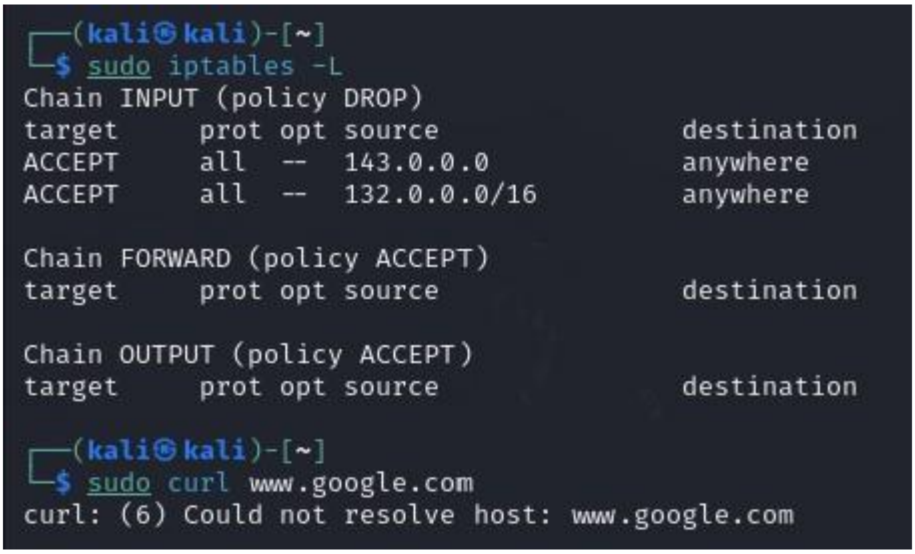
Name: Adwait Purao

UID: 2021300101
Batch: V
Div: COMPS B

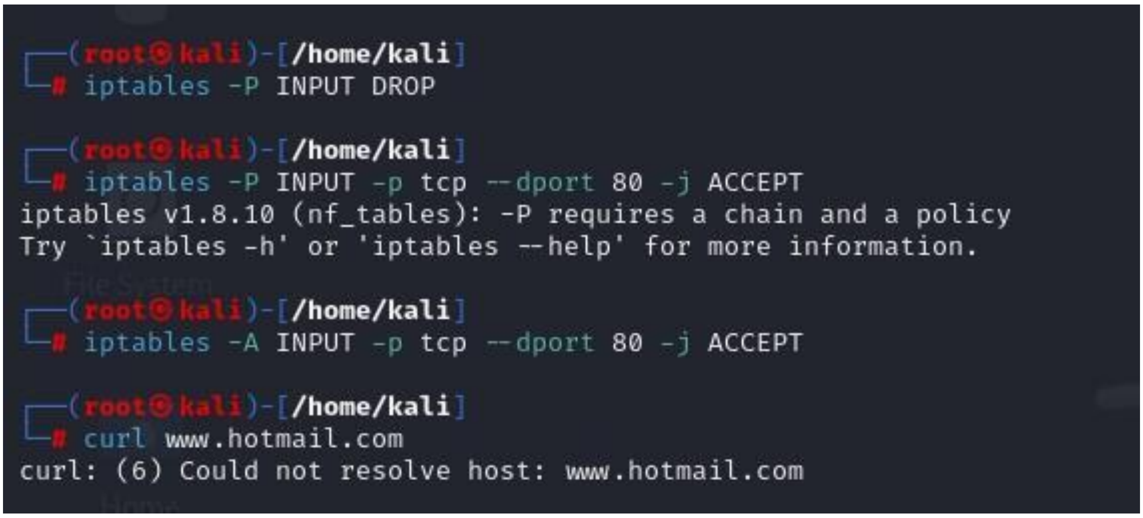
Q1) Set the default policy for the INPUT chain to DROP. The firewall should only allow incoming packets from the network prefix 143.132.0.0/16. The default policy for the OUTPUT chain is ACCEPT. So, the user working on the machine could visit any website like www.google.com. Given the above policy for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



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  143.0.0.0            anywhere
ACCEPT     all  --  132.0.0.0/16         anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

┌──(kali㉿kali)-[~]
└─$ sudo curl www.google.com
curl: (6) Could not resolve host: www.google.com
```

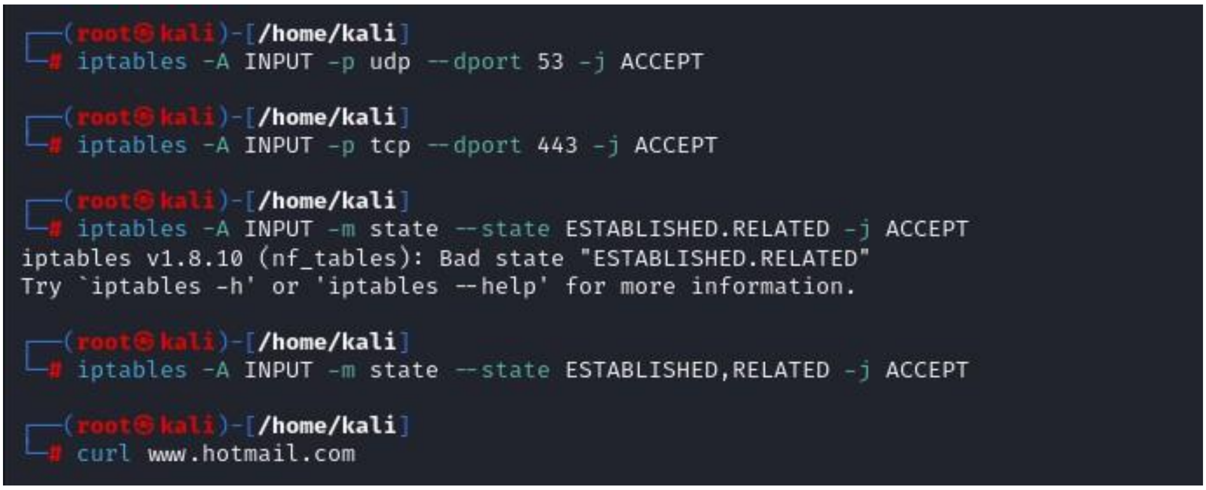
We cannot open www.google.com as we set the default policy to DROP all incoming traffic and only allowed traffic from the 143.132.0.0/16 subnet.

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?

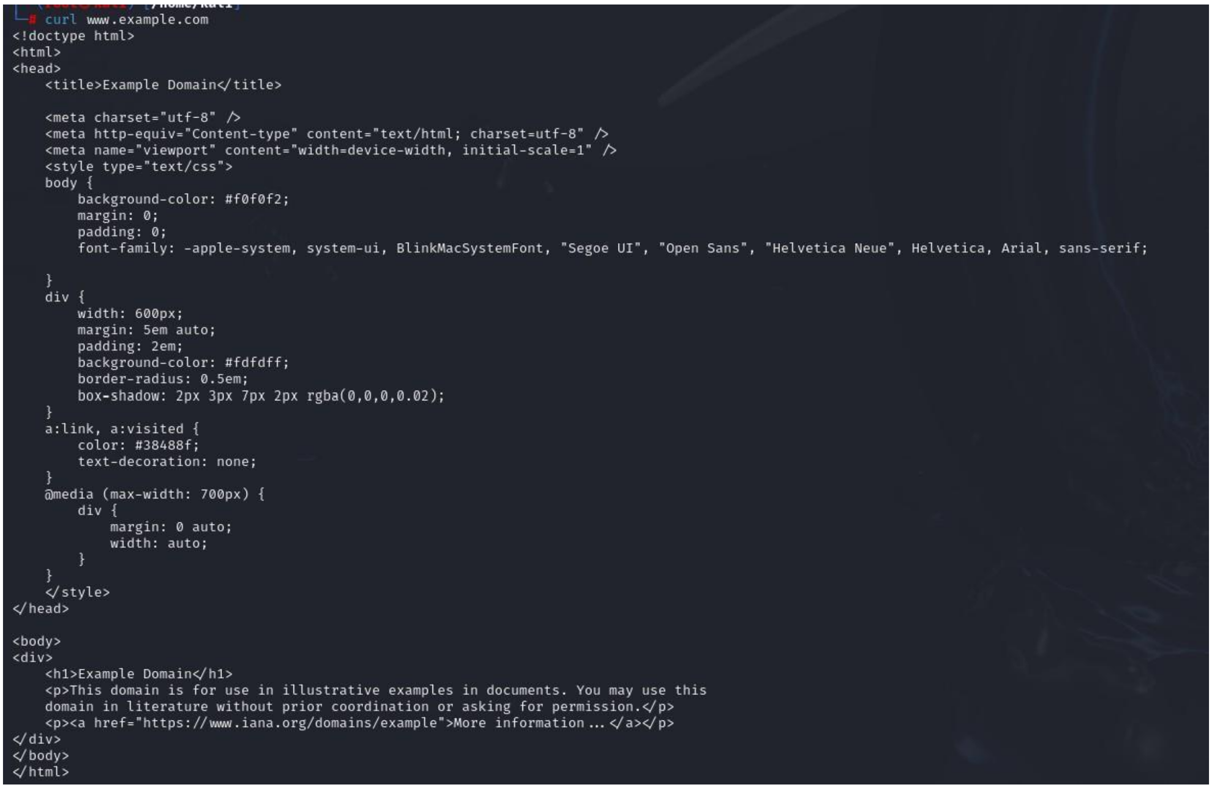


