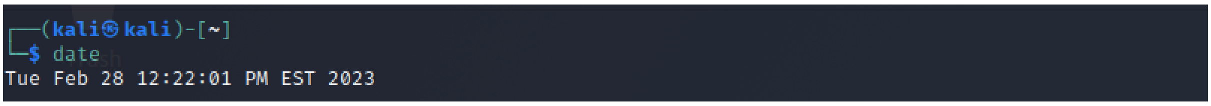
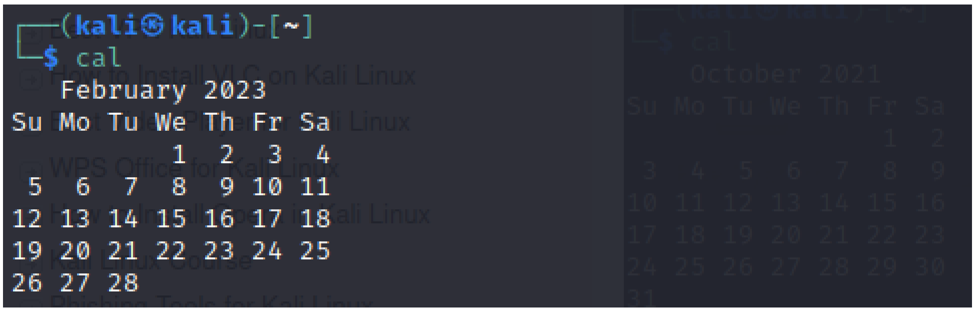
BASIC LINUX COMMANDS:

date - command is used to display the system date and time



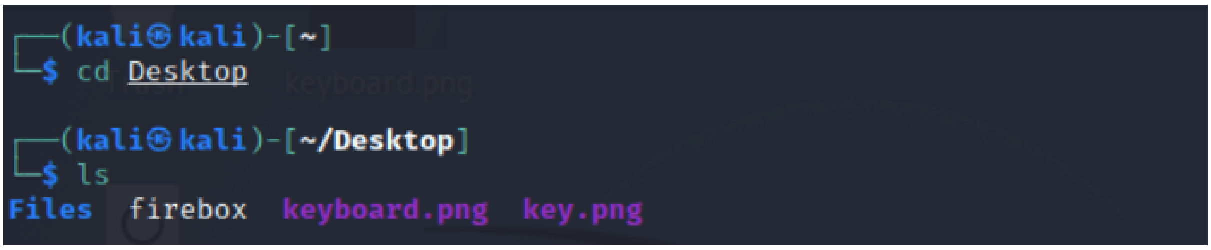
```
┌──(kali㉿kali)-[~]
└─$ date
Tue Feb 28 12:22:01 PM EST 2023
```

cal - command displays the current month's formatted calendar on our terminal screen



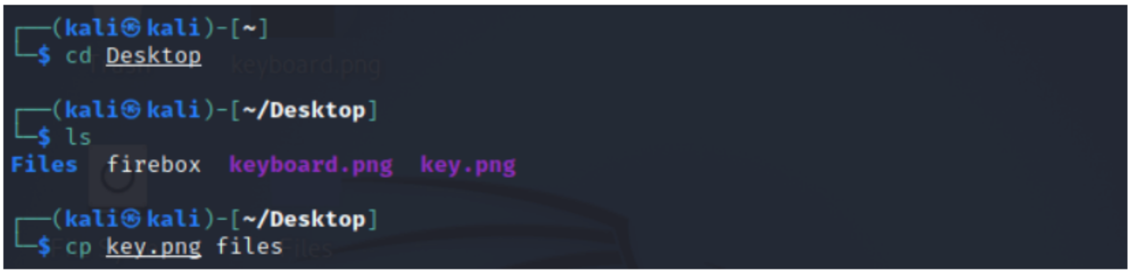
```
┌──(kali㉿kali)-[~]
└─$ cal
   February 2023
Su Mo Tu We Th Fr Sa
          1  2  3  4
 5  6  7  8  9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28
```

cd - command is also called **chdir** (Change Directory). We used this command to **change** or **switch** the current working directory.



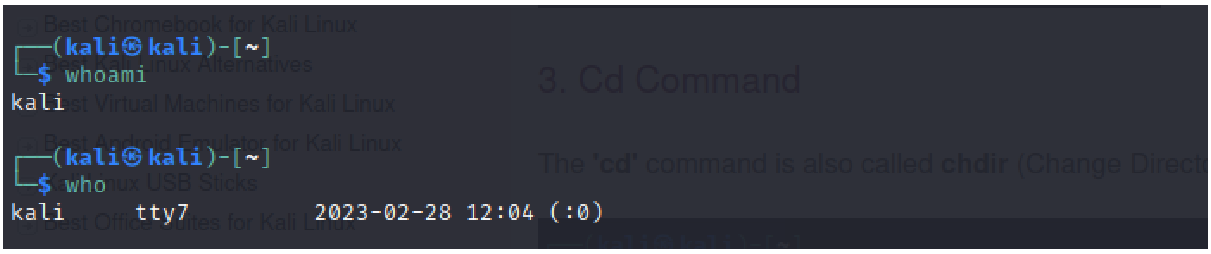
```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
Files  firebox  keyboard.png  key.png
```

cp - command is used to **copy** files or a group of files or directories that create an exact image of a file on a disk with a different file name.



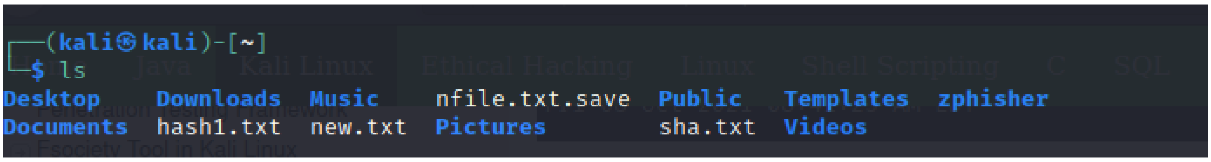
```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
Files  firebox  keyboard.png  key.png

┌──(kali㉿kali)-[~/Desktop]
└─$ cp key.png files
```

whoami - command is used to print the effective **user ID** whereas the **who** command prints information regarding users who are presently logged in



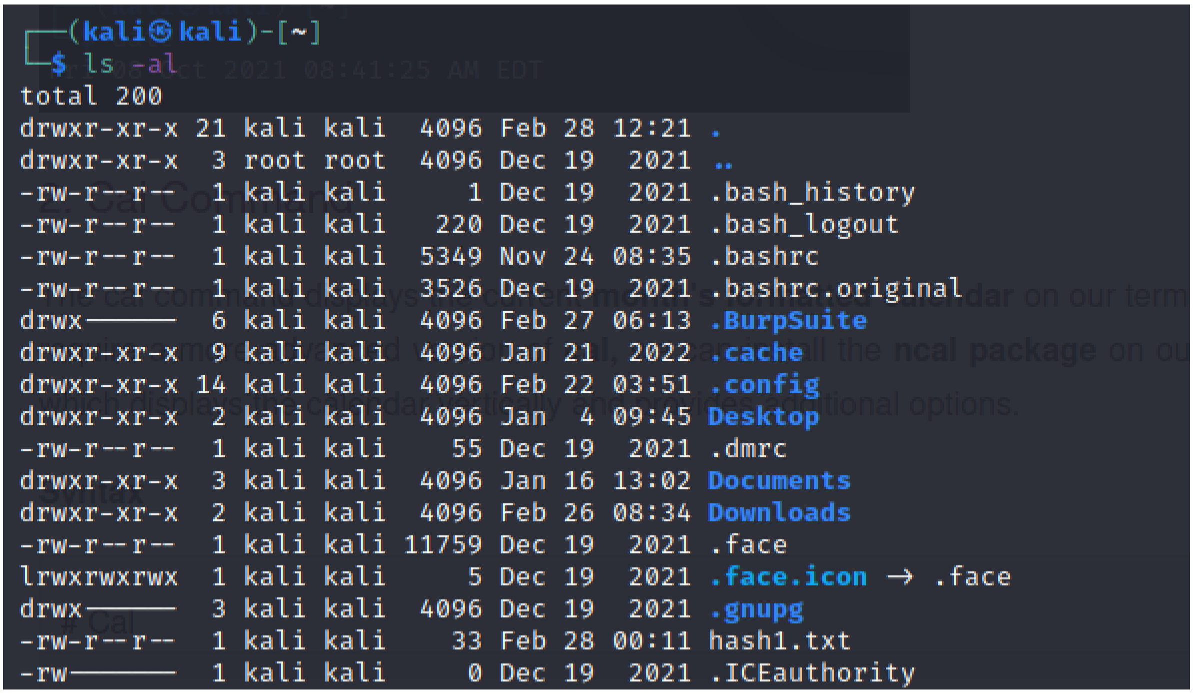
```
┌──(kali㉿kali)-[~]
└─$ whoami
kali

┌──(kali㉿kali)-[~]
└─$ who
kali     tty7         2023-02-28 12:04 (:0)
```

ls - command lists the directory contents of files and directories



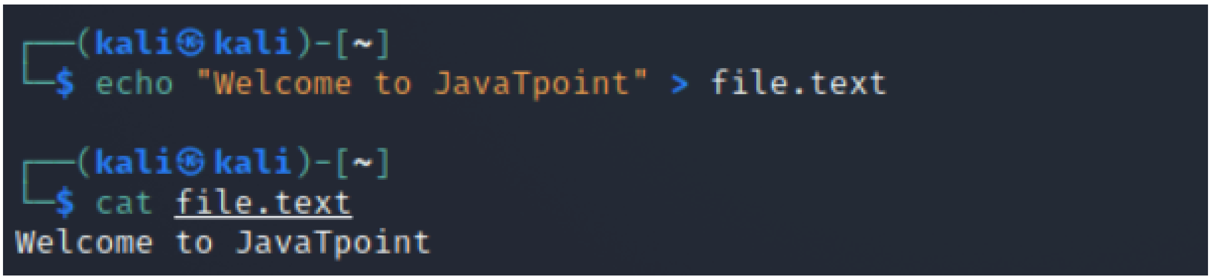
```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  Music    nfile.txt.save  Public   Templates  zphisher
Documents  hash1.txt  new.txt  Pictures        sha.txt  Videos
```

