

Computer Network Security

Firewall Lab

PES1201801948
Bharath S Bhambore
Section H

Lab Setup :

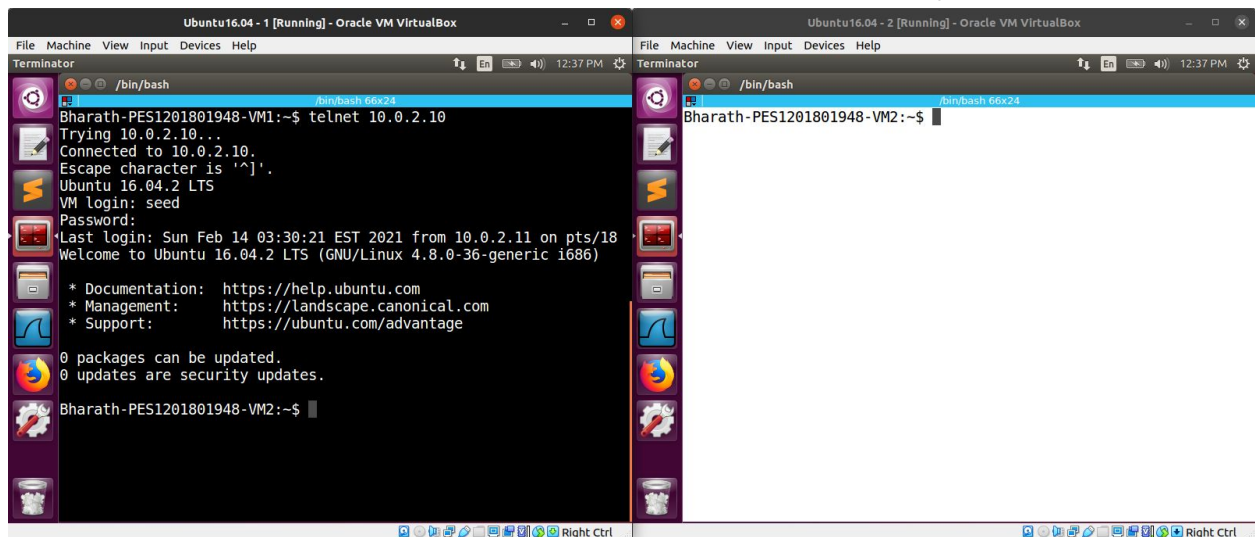
Machine 1 : Ubuntu 16.04 -1 [Black Terminal]
IP : 10.0.2.9

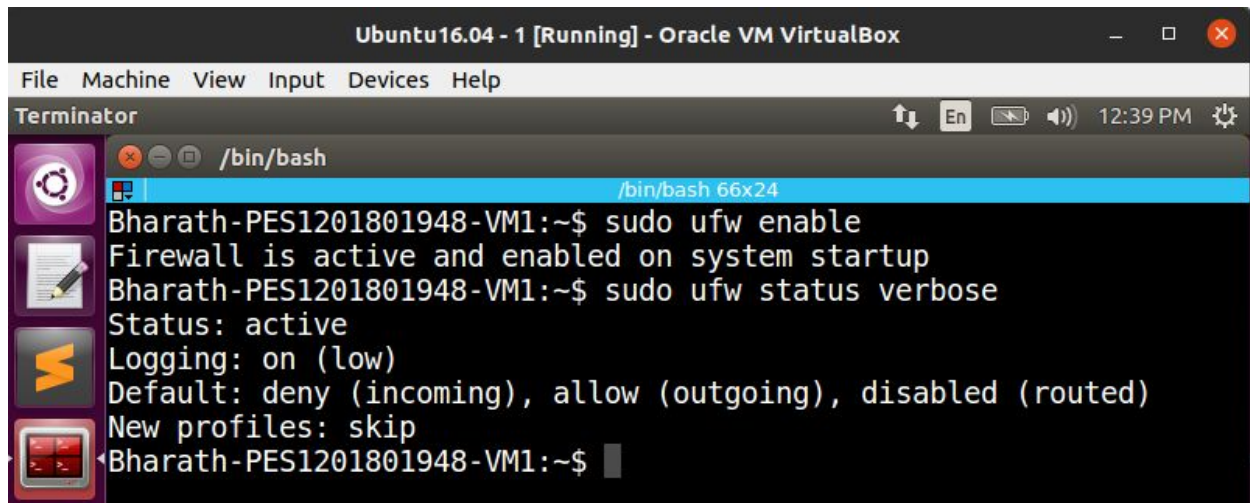
Machine 2 : Ubuntu 16.04 -2 [White Terminal]
IP : 10.0.2.10

Machine 3 : Ubuntu 16.04 -3
IP : 10.0.2.11

Task 1: Using Firewall

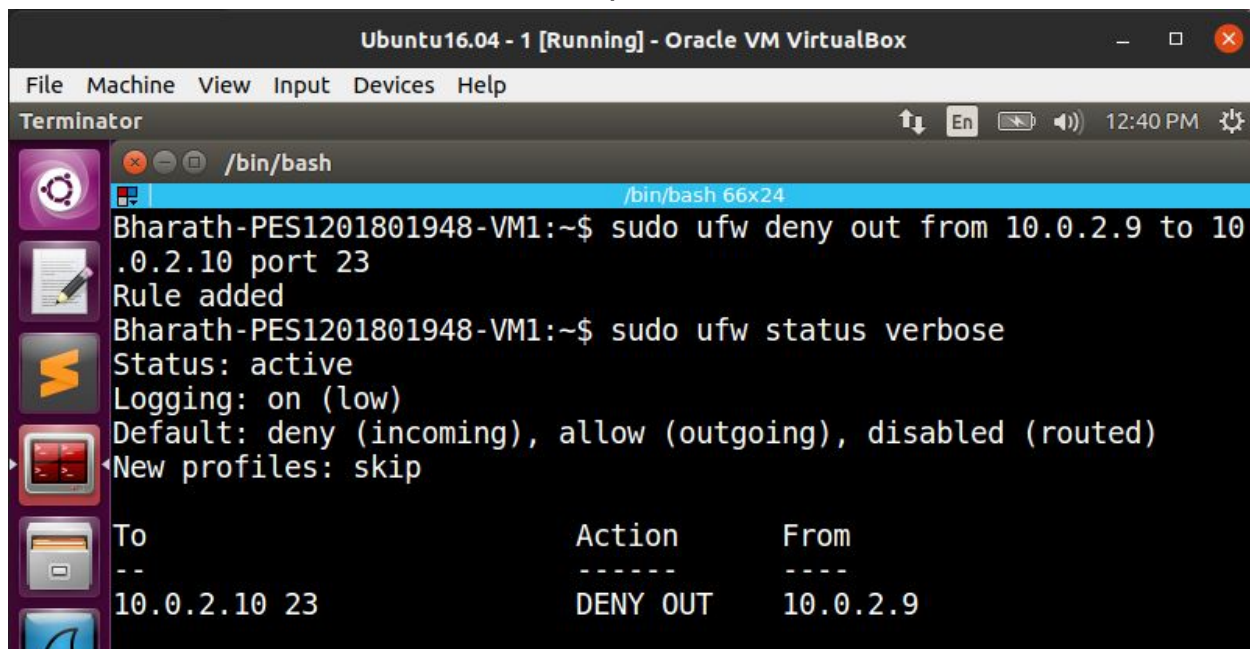
VM1[10.0.2.9] can telnet into VM2[10.0.2.10] successfully as shown below





```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~$ sudo ufw enable
Firewall is active and enabled on system startup
Bharath-PES1201801948-VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
Bharath-PES1201801948-VM1:~$
```

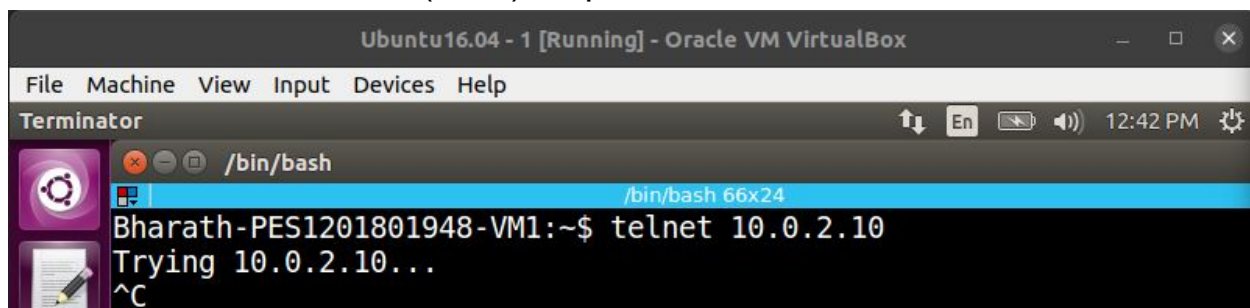
We have now enabled ufw -> uncomplicated firewall on VM 1



```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~$ sudo ufw deny out from 10.0.2.9 to 10
.0.2.10 port 23
Rule added
Bharath-PES1201801948-VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

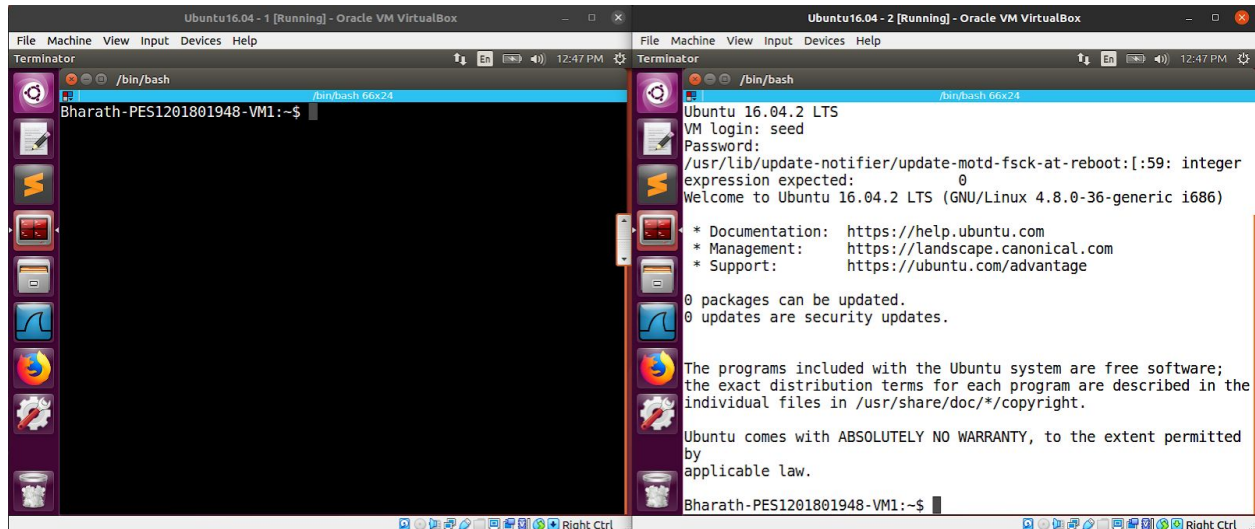
To Action From
--
10.0.2.10 23 DENY OUT 10.0.2.9
```

Telnet from 10.0.2.9 (VM1) fails as we have a firewall rule to deny outgoing connections to 10.0.2.10 (VM2) on port 23

