

CNS LAB

LAB - 4

Linux Firewall Exploration Lab

NAME : SIRI S

SEMESTER : 5

SECTION :H

SRN : PES1UG19CS485

Lab Setup:

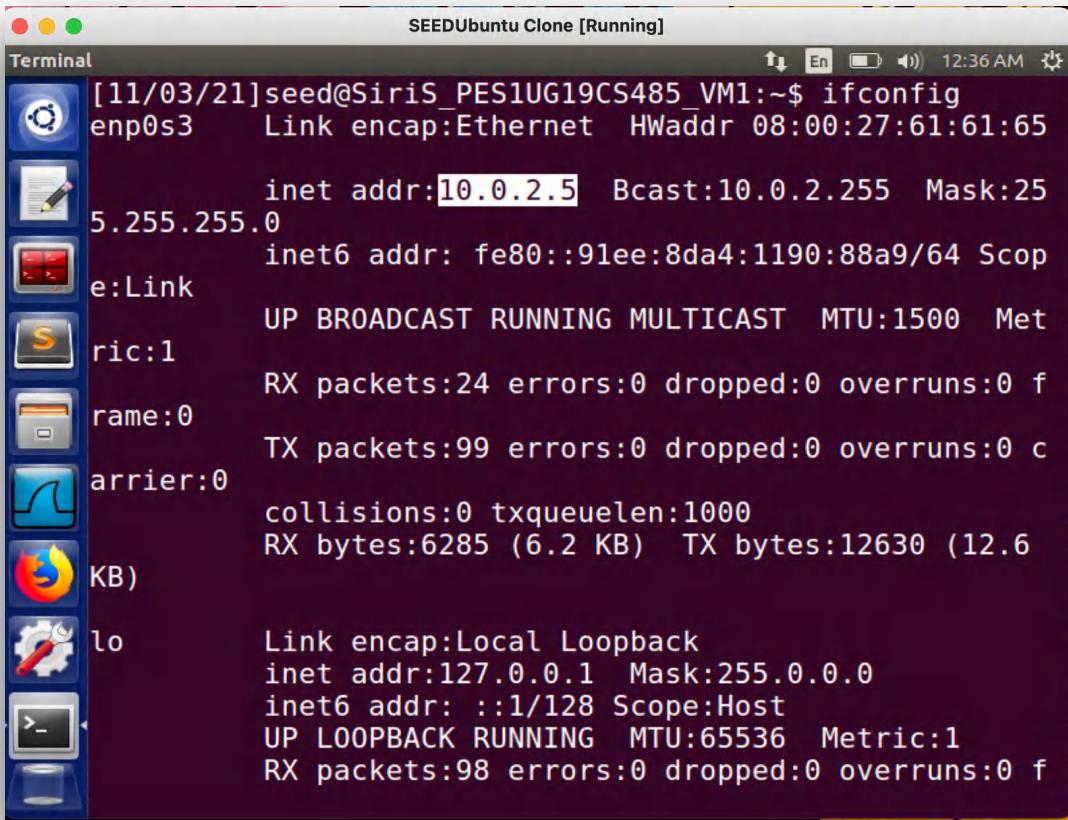
VM 2: 10.0.2.4

VM 1: 10.0.2.5

VM 3: 10.0.2.6

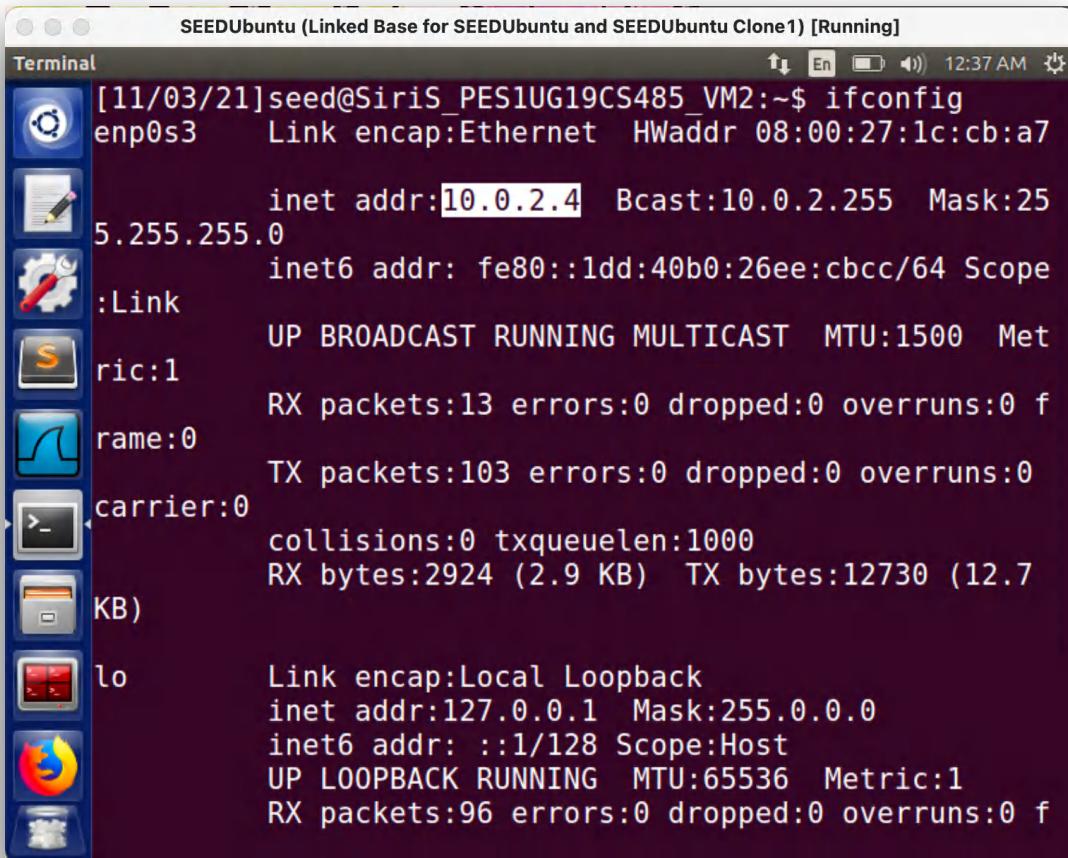
IP Addresses

VM 1:



```
SEEDUbuntu Clone [Running]
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:61:61:65
              inet addr:10.0.2.5    Bcast:10.0.2.255  Mask:25
              5.255.255.0
              inet6 addr: fe80::91ee:8da4:1190:88a9/64 Scope
e:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Met
ric:1
              RX packets:24 errors:0 dropped:0 overruns:0 f
rame:0
              TX packets:99 errors:0 dropped:0 overruns:0 c
arrier:0
              collisions:0 txqueuelen:1000
              RX bytes:6285 (6.2 KB)   TX bytes:12630 (12.6
KB)
lo          Link encap:Local Loopback
              inet addr:127.0.0.1  Mask:255.0.0.0
              inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING  MTU:65536 Metric:1
              RX packets:98 errors:0 dropped:0 overruns:0 f
```

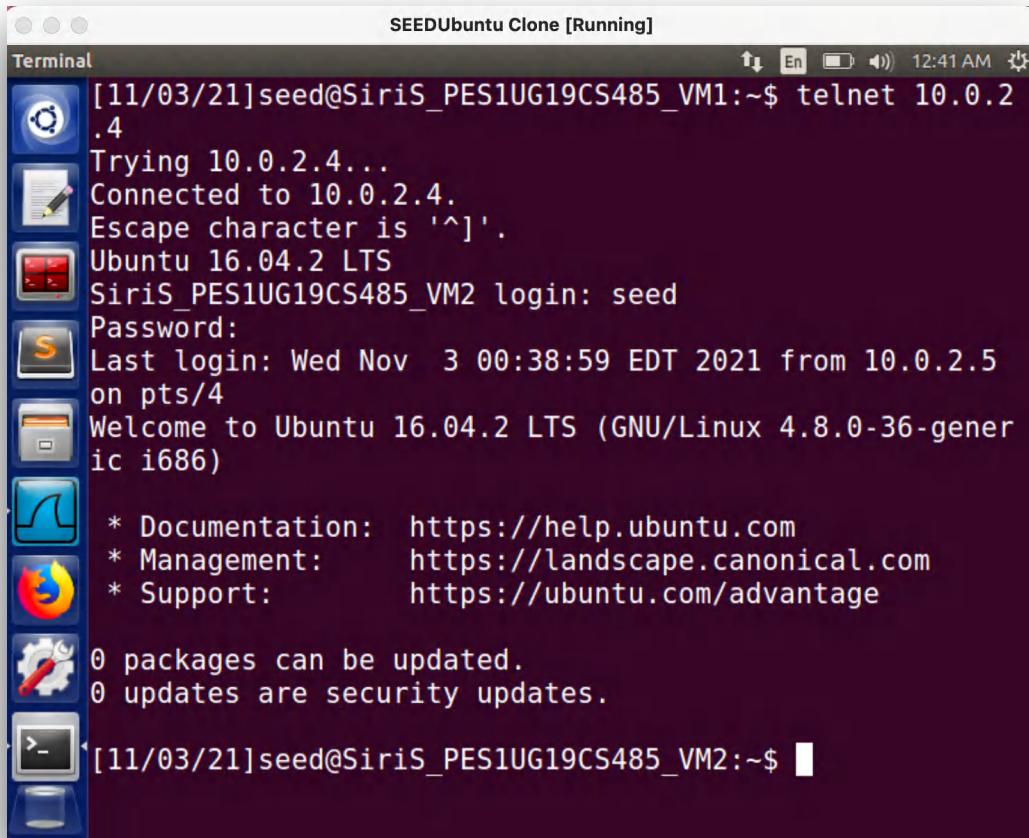
VM 2:



```
SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:1c:cb:a7
              inet addr:10.0.2.4    Bcast:10.0.2.255  Mask:25
              5.255.255.0
              inet6 addr: fe80::1dd:40b0:26ee:cbcc/64 Scope
:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Met
ric:1
              RX packets:13 errors:0 dropped:0 overruns:0 f
rame:0
              TX packets:103 errors:0 dropped:0 overruns:0 c
arrier:0
              collisions:0 txqueuelen:1000
              RX bytes:2924 (2.9 KB)   TX bytes:12730 (12.7
KB)
lo          Link encap:Local Loopback
              inet addr:127.0.0.1  Mask:255.0.0.0
              inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING  MTU:65536 Metric:1
              RX packets:96 errors:0 dropped:0 overruns:0 f
```

Task 1: Using Firewall

To show that we are able to establish a telnet connection from VM 1 to VM 2:



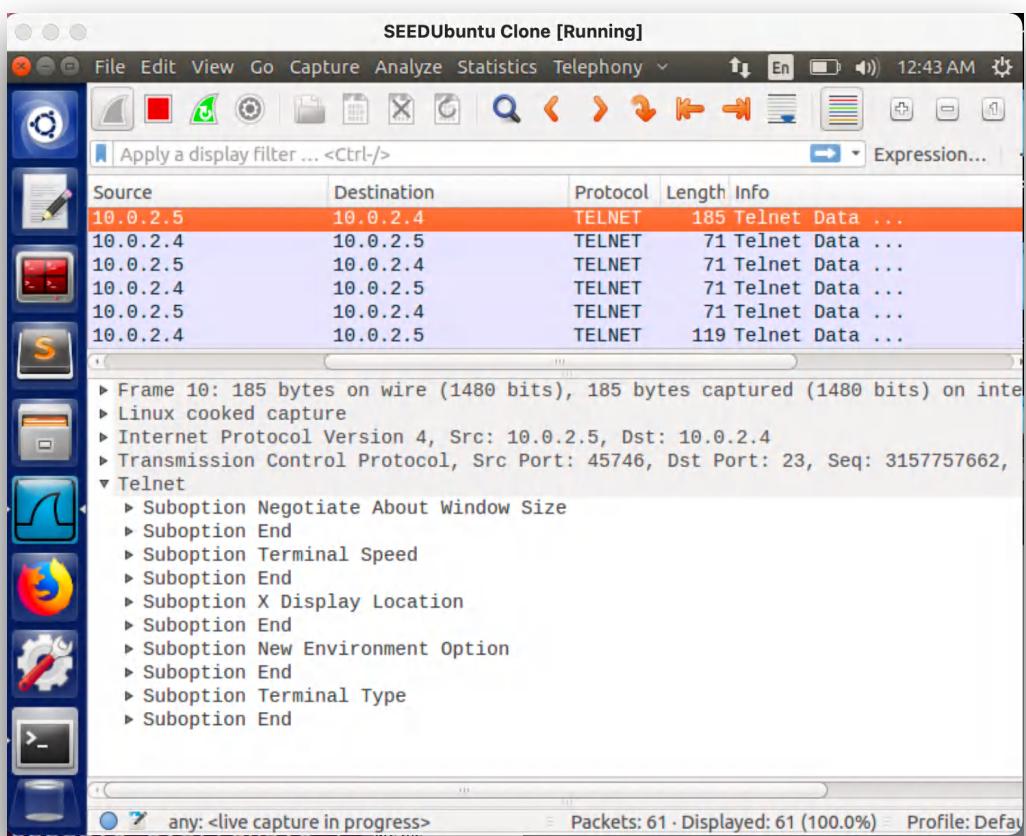
```
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
SiriS_PES1UG19CS485_VM2 login: seed
Password:
Last login: Wed Nov  3 00:38:59 EDT 2021 from 10.0.2.5
on pts/4
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

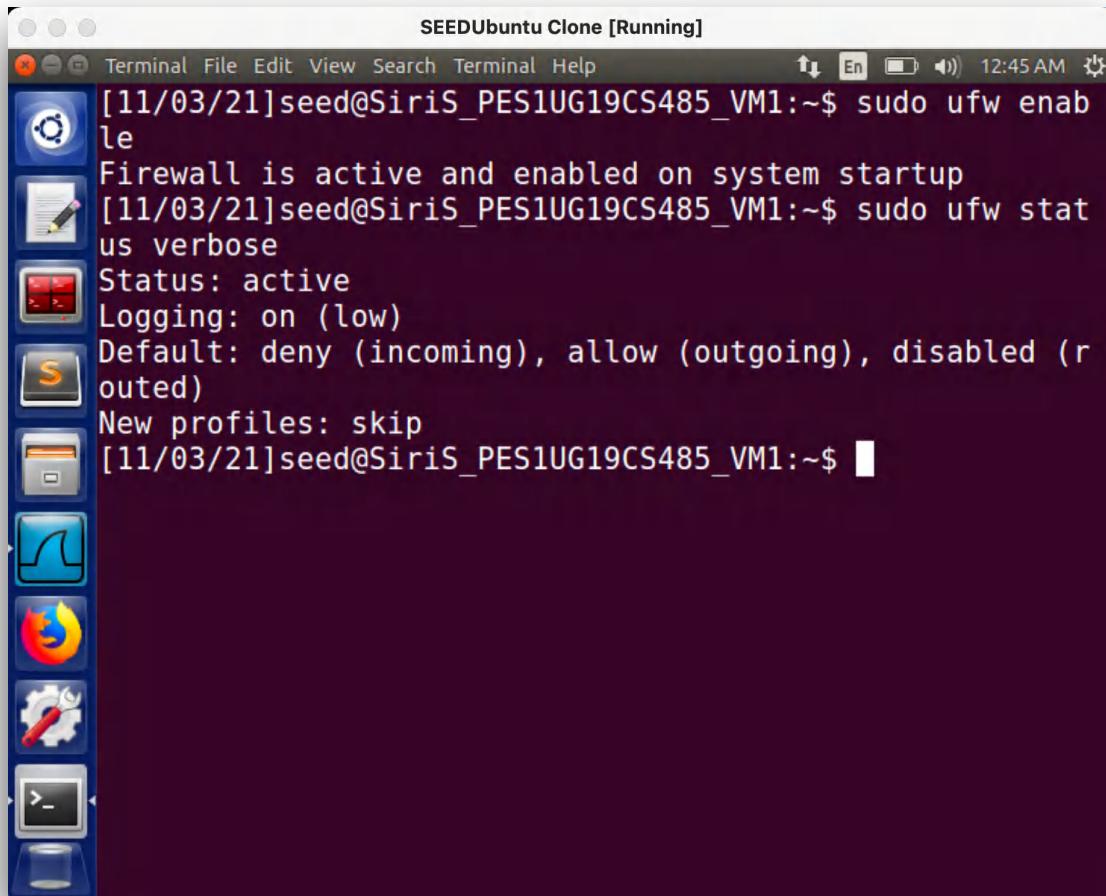
0 packages can be updated.
0 updates are security updates.

[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~$
```

