Lab 1

Name- Adarsh Nandanwar
BITS ID- 2018A7PS0396G

tcpdump

```
(base) adarshnandanwar@predator-pop-os:~$ sudo tcpdump
[sudo] password for adarshnandanwar:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
20:39:34.692884 IP6 fe80::ca25:e1ff:fed4:fe44 > ff02::1:ff45:a182: ICMP6, neighbor solicitation, who has fe80::c6e9:aff:fe45:a182, length 32
20:39:34.693811 IP6 predator-pop-os.59721 > fe80::c6e9:aff:fe45:a182.domain: 54504+ [1au] PTR? 2.8.1.a.5.4.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)
20:39:35.100456 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.59721: 54504 NXDomain 0/1/1 (165)
20:39:35.100635 IP6 predator-pop-os.59721 > fe80::c6e9:aff:fe45:a182.domain: 54504+ PTR? 2.8.1.a.5.4.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)
20:39:35.105002 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.59721: 54504 NXDomain 0/1/0 (154)
20:39:35.105839 IP6 predator-pop-os.59008 > fe80::c6e9:aff:fe45:a182.domain: 60158+ [1au] PTR? 4.4.e.f.4.d.e.f.f.f.1.e.5.2.a.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (101)
20:39:35.114409 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.59008: 60158 NXDomain* 0/1/1 (150)
20:39:35.114536 IP6 predator-pop-os.59008 > fe80::c6e9:aff:fe45:a182.domain: 60158+ PTR? 4.4.e.f.4.d.e.f.f.f.1.e.5.2.a.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
20:39:35.120458 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.59008: 60158 NXDomain* 0/1/0 (139)
20:39:35.121240 IP6 predator-pop-os.50109 > fe80::c6e9:aff:fe45:a182.domain: 53662+ [1au] PTR? 2.8.1.a.5.4.e.f.f.f.a.0.9.e.6.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (101)
20:39:35.130247 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.50109: 53662 NXDomain* 0/1/1 (150)
20:39:35.130381 IP6 predator-pop-os.50109 > fe80::c6e9:aff:fe45:a182.domain: 53662+ PTR? 2.8.1.a.5.4.e.f.f.f.a.0.9.e.6.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
20:39:35.157832 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.50109: 53662 NXDomain* 0/1/0 (139)
20:39:35.158695 IP6 predator-pop-os.50121 > fe80::c6e9:aff:fe45:a182.domain: 31842+ [1au] PTR? 3.1.7.9.8.9.2.6.8.4.0.2.5.f.b.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (101)
20:39:35.164835 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.50121: 31842 NXDomain* 0/1/1 (150)
20:39:35.164959 IP6 predator-pop-os.50121 > fe80::c6e9:aff:fe45:a182.domain: 31842+ PTR? 3.1.7.9.8.9.2.6.8.4.0.2.5.f.b.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
20:39:35.181545 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.50121: 31842 NXDomain* 0/1/0 (139)
20:39:35.304321 IP 192.168.0.189.6537 > 255.255.255.255.6537: UDP, length 121
20:39:35.305210 IP6 predator-pop-os.39771 > fe80::c6e9:aff:fe45:a182.domain: 39149+ [1au] PTR? 189.0.168.192.in-addr.arpa. (55)
20:39:35.311977 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.39771: 39149 NXDomain* 0/1/1 (110)
20:39:35.312084 IP6 predator-pop-os.39771 > fe80::c6e9:aff:fe45:a182.domain: 39149+ PTR? 189.0.168.192.in-addr.arpa. (44)
20:39:35.323940 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.39771: 39149 NXDomain* 0/1/0 (99)
20:39:35.509118 IP 192.168.0.189.6537 > 255.255.255.255.6537: UDP, length 121
20:39:35.618249 IP predator-pop-os.Dlink.50630 > 192.168.0.189.8009: Flags [P.], seq 2468592839:2468592949, ack 2115181467, win 501, options [nop,nop,TS val 2194725192 ecr 3363086], length 110
20:39:35.618524 IP6 predator-pop-os.46922 > fe80::c6e9:aff:fe45:a182.domain: 48051+ [1au] PTR? 195.0.168.192.in-addr.arpa. (55)
20:39:35.621151 IP 192.168.0.189.8009 > predator-pop-os.Dlink.50630: Flags [P.], seq 1:111, ack 110, win 1408, options [nop,nop,TS val 3364086 ecr 2194725192], length 110
20:39:35.621159 IP predator-pop-os.Dlink.50630 > 192.168.0.189.8009: Flags [.], ack 111, win 501, options [nop,nop,TS val 2194725195 ecr 3364086], length 0
20:39:35.621239 IP6 fe80::c6e9:aff:fe45:a182.domain > predator-pop-os.46922: 48051* 1/0/1 PTR predator-pop-os.Dlink. (90)
20:39:35.713956 IP 192.168.0.189.6537 > 255.255.255.255.6537: UDP, length 121
^C
29 packets captured
29 packets received by filter
0 packets dropped by kernel
```