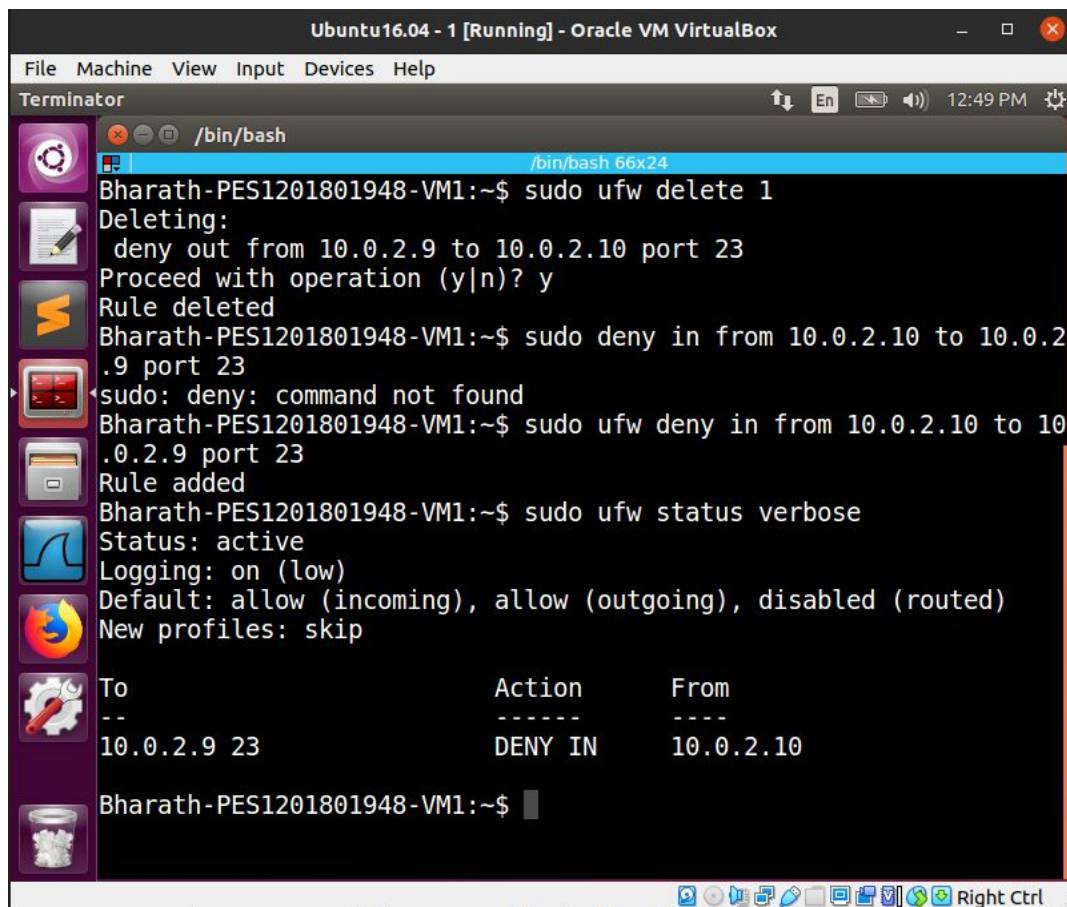


```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~$ telnet 10.0.2.10
Trying 10.0.2.10...
^C
```

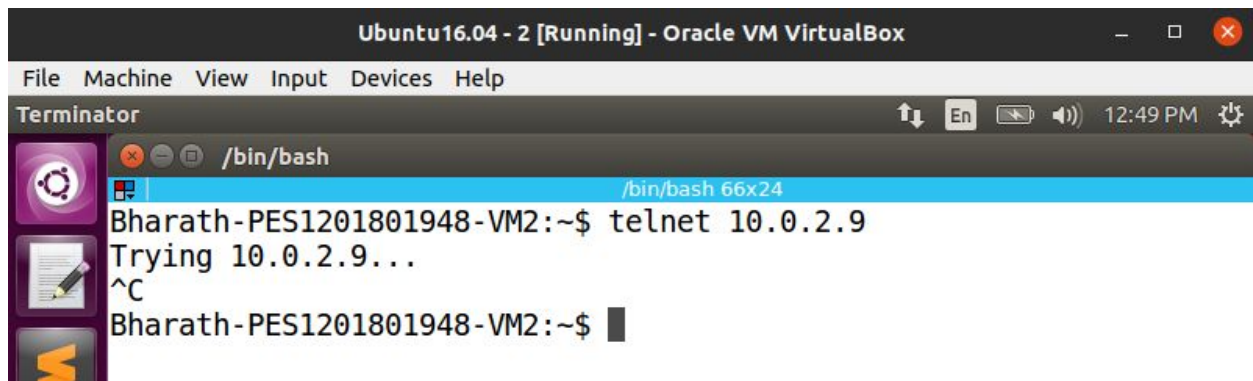
But incoming telnet connections aren't blocked, therefore we can successfully telnet into VM1 from VM2



Deleting the first firewall rule, and setting up a new one to deny incoming connections to VM1



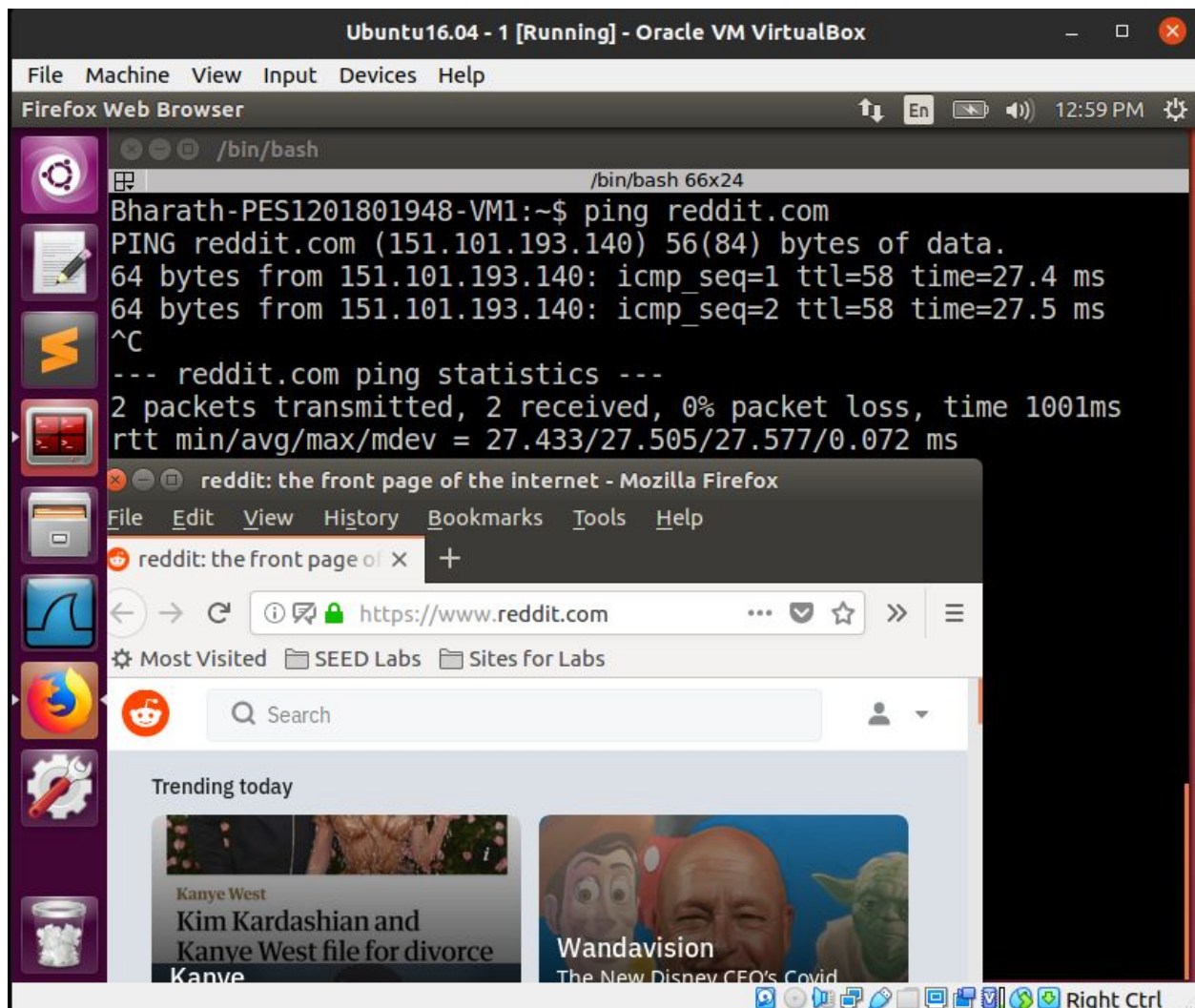
Telnet into VM1 from VM2 is unsuccessful



```
Ubuntu16.04 - 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
Bharath-PES1201801948-VM2:~$ telnet 10.0.2.9
Trying 10.0.2.9...
^C
Bharath-PES1201801948-VM2:~$
```

Since pes.edu wasnt working, i have used reddit.com

We find the IP of reddit using ping, also open in the browser showing it works



```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox Web Browser
/bin/bash
Bharath-PES1201801948-VM1:~$ ping reddit.com
PING reddit.com (151.101.193.140) 56(84) bytes of data.
64 bytes from 151.101.193.140: icmp_seq=1 ttl=58 time=27.4 ms
64 bytes from 151.101.193.140: icmp_seq=2 ttl=58 time=27.5 ms
^C
--- reddit.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 27.433/27.505/27.577/0.072 ms
```

