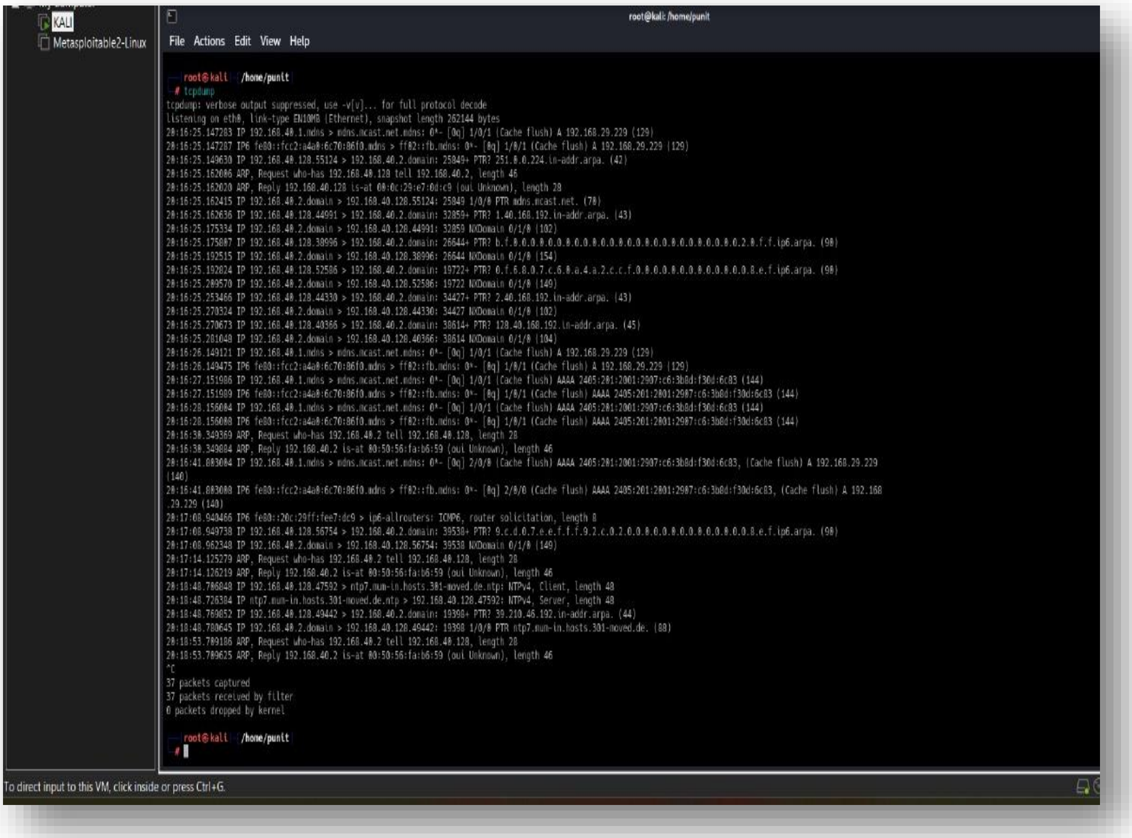
ADVANCE NETWORK SECURITY

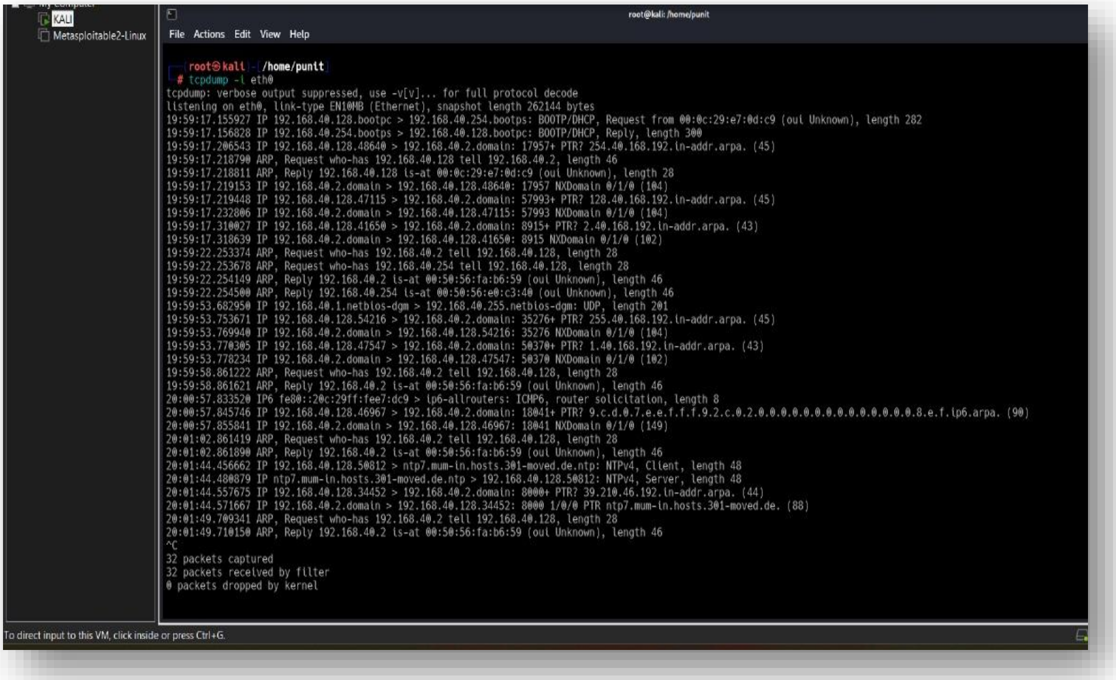
LAB-1: Learn to use commands like tcpdump, netstat, ifconfig, nslookup and traceroute.

1. **TCPDUMP**: tcpdump is a command-line packet analyzer tool used for capturing and analyzing network traffic in real-time.

