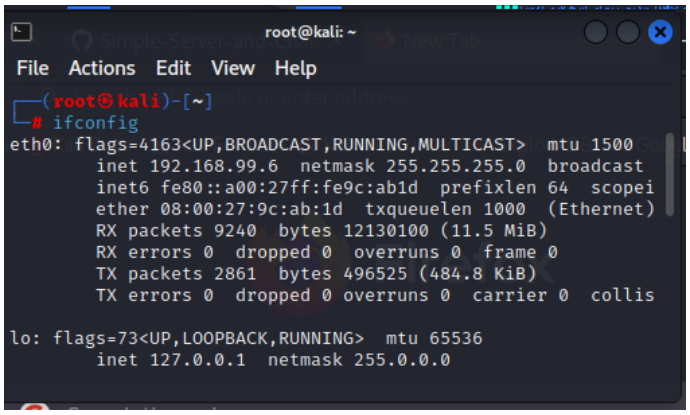
Basic Networking Commands Usage

1. **ifconfig command usage**

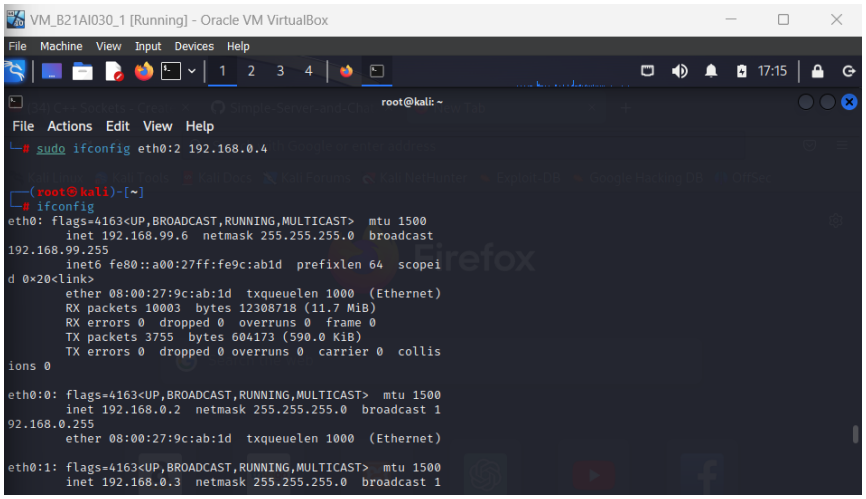
   a. The ifconfig command is used to configure network interfaces and display their current configuration.

   b.Two



   c.To change the IP address, you can use command:-**sudo ifconfig eth0 <new-ip-address> netmask <subnet-mask>**

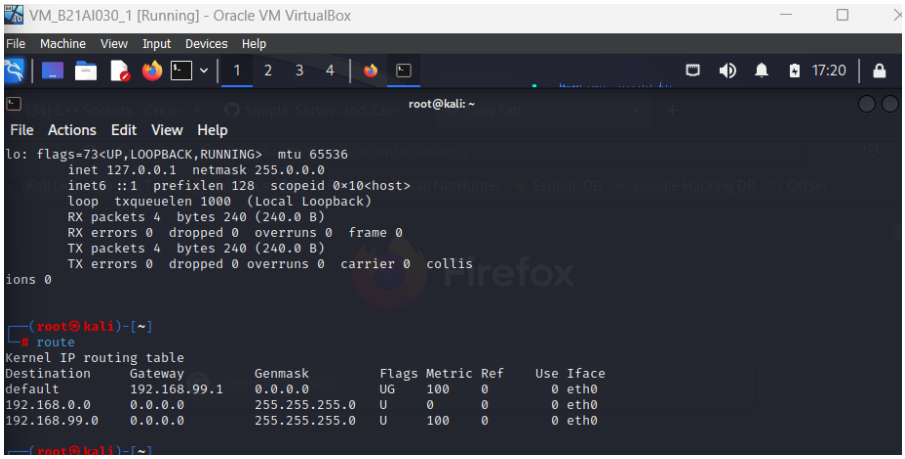
   d.Virtual IP addresses are additional IP addresses that can be assigned to a single network interface. To add virtual IP addresses to interface using ifconfig, you can use the following commands:
   sudo ifconfig eth0:0 <ip-address-1>



2. route command usage

a. The route command **allows you to make manual entries into the network routing tables.**

b. When you enter the "route" command in the terminal, it will display the routing table which contains information about the network destinations and their associated gateways and interfaces.