reddit: the front page of the internet - Mozilla Firefox

File Edit View History Bookmarks Tools Help

reddit: the front page of X +

https://www.reddit.com

Most Visited SEED Labs Sites for Labs

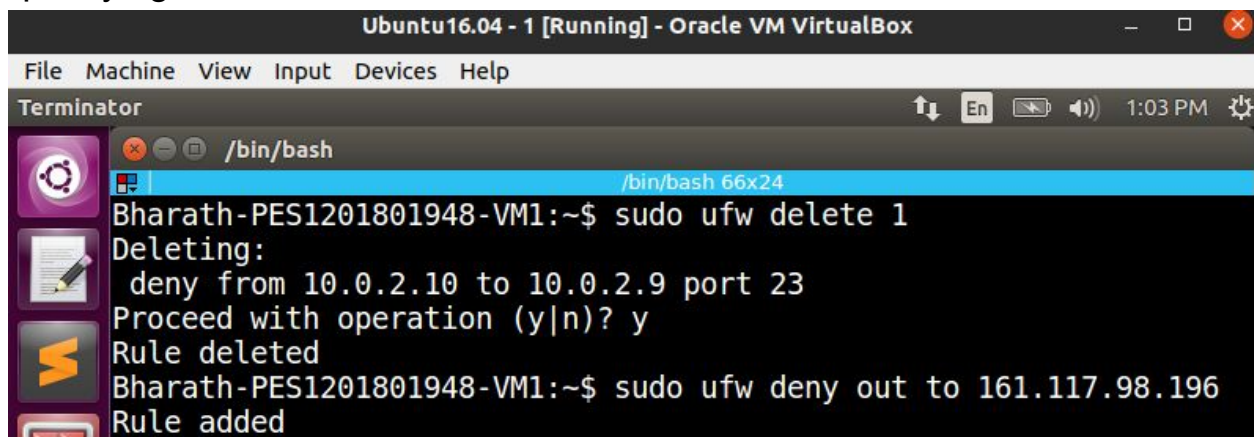
Search

Trending today

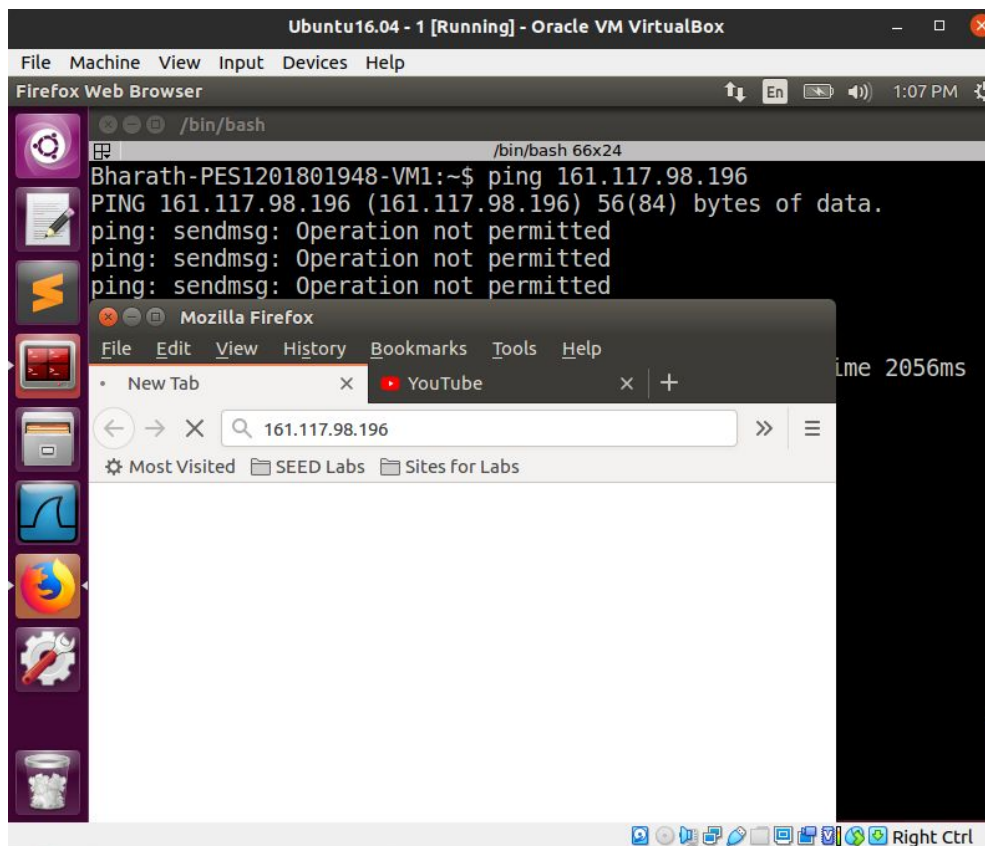
Kanye West Kim Kardashian and Kanye West file for divorce

Wandavision The New Disney CEO's Covid

Adding a new firewall rule to deny outgoing connections to reddit by specifying its IP



```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~$ sudo ufw delete 1
Deleting:
deny from 10.0.2.10 to 10.0.2.9 port 23
Proceed with operation (y|n)? y
Rule deleted
Bharath-PES1201801948-VM1:~$ sudo ufw deny out to 161.117.98.196
Rule added
```

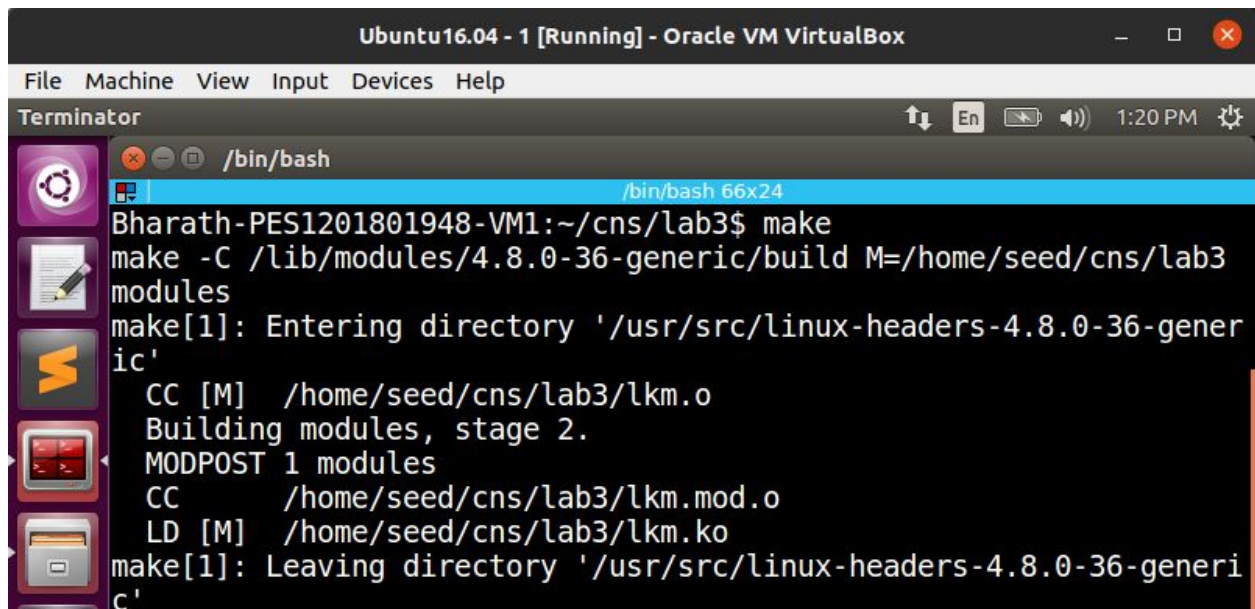


```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox Web Browser
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~$ ping 161.117.98.196
PING 161.117.98.196 (161.117.98.196) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
time 2056ms

Mozilla Firefox
File Edit View History Bookmarks Tools Help
New Tab x YouTube x +
161.117.98.196
Most Visited SEED Labs Sites for Labs
```

We get operation not permitted on ping, and we cant access the webpage in the browser as well.

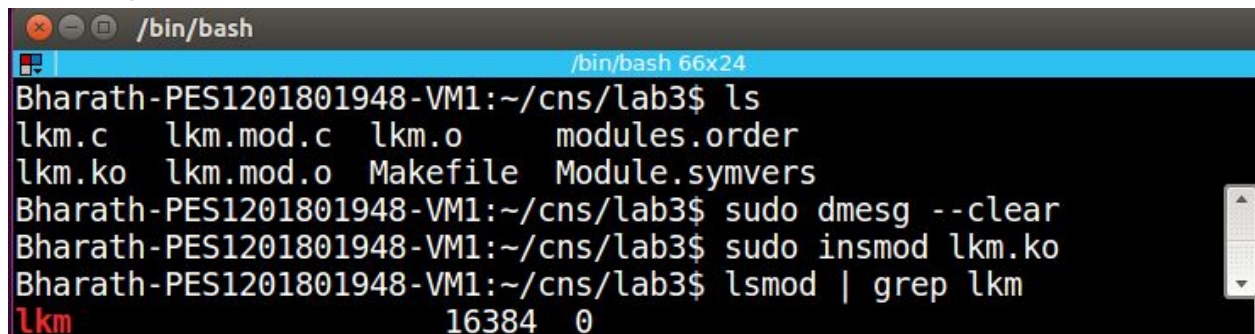
Task 2: How Firewall Works



The screenshot shows a terminal window titled "Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox". The terminal is running a shell prompt "Bharath-PES1201801948-VM1:~/cns/lab3\$". The user has entered the command "make". The output shows the compilation process for a kernel module named "lkm.o". The process involves entering the directory "/usr/src/linux-headers-4.8.0-36-generic", compiling the module, and then leaving the directory. The final output is "make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'".

```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~/cns/lab3$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed/cns/lab3
modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
CC [M] /home/seed/cns/lab3/lkm.o
Building modules, stage 2.
MODPOST 1 modules
CC /home/seed/cns/lab3/lkm.mod.o
LD [M] /home/seed/cns/lab3/lkm.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
```

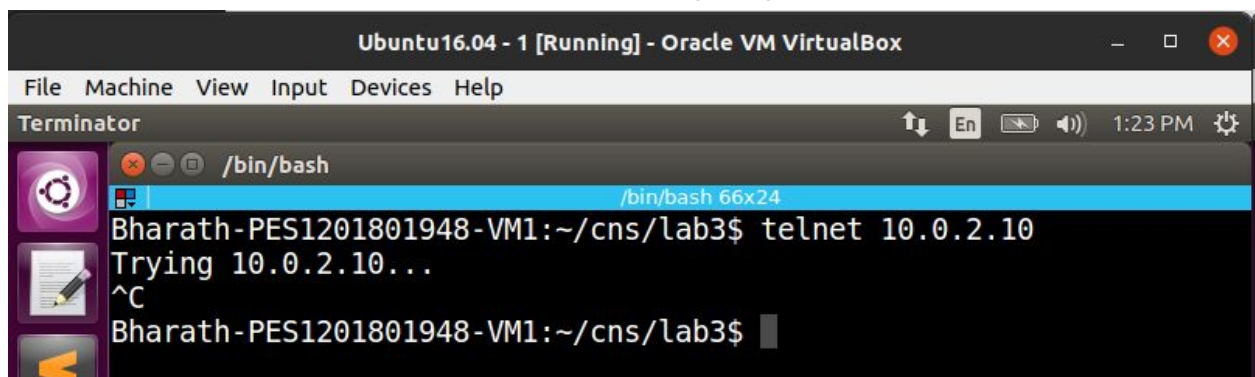
Running the make file sets up the lkm.c file in the kernel space.



The screenshot shows a terminal window titled "Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox". The terminal is running a shell prompt "Bharath-PES1201801948-VM1:~/cns/lab3\$". The user has entered the command "ls", which lists the files in the directory: "lkm.c", "lkm.mod.c", "lkm.o", "modules.order", "lkm.ko", "lkm.mod.o", "Makefile", and "Module.symvers". The user then enters "sudo dmesg --clear", "sudo insmod lkm.ko", and "lsmod | grep lkm". The output of "lsmod | grep lkm" shows "lkm" loaded with size 16384 and priority 0.

