Name: **Mareena Fernandes**
Roll No.: **8669**
Class: **TE IT**
Batch: **B**

EXPERIMENT NO: 5

1)

```
mareenalinux@mareenalinux:~Desktop$ sudo ufw status
[sudo] password for linux:
Status: inactive
```

2)

```
mareenalinux@mareenalinux:~Desktop$ sudo ufw enable
Firewall is active and enabled on system startup
```

3)

```
mareenalinux@mareenalinux:~Desktop$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ufw-before-logging-input  all  --  anywhere             anywhere
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere
ufw-after-logging-input  all  --  anywhere             anywhere
ufw-reject-input  all  --  anywhere             anywhere
ufw-track-input  all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ufw-before-logging-forward  all  --  anywhere             anywhere
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere
ufw-after-logging-forward  all  --  anywhere             anywhere
ufw-reject-forward  all  --  anywhere             anywhere
ufw-track-forward  all  --  anywhere             anywhere
```

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-output  all  --  anywhere             anywhere
ufw-before-output  all  --  anywhere             anywhere
ufw-after-output  all  --  anywhere             anywhere
ufw-after-logging-output  all  --  anywhere             anywhere
ufw-reject-output  all  --  anywhere             anywhere
ufw-track-output  all  --  anywhere             anywhere

Chain ufw-after-forward (1 references)
target     prot opt source               destination

Chain ufw-after-input (1 references)
target     prot opt source               destination
ufw-skip-to-policy-input  udp  --  anywhere             anywhere             udp dpt:netbios-ns
ufw-skip-to-policy-input  udp  --  anywhere             anywhere             udp dpt:netbios-dgm
ufw-skip-to-policy-input  tcp  --  anywhere             anywhere             tcp dpt:netbios-ssn
ufw-skip-to-policy-input  tcp  --  anywhere             anywhere             tcp dpt:microsoft-ds
ufw-skip-to-policy-input  udp  --  anywhere             anywhere             udp dpt:bootps
ufw-skip-to-policy-input  udp  --  anywhere             anywhere             udp dpt:bootpc
ufw-skip-to-policy-input  all  --  anywhere             anywhere             ADDRTYPE match dst-type
BROADCAST

Chain ufw-after-logging-forward (1 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
"[UFW BLOCK] "

Chain ufw-after-logging-input (1 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
"[UFW BLOCK] "

Chain ufw-after-logging-output (1 references)
target     prot opt source               destination
```

```
Chain ufw-after-output (1 references)
target     prot opt source               destination

Chain ufw-before-forward (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere             icmp destination-unreachable
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded
ACCEPT     icmp --  anywhere             anywhere             icmp parameter-problem
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ufw-user-forward  all  --  anywhere             anywhere

Chain ufw-before-input (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ufw-logging-deny  all  --  anywhere             anywhere             ctstate INVALID
DROP       all  --  anywhere             anywhere             ctstate INVALID
ACCEPT     icmp --  anywhere             anywhere             icmp destination-unreachable
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded
ACCEPT     icmp --  anywhere             anywhere             icmp parameter-problem
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     udp  --  anywhere             anywhere             udp spt:bootps dpt:bootpc
ufw-not-local  all  --  anywhere             anywhere
ACCEPT     udp  --  anywhere             224.0.0.251          udp dpt:mdns
ACCEPT     udp  --  anywhere             239.255.255.250      udp dpt:1900
ufw-user-input  all  --  anywhere             anywhere

Chain ufw-before-logging-forward (1 references)
target     prot opt source               destination

Chain ufw-before-logging-input (1 references)
target     prot opt source               destination

Chain ufw-before-logging-output (1 references)
target     prot opt source               destination
```

```
Chain ufw-before-output (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ufw-user-output  all  --  anywhere             anywhere

Chain ufw-logging-allow (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
"[UFW ALLOW] "

Chain ufw-logging-deny (2 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere             ctstate INVALID limit: avg 3/min burst 10
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
"[UFW BLOCK] "

Chain ufw-not-local (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere             ADDRTYPE match dst-type LOCAL
RETURN     all  --  anywhere             anywhere             ADDRTYPE match dst-type MULTICAST
RETURN     all  --  anywhere             anywhere             ADDRTYPE match dst-type BROADCAST
ufw-logging-deny  all  --  anywhere             anywhere             limit: avg 3/min burst 10
DROP       all  --  anywhere             anywhere

