Lab 7

Course: Networking and Data Security

COMP8677-1-R-2023F

Professor: Dr. Shaoquan Jiang

Prepared by

Harshil Hitendrabhai Panchal (110096129)

Due date: November 9, 2023

1. Use the following commands on router to set the default policies for a table.

sudo iptables –P INPUT ACCEPT

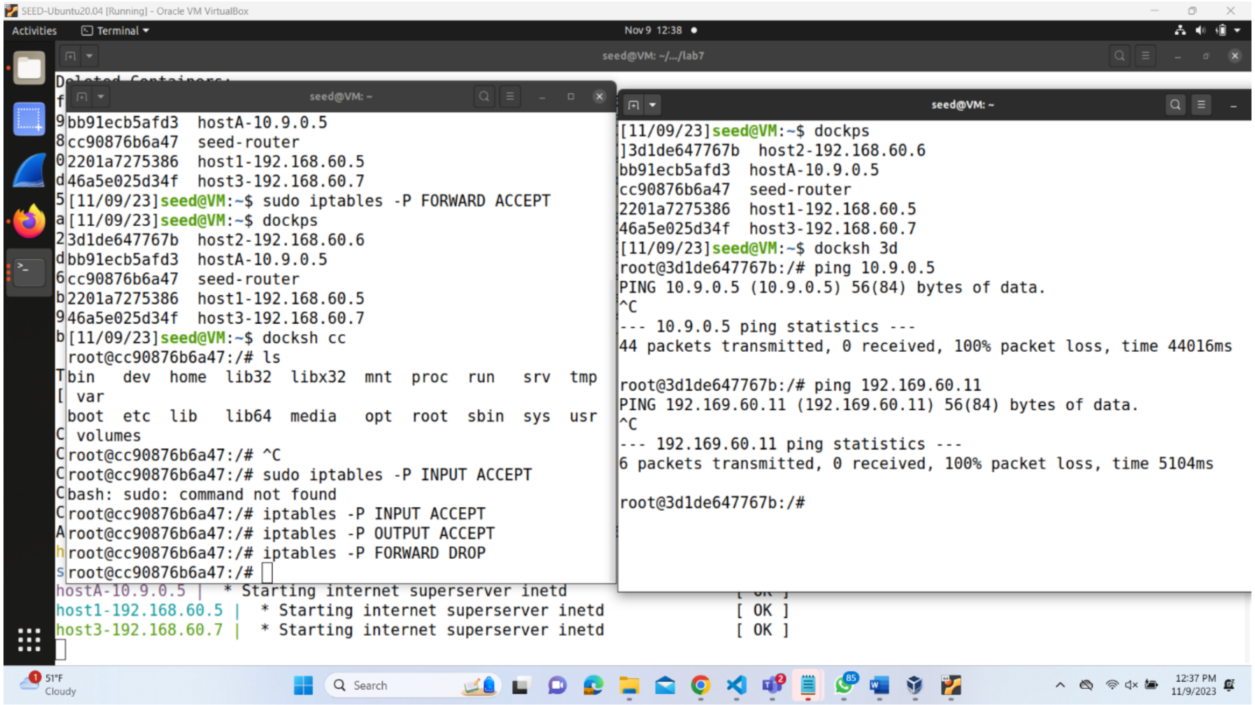
sudo iptables –P OUTPUT ACCEPT

sudo iptables –P FORWARD DROP

Recall, INPUT is to check incoming packet; OUTPUT is to check outgoing packet; FORWARDING is to check the passing packet (at router). Further, the commands assume the default table.

filter (-t filter).

- On 192.168.60.6, run **$ ping 10.9.0.5** and then ping 192.168.60.11. Does it succeed? Explain your observation.



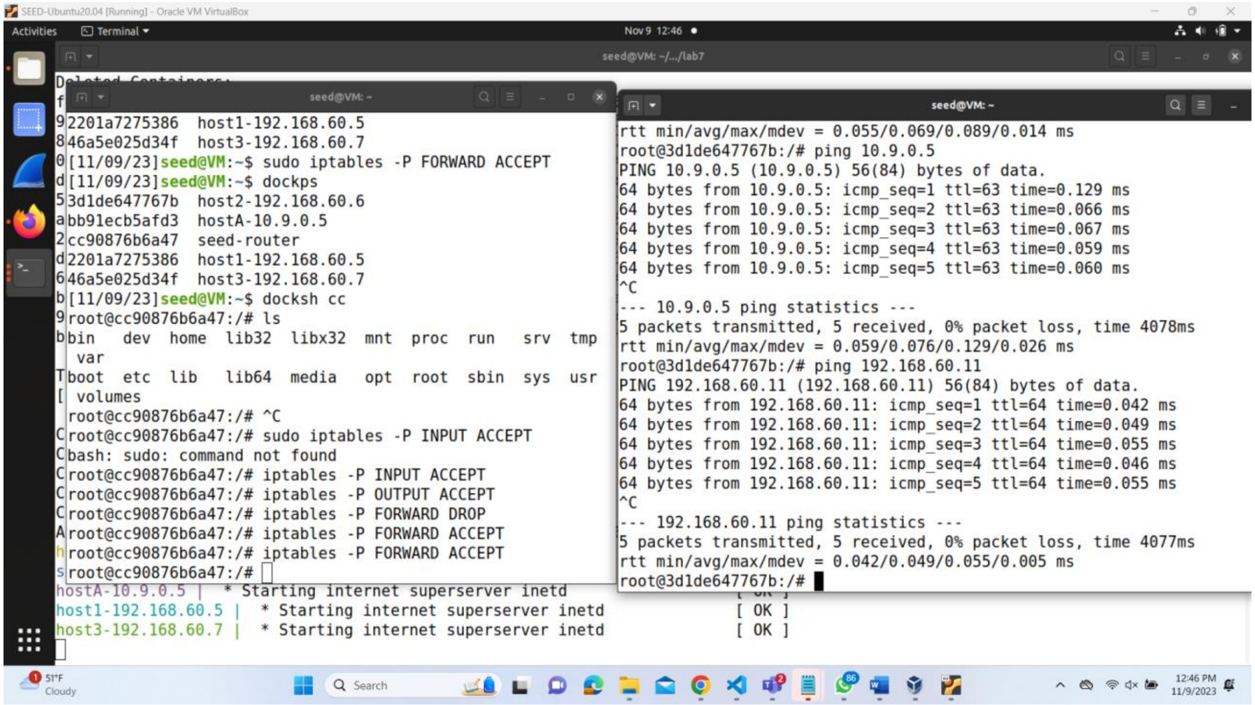
```
bb91ecb5afd3   hostA-10.9.0.5
cc90876b6a47   seed-router
2201a7275386   host1-192.168.60.5
46a5e025d34f   host3-192.168.60.7
[11/09/23]seed@VM:~$ sudo iptables -P FORWARD ACCEPT
[11/09/23]seed@VM:~$ dockps
3d1de647767b   host2-192.168.60.6
bb91ecb5afd3   hostA-10.9.0.5
cc90876b6a47   seed-router
2201a7275386   host1-192.168.60.5
46a5e025d34f   host3-192.168.60.7
[11/09/23]seed@VM:~$ docksh cc
root@cc90876b6a47:/# ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp
 var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr
 volumes
root@cc90876b6a47:/# ^C
root@cc90876b6a47:/# sudo iptables -P INPUT ACCEPT
bash: sudo: command not found
root@cc90876b6a47:/# iptables -P INPUT ACCEPT
root@cc90876b6a47:/# iptables -P OUTPUT ACCEPT
root@cc90876b6a47:/# iptables -P FORWARD DROP
root@cc90876b6a47:/# 
```

```
hostA-10.9.0.5 |  * Starting internet superserver inetd
host1-192.168.60.5 |  * Starting internet superserver inetd            [ OK ]
host3-192.168.60.7 |  * Starting internet superserver inetd            [ OK ]
```

```
[11/09/23]seed@VM:~$ dockps
]3d1de647767b  host2-192.168.60.6
bb91ecb5afd3  hostA-10.9.0.5
cc90876b6a47  seed-router
2201a7275386  host1-192.168.60.5
46a5e025d34f  host3-192.168.60.7
[11/09/23]seed@VM:~$ docksh 3d
root@3d1de647767b:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
^C
--- 10.9.0.5 ping statistics ---
44 packets transmitted, 0 received, 100% packet loss, time 44016ms

root@3d1de647767b:/# ping 192.169.60.11
PING 192.169.60.11 (192.169.60.11) 56(84) bytes of data.
^C
--- 192.169.60.11 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5104ms

root@3d1de647767b:/#
```

- Change **DROP** to **ACCEPT**, for FORWARD case. Try the pings in the above step again. Now does it succeed?

