Name	**Hatim Sawai**
UID no.	**2021300108**
Experiment No.	8
AIM	**Configure Firewall rules using IP tables. Upload the compressed file as per the instruction given in one page manual of this experiment.**

IP Tables Project Exercises (all questions are with respect to the filter table, and are to be executed independent of the other questions, unless otherwise noted. So, remember to flush the iptables after executing each question, unless you are asked to follow up from a previous question):

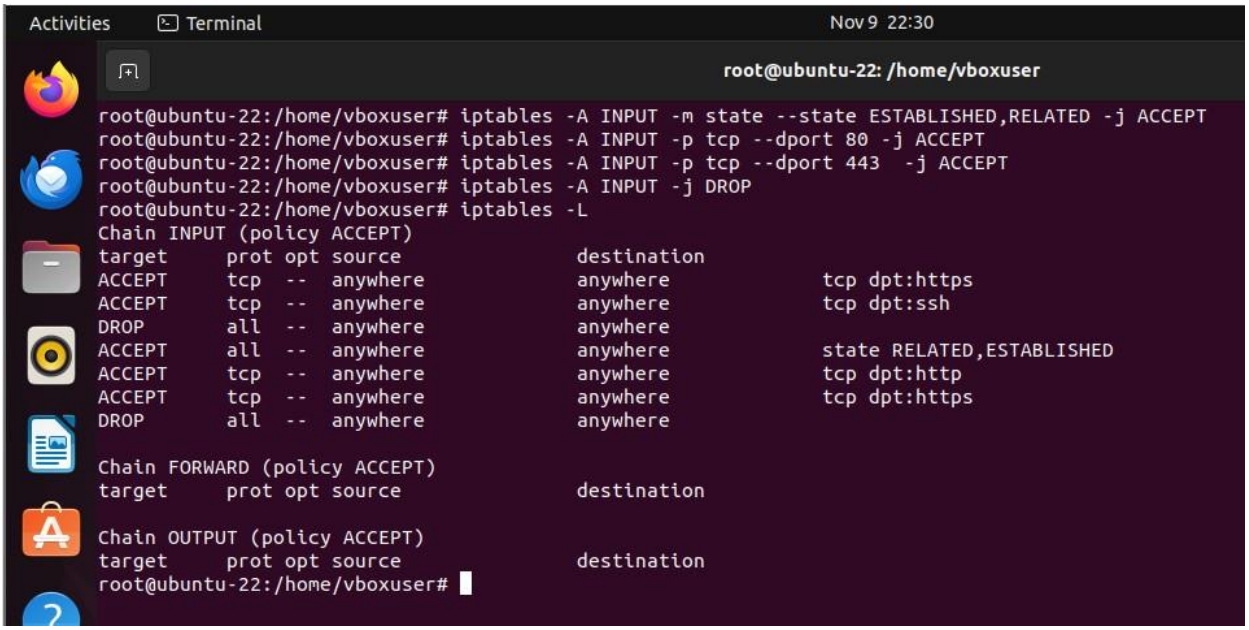
Q1) Set the default policy for the INPUT chain to DROP. The firewall should only allow incoming packets from the network prefix 143.132.0.0/16. The default policy for the OUTPUT chain is ACCEPT. So, the user working on the machine could visit any website like www.google.com. Given the above policy for incoming packets, can the web pages visited by the user be displayed in the browser? Explain