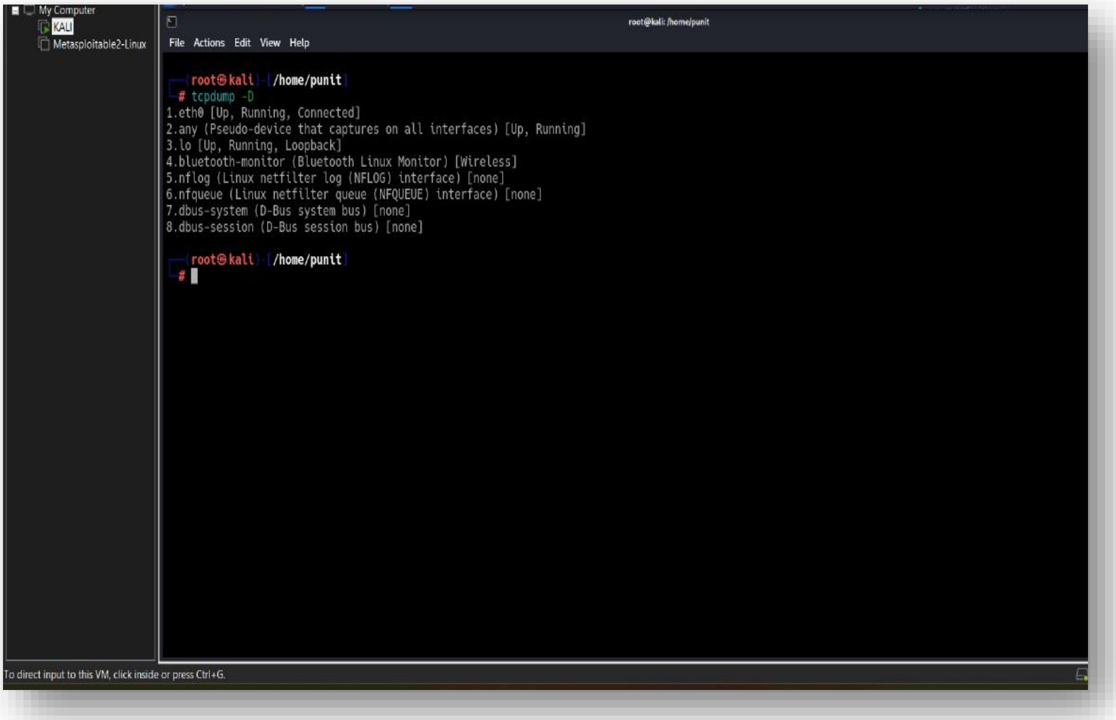


KALI
Metasploitable2-Linux
root@kali: /home/punit
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

```
┌──(root㉿kali)-[/home/punit]
└─# tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20:16:25.147283 IP 192.168.40.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 1/0/1 (Cache flush) A 192.168.29.229 (129)
20:16:25.147287 IP6 fe80::fcc2:a4a0:6c70:86f0.mdns > ff02::fb.mdns: 0*- [0q] 1/0/1 (Cache flush) A 192.168.29.229 (129)
20:16:25.149630 IP 192.168.40.128.55124 > 192.168.40.2.domain: 25849+ PTR? 251.0.0.224.in-addr.arpa. (42)
20:16:25.162006 ARP, Request who-has 192.168.40.128 tell 192.168.40.2, length 46
20:16:25.162020 ARP, Reply 192.168.40.128 is-at 00:0c:29:e7:0d:c9 (oui Unknown), length 28
20:16:25.162415 IP 192.168.40.2.domain > 192.168.40.128.55124: 25849 1/0/0 PTR mdns.mcast.net. (78)
20:16:25.162636 IP 192.168.40.128.44991 > 192.168.40.2.domain: 32859+ PTR? 1.40.168.192.in-addr.arpa. (43)
20:16:25.175334 IP 192.168.40.2.domain > 192.168.40.128.44991: 32859 NXDomain 0/1/0 (102)
20:16:25.175807 IP 192.168.40.128.38996 > 192.168.40.2.domain: 26644+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
20:16:25.192515 IP 192.168.40.2.domain > 192.168.40.128.38996: 26644 NXDomain 0/1/0 (154)
20:16:25.192824 IP 192.168.40.128.52586 > 192.168.40.2.domain: 19722+ PTR? 0.f.6.8.0.7.c.6.0.a.4.a.2.c.c.f.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
20:16:25.209570 IP 192.168.40.2.domain > 192.168.40.128.52586: 19722 NXDomain 0/1/0 (149)
20:16:25.253466 IP 192.168.40.128.44330 > 192.168.40.2.domain: 34427+ PTR? 2.40.168.192.in-addr.arpa. (43)
20:16:25.270324 IP 192.168.40.2.domain > 192.168.40.128.44330: 34427 NXDomain 0/1/0 (102)
20:16:25.270673 IP 192.168.40.128.40366 > 192.168.40.2.domain: 38614+ PTR? 128.40.168.192.in-addr.arpa. (45)
20:16:25.281048 IP 192.168.40.2.domain > 192.168.40.128.40366: 38614 NXDomain 0/1/0 (104)
20:16:26.149121 IP 192.168.40.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 1/0/1 (Cache flush) A 192.168.29.229 (129)
20:16:26.149475 IP6 fe80::fcc2:a4a0:6c70:86f0.mdns > ff02::fb.mdns: 0*- [0q] 1/0/1 (Cache flush) A 192.168.29.229 (129)
20:16:27.151986 IP 192.168.40.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 1/0/1 (Cache flush) AAAA 2405:201:2001:2907:c6:3b8d:f30d:6c83 (144)
20:16:27.151989 IP6 fe80::fcc2:a4a0:6c70:86f0.mdns > ff02::fb.mdns: 0*- [0q] 1/0/1 (Cache flush) AAAA 2405:201:2001:2907:c6:3b8d:f30d:6c83 (144)
20:16:28.156084 IP 192.168.40.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 1/0/1 (Cache flush) AAAA 2405:201:2001:2907:c6:3b8d:f30d:6c83 (144)
20:16:28.156088 IP6 fe80::fcc2:a4a0:6c70:86f0.mdns > ff02::fb.mdns: 0*- [0q] 1/0/1 (Cache flush) AAAA 2405:201:2001:2907:c6:3b8d:f30d:6c83 (144)
20:16:30.349369 ARP, Request who-has 192.168.40.2 tell 192.168.40.128, length 28
20:16:30.349884 ARP, Reply 192.168.40.2 is-at 00:50:56:fa:b6:59 (oui Unknown), length 46
20:16:41.883084 IP 192.168.40.1.mdns > mdns.mcast.net.mdns: 0*- [0q] 2/0/0 (Cache flush) AAAA 2405:201:2001:2907:c6:3b8d:f30d:6c83, (Cache flush) A 192.168.29.229
(140)
20:16:41.883088 IP6 fe80::fcc2:a4a0:6c70:86f0.mdns > ff02::fb.mdns: 0*- [0q] 2/0/0 (Cache flush) AAAA 2405:201:2001:2907:c6:3b8d:f30d:6c83, (Cache flush) A 192.168
.29.229 (140)
20:17:08.940466 IP6 fe80::20c:29ff:fee7:dc9 > ip6-allrouters: ICMP6, router solicitation, length 8
20:17:08.949738 IP 192.168.40.128.56754 > 192.168.40.2.domain: 39538+ PTR? 9.c.d.0.7.e.e.f.f.f.9.2.c.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
20:17:08.962348 IP 192.168.40.2.domain > 192.168.40.128.56754: 39538 NXDomain 0/1/0 (149)
20:17:14.125279 ARP, Request who-has 192.168.40.2 tell 192.168.40.128, length 28
20:17:14.126219 ARP, Reply 192.168.40.2 is-at 00:50:56:fa:b6:59 (oui Unknown), length 46
20:18:48.706848 IP 192.168.40.128.47592 > ntp7.mum-in.hosts.301-moved.de.ntp: NTPv4, Client, length 48
20:18:48.726384 IP ntp7.mum-in.hosts.301-moved.de.ntp > 192.168.40.128.47592: NTPv4, Server, length 48
20:18:48.769852 IP 192.168.40.128.49442 > 192.168.40.2.domain: 19398+ PTR? 39.210.46.192.in-addr.arpa. (44)
20:18:48.780645 IP 192.168.40.2.domain > 192.168.40.128.49442: 19398 1/0/0 PTR ntp7.mum-in.hosts.301-moved.de. (88)
20:18:53.709186 ARP, Request who-has 192.168.40.2 tell 192.168.40.128, length 28
20:18:53.709625 ARP, Reply 192.168.40.2 is-at 00:50:56:fa:b6:59 (oui Unknown), length 46
^C
37 packets captured
37 packets received by filter
0 packets dropped by kernel

┌──(root㉿kali)-[/home/punit]
└─#
```

