

# CN-LAB

## TASK 1

Ali Muzahir  
P18-0058

1- netstat -a // The 'a' stands for all here. And this command shows us both listening and non-listening sockets. So here as you can see, it is showing us established ones and listening ones etc.

```
(anaconda3) ali@weirdo:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:microsoft-ds    0.0.0.0:*                LISTEN
tcp        0      0 0.0.0.0:netbios-ssn       0.0.0.0:*                LISTEN
tcp        0      0 localhost:domain       0.0.0.0:*                LISTEN
tcp        0      0 localhost:ipp          0.0.0.0:*                LISTEN
tcp        0      0 weirdo:60424           wm-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 weirdo:42372           ec2-34-241-71-237:https ESTABLISHED
tcp        0      0 weirdo:43472           93.184.220.29:http      TIME_WAIT
tcp        0      0 weirdo:43474           93.184.220.29:http      TIME_WAIT
tcp        0      0 weirdo:46852           a23-50-163-153.de:https ESTABLISHED
```

2- netstat -at // This commands shows us all tcp ports. It shows us all who might be listening or established or waiting etc.

```
(anaconda3) ali@weirdo:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:microsoft-ds    0.0.0.0:*                LISTEN
tcp        0      0 0.0.0.0:netbios-ssn       0.0.0.0:*                LISTEN
tcp        0      0 localhost:domain       0.0.0.0:*                LISTEN
tcp        0      0 localhost:ipp          0.0.0.0:*                LISTEN
tcp        0      0 weirdo:60424           wm-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 weirdo:42372           ec2-34-241-71-237:https ESTABLISHED
tcp        0      0 weirdo:46852           a23-50-163-153.de:https ESTABLISHED
tcp        0      0 weirdo:56278           ec2-3-6-207-117.a:https ESTABLISHED
```

3- netstat -au // This commands shows us all udp ports. These are also transport protocols like tcp.

```
(anaconda3) ali@weirdo:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp      0      0 224.0.0.251:mdns        0.0.0.0:*
udp      0      0 224.0.0.251:mdns        0.0.0.0:*
udp      0      0 224.0.0.251:mdns        0.0.0.0:*
udp      0      0 0.0.0.0:mdns            0.0.0.0:*
udp      0      0 localhost:domain         0.0.0.0:*
udp      0      0 weirdo:bootpc            _gateway:bootps        ESTABLISHED
udp      0      0 192.168.1.25:netbios-ns 0.0.0.0:*
udp      0      0 weirdo:netbios-ns        0.0.0.0:*
udp      0      0 0.0.0.0:netbios-ns      0.0.0.0:*
udp      0      0 192.168.1.2:netbios-dgm 0.0.0.0:*
udp      0      0 weirdo:netbios-dgm       0.0.0.0:*
udp      0      0 0.0.0.0:netbios-dgm     0.0.0.0:*
udp      0      0 0.0.0.0:53758           0.0.0.0:*
udp      0      0 0.0.0.0:631             0.0.0.0:*
udp6     0      0 [::]:mdns               [::]:*
udp6     0      0 [::]:36467              [::]:*
```

