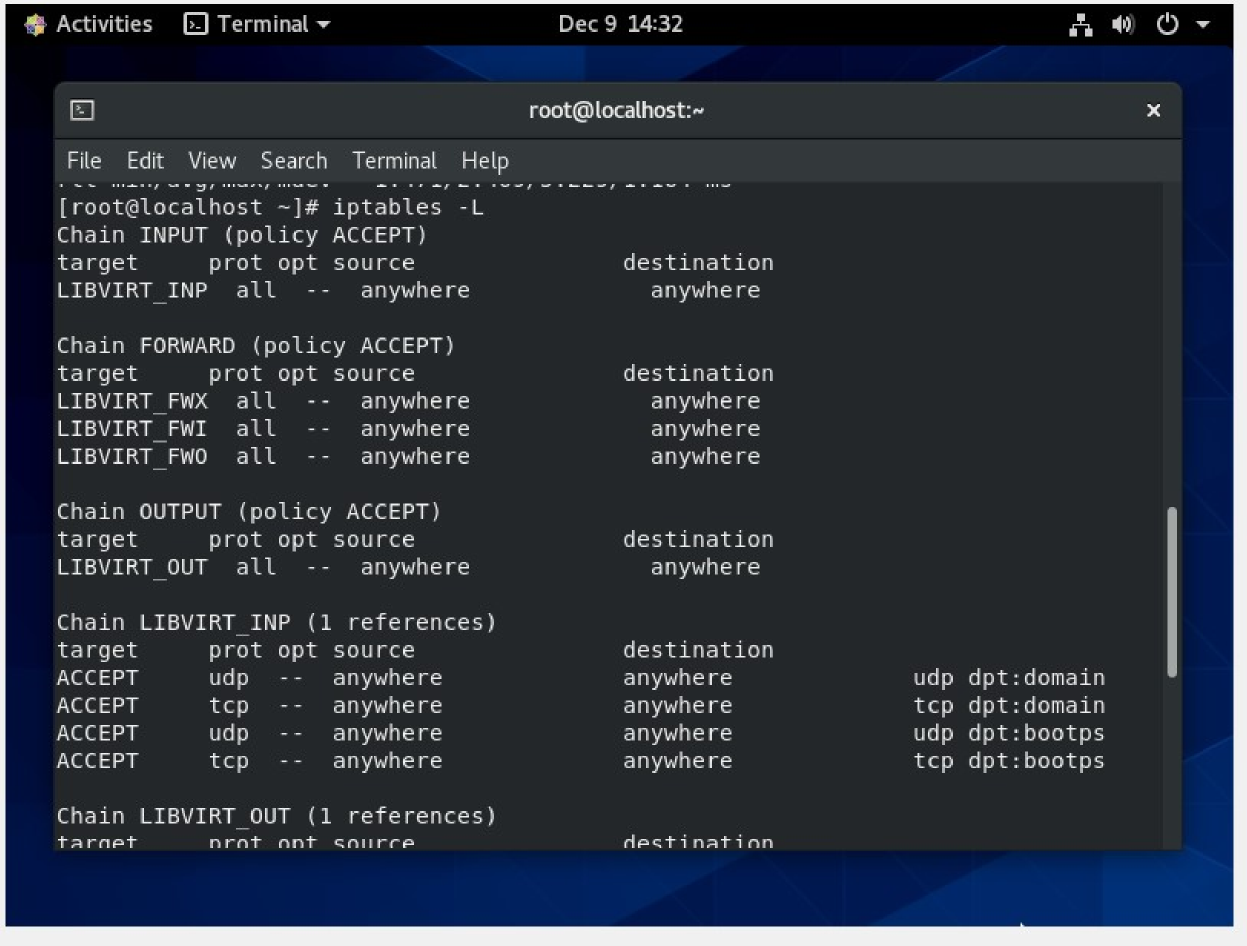
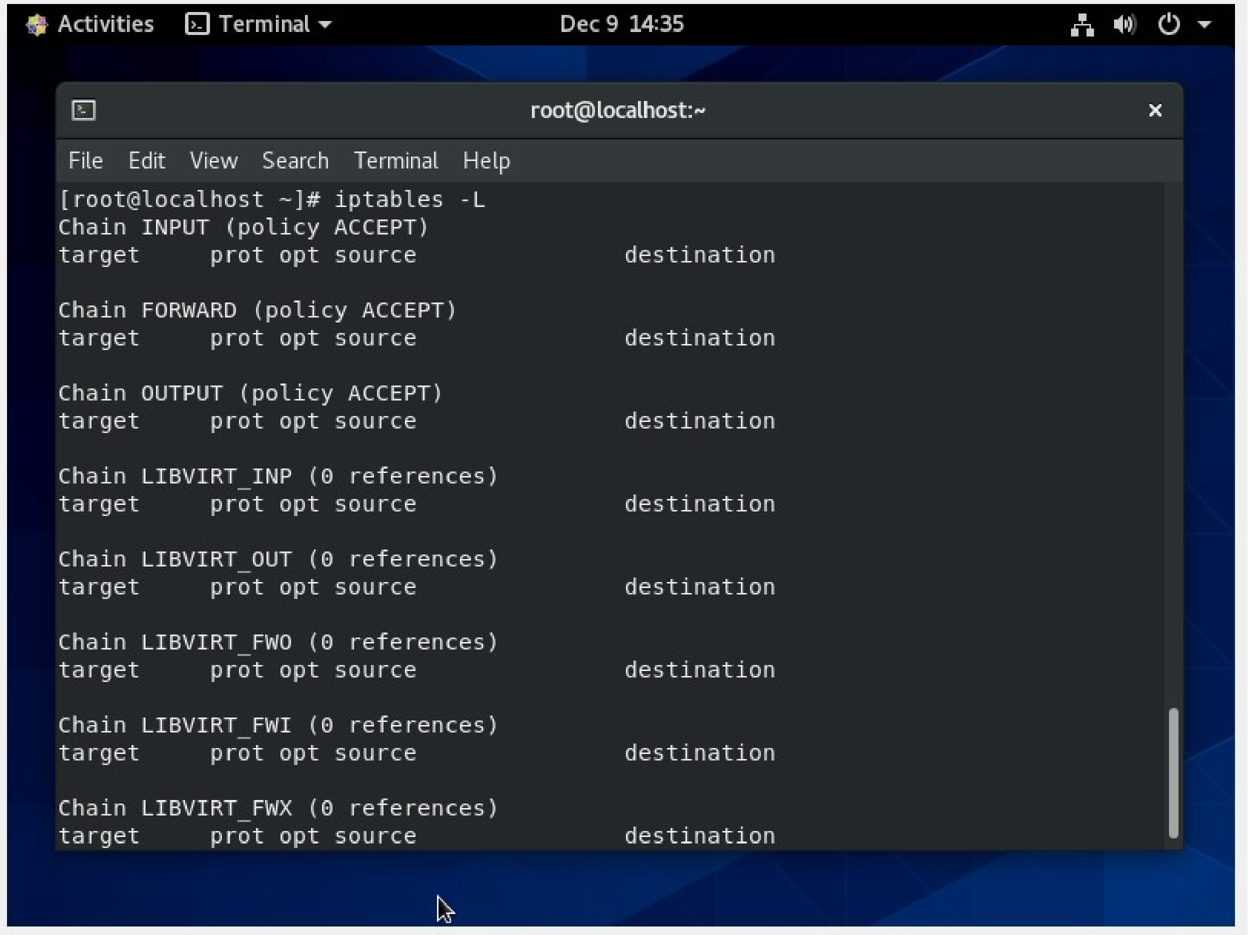
Assignment 2 : Firewall configuration using IPTABLES

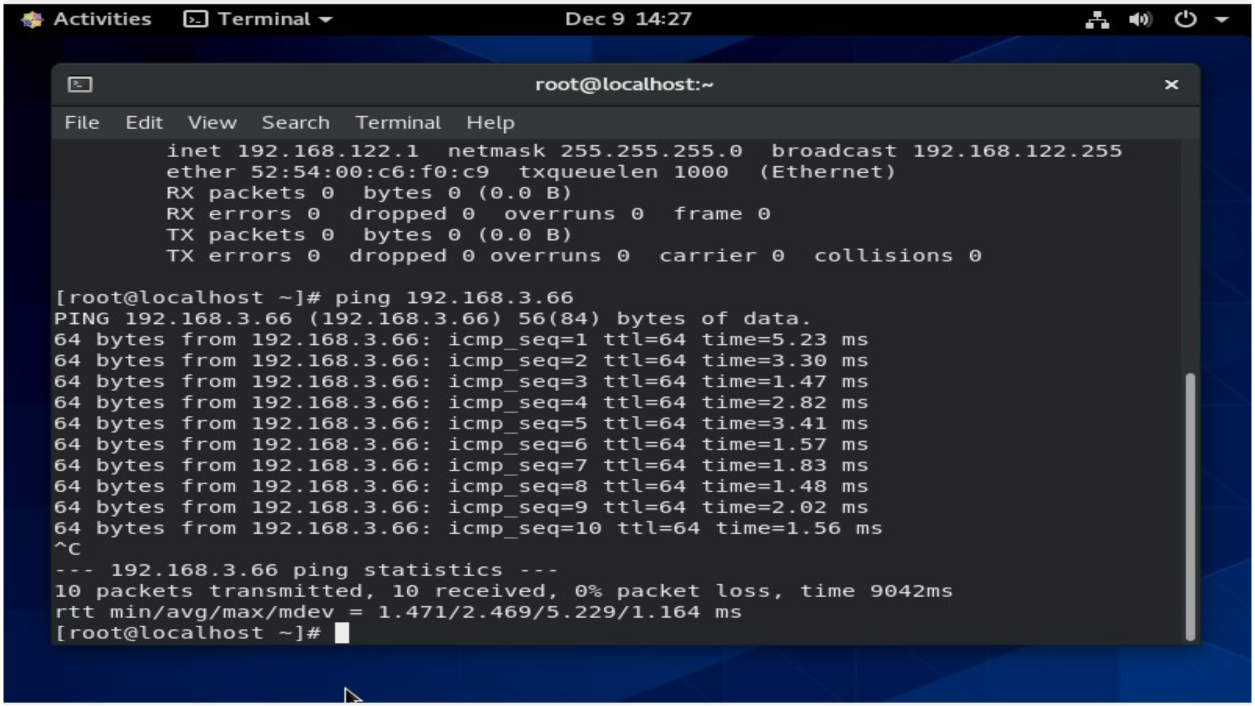
Step 1:List the existing firewall rules and default policy in each chain



```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
LIBVIRT_INP  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
LIBVIRT_FWX  all  --  anywhere             anywhere
LIBVIRT_FWI  all  --  anywhere             anywhere
LIBVIRT_FWO  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
LIBVIRT_OUT  all  --  anywhere             anywhere

Chain LIBVIRT_INP (1 references)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:bootps
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:bootps

Chain LIBVIRT_OUT (1 references)
target     prot opt source               destination
```

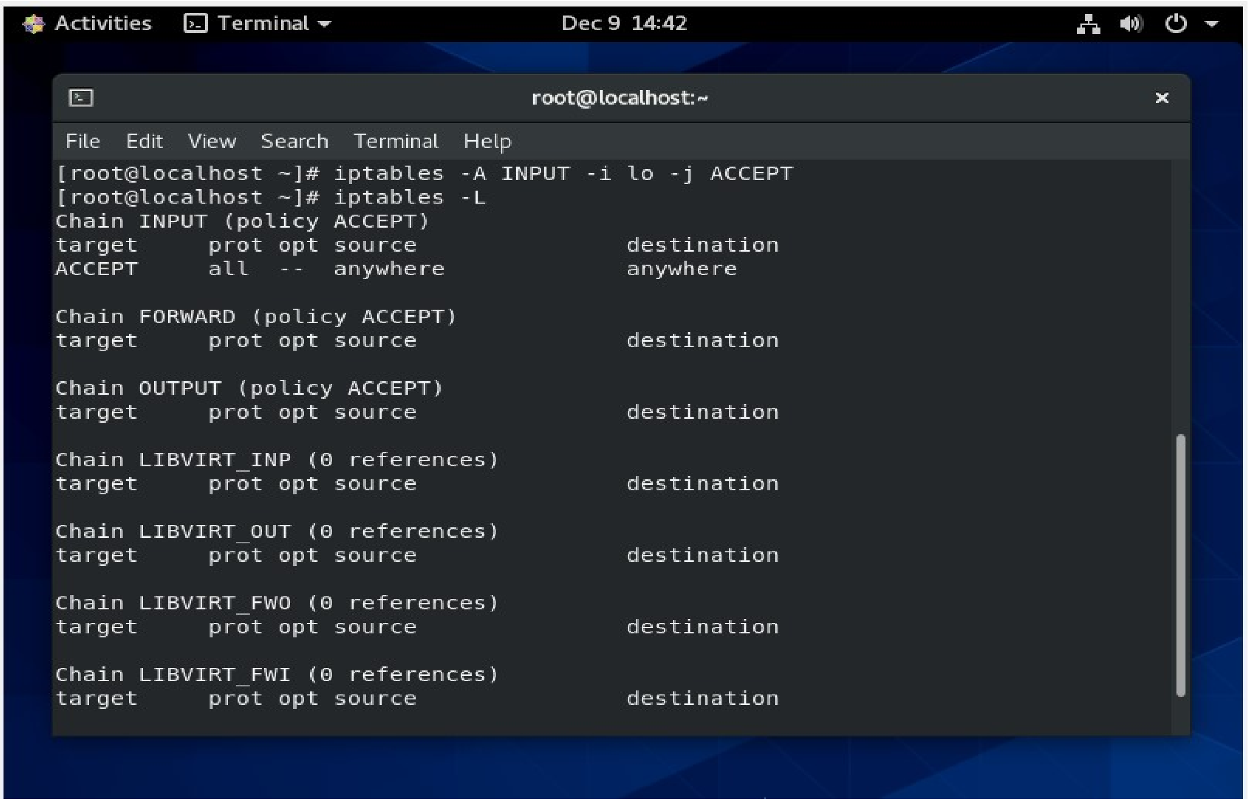


```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain LIBVIRT_INP (0 references)
target     prot opt source               destination

Chain LIBVIRT_OUT (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWO (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWI (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWX (0 references)
target     prot opt source               destination
```



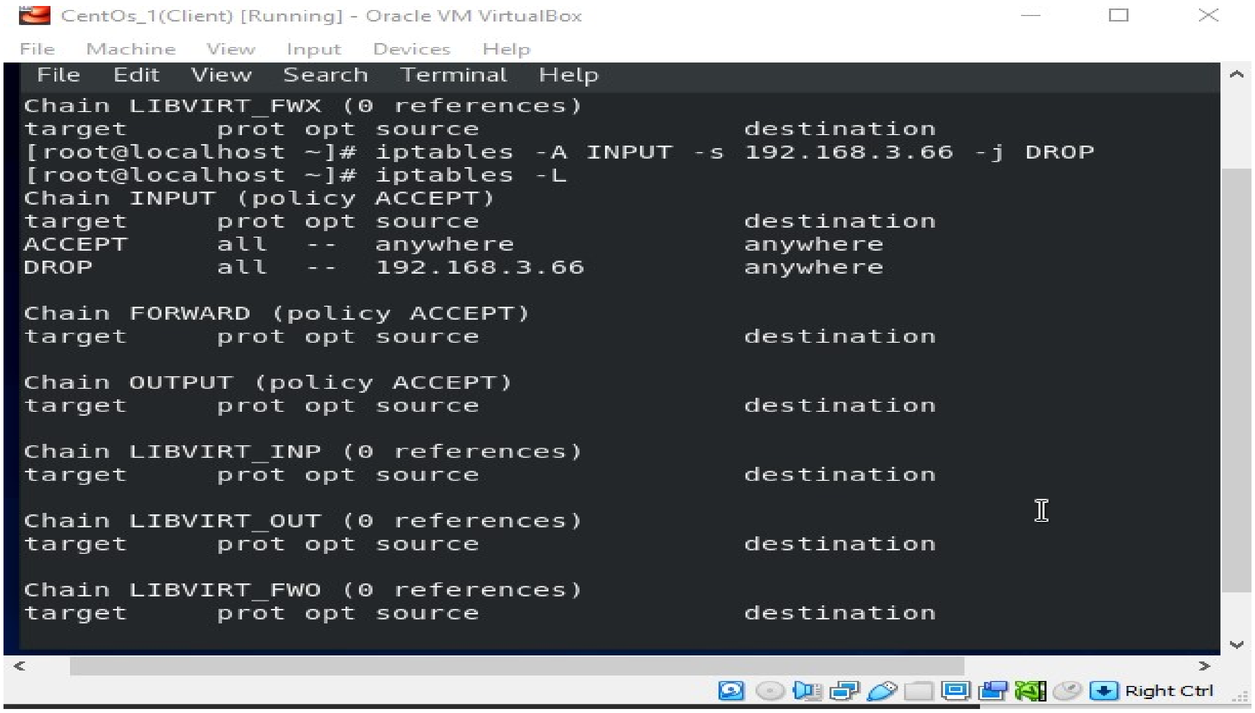
```
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:c6:f0:c9  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost ~]# ping 192.168.3.66
PING 192.168.3.66 (192.168.3.66) 56(84) bytes of data.
64 bytes from 192.168.3.66: icmp_seq=1 ttl=64 time=5.23 ms
64 bytes from 192.168.3.66: icmp_seq=2 ttl=64 time=3.30 ms
64 bytes from 192.168.3.66: icmp_seq=3 ttl=64 time=1.47 ms
64 bytes from 192.168.3.66: icmp_seq=4 ttl=64 time=2.82 ms
64 bytes from 192.168.3.66: icmp_seq=5 ttl=64 time=3.41 ms
64 bytes from 192.168.3.66: icmp_seq=6 ttl=64 time=1.57 ms
64 bytes from 192.168.3.66: icmp_seq=7 ttl=64 time=1.83 ms
64 bytes from 192.168.3.66: icmp_seq=8 ttl=64 time=1.48 ms
64 bytes from 192.168.3.66: icmp_seq=9 ttl=64 time=2.02 ms
64 bytes from 192.168.3.66: icmp_seq=10 ttl=64 time=1.56 ms
^C
--- 192.168.3.66 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9042ms
rtt min/avg/max/mdev = 1.471/2.469/5.229/1.164 ms
[root@localhost ~]#
```

