NAME – KAUSHAL OZA
SRN - 201900754

ROLL NO – 40

Study of Linux and Windows network commands. [ping, pathping, ipconfig/ifconfig, arp, netstat, nbtstat, nslookup, route, traceroute/tracert, nmap, etc]

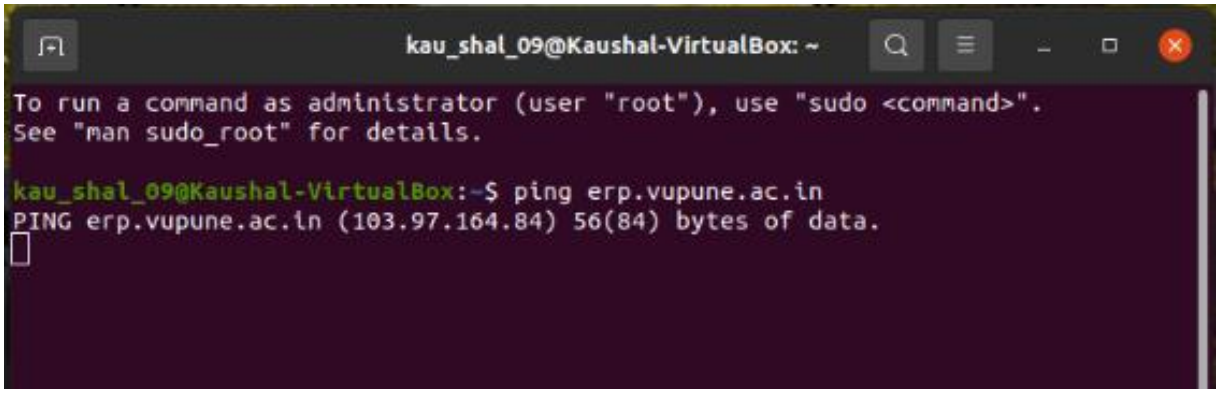
Ping Command:

The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer.

It's usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command provides.

```
Microsoft Windows [Version 10.0.22000.194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ozaka>ping erp.vupune.ac.in

Pinging erp.vupune.ac.in [103.97.164.84] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 103.97.164.84:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



Pathping Command:

Pathping is a TCP/IP based utility (command-line tool) that provides useful information about network latency and network loss at intermediate hops between a source address and a destination address. It does this by sending echo requests via ICMP and analyzing the results. ICMP stands for Internet Control Message Protocol. ICMP is an extension to the Internet Protocol (IP - part of the TCP/IP protocol suite) defined by RFC 792. ICMP supports packets containing error, control and informational messages.

Pathping will send multiple echo request messages to each router between what you are attempting to ping – the source address. If your destination is across a WAN link then it’s certain that you will be using some form of router, most likely two, which would mean that you could test pathping across a two hop network – two router hops.

```
Command Prompt
Request timed out.

Ping statistics for 103.97.164.84:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\ozaka>pathping -n erp.vupune.ac.in

Tracing route to erp.vupune.ac.in [103.97.164.84]
over a maximum of 30 hops:
  0  192.168.1.36
  1  192.168.1.1
  2  10.122.0.1
  3  192.168.25.113
  4  202.88.186.66
  5  202.88.186.61
  6  136.232.32.29
  7  115.110.206.73
  8     *        *        *
Computing statistics for 175 seconds...
           Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           192.168.1.36
                                 0/ 100 =  0%   |
  1    1ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.1
                                 0/ 100 =  0%   |
  2   10ms     0/ 100 =  0%     0/ 100 =  0%  10.122.0.1
                                 0/ 100 =  0%   |
  3    8ms     0/ 100 =  0%     0/ 100 =  0%  192.168.25.113
                                 0/ 100 =  0%   |
  4    8ms     0/ 100 =  0%     0/ 100 =  0%  202.88.186.66
                               0/ 100 =  0%   |
  5    8ms     0/ 100 =  0%     0/ 100 =  0%  202.88.186.61
                                 0/ 100 =  0%   |
  6   13ms     0/ 100 =  0%     0/ 100 =  0%  136.232.32.29
            0/ 100 =  0%   |
  7   13ms     0/ 100 =  0%     0/ 100 =  0%  115.110.206.73

Trace complete.

