

Lab Assignment 7

AIM: Study of packet sniffer tools TCPDUMP.

LO3: Explore the different network reconnaissance tools to gather information about networks.

THEORY:

What is TCPDUMP and how to install it?

Tcpdump is a command-line packet analyzer that allows you to capture and analyze network traffic in real-time. It's commonly used for troubleshooting network issues, analyzing network behavior, and diagnosing problems related to network communication. tcpdump captures packets as they travel through a network interface and provides detailed information about each packet, including source and destination addresses, protocol information, payload data, and more.

Linux (Debian/Ubuntu):

Open a terminal and run the following command to install tcpdump:

```
sudo apt-get update
```

```
sudo apt-get install tcpdump
```

Explain various commands in tcpdump to capture different types of packets.

tcpdump provides a wide range of commands and options to capture and analyze different types of packets. Here are some common tcpdump commands and filters to capture specific types of packets:

1. Capture All Traffic on a Specific Interface:

```
sudo tcpdump -i eth0
```

This captures all traffic on the "eth0" network interface.

2. Capture Traffic to or from a Specific IP Address:

```
sudo tcpdump host 192.168.1.100
```

This captures all traffic to or from the IP address "192.168.1.100".

3. Capture Traffic on a Specific Port:

```
sudo tcpdump port 80
```

This captures all traffic on port 80.

4. Capture Traffic Using a Specific Protocol:

```
sudo tcpdump icmp
```

This captures ICMP (ping) traffic.

5. Capture Traffic from a Specific Source IP:

```
sudo tcpdump src 192.168.1.200
```

This captures traffic originating from IP address "192.168.1.200".

6. Capture Traffic to a Specific Destination IP:

```
sudo tcpdump dst 192.168.1.100
```

This captures traffic directed to IP address "192.168.1.100".

7. Capture Traffic on a Specific Port Using a Protocol:

```
sudo tcpdump udp port 53
```

This captures UDP traffic on port 53 (DNS).

8. Capture Traffic Using a Combination of Filters:

```
sudo tcpdump src 192.168.1.100 and port 22
```

This captures traffic originating from IP address "192.168.1.100" and using port 22 (SSH).

9. Capture Traffic with Specific Packet Size:

```
sudo tcpdump greater 1000
```

This captures packets larger than 1000 bytes.

10. Capture Specific Number of Packets:

```
sudo tcpdump -c 10
```

This captures 10 packets and then exits.

11. Capture Packets Using Hexadecimal Filter:

```
sudo tcpdump -X 'tcp[13] & 2 != 0'
```

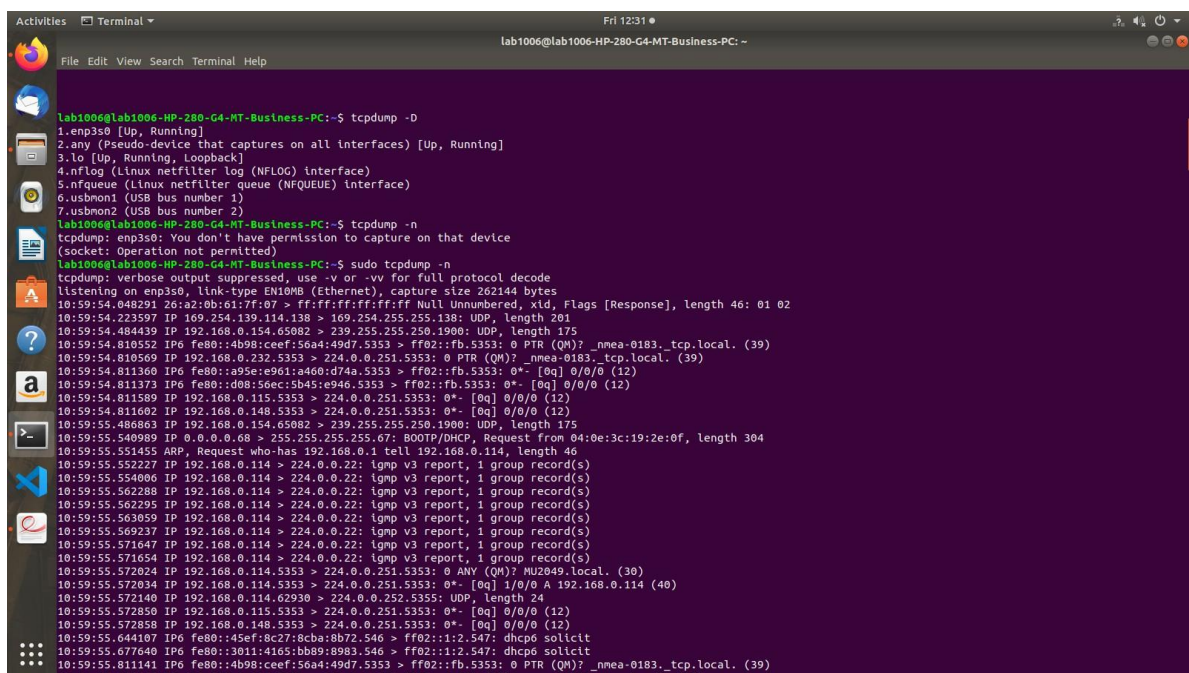
This captures only SYN packets (TCP packets with the SYN flag set).

