NETWORKING & SYSTEM ADMINISTRATION LAB

Name: vismaya

Roll No: 54

Batch: B

Date: 06-06-2022

Experiment No: 25

Aim

TCP dump

Procedure

Commands:

$ sudo update && sudo apt install tcpdump

```
mca@T70:~$ sudo apt update && sudo apt install tcpdump
[sudo] password for mca:
Hit:1 https://dl.google.com/linux/chrome/deb stable InRelease
Err:2 http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease
  403  Forbidden [IP: 185.125.190.52 80]
Hit:3 http://archive.ubuntu.com/ubuntu bionic InRelease
Hit:4 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Reading package lists... Done
E: Failed to fetch http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu/dists/bionic/InRelease  403  Forbid
E: The repository 'http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease' is no longer sign
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.
```

$sudo tcpdump

```
mca@T70:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:01:53.549197 ARP, Request who-has 192.168.6.74 tell 192.168.6.74, length 46
16:01:53.550464 IP T70.60114 > dns.google.domain: 9671+ [1au] PTR? 74.6.168.192.in-addr.arpa. (5
16:01:53.566399 IP dns.google.domain > T70.60114: 9671 NXDomain 0/0/1 (54)
16:01:53.566557 IP T70.60114 > dns.google.domain: 9671+ PTR? 74.6.168.192.in-addr.arpa. (43)
16:01:53.581393 IP 192.168.6.179.netbios-ns > 192.168.6.255.netbios-ns: NBT UDP PACKET(137): QUE
16:01:53.581402 IP 192.168.6.179.netbios-ns > 192.168.6.255.netbios-ns: NBT UDP PACKET(137): QUE
16:01:53.582366 IP dns.google.domain > T70.60114: 9671 NXDomain 0/0/0 (43)
16:01:53.584599 IP T70.60883 > dns.google.domain: 8450+ [1au] PTR? 224.6.168.192.in-addr.arpa. (
16:01:53.619617 IP T70.51401 > dns.google.domain: 25502+ [1au] PTR? 255.6.168.192.in-addr.arpa.
16:01:53.635040 IP dns.google.domain > T70.51401: 25502 NXDomain 0/0/1 (55)
16:01:53.635189 IP T70.51401 > dns.google.domain: 25502+ PTR? 255.6.168.192.in-addr.arpa. (44)
16:01:53.745625 IP 192.168.6.180.63159 > 239.255.255.250.1900: UDP, length 175
16:01:53.747126 IP T70.34227 > dns.google.domain: 32960+ [1au] PTR? 180.6.168.192.in-addr.arpa.
16:01:53.762596 IP dns.google.domain > T70.34227: 32960 NXDomain 0/0/1 (55)
16:01:53.762750 IP T70.34227 > dns.google.domain: 32960+ PTR? 180.6.168.192.in-addr.arpa. (44)
16:01:53.778211 IP dns.google.domain > T70.34227: 32960 NXDomain 0/0/0 (44)
16:01:53.786645 IP 192.168.6.170.51346 > 239.255.255.250.1900: UDP, length 174
16:01:53.787136 IP T70.59731 > dns.google.domain: 1664+ [1au] PTR? 170.6.168.192.in-addr.arpa. (
16:01:53.787143 IP 192.168.6.170.51347 > 239.255.255.250.1900: UDP, length 175
16:01:53.803792 IP dns.google.domain > T70.59731: 1664 NXDomain 0/0/1 (55)
16:01:53.803965 IP T70.59731 > dns.google.domain: 1664+ PTR? 170.6.168.192.in-addr.arpa. (44)
```

$ sudo tcpdump –D

```
mca@T70:~$ sudo tcpdump -D
1.enp5s0 [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)
```