C:\Users\ozaka>_
```

Ipconfig Command:

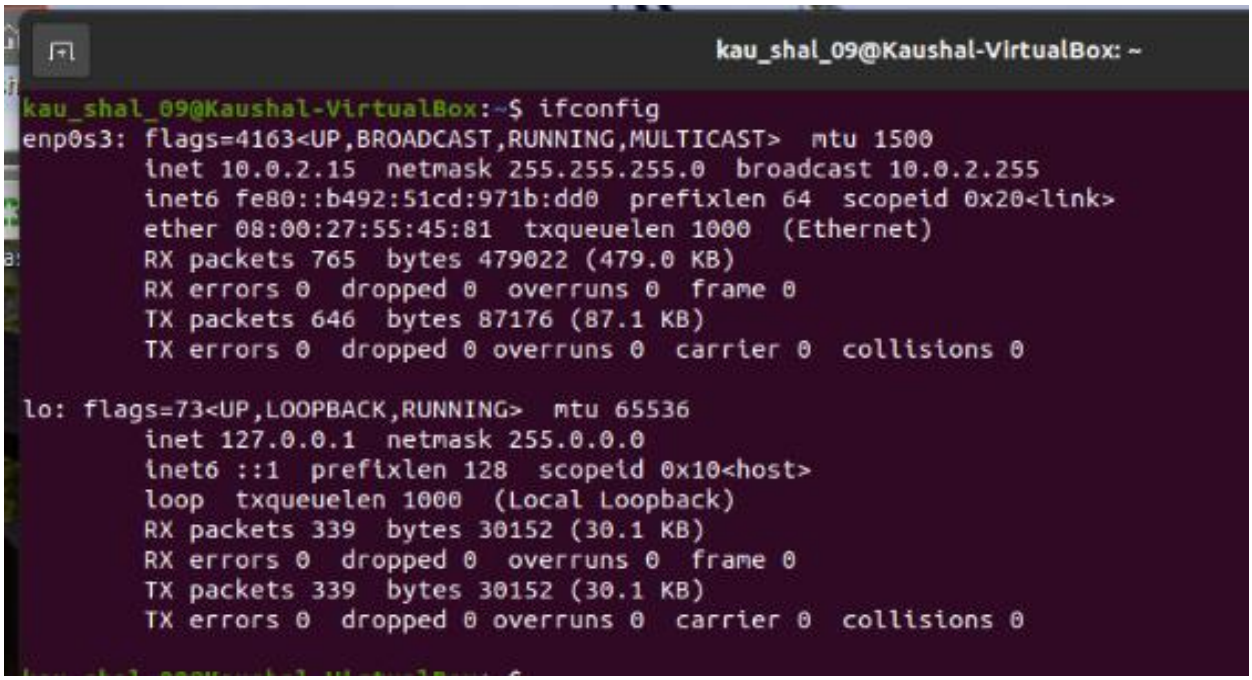
Ipconfig is a console application designed to run from the Windows command prompt. This utility allows you to get the IP address information of a Windows computer. It also allows some control over your network adapters, IP addresses (DHCP-assigned specifically), even your DNS cache.

Ipconfig replaced the older winipcfg utility.

```
Command Prompt
C:\Users\ozaka>ipconfig

Windows IP Configuration


Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5caf:8f9a:2fed:d988%7
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Local Area Connection* 4:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::40b:c6e5:998e:577b%24
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::89fb:6095:d7a0:4419%4
   IPv4 Address. . . . . . . . . . . : 192.168.1.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\ozaka>
```

ifconfig Command:

The “ifconfig” command is used for displaying current network configuration information, setting up an ip address, netmask, or broadcast address to a network interface, creating an alias for the network interface, setting up hardware address, and enabling or disabling network interfaces.



Arp Command:

Using the arp command allows you to display and modify the Address Resolution Protocol (ARP) cache. An ARP cache is a simple mapping of IP addresses to MAC addresses. Each time a computer's TCP/IP stack uses ARP to determine the Media Access Control (MAC) address for an IP address, it records the mapping in the ARP cache so that future ARP lookups go faster. If you use the arp command without any parameters, you get a list of the command's parameters. To display the ARP cache entry for a specific IP address, use an -a switch followed by the IP address.

Command Prompt