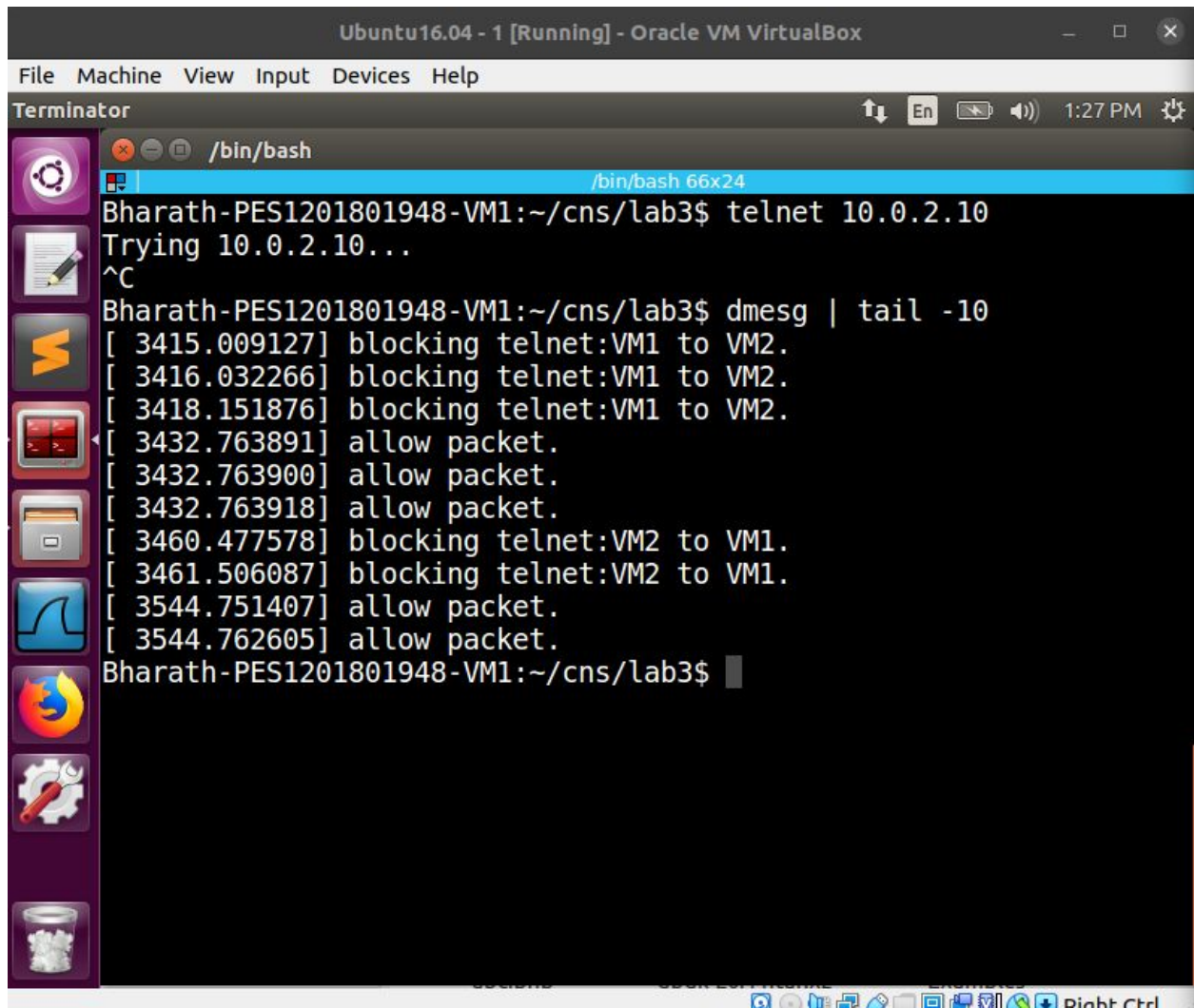
```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~/cns/lab3$ ls
lkm.c  lkm.mod.c  lkm.o      modules.order
lkm.ko  lkm.mod.o  Makefile   Module.symvers
Bharath-PES1201801948-VM1:~/cns/lab3$ sudo dmesg --clear
Bharath-PES1201801948-VM1:~/cns/lab3$ sudo insmod lkm.ko
Bharath-PES1201801948-VM1:~/cns/lab3$ lsmod | grep lkm
lkm                16384  0
```

Telnet into VM2 fails as we prevented outgoing telnet connections



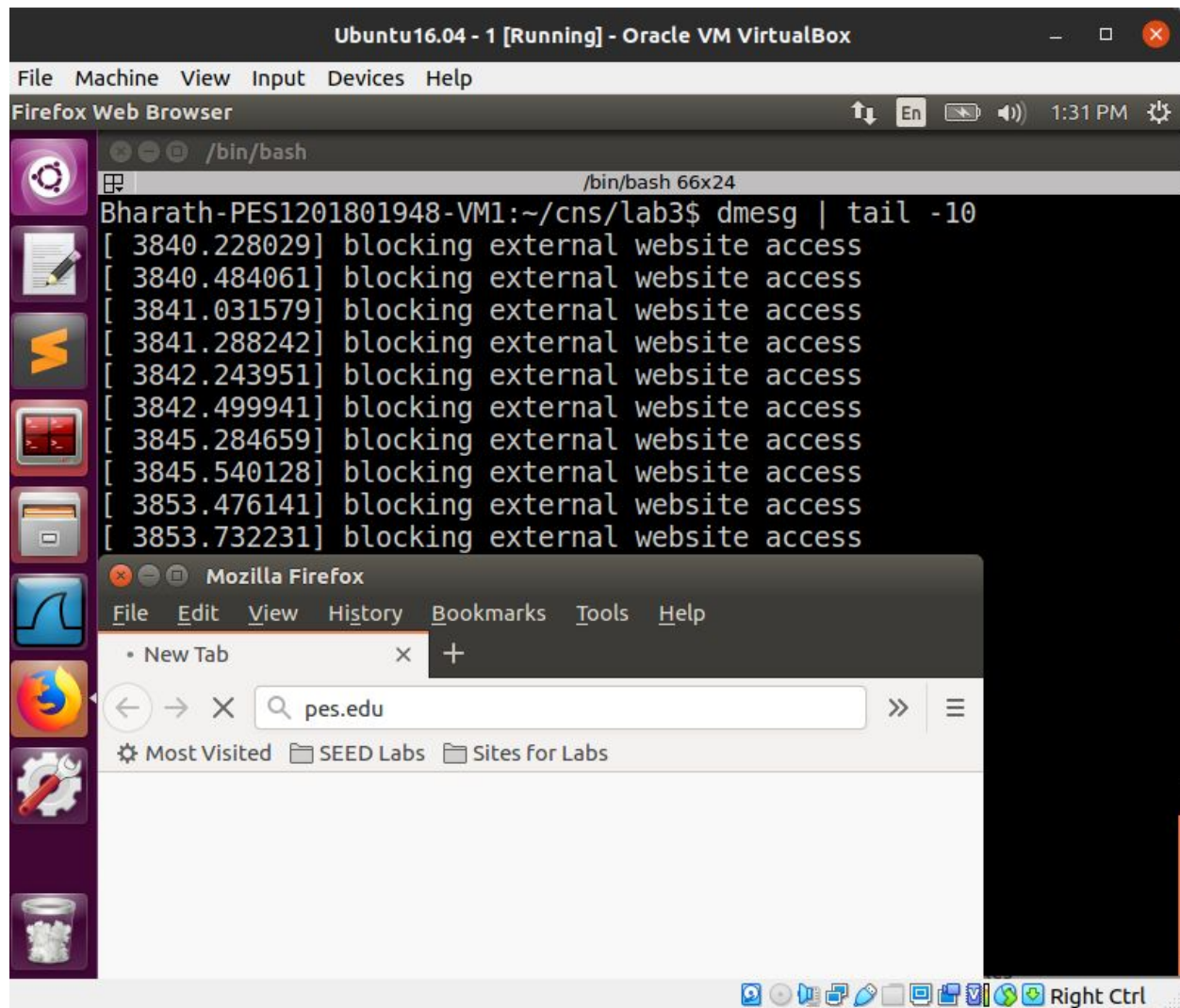
The screenshot shows a terminal window titled "Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox". The terminal is running a shell prompt "Bharath-PES1201801948-VM1:~/cns/lab3\$". The user has entered the command "telnet 10.0.2.10". The output shows "Trying 10.0.2.10..." followed by a carriage return (^C) and the prompt "Bharath-PES1201801948-VM1:~/cns/lab3\$".

```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~/cns/lab3$ telnet 10.0.2.10
Trying 10.0.2.10...
^C
Bharath-PES1201801948-VM1:~/cns/lab3$
```

```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~/cns/lab3$ telnet 10.0.2.10
Trying 10.0.2.10...
^C
Bharath-PES1201801948-VM1:~/cns/lab3$ dmesg | tail -10
[ 3415.009127] blocking telnet:VM1 to VM2.
[ 3416.032266] blocking telnet:VM1 to VM2.
[ 3418.151876] blocking telnet:VM1 to VM2.
[ 3432.763891] allow packet.
[ 3432.763900] allow packet.
[ 3432.763918] allow packet.
[ 3460.477578] blocking telnet:VM2 to VM1.
[ 3461.506087] blocking telnet:VM2 to VM1.
[ 3544.751407] allow packet.
[ 3544.762605] allow packet.
Bharath-PES1201801948-VM1:~/cns/lab3$
```

We can see the logs of this file, shows the telnet is blocked from both ends, ie VM1 to VM2 and VM2 to VM1



Website access is also blocked as we can see in the browser request, it fails.


```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~/cns/lab3$ ssh seed@10.0.2.10
^C
Bharath-PES1201801948-VM1:~/cns/lab3$ dmesg | tail -10
[ 3632.785516] blocking telnet:VM2 to VM1.
[ 3634.803915] blocking telnet:VM2 to VM1.
[ 3688.750142] allow packet.
[ 3688.750268] allow packet.
[ 3688.750285] allow packet.
[ 3729.592923] blocking ssh: VM1 to VM2.
[ 3730.596061] blocking ssh: VM1 to VM2.
[ 3732.611995] blocking ssh: VM1 to VM2.
[ 3747.880635] blocking ssh:VM2 to VM1.
[ 3748.909026] blocking ssh:VM2 to VM1.
```

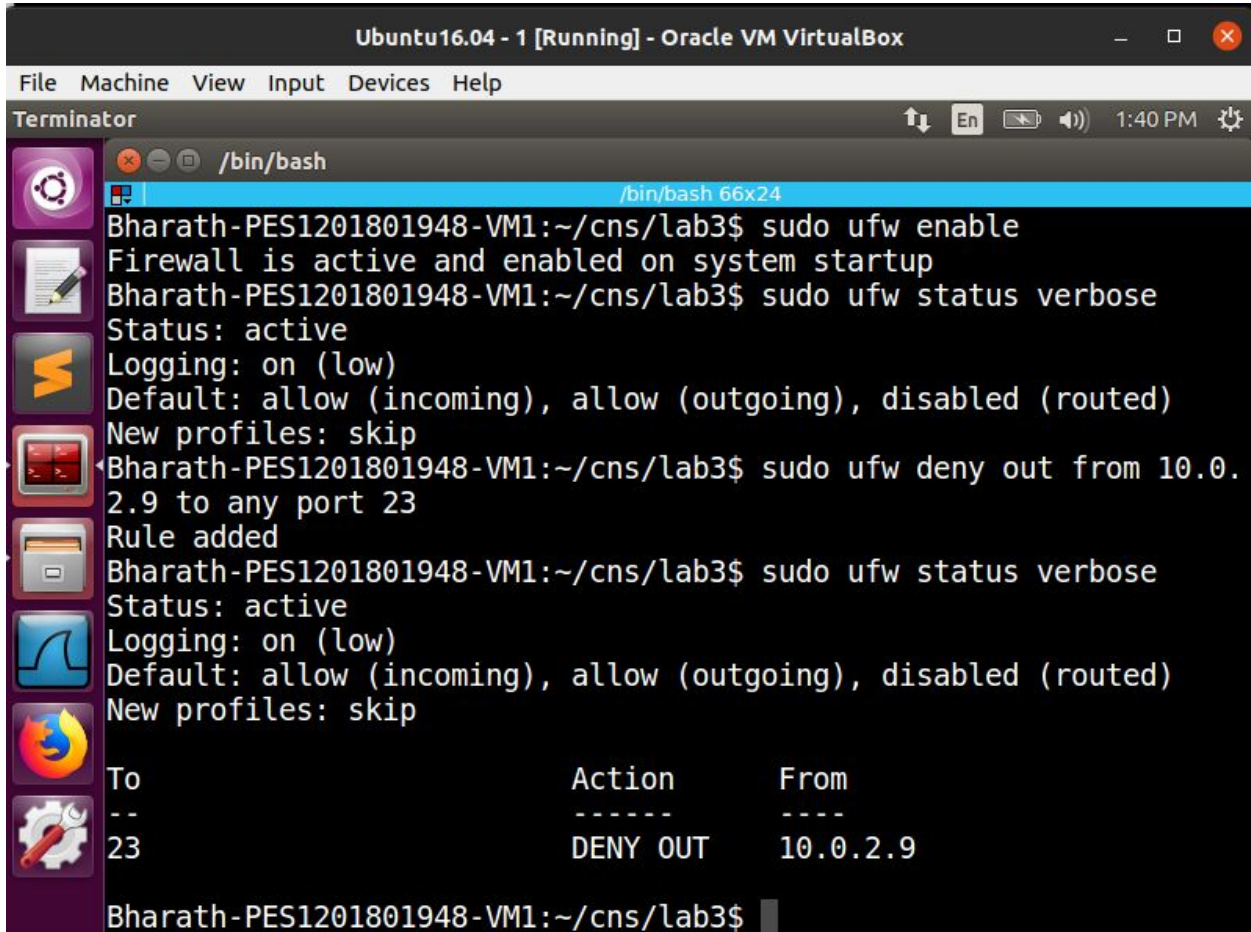
```
Ubuntu16.04 - 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM2:~$ ssh seed@10.0.2.9
^C
```

