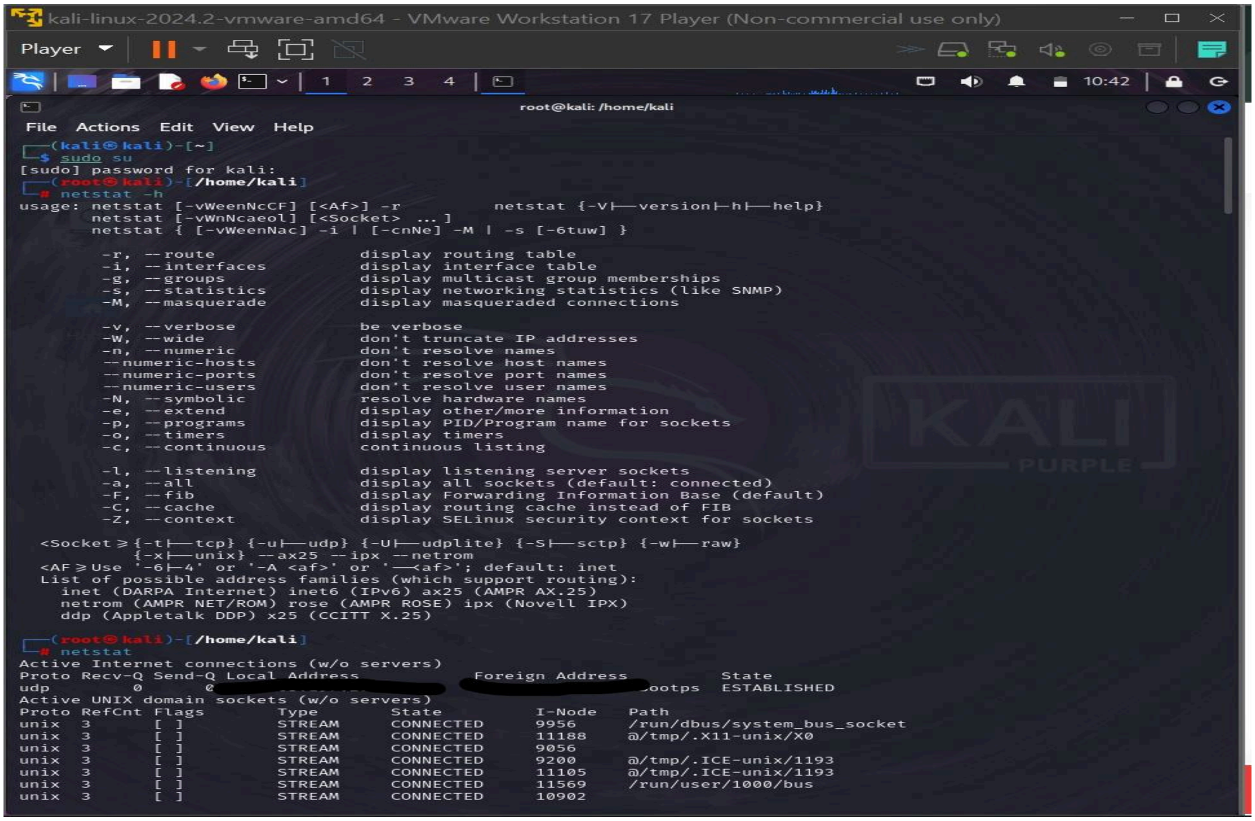
USING NETSTAT COMMAND TO VIEW NETWORKING INFORMATION

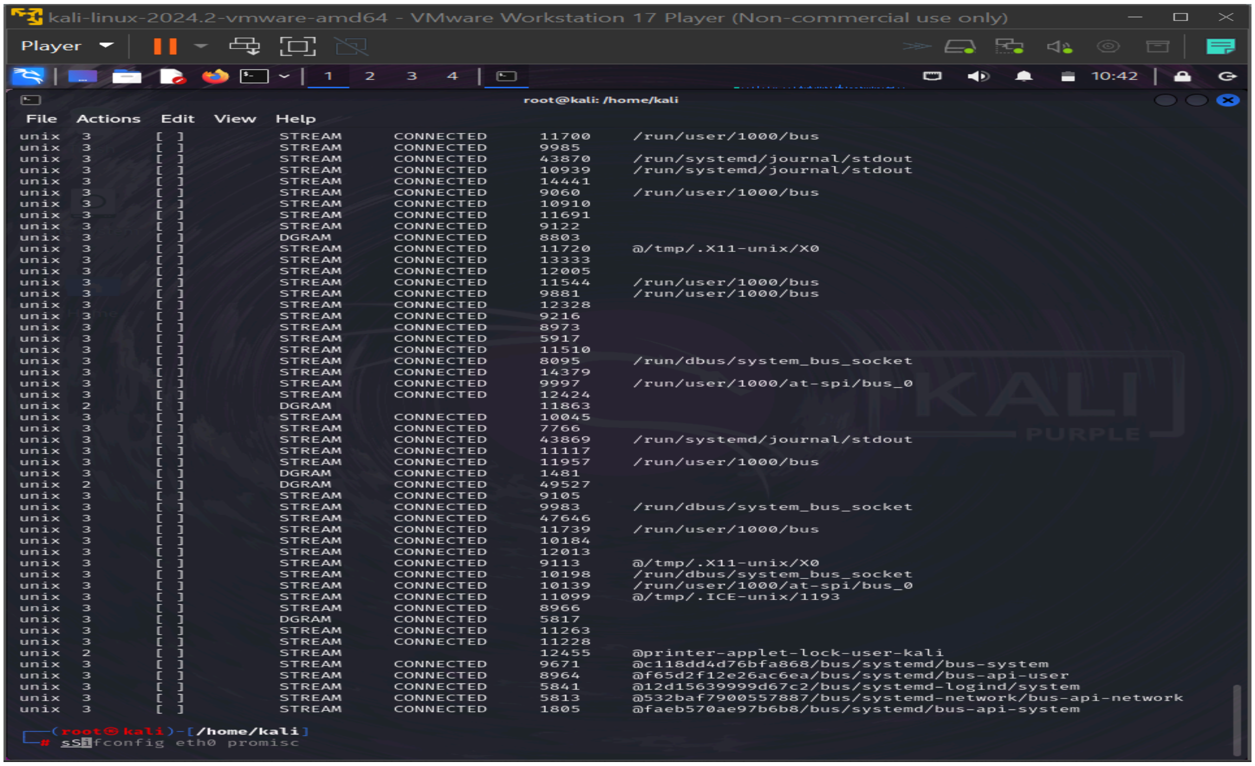
Tools : NETSTAT on KALI

NETSTAT (Network Statistics) is a command-line tool used to display network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. It's typically used for troubleshooting network issues and monitoring the network activity on a system.