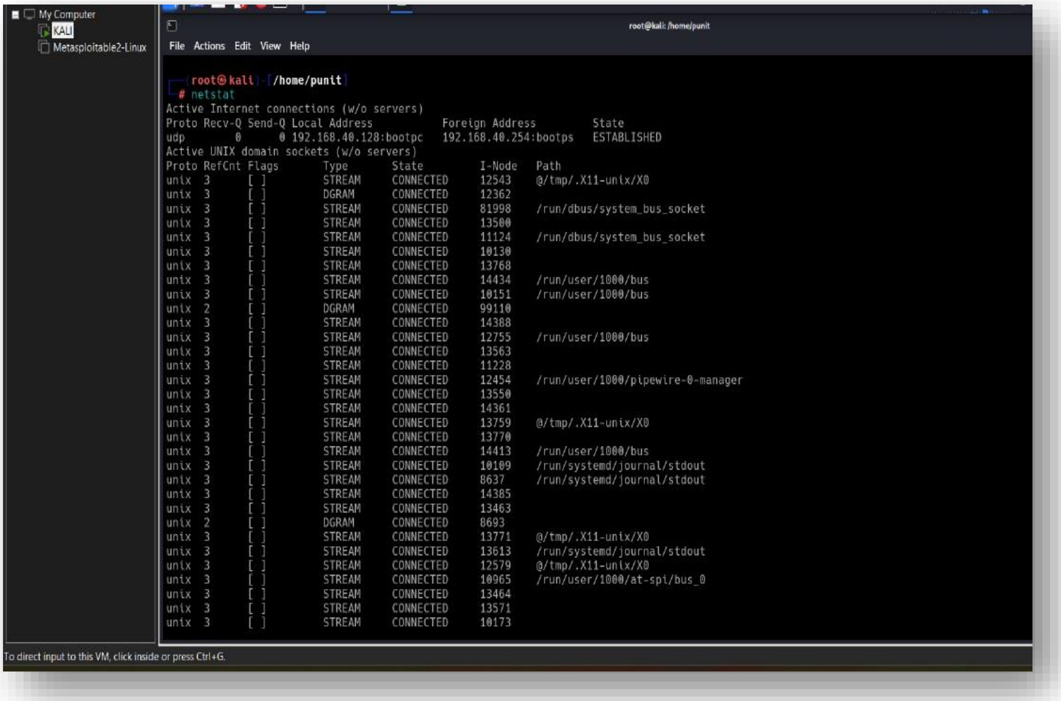

My Computer
KALI
Metasploitable2-Linux
root@kali: /home/punit
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

```
┌──(root㉿kali)-[/home/punit]
└─# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:59:17.155927 IP 192.168.40.128.bootpc > 192.168.40.254.bootps: BOOTP/DHCP, Request from 00:0c:29:e7:0d:c9 (oui Unknown), length 282
19:59:17.156828 IP 192.168.40.254.bootps > 192.168.40.128.bootpc: BOOTP/DHCP, Reply, length 300
19:59:17.206543 IP 192.168.40.128.48640 > 192.168.40.2.domain: 17957+ PTR? 254.40.168.192.in-addr.arpa. (45)
19:59:17.218790 ARP, Request who-has 192.168.40.128 tell 192.168.40.2, length 46
19:59:17.218811 ARP, Reply 192.168.40.128 is-at 00:0c:29:e7:0d:c9 (oui Unknown), length 28
19:59:17.219153 IP 192.168.40.2.domain > 192.168.40.128.48640: 17957 NXDomain 0/1/0 (104)
19:59:17.219448 IP 192.168.40.128.47115 > 192.168.40.2.domain: 57993+ PTR? 128.40.168.192.in-addr.arpa. (45)
19:59:17.232806 IP 192.168.40.2.domain > 192.168.40.128.47115: 57993 NXDomain 0/1/0 (104)
19:59:17.310027 IP 192.168.40.128.41650 > 192.168.40.2.domain: 8915+ PTR? 2.40.168.192.in-addr.arpa. (43)
19:59:17.318639 IP 192.168.40.2.domain > 192.168.40.128.41650: 8915 NXDomain 0/1/0 (102)
19:59:22.253374 ARP, Request who-has 192.168.40.2 tell 192.168.40.128, length 28
19:59:22.253678 ARP, Request who-has 192.168.40.254 tell 192.168.40.128, length 28
19:59:22.254149 ARP, Reply 192.168.40.2 is-at 00:50:56:fa:b6:59 (oui Unknown), length 46
19:59:22.254500 ARP, Reply 192.168.40.254 is-at 00:50:56:e0:c3:40 (oui Unknown), length 46
19:59:53.682950 IP 192.168.40.1.netbios-dgm > 192.168.40.255.netbios-dgm: UDP, length 201
19:59:53.753671 IP 192.168.40.128.54216 > 192.168.40.2.domain: 35276+ PTR? 255.40.168.192.in-addr.arpa. (45)
19:59:53.769940 IP 192.168.40.2.domain > 192.168.40.128.54216: 35276 NXDomain 0/1/0 (104)
19:59:53.770305 IP 192.168.40.128.47547 > 192.168.40.2.domain: 50370+ PTR? 1.40.168.192.in-addr.arpa. (43)
19:59:53.778234 IP 192.168.40.2.domain > 192.168.40.128.47547: 50370 NXDomain 0/1/0 (102)
19:59:58.861222 ARP, Request who-has 192.168.40.2 tell 192.168.40.128, length 28
19:59:58.861621 ARP, Reply 192.168.40.2 is-at 00:50:56:fa:b6:59 (oui Unknown), length 46
20:00:57.833520 IP6 fe80::20c:29ff:fee7:dc9 > ip6-allrouters: ICMP6, router solicitation, length 8
20:00:57.845746 IP 192.168.40.128.46967 > 192.168.40.2.domain: 18041+ PTR? 9.c.d.0.7.e.e.f.f.f.9.2.c.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
20:00:57.855841 IP 192.168.40.2.domain > 192.168.40.128.46967: 18041 NXDomain 0/1/0 (149)
20:01:02.861419 ARP, Request who-has 192.168.40.2 tell 192.168.40.128, length 28
20:01:02.861890 ARP, Reply 192.168.40.2 is-at 00:50:56:fa:b6:59 (oui Unknown), length 46
20:01:44.456662 IP 192.168.40.128.50812 > ntp7.mum-in.hosts.301-moved.de.ntp: NTPv4, Client, length 48
20:01:44.480879 IP ntp7.mum-in.hosts.301-moved.de.ntp > 192.168.40.128.50812: NTPv4, Server, length 48
20:01:44.557675 IP 192.168.40.128.34452 > 192.168.40.2.domain: 8000+ PTR? 39.210.46.192.in-addr.arpa. (44)
20:01:44.571667 IP 192.168.40.2.domain > 192.168.40.128.34452: 8000 1/0/0 PTR ntp7.mum-in.hosts.301-moved.de. (88)
20:01:49.709341 ARP, Request who-has 192.168.40.2 tell 192.168.40.128, length 28
20:01:49.710150 ARP, Reply 192.168.40.2 is-at 00:50:56:fa:b6:59 (oui Unknown), length 46
^C
32 packets captured
32 packets received by filter
0 packets dropped by kernel
```


My Computer
KALI
Metasploitable2-Linux
root@kali: /home/punit
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

