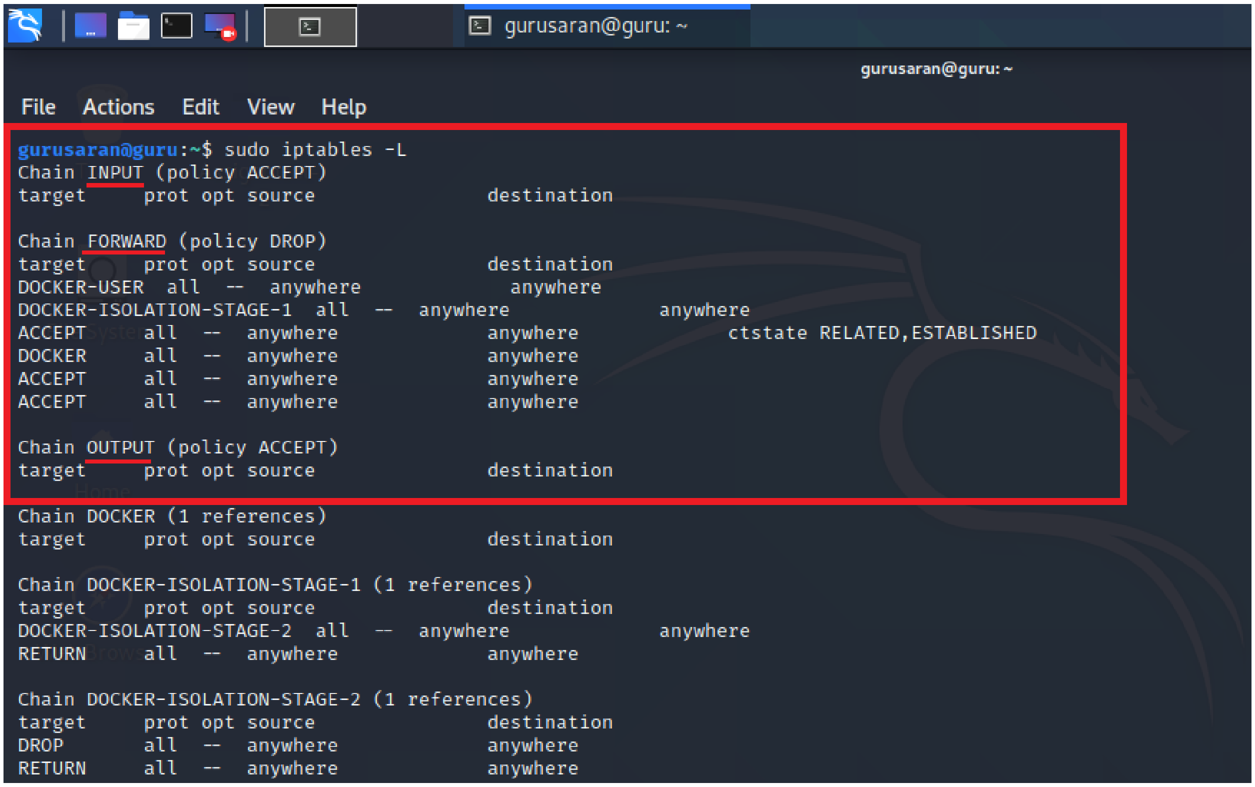
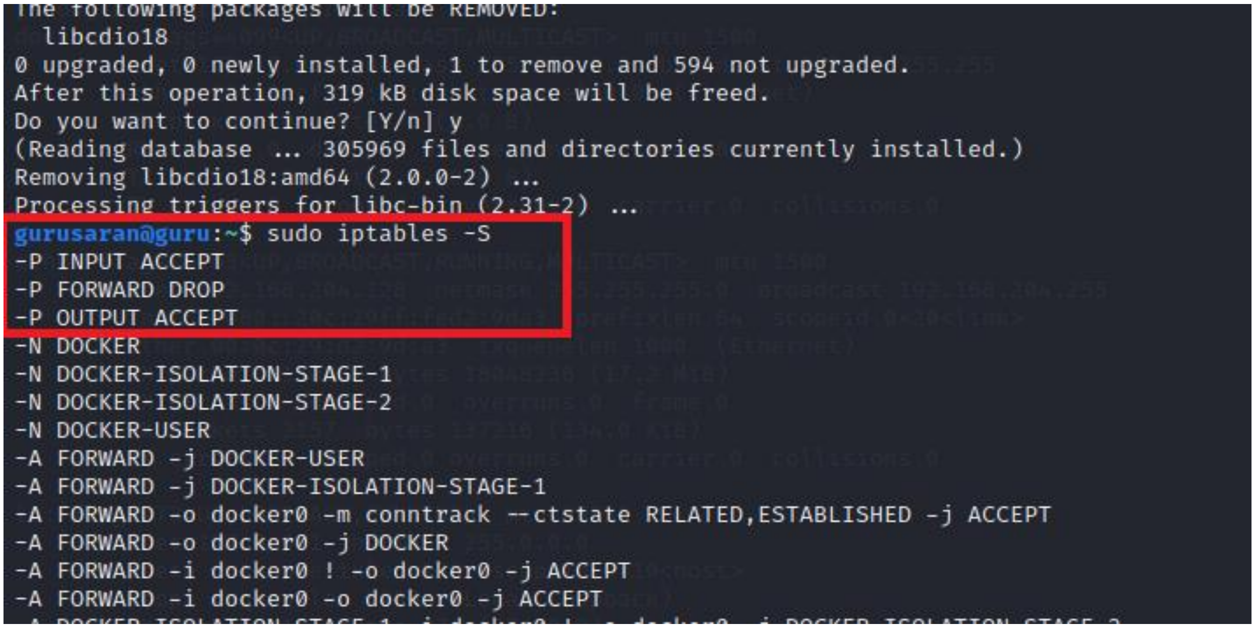
IPTABLES(LAB)

