Lab 21 – Using Netstat command to view networking information

Lab Objective:

Learn how to use netstat to view networking information.

Lab Purpose:

Netstat is a command line tool which let's you print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

Lab Tool:

Kali Linux

Lab Topology:

You can use Kali Linux for this lab. Some netstat command features may requires privileges to work. First of all, we have to be the "root" user using the terminal:

sudo su –

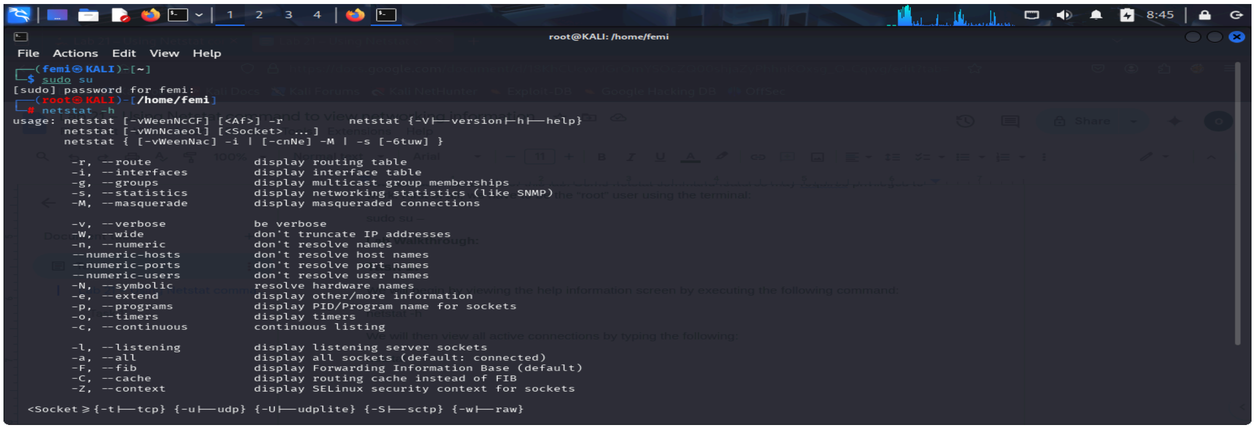
Lab Walkthrough:

Task 1:

We will begin by viewing the help information screen by executing the following command:

netstat -h

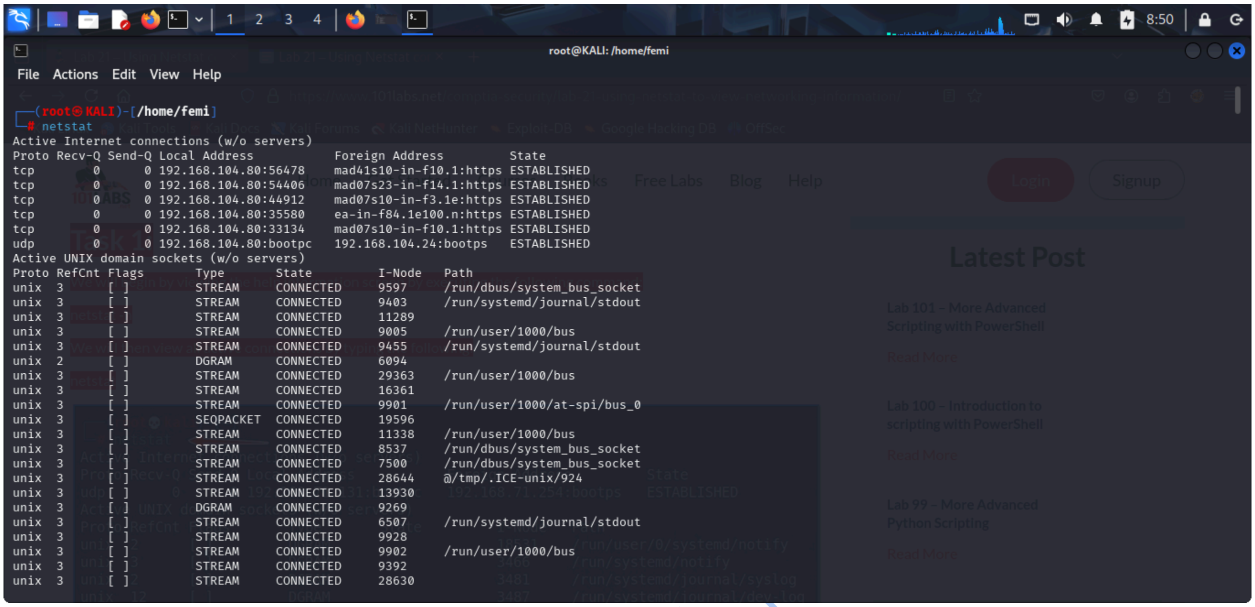
FEMI LANA



```
┌──(femi㉿KALI)-[~]
└─$ sudo su
[sudo] password for femi:
┌──(root㉿KALI)-[/home/femi]
└─# netstat -h
usage: netstat [-vWeenNcCF] [<Af>] -r         netstat {-V|--version|-h|--help}
       netstat [-vWnNcaeol] [<Socket> ...]
       netstat { [-vWeenNac] -i | [-cnNe] -M | -s [-6tuw] }

        -r, --route              display routing table
        -i, --interfaces         display interface table
        -g, --groups             display multicast group memberships
        -s, --statistics         display networking statistics (like SNMP)
        -M, --masquerade         display masqueraded connections

        -v, --verbose            be verbose
        -W, --wide               don't truncate IP addresses
        -n, --numeric            don't resolve names
        --numeric-hosts          don't resolve host names
        --numeric-ports          don't resolve port names
        --numeric-users          don't resolve user names
        -N, --symbolic           resolve hardware names
        -e, --extend             display other/more information
        -p, --programs           display PID/Program name for sockets
        -o, --timers             display timers
        -c, --continuous         continuous listing

        -l, --listening          display listening server sockets
        -a, --all                display all sockets (default: connected)
        -F, --fib                display Forwarding Information Base (default)
        -C, --cache              display routing cache instead of FIB
        -Z, --context            display SELinux security context for sockets

  <Socket>={-t|--tcp} {-u|--udp} {-U|--udplite} {-S|--sctp} {-w|--raw}
```

We will then view all active connections by typing the following:

Netstat

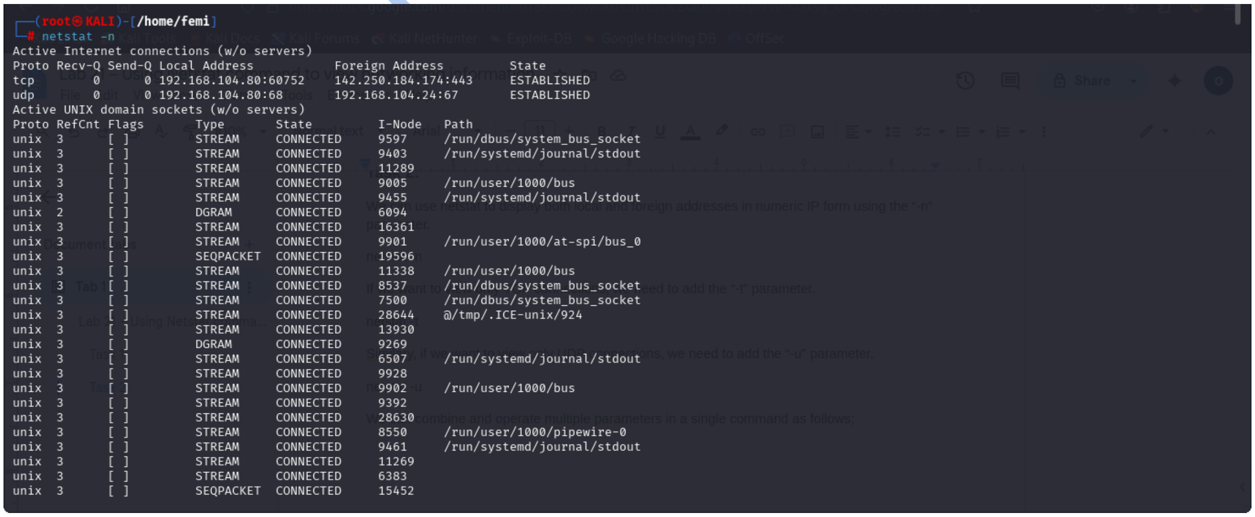


```
┌──(root㉿KALI)-[/home/femi]
└─# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.104.80:56478    mad41s10-in-f10.1:https ESTABLISHED
tcp        0      0 192.168.104.80:54406    mad07s23-in-f14.1:https ESTABLISHED
tcp        0      0 192.168.104.80:44912    mad07s10-in-f3.1e:https ESTABLISHED
tcp        0      0 192.168.104.80:35580    ea-in-f84.1e100.n:https ESTABLISHED
tcp        0      0 192.168.104.80:33134    mad07s10-in-f10.1:https ESTABLISHED
udp        0      0 192.168.104.80:bootpc   192.168.104.24:bootps   ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     9597     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     9403     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     11289
unix  3      [ ]         STREAM     CONNECTED     9005     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9455     /run/systemd/journal/stdout
unix  2      [ ]         DGRAM      CONNECTED     6094
unix  3      [ ]         STREAM     CONNECTED     29363    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     16361
unix  3      [ ]         STREAM     CONNECTED     9901     /run/user/1000/at-spi/bus_0
unix  3      [ ]         SEQPACKET  CONNECTED     19596
unix  3      [ ]         STREAM     CONNECTED     11338    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8537     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     7500     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     28644    @/tmp/.ICE-unix/924
unix  3      [ ]         STREAM     CONNECTED     13930
unix  3      [ ]         DGRAM      CONNECTED     9269
unix  3      [ ]         STREAM     CONNECTED     6507     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9928
unix  3      [ ]         STREAM     CONNECTED     9902     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9392
unix  3      [ ]         STREAM     CONNECTED     28630
```

