Batch: C-2	**Roll No.: 16010122323**
Experiment / assignment / tutorial No.02	
Grade: AA / AB / BB / BC / CC / CD /DD	
Signature of the Staff In-charge with date	

Experiment No. 2

Title: Study of basic network administration commands and network configuration.

AIM: Study networking commands –ping, traceroute, nslookup, arp, rarp, netstat, telnet.

Expected Outcome of Experiment:

1. Understand the fundamentals of network administration.

Books/ Journals/ Websites referred:

1. *Linux Lab - Open source Technology : Ambavade –Dreamtech*
2. http://manpages.ubuntu.com/manpages/trusty/man8/rarp.8.html
3. http://computernetworkingnotes.com/comptia-n-plus-study-guide/network-tool-command.html

---

Pre Lab/ Prior Concepts: Computer Network

New Concepts to be learned: Command line operation to handle networks.

Computers are connected in a network to exchange information or resources each other. Two or more computer connected through network media called computer network. There are number of network devices or media are involved to form computer network. Computer loaded with Windows and Linux Operating System can also be a part of network whether it is small or large network by its multitasking and multiuser natures. Maintaining of system and network up and running is a task of System / Network Administrator's job.

Frequently used network configuration and troubleshoot commands in Linux/Windows are as follows:

1. IFCONFIG/ IPCONFIG

ifconfig (interface configurator) command is use to initialize an interface, assign IP Address to interface and enable or disable interface on demand. With this command you can view IP Address and Hardware / MAC address assign to interface and also MTU (Maximum transmission unit) size.

ifconfig with interface (eth0) command only shows specific interface details like IP Address, MAC Address etc. with -a options will display all available interface details if it is disable also.

Syntax: # ifconfig eth0

To enable or **disable** specific Interface, we use example command as follows.

Enable eth0: # ifup eth0

Disable eth0: # ifdown eth0

To Setting MTU Size:

By default, MTU size is 1500. We can set required MTU size with below command.

Replace XXXX with size.

Syntax: # ifconfig eth0 mtu XXXX

Set Interface in Promiscuous mode.

Network interface only received packets belongs to that particular NIC. If you put interface in promiscuous mode, it will receive all the packets. This is very useful to capture packets and analyse later. For this you may require superuser access.

Syntax: # ifconfig eth0 - promisc

2. PING

PING (Packet INternet Groper) command is the best way to test connectivity between two nodes. Whether it is Local Area Network (LAN) or Wide Area Network (WAN). Ping use ICMP (Internet Control Message Protocol) to communicate to other devices.

It verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

ping [-c count] [-i wait] [-l preload][-s packetsize] host

-c count
Stop after sending (and receiving) count ECHO_RESPONSE packets.

-i wait
Wait wait seconds between sending each packet. The default is to wait for one second between each packet. This option is incompatible with the -f option.

-l preload
If preload is specified, ping sends that many packets as fast as possible before falling into its normal mode of behavior.

-s packetsize
Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

PING Command Example:

ping 4.2.2.2

ping -c 5 www.tecmint.com

3. TRACEROUTE/ TRACERT

traceroute is a network troubleshooting utility which shows number of hops taken to reach destination also determine packets traveling path. Below we are tracing route to global DNS server IP Address and able to reach destination also shows path of that packet is traveling.

Syntax:

tracert [**-d**] [**-h MaximumHops**] [**-j HostList**] [**-w Timeout**] [**TargetName**]

Parameters

-d : Prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of tracert results.

-h: MaximumHops Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.

-j: HostList Specifies that Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in

HostListThe HostList is a series of IP addresses (in dotted decimal notation) separated by spaces.

-w : Timeout Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds).

4. **NETSTAT command**

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols).

Netstat provides statistics for the following:

Proto - The name of the protocol (TCP or UDP).

Local Address - The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).

Foreign Address - The IP address and port number of the remote computer to which the socket is connected. The names that correspond to the IP address and the port are shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).

(**state**) Indicates the state of a TCP connection. The possible states are as follows:
CLOSE_WAIT
CLOSED
ESTABLISHED
FIN_WAIT_1
FIN_WAIT_2

LAST_ACK
LISTEN
SYN_RECEIVED
SYN_SEND
TIMED_WAIT

Syntax
netstat [**-a**] [**-e**] [**-n**] [**-o**] [**-p Protocol**] [**-r**] [**-s**] [**Interval**]

Parameters

Used without parameters, netstat displays active TCP connections.