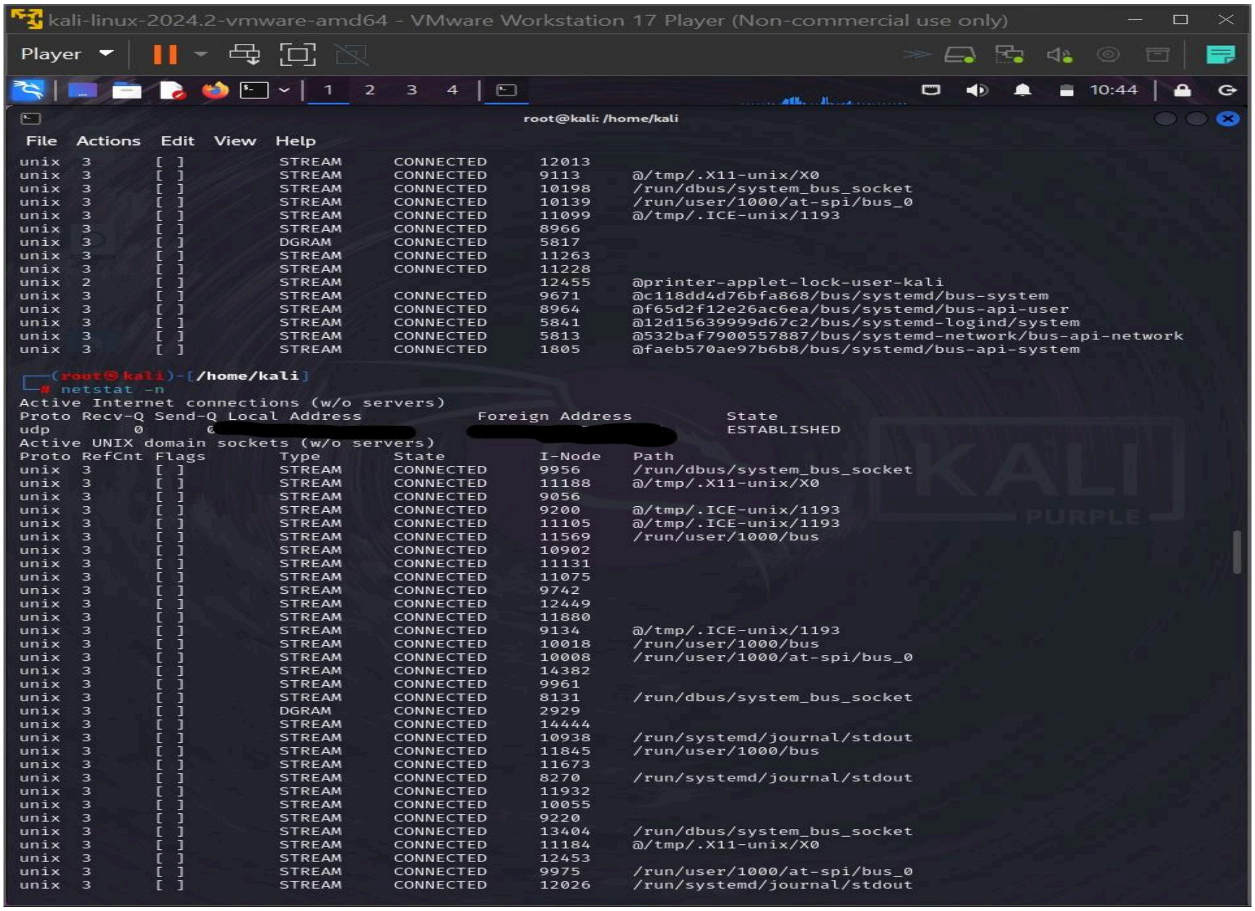
Input from netstat :


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
10:42
root@kali: /home/kali
File Actions Edit View Help

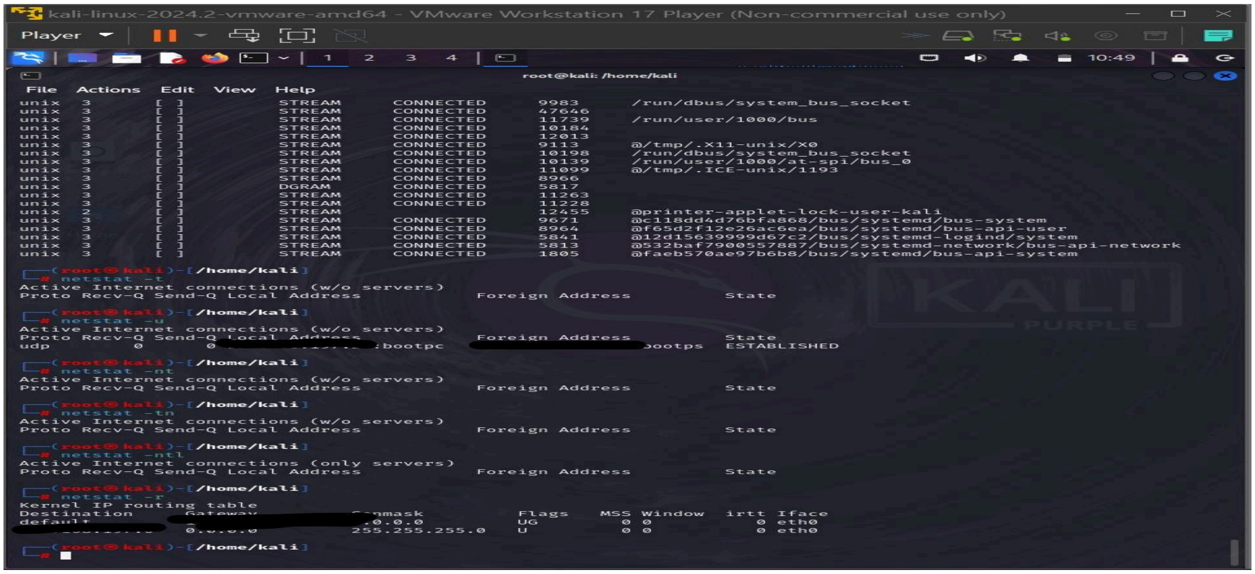
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# netstat -h
usage: netstat [-vWeenNcCF] [<Af>] -r         netstat {-V|--version|-h|--help}
       netstat [-vWnNcaeol] [<Socket> ...]
       netstat { [-vWeenNac] -i | [-cnNe] -M | -s [-6tuw] }