ls -al



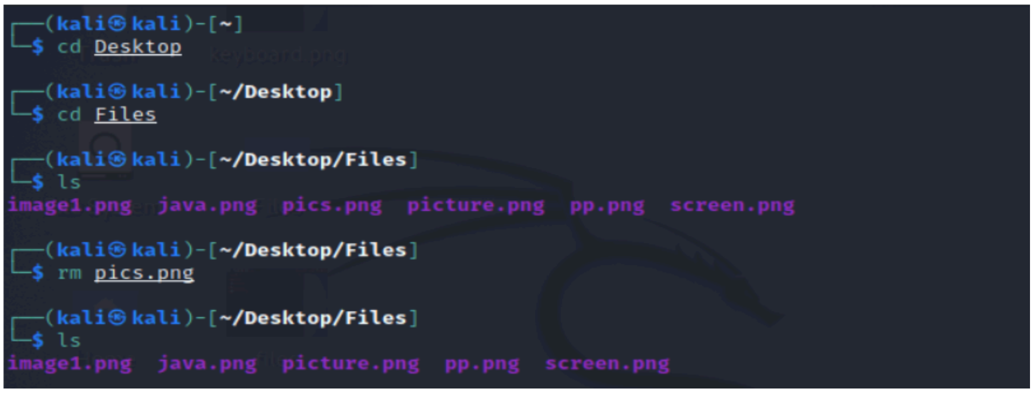
```
┌──(kali㉿kali)-[~]
└─$ ls -al
total 200
drwxr-xr-x 21 kali kali  4096 Feb 28 12:21 .
drwxr-xr-x  3 root root  4096 Dec 19  2021 ..
-rw-r--r--  1 kali kali     1 Dec 19  2021 .bash_history
-rw-r--r--  1 kali kali   220 Dec 19  2021 .bash_logout
-rw-r--r--  1 kali kali  5349 Nov 24 08:35 .bashrc
-rw-r--r--  1 kali kali  3526 Dec 19  2021 .bashrc.original
drwx------  6 kali kali  4096 Feb 27 06:13 .BurpSuite
drwxr-xr-x  9 kali kali  4096 Jan 21  2022 .cache
drwxr-xr-x 14 kali kali  4096 Feb 22 03:51 .config
drwxr-xr-x  2 kali kali  4096 Jan  4 09:45 Desktop
-rw-r--r--  1 kali kali    55 Dec 19  2021 .dmrc
drwxr-xr-x  3 kali kali  4096 Jan 16 13:02 Documents
drwxr-xr-x  2 kali kali  4096 Feb 26 08:34 Downloads
-rw-r--r--  1 kali kali 11759 Dec 19  2021 .face
lrwxrwxrwx  1 kali kali     5 Dec 19  2021 .face.icon → .face
drwx------  3 kali kali  4096 Dec 19  2021 .gnupg
-rw-r--r--  1 kali kali    33 Feb 28 00:11 hash1.txt
-rw-------  1 kali kali     0 Dec 19  2021 .ICEauthority
```

cat - (concatenate) command is used to permitting us to create single or many files, concatenate files and redirect, view contain of file output in terminal or files



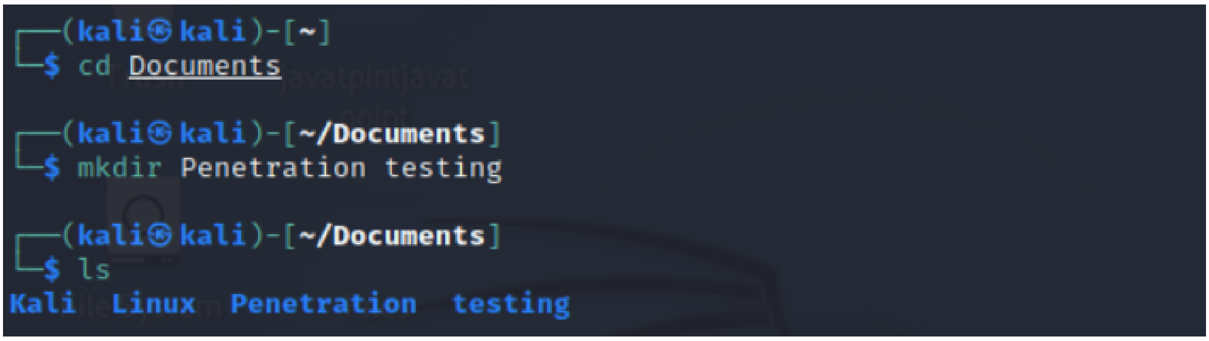
```
┌──(kali㉿kali)-[~]
└─$ echo "Welcome to JavaTpoint" > file.text

┌──(kali㉿kali)-[~]
└─$ cat file.text
Welcome to JavaTpoint
```

rm - command is used to **delete files**



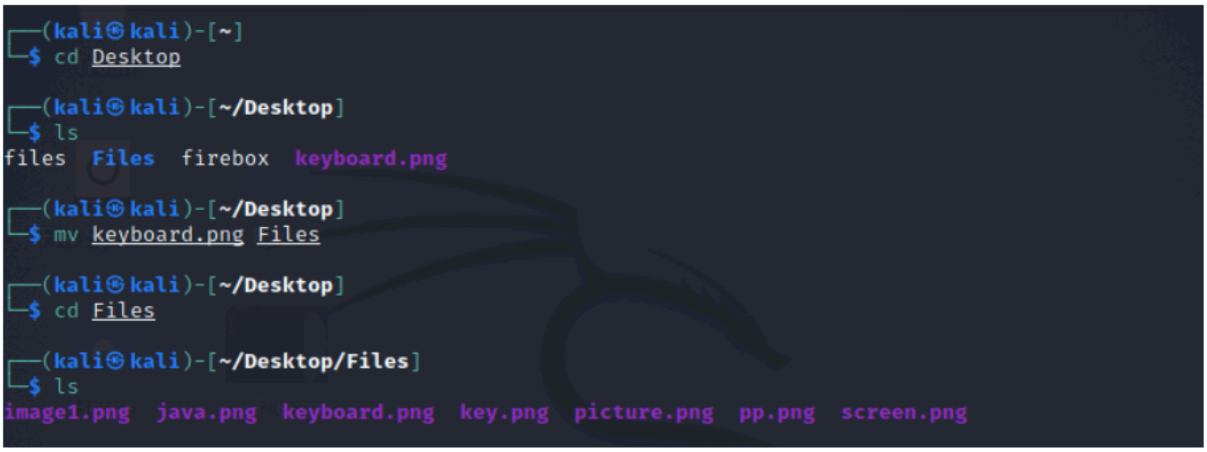
```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Files

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ ls
image1.png  java.png  pics.png  picture.png  pp.png  screen.png

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ rm pics.png

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ ls
image1.png  java.png  picture.png  pp.png  screen.png
```

mkdir – command used to create the directory



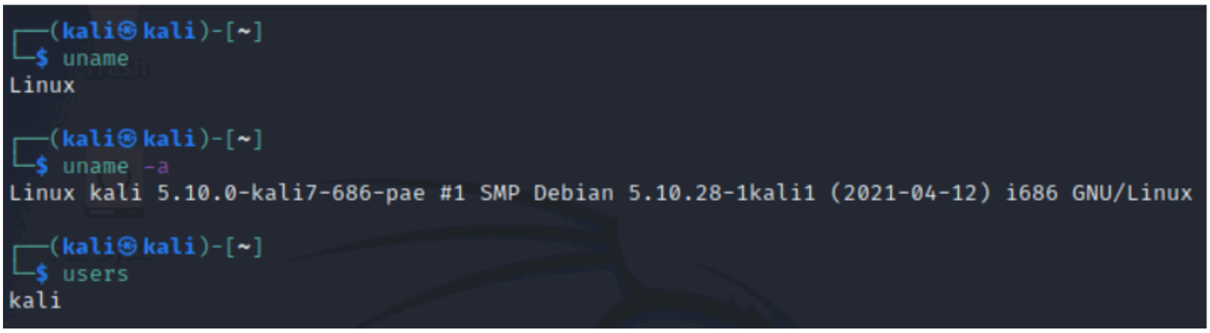
```
┌──(kali㉿kali)-[~]
└─$ cd Documents

┌──(kali㉿kali)-[~/Documents]
└─$ mkdir Penetration testing

┌──(kali㉿kali)-[~/Documents]
└─$ ls
Kali  Linux  Penetration  testing
```

mv - command, we can **move** files and directories on our file system.



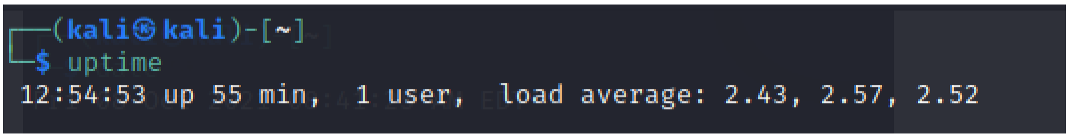
```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
files  Files  firebox  keyboard.png

┌──(kali㉿kali)-[~/Desktop]
└─$ mv keyboard.png Files

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Files

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ ls
image1.png  java.png  keyboard.png  key.png  picture.png  pp.png  screen.png
```

uname - command displays the **current system's information.** We can view system information about our Linux environment with the uname command in Linux. With the **uname -a command,** we can learn more about our system, including **Kernel Name, Node Name, Kernel Release, Kernel Version, Hardware Platform, Processor,** and **Operating System.**



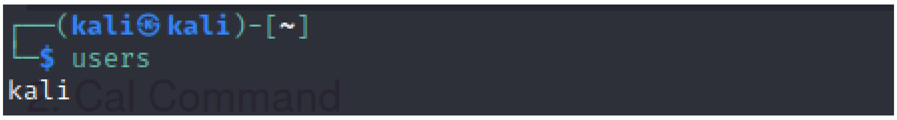
```
┌──(kali㉿kali)-[~]
└─$ uname
Linux

┌──(kali㉿kali)-[~]
└─$ uname -a
Linux kali 5.10.0-kali7-686-pae #1 SMP Debian 5.10.28-1kali1 (2021-04-12) i686 GNU/Linux

┌──(kali㉿kali)-[~]
└─$ users
kali
```

uptime - command displays the amount of time the system has been running.



