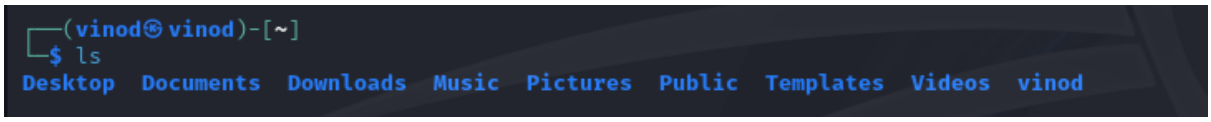
Vinod Mishra

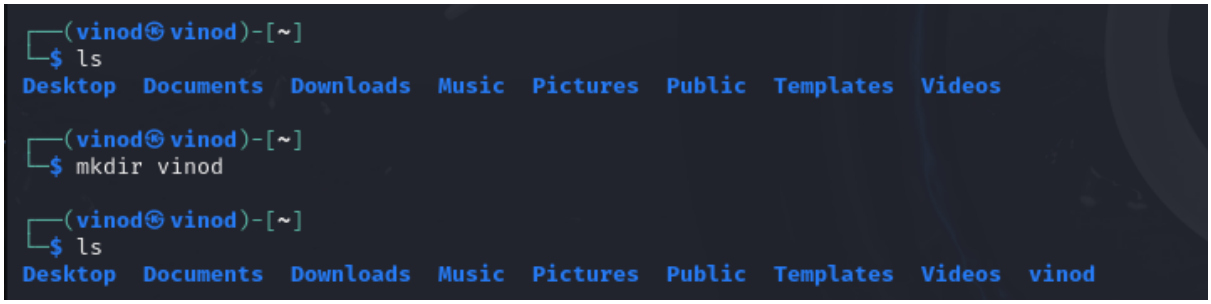
Intern id :- 2037

Pwd :-Shows the current directory path

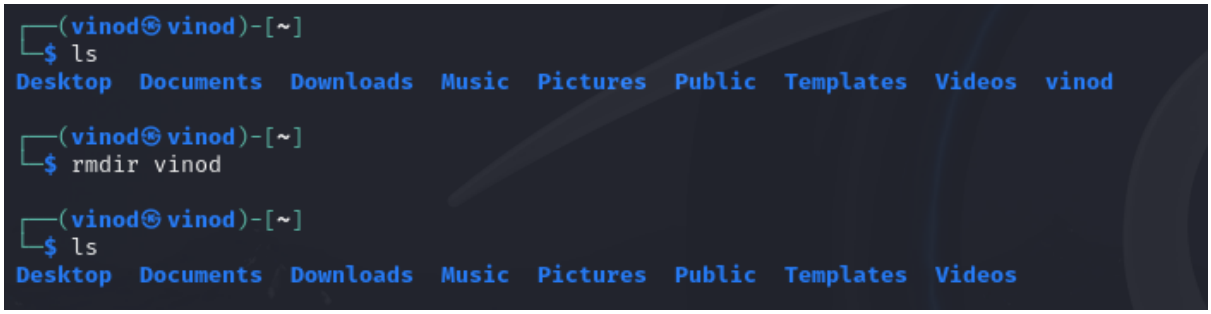
Ls:- Lists files and folders



Mkdir:- Creates a new directory

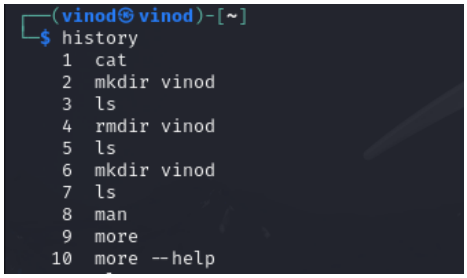


Rmdir:- Deletes an empty directory

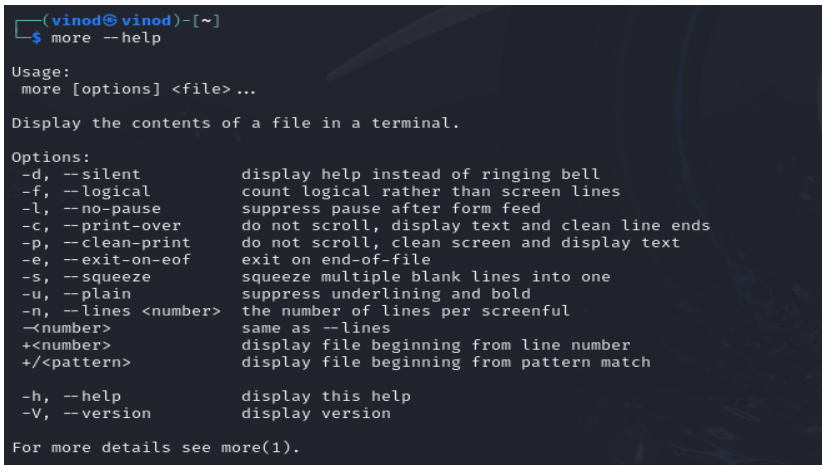


Clear:- Clears the terminal screen

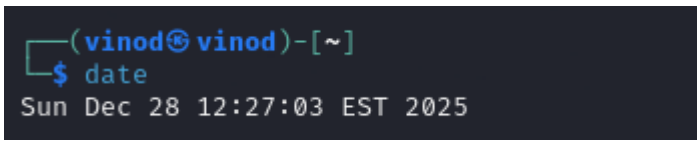
History:- commands history



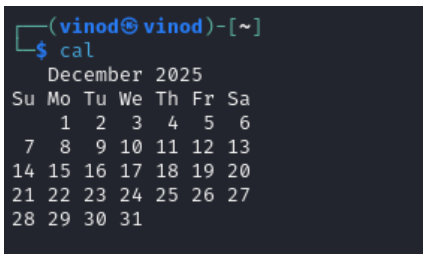