2. Set the default INPUT policy ACCEPT



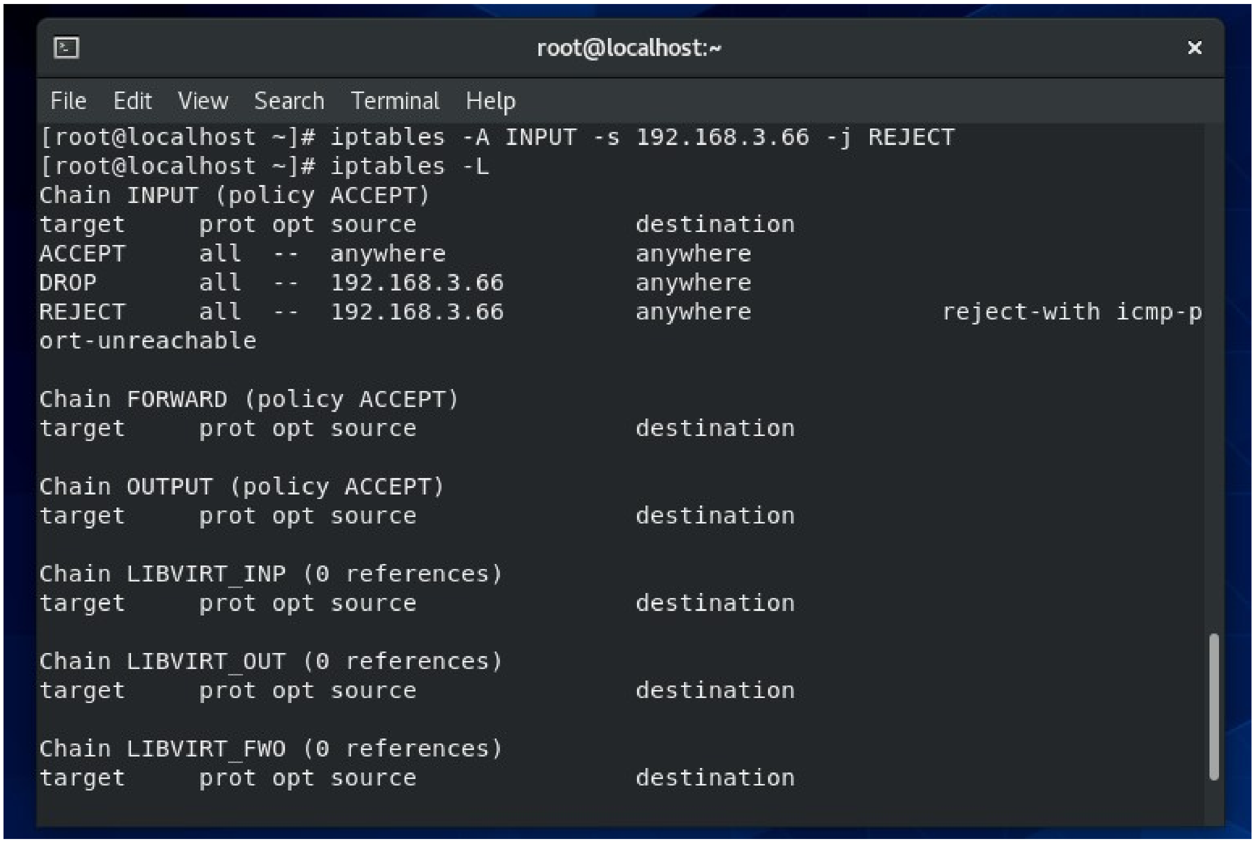
```
[root@localhost ~]# iptables -A INPUT -i lo -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain LIBVIRT_INP (0 references)
target     prot opt source               destination

Chain LIBVIRT_OUT (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWO (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWI (0 references)
target     prot opt source               destination
```

3. Except the machine2 IP, deny all the ping request to machine 1,


CentOs_1(Client) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View Search Terminal Help
Right Ctrl

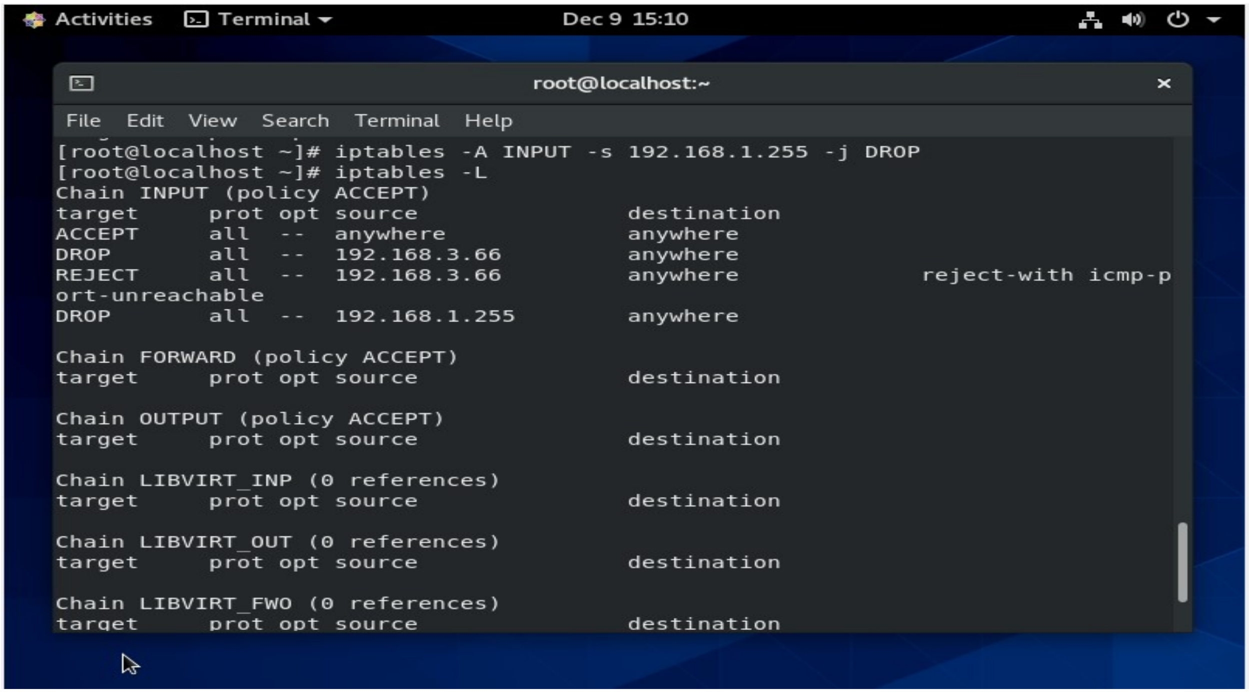
```
Chain LIBVIRT_FWX (0 references)
target     prot opt source               destination
[root@localhost ~]# iptables -A INPUT -s 192.168.3.66 -j DROP
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
DROP       all  --  192.168.3.66         anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain LIBVIRT_INP (0 references)
target     prot opt source               destination

Chain LIBVIRT_OUT (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWO (0 references)
target     prot opt source               destination
```

4. Reject all traffic except from the IP address of machine B



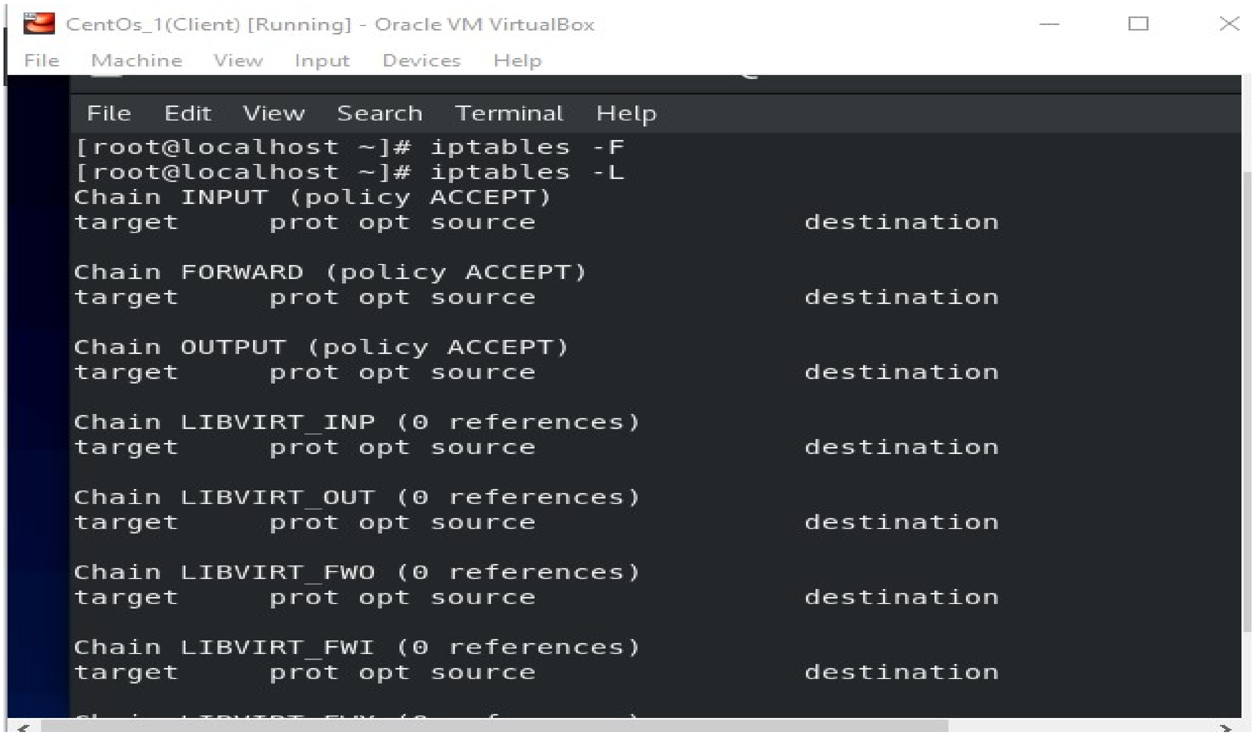
```
[root@localhost ~]# iptables -A INPUT -s 192.168.3.66 -j REJECT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
DROP       all  --  192.168.3.66         anywhere
REJECT     all  --  192.168.3.66         anywhere            reject-with icmp-p
ort-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain LIBVIRT_INP (0 references)
target     prot opt source               destination

Chain LIBVIRT_OUT (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWO (0 references)
target     prot opt source               destination
```

5. Block all the traffic from IP address 192.168.1.255



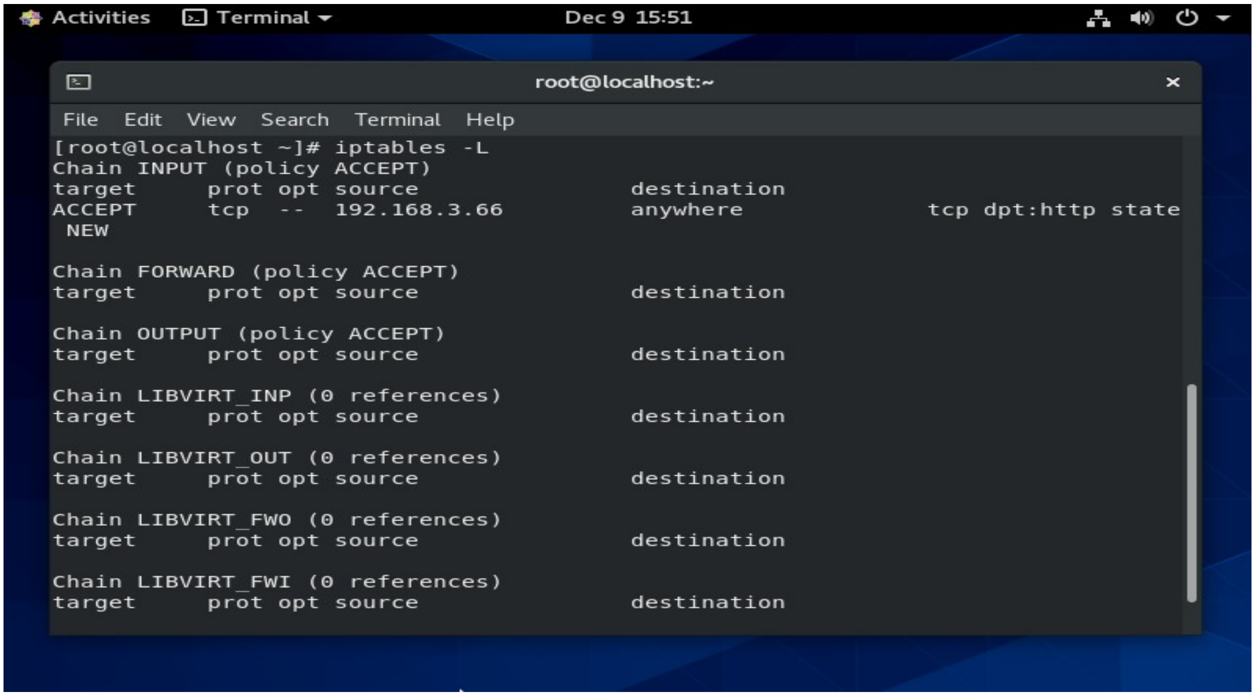
```
[root@localhost ~]# iptables -A INPUT -s 192.168.1.255 -j DROP
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
DROP       all  --  192.168.3.66         anywhere
REJECT     all  --  192.168.3.66         anywhere            reject-with icmp-p
ort-unreachable
DROP       all  --  192.168.1.255        anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain LIBVIRT_INP (0 references)
target     prot opt source               destination

Chain LIBVIRT_OUT (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWO (0 references)
target     prot opt source               destination
```

6. Except the machine 2 IP, deny all incoming HTTP and HTTPS traffic

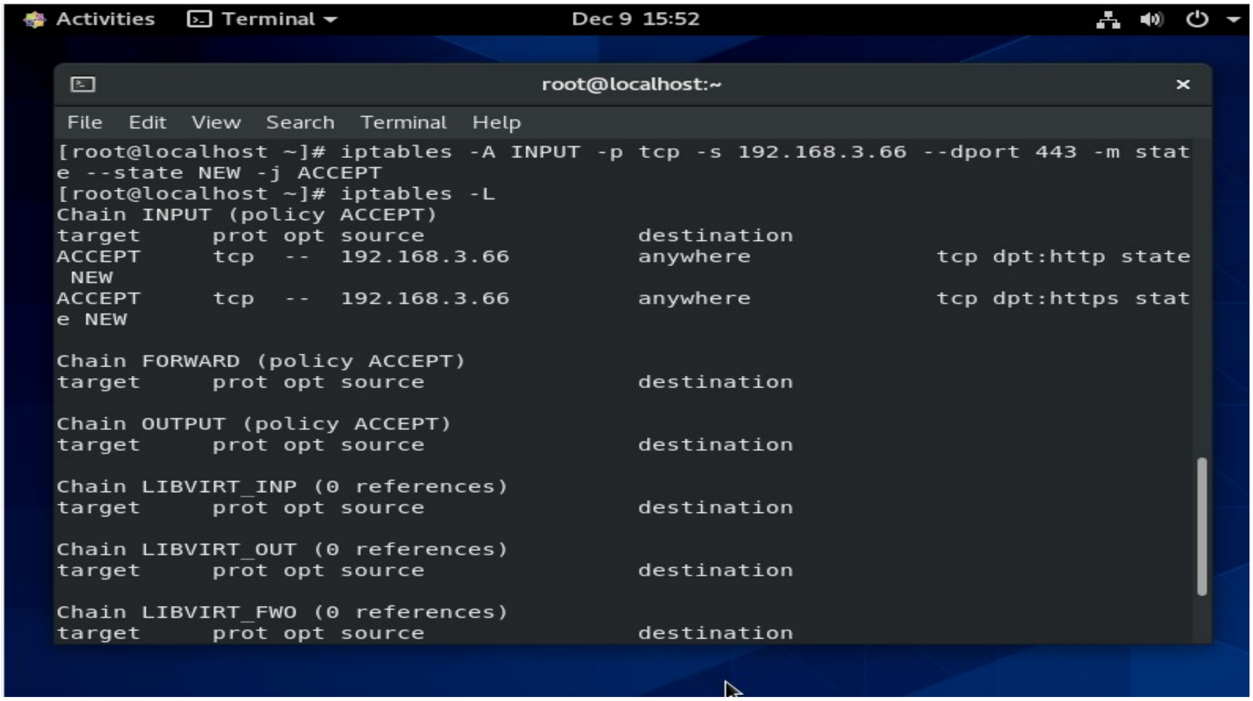


CentOs_1(Client) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View Search Terminal Help

