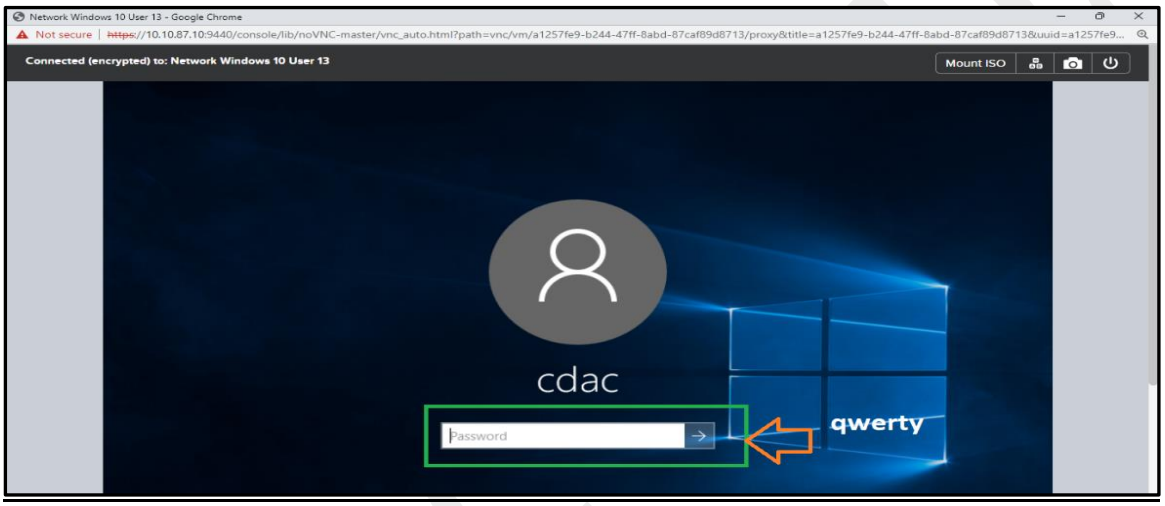
Basic understanding of Networking Commands and their functions with examples

Networking Commands

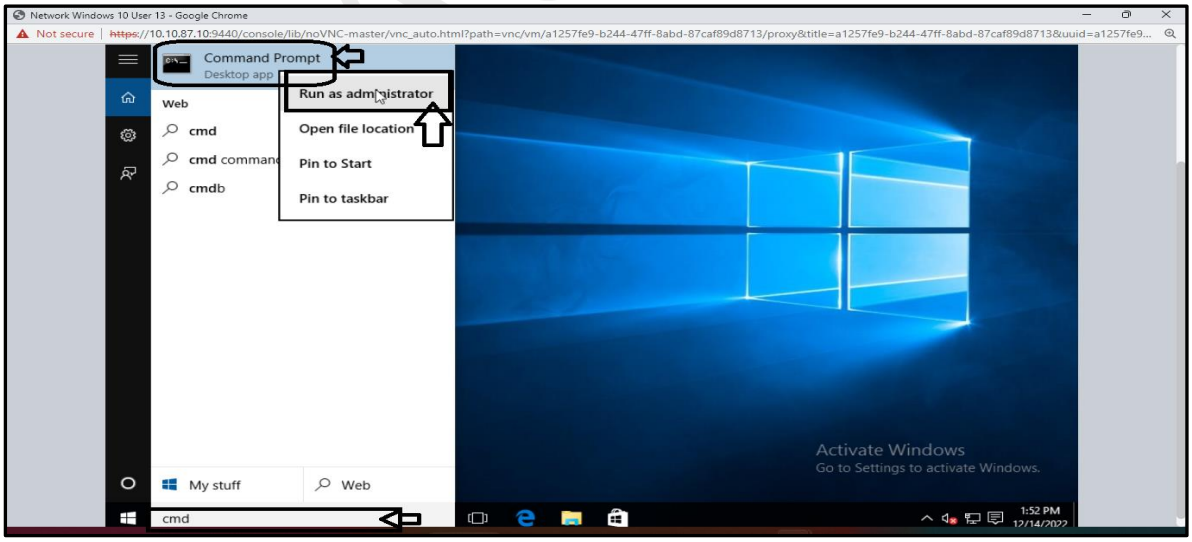
Each operating system comes equipped with some tools known as commands, to troubleshoot the general issues associated with it. Networking commands are used to troubleshoot networking problems along with the display of some important information related to networks. In this lab manual, you will explore various networking commands based on Windows/ Linux operating systems, which may be very helpful to understand and counter cyber-attacks.

Lab Instructions for running commands in Windows:

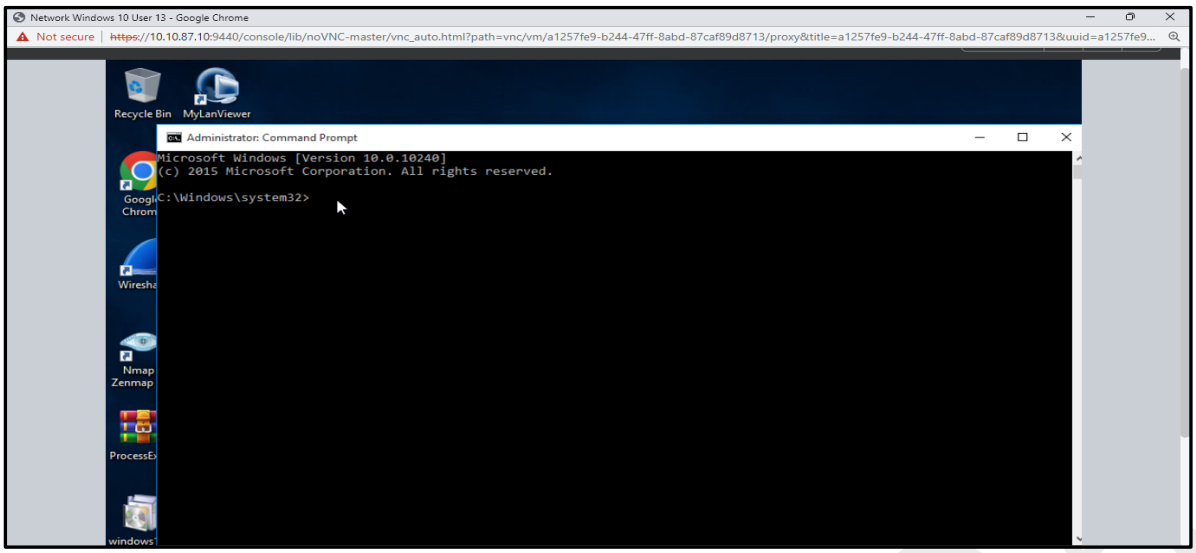
1. Connect to the Windows machine, created by you, using the RDP protocol.
2. When prompted for the password, enter qwerty as the password. Cdac is the administrator user of the machine.



On Windows 10 type cmd into the search box and select the command prompt from the displayed programs run as an administrator privilege.