4- netstat -l // This commands shows us all those ports which are listening.

```
(anaconda3) ali@weirdo:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 0.0.0.0:microsoft-ds    0.0.0.0:*              LISTEN
tcp      0      0 0.0.0.0:netbios-ssn     0.0.0.0:*              LISTEN
tcp      0      0 localhost:domain         0.0.0.0:*              LISTEN
tcp      0      0 localhost:ipp            0.0.0.0:*              LISTEN
tcp6     0      0 [::]:microsoft-ds       [::]:*                  LISTEN
tcp6     0      0 [::]:netbios-ssn        [::]:*                  LISTEN
tcp6     0      0 [::]:http                [::]:*                  LISTEN
tcp6     0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp      0      0 224.0.0.251:mdns        0.0.0.0:*
udp      0      0 224.0.0.251:mdns        0.0.0.0:*
udp      0      0 224.0.0.251:mdns        0.0.0.0:*
udp      0      0 0.0.0.0:mdns            0.0.0.0:*
udp      0      0 localhost:domain         0.0.0.0:*
udp      0      0 192.168.1.25:netbios-ns 0.0.0.0:*
udp      0      0 weirdo:netbios-ns        0.0.0.0:*
udp      0      0 0.0.0.0:netbios-ns      0.0.0.0:*
udp      0      0 192.168.1.2:netbios-dgm 0.0.0.0:*
udp      0      0 weirdo:netbios-dgm       0.0.0.0:*
udp      0      0 0.0.0.0:netbios-dgm     0.0.0.0:*
udp      0      0 0.0.0.0:53758           0.0.0.0:*
udp      0      0 0.0.0.0:631             0.0.0.0:*
udp6     0      0 [::]:mdns               [::]:*
udp6     0      0 [::]:36467              [::]:*
raw6     0      0 [::]:ipv6-icmp          [::]:*                  7

Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State       I-Node     Path
unix   2      [ ACC ] STREAM    LISTENING   43148      @/tmp/.ICE-unix/1994
unix   2      [ ACC ] SEQPACKET LISTENING   16629      /run/udev/control
unix   2      [ ACC ] STREAM    LISTENING   35958      /var/run/samba/nmbd/unexpected
unix   2      [ ACC ] STREAM    LISTENING   41512      @/tmp/dbus-Bkd1gltXZD
unix   2      [ ACC ] STREAM    LISTENING   39256      /run/user/1000/systemd/private
unix   2      [ ACC ] STREAM    LISTENING   39261      /run/user/1000/bus
unix   2      [ ACC ] STREAM    LISTENING   39262      /run/user/1000/gnupg/S.dirmngr
unix   2      [ ACC ] STREAM    LISTENING   39263      /run/user/1000/gnupg/S.gpg-agent.browser
unix   2      [ ACC ] STREAM    LISTENING   39264      /run/user/1000/gnupg/S.gpg-agent.extra
unix   2      [ ACC ] STREAM    LISTENING   1484548    /tmp/OSL_PIPE_1000_SingleOfficeIPC_e425c4a3275
c4369f118e87169df2f5
unix   2      [ ACC ] STREAM    LISTENING   39265      /run/user/1000/gnupg/S.gpg-agent.ssh
```

5- netstat -lt // This commands shows us all TCP ports that are listening.

```
(anaconda3) ali@weirdo:~$ netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:microsoft-ds    0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:netbios-ssn      0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp6       0      0 [::]:microsoft-ds      [::]:*                  LISTEN
tcp6       0      0 [::]:netbios-ssn       [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp      [::]:*                  LISTEN
```

6- netstat -lu // This commands shows us all udp ports which are listening.

```
(anaconda3) ali@weirdo:~$ netstat -lu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 224.0.0.251:mdns        0.0.0.0:*               LISTEN
udp        0      0 224.0.0.251:mdns        0.0.0.0:*               LISTEN
udp        0      0 224.0.0.251:mdns        0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:mdns            0.0.0.0:*               LISTEN
udp        0      0 localhost:domain        0.0.0.0:*               LISTEN
udp        0      0 192.168.1.25:netbios-ns 0.0.0.0:*               LISTEN
udp        0      0 weirdo:netbios-ns       0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:netbios-ns      0.0.0.0:*               LISTEN
udp        0      0 192.168.1.2:netbios-dgm 0.0.0.0:*               LISTEN
udp        0      0 weirdo:netbios-dgm      0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:netbios-dgm     0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:53758           0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:631             0.0.0.0:*               LISTEN
udp6       0      0 [::]:mdns               [::]:*                  LISTEN
udp6       0      0 [::]:36467              [::]:*                  LISTEN
```