- dumps traffic or TCP/IP packets on a network
- In the output line from left to right
    1. Timestamp
    2. protocol (e.g. IP)
    3. source hostname/IP along with the port number
    4. destination hostname/IP along with the port number
    5. TCP Flags. Theses are some combination of S (SYN), F (FIN), P (PUSH), R (RST), U (URG), W (ECN CWR), E (ECN-Echo) or '.' (ACK), or 'none' if no flags are set.
    6. Data sequence number. Data-seqno describes the portion of sequence space covered by the data in this packet
    7. Acknowledgement number. It is sequence number of the next data expected the other direction on this connection.
    8. Window size. This is number of bytes of receive buffer space available the other direction on this connection.
    9. TCP options
    10. Len or length of the data payload.

ifconfig

```
(base) adarshnandanwar@predator-pop-os:~$ ifconfig
enp3s0f1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 98:28:a6:03:9d:dc  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 325927  bytes 128524181 (128.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 325927  bytes 128524181 (128.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.195  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fd01::ffde:6d5b:7412:4eda  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::cbf5:2048:6298:9713  prefixlen 64  scopeid 0x20<link>
        inet6 fd01::c6da:f4cd:74df:c32f  prefixlen 64  scopeid 0x0<global>
        ether 98:22:ef:b9:98:87  txqueuelen 1000  (Ethernet)
        RX packets 278999  bytes 182142023 (182.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 176176  bytes 41747476 (41.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Ifconfig is used to configure the kernel-resident network interfaces.
- If no arguments are given, ifconfig displays the status of the currently active interfaces.
- In the screenshot, there are ethernet, loopback and wlan interfaces
- line 1 has flags (e.g. UP, BROADCAST, MULTICAST)
- inet adderess is the IPv4 address, inet6 is the IPv6 address of the interface. Similarly, subnet mask and broadcast address is also mentioned.
- In the end, some packet stats are mentioned
    - RX packets, errors, dropped - total number of packets received, recieved error and dropped respectively
    - TX packets, errors, dropped - total number of packets transmitted, recieved error and dropped respectively

dig

```
(base) adarshnandanwar@predator-pop-os:~$ dig google.co.in

; <<>> DiG 9.16.6-Ubuntu <<>> google.co.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31215
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.co.in.                  IN      A

;; ANSWER SECTION:
google.co.in.           24      IN      A       172.217.160.163

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Jan 24 23:23:47 IST 2021
;; MSG SIZE  rcvd: 57
```

- `dig` is command for DNS lookup utility
- using query options (e.g. +nocomments), we can modify the output
- First, dig command's version number is printed in the header
- QUESTION SECTION displays our input
- ANSWER SECTION displays the response (A Record) to our query
- In the end, dig prints some stats like time taken, timestamp, etc

arp

```
(base) adarshnandanwar@predator-pop-os:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.189                    (incomplete)                              wlp2s0
dlinkrouter.Dlink        ether   c4:e9:0a:45:a1:82   C                     wlp2s0
```

- Arp manipulates or displays the kernel's IP network neighbour cache. It can add entries to the table, delete one or display the current content.
- The output is a table with the columns: IP address, HW Type, HW address, Flags, Interface
- Here dlinkrouter.Dlink is the router on the interface wlp2s0

netstat

```
(base) adarshnandanwar@predator-pop-os:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 predator-pop-os.D:56252 104.16.68.69:https      ESTABLISHED
tcp        0      0 predator-pop-os.D:54550 bom12s01-in-f14.1e:http ESTABLISHED
tcp        0      0 predator-pop-os.D:38040 199.232.252.84:https    ESTABLISHED
tcp        0      0 predator-pop-os.D:60084 151.101.120.64:https    ESTABLISHED
tcp        0      0 localhost:46624         localhost:49010         TIME_WAIT
tcp        0      0 predator-pop-os.D:40038 205.180.87.146:https    TIME_WAIT
tcp        0      0 predator-pop-os.D:56862 bom12s10-in-f2.1e:https ESTABLISHED
tcp        0      1 predator-pop-os.D:57936 594.bm-nginx-load:https SYN_SENT
tcp        0      0 predator-pop-os.D:33386 vps-cc0b988f.vps.:https ESTABLISHED
tcp        0      1 predator-pop-os.D:58016 594.bm-nginx-load:https SYN_SENT
tcp        0      0 predator-pop-os.D:60070 151.101.120.64:https    ESTABLISHED
tcp        0      0 predator-pop-os.D:37628 192.229.237.96:https    ESTABLISHED
tcp        0      0 predator-pop-os.D:47700 193.244.178.107.b:https ESTABLISHED
^C
```

