

REPORT ON
KALI LINUX ESSENTIALS COMMAND

By

Intern Name

Ramesh Yadav

Intern ID

2052

1. pwd

1. **Purpose:** Identifies the current directory location within the filesystem hierarchy.
2. **Command:** `pwd`
3. **Description:** Prints the full absolute path of the current working directory to the standard output.

2. ls

1. **Purpose:** Enumerates files and directories within the current or specified location.
2. **Command:** `ls`
3. **Description:** Lists the names of files and subdirectories contained within the active directory.

3. cd

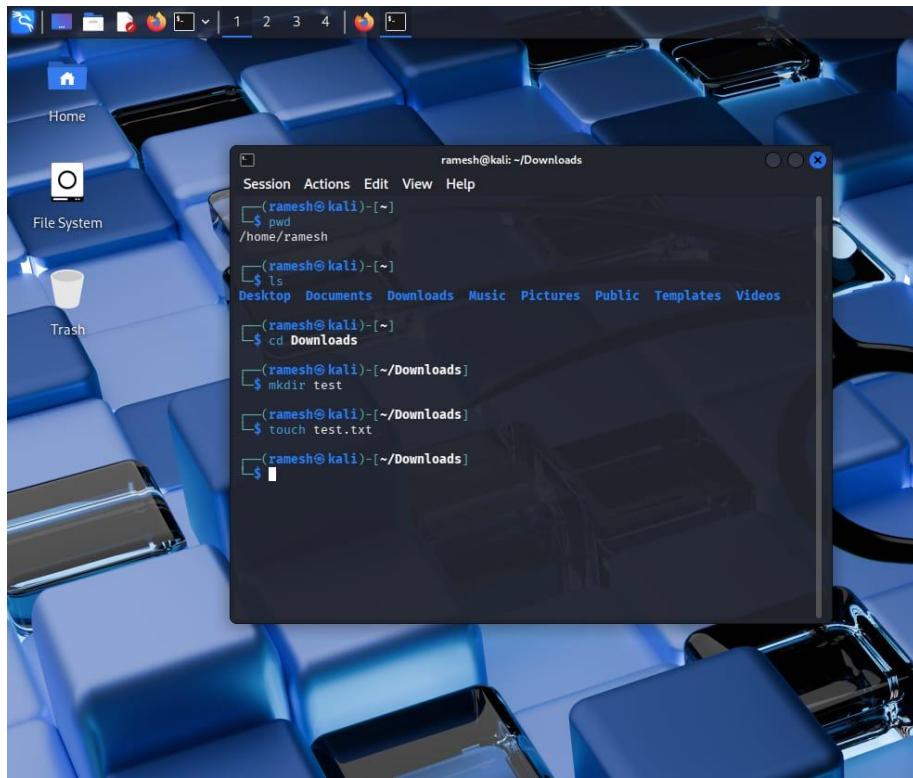
1. **Purpose:** Navigates between different directories in the filesystem.
2. **Command:** `cd`
3. **Description:** Changes the shell's current working directory to the path specified.

4. mkdir

1. **Purpose:** Creates new folders to organize files and data.
2. **Command:** `mkdir`
3. **Description:** Generates a new, empty directory with the specified name at the target location.

5. touch

1. **Purpose:** Updates file timestamps or creates new empty files.
2. **Command:** `touch`
3. **Description:** Creates a new zero-byte file if it does not exist or updates the modification time if it does.



6. rm

1. **Purpose:** Removes files from the filesystem.
2. **Command:** rm
3. **Description:** Unlinks and deletes the specified file from the disk storage.

7. rm -r

1. **Purpose:** Removes directories and their contents recursively.
2. **Command:** rm -r
3. **Description:** Deletes a directory along with all files and subdirectories contained inside it.

8. nano

1. **Purpose:** Edits text files directly within the terminal interface.
2. **Command:** nano
3. **Description:** Launches a simple, modeless command-line text editor for modifying file contents.