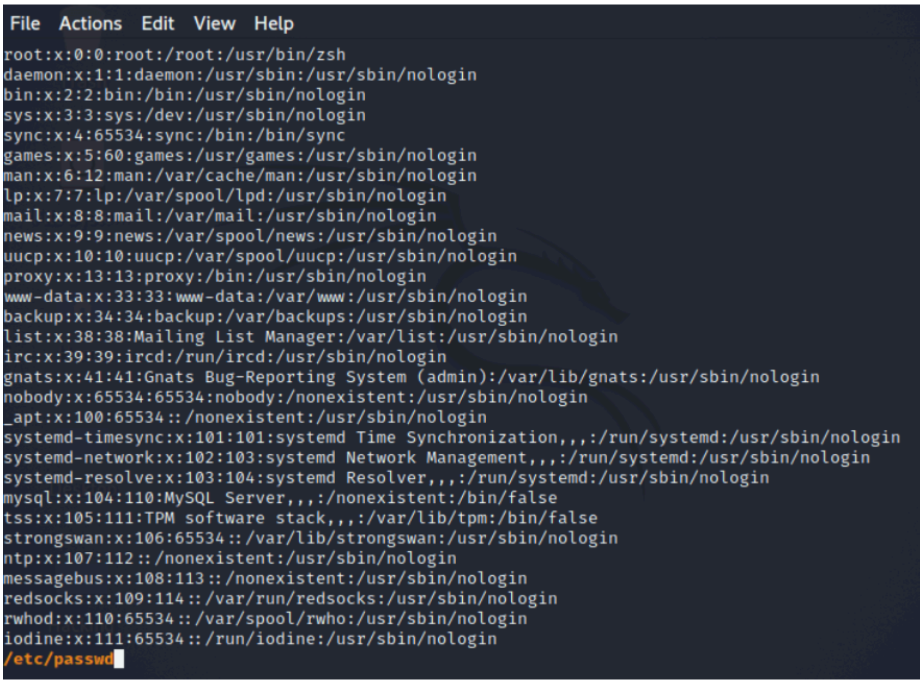
```
┌──(kali㉿kali)-[~]
└─$ uptime
 12:54:53 up 55 min,  1 user,  load average: 2.43, 2.57, 2.52
```

users - command is used to display the **login names** of users logged in on the system.



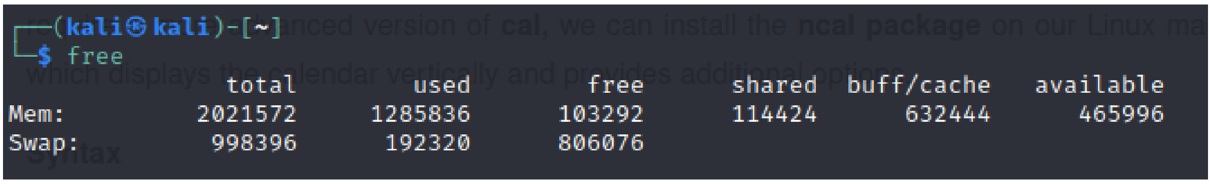
```
┌──(kali㉿kali)-[~]
└─$ users
kali
```

less - command is used to view files instead of opening the file. The less command is a more powerful variant of the "**more**" command which is used to show information one page at a time to the terminal. Ex: # less /etc/passwd



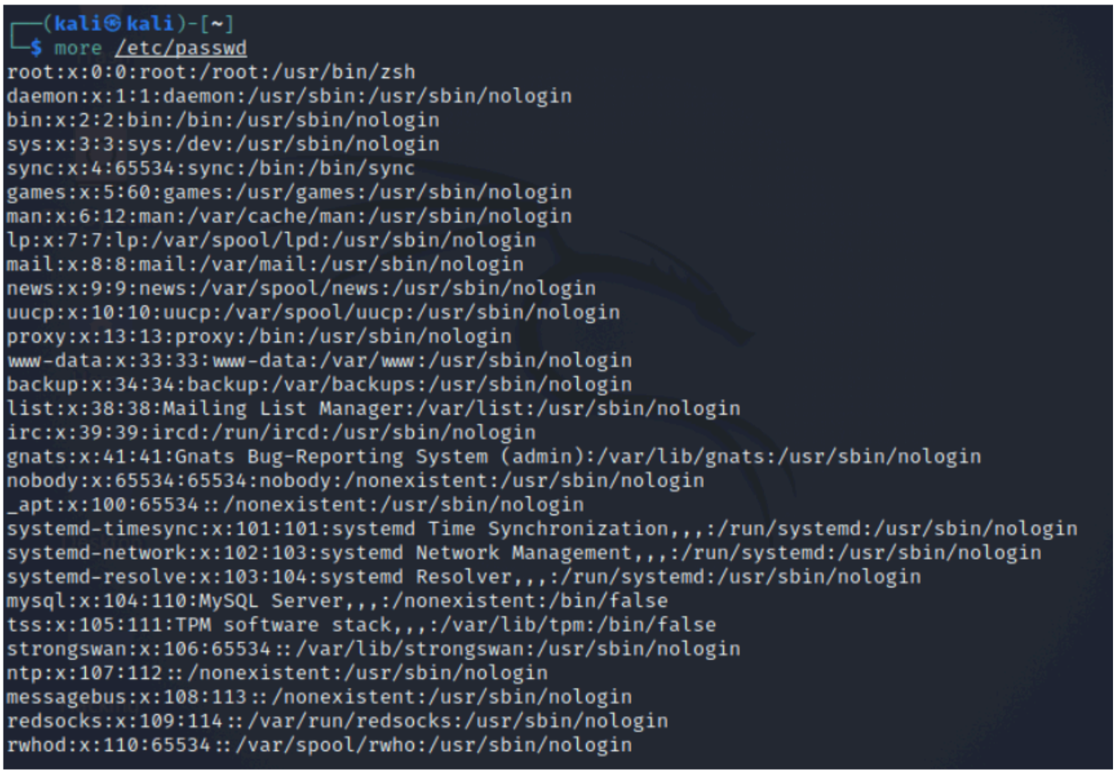
```
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
messagebus:x:108:113::/nonexistent:/usr/sbin/nologin
redsocks:x:109:114::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:111:65534::/run/iodine:/usr/sbin/nologin
/etc/passwd
```

free - command provides us the useful information about the **amount of RAM** available on a Linux machine. It also displays the entire amount of **physical memory** used and available space, as well as **swap memory** with **kernel buffers.**



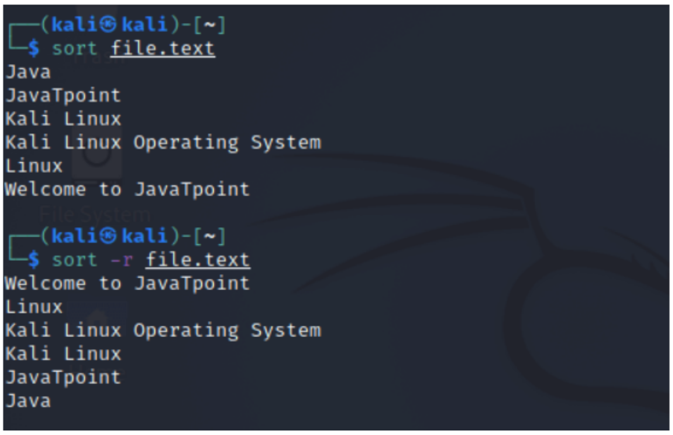
```
┌──(kali㉿kali)-[~]
└─$ free
               total        used        free      shared  buff/cache   available
Mem:         2021572     1285836      103292      114424      632444      465996
Swap:         998396      192320      806076
```

more - command permits us to show output in the terminal one page at a time. This is particularly beneficial when using a command that requires a lot of scrolling



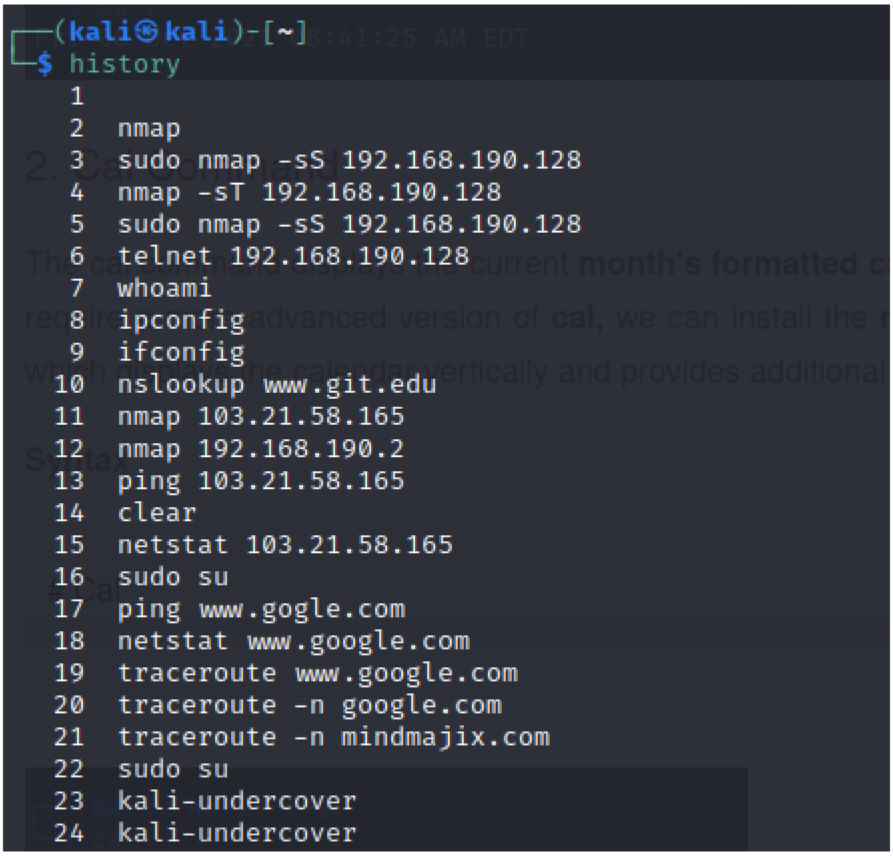
```
┌──(kali㉿kali)-[~]
└─$ more /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
messagebus:x:108:113::/nonexistent:/usr/sbin/nologin
redsocks:x:109:114::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
```

sort -command, we can sort the content of the text file, line by line



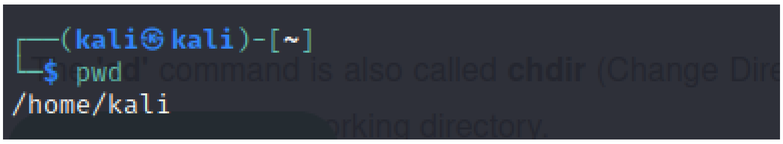
```
┌──(kali㉿kali)-[~]
└─$ sort file.text
Java
JavaTpoint
Kali Linux
Kali Linux Operating System
Linux
Welcome to JavaTpoint

┌──(kali㉿kali)-[~]
└─$ sort -r file.text
Welcome to JavaTpoint
Linux
Kali Linux Operating System
Kali Linux
JavaTpoint
Java
```