Chain ufw-reject-forward (1 references)
target     prot opt source               destination

Chain ufw-reject-input (1 references)
target     prot opt source               destination

Chain ufw-reject-output (1 references)
target     prot opt source               destination

Chain ufw-skip-to-policy-forward (0 references)
```

```
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain ufw-skip-to-policy-input (7 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain ufw-skip-to-policy-output (0 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain ufw-track-forward (1 references)
target     prot opt source               destination

Chain ufw-track-input (1 references)
target     prot opt source               destination

Chain ufw-track-output (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             ctstate NEW
ACCEPT     udp  --  anywhere             anywhere             ctstate NEW

Chain ufw-user-forward (1 references)
target     prot opt source               destination

Chain ufw-user-input (1 references)
target     prot opt source               destination

Chain ufw-user-limit (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 5 LOG level warning prefix "[UFW
LIMIT BLOCK] "
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-unreachable

Chain ufw-user-limit-accept (0 references)
target     prot opt source               destination
```

```
ACCEPT     all  --  anywhere             anywhere

Chain ufw-user-logging-forward (0 references)
target     prot opt source               destination

Chain ufw-user-logging-input (0 references)
target     prot opt source               destination

Chain ufw-user-logging-output (0 references)
target     prot opt source               destination

Chain ufw-user-output (1 references)
target     prot opt source               destination
```

4)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

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

5)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -t mangle -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

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

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

6)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -t raw -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

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

7)

```
mareenalinux@mareenalinux:~Desktop$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=63 time=19.3 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=63 time=3.26 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=63 time=3.08 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=63 time=5.18 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=63 time=3.27 ms
^Z
[1]+  Stopped                 ping 192.168.0.1
```

8)

```
mareenalinux@mareenalinux:~Desktop$ ping 34.69.218.223
PING 34.69.218.223 (34.69.218.223) 56(84) bytes of data.
```

```
64 bytes from 34.69.218.223: icmp_seq=1 ttl=54 time=362 ms
64 bytes from 34.69.218.223: icmp_seq=2 ttl=54 time=288 ms
64 bytes from 34.69.218.223: icmp_seq=3 ttl=54 time=357 ms
64 bytes from 34.69.218.223: icmp_seq=4 ttl=54 time=268 ms
64 bytes from 34.69.218.223: icmp_seq=5 ttl=54 time=264 ms
^C
--- 34.69.218.223 ping statistics ---
27 packets transmitted, 27 received, 0% packet loss, time 26261ms
rtt min/avg/max/mdev = 263.104/277.224/362.299/25.076 ms
```

9)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -A INPUT -s 34.69.218.223 -j DROP
```