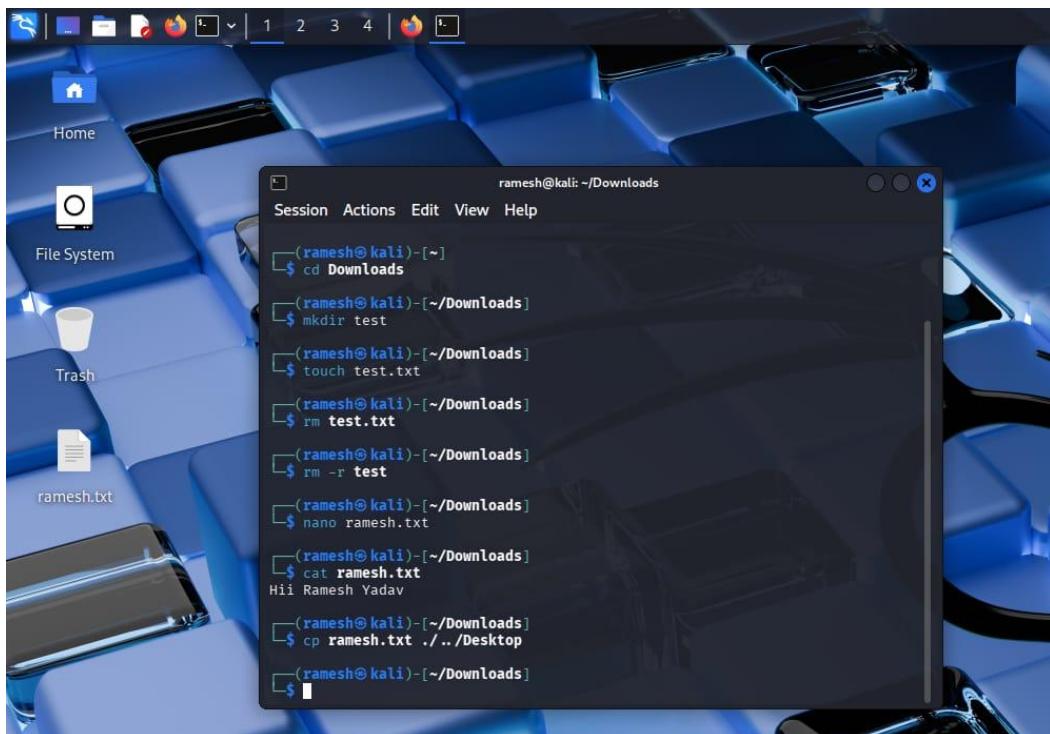
9. cat

1. **Purpose:** Displays file contents or concatenates multiple files.
2. **Command:** cat

3. **Description:** Reads data from a file and outputs it directly to the terminal screen.

10. cp

1. **Purpose:** Duplicates files or directories to a new location.
2. **Command:** cp
3. **Description:** Creates an exact copy of the source file at the specified destination path.



11. mv

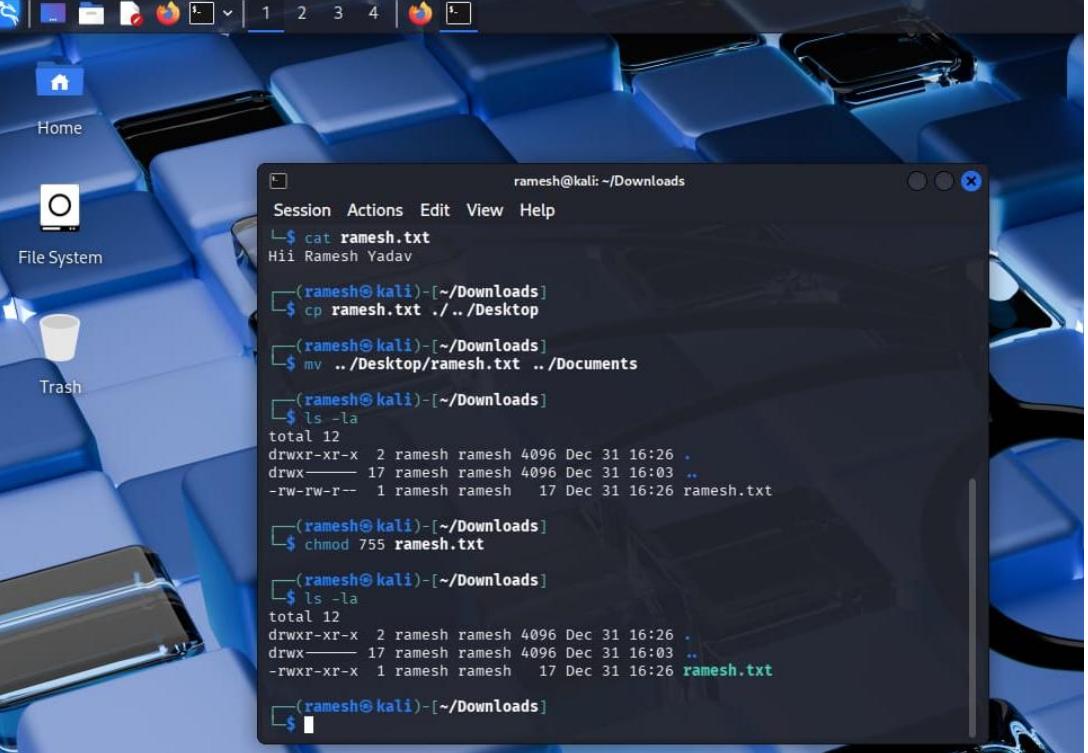
1. **Purpose:** Moves files to a new location or renames them.
2. **Command:** mv
3. **Description:** Relocates a file to a new directory or changes its filename in place.

12. ls -la

1. **Purpose:** Lists all files including hidden ones with detailed permission information.
2. **Command:** ls -la
3. **Description:** Displays a detailed long-format list of all files, including those starting with a dot.

13. chmod

1. **Purpose:** Modifies file access permissions for users and groups.
2. **Command:** chmod
3. **Description:** Changes the read, write, and execute permissions of a specific file or directory.



The screenshot shows a Kali Linux desktop environment with a blue keyboard background. A terminal window is open in the center, displaying the following command history:

```
ramesh@kali: ~/Downloads
Session Actions Edit View Help
└$ cat ramesh.txt
Hi! Ramesh Yadav

└(ramesh@kali)-[~/Downloads]
└$ cp ramesh.txt ./..../Desktop
└(ramesh@kali)-[~/Downloads]
└$ mv ..../Desktop/ramesh.txt ..../Documents
└(ramesh@kali)-[~/Downloads]
└$ ls -la
total 12
drwxr-xr-x  2 ramesh ramesh 4096 Dec 31 16:26 .
drwxr-xr-x  17 ramesh ramesh 4096 Dec 31 16:03 ..
-rw-rw-r--  1 ramesh ramesh   17 Dec 31 16:26 ramesh.txt

└(ramesh@kali)-[~/Downloads]
└$ chmod 755 ramesh.txt

└(ramesh@kali)-[~/Downloads]
└$ ls -la
total 12
drwxr-xr-x  2 ramesh ramesh 4096 Dec 31 16:26 .
drwxr-xr-x  17 ramesh ramesh 4096 Dec 31 16:03 ..
-rwxr-xr-x  1 ramesh ramesh   17 Dec 31 16:26 ramesh.txt

└(ramesh@kali)-[~/Downloads]
└$
```