        -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}
           {-x|--unix} --ax25 --ipx --netrom
  <AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
  List of possible address families (which support routing):
    inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) ipx (Novell IPX)
    ddp (Appletalk DDP) x25 (CCITT X.25)

┌──(root㉿kali)-[/home/kali]
└─# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 [redacted]              [redacted]ootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     9956     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     11188    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     9056
unix  3      [ ]         STREAM     CONNECTED     9200     @/tmp/.ICE-unix/1193
unix  3      [ ]         STREAM     CONNECTED     11105    @/tmp/.ICE-unix/1193
unix  3      [ ]         STREAM     CONNECTED     11569    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10902
```


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
10:42
root@kali: /home/kali
File Actions Edit View Help

```
unix  3      [ ]         STREAM     CONNECTED     11700    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9985
unix  3      [ ]         STREAM     CONNECTED     43870    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     10939    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     14441
unix  3      [ ]         STREAM     CONNECTED     9060     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10910
unix  3      [ ]         STREAM     CONNECTED     11691
unix  3      [ ]         STREAM     CONNECTED     9122
unix  3      [ ]         DGRAM      CONNECTED     8803
unix  3      [ ]         STREAM     CONNECTED     11720    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     13333
unix  3      [ ]         STREAM     CONNECTED     12005
unix  3      [ ]         STREAM     CONNECTED     11544    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9881     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     12328
unix  3      [ ]         STREAM     CONNECTED     9216
unix  3      [ ]         STREAM     CONNECTED     8973
unix  3      [ ]         STREAM     CONNECTED     5917
unix  3      [ ]         STREAM     CONNECTED     11510
unix  3      [ ]         STREAM     CONNECTED     8095     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     14379
unix  3      [ ]         STREAM     CONNECTED     9997     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     12424
unix  2      [ ]         DGRAM                    11863
unix  3      [ ]         STREAM     CONNECTED     10045
unix  3      [ ]         STREAM     CONNECTED     7766
unix  3      [ ]         STREAM     CONNECTED     43869    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     11117
unix  3      [ ]         STREAM     CONNECTED     11957    /run/user/1000/bus
unix  3      [ ]         DGRAM      CONNECTED     1481
unix  2      [ ]         DGRAM      CONNECTED     49527
unix  3      [ ]         STREAM     CONNECTED     9105
unix  3      [ ]         STREAM     CONNECTED     9983     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     47646
unix  3      [ ]         STREAM     CONNECTED     11739    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10184
unix  3      [ ]         STREAM     CONNECTED     12013
unix  3      [ ]         STREAM     CONNECTED     9113     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     10198    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     10139    /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     11099    @/tmp/.ICE-unix/1193
unix  3      [ ]         STREAM     CONNECTED     8966
unix  3      [ ]         DGRAM      CONNECTED     5817
unix  3      [ ]         STREAM     CONNECTED     11263
unix  3      [ ]         STREAM     CONNECTED     11228
unix  2      [ ]         STREAM                   12455    @printer-applet-lock-user-kali
unix  3      [ ]         STREAM     CONNECTED     9671     @c118dd4d76bfa868/bus/systemd/bus-system
unix  3      [ ]         STREAM     CONNECTED     8964     @f65d2f12e26ac6ea/bus/systemd/bus-api-user
unix  3      [ ]         STREAM     CONNECTED     5841     @12d15639999d67c2/bus/systemd-logind/system
unix  3      [ ]         STREAM     CONNECTED     5813     @532baf7900557887/bus/systemd-network/bus-api-network
unix  3      [ ]         STREAM     CONNECTED     1805     @faeb570ae97b6b8/bus/systemd/bus-api-system