Observation: the default policy of FORWARD DROP prevents the router from forwarding packets between the specified networks, leading to unsuccessful pings between 192.168.60.6 and 10.9.0.5 or 192.168.60.11.



```
Deleted Containers:
f
92201a7275386  host1-192.168.60.5
846a5e025d34f  host3-192.168.60.7
0[11/09/23]seed@VM:~$ sudo iptables -P FORWARD ACCEPT
d[11/09/23]seed@VM:~$ dockps
53d1de647767b  host2-192.168.60.6
abb91ecb5afd3  hostA-10.9.0.5
2cc90876b6a47  seed-router
d2201a7275386  host1-192.168.60.5
646a5e025d34f  host3-192.168.60.7
b[11/09/23]seed@VM:~$ docksh cc
9root@cc90876b6a47:/# ls
bbin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp
  var
Tboot  etc  lib   lib64  media   opt  root  sbin  sys  usr
[ volumes
 root@cc90876b6a47:/# ^C
Croot@cc90876b6a47:/# sudo iptables -P INPUT ACCEPT
Cbash: sudo: command not found
Croot@cc90876b6a47:/# iptables -P INPUT ACCEPT
Croot@cc90876b6a47:/# iptables -P OUTPUT ACCEPT
Croot@cc90876b6a47:/# iptables -P FORWARD DROP
Aroot@cc90876b6a47:/# iptables -P FORWARD ACCEPT
hroot@cc90876b6a47:/# iptables -P FORWARD ACCEPT
sroot@cc90876b6a47:/# 
hostA-10.9.0.5 |  * Starting internet superserver inetd
host1-192.168.60.5 |  * Starting internet superserver inetd        [ OK ]
host3-192.168.60.7 |  * Starting internet superserver inetd        [ OK ]
```

```
rtt min/avg/max/mdev = 0.055/0.069/0.089/0.014 ms
root@3d1de647767b:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.129 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.066 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.067 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.059 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.060 ms
^C
--- 10.9.0.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.059/0.076/0.129/0.026 ms
root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
64 bytes from 192.168.60.11: icmp_seq=1 ttl=64 time=0.042 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 192.168.60.11: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 192.168.60.11: icmp_seq=4 ttl=64 time=0.046 ms
64 bytes from 192.168.60.11: icmp_seq=5 ttl=64 time=0.055 ms
^C
--- 192.168.60.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 0.042/0.049/0.055/0.005 ms
root@3d1de647767b:/# 
```

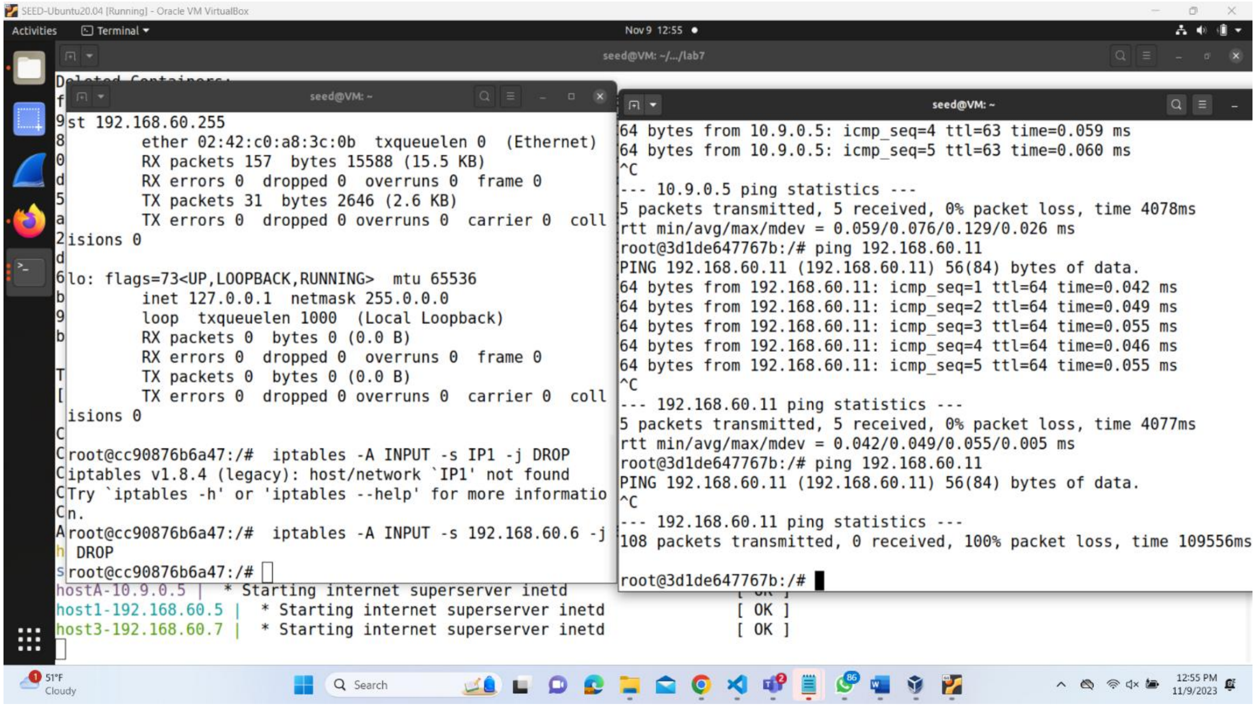
2. . [blocking an IP]

a. On 192.168.60.11, if we want to block packets from an ip address IP1, use command

sudo iptables -A INPUT -s IP1 -j DROP

/*this uses INPUT chain because it is incoming packet*/

On IP1, ping 192.168.60.11 and what can be observed? Explain.



```
Deleted Containers:
f
9st 192.168.60.255
8        ether 02:42:c0:a8:3c:0b  txqueuelen 0  (Ethernet)
0        RX packets 157  bytes 15588 (15.5 KB)
d        RX errors 0  dropped 0  overruns 0  frame 0
5        TX packets 31  bytes 2646 (2.6 KB)
a        TX errors 0  dropped 0 overruns 0  carrier 0  coll
2isions 0
d
6lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
b        inet 127.0.0.1  netmask 255.0.0.0
9        loop  txqueuelen 1000  (Local Loopback)
b        RX packets 0  bytes 0 (0.0 B)
         RX errors 0  dropped 0  overruns 0  frame 0
T        TX packets 0  bytes 0 (0.0 B)
[        TX errors 0  dropped 0 overruns 0  carrier 0  coll
 isions 0
C
Croot@cc90876b6a47:/#  iptables -A INPUT -s IP1 -j DROP
Ciptables v1.8.4 (legacy): host/network `IP1' not found
CTry `iptables -h' or 'iptables --help' for more informatio
Cn.
Aroot@cc90876b6a47:/#  iptables -A INPUT -s 192.168.60.6 -j
h DROP
sroot@cc90876b6a47:/# 
hostA-10.9.0.5 |  * Starting internet superserver inetd
host1-192.168.60.5 |  * Starting internet superserver inetd        [ OK ]
host3-192.168.60.7 |  * Starting internet superserver inetd        [ OK ]
```

```
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.059 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.060 ms
^C
--- 10.9.0.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.059/0.076/0.129/0.026 ms
root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
64 bytes from 192.168.60.11: icmp_seq=1 ttl=64 time=0.042 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 192.168.60.11: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 192.168.60.11: icmp_seq=4 ttl=64 time=0.046 ms
64 bytes from 192.168.60.11: icmp_seq=5 ttl=64 time=0.055 ms
^C
--- 192.168.60.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 0.042/0.049/0.055/0.005 ms
root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
^C
--- 192.168.60.11 ping statistics ---
108 packets transmitted, 0 received, 100% packet loss, time 109556ms

root@3d1de647767b:/# 
```