14. chown

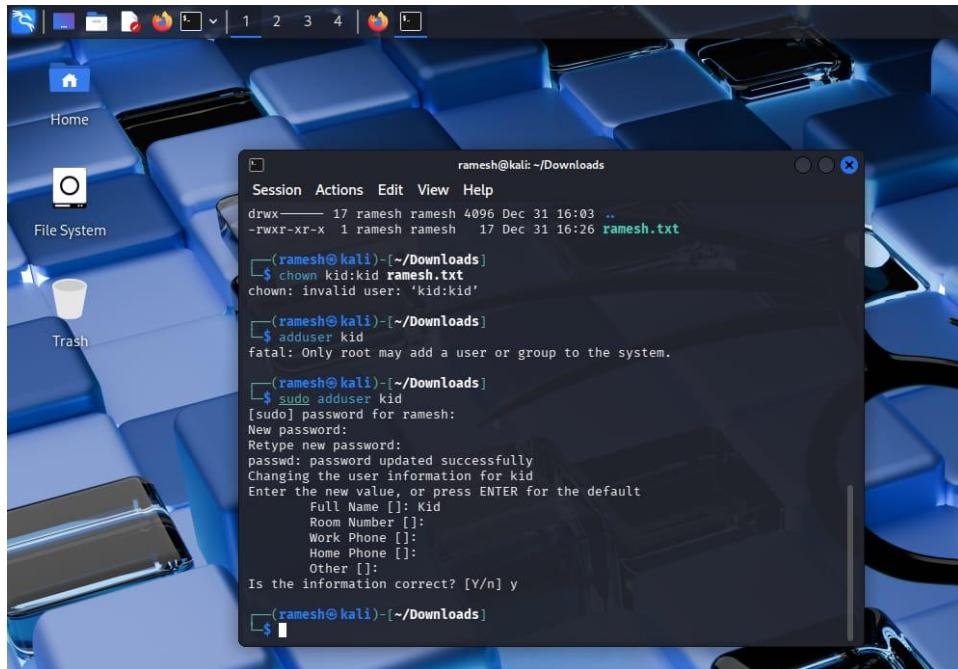
1. **Purpose:** Changes the user and group ownership of a file.
2. **Command:** chown
3. **Description:** Reassigns the ownership rights of a file or directory to a different user or group.

15. adduser

1. **Purpose:** Creates a new user account on the system.
2. **Command:** adduser
3. **Description:** Adds a new user to the system and creates their home directory and configuration.

16. sudo adduser

1. **Purpose:** Executes a command with superuser (root) privileges.
2. **Command:** sudo
3. **Description:** Temporarily grants administrative rights to a standard user for command execution.



A screenshot of a Kali Linux desktop environment. In the center, a terminal window titled 'Session Actions Edit View Help' is open. The terminal shows the following command sequence:

```
(ramesh㉿kali)-[~/Downloads]
$ chown kid:kid ramesh.txt
chown: invalid user: 'kid:kid'

(ramesh㉿kali)-[~/Downloads]
$ adduser kid
fatal: Only root may add a user or group to the system.

(ramesh㉿kali)-[~/Downloads]
$ sudo adduser kid
[sudo] password for ramesh:
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for kid
Enter the new value, or press ENTER for the default
    Full Name []: Kid
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y

(ramesh㉿kali)-[~/Downloads]
$
```

17. sudo chown

1. **Purpose:** Changes file ownership using administrative privileges.
2. **Command:** sudo chown
3. **Description:** Forces a change in file ownership that a standard user permission would normally deny.

18. df -h

1. **Purpose:** Displays disk space usage in a human-readable format.
2. **Command:** df -h
3. **Description:** Shows available and used disk space on mounted filesystems using units like GB and MB.

19. ps aux

1. **Purpose:** precise snapshot of all running processes on the system.
2. **Command:** ps aux

- 3. Description:** Lists detailed information for all active processes from all users.

```

Session Actions Edit View Help
Room Number []:
Work Phone []:
Home Phone []:
Other []
Is the information correct? [Y/n] y
(ramesh㉿kali)-[~/Downloads]
$ chown kid:kid ramesh.txt
chown: changing ownership of 'ramesh.txt': Operation not permitted

(ramesh㉿kali)-[~/Downloads]
$ sudo chown kid:kid ramesh.txt

(ramesh㉿kali)-[~/Downloads]
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            3.7G   0    3.7G  0% /dev
tmpfs           769M  1.5M  767M  1% /run
/dev/sda1        909G  15G  848G  2% /
tmpfs           3.8G  4.0M  3.8G  1% /dev/shm
none            1.0M   0    1.0M  0% /run/credentials/systemd-journald.servi
ce
tmpfs           3.8G  7.5M  3.8G  1% /tmp
none            1.0M   0    1.0M  0% /run/credentials/getty@tty1.service
tmpfs           769M  116K  769M  1% /run/user/1000

(ramesh㉿kali)-[~/Downloads]
$ 

```

20. kill

- Purpose:** Terminates a specific running process.
- Command:** kill
- Description:** Sends a signal to a process ID (PID) instructing it to stop or exit.