-a Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

-e Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.

-n Displays active TCP connections, however, addresses and port numbers are expressed numerically, and no attempt is made to determine names.

-o Displays active TCP connections and includes the process ID (PID) for each connection.

-p Shows connections for the protocol specified by Protocol.

-s Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.

-r Displays the contents of the IP routing table.

Netstat (Network Statistic) command display connection info, routing table information etc. To displays routing table information use option as -r.

netstat –r

5. DIG

Dig (domain information groper) query DNS related information like A Record, CNAME, MX Record etc. This command mainly uses to troubleshoot DNS related query.

dig www. Ipadress.com

6. NSLOOKUP

The name "nslookup" means "name server lookup". nslookup is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record. It displays information from Domain Name System (DNS) name servers.

nslookup command also use to find out DNS related query.

Example:

C:\Documents and Settings\sysadm>nslookup itu.dk
Server: ns3.inet.tele.dk
Address: 193.162.153.164

Non-authoritative answer:
Name: itu.dk
Address: 130.226.133.2
nslookup www. Googel.com

7. ROUTE

Route command also shows and manipulate ip routing table. To see default routing table in Linux, type the following command.

route

8. ARP

When we need an Ethernet (MAC) address we can use arp(address resolution protocol).
In other words it shows the physical address of an host.

Syntax
arp [**-a** [**InetAddr**] [**-N IfaceAddr**]] [**-g** [**InetAddr**] [**-N IfaceAddr**]] [**-d InetAddr** [**IfaceAddr**]] [**-s InetAddr EtherAddr** [**IfaceAddr**]]

Parameters

Used without parameters, ping displays help
-a [InetAddr] [-N IfaceAddr] Displays current ARP cache tables for all interfaces.

-g [InetAddr] [-N IfaceAddr] Identical to -a.

-d InetAddr [IfaceAddr] Deletes an entry with a specific IP address, where InetAddr is the IP address.

-s InetAddr EtherAddr [IfaceAddr] Adds a static entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr.

To add a static ARP cache entry to the table for a specific interface, use the IfaceAddr parameter where IfaceAddr is an IP address assigned to the interface

ARP (Address Resolution Protocol) is useful to view / add the contents of the kernel's ARP tables. To see default table use the command as.

arp -e

Address HWtype HWaddress Flags Mask Iface

192.168.50.1 ether 00:50:56:c0:00:08 C eth0

9 . ETHTOOL

ethtool is a replacement of mii-tool. It is to view, setting speed and duplex of your Network Interface Card (NIC). You can set duplex permanently in /etc/sysconfig/network-scripts/ifcfg-eth0 with ETHTOOL_OPTS variable.

Syntax: # ethtool eth0

10. **TELNET**

The telnet command is used to communicate with another host using the TELNET protocol. If telnet is invoked without the host argument, it enters command mode, indicated by its prompt (telnet>) In this mode, it accepts and executes the commands listed below. If it is invoked with arguments, it performs an open command with those arguments.

To login to a remote machine, use this syntax:

% **telnet** <***hostname***>

The options are as follows:

-8 Specifies an 8-bit data path. This causes an attempt to negotiate the TELNET BINARY option on both input and output.

-E Stops any character from being recognized as an escape character.

-K Specifies no automatic login to the remote system.

11. HOTENAME

hostname is to identify in a network. Execute hostname command to see the hostname of your box. You can set hostname permanently in /etc/sysconfig/network. Need to reboot box once set a proper hostname.

hostname

12. SYSTEMINFO

Display information about a system.