--help:- display help for built-in commands



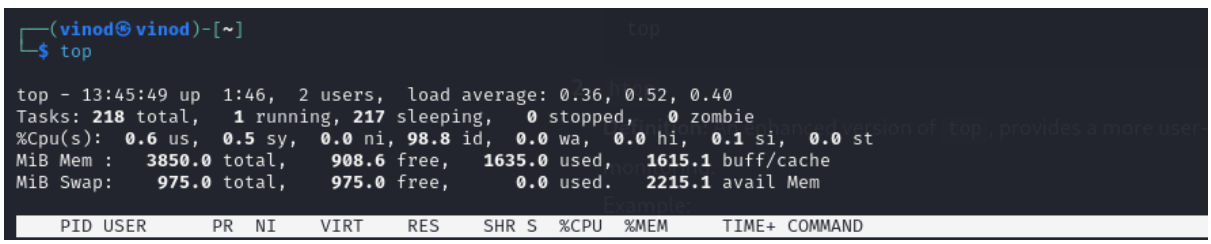
Date:- display or change the date and time



Cal:- display a calendar



Top:- change file timestamps



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               Send-Q                             Local Address:Port                              Peer Address:Port
tcp                 LISTEN               0                    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
```

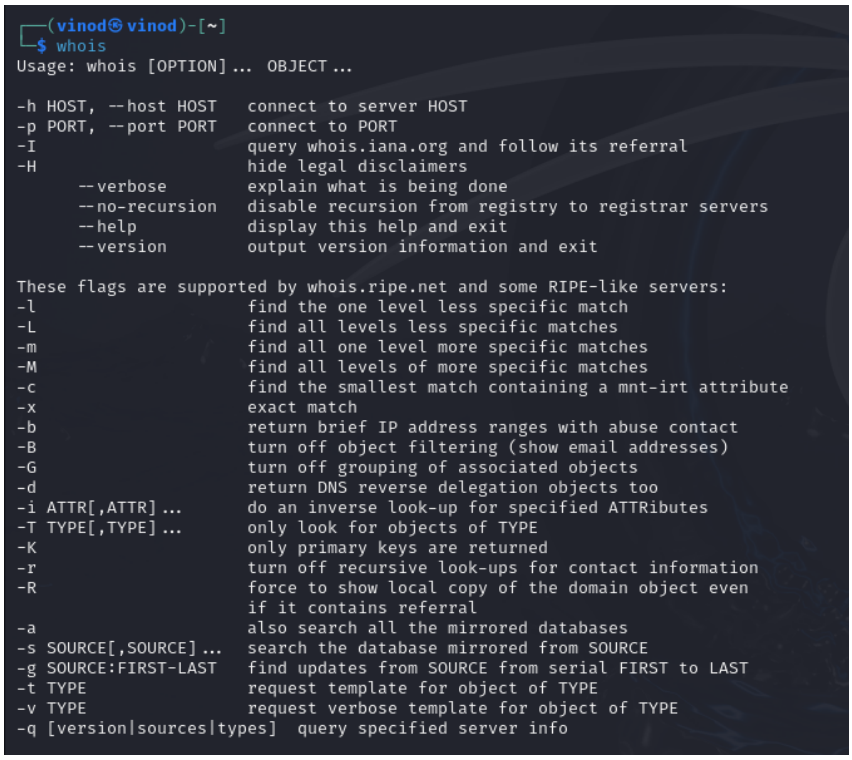
Whoami:- Displays current user

