NETWORKING & SYSTEM ADMINISTRATION LAB

Name: Manya Madhu

Roll No: 17

Batch: S2 RMCA B

Date: 06-06-2022

Experiment No: 25

Aim

TCP dump

Procedure

Commands:

$ sudo update && sudo apt install tcpdump

```
mca@S17:~$ sudo apt update && sudo apt install tcpdump
Hit:1 http://in.archive.ubuntu.com/ubuntu bionic InRelease
Err:2 http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease
  403  Forbidden [IP: 185.125.190.52 80]
Ign:3 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 InRelease
Hit:4 http://ppa.launchpad.net/pasgui/ppa/ubuntu bionic InRelease
Hit:5 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Get:6 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release [2,495 B]
Get:7 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release.gpg [801 B]
Err:7 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release.gpg
  The following signatures were invalid: EXPKEYSIG 58712A2291FA4AD5 MongoDB 3.6 Release Signing Key <packaging@mongodb.com>
Reading package lists... Done
E: Failed to fetch http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu/dists/bionic/InRelease  403  Forbidden [IP: 185.125.190.52 80]
E: The repository 'http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease' is no longer signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: ht
tps://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release: The following signatures were invalid: EXPKEYSIG 58712A2291FA4AD5 MongoDB 3.
6 Release Signing Key <packaging@mongodb.com>
```

$sudo tcpdump

```
mca@S17:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:16:09.416440 IP 192.168.6.175.58403 > 239.255.255.250.1900: UDP, length 174
15:16:09.419398 IP S17.60448 > dns.google.domain: 31139+ [1au] PTR? 175.6.168.192.in-addr.arpa. (55)
15:16:09.435252 IP dns.google.domain > S17.60448: 31139 NXDomain 0/0/1 (55)
15:16:09.437415 IP S17.35566 > dns.google.domain: 23314+ [1au] PTR? 17.6.168.192.in-addr.arpa. (54)
15:16:09.453159 IP 192.168.6.184.60587 > 239.255.255.250.1900: UDP, length 175
15:16:09.453470 IP dns.google.domain > S17.35566: 23314 NXDomain 0/0/1 (54)
15:16:09.454730 IP S17.40853 > dns.google.domain: 40615+ [1au] PTR? 184.6.168.192.in-addr.arpa. (55)
15:16:09.470026 IP dns.google.domain > S17.40853: 40615 NXDomain 0/0/1 (55)
15:16:09.657785 IP 192.168.6.204.54368 > 239.255.255.250.1900: UDP, length 137
15:16:09.658495 IP S17.59438 > dns.google.domain: 36231+ [1au] PTR? 204.6.168.192.in-addr.arpa. (55)
15:16:09.673754 IP 192.168.6.204.54368 > 239.255.255.250.1900: UDP, length 137
```

Terminal

$ sudo tcpdump –D

```
mca@S17:~$ sudo tcpdump -D
1.enp3s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.docker0 [Up]
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
9.usbmon3 (USB bus number 3)
10.usbmon4 (USB bus number 4)
```

$ sudo tcpdump –i enp3s0

```
mca@S17:~$ sudo tcpdump -i enp3s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:17:24.107401 IP 192.168.6.214.56506 > 239.255.255.250.1900: UDP, length 175
15:17:24.110378 IP S17.49527 > dns.google.domain: 54720+ [1au] PTR? 214.6.168.192.in-addr.arpa. (55)
15:17:24.121946 IP 192.168.6.218.54761 > 239.255.255.250.1900: UDP, length 174
15:17:24.127123 IP dns.google.domain > S17.49527: 54720 NXDomain 0/0/1 (55)
15:17:24.129257 IP S17.55046 > dns.google.domain: 6002+ [1au] PTR? 17.6.168.192.in-addr.arpa. (54)
15:17:24.145609 IP dns.google.domain > S17.55046: 6002 NXDomain 0/0/1 (54)
15:17:24.146902 IP S17.38453 > dns.google.domain: 17470+ [1au] PTR? 218.6.168.192.in-addr.arpa. (55)
15:17:24.160148 IP 192.168.6.36.53084 > 239.255.255.250.1900: UDP, length 171
```

