Ex:1b   **LINUX COMMANDS**

Date:27.7.24

1.ifconfig: ifconfig is short for interface configurator. This command is utilized in network inspection, initializing the interface, enabling or disabling an IP address, and configuring an interface with an IP address. Also, it is used to show the network and route interface. The basic details shown with ifconfig are:

- MTU
- MAC address
- IP address

Syntax:
ifconfig

2. ip: It is the updated and latest edition of ifconfig command. The command provides the information of every network, such as ifconfig. Also, it can be used to get information about a particular interface. **Syntax:**

ip a
ip addr

```
File  Actions  Edit  View  Help
(root@kali)-[/home/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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86232sec preferred_lft 86232sec
    inet6 fd00::a26b:5af3:4cda:29cb/64 scope global dynamic noprefixroute
       valid_lft 86234sec preferred_lft 14234sec
    inet6 fe80::f510:77a5:bdfb:fc6d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

(root@kali)-[/home/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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86205sec preferred_lft 86205sec
    inet6 fd00::a26b:5af3:4cda:29cb/64 scope global dynamic noprefixroute
       valid_lft 86207sec preferred_lft 14207sec
    inet6 fe80::f510:77a5:bdfb:fc6d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

3.**traceroute:** The traceroute command is one of the most helpful commands in the networking field. It's used to balance the network. It identifies the delay and decides the pathway to our target. Basically, it aids in the below ways: It determines the location of the network latency and informs it.

- It follows the path to the destination.
- It gives the names and recognizes all devices on the path.

Syntax:

traceroute**< destination>**

```
┌──(root💀kali)-[/home/kali]
└─# traceroute www.facebook.com;
traceroute to www.facebook.com (157.240.192.35), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.687 ms  1.008 ms  1.151 ms
 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  * * *
```

4.tracepath: The tracepath command is the same as the traceroute command, and it is used to find network delays. Besides, it does not need root privileges. By default, it comes pre-installed in Ubuntu. It traces the path to the destination and recognizes all hops in it.

It identifies the point at which the network is weak if our network is not strong enough.

Syntax:

tracepath **<destination>**

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/kali]
└─# tracepath www.google.com
1?: [LOCALHOST]                       pmtu 1500
1:   10.0.2.2                                          0.780ms
1:   10.0.2.2                                          0.323ms
2:   no reply
3:   no reply
4:   no reply
5:   no reply
6:   no reply
7:   no reply
8:   no reply
9:   no reply
10:  no reply
11:  no reply
12:  no reply
13:  no reply
```

5.

ping: It is short for Packet Internet Groper. The ping command is one of the widely used commands for network troubleshooting. Basically, it inspects the network connectivity between two different nodes.

Syntax:

ping **<destination>**

```
File   Actions   Edit   View   Help
└─# ping www.google.com
PING www.google.com (142.250.182.4) 56(84) bytes of data.
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=1 ttl=255 time=6.94 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=2 ttl=255 time=9.37 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=3 ttl=255 time=9.73 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=4 ttl=255 time=9.21 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=5 ttl=255 time=9.76 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=6 ttl=255 time=10.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=7 ttl=255 time=9.76 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=8 ttl=255 time=9.75 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=9 ttl=255 time=11.3 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=10 ttl=255 time=9.62 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=11 ttl=255 time=11.4 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=12 ttl=255 time=9.48 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=13 ttl=255 time=7.15 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=14 ttl=255 time=10.5 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=15 ttl=255 time=10.6 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=16 ttl=255 time=9.48 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=17 ttl=255 time=8.62 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=18 ttl=255 time=9.36 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=19 ttl=255 time=12.7 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=20 ttl=255 time=9.26 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=21 ttl=255 time=9.84 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=22 ttl=255 time=16.6 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=23 ttl=255 time=9.45 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=24 ttl=255 time=8.90 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=25 ttl=255 time=8.40 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=26 ttl=255 time=8.94 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=27 ttl=255 time=9.33 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=28 ttl=255 time=8.64 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=29 ttl=255 time=9.15 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=30 ttl=255 time=9.30 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=31 ttl=255 time=8.01 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=32 ttl=255 time=9.68 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=33 ttl=255 time=8.89 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=34 ttl=255 time=9.16 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=35 ttl=255 time=8.90 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=36 ttl=255 time=8.66 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=37 ttl=255 time=8.16 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=38 ttl=255 time=9.48 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=39 ttl=255 time=9.11 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=40 ttl=255 time=9.74 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=41 ttl=255 time=8.10 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=42 ttl=255 time=8.55 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=43 ttl=255 time=7.55 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=44 ttl=255 time=11.4 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=45 ttl=255 time=8.04 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=46 ttl=255 time=9.11 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=47 ttl=255 time=8.81 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=48 ttl=255 time=8.73 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=49 ttl=255 time=8.82 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=50 ttl=255 time=8.55 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=51 ttl=255 time=8.62 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=52 ttl=255 time=8.01 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=53 ttl=255 time=7.78 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=54 ttl=255 time=8.46 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=55 ttl=255 time=8.45 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=56 ttl=255 time=7.36 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=57 ttl=255 time=8.93 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=58 ttl=255 time=7.80 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=59 ttl=255 time=7.73 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=60 ttl=255 time=8.42 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=61 ttl=255 time=7.77 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=62 ttl=255 time=7.86 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=63 ttl=255 time=8.09 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=64 ttl=255 time=9.05 ms
^C
--- www.google.com ping statistics ---
64 packets transmitted, 64 received, 0% packet loss, time 63648ms
rtt min/avg/max/mdev = 6.944/9.131/16.564/1.405 ms
```