12. Capture and Save Output to a File:

```
sudo tcpdump -i eth0 -w output.pcap
```

This captures traffic on the "eth0" interface and saves it to the "output.pcap" file.

OUTPUT



```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ tcpdump -D
1.enp3s0 [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)
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ tcpdump -n
tcpdump: enp3s0: You don't have permission to capture on that device
(socket: Operation not permitted)
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:59:54.048291 26:a2:0b:61:7f:07 > ff:ff:ff:ff:ff:ff Null Unnumbered, xid, Flags [Response], length 46: 01 02
10:59:54.223597 IP 169.254.139.114.138 > 169.254.255.255.138: UDP, length 201
10:59:54.484439 IP 192.168.0.154.65082 > 239.255.255.250.1900: UDP, length 175
10:59:54.810552 IP6 fe80::d09b:ceef:56a4:49d7:5353 > ff02::fb:5353: 0 PTR (QM)? nmea-0183_tcp.local. (39)
10:59:54.810569 IP 192.168.0.232.5353 > 224.0.0.251.5353: 0 PTR (QM)? nmea-0183_tcp.local. (39)
10:59:54.811360 IP6 fe80::a95e:e961:a400:d74a:5353 > ff02::fb:5353: 0*- [0q] 0/0/0 (12)
10:59:54.811373 IP6 fe80::d08:56ec:5b45:e946:5353 > ff02::fb:5353: 0*- [0q] 0/0/0 (12)
10:59:54.811589 IP 192.168.0.115.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
10:59:54.811602 IP 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
10:59:55.486863 IP 192.168.0.154.65082 > 239.255.255.250.1900: UDP, length 175
10:59:55.540989 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 04:0e:3c:19:2e:0f, length 304
10:59:55.551455 ARP, Request who-has 192.168.0.1 tell 192.168.0.114, length 46
10:59:55.552227 IP 192.168.0.114 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:59:55.554006 IP 192.168.0.114 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:59:55.562288 IP 192.168.0.114 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:59:55.562295 IP 192.168.0.114 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:59:55.563059 IP 192.168.0.114 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:59:55.569237 IP 192.168.0.114 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:59:55.571647 IP 192.168.0.114 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:59:55.571654 IP 192.168.0.114 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:59:55.572024 IP 192.168.0.114.5353 > 224.0.0.251.5353: 0 ANY (QM)? MUP209.local. (36)
10:59:55.572034 IP 192.168.0.114.5353 > 224.0.0.251.5353: 0*- [0q] 1/0/0 A 192.168.0.114 (40)
10:59:55.572140 IP 192.168.0.114.62930 > 224.0.0.252.5355: UDP, length 24
10:59:55.572850 IP 192.168.0.115.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
10:59:55.572858 IP 192.168.0.148.5353 > 224.0.0.251.5353: 0*- [0q] 0/0/0 (12)
10:59:55.644107 IP6 fe80::45ef:8c27:8cba:8b72:546 > ff02::12:547: dhcp6 solicit
10:59:55.677640 IP6 fe80::3011:4165:bb89:b983:546 > ff02::12:547: dhcp6 solicit
10:59:55.811141 IP6 fe80::d09b:ceef:56a4:49d7:5353 > ff02::fb:5353: 0 PTR (QM)? nmea-0183_tcp.local. (39)
10:59:55.811145 IP 192.168.0.232.5353 > 224.0.0.251.5353: 0 PTR (QM)? nmea-0183_tcp.local. (39)
```



```
10.8:SSH12? IP 102.168.0.141:80 > 2%0.0 SI JSJ: 0/- [0/ n/ 0 (2)
```



```
0 packets dropped by kernel
```



```
!=$ sudo tcpdump -v -n
```



```
command 'sudo' from deb sudo
```



```
See 'snap info <snapname>' for additional versions.