```
root@ubuntu-22:/home/vboxuser# iptables -t mangle -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

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 POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

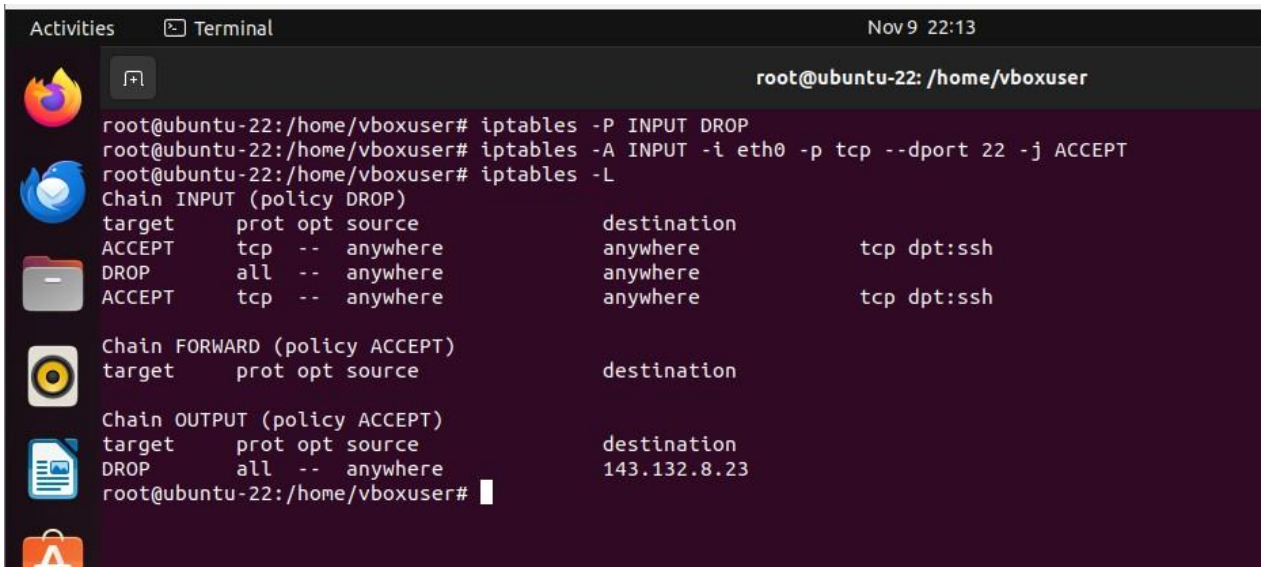
```
root@ubuntu-22:/home/vboxuser# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu-22:/home/vboxuser#
```

Q2) Set the default policy for the INPUT chain be DROP and the default policy for the OUTPUT chain be ACCEPT. Configure the INPUT chain to accept all incoming web traffic to port 80 and drop any other incoming traffic. Can you visit the website: www.hotmail.com? Why or why not? If you cannot visit the website, what aspect of this website is preventing you from visiting it, given that your default OUTPUT policy is ACCEPT and the