history - command print the **current user's bash history**



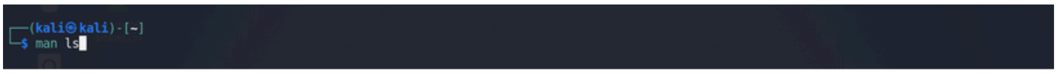
```
┌──(kali㉿kali)-[~]
└─$ history
    1
    2  nmap
    3  sudo nmap -sS 192.168.190.128
    4  nmap -sT 192.168.190.128
    5  sudo nmap -sS 192.168.190.128
    6  telnet 192.168.190.128
    7  whoami
    8  ipconfig
    9  ifconfig
   10  nslookup www.git.edu
   11  nmap 103.21.58.165
   12  nmap 192.168.190.2
   13  ping 103.21.58.165
   14  clear
   15  netstat 103.21.58.165
   16  sudo su
   17  ping www.gogle.com
   18  netstat www.google.com
   19  traceroute www.google.com
   20  traceroute -n google.com
   21  traceroute -n mindmajix.com
   22  sudo su
   23  kali-undercover
   24  kali-undercover
```

pwd – command is used to **print working directory.**

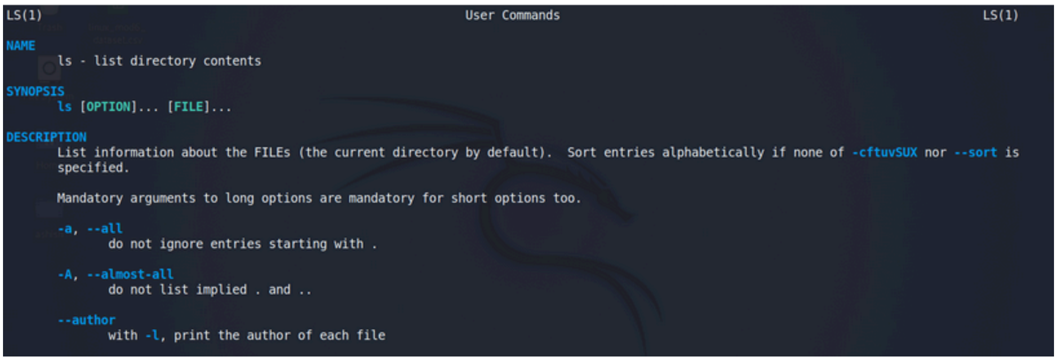


```
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali
```

man -It displays the user manual for all commands in Kali Linux. It includes Bash command and detailed synopsis with a short description.

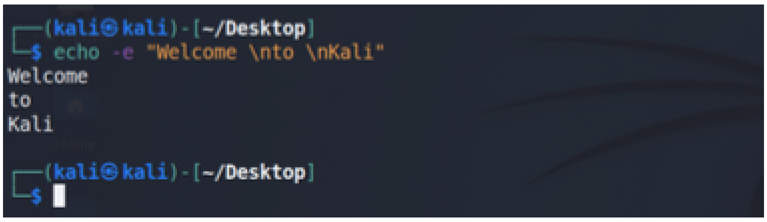


```
┌──(kali㉿kali)-[~]
└─$ man ls
```



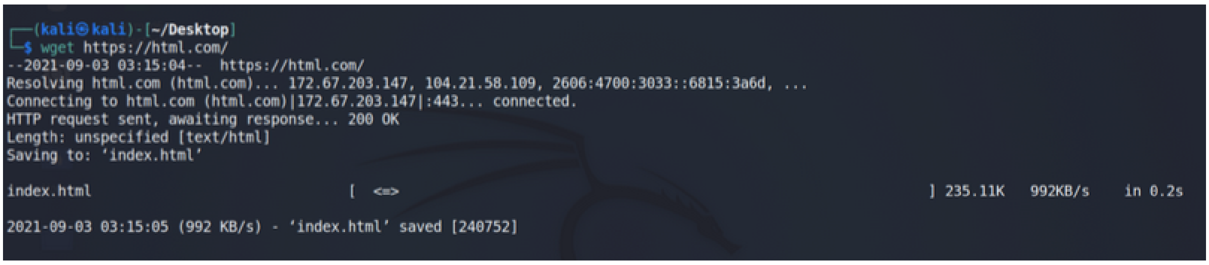
```
LS(1)                                   User Commands                                   LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List information about the FILEs (the current directory by default).  Sort entries alphabetically if none of -cftuvSUX nor --sort is
       specified.

       Mandatory arguments to long options are mandatory for short options too.

       -a, --all
              do not ignore entries starting with .

       -A, --almost-all
              do not list implied . and ..

       --author
              with -l, print the author of each file
```

echo – This command displays any text as arguments. It is used for debugging shell programs.



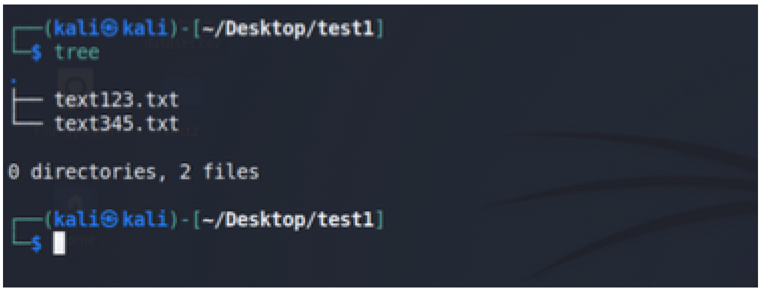
```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo -e "Welcome \nto \nKali"
Welcome
to
Kali

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

wget - This command downloads applications and web pages directly from the web.



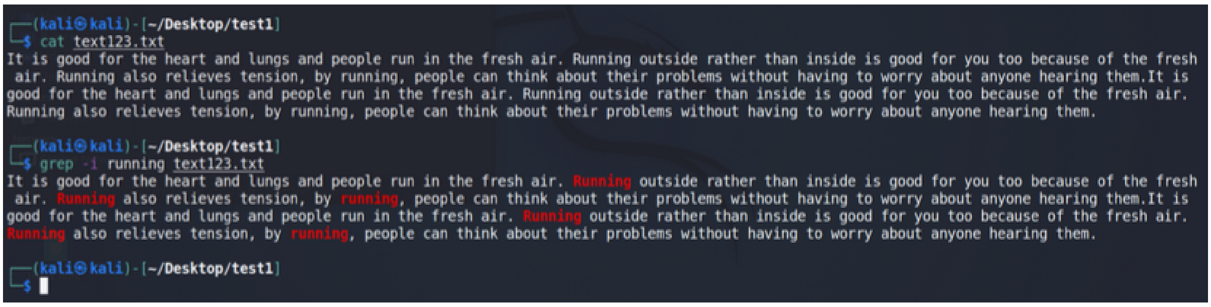
```
┌──(kali㉿kali)-[~/Desktop]
└─$ wget https://html.com/
--2021-09-03 03:15:04--  https://html.com/
Resolving html.com (html.com)... 172.67.203.147, 104.21.58.109, 2606:4700:3033::6815:3a6d, ...
Connecting to html.com (html.com)|172.67.203.147|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html’

index.html                     [  <=>                                                    ] 235.11K   992KB/s    in 0.2s

2021-09-03 03:15:05 (992 KB/s) - ‘index.html’ saved [240752]
```

tree -This command shows the list of contents from a director in the tree fashion



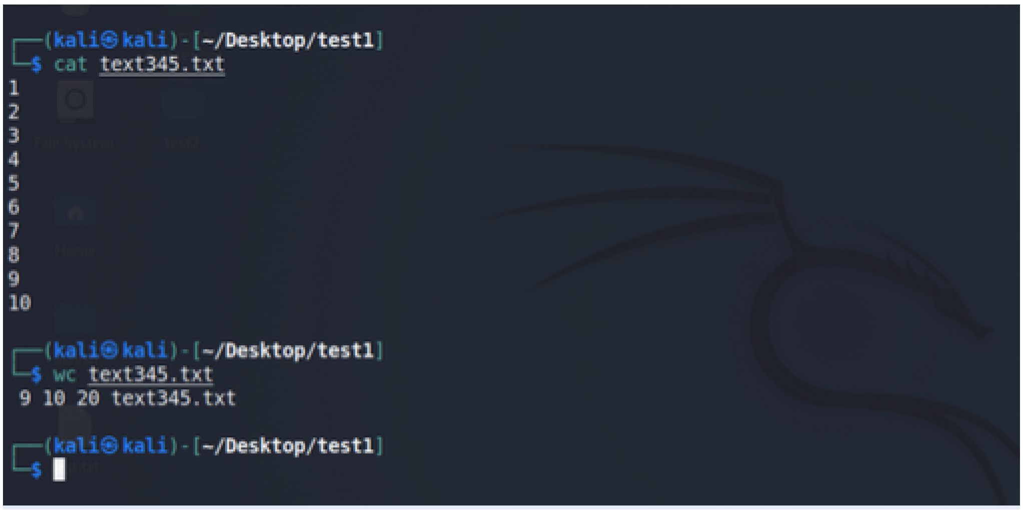
```
┌──(kali㉿kali)-[~/Desktop/test1]
└─$ tree
.
├── text123.txt
└── text345.txt

0 directories, 2 files

┌──(kali㉿kali)-[~/Desktop/test1]
└─$ 
```

grep - This command searches files and prints lines that match patterns.



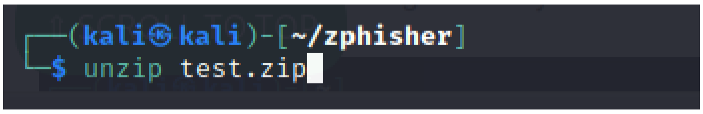
```
┌──(kali㉿kali)-[~/Desktop/test1]
└─$ cat text123.txt
It is good for the heart and lungs and people run in the fresh air. Running outside rather than inside is good for you too because of the fresh
 air. Running also relieves tension, by running, people can think about their problems without having to worry about anyone hearing them.It is
good for the heart and lungs and people run in the fresh air. Running outside rather than inside is good for you too because of the fresh air.
Running also relieves tension, by running, people can think about their problems without having to worry about anyone hearing them.

┌──(kali㉿kali)-[~/Desktop/test1]
└─$ grep -i running text123.txt
It is good for the heart and lungs and people run in the fresh air. Running outside rather than inside is good for you too because of the fresh
 air. Running also relieves tension, by running, people can think about their problems without having to worry about anyone hearing them.It is
good for the heart and lungs and people run in the fresh air. Running outside rather than inside is good for you too because of the fresh air.
Running also relieves tension, by running, people can think about their problems without having to worry about anyone hearing them.

