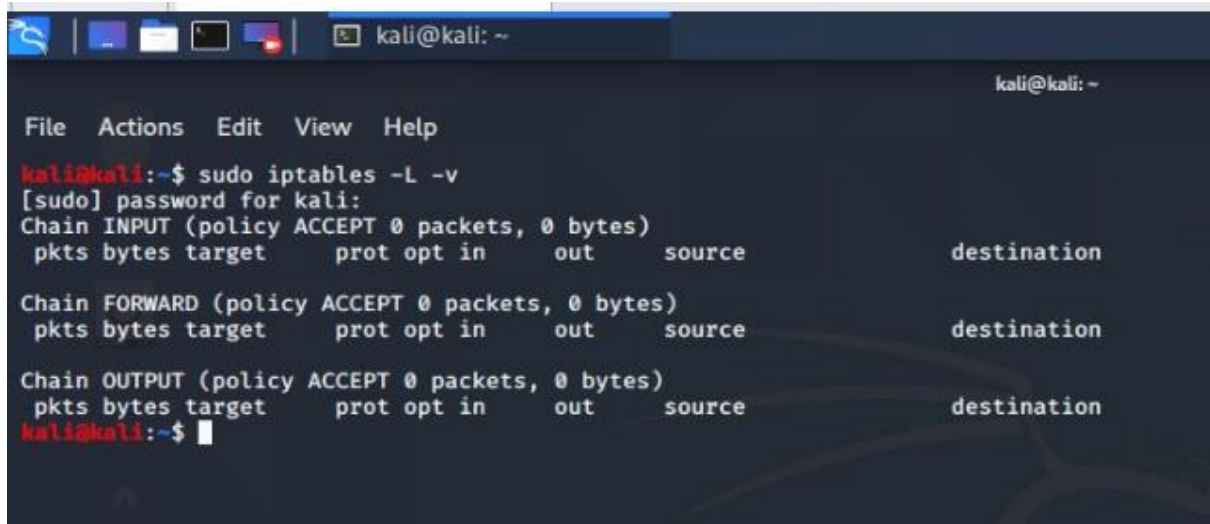


Steps to execute Practical 4

Steps to block ICMP ping using OUTPUT chain

Step 1: To show the permission of iptables command.

`sudo iptables -L -v`



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

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     out     source                   destination
kali@kali:~$
```

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`

```
kali@kali:~$ sudo iptables -P INPUT DROP
kali@kali:~$ sudo iptables -P FORWARD DROP
kali@kali:~$ sudo iptables -P output ACCEPT
iptables: Bad built-in chain name.
kali@kali:~$ sudo iptables -A OUTPUT -s 192.168.200 -p tcp-type echo-reply -j DROP
iptables v1.8.5 (nf_tables): unknown protocol "tcp-type" specified
Try 'iptables -h' or 'iptables --help' for more information.
kali@kali:~$ sudo iptables -A OUTPUT -s 192.168.200 -p icmp --icmp-type echo-reply -j DROP
kali@kali:~$ 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     out     source                   destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source                   destination
    0    0 DROP      icmp -- any    any    192.168.200.0           anywhere                icmp echo-reply
kali@kali:~$
```

Steps to allow all outgoing connections

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

```
File Actions Edit View Help
kali@kali:~$ sudo iptables -A INPUT -s 192.168.200.49 -j ACCEPT
kali@kali:~$ sudo iptables -L -v
Chain INPUT (policy DROP 5 packets, 1086 bytes)
  pkts bytes target    prot opt in     out     source                   destination
    0    0 ACCEPT   all  -- any    any    192.168.200.49           anywhere
Chain FORWARD (policy DROP 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     out     source                   destination
    0    0 DROP      icmp -- any    any    192.168.200.0           anywhere                icmp echo-reply
kali@kali:~$
```

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

```
kali@kali:~$ sudo iptables -A INPUT -s 192.168.200.49 -j ACCEPT
kali@kali:~$ sudo iptables -L -v
Chain INPUT (policy DROP 5 packets, 1086 bytes)
  pkts bytes target     prot opt in     out     source         destination
    0    0 ACCEPT     all  --  any    any    192.168.200.49 anywhere

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

Chain FORWARD (policy DROP 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     out     source         destination
    0    0 DROP      icmp  --  any    any    192.168.20.0   anywhere      icmp echo-reply
kali@kali:~$
```