21. hostname

- Purpose:** Displays or sets the system's network name.
- Command:** hostname
- Description:** specific command to show or change the name of the host machine.

```

Session Actions Edit View Help
(ramesh㉿kali)-[~/Downloads]
$ ps aux
USER  PID %CPU %MEM   VSZ   RSS TTY STAT START TIME COMMAND
root   1  0.0  0.1 24236 15120 ? S 15:54 0:02 /sbin/init
root   2  0.0  0.0  0 0 ? S 15:54 0:00 [kthread]
root   3  0.0  0.0  0 0 ? S 15:54 0:00 [pool_work
root   4  0.0  0.0  0 0 ? I< 15:54 0:00 [kworker/R
root   5  0.0  0.0  0 0 ? I< 15:54 0:00 [kworker/R
root   6  0.0  0.0  0 0 ? I< 15:54 0:00 [kworker/R
root   7  0.0  0.0  0 0 ? I< 15:54 0:00 [kworker/R
root   8  0.0  0.0  0 0 ? I< 15:54 0:00 [kworker/R
root   10 0.0  0.0  0 0 ? I< 15:54 0:00 [kworker/R
root   11 0.0  0.0  0 0 ? I 15:54 0:00 [kworker/R
root   12 0.0  0.0  0 0 ? I< 15:54 0:00 [kworker/R
root   14 0.0  0.0  0 0 ? S 15:54 0:00 [kworker/R
root   15 0.0  0.0  0 0 ? I 15:54 0:01 [rcu_prem
root   16 0.0  0.0  0 0 ? S 15:54 0:00 [rcu_exp_p
root   17 0.0  0.0  0 0 ? S 15:54 0:00 [rcu_exp_g
root   18 0.0  0.0  0 0 ? S 15:54 0:00 [migration
root   19 0.0  0.0  0 0 ? S 15:54 0:00 [cpuhub/0]
root   20 0.0  0.0  0 0 ? S 15:54 0:00 [cpuhub/0]
root   21 0.0  0.0  0 0 ? S 15:54 0:00 [cpuhub/1]
root   22 0.0  0.0  0 0 ? S 15:54 0:00 [idle_inje
root   23 0.0  0.0  0 0 ? S 15:54 0:00 [migration
root   24 0.0  0.0  0 0 ? S 15:54 0:00 [migration
root   25 0.0  0.0  0 0 ? I< 15:54 0:00 [kworker/1
root   26 0.0  0.0  0 0 ? S 15:54 0:00 [cpuhub/2]
root   27 0.0  0.0  0 0 ? S 15:54 0:00 [cpuhub/2]
root   28 0.0  0.0  0 0 ? S 15:54 0:00 [idle_inje

Session Actions Edit View Help
ramesh 5370 0.1 1.0 2448224 81440 ? Sl 16:03 0:02 /usr/lib/f
ramesh 5425 0.1 1.4 2478844 117420 ? Sl 16:03 0:02 /usr/lib/f
ramesh 5547 0.0 0.6 374404 53764 ? Sl 16:03 0:00 /usr/lib/f
ramesh 5573 0.2 1.7 2492276 138020 ? Sl 16:03 0:03 /usr/lib/f
ramesh 9330 0.0 0.0 0 0 ? Ssl 16:10 0:00 /usr/lib/f
ramesh 10281 0.1 0.1 2448224 52278 ? Sl 16:12 0:01 /usr/lib/f
ramesh 12199 0.0 0.1 461040 9284 ? Sl 16:16 0:00 /usr/libexec
ramesh 12209 0.0 0.1 388336 9240 ? Sl 16:16 0:00 /usr/libexec
root 14816 0.0 0.0 0 0 ? I 16:21 0:00 [kworker/u
root 15296 0.0 0.0 0 0 ? I 16:22 0:00 [kworker/6
root 16734 0.0 0.0 0 0 ? I 16:25 0:00 [kworker/2
root 16747 0.0 0.0 0 0 ? I 16:26 0:00 [kworker/7
root 17626 0.0 0.0 0 0 ? I 16:26 0:00 [kworker/0
ramesh 18678 0.0 0.3 412732 27540 ? Ssl 16:28 0:00 /usr/lib/x
root 18738 0.0 0.0 0 0 ? I 16:28 0:00 [kworker/4
root 20642 0.0 0.1 17256 7896 ? Ss 16:32 0:00 /usr/lib/s
ramesh 21428 0.0 0.0 9504 4300 pts/0 R+ 16:33 0:00 ps aux

Session Actions Edit View Help
(ramesh㉿kali)-[~/Downloads]
$ kill 18678
kill: kill 18678 failed: no such process

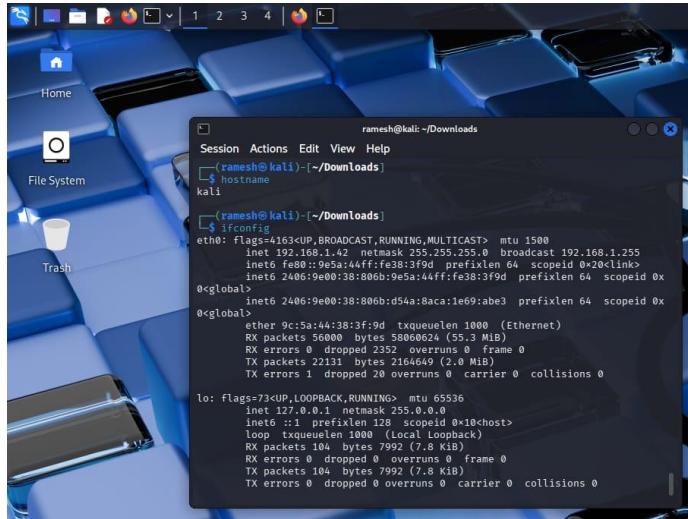
(ramesh㉿kali)-[~/Downloads]
$ hostname
kali

(ramesh㉿kali)-[~/Downloads]
$ 

```

22. ifconfig

- Purpose:** Configures or displays network interface parameters.
- Command:** ifconfig
- Description:** specific legacy tool to view IP addresses, MAC addresses, and active network interfaces.