```
(base) adarshnandanwar@predator-pop-os:~$ netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG        0 0          0 wlp2s0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 wlp2s0
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0 wlp2s0
```

- `netstat` prints network connections, routing tables, interface statistics, masquerade connections, and multicast memberships
- The output is a table with columns Protocol, Recv-Q, Send-Q, Local Address, Foreign Address, State for all connections
- Local Address- address and port number of the local end of the socket.
- Foreign Address- address and port number of the remote end of the socket.
- Using flags -n, we can print the numerical addresses and with -r we can view kernel routing table

telnet

```
(base) adarshnandanwar@predator-pop-os:~$ telnet localhost 80
Trying ::1...
Connected to localhost.
Escape character is '^]'.
```

- The telnet command is used for interactive communication with another host using the TELNET protocol.

traceroute

```
(base) adarshnandanwar@predator-pop-os:~$ traceroute google.co.in
traceroute to google.co.in (142.250.67.131), 30 hops max, 60 byte packets
 1  dlinkrouter.Dlink (192.168.0.1)  1.675 ms  1.614 ms  1.871 ms
 2  10.20.0.1 (10.20.0.1)  9.453 ms  9.418 ms  9.383 ms
 3  103.48.58.217 (103.48.58.217)  15.109 ms  15.077 ms  15.044 ms
 4  10.241.1.6 (10.241.1.6)  5.659 ms  5.702 ms *
 5  10.240.254.130 (10.240.254.130)  9.157 ms  9.123 ms  9.090 ms
 6  * * *
 7  10.241.1.1 (10.241.1.1)  3.615 ms  3.650 ms  3.634 ms
 8  150-232-14-103.intechonline.net (103.14.232.150)  3.930 ms  3.916 ms  4.415 ms
 9  * 10.252.183.30 (10.252.183.30)  4.704 ms 10.252.227.158 (10.252.227.158)  5.239 ms
10  142.250.228.46 (142.250.228.46)  4.747 ms 108.170.248.209 (108.170.248.209)  4.917 ms  4.884 ms
11  142.250.227.71 (142.250.227.71)  5.494 ms 108.170.248.218 (108.170.248.218)  3.605 ms 108.170.248.219 (108.170.248.219)  3.970 ms
12  bom12s06-in-f3.1e100.net (142.250.67.131)  3.678 ms 108.170.248.177 (108.170.248.177)  5.312 ms 108.170.248.161 (108.170.248.161)  4.192 ms
```

- `traceroute` tracks the route packets taken from an IP network on their way to a given host.
- First line describes the destination, max hops set, packet size.
- The following lines displays the info for all the hops
- each line contains the hop number, destination and the time information.

ping

```
(base) adarshnandanwar@predator-pop-os:~$ ping google.co.in
PING google.co.in (172.217.160.163) 56(84) bytes of data.
64 bytes from bom05s12-in-f3.1e100.net (172.217.160.163): icmp_seq=1 ttl=118 time=5.72 ms
64 bytes from bom05s12-in-f3.1e100.net (172.217.160.163): icmp_seq=2 ttl=118 time=6.08 ms
64 bytes from bom05s12-in-f3.1e100.net (172.217.160.163): icmp_seq=3 ttl=118 time=43.0 ms
64 bytes from bom05s12-in-f3.1e100.net (172.217.160.163): icmp_seq=4 ttl=118 time=11.7 ms
64 bytes from bom05s12-in-f3.1e100.net (172.217.160.163): icmp_seq=5 ttl=118 time=13.0 ms
64 bytes from bom05s12-in-f3.1e100.net (172.217.160.163): icmp_seq=6 ttl=118 time=22.6 ms
64 bytes from bom05s12-in-f3.1e100.net (172.217.160.163): icmp_seq=7 ttl=118 time=6.87 ms
^C
--- google.co.in ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 5.720/15.572/43.000/12.457 ms
```

- ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway.
- First line shows the destination and the size of packet.
- It sends one datagram per second and prints one line of output for every response received. It calculates round-trip times and packet loss statistics
- It also displays a brief summary about packages and time taken on completion.

top