IMPLEMENTATION:

Show the use of different network commands:

ipconfig(DOS)

```
C:\Users\ASUS>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

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

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a5d3:da00:484f:ba8%50
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : SVV.local
   Link-local IPv6 Address . . . . . : fe80::8f76:9518:affa:a9e7%13
   IPv4 Address. . . . . . . . . . . : 10.0.13.39
   Subnet Mask . . . . . . . . . . . : 255.255.128.0
   Default Gateway . . . . . . . . . : 10.0.0.1

Ethernet adapter Bluetooth Network Connection:

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

ifconfig(Linux)

```
┌──(kartik㉿kartikVM)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fed7:a00a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d7:a0:0a  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 3280 (3.2 KiB)
        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
```

ping(DOS)

```
C:\Users\ASUS>ping google.com

Pinging google.com [142.250.192.14] with 32 bytes of data:
Reply from 142.250.192.14: bytes=32 time=5ms TTL=59
Reply from 142.250.192.14: bytes=32 time=7ms TTL=59
Reply from 142.250.192.14: bytes=32 time=5ms TTL=59
Reply from 142.250.192.14: bytes=32 time=6ms TTL=59

Ping statistics for 142.250.192.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 7ms, Average = 5ms
```

tracert(DOS)

```
C:\Users\ASUS>tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [142.250.183.110]
over a maximum of 30 hops:

  1     4 ms     3 ms     4 ms  10.0.0.1
  2     3 ms     1 ms     2 ms  172.30.250.250
  3     7 ms    12 ms    11 ms  14.142.143.97.static-mumbai.vsnl.net.in [14.142.143.97]
  4    17 ms    12 ms    24 ms  115.113.165.98.static-mumbai.vsnl.net.in [115.113.165.98]
  5    20 ms    16 ms    19 ms  216.239.57.17
  6     7 ms     5 ms     4 ms  72.14.239.247
  7    16 ms     4 ms     5 ms  bom12s13-in-f14.1e100.net [142.250.183.110]

Trace complete.
```

netstat(Unix)

```
┌──(kartik㉿kartikVM)-[~]
└─$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 10.0.2.15:bootpc        10.0.2.2:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     9719
unix  3      [ ]         STREAM     CONNECTED     9684     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     9460     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9419     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     11459    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9593
unix  3      [ ]         STREAM     CONNECTED     8166
unix  3      [ ]         STREAM     CONNECTED     7649
unix  3      [ ]         STREAM     CONNECTED     12451    /run/user/1000/gvfsd/socket-LUraWpdB
unix  3      [ ]         STREAM     CONNECTED     11493
unix  3      [ ]         STREAM     CONNECTED     12410    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     10330    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10320    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     11375
unix  3      [ ]         STREAM     CONNECTED     9646     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8191     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     9383     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12306
unix  3      [ ]         STREAM     CONNECTED     9207
unix  2      [ ]         DGRAM      CONNECTED     8785
unix  3      [ ]         STREAM     CONNECTED     12393    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9413
unix  3      [ ]         STREAM     CONNECTED     6058
unix  3      [ ]         STREAM     CONNECTED     952
unix  3      [ ]         STREAM     CONNECTED     7607
unix  3      [ ]         STREAM     CONNECTED     2952     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     11371
unix  3      [ ]         STREAM     CONNECTED     8037
unix  3      [ ]         STREAM     CONNECTED     10362
unix  3      [ ]         STREAM     CONNECTED     9115
unix  3      [ ]         STREAM     CONNECTED     11288    /run/user/1000/at-spi/bus_0
```

Netstat(DOS)