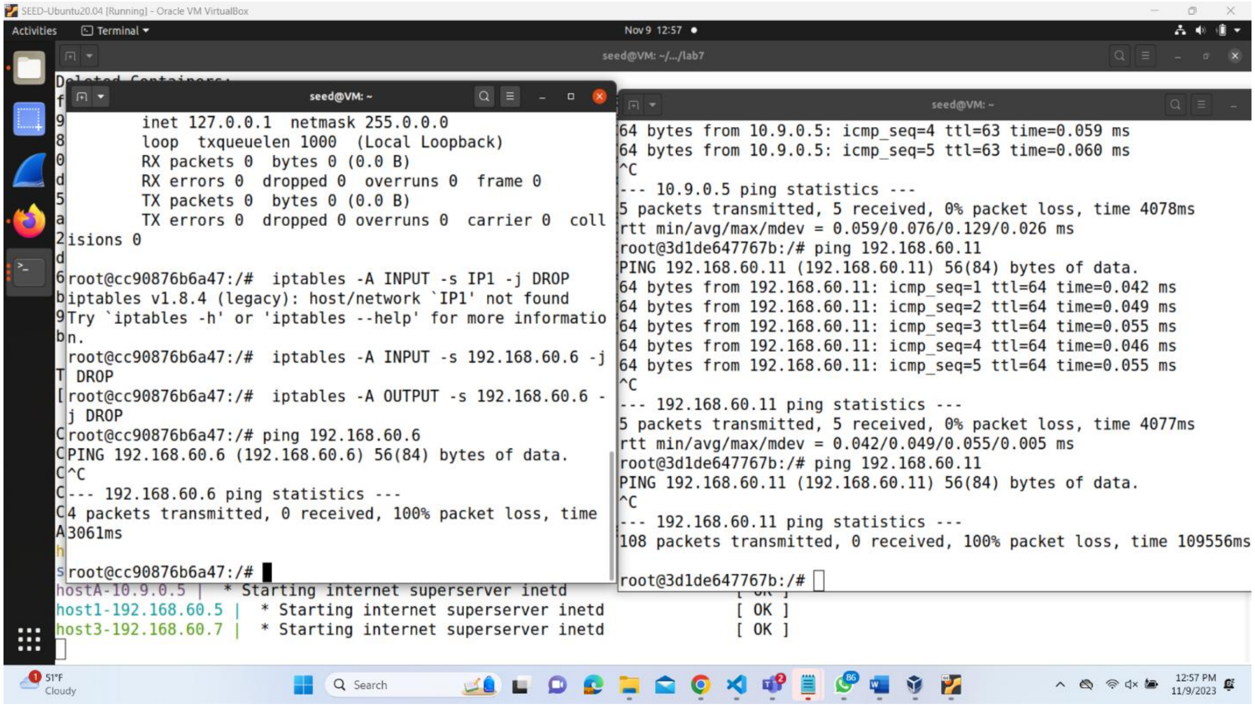
Observation: As we have blocked 192.168.60.6 on Router, if I ping from 192.168.60.6 to Router, all packets will be lost, and no packets are received on Router end.

b. On 192.168.60.11, if we want to block packets to an ip address IP1, use command

sudo iptables -A OUTPUT -d IP1 -j DROP

/*this uses OUTPUT chain because it is outgoing packet*/

On 192.168.60.11, ping IP1 and what can be observed? Explain.



```
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        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  coll
isions 0

root@cc90876b6a47:/#  iptables -A INPUT -s IP1 -j DROP
iptables v1.8.4 (legacy): host/network `IP1' not found
Try `iptables -h' or 'iptables --help' for more informatio
n.
root@cc90876b6a47:/#  iptables -A INPUT -s 192.168.60.6 -j
 DROP
root@cc90876b6a47:/#  iptables -A OUTPUT -s 192.168.60.6 -
j DROP
root@cc90876b6a47:/# ping 192.168.60.6
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
^C
--- 192.168.60.6 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time
3061ms

root@cc90876b6a47:/# 
```

```
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.059 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=63 time=0.060 ms
^C
--- 10.9.0.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.059/0.076/0.129/0.026 ms
root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
64 bytes from 192.168.60.11: icmp_seq=1 ttl=64 time=0.042 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 192.168.60.11: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 192.168.60.11: icmp_seq=4 ttl=64 time=0.046 ms
64 bytes from 192.168.60.11: icmp_seq=5 ttl=64 time=0.055 ms
^C
--- 192.168.60.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 0.042/0.049/0.055/0.005 ms
root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
^C
--- 192.168.60.11 ping statistics ---
108 packets transmitted, 0 received, 100% packet loss, time 109556ms

root@3d1de647767b:/# 
```

```
hostA-10.9.0.5 |   * Starting internet superserver inetd
host1-192.168.60.5 |  * Starting internet superserver inetd          [ OK ]
host3-192.168.60.7 |  * Starting internet superserver inetd          [ OK ]
```

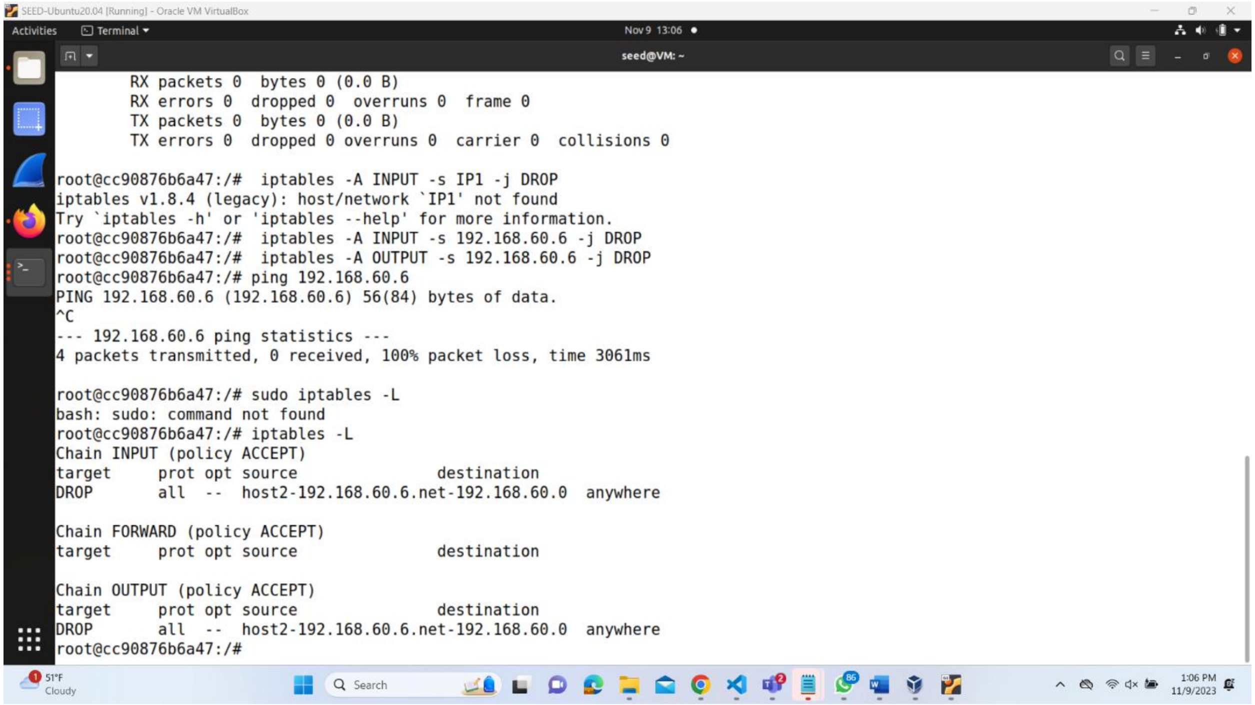
Observation: As we have blocked the OUTPUT to 192.168.60.6, when we try to send packets from router to this IP, it will drop all the packets.