SSH from either of the machines to one another fails

Task 3: Evading Egress Filtering

Task 3.a: Telnet to Machine B through the firewall

Firewall rule added denying outgoing telnet connections.



```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~/cns/lab3$ sudo ufw enable
Firewall is active and enabled on system startup
Bharath-PES1201801948-VM1:~/cns/lab3$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
Bharath-PES1201801948-VM1:~/cns/lab3$ sudo ufw deny out from 10.0.
2.9 to any port 23
Rule added
Bharath-PES1201801948-VM1:~/cns/lab3$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To Action From
--
23 DENY OUT 10.0.2.9
Bharath-PES1201801948-VM1:~/cns/lab3$
```

As we can see both the telnet connections are blocked.

```
Bharath-PES1201801948-VM1:~/cns/lab3$ telnet 10.0.2.10
Trying 10.0.2.10...
^C
Bharath-PES1201801948-VM1:~/cns/lab3$ telnet 10.0.2.11
Trying 10.0.2.11...
^C
Bharath-PES1201801948-VM1:~/cns/lab3$
```

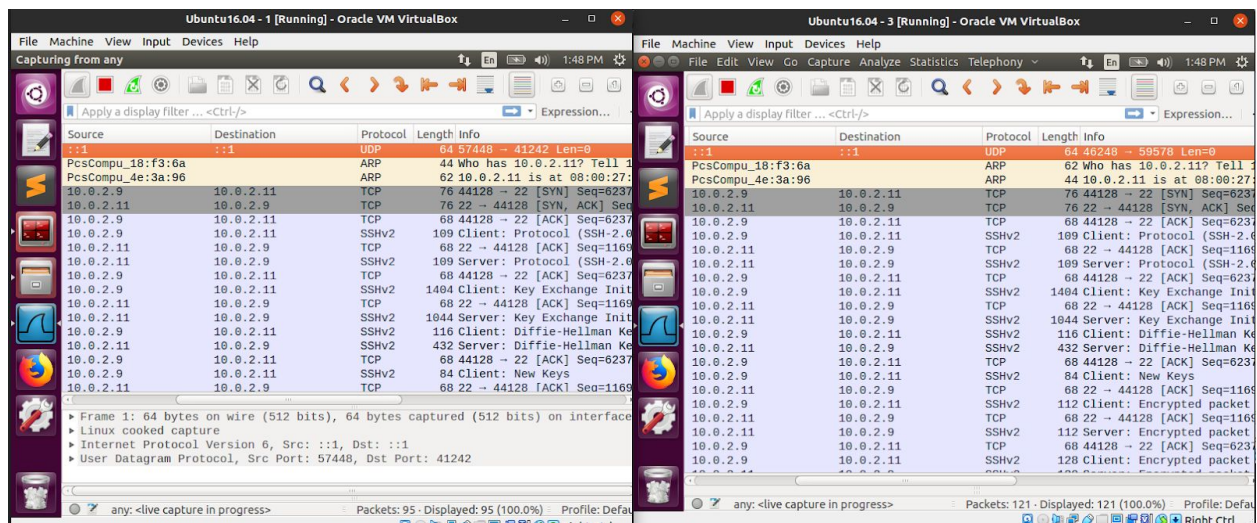
We setup an ssh tunnel between 10.0.2.9 and 10.0.2.11, to telnet into 10.0.2.10

```
Bharath-PES1201801948-VM1:~/cns/lab3$ ssh -L 8000:10.0.2.10:23 seed@10.0.2.11
The authenticity of host '10.0.2.11 (10.0.2.11)' can't be established.
ECDSA key fingerprint is SHA256:plzAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xqlEYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.11' (ECDSA) to the list of known hosts.
seed@10.0.2.11's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

0 packages can be updated.
0 updates are security updates.

Last login: Sun Feb 14 12:24:16 2021 from 10.0.2.10
Bharath-PES1201801948-VM3:~$ echo $USER
seed
```



We can see the wireshark captures of both 10.0.2.9 and 10.0.2.11


```
/bin/bash
Bharath-PES1201801948-VM1:~$ ssh -L 8000:10.0.2.10:23 seed@10.0.2.11
seed@10.0.2.11's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

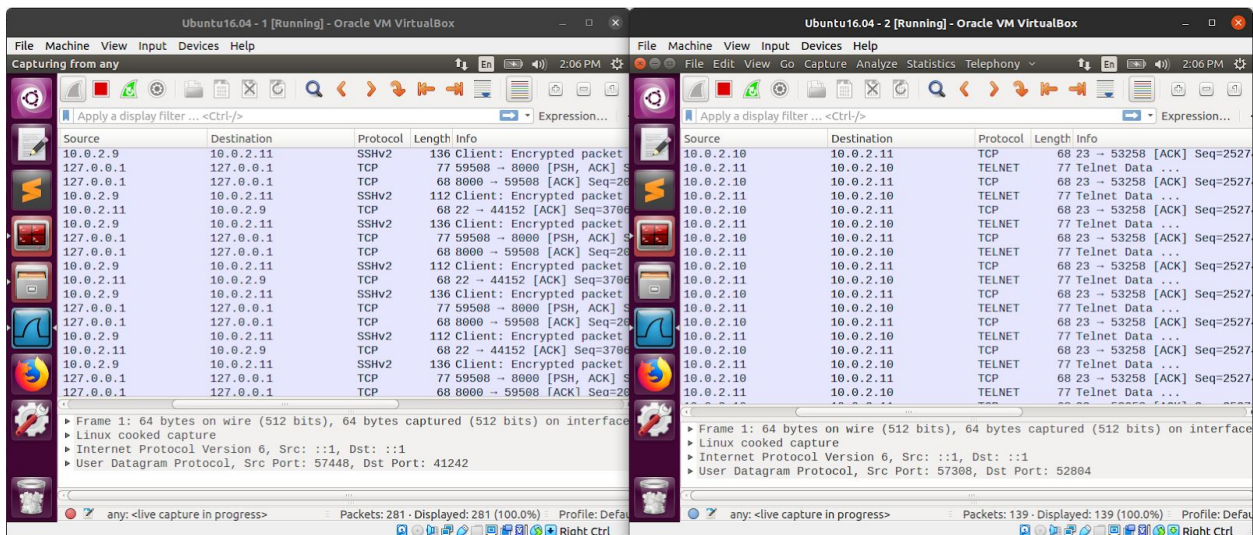
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

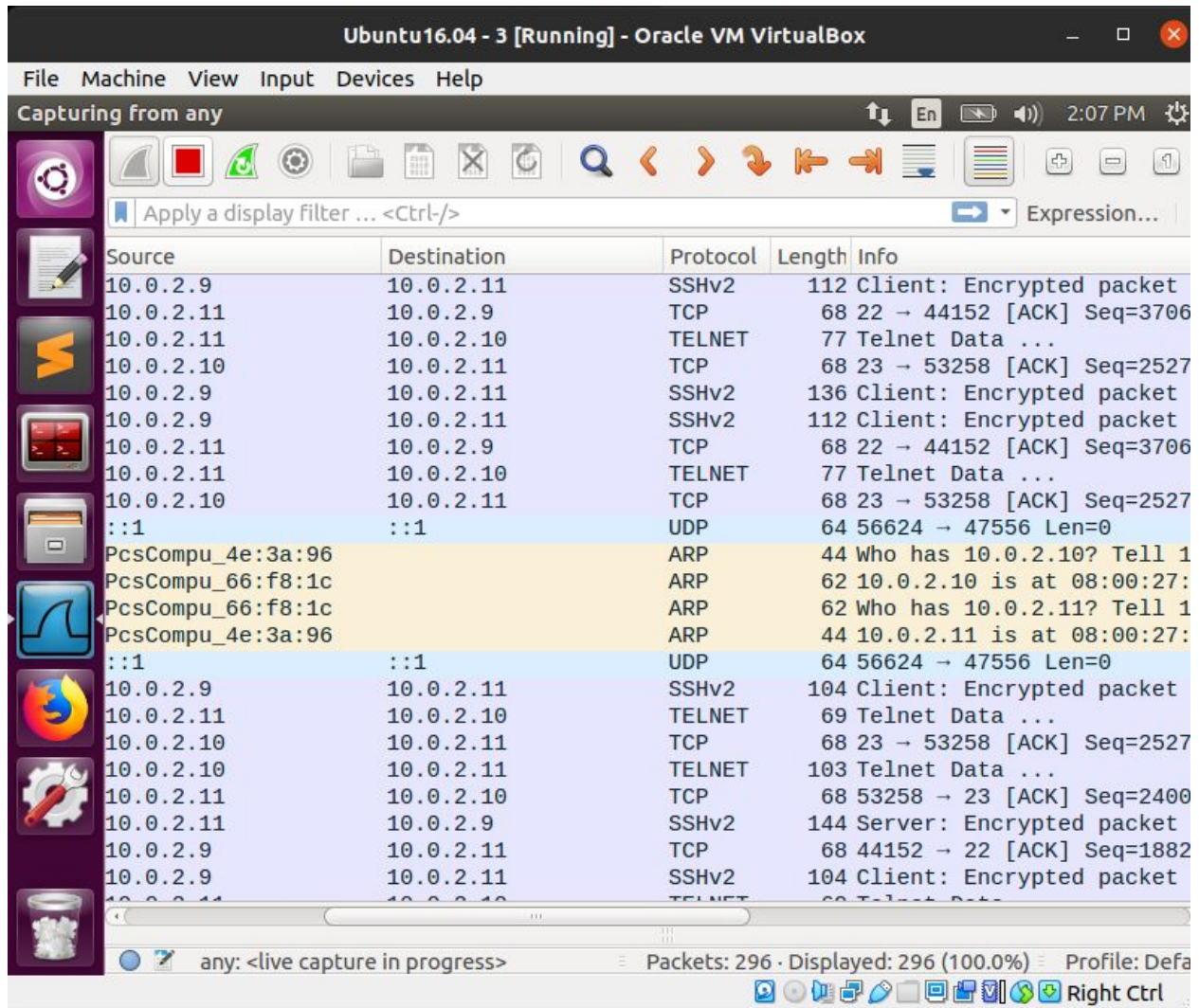
Last login: Sat Feb 20 13:58:32 2021 from 10.0.2.9
Bharath-PES1201801948-VM3:~$

/bin/bash 66x8
Bharath-PES1201801948-VM1:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Feb 20 13:59:33 EST 2021 from 10.0.2.11 on pts/18
```