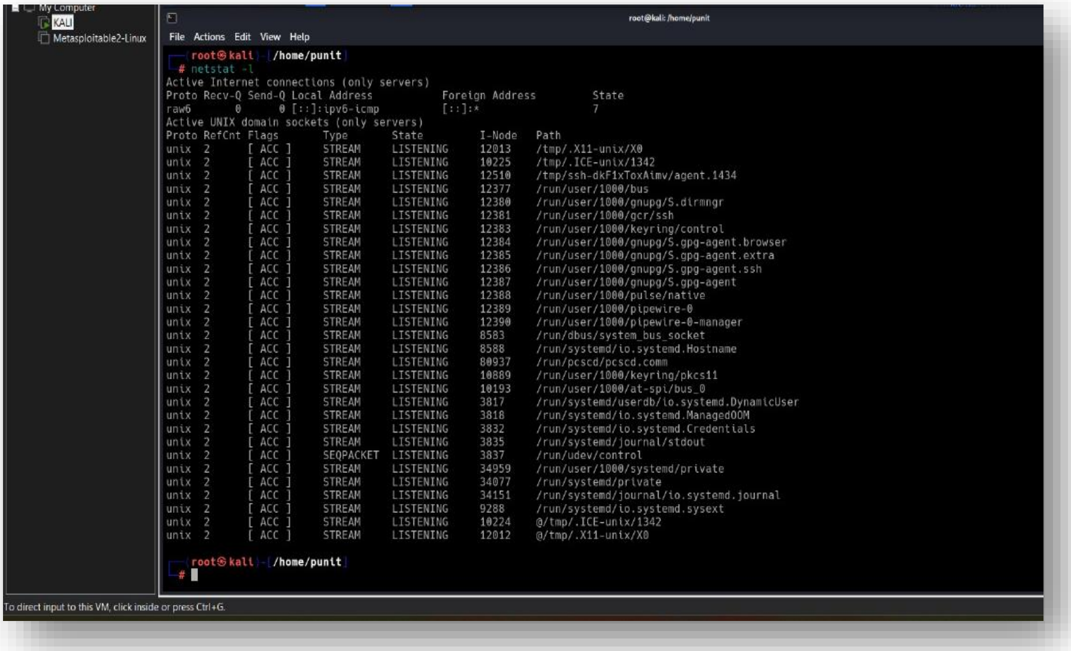
```
┌──(root㉿kali)-[/home/punit]
└─# tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]

┌──(root㉿kali)-[/home/punit]
└─# 
```

2. **NETSTAT:** netstat (short for "network statistics") is a command-line tool used for displaying network-related information on a computer or network device.



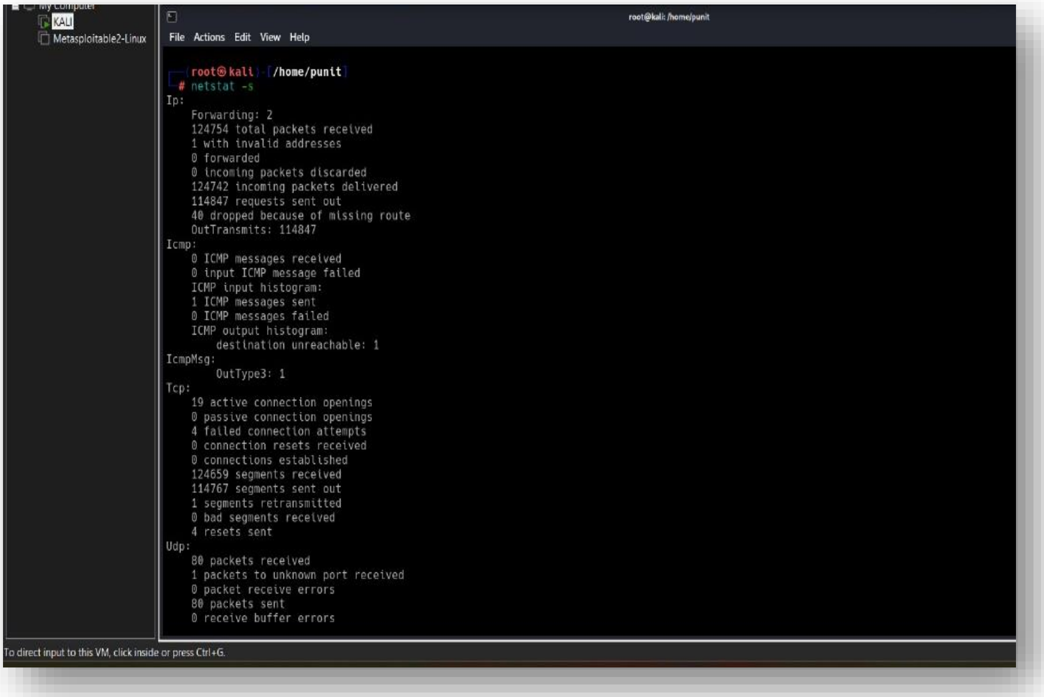
```
┌──(root㉿kali)-[/home/punit]
└─# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.40.128:bootpc   192.168.40.254:bootps   ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     12543    @/tmp/.X11-unix/X0
unix  3      [ ]         DGRAM      CONNECTED     12362
unix  3      [ ]         STREAM     CONNECTED     81998    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     13500
unix  3      [ ]         STREAM     CONNECTED     11124    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     10130
unix  3      [ ]         STREAM     CONNECTED     13768
unix  3      [ ]         STREAM     CONNECTED     14434    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10151    /run/user/1000/bus
unix  2      [ ]         DGRAM      CONNECTED     99110
unix  3      [ ]         STREAM     CONNECTED     14388
unix  3      [ ]         STREAM     CONNECTED     12755    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     13563
unix  3      [ ]         STREAM     CONNECTED     11228
unix  3      [ ]         STREAM     CONNECTED     12454    /run/user/1000/pipewire-0-manager
unix  3      [ ]         STREAM     CONNECTED     13550
unix  3      [ ]         STREAM     CONNECTED     14361
unix  3      [ ]         STREAM     CONNECTED     13759    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     13770
unix  3      [ ]         STREAM     CONNECTED     14413    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10109    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     8637     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     14385
unix  3      [ ]         STREAM     CONNECTED     13463
unix  2      [ ]         DGRAM      CONNECTED     8693
unix  3      [ ]         STREAM     CONNECTED     13771    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     13613    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12579    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     10965    /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     13464
unix  3      [ ]         STREAM     CONNECTED     13571
unix  3      [ ]         STREAM     CONNECTED     10173
```

To direct input to this VM, click inside or press Ctrl+G.



```
┌──(root㉿kali)-[/home/punit]
└─# netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
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     12013    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     10225    /tmp/.ICE-unix/1342
unix  2      [ ACC ]     STREAM     LISTENING     12510    /tmp/ssh-dkF1xToxAimv/agent.1434
unix  2      [ ACC ]     STREAM     LISTENING     12377    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     12380    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     12381    /run/user/1000/gcr/ssh
unix  2      [ ACC ]     STREAM     LISTENING     12383    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     12384    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     12385    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     12386    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     12387    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     12388    /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     12389    /run/user/1000/pipewire-0
unix  2      [ ACC ]     STREAM     LISTENING     12390    /run/user/1000/pipewire-0-manager
unix  2      [ ACC ]     STREAM     LISTENING     8583     /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     8588     /run/systemd/io.systemd.Hostname
unix  2      [ ACC ]     STREAM     LISTENING     80937    /run/pcscd/pcscd.comm
unix  2      [ ACC ]     STREAM     LISTENING     10889    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     10193    /run/user/1000/at-spi/bus_0
unix  2      [ ACC ]     STREAM     LISTENING     3817     /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING     3818     /run/systemd/io.systemd.ManagedOOM
unix  2      [ ACC ]     STREAM     LISTENING     3832     /run/systemd/io.systemd.Credentials
unix  2      [ ACC ]     STREAM     LISTENING     3835     /run/systemd/journal/stdout
unix  2      [ ACC ]     SEQPACKET  LISTENING     3837     /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     34959    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     34077    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     34151    /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     9288     /run/systemd/io.systemd.sysext
unix  2      [ ACC ]     STREAM     LISTENING     10224    @/tmp/.ICE-unix/1342
unix  2      [ ACC ]     STREAM     LISTENING     12012    @/tmp/.X11-unix/X0

┌──(root㉿kali)-[/home/punit]
└─# 
```