Wireshark screenshot:

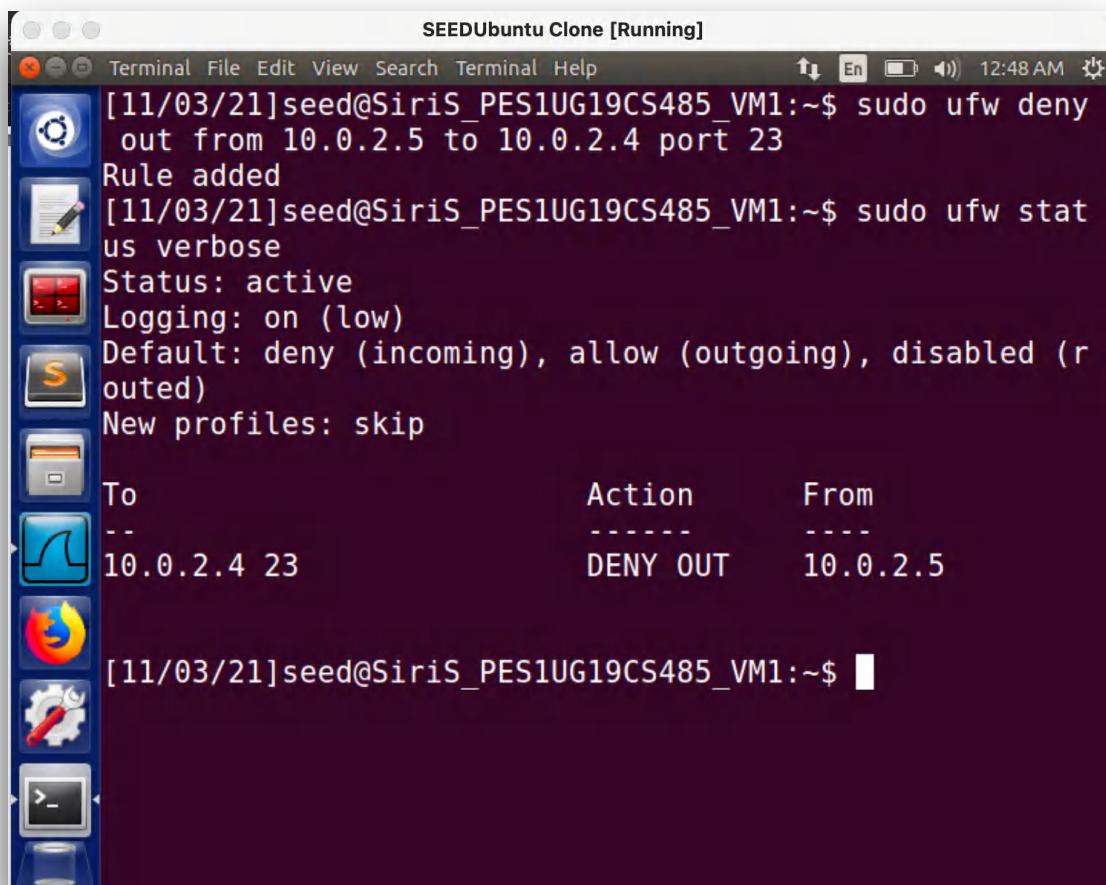


Configuring a firewall using *ufw* to prevent VM1 from being able to telnet to VM2:



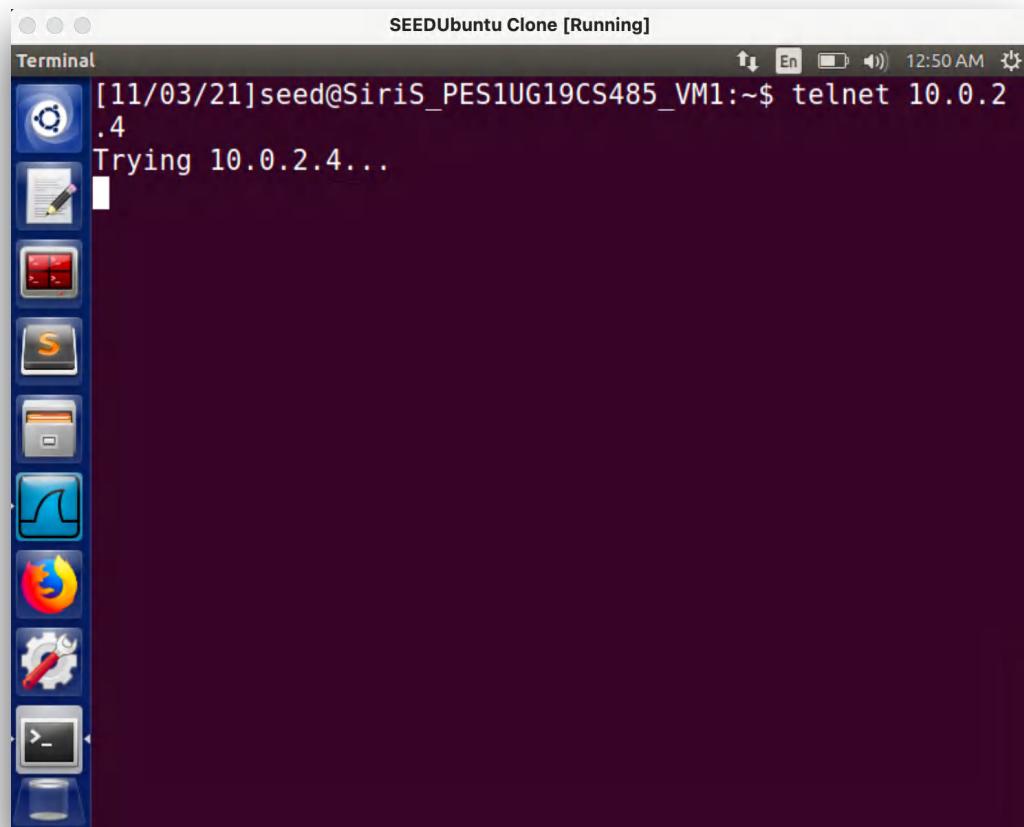
```
SEEDUbuntu Clone [Running]
Terminal File Edit View Search Terminal Help 12:45 AM
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw enable
Firewall is active and enabled on system startup
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$
```

Configuring a firewall on VM1 to deny telnet (port 23) to VM2:

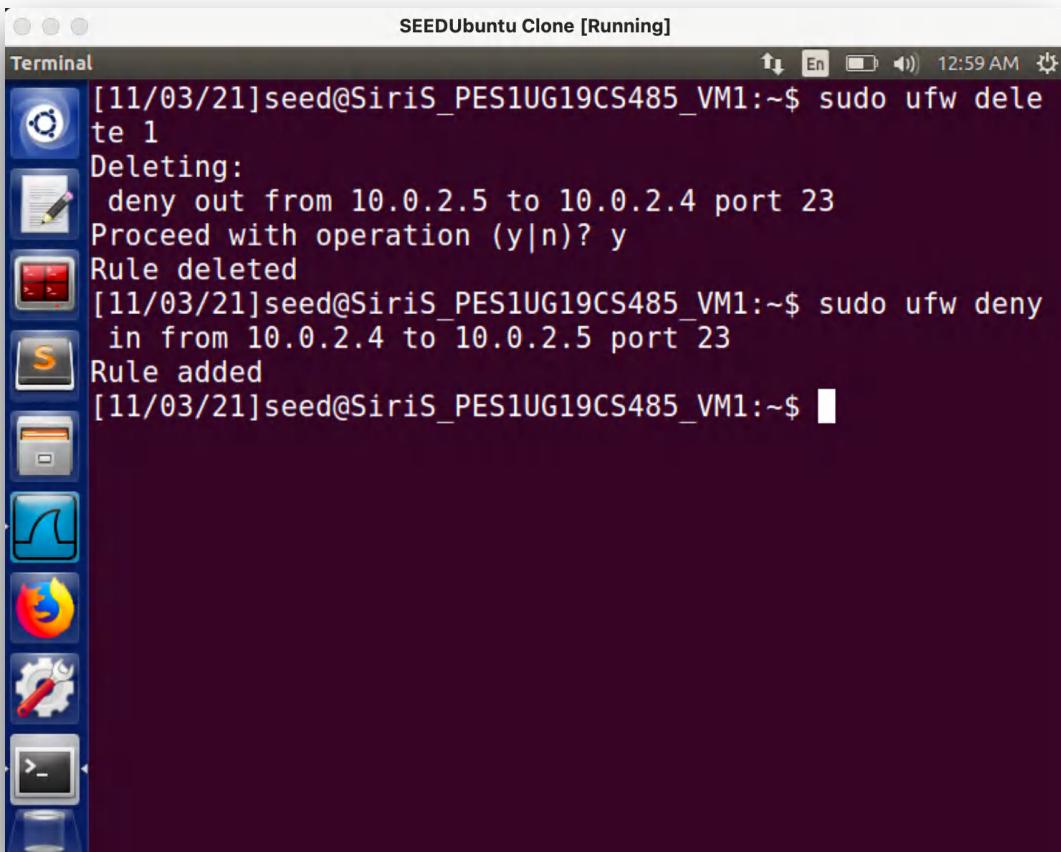


```
SEEDUbuntu Clone [Running]
Terminal File Edit View Search Terminal Help 12:48 AM
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw deny out from 10.0.2.5 to 10.0.2.4 port 23
Rule added
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To          Action    From
--          -----   ---
10.0.2.4 23  DENY OUT  10.0.2.5
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$
```

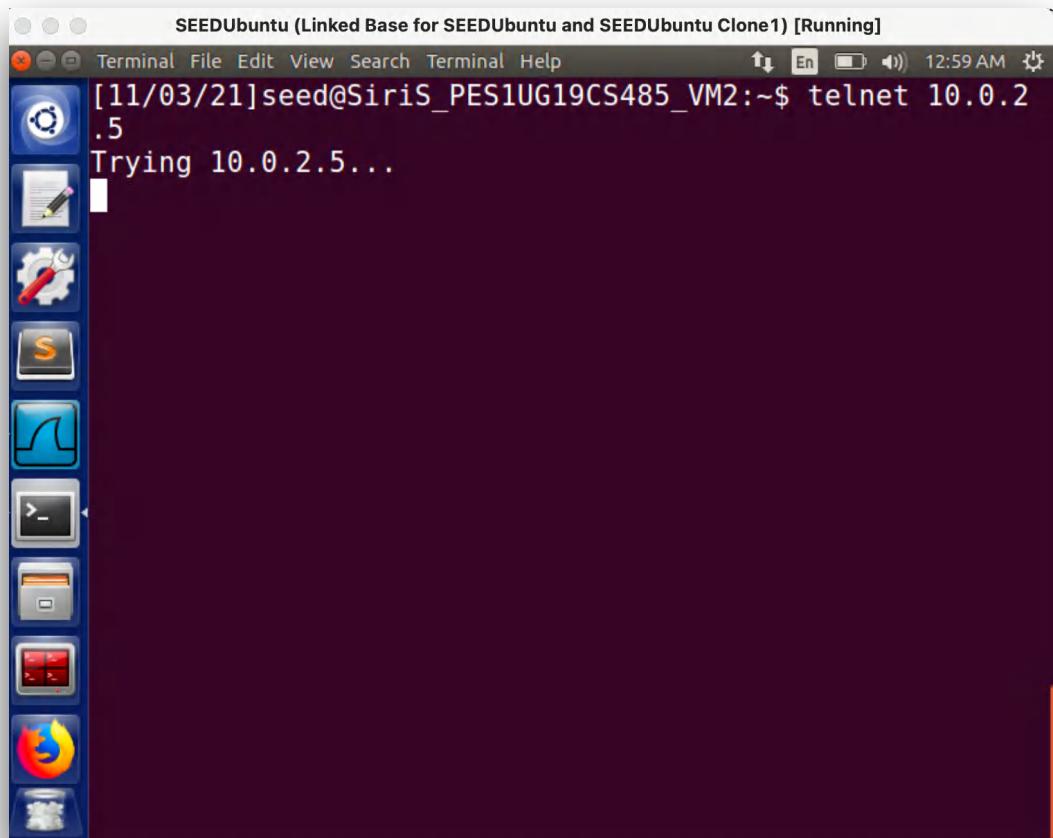
To show that because of the firewall that's enabled, telnet is denied from VM1 to VM2:



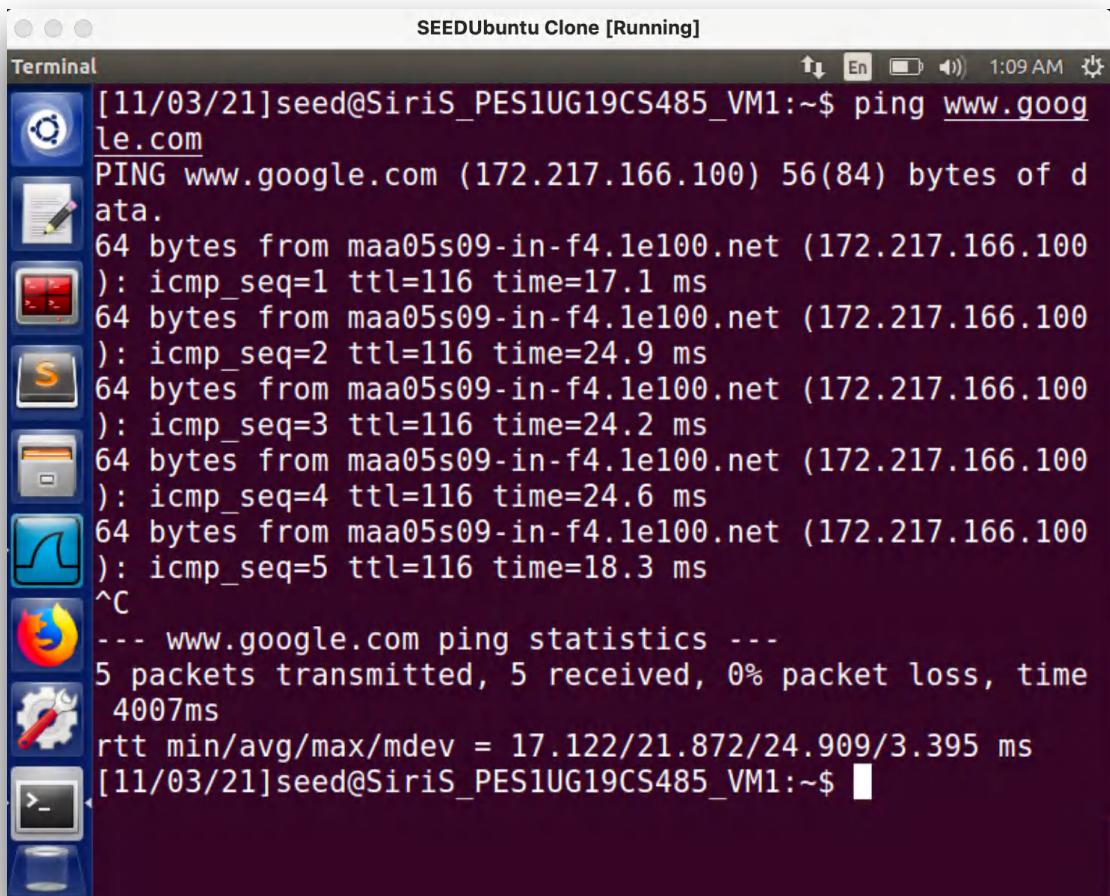
We next delete the firewall rule in VM1. We add a rule to prevent VM2 from being able to do telnet to VM1:



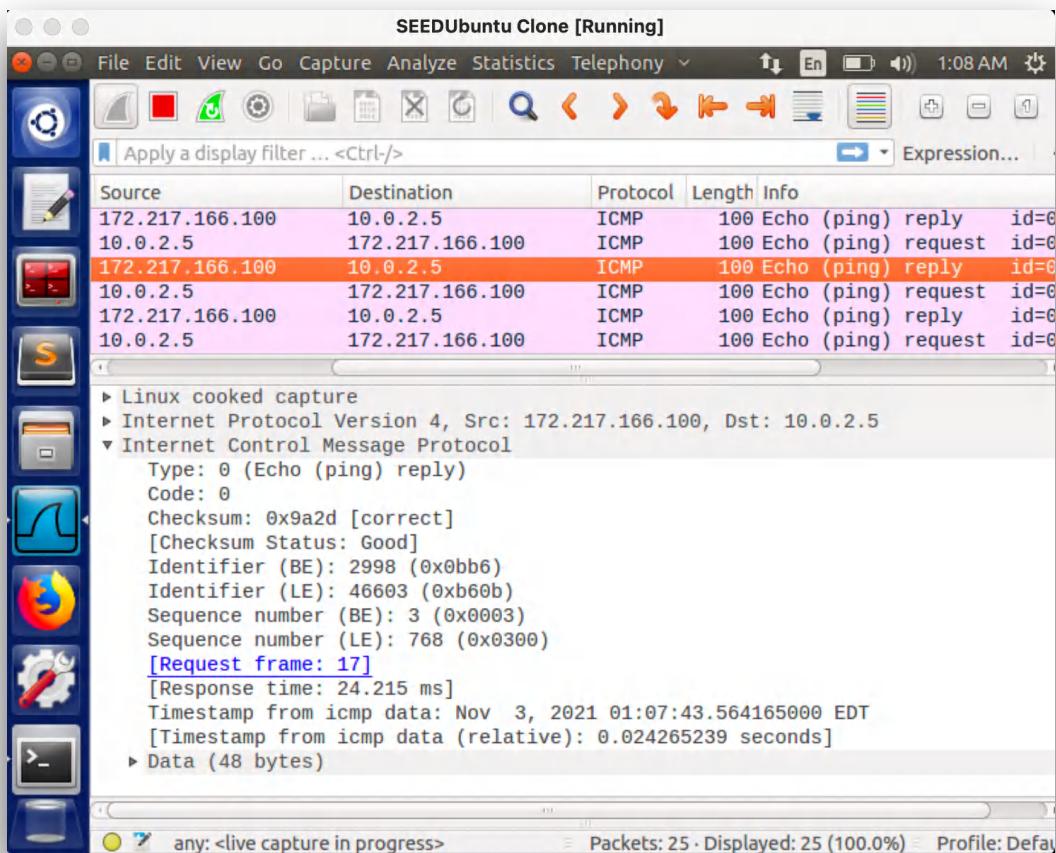
Now, telnet is blocked from VM2 to VM1:



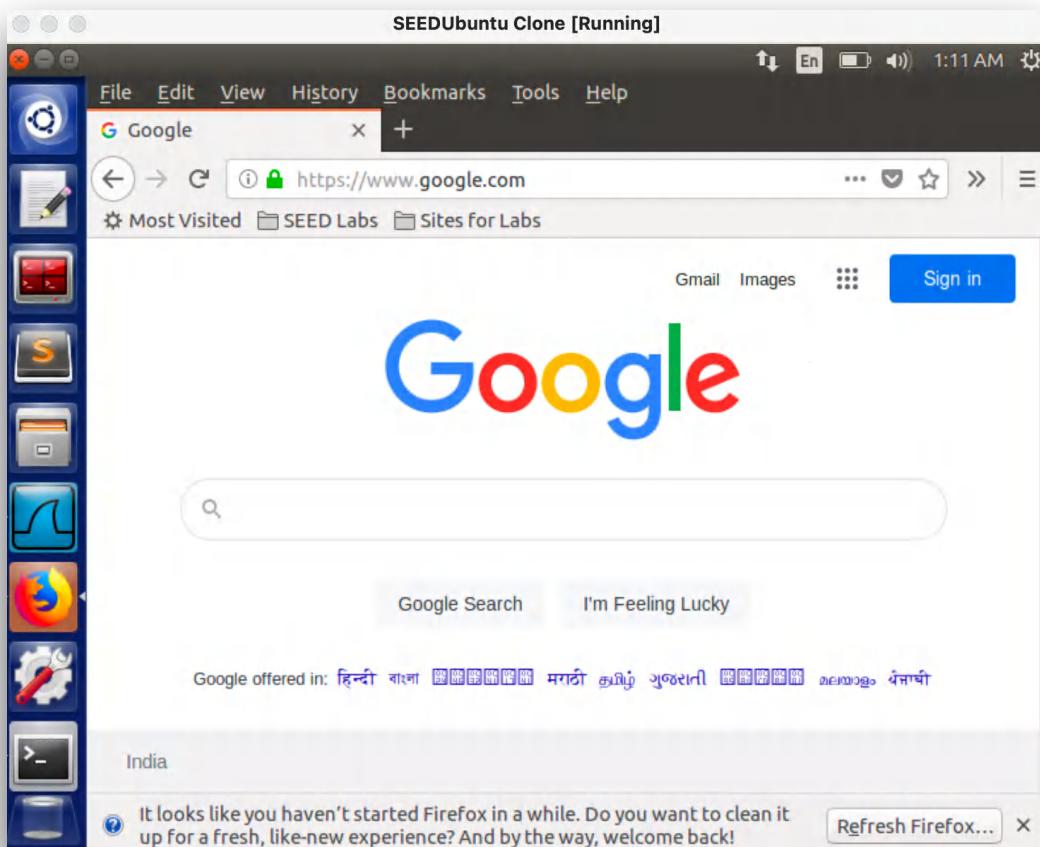
We next need to block VM1 from visiting a website. ‘www.google.com’:



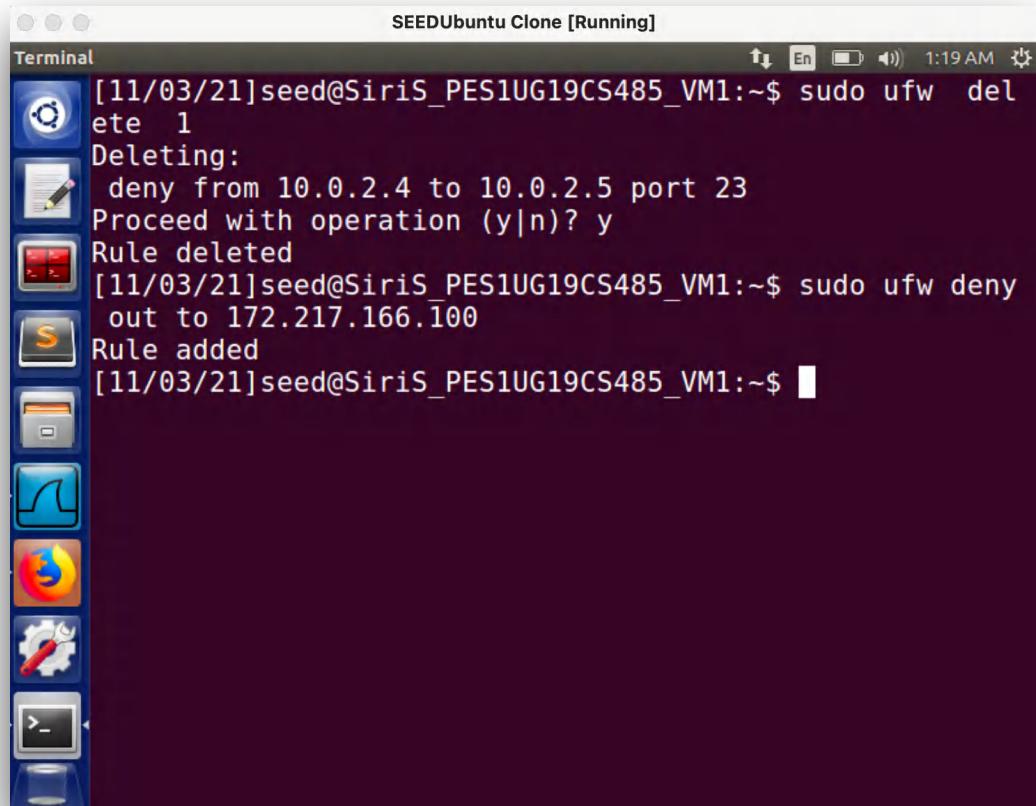
Wireshark screenshot:



Testing whether the website is accessible to the browser:



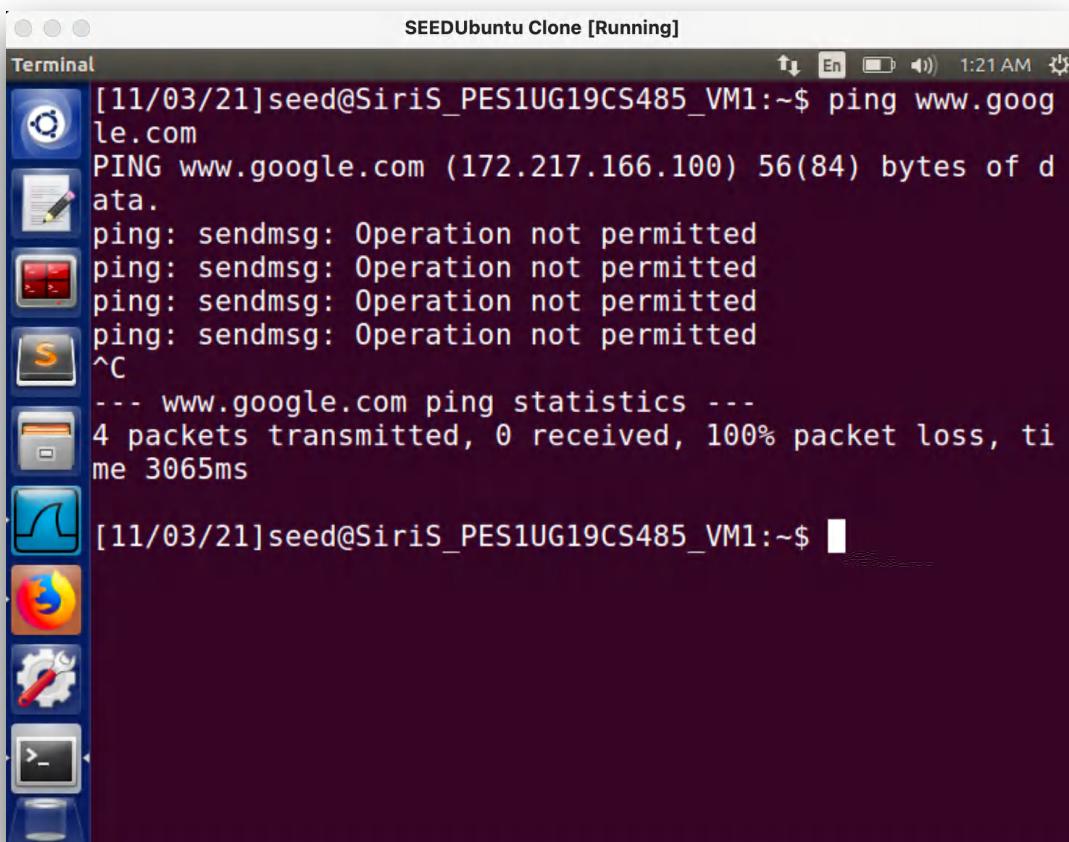
We then clear the browser cache by deleting Cache from the browser history. We next add the firewall rule to prevent VM1 from accessing the IP address for **www.google.com** (172.217.166.100)



The screenshot shows a terminal window titled "SEEDUbuntu Clone [Running]". The terminal contains the following command history:

```
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw delete 1
Deleting:
  deny from 10.0.2.4 to 10.0.2.5 port 23
Proceed with operation (y|n)? y
Rule deleted
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw deny out to 172.217.166.100
Rule added
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$
```

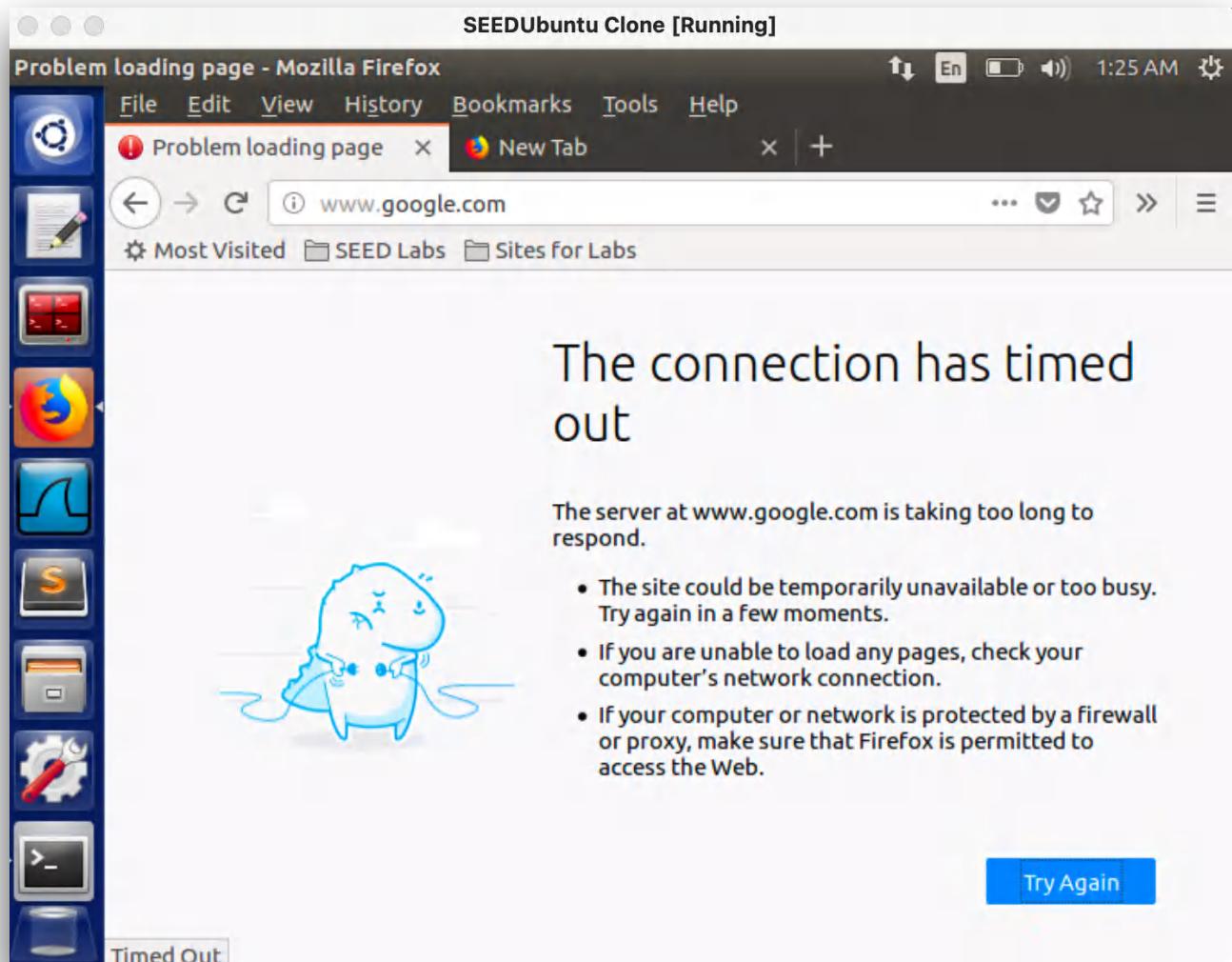
To show that firewall has blocked www.google.com:



The screenshot shows a terminal window titled "SEEDUbuntu Clone [Running]". The terminal contains the following command history:

```
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ ping www.google.com
PING www.google.com (172.217.166.100) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
^C
--- www.google.com ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3065ms
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$
```

This can be verified by revisiting www.google.com in the Firefox browser. The page is not loaded.

