 IP whatsapp-cdn-shv-02-bom1.fbcdn.net.https > lab1003-OptiPlex-3020.35516: Flags [.], ack 145, win 2038, options [nop,nop,TS va
l 401716347 ecr 3694096870], length 0
15:45:35.190771 IP lab1003-OptiPlex-3020.35516 > whatsapp-cdn-shv-02-bom1.fbcdn.net.https: Flags [P.], seq 145:217, ack 187, win 2728, options
[nop,nop,TS val 3694096950 ecr 401716347], length 72
15:45:35.208854 IP whatsapp-cdn-shv-02-bom1.fbcdn.net.https > lab1003-OptiPlex-3020.35516: Flags [.], ack 217, win 2038, options [nop,nop,TS va
l 401716428 ecr 3694096950], length 0
^Z
[1]+  Stopped                 sudo tcpdump 'tcp[13] & 16!=0'
lab1003@lab1003-OptiPlex-3020:~$
```

21. sudo tcpdump 'tcp[13] & 8!=0'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump 'tcp[13] & 8!=0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:46:34.924454 IP whatsapp-cdn-shv-02-bom1.fbcdn.net.https > lab1003-OptiPlex-3020.35516: Flags [P.], seq 909504256:909504536, ack 1139371029,
 win 2038, options [nop,nop,TS val 401776159 ecr 3694145460], length 280
15:46:37.026907 IP lab1003-OptiPlex-3020.35516 > whatsapp-cdn-shv-02-bom1.fbcdn.net.https: Flags [P.], seq 1:73, ack 280, win 2728, options [no
p,nop,TS val 3694158786 ecr 401776159], length 72
^Z
[2]+  Stopped                 sudo tcpdump 'tcp[13] & 8!=0'
lab1003@lab1003-OptiPlex-3020:~$
```

22. sudo tcpdump 'tcp[13] & 4!=0'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo  tcpdump 'tcp[13] & 4!=0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

23. sudo tcpdump 'tcp[13] & 2!=0'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump 'tcp[13] & 2!=0'
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:18:46.609716 IP 192.168.0.166.50734 > 192.168.0.121.7680: Flags [S], seq 3031941878, win 64240, options [mss 1360,nop,wscale 8,nop,nop,sackO
K], length 0
15:18:46.625689 IP 192.168.0.166.50736 > 192.168.0.234.7680: Flags [S], seq 2455125911, win 64240, options [mss 1360,nop,wscale 8,nop,nop,sackO
K], length 0
15:18:46.701154 IP 192.168.0.166.52862 > 192.168.0.121.7680: Flags [S], seq 1140287803, win 64240, options [mss 1360,nop,wscale 8,nop,nop,sackO
K], length 0
15:18:48.298052 IP 192.168.0.166.51395 > 192.168.0.133.7680: Flags [S], seq 306942126, win 64240, options [mss 1360,nop,wscale 8,nop,nop,sackOK
], length 0
^C
4 packets captured
5 packets received by filter
0 packets dropped by kernel
```

24. sudo tcpdump 'tcp[13] & 1!=0'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump 'tcp[13] & 1!=0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-OptiPlex-3020:~$
```

25. sudo tcpdump 'tcp[13]=18'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump 'tcp[13] & 1!=0'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:23:29.211864 IP is-content-cache-1.ps5.canonical.com.http > lab1003-OptiPlex-3020.42134: Flags [F.], seq 3057788836, ack 3590279796, win 506
, options [nop,nop,TS val 3387316835 ecr 2686514136], length 0
15:23:29.212027 IP lab1003-OptiPlex-3020.42134 > is-content-cache-1.ps5.canonical.com.http: Flags [F.], seq 1, ack 1, win 501, options [nop,nop
,TS val 2686514274 ecr 3387316835], length 0
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

26. sudo tcpdump 'tcp[tcpflags] == tcp-syn'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump 'tcp[tcpflags] == tcp-syn'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:24:31.279986 IP 192.168.0.166.51024 > 192.168.0.121.7680: Flags [S], seq 4185928844, win 64240, options [mss 1360,nop,wscale 8,nop,nop,sackO
K], length 0
15:24:32.376268 IP 192.168.0.166.51024 > 192.168.0.121.7680: Flags [S], seq 4185928844, win 64240, options [mss 1360,nop,wscale 8,nop,nop,sackO
K], length 0
15:24:32.794678 IP 192.168.0.166.51022 > 192.168.0.117.7680: Flags [S], seq 1204231545, win 64240, options [mss 1360,nop,wscale 8,nop,nop,sackO
K], length 0
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

27. sudo tcpdump 'tcp[tcpflags] == tcp-rst'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump 'tcp[tcpflags] == tcp-rst'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-OptiPlex-3020:~$
```

28. sudo tcpdump 'tcp[tcpflags] == tcp-fin'

```
lab1003@lab1003-OptiPlex-3020:~$ sudo tcpdump 'tcp[tcpflags] == tcp-fin'
[sudo] password for lab1003:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
1 packet received by filter
0 packets dropped by kernel
lab1003@lab1003-OptiPlex-3020:~$
```

Conclusion: Explored the different network reconnaissance tools to gather information about networks (LO3 is achieved).