```
┌──(root㉿kali)-[/home/kali]
└─# iptables -P INPUT DROP

┌──(root㉿kali)-[/home/kali]
└─# iptables -P INPUT -p tcp --dport 80 -j ACCEPT
iptables v1.8.10 (nf_tables): -P requires a chain and a policy
Try `iptables -h' or 'iptables --help' for more information.

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -p tcp --dport 80 -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# curl www.hotmail.com
curl: (6) Could not resolve host: www.hotmail.com
```

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.

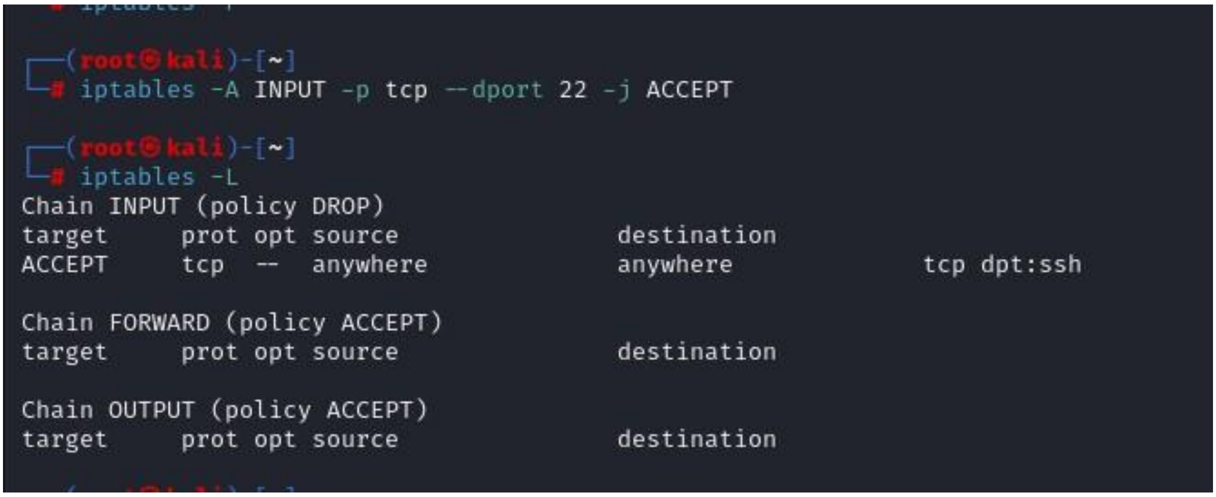


```
┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -p udp --dport 53 -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -p tcp --dport 443 -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -m state --state ESTABLISHED.RELATED -j ACCEPT
iptables v1.8.10 (nf_tables): Bad state "ESTABLISHED.RELATED"
Try `iptables -h' or 'iptables --help' for more information.