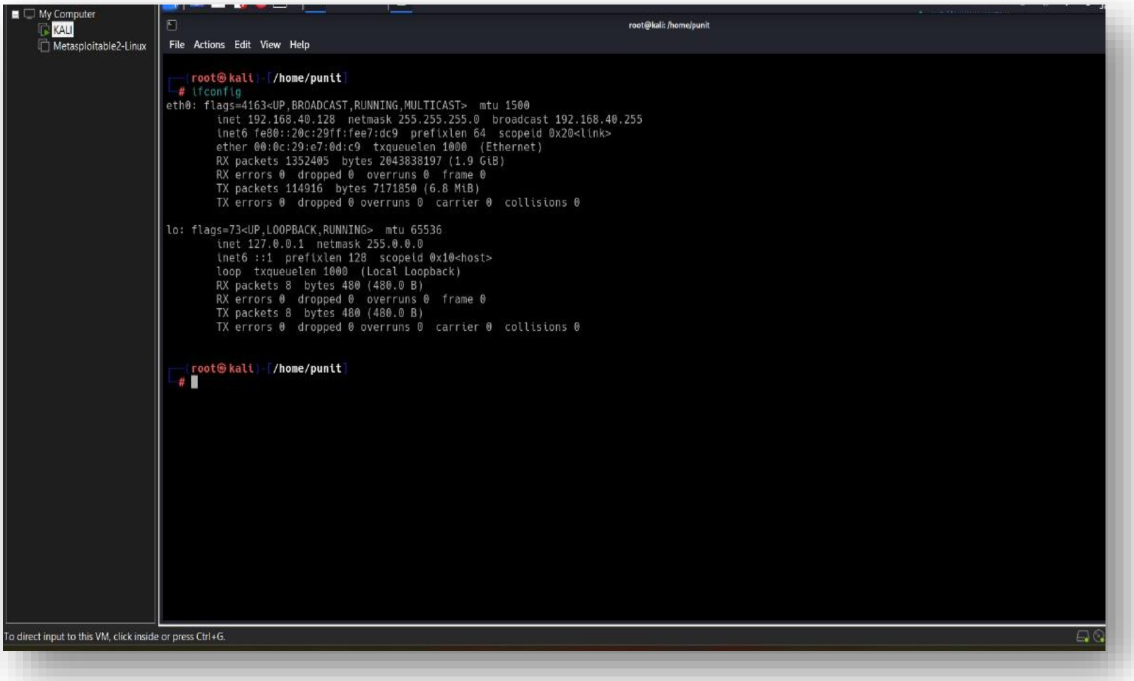
To direct input to this VM, click inside or press Ctrl+G.



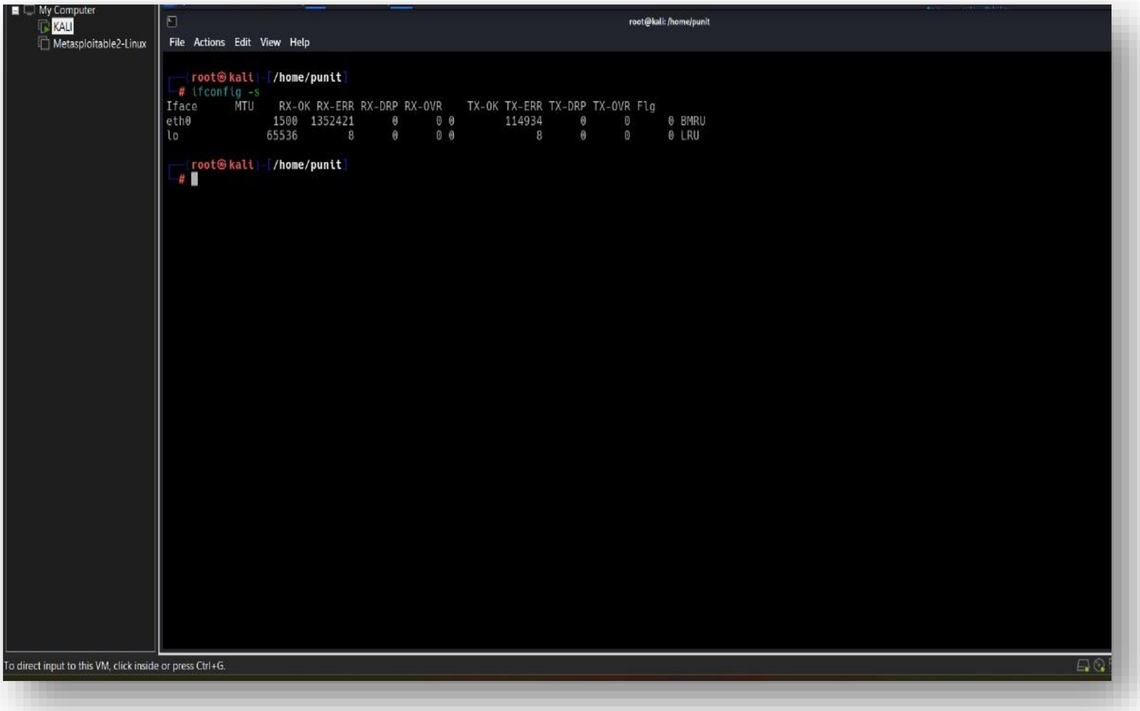
```
┌──(root㉿kali)-[/home/punit]
└─# netstat -s
Ip:
    Forwarding: 2
    124754 total packets received
    1 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    124742 incoming packets delivered
    114847 requests sent out
    40 dropped because of missing route
    OutTransmits: 114847
Icmp:
    0 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
    1 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 1
IcmpMsg:
        OutType3: 1
Tcp:
    19 active connection openings
    0 passive connection openings
    4 failed connection attempts
    0 connection resets received
    0 connections established
    124659 segments received
    114767 segments sent out
    1 segments retransmitted
    0 bad segments received
    4 resets sent
Udp:
    80 packets received
    1 packets to unknown port received
    0 packet receive errors
    80 packets sent
    0 receive buffer errors
```

To direct input to this VM, click inside or press Ctrl+G.

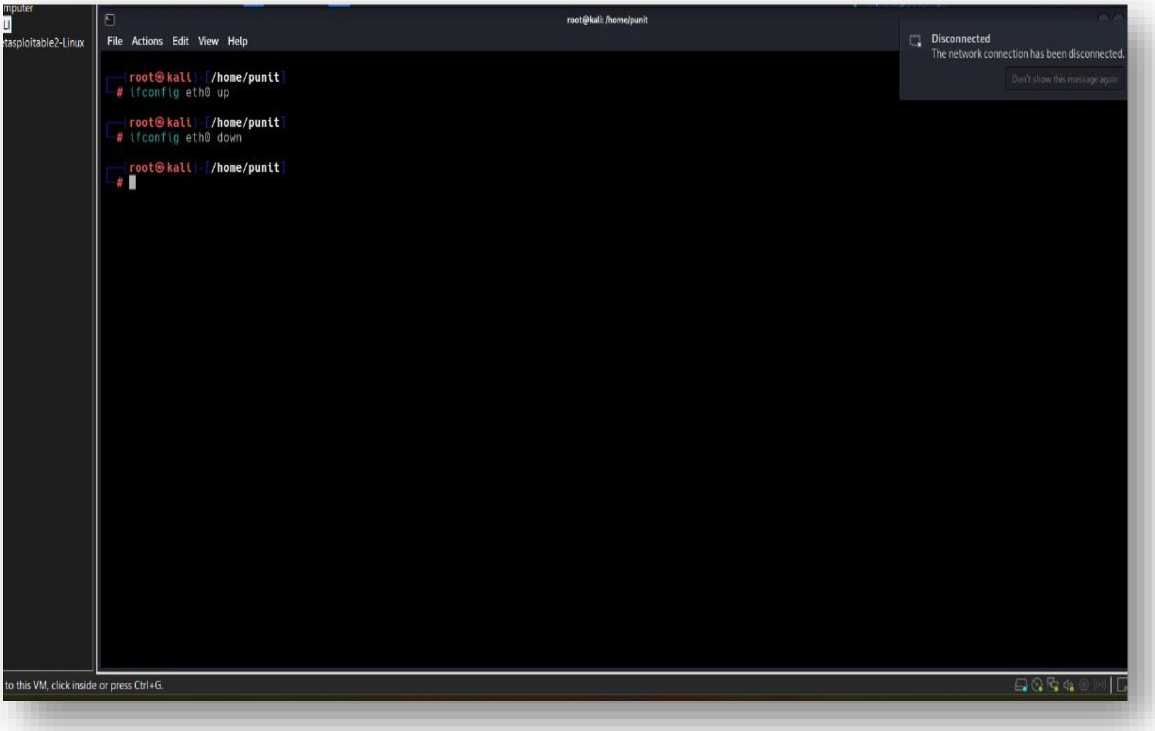
3. **IFCONFIG:** ifconfig (short for "interface configuration") is a command-line tool used to configure, manage, and display information about network interfaces on Unix-like operating systems.