┌──(root㉿kali)-[/home/kali]
└─# sSifconfig eth0 promisc
```

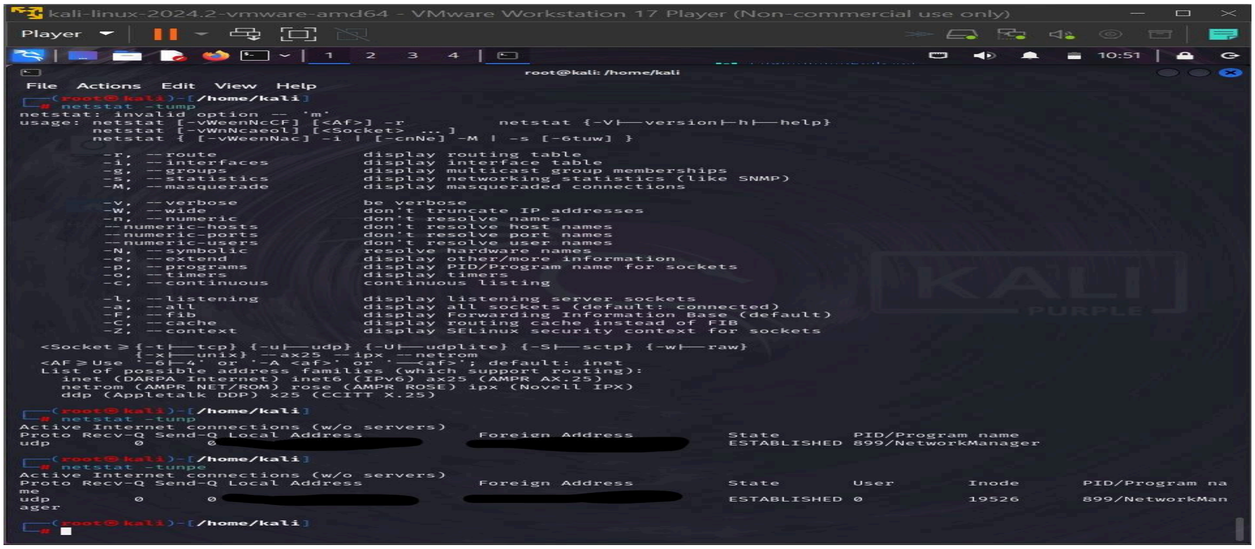

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
10:44
root@kali: /home/kali
File Actions Edit View Help

```
unix  3      [ ]         STREAM     CONNECTED     12013
unix  3      [ ]         STREAM     CONNECTED     9113     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     10198    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     10139    /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     11099    @/tmp/.ICE-unix/1193
unix  3      [ ]         STREAM     CONNECTED     8966
unix  3      [ ]         DGRAM      CONNECTED     5817
unix  3      [ ]         STREAM     CONNECTED     11263
unix  3      [ ]         STREAM     CONNECTED     11228
unix  2      [ ]         STREAM                   12455    @printer-applet-lock-user-kali
unix  3      [ ]         STREAM     CONNECTED     9671     @c118dd4d76bfa868/bus/systemd/bus-system
unix  3      [ ]         STREAM     CONNECTED     8964     @f65d2f12e26ac6ea/bus/systemd/bus-api-user
unix  3      [ ]         STREAM     CONNECTED     5841     @12d15639999d67c2/bus/systemd-logind/system
unix  3      [ ]         STREAM     CONNECTED     5813     @532baf7900557887/bus/systemd-network/bus-api-network
unix  3      [ ]         STREAM     CONNECTED     1805     @faeb570ae97b6b8/bus/systemd/bus-api-system