┌──(kali㉿kali)-[~/Desktop/test1]
└─$ 
```

wc - wc stands for word count. It shows the number of lines, words, characters, and bytes.



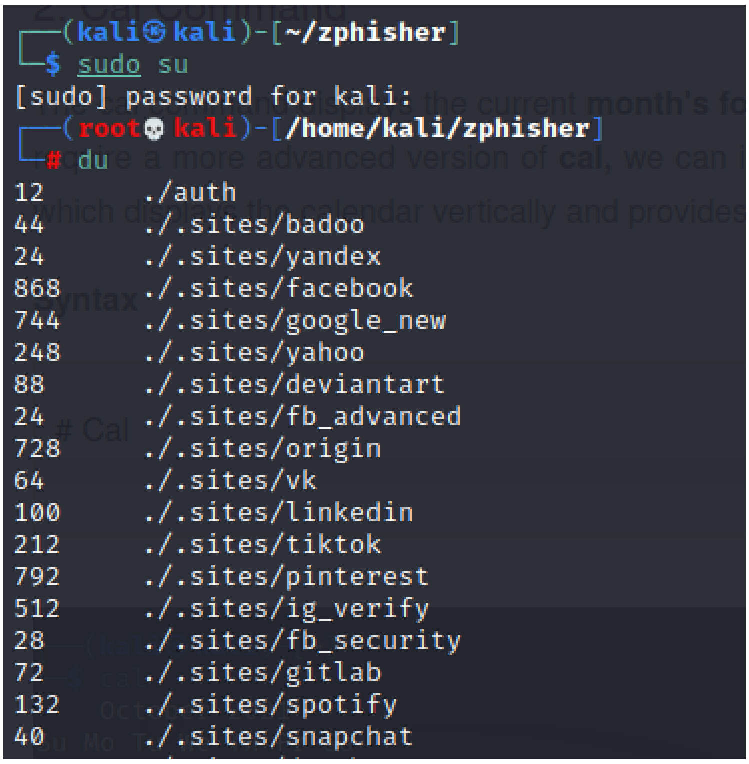
```
┌──(kali㉿kali)-[~/Desktop/test1]
└─$ cat text345.txt
1
2
3
4
5
6
7
8
9
10

┌──(kali㉿kali)-[~/Desktop/test1]
└─$ wc text345.txt
 9 10 20 text345.txt

┌──(kali㉿kali)-[~/Desktop/test1]
└─$ 
```

unzip - Command used to extract the files from zip file



```
┌──(kali㉿kali)-[~/zphisher]
└─$ unzip test.zip
```

du - The du command is used to display the amount of disk space used by files and directories.

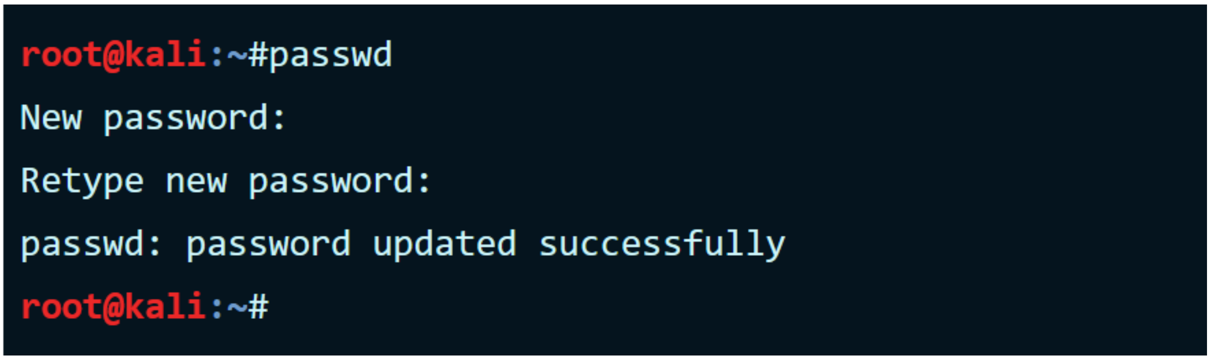


```
┌──(kali㉿kali)-[~/zphisher]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali/zphisher]
└─# du
12      ./auth
44      ./.sites/badoo
24      ./.sites/yandex
868     ./.sites/facebook
744     ./.sites/google_new
248     ./.sites/yahoo
88      ./.sites/deviantart
24      ./.sites/fb_advanced
728     ./.sites/origin
64      ./.sites/vk
100     ./.sites/linkedin
212     ./.sites/tiktok
792     ./.sites/pinterest
512     ./.sites/ig_verify
28      ./.sites/fb_security
72      ./.sites/gitlab
132     ./.sites/spotify
40      ./.sites/snapchat
```

adduser -

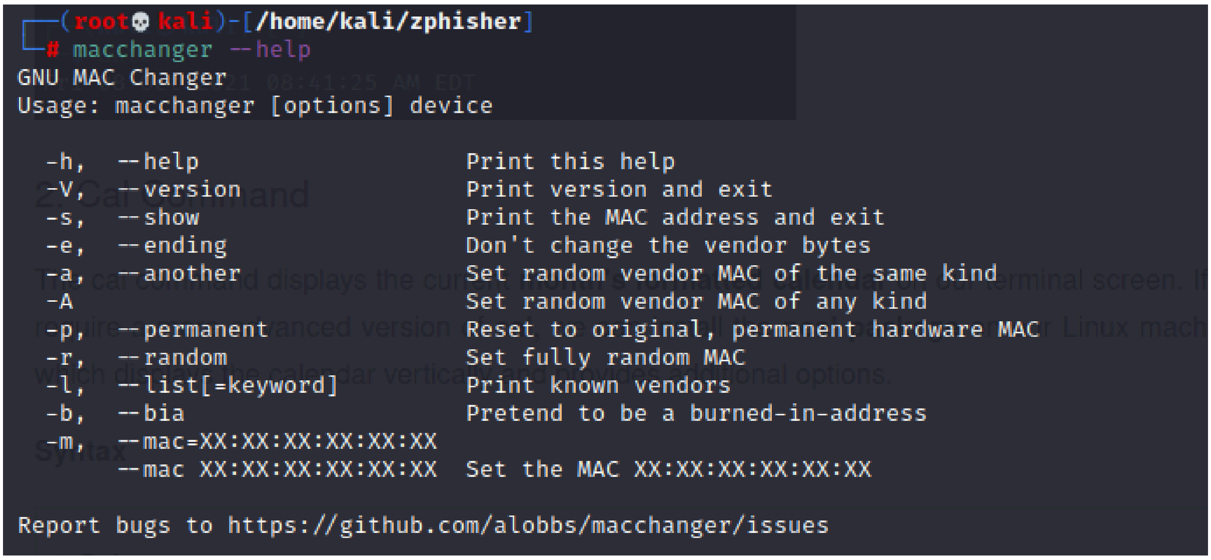
Adduser command is used to add a new user. You can create multiple users by using adduser command.

passwd - command To change password



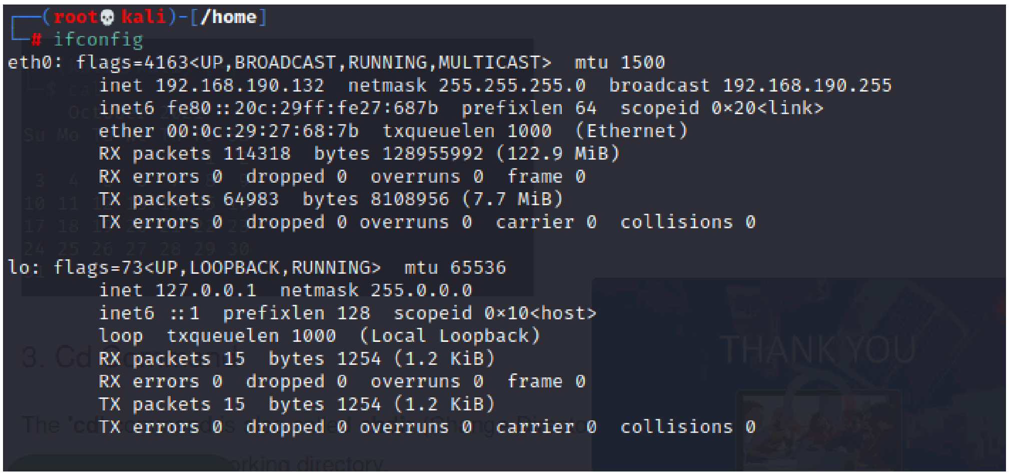
```
root@kali:~#passwd
New password:
Retype new password:
passwd: password updated successfully
root@kali:~#
```

macchanger - macchanger changes your mac address, essentially changing your identity. It helps with protecting your anonymity on the internet, making your IP untraceable.



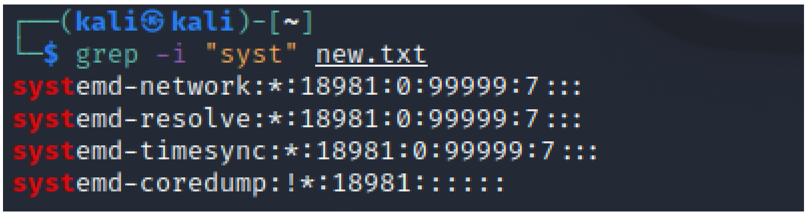
```
┌──(root💀kali)-[/home/kali/zphisher]
└─# macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