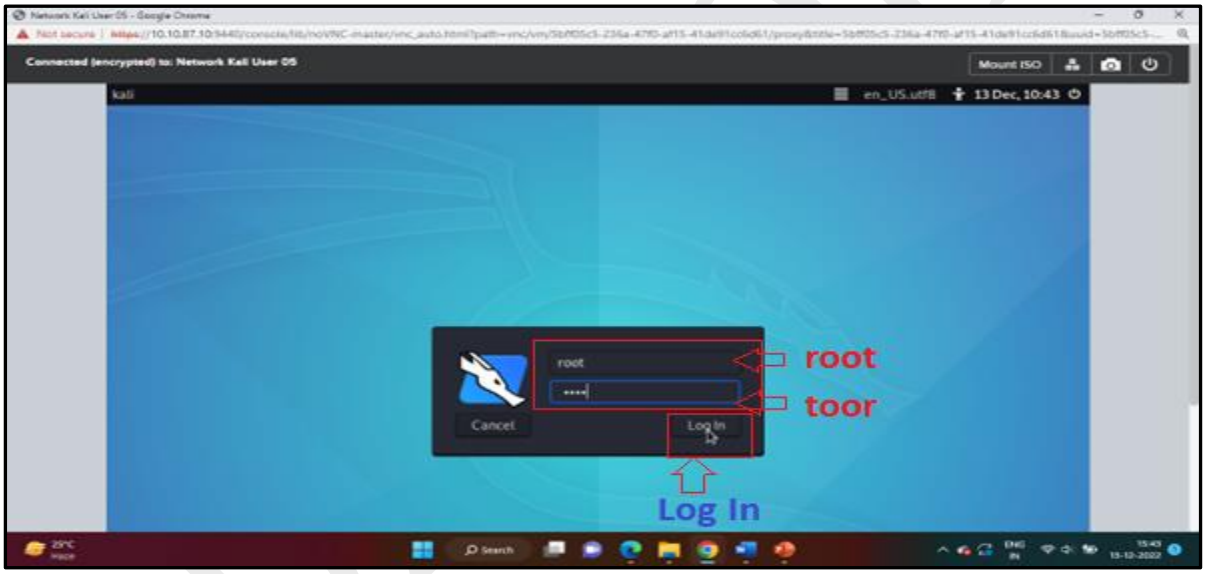


Running the cmd while using the admin account, allows you to run various commands with administrator rights.

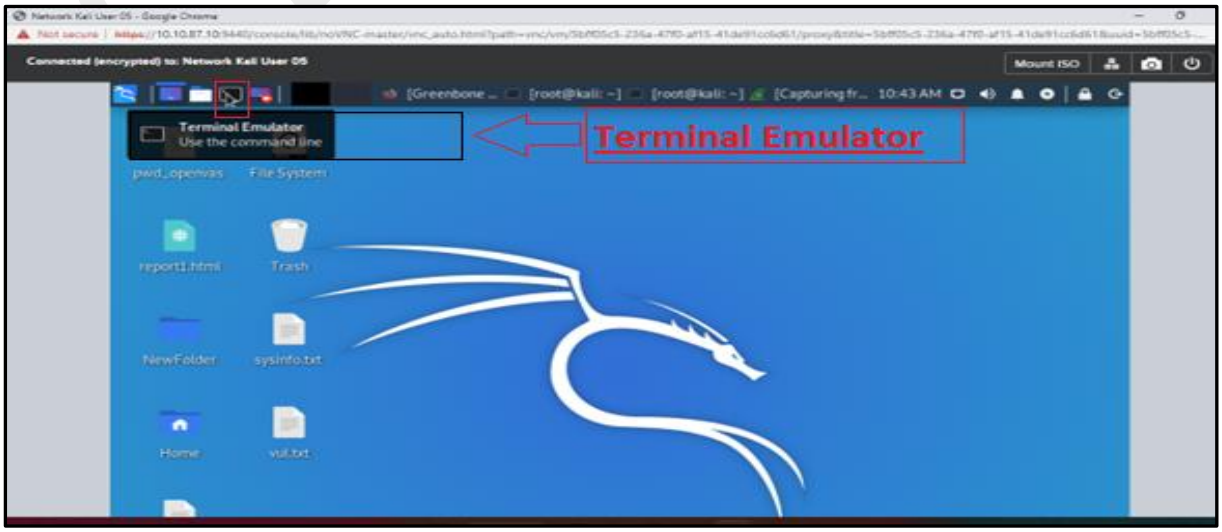


Lab Instructions for running commands in Linux:

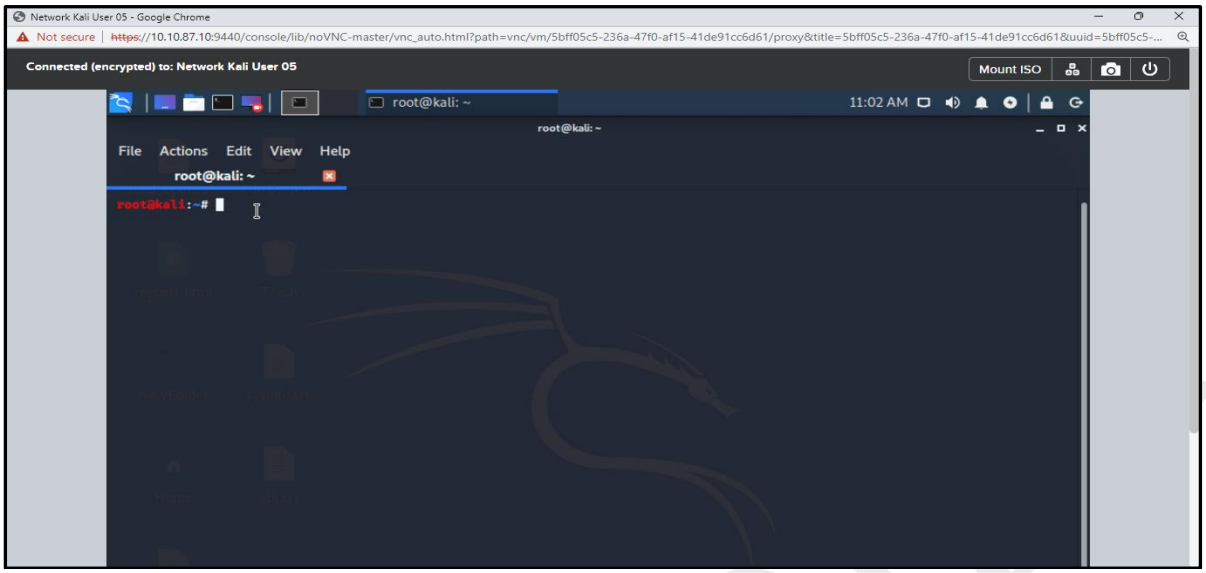
1. Connect to the kali Linux machine, created by you, using the RDP protocol.
2. When prompted for the username and password, enter root as username and toor as password. The root is the administrator user of the machine.



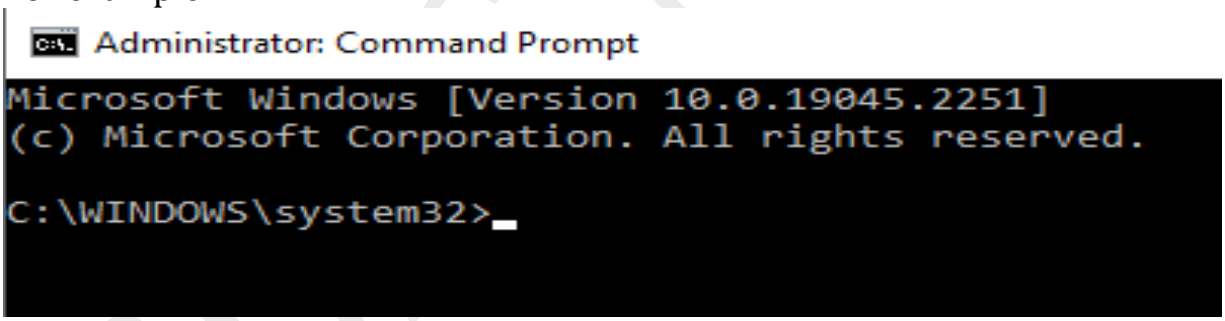
3. click on the black box icon (Terminal Emulator) in the top left corner of the Kali Linux Desktop.



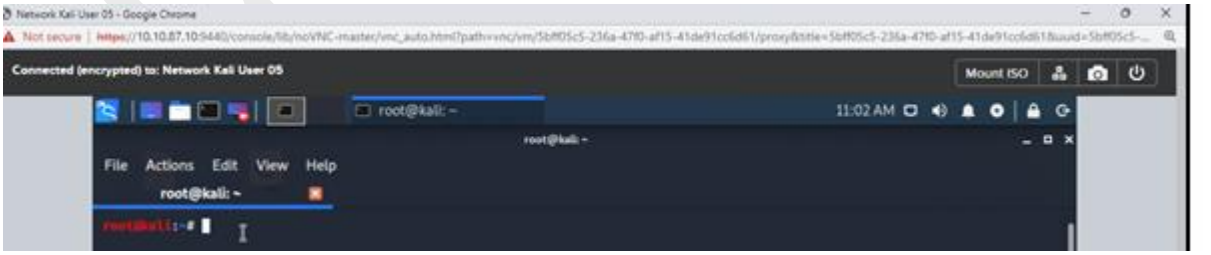
Running the terminal while using the root account, allows you to run various commands with administrator rights.