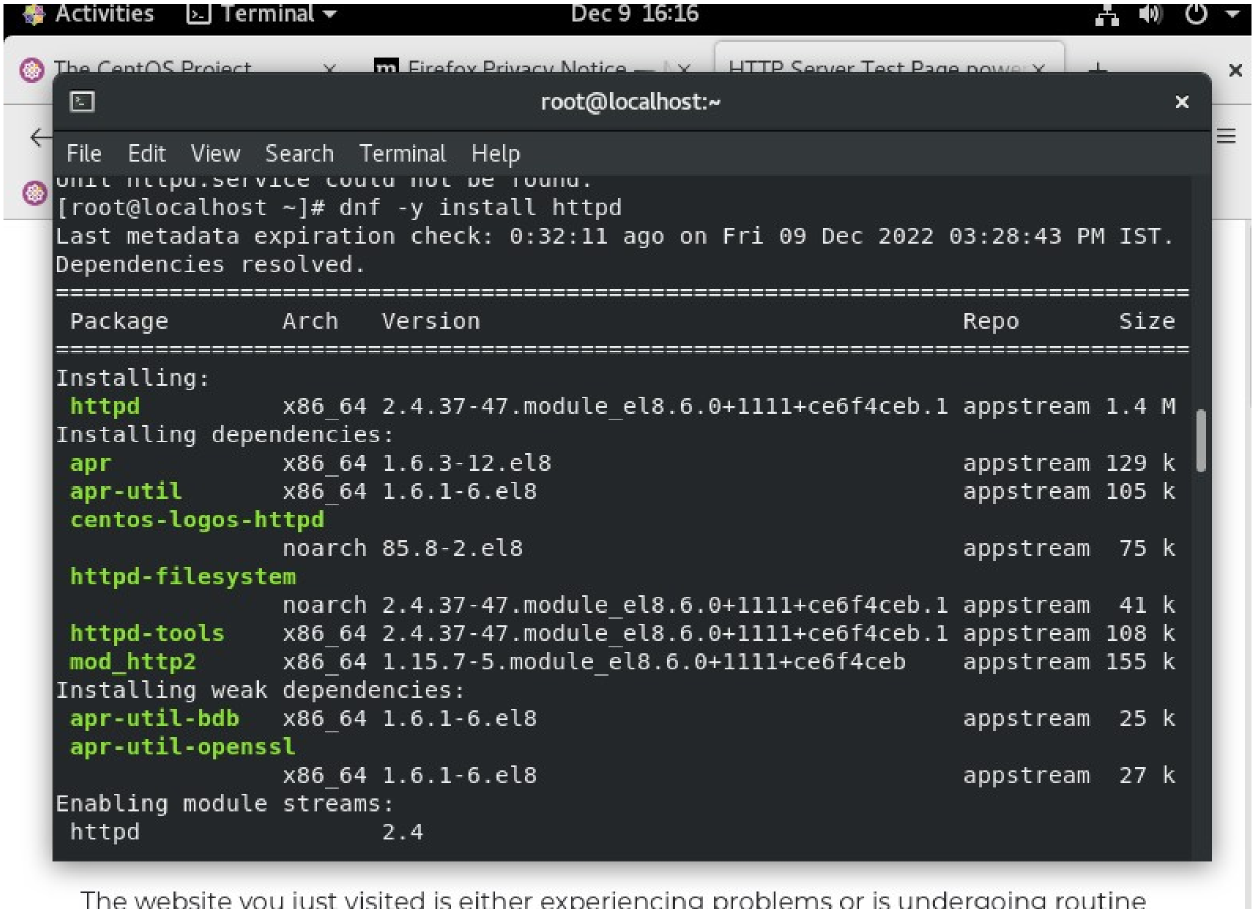
```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain LIBVIRT_INP (0 references)
target     prot opt source               destination

Chain LIBVIRT_OUT (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWO (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWI (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWX (0 references)
```



```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.3.66         anywhere             tcp dpt:http state
 NEW

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain LIBVIRT_INP (0 references)
target     prot opt source               destination

Chain LIBVIRT_OUT (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWO (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWI (0 references)
target     prot opt source               destination
```

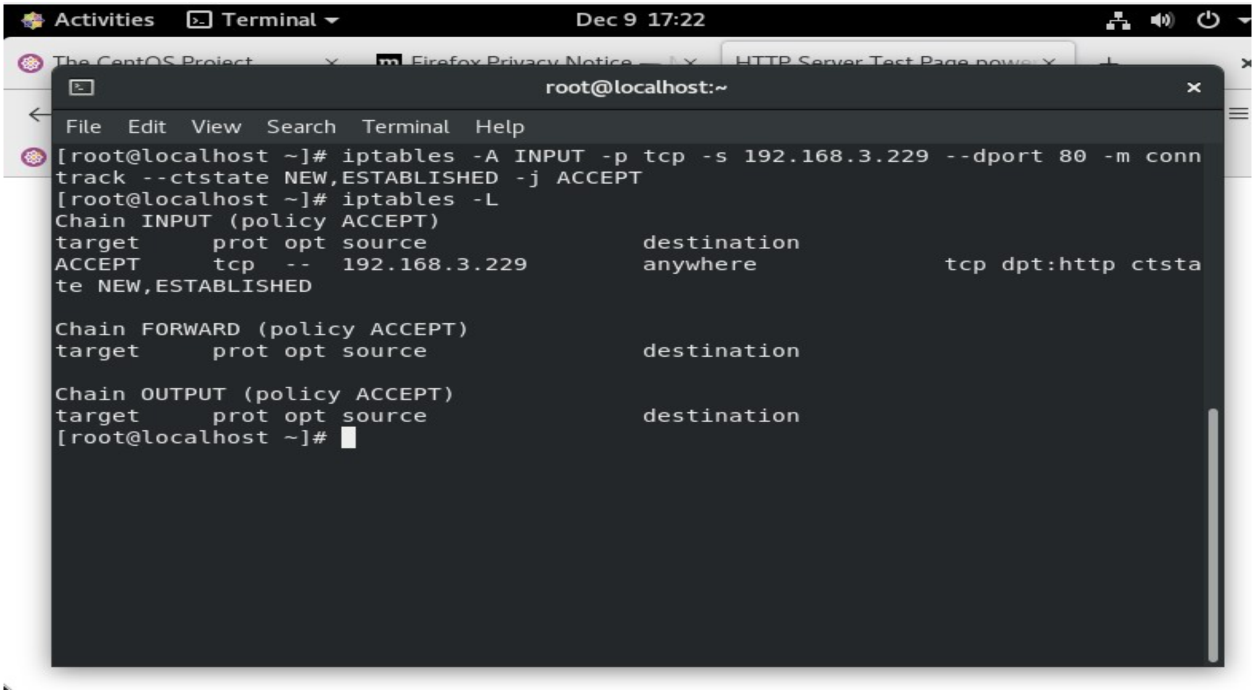


```
[root@localhost ~]# iptables -A INPUT -p tcp -s 192.168.3.66 --dport 443 -m stat
e --state NEW -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.3.66         anywhere             tcp dpt:http state
 NEW
ACCEPT     tcp  --  192.168.3.66         anywhere             tcp dpt:https stat
e NEW

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain LIBVIRT_INP (0 references)
target     prot opt source               destination

Chain LIBVIRT_OUT (0 references)
target     prot opt source               destination

Chain LIBVIRT_FWO (0 references)
target     prot opt source               destination
```

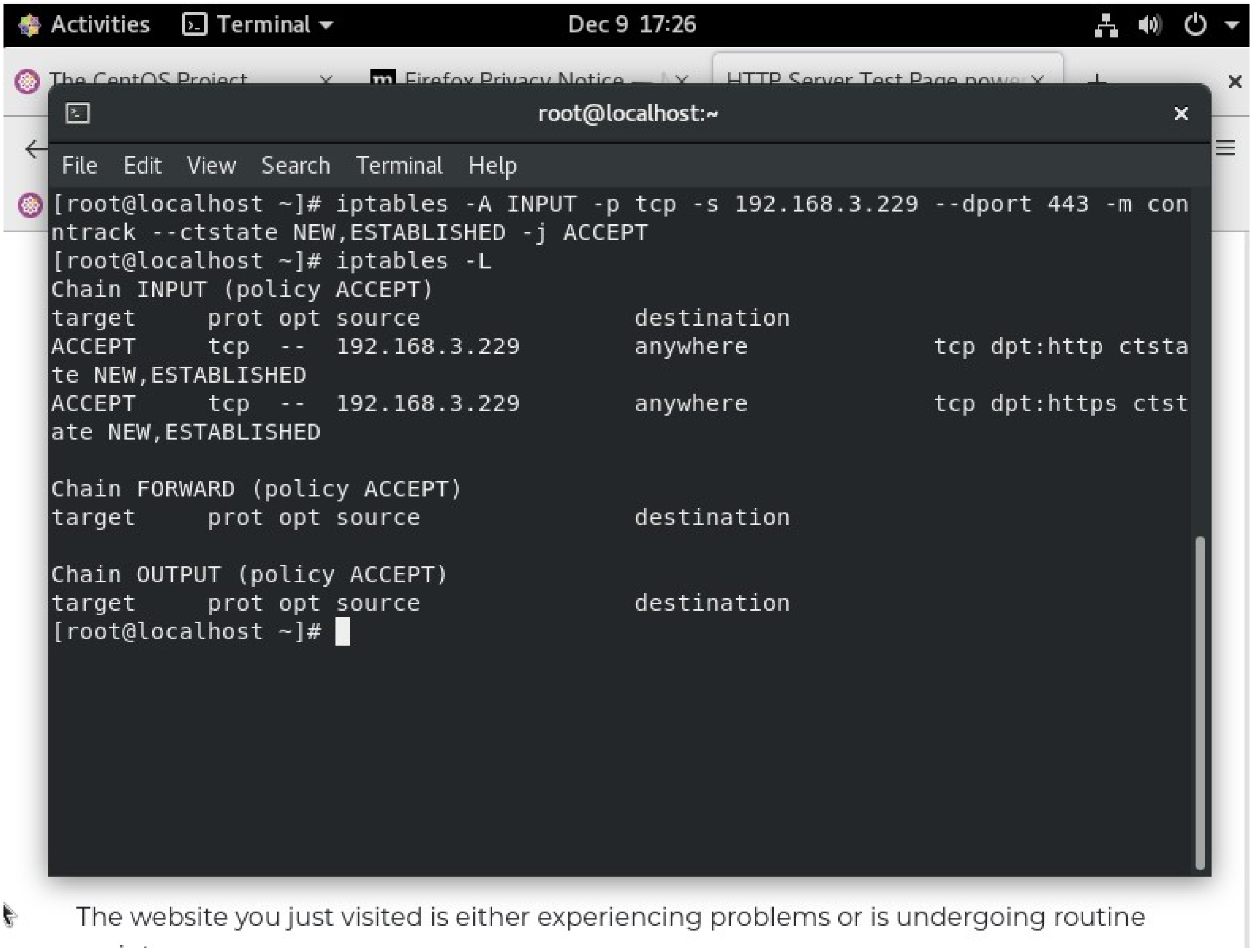


```
Unit httpd.service could not be found.
[root@localhost ~]# dnf -y install httpd
Last metadata expiration check: 0:32:11 ago on Fri 09 Dec 2022 03:28:43 PM IST.
Dependencies resolved.
================================================================================
 Package         Arch   Version                                 Repo       Size
================================================================================
Installing:
 httpd           x86_64 2.4.37-47.module_el8.6.0+1111+ce6f4ceb.1 appstream 1.4 M
Installing dependencies:
 apr             x86_64 1.6.3-12.el8                            appstream 129 k
 apr-util        x86_64 1.6.1-6.el8                             appstream 105 k
 centos-logos-httpd
                 noarch 85.8-2.el8                              appstream  75 k
 httpd-filesystem
                 noarch 2.4.37-47.module_el8.6.0+1111+ce6f4ceb.1 appstream  41 k
 httpd-tools     x86_64 2.4.37-47.module_el8.6.0+1111+ce6f4ceb.1 appstream 108 k
 mod_http2       x86_64 1.15.7-5.module_el8.6.0+1111+ce6f4ceb   appstream 155 k
Installing weak dependencies:
 apr-util-bdb    x86_64 1.6.1-6.el8                             appstream  25 k
 apr-util-openssl
                 x86_64 1.6.1-6.el8                             appstream  27 k
Enabling module streams:
 httpd                  2.4
```

The website you just visited is either experiencing problems or is undergoing routine

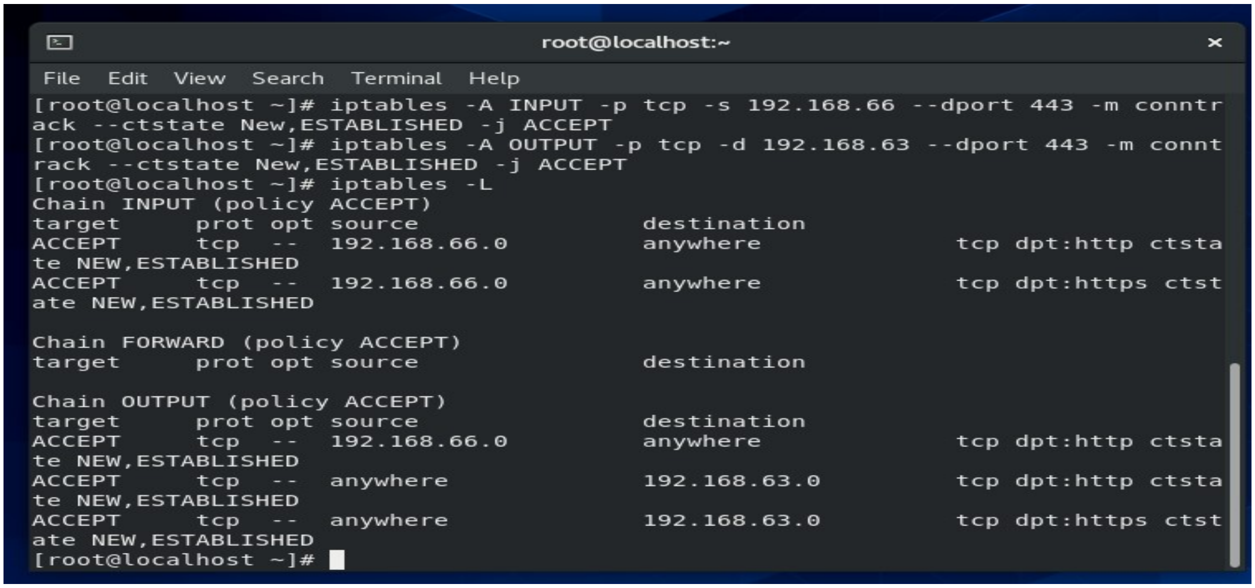


```
[root@localhost ~]# iptables -A INPUT -p tcp -s 192.168.3.229 --dport 80 -m conn
track --ctstate NEW,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.3.229        anywhere             tcp dpt:http ctsta
te NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]# 
```



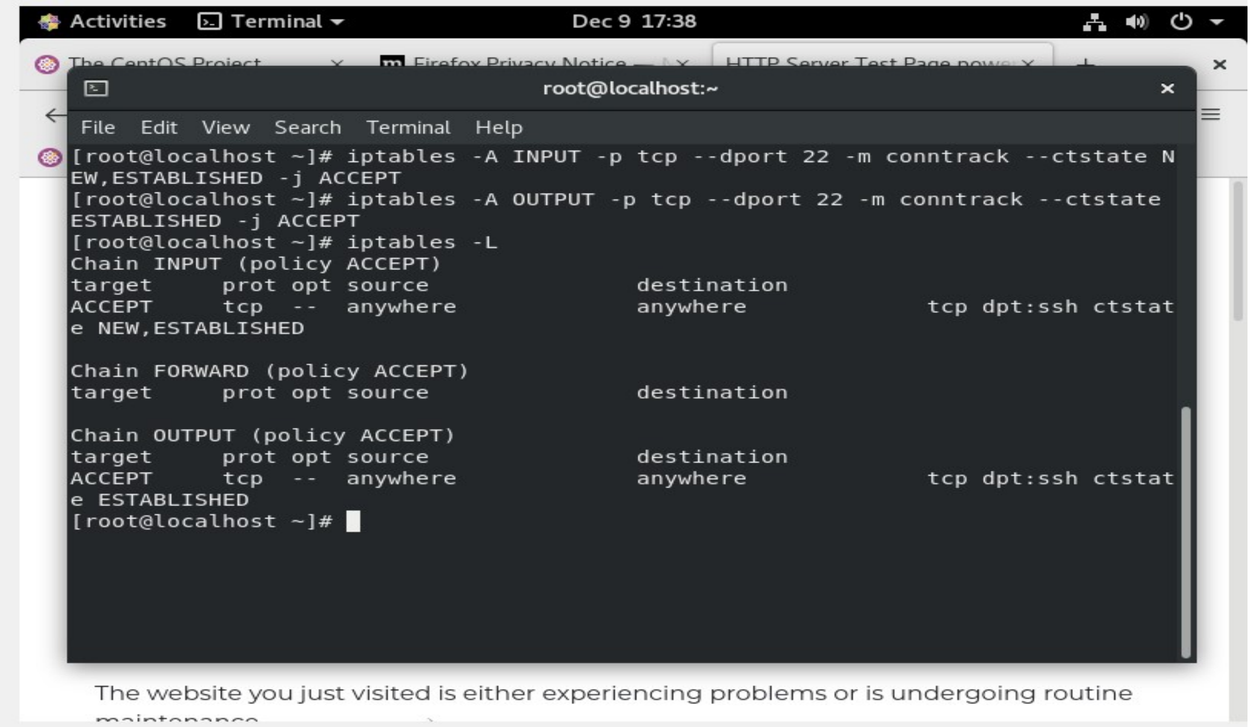
```
[root@localhost ~]# iptables -A INPUT -p tcp -s 192.168.3.229 --dport 443 -m con
ntrack --ctstate NEW,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.3.229        anywhere             tcp dpt:http ctsta
te NEW,ESTABLISHED
ACCEPT     tcp  --  192.168.3.229        anywhere             tcp dpt:https ctst
ate NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]# 
```

The website you just visited is either experiencing problems or is undergoing routine



