

**Vinod Mishra**

**Intern id :- 2037**

Pwd :-Shows the current directory path

```
└─(vinod@vinod)~  
└─$ pwd  
/home/vinod
```

Ls:- Lists files and folders

```
└─(vinod@vinod)~  
└─$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos vinod
```

Mkdir:- Creates a new directory

```
└─(vinod@vinod)~  
└─$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos  
  
└─(vinod@vinod)~  
└─$ mkdir vinod  
  
└─(vinod@vinod)~  
└─$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos vinod
```

Rmdir:- Deletes an empty directory

```
└─(vinod@vinod)~  
└─$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos vinod  
  
└─(vinod@vinod)~  
└─$ rmdir vinod  
  
└─(vinod@vinod)~  
└─$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos
```

Clear:- Clears the terminal screen

```
y  
^C  
  
└─(vinod@vinod)~  
└─$ clear█
```

## History:- commands history

```
└─(vinod㉿vinod)-[~]
$ history
 1 cat
 2 mkdir vinod
 3 ls
 4 rmdir vinod
 5 ls
 6 mkdir vinod
 7 ls
 8 man
 9 more
10 more --help
```

## --help:- display help for built-in commands

```
└─(vinod㉿vinod)-[~]
$ more --help

Usage:
more [options] <file> ...

Display the contents of a file in a terminal.

Options:
-d, --silent      display help instead of ringing bell
-f, --logical     count logical rather than screen lines
-l, --no-pause    suppress pause after form feed
-c, --print-over  do not scroll, display text and clean line ends
-p, --clean-print do not scroll, clean screen and display text
-e, --exit-on-eof  exit on end-of-file
-s, --squeeze     squeeze multiple blank lines into one
-u, --plain       suppress underlining and bold
-n, --lines <number> the number of lines per screenful
-<number>          same as --lines
+<number>         display file beginning from line number
+/<pattern>       display file beginning from pattern match

-h, --help         display this help
-V, --version      display version

For more details see more(1).
```

## Date:- display or change the date and time

```
└─(vinod㉿vinod)-[~]
$ date
Sun Dec 28 12:27:03 EST 2025
```

## Cal:- display a calendar

```
└─(vinod㉿vinod)-[~]
$ cal
December 2025
Su Mo Tu We Th Fr Sa
   1  2  3  4  5  6
  7  8  9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31
```

## Top:- change file timestamps

```
└─(vinod㉿vinod)-[~]
$ top

top - 13:45:49 up 1:46, 2 users, load average: 0.36, 0.52, 0.40
Tasks: 218 total, 1 running, 217 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.6 us, 0.5 sy, 0.0 ni, 98.8 id, 0.0 wa, 0.0 hi, 0.1 si, 0.0 st
MiB Mem : 3850.0 total, 908.6 free, 1635.0 used, 1615.1 buff/cache
MiB Swap: 975.0 total, 975.0 free, 0.0 used. 2215.1 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
-----	------	----	----	------	-----	-----	---	------	------	-------	---------

**Netstat -tuln:-** netstat -tuln is a Linux networking command used to display all listening TCP and UDP ports on the system in numeric format.

```
(vinod@vinod) [~]
$ netstat -tuln

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 127.0.0.1:41951          0.0.0.0:*
                                         LISTEN
```

**Ss -tuln:-** ss -tuln is a Linux command used to display all listening TCP and UDP ports on the system in a fast and modern way, and it is the replacement for netstat.

```
(vinod@vinod) [~]
$ ss -tuln

Netid      State      Recv-Q      Ask anything      Send-Q      Local Address:Port      Peer Address:Port
tcp      LISTEN      0          0.0.0.0:41951      4096      127.0.0.1:41951      0.0.0.0:*
```

**Uptime:-** show uptime

```
(vinod@vinod) [~]
$ uptime

13:52:17 up 1:52, 2 users, load average: 0.74, 0.63, 0.48
```

**Df:-** display free disk space