Let's explore some very important networking commands. Few of these commands run on a windows machine and few run on Linux machines. You can easily identify the machine to use for running the command by the prompt . For example



Windows Prompt



Linux Prompt

1. PING

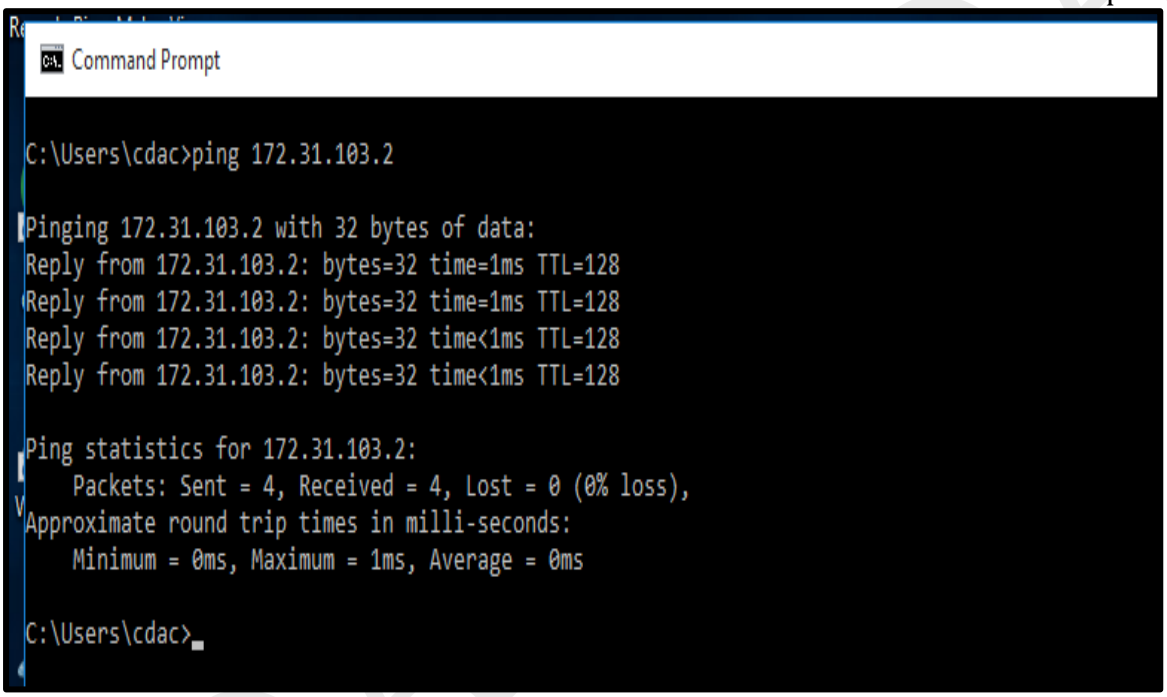
ping command tests the availability of a networking device (usually a computer) on a network. Ping works by sending an Internet Control Message Protocol (ICMP) Echo Request to a specified interface on the network and waiting for a reply. The device responds by sending the Echo Reply ICMP packets. ICMP is Internet Control Message Protocol, used by network devices to diagnose network communication issues.

(i) Ping command to check the availability of a machine using an IP address or computer name.

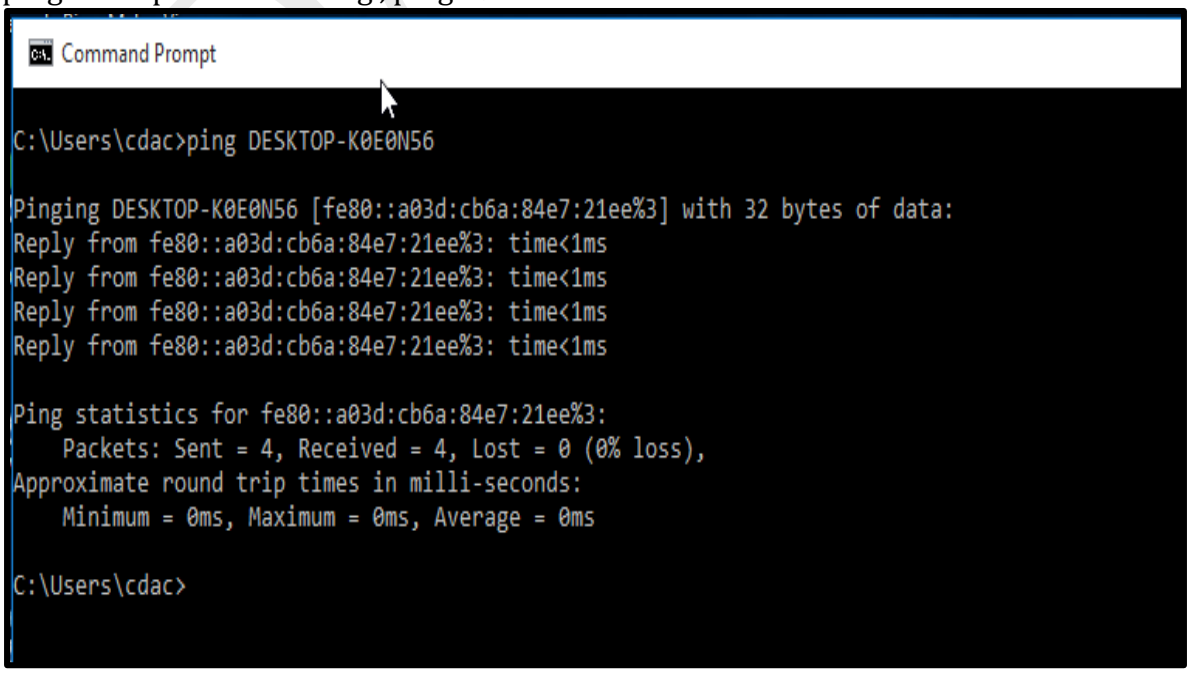
To check the availability of a machine, the ping command can be used with an IP address or computer name. Go to a cmd prompt and enter:

ping IP Address e.g., **ping 172.31.103.2** or **ping < computer name>** :

The screenshots below show how to use the command with an IP address or computer name.



ping <computer name> e.g., ping DESKTOP-K0E0N56



(ii) Ping Command to Identify the Operating System of the remote host.

The TTL value mentioned in the Echo Reply packets may be used to determine the Operating system of the remote host. The default initial TTL value for Linux/Unix is 64, and for Windows, it is 128.

To view the TTL value of a Linux/Windows host, simply ping the host, as shown in the below snapshot.

```
Administrator: Command Prompt

C:\Windows\system32>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>_
```

Here the TTL value is 128 which indicates that the remote host is running a Windows Operating System.

(iii) Ping command to find Hostname

Ping command can also be used to find the hostname corresponding to a known IP address using the -a option.

In the below snapshot, the ping command is used to find the hostname assigned to the IP address 172.31.103.2.

```
Administrator: Command Prompt

C:\Windows\system32>ping -a 172.31.103.2

Pinging DESKTOP-K0E0N56 [172.31.103.2] with 32 bytes of data:
Reply from 172.31.103.2: bytes=32 time=1ms TTL=128
Reply from 172.31.103.2: bytes=32 time<1ms TTL=128
Reply from 172.31.103.2: bytes=32 time<1ms TTL=128
Reply from 172.31.103.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.31.103.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\system32>
```

2. ROUTE

The route is a very important networking command for network administrators. It is used to display or modify the computer's routing table.