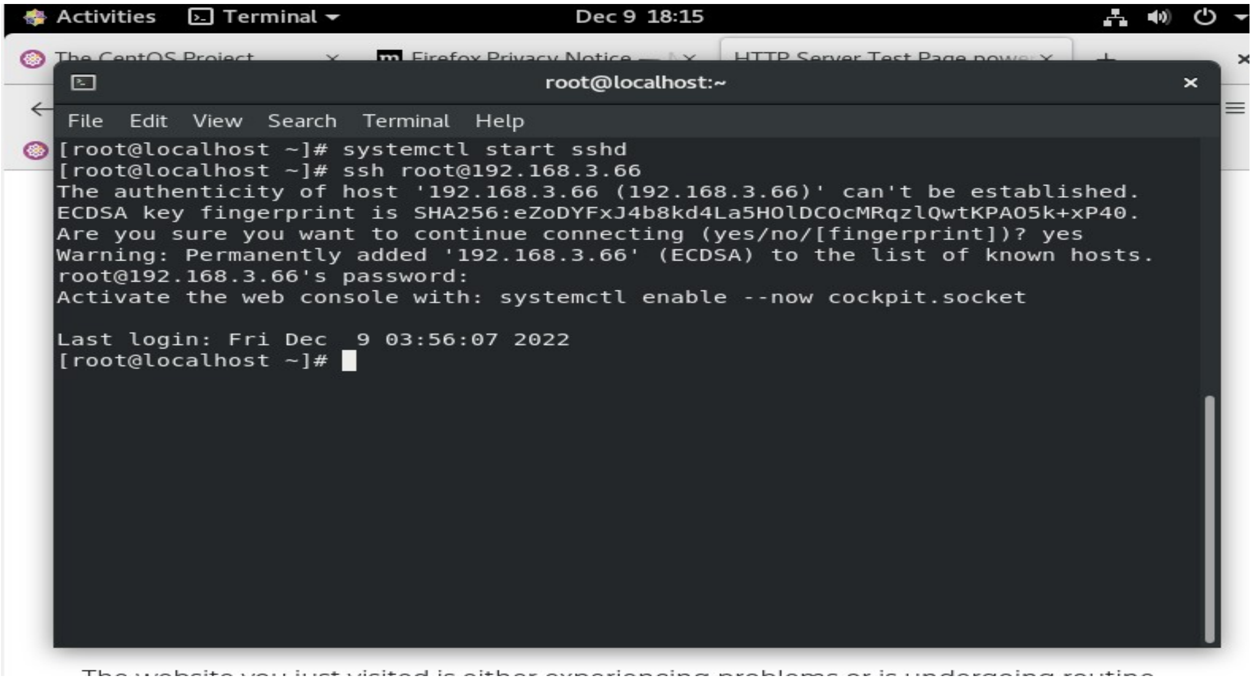
```
[root@localhost ~]# iptables -A INPUT -p tcp -s 192.168.66 --dport 443 -m conntr
ack --ctstate New,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -A OUTPUT -p tcp -d 192.168.63 --dport 443 -m connt
rack --ctstate New,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.66.0         anywhere             tcp dpt:http ctsta
te NEW,ESTABLISHED
ACCEPT     tcp  --  192.168.66.0         anywhere             tcp dpt:https ctst
ate NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.66.0         anywhere             tcp dpt:http ctsta
te NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere             192.168.63.0         tcp dpt:http ctsta
te NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere             192.168.63.0         tcp dpt:https ctst
ate NEW,ESTABLISHED
[root@localhost ~]# 
```

7. Block all incoming or outgoing traffic on a port 22.

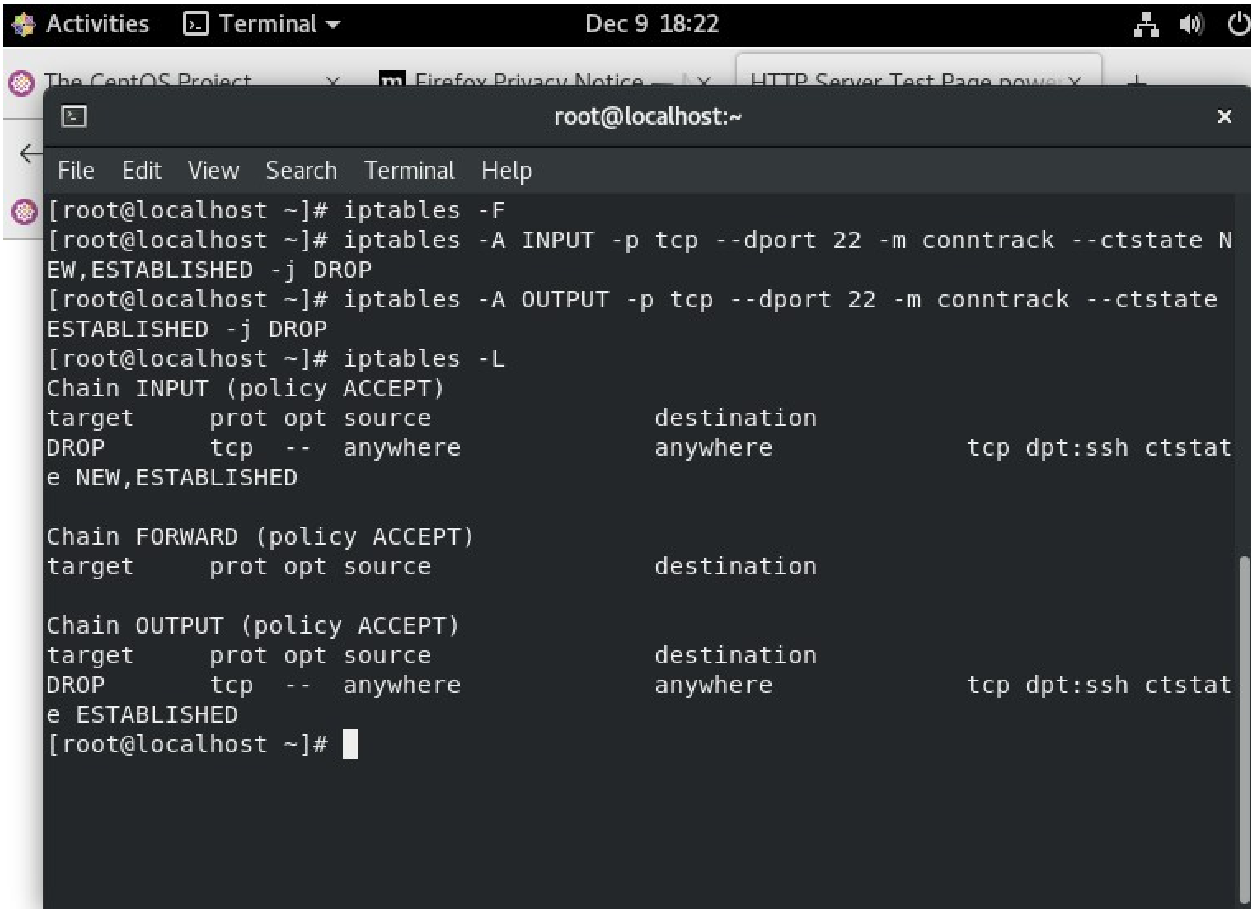


```
[root@localhost ~]# iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate N
EW,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -A OUTPUT -p tcp --dport 22 -m conntrack --ctstate
ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh ctstat
e NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh ctstat
e ESTABLISHED
[root@localhost ~]# 
```

The website you just visited is either experiencing problems or is undergoing routine maintenance

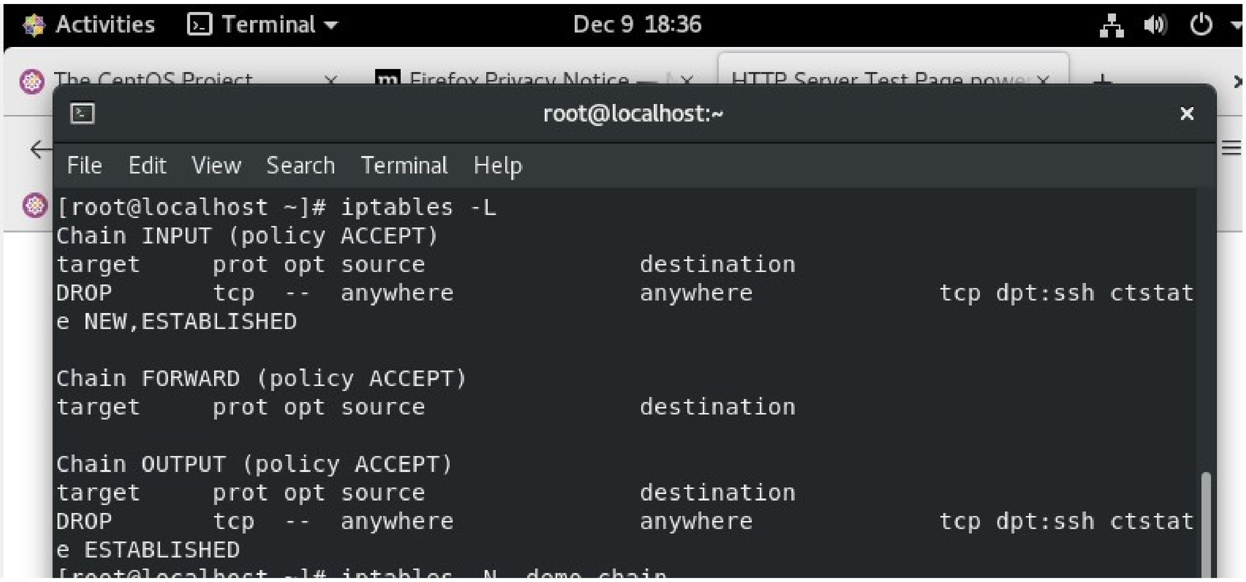


```
[root@localhost ~]# systemctl start sshd
[root@localhost ~]# ssh root@192.168.3.66
The authenticity of host '192.168.3.66 (192.168.3.66)' can't be established.
ECDSA key fingerprint is SHA256:eZoDYFxJ4b8kd4La5HOlDCOcMRqzlQwtKPAO5k+xP40.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.3.66' (ECDSA) to the list of known hosts.
root@192.168.3.66's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Dec  9 03:56:07 2022
[root@localhost ~]#
```

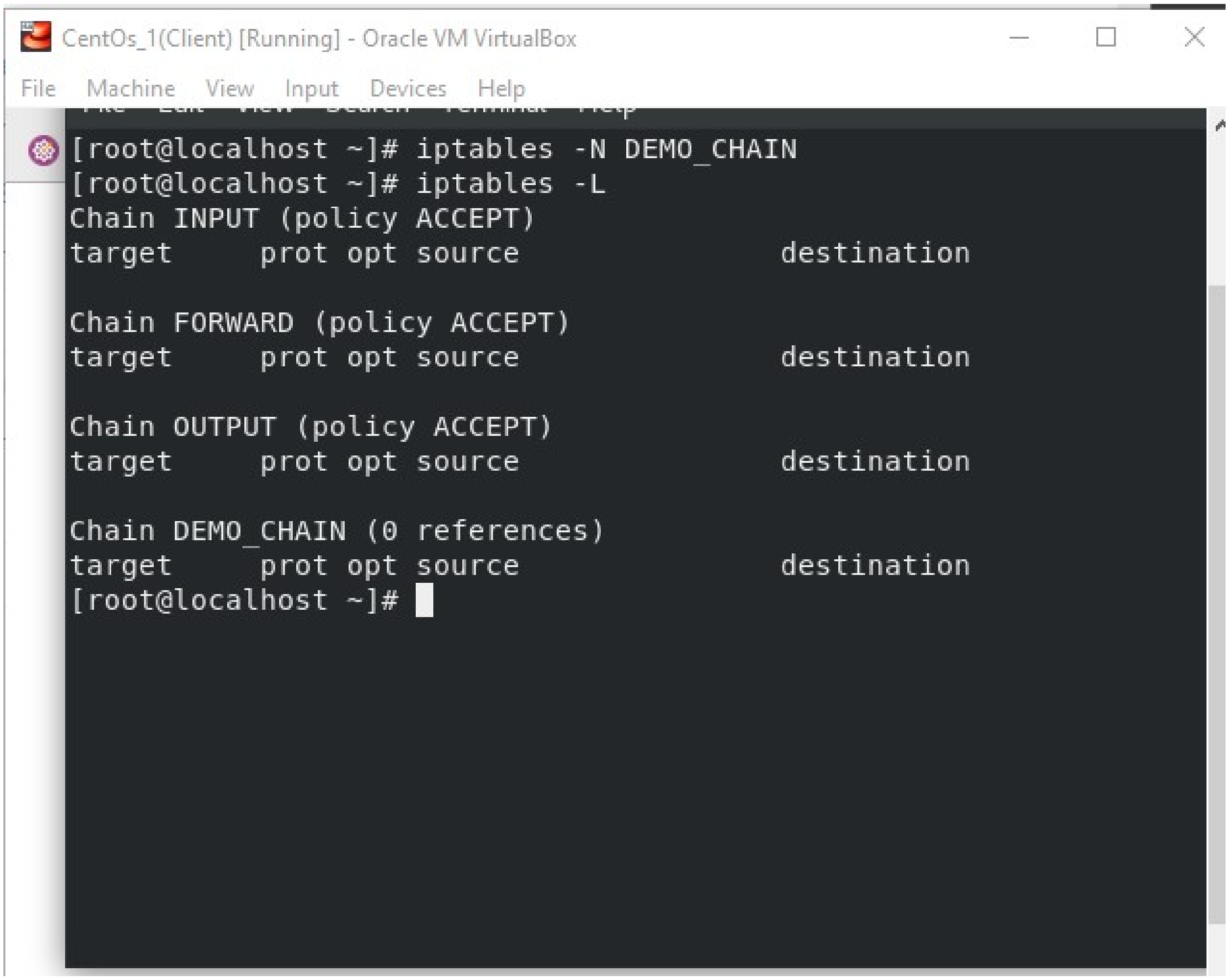


```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate N
EW,ESTABLISHED -j DROP
[root@localhost ~]# iptables -A OUTPUT -p tcp --dport 22 -m conntrack --ctstate
ESTABLISHED -j DROP
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh ctstat
e NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh ctstat
e ESTABLISHED
[root@localhost ~]#
```

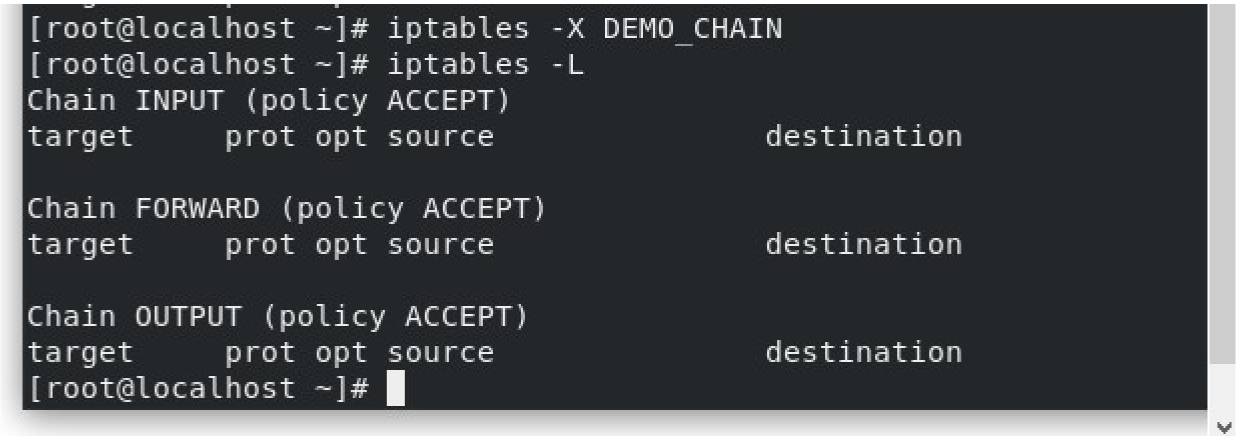
8. Add a new chain called “ Demo Chain“



```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh ctstat
e NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh ctstat
e ESTABLISHED
[root@localhost ~]# iptables -N demo_chain
```