```
C:\Users\ozaka>arp -a

Interface: 192.168.1.11 --- 0x4
  Internet Address      Physical Address      Type
  192.168.1.1           00-1a-9a-de-ad-05     dynamic
  192.168.1.12          ac-35-ee-89-cf-a1     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.137.1 --- 0x18
  Internet Address      Physical Address      Type
  192.168.137.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\ozaka>
```

kau_shal_09@Kaushal-VirtualBox: ~

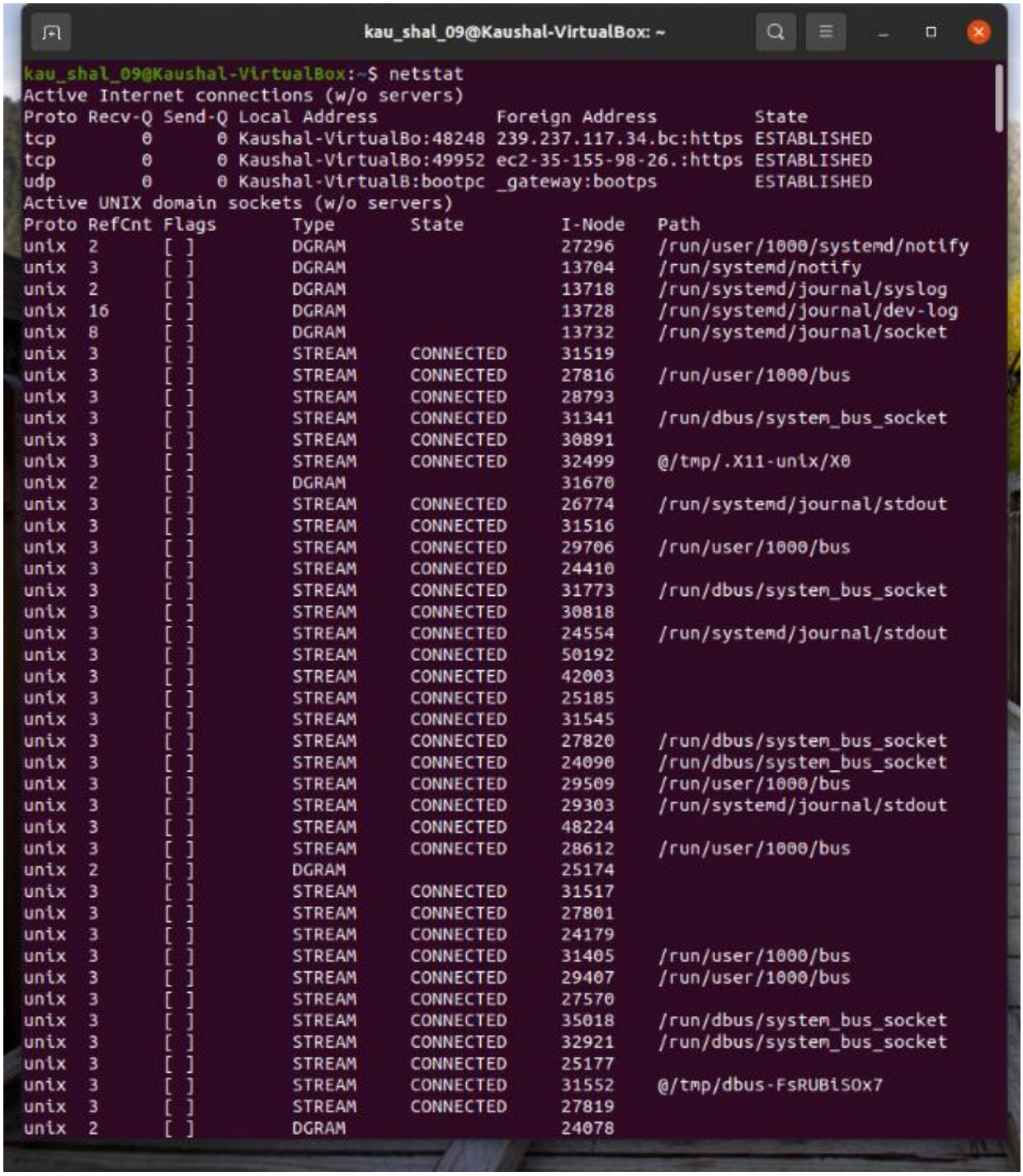
```
kau_shal_09@Kaushal-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask
_gateway                 ether   52:54:00:12:35:02   C
3
kau_shal_09@Kaushal-VirtualBox:~$ arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
kau_shal_09@Kaushal-VirtualBox:~$
```

Netstat Command:

The network statistics (netstat) command is a networking tool used for troubleshooting and configuration that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common uses for this command. Let's take a look at some of the basic usage for netstat and the most used cases. List all listening ports To list all listening ports, using both TCP and UDP, **use netstat -a:**

Command Prompt - netstat -a