7- netstat -lx // This commands shows us only UNIX ports which are listening.

```
(anaconda3) ali@weirdo:~$ netstat -lx
Active UNIX domain sockets (only servers)
Proto RefCnt Flags      Type       State      I-Node    Path
unix  2      [ ACC ]     STREAM    LISTENING   43148     @/tmp/.ICE-unix/1994
unix  2      [ ACC ]     STREAM    LISTENING   16629     /run/udev/control
unix  2      [ ACC ]     STREAM    LISTENING   35958     /var/run/samba/nmbd/unexpected
unix  2      [ ACC ]     STREAM    LISTENING   41512     @/tmp/dbus-Bkd1gLtXZD
unix  2      [ ACC ]     STREAM    LISTENING   39256     /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM    LISTENING   39261     /run/user/1000/bus
unix  2      [ ACC ]     STREAM    LISTENING   39262     /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM    LISTENING   39263     /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM    LISTENING   39264     /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM    LISTENING   1484548   /tmp/OSL_PIPE_1000_SingleOfficeIPC_e425c4a3275
c4369f118e87169df2f5
unix  2      [ ACC ]     STREAM    LISTENING   39265     /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM    LISTENING   39266     /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM    LISTENING   39267     /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM    LISTENING   39268     /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM    LISTENING   39269     /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM    LISTENING   38572     @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM    LISTENING   37860     /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM    LISTENING   40900     /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM    LISTENING   31863     @/tmp/dbus-FEnOE3C2
unix  2      [ ACC ]     STREAM    LISTENING   40933     /run/user/1000/keyring/ssh
unix  2      [ ACC ]     STREAM    LISTENING   26910     /run/avahi-daemon/socket
unix  2      [ ACC ]     STREAM    LISTENING   236753    @/tmp/dbus-UGVcY2jv
unix  2      [ ACC ]     STREAM    LISTENING   16602     /run/systemd/private
unix  2      [ ACC ]     STREAM    LISTENING   1593056   /run/user/1000/snap.slack/.org.chromium.Chromi
um.rR5g6i/SS
unix  2      [ ACC ]     STREAM    LISTENING   16604     /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM    LISTENING   16615     /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM    LISTENING   40840     @/home/ali/.cache/ibus/dbus-gJmfrTC
unix  2      [ ACC ]     STREAM    LISTENING   26912     /run/cups/cups.sock
unix  2      [ ACC ]     STREAM    LISTENING   26914     /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM    LISTENING   16625     /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM    LISTENING   26916     /run/snapd.socket
unix  2      [ ACC ]     STREAM    LISTENING   26918     /run/snapd-snap.socket
unix  2      [ ACC ]     STREAM    LISTENING   26920     /run/uidd/request
unix  2      [ ACC ]     STREAM    LISTENING   13298     /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM    LISTENING   31574     /var/snap/canonical-livepatch/95/livepatchd.so
ck
unix  2      [ ACC ]     STREAM    LISTENING   446358    @/dbus-vfs-daemon/socket-taFLsjid
```



8- netstat -s // This command shows us all statistics of all ports. These statistics range from number of packets received, to discarded, to outgoing.

```
(anaconda3) ali@weirdo:~$ netstat -s
Ip:
    Forwarding: 2
    4599642 total packets received
    53 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    4599508 incoming packets delivered
    2815372 requests sent out
    22 outgoing packets dropped
    908 dropped because of missing route
Icmp:
    457 ICMP messages received
    14 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 447
        timeout in transit: 10
    434 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 434
IcmpMsg:
    InType3: 447
    InType11: 10
    OutType3: 434
Tcp:
    12653 active connection openings
    8 passive connection openings
    3247 failed connection attempts
    408 connection resets received
    28 connections established
    1447274 segments received
    1285905 segments sent out
    9562 segments retransmitted
    130 bad segments received
    6974 resets sent
Udp:
    3164225 packets received
    431 packets to unknown port received
    74 packet receive errors
    1528494 packets sent
    74 receive buffer errors
    2 send buffer errors
    IgnoredMulti: 8
```

9- netstat -st // This commands shows us statistics for TCP ports.

```
(anaconda3) ali@weirdo:~$ netstat -st
IcmpMsg:
  InType3: 447
  InType11: 10
  OutType3: 434
Tcp:
  12653 active connection openings
  8 passive connection openings
  3247 failed connection attempts
  408 connection resets received
  24 connections established
  1447361 segments received
  1286000 segments sent out
  9567 segments retransmitted
  130 bad segments received
  6976 resets sent
UdpLite:
TcpExt:
  17 packets pruned from receive queue because of socket buffer overrun
  20 ICMP packets dropped because they were out-of-window
  1396 TCP sockets finished time wait in fast timer
  6188 packetes rejected in established connections because of timestamp
  5177 delayed acks sent
  1 delayed acks further delayed because of locked socket
  Quick ack mode was activated 10031 times
  990574 packet headers predicted
  53224 acknowledgments not containing data payload received
  135962 predicted acknowledgments
  TCPSackRecovery: 128
  Detected reordering 5173 times using SACK
  Detected reordering 33 times using time stamp
  63 congestion windows fully recovered without slow start
  27 congestion windows partially recovered using Hoe heuristic
  TCPDSACKUndo: 17
  618 congestion windows recovered without slow start after partial ack
  TCPLostRetransmit: 4281
  TCPSackFailures: 14
  2 timeouts in loss state
  133 fast retransmits
  26 retransmits in slow start
  TCPTimeouts: 6917
  TCPLossProbes: 3278
  TCPLossProbeRecovery: 350
  TCPSackRecoveryFail: 3
  2386 packets collapsed in receive queue due to low socket buffer
  TCPBacklogCoalesce: 98
  TCPDSACKOldSent: 10067
  TCPDSACKOfoSent: 79
  TCPDSACKRecv: 3397
  TCPDSACKOfoRecv: 2
  1241 connections reset due to unexpected data
  169 connections reset due to early user close
  527 connections aborted due to timeout
```