```



```
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
11:01:45.431136 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.240 tell 192.168.0.107, length 46  
11:01:45.431136 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.141 tell 192.168.0.107, length 46
```

```
11:01:46.097290 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.240 tell 192.168.0.107, length 46
```

```
11:01:46.108753 IP (tos 0x0, ttl 1, id 32933, offset 0, flags [none], proto UDP (17), length 203)  
11:01:46.108753 IP (tos 0x0, ttl 1, id 32933, offset 0, flags [none], proto UDP (17), length 203)
```



```
DB 63 03 J (ed tent T D head dr /line type 1 line 7 4 44 92727 0 4 0 e3C 19 ZB8) TA OA T A ID: 5 05 97436 T1: 0 T 2: 0 C lte nt PQDN J ve nd O r ed a 5 5 / apt ion reg ue 5 I DNS 5 ea ch l is I D NS S 8 F
```



```
11:00:18.105956 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:ff:Ta, ether type IPv4 (0x0800), length 288: (tos 0x0, ttl 1, id 620, offset 0, flags [none], proto UDP (17), length 204)
```

```
192.168.0.107:80 > 239.255.255.250:1900: UDP, length 176
```

```
11:06:49.943390 04:0e:3c:1a:60:2f > ff:ff:ff:ff:ff:ff, ether type ARP (0x0806), length 60: Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.0.141 tell 192.168.0.1
```



```
11:06:50.170534 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:ff, ether type IPv4 (0x0800), length 218: (tos 0x0, ttl 1, id 621, offset 0, flags [none], proto UDP (17), length 204)
```



```
11:06:50.584752 04:0e:3c:1b:bd:42 > ac:15:a2:b9:9e:29, ether type IPv4 (0x0800), length 185: (tos 0x0, ttl 64, id 15889, offset 0, flags [DF], proto TCP (6), length 91)  
192.168.0.213:51252 > 185.199.108.154:443: Flags [P.], cksum 0xe82c (incorrect -> 0xc33f), seq 1873020086:1873020047, ack 1011178678, win 4607, options [nop,nop,T
```

```
tz m so,oozz99 ac:Ts:a2:b9:9e:29 > 04:0e:3c:1b:bd:42, ether type IPv4 (0x0800), length 200: (tos 0x0, ttl 64, id 15889, offset 0, flags [DF], proto TCP (6), length 91)  
192.168.0.213:51252 > 185.199.108.154:443: Flags [P.], cksum 0xe82c (incorrect -> 0xc33f), seq 1873020086:1873020047, ack 1011178678, win 4607, options [nop,nop,T
```



```
11:06:50.675567 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:ff:Ta, ether type IPv4 (0x0800), length 500: (tos 0x0, ttl 2, id 37644, offset 0, flags [DF], proto UDP (17), length 486)
```

```
11:06:50.675836 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:ff, ether type IPv4 (0x0800), length 496: (tos 0x0, ttl 2, id 37642, offset 0, flags [DF], proto UDP (17), length 482)  
192.168.0.1.60033 > 239.255.255.250:1900: UDP, length 454
```



```
11:06:50.676187 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:ff:Ta, ether type IPv4 (0x0800), length 508: (tos 0x0, ttl 2, id 37644, offset 0, flags [DF], proto UDP (17), length 494)
```

```
192.168.0.1.60033 > 239.255.255.250:1900: UDP, length 466
```

```
11:06:50.676299 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:ff, ether type IPv4 (0x0800), length 490: (tos 0x0, ttl 2, id 37645, offset 0, flags [DF], proto UDP (17), length 476)
```

```
11:06:50.676669 ac:15:a2:b9:9e:29 > 01:00:5e:7f:ff:ff:Ta, ether type IPv4 (0x0800), length 492: (tos 0x0, ttl 2, id 37647, offset 0, flags [DF], proto UDP (17), length 478)
```