Task 2:

We can use netstat to display both local and foreign addresses in numeric IP form using the "-n" parameter.

netstat -n

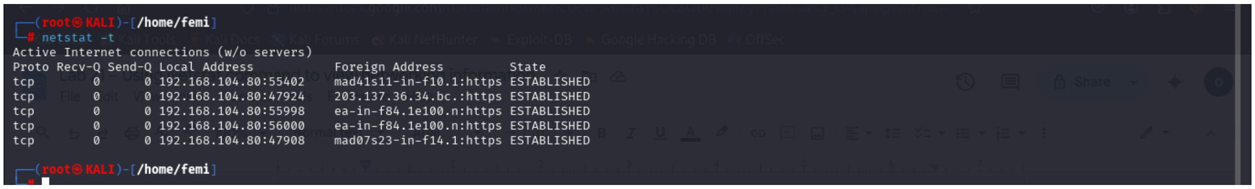


```
┌──(root㉿KALI)-[/home/femi]
└─# netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.104.80:60752    142.250.184.174:443     ESTABLISHED
udp        0      0 192.168.104.80:68       192.168.104.24:67       ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     9597     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     9403     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     11289
unix  3      [ ]         STREAM     CONNECTED     9005     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9455     /run/systemd/journal/stdout
unix  2      [ ]         DGRAM      CONNECTED     6094
unix  3      [ ]         STREAM     CONNECTED     16361
unix  3      [ ]         STREAM     CONNECTED     9901     /run/user/1000/at-spi/bus_0
unix  3      [ ]         SEQPACKET  CONNECTED     19596
unix  3      [ ]         STREAM     CONNECTED     11338    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8537     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     7500     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     28644    @/tmp/.ICE-unix/924
unix  3      [ ]         STREAM     CONNECTED     13930
unix  3      [ ]         DGRAM      CONNECTED     9269
unix  3      [ ]         STREAM     CONNECTED     6507     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9928
unix  3      [ ]         STREAM     CONNECTED     9902     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9392
unix  3      [ ]         STREAM     CONNECTED     28630
unix  3      [ ]         STREAM     CONNECTED     8550     /run/user/1000/pipewire-0
unix  3      [ ]         STREAM     CONNECTED     9461     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     11269
unix  3      [ ]         STREAM     CONNECTED     6383
unix  3      [ ]         SEQPACKET  CONNECTED     15452
```

FEMI LABS

If we want to view only TCP connections, we need to add the “-t” parameter.

