Lab 2

Name- Adarsh Nandanwar
BITS ID- 2018A7PS0396G

1. See the statistics of TCP and UDP ports on Linux machine
    - `netstat` is used to print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships
    - `-s`, `--statistics` - Display summary statistics for each protocol.
    - `-t`, `--tcp` - Show TCP ports.
    - `-u`, `--udp` - Show UDP ports.

```
$ netstat -stu
$ netstat -tu
```

```
(base) adarshnandanwar@predator-pop-os:~$ netstat -stu
IcmpMsg:
    InType3: 47
    OutType3: 47
Tcp:
    204 active connection openings
    2 passive connection openings
    4 failed connection attempts
    8 connection resets received
    8 connections established
    6798 segments received
    5986 segments sent out
    16 segments retransmitted
    0 bad segments received
    72 resets sent
Udp:
    4610 packets received
    47 packets to unknown port received
    0 packet receive errors
    3329 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 58
UdpLite:
TcpExt:
    89 TCP sockets finished time wait in fast timer
    23 delayed acks sent
    Quick ack mode was activated 34 times
    2779 packet headers predicted
    765 acknowledgments not containing data payload received
    512 predicted acknowledgments
    TCPSackRecovery: 1
    1 congestion windows recovered without slow start after partial ack
    1 fast retransmits
    TCPTimeouts: 5
    TCPLossProbes: 10
    TCPLossProbeRecovery: 1
    TCPDSACKOldSent: 34
```

```
    TCPDSACKOfoSent: 2
    TCPDSACKRecv: 4
    19 connections reset due to unexpected data
    6 connections reset due to early user close
    TCPDSACKIgnoredNoUndo: 2
    TCPSackShiftFallback: 2
    TCPRcvCoalesce: 986
    TCPOFOQueue: 1222
    TCPOFOMerge: 2
    TCPAutoCorking: 158
    TCPSynRetrans: 2
    TCPOrigDataSent: 1692
    TCPKeepAlive: 221
    TCPDelivered: 1803
    TCPAckCompressed: 504
    TcpTimeoutRehash: 5
IpExt:
    InMcastPkts: 424
    OutMcastPkts: 139
    InBcastPkts: 58
    OutBcastPkts: 3
    InOctets: 15078083
    OutOctets: 1701802
    InMcastOctets: 46401
    OutMcastOctets: 17950
    InBcastOctets: 5000
    OutBcastOctets: 234
    InNoECTPkts: 15982
MPTcpExt:
(base) adarshnandanwar@predator-pop-os:~$
```

```
(base) adarshnandanwar@predator-pop-os:~$ netstat -tu
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:46624         localhost:55680         TIME_WAIT
tcp        0      0 localhost:46624         localhost:55692         TIME_WAIT
tcp        0      0 localhost:46624         localhost:55666         TIME_WAIT
tcp        0      0 predator-pop-os.D:45936 117.18.232.200:https    ESTABLISHED
tcp        0      0 predator-pop-os.D:37136 server-13-33-179-:https ESTABLISHED
tcp        0      0 predator-pop-os.D:35380 142.250.192.46:https    ESTABLISHED
tcp        0      0 localhost:46624         localhost:55676         TIME_WAIT
tcp        0      0 predator-pop-os.D:44844 sa-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 localhost:46624         localhost:55674         TIME_WAIT
tcp        0      0 localhost:46624         localhost:55694         TIME_WAIT
tcp        0      0 localhost:46624         localhost:55690         TIME_WAIT
tcp        0      0 localhost:46624         localhost:55670         TIME_WAIT
tcp        0      0 localhost:46624         localhost:55686         TIME_WAIT
tcp        0      0 predator-pop-os.D:35114 156.247.107.34.bc:https ESTABLISHED
tcp        0      0 predator-pop-os.D:35376 142.250.192.46:https    TIME_WAIT
tcp        0      0 predator-pop-os.D:41270 bom12s01-in-f14.1e:http ESTABLISHED
tcp        0      0 localhost:46624         localhost:55672         TIME_WAIT
tcp        0      0 localhost:46624         localhost:55678         TIME_WAIT
tcp        0      0 localhost:46624         localhost:55684         TIME_WAIT
udp        0      0 predator-pop-os.:bootpc dlinkrouter.Dlin:bootps ESTABLISHED
udp        0      0 predator-pop-os.D:58318 172.217.194.189:443     ESTABLISHED
udp6       0      0 localhost:40934         localhost:40934         ESTABLISHED
```