```
(vinod@vinod) [~]
$ df

Filesystem 1K-blocks Used Available Use% Mounted on
udev      1928384   0 1928384  0% /dev
tmpfs     394244 1040 393204  1% /run
/dev/sda1 101639152 16616856 79813108 18% /
tmpfs     1971216   0 1971216  0% /dev/shm
tmpfs      5120   0  5120  0% /run/lock
tmpfs     1024   0  1024  0% /run/credentials/systemd-journald.service
tmpfs     1024   0  1024  0% /run/credentials/systemd-udev-load-credentials.service
tmpfs     1024   0  1024  0% /run/credentials/systemd-tmpfiles-setup-dev-early.service
tmpfs     1024   0  1024  0% /run/credentials/systemd-sysctl.service
tmpfs     1024   0  1024  0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs     1971216   52 1971164  1% /tmp
tmpfs     1024   0  1024  0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs     1024   0  1024  0% /run/credentials/getty@tty1.service
tmpfs    394240  120 394120  1% /run/user/1000
```

**Whoami:-** Displays current user

```
(vinod@vinod) [~]
$ whoami
vinod
```

**Find:-** search for files that meet a desired criteria

```
(vinod@vinod) [~]
$ find vinod
vinod
```

**Whois:-** whois is a Linux command-line tool used to retrieve domain name and IP address registration information from WHOIS databases.

```
(vinod@vinod) [~]
$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST      connect to server HOST
-p PORT, --port PORT     connect to PORT
-I                         query whois.iana.org and follow its referral
-H                         hide legal disclaimers
--verbose                  explain what is being done
--no-recursion             disable recursion from registry to registrar servers
--help                      display this help and exit
--version                  output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                         find the one level less specific match
-L                         find all levels less specific matches
-m                         find all one level more specific matches
-M                         find all levels of more specific matches
-c                         find the smallest match containing a mnt-irt attribute
-x                         exact match
-b                         return brief IP address ranges with abuse contact
-B                         turn off object filtering (show email addresses)
-G                         turn off grouping of associated objects
-d                         return DNS reverse delegation objects too
-i ATTR[,ATTR]...          do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...          only look for objects of TYPE
-K                         only primary keys are returned
-r                         turn off recursive look-ups for contact information
-R                         force to show local copy of the domain object even
                           if it contains referral
-a                         also search all the mirrored databases
-s SOURCE[,SOURCE]...       search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST        find updates from SOURCE from serial FIRST to LAST
-t TYPE                     request template for object of TYPE
-v TYPE                     request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
```

**Apt update:-**Updates package list

```
(vinod@vinod) [~]
$ apt update
```

**Apt upgrade:-** Upgrades installed packages

```
(vinod@vinod) [~]
$ apt upgrade
```

**apt install <tool>:-**Installs a tool

```
(vinod@vinod) [~]
$ apt install quota
```

**apt remove <tool>:-**Removes a tool

```
(vinod@vinod) [~]
$ apt remove nmap
```

Groups:- print group names a user is in

```
(vinod@vinod)-[~] free -h
$ groups
vinod adm dialout cdrom floppy sudo audio dip video plugdev users netdev bluetooth wireshark scanner vboxsf kaboxer
```

Man nmap:- man nmap is a Linux command used to open the manual (man page) for the Nmap tool.

```
(vinod@vinod)-[~]
$ man nmap
```

```
NMAP(1)                               36.  Amap                               Nmap Reference Guide                               NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

SYNOPSIS
    nmap [Scan Type ...] [Options] {target specification} ...

DESCRIPTION
    Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

    The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name and state. The state is either open|filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.

    In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

    A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution; and then the hostname.

Example 1. A representative Nmap scan
# nmap -A -T4 scanme.nmap.org
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: lib6-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:08:09:ac:d4:e2:32:42:c4:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open  http  Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
Manual page nmap(1) line 1 (press h for help or q to quit)
```

Ifconfig:- Shows network interfaces

```
KaliLinux  File Actions Edit View Help
zsh: corrupt history file /home/vinod/.zsh_history
(vinod@vinod)-[~]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0 broadcast 172.17.255.255
              ether 02:42:1c:28:f3:09 txqueuelen 0  (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.0.36  netmask 255.255.255.0 broadcast 192.168.0.255
              inet6 fe80::a00:27ff:fe75:b83  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:5b:83 txqueuelen 1000  (Ethernet)
        RX packets 138220 bytes 63137226 (60.2 MiB)
        RX errors 0 dropped 2901 overruns 0 frame 0
        TX packets 23959 bytes 4710815 (4.4 MiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
              inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 15589 bytes 1187422 (1.1 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 15589 bytes 1187422 (1.1 MiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Iwconfig:- Shows wireless info

```
└─(vinod㉿vinod)-[~]
$ iwconfig
lo      no wireless extensions.

eth0     no wireless extensions.

docker0  no wireless extensions.
```

