NETWORKING & SYSTEM ADMINISTRATION LAB

Name: VYSHNAVI BABU S

Roll No: 55

Batch: MCA B

Date: 06-06-2022

Experiment No: 24

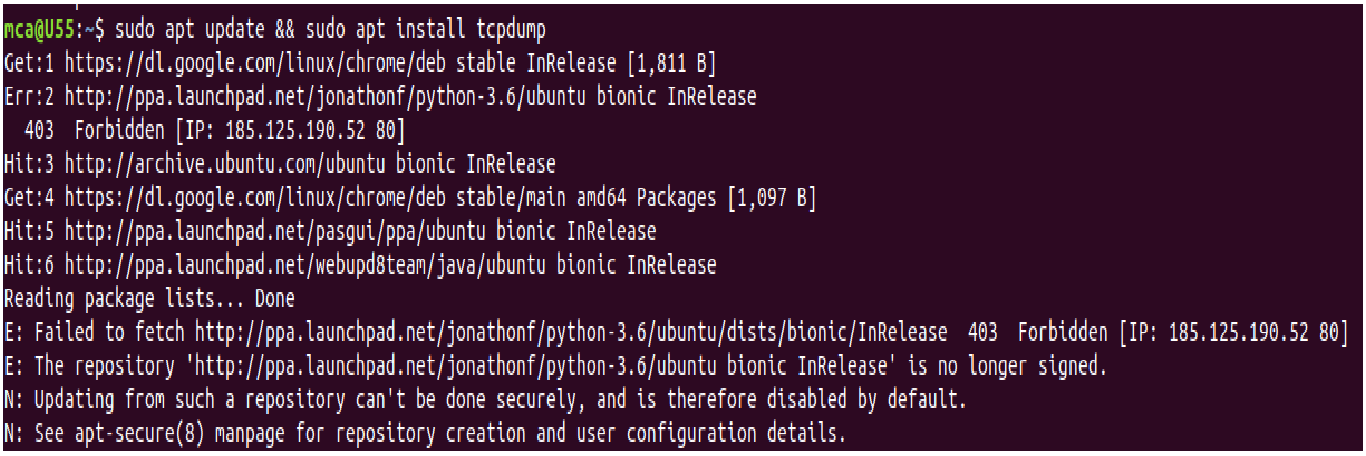
Aim

TCP dump

Procedure

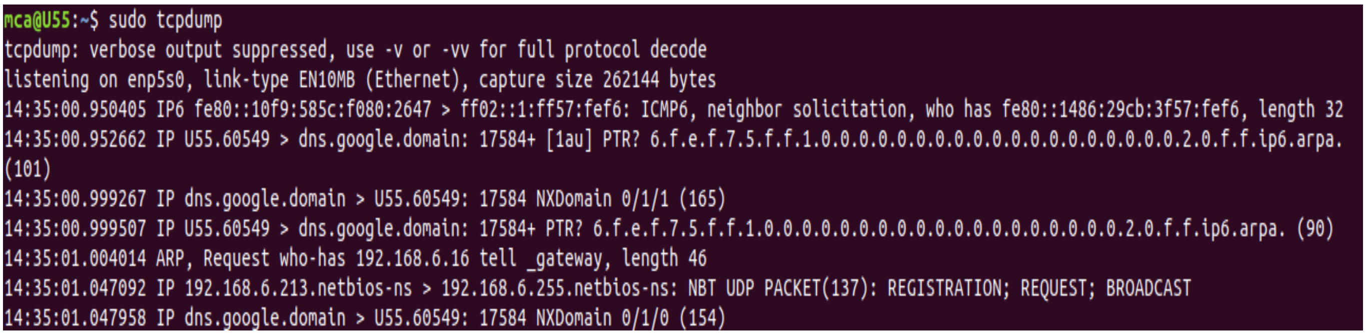
Commands:

