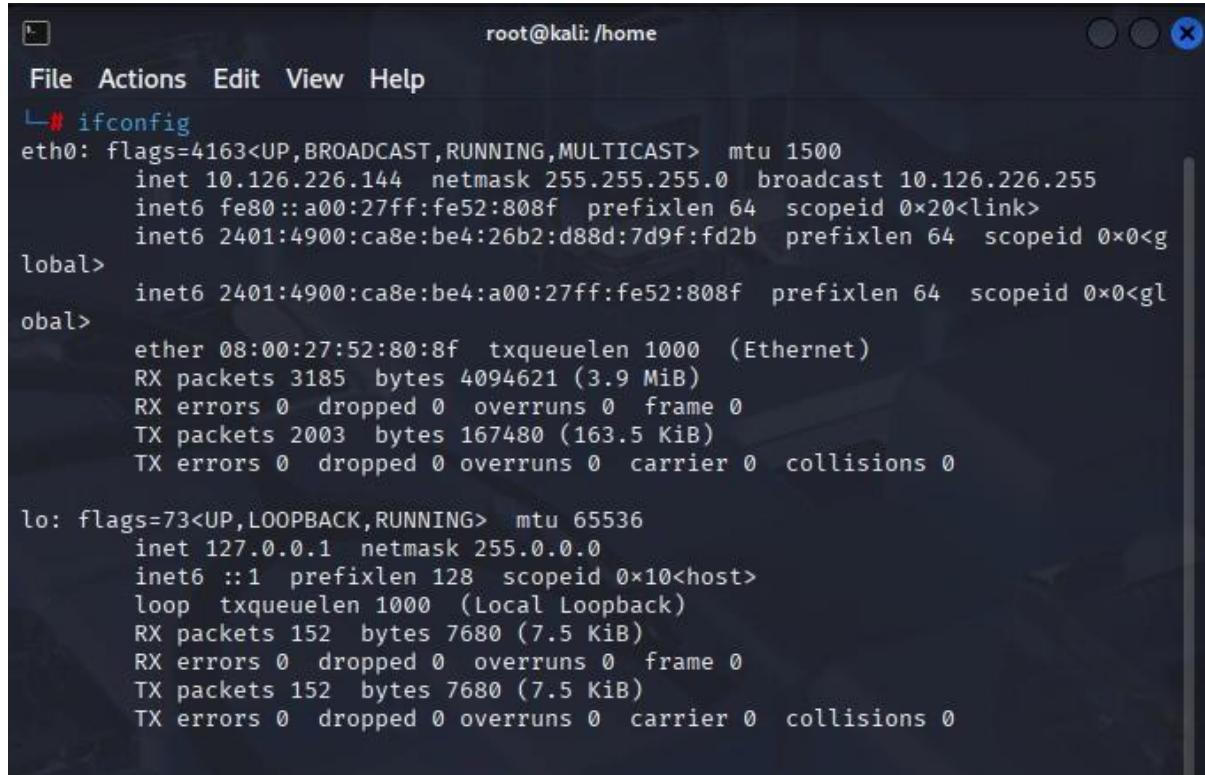**TASK – 1**

Port Scanning, TCP SYN Scan, IP ranges, Network Reconnaissance, Open Ports.

To get the IP address of the machine :

Command : ifconfig

OUTPUT :


```
root@kali: /home

File  Actions  Edit  View  Help
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.126.226.144  netmask 255.255.255.0  broadcast 10.126.226.255
        inet6 fe80::a00:27ff:fe52:808f  prefixlen 64  scopeid 0×20<link>
        inet6 2401:4900:ca8e:be4:26b2:d88d:7d9f:fd2b  prefixlen 64  scopeid 0×0<g
lobal>
        inet6 2401:4900:ca8e:be4:a00:27ff:fe52:808f  prefixlen 64  scopeid 0×0<gl
obal>
        ether 08:00:27:52:80:8f  txqueuelen 1000  (Ethernet)
        RX packets 3185  bytes 4094621 (3.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2003  bytes 167480 (163.5 KiB)
        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 152  bytes 7680 (7.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 152  bytes 7680 (7.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To get the Open Ports :

Command : nmap 10.126.226.202 -p-

OUTPUT :

```
                                                    root@kali: /home

 File  Actions  Edit  View  Help

 ┌──(root㉿kali)-[/home]
 └─# nmap  10.126.226.202 -p-
 Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-12 21:21 IST
 Nmap scan report for 10.126.226.202
 Host is up (0.00035s latency).
 Not shown: 65505 closed tcp ports (reset)
 PORT       STATE  SERVICE
 21/tcp     open   ftp
 22/tcp     open   ssh
 23/tcp     open   telnet
 25/tcp     open   smtp
 53/tcp     open   domain
 80/tcp     open   http
 111/tcp    open   rpcbind
 139/tcp    open   netbios-ssn
 445/tcp    open   microsoft-ds
 512/tcp    open   exec
 513/tcp    open   login
 514/tcp    open   shell
 1099/tcp   open   rmiregistry
 1524/tcp   open   ingreslock
 2049/tcp   open   nfs
 2121/tcp   open   ccproxy-ftp
 3306/tcp   open   mysql
 3632/tcp   open   distccd
 5432/tcp   open   postgresql
 5900/tcp   open   vnc
 6000/tcp   open   X11
 6667/tcp   open   irc
 6697/tcp   open   ircs-u
 8009/tcp   open   ajp13
 8180/tcp   open   unknown
 8787/tcp   open   msgsrvr
 41191/tcp open    unknown
 48963/tcp open    unknown
 49398/tcp open    unknown
 57314/tcp open    unknown
 MAC Address: 08:00:27:CE:91:3C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

 Nmap done: 1 IP address (1 host up) scanned in 4.72 seconds

 ┌──(root㉿kali)-[/home]
 └─# 
```