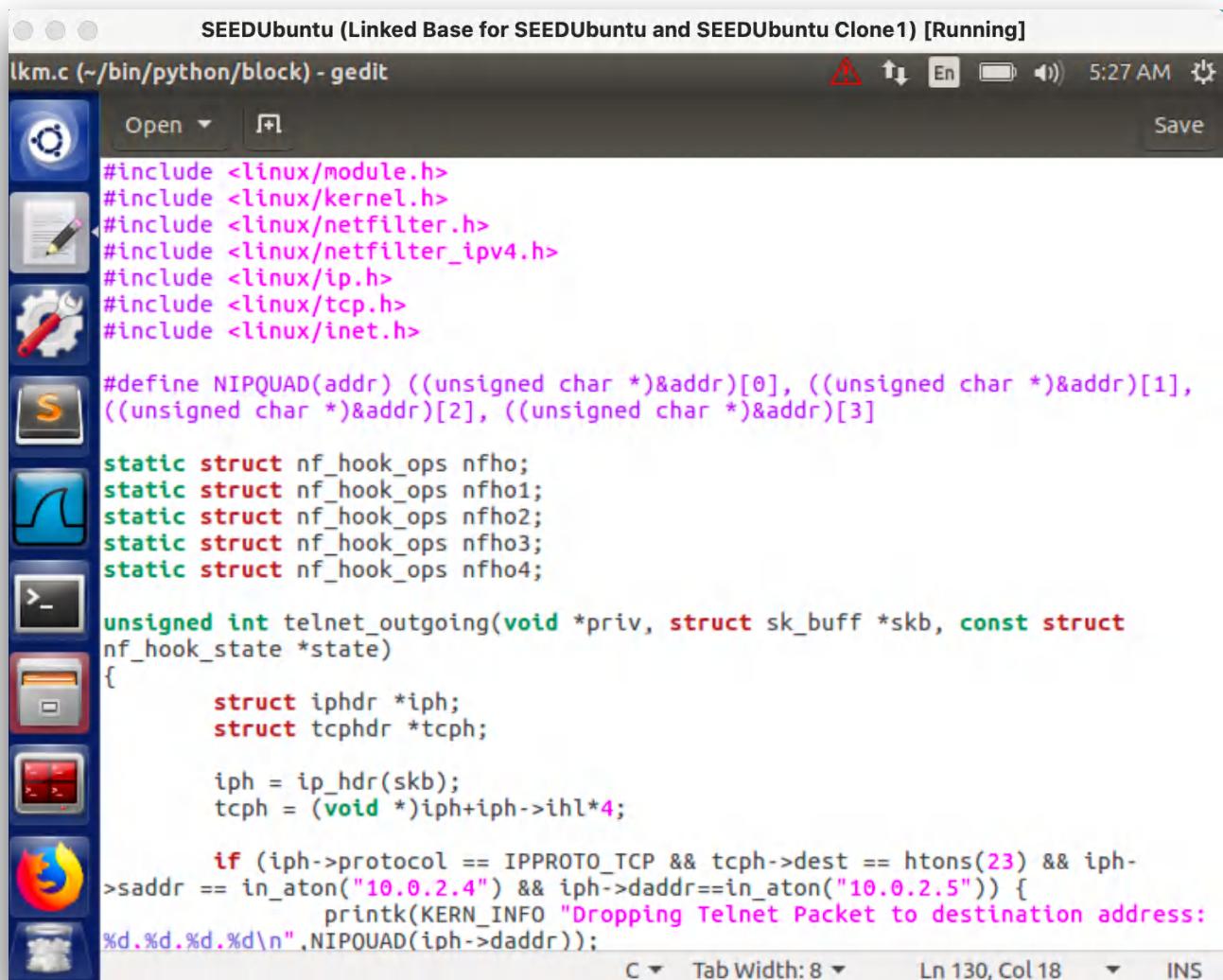


Task 2: How Firewall Works

In this task, we will develop a firewall using netfilter and LKM. We implement five rules in this firewall:

- Block telnet from VM1 to VM2
- Block telnet from VM2 to VM1
- Block external website access from VM1
- Block ssh from VM1 to VM2
- Block ssh from VM2 to VM1

Code for the firewall:



```
SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
lkm.c (~/bin/python/block) - gedit
Open ▾ Save
#include <linux/module.h>
#include <linux/kernel.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>
#include <linux/ip.h>
#include <linux/tcp.h>
#include <linux/inet.h>

#define NIPQUAD(addr) ((unsigned char *)&addr)[0], ((unsigned char *)&addr)[1],
((unsigned char *)&addr)[2], ((unsigned char *)&addr)[3]

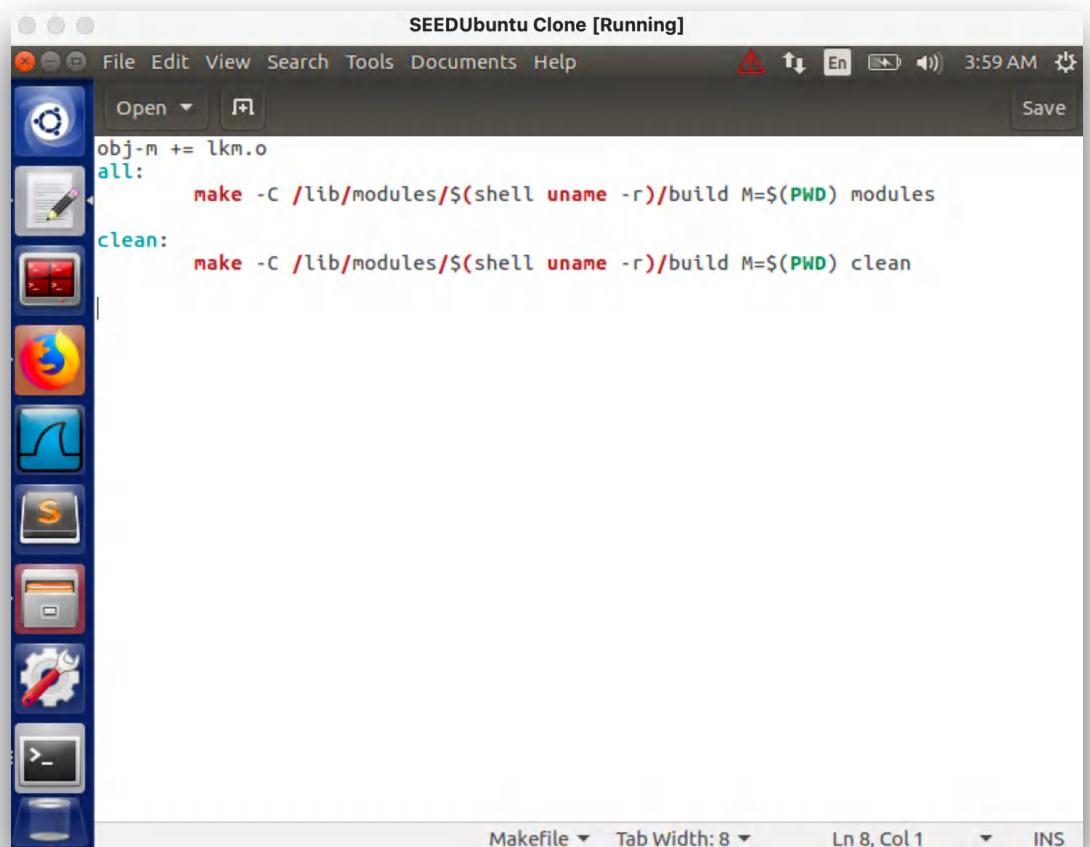
static struct nf_hook_ops nfho;
static struct nf_hook_ops nfho1;
static struct nf_hook_ops nfho2;
static struct nf_hook_ops nfho3;
static struct nf_hook_ops nfho4;

unsigned int telnet_outgoing(void *priv, struct sk_buff *skb, const struct
nf_hook_state *state)
{
    struct iphdr *iph;
    struct tcphdr *tcpiph;

    iph = ip_hdr(skb);
    tcpiph = (void *)iph+iph->ihl*4;

    if (iph->protocol == IPPROTO_TCP && tcpiph->dest == htons(23) && iph-
>saddr == in_aton("10.0.2.4") && iph->daddr==in_aton("10.0.2.5")) {
        printk(KERN_INFO "Dropping Telnet Packet to destination address:
%d.%d.%d.%d\n",NIPQUAD(iph->daddr));
    }
}
```

Makefile used:

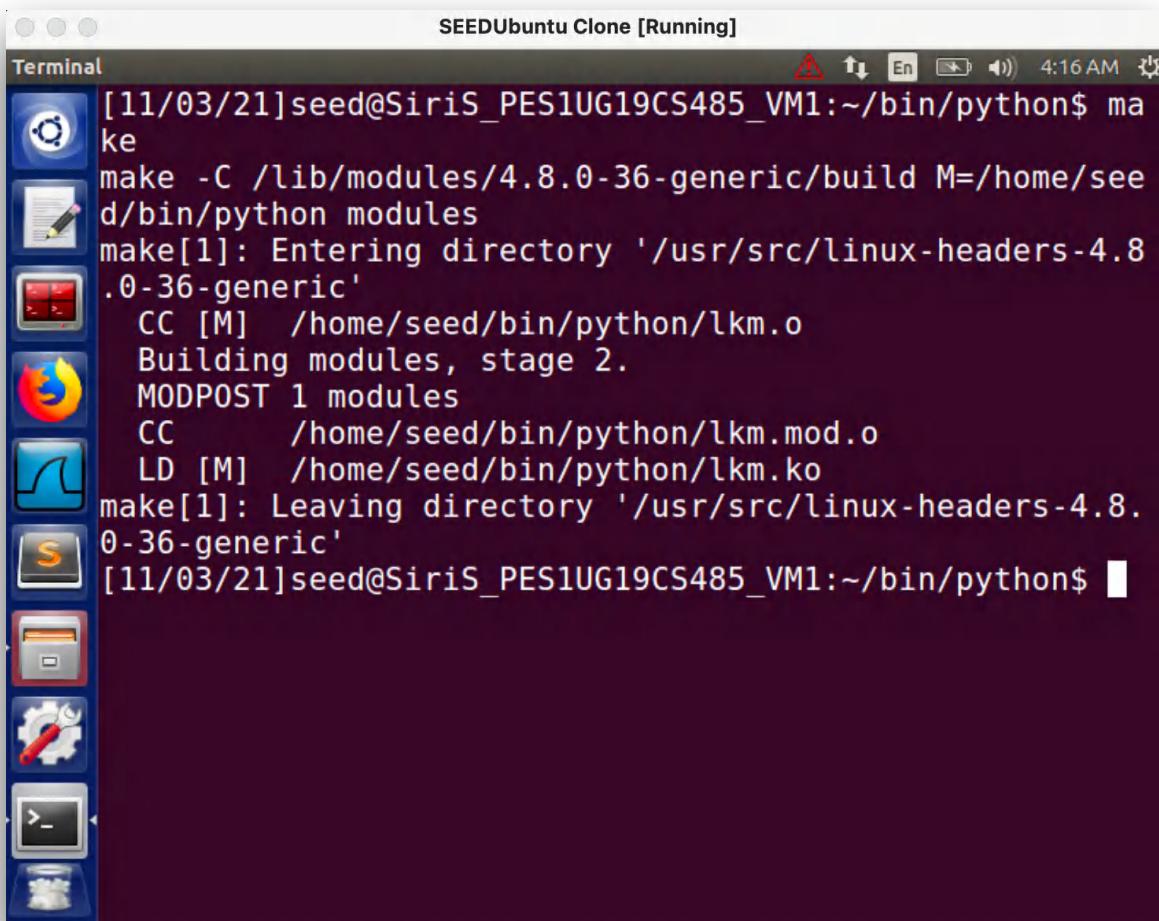


The screenshot shows a desktop environment with a dock on the left containing icons for various applications like a terminal, file manager, and system tools. A window titled "SEEDUbuntu Clone [Running]" is open, displaying a Makefile. The Makefile contains the following content:

```
obj-m += lkm.o
all:
    make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules
clean:
    make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean
```

The window has a standard Linux-style title bar with "File", "Edit", "View", "Search", "Tools", "Documents", and "Help" menus. There are also standard window control buttons (minimize, maximize, close) at the top. The status bar at the bottom shows "Makefile", "Tab Width: 8", "Ln 8, Col 1", and "INS".

Upon running these two files:

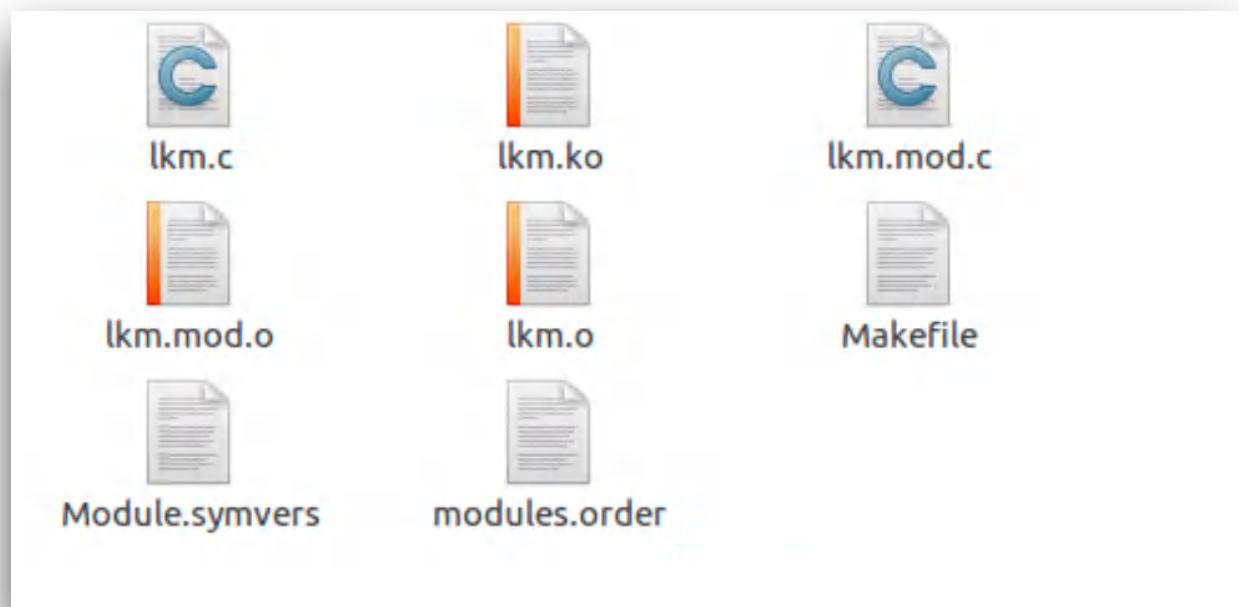


The screenshot shows a terminal window titled "SEEDUbuntu Clone [Running]". The terminal output is as follows:

```
[11/03/21]seed@Siris_PES1UG19CS485_VM1:~/bin/python$ make
make -C /lib/modules/4.8.0-36-generic/build M=/home/seed/bin/python modules
make[1]: Entering directory '/usr/src/linux-headers-4.8.0-36-generic'
CC [M] /home/seed/bin/python/lkm.o
Building modules, stage 2.
MODPOST 1 modules
CC      /home/seed/bin/python/lkm.mod.o
LD [M] /home/seed/bin/python/lkm.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.8.0-36-generic'
[11/03/21]seed@Siris_PES1UG19CS485_VM1:~/bin/python$
```

The terminal window has a dark background and a light-colored font. It includes standard Linux terminal controls like arrows for navigating history and a clear button.

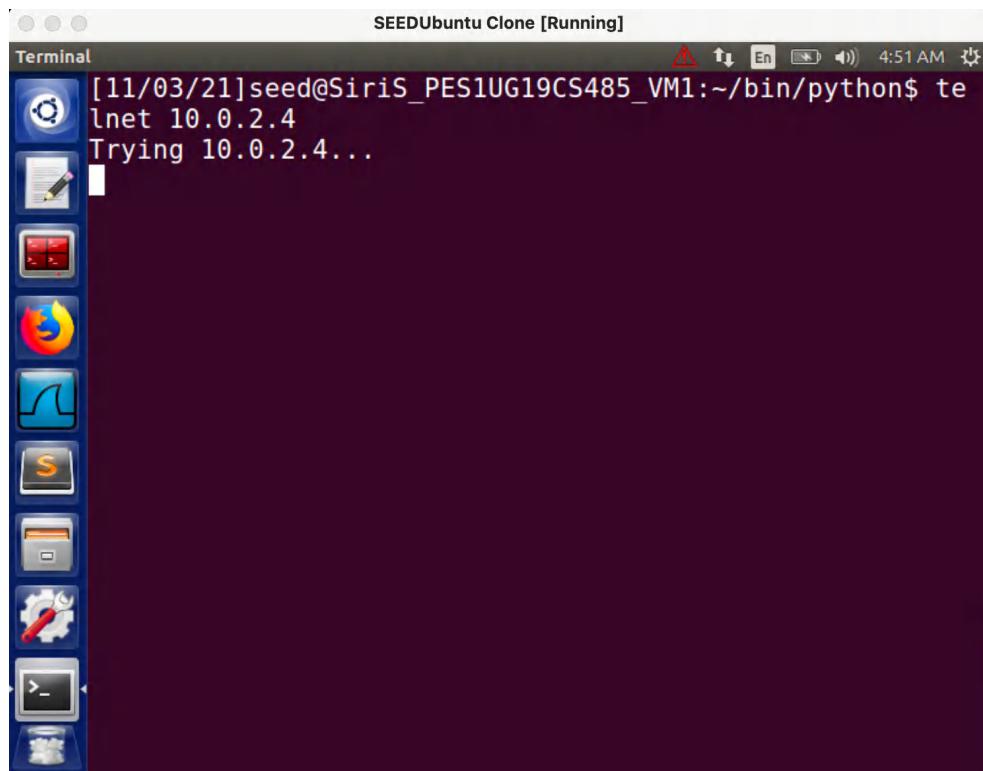
On running make command, all the different files get created and is stored in the same directory.