$ sudo apt update && sudo apt install tcpdump



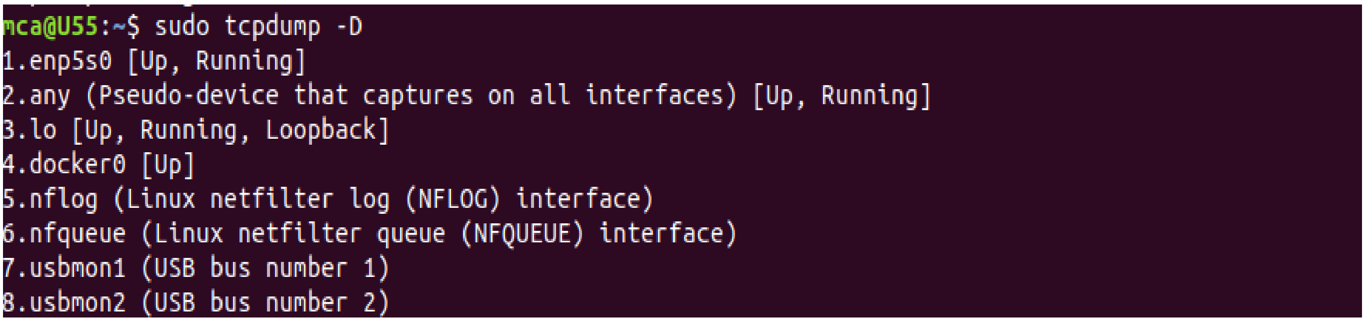
```
mca@U55:~$ sudo apt update && sudo apt install tcpdump
Get:1 https://dl.google.com/linux/chrome/deb stable InRelease [1,811 B]
Err:2 http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease
  403  Forbidden [IP: 185.125.190.52 80]
Hit:3 http://archive.ubuntu.com/ubuntu bionic InRelease
Get:4 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,097 B]
Hit:5 http://ppa.launchpad.net/pasgui/ppa/ubuntu bionic InRelease
Hit:6 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  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.
```

$sudo tcpdump



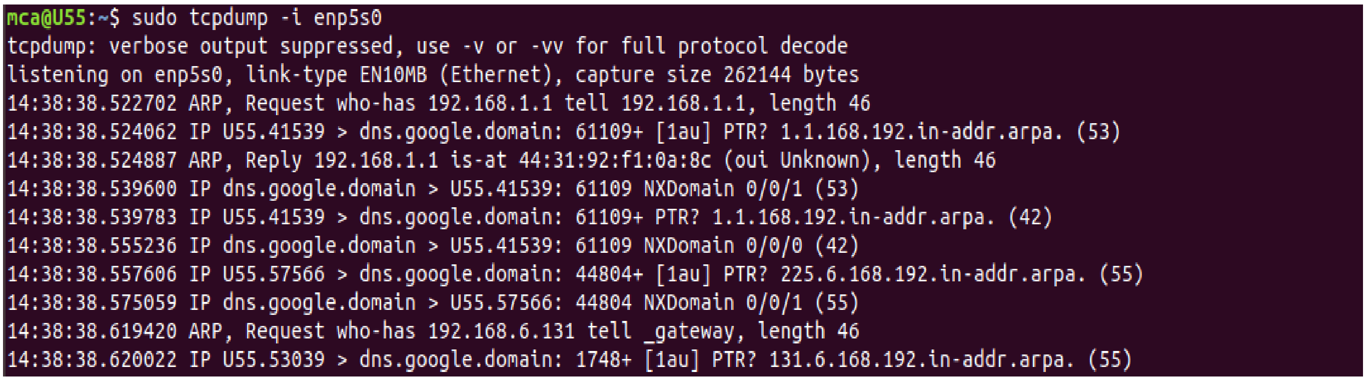
```
mca@U55:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:35:00.950405 IP6 fe80::10f9:585c:f080:2647 > ff02::1:ff57:fef6: ICMP6, neighbor solicitation, who has fe80::1486:29cb:3f57:fef6, length 32
14:35:00.952662 IP U55.60549 > dns.google.domain: 17584+ [1au] PTR? 6.f.e.f.7.5.f.f.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (101)
14:35:00.999267 IP dns.google.domain > U55.60549: 17584 NXDomain 0/1/1 (165)
14:35:00.999507 IP U55.60549 > dns.google.domain: 17584+ PTR? 6.f.e.f.7.5.f.f.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
14:35:01.004014 ARP, Request who-has 192.168.6.16 tell _gateway, length 46
14:35:01.047092 IP 192.168.6.213.netbios-ns > 192.168.6.255.netbios-ns: NBT UDP PACKET(137): REGISTRATION; REQUEST; BROADCAST
14:35:01.047958 IP dns.google.domain > U55.60549: 17584 NXDomain 0/1/0 (154)
```