- Listing the iptables and policies



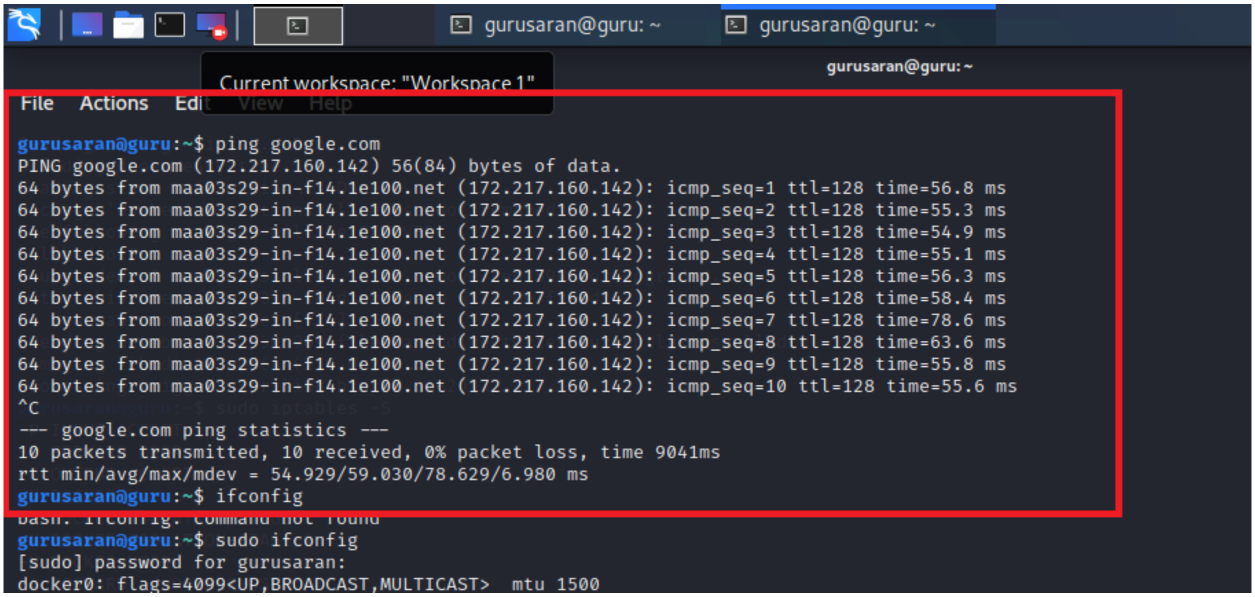
```
gurusaran@guru:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
DOCKER-USER  all  --  anywhere             anywhere
DOCKER-ISOLATION-STAGE-1  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
DOCKER     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain DOCKER (1 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source               destination
DOCKER-ISOLATION-STAGE-2  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere
```