Now we need to insert the kernel module (task2.ko) using insmod :

```
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~/bin/python$ su
do dmesg --clear
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~/bin/python$ su
do insmod lkm.ko
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~/bin/python$ ls
mod | grep lkm
lkm          16384  0
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~/bin/python$
```

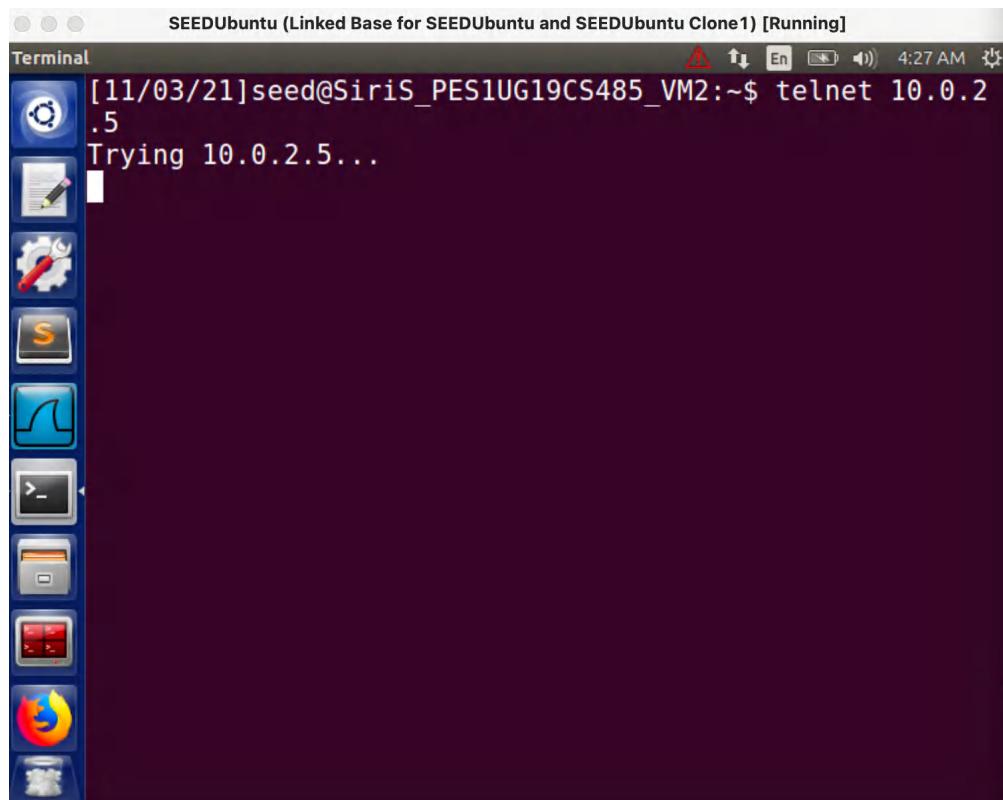
Step 1: Testing whether telnet from VM1 to VM2 is blocked



The screenshot shows a terminal window titled "SEEDUbuntu Clone [Running]". The command entered is "telnet 10.0.2.4". The output shows "Trying 10.0.2.4...". The desktop environment includes a vertical dock on the left with icons for Terminal, Nautilus, Dash, System Settings, and a terminal icon.

```
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~/bin/python$ telnet 10.0.2.4
Trying 10.0.2.4...
```

Step 2: Testing whether telnet from VM2 to VM1 is blocked

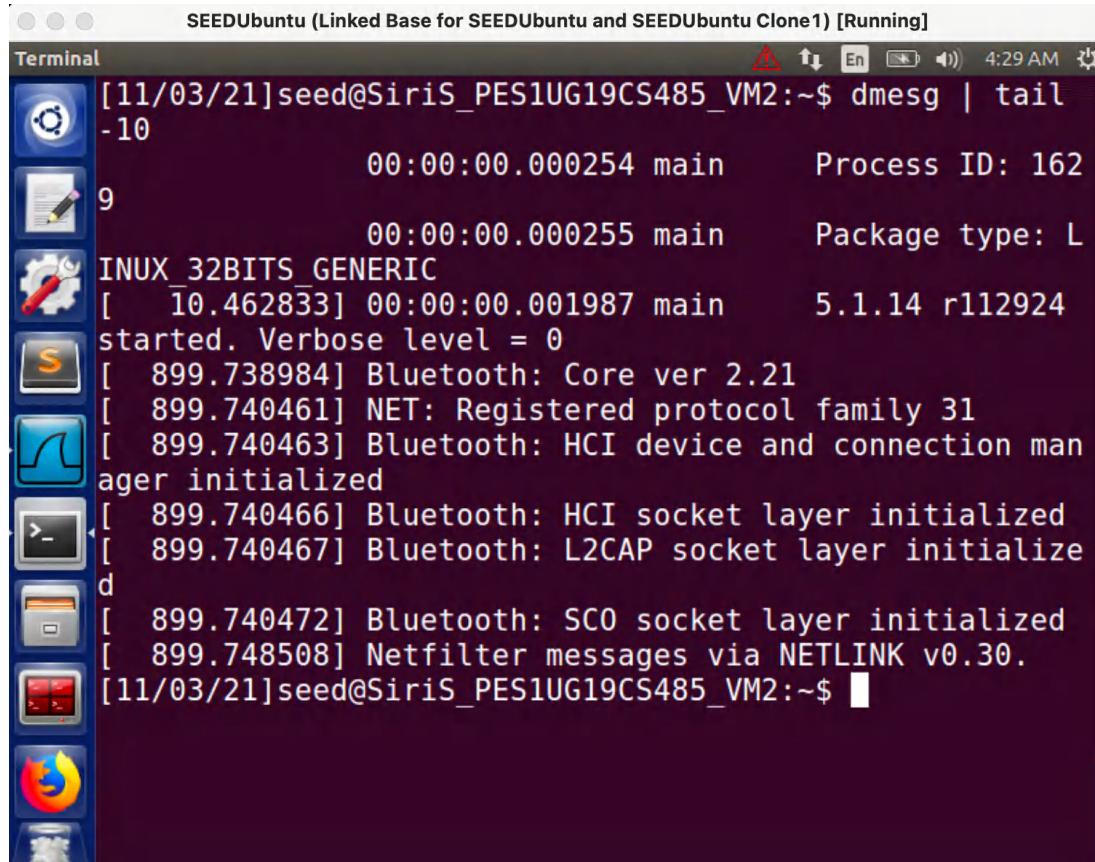


The screenshot shows a terminal window titled "SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]". The command entered is "telnet 10.0.2.5". The output shows "Trying 10.0.2.5...". The desktop environment includes a vertical dock on the left with icons for Terminal, Nautilus, Dash, System Settings, and a terminal icon.

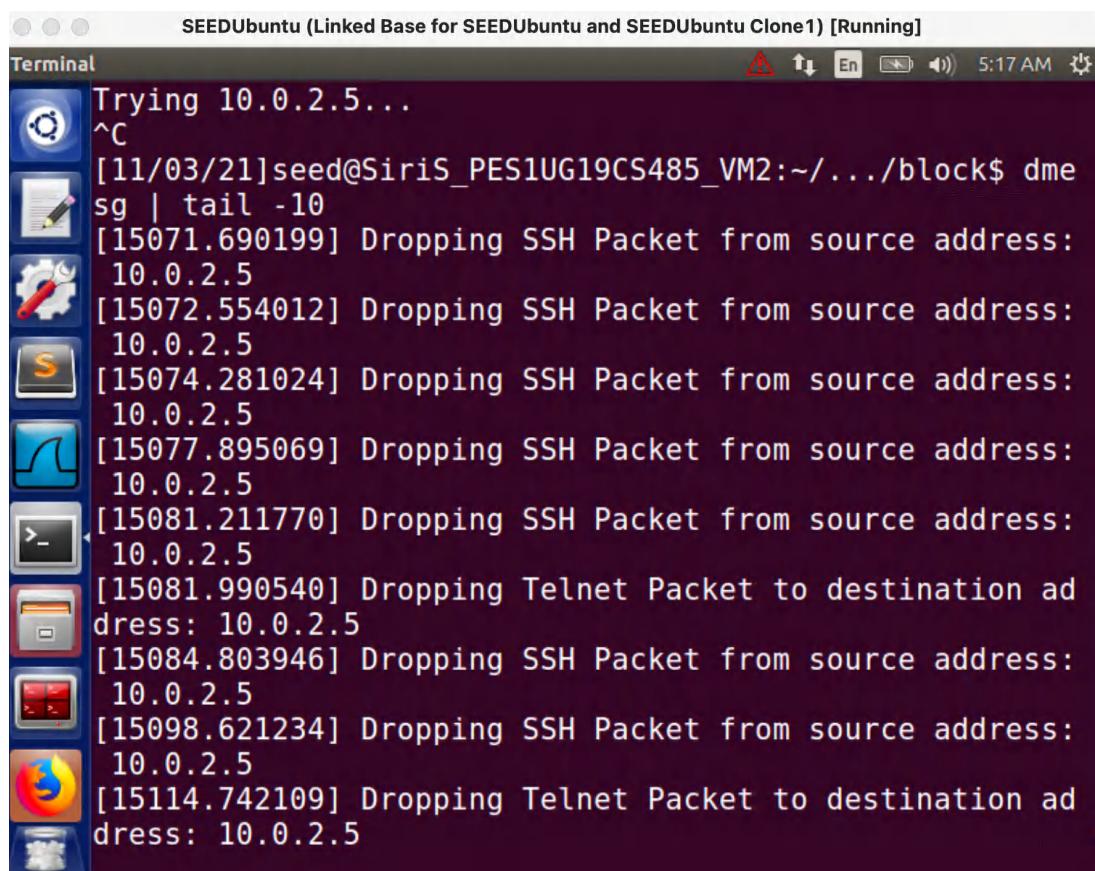
```
[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~$ telnet 10.0.2.5
Trying 10.0.2.5...
```

We can see that telnet is blocked from both ways.

Command that is used to show the dropping of packets because of the firewall:



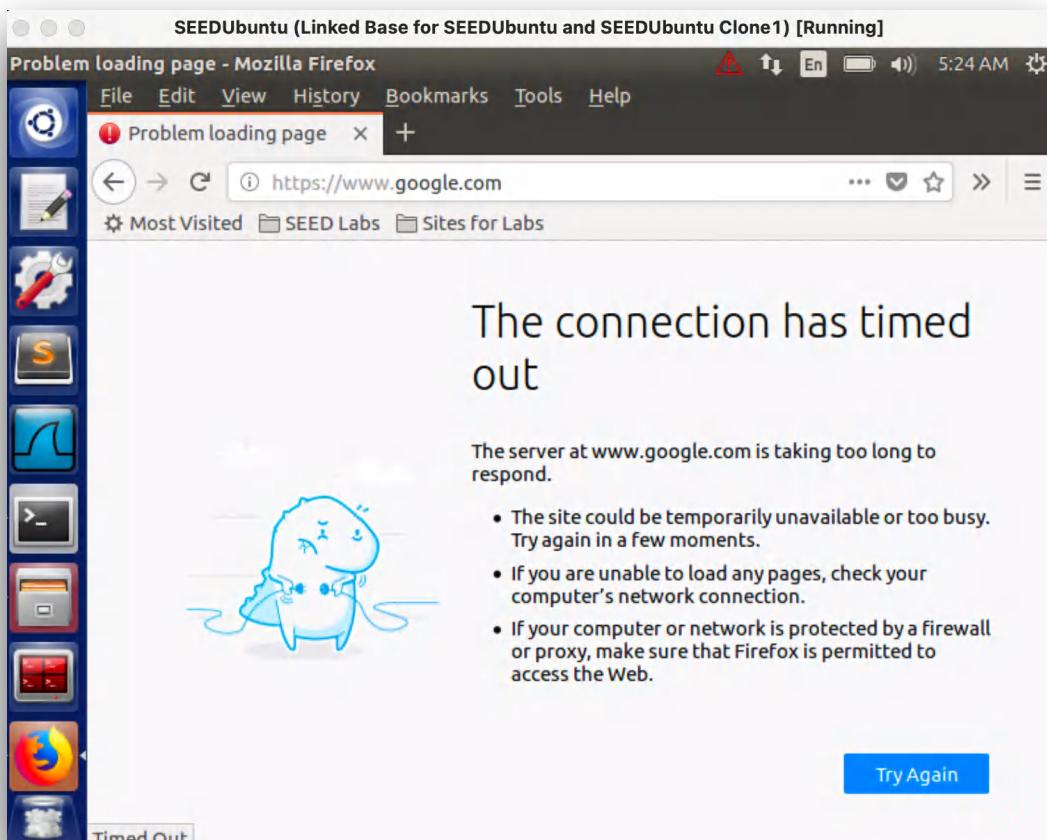
```
[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~$ dmesg | tail -10
          00:00:00.000254 main      Process ID: 162
9          00:00:00.000255 main      Package type: L
INUX_32BITS_GENERIC
[ 10.462833] 00:00:00.001987 main      5.1.14 r112924
started. Verbose level = 0
[ 899.738984] Bluetooth: Core ver 2.21
[ 899.740461] NET: Registered protocol family 31
[ 899.740463] Bluetooth: HCI device and connection manager initialized
[ 899.740466] Bluetooth: HCI socket layer initialized
[ 899.740467] Bluetooth: L2CAP socket layer initialized
[ 899.740472] Bluetooth: SCO socket layer initialized
[ 899.748508] Netfilter messages via NETLINK v0.30.
[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~$
```



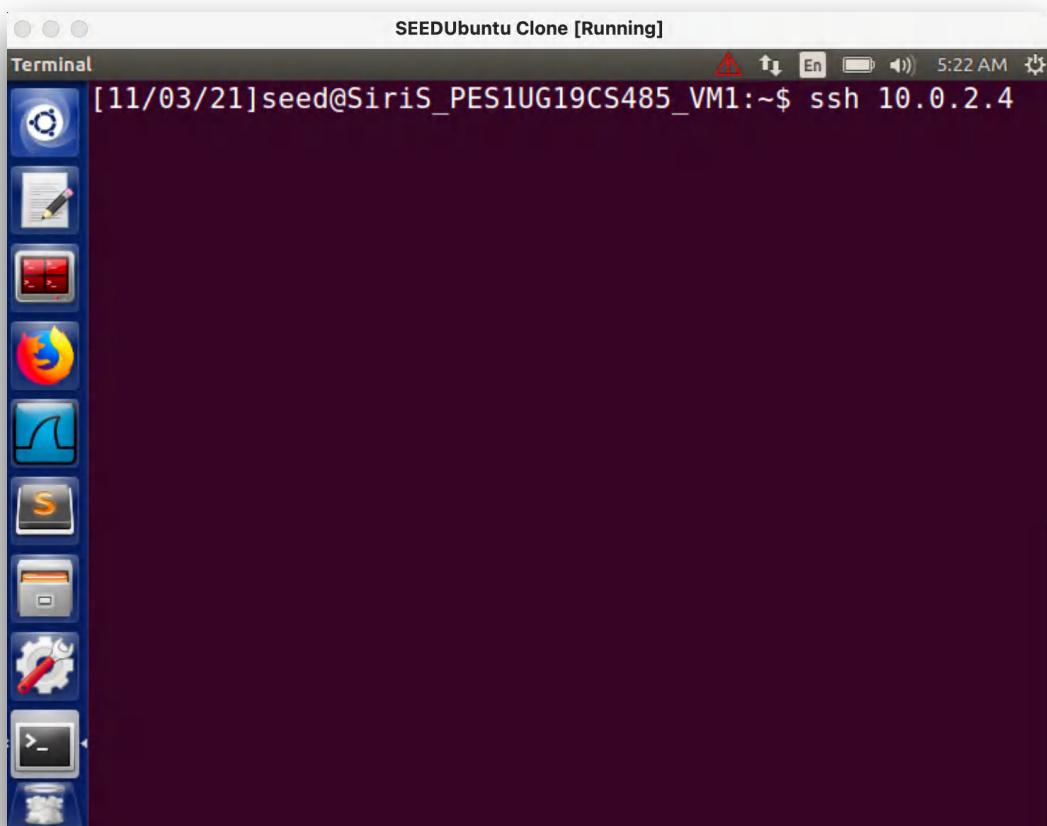
```
Trying 10.0.2.5...
^C
[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~/.../block$ dme
sg | tail -10
[15071.690199] Dropping SSH Packet from source address:
10.0.2.5
[15072.554012] Dropping SSH Packet from source address:
10.0.2.5
[15074.281024] Dropping SSH Packet from source address:
10.0.2.5
[15077.895069] Dropping SSH Packet from source address:
10.0.2.5
[15081.211770] Dropping SSH Packet from source address:
10.0.2.5
[15081.990540] Dropping Telnet Packet to destination ad
dress: 10.0.2.5
[15084.803946] Dropping SSH Packet from source address:
10.0.2.5
[15098.621234] Dropping SSH Packet from source address:
10.0.2.5
[15114.742109] Dropping Telnet Packet to destination ad
dress: 10.0.2.5
```

Step 3: Testing whether external website is blocked from VM1.