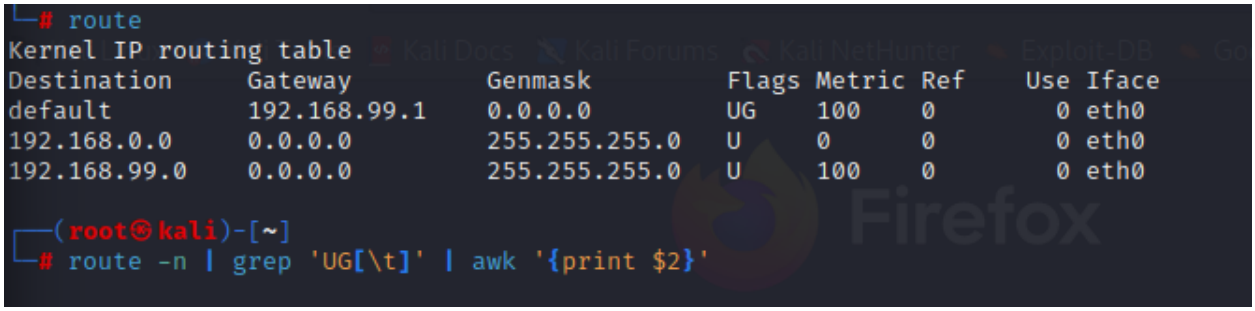
c. To find out the address of the gateway to which your WiFi interface would forward packets, you can use the following command:

route -n | grep 'UG[\t]' | awk '{print $2}'

You can use the `route` command to check the default gateway for your WiFi interface.

Open a terminal and type the following command:

route -n



```
┌──(root㉿kali)-[~]
└─# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.99.1    0.0.0.0         UG    100    0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.99.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

d.Here are three uses of the route command:

a. Adding a new route to the routing table: `sudo route add -net <destination-ip-address> netmask <netmask> gw <gateway-ip-address> dev <interface>`
b. Deleting a route from the routing table: `sudo route del -net <destination-ip-address> netmask <netmask> gw <gateway-ip-address> dev <interface>`
c. Displaying the routing table in human-readable format: `route -n`
d. `Reject Routing to a Particular Host or Network`

3. arp command usage

a. The `arp` command is used to display and manipulate the kernel's ARP cache.It is similar to the ping command, but instead of using ICMP packets, it uses ARP packets. Some of the flags that can be used with `arp` command are:

- `-a`: Display the ARP cache.
- `-s`: Add a static ARP table entry.
- `-d`: Delete an entry from the ARP cache.

```
┌──(root㉿kali)-[~]
└─# arp -a
? (192.168.99.1) at 52:54:00:12:35:00 [ether] on eth0
? (192.168.99.3) at 08:00:27:1c:11:21 [ether] on eth0
```

```
┌──(root㉿kali)-[~]
└─# sudo arp -s 192.168.0.10 00:11:22:33:44:55

┌──(root㉿kali)-[~]
└─# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.99.1             ether   52:54:00:12:35:00   C                     eth0
192.168.0.10             ether   00:11:22:33:44:55   CM                    eth0
192.168.99.3             ether   08:00:27:1c:11:21   C                     eth0