My Computer
KALI
Metasploitable2-Linux
root@kali: /home/punit
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

```
┌──(root㉿kali)-[/home/punit]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.40.128  netmask 255.255.255.0  broadcast 192.168.40.255
        inet6 fe80::20c:29ff:fee7:dc9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e7:0d:c9  txqueuelen 1000  (Ethernet)
        RX packets 1352405  bytes 2043838197 (1.9 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 114916  bytes 7171850 (6.8 MiB)
        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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/punit]
└─# 
```


My Computer
KALI
Metasploitable2-Linux
root@kali: /home/punit
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

```
┌──(root㉿kali)-[/home/punit]
└─# ifconfig -s
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0            1500  1352421      0      0 0        114934      0      0      0 BMRU
lo             65536        8      0      0 0             8      0      0      0 LRU

┌──(root㉿kali)-[/home/punit]
└─# 
```

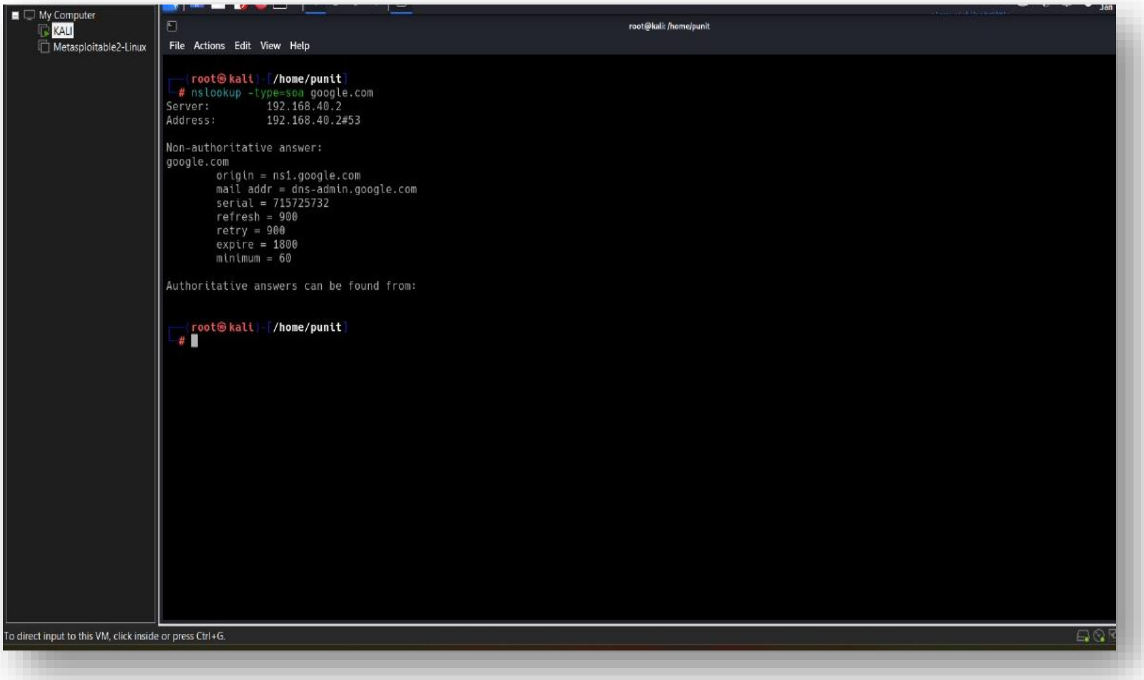


mputer
tasploitable2-Linux
root@kali: /home/punit
File Actions Edit View Help
Don't show this message again
to this VM, click inside or press Ctrl+G.

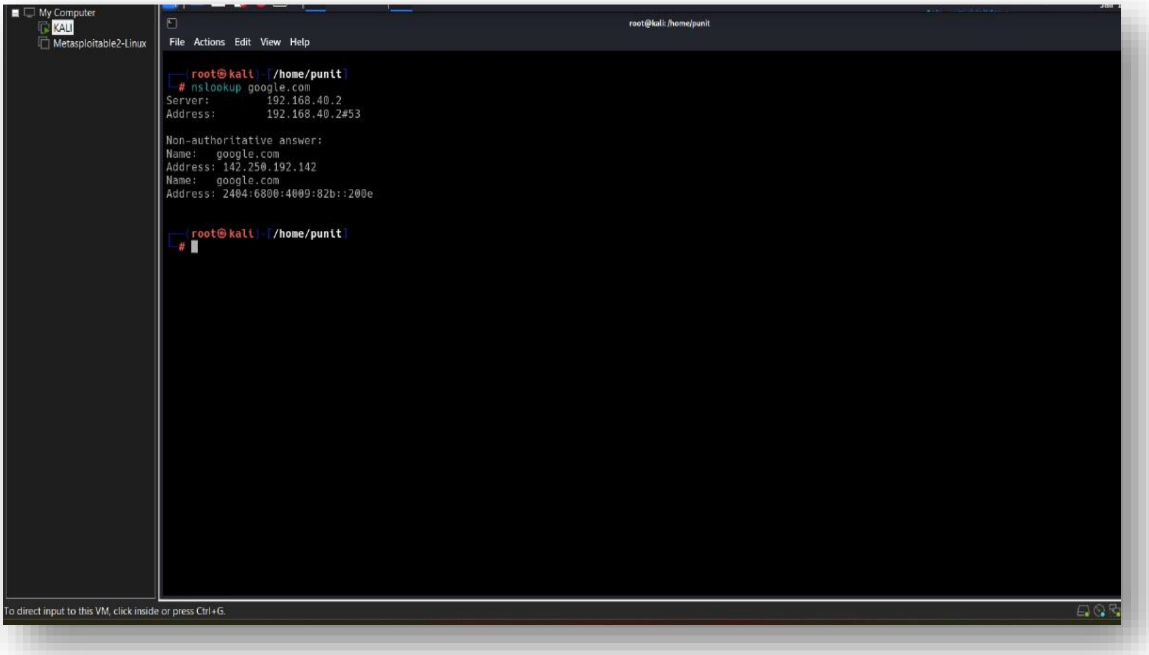
```
┌──(root㉿kali)-[/home/punit]
└─# ifconfig eth0 up

┌──(root㉿kali)-[/home/punit]
└─# ifconfig eth0 down

┌──(root㉿kali)-[/home/punit]
└─# 
```

Disconnected
The network connection has been disconnected.