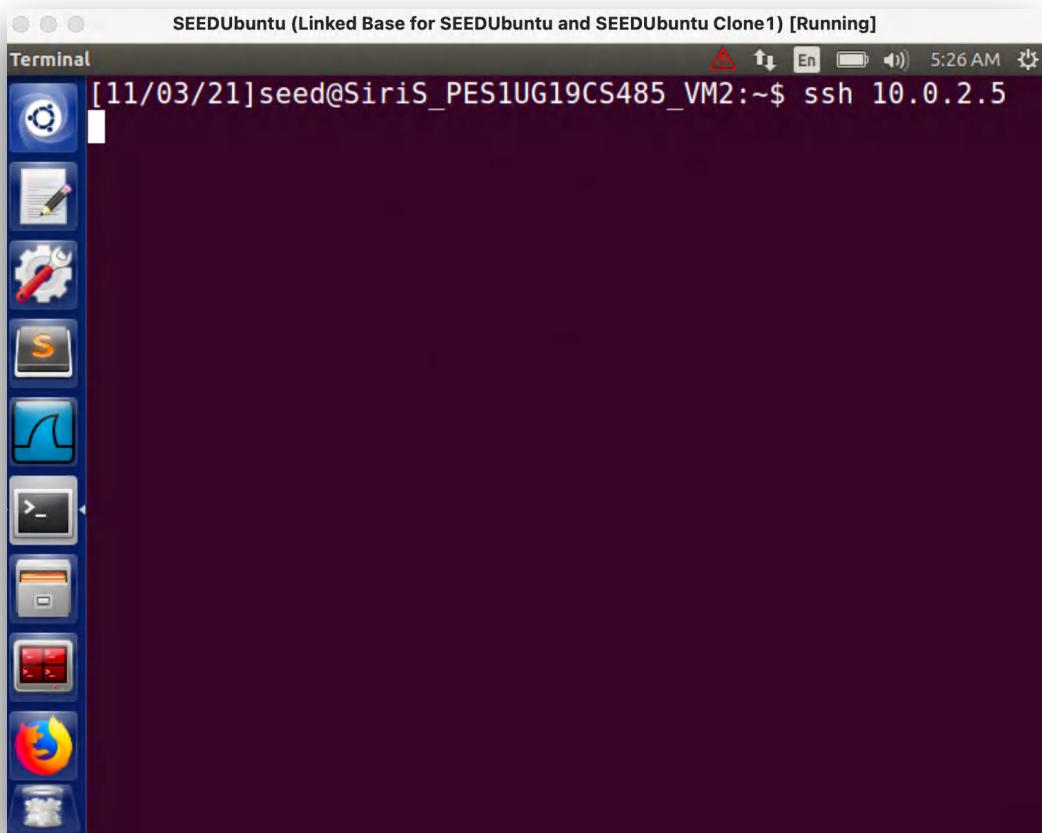
We can see that www.google.com does not load in the browser



Step 4: Testing whether *ssh* from VM1 to VM2 is blocked



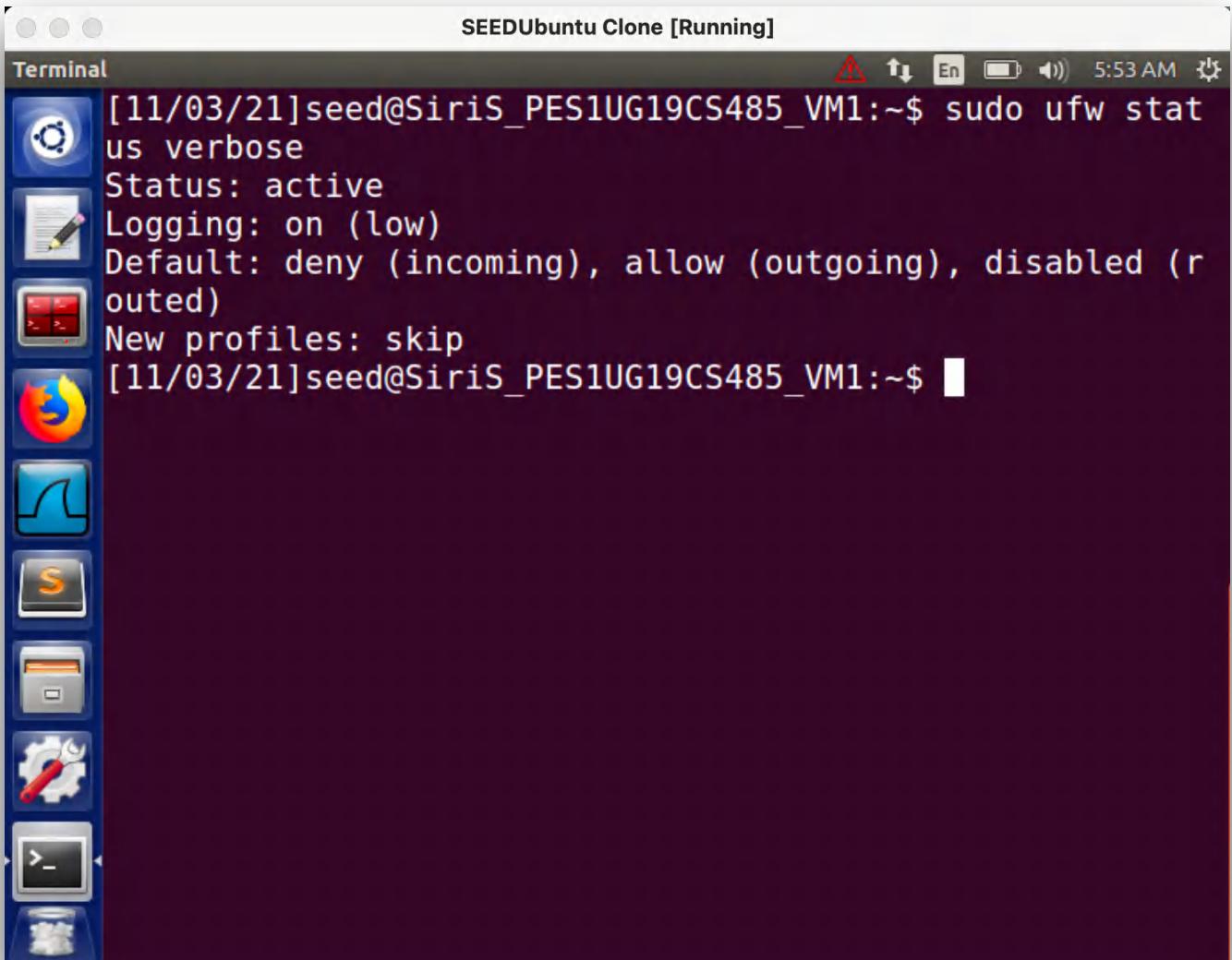
Step 5: Testing whether telnet from VM2 to VM1 is blocked



We can see that ssh is blocked both ways.

Task 3: Evading Egress Filtering

Deleting all the firewall rules from the previous task, we can see that the status is empty:



The screenshot shows a desktop environment with a terminal window open. The terminal window title is "SEEDUbuntu Clone [Running]". The system tray icons include a warning triangle, signal strength, battery level, and a gear icon. The date and time are 5:53 AM. The terminal output is as follows:

```
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw stat
us verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ █
```

The desktop interface includes a vertical dock on the left with icons for the terminal, file manager, browser, and other system applications.

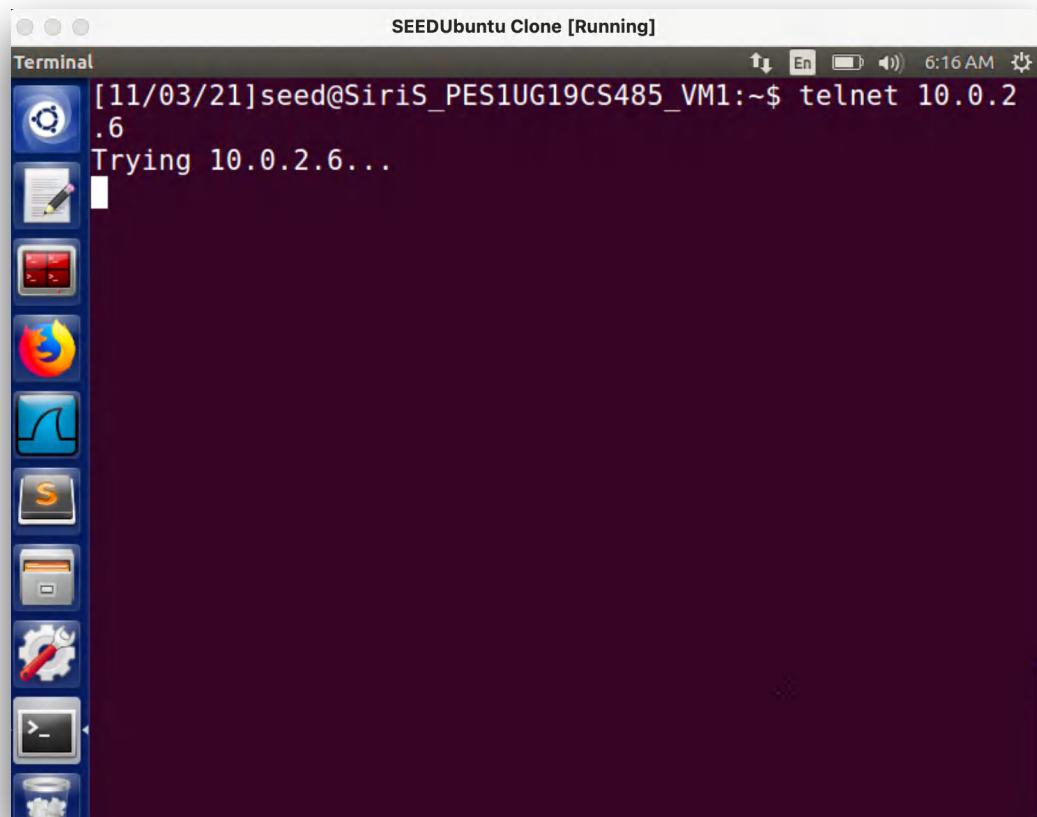
Task 3. a: Telnet to Machine B through the firewall

We will first block VM1 from being able to telnet to any other machine.

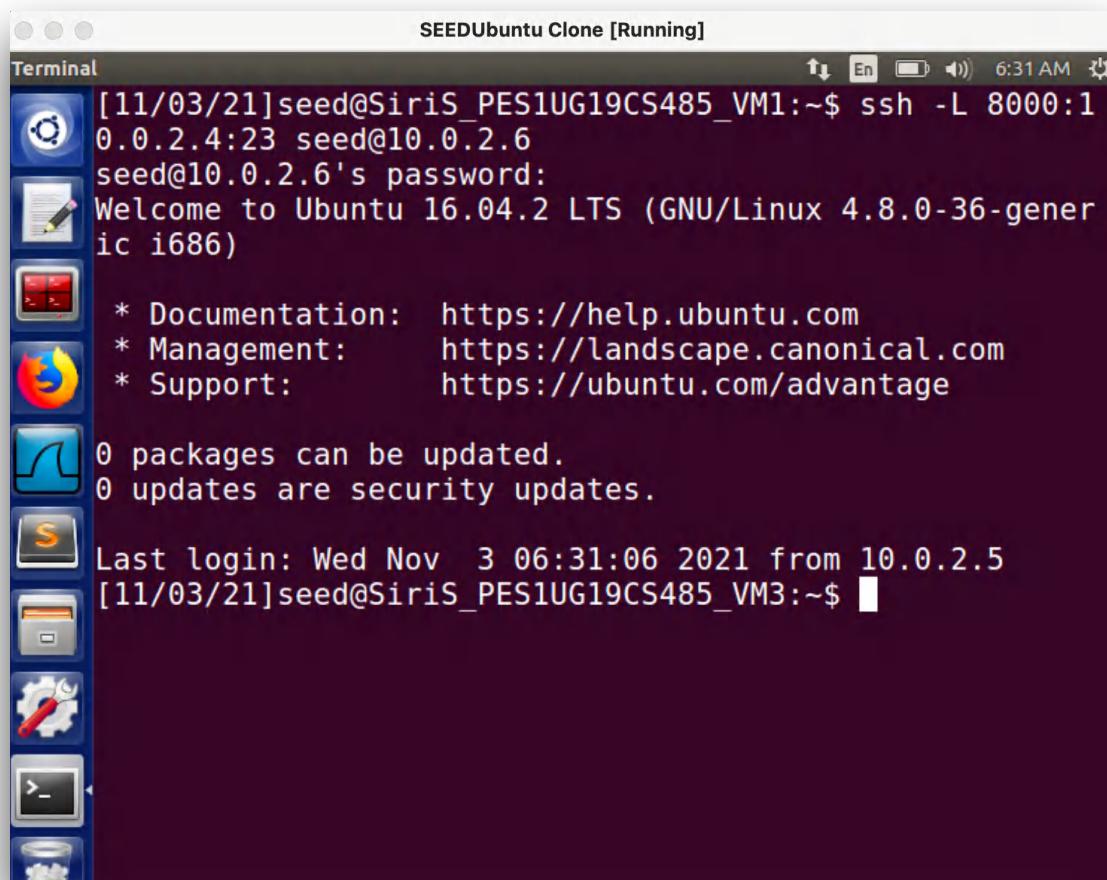
```
SEEDUbuntu Clone [Running]
Terminal File Edit View Search Terminal Help 6:13 AM
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw enable
Firewall is active and enabled on system startup
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw deny out from 10.0.2.5 to any port 23
Rule added
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

```
SEEDUbuntu Clone [Running]
Terminal Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw deny out from 10.0.2.5 to any port 23
Rule added
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To Action From
-- -----
23 DENY OUT 10.0.2.5
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ █
```

Now we check if we're able to telnet to VM3 from VM1:



It doesn't work so we establish an ssh tunnel between VM1 and VM2 to allow VM1 to telnet to VM3 via VM2 :



With the ssh tunnel setup, we can now telnet from VM1 to VM3 even though the firewall policy on VM1 denies outgoing telnet.

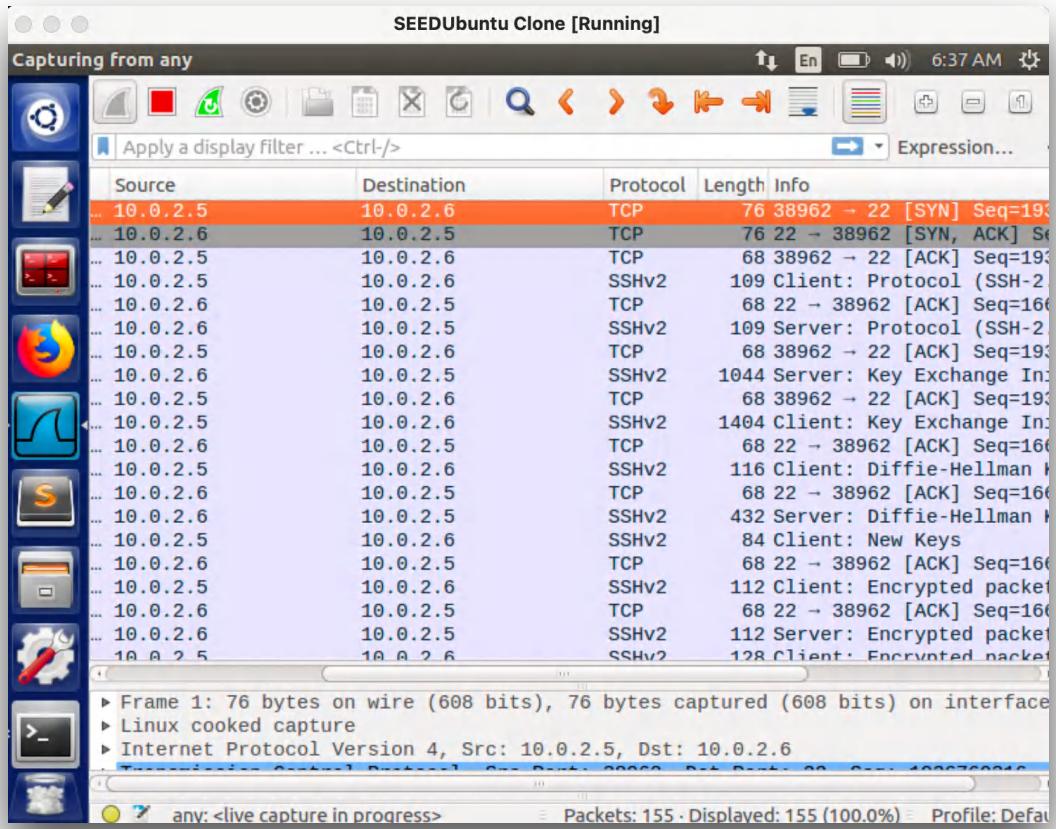
```
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ ssh -L 8000:1  
0.0.2.4:23 seed@10.0.2.6  
seed@10.0.2.6's password:  
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)  
  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/advantage  
  
0 packages can be updated.  
0 updates are security updates.  
  