```
C:\Users\ozaka>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            KURO:0                 LISTENING
  TCP    0.0.0.0:445            KURO:0                 LISTENING
  TCP    0.0.0.0:1042           KURO:0                 LISTENING
  TCP    0.0.0.0:1043           KURO:0                 LISTENING
  TCP    0.0.0.0:3306           KURO:0                 LISTENING
  TCP    0.0.0.0:5040           KURO:0                 LISTENING
  TCP    0.0.0.0:5357           KURO:0                 LISTENING
  TCP    0.0.0.0:7250           KURO:0                 LISTENING
  TCP    0.0.0.0:9012           KURO:0                 LISTENING
  TCP    0.0.0.0:9013           KURO:0                 LISTENING
  TCP    0.0.0.0:12177          KURO:0                 LISTENING
  TCP    0.0.0.0:33060          KURO:0                 LISTENING
  TCP    0.0.0.0:49664          KURO:0                 LISTENING
  TCP    0.0.0.0:49665          KURO:0                 LISTENING
  TCP    0.0.0.0:49666          KURO:0                 LISTENING
  TCP    0.0.0.0:49667          KURO:0                 LISTENING
  TCP    0.0.0.0:49668          KURO:0                 LISTENING
  TCP    0.0.0.0:49669          KURO:0                 LISTENING
  TCP    0.0.0.0:49678          KURO:0                 LISTENING
  TCP    0.0.0.0:49715          KURO:0                 LISTENING
  TCP    0.0.0.0:53204          KURO:0                 LISTENING
  TCP    0.0.0.0:57621          KURO:0                 LISTENING
  TCP    127.0.0.1:1042         thepiratebay:64570     ESTABLISHED
  TCP    127.0.0.1:1043         thepiratebay:64578     ESTABLISHED
  TCP    127.0.0.1:5939         KURO:0                 LISTENING
  TCP    127.0.0.1:6463         KURO:0                 LISTENING
  TCP    127.0.0.1:7777         KURO:0                 LISTENING
  TCP    127.0.0.1:9012         thepiratebay:64712     ESTABLISHED
  TCP    127.0.0.1:9093         KURO:0                 LISTENING
  TCP    127.0.0.1:9487         KURO:0                 LISTENING
  TCP    127.0.0.1:9487         thepiratebay:64653     ESTABLISHED
  TCP    127.0.0.1:13010        KURO:0                 LISTENING
  TCP    127.0.0.1:13030        KURO:0                 LISTENING
  TCP    127.0.0.1:13031        KURO:0                 LISTENING
  TCP    127.0.0.1:13032        KURO:0                 LISTENING
  TCP    127.0.0.1:17400        KURO:0                 LISTENING
  TCP    127.0.0.1:17945        KURO:0                 LISTENING
  TCP    127.0.0.1:37014        KURO:0                 LISTENING
  TCP    127.0.0.1:37114        KURO:0                 LISTENING
  TCP    127.0.0.1:49679        thepiratebay:49680     ESTABLISHED
  TCP    127.0.0.1:49680        thepiratebay:49679     ESTABLISHED
  TCP    127.0.0.1:49681        thepiratebay:49682     ESTABLISHED
  TCP    127.0.0.1:49682        thepiratebay:49681     ESTABLISHED
  TCP    127.0.0.1:52530        thepiratebay:52531     ESTABLISHED
  TCP    127.0.0.1:52531        thepiratebay:52530     ESTABLISHED
  TCP    127.0.0.1:53199        thepiratebay:53198     TIME_WAIT
  TCP    127.0.0.1:55681        thepiratebay:55680     TIME_WAIT
  TCP    127.0.0.1:57751        thepiratebay:65001     ESTABLISHED
  TCP    127.0.0.1:57769        thepiratebay:64602     ESTABLISHED
  TCP    127.0.0.1:58945        thepiratebay:58944     TIME_WAIT
  TCP    127.0.0.1:59619        thepiratebay:59617     TIME_WAIT
  TCP    127.0.0.1:59620        thepiratebay:59618     TIME_WAIT
  TCP    127.0.0.1:60071        KURO:0                 LISTENING
```