```
C:\Users\ASUS>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.0.13.39:49992       20.198.119.143:https   ESTABLISHED
  TCP    10.0.13.39:53405       20.212.88.117:https    ESTABLISHED
  TCP    10.0.13.39:53467       sm-in-f188:5228        ESTABLISHED
  TCP    10.0.13.39:53599       bom12s17-in-f10:https  TIME_WAIT
  TCP    10.0.13.39:53614       whatsapp-cdn-shv-02-pnq1:https  CLOSE_WAIT
  TCP    10.0.13.39:53629       bom12s11-in-f14:https  ESTABLISHED
  TCP    10.0.13.39:53631       bom12s01-in-f3:https   ESTABLISHED
  TCP    10.0.13.39:53635       pnbomb-aa-in-f3:https  TIME_WAIT
  TCP    10.0.13.39:53636       bom12s14-in-f14:https  ESTABLISHED
  TCP    10.0.13.39:53640       20.24.121.134:https    CLOSE_WAIT
  TCP    10.0.13.39:53648       bom12s11-in-f14:https  TIME_WAIT
  TCP    10.0.13.39:53658       bom12s12-in-f22:https  TIME_WAIT
  TCP    10.0.13.39:53663       bom07s30-in-f14:https  TIME_WAIT
  TCP    10.0.13.39:53670       bom12s20-in-f3:https   TIME_WAIT
  TCP    10.0.13.39:53673       hkg12s10-in-f46:https  TIME_WAIT
  TCP    10.0.13.39:53680       bom12s01-in-f3:https   ESTABLISHED
  TCP    10.0.13.39:53686       bom07s45-in-f14:https  TIME_WAIT
  TCP    10.0.13.39:53689       bom12s14-in-f10:https  TIME_WAIT
  TCP    10.0.13.39:53703       bom12s14-in-f14:https  ESTABLISHED
  TCP    10.0.13.39:53709       bom12s01-in-f3:https   TIME_WAIT
  TCP    10.0.13.39:53712       52.98.59.18:https      ESTABLISHED
  TCP    10.0.13.39:53716       a23-32-29-106:https    CLOSE_WAIT
  TCP    10.0.13.39:53717       52.98.34.194:https     ESTABLISHED
  TCP    10.0.13.39:53720       104.208.16.91:https    CLOSE_WAIT
  TCP    10.0.13.39:53721       bom07s18-in-f10:https  TIME_WAIT
  TCP    10.0.13.39:53722       13.107.246.254:https   CLOSE_WAIT
  TCP    10.0.13.39:53723       20.215.216.50:https    CLOSE_WAIT
  TCP    10.0.13.39:53724       204.79.197.222:https   CLOSE_WAIT
  TCP    10.0.13.39:53727       ec2-3-6-211-252:https  TIME_WAIT
  TCP    10.0.13.39:53745       13.70.79.200:https     TIME_WAIT
```

Dig(Linux)

```
┌──(kartik㉿kartikVM)-[~]
└─$ dig youtube.com

; <<>> DiG 9.19.21-1+b1-Debian <<>> youtube.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49771
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;youtube.com.                   IN      A

;; ANSWER SECTION:
youtube.com.            275     IN      A       216.58.196.78

;; Query time: 4 msec
;; SERVER: 172.31.0.26#53(172.31.0.26) (UDP)
;; WHEN: Tue Jul 30 09:24:59 IST 2024
;; MSG SIZE  rcvd: 56
```

nslookup(DOS) – KJSCE LMS

```
C:\Users\ASUS>nslookup lms-kjsce.somaiya.edu
Server:  svvdc02.svv.local
Address:  172.31.0.26

Non-authoritative answer:
Name:    lms-kjsce.somaiya.edu
Addresses:  152.52.34.132
          115.112.43.147
```

ethtool(Linux)

```
┌──(kartik㉿kartikVM)-[~]
└─$ ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: Yes
        Advertised FEC modes: Not reported
        Speed: 1000Mb/s
        Duplex: Full
        Auto-negotiation: on
        Port: Twisted Pair
        PHYAD: 0
        Transceiver: internal
        MDI-X: off (auto)
netlink error: Operation not permitted
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes
```

Systeminfo(DOS)

```
C:\Users\ASUS>systeminfo

Host Name:                 KARTIK-TUF
OS Name:                   Microsoft Windows 11 Home Single Language
OS Version:                10.0.22631 N/A Build 22631
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          ASUS
Registered Organization:   N/A
Product ID:                00327-30000-00000-AAOEM
Original Install Date:     21-Apr-24, 5:47:32 AM
System Boot Time:          16-Jul-24, 6:18:04 PM
System Manufacturer:       ASUSTeK COMPUTER INC.
System Model:              ASUS TUF Dash F15 FX517ZC
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 154 Stepping 3 GenuineIntel ~2300 Mhz
BIOS Version:              American Megatrends International, LLC. FX517ZC.318, 28-Jun-23
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     16,006 MB
Available Physical Memory: 3,718 MB
Virtual Memory: Max Size:  20,620 MB
Virtual Memory: Available: 4,034 MB
Virtual Memory: In Use:    16,586 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\KARTIK-TUF
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB5039895
                           [02]: KB5027397
                           [03]: KB5040442
                           [04]: KB5039338
Network Card(s):           4 NIC(s) Installed.
                           [01]: Intel(R) Wi-Fi 6 AX201 160MHz
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     172.31.0.25
                                 IP address(es)
                                 [01]: 10.0.13.39
                                 [02]: fe80::8f76:9518:affa:a9e7
                           [02]: Intel(R) Ethernet Connection (16) I219-V
                                 Connection Name: Ethernet 2
                                 Status:          Media disconnected
                           [03]: Bluetooth Device (Personal Area Network)
                                 Connection Name: Bluetooth Network Connection
                                 Status:          Media disconnected
                           [04]: VirtualBox Host-Only Ethernet Adapter
                                 Connection Name: Ethernet 3
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.56.1
                                 [02]: fe80::a5d3:da00:484f:ba8
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