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ telnet localhost 8000  
Trying 127.0.0.1...  
Connected to localhost.localdomain.  
Escape character is '^]'.  
Ubuntu 16.04.2 LTS  
SiriS_PES1UG19CS485_VM2 login: seed  
Password:  
Last login: Wed Nov 3 05:25:09 EDT 2021 from 10.0.2.4  
on pts/17
```

Wireshark Screenshots:

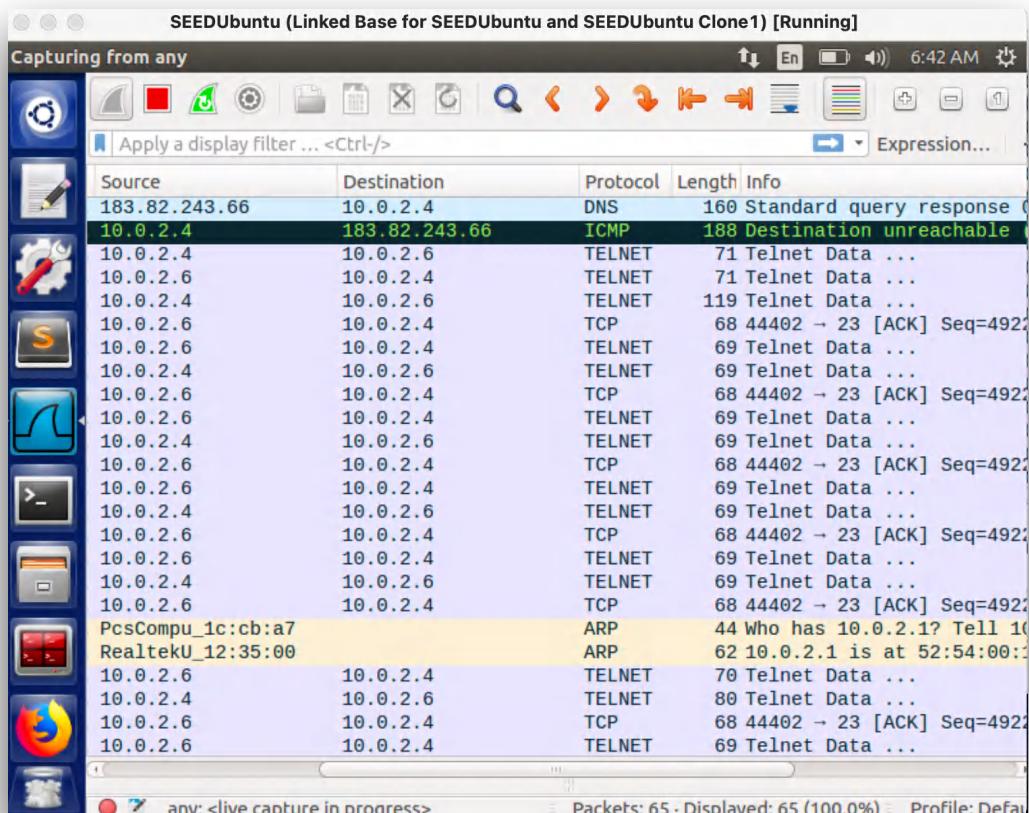
Source	Destination	Protocol	Length	Info
10.0.2.5	10.0.2.6	TCP	68	38966 → 22 [ACK] Seq=2654
10.0.2.5	10.0.2.6	SSHv2	109	Client: Protocol (SSH-2.0)
10.0.2.6	10.0.2.5	TCP	68	22 → 38966 [ACK] Seq=3348
10.0.2.6	10.0.2.5	SSHv2	109	Server: Protocol (SSH-2.0)
10.0.2.5	10.0.2.6	TCP	68	38966 → 22 [ACK] Seq=2654
10.0.2.6	10.0.2.5	SSHv2	1044	Server: Key Exchange Init
10.0.2.5	10.0.2.6	TCP	68	38966 → 22 [ACK] Seq=2654
10.0.2.5	10.0.2.6	SSHv2	1404	Client: Key Exchange Init
10.0.2.6	10.0.2.5	TCP	68	22 → 38966 [ACK] Seq=3348
10.0.2.5	10.0.2.6	SSHv2	116	Client: Diffie-Hellman Key Exchange
10.0.2.6	10.0.2.5	TCP	68	22 → 38966 [ACK] Seq=3348
10.0.2.6	10.0.2.5	SSHv2	432	Server: Diffie-Hellman Key Exchange
10.0.2.5	10.0.2.6	SSHv2	84	Client: New Keys
10.0.2.6	10.0.2.5	TCP	68	22 → 38966 [ACK] Seq=3348
10.0.2.5	10.0.2.6	SSHv2	112	Client: Encrypted packet
10.0.2.6	10.0.2.5	TCP	68	22 → 38966 [ACK] Seq=3348
10.0.2.6	10.0.2.5	SSHv2	112	Server: Encrypted packet
10.0.2.5	10.0.2.6	SSHv2	128	Client: Encrypted packet

Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface
▶ Linux cooked capture
▶ Internet Protocol Version 6, Src: ::1, Dst: ::1
▶ User Datagram Protocol, Src Port: 42900, Dst Port: 51586

VM1's Wireshark shows that packets were sent and received from VM3



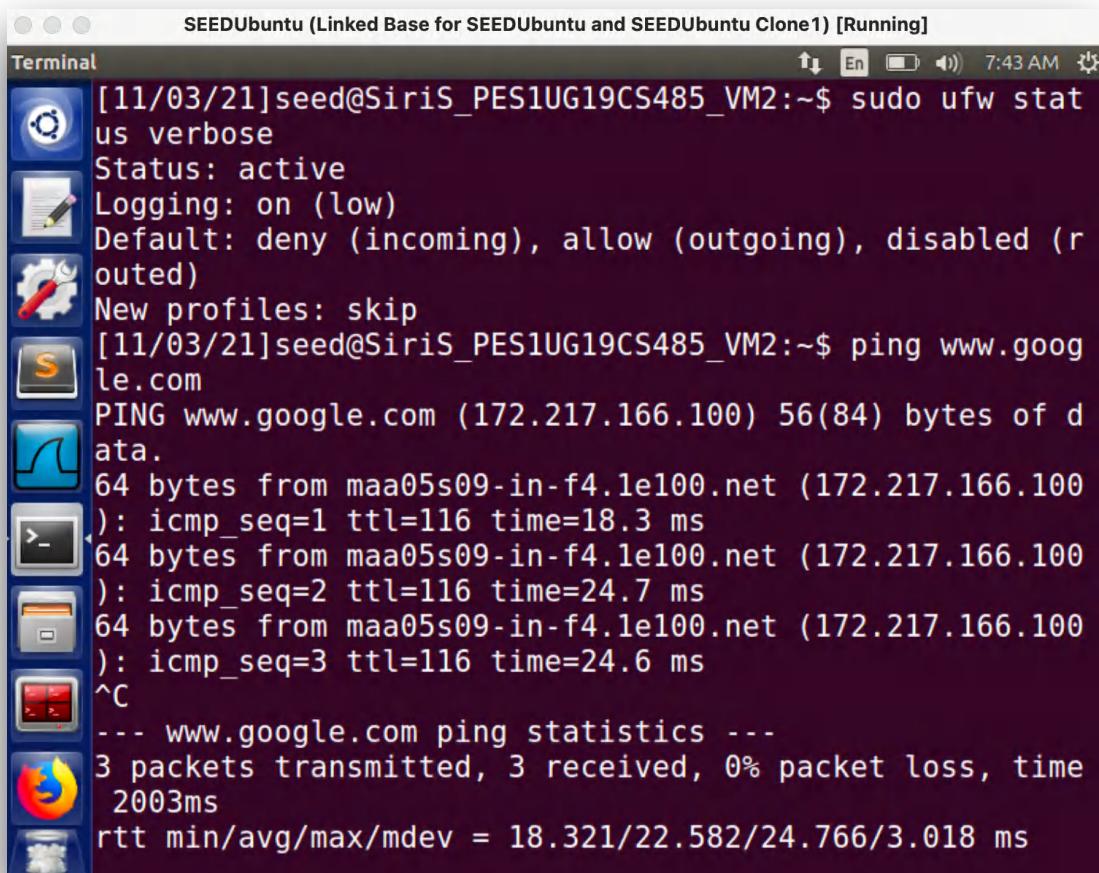
VM2's Wireshark shows that packets were sent and received from VM3.



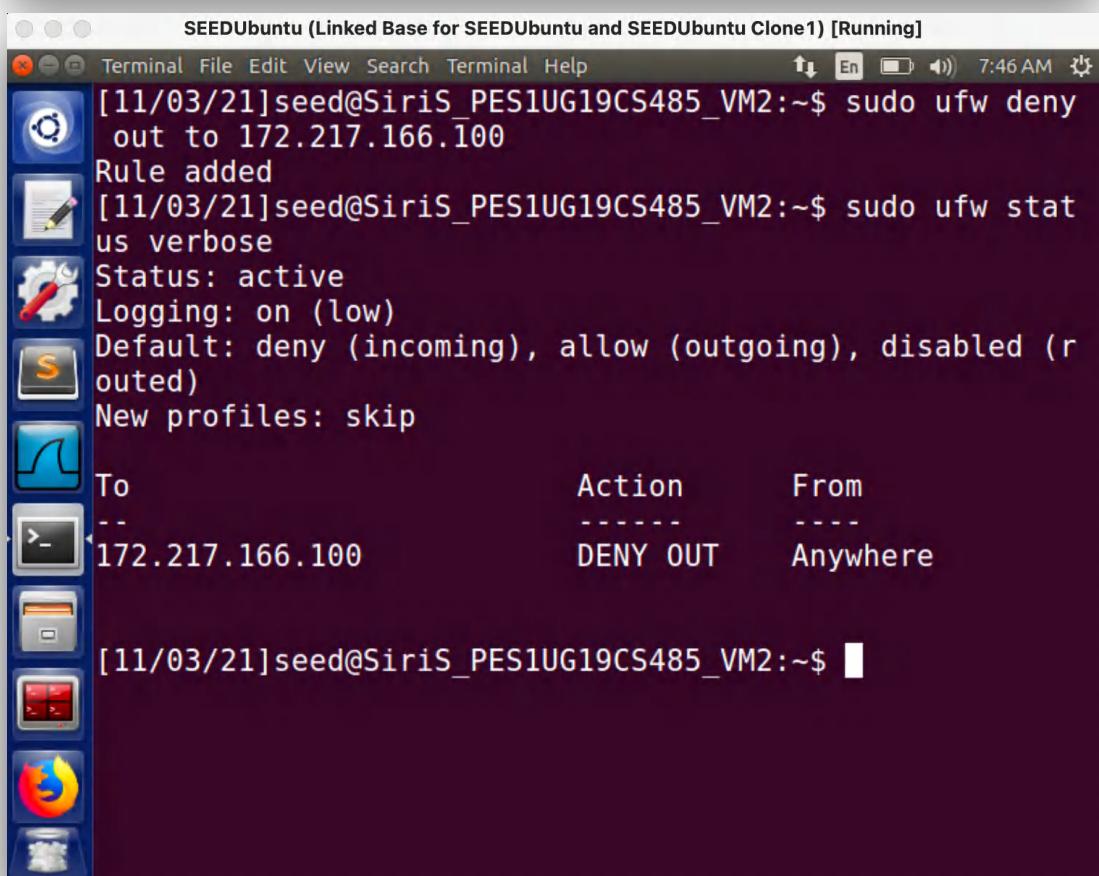
VM3's Wireshark shows that the packets were sent back to VM1. Hence all packets obtained by VM2 are forwarded to VM3 through port 23. VM3 is able to respond back to the telnet request from VM1, evading the firewall.

Task 3. b: Connecting to Google using SSH tunnel

First we delete other firewall rules, then we check the status of *ufw* and setup a firewall rule:

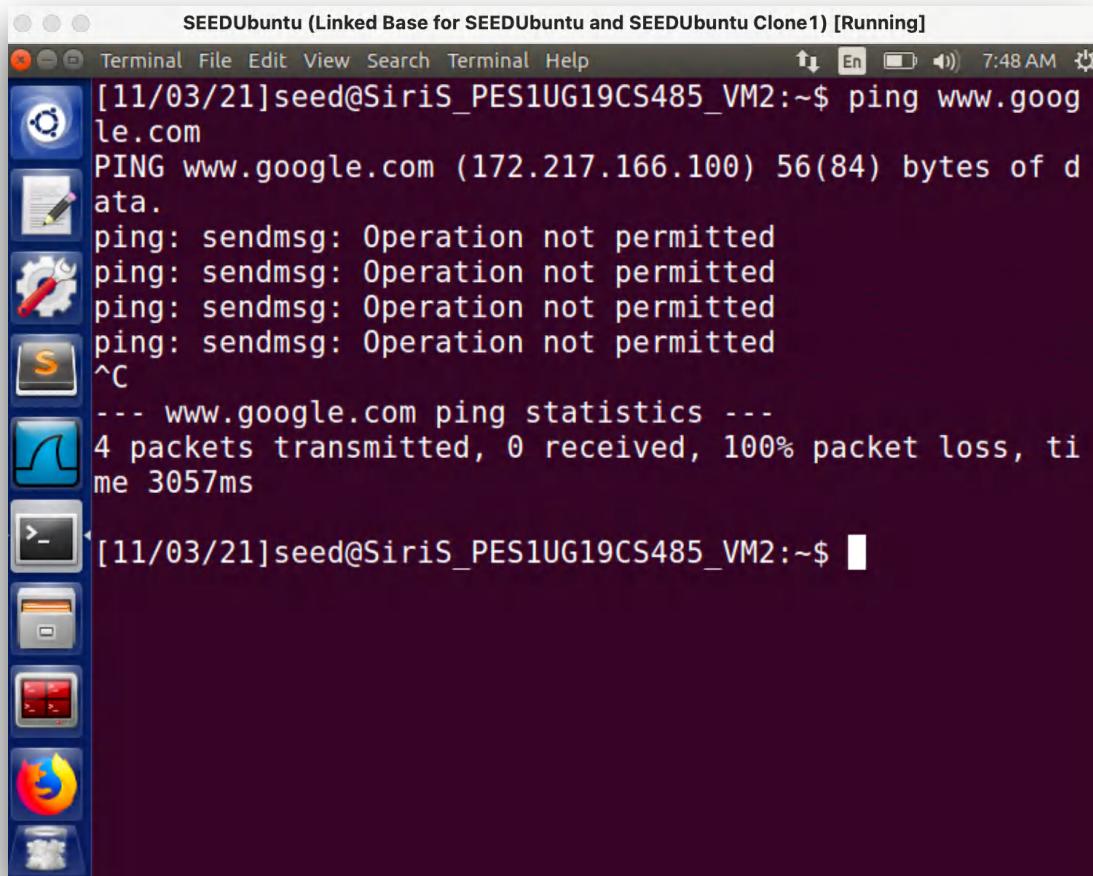