10)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ufw-before-logging-input  all  --  anywhere             anywhere
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere
ufw-after-logging-input  all  --  anywhere             anywhere
ufw-reject-input  all  --  anywhere             anywhere
ufw-track-input  all  --  anywhere             anywhere
DROP       all  --  223.218.69.34.bc.googleusercontent.com  anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ufw-before-logging-forward  all  --  anywhere             anywhere
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere
ufw-after-logging-forward  all  --  anywhere             anywhere
ufw-reject-forward  all  --  anywhere             anywhere
ufw-track-forward  all  --  anywhere             anywhere
```

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-output  all  --  anywhere             anywhere
ufw-before-output  all  --  anywhere             anywhere
ufw-after-output  all  --  anywhere             anywhere
ufw-after-logging-output  all  --  anywhere             anywhere
ufw-reject-output  all  --  anywhere             anywhere
ufw-track-output  all  --  anywhere             anywhere

Chain ufw-after-forward (1 references)
target     prot opt source               destination

Chain ufw-after-input (1 references)
target     prot opt source               destination
ufw-skip-to-policy-input  udp  --  anywhere             anywhere             udp dpt:netbios-ns
ufw-skip-to-policy-input  udp  --  anywhere             anywhere             udp dpt:netbios-dgm
ufw-skip-to-policy-input  tcp  --  anywhere             anywhere             tcp dpt:netbios-ssn
ufw-skip-to-policy-input  tcp  --  anywhere             anywhere             tcp dpt:microsoft-ds
ufw-skip-to-policy-input  udp  --  anywhere             anywhere             udp dpt:bootps
ufw-skip-to-policy-input  udp  --  anywhere             anywhere             udp dpt:bootpc
ufw-skip-to-policy-input  all  --  anywhere             anywhere             ADDRTYPE match dst-type
BROADCAST

Chain ufw-after-logging-forward (1 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
"[UFW BLOCK] "

Chain ufw-after-logging-input (1 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
"[UFW BLOCK] "

Chain ufw-after-logging-output (1 references)
target     prot opt source               destination
```

```
Chain ufw-after-output (1 references)
target     prot opt source               destination

Chain ufw-before-forward (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere             icmp destination-unreachable
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded
ACCEPT     icmp --  anywhere             anywhere             icmp parameter-problem
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ufw-user-forward  all  --  anywhere             anywhere

Chain ufw-before-input (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ufw-logging-deny  all  --  anywhere             anywhere             ctstate INVALID
DROP       all  --  anywhere             anywhere             ctstate INVALID
ACCEPT     icmp --  anywhere             anywhere             icmp destination-unreachable
ACCEPT     icmp --  anywhere             anywhere             icmp time-exceeded
ACCEPT     icmp --  anywhere             anywhere             icmp parameter-problem
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     udp  --  anywhere             anywhere             udp spt:bootps dpt:bootpc
ufw-not-local  all  --  anywhere             anywhere
ACCEPT     udp  --  anywhere             224.0.0.251          udp dpt:mdns
ACCEPT     udp  --  anywhere             239.255.255.250      udp dpt:1900
ufw-user-input  all  --  anywhere             anywhere

Chain ufw-before-logging-forward (1 references)
target     prot opt source               destination

Chain ufw-before-logging-input (1 references)
target     prot opt source               destination

Chain ufw-before-logging-output (1 references)
target     prot opt source               destination
```

```
Chain ufw-before-output (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ufw-user-output  all  --  anywhere             anywhere

Chain ufw-logging-allow (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
"[UFW ALLOW] "

Chain ufw-logging-deny (2 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere             ctstate INVALID limit: avg 3/min burst 10
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 10 LOG level warning prefix
"[UFW BLOCK] "

Chain ufw-not-local (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere             ADDRTYPE match dst-type LOCAL
RETURN     all  --  anywhere             anywhere             ADDRTYPE match dst-type MULTICAST
RETURN     all  --  anywhere             anywhere             ADDRTYPE match dst-type BROADCAST
ufw-logging-deny  all  --  anywhere             anywhere             limit: avg 3/min burst 10
DROP       all  --  anywhere             anywhere

Chain ufw-reject-forward (1 references)
target     prot opt source               destination

Chain ufw-reject-input (1 references)
target     prot opt source               destination

Chain ufw-reject-output (1 references)
target     prot opt source               destination

Chain ufw-skip-to-policy-forward (0 references)
```

```
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain ufw-skip-to-policy-input (7 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain ufw-skip-to-policy-output (0 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain ufw-track-forward (1 references)
target     prot opt source               destination

Chain ufw-track-input (1 references)
target     prot opt source               destination

Chain ufw-track-output (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             ctstate NEW
ACCEPT     udp  --  anywhere             anywhere             ctstate NEW

Chain ufw-user-forward (1 references)
target     prot opt source               destination

Chain ufw-user-input (1 references)
target     prot opt source               destination

Chain ufw-user-limit (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere             limit: avg 3/min burst 5 LOG level warning prefix "[UFW
LIMIT BLOCK] "
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-unreachable

Chain ufw-user-limit-accept (0 references)
target     prot opt source               destination
```

```
ACCEPT     all  --  anywhere             anywhere

Chain ufw-user-logging-forward (0 references)
target     prot opt source               destination

Chain ufw-user-logging-input (0 references)
target     prot opt source               destination

Chain ufw-user-logging-output (0 references)
target     prot opt source               destination

Chain ufw-user-output (1 references)
target     prot opt source               destination
```