```
kau_shal_09@Kaushal-VirtualBox: ~
kau_shal_09@Kaushal-VirtualBox:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 Kaushal-VirtualBo:48248 239.237.117.34.bc:https ESTABLISHED
tcp        0      0 Kaushal-VirtualBo:49952 ec2-35-155-98-26.:https ESTABLISHED
udp        0      0 Kaushal-VirtualB:bootpc _gateway:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    27296    /run/user/1000/systemd/notify
unix  3      [ ]         DGRAM                    13704    /run/systemd/notify
unix  2      [ ]         DGRAM                    13718    /run/systemd/journal/syslog
unix  16     [ ]         DGRAM                    13728    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM                    13732    /run/systemd/journal/socket
unix  3      [ ]         STREAM     CONNECTED     31519
unix  3      [ ]         STREAM     CONNECTED     27816    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     28793
unix  3      [ ]         STREAM     CONNECTED     31341    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     30891
unix  3      [ ]         STREAM     CONNECTED     32499    @/tmp/.X11-unix/X0
unix  2      [ ]         DGRAM                    31670
unix  3      [ ]         STREAM     CONNECTED     26774    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     31516
unix  3      [ ]         STREAM     CONNECTED     29706    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     24410
unix  3      [ ]         STREAM     CONNECTED     31773    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     30818
unix  3      [ ]         STREAM     CONNECTED     24554    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     50192
unix  3      [ ]         STREAM     CONNECTED     42003
unix  3      [ ]         STREAM     CONNECTED     25185
unix  3      [ ]         STREAM     CONNECTED     31545
unix  3      [ ]         STREAM     CONNECTED     27820    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     24090    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     29509    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     29303    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     48224
unix  3      [ ]         STREAM     CONNECTED     28612    /run/user/1000/bus
unix  2      [ ]         DGRAM                    25174
unix  3      [ ]         STREAM     CONNECTED     31517
unix  3      [ ]         STREAM     CONNECTED     27801
unix  3      [ ]         STREAM     CONNECTED     24179
unix  3      [ ]         STREAM     CONNECTED     31405    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     29407    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     27570
unix  3      [ ]         STREAM     CONNECTED     35018    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     32921    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     25177
unix  3      [ ]         STREAM     CONNECTED     31552    @/tmp/dbus-FsRUBiSOx7
unix  3      [ ]         STREAM     CONNECTED     27819
unix  2      [ ]         DGRAM                    24078
```

Nbtstat Command:

The nbtstat utility is used to view protocol statistics and information for

NetBIOS over TCP/IP connections. nbtstat is commonly used to troubleshoot NetBIOS name resolution problems. Because nbtstat provides the resolution of NetBIOS names, it's available only on Windows systems.

```
Command Prompt
Microsoft Windows [Version 10.0.22000.194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ozaka>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.