3. [List all rules] do it on Router.

a. You can see all the firewall rules by the following command

$ sudo iptables -L

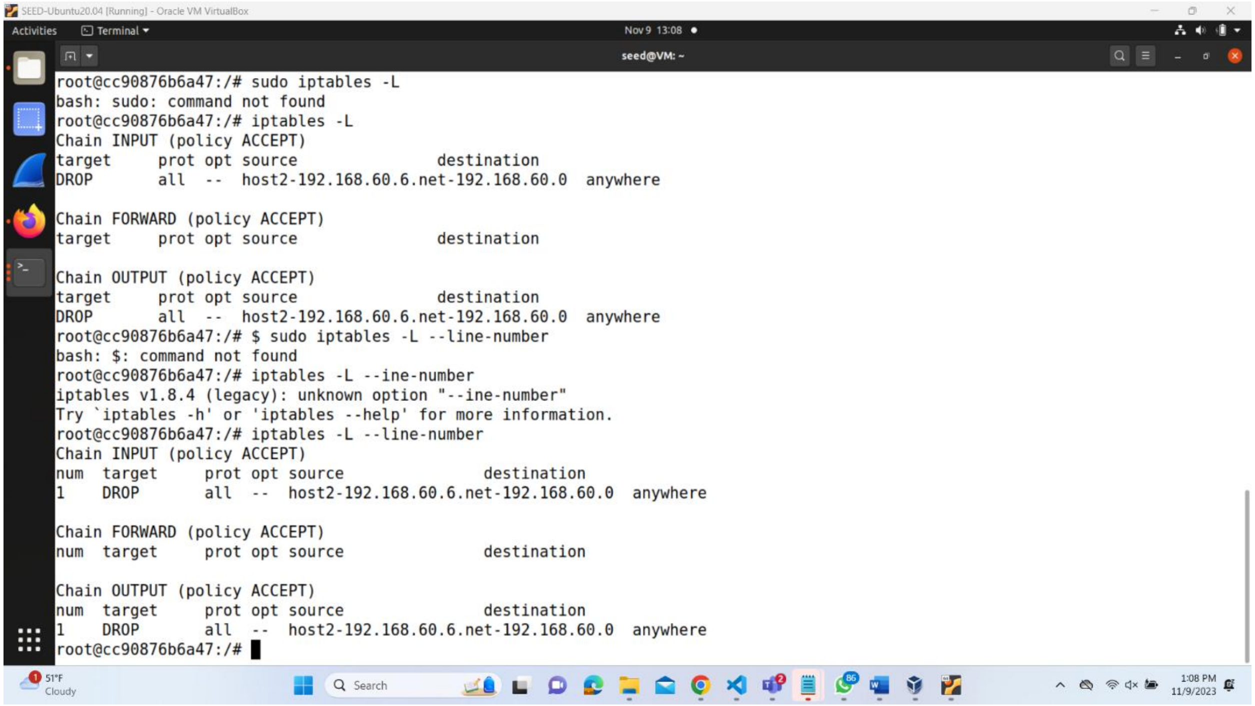
/* again, this assume filter table (i.e., **-t filter**) by default*/



```
        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@cc90876b6a47:/#  iptables -A INPUT -s IP1 -j DROP
iptables v1.8.4 (legacy): host/network `IP1' not found
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/#  iptables -A INPUT -s 192.168.60.6 -j DROP
root@cc90876b6a47:/#  iptables -A OUTPUT -s 192.168.60.6 -j DROP
root@cc90876b6a47:/# ping 192.168.60.6
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
^C
--- 192.168.60.6 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3061ms

root@cc90876b6a47:/# sudo iptables -L
bash: sudo: command not found
root@cc90876b6a47:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere
root@cc90876b6a47:/#
```

b. You can see all the fire rules in each chain with index number. The index will be used for other operation such as deletion later.

$ sudo iptables -L --line-number



```
root@cc90876b6a47:/# sudo iptables -L
bash: sudo: command not found
root@cc90876b6a47:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere
root@cc90876b6a47:/# $ sudo iptables -L --line-number
bash: $: command not found
root@cc90876b6a47:/# iptables -L --ine-number
iptables v1.8.4 (legacy): unknown option "--ine-number"
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere
root@cc90876b6a47:/# 
```

4. [Delete a rule] on Router, delete a rule in a chain (such as INPUT) in two steps:

first, list with index:

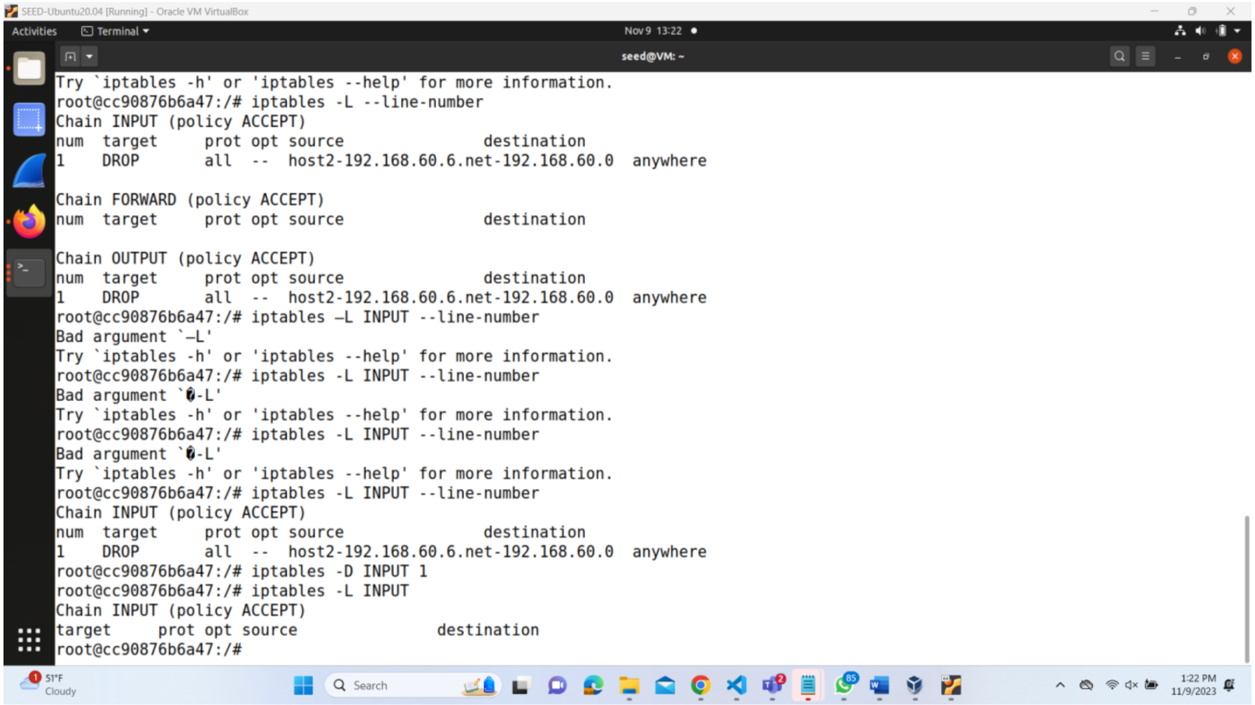
$ sudo iptables –L INPUT --line-number

Then, delete the rule using the index:

$sudo iptables -D INPUT 1

Now use the method to delete the first rule in your current INPUT table and then

$ sudo iptables -L INPUT to verify whether rule 1 is deleted or not.