$ sudo tcpdump –i enp3s0

```
mca@T70:~$ sudo tcpdump -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:03:11.794249 STP 802.1s, Rapid STP, CIST Flags [Learn, Forward, Agreement], length 102
16:03:11.796457 ARP, Request who-has 192.168.1.1 tell 192.168.1.1, length 46
16:03:11.797854 IP T70.49153 > dns.google.domain: 4479+ [1au] PTR? 1.1.168.192.in-addr.arp
16:03:11.798558 ARP, Reply 192.168.1.1 is-at d8:94:03:38:83:40 (oui Unknown), length 46
16:03:11.813081 IP dns.google.domain > T70.49153: 4479 NXDomain 0/0/1 (53)
16:03:11.813242 IP T70.49153 > dns.google.domain: 4479+ PTR? 1.1.168.192.in-addr.arpa. (42
16:03:11.828513 IP dns.google.domain > T70.49153: 4479 NXDomain 0/0/0 (42)
16:03:11.830754 IP T70.50050 > dns.google.domain: 54198+ [1au] PTR? 224.6.168.192.in-addr.
16:03:11.845960 IP dns.google.domain > T70.50050: 54198 NXDomain 0/0/1 (55)
16:03:12.034442 IP 192.168.6.210.58557 > 239.255.255.250.1900: UDP, length 172
16:03:12.035026 IP T70.34131 > dns.google.domain: 21219+ [1au] PTR? 250.255.255.239.in-add
16:03:12.037437 IP6 fe80::8d2c:e415:e2b3:99cb.58418 > ff02::1:3.hostmon: UDP, length 22
16:03:12.037451 IP 192.168.6.203.58418 > 224.0.0.252.hostmon: UDP, length 22
16:03:12.049804 IP dns.google.domain > T70.34131: 21219 NXDomain 0/1/1 (114)
16:03:12.049962 IP T70.34131 > dns.google.domain: 21219+ PTR? 250.255.255.239.in-addr.arpa
16:03:12.064779 IP dns.google.domain > T70.34131: 21219 NXDomain 0/1/0 (103)
16:03:12.104338 IP T70.53978 > dns.google.domain: 4073+ [1au] PTR? 203.6.168.192.in-addr.a
16:03:12.121562 IP dns.google.domain > T70.53978: 4073 NXDomain 0/0/1 (55)
16:03:12.121722 IP T70.53978 > dns.google.domain: 4073+ PTR? 203.6.168.192.in-addr.arpa. (
16:03:12.154861 IP 192.168.6.192.mdns > 224.0.0.251.mdns: 0 PTR (QM)? _googlecast._tcp.loc
```

$ sudo tcpdump –c n –I enp3s0

```
mca@T70:~$ sudo tcpdump -c 5 -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:06:31.154996 IP 192.168.6.205.54726 > 239.255.255.250.1900: UDP, length 175
16:06:31.155468 IP T70.60003 > dns.google.domain: 13571+ [1au] PTR? 250.255.255.239.in-addr.arpa. (57)
16:06:31.172707 IP dns.google.domain > T70.60003: 13571 NXDomain 0/1/1 (114)
16:06:31.172795 IP T70.60003 > dns.google.domain: 13571+ PTR? 250.255.255.239.in-addr.arpa. (46)
16:06:31.175674 ARP, Request who-has 192.168.6.69 tell _gateway, length 46
5 packets captured
24 packets received by filter
13 packets dropped by kernel
mca@T70:~$ sudo tcpdump -XX -i enp5s0
```

$ sudo tcpdump –xx –I enp3s0

```
mca@T70:~$ sudo tcpdump -XX -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:07:18.869329 IP 192.168.6.93.54370 > 239.255.255.250.1900: UDP, length 174
        0x0000:  0100 5e7f fffa 0c9d 920f 6be2 0800 4500  ..^.......k...E.
        0x0010:  00ca 94ed 0000 0111 6d36 c0a8 065d efff  ........m6...]..
        0x0020:  fffa d462 076c 00b6 7108 4d2d 5345 4152  ...b.l..q.M-SEAR
        0x0030:  4348 202a 2048 5454 502f 312e 310d 0a48  CH.*.HTTP/1.1..H
        0x0040:  4f53 543a 2032 3339 2e32 3535 2e32 3535  OST:.239.255.255
        0x0050:  2e32 3530 3a31 3930 300d 0a4d 414e 3a20  .250:1900..MAN:.
        0x0060:  2273 7364 703a 6469 7363 6f76 6572 220d  "ssdp:discover".
        0x0070:  0a4d 583a 2031 0d0a 5354 3a20 7572 6e3a  .MX:.1..ST:.urn:
        0x0080:  6469 616c 2d6d 756c 7469 7363 7265 656e  dial-multiscreen
        0x0090:  2d6f 7267 3a73 6572 7669 6365 3a64 6961  -org:service:dia
        0x00a0:  6c3a 310d 0a55 5345 522d 4147 454e 543a  l:1..USER-AGENT:
        0x00b0:  2047 6f6f 676c 6520 4368 726f 6d65 2f31  .Google.Chrome/1
        0x00c0:  3032 2e30 2e35 3030 352e 3633 2057 696e  02.0.5005.63.Win
        0x00d0:  646f 7773 0d0a 0d0a                      dows....
16:07:18.872069 IP T70.50730 > dns.google.domain: 11863+ [1au] PTR? 93.6.168.192.in-addr.arpa
        0x0000:  001a 8c6b 54cf 0c9d 920e 9127 0800 4500  ...kT......'..E.
```

$ sudo tcpdump –i enp3s0 -c n port 80

```
mca@T70:~$ sudo tcpdump -i enp5s0 -c 5 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^Z
[4]+  Stopped                 sudo tcpdump -i enp5s0 -c 5 port 80
```

$ sudo tcpdump –i enp3s0 icmp

```
mca@T70:~$ sudo tcpdump -i enp5s0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^Z
[5]+  Stopped                 sudo tcpdump -i enp5s0 icmp
```

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

```
mca@T70:~$ sudo tcpdump -i enp5s0 -c 10 -w icmp.pcap
tcpdump: listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
18 packets received by filter
0 packets dropped by kernel
```

$ tcpdump –r icmp.pcap