firewall has been configured to accept traffic coming to port 80? Also, if you cannot visit the website, configure the firewall to let you be able to visit websites of such type. What changes/deletions/additions to the rules had to be done to facilitate this?

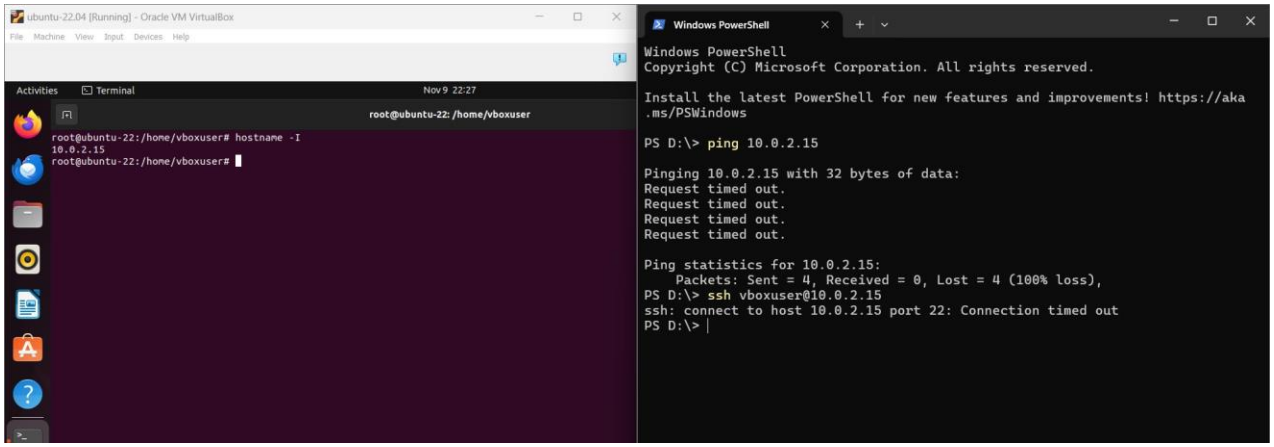
HTTPS sites may not load because they require port 443. To access such site we have to accept port 443 as well and DNS resolution has to take place before that's why we also have to accept port 53.



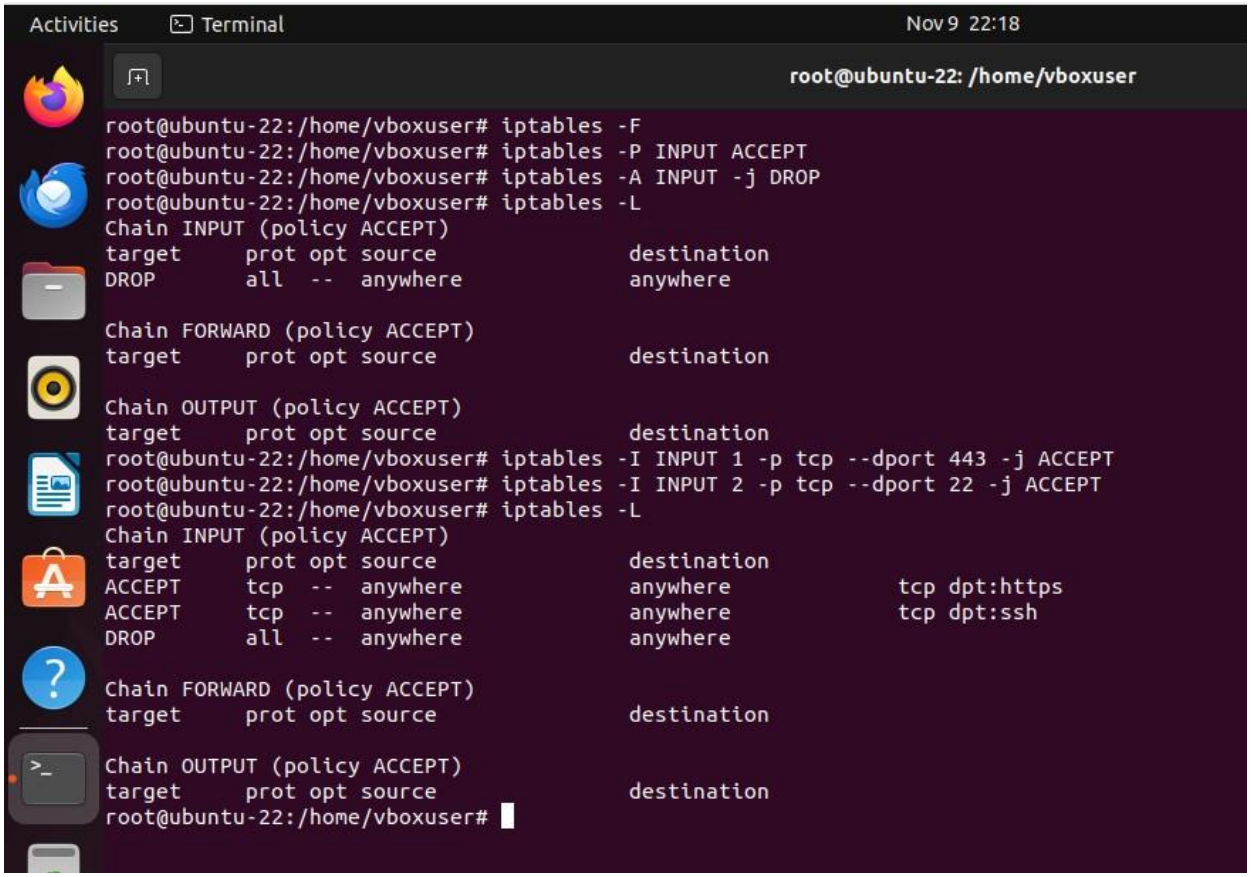
Q3) The previous question permitted only incoming packets related to web traffic. Do an insertion to the rules in the INPUT chain to permit SSH traffic. Show that you can connect to the SSH server running on the Ubuntu VM by connecting to it from another VM (centos or anything) or from the physical host machine (Windows). Include