┌──(root㉿kali)-[~]
└─# arp -d 192.168.0.1
No ARP entry for 192.168.0.1

┌──(root㉿kali)-[~]
└─# arp -d 192.168.0.10

┌──(root㉿kali)-[~]
└─# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.99.1             ether   52:54:00:12:35:00   C                     eth0
192.168.99.3             ether   08:00:27:1c:11:21   C                     eth0
```

b. No, the `arp` command cannot be used to find the MAC address of a domain name such as www.google.com. The `arp` command works only with IP addresses, and it is used to map an IP address to a MAC address on the local network. In order to find the MAC address of a domain name, you need to perform a DNS lookup to obtain the IP address associated with the domain name, and then use the `arp` command to map the IP address to a MAC address.

4. arping command usage

a. An almost unknown command (mostly because it is not frequently necessary), the **arping** utility performs an action similar to **ping**, but at the Ethernet layer. Where **ping** tests the reachability of an IP address, **arping** reports the reachability and round-trip time of an IP address hosted on the local network. It is primarily used to test whether a specific host is reachable over the network and to determine its MAC address.
b. The arping command is different from the **ping command** in the sense that it operates at the link layer (Layer 2) of the OSI model, whereas the ping command operates at the network layer (Layer 3). The ping command sends ICMP (Internet Control Message Protocol) packets to a remote host to test its connectivity, while the arping command sends ARP packets to a remote host to test its reachability and obtain its MAC address. In other words, the ping command works with IP addresses, while the arping command works with MAC addresses. And, the arping command can be used to test the connectivity of hosts that are not configured to respond to ICMP packets.

5.netstat command usage:

a. The netstat(network statistics) command is used to display various network-related information such as active network connections, routing tables, and network interfaces on a Linux system. It can be used to:

- Display all active network connections and their states.
- Show the routing table for the system.
- Display statistics for network protocols such as TCP, UDP, and ICMP.
- Show the status of network interfaces on the system.
- Displaying routing tables and their information

To filter the netstat command output based on either UDP or TCP protocol,we can use the "-u" option for udp connections and "-t" option for tcp connections, the following command can be used:

netstat -tunap | grep 'udp\|tcp'

This will display all active UDP and TCP connections along with their process IDs and other information.

```
┌──(root㉿kali)-[~]
└─# netstat -tunap | grep 'udp\|tcp'
tcp        0      0 192.168.99.6:44446      34.117.65.55:443        ESTABLISHED 1108/firefox-esr
udp        0      0 192.168.99.6:68         192.168.99.3:67         ESTABLISHED 522/NetworkManager

┌──(root㉿kali)-[~]
└─# netstat -tunap | grep 'udp\|tcp' > netstat_output.txt

┌──(root㉿kali)-[~]
```

Method2:

To store the output in a file:

netstat -a > netstat_output.txt

To filter based on TCP protocol:

netstat -at

To filter based on UDP protocol:

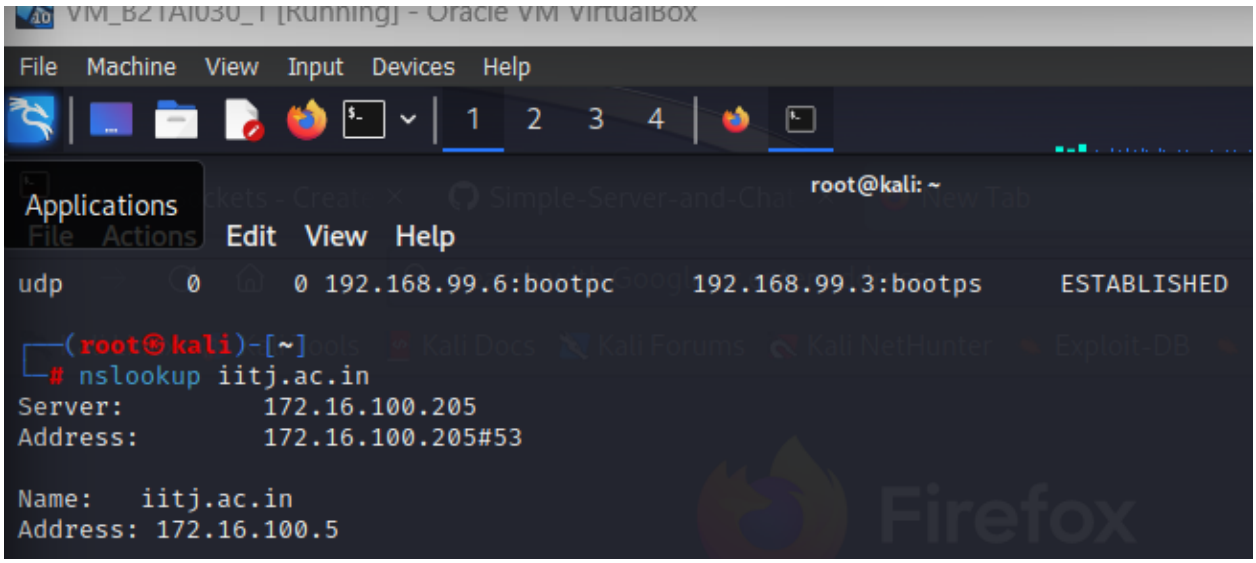
netstat -au