$ sudo tcpdump -D



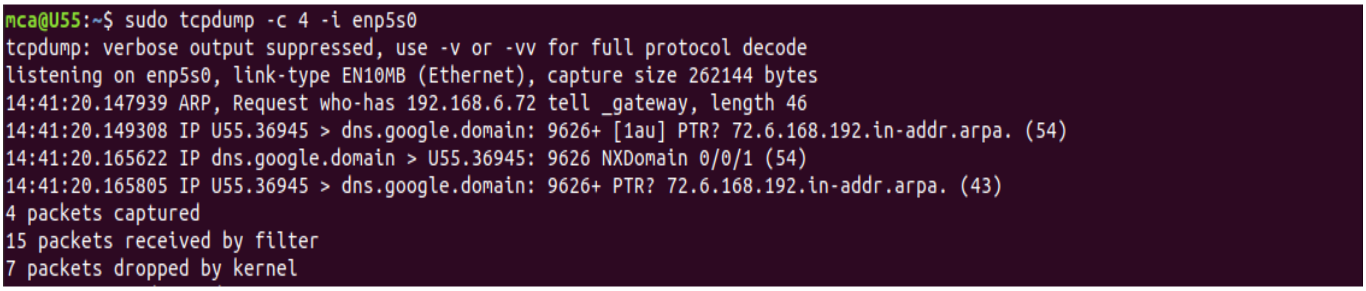
```
mca@U55:~$ sudo tcpdump -D
1.enp5s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.docker0 [Up]
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
```

$ sudo tcpdump -i enp5s0



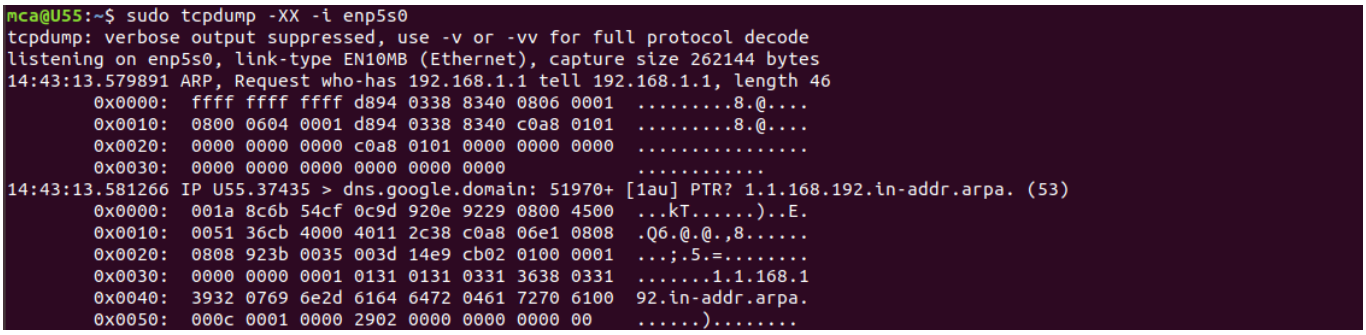
```
mca@U55:~$ sudo tcpdump -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:38:38.522702 ARP, Request who-has 192.168.1.1 tell 192.168.1.1, length 46
14:38:38.524062 IP U55.41539 > dns.google.domain: 61109+ [1au] PTR? 1.1.168.192.in-addr.arpa. (53)
14:38:38.524887 ARP, Reply 192.168.1.1 is-at 44:31:92:f1:0a:8c (oui Unknown), length 46
14:38:38.539600 IP dns.google.domain > U55.41539: 61109 NXDomain 0/0/1 (53)
14:38:38.539783 IP U55.41539 > dns.google.domain: 61109+ PTR? 1.1.168.192.in-addr.arpa. (42)
14:38:38.555236 IP dns.google.domain > U55.41539: 61109 NXDomain 0/0/0 (42)
14:38:38.557606 IP U55.57566 > dns.google.domain: 44804+ [1au] PTR? 225.6.168.192.in-addr.arpa. (55)
14:38:38.575059 IP dns.google.domain > U55.57566: 44804 NXDomain 0/0/1 (55)
14:38:38.619420 ARP, Request who-has 192.168.6.131 tell _gateway, length 46
14:38:38.620022 IP U55.53039 > dns.google.domain: 1748+ [1au] PTR? 131.6.168.192.in-addr.arpa. (55)
```