```
┌──(vinod㉿vinod)-[~]
└─$ whoami
vinod
```

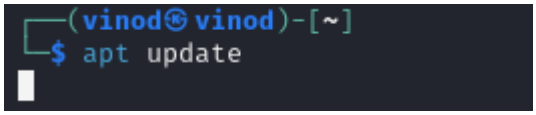
Find:- search for files that meet a desired criteria

```
┌──(vinod㉿vinod)-[~]
└─$ find vinod
vinod
```

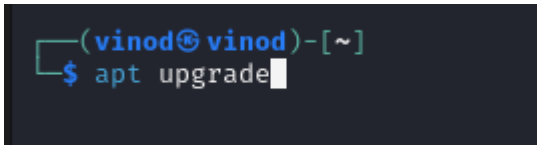
Whois:- whois is a Linux command-line tool used to retrieve domain name and IP address registration information from WHOIS databases.



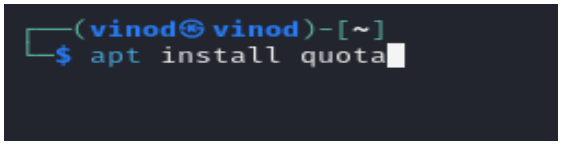
Apt update:-Updates package list



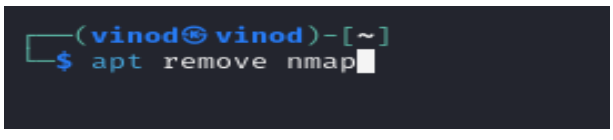
Apt upgrade:- Upgrades installed packages



apt install <tool>:-Installs a tool



apt remove <tool>:-Removes a tool



Groups:- print group names a user is in

```
┌──(vinod㉿vinod)-[~]
└─$ 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.

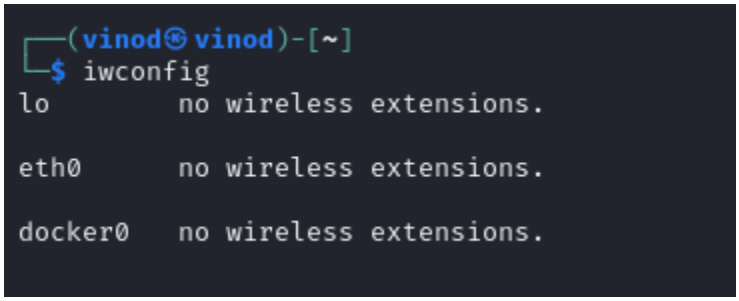
```
┌──(vinod㉿vinod)-[~]
└─$ man nmap
```

```
NMAP(1)                                  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: li86-221.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:f8:09:ac:d4:e2:32:42:10:49: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)
```

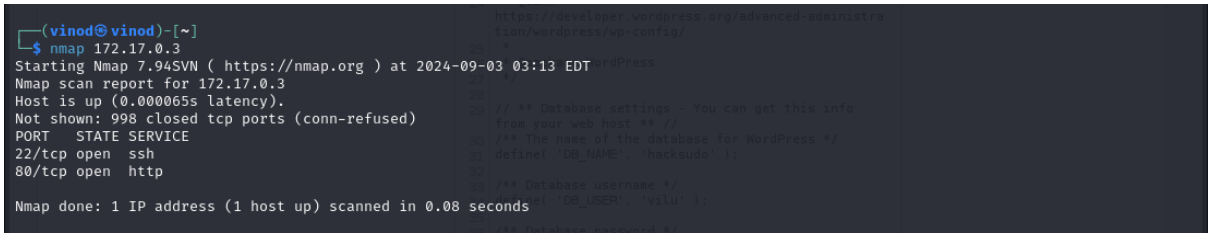
Ifconfig:- Shows network interfaces

```
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:fec7:5b83  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
```