```
└─# netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.99.6:44446      55.65.117.34.bc.g:https ESTABLISHED
tcp        0      0 192.168.99.6:56736      102.115.120.34.bc:https TIME_WAIT
tcp        0      0 192.168.99.6:59158      239.237.117.34.bc:https TIME_WAIT

┌──(root㉿kali)-[~]
└─# netstat -a > netstat_output1.txt

┌──(root㉿kali)-[~]
└─# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.99.6:44446      55.65.117.34.bc.g:https ESTABLISHED

┌──(root㉿kali)-[~]
└─# netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.99.6:bootpc     192.168.99.3:bootps     ESTABLISHED
```

6.nslookup iitj.ac.in

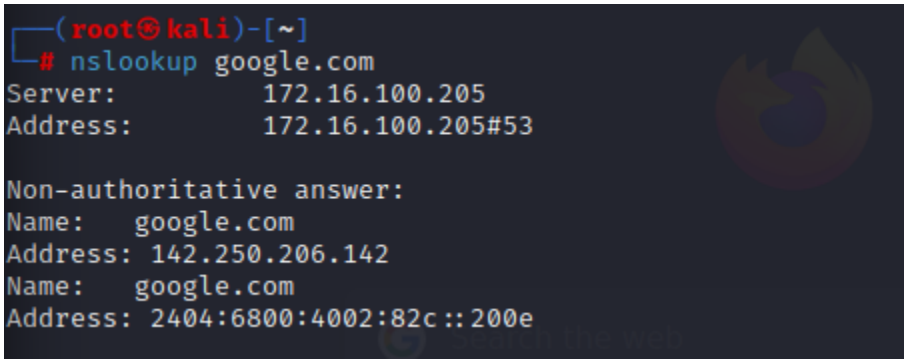
The nslookup command is used to query the Domain Name System (DNS) to obtain domain name or IP address mapping. The output for each of the three cases is as follows:

a. nslookup iitj.ac.in



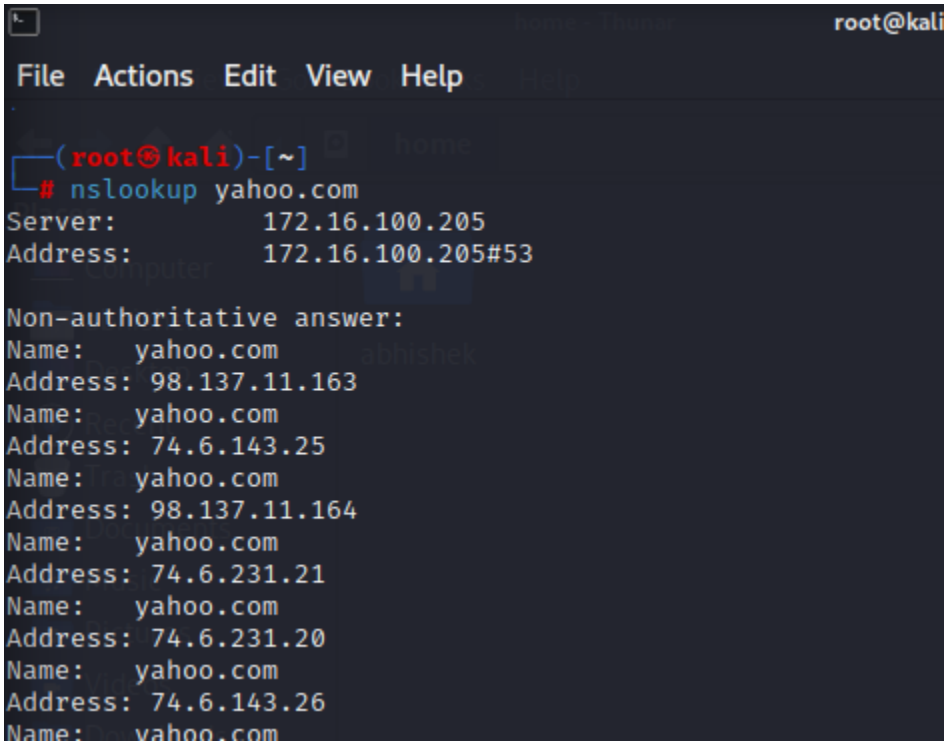
This command queries the DNS server (in this case, the local router at 172.16.100.205) for the IP address associated with the domain name "iitj.ac.in". The output shows that the IP address 172.16.100.5

b. nslookup google.com



This command queries the DNS server for the IP address associated with the domain name "google.com". The output shows that the IP address is 2404:6800:4002:82c::200e

c. nslookup yahoo.com7. ssh and scp. For this part, please use VPN to connect to iitj.



This command queries the DNS server for the IP addresses associated with the domain name "yahoo.com". The output shows that there are multiple IP addresses associated with this domain, including both IPv4 and IPv6 addresses.

7.ssh and scp.

a. The command to login to the home.iitj.ac.in account using ssh is:

   ssh arya.7@home.iitj.ac.in

b. To generate a new RSA key pair using ssh-keygen, follow these steps:

   Type the following command:

   ssh-keygen -t rsa