$ sudo tcpdump -c n -i enp3s0



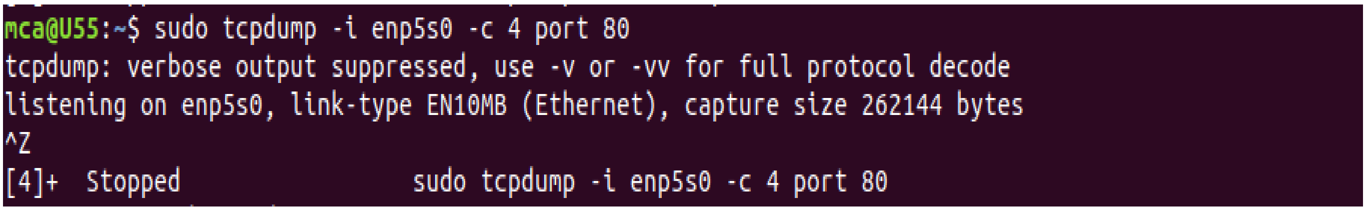
```
mca@U55:~$ sudo tcpdump -c 4 -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:41:20.147939 ARP, Request who-has 192.168.6.72 tell _gateway, length 46
14:41:20.149308 IP U55.36945 > dns.google.domain: 9626+ [1au] PTR? 72.6.168.192.in-addr.arpa. (54)
14:41:20.165622 IP dns.google.domain > U55.36945: 9626 NXDomain 0/0/1 (54)
14:41:20.165805 IP U55.36945 > dns.google.domain: 9626+ PTR? 72.6.168.192.in-addr.arpa. (43)
4 packets captured
15 packets received by filter
7 packets dropped by kernel
```

$ sudo tcpdump -XX -i enp5s0



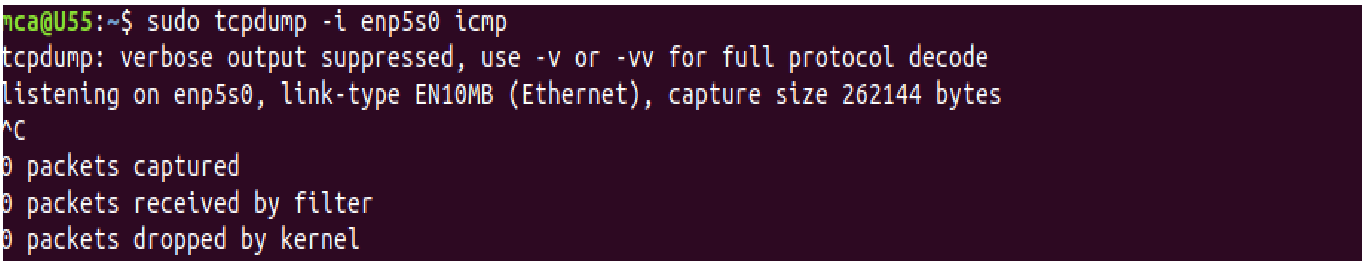
```
mca@U55:~$ sudo tcpdump -XX -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:43:13.579891 ARP, Request who-has 192.168.1.1 tell 192.168.1.1, length 46
        0x0000:  ffff ffff ffff d894 0338 8340 0806 0001  .........8.@....
        0x0010:  0800 0604 0001 d894 0338 8340 c0a8 0101  .........8.@....
        0x0020:  0000 0000 0000 c0a8 0101 0000 0000 0000  ................
        0x0030:  0000 0000 0000 0000 0000 0000            ............
14:43:13.581266 IP U55.37435 > dns.google.domain: 51970+ [1au] PTR? 1.1.168.192.in-addr.arpa. (53)
        0x0000:  001a 8c6b 54cf 0c9d 920e 9229 0800 4500  ...kT......)..E.
        0x0010:  0051 36cb 4000 4011 2c38 c0a8 06e1 0808  .Q6.@.@.,8......
        0x0020:  0808 923b 0035 003d 14e9 cb02 0100 0001  ...;.5.=........
        0x0030:  0000 0000 0001 0131 0131 0331 3638 0331  .......1.1.168.1
        0x0040:  3932 0769 6e2d 6164 6472 0461 7270 6100  92.in-addr.arpa.
        0x0050:  000c 0001 0000 2902 0000 0000 0000 00    ......)........
```