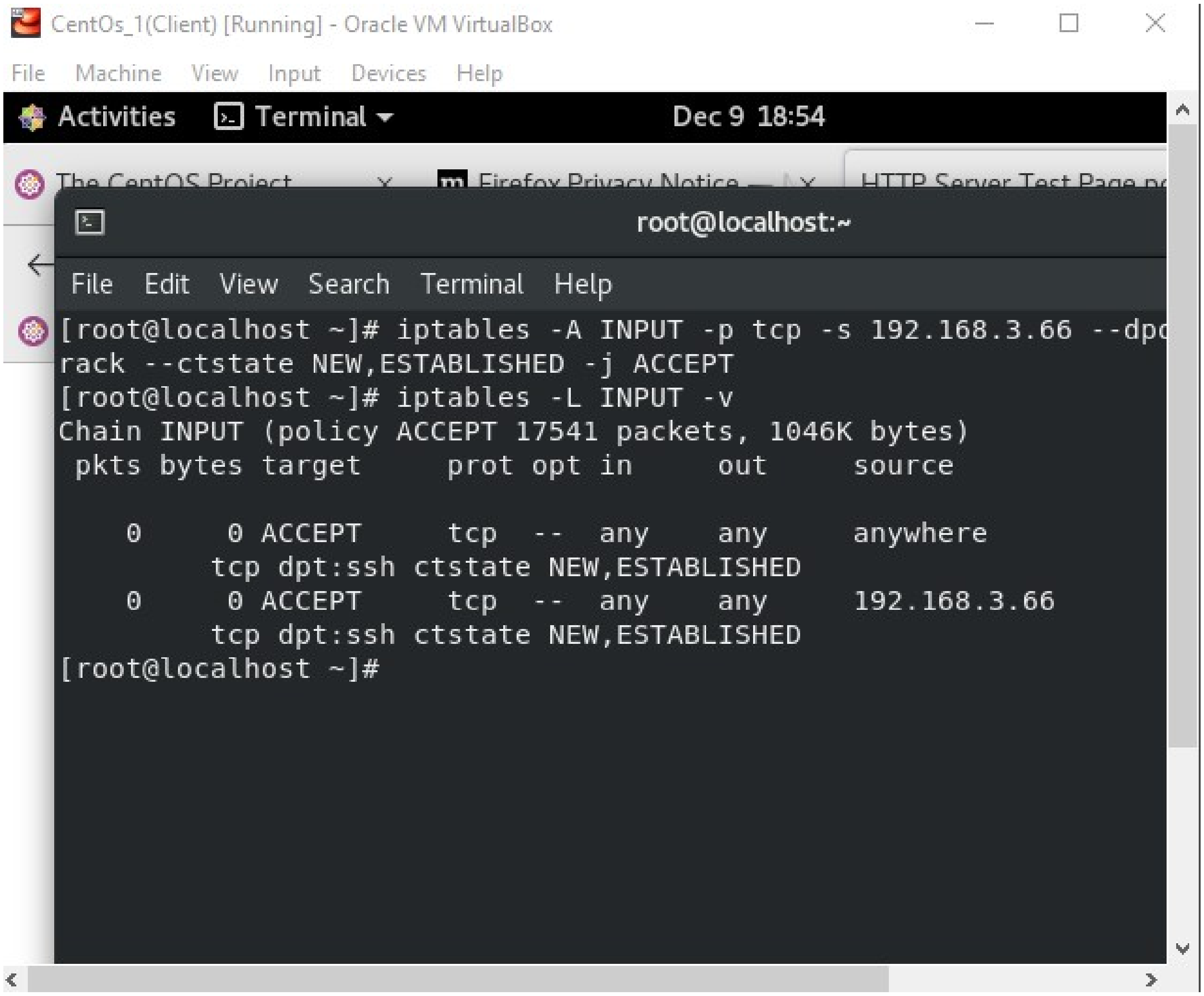

CentOs_1(Client) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
[root@localhost ~]# iptables -N DEMO_CHAIN
[root@localhost ~]# 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

Chain DEMO_CHAIN (0 references)
target     prot opt source               destination
[root@localhost ~]#
```



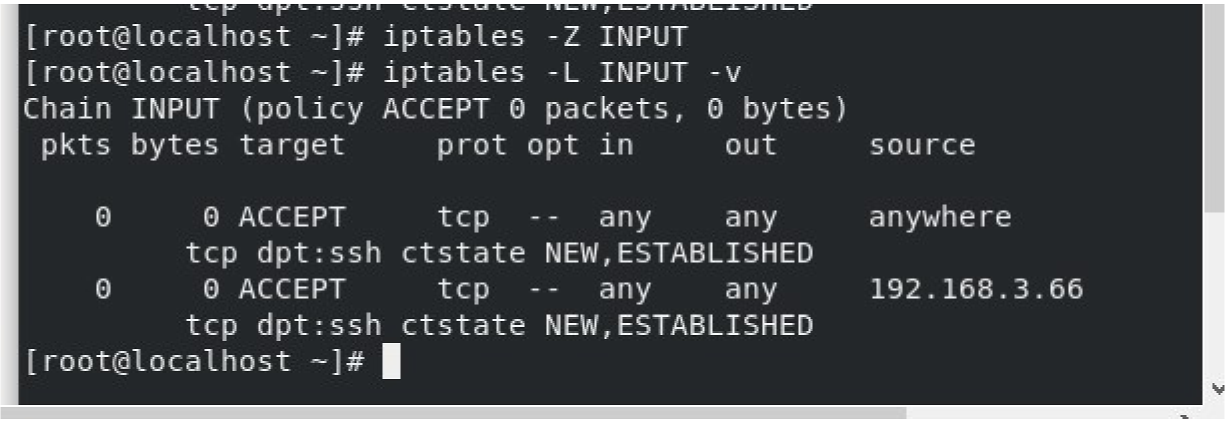
```
[root@localhost ~]# iptables -X DEMO_CHAIN
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]#
```

9. List the number of packets and bytes matched in each rule



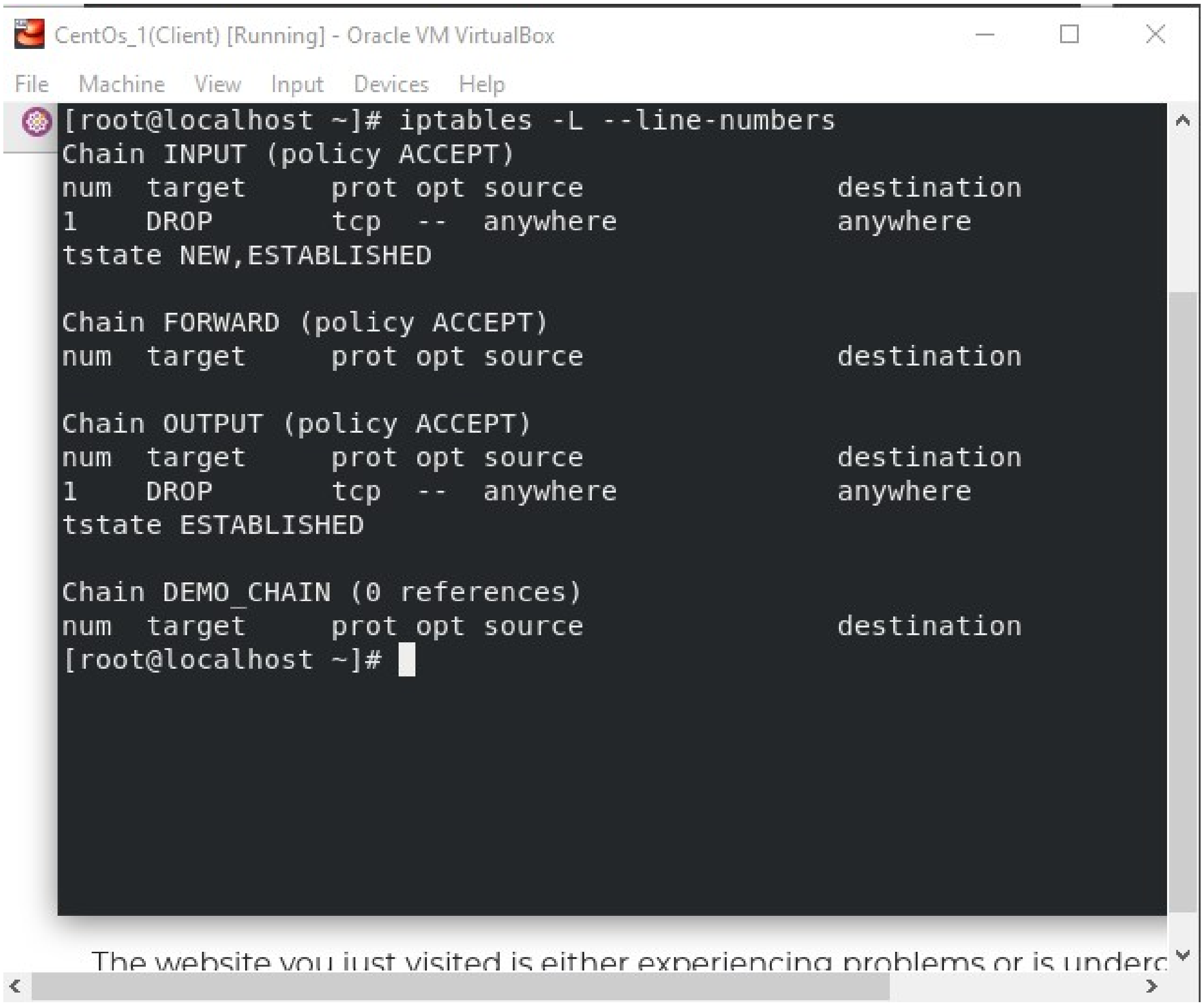
CentOs_1(Client) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Dec 9 18:54
The CentOS Project
Firefox Privacy Notice —
HTTP Server Test Page p
root@localhost:~
File Edit View Search Terminal Help

```
[root@localhost ~]# iptables -A INPUT -p tcp -s 192.168.3.66 --dpc
rack --ctstate NEW,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -L INPUT -v
Chain INPUT (policy ACCEPT 17541 packets, 1046K bytes)
 pkts bytes target     prot opt in     out     source

    0     0 ACCEPT     tcp  --  any    any     anywhere
        tcp dpt:ssh ctstate NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     192.168.3.66
        tcp dpt:ssh ctstate NEW,ESTABLISHED
[root@localhost ~]#
```



```
        tcp dpt:ssh ctstate NEW,ESTABLISHED
[root@localhost ~]# iptables -Z INPUT
[root@localhost ~]# iptables -L INPUT -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source

    0     0 ACCEPT     tcp  --  any    any     anywhere
        tcp dpt:ssh ctstate NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     192.168.3.66
        tcp dpt:ssh ctstate NEW,ESTABLISHED
[root@localhost ~]#
```

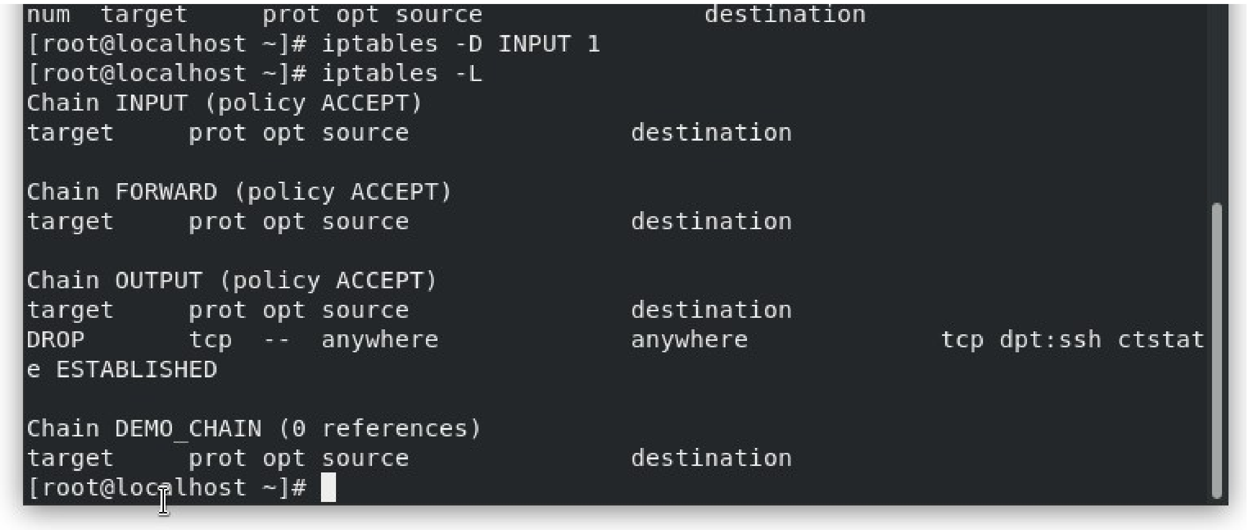
10. List all the rules with line numbers



```
[root@localhost ~]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  anywhere             anywhere
tstate NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  anywhere             anywhere
tstate ESTABLISHED

Chain DEMO_CHAIN (0 references)
num  target     prot opt source               destination
[root@localhost ~]#
```

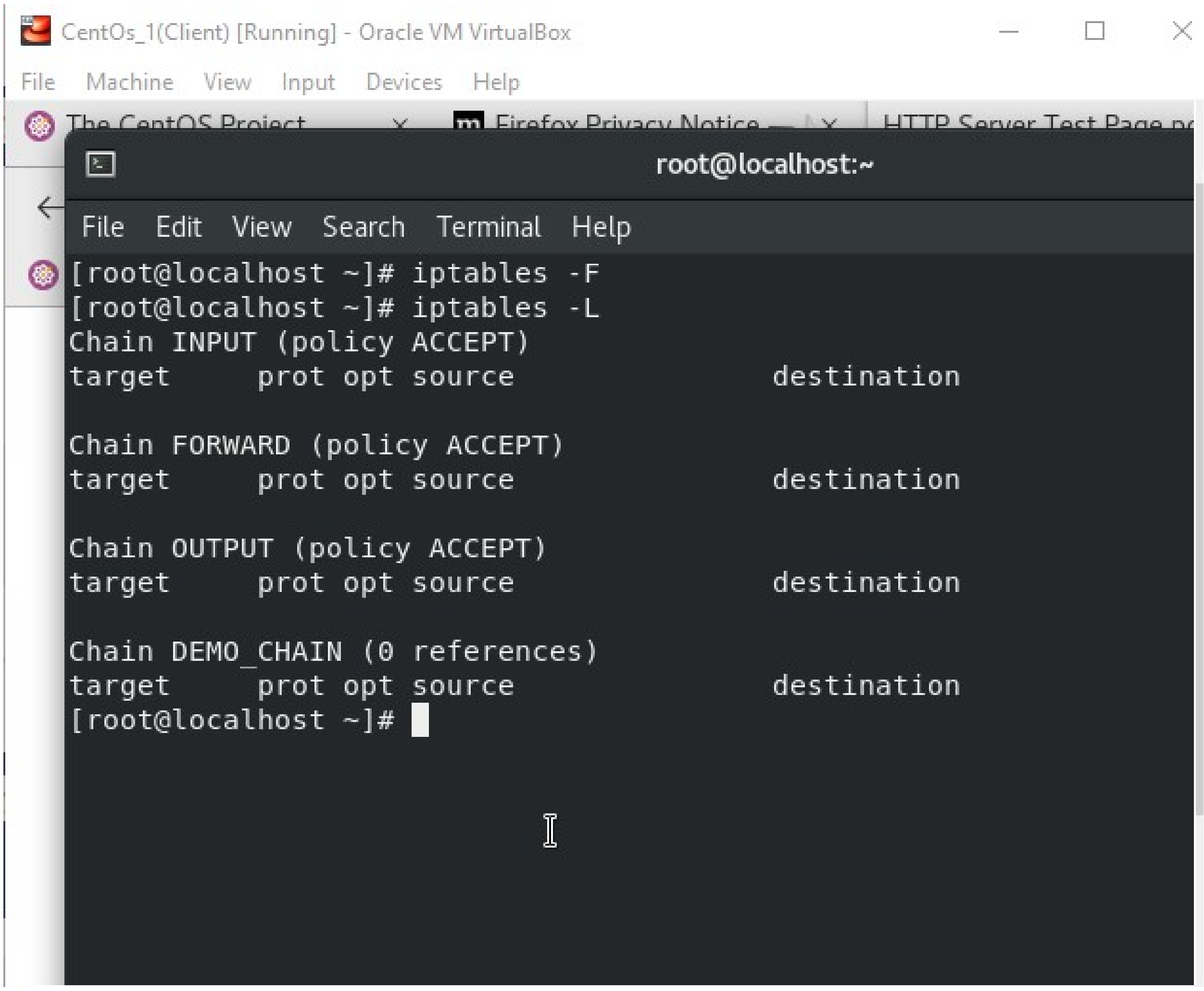
The website you just visited is either experiencing problems or is underc

11. Delete the rule number 2

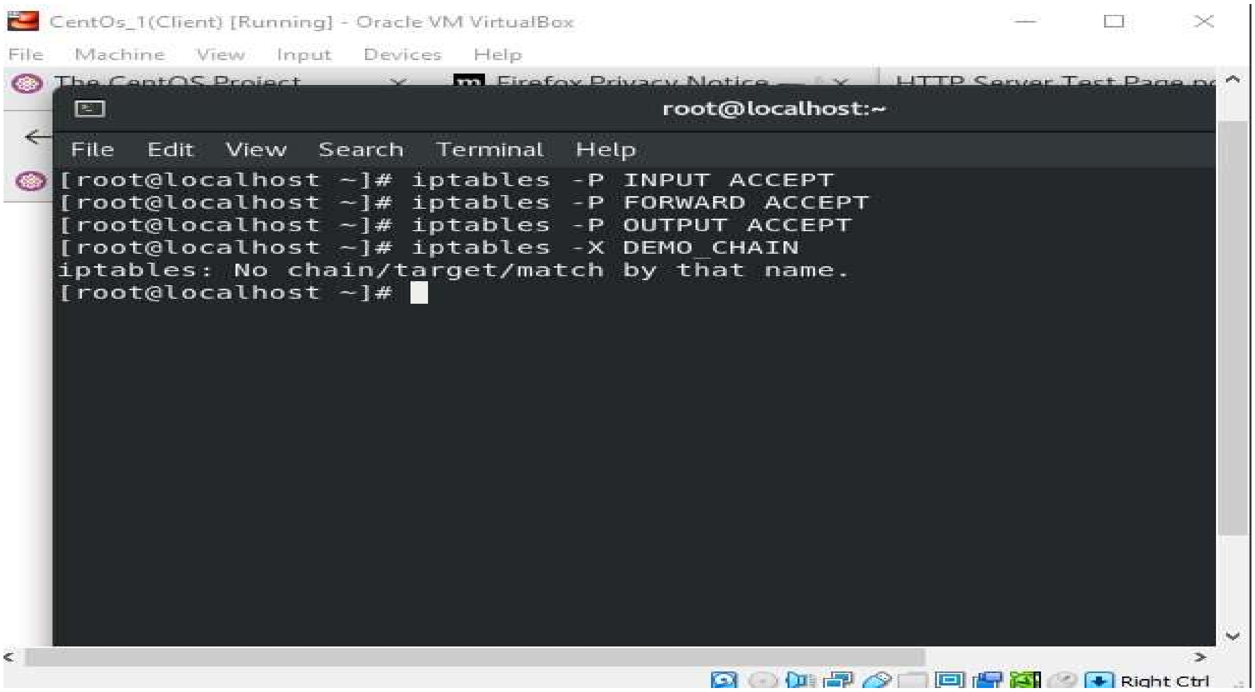