  -h,  --help                     Print this help
  -V,  --version                  Print version and exit
  -s,  --show                     Print the MAC address and exit
  -e,  --ending                   Don't change the vendor bytes
  -a,  --another                  Set random vendor MAC of the same kind
  -A                              Set random vendor MAC of any kind
  -p,  --permanent                Reset to original, permanent hardware MAC
  -r,  --random                   Set fully random MAC
  -l,  --list[=keyword]           Print known vendors
  -b,  --bia                      Pretend to be a burned-in-address
  -m,  --mac=XX:XX:XX:XX:XX:XX
       --mac XX:XX:XX:XX:XX:XX  Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
```

ifconfig - ifconfig <=> interface configuration. Used to detect the IP address



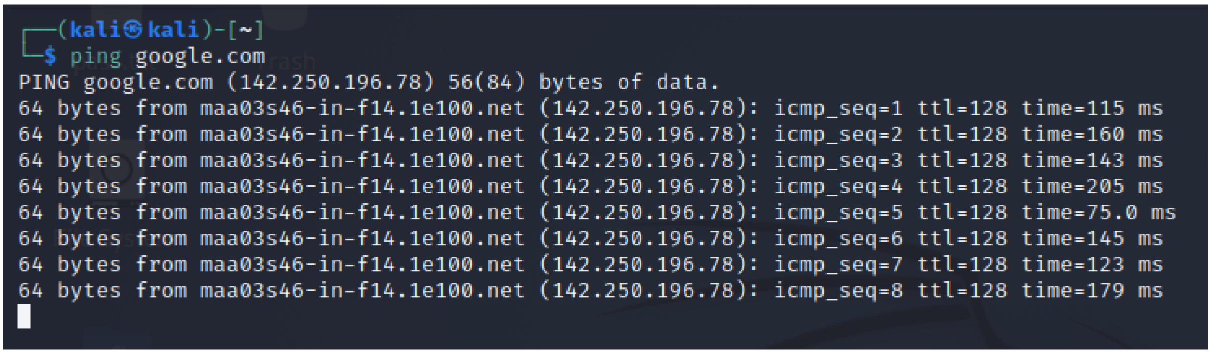
```
┌──(root💀kali)-[/home]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.190.132  netmask 255.255.255.0  broadcast 192.168.190.255
        inet6 fe80::20c:29ff:fe27:687b  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:27:68:7b  txqueuelen 1000  (Ethernet)
        RX packets 114318  bytes 128955992 (122.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 64983  bytes 8108956 (7.7 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 15  bytes 1254 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 1254 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

grep [options] pattern [files]
command used to search the pattern



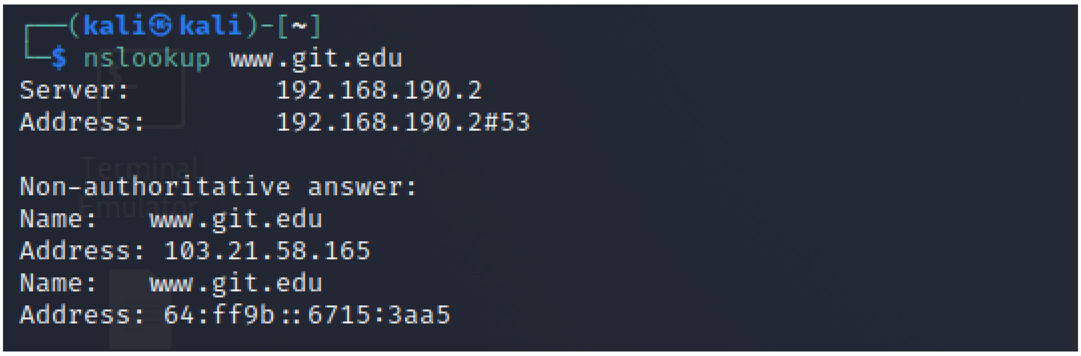
```
┌──(kali㉿kali)-[~]
└─$ grep -i "syst" new.txt
systemd-network:*:18981:0:99999:7:::
systemd-resolve:*:18981:0:99999:7:::
systemd-timesync:*:18981:0:99999:7:::
systemd-coredump:!*:18981::::::
```

ping – command used to troubleshoot devices present in the network



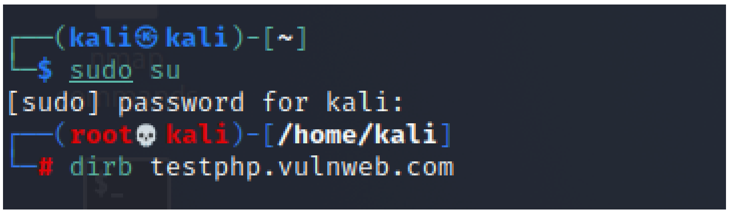
```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (142.250.196.78) 56(84) bytes of data.
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=1 ttl=128 time=115 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=2 ttl=128 time=160 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=3 ttl=128 time=143 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=4 ttl=128 time=205 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=5 ttl=128 time=75.0 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=6 ttl=128 time=145 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=7 ttl=128 time=123 ms
64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78): icmp_seq=8 ttl=128 time=179 ms
█
```

nslookup – command used to find the IP of url



```
┌──(kali㉿kali)-[~]
└─$ nslookup www.git.edu
Server:         192.168.190.2
Address:        192.168.190.2#53

Non-authoritative answer:
Name:   www.git.edu
Address: 103.21.58.165
Name:   www.git.edu
Address: 64:ff9b::6715:3aa5
```

durb – command used to find the directories of the target



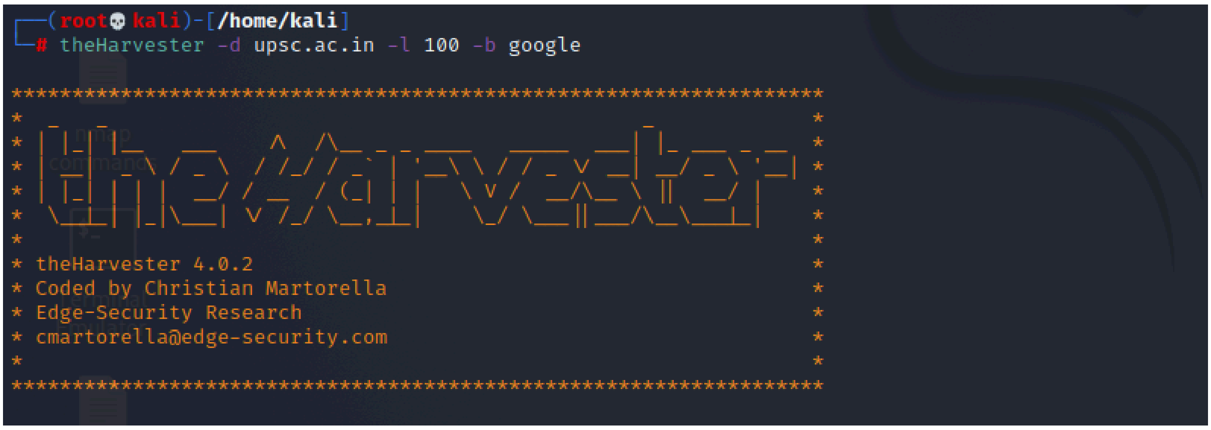
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# dirb testphp.vulnweb.com
```

theHarvester – command used to find the official email ids

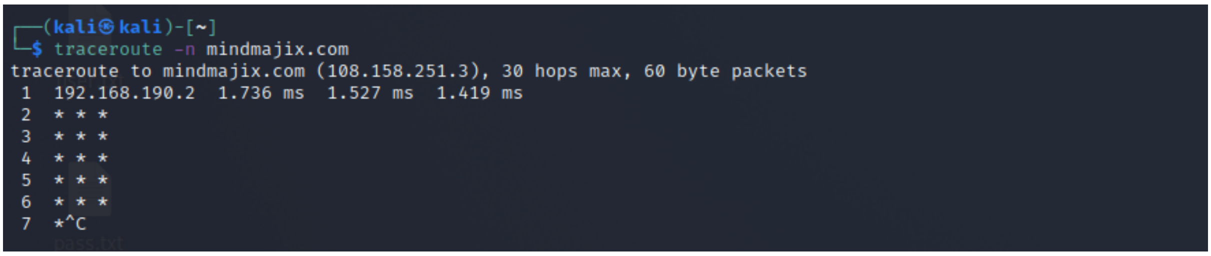
traceroute –It provides the names and identifies every device on the path.

1. It follows the route to the destination

2. It determines where the network latency comes from and reports it.

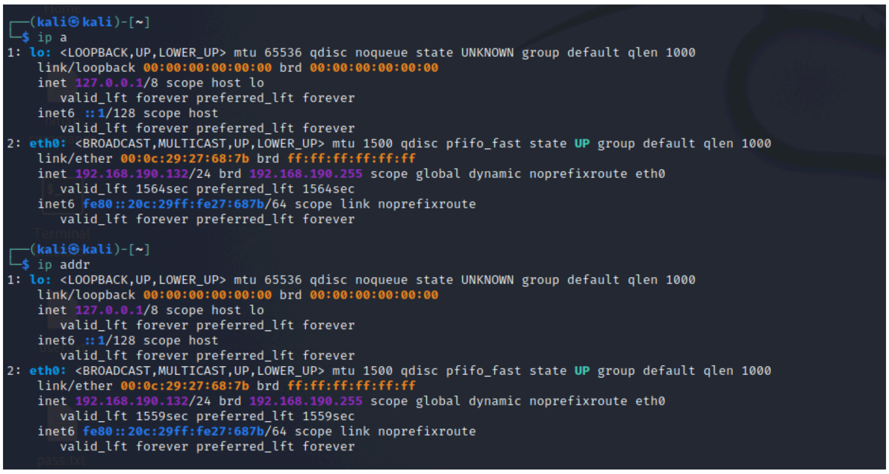


```
┌──(root💀 kali)-[/home/kali]
└─# theHarvester -d upsc.ac.in -l 100 -b google

*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.0.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
```