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# curl www.hotmail.com
```



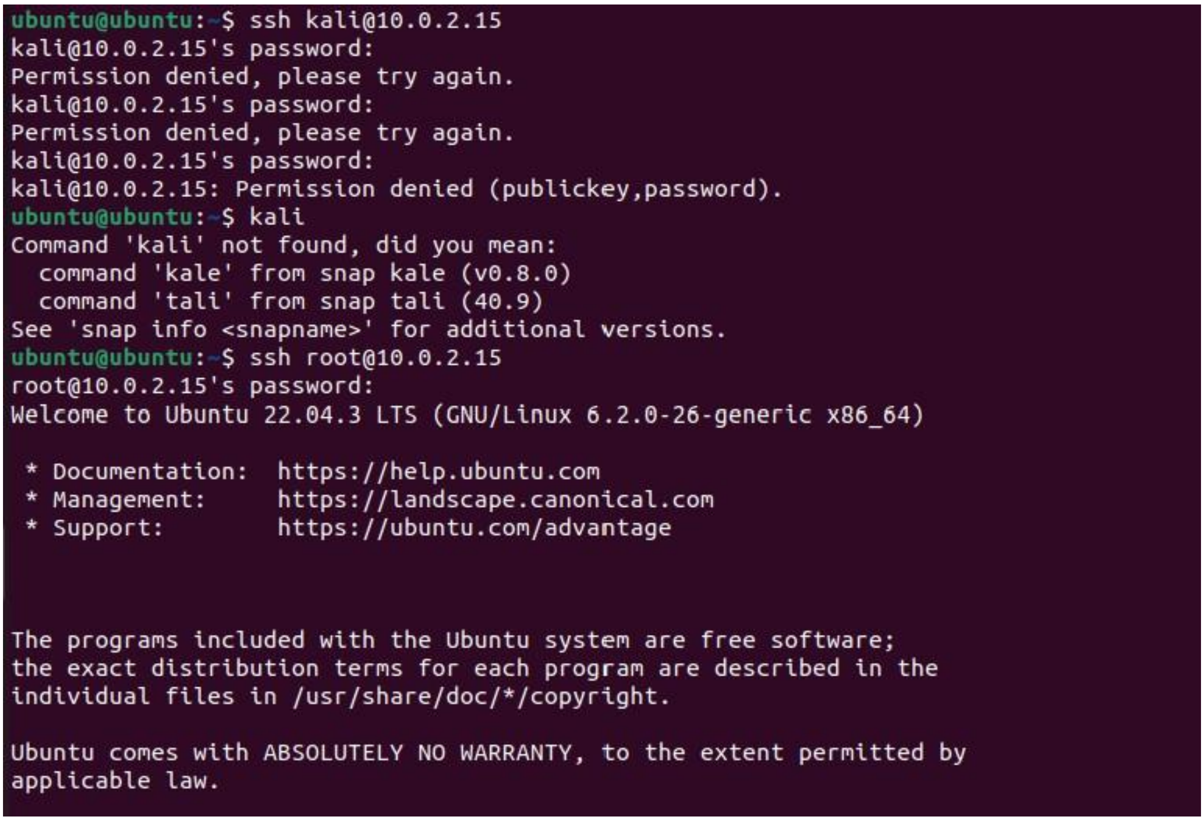
```
└─# curl www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You may use this
    domain in literature without prior coordination or asking for permission.</p>
    <p><a href="https://www.iana.org/domains/example">More information...</a></p>
</div>
</body>
</html>
```

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.



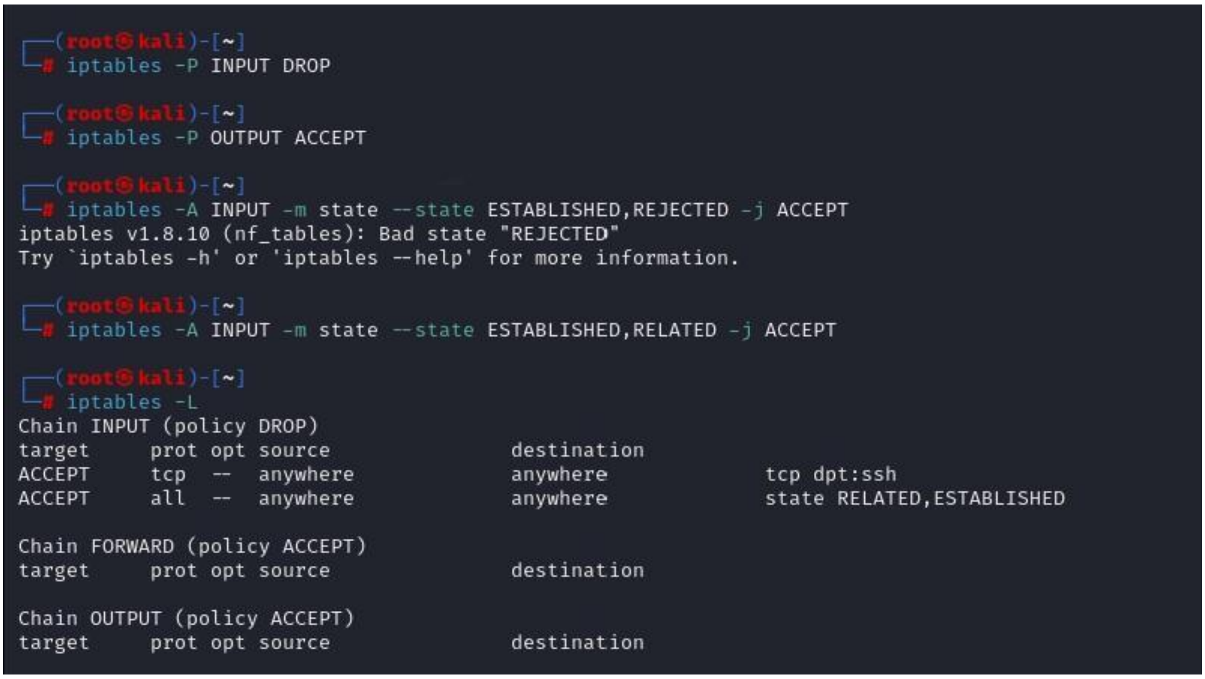
```
┌──(root㉿kali)-[~]
└─# iptables -A INPUT -p tcp --dport 22 -j ACCEPT

┌──(root㉿kali)-[~]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

Ssh vm from remote machine



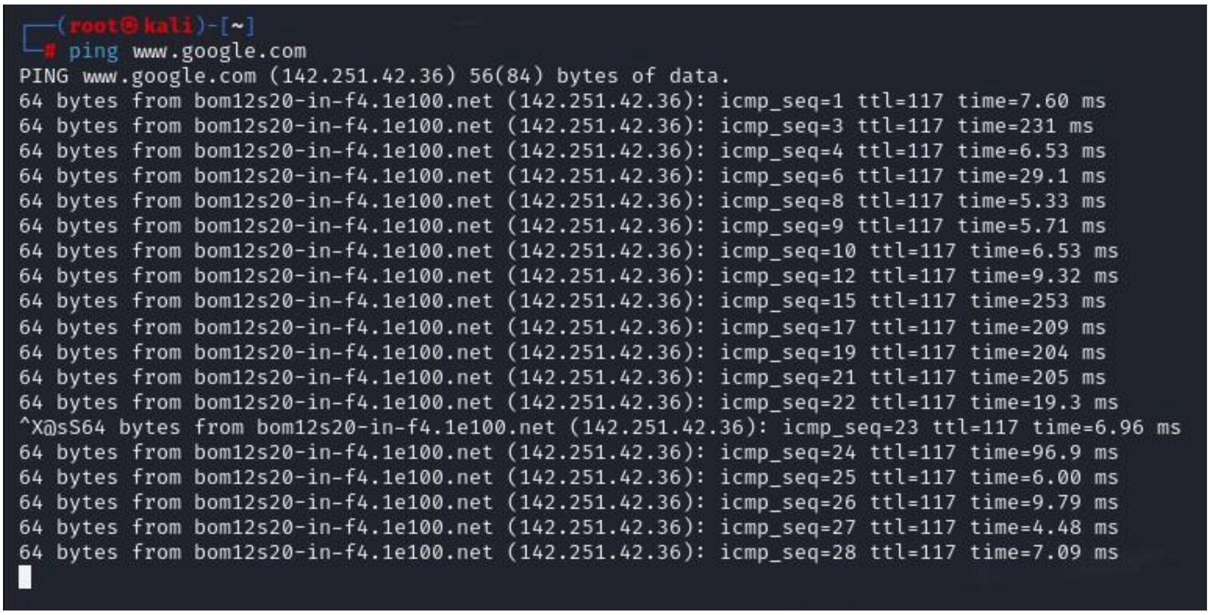
```
ubuntu@ubuntu:~$ ssh kali@10.0.2.15
kali@10.0.2.15's password:
Permission denied, please try again.
kali@10.0.2.15's password:
Permission denied, please try again.
kali@10.0.2.15's password:
kali@10.0.2.15: Permission denied (publickey,password).
ubuntu@ubuntu:~$ kali
Command 'kali' not found, did you mean:
  command 'kale' from snap kale (v0.8.0)
  command 'tali' from snap tali (40.9)
See 'snap info <snapname>' for additional versions.
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.
```