- Listing the chain policy and their target



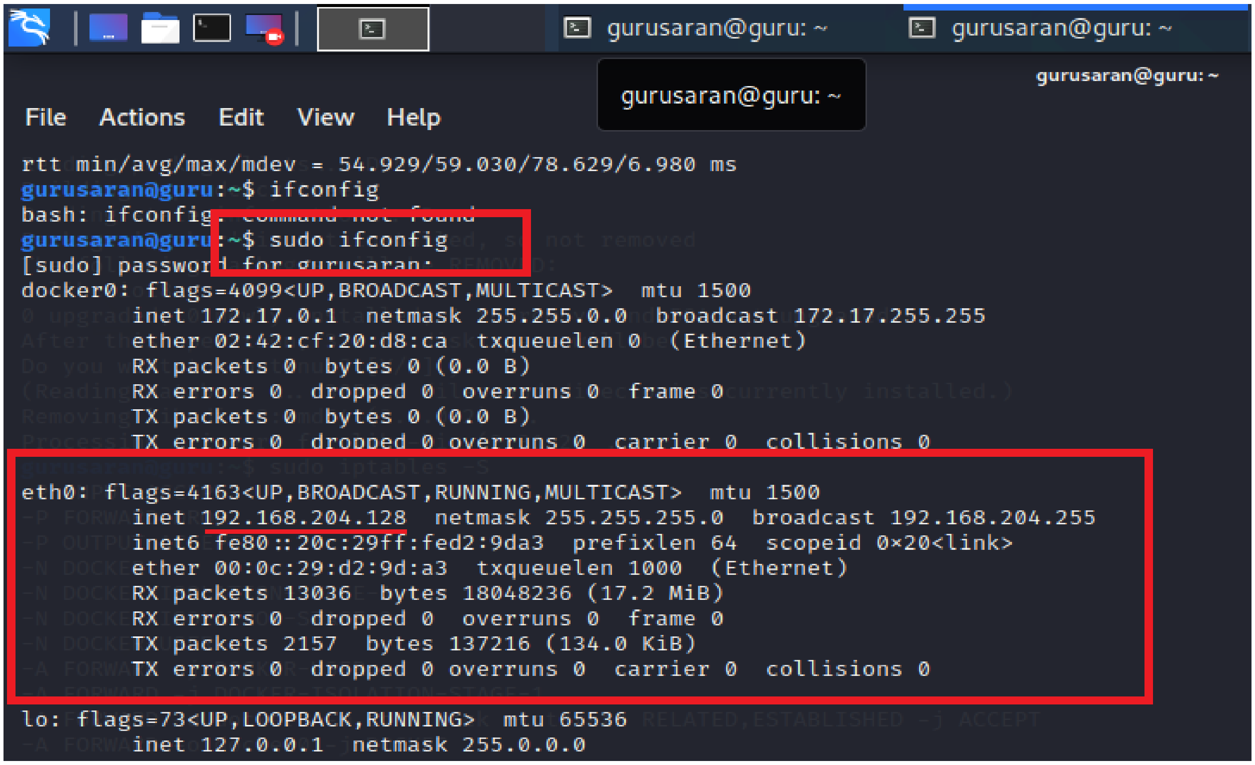
```
The following packages will be REMOVED:
  libcdio18
0 upgraded, 0 newly installed, 1 to remove and 594 not upgraded.
After this operation, 319 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 305969 files and directories currently installed.)
Removing libcdio18:amd64 (2.0.0-2) ...
Processing triggers for libc-bin (2.31-2) ...
gurusaran@guru:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD DROP
-P OUTPUT ACCEPT
-N DOCKER
-N DOCKER-ISOLATION-STAGE-1
-N DOCKER-ISOLATION-STAGE-2
-N DOCKER-USER
-A FORWARD -j DOCKER-USER
-A FORWARD -j DOCKER-ISOLATION-STAGE-1
-A FORWARD -o docker0 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -o docker0 -j DOCKER
-A FORWARD -i docker0 ! -o docker0 -j ACCEPT
-A FORWARD -i docker0 -o docker0 -j ACCEPT
-A DOCKER-ISOLATION-STAGE-1 -i docker0 ! -o docker0 -j DOCKER-ISOLATION-STAGE-2
```