(i) Displaying the routing table

To display the routing table (both IPv4 and IPv6) in Windows, a **route command with a print** option may be used.
In Unix/Linux, the **route command** without any option may be used to print the routing table. The output displayed by the Windows and Unix/Linux commands is similar. Here's an example from a typical Windows client computer:

```
C:\Users\cdac>route PRINT
===========================================================================
Interface List
 23...02 00 4c 4f 4f 50 ......Npcap Loopback Adapter
 26...b0 83 fe 92 16 fa ......Realtek PCIe GbE Family Controller
 14...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 18...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  2...00 50 56 c0 00 02 ......VMware Virtual Ethernet Adapter for VMnet2
 24...00 50 56 c0 00 03 ......VMware Virtual Ethernet Adapter for VMnet3
 12...00 50 56 c0 00 04 ......VMware Virtual Ethernet Adapter for VMnet4
 21...00 50 56 c0 00 05 ......VMware Virtual Ethernet Adapter for VMnet5
 19...00 50 56 c0 00 06 ......VMware Virtual Ethernet Adapter for VMnet6
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.226.32.1     10.226.40.10     35
      10.226.32.0    255.255.240.0         On-link      10.226.40.10    291
     10.226.40.10  255.255.255.255         On-link      10.226.40.10    291
    10.226.47.255  255.255.255.255         On-link      10.226.40.10    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      169.254.0.0      255.255.0.0         On-link     169.254.215.76    281
```

```
Command Prompt
  255.255.255.255  255.255.255.255         On-link     192.168.181.1    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 16    311 ::/0                     fe80::16d6:4dff:fe14:b9ec
  1    331 ::1/128                  On-link
 16    311 fc00:cdac:8010:620::/64  On-link
 16    311 fe80::/64                On-link
 21    291 fe80::/64                On-link
 22    291 fe80::/64                On-link
 22    291 fe80::1847:5378:fbfd:bac3/128
                                    On-link
 21    291 fe80::a51d:2d0a:462d:f787/128
                                    On-link
 16    311 fe80::adb4:8c4e:cdf8:1839/128
                                    On-link
  1    331 ff00::/8                 On-link
 16    311 ff00::/8                 On-link
 21    291 ff00::/8                 On-link
 22    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None

C:\>
```

For each entry in the routing table, five items of information are listed:

a. The destination IP address: This is the address of the destination subnet and must be interpreted in the context of the subnet mask.
b. The subnet mask must be applied to the destination address to determine the destination subnet.
c. The IP address of the gateway to which traffic intended for the destination subnet will be sent.
d. The IP address of the interface through which the traffic will be sent to the destination subnet.
e. The metric indicates the number of hops required to reach destinations via the gateway.

route command in Linux with Examples

Here is an example of a Linux system.

$route

```
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         172.31.100.1    0.0.0.0         UG    100    0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.31.100.0    0.0.0.0         255.255.252.0   U     100    0        0 eth0
```

(ii) To display the routing table in full numeric form.

$route -n

```
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.31.100.1    0.0.0.0         UG    100    0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.31.100.0    0.0.0.0         255.255.252.0   U     100    0        0 eth0
root@kali:~#
```

(iii) To add a default gateway.

$sudo route add default gw 172.31.100.2

```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~
root@kali:~# sudo route add default gw 172.31.100.2
root@kali:~#
```

(iv) To list kernel's routing cache information.

$route -Cn

```
root@kali: ~

root@kali:~# route -Cn
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
root@kali:~#
```

(v) To reject routing to a particular host or network.

$sudo route add -host 172.31.103.2 reject

```
File  Actions  Edit  View  Help
root@kali: ~

root@kali:~# sudo route add -host 172.31.103.2 reject
root@kali:~#
```

(vi) To get details of the kernel/IP routing table using the IP command.

$ip route

```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~

root@kali:~# ip route
default via 172.31.100.2 dev eth0
default via 172.31.100.1 dev eth0 proto dhcp metric 100
172.31.100.0/22 dev eth0 proto kernel scope link src 172.31.100.202 metric 100
unreachable 172.31.103.2 scope host
root@kali:~#
```

Each line in the output represents an entry in the routing table (Linux kernel routing table). For example, the lines shown in the above snapshot represent the route for the local network. All network packets to a system in the same network are sent directly through the device eth0. The second default route, which is also set via the eth0 interface says that all network packets which cannot be sent according to the previous entries of the routing table are sent through the gateway defined in this entry i.e. 172.31.100.1 as the default gateway.

(vii) To delete the default gateway.

$route del default

```
File  Actions  Edit  View  Help
root@kali: ~
root@kali:~# route del default
root@kali:~#
```

(viii) To get the details of the local table with destination addresses assigned to the local host.

$ip route show table local

```
File  Actions  Edit  View  Help
root@kali: ~
root@kali:~# ip route show table local
broadcast 127.0.0.0 dev lo proto kernel scope link src 127.0.0.1
local 127.0.0.0/8 dev lo proto kernel scope host src 127.0.0.1
local 127.0.0.1 dev lo proto kernel scope host src 127.0.0.1
broadcast 127.255.255.255 dev lo proto kernel scope link src 127.0.0.1
broadcast 172.31.100.0 dev eth0 proto kernel scope link src 172.31.100.202
local 172.31.100.202 dev eth0 proto kernel scope host src 172.31.100.202
broadcast 172.31.103.255 dev eth0 proto kernel scope link src 172.31.100.202
root@kali:~#
```

(ix) To get output related to IPv4 only.

$ip -4 route

```
File  Actions  Edit  View  Help
root@kali: ~
root@kali:~# ip -4 route
default via 172.31.100.1 dev eth0 proto dhcp metric 100
172.31.100.0/22 dev eth0 proto kernel scope link src 172.31.100.202 metric 100
unreachable 172.31.103.2 scope host
root@kali:~#
```

3. IPCONFIG

The ipconfig command is used to display information about network configuration and refresh DHCP and DNS Settings in Windows systems. By default, the ipconfig command displays your IP Address, Subnet Mask, and default gateway.

(i) Using ipconfig command to display network configuration of the systems.

Type ipconfig and press Enter as shown below. The output displays the list of active network adapters/interfaces, whether they're connected or disconnected, and their IP addresses. Details such as their default gateway IP addresses, subnet masks, and the state of each network adapter are displayed.

```
Command Prompt
Microsoft Windows [Version 10.0.19045.2364]
(c) Microsoft Corporation. All rights reserved.

C:\Users\cdac>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8da5:31af:64c7:38c9%23
   Autoconfiguration IPv4 Address. . : 169.254.215.76
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : noida.cdac.in
   Link-local IPv6 Address . . . . . : fe80::14f0:8ac5:b0e4:4c48%26
   IPv4 Address. . . . . . . . . . . : 10.226.40.10
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 10.226.32.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e4cd:6c4e:1a83:d02b%14
   IPv4 Address. . . . . . . . . . . : 192.168.85.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

Adding a /all switch to the ipconfig command, a new level of details such as DNS information, the MAC (Media Access Control) (in the Physical Address field), and other information about each network component may be obtained. Check out the picture below to see the results.

ipconfig /all

```
Command Prompt
   Default Gateway . . . . . . . . . :

C:\Users\cdac>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : rekhasaraswat
   Primary Dns Suffix  . . . . . . . : cdacnoida.in
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cdacnoida.in
                                       noida.cdac.in

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Npcap Loopback Adapter
   Physical Address. . . . . . . . . : 02-00-4C-4F-4F-50
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8da5:31af:64c7:38c9%23(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.215.76(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 553779276
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-EF-52-3D-B0-83-FE-92-16-FA
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
```

(ii) Renewing the IP address of a network adapter.

When the network connection doesn't work as it should, the network adapter might not have the correct IP address assigned. A quick way of solving this issue is to renew its IP address. It can be done using the Ipconfig command. This is done in two steps.

a. The first one – use the command **ipconfig /release** to force the network adapter to drop its assigned IP address,

ipconfig /release

Command Prompt