┌──(root㉿kali)-[/home/kali]
└─# netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      [redacted]                [redacted]              ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     9956     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     11188    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     9056
unix  3      [ ]         STREAM     CONNECTED     9200     @/tmp/.ICE-unix/1193
unix  3      [ ]         STREAM     CONNECTED     11105    @/tmp/.ICE-unix/1193
unix  3      [ ]         STREAM     CONNECTED     11569    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10902
unix  3      [ ]         STREAM     CONNECTED     11131
unix  3      [ ]         STREAM     CONNECTED     11075
unix  3      [ ]         STREAM     CONNECTED     9742
unix  3      [ ]         STREAM     CONNECTED     12449
unix  3      [ ]         STREAM     CONNECTED     11880
unix  3      [ ]         STREAM     CONNECTED     9134     @/tmp/.ICE-unix/1193
unix  3      [ ]         STREAM     CONNECTED     10018    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10008    /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     14382
unix  3      [ ]         STREAM     CONNECTED     9961
unix  3      [ ]         STREAM     CONNECTED     8131     /run/dbus/system_bus_socket
unix  3      [ ]         DGRAM      CONNECTED     2929
unix  3      [ ]         STREAM     CONNECTED     14444
unix  3      [ ]         STREAM     CONNECTED     10938    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     11845    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     11673
unix  3      [ ]         STREAM     CONNECTED     8270     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     11932
unix  3      [ ]         STREAM     CONNECTED     10055
unix  3      [ ]         STREAM     CONNECTED     9220
unix  3      [ ]         STREAM     CONNECTED     13404    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     11184    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12453
unix  3      [ ]         STREAM     CONNECTED     9975     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     12026    /run/systemd/journal/stdout
```



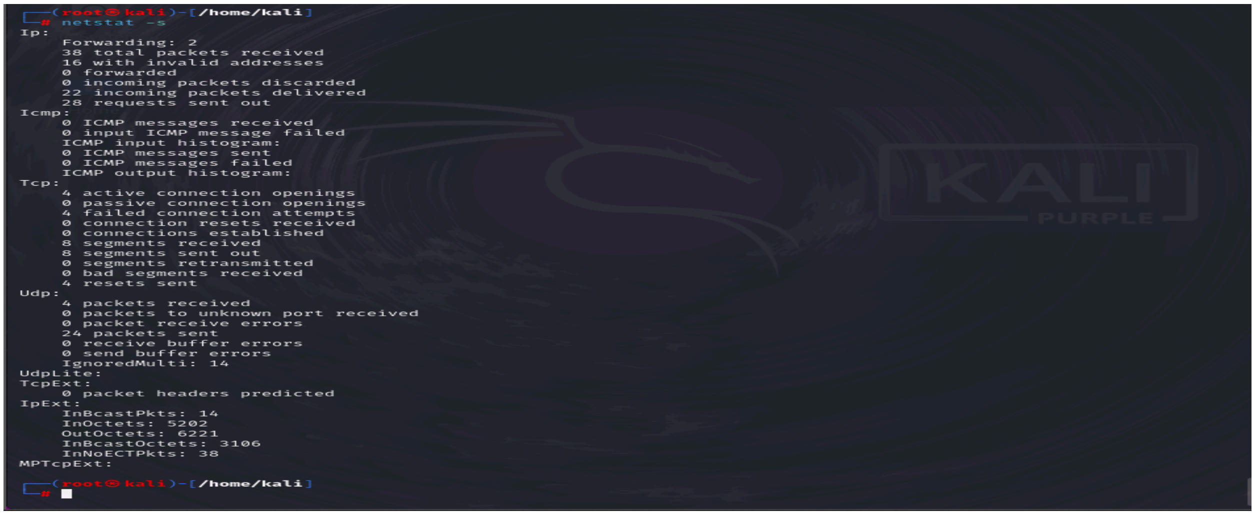
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
10:49
root@kali: /home/kali
File Actions Edit View Help

