Network and System Administration Lab

Lab Assignment: Performing various options of Tcpdump in terminal

Vimal Thomson

Roll no: 40

RMCA-B Sem-II

You need to be root to run tcpdump. It includes many options and filters. Running tcpdump without any options will capture all packets flowing through the default interface. To see the list of network interfaces available on the system and on which tcpdump can capture packets.

Command: Sudo tcpdump -D

```
vimalthomson@vimal-thomson:~$ sudo tcpdump -D
1.wlo1 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.enp2s0 [Up]
5.bluetooth-monitor (Bluetooth Linux Monitor) [none]
6.nflog (Linux netfilter log (NFLOG) interface) [none]
7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
8.bluetooth0 (Bluetooth adapter number 0) [none]
```

Command: Sudo tcpdump host 8.8.8.8

```
vimalthomson@vimal-thomson:~$ sudo tcpdump host 8.8.8.8
[sudo] password for vimalthomson:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes

^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

Command: sudo tcpdump –I any –c 5 port 80

```
vimalthomson@vimal-thomson:~$ sudo tcpdump -i any -c 5 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
12:13:26.007976 IP vimal-thomson.mshome.net.35960 > 82.221.107.34.bc.googleusercontent.com.http: F
12:13:26.267744 IP 82.221.107.34.bc.googleusercontent.com.http > vimal-thomson.mshome.net.35960: F
12:13:28.824027 IP vimal-thomson.mshome.net.56478 > maa05s22-in-f3.1e100.net.http: Flags [.], ack
12:13:28.865945 IP maa05s22-in-f3.1e100.net.http > vimal-thomson.mshome.net.56478: Flags [.], ack
12:13:29.591975 IP vimal-thomson.mshome.net.39454 > 117.18.237.29.http: Flags [.], ack 2293278109,
5 packets captured
8 packets received by filter
0 packets dropped by kernel
```

Command: sudo tcpdump –I wlo1

```
vimalthomson@vimal-thomson:~$ sudo tcpdump -i wlo1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
12:13:45.362539 IP 82.221.107.34.bc.googleusercontent.com.http > vimal-thomson.mshome.net.35956: Flags [.], ack 4174885558,
12:13:45.363622 IP vimal-thomson.mshome.net.33113 > LAPTOP-U2SEQKP4.mshome.net.domain: 16557+ PTR? 35.137.168.192.in-addr.a
12:13:45.694020 IP LAPTOP-U2SEQKP4.mshome.net.domain > vimal-thomson.mshome.net.33113: 16557- 1/0/0 PTR vimal-thomson.mshom
12:13:45.695434 IP vimal-thomson.mshome.net.43682 > LAPTOP-U2SEQKP4.mshome.net.domain: 23165+ PTR? 1.137.168.192.in-addr.ar
12:13:45.705315 IP LAPTOP-U2SEQKP4.mshome.net.domain > vimal-thomson.mshome.net.43682: 23165- 1/0/0 PTR LAPTOP-U2SEQKP4.msh
12:13:46.235520 IP vimal-thomson.mshome.net.52402 > 65.8.80.90.https: Flags [P.], seq 2714391647:2714391686, ack 1264927035
12:13:46.235657 IP vimal-thomson.mshome.net.60914 > ec2-35-164-91-82.us-west-2.compute.amazonaws.com.https: Flags [F.], seq
ength 0
12:13:46.236136 IP vimal-thomson.mshome.net.40846 > LAPTOP-U2SEQKP4.mshome.net.domain: 41615+ PTR? 90.80.8.65.in-addr.arpa.
12:13:46.551982 IP vimal-thomson.mshome.net.52402 > 65.8.80.90.https: Flags [P.], seq 0:39, ack 1, win 501, options [nop,no
12:13:46.614252 IP LAPTOP-U2SEQKP4.mshome.net.51450 > 239.255.255.250.1900: UDP, length 173
12:13:46.614264 IP ec2-35-164-91-82.us-west-2.compute.amazonaws.com.https > vimal-thomson.mshome.net.60914: Flags [.], ack
12:13:46.614285 IP vimal-thomson.mshome.net.60914 > ec2-35-164-91-82.us-west-2.compute.amazonaws.com.https: Flags [.], ack
12:13:46.614294 IP 65.8.80.90.https > vimal-thomson.mshome.net.52402: Flags [.], ack 39, win 135, options [nop,nop,TS val 2
12:13:46.614304 IP 65.8.80.90.https > vimal-thomson.mshome.net.52402: Flags [P.], seq 1:40, ack 39, win 135, options [nop,n
12:13:46.614310 IP vimal-thomson.mshome.net.52402 > 65.8.80.90.https: Flags [.], ack 40, win 501, options [nop,nop,TS val 2
12:13:46.630592 IP LAPTOP-U2SEQKP4.mshome.net.51454 > 239.255.255.250.1900: UDP, length 173
```

Command: sudo tcpdump –c 5 –I wlo1 –n –A port 80

