Steps to execute Practical 4

Steps to block ICMP ping using OUTPUT chain

Step 1: To show the permission of iptables command.

sudo iptables -L -v

```
kali@kali: ~
                                                                       kali@kali: ~
     Actions Edit View Help
        :-$ sudo iptables -L -v
[sudo] password for kali:
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target
                                                                   destination
                     prot opt in
                                              source
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target
                    prot opt in
                                      out
                                              source
                                                                   destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in wlimbuli:-$
                                                                   destination
                                     out source
```

Step 2: To enable Firewall

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P output ACCEPT

Step 3: To block ICMP ping

sudo iptables -A OUTPUT -s 192.168.200.49 -p icmp --icmp-type echo-reply -j DROP

```
:-$ sudo iptables -P INPUT DROP
:-$ sudo iptables -P FORWARD DROP
:-$ sudo iptables -P output ACCEPT
iptables: Bad built-in chain name.
intiligial:--$ sudo iptables -A OUTPUT -s 192.168.20 -p tcmp-type echo-reply -j DROP
iptables v1.8.5 (nf_tables): unknown protocol "tcmp-type" specified
Try 'iptables -h' or 'iptables -help' for more information.
Interpretation of intentions — neep for more information.

Interpretation — icmp-type echo-reply -j DROP intentional: - s sudo iptables -L -v

Chain INPUT (policy DROP 0 packets, 0 bytes) pkts bytes target prot opt in out source destination
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target
                                      prot opt in
                                                                                   source
                                                                                                                       destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target
0 0 DROP
kaliakali:~$
                                    prot opt in icmp — any
                                                                                                                       destination
                                                                                   source
                                                                    out
                                                                                   192.168.20.0
                                                                                                                        anywhere
                                                                                                                                                             icmp echo-reply
```

Steps to allow all outgoing connections

Step 4: sudo iptables -A INPUT -s 192.168.200.49 -j ACCEPT

```
File Actions Edit View Help
            :-$ sudo iptables -A INPUT -s 192.168.200.49 -j ACCEPT :-$ sudo iptables -L -v
Chain INPUT (policy DROP 5 packets, 1086 bytes)
pkts bytes target prot opt in out s
0 0 ACCEPT all -- any any
                                                                                            destination
                                                                source
                                                               192.168.200.49
                                                                                            anywhere
Chain FORWARD (policy DROP 0 packets, 0 bytes) pkts bytes target prot opt in out
                                                                                            destination
                                                                source
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target
0 0 DROP
                             prot opt in icmp -- any
                                                     out
                                                                source
192.168.20.0
                                                                                            destination
                                                                                                                         icmp echo-reply
                                                                                            anywhere
                                                     any
            :--$
```

Step to block all unwanted incoming connections

Step 1: sudo iptables -L -v

Step 2: sudo iptables -A INPUT -s 192.168.200.49 -j

```
kmli@kali:~$ sudo iptables -A INPUT -s 192.168.200.49 -j ACCEPT
kmli@kali:~$ sudo iptables -L -v
Chain INPUT (policy DROP 5 packets, 1086 bytes)
  pkts bytes target
0 0 ACCEPT
                                      prot opt in
all -- any
                                                                                        source
192.168.200.49
                                                                                                                               destination
                                                                        out
                                                                                                                               anywhere
Chain FORWARD (policy DROP 0 packets, 0 bytes) pkts bytes target prot opt in out
                                                                                                                               destination
                                                                                        source
 Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source
0 0 DROP icmp -- any any 192.168.20.0
kaliakali:-$ sudo iptables -A INPUT -s 192.168.200.49 -j DROP
kaliakali:-$ sudo iptables -A INPUT -s 192.168.200.49 -j ACCEPT
kaliakali:-$ sudo iptables -L -v
Chain INPUT (policy DROP 11 packets, 2089 bytes)
pkts bytes target prot opt in out source
0 0 ACCEPT all -- any any 192.168.200.49
0 0 DROP all -- any any 192.168.200.49
                                                                                                                               destination
                                                                                                                                                                       icmp echo-reply
                                                                                                                               anywhere
                                          prot opt in
all — any
all — any
all — any
                                                                                       source
192.168.200.49
192.168.200.49
192.168.200.49
                                                                                                                               destination
                                                                                                                               anywhere
                  0 DROP
                                                                         апу
                                                                                                                               anywhere
                  0 ACCEPT
                                                                                                                               anywhere
                                                                         апу
Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target
                                        prot opt in
                                                                                        source
                                                                                                                               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
                                                                      out
 pkts bytes target
0 0 DROP
kaliakali:~$
                                        prot opt in
                                                                                                                               destination
                                           icmp -- any
                                                                         any
                                                                                        192.168.20.0
                                                                                                                               anywhere
                                                                                                                                                                       icmp echo-reply
```