```
C:\Users\cdac>ipconfig /release

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8da5:31af:64c7:38c9%23
   Autoconfiguration IPv4 Address. . : 169.254.215.76
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::14f0:8ac5:b0e4:4c48%26
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e4cd:6c4e:1a83:d02b%14
   IPv4 Address. . . . . . . . . . . : 192.168.85.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:
```

b. Use the ipconfig /renew command to renew the IP address.

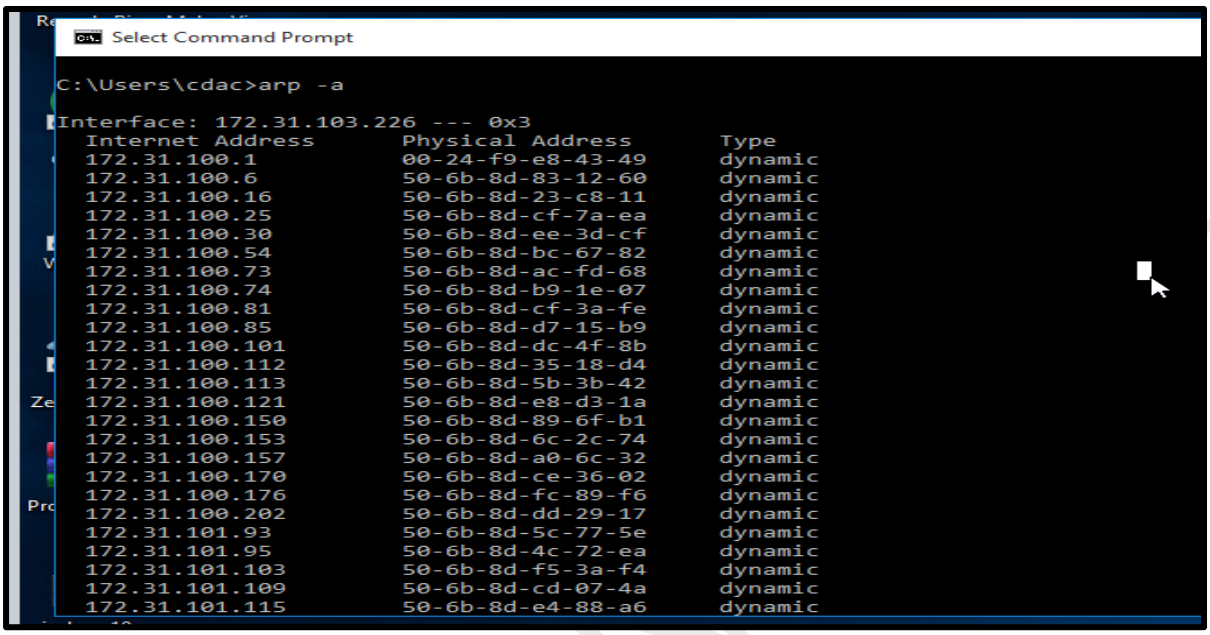
Command Prompt

```
:\Users\cdac>ipconfig /renew

indows IP Configuration


thernet adapter Ethernet:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::a03d:cb6a:84e7:21ee%3
  IPv4 Address. . . . . . . . . . . : 172.31.103.226
  Subnet Mask . . . . . . . . . . . : 255.255.252.0
  Default Gateway . . . . . . . . . : 172.31.100.1

unnel adapter Teredo Tunneling Pseudo-Interface:

  Connection-specific DNS Suffix  . :
  IPv6 Address. . . . . . . . . . . : 2001:0:348b:fb58:2cd7:ec1:53e0:981d
  Link-local IPv6 Address . . . . . : fe80::2cd7:ec1:53e0:981d%5
  Default Gateway . . . . . . . . . : ::

unnel adapter isatap.{5DF3A3DE-E1C3-43E5-B257-CAA1465C6BF9}:

  Media State . . . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

:\Users\cdac>
```

4. ARP

ARP stands for Address Resolution Protocol. Arp, command displays and manipulates the System's ARP cache. It also allows a complete dump of the ARP cache. As you are aware that the primary function of ARP protocol is to resolve the IP address of a system to its MAC address, and hence it works between level 2(Data link layer) and level 3(Network layer).

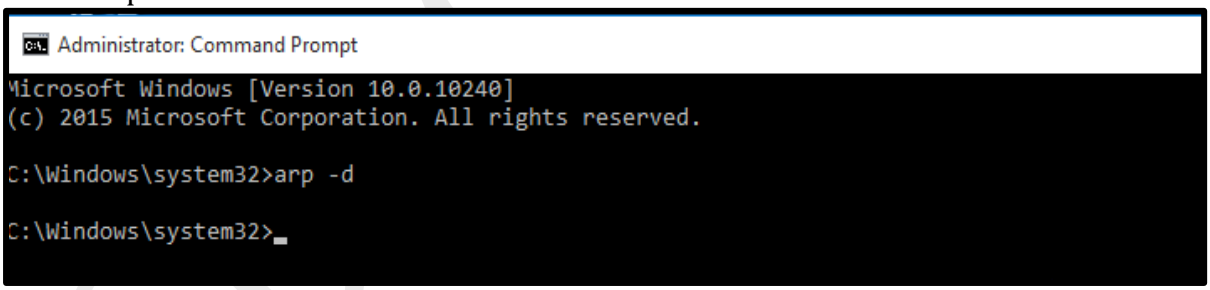
(i) using the arp command to display all the IP and MAC pairs for all the interfaces. Use the command "arp –a" .



```
Select Command Prompt

C:\Users\cdac>arp -a

Interface: 172.31.103.226 --- 0x3
  Internet Address      Physical Address      Type
  172.31.100.1          00-24-f9-e8-43-49     dynamic
  172.31.100.6          50-6b-8d-83-12-60     dynamic
  172.31.100.16         50-6b-8d-23-c8-11     dynamic
  172.31.100.25         50-6b-8d-cf-7a-ea     dynamic
  172.31.100.30         50-6b-8d-ee-3d-cf     dynamic
  172.31.100.54         50-6b-8d-bc-67-82     dynamic
  172.31.100.73         50-6b-8d-ac-fd-68     dynamic
  172.31.100.74         50-6b-8d-b9-1e-07     dynamic
  172.31.100.81         50-6b-8d-cf-3a-fe     dynamic
  172.31.100.85         50-6b-8d-d7-15-b9     dynamic
  172.31.100.101        50-6b-8d-dc-4f-8b     dynamic
  172.31.100.112        50-6b-8d-35-18-d4     dynamic
  172.31.100.113        50-6b-8d-5b-3b-42     dynamic
  172.31.100.121        50-6b-8d-e8-d3-1a     dynamic
  172.31.100.150        50-6b-8d-89-6f-b1     dynamic
  172.31.100.153        50-6b-8d-6c-2c-74     dynamic
  172.31.100.157        50-6b-8d-a0-6c-32     dynamic
  172.31.100.170        50-6b-8d-ce-36-02     dynamic
  172.31.100.176        50-6b-8d-fc-89-f6     dynamic
  172.31.100.202        50-6b-8d-dd-29-17     dynamic
  172.31.101.93         50-6b-8d-5c-77-5e     dynamic
  172.31.101.95         50-6b-8d-4c-72-ea     dynamic
  172.31.101.103        50-6b-8d-f5-3a-f4     dynamic
  172.31.101.109        50-6b-8d-cd-07-4a     dynamic
  172.31.101.115        50-6b-8d-e4-88-a6     dynamic
```

(ii) Deleting all the entries from the ARP table.
Use the command arp- d to flush out all the entries from the ARP table.

arp -d



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>arp -d

C:\Windows\system32>_
```

(iii) Using arp command in Linux

(iv) In Linux there are some more options available. following are the examples.