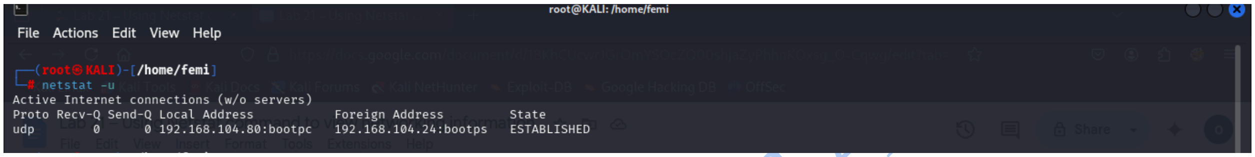
netstat -t



```
┌──(root㉿KALI)-[/home/femi]
└─# netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.104.80:55402    mad41s11-in-f10.1:https ESTABLISHED
tcp        0      0 192.168.104.80:47924    203.137.36.34.bc.:https ESTABLISHED
tcp        0      0 192.168.104.80:55998    ea-in-f84.1e100.n:https ESTABLISHED
tcp        0      0 192.168.104.80:56000    ea-in-f84.1e100.n:https ESTABLISHED
tcp        0      0 192.168.104.80:47908    mad07s23-in-f14.1:https ESTABLISHED

┌──(root㉿KALI)-[/home/femi]
└─# 
```

Similary, if we want to view only UDP connections, we need to add the “-u” parameter.

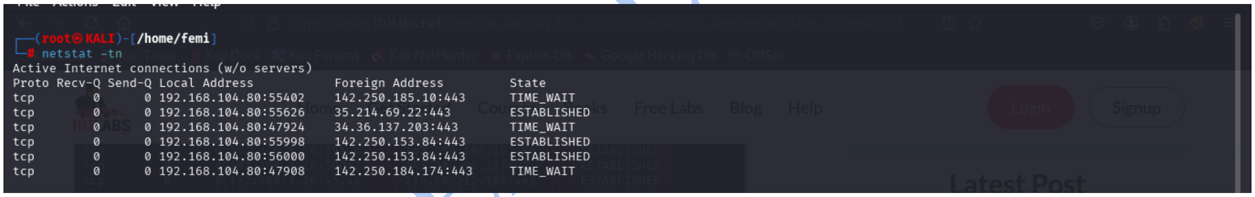
netstat -u



```
┌──(root㉿KALI)-[/home/femi]
└─# netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.104.80:bootpc   192.168.104.24:bootps   ESTABLISHED
```

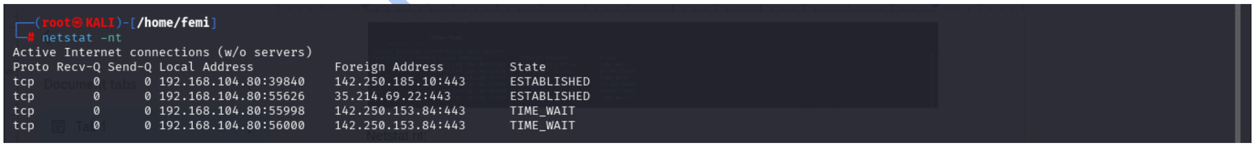
We can combine and operate multiple parameters in a single command as follows;

Netstat tn



```
┌──(root㉿KALI)-[/home/femi]
└─# netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.104.80:55402    142.250.185.10:443      TIME_WAIT
tcp        0      0 192.168.104.80:55626    35.214.69.22:443        ESTABLISHED
tcp        0      0 192.168.104.80:47924    34.36.137.203:443       TIME_WAIT
tcp        0      0 192.168.104.80:55998    142.250.153.84:443      ESTABLISHED
tcp        0      0 192.168.104.80:56000    142.250.153.84:443      ESTABLISHED
tcp        0      0 192.168.104.80:47908    142.250.184.174:443     TIME_WAIT
```

Netstat nt;