2. Enlist the listening ports on your machine
    - `netstat` is used to print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships
    - `-l`, `--listening` - Show only listening sockets. (These are omitted by default.)
    - `-p`, `--program` - Show the PID and name of the program to which each socket belongs.

```
$ netstat -lp
```

```
(base) adarshnandanwar@predator-pop-os:~$ sudo netstat -lp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:9510            0.0.0.0:*               LISTEN      2190/urserver
tcp        0      0 0.0.0.0:9512            0.0.0.0:*               LISTEN      2190/urserver
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      637/systemd-resolve
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      714/cupsd
tcp        0      0 localhost:postgresql    0.0.0.0:*               LISTEN      970/postgres
tcp        0      0 localhost:46624         0.0.0.0:*               LISTEN      1420/kited
tcp6       0      0 [::]:http               [::]:*                  LISTEN      909/apache2
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN      714/cupsd
tcp6       0      0 localhost:postgresql    [::]:*                  LISTEN      970/postgres
udp        0      0 0.0.0.0:46011           0.0.0.0:*                           709/avahi-daemon: r
udp        0      0 224.0.0.251:mdns        0.0.0.0:*                           3564/chrome
udp        0      0 0.0.0.0:mdns            0.0.0.0:*                           709/avahi-daemon: r
udp        0      0 localhost:domain        0.0.0.0:*                           637/systemd-resolve
udp        0      0 0.0.0.0:631             0.0.0.0:*                           814/cups-browsed
udp        0      0 0.0.0.0:9511            0.0.0.0:*                           2190/urserver
udp        0      0 0.0.0.0:9512            0.0.0.0:*                           2190/urserver
udp6       0      0 [::]:46170              [::]:*                              709/avahi-daemon: r
udp6       0      0 [::]:mdns               [::]:*                              709/avahi-daemon: r
udp6       0      0 predator-:dhcpv6-client [::]:*                              718/NetworkManager
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7           718/NetworkManager
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     43820    1778/gnome-session-  @/tmp/.ICE-unix/1778
unix  2      [ ACC ]     SEQPACKET  LISTENING     19521    1/init               /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     40607    1409/systemd         /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     75139    2439/gvfsd-trash     @/dbus-vfs-daemon/socket-o6iOP4l1
unix  2      [ ACC ]     STREAM     LISTENING     41553    1845/ibus-daemon     @/home/adarshnandanwar/.cache/ibus/dbus-PenQxjqP
unix  2      [ ACC ]     STREAM     LISTENING     57888    3564/chrome          /tmp/.com.google.Chrome.DxHVXI/SingletonSocket
unix  2      [ ACC ]     STREAM     LISTENING     42153    1547/Xorg            @/tmp/.X11-unix/X1
unix  2      [ ACC ]     STREAM     LISTENING     41166    987/gdm3             @/tmp/dbus-QlinxJkg
unix  2      [ ACC ]     STREAM     LISTENING     40612    1409/systemd         /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     31727    900/nvidia-persiste  /var/run/nvidia-persistenced/socket
unix  2      [ ACC ]     STREAM     LISTENING     40613    1409/systemd         /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     40614    1409/systemd         /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     33284    970/postgres         /var/run/postgresql/.s.PGSQL.5432
unix  2      [ ACC ]     STREAM     LISTENING     40615    1409/systemd         /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     40616    1409/systemd         /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     40617    1409/systemd         /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     40618    1409/systemd         /run/user/1000/pipewire-0
unix  2      [ ACC ]     STREAM     LISTENING     40619    1409/systemd         /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM     LISTENING     40620    1409/systemd         /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     39805    1442/gnome-keyring-  /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     48623    2439/gvfsd-trash     @/dbus-vfs-daemon/socket-DQJyISCA
unix  2      [ ACC ]     STREAM     LISTENING     43804    1442/gnome-keyring-  /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     75137    2439/gvfsd-trash     @/dbus-vfs-daemon/socket-bCOJiSLE
unix  2      [ ACC ]     STREAM     LISTENING     41454    1442/gnome-keyring-  /run/user/1000/keyring/ssh
unix  2      [ ACC ]     STREAM     LISTENING     41167    987/gdm3             @/tmp/dbus-uWxlb24r
unix  2      [ ACC ]     STREAM     LISTENING     33621    987/gdm3             @/tmp/dbus-aMCwfhFu
unix  2      [ ACC ]     STREAM     LISTENING     73462    6283/code --no-sand  /run/user/1000/vscode-c3b4d090-1.52.1-main.sock
unix  2      [ ACC ]     STREAM     LISTENING     48621    2439/gvfsd-trash     @/dbus-vfs-daemon/socket-ovSOIvt0
unix  2      [ ACC ]     STREAM     LISTENING     77286    6415/code --type=re  /run/user/1000/vscode-c3b4d090-1.52.1-shared.sock
unix  2      [ ACC ]     STREAM     LISTENING     43700    1747/dbus-daemon     @/tmp/dbus-tySnJ96DBQ
unix  2      [ ACC ]     STREAM     LISTENING     28035    1/init               /run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     75731    6524/code            /run/user/1000/vscode-git-1a1ed4b194.sock
unix  2      [ ACC ]     STREAM     LISTENING     33620    987/gdm3             @/tmp/dbus-CgKY5UfW
unix  2      [ ACC ]     STREAM     LISTENING     19494    1/init               /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     19496    1/init               /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING     19506    1/init               /run/lvm/lvmpolld.socket
unix  2      [ ACC ]     STREAM     LISTENING     28037    1/init               /run/avahi-daemon/socket
unix  2      [ ACC ]     STREAM     LISTENING     19517    1/init               /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM     LISTENING     28039    1/init               /run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     28041    1/init               /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     28043    1/init               /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     42154    1547/Xorg            /tmp/.X11-unix/X1
unix  2      [ ACC ]     STREAM     LISTENING     20506    353/systemd-journal  /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     43662    1736/ssh-agent       /tmp/ssh-YE3JIikNA2zR/agent.1675
unix  2      [ ACC ]     STREAM     LISTENING     43821    1778/gnome-session-  /tmp/.ICE-unix/1778
unix  2      [ ACC ]     STREAM     LISTENING     30045    722/irqbalance       /run/irqbalance/irqbalance722.sock
```