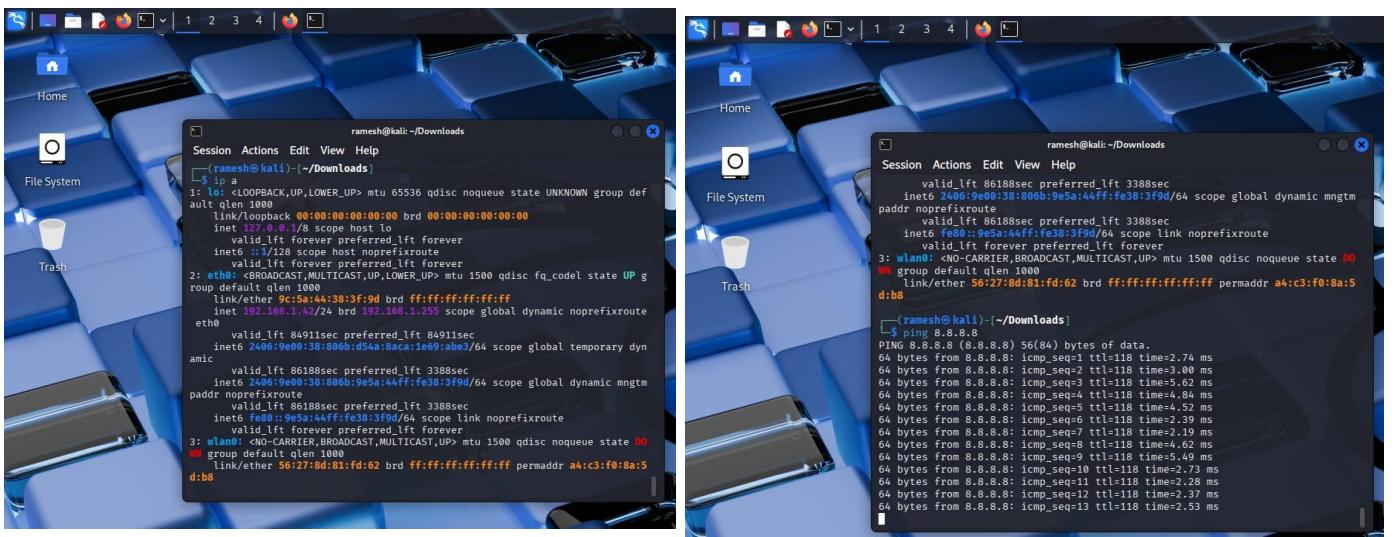


```
ramesh@kali: ~/Downloads
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.42 netmask 255.255.255.0 broadcast 192.168.1.255
                inetb fe80::9e0a:44ff:fe38:3f9d prefixlen 64 scopeid 0x0<global>
        ether 9c:5a:44:38:3f:9d txqueuelen 1000 (Ethernet)
        RX packets 56000 bytes 58060624 (55.3 MiB)
        RX errors 0 dropped 2392 overruns 0 frame 0
        TX packets 21311 bytes 2164649 (2.0 MiB)
        TX errors 1 dropped 20 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 0.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x1<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 700 bytes 700 (7.8 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 104 bytes 7992 (7.8 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

23. ip

- Purpose:** Manages network routing, devices, and tunnels.
- Command:** ip
- Description:** Modern and powerful utility for configuring network interfaces and viewing routing tables.



