Networking & System Administration Lab

NIMISHA JAMES

RMCA-B S2

ROLL NO:11

Q. Execute tcpdump and its options on your own system, and submit the output screenshot as a document.

- **apt install tcpdump**

```
File  Actions  Edit  View  Help

┌──(root💀kali)-[~]
└─# apt install tcpdump
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  ettercap-common ettercap-graphical libluajit-5.1-2 libluajit-5.1-common python3-qrcode
Use 'apt autoremove' to remove them.
The following packages will be upgraded:
  tcpdump
1 upgraded, 0 newly installed, 0 to remove and 814 not upgraded.
Need to get 466 kB of archives.
After this operation, 1,024 B of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 tcpdump amd64 4.99.1-3 [466 kB]
Fetched 466 kB in 7s (62.8 kB/s)
(Reading database ... 312901 files and directories currently installed.)
Preparing to unpack .../tcpdump_4.99.1-3_amd64.deb ...
Unpacking tcpdump (4.99.1-3) over (4.99.0-2) ...
Setting up tcpdump (4.99.1-3) ...
Installing new version of config file /etc/apparmor.d/usr.bin.tcpdump ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.2.3) ...
```

- **tcpdump**

```
┌──(root💀kali)-[~]
└─# tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
02:43:21.754837 ARP, Request who-has 192.168.192.217 (96:2d:01:da:8e:4a (oui Unknown)) tell 192.168.192.61, length 46
02:43:21.760206 ARP, Reply 192.168.192.217 is-at 96:2d:01:da:8e:4a (oui Unknown), length 46
02:43:21.849449 IP 192.168.192.254.41299 > 192.168.192.217.domain: 17304+ PTR? 217.192.168.192.in-addr.arpa. (46)
02:43:22.084082 IP 192.168.192.217.domain > 192.168.192.254.41299: 17304 NXDomain 0/0/0 (46)
02:43:22.084462 IP 192.168.192.254.59375 > 192.168.192.217.domain: 18006+ PTR? 61.192.168.192.in-addr.arpa. (45)
02:43:22.201501 IP 192.168.192.217.domain > 192.168.192.254.59375: 18006 NXDomain 0/0/0 (45)
02:43:22.201958 IP 192.168.192.254.56453 > 192.168.192.217.domain: 5023+ PTR? 254.192.168.192.in-addr.arpa. (46)
02:43:22.276058 IP 192.168.192.217.domain > 192.168.192.254.56453: 5023 NXDomain 0/0/0 (46)
02:43:25.752676 IP 192.168.192.61.59058 > sb-in-f188.1e100.net.https: Flags [.], seq 2091335895:2091335896, ack 4181321158, win 259, length 1
02:43:25.832062 IP 192.168.192.254.35986 > 192.168.192.217.domain: 21037+ PTR? 188.130.125.74.in-addr.arpa. (45)
02:43:26.172346 IP sb-in-f188.1e100.net.https > 192.168.192.61.59058: Flags [.], ack 1, win 265, options [nop,nop,sack 1 {0:1}], length 0
02:43:26.172348 IP 192.168.192.217.domain > 192.168.192.254.35986: 21037 1/0/0 PTR sb-in-f188.1e100.net. (79)
02:43:27.801975 ARP, Request who-has 192.168.192.217 tell 192.168.192.254, length 28
02:43:27.808941 ARP, Reply 192.168.192.217 is-at 96:2d:01:da:8e:4a (oui Unknown), length 46
02:43:29.074389 ARP, Request who-has 192.168.192.254 tell 192.168.192.217, length 46
02:43:29.074413 ARP, Reply 192.168.192.254 is-at 08:00:27:0e:34:8d (oui Unknown), length 28
02:43:30.921286 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [S], seq 3237987242, win 65535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
02:43:30.923227 IP 192.168.192.254.33085 > 192.168.192.217.domain: 44360+ PTR? 9.173.189.20.in-addr.arpa. (43)
02:43:31.187098 IP 192.168.192.217.domain > 192.168.192.254.33085: 44360 NXDomain 0/1/0 (129)
02:43:31.289465 IP 20.189.173.9.https > 192.168.192.61.49488: Flags [S.], seq 4132866116, ack 3237987243, win 65535, options [mss 1360,nop,wscale 8,nop,nop,sackOK], length 0
02:43:31.289535 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [.], ack 1, win 1024, length 0
02:43:31.290040 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [P.], seq 1:230, ack 1, win 1024, length 229
02:43:32.028761 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [P.], seq 1:230, ack 1, win 1024, length 229
02:43:33.108010 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [P.], seq 1:230, ack 1, win 1024, length 229
02:43:33.647058 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [.], ack 2721, win 1024, length 0
02:43:33.647063 IP 20.189.173.9.https > 192.168.192.61.49488: Flags [.], seq 1:2721, ack 230, win 2049, length 2720
02:43:33.648654 IP 20.189.173.9.https > 192.168.192.61.49488: Flags [P.], seq 5441:6210, ack 230, win 2049, length 769
02:43:33.648656 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [.], ack 2721, win 1024, options [nop,nop,sack 1 {5441:6210}], length 0
02:43:33.648657 IP 20.189.173.9.https > 192.168.192.61.49488: Flags [.], seq 2721:4081, ack 230, win 2049, length 1360
02:43:33.648765 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [.], ack 4081, win 1024, options [nop,nop,sack 1 {5441:6210}], length 0
02:43:33.650175 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [.], ack 6210, win 1024, length 0
02:43:33.650177 IP 20.189.173.9.https > 192.168.192.61.49488: Flags [.], seq 4081:5441, ack 230, win 2049, length 1360
02:43:33.656752 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [P.], seq 230:388, ack 6210, win 1024, length 158
02:43:33.922214 IP 20.189.173.9.https > 192.168.192.61.49488: Flags [P.], seq 6210:6261, ack 388, win 2049, length 51
02:43:33.922216 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [.], ack 6261, win 1023, length 0
02:43:33.923291 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [P.], seq 388:846, ack 6261, win 1023, length 458
02:43:34.257572 IP 20.189.173.9.https > 192.168.192.61.49488: Flags [P.], seq 6261:6315, ack 846, win 2047, length 54
02:43:34.257574 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [.], seq 846:2206, ack 6315, win 1023, length 1360
02:43:34.596276 IP 20.189.173.9.https > 192.168.192.61.49488: Flags [.], ack 2206, win 2050, length 0
02:43:34.596279 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [P.], seq 2206:3761, ack 6315, win 1023, length 1555
02:43:34.907308 IP 20.189.173.9.https > 192.168.192.61.49488: Flags [.], ack 3761, win 2050, length 0
02:43:34.907311 IP 20.189.173.9.https > 192.168.192.61.49488: Flags [P.], seq 6315:6673, ack 3761, win 2050, length 358
02:43:34.907973 IP 192.168.192.61.49488 > 20.189.173.9.https: Flags [.], ack 6673, win 1022, length 0
02:44:11.161263 IP 192.168.192.61.59058 > sb-in-f188.1e100.net.https: Flags [.], seq 0:1, ack 1, win 259, length 1
02:44:11.419463 IP sb-in-f188.1e100.net.https > 192.168.192.61.59058: Flags [.], ack 1, win 265, options [nop,nop,sack 1 {0:1}], length 0
02:44:16.230215 IP 219.144.247.35.bc.googleusercontent.com.https > 192.168.192.61.60531: Flags [P.], seq 2729959343:2729959374, ack 2617887749, win 160, length 31
02:44:16.231067 IP 192.168.192.61.60531 > 219.144.247.35.bc.googleusercontent.com.https: Flags [P.], seq 1:32, ack 31, win 260, length 31
```