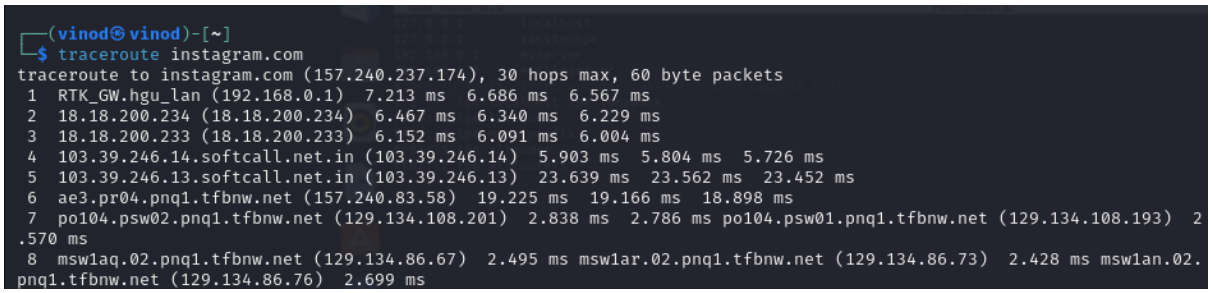
Iwconfig:- Shows wireless info



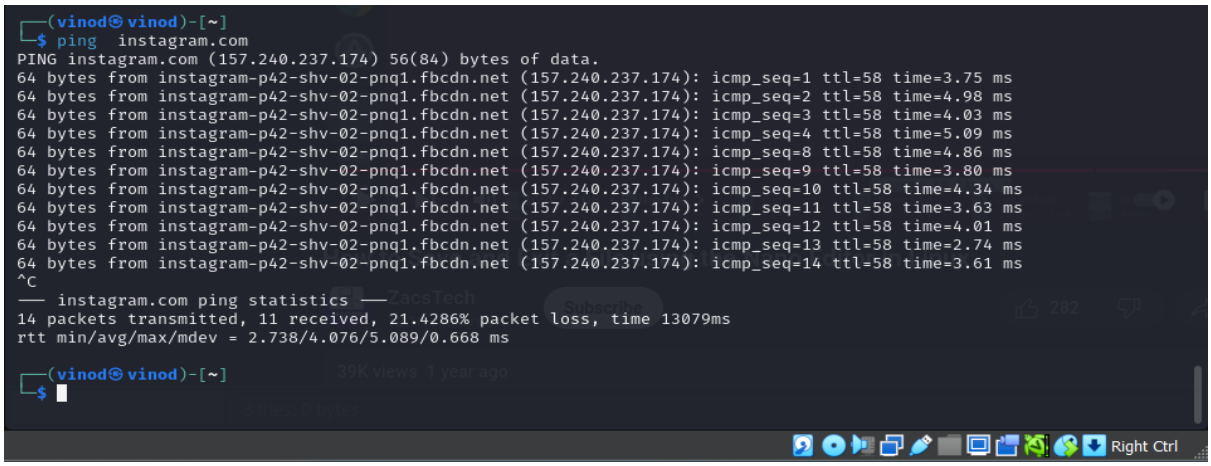
Nmap:- nmap (Network Mapper) is a network scanning and security auditing tool used to discover hosts, open ports, services, and vulnerabilities on a network.