10- netstat -su // This commands shows us the statistics for udp ports.

```
(anaconda3) ali@weirdo:~$ netstat -su
IcmpMsg:
  InType3: 447
  InType11: 10
  OutType3: 434
Udp:
  3164242 packets received
  431 packets to unknown port received
  74 packet receive errors
  1528512 packets sent
  74 receive buffer errors
  2 send buffer errors
  IgnoredMulti: 8
UdpLite:
IpExt:
  InMcastPkts: 9180
  OutMcastPkts: 2570
  InBcastPkts: 372
  OutBcastPkts: 364
  InOctets: 6606052763
  OutOctets: 312705291
  InMcastOctets: 1584281
  OutMcastOctets: 489673
  InBcastOctets: 86584
  OutBcastOctets: 83816
  InNoECTPkts: 5581856
```

11- netstat -pt // This commands shows us the PID and program names of all ports.

```
(anaconda3) ali@weirdo:~$ netstat -pt
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         State       PID/Program name
tcp        0      0 weirdo:60424          wm-in-f188.1e100.n:5228 ESTABLISHED 42659/chrome --type
tcp        0      0 weirdo:42372          ec2-34-241-71-237:https ESTABLISHED 103600/firefox
tcp        0      0 weirdo:56278          ec2-3-6-207-117.a:https ESTABLISHED 104717/slack --type
tcp        0      0 weirdo:54370          ec2-54-69-165-95.:https ESTABLISHED 103600/firefox
tcp        0      0 weirdo:54224          ec2-3-123-248-34.:https ESTABLISHED 104717/slack --type
tcp        0      0 weirdo:56234          ec2-3-6-207-117.a:https ESTABLISHED 104717/slack --type
tcp        0      0 weirdo:56268          ec2-3-6-207-117.a:https ESTABLISHED 104717/slack --type
tcp        0      0 weirdo:56266          ec2-3-6-207-117.a:https ESTABLISHED 104717/slack --type
tcp        0      0 weirdo:46782          159.127.41.210:https   ESTABLISHED 103600/firefox
tcp        0      0 weirdo:56862          ads.us.e-planning:https ESTABLISHED 103600/firefox
tcp        0      0 weirdo:58616          mct01s06-in-f14.1:https ESTABLISHED 103600/firefox
tcp        0      0 weirdo:43440          mct01s10-in-f22.1:https ESTABLISHED 103600/firefox
tcp        0      0 weirdo:56254          ec2-3-6-207-117.a:https ESTABLISHED 104717/slack --type
tcp        0      0 weirdo:56270          ec2-3-6-207-117.a:https ESTABLISHED 104717/slack --type
tcp        0      0 weirdo:56274          ec2-3-6-207-117.a:https ESTABLISHED 104717/slack --type
tcp        0      0 weirdo:57606          server-143-204-11:https ESTABLISHED 103600/firefox
tcp        0      0 weirdo:60304          103.231.98.193:https   ESTABLISHED 103600/firefox
tcp        0      0 weirdo:56150          mct01s05-in-f2.1e:https ESTABLISHED 103600/firefox
tcp        0      0 weirdo:33522          mct01s10-in-f3.1e:https ESTABLISHED 103600/firefox
tcp        0      0 weirdo:35282          eg-in-f189.1e100.:https ESTABLISHED 103600/firefox
tcp        0      0 weirdo:53806          ionos.com:https        ESTABLISHED 103600/firefox
tcp        0      0 weirdo:49034          218.64.98.34.bc.g:https ESTABLISHED 103600/firefox
tcp        0      0 weirdo:36670          ec2-13-230-175-32:https ESTABLISHED 103600/firefox
```