- Checking the network service using ping. The ping command sends packets of data to a specific IP address or domain name on a network.



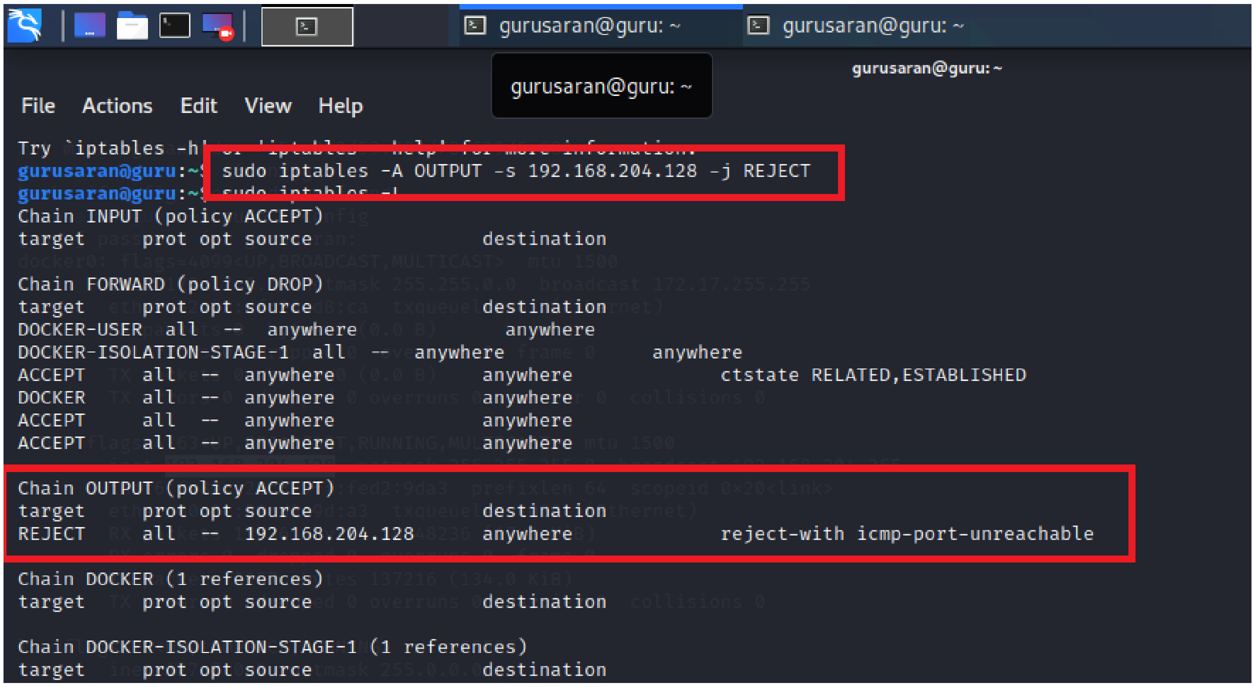
```
gurusaran@guru:~$ ping google.com
PING google.com (172.217.160.142) 56(84) bytes of data.
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=1 ttl=128 time=56.8 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=2 ttl=128 time=55.3 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=3 ttl=128 time=54.9 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=4 ttl=128 time=55.1 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=5 ttl=128 time=56.3 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=6 ttl=128 time=58.4 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=7 ttl=128 time=78.6 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=8 ttl=128 time=63.6 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=9 ttl=128 time=55.8 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=10 ttl=128 time=55.6 ms
^C
--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9041ms
rtt min/avg/max/mdev = 54.929/59.030/78.629/6.980 ms
gurusaran@guru:~$ ifconfig
bash: ifconfig: command not found
gurusaran@guru:~$ sudo ifconfig
[sudo] password for gurusaran:
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
```