0

0 2 2 3 2.160.0.213.31992: Flags [P...cksum 0xdbc4 (car rec), seq 350114076+3501814901, ack 4276702204, u?n 77, Options nOp,nop,TS val 3554971416 e

?

11:00:57.451029 IP 192.168.0.213.31170: Flags [..] ack 0 u n 377, options [nop,nop,TS val 1305742873 ec 355589:1044,nop,nop,sack 1 (38.19) , leng

25 packets received by filter

Link type EN10MB (Ethernet), Capture size 262144 bytes

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s8, link-type EN10MB (Ethernet), capture size 262144 bytes
11:23:14.623598 IP 192.168.0.213 > 103.246.224.160: ICMP echo request, id 13898, seq 10, length 64

11:23:15.648227 IP 103.246.224.160 > 192.168.0.213: ICMP echo reply, id 13898, seq 11, length 64
11:23:16.671565 IP 192.168.0.213 > 103.246.224.160: ICMP echo request, id 13898, seq 12, length 64



M.??J:17.69094 IP M2.A8.OU • I#L246.24.10. 8f1B xho rvg al, lt W898, avg IJ, lngt 64

```
11 8 18 6IP 2.2.fl2i4.b .goo I=avr on nt. onftip • Cab1-6-H 780ttf1TJvai aa-PCM9J06: Na a [\, at 89, in 8#4, option [nop,nop,TS wat 1089842F8
```

```
so:to,al, ,A,A woot00Qiz,zb: oQ:lais,zsifo0:0,al, ,A,A zsoo:0QQ:z,zb:d4Q0:ia:suss:f0aQ:soar, ,A,A 2oQ0:0Q0:iz, 0ze0Q:ia:z,zsifo0:0,al, ,A, zvoQ:0Q0:z,zb:zeQ0:ia:
```

```
11 35:13:0 922035 IP 0.0.0.0.bootpc > 255.255.255.255.bootpc.1
```

```
*** 11:13:42 879208 11: gateway.domain > 11: lab1006-HP-280-G4-MT-Business-PC.417207 3089 1/0/1 AAAA 2:04:6800:4009:82b:1:2003 (72)
```

```
Activities Terminal
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
11:35:42.744434 IP lab1006-HP-280-G4-MT-Business-PC.55375 > _gateway.domain: 35292+ [1au] A? apis.google.com. (44)
11:35:42.744508 IP lab1006-HP-280-G4-MT-Business-PC.47730 > _gateway.domain: 45730+ [1au] AAAA? apis.google.com. (44)
11:35:42.745662 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.55375: 35292 2/0/1 CNAME plus.l.google.com., A 142.251.42.78 (81)
11:35:42.745668 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.47730: 45730 2/0/1 CNAME plus.l.google.com., AAAA 2404:6800:4009:831::200e (93)
11:35:42.845172 IP lab1006-HP-280-G4-MT-Business-PC.55210 > _gateway.domain: 48143+ [1au] A? adservice.google.com. (49)
11:35:42.845258 IP lab1006-HP-280-G4-MT-Business-PC.51043 > _gateway.domain: 27592+ [1au] AAAA? adservice.google.com. (49)
11:35:42.846395 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.55210: 48143 1/0/1 A 142.250.192.98 (65)
11:35:42.846733 IP lab1006-HP-280-G4-MT-Business-PC.39609 > _gateway.domain: 31102+ [1au] A? safebrowsing.googleapis.com. (56)
11:35:42.846788 IP lab1006-HP-280-G4-MT-Business-PC.48992 > _gateway.domain: 03325+ [1au] AAAA? safebrowsing.googleapis.com. (56)
11:35:42.847895 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.48992: 03325 1/0/1 AAAA 2404:6800:4009:823::200a (84)
11:35:42.847898 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.39609: 31102 1/0/1 A 142.250.183.186 (72)
11:35:42.850258 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.51043: 27592 1/0/1 AAAA 2404:6800:4009:820::2002 (77)
11:35:43.014836 IP lab1006-HP-280-G4-MT-Business-PC.43491 > _gateway.domain: 41945+ [1au] A? adservice.google.co.in. (51)
11:35:43.014910 IP lab1006-HP-280-G4-MT-Business-PC.35711 > _gateway.domain: 33071+ [1au] AAAA? adservice.google.co.in. (51)
11:35:43.015190 IP lab1006-HP-280-G4-MT-Business-PC.54633 > _gateway.domain: 59138+ [1au] A? googleads.g.doubleclick.net. (56)
11:35:43.015221 IP lab1006-HP-280-G4-MT-Business-PC.34413 > _gateway.domain: 1007+ [1au] AAAA? googleads.g.doubleclick.net. (56)
11:35:43.016017 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.43491: 41945 2/0/1 CNAME pagead46.l.doubleclick.net., A 142.250.192.34 (107)
11:35:43.016055 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.35711: 33071 2/0/1 CNAME pagead46.l.doubleclick.net., AAAA 2404:6800:4009:823::2002 (119)
11:35:43.016261 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.54633: 59138 1/0/1 A 142.250.199.130 (72)
11:35:43.039586 IP _gateway.domain > lab1006-HP-280-G4-MT-Business-PC.34413: 1087 1/0/1 AAAA 2404:6800:4009:82c::2002 (84)
11:35:45.130757 IP 0.0.0.0.bootpc > 255.255.255.255.bootpc: BOOTP/DHCP, Request from 04:0e:3c:1a:5c:74 (out Unknown), length 300
^C
38 packets captured
38 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump port 80 -w capture_1
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C86 packets captured
86 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -nnvv5 src 10.5.2.3 and dst port 3389
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -nnvv5 src 103.246.224.160 and dst port 3389
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ tcpdump 'tcp[13] & 32!=0'
tcpdump: enp3s0: You don't have permission to capture on that device
(socket: Operation not permitted)
```