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



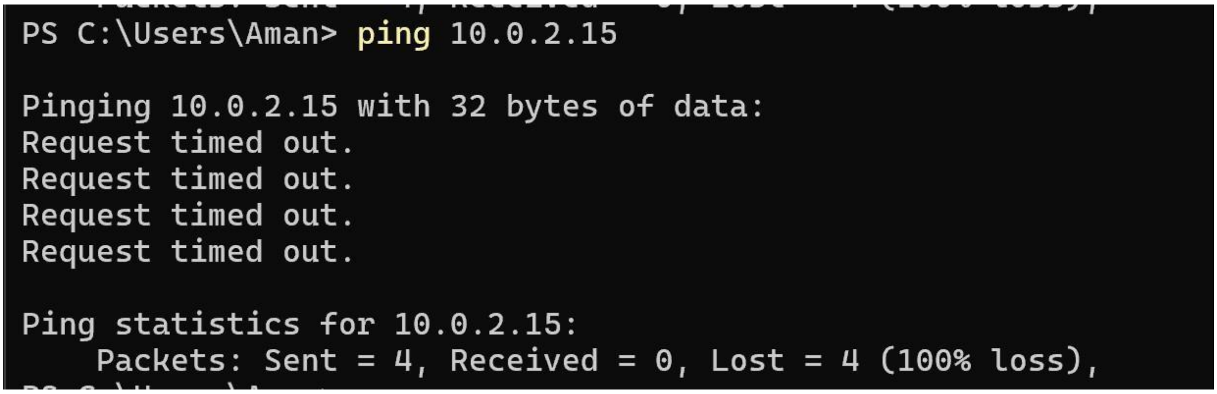
```
┌──(root㉿kali)-[~]
└─# iptables -P INPUT DROP

┌──(root㉿kali)-[~]
└─# iptables -P OUTPUT ACCEPT

┌──(root㉿kali)-[~]
└─# iptables -A INPUT -m state --state ESTABLISHED,REJECTED -j ACCEPT
iptables v1.8.10 (nf_tables): Bad state "REJECTED"
Try `iptables -h' or 'iptables --help' for more information.

┌──(root㉿kali)-[~]
└─# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

┌──(root㉿kali)-[~]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

Ping google.com



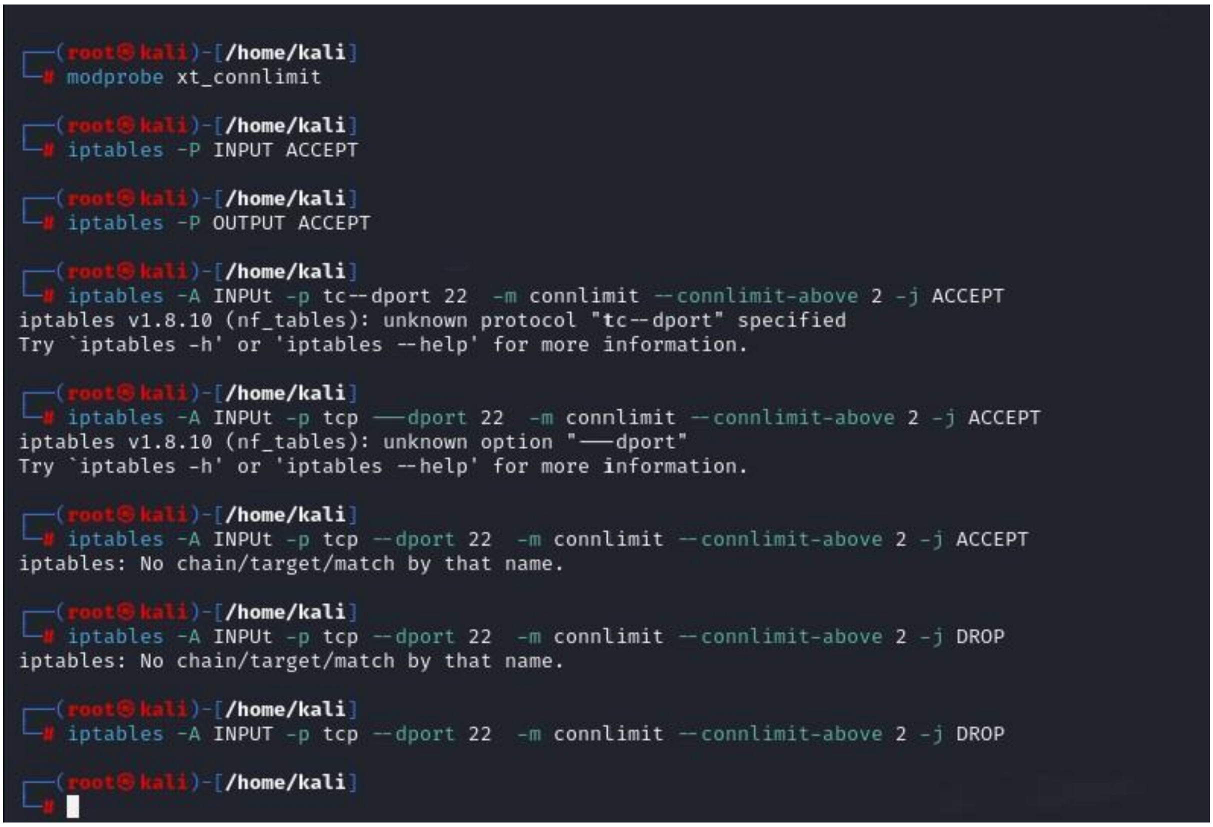
```
┌──(root㉿kali)-[~]
└─# ping www.google.com
PING www.google.com (142.251.42.36) 56(84) bytes of data.
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=1 ttl=117 time=7.60 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=3 ttl=117 time=231 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=4 ttl=117 time=6.53 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=6 ttl=117 time=29.1 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=8 ttl=117 time=5.33 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=9 ttl=117 time=5.71 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=10 ttl=117 time=6.53 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=12 ttl=117 time=9.32 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=15 ttl=117 time=253 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=17 ttl=117 time=209 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=19 ttl=117 time=204 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=21 ttl=117 time=205 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=22 ttl=117 time=19.3 ms
^X@sS64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=23 ttl=117 time=6.96 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=24 ttl=117 time=96.9 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=25 ttl=117 time=6.00 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=26 ttl=117 time=9.79 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=27 ttl=117 time=4.48 ms
64 bytes from bom12s20-in-f4.1e100.net (142.251.42.36): icmp_seq=28 ttl=117 time=7.09 ms
```

Unable to ping vm from my local machine



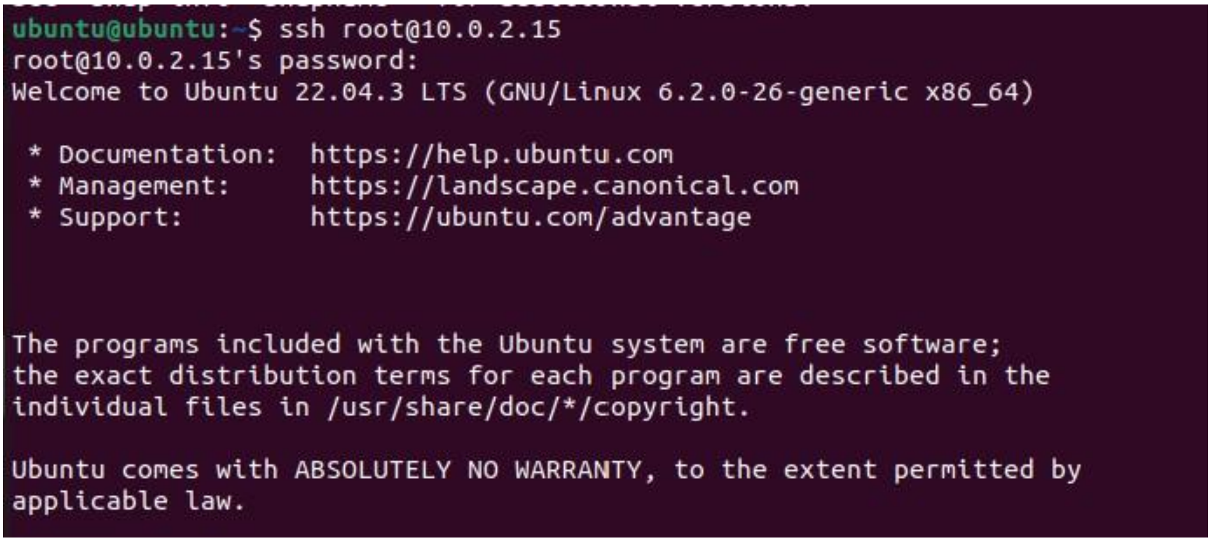
```
PS C:\Users\Aman> ping 10.0.2.15