```
num  target     prot opt source               destination
[root@localhost ~]# iptables -D INPUT 1
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh ctstat
e ESTABLISHED

Chain DEMO_CHAIN (0 references)
target     prot opt source               destination
[root@localhost ~]# 
```

12. Delete all the rules from all the chain


CentOs_1(Client) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The CentOS Project
Firefox Privacy Notice —
HTTP Server Test Page po
root@localhost:~
File Edit View Search Terminal Help

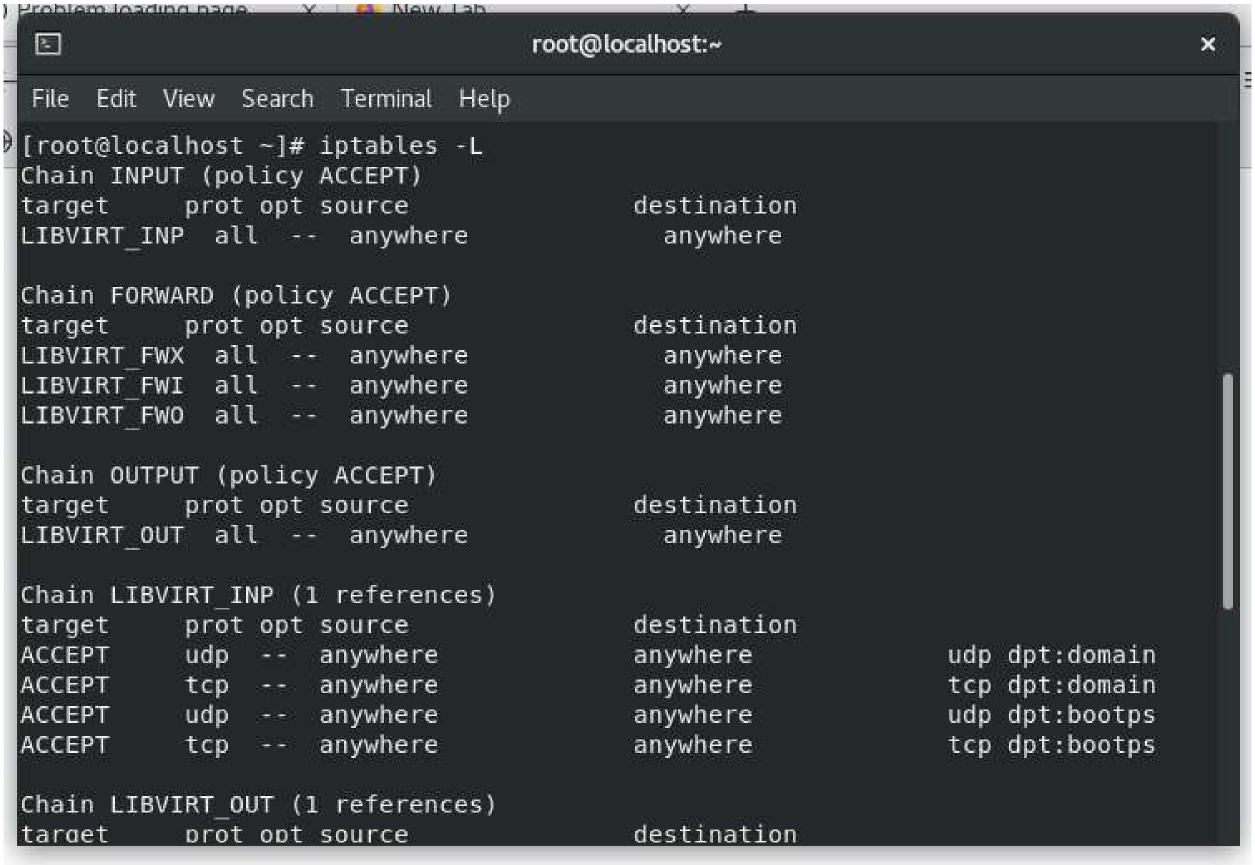
```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain DEMO_CHAIN (0 references)
target     prot opt source               destination
[root@localhost ~]# 
```



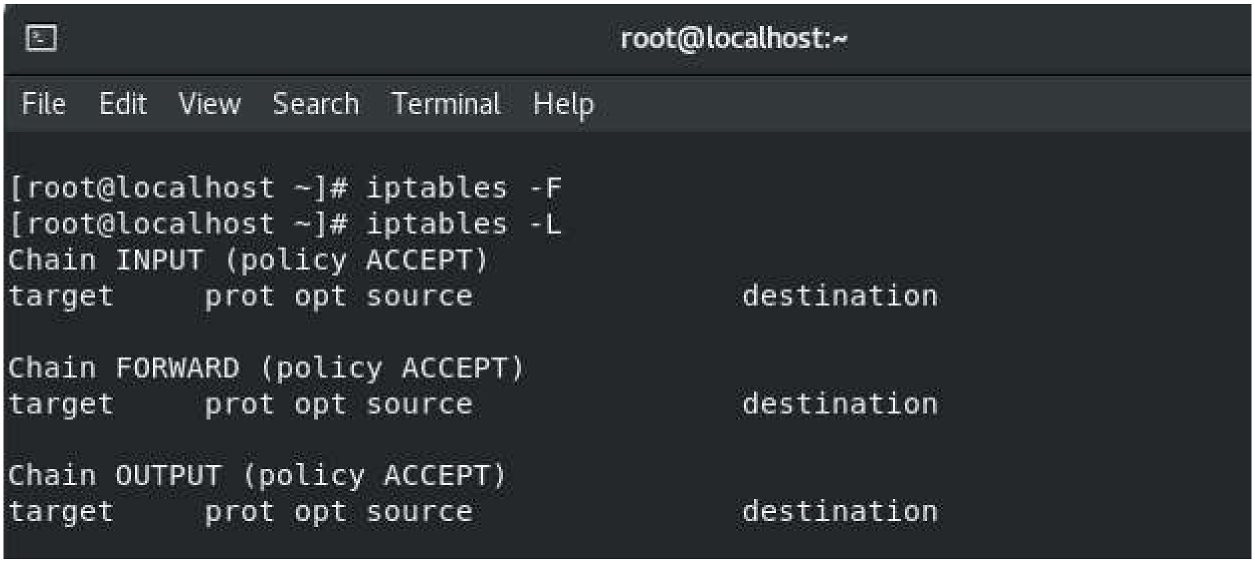
CentOs_1(Client) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@localhost:~
File Edit View Search Terminal Help
Right Ctrl

```
[root@localhost ~]# iptables -P INPUT ACCEPT
[root@localhost ~]# iptables -P FORWARD ACCEPT
[root@localhost ~]# iptables -P OUTPUT ACCEPT
[root@localhost ~]# iptables -X DEMO_CHAIN
iptables: No chain/target/match by that name.
[root@localhost ~]#
```

13. List the existing firewall rules and default policy in each chain

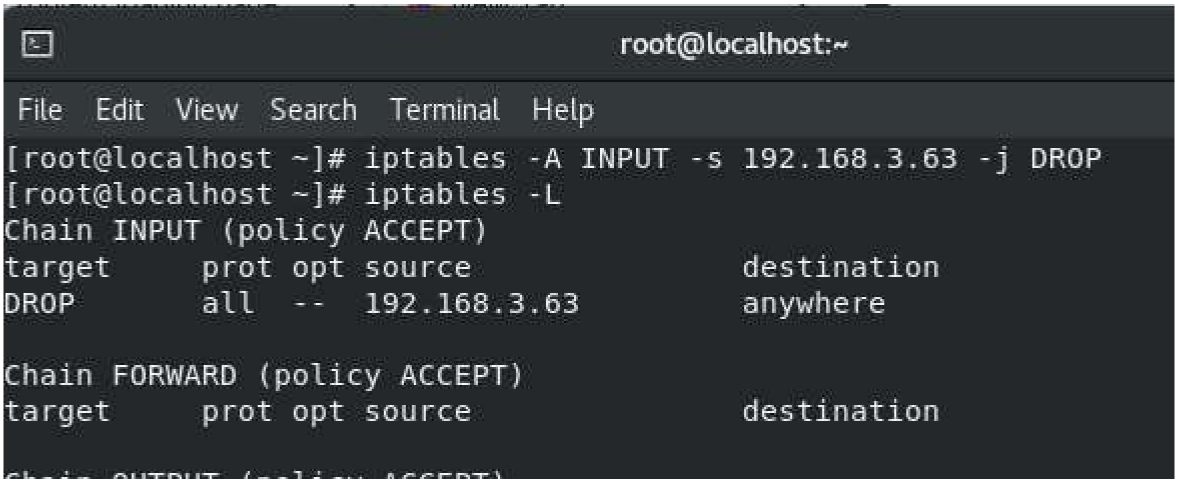


```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
LIBVIRT_INP  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
LIBVIRT_FWX  all  --  anywhere             anywhere
LIBVIRT_FWI  all  --  anywhere             anywhere
LIBVIRT_FWO  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
LIBVIRT_OUT  all  --  anywhere             anywhere

Chain LIBVIRT_INP (1 references)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:bootps
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:bootps

Chain LIBVIRT_OUT (1 references)
target     prot opt source               destination
```

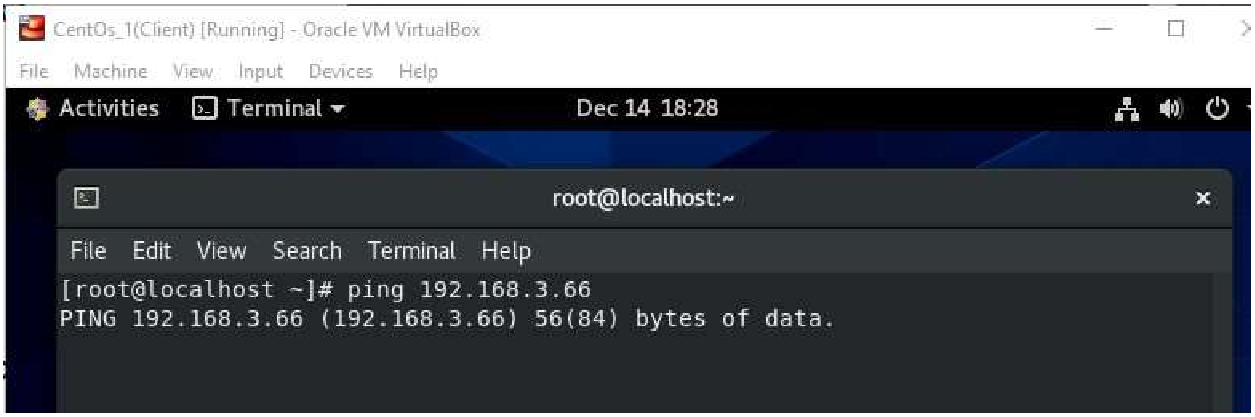


```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

14. Set the default INPUT policy as DROP

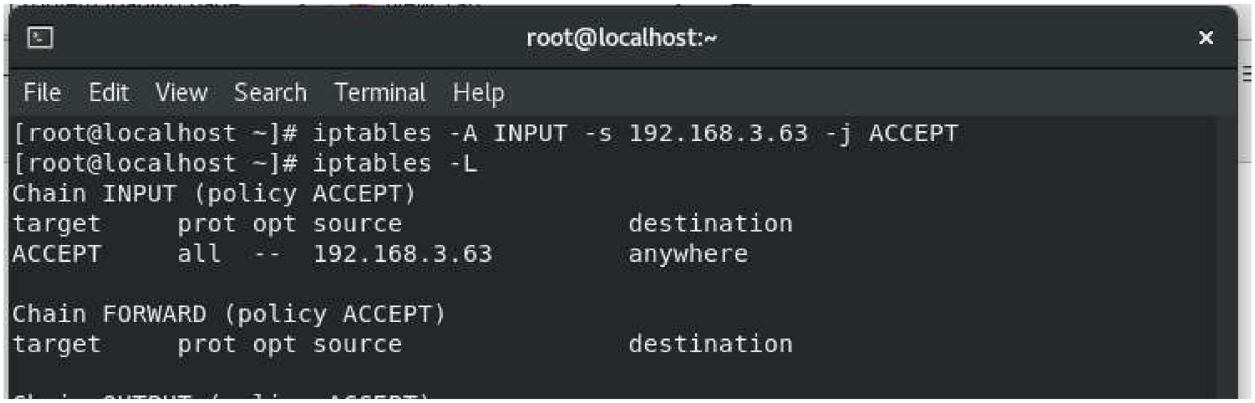


```
[root@localhost ~]# iptables -A INPUT -s 192.168.3.63 -j DROP
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.3.63         anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
```

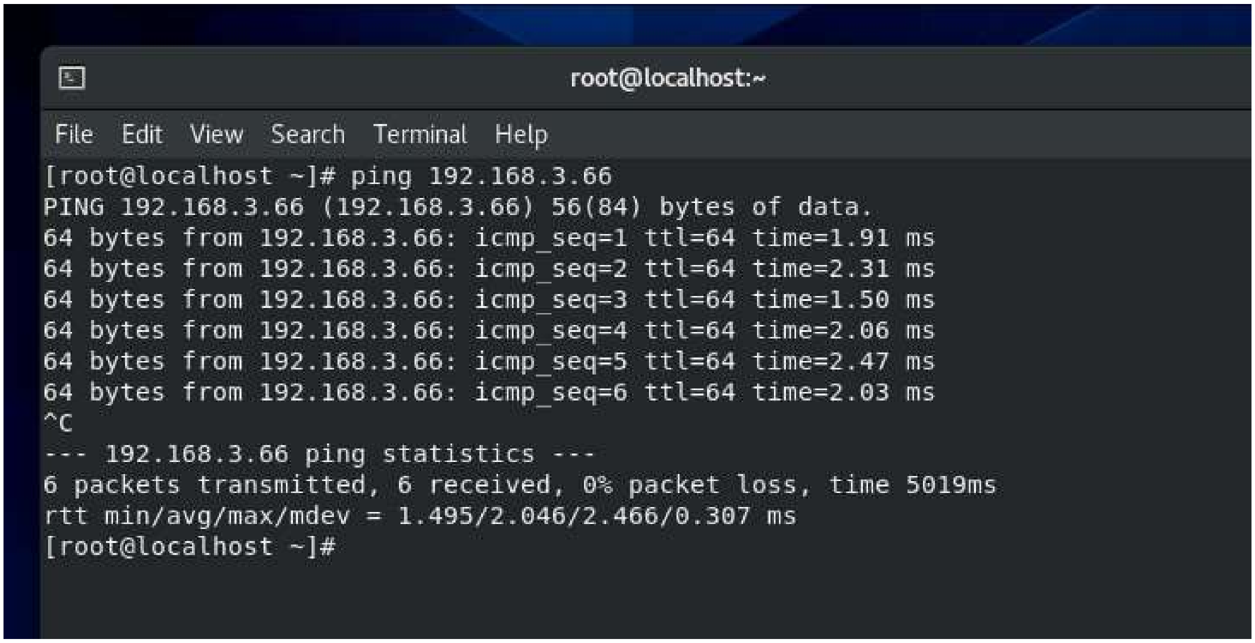

CentOs_1(Client) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Dec 14 18:28
root@localhost:~
File Edit View Search Terminal Help

```
[root@localhost ~]# ping 192.168.3.66
PING 192.168.3.66 (192.168.3.66) 56(84) bytes of data.
```

15. In machine 2, allow the ping request only from machine 1

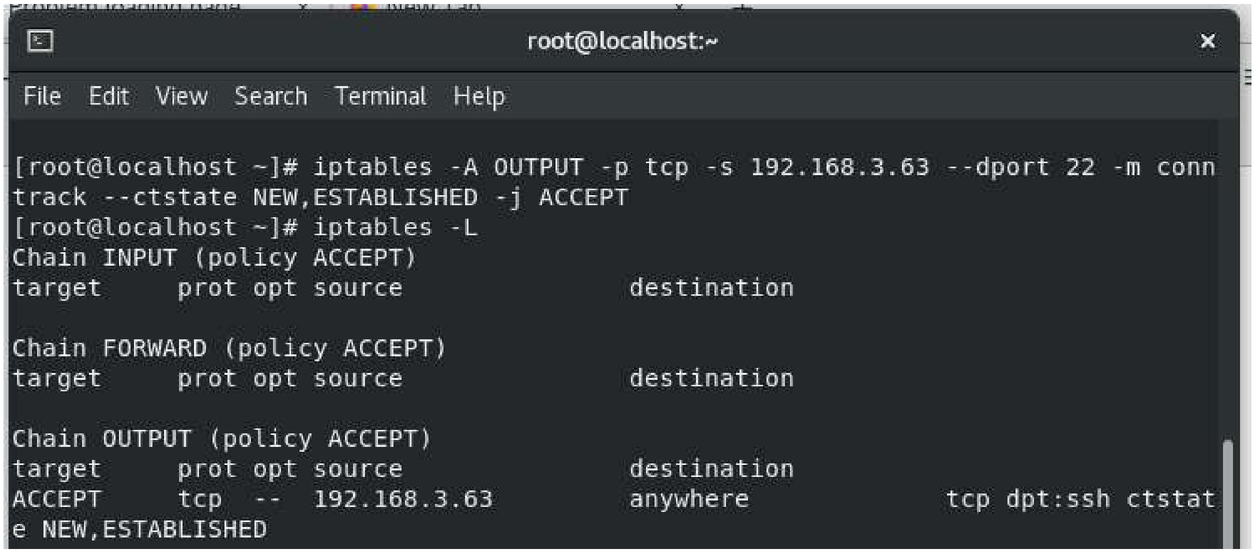


```
[root@localhost ~]# iptables -A INPUT -s 192.168.3.63 -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  192.168.3.63         anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
```