6.netstat : It is short for network statistics. It gives statistical figures of many interfaces, which contain open sockets, connection information, and routing tables

```
┌──(root@kali)-[/home/kali]
└─# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         State
udp        0      0 10.0.2.15:bootpc        10.0.2.2:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     9567     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     8014
unix  3      [ ]         STREAM     CONNECTED     8939     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     7965
unix  3      [ ]         STREAM     CONNECTED     9503     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     9234
unix  3      [ ]         STREAM     CONNECTED     9015
unix  3      [ ]         STREAM     CONNECTED     10280
unix  3      [ ]         STREAM     CONNECTED     8847     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     7976
unix  3      [ ]         STREAM     CONNECTED     9184     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8241     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9328     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9571     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8038     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8020
unix  3      [ ]         STREAM     CONNECTED     8845     @/tmp/.ICE-unix/863
unix  3      [ ]         STREAM     CONNECTED     8642     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9593
unix  3      [ ]         STREAM     CONNECTED     9175
unix  3      [ ]         STREAM     CONNECTED     8030     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     8004     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     7970
unix  3      [ ]         STREAM     CONNECTED     10298
unix  3      [ ]         STREAM     CONNECTED     9479     /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9271
unix  3      [ ]         STREAM     CONNECTED     9385     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8015
unix  3      [ ]         STREAM     CONNECTED     8865     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     7974
unix  3      [ ]         STREAM     CONNECTED     9604
unix  3      [ ]         STREAM     CONNECTED     9231     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     7660
unix  3      [ ]         STREAM     CONNECTED     10281    /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     8810     @/tmp/.ICE-unix/863
unix  3      [ ]         STREAM     CONNECTED     11408
unix  3      [ ]         STREAM     CONNECTED     8043     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8011     /run/user/1000/bus
unix  3      [ ]         DGRAM      CONNECTED     4199     /run/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     9627
unix  3      [ ]         STREAM     CONNECTED     9605
```

7.ss: This command is the substitution for the netstat command. The ss command is more informative and much faster than netstat. The ss command's faster response is possible because it fetches every information from inside the kernel userspace.
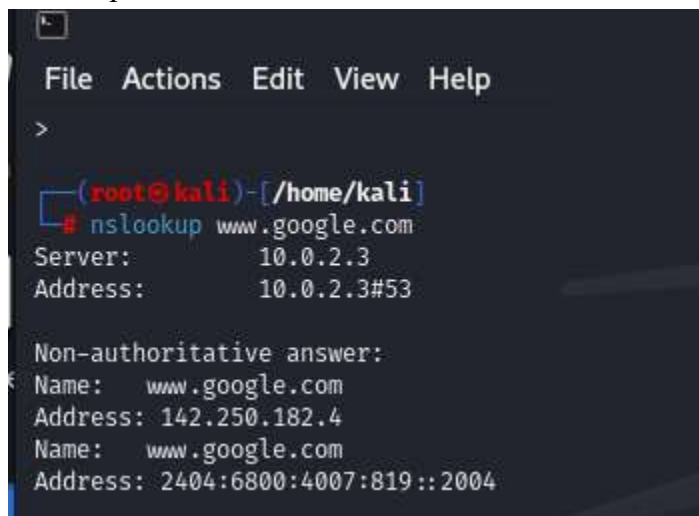
Syntax:

ss

8.nsloopup: The nslookup command is an older edition of the dig command. Also, it is utilized for DNS related problems.