Nmap:- nmap (Network Mapper) is a network scanning and security auditing tool used to discover hosts, open ports, services, and vulnerabilities on a network.

```
└─(vinod㉿vinod)-[~]
$ nmap 172.17.0.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 03:13 EDT
Nmap scan report for 172.17.0.3
Host is up (0.000065s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

## Traceroute:- trace route to host

```
└─(vinod㉿vinod)-[~]
$ traceroute instagram.com
traceroute to instagram.com (157.240.237.174), 30 hops max, 60 byte packets
1 RTK_GW.hgu_lan (192.168.0.1) 7.213 ms 6.686 ms 6.567 ms
2 18.18.200.234 (18.18.200.234) 6.467 ms 6.340 ms 6.229 ms
3 18.18.200.233 (18.18.200.233) 6.152 ms 6.091 ms 6.004 ms
4 103.39.246.14.softcall.net.in (103.39.246.14) 5.903 ms 5.804 ms 5.726 ms
5 103.39.246.13.softcall.net.in (103.39.246.13) 23.639 ms 23.562 ms 23.452 ms
6 ae3.pr04.pnq1.tfbnw.net (157.240.83.58) 19.225 ms 19.166 ms 18.898 ms
7 po104.psw02.pnq1.tfbnw.net (129.134.108.201) 2.838 ms 2.786 ms po104.psw01.pnq1.tfbnw.net (129.134.108.193) 2
.570 ms
8 mswlaq.02.pnq1.tfbnw.net (129.134.86.67) 2.495 ms mswlar.02.pnq1.tfbnw.net (129.134.86.73) 2.428 ms mswlan.02.
pnq1.tfbnw.net (129.134.86.76) 2.699 ms
```

## Ping:- test a network connection

```
└─(vinod㉿vinod)-[~]
$ ping instagram.com
PING instagram.com (157.240.237.174) 56(84) bytes of data.
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=1 ttl=58 time=3.75 ms
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=2 ttl=58 time=4.98 ms
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=3 ttl=58 time=4.03 ms
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=4 ttl=58 time=5.09 ms
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=8 ttl=58 time=4.86 ms
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=9 ttl=58 time=3.80 ms
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=10 ttl=58 time=4.34 ms
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=11 ttl=58 time=3.63 ms
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=12 ttl=58 time=4.01 ms
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=13 ttl=58 time=2.74 ms
64 bytes from instagram-p42-shv-02-pnq1.fbcnd.net (157.240.237.174): icmp_seq=14 ttl=58 time=3.61 ms
^C
--- instagram.com ping statistics ---
14 packets transmitted, 11 received, 21.4286% packet loss, time 13079ms
rtt min/avg/max/mdev = 2.738/4.076/5.089/0.668 ms
```

## Netstat:- networking information