Check IP address using ifconfig command



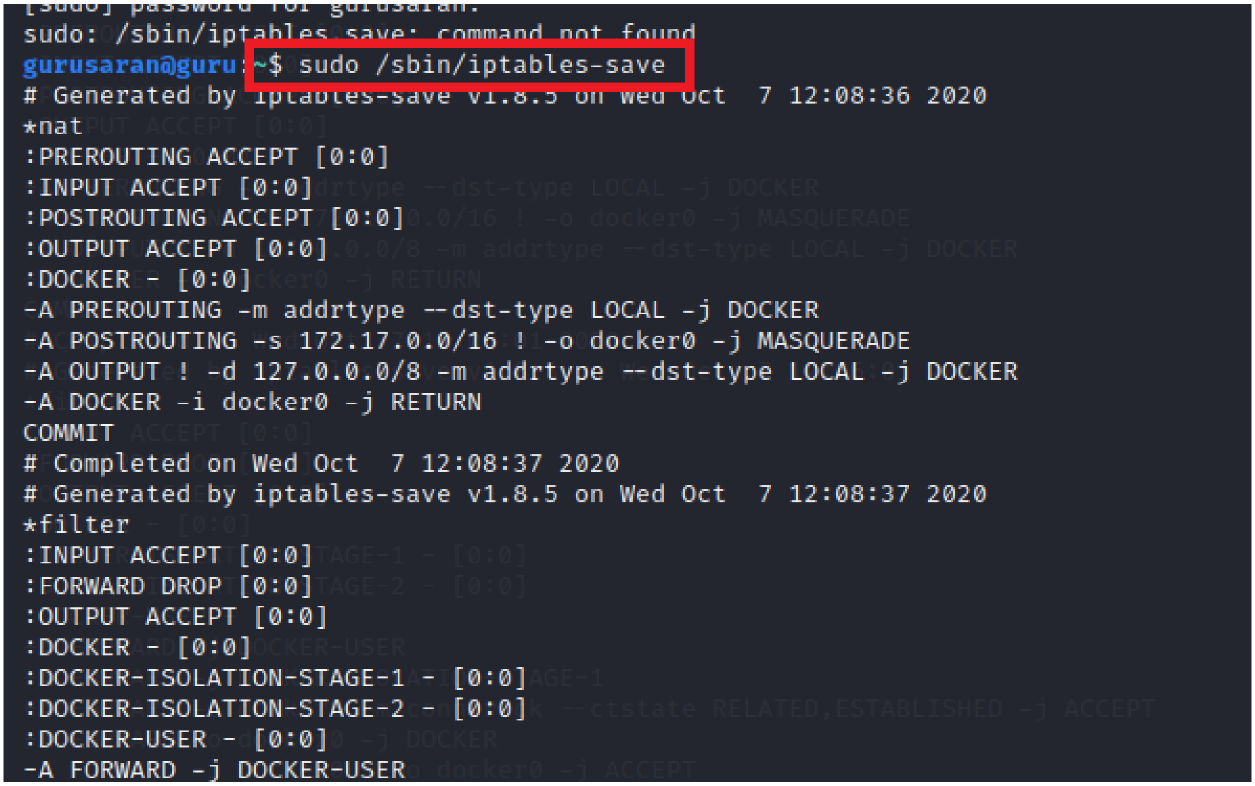
```
rtt min/avg/max/mdev = 54.929/59.030/78.629/6.980 ms
gurusaran@guru:~$ ifconfig
bash: ifconfig: command not found
gurusaran@guru:~$ sudo ifconfig
[sudo] password for gurusaran:
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:cf:20:d8:ca  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.204.128  netmask 255.255.255.0  broadcast 192.168.204.255
        inet6 fe80::20c:29ff:fed2:9da3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d2:9d:a3  txqueuelen 1000  (Ethernet)
        RX packets 13036  bytes 18048236 (17.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2157  bytes 137216 (134.0 KiB)
        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
```