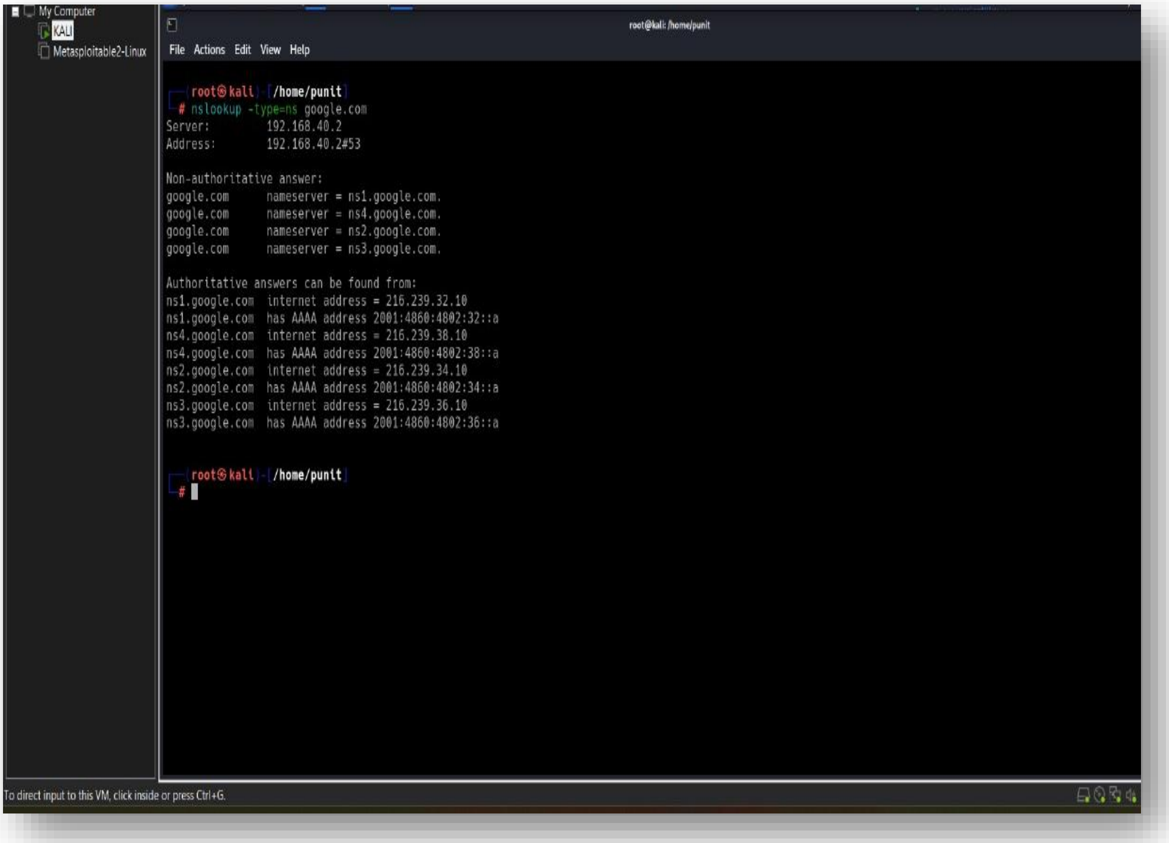
4. **NSLOOKUP:** nslookup (short for "name server lookup") is a command-line tool used to query Domain Name System (DNS) servers to retrieve domain name information, such as IP addresses associated with a domain, or to perform reverse lookups (getting domain names from IP addresses).


My Computer
KALI
Metasploitable2-Linux
root@kali: /home/punit
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

```
┌──(root㉿kali)-[/home/punit]
└─# nslookup -type=soa google.com
Server:         192.168.40.2
Address:        192.168.40.2#53

Non-authoritative answer:
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 715725732
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60

Authoritative answers can be found from:


┌──(root㉿kali)-[/home/punit]
└─#
```

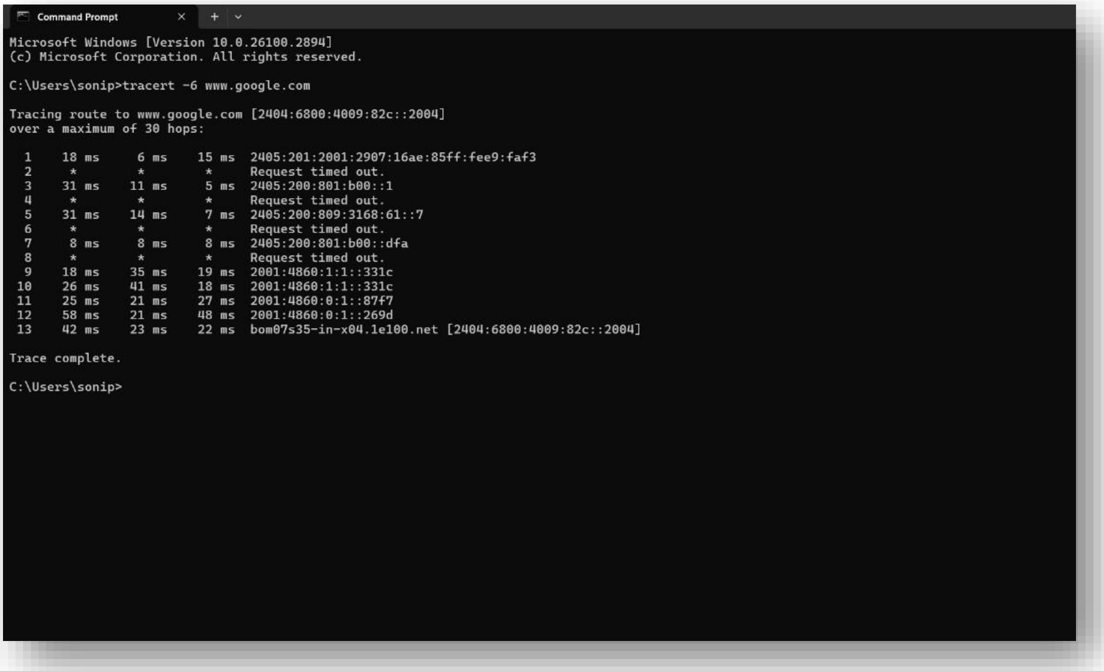

My Computer
KALI
Metasploitable2-Linux
root@kali: /home/punit
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

```
┌──(root㉿kali)-[/home/punit]
└─# nslookup google.com
Server:         192.168.40.2
Address:        192.168.40.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.192.142
Name:   google.com
Address: 2404:6800:4009:82b::200e


┌──(root㉿kali)-[/home/punit]
└─#
```