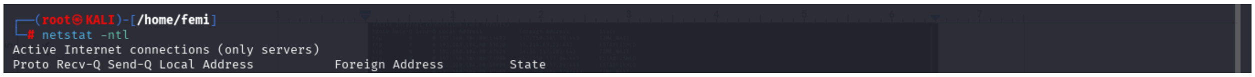


```
┌──(root㉿KALI)-[/home/femi]
└─# netstat -nt
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.104.80:39840    142.250.185.10:443      ESTABLISHED
tcp        0      0 192.168.104.80:55626    35.214.69.22:443        ESTABLISHED
tcp        0      0 192.168.104.80:55998    142.250.153.84:443      TIME_WAIT
tcp        0      0 192.168.104.80:56000    142.250.153.84:443      TIME_WAIT
```

Task 3:

netstat allows us to view only connections which are listening. We can do this by typing this command:

netstat -ntl

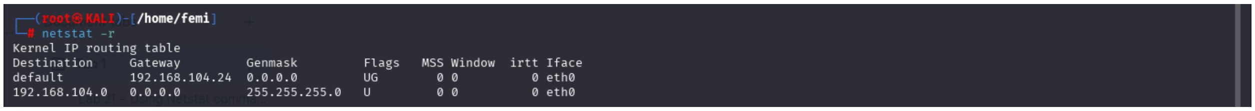


```
┌──(root㉿KALI)-[/home/femi]
└─# netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

Task 4:

We can view the kernel routing table by using the following command:

netstat -r



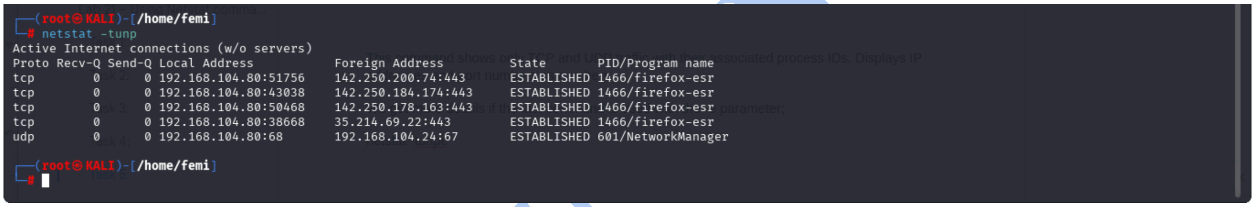
```
┌──(root㉿KALI)-[/home/femi]
└─# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.104.24  0.0.0.0         UG        0 0          0 eth0
192.168.104.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

Note: netstat -r and route -e product the same result.

Task 5:

We can make netstat show us the process IDs and where they belong by using the following command:

netstat -tunp

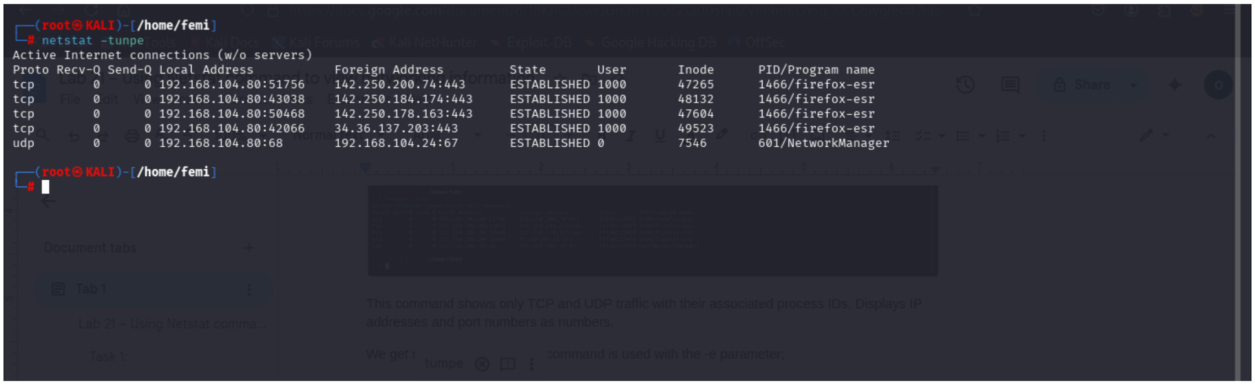


```
┌──(root㉿KALI)-[/home/femi]
└─# netstat -tunp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.104.80:51756    142.250.200.74:443      ESTABLISHED 1466/firefox-esr
tcp        0      0 192.168.104.80:43038    142.250.184.174:443     ESTABLISHED 1466/firefox-esr
tcp        0      0 192.168.104.80:50468    142.250.178.163:443     ESTABLISHED 1466/firefox-esr
tcp        0      0 192.168.104.80:38668    35.214.69.22:443        ESTABLISHED 1466/firefox-esr
udp        0      0 192.168.104.80:68       192.168.104.24:67       ESTABLISHED 601/NetworkManager

┌──(root㉿KALI)-[/home/femi]
└─# █
```