11)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -F
```

12)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain ufw-after-forward (0 references)
target     prot opt source               destination

Chain ufw-after-input (0 references)
target     prot opt source               destination
```

```
Chain ufw-after-logging-forward (0 references)
target     prot opt source               destination

Chain ufw-after-logging-input (0 references)
target     prot opt source               destination

Chain ufw-after-logging-output (0 references)
target     prot opt source               destination

Chain ufw-after-output (0 references)
target     prot opt source               destination

Chain ufw-before-forward (0 references)
target     prot opt source               destination

Chain ufw-before-input (0 references)
target     prot opt source               destination

Chain ufw-before-logging-forward (0 references)
target     prot opt source               destination

Chain ufw-before-logging-input (0 references)
target     prot opt source               destination

Chain ufw-before-logging-output (0 references)
target     prot opt source               destination

Chain ufw-before-output (0 references)
target     prot opt source               destination

Chain ufw-logging-allow (0 references)
target     prot opt source               destination

Chain ufw-logging-deny (0 references)
target     prot opt source               destination
```

```
Chain ufw-not-local (0 references)
target     prot opt source               destination

Chain ufw-reject-forward (0 references)
target     prot opt source               destination

Chain ufw-reject-input (0 references)
target     prot opt source               destination

Chain ufw-reject-output (0 references)
target     prot opt source               destination

Chain ufw-skip-to-policy-forward (0 references)
target     prot opt source               destination

Chain ufw-skip-to-policy-input (0 references)
target     prot opt source               destination

Chain ufw-skip-to-policy-output (0 references)
target     prot opt source               destination

Chain ufw-track-forward (0 references)
target     prot opt source               destination

Chain ufw-track-input (0 references)
target     prot opt source               destination

Chain ufw-track-output (0 references)
target     prot opt source               destination

Chain ufw-user-forward (0 references)
target     prot opt source               destination

Chain ufw-user-input (0 references)
target     prot opt source               destination
```

```
Chain ufw-user-limit (0 references)
target     prot opt source               destination

Chain ufw-user-limit-accept (0 references)
target     prot opt source               destination

Chain ufw-user-logging-forward (0 references)
target     prot opt source               destination

Chain ufw-user-logging-input (0 references)
target     prot opt source               destination

Chain ufw-user-logging-output (0 references)
target     prot opt source               destination

Chain ufw-user-output (0 references)
target     prot opt source               destination
```

13)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -A INPUT -s 34.69.218.223 -j DROP
```

14)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -L INPUT -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    DROP       all  --  34.69.218.223        0.0.0.0/0
```

15)

```
mareenalinux@mareenalinux:~Desktop$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::22a2:11af:4ecb:5311  prefixlen 64  scopeid 0x20<link>
```

```
        ether 08:00:27:13:b3:29  txqueuelen 1000  (Ethernet)
        RX packets 900  bytes 1022000 (1.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 568  bytes 52747 (52.7 KB)
        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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 191  bytes 16030 (16.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 191  bytes 16030 (16.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

16)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -A INPUT -s 34.69.218.223 -j DROP
```

17)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -A INPUT -s 34.69.218.223 -j DROP
```

18)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -A INPUT -s 34.69.218.223/225 -j DROP
iptables v1.8.4 (legacy): invalid mask `225' specified
Try `iptables -h' or 'iptables --help' for more information.
```

19)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -A INPUT -s 34.69.218.223/225 -j ACCEPT
iptables v1.8.4 (legacy): invalid mask `225' specified
Try `iptables -h' or 'iptables --help' for more information.
```

20)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -A INPUT -s 34.69.218.223 -j ACCEPT
```

21)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -L INPUT -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    DROP       all  --  34.69.218.223       0.0.0.0/0
2    DROP       all  --  34.69.218.223       0.0.0.0/0
3    DROP       all  --  34.69.218.223       0.0.0.0/0
4    ACCEPT     all  --  34.69.218.223        0.0.0.0/0
```

22)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -I INPUT 4 -s 10.0.2.15 -j DROP
```

23)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -L INPUT -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    DROP       all  --  34.69.218.223       0.0.0.0/0
2    DROP       all  --  34.69.218.223       0.0.0.0/0
3    DROP       all  --  34.69.218.223       0.0.0.0/0
4    DROP       all  --  10.0.2.15           0.0.0.0/0
5    ACCEPT     all  --  34.69.218.223        0.0.0.0/0
```

24)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -D INPUT 2
```

25)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables -L INPUT -n --line-numbers
```

```
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    DROP       all  --  34.69.218.223       0.0.0.0/0
2    DROP       all  --  34.69.218.223       0.0.0.0/0
3    DROP       all  --  10.0.2.15           0.0.0.0/0
4    ACCEPT     all  --  34.69.218.223       0.0.0.0/0
```

26)