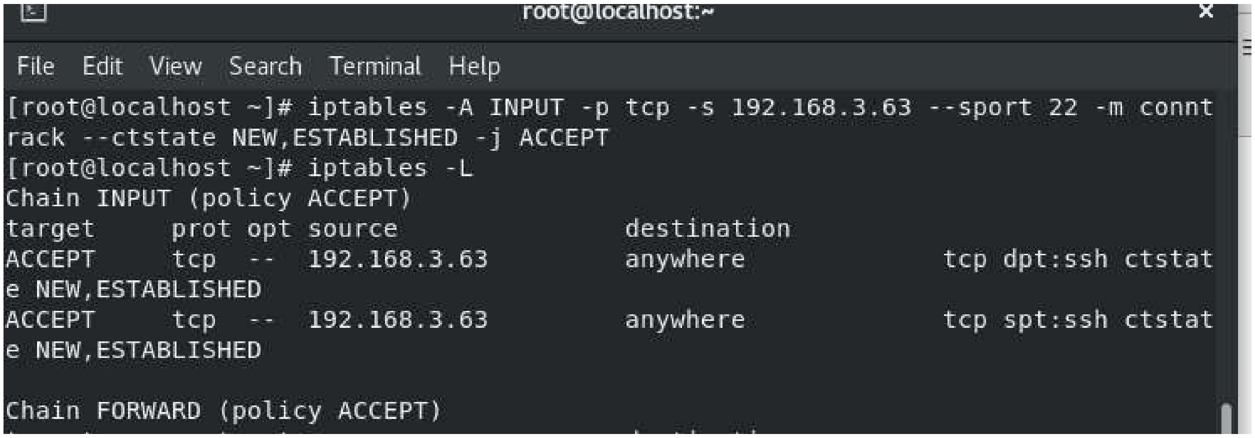


```
[root@localhost ~]# ping 192.168.3.66
PING 192.168.3.66 (192.168.3.66) 56(84) bytes of data.
64 bytes from 192.168.3.66: icmp_seq=1 ttl=64 time=1.91 ms
64 bytes from 192.168.3.66: icmp_seq=2 ttl=64 time=2.31 ms
64 bytes from 192.168.3.66: icmp_seq=3 ttl=64 time=1.50 ms
64 bytes from 192.168.3.66: icmp_seq=4 ttl=64 time=2.06 ms
64 bytes from 192.168.3.66: icmp_seq=5 ttl=64 time=2.47 ms
64 bytes from 192.168.3.66: icmp_seq=6 ttl=64 time=2.03 ms
^C
--- 192.168.3.66 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5019ms
rtt min/avg/max/mdev = 1.495/2.046/2.466/0.307 ms
[root@localhost ~]#
```

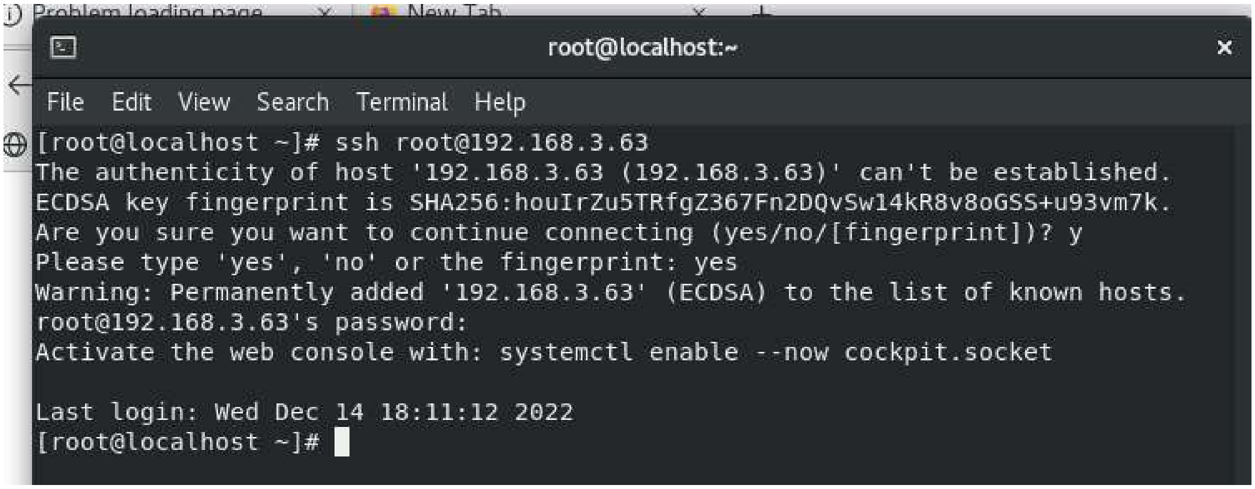
16. Allow outgoing connection on port 22 to the IP 192.168.1.2



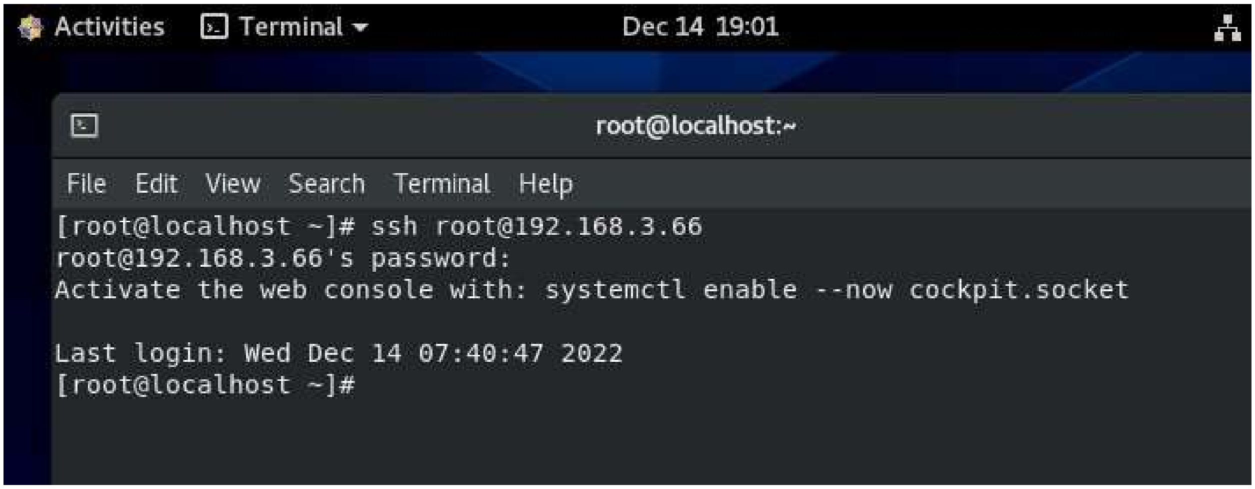
```
[root@localhost ~]# iptables -A OUTPUT -p tcp -s 192.168.3.63 --dport 22 -m conn
track --ctstate NEW,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.3.63         anywhere             tcp dpt:ssh ctstat
e NEW,ESTABLISHED
```



```
[root@localhost ~]# iptables -A INPUT -p tcp -s 192.168.3.63 --sport 22 -m connt
rack --ctstate NEW,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.3.63         anywhere             tcp dpt:ssh ctstat
e NEW,ESTABLISHED
ACCEPT     tcp  --  192.168.3.63         anywhere             tcp spt:ssh ctstat
e NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT)
```

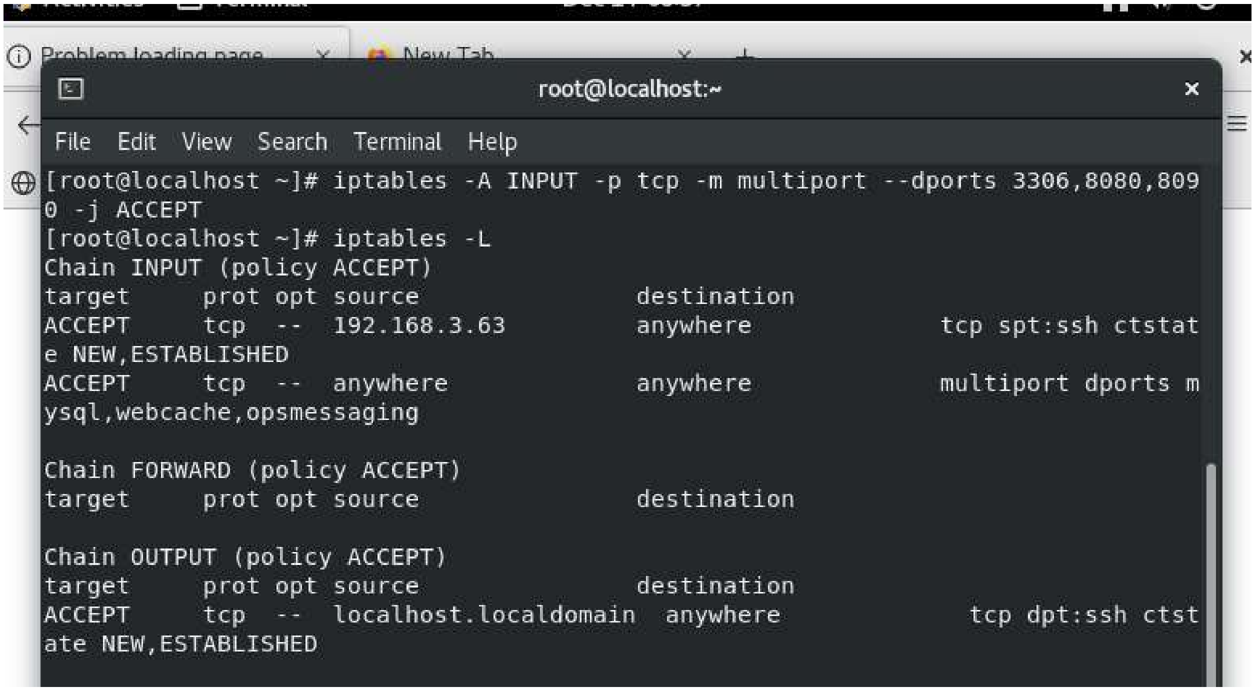


```
[root@localhost ~]# ssh root@192.168.3.63
The authenticity of host '192.168.3.63 (192.168.3.63)' can't be established.
ECDSA key fingerprint is SHA256:houIrZu5TRfgZ367Fn2DQvSw14kR8v8oGSS+u93vm7k.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.3.63' (ECDSA) to the list of known hosts.
root@192.168.3.63's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Dec 14 18:11:12 2022
[root@localhost ~]#
```



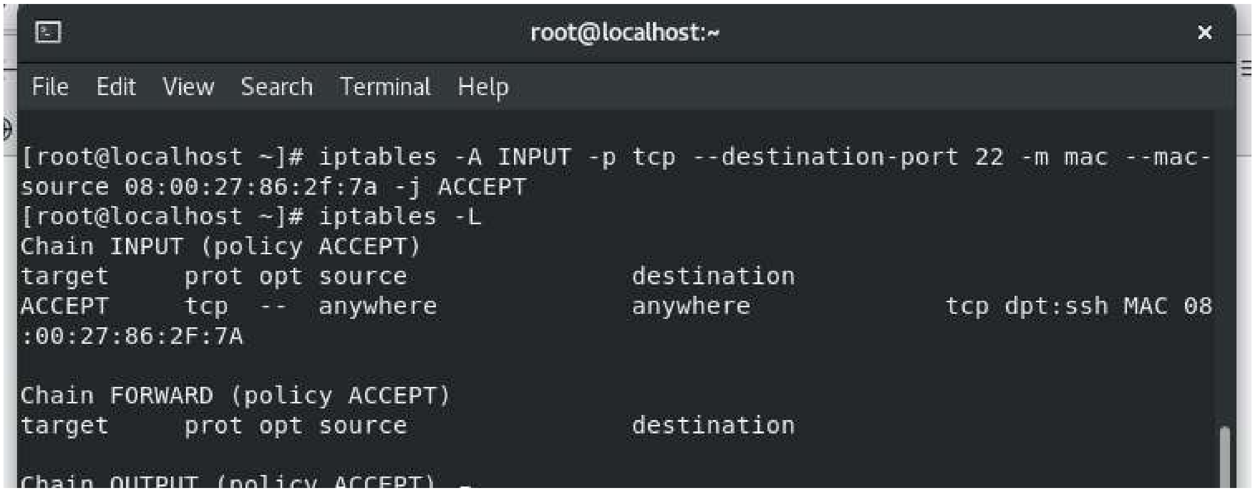
```
[root@localhost ~]# ssh root@192.168.3.66
root@192.168.3.66's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Dec 14 07:40:47 2022
[root@localhost ~]#
```

17. Write command to configure ports 3306,8080 and 8090 in a single command.

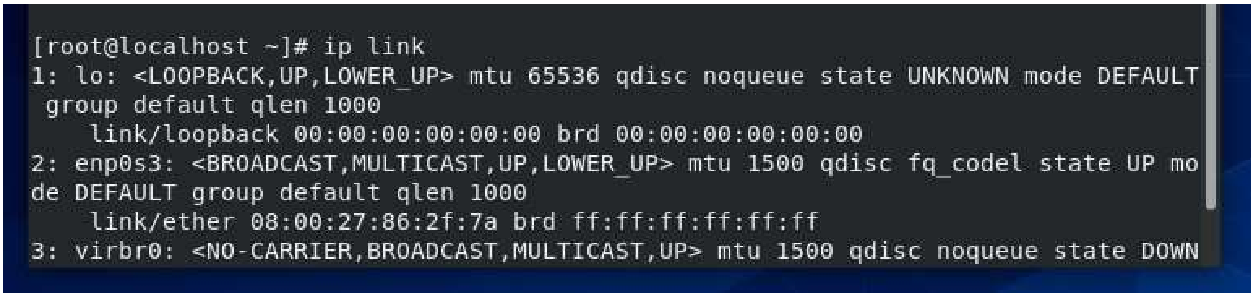


```
[root@localhost ~]# iptables -A INPUT -p tcp -m multiport --dports 3306,8080,809
0 -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.3.63         anywhere             tcp spt:ssh ctstat
e NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             multiport dports m
ysql,webcache,opsmessaging

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  localhost.localdomain  anywhere             tcp dpt:ssh ctst
ate NEW,ESTABLISHED
```

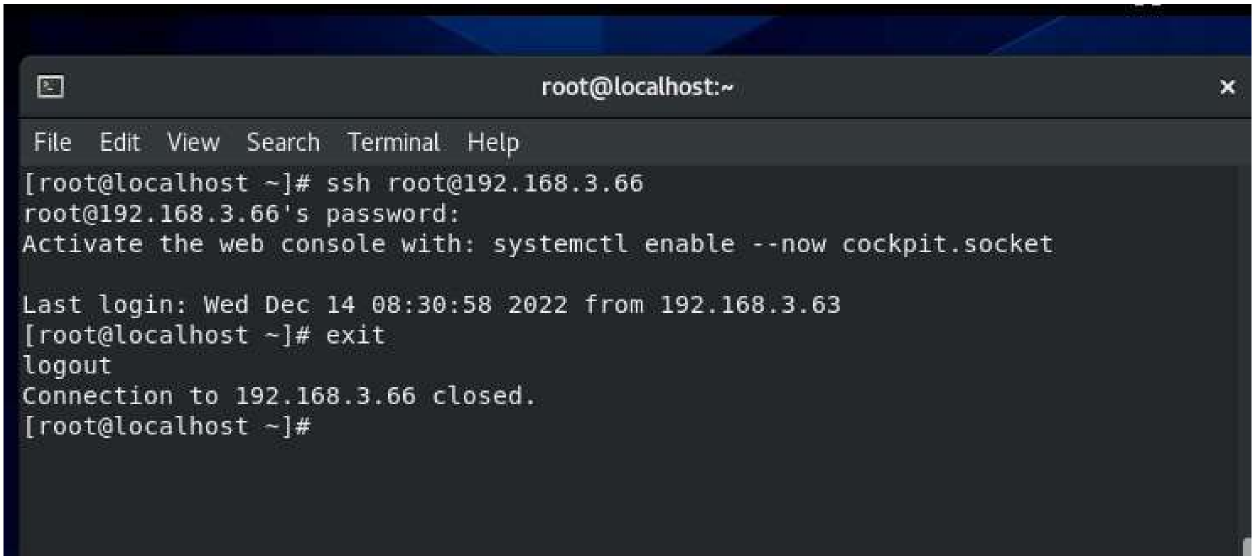
18. Allow the access of your system from the MAC address of machine1



```
[root@localhost ~]# iptables -A INPUT -p tcp --destination-port 22 -m mac --mac-
source 08:00:27:86:2f:7a -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh MAC 08
:00:27:86:2F:7A

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
```