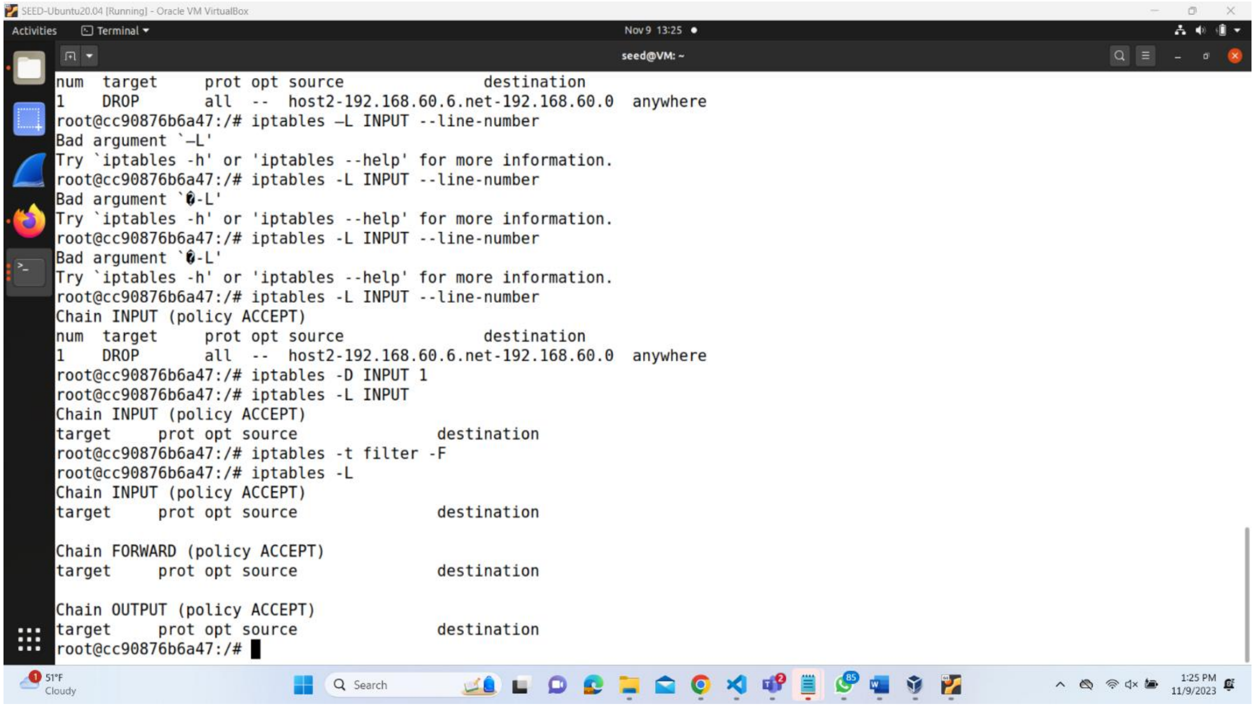


```
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere
root@cc90876b6a47:/# iptables –L INPUT --line-number
Bad argument `–L'
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -L INPUT --line-number
Bad argument `�-L'
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -L INPUT --line-number
Bad argument `�-L'
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -L INPUT --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere
root@cc90876b6a47:/# iptables -D INPUT 1
root@cc90876b6a47:/# iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
root@cc90876b6a47:/#
```

5. [Delete all rules in a TABLE]

On router, flush the rules in a table (e.g., filter):
$sudo iptables -t filter -F
/*again,**-t filter** can be omitted*/

Then, run **$sudo iptables -L** and you will not see any rule.



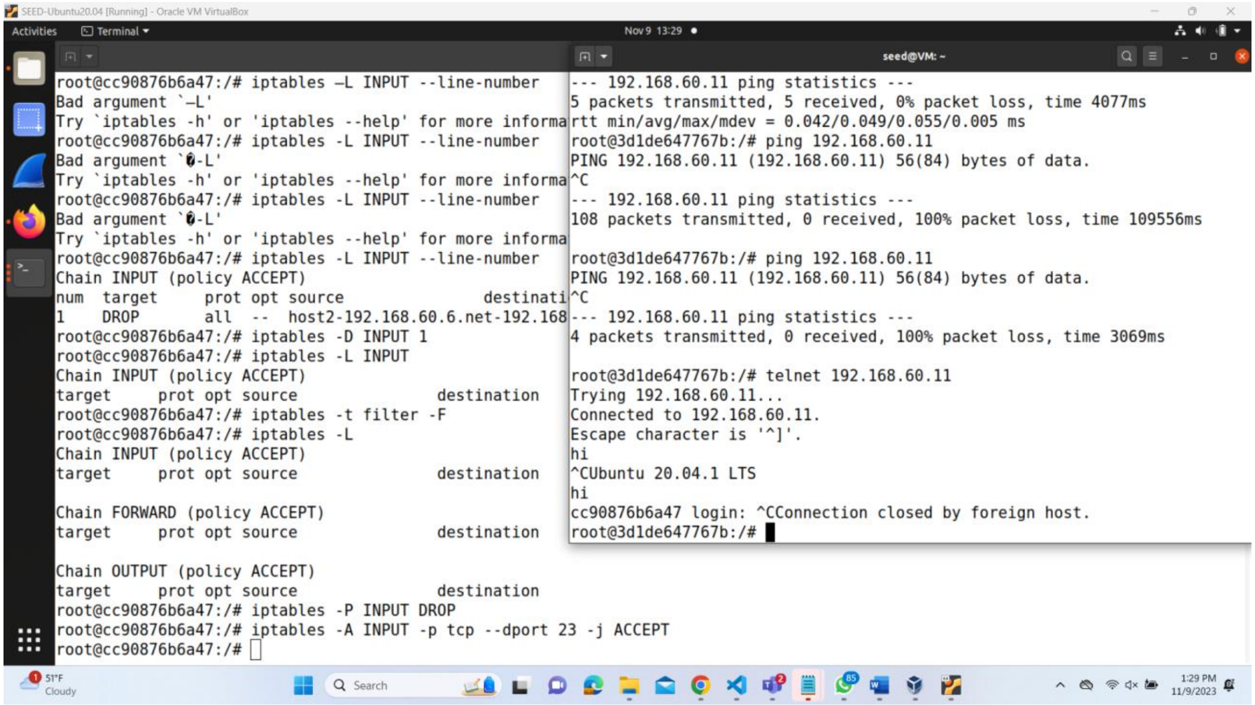
```
num  target     prot opt source               destination
1    DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere
root@cc90876b6a47:/# iptables –L INPUT --line-number
Bad argument `–L'
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -L INPUT --line-number
Bad argument `�-L'
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -L INPUT --line-number
Bad argument `�-L'
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -L INPUT --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  host2-192.168.60.6.net-192.168.60.0  anywhere
root@cc90876b6a47:/# iptables -D INPUT 1
root@cc90876b6a47:/# iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
root@cc90876b6a47:/# iptables -t filter -F
root@cc90876b6a47:/# 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@cc90876b6a47:/# 
```

6. [Drop all incoming connections, except telnet]

On router, block incoming connections to any service except for telnet. To do this, we can set default policy for INPUT chain of filter Table to be DROP and then specify a rule to accept incoming telnet connection.

$ sudo iptables -P INPUT DROP
$ sudo iptables -A INPUT -p tcp - -dport 23 -j ACCEPT
/* A default policy is applied only if all the rules in the chain have been executed without making a decision (either ACCEPT or DROP or REJECT). For example, if we ssh to router, then the rule does not ACCEPT but also not REJECT. So the default policy applies. Note: here -p stands for protocol. */