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



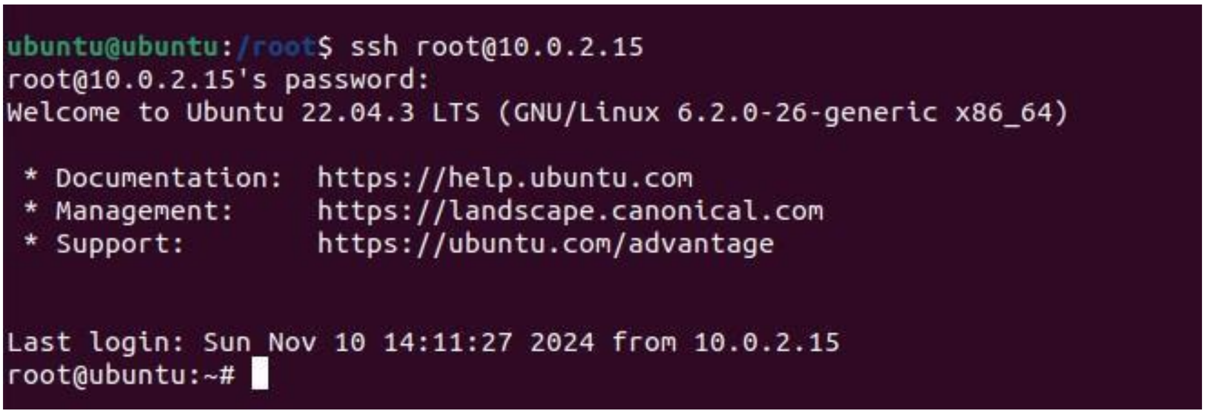
```
┌──(root㉿kali)-[/home/kali]
└─# modprobe xt_connlimit

┌──(root㉿kali)-[/home/kali]
└─# iptables -P INPUT ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# iptables -P OUTPUT ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUt -p tc--dport 22  -m connlimit --connlimit-above 2 -j ACCEPT
iptables v1.8.10 (nf_tables): unknown protocol "tc--dport" specified
Try `iptables -h' or 'iptables --help' for more information.

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUt -p tcp ——dport 22  -m connlimit --connlimit-above 2 -j ACCEPT
iptables v1.8.10 (nf_tables): unknown option "——dport"
Try `iptables -h' or 'iptables --help' for more information.

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUt -p tcp --dport 22  -m connlimit --connlimit-above 2 -j ACCEPT
iptables: No chain/target/match by that name.

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUt -p tcp --dport 22  -m connlimit --connlimit-above 2 -j DROP
iptables: No chain/target/match by that name.

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -p tcp --dport 22  -m connlimit --connlimit-above 2 -j DROP

┌──(root㉿kali)-[/home/kali]
└─# 
```

Ssh connection 1:



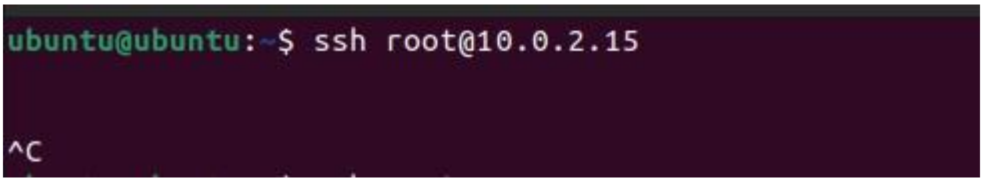
```
ubuntu@ubuntu:~$ ssh root@10.0.2.15
root@10.0.2.15's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-26-generic x86_64)

 * 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:~#
```

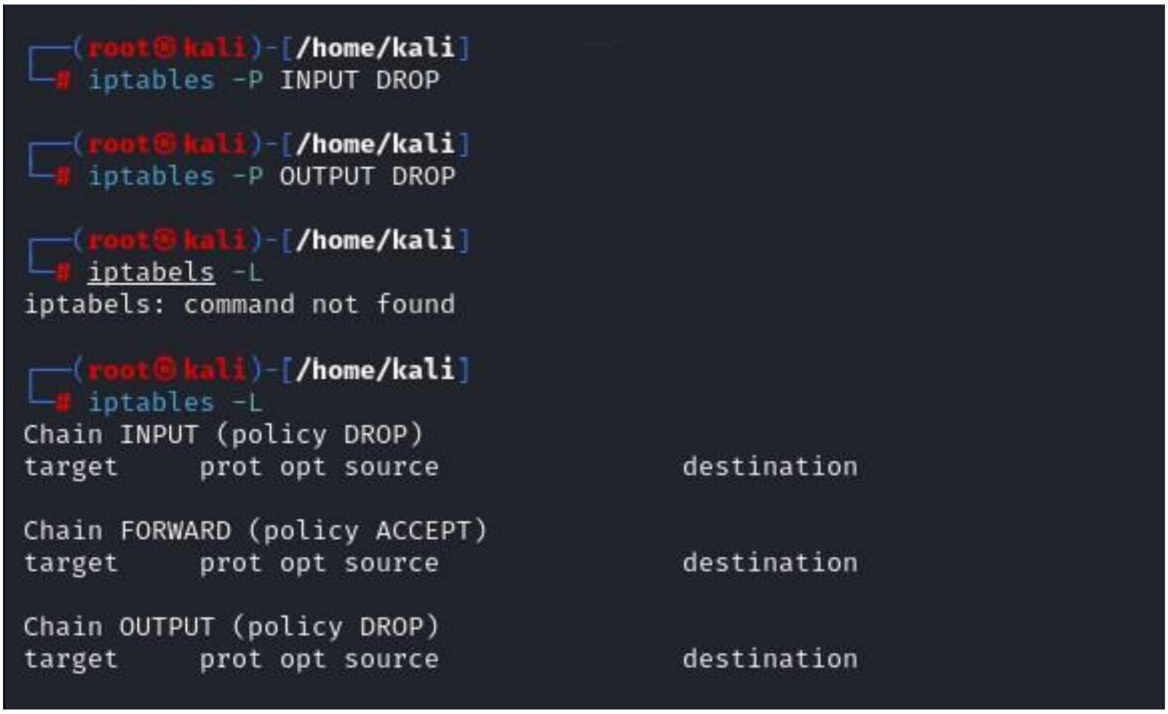
Ssh connection 3:



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


^C
```

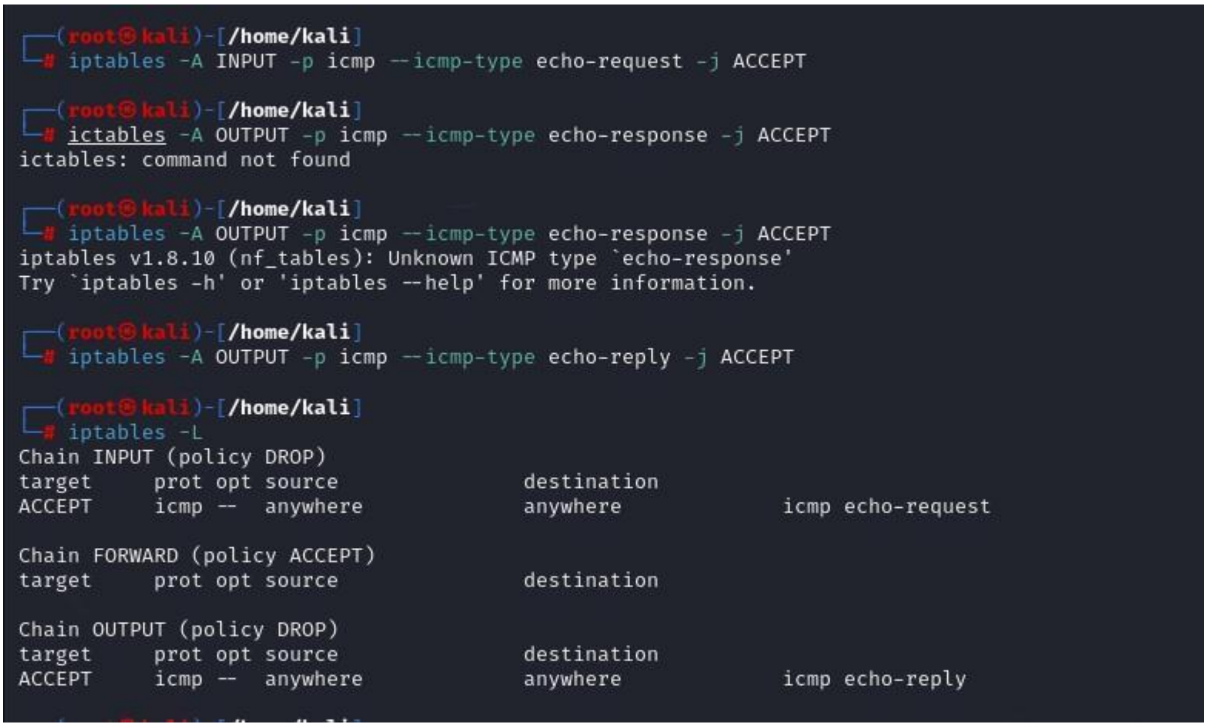
Can’t connect via third ssh connection.

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).



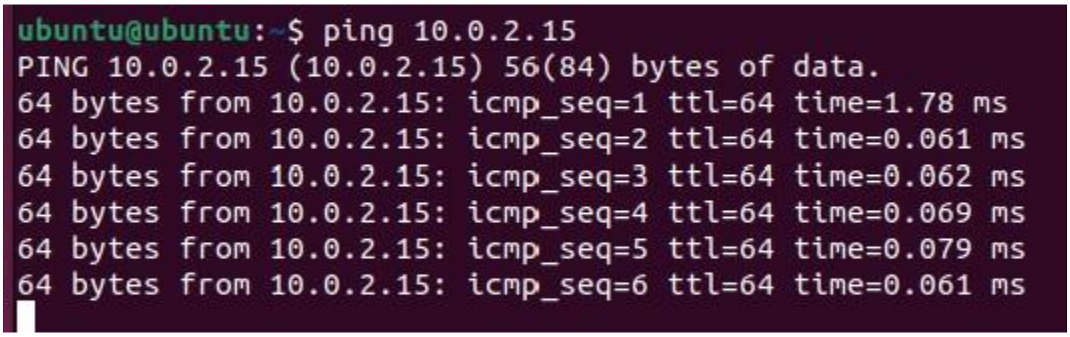
```
┌──(root㉿kali)-[/home/kali]
└─# iptables -P INPUT DROP

┌──(root㉿kali)-[/home/kali]
└─# iptables -P OUTPUT DROP

┌──(root㉿kali)-[/home/kali]
└─# iptabels -L
iptabels: command not found

┌──(root㉿kali)-[/home/kali]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

Part a :



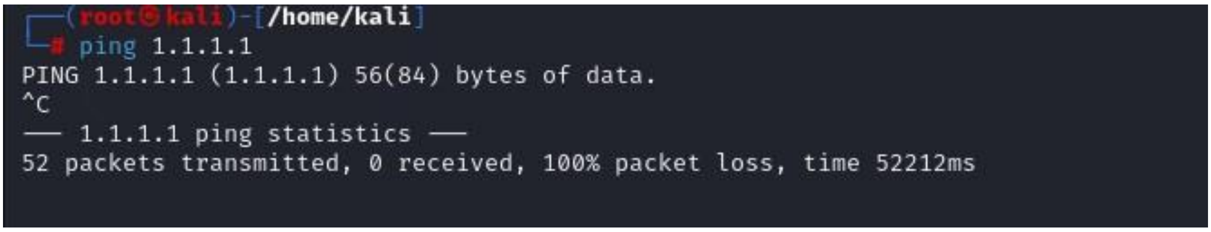
```
┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# ictables -A OUTPUT -p icmp --icmp-type echo-response -j ACCEPT
ictables: command not found

┌──(root㉿kali)-[/home/kali]
└─# iptables -A OUTPUT -p icmp --icmp-type echo-response -j ACCEPT
iptables v1.8.10 (nf_tables): Unknown ICMP type `echo-response'
Try `iptables -h' or 'iptables --help' for more information.

┌──(root㉿kali)-[/home/kali]
└─# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request

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
```

Ping vm from remote machine



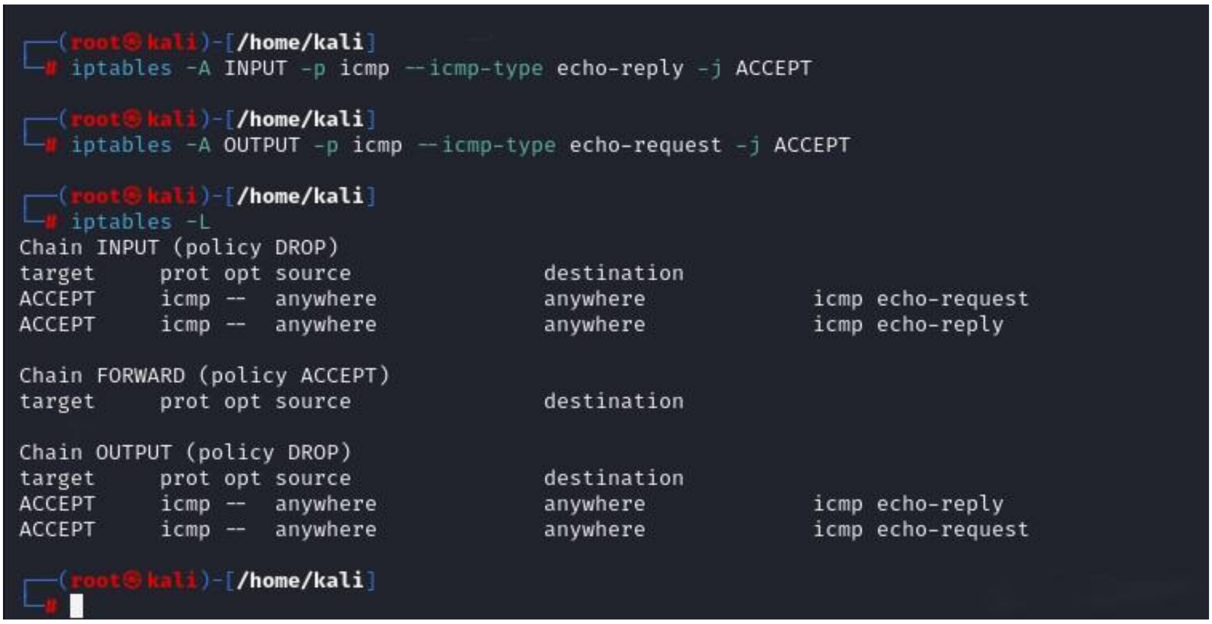
```
ubuntu@ubuntu:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=1.78 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.061 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.062 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.069 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.079 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.061 ms
```