appropriate screenshots. You can get the IP address of a Linux machine by running the ifconfig command in the terminal. Refer to the screenshots (for example, under scenarios S5, S8) in the tutorial to see how you could SSH to a machine under a particular username.

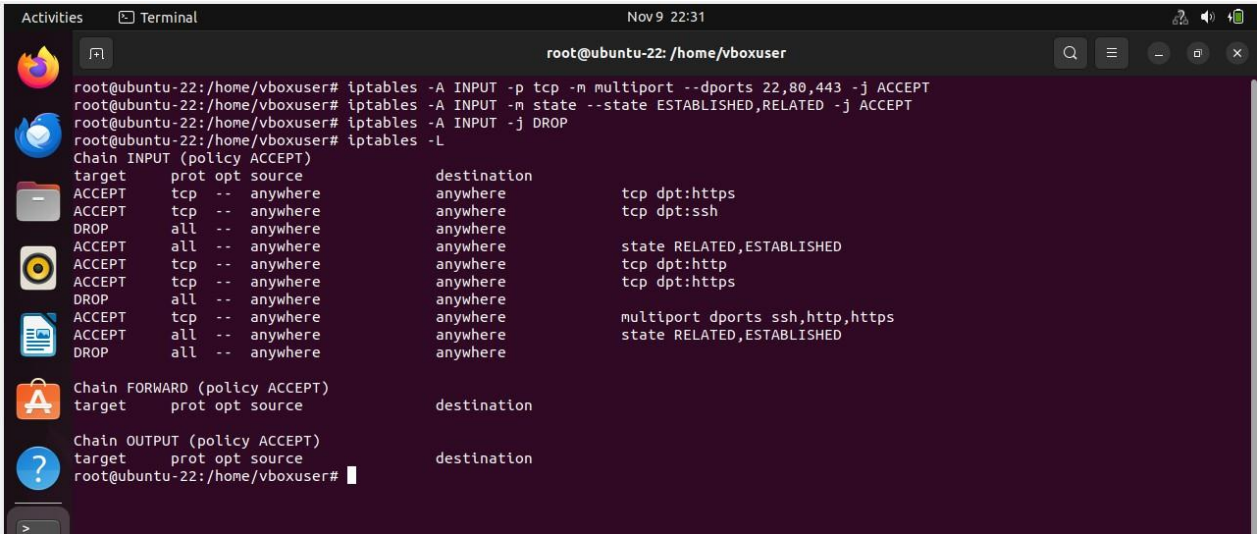


Ssh vm from remote machine



Q4) Configure your IPtables filter table on your Ubuntu VM such that sessions/packet exchange originating from the Ubuntu VM (as the source) are successful; on the other hand, sessions/packet exchange originating from a remote machine to the Ubuntu VM (as the destination) are not successful. You need to implement this scenario with the minimal number of rules and policy changes, if any. Also, explain why your set of rules and policies implementing the stated scenario will work





Unable to ping vm from my local machine

