Mokshada Sawant C-23 20102041

Experiment No. 03

Aim: Using netstat and route commands of Linux. To Perform packet filtering by enabling IP forwarding using IPtables in Linux.

Outcomes:

Method 1: Through the netstat command

```
apsit@apsit-HP-280-G3-MT:~$ netstat -rn
Kernel IP routing table
Destination
                                                 Flags
                                                         MSS Window
                                                                      irtt Iface
                Gateway
                                 Genmask
0.0.0.0
                192.168.192.193 0.0.0.0
                                                 UG
                                                            0 0
                                                                         0 enp4s0
169.254.0.0
                0.0.0.0
                                 255.255.0.0
                                                            0 0
                                                                         0 enp4s0
                                                 Ü
                                                                         0 enp4s0
192.168.0.0
                0.0.0.0
                                 255.255.0.0
                                                 U
                                                            0
                                                             0
apsit@apsit-HP-280-G3-MT:~$
```

Method 2: Through the route command

```
apsit@apsit-HP-280-G3-MT:~$ route -n
Kernel IP routing table
Destination
                                                   Flags Metric Ref
                                                                        Use Iface
                 Gateway
                                 Genmask
0.0.0.0
                 192.168.192.193 0.0.0.0
                                                   UG
                                                         100
                                                                0
                                                                          0 enp4s0
169.254.0.0
                 0.0.0.0
                                 255.255.0.0
                                                   U
                                                         1000
                                                                0
                                                                          0 enp4s0
192.168.0.0
                 0.0.0.0
                                 255.255.0.0
                                                   П
                                                         100
                                                                0
                                                                          0 enp4s0
```

Method 3: Through the ip route command

```
apsit@apsit-HP-280-G3-MT:~$ ip route
default via 192.168.192.193 dev enp4s0 proto static metric 100
169.254.0.0/16 dev enp4s0 scope link metric 1000
192.168.0.0/16 dev enp4s0 proto kernel scope link src 192.168.99.6 metric 100
apsit@apsit-HP-280-G3-MT:~$
```

Adding a static route using IP command

```
apsit@apsit-HP-280-G3-MT:~$ sudo ip route add 10.0.2.0 via 192.168.43.223 dev enp4s0
apsit@apsit-HP-280-G3-MT:~$ route -n
Kernel IP routing table
                                                  Flags Metric Ref
Destination
                Gateway
                                 Genmask
                                                                       Use Iface
0.0.0.0
                192.168.192.193 0.0.0.0
                                                                         0 enp4s0
                                                  UG
                                                        20100 0
10.0.2.0
                192.168.43.223 255.255.255.255 UGH
                                                                0
                                                        0
                                                                         0 enp4s0
169.254.0.0
                0.0.0.0
                                 255.255.0.0
                                                  U
                                                         1000
                                                                0
                                                                         0 enp4s0
192.168.0.0
                0.0.0.0
                                 255.255.0.0
                                                                0
                                                                         0 enp4s0
                                                  U
                                                        100
apsit@apsit-HP-280-G3-MT:~$ sudo ip route add 10.0.2.0/24 via 192.168.43.223 dev enp4s0
apsit@apsit-HP-280-G3-MT:~$ route -n
Kernel IP routing table
Destination
                Gateway
                                                  Flags Metric Ref
                                                                       Use Iface
0.0.0.0
                192.168.192.193 0.0.0.0
                                                  UG
                                                        20100
                                                                0
                                                                         0 enp4s0
                192.168.43.223 255.255.255.255 UGH
192.168.43.223 255.255.255.0 UG
10.0.2.0
                                                        0
                                                                0
                                                                         0 enp4s0
10.0.2.0
                                                        0
                                                                0
                                                                         0 enp4s0
169.254.0.0
                0.0.0.0
                                 255.255.0.0
                                                  U
                                                         1000
                                                                0
                                                                         0 enp4s0
                                 255.255.0.0
                                                                0
192.168.0.0
                0.0.0.0
                                                  U
                                                         100
                                                                         0 enp4s0
apsit@apsit-HP-280-G3-MT:~$
```