```
┌──(kali㉿kali)-[~]
└─$ traceroute -n mindmajix.com
traceroute to mindmajix.com (108.158.251.3), 30 hops max, 60 byte packets
 1  192.168.190.2  1.736 ms  1.527 ms  1.419 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  *^C
```

ip – This command gives the details of all networks like ifconfig.This command can also be used to get the details of a specific interface.



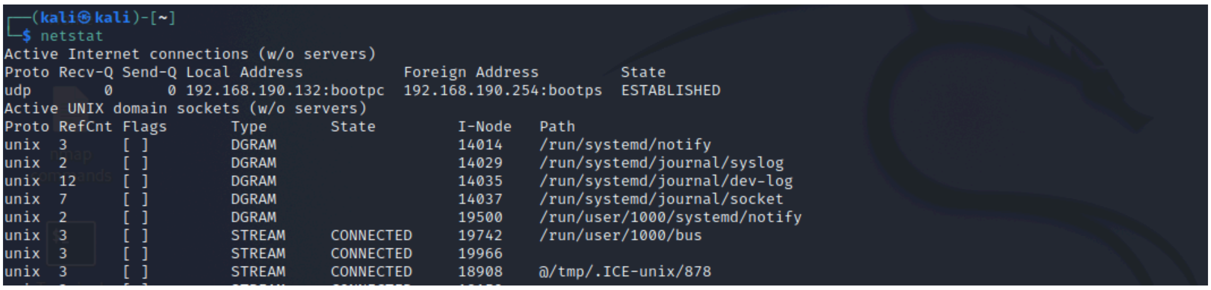
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:27:68:7b brd ff:ff:ff:ff:ff:ff
    inet 192.168.190.132/24 brd 192.168.190.255 scope global dynamic noprefixroute eth0
       valid_lft 1564sec preferred_lft 1564sec
    inet6 fe80::20c:29ff:fe27:687b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:27:68:7b brd ff:ff:ff:ff:ff:ff
    inet 192.168.190.132/24 brd 192.168.190.255 scope global dynamic noprefixroute eth0
       valid_lft 1559sec preferred_lft 1559sec
    inet6 fe80::20c:29ff:fe27:687b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

tracepath - Linux tracepath is similar to traceroute command. It is used to detect network delays. However, it doesn't require root privileges.

Syntax : tracepath mindmajix.com

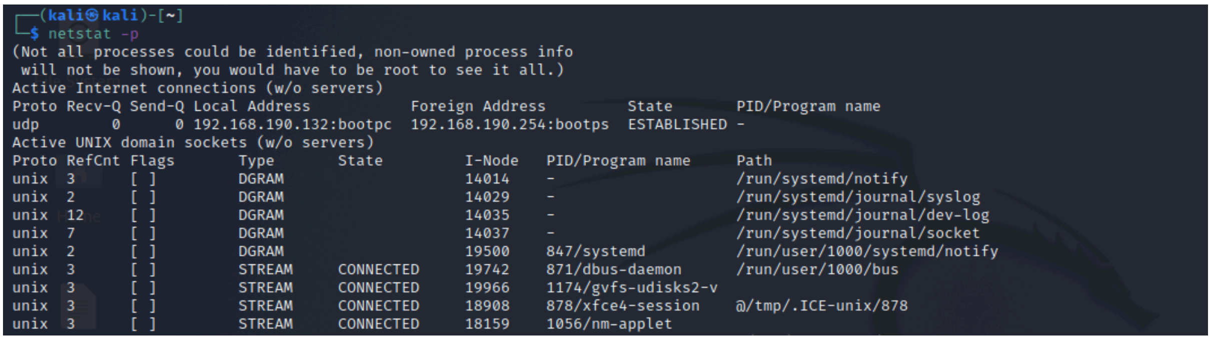
netstat - Linux netstat command refers to the network statistics.

It provides statistical figures about different interfaces which include open sockets, routing tables, and connection information.



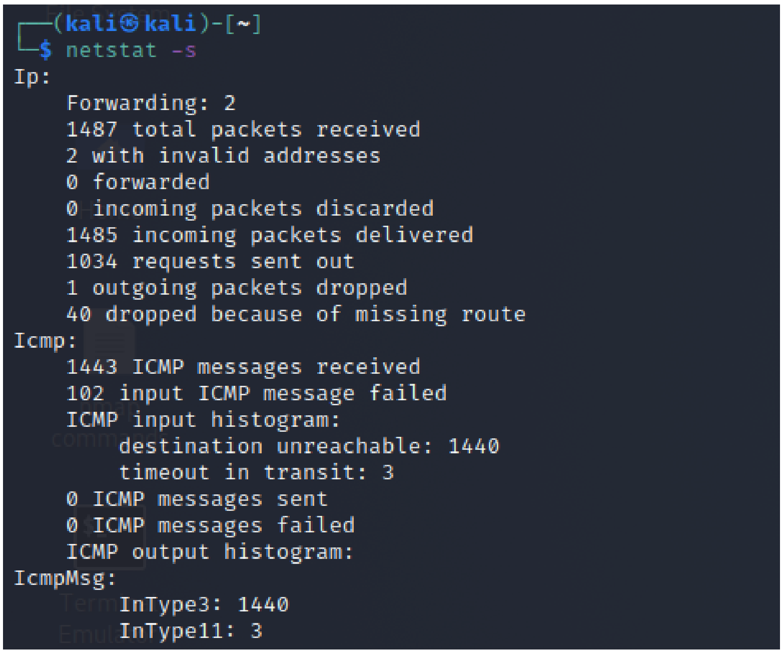
```
┌──(kali㉿kali)-[~]
└─$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.190.132:bootpc  192.168.190.254:bootps  ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         DGRAM                    14014    /run/systemd/notify
unix  2      [ ]         DGRAM                    14029    /run/systemd/journal/syslog
unix  12     [ ]         DGRAM                    14035    /run/systemd/journal/dev-log
unix  7      [ ]         DGRAM                    14037    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    19500    /run/user/1000/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     19742    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     19966
unix  3      [ ]         STREAM     CONNECTED     18908    @/tmp/.ICE-unix/878
```

This displays the programs associated with the open socket.



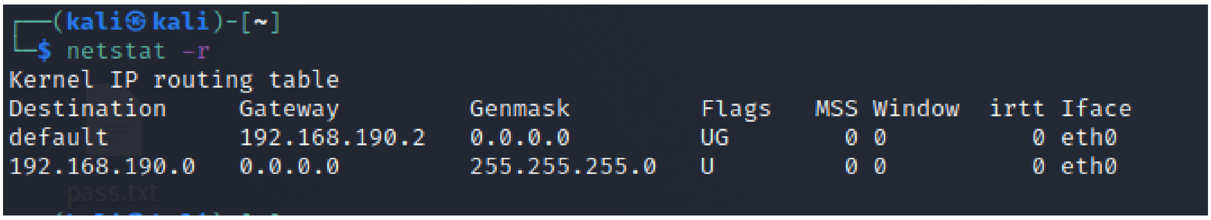
```
┌──(kali㉿kali)-[~]
└─$ netstat -p
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 192.168.190.132:bootpc  192.168.190.254:bootps  ESTABLISHED -
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  3      [ ]         DGRAM                    14014    -                    /run/systemd/notify
unix  2      [ ]         DGRAM                    14029    -                    /run/systemd/journal/syslog
unix  12     [ ]         DGRAM                    14035    -                    /run/systemd/journal/dev-log
unix  7      [ ]         DGRAM                    14037    -                    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    19500    847/systemd          /run/user/1000/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     19742    871/dbus-daemon      /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     19966    1174/gvfs-udisks2-v
unix  3      [ ]         STREAM     CONNECTED     18908    878/xfce4-session    @/tmp/.ICE-unix/878
unix  3      [ ]         STREAM     CONNECTED     18159    1056/nm-applet
```

This gives detailed statistics of all the ports.



```
┌──(kali㉿kali)-[~]
└─$ netstat -s
Ip:
    Forwarding: 2
    1487 total packets received
    2 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    1485 incoming packets delivered
    1034 requests sent out
    1 outgoing packets dropped
    40 dropped because of missing route
Icmp:
    1443 ICMP messages received
    102 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 1440
        timeout in transit: 3
    0 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
IcmpMsg:
        InType3: 1440
        InType11: 3
```

information related to the routing table.



```
┌──(kali㉿kali)-[~]
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.190.2   0.0.0.0         UG        0 0          0 eth0
192.168.190.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

ss –

This command gives information about all TCP, UDP, and UNIX socket connections.

You can use -t, -u, -x in the command respectively to show TCP/UDP or UNIX sockets. You can combine each of these with "a" to show the connected and listening sockets.

Syntax:

```
ss -ta
ss -ua
ss -xa
```

If you want to see only the listening sockets of TCP/UDP or UNIX sockets, combine it with "l"

Syntax:

```
ss -lt
ss -lu
ss -lx
```

- To get a list of all the established sockets of TCP for IPV4,

Command:

```
$ ss -t4 state established
```

- To get a list of all closed TCP sockets,

Command:

```
 $ ss -t4 state closed
```

- To get a list of all connected ports for a specific IP address:

dig -Linux dig command stands for Domain Information Groper. This command is used in DNS lookup to query the DNS name server. It is also used to troubleshoot DNS related issues.

It is mainly used to verify DNS mappings, MX Records, host addresses, and all other DNS records for a better understanding of the DNS topography.

Command:

```
 $ dig google.com MX
```

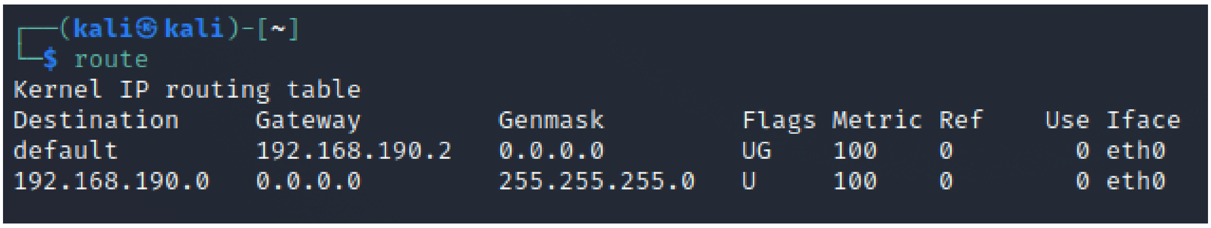
- To get all types of records at once, use the keyword ANY ass below:

Command:

```
 $ dig google.com ANY
```

route-

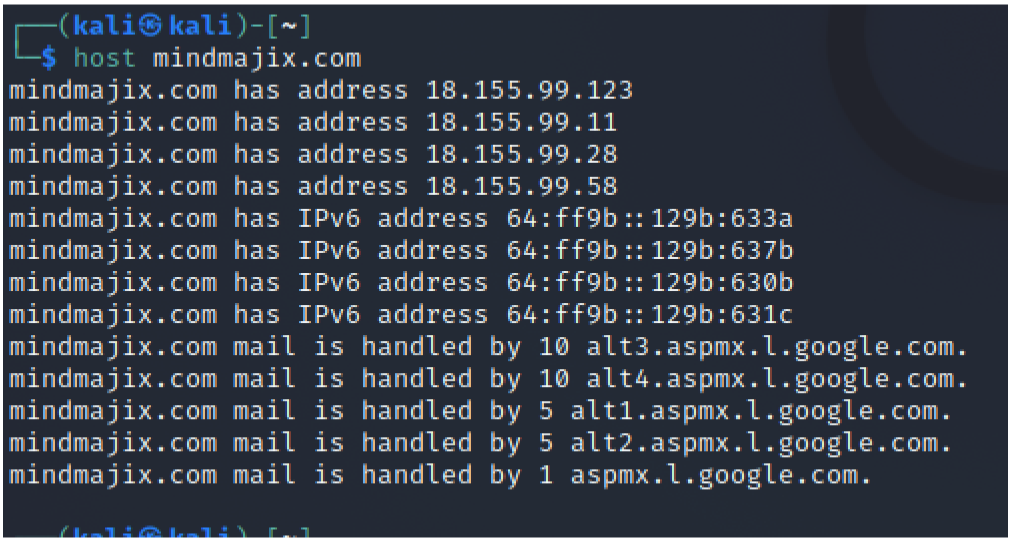
Linux route command displays and manipulates the routing table existing for your system.A router is basically used to find the best way to send the packets across to a destination



```
┌──(kali㉿kali)-[~]
└─$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.190.2   0.0.0.0         UG    100    0        0 eth0
192.168.190.0   0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

host –

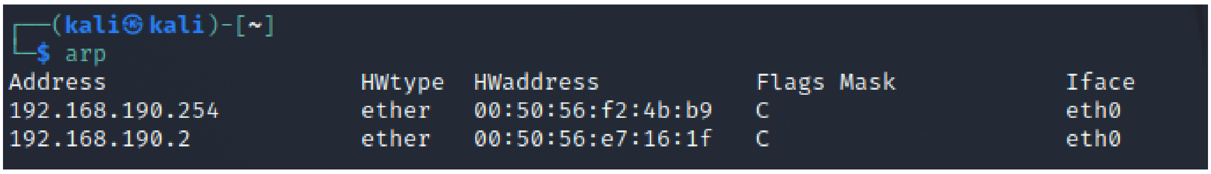
Linux host command displays the domain name for a given IP address and IP address for a given hostname. It is also used to fetch DNS lookup for DNS related query.