```
┌──(root㉿kali)-[~]
└─# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): pcs22
pcs22 already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in pcs22
Your public key has been saved in pcs22.pub
The key fingerprint is:
SHA256:XtwqHGRCyvvHZ2U+7ehwdyEXBI49d5O2Gf6ZIS4BioI root@kali
The key's randomart image is:
+---[RSA 3072]----+
|       .       ... |
|    . o      + . .|
|     o . o. . + B.|
|   .   ..+....  = B|
| E  ...  .S o.+o B |
|     .. + o =o.+ *|
|       . * =.+.ooo|
|        . + o.= . |
|           .o .   |
+----[SHA256]-----+
```

c. The scp command to transfer a file from your local machine to the IITJ server is:

scp ~/abhishek/download/pcs22.txt username@home.iitj.ac.in:~/abhishek/Desktop

d. The scp command to transfer a file from the IITJ server to your local machine is:

scp arya.7@home.iitj.ac.in:/abhishek/Downloads /abhishek/to/Desktop

8.traceroute command usage.

a. What is the traceroute command used for?
Ans:- The traceroute command is used to trace the route taken by packets of data from a source to a destination over a network.

b. Can you trace the route a packet is taking from your machine to reach iitj.ac.in? Why or why not?.
Ans:- Yes, you can trace the route a packet is taking from your machine to reach iitj.ac.in using the traceroute command.

c.Is it possible to find the round trip time using this command?
Ans:-Yes, it is possible to find the round trip time using the traceroute command. The round trip time is the time it takes for a packet to travel from the source to the destination and back again.

d.What kind of packets the traditional traceroute uses/sends?.
Ans:-The traditional traceroute uses ICMP (Internet Control Message Protocol) packets to trace the route taken by packets from the source to the destination. ICMP packets are used to send messages between network devices and to report errors.