This command shows only TCP and UDP traffic with their associated process IDs. Displays IP addresses and port numbers as numbers.

We get more details if the last command is used with the -e parameter;

netstat -tunpe

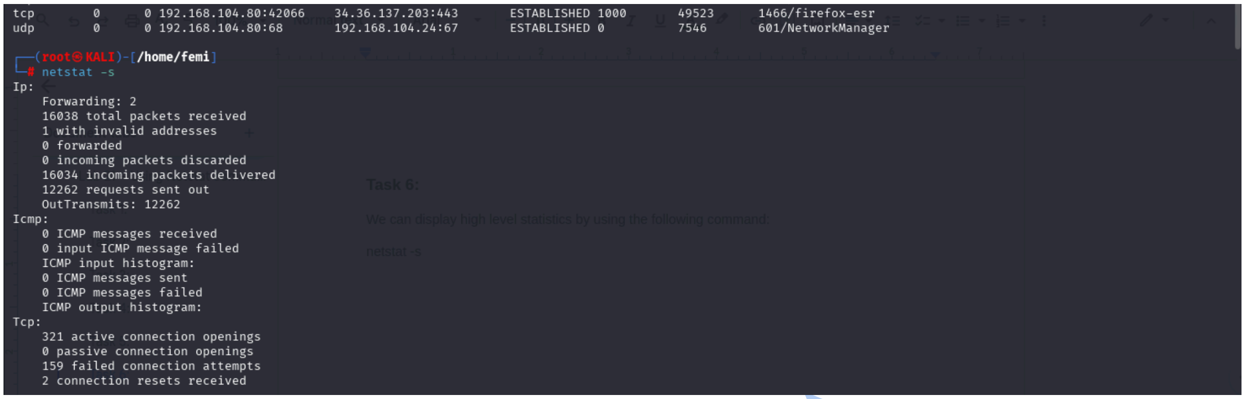


```
┌──(root㉿KALI)-[/home/femi]
└─# netstat -tunpe
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 192.168.104.80:51756    142.250.200.74:443      ESTABLISHED 1000       47265      1466/firefox-esr
tcp        0      0 192.168.104.80:43038    142.250.184.174:443     ESTABLISHED 1000       48132      1466/firefox-esr
tcp        0      0 192.168.104.80:50468    142.250.178.163:443     ESTABLISHED 1000       47604      1466/firefox-esr
tcp        0      0 192.168.104.80:42066    34.36.137.203:443       ESTABLISHED 1000       49523      1466/firefox-esr
udp        0      0 192.168.104.80:68       192.168.104.24:67       ESTABLISHED 0          7546       601/NetworkManager

┌──(root㉿KALI)-[/home/femi]
└─# █
```

Task 6:

We can display high level statistics by using the following command:

netstat -s



```
tcp        0      0 192.168.104.80:42066    34.36.137.203:443       ESTABLISHED 1000       49523      1466/firefox-esr
udp        0      0 192.168.104.80:68       192.168.104.24:67       ESTABLISHED 0          7546       601/NetworkManager

┌──(root㉿KALI)-[/home/femi]
└─# netstat -s
Ip:
    Forwarding: 2
    16038 total packets received
    1 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    16034 incoming packets delivered
    12262 requests sent out
    OutTransmits: 12262
Icmp:
    0 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
    0 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
Tcp:
    321 active connection openings
    0 passive connection openings
    159 failed connection attempts
    2 connection resets received
```

END

FEMI LANA