```
vimalthomson@vimal-thomson:~$ sudo tcpdump -c 5 -i wlo1 -n -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
12:14:50.999973 IP 192.168.137.35.56478 > 142.250.182.131.80: Flags [.], ack 382654594, win 501, options [nop,nop,TS val 2844057322 ecr 2613070546], length 0
E..4..@.@.....#.......P.................
.....J.
12:14:51.042148 IP 142.250.182.131.80 > 192.168.137.35.56478: Flags [.], ack 1, win 265, options [nop,nop,TS val 2613080756 ecr 2843944324], length 0
E..4....9. r.......#.P.............     )E.....
..r...%.
12:14:53.560060 IP 192.168.137.35.56480 > 142.250.182.131.80: Flags [.], ack 72505591, win 501, options [nop,nop,TS val 2844059882 ecr 3563992377], length 0
E..4.y@.@.....#.......P..FN.RX..........
.....n59
12:14:53.560100 IP 192.168.137.35.56476 > 142.250.182.131.80: Flags [.], ack 2608649050, win 501, options [nop,nop,TS val 2844059882 ecr 2625550507], length 0
E..4.1@.@..I...#.......PC"...|.Z....._.....
....~..
12:14:53.560242 IP 192.168.137.35.39454 > 117.18.237.29.80: Flags [.], ack 2293278109, win 501, options [nop,nop,TS val 1537812176 ecr 3541123674], length 0
E..4.T@.@..s...#u......P..KB.........].....
[.&...BZ
5 packets captured
6 packets received by filter
0 packets dropped by kernel
```

Command: sudo tcpdump –r icmp.pcap

```
vimalthomson@vimal-thomson:~$ sudo tcpdump -r icmp.pcap
reading from file icmp.pcap, link-type EN10MB (Ethernet)
12:36:27.787721 IP 142.250.82.18.19305 > 192.168.43.30.53597: UDP, length 254
12:36:27.787746 IP 142.250.82.18.19305 > 192.168.43.30.53597: UDP, length 254
12:36:27.787749 IP 142.250.82.18.19305 > 192.168.43.30.53597: UDP, length 133
12:36:27.787752 IP 142.250.82.18.19305 > 192.168.43.30.53597: UDP, length 254
12:36:27.787756 IP 142.250.82.18.19305 > 192.168.43.30.53597: UDP, length 254
12:36:27.787759 IP 142.250.82.18.19305 > 192.168.43.30.53597: UDP, length 254
12:36:27.787763 IP 142.250.82.18.19305 > 192.168.43.30.53597: UDP, length 254
12:36:27.787765 IP 142.250.82.18.19305 > 192.168.43.30.53597: UDP, length 254
12:36:27.787769 IP 142.250.82.18.19305 > 192.168.43.30.53597: UDP, length 254
12:36:27.787772 IP 142.250.82.18.19305 > 192.168.43.30.53597: UDP, length 254
```

Command: sudo tcpdump –I wlo1 not icmp