Deleting a static route using IP command

```
apsit@apsit-HP-280-G3-MT:~$ sudo ip route delete 10.0.2.0 via 192.168.43.223 dev enp4s0
apsit@apsit-HP-280-G3-MT:~$ route -n
Kernel IP routing table
Destination
                Gateway
                                Genmask
                                                 Flags Metric Ref
                                                                     Use Iface
                192.168.192.193 0.0.0.0
0.0.0.0
                                                       20100
                                                                       0 enp4s0
                                                 UG
                                                              0
10.0.2.0
                                                                        0 enp4s0
                192.168.43.223 255.255.255.0
                                                 UG
                                                       0
                                                              0
                0.0.0.0
                                255.255.0.0
169.254.0.0
                                                 U
                                                       1000
                                                              0
                                                                        0 enp4s0
                                255.255.0.0
                                                              0
                                                                        0 enp4s0
192.168.0.0
                0.0.0.0
                                                 Ü
                                                       100
```

To set default gateway-

apsit@apsit-H Kernel IP rou	P-280-G3-MT:~\$ rou ting table	te-n					
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192,168,1,254	0.0.0.0	UG	0	0	0	enp4s0
0.0.0.0	192.168.192.193	0.0.0.0	UG	20100	0	0	enp4s0
10.0.2.0	192.168.43.223	255.255.255.0	UG	0	0	0	enp4s0
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	enp4s0
192.168.0.0	0.0.0.0	255.255.0.0	U	100	0	0	enp4s0



This site can't be reached

http://google.com/ is unreachable.

ERR_ADDRESS_UNREACHABLE

Reload

To delete default gateway-

```
apsit@apsit-HP-280-G3-MT:~$ sudo route delete default gw 192.168.1.254
apsit@apsit-HP-280-G3-MT:~$ route -n
Kernel IP routing table
                                                                       Use Iface
Destination
                Gateway
                                 Genmask
                                                  Flags Metric Ref
0.0.0.0
                192.168.192.193 0.0.0.0
                                                  UG
                                                        20100
                                                               0
                                                                         0 enp4s0
10.0.2.0
                192.168.43.223
                                 255.255.255.0
                                                  UG
                                                        0
                                                               0
                                                                         0 enp4s0
169.254.0.0
                0.0.0.0
                                 255.255.0.0
                                                  U
                                                        1000
                                                               0
                                                                         0 enp4s0
                                                                         0 enp4s0
192.168.0.0
                0.0.0.0
                                 255.255.0.0
                                                  U
                                                        100
                                                               0
```



To check current iptable rule-

```
apsit@apsit-HP-280-G3-MT:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

To drop forward chain-(It drops packets for router)

```
apsit@apsit-HP-280-G3-MT:~$ sudo iptables -P FORWARD DROP
apsit@apsit-HP-280-G3-MT:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy DROP)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

To drop packets incoming from specific ip address-

```
apsit@apsit-HP-280-G3-MT:~S sudo iptables -A INPUT -s 192.168.0.23 -i DROP
apsit@apsit-HP-280-G3-MT:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source
                                        destination
          all -- 192.168.0.23
DROP
                                        anywhere
Chain FORWARD (policy ACCEPT)
target
          prot opt source
                                        destination
Chain OUTPUT (policy ACCEPT)
target
          prot opt source
                                        destination
```

To drop packets from particular network:

```
apsit@apsit-HP-280-G3-MT:~$ sudo iptables -A INPUT -s 192.168.0.23 -p tcp --destination-port 25 -j DROP
apsit@apsit-HP-280-G3-MT:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
          prot opt source
                                       destination
target
          all -- 192.168.0.23
DROP
                                       anvwhere
          tcp -- 192.168.0.23
                                       anywhere
          tcp -- 192.168.0.23
DROP
                                       anywhere
                                                           tcp dpt:smtp
Chain FORWARD (policy ACCEPT)
          prot opt source
                                       destination
target
Chain OUTPUT (policy ACCEPT)
target prot opt source
                                       destination
```