.

Syntax:

nslookup **<domainname>**

```
File  Actions  Edit  View  Help
>

  ┌──(root㉿kali)-[/home/kali]
  └─# nslookup www.google.com
  Server:          10.0.2.3
  Address:         10.0.2.3#53

  Non-authoritative answer:
  Name:   www.google.com
  Address: 142.250.182.4
  Name:   www.google.com
  Address: 2404:6800:4007:819::2004
```

9.

dig: dig is short for Domain Information Groper. The dig command is an improvised edition of the nslookup command. It is utilized in DNS lookup to reserve the DNS name server.

Also, it is used to balance DNS related problems. Mainly, it is used to authorize DNS mappings, host addresses, MX records, and every other DNS record for the best DNS topography understanding. **Syntax:**

dig **<domainname>**

```
File  Actions  Edit  View  Help

  ┌──(root@kali)-[/home/kali]
  └─# dig

; <<>> DiG 9.20.0-Debian <<>>
;; global options: +cmd
;; Got answer:
;; ─»HEADER«─ opcode: QUERY, status: NOERROR, id: 29334
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;.                                  IN      NS

;; ANSWER SECTION:
.                       5098    IN      NS      h.root-servers.net.
.                       5098    IN      NS      g.root-servers.net.
.                       5098    IN      NS      m.root-servers.net.
.                       5098    IN      NS      j.root-servers.net.
.                       5098    IN      NS      b.root-servers.net.
.                       5098    IN      NS      c.root-servers.net.
.                       5098    IN      NS      d.root-servers.net.
.                       5098    IN      NS      k.root-servers.net.
.                       5098    IN      NS      f.root-servers.net.
.                       5098    IN      NS      a.root-servers.net.
.                       5098    IN      NS      l.root-servers.net.
.                       5098    IN      NS      i.root-servers.net.
.                       5098    IN      NS      e.root-servers.net.

;; Query time: 28 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sat Nov 23 06:17:27 EST 2024
;; MSG SIZE  rcvd: 239
```
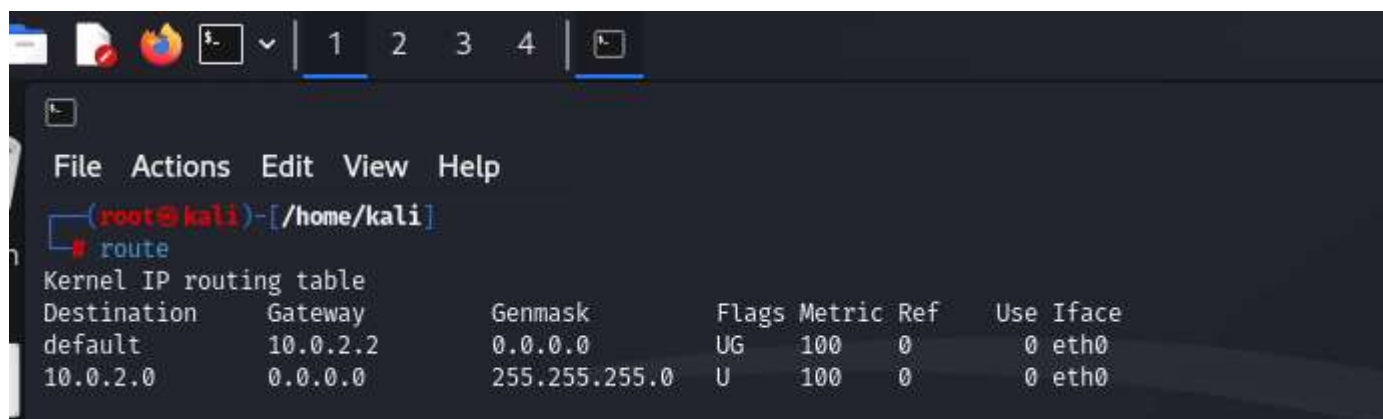
10.

route: The route command shows and employs the routing table available for our system. Basically, a router is used to detect a better way to transfer the packets around a destination.

Syntax:

    route

RESULT :

    Basic networking linux commands are executed successfully.