Telnet into localhost connects us to 10.0.2.10 which was desired

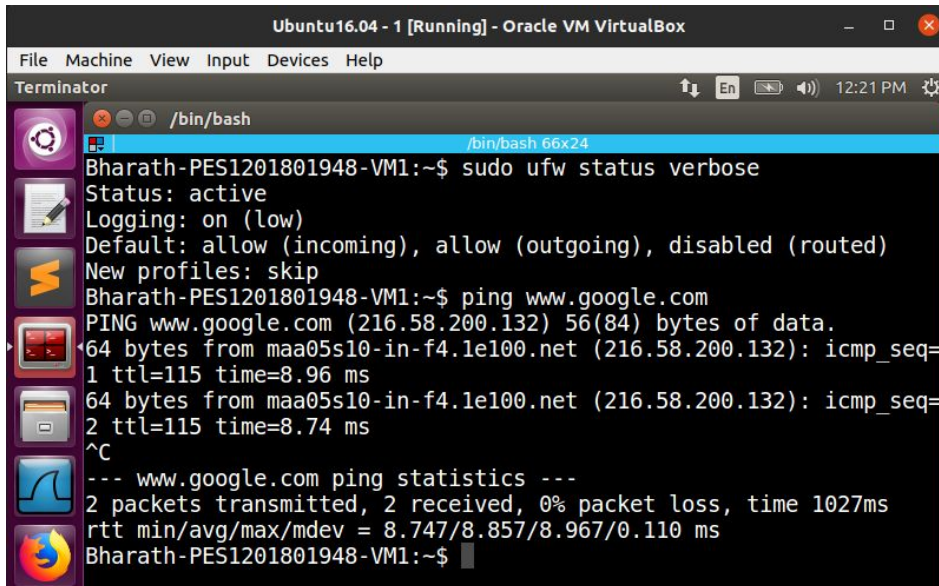


Above are the wireshark captures of 10.0.2.9 and 10.0.2.10



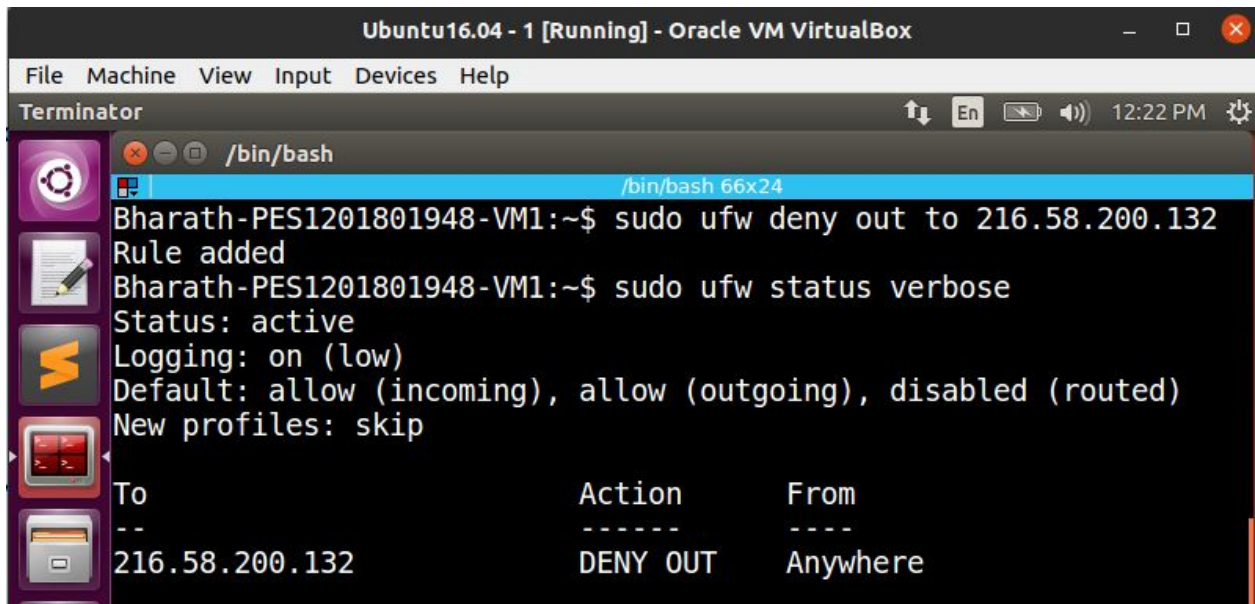
Wireshark capture of 10.0.2.11

Task 3.b: Connecting to Google using SSH tunnel



```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
Bharath-PES1201801948-VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip
Bharath-PES1201801948-VM1:~$ ping www.google.com
PING www.google.com (216.58.200.132) 56(84) bytes of data.
64 bytes from maa05s10-in-f4.1e100.net (216.58.200.132): icmp_seq=
1 ttl=115 time=8.96 ms
64 bytes from maa05s10-in-f4.1e100.net (216.58.200.132): icmp_seq=
2 ttl=115 time=8.74 ms
^C
--- www.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1027ms
rtt min/avg/max/mdev = 8.747/8.857/8.967/0.110 ms
Bharath-PES1201801948-VM1:~$
```

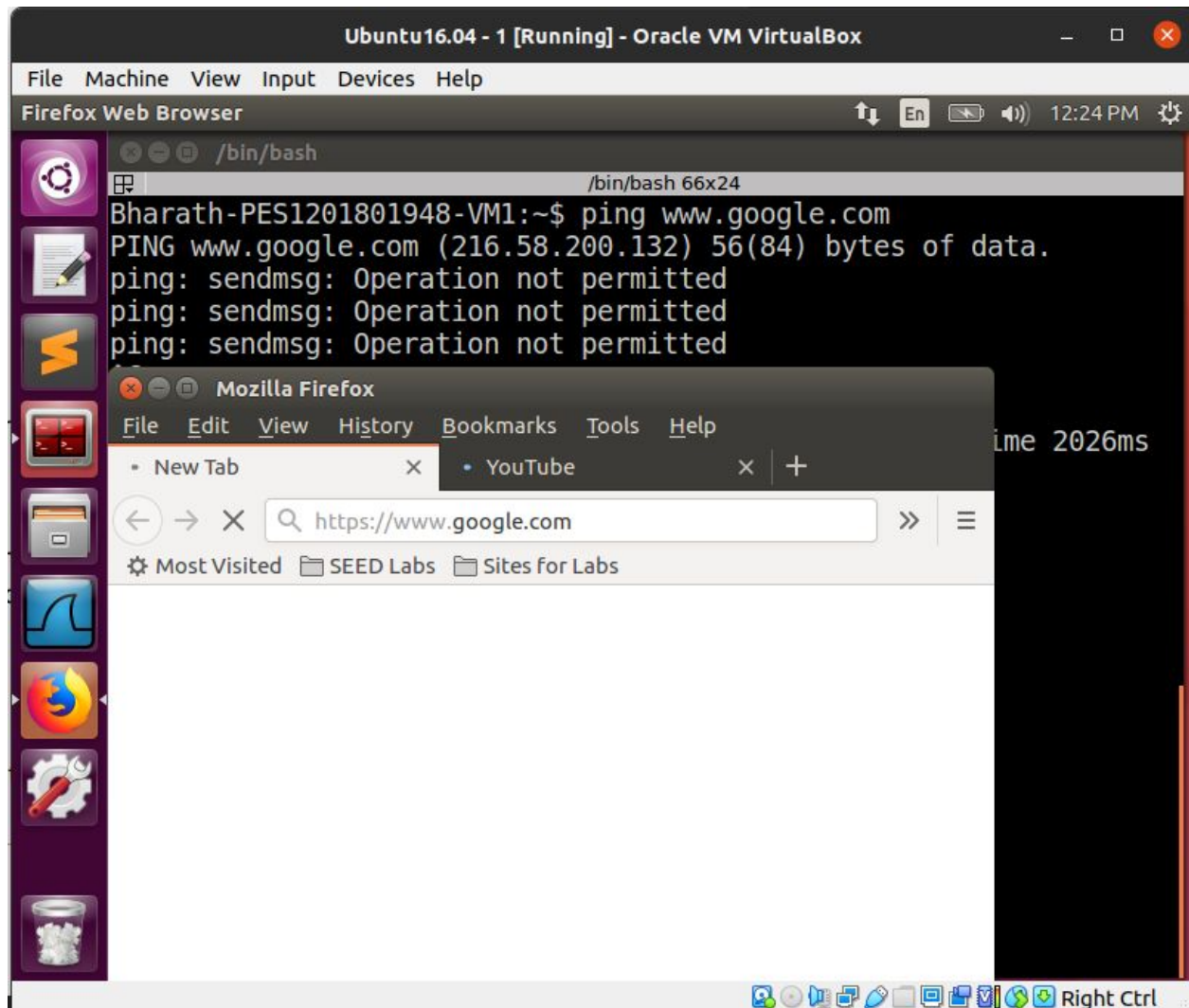
We get the IP of Google.com, and add a firewall rule to deny outgoing connections to it