-v, –verbose: This option shows the verbose information.
-n, –numeric: This option shows numerical addresses instead of symbolic host, port, or usernames.

```
File  Actions  Edit  View  Help
root@kali: ~
root@kali:~# arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
172.31.103.41            ether   50:6b:8d:77:8e:04   C                     eth0
172.31.101.20            ether   50:6b:8d:8c:58:40   C                     eth0
172.31.103.226           ether   50:6b:8d:c5:27:08   C                     eth0
172.31.101.139           ether   50:6b:8d:ae:5d:be   C                     eth0
172.31.102.82            ether   50:6b:8d:4a:50:4b   C                     eth0
172.31.100.206           ether   50:6b:8d:ba:4c:9b   C                     eth0
172.31.100.205           ether   50:6b:8d:39:45:60   C                     eth0
172.31.101.148           ether   50:6b:8d:bc:ca:93   C                     eth0
172.31.103.2             ether   50:6b:8d:d5:89:17   C                     eth0
172.31.100.2             ether   00:24:e8:7c:b4:5b   C                     eth0
172.31.100.1             ether   00:24:f9:e8:43:49   C                     eth0
Entries: 11      Skipped: 0      Found: 11
root@kali:~# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.31.103.41            ether   50:6b:8d:77:8e:04   C                     eth0
172.31.101.20            ether   50:6b:8d:8c:58:40   C                     eth0
172.31.103.226           ether   50:6b:8d:c5:27:08   C                     eth0
172.31.101.139           ether   50:6b:8d:ae:5d:be   C                     eth0
172.31.102.82            ether   50:6b:8d:4a:50:4b   C                     eth0
172.31.100.206           ether   50:6b:8d:ba:4c:9b   C                     eth0
172.31.100.205           ether   50:6b:8d:39:45:60   C                     eth0
172.31.101.148           ether   50:6b:8d:bc:ca:93   C                     eth0
172.31.103.2             ether   50:6b:8d:d5:89:17   C                     eth0
172.31.100.2             ether   00:24:e8:7c:b4:5b   C                     eth0
172.31.100.1             ether   00:24:f9:e8:43:49   C                     eth0
root@kali:~#
```

5. NETSTAT

The netstat command displays the network status and status of TCP and UDP endpoints in the table format.

Here are some examples of using Netstat Command.

(i) Show Active TCP Connections

Run the netstat command with the o option to show all active TCP connections.
netstat -o

```
netstat broken with bluet...  root@kali: ~  07:52 AM
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~
root@kali:~# netstat -o
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 172.31.100.202:47498    ec2-13-251-234-23:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:55804    146.60.190.35.bc.:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:55298    104.18.21.226:http      ESTABLISHED keepalive (5.11/0/0)
tcp        0      0 172.31.100.202:49006    del12s06-in-f3.1e:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:57778    server-143-204-253:http TIME_WAIT   timewait (38.03/0/0)
tcp        0      0 172.31.100.202:33794    69.173.158.64:https     TIME_WAIT   timewait (45.80/0/0)
tcp        0      0 172.31.100.202:39528    www.launchpad.net:https ESTABLISHED keepalive (7.70/0/0)
tcp        0      0 172.31.100.202:60360    a6370ebea231e0c9a:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:33792    69.173.158.64:https     TIME_WAIT   timewait (45.78/0/0)
tcp        0      0 172.31.100.202:60126    del11s09-in-f3.1e:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:41326    del03s18-in-f10.1:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:37292    49.44.175.24:http       TIME_WAIT   timewait (36.07/0/0)
tcp        0      0 172.31.100.202:59540    ec2-18-209-25-109:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:37394    del11s10-in-f2.1e:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:42880    ec2-100-24-202-73:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:36350    cdn-185-199-110-1:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:48962    del11s18-in-f4.1e:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:37584    del12s03-in-f3.1e1:http TIME_WAIT   timewait (37.03/0/0)
tcp        0      0 172.31.100.202:60614    cdn-185-199-109-1:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:50066    ec2-35-172-49-77.:https ESTABLISHED off (0.00/0/0)
tcp        0      0 172.31.100.202:48378    117.18.237.29:http      ESTABLISHED keepalive (5.11/0/0)
tcp        0      0 172.31.100.202:51424    172.64.155.188:http     TIME_WAIT   timewait (40.03/0/0)
```

(ii) To see the connected computers in FQDN format instead of a simple IP address, use the -f option.

netstat -f

```
C:\Users\cdac>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.226.40.10:50081     a104-71-61-50.deploy.static.akamaitechnologies.com:https  CLOSE_WAIT
  TCP    10.226.40.10:50082     a104-71-61-50.deploy.static.akamaitechnologies.com:https  CLOSE_WAIT
  TCP    10.226.40.10:50083     a104-90-5-73.deploy.static.akamaitechnologies.com:https  CLOSE_WAIT
  TCP    10.226.40.10:50115     cdac.in:https          CLOSE_WAIT
  TCP    10.226.40.10:50118     cdac.in:https          CLOSE_WAIT
  TCP    10.226.40.10:50119     cdac.in:https          CLOSE_WAIT
  TCP    10.226.40.10:51654     a104-91-64-10.deploy.static.akamaitechnologies.com:https  ESTABLISHED
  TCP    10.226.40.10:58131     bom12s20-in-f5.1e100.net:https  CLOSE_WAIT
  TCP    10.226.40.10:58132     bom12s20-in-f5.1e100.net:https  CLOSE_WAIT
  TCP    10.226.40.10:58775     ec2-52-43-61-95.us-west-2.compute.amazonaws.com:https  ESTABLISHED
  TCP    10.226.40.10:59740     cdac.in:https          CLOSE_WAIT
  TCP    10.226.40.10:60782     server-13-35-191-82.del54.r.cloudfront.net:https  ESTABLISHED
  TCP    10.226.40.10:60783     a23-76-157-18.deploy.static.akamaitechnologies.com:https  CLOSE_WAIT
  TCP    10.226.40.10:60789     ec2-54-209-22-48.compute-1.amazonaws.com:https  ESTABLISHED
  TCP    10.226.40.10:60809     a23-49-73-193.deploy.static.akamaitechnologies.com:http  TIME_WAIT
  TCP    10.226.40.10:60811     ec2-34-197-204-185.compute-1.amazonaws.com:https  ESTABLISHED
  TCP    10.226.40.10:60817     13.107.21.239:https    ESTABLISHED
  TCP    10.226.40.10:60818     aeab55d76dd13c9bb.awsglobalaccelerator.com:https  TIME_WAIT
  TCP    10.226.40.10:60819     ec2-18-205-170-174.compute-1.amazonaws.com:https  ESTABLISHED
  TCP    10.226.40.10:60825     20.189.173.15:https    ESTABLISHED
  TCP    10.226.40.10:60826     20.189.173.15:https    ESTABLISHED
  TCP    10.226.40.10:60827     ec2-23-21-6-92.compute-1.amazonaws.com:https  CLOSE_WAIT
  TCP    10.226.40.10:60844     a23-58-105-159.deploy.static.akamaitechnologies.com:http  TIME_WAIT
  TCP    10.226.40.10:60847     server-13-35-238-168.hyd50.r.cloudfront.net:https  ESTABLISHED
```

(iii) Show Protocol-Specific Stats: To display the stats of a specific protocol such as the TCP use -p option.
netstat -p tcp