3. See the mail xchange (MX) record for www.gmail.com
    - `nslookup` is a program to query Internet domain name servers.
    - `type=mx` will output a list of mail exchange servers for that domain.

```
$ nslookup -type=mx gmail.com
```

```
(base) adarshnandanwar@predator-pop-os:~$ nslookup -type=mx gmail.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
gmail.com       mail exchanger = 20 alt2.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 5 gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 10 alt1.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 30 alt3.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 40 alt4.gmail-smtp-in.l.google.com.

Authoritative answers can be found from:

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

4. Display the all network interfaces on your machine
    - `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

```
$ 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 8747  bytes 913542 (913.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8747  bytes 913542 (913.5 KB)
        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 fe80::cbf5:2048:6298:9713  prefixlen 64  scopeid 0x20<link>
        ether 98:22:ef:b9:98:87  txqueuelen 1000  (Ethernet)
        RX packets 52291  bytes 41595163 (41.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37226  bytes 10832286 (10.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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

5. A list of intermediate routers to reach 8.8.8.8 from your machine, with latency
    - `traceroute` tracks the route packets taken from an IP network on their way to a given host.

```
$ traceroute 8.8.8.8
```

```
(base) adarshnandanwar@predator-pop-os:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  dlinkrouter.Dlink (192.168.0.1)  4.288 ms  4.254 ms  4.590 ms
 2  10.20.0.1 (10.20.0.1)  12.628 ms  12.727 ms  13.143 ms
 3  103.48.58.217 (103.48.58.217)  7.976 ms  7.964 ms  8.488 ms
 4  150-232-14-103.intechonline.net (103.14.232.150)  9.077 ms  9.065 ms  9.053 ms
 5  10.252.211.62 (10.252.211.62)  9.041 ms 10.23.211.30 (10.23.211.30)  9.619 ms *
 6  142.250.208.222 (142.250.208.222)  10.237 ms 108.170.231.78 (108.170.231.78)  10.278 ms dns.google (8.8.8.8)  8.181 ms
(base) adarshnandanwar@predator-pop-os:~$
```

6. Send 10 echo requests to 8.8.8.8 server from your machine
    - `ping` uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway.
    - `-c` - count. Stop after sending "count" ECHO_REQUEST packets. With deadline option, ping waits for count ECHO_REPLY packets, until the timeout expires.

```
$ ping -c 10 8.8.8.8
```

```
(base) adarshnandanwar@predator-pop-os:~$ ping -c 10 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=6.67 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=6.59 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=7.20 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=119 time=6.53 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=119 time=7.40 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=119 time=10.2 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=119 time=4.94 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=119 time=7.64 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=119 time=4.91 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=119 time=7.68 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9016ms
rtt min/avg/max/mdev = 4.909/6.977/10.201/1.429 ms
(base) adarshnandanwar@predator-pop-os:~$
```

7. Get the IP address of www.bits-pilani.ac.in domain.
    - There are many ways to get this
        - `dig` - It is command for DNS lookup utility. We can use `+short` to get only the ip address
        - `nslookup` - It is a program to query Internet domain name servers. `-type=a` is optional as it is the default type.

```
$ dig www.bits-pilani.ac.in
$ dig +short www.bits-pilani.ac.in
$ nslookup -type=a www.bits-pilani.ac.in
```

```
(base) adarshnandanwar@predator-pop-os:~$ dig www.bits-pilani.ac.in

; <<>> DiG 9.16.6-Ubuntu <<>> www.bits-pilani.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35972
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.bits-pilani.ac.in.         IN      A

;; ANSWER SECTION:
www.bits-pilani.ac.in.  78450   IN      CNAME   universe.bits-pilani.ac.in.
universe.bits-pilani.ac.in. 7199 IN     A       14.139.243.20
universe.bits-pilani.ac.in. 7199 IN     A       103.144.92.33

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Jan 31 18:55:40 IST 2021
;; MSG SIZE  rcvd: 105

(base) adarshnandanwar@predator-pop-os:~$ dig +short www.bits-pilani.ac.in
universe.bits-pilani.ac.in.
14.139.243.20
103.144.92.33
(base) adarshnandanwar@predator-pop-os:~$ nslookup -type=a www.bits-pilani.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.bits-pilani.ac.in   canonical name = universe.bits-pilani.ac.in.
Name:   universe.bits-pilani.ac.in
Address: 14.139.243.20
Name:   universe.bits-pilani.ac.in
Address: 103.144.92.33
```