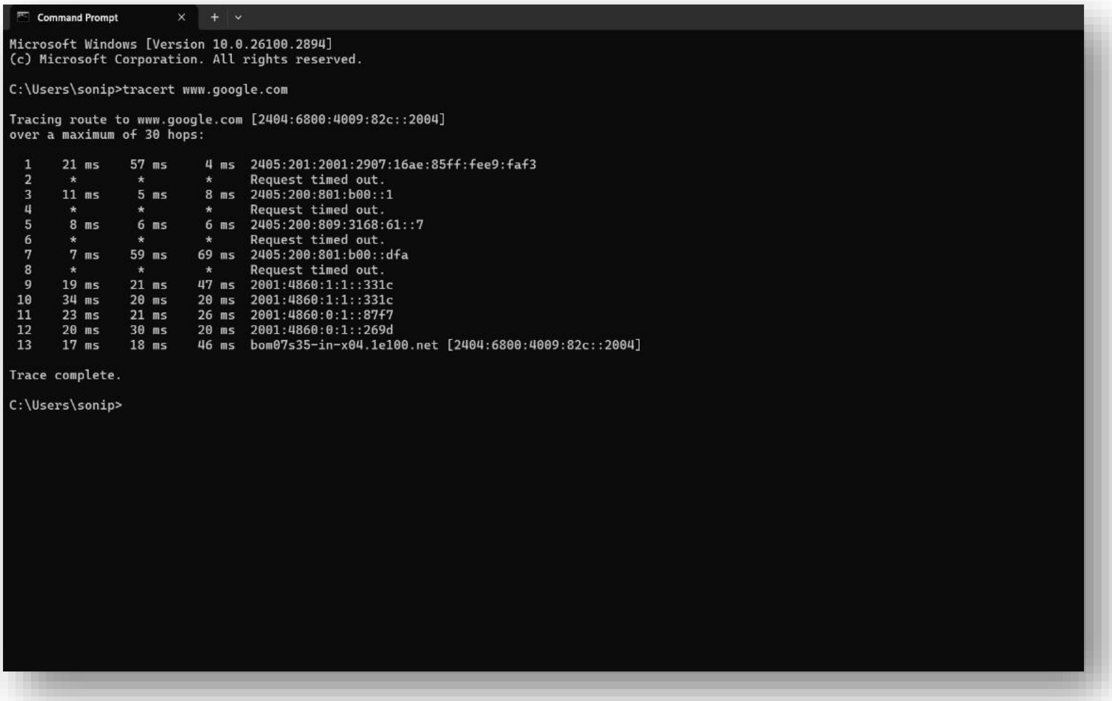

My Computer
KALI
Metasploitable2-Linux
root@kali: /home/punit
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

```
┌──(root㉿kali)-[/home/punit]
└─# nslookup -type=ns google.com
Server:         192.168.40.2
Address:        192.168.40.2#53

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

Authoritative answers can be found from:
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a


┌──(root㉿kali)-[/home/punit]
└─# 
```

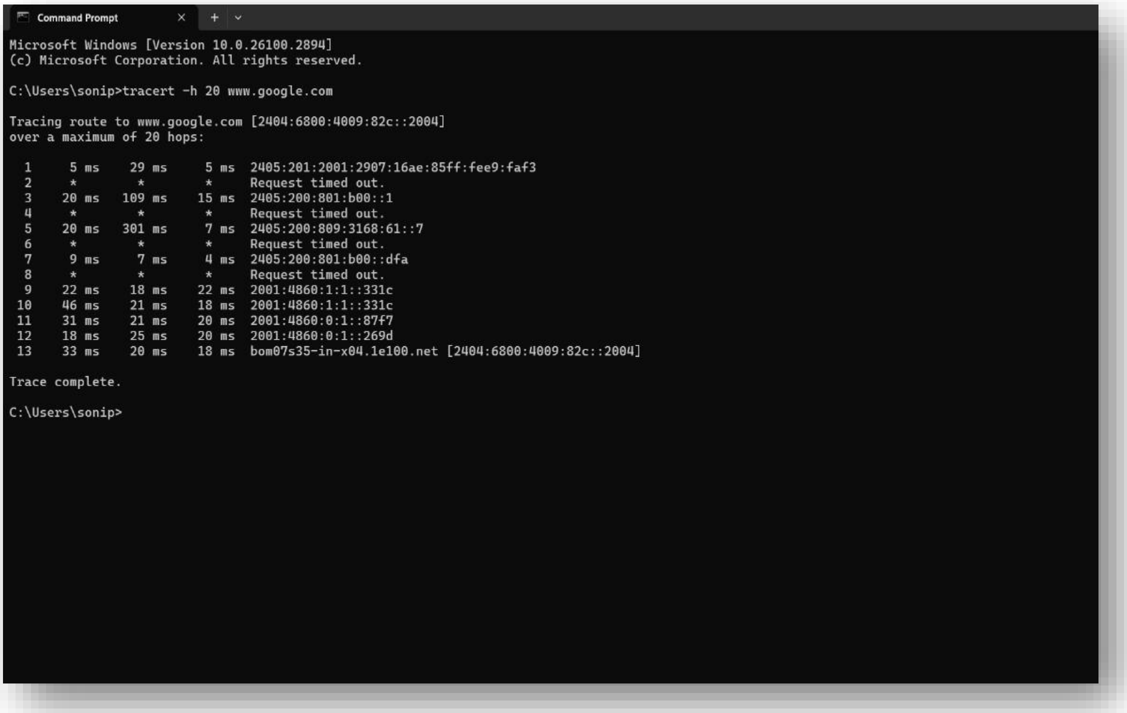
5. **TRACEROUTE:** traceroute is a command-line tool used to trace the path that data packets take from one computer to another across an IP network.



```
Microsoft Windows [Version 10.0.26100.2894]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sonip>tracert -6 www.google.com

Tracing route to www.google.com [2404:6800:4009:82c::2004]
over a maximum of 30 hops:

  1    18 ms     6 ms    15 ms  2405:201:2001:2907:16ae:85ff:fee9:faf3
  2     *        *        *     Request timed out.
  3    31 ms    11 ms     5 ms  2405:200:801:b00::1
  4     *        *        *     Request timed out.
  5    31 ms    14 ms     7 ms  2405:200:809:3168:61::7
  6     *        *        *     Request timed out.
  7     8 ms     8 ms     8 ms  2405:200:801:b00::dfa
  8     *        *        *     Request timed out.
  9    18 ms    35 ms    19 ms  2001:4860:1:1::331c
 10    26 ms    41 ms    18 ms  2001:4860:1:1::331c
 11    25 ms    21 ms    27 ms  2001:4860:0:1::87f7
 12    58 ms    21 ms    48 ms  2001:4860:0:1::269d
 13    42 ms    23 ms    22 ms  bom07s35-in-x04.1e100.net [2404:6800:4009:82c::2004]

Trace complete.

C:\Users\sonip>
```



```
Microsoft Windows [Version 10.0.26100.2894]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sonip>tracert www.google.com

Tracing route to www.google.com [2404:6800:4009:82c::2004]
over a maximum of 30 hops:

  1    21 ms    57 ms     4 ms  2405:201:2001:2907:16ae:85ff:fee9:faf3
  2     *        *        *     Request timed out.
  3    11 ms     5 ms     8 ms  2405:200:801:b00::1
  4     *        *        *     Request timed out.
  5     8 ms     6 ms     6 ms  2405:200:809:3168:61::7
  6     *        *        *     Request timed out.
  7     7 ms    59 ms    69 ms  2405:200:801:b00::dfa
  8     *        *        *     Request timed out.
  9    19 ms    21 ms    47 ms  2001:4860:1:1::331c
 10    34 ms    20 ms    20 ms  2001:4860:1:1::331c
 11    23 ms    21 ms    26 ms  2001:4860:0:1::87f7
 12    20 ms    30 ms    20 ms  2001:4860:0:1::269d
 13    17 ms    18 ms    46 ms  bom07s35-in-x04.1e100.net [2404:6800:4009:82c::2004]

Trace complete.

C:\Users\sonip>
```



```
Microsoft Windows [Version 10.0.26100.2894]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sonip>tracert -h 20 www.google.com

Tracing route to www.google.com [2404:6800:4009:82c::2004]
over a maximum of 20 hops:

  1     5 ms    29 ms     5 ms  2405:201:2001:2907:16ae:85ff:fee9:faf3
  2     *        *        *     Request timed out.
  3    20 ms   109 ms    15 ms  2405:200:801:b00::1
  4     *        *        *     Request timed out.
  5    20 ms   301 ms     7 ms  2405:200:809:3168:61::7
  6     *        *        *     Request timed out.
  7     9 ms     7 ms     4 ms  2405:200:801:b00::dfa
  8     *        *        *     Request timed out.
  9    22 ms    18 ms    22 ms  2001:4860:1:1::331c
 10    46 ms    21 ms    18 ms  2001:4860:1:1::331c
 11    31 ms    21 ms    20 ms  2001:4860:0:1::87f7
 12    18 ms    25 ms    20 ms  2001:4860:0:1::269d
 13    33 ms    20 ms    18 ms  bom07s35-in-x04.1e100.net [2404:6800:4009:82c::2004]

Trace complete.

C:\Users\sonip>
```