Command Prompt

```
C:\Users\cdac>netstat -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.226.40.10:53555     162.159.133.234:https  ESTABLISHED
  TCP    10.226.40.10:58407     20.198.119.84:https    ESTABLISHED
  TCP    10.226.40.10:59995     server-13-224-22-202:https  TIME_WAIT
  TCP    10.226.40.10:60035     123:https              TIME_WAIT
  TCP    10.226.40.10:60036     102:https              TIME_WAIT
  TCP    10.226.40.10:60037     76:https               TIME_WAIT
  TCP    10.226.40.10:60040     bom12s17-in-f4:https   TIME_WAIT
  TCP    10.226.40.10:60042     10.226.1.75:pop3s      CLOSE_WAIT
  TCP    10.226.40.10:60045     bom12s17-in-f4:https   TIME_WAIT
  TCP    10.226.40.10:60048     bom07s36-in-f3:https   TIME_WAIT
  TCP    10.226.40.10:60049     bom07s36-in-f3:https   TIME_WAIT
  TCP    10.226.40.10:60055     bom12s01-in-f14:https  TIME_WAIT
  TCP    10.226.40.10:60058     del11s12-in-f2:https   TIME_WAIT
  TCP    10.226.40.10:60059     bom07s30-in-f2:https   TIME_WAIT
  TCP    10.226.40.10:60060     bom12s16-in-f2:https   TIME_WAIT
  TCP    10.226.40.10:60061     172.67.165.120:https   ESTABLISHED
  TCP    10.226.40.10:60062     bom07s35-in-f10:https  ESTABLISHED
  TCP    10.226.40.10:60064     bom12s04-in-f2:https   ESTABLISHED
  TCP    10.226.40.10:60065     104.22.71.197:https    TIME_WAIT
  TCP    10.226.40.10:60066     bom07s24-in-f14:https  ESTABLISHED
  TCP    10.226.40.10:60068     bom07s24-in-f3:https   TIME_WAIT
  TCP    10.226.40.10:60069     server-13-35-230-125:https  TIME_WAIT
  TCP    10.226.40.10:60071     104.22.71.197:https    TIME_WAIT
  TCP    10.226.40.10:60074     bom12s16-in-f2:https   ESTABLISHED
```

(iv) Show ethernet network statistics:

Ethernet network statistics can be displayed using the -e option of the netstat command.

```
C:\Users\cdac>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    1242732782       453747548
Unicast packets             1870620         1377288
Non-unicast packets        13099596          180632
Discards                        150               0
Errors                            0               0
Unknown protocols                 0
```

(v) Displaying kernel routing table

Using the netstat command with the -r option lists the kernel routing information in the same way as with the route command.

netstat -r

```
C:\Users\cdac>netstat -r
===========================================================================
Interface List
 23...02 00 4c 4f 4f 50 ......Npcap Loopback Adapter
 26...b0 83 fe 92 16 fa ......Realtek PCIe GbE Family Controller
 14...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 18...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  2...00 50 56 c0 00 02 ......VMware Virtual Ethernet Adapter for VMnet2
 24...00 50 56 c0 00 03 ......VMware Virtual Ethernet Adapter for VMnet3
 12...00 50 56 c0 00 04 ......VMware Virtual Ethernet Adapter for VMnet4
 21...00 50 56 c0 00 05 ......VMware Virtual Ethernet Adapter for VMnet5
 19...00 50 56 c0 00 06 ......VMware Virtual Ethernet Adapter for VMnet6
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      10.226.32.1     10.226.40.10     35
      10.226.32.0    255.255.240.0         On-link      10.226.40.10    291
     10.226.40.10  255.255.255.255         On-link      10.226.40.10    291
    10.226.47.255  255.255.255.255         On-link      10.226.40.10    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      169.254.0.0      255.255.0.0         On-link    169.254.20.183    291
      169.254.0.0      255.255.0.0         On-link    169.254.215.76    281
```

(vi) Displaying all the ports related to tcp connections

To display the ports/protocols associated with the connections, the -o option is used.

netstat -o

```
C:\Users\cdac>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    10.226.40.10:53555     162.159.133.234:https  ESTABLISHED     15072
  TCP    10.226.40.10:58407     20.198.119.84:https    ESTABLISHED     4316
  TCP    10.226.40.10:60042     10.226.1.75:pop3s      CLOSE_WAIT      13304
  TCP    10.226.40.10:60370     ec2-35-164-47-107:https  ESTABLISHED     12528
  TCP    10.226.40.10:60536     server-13-35-238-152:https  TIME_WAIT       0
  TCP    10.226.40.10:60537     ec2-52-55-97-7:https   TIME_WAIT       0
  TCP    10.226.40.10:60587     bom07s29-in-f2:https   TIME_WAIT       0
  TCP    10.226.40.10:60591     a23-58-105-159:http    TIME_WAIT       0
  TCP    10.226.40.10:60618     ec2-18-235-70-143:https  CLOSE_WAIT      13140
  TCP    10.226.40.10:60621     a23-49-73-193:http     ESTABLISHED     10144
  TCP    10.226.40.10:60622     a104-90-5-178:https    ESTABLISHED     10144
  TCP    10.226.40.10:60628     52.143.81.222:https    ESTABLISHED     8076
  TCP    10.226.40.10:60629     relay-ac5c9eb2:6568    SYN_SENT        4284
  TCP    10.226.40.10:60630     52.137.102.105:https   ESTABLISHED     8076
  TCP    10.226.40.10:60631     a173-223-217-220:https  ESTABLISHED     8076
  TCP    10.226.40.10:64405     a104-91-64-10:https    ESTABLISHED     14444
  TCP    127.0.0.1:8191         rekhasaraswat:49853    ESTABLISHED     1360
  TCP    127.0.0.1:8191         rekhasaraswat:49858    ESTABLISHED     1360
  TCP    127.0.0.1:8191         rekhasaraswat:49859    ESTABLISHED     1360
  TCP    127.0.0.1:8191         rekhasaraswat:49860    ESTABLISHED     1360
  TCP    127.0.0.1:8191         rekhasaraswat:49861    ESTABLISHED     1360
  TCP    127.0.0.1:8191         rekhasaraswat:49862    ESTABLISHED     1360
  TCP    127.0.0.1:8191         rekhasaraswat:49865    ESTABLISHED     1360
  TCP    127.0.0.1:8191         rekhasaraswat:49866    ESTABLISHED     1360
  TCP    127.0.0.1:8191         rekhasaraswat:49867    ESTABLISHED     1360
```

Here, you can see that the application layer protocols are listed with their names such as https, pop3s, etc. ephemeral ports are shown as numerical values.

To display the ports, associated with the application layer protocols, use the -n option, along with option -o.
netstat -on

```
C:\Users\cdac>netstat -on

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    10.226.40.10:53555     162.159.133.234:443    ESTABLISHED     15072
  TCP    10.226.40.10:55534     162.159.133.233:443    ESTABLISHED     15072
  TCP    10.226.40.10:55538     172.217.160.162:443    ESTABLISHED     12528
  TCP    10.226.40.10:55539     142.250.183.42:443     TIME_WAIT       0
  TCP    10.226.40.10:55540     142.250.183.42:443     TIME_WAIT       0
  TCP    10.226.40.10:55541     34.225.15.81:443       ESTABLISHED     13140
  TCP    10.226.40.10:58407     20.198.119.84:443      ESTABLISHED     4316
  TCP    10.226.40.10:60042     10.226.1.75:995        CLOSE_WAIT      13304
  TCP    10.226.40.10:60370     35.164.47.107:443      ESTABLISHED     12528
  TCP    10.226.40.10:60635     13.35.238.152:443      TIME_WAIT       0
  TCP    10.226.40.10:60636     107.23.229.120:443     TIME_WAIT       0
  TCP    10.226.40.10:60651     34.120.208.123:443     ESTABLISHED     12528
  TCP    10.226.40.10:60652     54.163.176.62:443      ESTABLISHED     13140
  TCP    10.226.40.10:60656     8.241.129.254:80       TIME_WAIT       0
  TCP    10.226.40.10:60659     118.214.137.233:80     TIME_WAIT       0
  TCP    10.226.40.10:60660     118.214.137.233:80     TIME_WAIT       0
  TCP    10.226.40.10:60661     104.90.6.9:80          TIME_WAIT       0
  TCP    10.226.40.10:60662     8.241.129.254:80       TIME_WAIT       0
  TCP    10.226.40.10:60682     162.159.136.232:443    ESTABLISHED     10664
  TCP    10.226.40.10:64405     104.91.64.10:443       ESTABLISHED     14444
  TCP    127.0.0.1:8191         127.0.0.1:49853        ESTABLISHED     1360
  TCP    127.0.0.1:8191         127.0.0.1:49858        ESTABLISHED     1360
  TCP    127.0.0.1:8191         127.0.0.1:49859        ESTABLISHED     1360
```