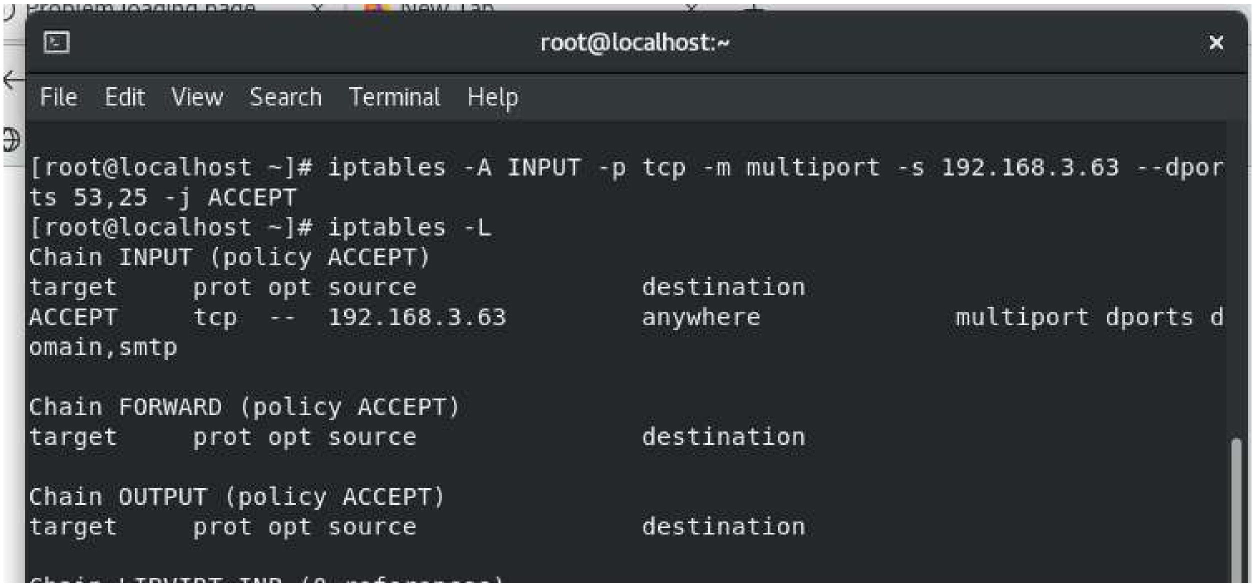


```
[root@localhost ~]# ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
 group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:86:2f:7a brd ff:ff:ff:ff:ff:ff
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
```

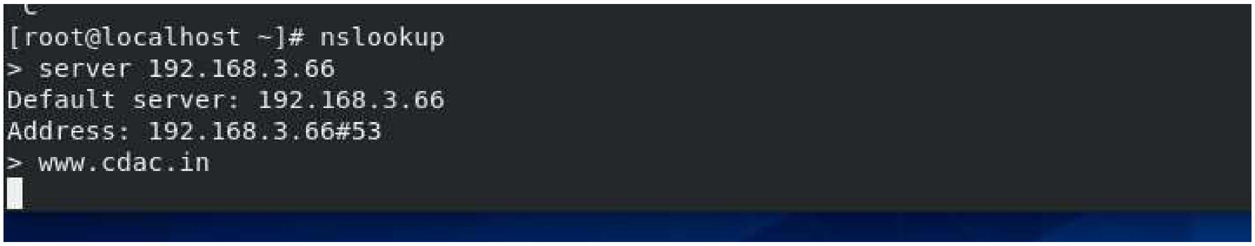


```
[root@localhost ~]# ssh root@192.168.3.66
root@192.168.3.66's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Dec 14 08:30:58 2022 from 192.168.3.63
[root@localhost ~]# exit
logout
Connection to 192.168.3.66 closed.
[root@localhost ~]#
```

19. Allow DNS & SMTP packets to travel in & out your machine

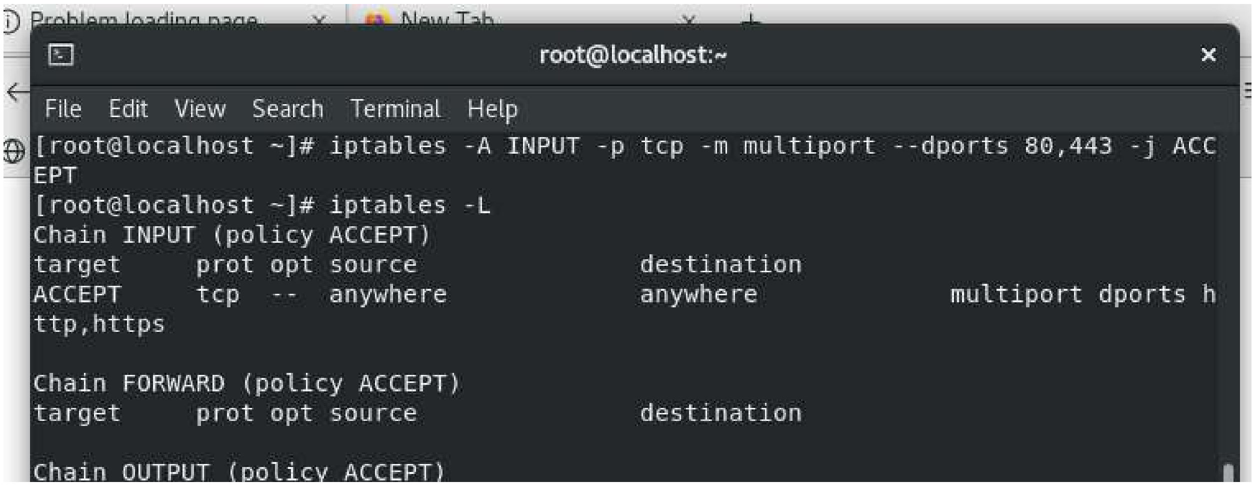


```
[root@localhost ~]# iptables -A INPUT -p tcp -m multiport -s 192.168.3.63 --dpor
ts 53,25 -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.3.63         anywhere             multiport dports d
omain,smtp

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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



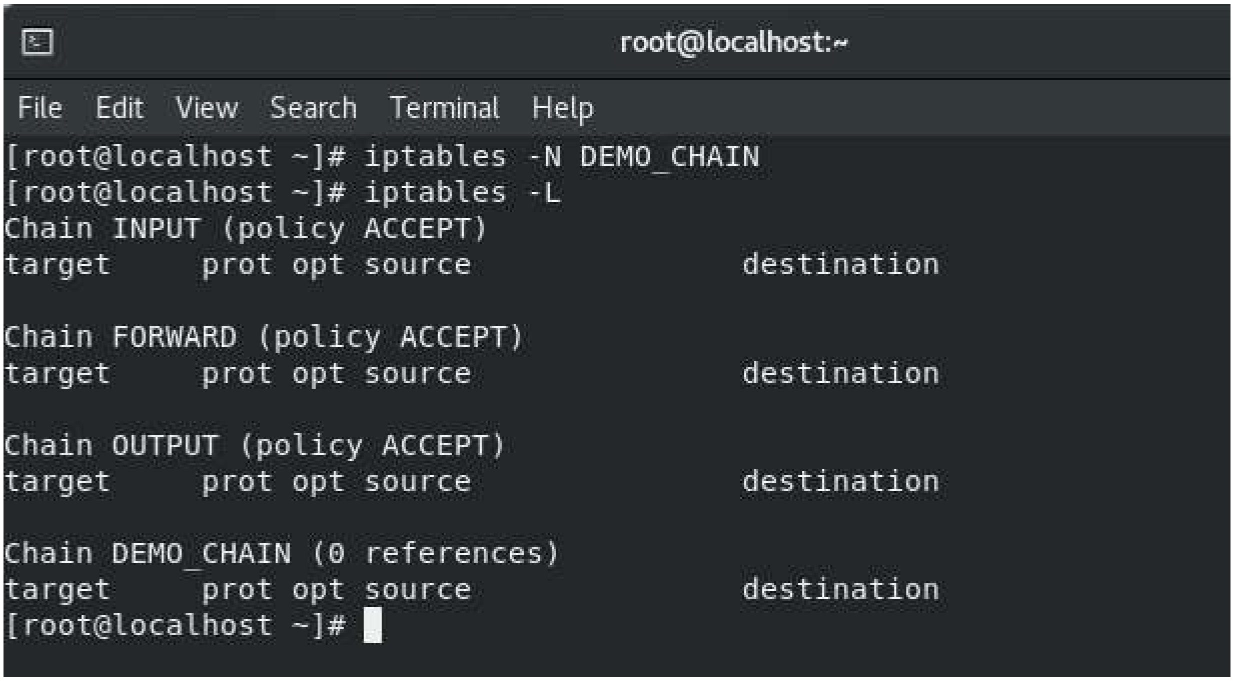
```
[root@localhost ~]# nslookup
> server 192.168.3.66
Default server: 192.168.3.66
Address: 192.168.3.66#53
> www.cdac.in
```

20. Allowing all incoming HTTP and HTTPS traffic



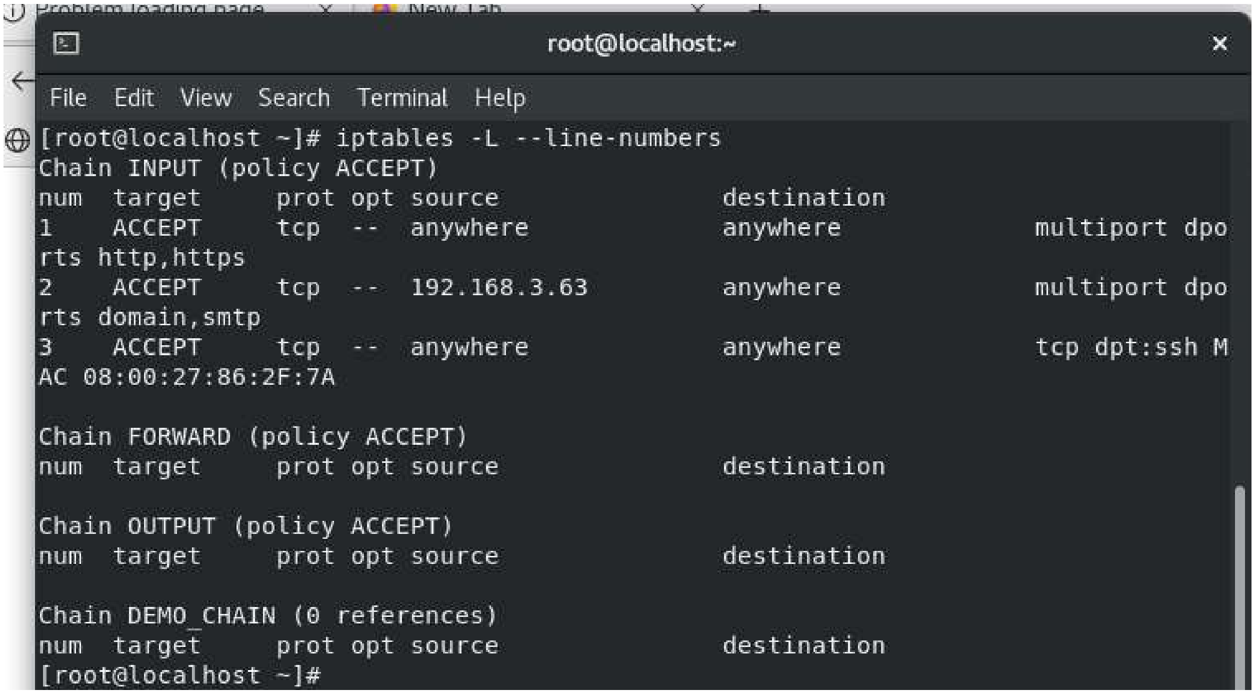
```
[root@localhost ~]# iptables -A INPUT -p tcp -m multiport --dports 80,443 -j ACC
EPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             multiport dports h
ttp,https

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
```

21. Add a new chain called “ DemoChain”



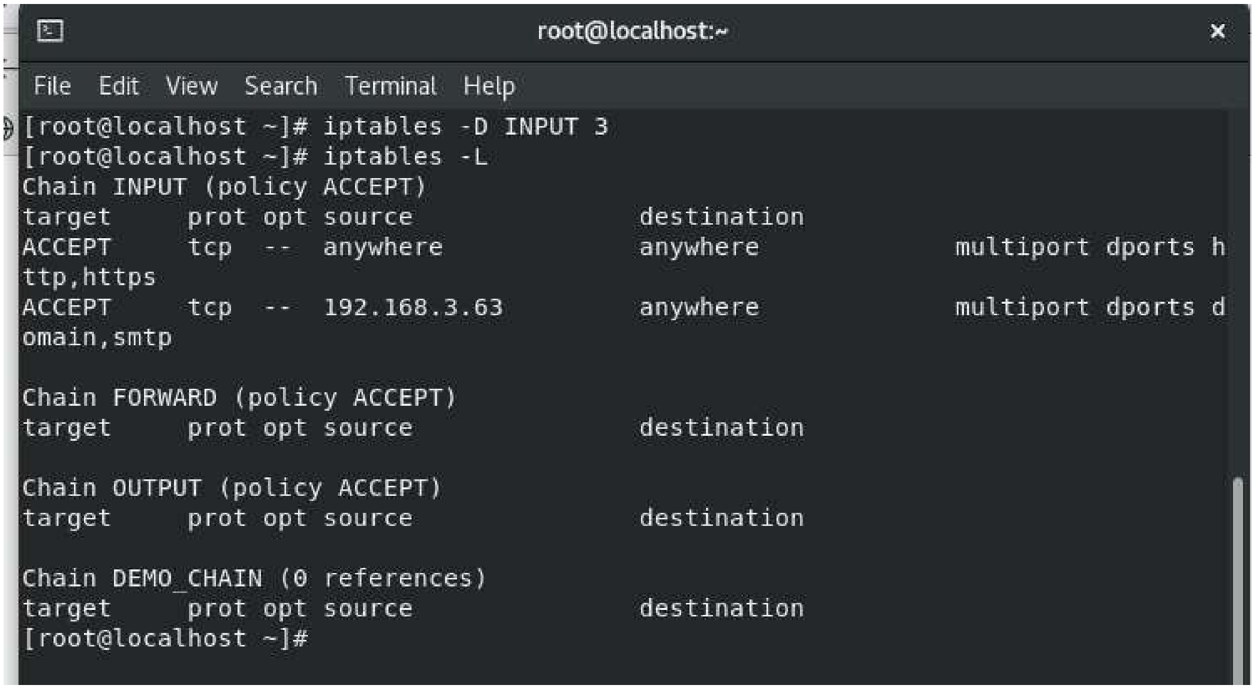
```
[root@localhost ~]# iptables -N DEMO_CHAIN
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain DEMO_CHAIN (0 references)
target     prot opt source               destination
[root@localhost ~]# 
```

22. List all the rules with line numbers



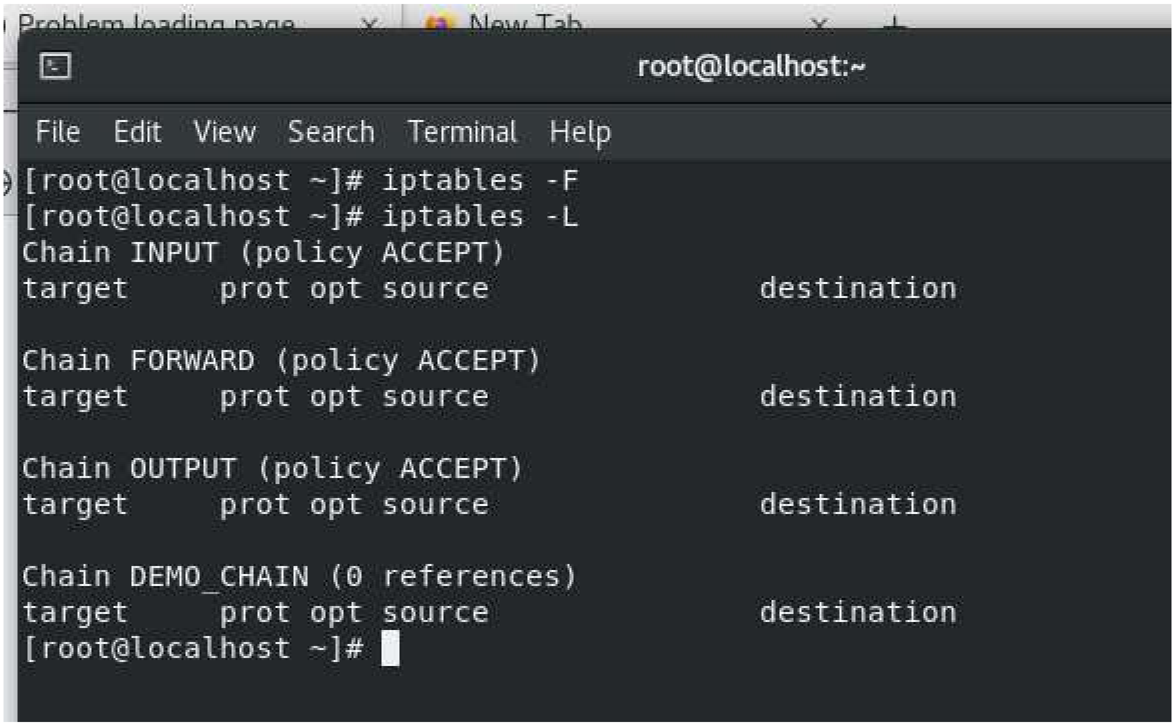
```
[root@localhost ~]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  anywhere             anywhere             multiport dpo
rts http,https
2    ACCEPT     tcp  --  192.168.3.63         anywhere             multiport dpo
rts domain,smtp
3    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh M
AC 08:00:27:86:2F:7A

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

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

Chain DEMO_CHAIN (0 references)
num  target     prot opt source               destination
[root@localhost ~]#
```

23. Delete the rule number 6



```
[root@localhost ~]# iptables -D INPUT 3
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             multiport dports h
ttp,https
ACCEPT     tcp  --  192.168.3.63         anywhere             multiport dports d
omain,smtp

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain DEMO_CHAIN (0 references)
target     prot opt source               destination
[root@localhost ~]#
```

24. Delete all the rules



```
[root@localhost ~]# iptables -F
[root@localhost ~]# 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

Chain DEMO_CHAIN (0 references)
target     prot opt source               destination
[root@localhost ~]#
```