pstree(Linux): Pstree command in Linux that shows the running processes as a tree which is a more convenient way to display the processes hierarchy and makes the output more visually appealing. The root of the tree is either init or the process with the given pid. Pstree can also be installed in other Unix systems.

cat /etc/passwd(Linux): Displays all the users on the system

```
┌──(kartik㉿kartikVM)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
tss:x:102:103:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:105:105::/var/lib/gophish:/usr/sbin/nologin
iodine:x:106:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:107:106::/nonexistent:/usr/sbin/nologin
tcpdump:x:108:107::/nonexistent:/usr/sbin/nologin
miredo:x:109:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:110:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmp:x:111:109::/var/lib/snmp:/bin/false
redis:x:112:111::/var/lib/redis:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mosquitto:x:114:114::/var/lib/mosquitto:/usr/sbin/nologin
redsocks:x:115:115::/var/run/redsocks:/usr/sbin/nologin
stunnel4:x:991:991:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
sshd:x:116:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
statd:x:117:65534::/var/lib/nfs:/usr/sbin/nologin
sslh:x:118:118::/nonexistent:/usr/sbin/nologin
postgres:x:119:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi:x:120:120:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
_gvm:x:121:122::/var/lib/openvas:/usr/sbin/nologin
speech-dispatcher:x:122:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
inetsim:x:123:124::/var/lib/inetsim:/usr/sbin/nologin
pulse:x:124:125:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
geoclue:x:125:127::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:126:128:Light Display Manager:/var/lib/lightdm:/bin/false
saned:x:127:130::/var/lib/saned:/usr/sbin/nologin
polkitd:x:989:989:User for polkitd:/:/usr/sbin/nologin
rtkit:x:128:131:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:129:132:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:130:133:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:131:134:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
kartik:x:1000:1000:kartik,,,:/home/kartik:/bin/bash
hulk:x:1002:1002::/home/hulk:/bin/bash
nebula:x:1007:1007::/home/nebula:/bin/sh
loki:x:1008:1009::/home/loki:/bin/sh
```

pwd: Print working directory
whoami: displays current user name
ls: Lists all the files in the current directory

CONCLUSION: Learnt and implemented various DOS and Unix commands and network configuration.

Post Lab Questions

1) Give details of minimum 5 commands which is not included in the write-up.

DOS:

1. **fc**: Compares two files or sets of files and displays the differences.
2. **cipher**: Displays or alters the encryption of directories and files on NTFS volumes.
3. **tree**: Graphically displays the directory structure of a drive or path.
4. **tasklist**: Displays a list of currently running processes.
5. **shutdown**: Allows for the shutdown, restart, or log off of a computer.

Unix:

1. **grep**: Searches for patterns within files.
2. **awk**: Pattern scanning and processing language for files.
3. **sed:** Stream editor for filtering and transforming text.
   Eg. sed 's/old/new/g' file.txt replaces all occurrences of "old" with "new" in file.txt.
4. **rsync:** Synchronizes files and directories between two locations.
   Eg. rsync -avz /source/ /destination/ syncs /source/ to /destination/ with archive, verbose, and compression options.
5. **tmux:** Terminal multiplexer allowing multiple sessions in one terminal.
   Eg. tmux new -s session_name starts a new tmux session named session_name.

2) Give the reason why some commands are not working in the Lab.

- In the lab environment, some commands may not be working due to permission issues, where users lack the necessary privileges to execute them. Additionally, the commands might not be in the system's PATH environment variable, preventing the system from locating the executable. Network restrictions could also play a role, as certain commands requiring internet access might be blocked by lab network policies. Furthermore, in lab, we have virtual machines which have

some restricted capabilities, limiting the functionality of some commands.