C:\Users\ozaka>_
```

Netcat (nc) Command :

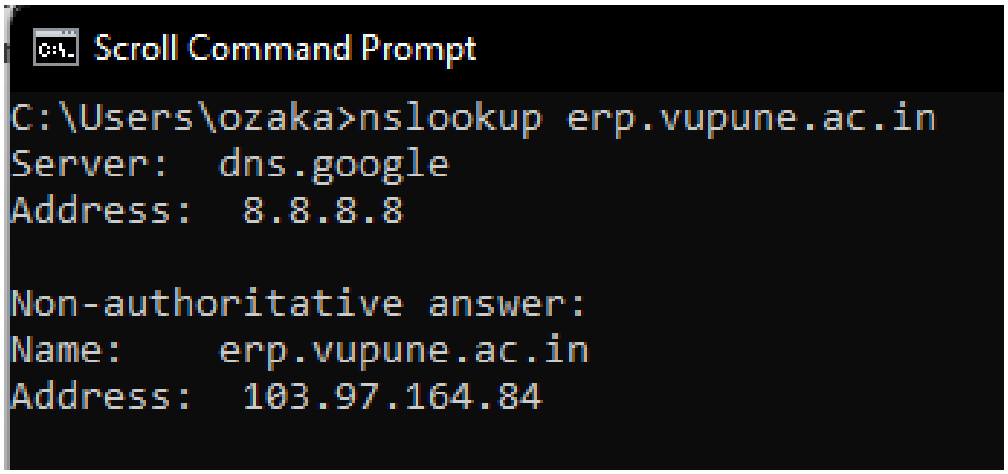
Netcat (or nc) is a command-line utility that reads and writes data across network connections, using the TCP or UDP protocols. It is one of the most powerful tools in the network and system administrators arsenal, and it is considered as a Swiss army knife of networking tools.

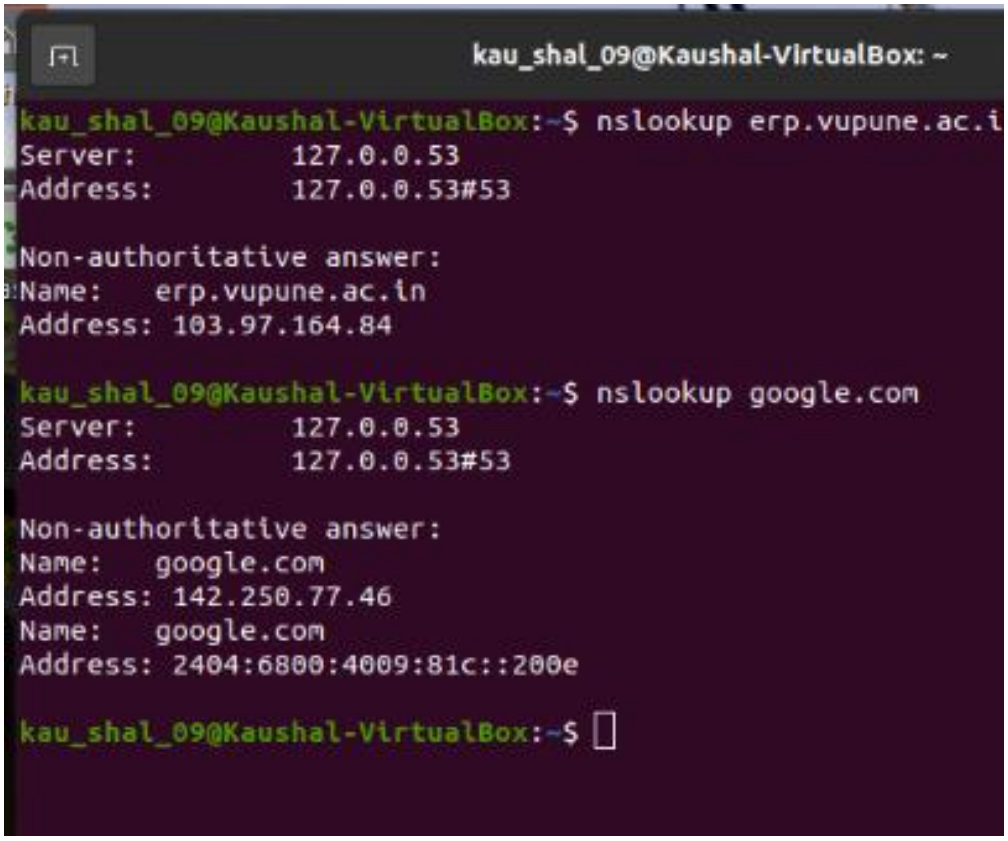
Netcat Syntax:

nc [options] host port

Nslookup Command:

nslookup is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, "whatis.com") and find out the corresponding IP address or domain name system (DNS) record. The user