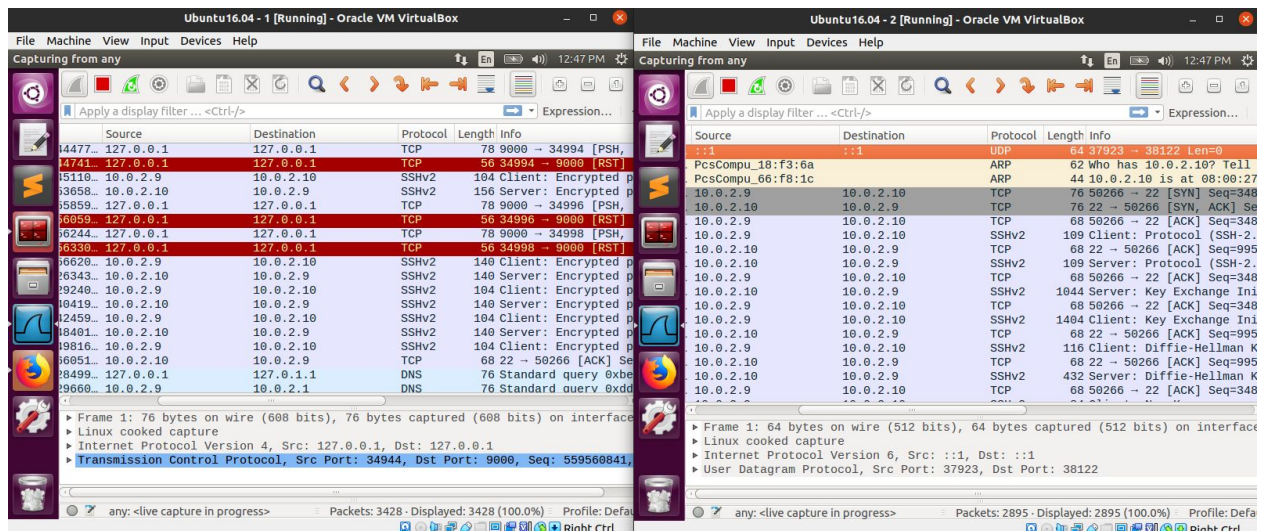
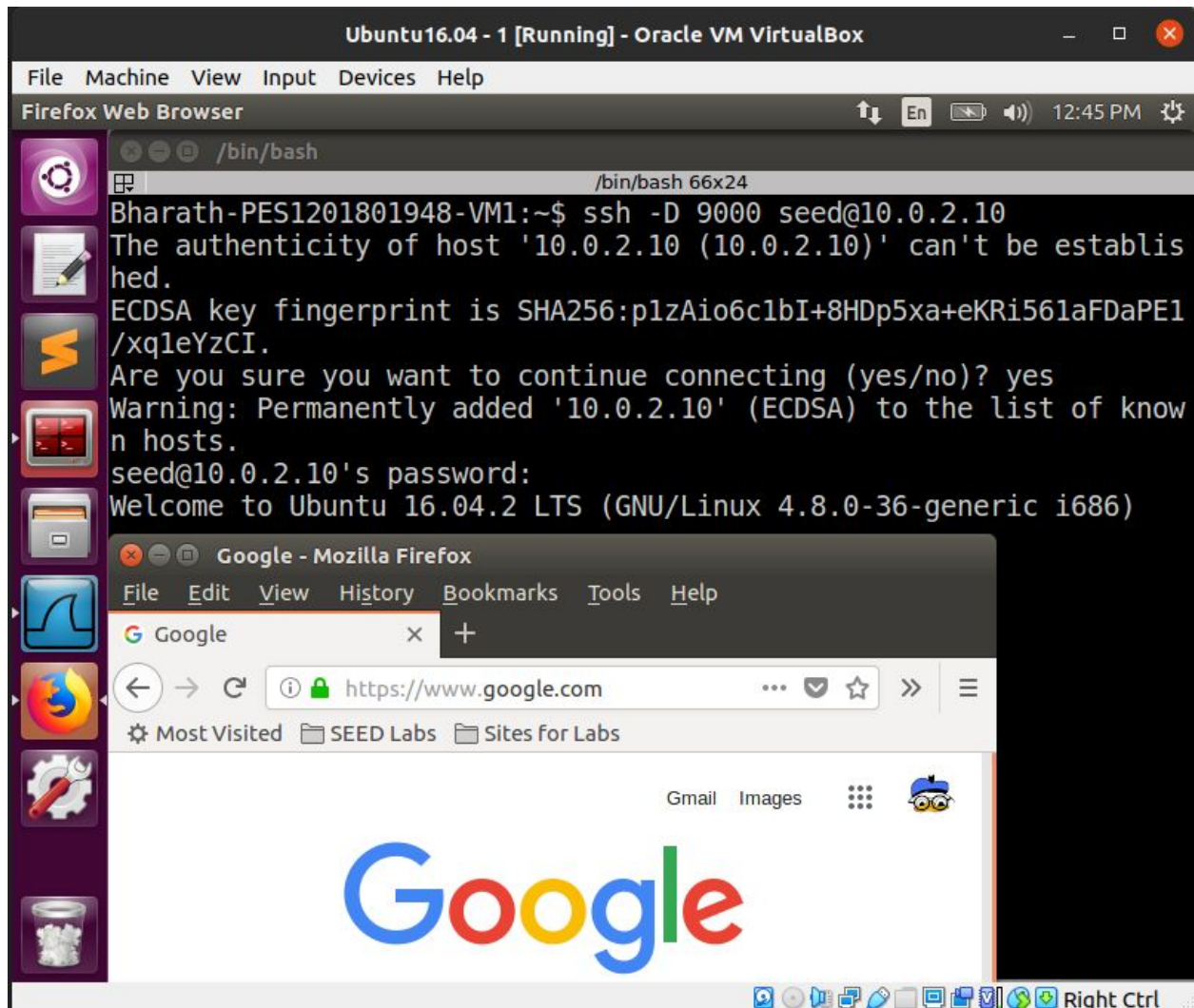
```
Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
Bharath-PES1201801948-VM1:~$ sudo ufw deny out to 216.58.200.132
Rule added
Bharath-PES1201801948-VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
216.58.200.132 DENY OUT Anywhere
```

Therefore, both ping and the browser request fail

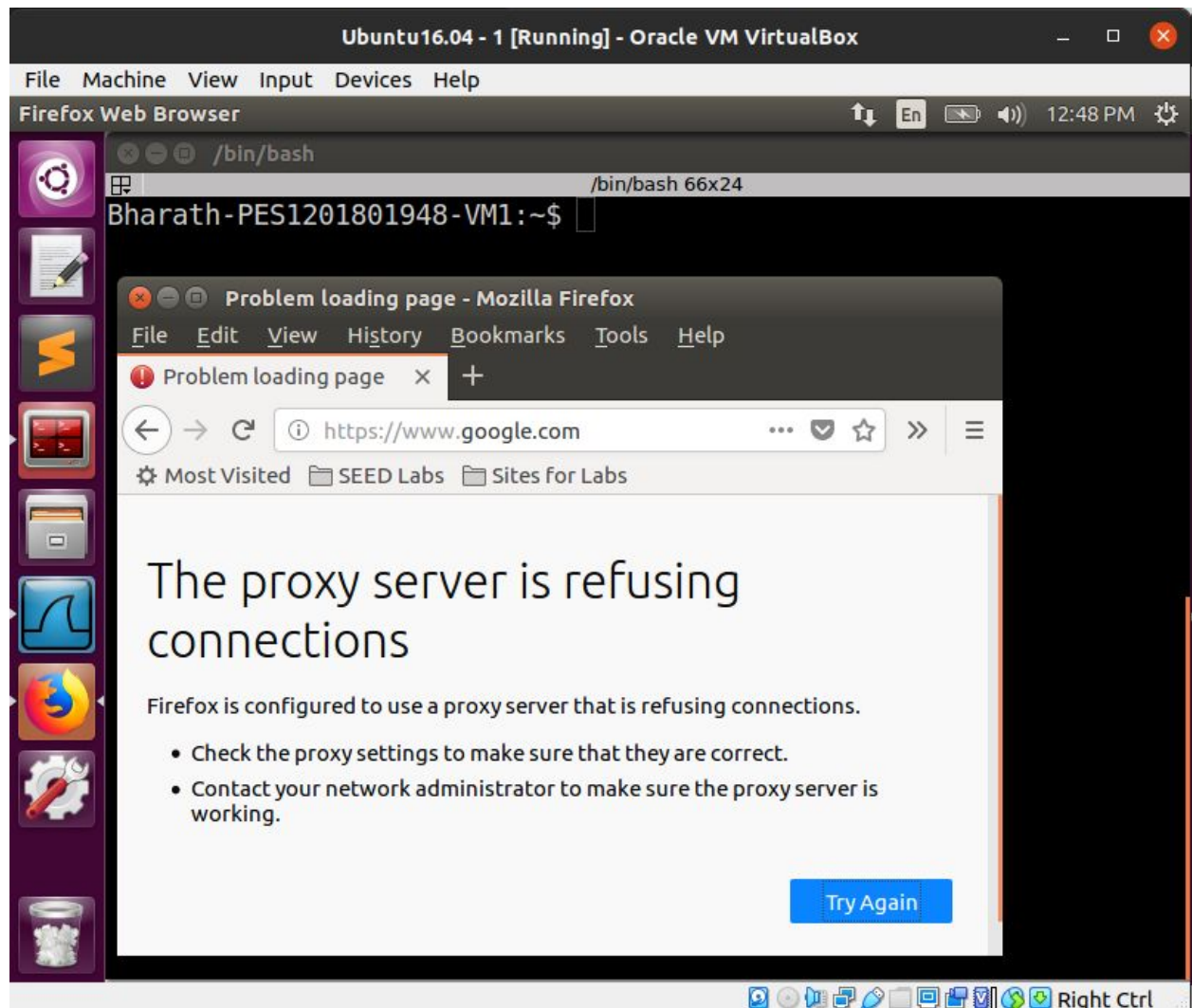


We setup a ssh tunnel between 10.0.2.9 and 10.0.2.10 to access google even with the firewall present.

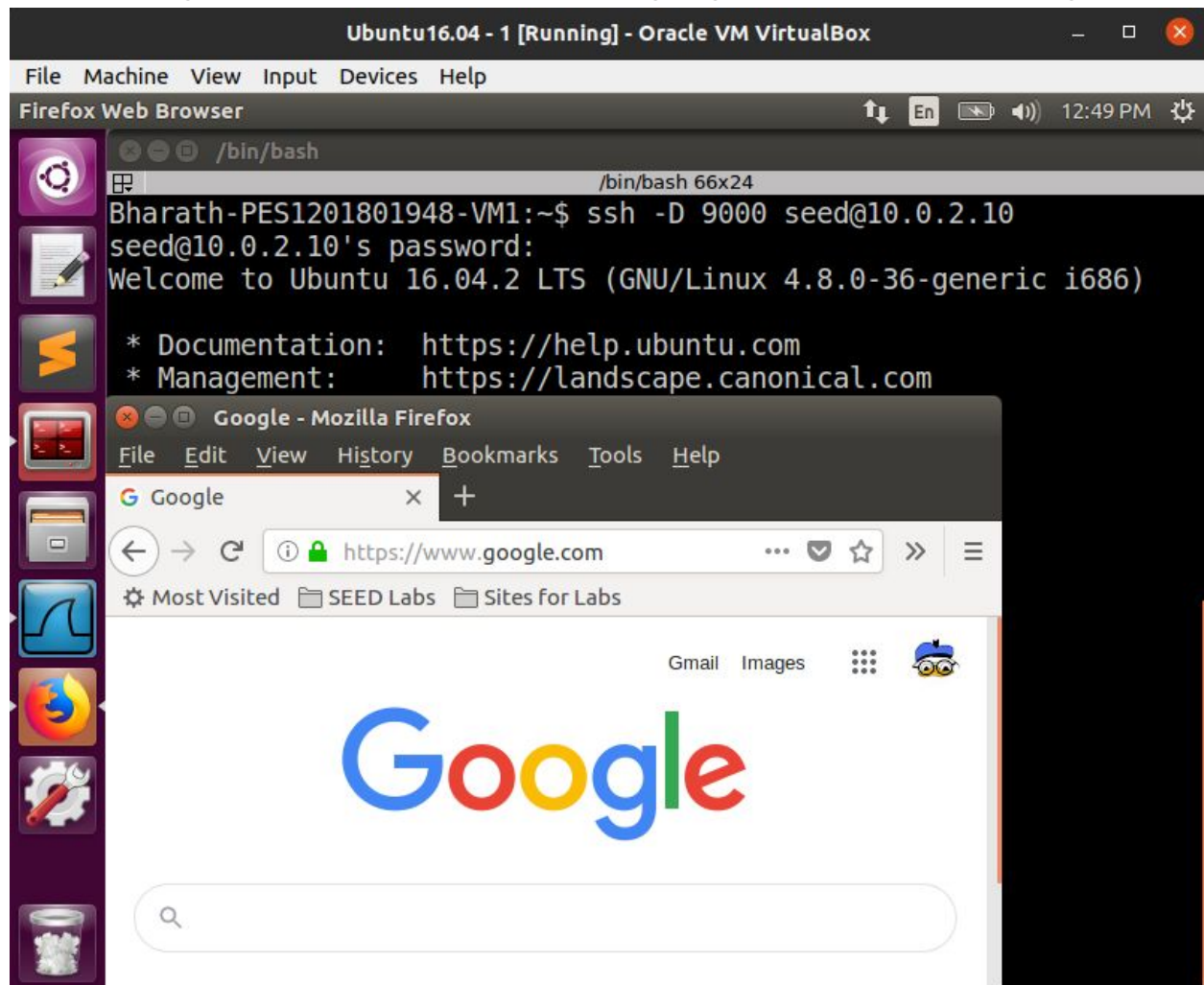


We can see that we could access google as well as the wireshark captures are shown

Closing the ssh tunnel, we can see that google.com cant be accessed



Re-enabling the tunnel, we can see that google can be accessed again.