Vm trying to ping machine



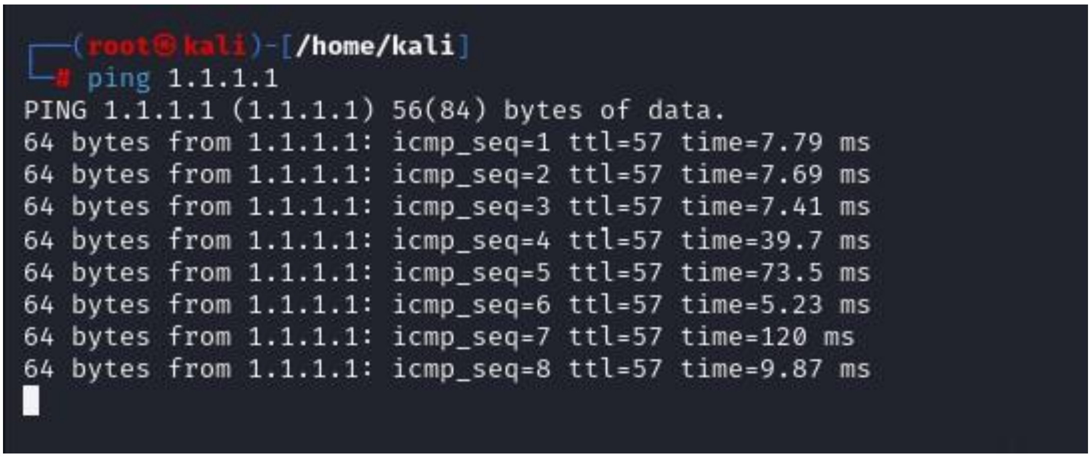
```
┌──(root㉿kali)-[/home/kali]
└─# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
^C
── 1.1.1.1 ping statistics ──
52 packets transmitted, 0 received, 100% packet loss, time 52212ms
```

Part b:



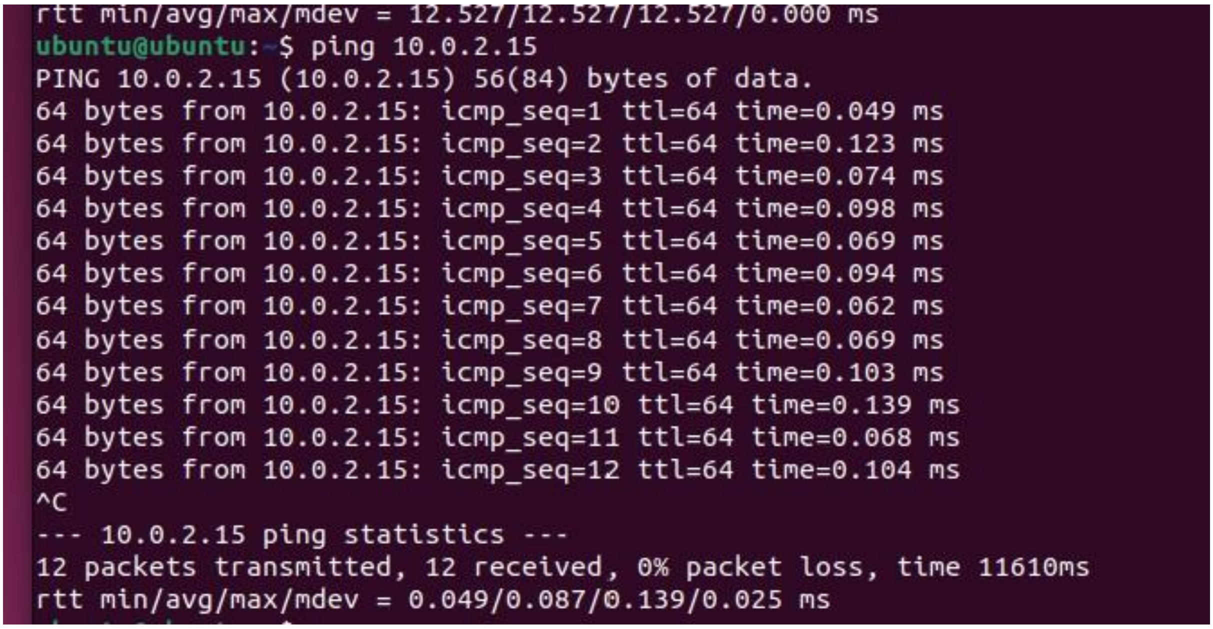
```
┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# 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㉿kali)-[/home/kali]
└─#
```