$ sudo tcpdump –c n –I enp3s0

```
mca@S17:~$ sudo tcpdump -c 4 -i enp3s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:17:39.956993 IP 192.168.6.236.64986 > 192.168.6.255.6866: UDP, length 397
15:17:39.958385 IP S17.42251 > dns.google.domain: 29063+ [1au] PTR? 255.6.168.192.in-addr.arpa. (55)
15:17:39.968377 ARP, Request who-has 192.168.6.95 tell _gateway, length 46
15:17:39.975468 IP dns.google.domain > S17.42251: 29063 NXDomain 0/0/1 (55)
4 packets captured
13 packets received by filter
4 packets dropped by kernel
```

$ sudo tcpdump –xx –I enp3s0

```
mca@S17:~$ sudo tcpdump -XX -i enp3s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:18:04.341111 STP 802.1w, Rapid STP, Flags [Forward], bridge-id 8000.44:31:92:f1:18:5b.800b, length 47
        0x0000:  0180 c200 0000 4431 92f1 1867 0027 4242  ......D1...g.'BB
        0x0010:  0300 0002 022c 8000 0836 c916 1d25 0000  .....,...6...%..
        0x0020:  4e34 8000 4431 92f1 185b 800b 0200 1400  N4..D1...[......
        0x0030:  0200 0f00 0000 0000 0000 0000 0000 0000  ................
15:18:04.372404 ARP, Request who-has 192.168.6.115 tell _gateway, length 46
        0x0000:  ffff ffff ffff 001a 8c6b 54cf 0806 0001  .........kT.....
        0x0010:  0800 0604 0001 001a 8c6b 54cf c0a8 0664  .........kT....d
        0x0020:  0000 0000 0000 c0a8 0673 0000 0000 0000  .........s......
        0x0030:  0000 0000 0000 0000 0000 0000            ............
```

$ sudo tcpdump –i enp3s0 -c n port 80

```
mca@S17:~$ sudo tcpdump -i enp3s0 -c 5 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^Z
[2]+  Stopped                 sudo tcpdump -i enp3s0 -c 5 port 80
```

$ sudo tcpdump –i enp3s0 icmp

```
mca@S17:~$ sudo tcpdump -i enp3s0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
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
```

$ sudo tcpdump –i enp3s0 –c n –w icmp.pcap

```
mca@S17:~$ sudo tcpdump -i enp3s0 -c 10 -w icmp.pcap
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
11 packets received by filter
0 packets dropped by kernel
```

$ tcpdump –r icmp.pcap

```
mca@S17:~$ tcpdump -r icmp.pcap
reading from file icmp.pcap, link-type EN10MB (Ethernet)
14:19:34.588656 IP 192.168.6.69.57897 > 239.255.255.250.1900: UDP, length 175
14:19:34.758231 IP 192.168.6.190.37933 > 239.255.255.250.1900: UDP, length 172
14:19:34.858312 IP 192.168.6.26.48314 > 239.255.255.250.1900: UDP, length 171
14:19:35.183628 STP 802.1w, Rapid STP, Flags [Forward], bridge-id 8000.44:31:92:f1:18:5b.800b, length 47
14:19:35.198678 IP 192.168.6.240.50951 > 239.255.255.250.1900: UDP, length 175
14:19:35.207025 IP 192.168.6.236.57798 > 192.168.6.255.6866: UDP, length 395
14:19:35.492596 IP6 fe80::184b:57ad:c86c:fda7.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
14:19:35.748433 IP 169.254.95.210.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 78:48:59:b4:5f:d3 (oui Unknown), length 334
14:19:35.758881 IP 192.168.6.190.37933 > 239.255.255.250.1900: UDP, length 172
14:19:35.862400 IP 192.168.6.226.48303 > 239.255.255.250.1900: UDP, length 171
```