```
top - 14:59:36 up 1 day,  1:23,  1 user,  load average: 1.08, 1.18, 1.30
Tasks: 273 total,   1 running, 272 sleeping,   0 stopped,   0 zombie
%Cpu(s):  7.5 us,  5.9 sy,  0.0 ni, 86.6 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :  15892.8 total,   5506.1 free,   4117.2 used,   6269.5 buff/cache
MiB Swap:   8195.5 total,   8195.5 free,      0.0 used.  11703.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   1705 adarshn+  -2   0 4532600 610644 128920 S  43.5   3.8  23:45.57 gnome-shell
   1550 root      20   0  397136 166436  84520 S   6.3   1.0  22:50.33 Xorg
  57298 adarshn+  20   0 4731024 180732 106928 S   3.7   1.1   0:19.64 chrome
    553 root     -51   0       0      0      0 S   2.7   0.0   9:26.52 irq/133-nvidia
  37133 adarshn+  20   0 1138688 465616 287444 S   1.0   2.9  12:40.44 chrome
  37174 adarshn+  20   0  380912 105816  66904 S   1.0   0.7   1:51.20 chrome
  57810 root       0 -20       0      0      0 I   0.7   0.0   0:00.35 kworker/u9:1-i915_flip
    566 root      20   0       0      0      0 S   0.3   0.0   2:25.32 nv_queue
  37726 adarshn+  20   0   18.6g 247768 106252 S   0.3   1.5   7:01.70 code
  56147 adarshn+  20   0  612096 170448  82940 S   0.3   1.0   0:15.56 chrome
  58074 adarshn+  20   0   22636   4276   3452 R   0.3   0.0   0:00.06 top
      1 root      20   0  170780  12124   8804 S   0.0   0.1   0:01.80 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
```

- This command is used to display real-time information about Linux processes
- In the beginning, There is a summary including up time, load averages, task states, CPU states, system memory.
- Then there is a table of running process with their pid, user, priority, nice value, Virtual Memory Size (KiB), Resident Memory Size (KiB), Shared Memory Size (KiB), CPU usage, memory usage, CPU up time and command.

wall

```
(base) adarshnandanwar@predator-pop-os:~$ wall "Hello users"
(base) adarshnandanwar@predator-pop-os:~$
```

- Used to write messages to all currently logged in users.

uptime

```
(base) adarshnandanwar@predator-pop-os:~$ uptime
 15:12:39 up 1 day,  1:36,  1 user,  load average: 1.68, 1.38, 1.22
```

- Tells how long the system has been running
- The output is one line containing The current time, how long the system has been running, how many users are currently logged on, and the system load averages for the past 1, 5, and 15 minutes.

nslookup

```
(base) adarshnandanwar@predator-pop-os:~$ nslookup google.co.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.co.in
Address: 172.217.160.163
Name:   google.co.in
Address: 2404:6800:4009:80a::2003

(base) adarshnandanwar@predator-pop-os:~$ nslookup 172.217.160.163
163.160.217.172.in-addr.arpa    name = bom05s12-in-f3.1e100.net.

Authoritative answers can be found from:

(base) adarshnandanwar@predator-pop-os:~$ nslookup -type=ns google.co.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.co.in    nameserver = ns2.google.com.
google.co.in    nameserver = ns4.google.com.
google.co.in    nameserver = ns3.google.com.
google.co.in    nameserver = ns1.google.com.

Authoritative answers can be found from:

(base) adarshnandanwar@predator-pop-os:~$ nslookup -type=mx google.co.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.co.in    mail exchanger = 20 alt1.aspmx.l.google.com.
google.co.in    mail exchanger = 10 aspmx.l.google.com.
google.co.in    mail exchanger = 50 alt4.aspmx.l.google.com.
google.co.in    mail exchanger = 30 alt2.aspmx.l.google.com.
google.co.in    mail exchanger = 40 alt3.aspmx.l.google.com.

Authoritative answers can be found from:

(base) adarshnandanwar@predator-pop-os:~$
```

- Nslookup is a program to query Internet domain name servers.
- It has 2 modes, interactive and non-interactive
- It displays the A Record or IP Address of the domain.
- We can also do the reverse DNS look-up by providing the IP Address as argument to nslookup.
- Using flags or by setting types, we can change the query.
- type=ns will output the name serves which are associated with the given domain.
- type=mx will output a list of mail exchange servers for that domain.