can also enter a command for it to do a reverse DNS lookup and find the host name for an IP address that is specified.





traceroute/tracert Command:

Tracert:

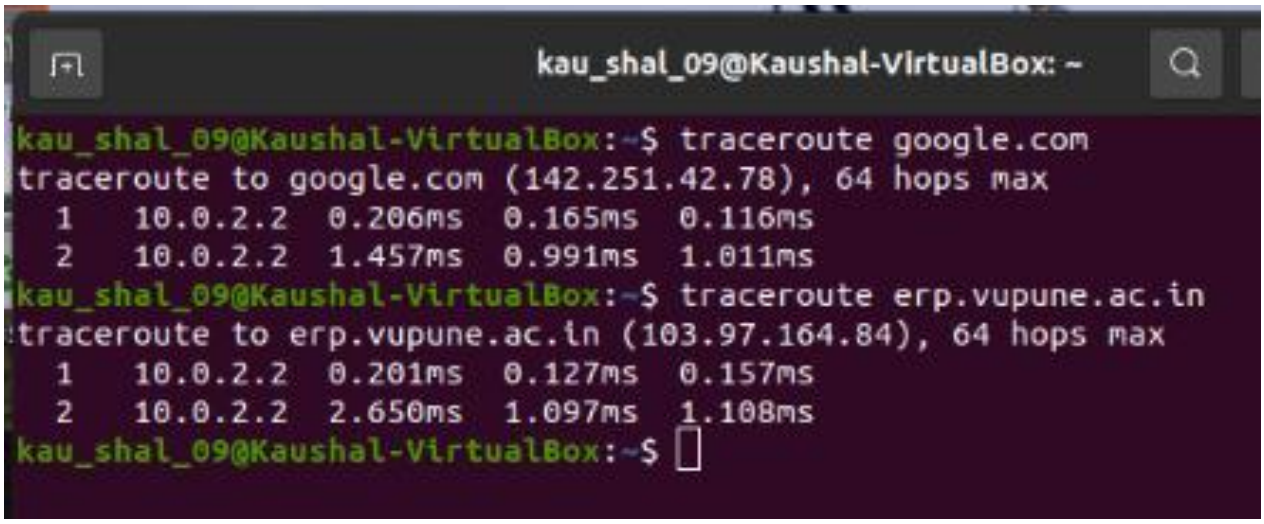
The Windows Tracert tool determines the route to a destination by sending
ICMP packets to the destination. In these packets, Tracert uses varying IP TimeTo-Live (TTL) values. The TTL is effectively a hop counter, where a hop is a location that the packet stops at, to reach the destination.

The tool may take some time to complete (particularly if there is a problem), as the tool waits for responses (which may not come).