- **tcpdump -c 5**


┌──(root💀kali)-[~]
└─# tcpdump -c 5
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
02:47:55.673849 IP6 2402:3a80:192a:d074:cdba:41bc:9cc3:a70c.65489 > maa05s10-in-x03.1e100.net.https: Flags [P.], seq 643730137:643730226, ack 3511030239, win 256, length 89
02:47:55.673853 IP6 2402:3a80:192a:d074:cdba:41bc:9cc3:a70c.65489 > maa05s10-in-x03.1e100.net.https: Flags [P.], seq 89:128, ack 1, win 256, length 39
02:47:55.673853 IP6 2402:3a80:192a:d074:cdba:41bc:9cc3:a70c.65489 > maa05s10-in-x03.1e100.net.https: Flags [P.], seq 128:287, ack 1, win 256, length 159
02:47:55.673854 IP6 2402:3a80:192a:d074:cdba:41bc:9cc3:a70c.65489 > maa05s10-in-x03.1e100.net.https: Flags [P.], seq 287:738, ack 1, win 256, length 451
02:47:55.727630 IP 192.168.192.254.34854 > 192.168.192.217.domain: 30522+ PTR? 3.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.8.0.7.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa. (90)
5 packets captured
54 packets received by filter
0 packets dropped by kernel