```
PS D:\> ping 10.0.2.15

Pinging 10.0.2.15 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Q5) Configure your IPtables filter table to limit the number of active SSH connections to the Ubuntu VM(hosting the SSH server) is 2. Test the working of this rule by attempting to open three SSH connections, each in separate terminals, from another VM (like a CentOS VM) or from the host machine itself. Show appropriate screenshots

```
root@ubuntu-22:/home/vboxuser# modprobe xt_connlimit
root@ubuntu-22:/home/vboxuser# iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 2 -j DROP
root@ubuntu-22:/home/vboxuser# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
DROP       all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
DROP       all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             multiport dports ssh,http,https
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
DROP       all  --  anywhere             anywhere
DROP       tcp  --  anywhere             anywhere             tcp dpt:http flags:FIN,SYN,RST,ACK/SYN #conn src/32 > 2
DROP       tcp  --  anywhere             anywhere             tcp dpt:http flags:FIN,SYN,RST,ACK/SYN #conn src/32 > 2

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ubuntu-22:/home/vboxuser#
```

Ssh connection 1:

```
ubuntu@ubuntu:~$ ssh root@10.0.2.15
root@10.0.2.15's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-26-generic x86_64)

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



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.
```

Ssh connection 2:

```
ubuntu@ubuntu:/root$ ssh root@10.0.2.15
root@10.0.2.15's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-26-generic x86_64)

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


Last login: Sun Nov 10 14:11:27 2024 from 10.0.2.15
root@ubuntu:~#
```

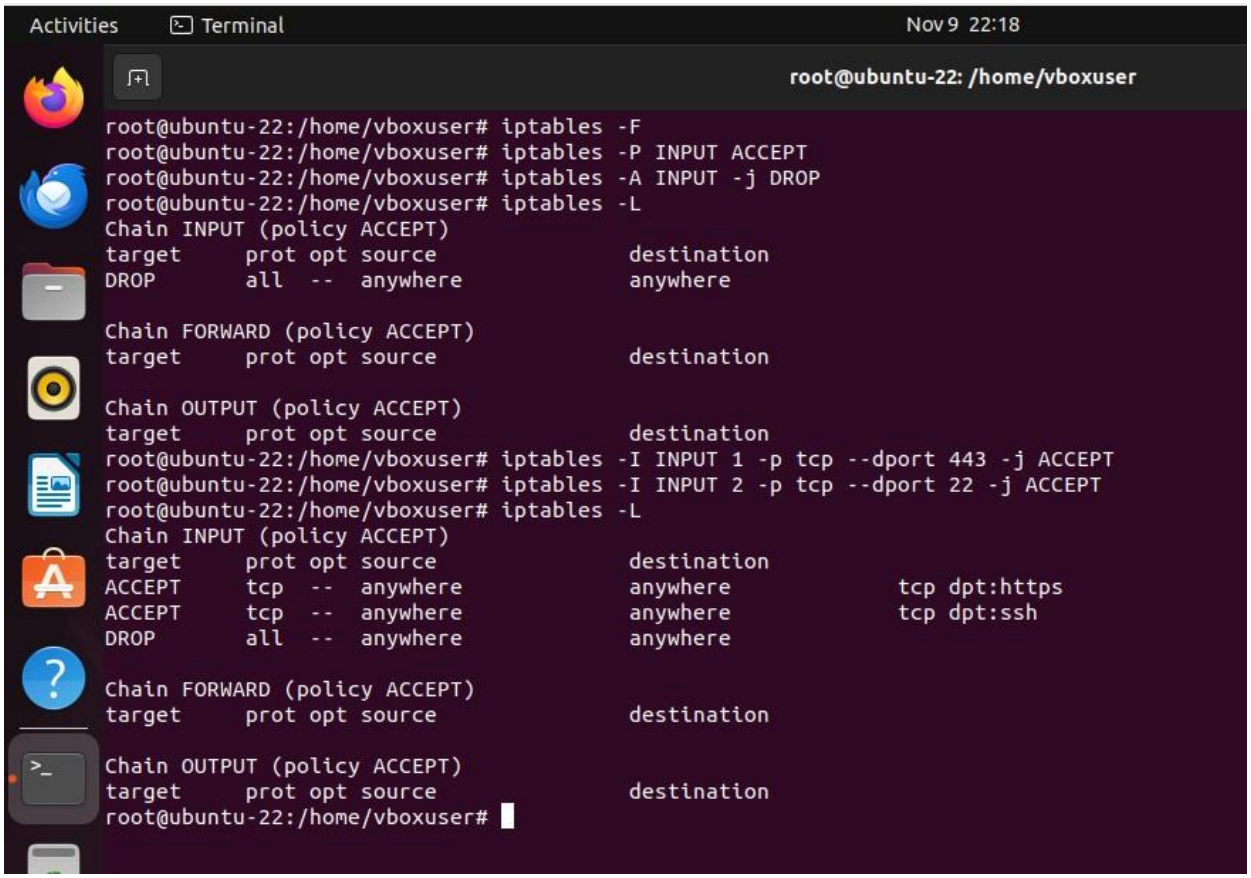
Ssh connection 3:

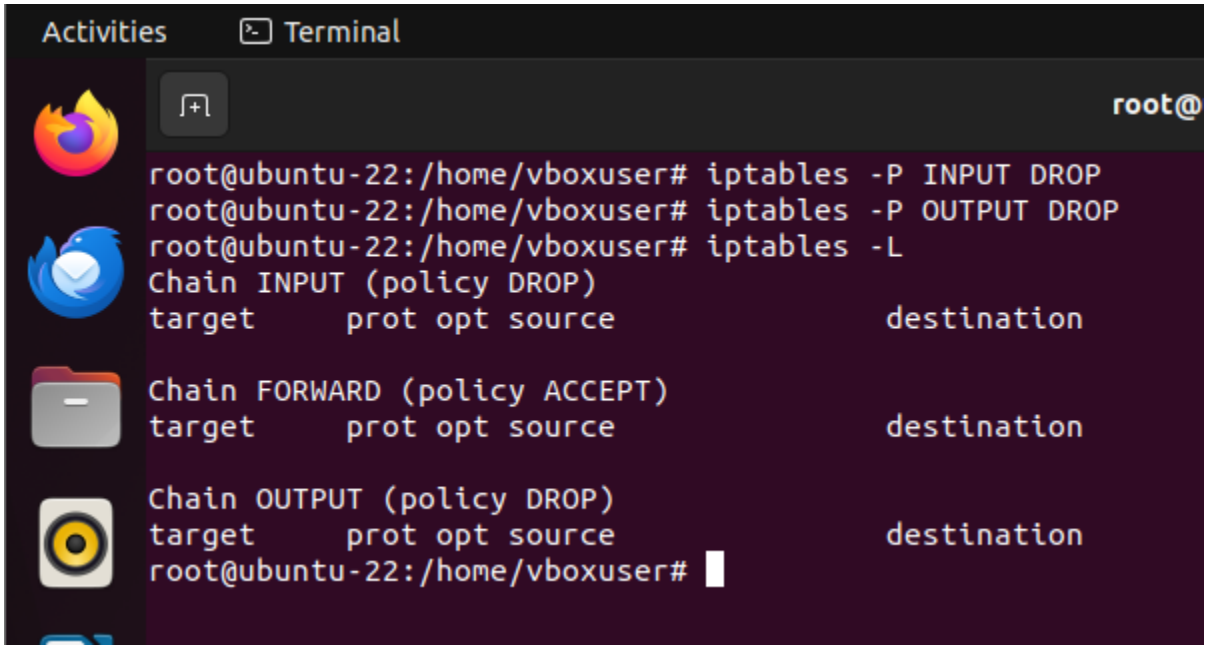
```
ubuntu@ubuntu:~$ ssh root@10.0.2.15



^C
```

Cannot connect

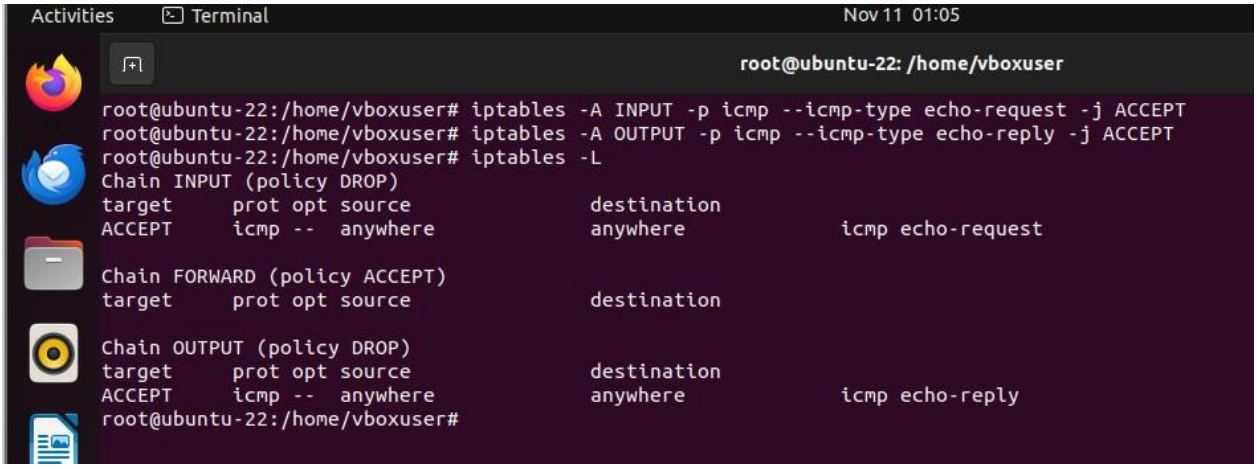
Q6) Set the default policy of the INPUT and OUTPUT chains of your filter table of iptables is to DROPusing an appropriate command (show a screenshot executing the command and the output of the iptables- L command). You could use the Ubuntu VM and CentOS