- Blocking/dropping connection for the given IP address



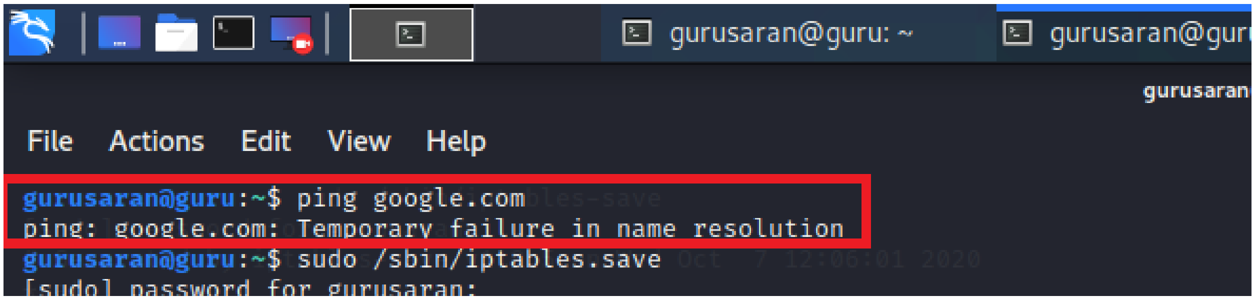
```
Try `iptables -h' or 'iptables --help' for more information.
gurusaran@guru:~$ sudo iptables -A OUTPUT -s 192.168.204.128 -j REJECT
gurusaran@guru:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
DOCKER-USER  all  --  anywhere             anywhere
DOCKER-ISOLATION-STAGE-1  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
DOCKER     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  192.168.204.128      anywhere             reject-with icmp-port-unreachable

Chain DOCKER (1 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source               destination
```