```
vinod@vinod: ~
File Actions Edit View Help
ls Netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0  vinod.ngu.lan:46398      93.243.107.34.bc:https ESTABLISHED
tcp        0      0  192.168.0.121:4444       192.168.0.77:45264    ESTABLISHED
tcp        0      0  b012508-in-f10.1:https   TIME_WAIT
udp       0      0  vinod.ngu.lan:bootpc    RTK_GW.ngu.lan:bootps ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto Refcnt Flags      Type      State          I-Node      Path
unix    3      [ ]      STREAM   CONNECTED  299547
unix    3      [ ]      STREAM   CONNECTED  1052
unix    3      [ ]      STREAM   CONNECTED  10565     /run/user/1000/at-spi/bus_0
unix    3      [ ]      STREAM   CONNECTED  10440
unix    3      [ ]      STREAM   CONNECTED  12366
unix    3      [ ]      STREAM   CONNECTED  10946
unix    3      [ ]      STREAM   CONNECTED  12290     /run/user/1000/at-spi/bus_0
unix    3      [ ]      STREAM   CONNECTED  8860      /run/user/1000/at-spi/bus_0
unix    3      [ ]      STREAM   CONNECTED  11531
unix    3      [ ]      STREAM   CONNECTED  100454
unix    3      [ ]      STREAM   CONNECTED  10916
unix    3      [ ]      STREAM   CONNECTED  10470     /run/user/1000/bus
unix    3      [ ]      STREAM   CONNECTED  2555      /run/systemd/journal/stdout
unix    3      [ ]      SEQPACKET CONNECTED  12081
unix    3      [ ]      SEQPACKET CONNECTED  10001
unix    3      [ ]      STREAM   CONNECTED  294339
unix    3      [ ]      STREAM   CONNECTED  46121     /run/user/1000/gvfsd/socket-gHogquVR
unix    3      [ ]      STREAM   CONNECTED  10660     /run/user/1000/bus
unix    3      [ ]      STREAM   CONNECTED  11503
unix    3      [ ]      SEQPACKET CONNECTED  10000449
unix    3      [ ]      SEQPACKET CONNECTED  27183
unix    3      [ ]      STREAM   CONNECTED  7045      @/tmp/.X11-unix/X0
unix    3      [ ]      STREAM   CONNECTED  12351
unix    3      [ ]      STREAM   CONNECTED  854
unix    3      [ ]      STREAM   CONNECTED  294624
unix    3      [ ]      STREAM   CONNECTED  8719      @/tmp/.ICE-unix/1026
unix    3      [ ]      STREAM   CONNECTED  301077
unix    3      [ ]      SEQPACKET CONNECTED  152935
unix    3      [ ]      STREAM   CONNECTED  10016     /run/user/1000/bus
unix    3      [ ]      SEQPACKET CONNECTED  26923
unix    3      [ ]      STREAM   CONNECTED  9721      /run/systemd/journal/stdout
unix    3      [ ]      STREAM   CONNECTED  876
unix    3      [ ]      STREAM   CONNECTED  11648
unix    3      [ ]      STREAM   CONNECTED  8711     @/tmp/.ICE-unix/1026
unix    3      [ ]      DGRAM   CONNECTED  442
```

Dirb:- dirb is a web content scanning tool used in penetration testing to brute-force hidden directories and files on a web server using a wordlist.

```
(vinod@vinod)-[~]
$ dirb http://172.17.0.2

DIRB v2.22
By The Dark Raver

START_TIME: Thu Oct 17 15:11:57 2024
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

-- Scanning URL: http://172.17.0.2/ --
+ http://172.17.0.2/index.php (CODE:200|SIZE:2613)
+ http://172.17.0.2/robots.txt (CODE:200|SIZE:44)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)

END_TIME: Thu Oct 17 15:11:58 2024
DOWNLOADED: 4612 - FOUND: 3
```

sudo sudo docker ps:- docker ps is a Docker command used to list all currently running containers on the system.

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
9a9160cf3c5a	hacksudo/localhostctf	"sh -c 'service apac..."	44 seconds ago	Up 43 seconds	0.0.0.0:22→22/tcp, ::22→22/tcp, 0.0.0.0:80→80/tcp, :

**msfconsole**: msfconsole is the main command-line interface of the Metasploit Framework, used for developing, testing, and executing exploits, payloads, and auxiliary modules in penetration testing.

```
[vino@vino ~]$ msfconsole  
Metasploit tip: Save the current environment with the save command,  
future console restarts will use this environment again  
  
(((_o_))' _\ )  
 \ / o_o / ( _ ) _ _ _ | \ *  
  o_o \ \ M S F | | \ / *  
   ||| —WW||| |||  
  
      =[ metasploit v6.4.18-dev ]  
+ -- =[ 2437 exploits - 1255 auxiliary - 429 post ]  
+ -- =[ 1471 payloads - 47 encoders - 11 nops ]  
+ -- =[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > █
```

**Sudo:-** Runs commands as admin

```
[vinod@vinod ~]$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-ABkNnS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABkNnS] [-g group] [-h host] [-p prompt] [-U user]
           [-u user] [command [arg ... ]]
usage: sudo [-ABbEHkNnP] [-r role] [-t type] [-C num] [-D directory]
           [-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
           [-u user] [VAR=value] [-i | -s] [command [arg ... ]]
usage: sudo -e [-ABkNnS] [-r role] [-t type] [-C num] [-D directory]
           [-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
           [-u user] file ...
```

Sudo su:- is a Linux command used to switch from the current user to the root (superuser) account with a full root login environment.

```
└─(vinod@vinod)-[~]
$ sudo su
[sudo] password for vinod:
└─(root@vinod)-[/home/vinod]
# exit
```