```
ramesh@kali: ~/Downloads
$ 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 noprefixroute
            valid_lft forever preferred_lft forever
2: eth0 <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 9c:5a:44:38:3f:9d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.42/24 brd 192.168.1.255 scope global dynamic noprefixroute
        valid_lft 8491sec preferred_lft 8491sec
        inet6 fe80::9e0a:44ff:fe38:3f9d/64 scope global dynamic mngmt
            valid_lft 86188sec preferred_lft 3388sec
            paddr noprefixroute
            valid_lft 86188sec preferred_lft 3388sec
            inet6 fe80::9e5a:44ff:fe38:3f9d/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
3: wlan0 <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 56:27:8d:81:fd:62 brd ff:ff:ff:ff:ff:ff permaddr a4:c3:f0:8a:5d:b8
```



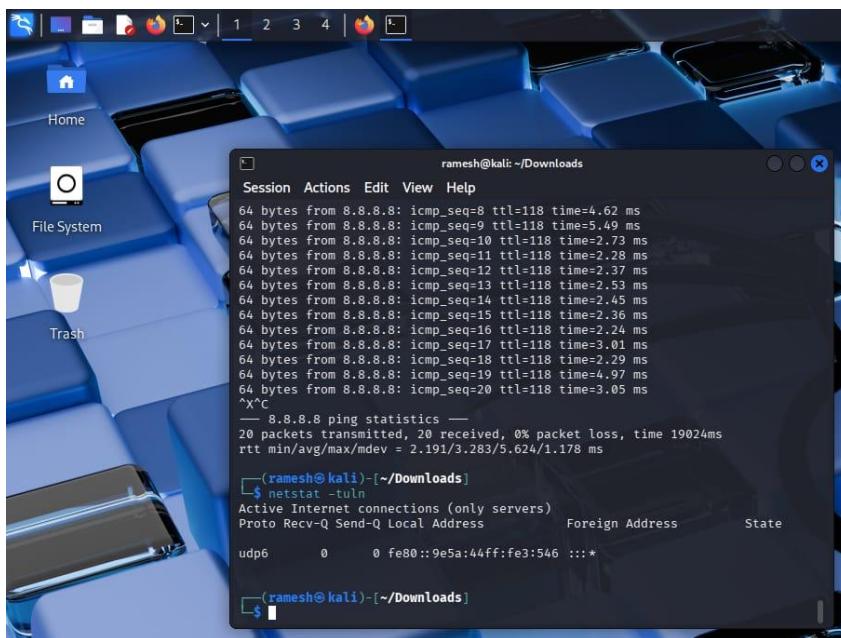
```
ramesh@kali: ~/Downloads
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=2.74 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=3.00 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=5.62 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=4.84 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=4.52 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=2.39 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=118 time=2.19 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=118 time=4.62 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=118 time=5.49 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=118 time=7.73 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=118 time=2.28 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=118 time=2.37 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=118 time=2.53 ms
```

24. ping

1. **Purpose:** Tests connectivity to a remote network host.
2. **Command:** ping
3. **Description:** Sends ICMP Echo Request packets to a target to verify reachability and measure latency.

25. netstat -tuln

1. **Purpose:** Lists all active listening ports on the system.
2. **Command:** netstat -tuln
3. **Description:** Displays TCP and UDP ports that are currently open and listening for connections.



The screenshot shows a Kali Linux desktop environment with a blue-themed wallpaper. A terminal window is open in the foreground, displaying the output of the `netstat -tuln` command. The terminal output includes a list of ICMP echo requests sent to 8.8.8.8, ping statistics, and a table of active Internet connections. The table shows one entry for udp6 on port 546.

```
Session Actions Edit View Help
ramesh@kali: ~/Downloads
4 bytes from 8.8.8.8: icmp_seq=8 ttl=118 time=4.62 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=118 time=5.49 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=118 time=2.73 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=118 time=2.28 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=118 time=2.37 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=118 time=2.53 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=118 time=2.45 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=118 time=2.36 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=118 time=2.24 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=118 time=3.01 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=118 time=2.29 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=118 time=4.97 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=118 time=3.05 ms
^C
-- 8.8.8.8 ping statistics --
20 packets transmitted, 20 received, 0% packet loss, time 19024ms
rtt min/avg/max/mdev = 2.191/3.283/5.624/1.178 ms
(ramesh@kali)-[~/Downloads]
$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp6      0      0 fe80::9e5a:44ff:fe3:546  ::*
(ramesh@kali)-[~/Downloads]
$
```

26. nmap

1. **Purpose:** Scans networks to discover hosts and open ports.
2. **Command:** nmap
3. **Description:** Probes a target IP to determine active services, operating systems, and vulnerabilities.

27. traceroute

1. **Purpose:** Traces the path packets take to reach a destination.
2. **Command:** traceroute

3. **Description:** Shows every router hop between the local system and the target server.



The screenshot shows a Kali Linux desktop environment with a blue-themed wallpaper. In the top dock, there are icons for Home, File System, and Trash. A terminal window titled '(ramesh㉿kali)-[~/Downloads]' is open, displaying the output of the 'nmap' command against the IP address 192.168.1.1. The output shows various ports and services open or filtered. Below it, another terminal window shows the output of the 'traceroute' command to the same host, indicating a path of 30 hops.

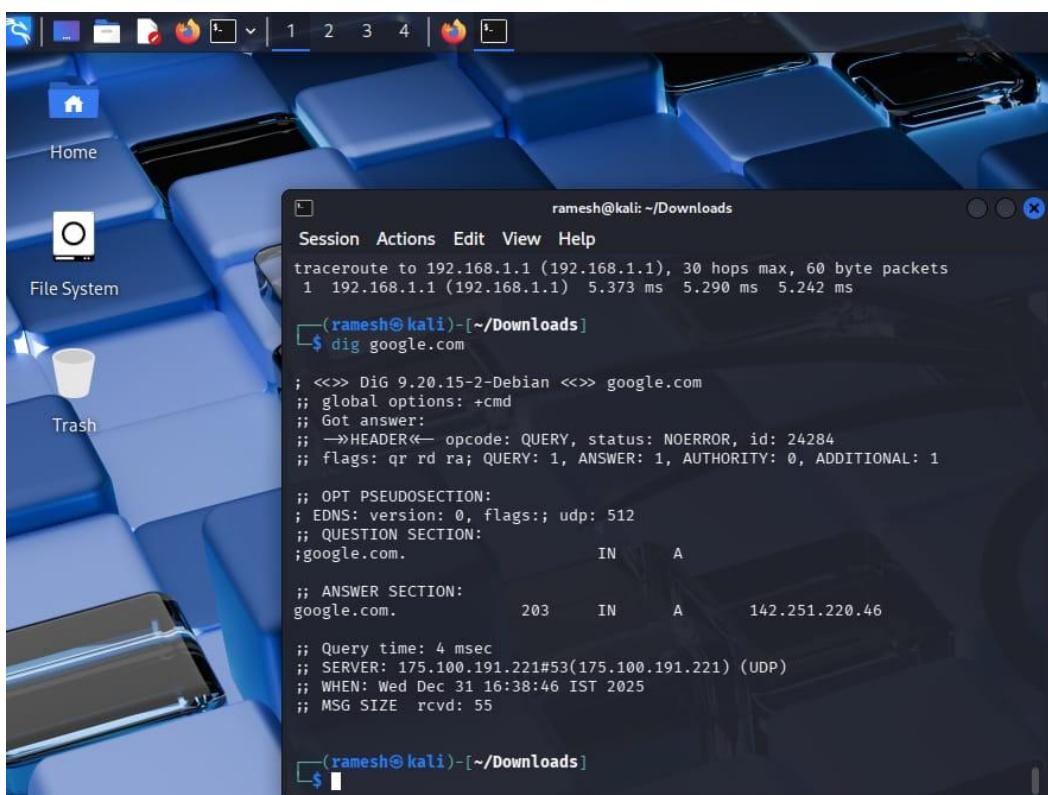
```
(ramesh㉿kali)-[~/Downloads]
$ nmap 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-31 16:37 IST
Nmap scan report for 192.168.1.1
Host is up (0.020s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    open     domain
80/tcp    open     http
139/tcp   filtered netbios-ssn
443/tcp   open     https
445/tcp   filtered microsoft-ds
8000/tcp  open     http-alt
MAC Address: 98:9D:B2:6F:2E:33 (Goip Global Services Pvt. )