VM in your virtual environment to implement this scenario. Now configure your iptables on the Ubuntu VM to (do parts a and b independently): (a) Only allow remote machines to ping the local machine and block the local machine from pinging others. (b) Only allow the local machine to ping the remote machines and block the remote machines from pinging the local machine. (c) Allow ping communication in both directions (from the local machine to remote machine and viceversa). Note that you have to use the--icmp-type echo-request and--icmp-type echo-reply options appropriately. Show appropriate screenshots executing the iptables commands to realize the above for (a), (b) and (c) and the structure of the iptables. Also, capture the successful or unsuccessful execution of the ping command from the local machine and remote machine (in either direction) for each of the three cases (a), (b), (c).





Part a:



Ping vm from remote machine

```
C:\Users\yash>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\yash>
```

Part B:

```
Activities    Terminal                                   Nov 11  01:14
                                        root@ubuntu-22: /home/vboxuser
root@ubuntu-22:/home/vboxuser# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@ubuntu-22:/home/vboxuser# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
root@ubuntu-22:/home/vboxuser# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
root@ubuntu-22:/home/vboxuser#
```

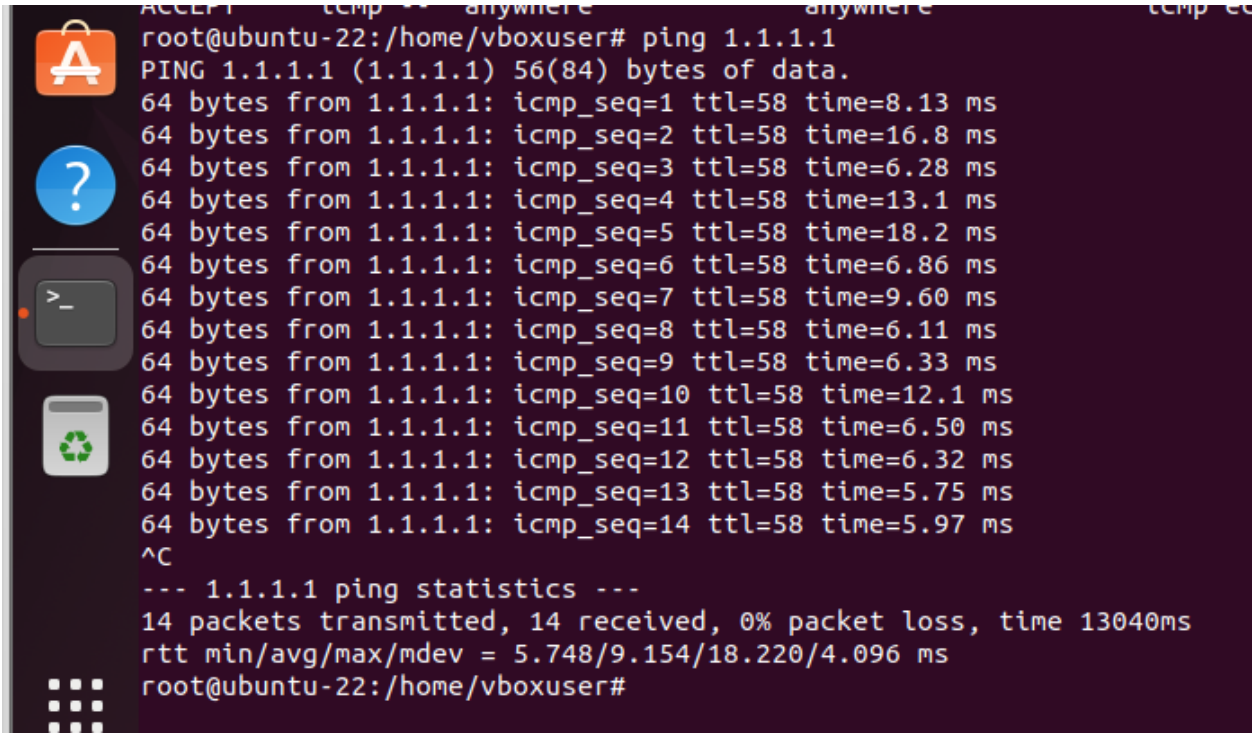
Pinging vm machine from remote machine:

```
rtt min/avg/max/mdev = 12.527/12.527/12.527/0.000 ms
ubuntu@ubuntu:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.049 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.123 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.074 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.098 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.069 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.094 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.062 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.069 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.103 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.139 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.068 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.104 ms
^C
--- 10.0.2.15 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11610ms
rtt min/avg/max/mdev = 0.049/0.087/0.139/0.025 ms
```