```
┌──(kali㉿kali)-[~]
└─$ host mindmajix.com
mindmajix.com has address 18.155.99.123
mindmajix.com has address 18.155.99.11
mindmajix.com has address 18.155.99.28
mindmajix.com has address 18.155.99.58
mindmajix.com has IPv6 address 64:ff9b::129b:633a
mindmajix.com has IPv6 address 64:ff9b::129b:637b
mindmajix.com has IPv6 address 64:ff9b::129b:630b
mindmajix.com has IPv6 address 64:ff9b::129b:631c
mindmajix.com mail is handled by 10 alt3.aspmx.l.google.com.
mindmajix.com mail is handled by 10 alt4.aspmx.l.google.com.
mindmajix.com mail is handled by 5 alt1.aspmx.l.google.com.
mindmajix.com mail is handled by 5 alt2.aspmx.l.google.com.
mindmajix.com mail is handled by 1 aspmx.l.google.com.

┌──(kali㉿kali)-[~]
```

arp-

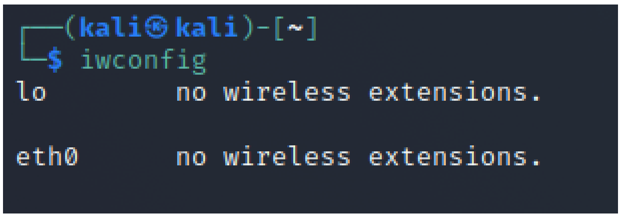
Linux arp command stands for Address Resolution Protocol. It is used to view and add content to the kernel's ARP table.



```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.190.254          ether   00:50:56:f2:4b:b9   C                     eth0
192.168.190.2            ether   00:50:56:e7:16:1f   C                     eth0
```

iwconfig –

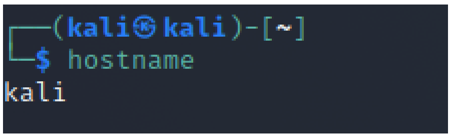
Linux iwconfig is used to configure the wireless network interface. It is used to set and view the basic WI-FI details like SSID and encryption. To know more about this command, refer to the man page.



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

eth0      no wireless extensions.
```

hostname-

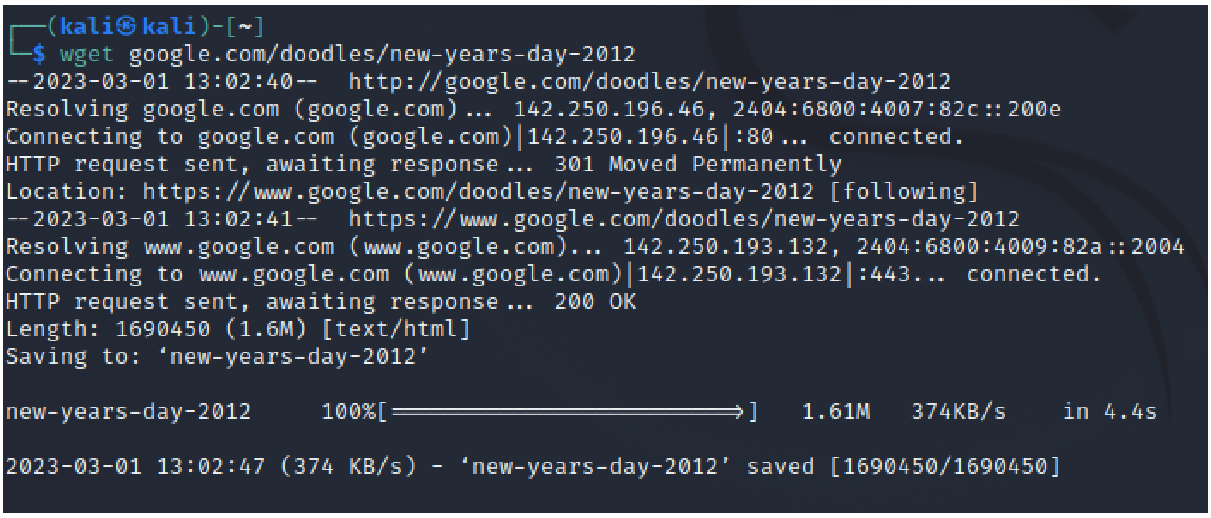
Linux hostname is the simple command used to view and set the hostname of a system.



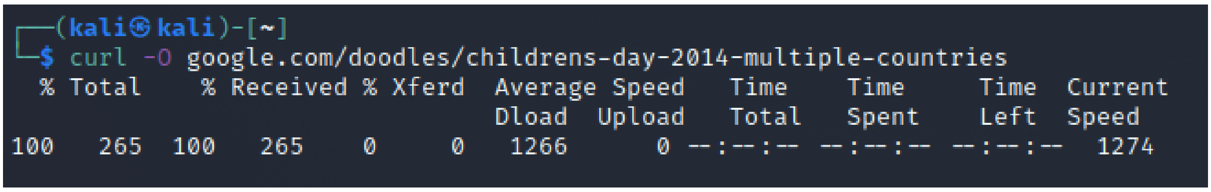
```
┌──(kali㉿kali)-[~]
└─$ hostname
kali
```

curl or wget –

Linux curl and wget commands are used in downloading files from the internet through CLI. The curl command has to be used with the option "O" to fetch the file, while the wget command is used directly.

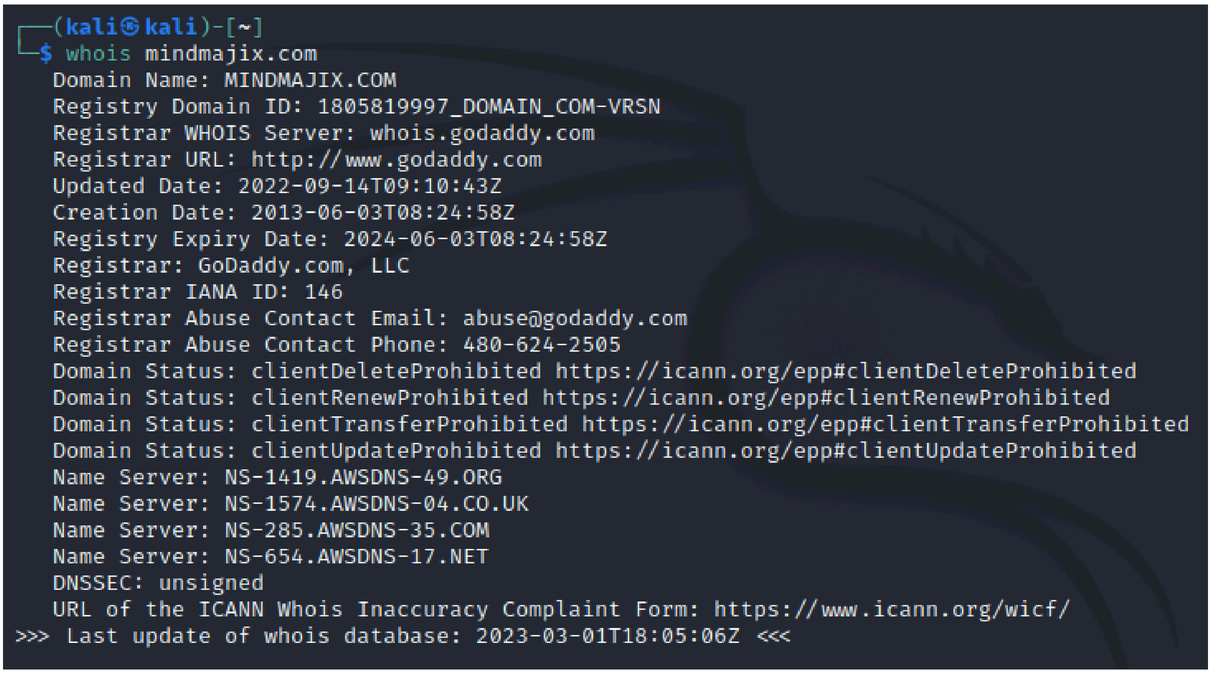


```
┌──(kali㉿kali)-[~]
└─$ wget google.com/doodles/new-years-day-2012
--2023-03-01 13:02:40--  http://google.com/doodles/new-years-day-2012
Resolving google.com (google.com)... 142.250.196.46, 2404:6800:4007:82c::200e
Connecting to google.com (google.com)|142.250.196.46|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.google.com/doodles/new-years-day-2012 [following]
--2023-03-01 13:02:41--  https://www.google.com/doodles/new-years-day-2012
Resolving www.google.com (www.google.com)... 142.250.193.132, 2404:6800:4009:82a::2004
Connecting to www.google.com (www.google.com)|142.250.193.132|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1690450 (1.6M) [text/html]
Saving to: ‘new-years-day-2012’

new-years-day-2012     100%[===================>]   1.61M   374KB/s    in 4.4s

2023-03-01 13:02:47 (374 KB/s) - ‘new-years-day-2012’ saved [1690450/1690450]
```



```
┌──(kali㉿kali)-[~]
└─$ curl -O google.com/doodles/childrens-day-2014-multiple-countries
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   265  100   265    0     0   1266      0 --:--:-- --:--:-- --:--:--  1274
```

whois - Linux whois command is used to fetch all the information related to a website. You can get all the information about a website including the registration and the owner information.



```
┌──(kali㉿kali)-[~]
└─$ whois mindmajix.com
   Domain Name: MINDMAJIX.COM
   Registry Domain ID: 1805819997_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2022-09-14T09:10:43Z
   Creation Date: 2013-06-03T08:24:58Z
   Registry Expiry Date: 2024-06-03T08:24:58Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS-1419.AWSDNS-49.ORG
   Name Server: NS-1574.AWSDNS-04.CO.UK
   Name Server: NS-285.AWSDNS-35.COM
   Name Server: NS-654.AWSDNS-17.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-03-01T18:05:06Z <<<
```