Nmap done: 1 IP address (1 host up) scanned in 3.94 seconds

(ramesh㉿kali)-[~/Downloads]
$ traceroute 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  5.373 ms  5.290 ms  5.242 ms
```

28. dig

1. **Purpose:** Queries DNS servers for domain records.
2. **Command:** dig
3. **Description:** Retrieves detailed DNS information like A, MX, and TXT records for a domain.



The screenshot shows a Kali Linux desktop environment with a blue-themed wallpaper. In the top dock, there are icons for Home, File System, and Trash. A terminal window titled '(ramesh㉿kali)-[~/Downloads]' is open, displaying the output of the 'dig' command for the domain 'google.com'. The output shows the DNS query process, including the question section, answer section (with the IP address 142.251.220.46), and other details like flags and time.

```
(ramesh㉿kali)-[~/Downloads]
traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  5.373 ms  5.290 ms  5.242 ms

(ramesh㉿kali)-[~/Downloads]
$ dig google.com

; <>> DIG 9.20.15-2-Debian <>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 24284
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.        203     IN      A      142.251.220.46

;; Query time: 4 msec
;; SERVER: 175.100.191.221#53(175.100.191.221) (UDP)
;; WHEN: Wed Dec 31 16:38:46 IST 2025
;; MSG SIZE  rcvd: 55

(ramesh㉿kali)-[~/Downloads]
```

29. route

1. **Purpose:** Viewing and manipulating the IP routing table.
2. **Command:** route
3. **Description:** Displays or modifies the table that controls where network traffic is directed.

30. curl

1. **Purpose:** Transfers data from or to a server using URLs.
2. **Command:** curl
3. **Description:** command line tool to send HTTP requests or download files from the web.

31. scp

1. **Purpose:** Securely copies files between hosts over a network.
2. **Command:** scp
3. **Description:** Transfers files using the SSH protocol to ensure data is encrypted during transit.

32. ssh

1. **Purpose:** Log into a remote machine securely.
2. **Command:** ssh
3. **Description:** Establishes an encrypted remote command-line session with another computer.

33. airmon-ng

1. **Purpose:** Enables monitor mode on wireless network interfaces.
2. **Command:** airmon-ng
3. **Description:** Configures a Wi-Fi card to capture all traffic rather than just packets sent to it.

34. iwconfig

1. **Purpose:** Configures wireless network interface parameters.
2. **Command:** iwconfig

3. **Description:** Sets specific wireless settings like frequency, channel, and transmission power.

The image shows two side-by-side screenshots of a Kali Linux terminal window. The left screenshot displays the output of the 'route' command, showing the kernel IP routing table with a default gateway of 192.168.1.1 and interfaces eth0 and wlan0. It also shows the output of curling Google's homepage and attempting to scp a file to a non-existent directory. The right screenshot shows the output of iwconfig, detailing the wireless interface (wlan0) which is currently not associated with any access point.

```

ramesh@kali: ~/Downloads
$ route
Kernel IP routing table
Destination     Gateway      Genmask      Flags Metric Ref    Use Iface
default         192.168.1.1  0.0.0.0      UG        100    0      0 eth0
192.168.1.0    0.0.0.0     255.255.255.0 U          100    0      0 eth0

(ramesh@kali)-[~/Downloads]
$ curl google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>
</BODY></HTML>

(ramesh@kali)-[~/Downloads]
$ scp ramesh.txt ramesh@192.168.1.111:/home/ramesh
cp: cannot stat 'ramesh': No such file or directory

(ramesh@kali)-[~/Downloads]
$ ssh ramesh@192.168.1.111
The authenticity of host '192.168.1.111 (192.168.1.111)' can't be established
ED25519 key fingerprint is: SHA256:uLcwwG9Fwsxbmfy9etTvlvriW1J6qNBfs4G8lk066j
g
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? ^C

(ramesh@kali)-[~/Downloads]
$ airmon-ng
Run it as root
(ramesh@kali)-[~/Downloads]
$ iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:

```

35. nikto -h

1. **Purpose:** Scans web servers for dangerous files and configurations.
2. **Command:** nikto -h
3. **Description:** Performs a comprehensive test against a specified web host for known vulnerabilities.

36. dirb

1. **Purpose:** Brute-forces hidden web directories and files.
2. **Command:** dirb
3. **Description:** Scans a website using a wordlist to find unlinked or hidden content.

37. john

1. **Purpose:** Cracks password hashes offline.
2. **Command:** john
3. **Description:** Detects weak passwords by processing stolen hash files against dictionary lists.