$ sudo tcpdump -i enp5s0 -c n port 80



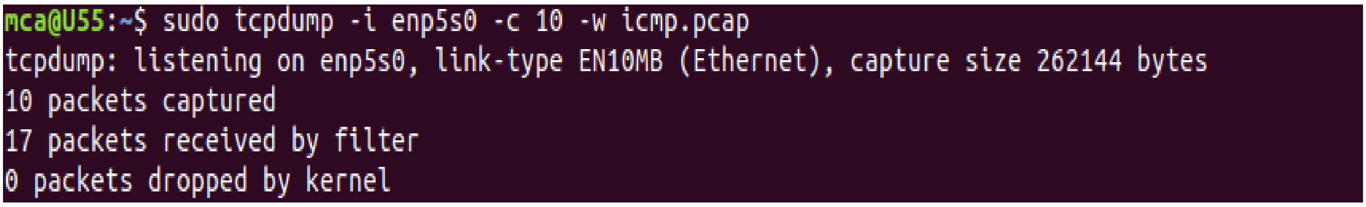
```
mca@U55:~$ sudo tcpdump -i enp5s0 -c 4 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^Z
[4]+  Stopped                 sudo tcpdump -i enp5s0 -c 4 port 80
```

$ sudo tcpdump -i enp5s0 icmp



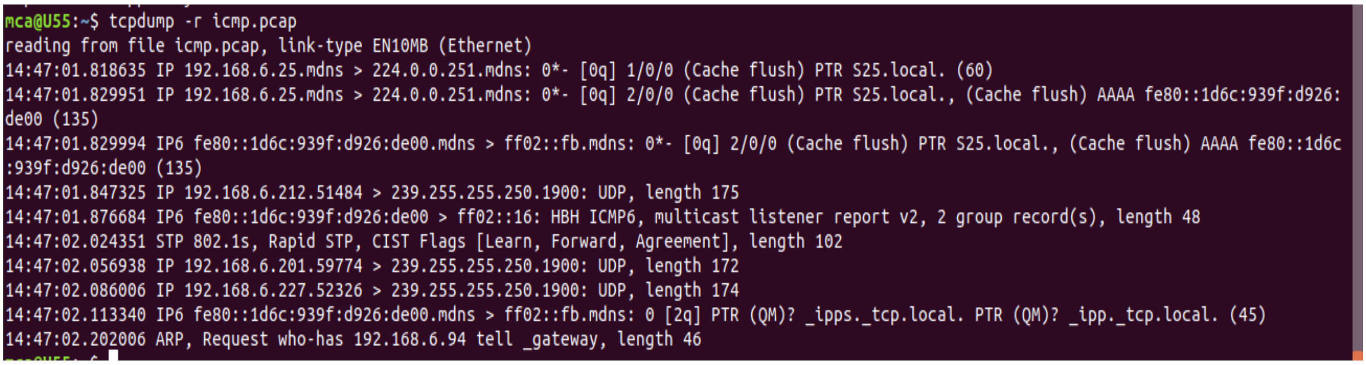
```
mca@U55:~$ sudo tcpdump -i enp5s0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

$ sudo tcpdump -i enp5s0 -c n -w icmp.pcap



```
mca@U55:~$ sudo tcpdump -i enp5s0 -c 10 -w icmp.pcap
tcpdump: listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
17 packets received by filter
0 packets dropped by kernel
```

$ tcpdump -r icmp.pcap



```
mca@U55:~$ tcpdump -r icmp.pcap
reading from file icmp.pcap, link-type EN10MB (Ethernet)
14:47:01.818635 IP 192.168.6.25.mdns > 224.0.0.251.mdns: 0*- [0q] 1/0/0 (Cache flush) PTR S25.local. (60)
14:47:01.829951 IP 192.168.6.25.mdns > 224.0.0.251.mdns: 0*- [0q] 2/0/0 (Cache flush) PTR S25.local., (Cache flush) AAAA fe80::1d6c:939f:d926:
de00 (135)
14:47:01.829994 IP6 fe80::1d6c:939f:d926:de00.mdns > ff02::fb.mdns: 0*- [0q] 2/0/0 (Cache flush) PTR S25.local., (Cache flush) AAAA fe80::1d6c
:939f:d926:de00 (135)
14:47:01.847325 IP 192.168.6.212.51484 > 239.255.255.250.1900: UDP, length 175
14:47:01.876684 IP6 fe80::1d6c:939f:d926:de00 > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
14:47:02.024351 STP 802.1s, Rapid STP, CIST Flags [Learn, Forward, Agreement], length 102
14:47:02.056938 IP 192.168.6.201.59774 > 239.255.255.250.1900: UDP, length 172
14:47:02.086006 IP 192.168.6.227.52326 > 239.255.255.250.1900: UDP, length 174
14:47:02.113340 IP6 fe80::1d6c:939f:d926:de00.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
14:47:02.202006 ARP, Request who-has 192.168.6.94 tell _gateway, length 46
```