Saving Iptables rules



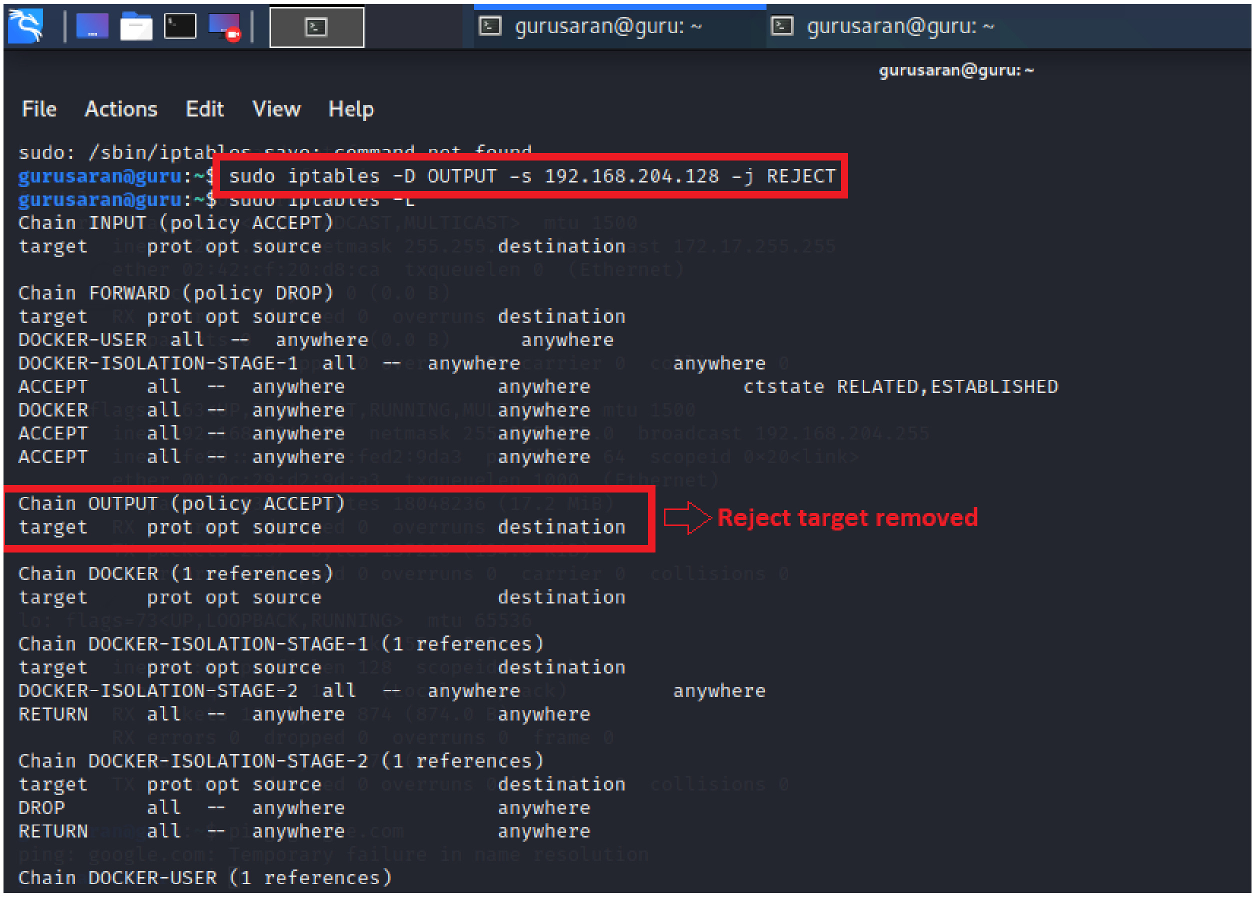
```
[sudo] password for gurusaran:
sudo: /sbin/iptables save: command not found
gurusaran@guru:~$ sudo /sbin/iptables-save
# Generated by iptables-save v1.8.5 on Wed Oct  7 12:08:36 2020
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:DOCKER - [0:0]
-A PREROUTING -m addrtype --dst-type LOCAL -j DOCKER
-A POSTROUTING -s 172.17.0.0/16 ! -o docker0 -j MASQUERADE
-A OUTPUT ! -d 127.0.0.0/8 -m addrtype --dst-type LOCAL -j DOCKER
-A DOCKER -i docker0 -j RETURN
COMMIT
# Completed on Wed Oct  7 12:08:37 2020
# Generated by iptables-save v1.8.5 on Wed Oct  7 12:08:37 2020
*filter
:INPUT ACCEPT [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:DOCKER - [0:0]
:DOCKER-ISOLATION-STAGE-1 - [0:0]
:DOCKER-ISOLATION-STAGE-2 - [0:0]
:DOCKER-USER - [0:0]
-A FORWARD -j DOCKER-USER
```

Check the network service



```
gurusaran@guru:~$ ping google.com
ping: google.com: Temporary failure in name resolution
gurusaran@guru:~$ sudo /sbin/iptables.save
[sudo] password for gurusaran:
```