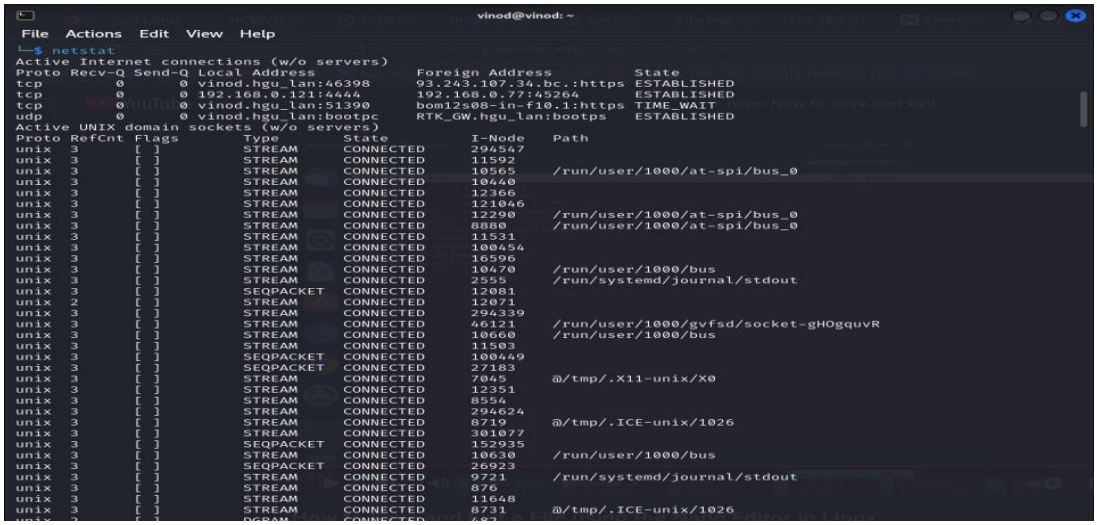
Traceroute:- trace route to host



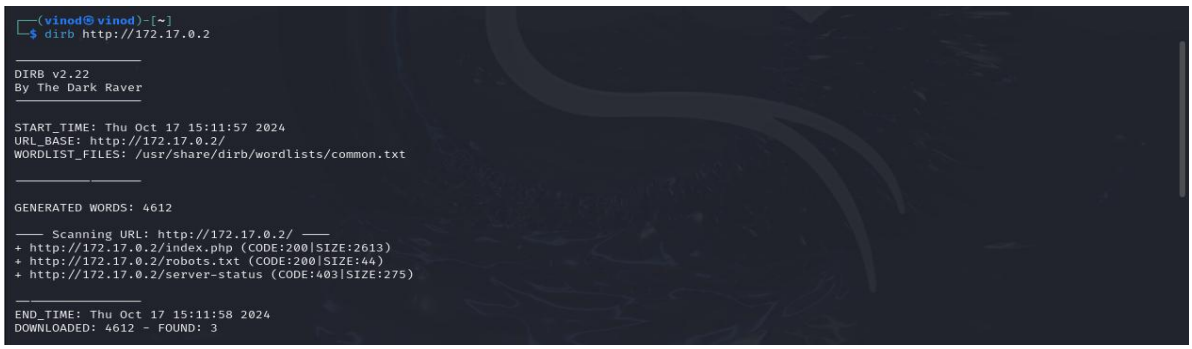
Ping:- test a network connection



Netstat:- networking information

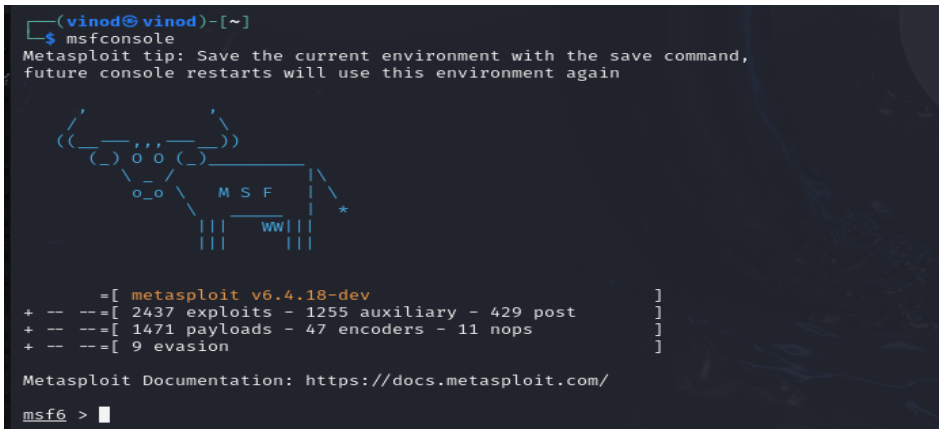


Dirb:- dirb is a web content scanning tool used in penetration testing to brute-force hidden directories and files on a web server using a wordlist.

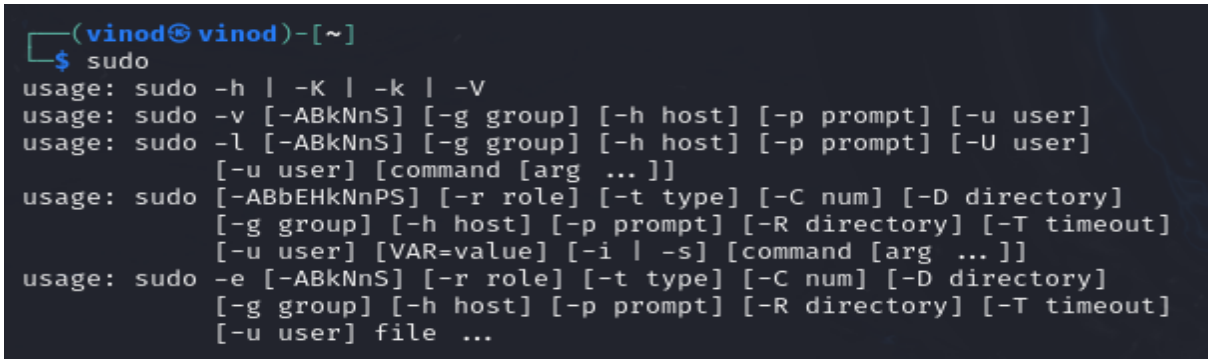


sudo sudo docker ps:- docker ps is a Docker command used to list all currently running containers on the system.

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.



Sudo:- Runs commands as admin



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