```
mareenalinux@mareenalinux:~Desktop$ sudo  iptables-save
# Generated by iptables-save v1.8.4 on Fri Nov  6 12:34:02 2020
*raw
:PREROUTING ACCEPT [612:43284]
:OUTPUT ACCEPT [325:26159]
COMMIT
# Completed on Fri Nov  6 12:34:02 2020
# Generated by iptables-save v1.8.4 on Fri Nov  6 12:34:02 2020
*mangle
:PREROUTING ACCEPT [618:43896]
:INPUT ACCEPT [618:43896]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [331:26649]
:POSTROUTING ACCEPT [332:26722]
COMMIT
# Completed on Fri Nov  6 12:34:02 2020
# Generated by iptables-save v1.8.4 on Fri Nov  6 12:34:02 2020
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [29:2348]
:POSTROUTING ACCEPT [29:2348]
COMMIT
# Completed on Fri Nov  6 12:34:02 2020
# Generated by iptables-save v1.8.4 on Fri Nov  6 12:34:02 2020
*filter
:INPUT DROP [0:0]
```

```
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:ufw-after-forward - [0:0]
:ufw-after-input - [0:0]
:ufw-after-logging-forward - [0:0]
:ufw-after-logging-input - [0:0]
:ufw-after-logging-output - [0:0]
:ufw-after-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-before-input - [0:0]
:ufw-before-logging-forward - [0:0]
:ufw-before-logging-input - [0:0]
:ufw-before-logging-output - [0:0]
:ufw-before-output - [0:0]
:ufw-logging-allow - [0:0]
:ufw-logging-deny - [0:0]
:ufw-not-local - [0:0]
:ufw-reject-forward - [0:0]
:ufw-reject-input - [0:0]
:ufw-reject-output - [0:0]
:ufw-skip-to-policy-forward - [0:0]
:ufw-skip-to-policy-input - [0:0]
:ufw-skip-to-policy-output - [0:0]
:ufw-track-forward - [0:0]
:ufw-track-input - [0:0]
:ufw-track-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-user-input - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]
:ufw-user-logging-forward - [0:0]
:ufw-user-logging-input - [0:0]
:ufw-user-logging-output - [0:0]
:ufw-user-output - [0:0]
-A INPUT -s 34.69.218.223/32 -j DROP
-A INPUT -s 34.69.218.223/32 -j DROP
```

```
-A INPUT -s 10.0.2.15/32 -j DROP
-A INPUT -s 34.69.218.223/32 -j ACCEPT
COMMIT
# Completed on Fri Nov  6 12:34:02 2020
```

Post labs:

1. What are the three built in rule chains for iptables?

Ans:
IPTables has the following 3 built-in tables.

1. Filter Table

Filter is default table for iptables. So, if you don't define you own table, you'll be using filter table. Iptables's filter table has the following built-in chains.

- INPUT chain – Incoming to firewall. For packets coming to the local server.
- OUTPUT chain – Outgoing from firewall. For packets generated locally and going out of the local server.
- FORWARD chain – Packet for another NIC on the local server. For packets routed through the local server.

2. NAT table

Iptable's NAT table has the following built-in chains.

- PREROUTING chain – Alters packets before routing. That is Packet translation happens immediately after the packet comes to the system (and before routing). This helps to translate the destination ip address of the packets to something that matches the routing on the local server. This is used for DNAT (destination NAT).
- POSTROUTING chain – Alters packets after routing. That is Packet translation happens when the packets are leaving the system. This helps to translate the source IP address of the packets to something that might match the routing on the destination server. This is used for SNAT (source NAT).
- OUTPUT chain – NAT for locally generated packets on the firewall.

3. Mangle table

Iptables's Mangle table is for specialized packet alteration. This alters QOS bits in the TCP header. Mangle table has the following built-in chains.

- PREROUTING chain
- OUTPUT chain
- FORWARD chain
- INPUT chain
- POSTROUTING chain

2. A packet arrives at your router. Its destination is not your machine. You are supposed to send it on. Which rule chain(s) does it use. You may name zero or more chains.

Ans:
The kernel starts with three lists of rules; these lists are called firewall chains or just chains. The three chains are called input, output and forward. When a packet comes in (say, through the Ethernet card) the kernel uses the input chain to decide its fate. If it survives that step, then the kernel decides where to send the packet next (this is called routing). If it is destined for another machine, it consults the forward chain. Finally, just before a packet is to go out, the kernel consults the output chain.

3. What command(s) will clear all rule chains and delete all user made chains?

Ans:
Deleting a chain: ipchains -X chain_name (Deletes all chains if no chain specified)
Deleting rules in a chain: ipchains -X chain_name (Deletes rules in all chains if no chain specified)