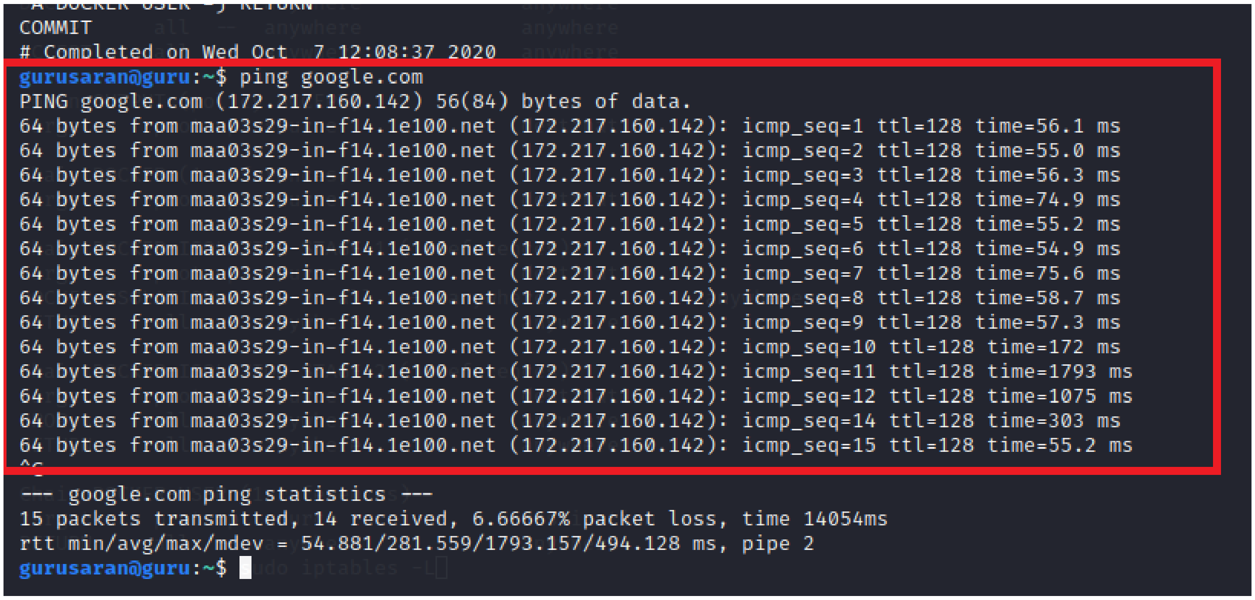
- Deleting the added REJECT rule



```
sudo: /sbin/iptables.save: command not found
gurusaran@guru:~$ sudo iptables -D OUTPUT -s 192.168.204.128 -j REJECT
gurusaran@guru:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
DOCKER-USER  all  --  anywhere             anywhere
DOCKER-ISOLATION-STAGE-1  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
DOCKER     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain DOCKER (1 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source               destination
DOCKER-ISOLATION-STAGE-2  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-USER (1 references)
```

Reject target removed

Checking the network service again



```
-A DOCKER-USER -j RETURN
COMMIT
# Completed on Wed Oct  7 12:08:37 2020
gurusaran@guru:~$ ping google.com
PING google.com (172.217.160.142) 56(84) bytes of data.
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=1 ttl=128 time=56.1 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=2 ttl=128 time=55.0 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=3 ttl=128 time=56.3 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=4 ttl=128 time=74.9 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=5 ttl=128 time=55.2 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=6 ttl=128 time=54.9 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=7 ttl=128 time=75.6 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=8 ttl=128 time=58.7 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=9 ttl=128 time=57.3 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=10 ttl=128 time=172 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=11 ttl=128 time=1793 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=12 ttl=128 time=1075 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=14 ttl=128 time=303 ms
64 bytes from maa03s29-in-f14.1e100.net (172.217.160.142): icmp_seq=15 ttl=128 time=55.2 ms
^C
--- google.com ping statistics ---
15 packets transmitted, 14 received, 6.66667% packet loss, time 14054ms
rtt min/avg/max/mdev = 54.881/281.559/1793.157/494.128 ms, pipe 2
gurusaran@guru:~$ 
```