Task 4: Evade Ingress Filtering

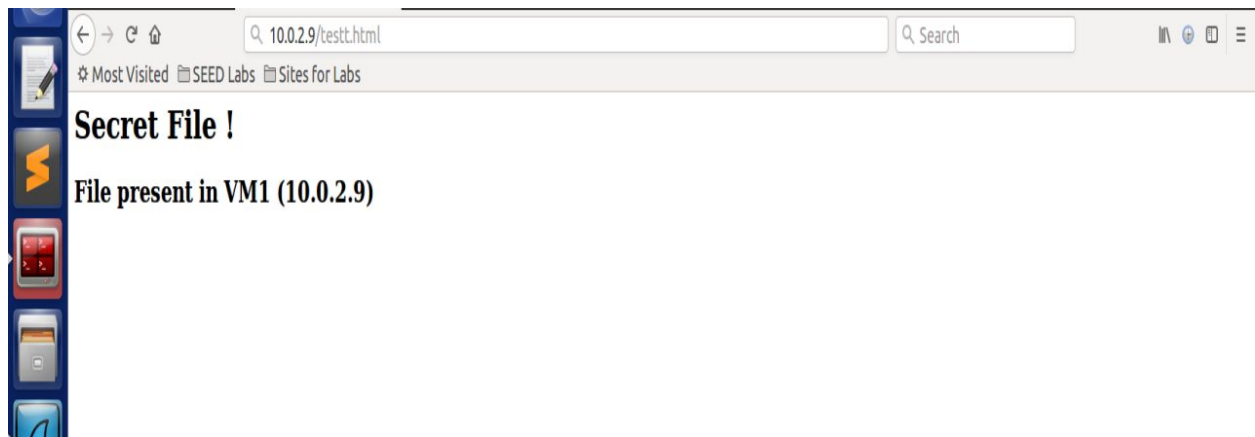
We can see that the test.html file can be accessed from VM2

```
Bharath-PES1201801948-VM1:~/html$ cat /var/www/html/test.html
<html>

<body>
<h1>Secret File ! </h1>

<h2>File present in VM1 (10.0.2.9) </h2>

</body>
</html>
Bharath-PES1201801948-VM1:~/html$
```

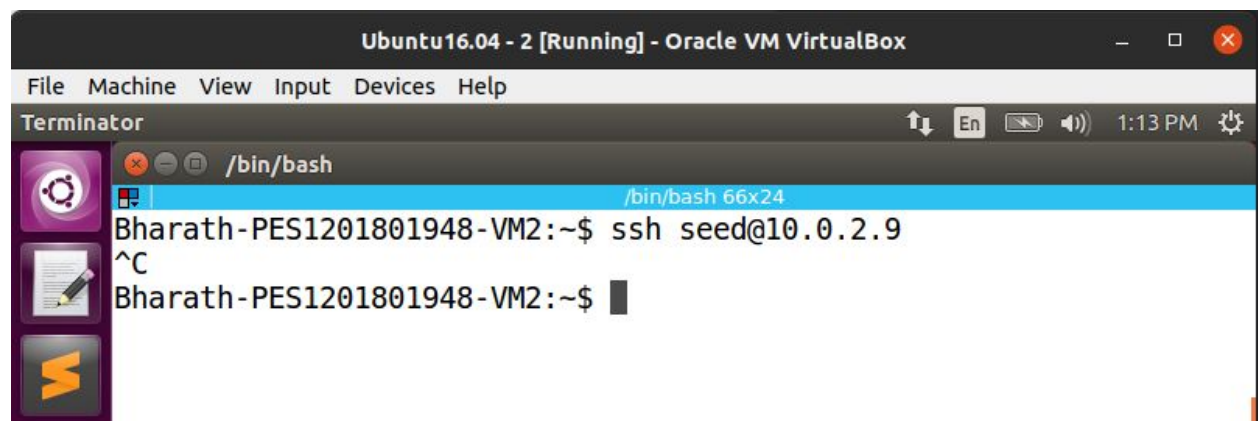


We then add firewall rules to deny incoming connections to VM1 on both port 80 and 22

```
Bharath-PES1201801948-VM1:~$ sudo ufw deny in from any to 10.0.2.9
port 80
Rule added
Bharath-PES1201801948-VM1:~$ sudo ufw deny in from any to 10.0.2.9
port 22
Rule added
Bharath-PES1201801948-VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
10.0.2.9 80 DENY IN Anywhere
10.0.2.9 22 DENY IN Anywhere

Bharath-PES1201801948-VM1:~$
```



Ssh into VM1 from VM2 fails

Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator

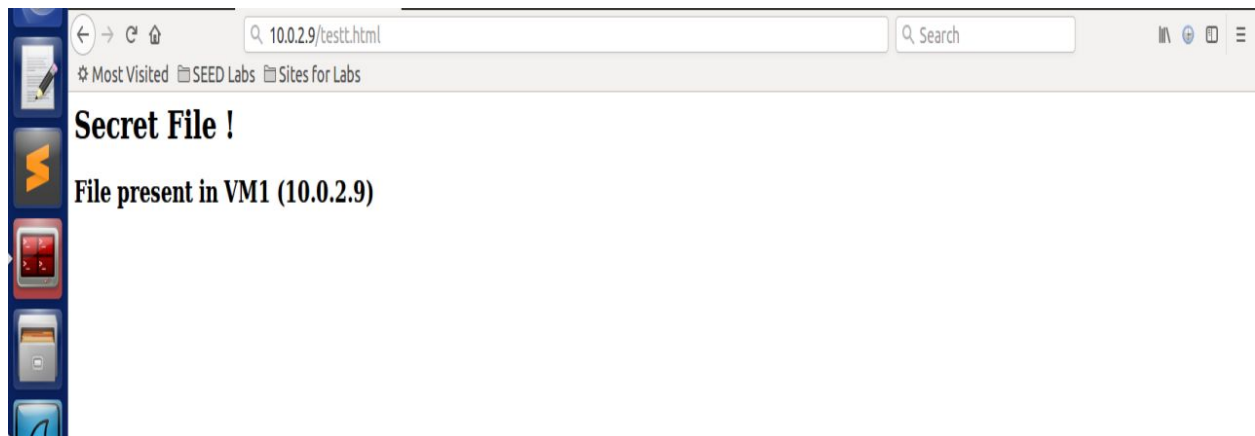
```
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM1:~$ ssh -R 9000:10.0.2.9:80 10.0.2.10
seed@10.0.2.10's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

0 packages can be updated.
0 updates are security updates.

Last login: Sun Feb 21 12:49:18 2021 from 10.0.2.9
Bharath-PES1201801948-VM2:~$
```

We setup a reverse ssh tunnel between the 2 machines, this helps evade the firewall rules and hence we can access the file on VM1



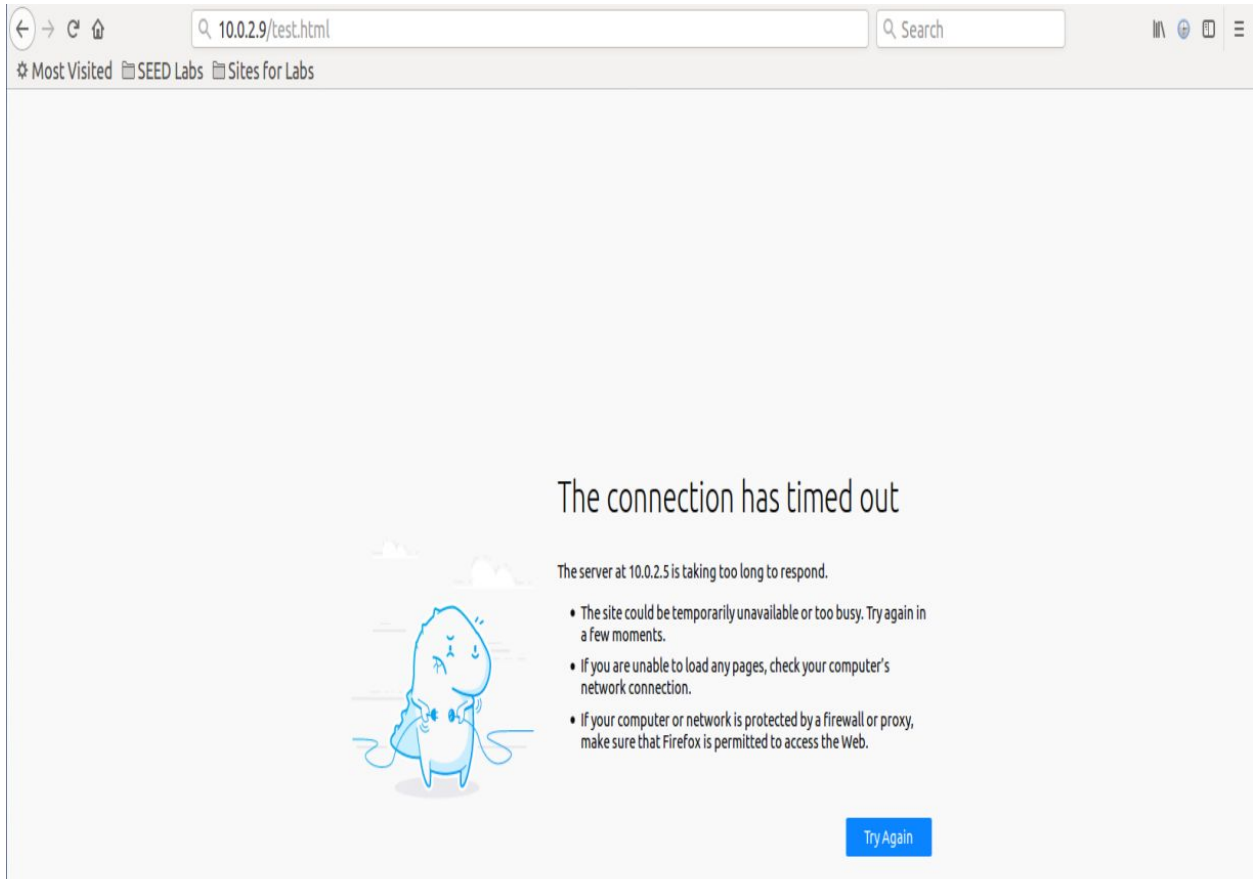
Closing the tunnel, we can see that the browser request fails as shown

Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator

```
/bin/bash
/bin/bash 66x24
Bharath-PES1201801948-VM2:~$
Bharath-PES1201801948-VM2:~$ exit
logout
Connection to 10.0.2.10 closed.
Bharath-PES1201801948-VM1:~$
```



Therefore, we need the reverse ssh tunnel to access the files on the webserver.