(vii) To display the executable involved in creating each connection or listening port, the -b option may be used. this option requires admin privileges.
netstat -b

```
C:\WINDOWS\system32>netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.226.40.10:53555     162.159.133.234:https  ESTABLISHED
 [Discord.exe]
  TCP    10.226.40.10:58407     20.198.119.84:https    ESTABLISHED
  WpnService
 [svchost.exe]
  TCP    10.226.40.10:60042     10.226.1.75:pop3s      CLOSE_WAIT
 [OUTLOOK.EXE]
  TCP    10.226.40.10:60370     ec2-35-164-47-107:https  ESTABLISHED
 [firefox.exe]
  TCP    10.226.40.10:60587     bom07s29-in-f2:https   TIME_WAIT
  TCP    10.226.40.10:60621     a23-49-73-193:http     TIME_WAIT
  TCP    10.226.40.10:60628     52.143.81.222:https    ESTABLISHED
 Can not obtain ownership information
  TCP    10.226.40.10:60630     52.137.102.105:https   ESTABLISHED
 Can not obtain ownership information
  TCP    10.226.40.10:60631     a173-223-217-220:https  ESTABLISHED
 Can not obtain ownership information
  TCP    10.226.40.10:60635     server-13-35-238-152:https  ESTABLISHED
 [firefox.exe]
  TCP    10.226.40.10:60636     ec2-107-23-229-120:https  ESTABLISHED
 [firefox.exe]
```

(viii) netstat command in Linux
netstat command has few different options while running in Linux. these options are shown below.

```
-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
```

Note: The participants are advised to explore the available options in Linux also, by running them in a command line interface like a Terminal in Kali Linux.

6. NSLOOKUP

The nslookup (which stands for name server lookup) command is used to perform DNS queries and receive: domain names or IP addresses, or any other specific DNS Records. To use the Windows version of nslookup, open Command Prompt and type nslookup to get a result similar to this one with your network's DNS server and your computer's IP address:

It can display the results related to your name server, mail server, or any other website as follows.

In DNS, non-authoritative answers refer to DNS records, which are kept on external DNS servers, and obtained from the "authoritative" servers that provide the original source of the data.

(i) Getting name server information.
Type nslookup into Command Prompt:

```
Administrator: Command Prompt - nslookup

C:\Windows\system32>nslookup
Default Server:  dns.google
Address:  8.8.8.8
```

It will prompt you to enter some information. type as below.

>set type=ns

```
Administrator: Command Prompt - nslookup

C:\Windows\system32>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set type=ns
> cdac.in
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
cdac.in nameserver = dns3.easydns.org
cdac.in nameserver = dns1.easydns.com
cdac.in nameserver = dns2.easydns.net
>
```

An authoritative address lookup can also be performed by specifying one of the domain's registered nameservers. Nslookup then uses that server instead of the default DNS server information of the local system.

(ii) Getting mail server information.
type C:\>nslookup in command prompt

for Mail Server Lookup type as below.
set type=mx
> cdac.in

```
> set type=mx
> cdac.in
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
cdac.in MX preference = 1, mail exchanger = mx1.cdac.in
cdac.in MX preference = 5, mail exchanger = mx4.cdac.in
>
```

(iii) Getting details of any external website.
nslookup can also provide the IP addresses of an external domain name by querying the dns server.

type the domain name as argument for the nslookup command.
nslookup <domain name>

```
C:\WINDOWS\system32>nslookup myntra.com
Server:  UnKnown
Address:  10.226.0.11

Non-authoritative answer:
Name:    myntra.com
Address:  23.33.245.22


C:\WINDOWS\system32>nslookup amazon.in
Server:  UnKnown
Address:  10.226.0.11

Non-authoritative answer:
Name:    amazon.in
Addresses:  52.95.120.67
          54.239.33.92
          52.95.116.115
```

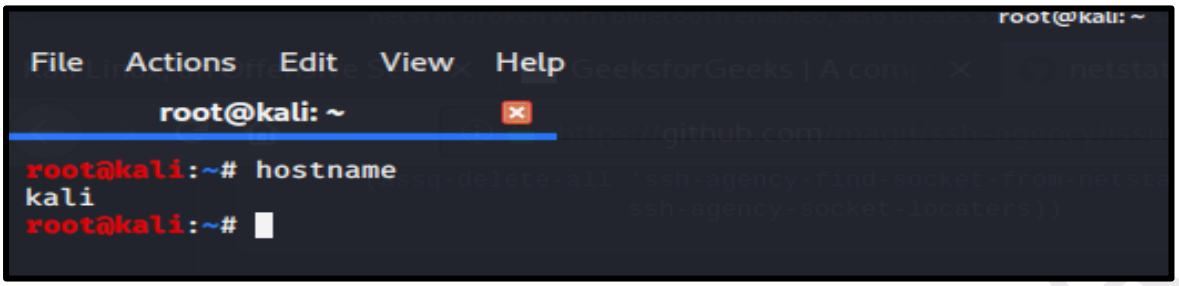
7. HOSTNAME

hostname command in Linus and windows machines is used to display the hostname of the computer or to change it.

(i) Display Hostname

Using the hostname command without any additional options displays the computer's hostname. Here is a snapshot of the Linux system.

hostname



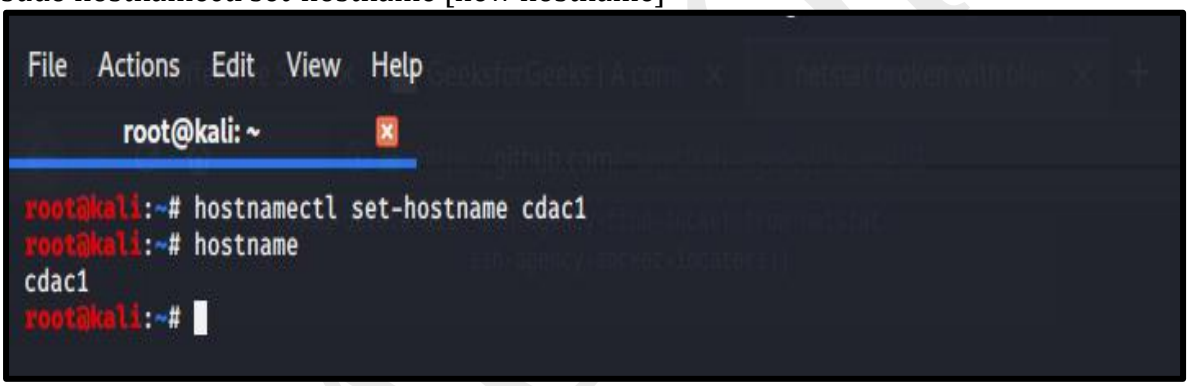
(ii) Change Hostname Permanently

To change the hostname permanently, use a text editor like Nano to make changes to the hostname by editing the host file:

Command **sudo nano /etc/hostname** can be used for this purpose.

Users can also use the hostnamectl command to permanently change the hostname:

sudo hostnamectl set-hostname [new hostname]



8. PATHPING

Pathping is one of the best network troubleshooting tools that are available with Windows. It provides information about network latency and network loss at intermediate hops between a source and a destination. This command sends multiple Echo Request messages to each router between a source and destination, over a period of time, and then computes results based on the packets returned from each router. Because this command displays the degree of packet loss at any given router or link, you can determine which routers or subnets might be having network problems.

pathping 172.31.103.2

```
Command Prompt

C:\Users\cdac>pathping 172.31.103.2

Tracing route to DESKTOP-K0E0N56 [172.31.103.2]
over a maximum of 30 hops:
  0  DESKTOP-K0E0N56 [172.31.103.226]
  1  DESKTOP-K0E0N56 [172.31.103.2]

Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           DESKTOP-K0E0N56 [172.31.103.226]
                                 0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  DESKTOP-K0E0N56 [172.31.103.2]

Trace complete.

C:\Users\cdac>
```

9. <u>NET</u>

NET command is used for viewing the network statistics. various options may be used to display different outcomes.

Using the net command with accounts option displays the network statistics of your computer.

net accounts

```
C:\Users\cdac>net
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\cdac>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          90
Minimum password length:                              8
Length of password history maintained:                3
Lockout threshold:                                    5
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.
```