Part C:

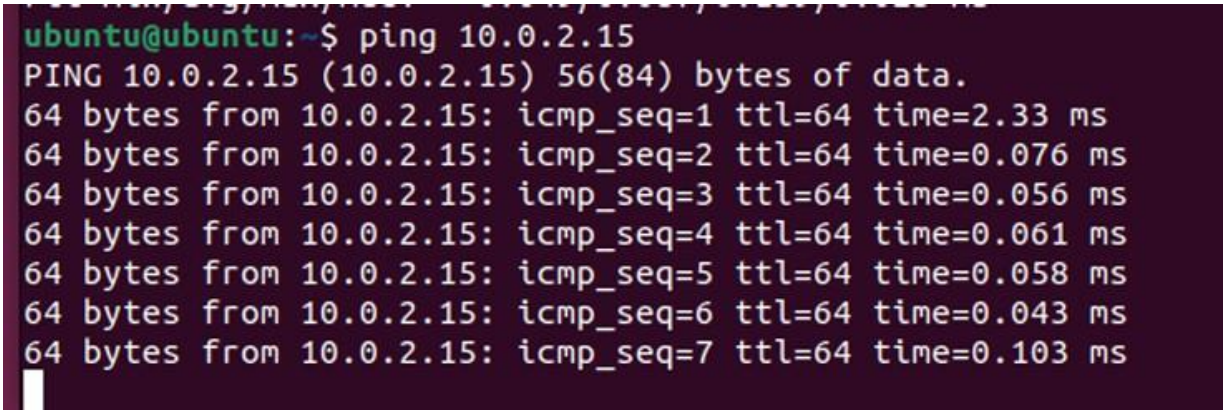
```
Activities    Terminal                                    Nov 11  01:19
                                        root@ubuntu-22: /home/vboxuser
root@ubuntu-22:/home/vboxuser# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@ubuntu-22:/home/vboxuser# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
root@ubuntu-22:/home/vboxuser# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
root@ubuntu-22:/home/vboxuser#
```

Ping another machine from VM



```
root@ubuntu-22:/home/vboxuser# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=58 time=8.13 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=58 time=16.8 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=58 time=6.28 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=58 time=13.1 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=58 time=18.2 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=58 time=6.86 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=58 time=9.60 ms
64 bytes from 1.1.1.1: icmp_seq=8 ttl=58 time=6.11 ms
64 bytes from 1.1.1.1: icmp_seq=9 ttl=58 time=6.33 ms
64 bytes from 1.1.1.1: icmp_seq=10 ttl=58 time=12.1 ms
64 bytes from 1.1.1.1: icmp_seq=11 ttl=58 time=6.50 ms
64 bytes from 1.1.1.1: icmp_seq=12 ttl=58 time=6.32 ms
64 bytes from 1.1.1.1: icmp_seq=13 ttl=58 time=5.75 ms
64 bytes from 1.1.1.1: icmp_seq=14 ttl=58 time=5.97 ms
^C
--- 1.1.1.1 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13040ms
rtt min/avg/max/mdev = 5.748/9.154/18.220/4.096 ms
root@ubuntu-22:/home/vboxuser#
```

Ping vm from remote machine:



```
ubuntu@ubuntu:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=2.33 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.076 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.056 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.061 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.058 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.043 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.103 ms
```