```
Command Prompt

Tracing route to erp.vupune.ac.in [103.97.164.84]
over a maximum of 30 hops:

  1     2 ms    <1 ms    <1 ms  192.168.1.1
  2     8 ms     9 ms     9 ms  10.122.0.1
  3    11 ms     7 ms     9 ms  192.168.25.113
  4     7 ms     7 ms     7 ms  202.88.186.66
  5     8 ms     7 ms     7 ms  202.88.186.61
  6    18 ms    22 ms    19 ms  136.232.32.29
  7    14 ms    16 ms    14 ms  115.110.206.73
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    29 ms    28 ms    28 ms  14.143.171.254
 11     *        *        *     Request timed out.
 12    19 ms    19 ms    18 ms  45.251.12.34
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

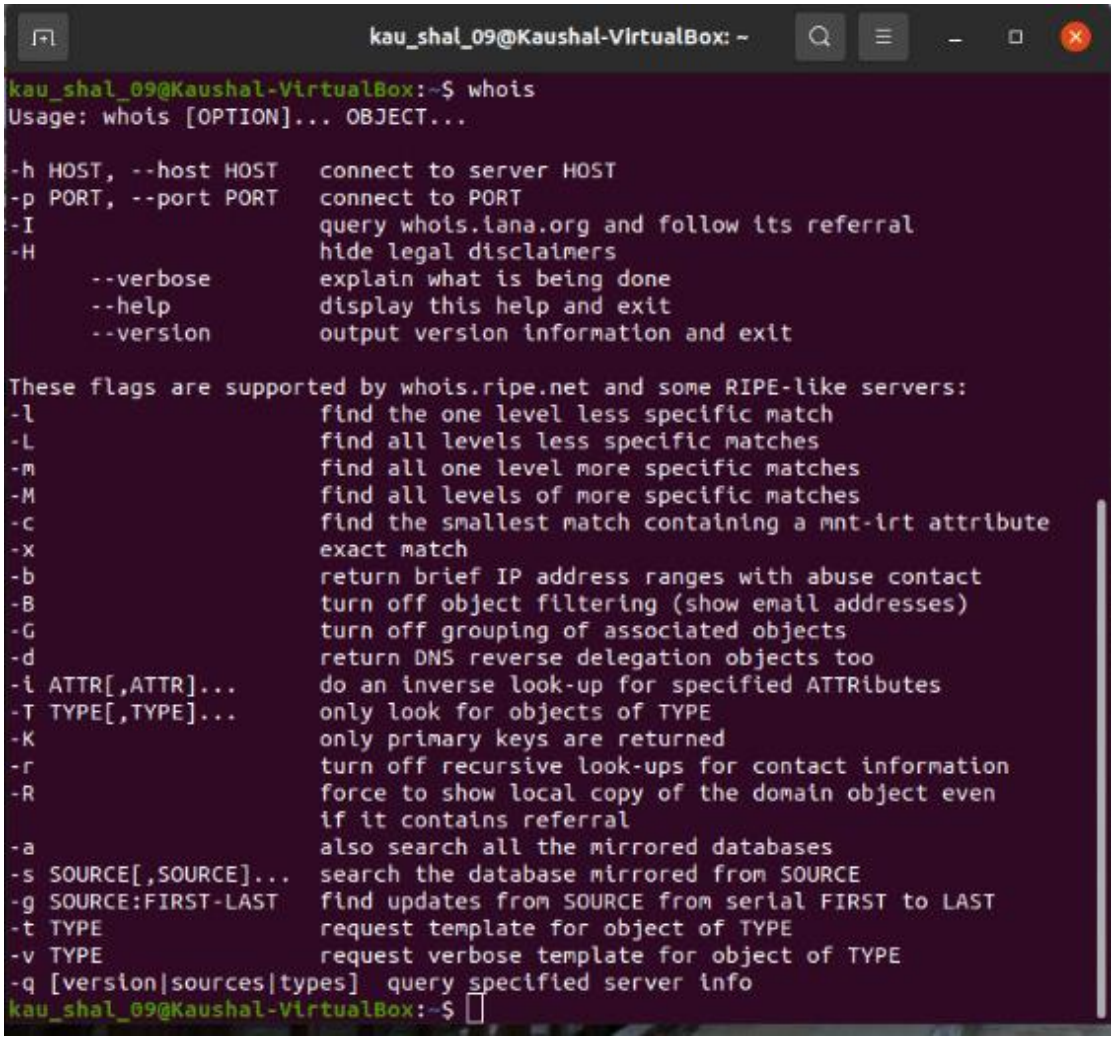
Traceroute:

Traceroute is the route tracing tool used on Unix-like Operating Systems (including Mac OS X). On Mac OS X, you can access Traceroute through the Network Utility.



Whois Command:

You can use the whois command in Linux to find out information about a domain, such as the owner of the domain, the owner's contact information, and the nameservers that the domain is using.



Host Command:

Host command is used to find domain name associated with the IP address or find IP address associated with domain name. The returned IP address is either IPv4 or IPv6.

```
kau_shal_09@Kaushal-VirtualBox: ~
kau_shal_09@Kaushal-VirtualBox:~$ host erp.vupune.ac.in
erp.vupune.ac.in has address 103.97.164.84
kau_shal_09@Kaushal-VirtualBox:~$ host 103.97.164.84
Host 84.164.97.103.in-addr.arpa. not found: 3(NXDOMAIN)
kau_shal_09@Kaushal-VirtualBox:~$ host google.com
google.com has address 142.251.42.78
google.com has IPv6 address 2404:6800:4009:81c::200e
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
kau_shal_09@Kaushal-VirtualBox:~$ host 142.251.42.78
78.42.251.142.in-addr.arpa domain name pointer bom12s21-in-f14.1e100.net.
kau_shal_09@Kaushal-VirtualBox:~$
```

Nmap Command:

Nmap is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators. It is used for the following purposes:

Real time information of a network

Detailed information of all the IPs activated on your network

Number of ports open in a network

Provide the list of live hosts

Port, OS and Host scanning

```
kau_shal_09@Kaushal-VirtualBox: ~
kau_shal_09@Kaushal-VirtualBox:~$ nmap erp.vupune.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-14 17:58 IST
Nmap scan report for erp.vupune.ac.in (103.97.164.84)
Host is up (0.10s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
110/tcp open  pop3
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 11.24 seconds
kau_shal_09@Kaushal-VirtualBox:~$
```