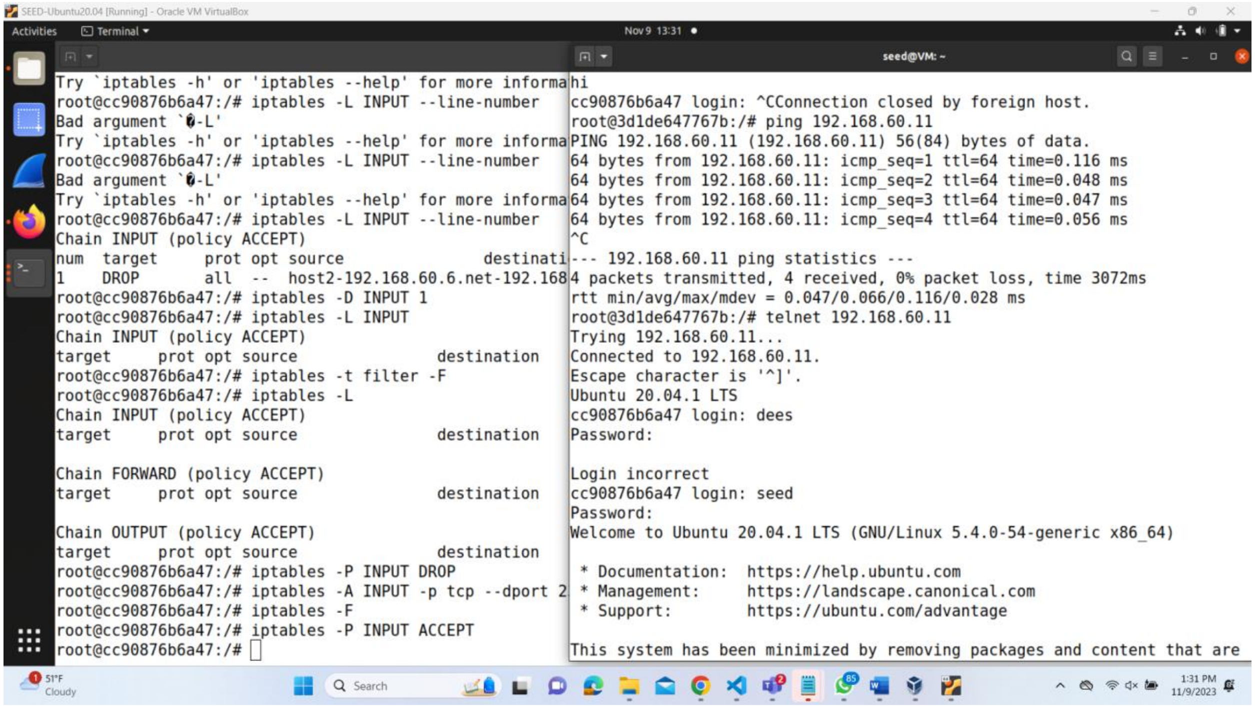
Then, ping and telnet to 192.168.60.11 (from other VM). Which succeeds (telnet or ping)?
Ping – Don’t
Telnet – Succeeded



```
root@cc90876b6a47:/# iptables –L INPUT --line-number
Bad argument `–L'
Try `iptables -h' or 'iptables --help' for more informa
root@cc90876b6a47:/# iptables -L INPUT --line-number
Bad argument `�-L'
Try `iptables -h' or 'iptables --help' for more informa
root@cc90876b6a47:/# iptables -L INPUT --line-number
Bad argument `�-L'
Try `iptables -h' or 'iptables --help' for more informa
root@cc90876b6a47:/# iptables -L INPUT --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destinati
1    DROP       all  --  host2-192.168.60.6.net-192.168
root@cc90876b6a47:/# iptables -D INPUT 1
root@cc90876b6a47:/# iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
root@cc90876b6a47:/# iptables -t filter -F
root@cc90876b6a47:/# 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@cc90876b6a47:/# iptables -P INPUT DROP
root@cc90876b6a47:/# iptables -A INPUT -p tcp --dport 23 -j ACCEPT
root@cc90876b6a47:/# 
```

```
--- 192.168.60.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 0.042/0.049/0.055/0.005 ms
root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
^C
--- 192.168.60.11 ping statistics ---
108 packets transmitted, 0 received, 100% packet loss, time 109556ms

root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
^C
--- 192.168.60.11 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3069ms

root@3d1de647767b:/# telnet 192.168.60.11
Trying 192.168.60.11...
Connected to 192.168.60.11.
Escape character is '^]'.
hi
^CUbuntu 20.04.1 LTS
hi
cc90876b6a47 login: ^CConnection closed by foreign host.
root@3d1de647767b:/# 
```

/*after this problem, run **$ sudo iptables -F** to flush all rules in filter table and recover the default policy: **$ sudo iptables -P INPUT ACCEPT */**



```
Try `iptables -h' or 'iptables --help' for more informa
root@cc90876b6a47:/# iptables -L INPUT --line-number
Bad argument `�-L'
Try `iptables -h' or 'iptables --help' for more informa
root@cc90876b6a47:/# iptables -L INPUT --line-number
Bad argument `�-L'
Try `iptables -h' or 'iptables --help' for more informa
root@cc90876b6a47:/# iptables -L INPUT --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destinati
1    DROP       all  --  host2-192.168.60.6.net-192.168
root@cc90876b6a47:/# iptables -D INPUT 1
root@cc90876b6a47:/# iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
root@cc90876b6a47:/# iptables -t filter -F
root@cc90876b6a47:/# 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@cc90876b6a47:/# iptables -P INPUT DROP
root@cc90876b6a47:/# iptables -A INPUT -p tcp --dport 2
root@cc90876b6a47:/# iptables -F
root@cc90876b6a47:/# iptables -P INPUT ACCEPT
root@cc90876b6a47:/# 
```

```
hi
cc90876b6a47 login: ^CConnection closed by foreign host.
root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
64 bytes from 192.168.60.11: icmp_seq=1 ttl=64 time=0.116 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=64 time=0.048 ms
64 bytes from 192.168.60.11: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 192.168.60.11: icmp_seq=4 ttl=64 time=0.056 ms
^C
--- 192.168.60.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.047/0.066/0.116/0.028 ms
root@3d1de647767b:/# telnet 192.168.60.11
Trying 192.168.60.11...
Connected to 192.168.60.11.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
cc90876b6a47 login: dees
Password:

Login incorrect
cc90876b6a47 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
```

7. [drop outgoing DNS request to 8.8.8.8]

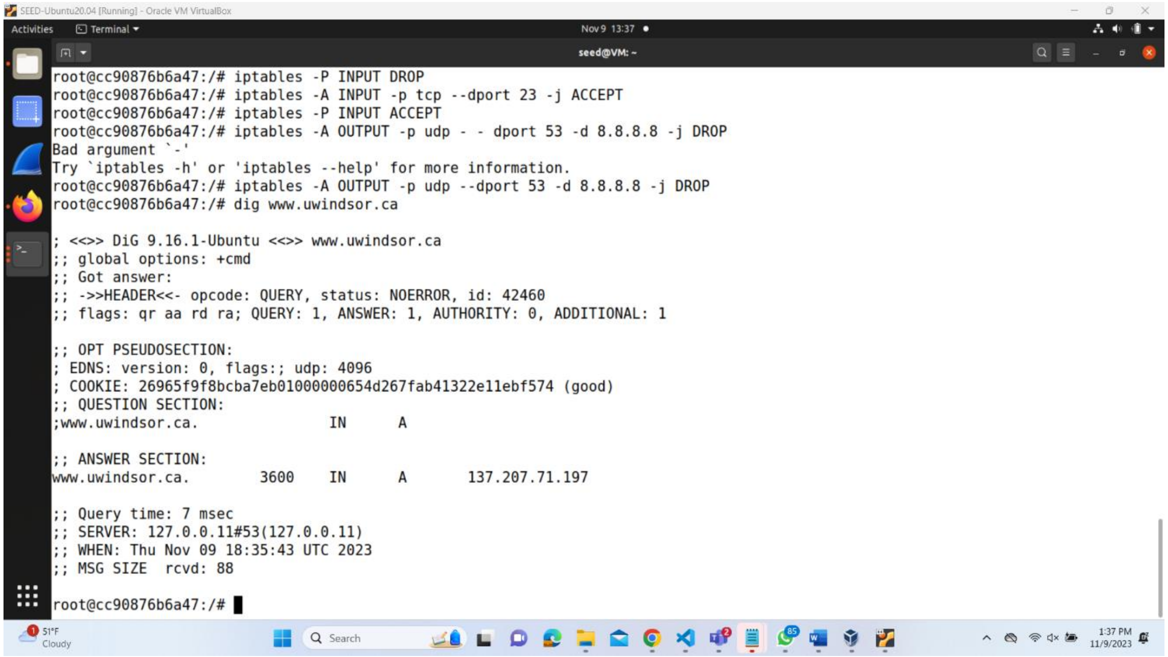
In this case, since it is outgoing packet, we add rule to OUTPUT chain. Since it is DNS request, the destination should be the DNS server, which has a port number 53. Finally, since DNS is implemented using UDP, we use protocol UDP. Hence, we add the following rule:

$ sudo iptables -A OUTPUT -p udp - - dport 53 -d 8.8.8.8 -j DROP

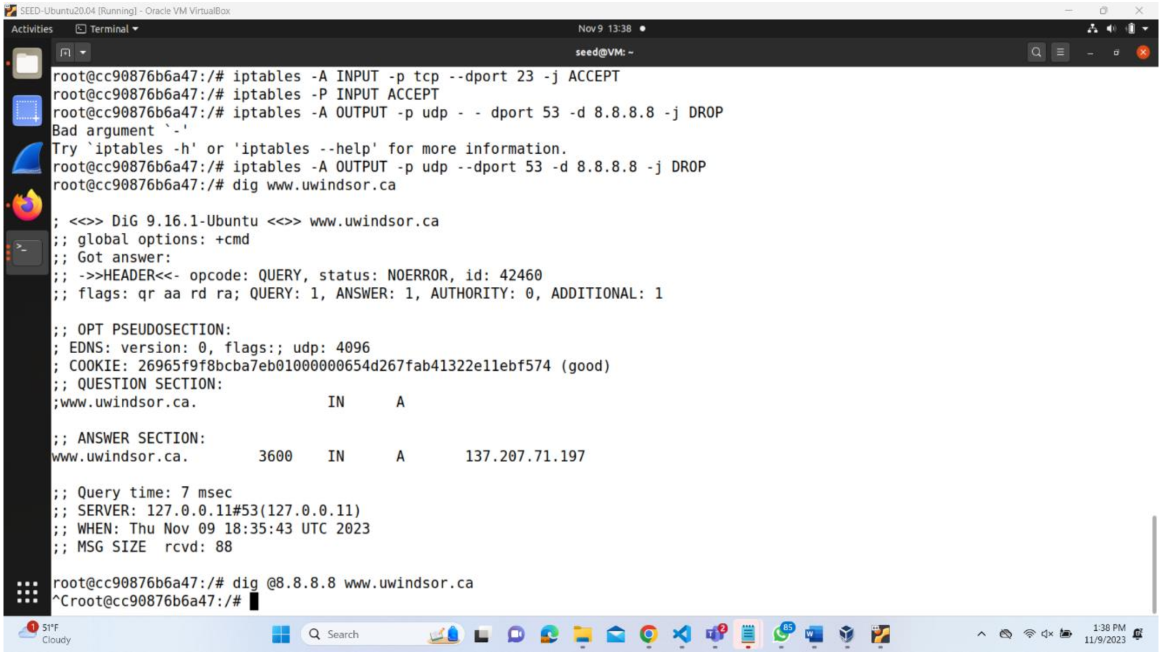
Then, try $ **dig www.uwindsor.ca** and **dig @8.8.8.8 www.uwindsor.ca.** Which succeeds?

/* delete the rule in order not to affect the following experiment */

dig www.uwindsor.ca - succeeds



```
root@cc90876b6a47:/# iptables -P INPUT DROP
root@cc90876b6a47:/# iptables -A INPUT -p tcp --dport 23 -j ACCEPT
root@cc90876b6a47:/# iptables -P INPUT ACCEPT
root@cc90876b6a47:/# iptables -A OUTPUT -p udp - - dport 53 -d 8.8.8.8 -j DROP
Bad argument `-'
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -A OUTPUT -p udp --dport 53 -d 8.8.8.8 -j DROP
root@cc90876b6a47:/# dig www.uwindsor.ca

; <<>> DiG 9.16.1-Ubuntu <<>> www.uwindsor.ca
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42460
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 26965f9f8bcba7eb01000000654d267fab41322e11ebf574 (good)
;; QUESTION SECTION:
;www.uwindsor.ca.               IN      A

;; ANSWER SECTION:
www.uwindsor.ca.        3600    IN      A       137.207.71.197

;; Query time: 7 msec
;; SERVER: 127.0.0.11#53(127.0.0.11)
;; WHEN: Thu Nov 09 18:35:43 UTC 2023
;; MSG SIZE  rcvd: 88

root@cc90876b6a47:/# 
```



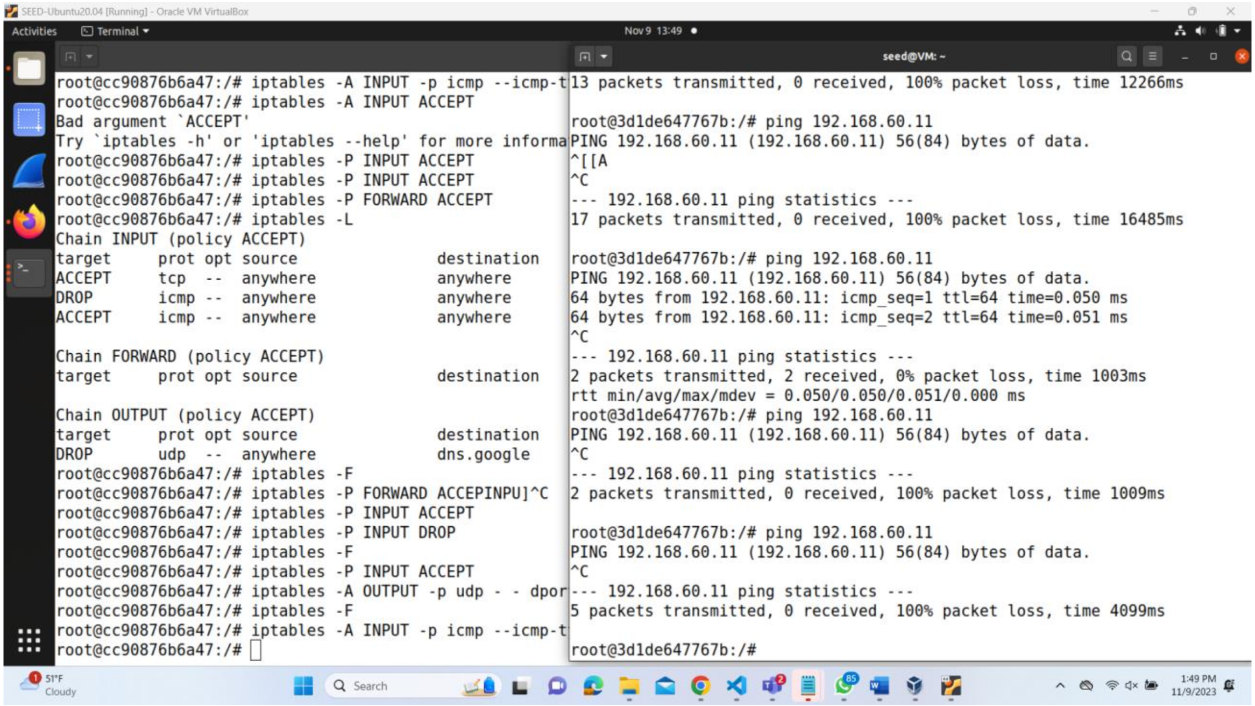
```
root@cc90876b6a47:/# iptables -A INPUT -p tcp --dport 23 -j ACCEPT
root@cc90876b6a47:/# iptables -P INPUT ACCEPT
root@cc90876b6a47:/# iptables -A OUTPUT -p udp - - dport 53 -d 8.8.8.8 -j DROP
Bad argument `-'
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -A OUTPUT -p udp --dport 53 -d 8.8.8.8 -j DROP
root@cc90876b6a47:/# dig www.uwindsor.ca

; <<>> DiG 9.16.1-Ubuntu <<>> www.uwindsor.ca
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42460
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 26965f9f8bcba7eb01000000654d267fab41322e11ebf574 (good)
;; QUESTION SECTION:
;www.uwindsor.ca.               IN      A

;; ANSWER SECTION:
www.uwindsor.ca.        3600    IN      A       137.207.71.197

;; Query time: 7 msec
;; SERVER: 127.0.0.11#53(127.0.0.11)
;; WHEN: Thu Nov 09 18:35:43 UTC 2023
;; MSG SIZE  rcvd: 88

root@cc90876b6a47:/# dig @8.8.8.8 www.uwindsor.ca
^Croot@cc90876b6a47:/# 
```

8. [block incoming ping request]

You can not ping uwindsor webserver. Most likely, this is blocked by firewall of uwindsor. Here is the way to block an incoming icmp request.

$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

Run this on router and ping router from another VM. Do you get any reply? Explain