Vm pinging another machine



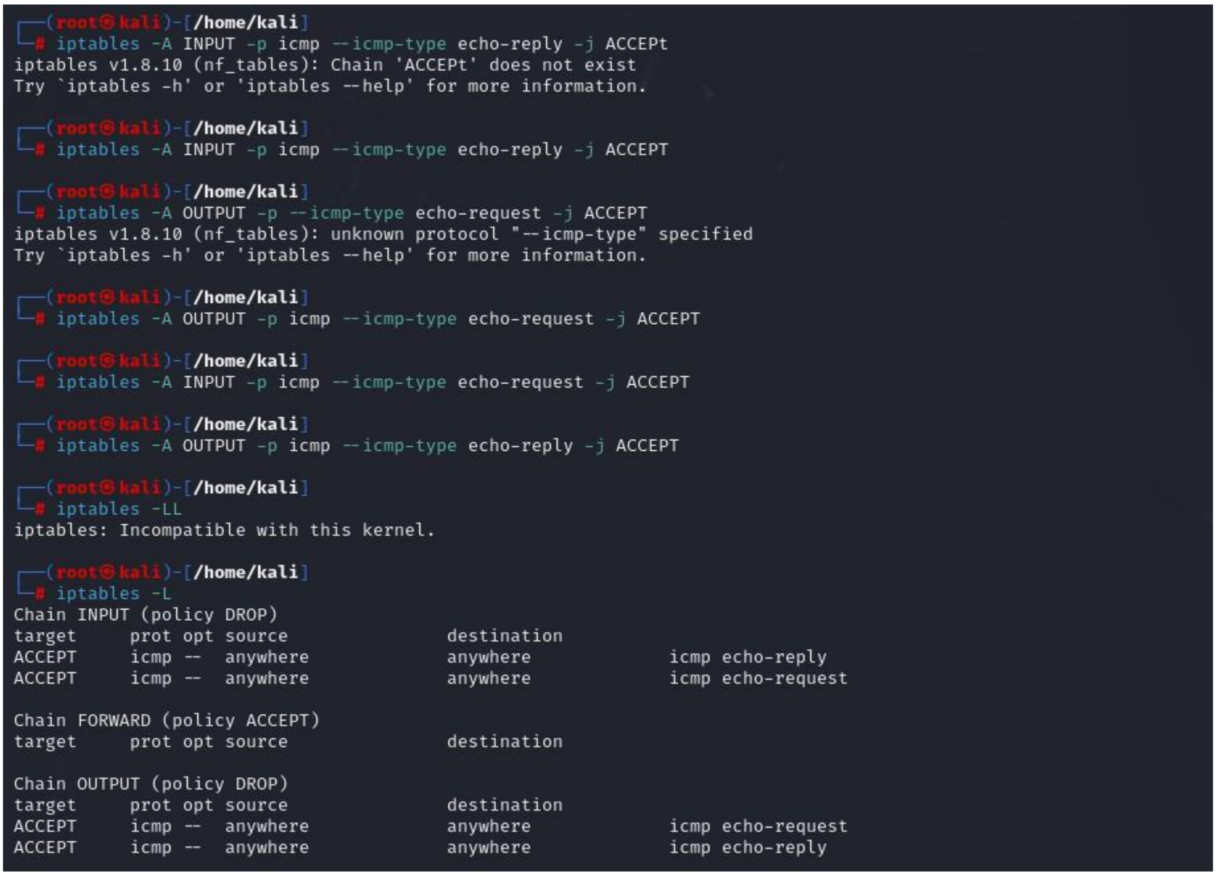
```
┌──(root㉿kali)-[/home/kali]
└─# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=57 time=7.79 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=57 time=7.69 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=57 time=7.41 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=57 time=39.7 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=57 time=73.5 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=57 time=5.23 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=57 time=120 ms
64 bytes from 1.1.1.1: icmp_seq=8 ttl=57 time=9.87 ms
```

Pinging vm machine from remote machine:



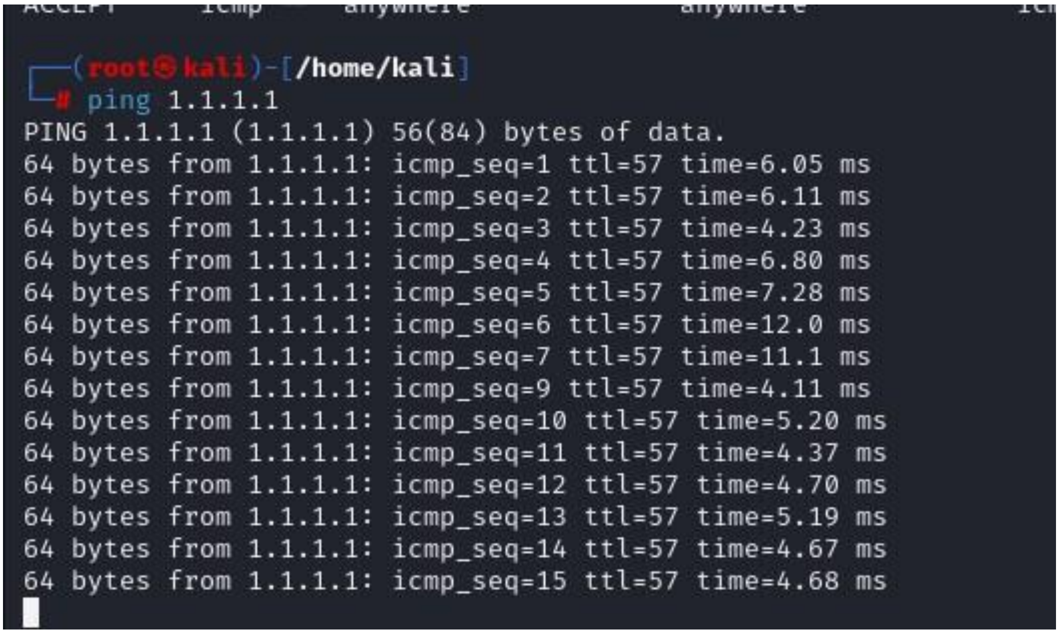
```
rtt min/avg/max/mdev = 12.527/12.527/12.527/0.000 ms
ubuntu@ubuntu:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.049 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.123 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.074 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 :



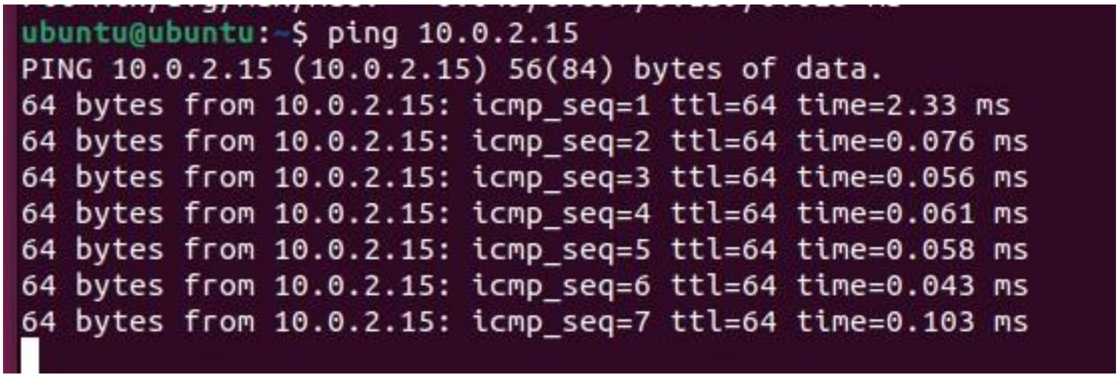
```
┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPt
iptables v1.8.10 (nf_tables): Chain 'ACCEPt' does not exist
Try `iptables -h' or 'iptables --help' for more information.

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# iptables -A OUTPUT -p --icmp-type echo-request -j ACCEPT
iptables v1.8.10 (nf_tables): unknown protocol "--icmp-type" specified
Try `iptables -h' or 'iptables --help' for more information.

┌──(root㉿kali)-[/home/kali]
└─# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# iptables -LL
iptables: Incompatible with this kernel.

┌──(root㉿kali)-[/home/kali]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
```

Ping another machine from VM



```
ACCEPT     icmp     anywhere             anywhere             ic

┌──(root㉿kali)-[/home/kali]
└─# 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=57 time=6.05 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=57 time=6.11 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=57 time=4.23 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=57 time=6.80 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=57 time=7.28 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=57 time=12.0 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=57 time=11.1 ms
64 bytes from 1.1.1.1: icmp_seq=9 ttl=57 time=4.11 ms
64 bytes from 1.1.1.1: icmp_seq=10 ttl=57 time=5.20 ms
64 bytes from 1.1.1.1: icmp_seq=11 ttl=57 time=4.37 ms
64 bytes from 1.1.1.1: icmp_seq=12 ttl=57 time=4.70 ms
64 bytes from 1.1.1.1: icmp_seq=13 ttl=57 time=5.19 ms
64 bytes from 1.1.1.1: icmp_seq=14 ttl=57 time=4.67 ms
64 bytes from 1.1.1.1: icmp_seq=15 ttl=57 time=4.68 ms
```

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
```