12- netstat -c // This commands shows us the netstat information continuously after every few seconds.

```
(anaconda3) ali@weirdo:~$ netstat -c
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 weirdo:60424           wm-in-f188.1e100.n:5228 ESTABLISHED
tcp      0      0 weirdo:56278           ec2-3-6-207-117.a:https ESTABLISHED
tcp      0      0 weirdo:54370           ec2-54-69-165-95.:https ESTABLISHED
tcp      0      0 weirdo:59104           a104-83-87-185.de:https ESTABLISHED
tcp      0      0 weirdo:59102           a104-83-87-185.de:https ESTABLISHED
tcp      0      0 weirdo:56234           ec2-3-6-207-117.a:https ESTABLISHED
tcp      0      0 weirdo:56268           ec2-3-6-207-117.a:https ESTABLISHED
tcp      0      0 weirdo:56266           ec2-3-6-207-117.a:https ESTABLISHED
tcp      0      0 weirdo:46782           159.127.41.210:https    TIME_WAIT
tcp      0      0 weirdo:56254           ec2-3-6-207-117.a:https ESTABLISHED
tcp      0      0 weirdo:56270           ec2-3-6-207-117.a:https ESTABLISHED
tcp      0      0 weirdo:56274           ec2-3-6-207-117.a:https ESTABLISHED
tcp      0      0 weirdo:56150           mct01s05-in-f2.1e:https ESTABLISHED
tcp      0      0 weirdo:33522           mct01s10-in-f3.1e:https ESTABLISHED
tcp      0      0 weirdo:35282           eg-in-f189.1e100.:https ESTABLISHED
tcp      0      0 weirdo:52388           185.29.132.23:https    ESTABLISHED
udp      0      0 weirdo:bootpc          _gateway:bootps        ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State         I-Node      Path
unix   2      [ ]      DGRAM          39253      /run/user/1000/systemd/notify
unix   2      [ ]      DGRAM          36106      /var/lib/samba/private/msg.sock/1325
unix   2      [ ]      DGRAM          35942      /var/lib/samba/private/msg.sock/1224
unix   4      [ ]      DGRAM          16599      /run/systemd/notify
unix   2      [ ]      DGRAM          34293      /var/lib/samba/private/msg.sock/1349
unix   2      [ ]      DGRAM          16613      /run/systemd/journal/syslog
unix  20      [ ]      DGRAM          16623      /run/systemd/journal/dev-log
unix   8      [ ]      DGRAM          16627      /run/systemd/journal/socket
unix   2      [ ]      DGRAM          33262      /var/lib/samba/private/msg.sock/1350
unix   2      [ ]      DGRAM          33264      /var/lib/samba/private/msg.sock/1351
unix   3      [ ]      SEQPACKET  CONNECTED    1594071     @0002f
unix   2      [ ]      DGRAM          1486936     /run/wpa_supplicant/wlp3s0
unix   3      [ ]      SEQPACKET  CONNECTED    1594073     @00030
unix   3      [ ]      SEQPACKET  CONNECTED    404146     @00022
unix   2      [ ]      DGRAM          1484105     /run/wpa_supplicant/p2p-dev-wlp3s0
unix   3      [ ]      SEQPACKET  CONNECTED    404148     @00023
unix   2      [ ]      STREAM      CONNECTED    1618391
unix   3      [ ]      STREAM      CONNECTED    1572668     /run/systemd/journal/stdout
unix   3      [ ]      STREAM      CONNECTED    44560       /run/user/1000/bus
unix   3      [ ]      STREAM      CONNECTED    43763       /run/systemd/journal/stdout
unix   3      [ ]      STREAM      CONNECTED    1591954
unix   3      [ ]      STREAM      CONNECTED    1591359
unix   3      [ ]      STREAM      CONNECTED    406674
unix   3      [ ]      STREAM      CONNECTED    43356
unix   3      [ ]      STREAM      CONNECTED    42214       /run/user/1000/bus
unix   3      [ ]      STREAM      CONNECTED    41691
unix   3      [ ]      DGRAM          39255
unix   3      [ ]      STREAM      CONNECTED    34026
unix   3      [ ]      STREAM      CONNECTED    1594254
unix   3      [ ]      STREAM      CONNECTED    42569       /run/systemd/journal/stdout
```