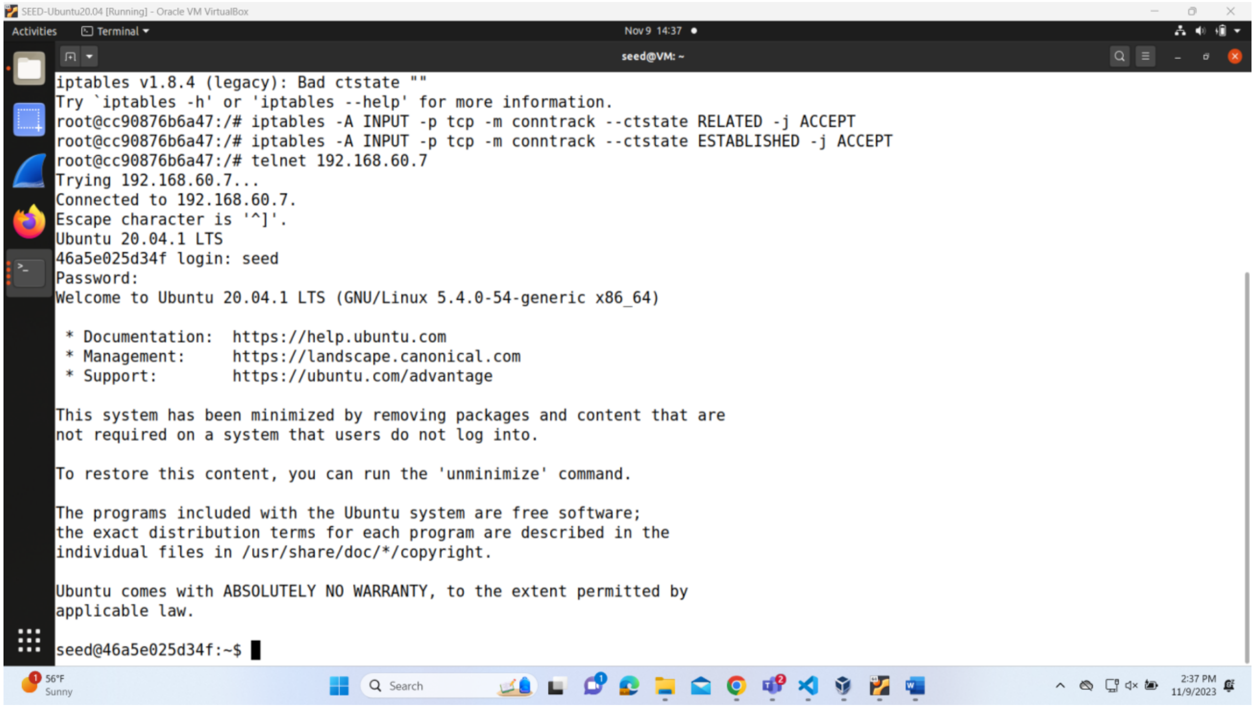


```
root@cc90876b6a47:/# iptables -A INPUT -p icmp --icmp-t
root@cc90876b6a47:/# iptables -A INPUT ACCEPT
Bad argument `ACCEPT'
Try `iptables -h' or 'iptables --help' for more informa
root@cc90876b6a47:/# iptables -P INPUT ACCEPT
root@cc90876b6a47:/# iptables -P INPUT ACCEPT
root@cc90876b6a47:/# iptables -P FORWARD ACCEPT
root@cc90876b6a47:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere
DROP       icmp --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       udp  --  anywhere             dns.google
root@cc90876b6a47:/# iptables -F
root@cc90876b6a47:/# iptables -P FORWARD ACCEPINPU]^C
root@cc90876b6a47:/# iptables -P INPUT ACCEPT
root@cc90876b6a47:/# iptables -P INPUT DROP
root@cc90876b6a47:/# iptables -F
root@cc90876b6a47:/# iptables -P INPUT ACCEPT
root@cc90876b6a47:/# iptables -A OUTPUT -p udp - - dpor
root@cc90876b6a47:/# iptables -F
root@cc90876b6a47:/# iptables -A INPUT -p icmp --icmp-t
root@cc90876b6a47:/# 
```

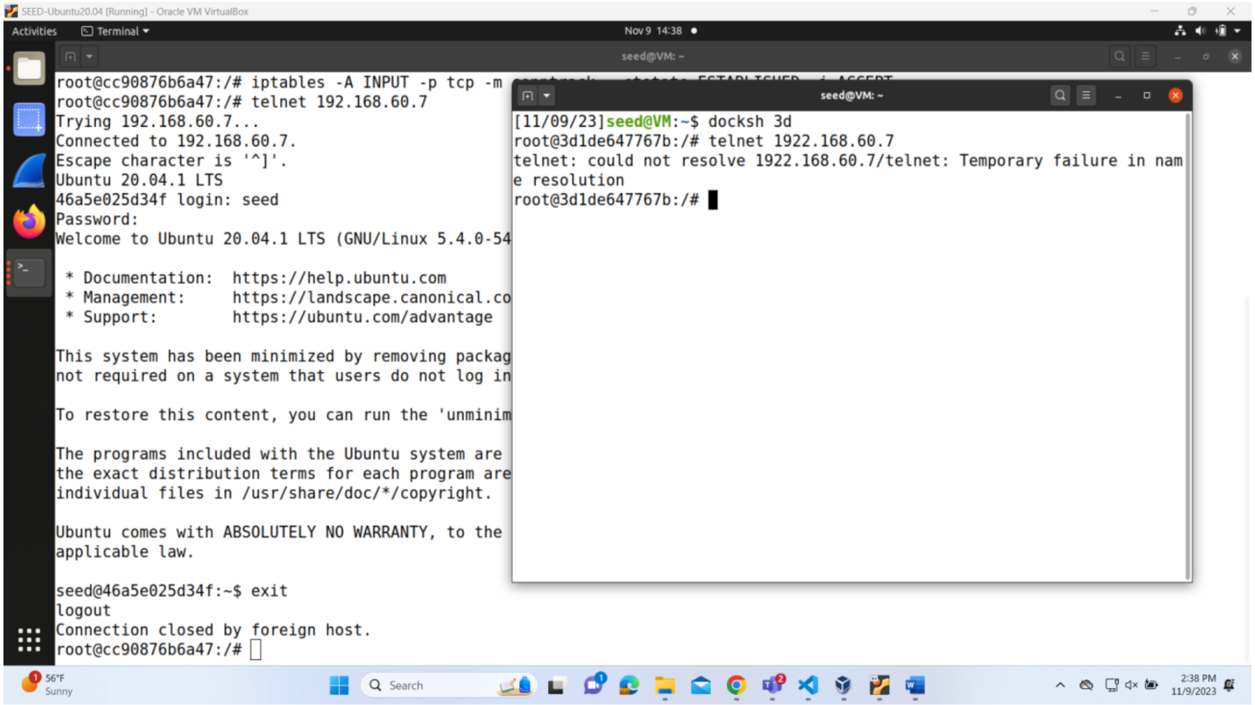
```
13 packets transmitted, 0 received, 100% packet loss, time 12266ms

root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
^[[A
^C
--- 192.168.60.11 ping statistics ---
17 packets transmitted, 0 received, 100% packet loss, time 16485ms

root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
64 bytes from 192.168.60.11: icmp_seq=1 ttl=64 time=0.050 ms
64 bytes from 192.168.60.11: icmp_seq=2 ttl=64 time=0.051 ms
^C
--- 192.168.60.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.050/0.050/0.051/0.000 ms
root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
^C
--- 192.168.60.11 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1009ms

root@3d1de647767b:/# ping 192.168.60.11
PING 192.168.60.11 (192.168.60.11) 56(84) bytes of data.
^C
--- 192.168.60.11 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4099ms

root@3d1de647767b:/#
```

9. **Suppose that you want to block all incoming connections while you do not want your visit to external servers to be affected.**
   However, if you send a request to an external server, the server will reply to you while this packet will be blocked by your firewall. To resolve this issue, you should regard the response packet (to your request) as related to your outgoing request packet and allowed to come in. This is achieved using the *conntrack* module.
   $ sudo iptables -P INPUT DROP
   $ sudo iptables -A INPUT -p tcp -m conntrack --ctstate RELATED, ESTABLISHED -j ACCEPT
   Try this on router VM. Then, telnet to a VM (e.g. 192.168.60.7).
   Next, telnet from the latter (192.168.60.7) to router. Which telnet session directly succeeds?

Answer: Router's Telnet directly succeeds, and when I try from 192.168.60.6, it Failed to telnet.



```
iptables v1.8.4 (legacy): Bad ctstate ""
Try `iptables -h' or 'iptables --help' for more information.
root@cc90876b6a47:/# iptables -A INPUT -p tcp -m conntrack --ctstate RELATED -j ACCEPT
root@cc90876b6a47:/# iptables -A INPUT -p tcp -m conntrack --ctstate ESTABLISHED -j ACCEPT
root@cc90876b6a47:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
46a5e025d34f login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@46a5e025d34f:~$ 
```



```
root@cc90876b6a47:/# iptables -A INPUT -p tcp -m
root@cc90876b6a47:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
46a5e025d34f login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.co
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packag
not required on a system that users do not log in

To restore this content, you can run the 'unminim

The programs included with the Ubuntu system are
the exact distribution terms for each program are
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the
applicable law.

seed@46a5e025d34f:~$ exit
logout
Connection closed by foreign host.
root@cc90876b6a47:/#
```

```
[11/09/23]seed@VM:~$ docksh 3d
root@3d1de647767b:/# telnet 1922.168.60.7
telnet: could not resolve 1922.168.60.7/telnet: Temporary failure in nam
e resolution
root@3d1de647767b:/#
```