```

ramesh@kali: ~/Downloads
Session Actions Edit View Help
(ramesh@kali)-[~/Downloads]
$ ssh ramesh@192.168.1.111
The authenticity of host '192.168.1.111 (192.168.1.111)' can't be established
.
ED25519 key fingerprint is: SHA256:uLcwG9Fwsxbmfy9etTvlvIW1J6qNBfs4G8lk066jg
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? `c

(ramesh@kali)-[~/Downloads]
$ airmon-ng
Run it as root

(ramesh@kali)-[~/Downloads]
$ iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated
        Retry short limit:7  RTS thr:off Fragment thr:off
        Power Management:on

(ramesh@kali)-[~/Downloads]
$ 

1 2 3 4 | Firefox
ramesh@kali: ~/Downloads
Session Actions Edit View Help
DIRB v2.22
By The Dark Raver

(!) FATAL: Invalid URL format: google.com/
(use: "http://host/" or "https://host/" for SSL)

(ramesh@kali)-[~/Downloads]
$ dirb https://google.com

DIRB v2.22
By The Dark Raver

START_TIME: Wed Dec 31 16:45:35 2025
URL_BASE: https://google.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
--- Scanning URL: https://google.com/ ---
[+] Testing: https://google.com/_mm

1 2 3 4 | Firefox
ramesh@kali: ~/Downloads
Session Actions Edit View Help
DIRB v2.22
By The Dark Raver

START_TIME: Wed Dec 31 16:45:35 2025
URL_BASE: https://google.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
--- Scanning URL: https://google.com/ ---
^C > Testing: https://google.com/100
(ramesh@kali)-[~/Downloads]
$ enum4linux
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

1 2 3 4 | Firefox
ramesh@kali: ~/Downloads
Session Actions Edit View Help
access: Allow anonymous SID/Name translation" enabled (XP, 2003).
NB: Samba servers often seem to have RIDs in the range 3000-3050.
Dependancy info: You will need to have the samba package installed as this
script is basically just a wrapper around rpcclient, net, nmblookup and
smbclient. Polenum from http://labs.portcullis.co.uk/application/polenum/
is required to get Password Policy info.

(ramesh@kali)-[~/Downloads]
$ enum4linux-U
enum4linux-U: command not found

(ramesh@kali)-[~/Downloads]
$ john
Created directory: /home/ramesh/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 O
MP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/
Usage: john [OPTIONS] [PASSWORD-FILES]
Use --help to list all available options.

(ramesh@kali)-[~/Downloads]
$ 

```

38. msfconsole

1. **Purpose:** Provides a centralized interface for the Metasploit Framework.
2. **Command:** msfconsole
3. **Description:** Manages and executes exploits, payloads, and auxiliary modules from a unified console.

```

Session Actions Edit View Help
Usage: john [OPTIONS] [PASSWORD-FILES]
Use --help to list all available options.

(ramesh㉿kali)-[~/Downloads]
└─$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

      IIIII   dTb,dTb
      II    4' v 'B
      II    6' .P
      II    'T1, -P'
      II    'T1, -P'
      IIIIII  'YVP'

I love shells --egypt

      =[ metasploit v6.4.99-dev
+ -- --=[ 2,572 exploits - 1,317 auxiliary - 1,680 payloads
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > 

```

39. sslscan

- Purpose:** Assesses SSL/TLS server configuration.
- Command:** sslscan
- Description:** Identifies supported ciphers and protocols to detect weak encryption settings.

40. dnsrecon

- Purpose:** Performs advanced DNS enumeration and scanning.
- Command:** dnsrecon
- Description:** Maps domain infrastructure by checking for zone transfers, subdomains, and records.

```

Session Actions Edit View Help
(ramesh㉿kali)-[~/Downloads]
└─$ sslscan 192.168.1.111
Version: 2.1.5
OpenSSL 3.5.4 30 Sep 2025

Connected to 192.168.1.111

Testing SSL server 192.168.1.111 on port 443 using SNI name 192.168.1.111

SSL/TLS Protocols:
SSLv2 disabled
SSLv3 disabled
TLSv1.0 disabled
TLSv1.1 disabled
TLSv1.2 enabled
TLSv1.3 enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:

```



```

Session Actions Edit View Help
(ramesh㉿kali)-[~/Downloads]
└─$ dnsrecon
usage: dnsrecon [-h] [-d DOMAIN] [-i INPUT_LIST] [-n NS_SERVER] [-r RANGE]
                [-D DICTIONARY] [-f] [-a] [-s] [-b] [-y] [-k] [-w] [-z]
                [-threads THREADS] [--lifetime LIFETIME]
                [-loglevel {DEBUG,INFO,WARNING,ERROR,CRITICAL}] [--tcp]
                [--db DB] [-x XML] [-c CSV] [-j JSON] [--iw]
                [--disable_check_nxdomain] [--disable_check_recursion]
                [--disable_check_bindversion] [-V] [-v] [-t TYPE]

```