```
unix  3      [ ]         STREAM     CONNECTED     9983     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     47646
unix  3      [ ]         STREAM     CONNECTED     11739    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10184
unix  3      [ ]         STREAM     CONNECTED     12013
unix  3      [ ]         STREAM     CONNECTED     9113     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     10198    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     10139    /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     11099    @/tmp/.ICE-unix/1193
unix  3      [ ]         STREAM     CONNECTED     8966
unix  3      [ ]         DGRAM      CONNECTED     5817
unix  3      [ ]         STREAM     CONNECTED     11263
unix  3      [ ]         STREAM     CONNECTED     11228
unix  2      [ ]         STREAM                   12455    @printer-applet-lock-user-kali
unix  3      [ ]         STREAM     CONNECTED     9671     @c118dd4d76bfa868/bus/systemd/bus-system
unix  3      [ ]         STREAM     CONNECTED     8964     @f65d2f12e26ac6ea/bus/systemd/bus-api-user
unix  3      [ ]         STREAM     CONNECTED     5841     @12d15639999d67c2/bus/systemd-logind/system
unix  3      [ ]         STREAM     CONNECTED     5813     @532baf7900557887/bus/systemd-network/bus-api-network
unix  3      [ ]         STREAM     CONNECTED     1805     @faeb570ae97b6b8/bus/systemd/bus-api-system

┌──(root㉿kali)-[/home/kali]
└─# netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

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

┌──(root㉿kali)-[/home/kali]
└─# netstat -nt
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

┌──(root㉿kali)-[/home/kali]
└─# netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

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

┌──(root㉿kali)-[/home/kali]
└─# netstat -r
Kernel IP routing table
Destination     [redacted]nmask         Flags   MSS Window  irtt Iface
default         [redacted].0.0.0        UG        0 0          0 eth0
[redacted]      0.0.0.0         255.255.255.0   U         0 0          0 eth0

┌──(root㉿kali)-[/home/kali]
└─# █
```



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
10:51
root@kali: /home/kali
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/kali]
└─# netstat -tump
netstat: invalid option -- 'm'
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}
           {-x|--unix} --ax25 --ipx --netrom
  <AF>=Use '-6|-4' or '-A <af>' or '--<af>'; default: inet
  List of possible address families (which support routing):
    inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) ipx (Novell IPX)
    ddp (Appletalk DDP) x25 (CCITT X.25)

┌──(root㉿kali)-[/home/kali]
└─# netstat -tunp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 [redacted]              [redacted]              ESTABLISHED 899/NetworkManager

┌──(root㉿kali)-[/home/kali]
└─# netstat -tunpe
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program na
me
udp        0      0 [redacted]              [redacted]              ESTABLISHED 0          19526      899/NetworkMan
ager

┌──(root㉿kali)-[/home/kali]
└─# █
```



```
┌──(root㉿kali)-[/home/kali]
└─# netstat -s
Ip:
    Forwarding: 2
    38 total packets received
    16 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    22 incoming packets delivered
    28 requests sent out
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:
    4 active connection openings
    0 passive connection openings
    4 failed connection attempts
    0 connection resets received
    0 connections established
    8 segments received
    8 segments sent out
    0 segments retransmitted
    0 bad segments received
    4 resets sent
Udp:
    4 packets received
    0 packets to unknown port received
    0 packet receive errors
    24 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 14
UdpLite:
TcpExt:
    0 packet headers predicted
IpExt:
    InBcastPkts: 14
    InOctets: 5202
    OutOctets: 6221
    InBcastOctets: 3106
    InNoECTPkts: 38
MPTcpExt:

┌──(root㉿kali)-[/home/kali]
└─# █
```

Here we would be using netstat to print network connection, routing tables, interface statistics, masquerade connections and multicast membership.

First of all, we have to be the ROOT user, we would go on and type SUDO SU in the terminal. Then we would begin by viewing the help information screen by executing the following command **netstat -h** We will then view all active connections by typing the following: **netstat.** We can use netstat to display both local and foreign addresses in numeric IP form using the "-n" parameter. **Netstat -n.** If we want to view only TCP connections, we need to add the "-t" parameter. **netstat -t**
Similarly, if we want to view only UDP connections, we need to add the "-u" parameter. netstat -u. We can also combine and operate multiple parameters in a single command as follows : **netstat -nt**

netstat allows us to view only connections which are listening. We can do this by typing this command: **netstat -ntl** "0.0.0.0" in the local address column indicates all IP addresses that are listening. "0.0.0.0:*" in the foreign address column indicates everyone and all ports in the IP space. In the last lines, it shows that we are in a state of listening for each connection. We can view the kernel routing table by using the following command**: netstat -r**

Kindly note that netstat -r and route -e produce the same result.

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

We can also display high level statistics by using the following command: **netstat -s**