```
SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal
[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~$ sudo ufw stat
us verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~$ ping www.google.com
PING www.google.com (172.217.166.100) 56(84) bytes of data.
64 bytes from maa05s09-in-f4.1e100.net (172.217.166.100):
icmp_seq=1 ttl=116 time=18.3 ms
64 bytes from maa05s09-in-f4.1e100.net (172.217.166.100):
icmp_seq=2 ttl=116 time=24.7 ms
64 bytes from maa05s09-in-f4.1e100.net (172.217.166.100):
icmp_seq=3 ttl=116 time=24.6 ms
^C
--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time
2003ms
rtt min/avg/max/mdev = 18.321/22.582/24.766/3.018 ms
```



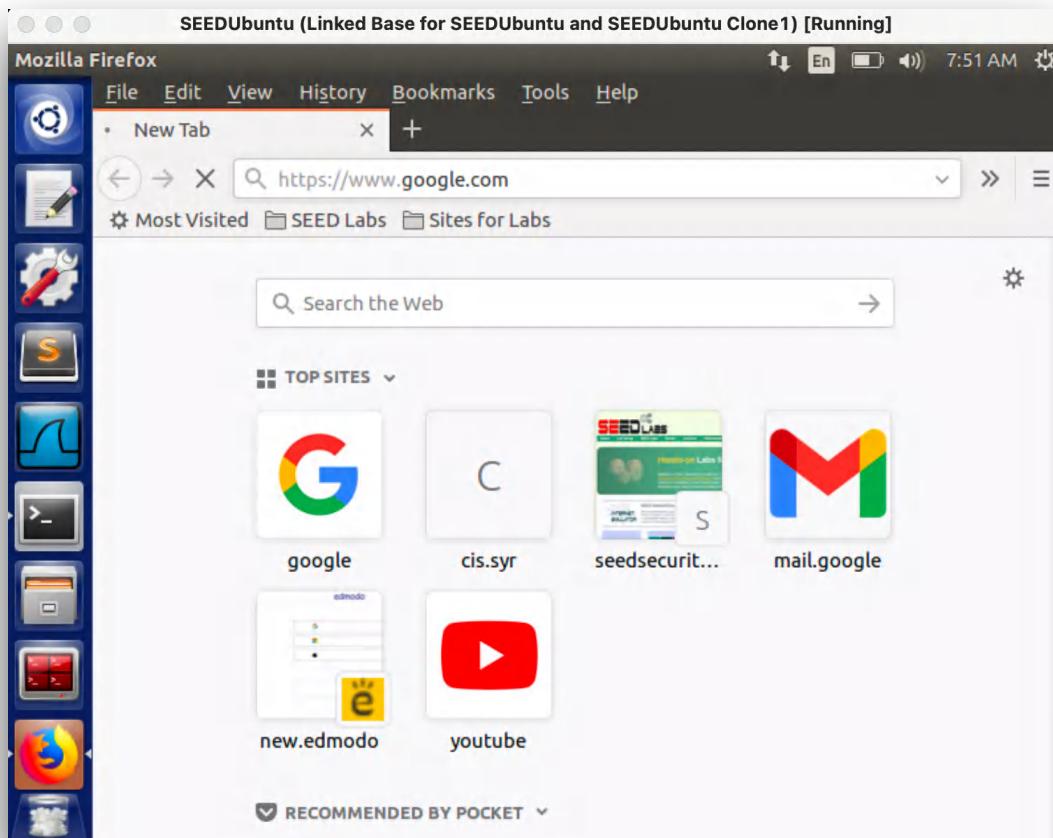
```
SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal File Edit View Search Terminal Help
[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~$ sudo ufw deny
out to 172.217.166.100
Rule added
[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~$ sudo ufw stat
us verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To Action From
-- -----
172.217.166.100 DENY OUT Anywhere
[11/03/21]seed@SiriS_PES1UG19CS485_VM2:~$
```

With the firewall rule in place, we can try to ping www.google.com. The operation is not permitted because it is being blocked by the firewall.



```
SEEDUbuntu (Linked Base for SEEDUbuntu and SEEDUbuntu Clone1) [Running]
Terminal File Edit View Search Terminal Help 7:48 AM
[11/03/21]seed@Siris_PES1UG19CS485_VM2:~$ ping www.google.com
PING www.google.com (172.217.166.100) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
^C
--- www.google.com ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3057ms
[11/03/21]seed@Siris_PES1UG19CS485_VM2:~$
```

We can also try to visit www.google.com through the browser, where we are unable to load the page.



We now setup a ssh tunnel with dynamic port forwarding between VM1 and VM3. With this tunnel setup, VM1 will be able to use its local port 9000 to send a request to www.google.com via VM3.

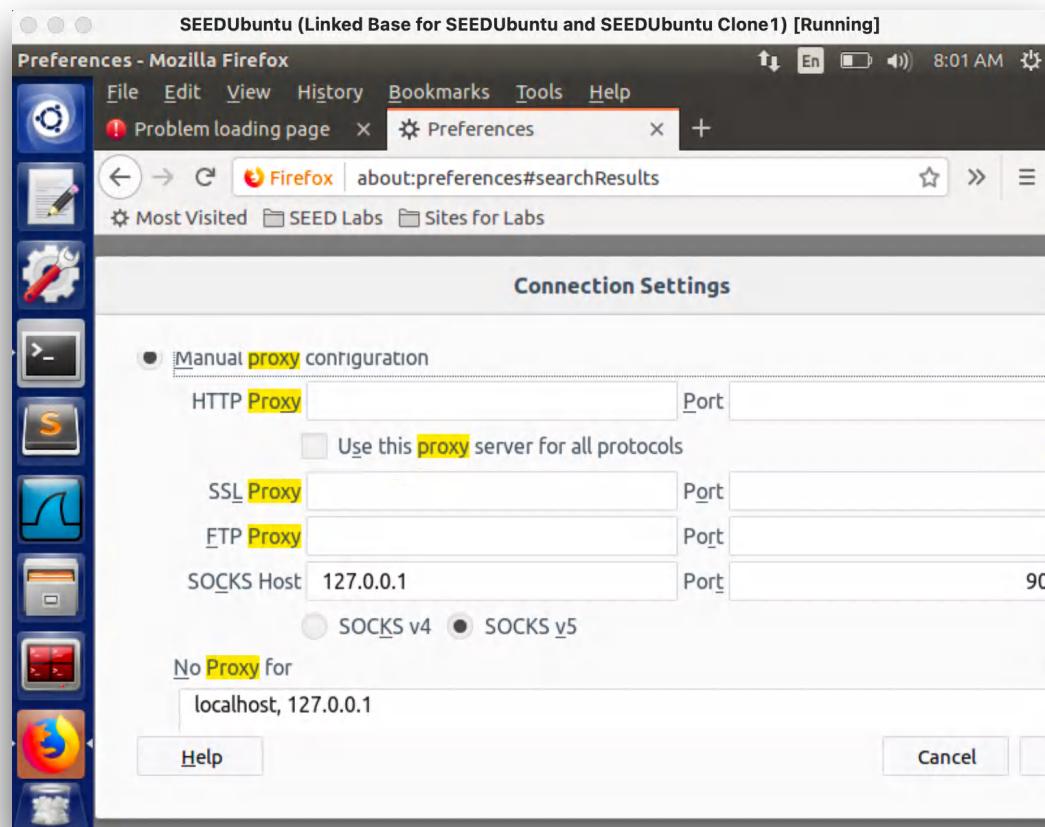
```
[11/03/21]seed@Siris_PES1UG19CS485_VM1:~$ ssh -D 9000 -C seed@10.0.2.6
seed@10.0.2.6's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

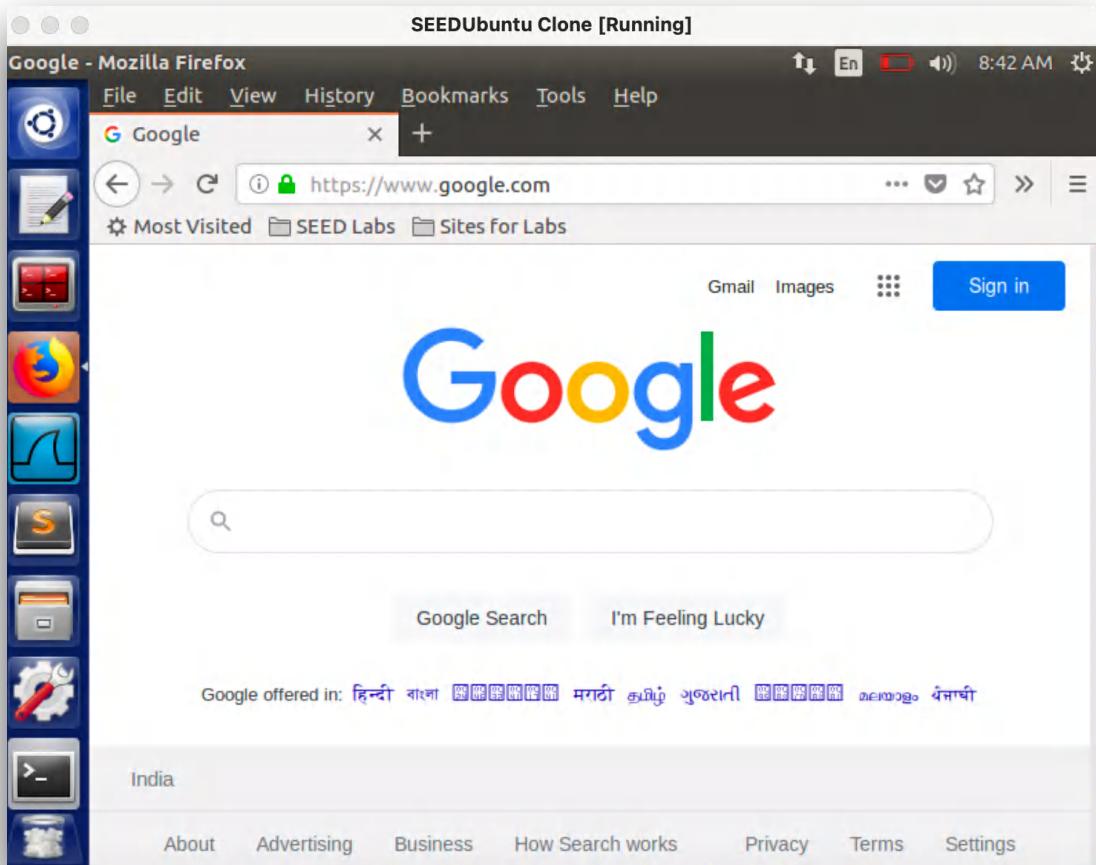
0 packages can be updated.
0 updates are security updates.

Last login: Wed Nov  3 08:38:10 2021 from 10.0.2.5
[11/03/21]seed@Siris_PES1UG19CS485_VM3:~$
```

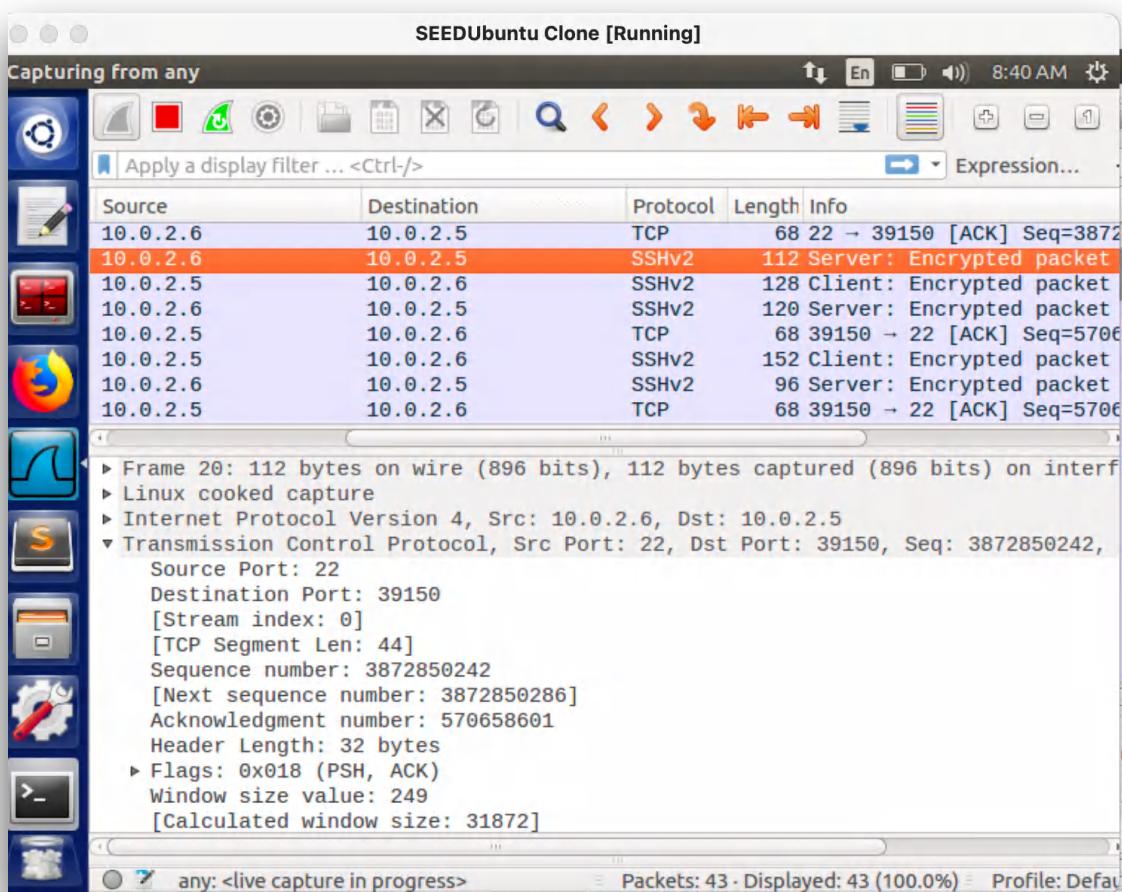
To use the established tunnel, we need to set the proxy settings in the Firefox browser as shown below.



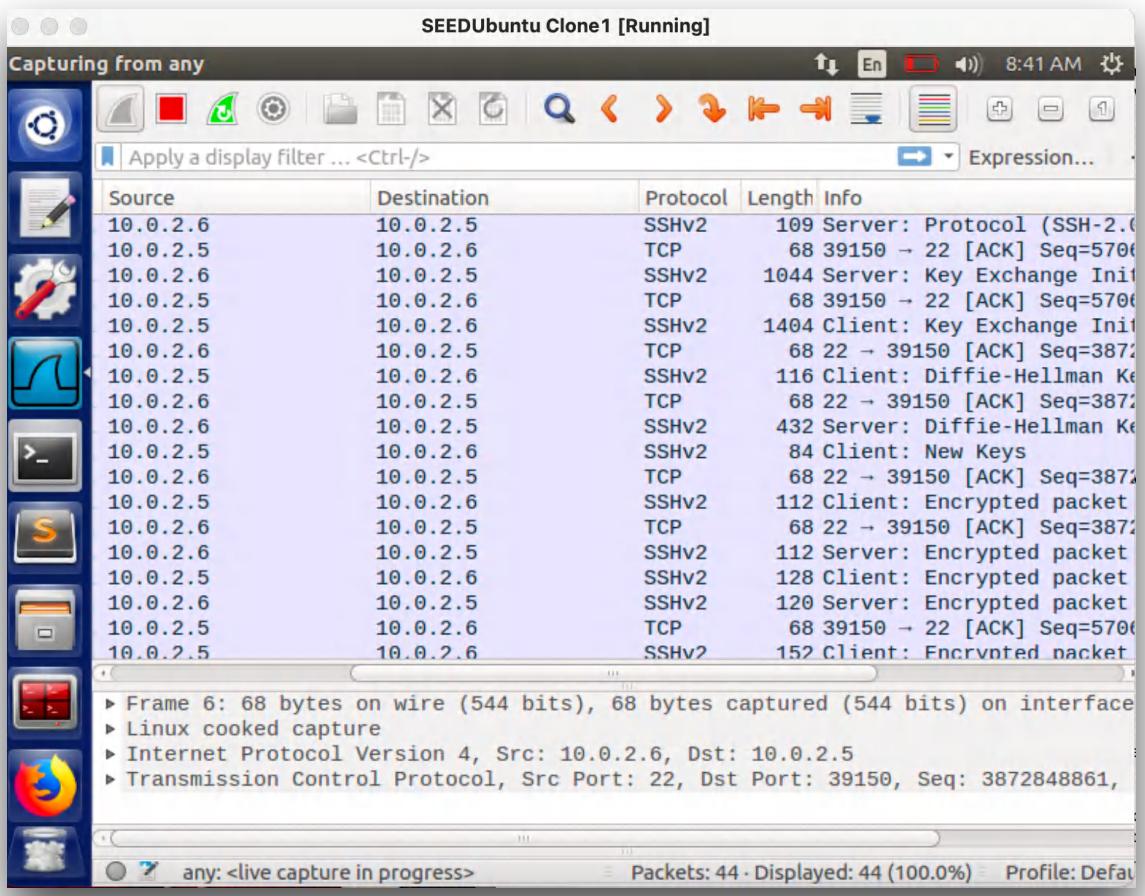
With the proxy settings in place, we are able to visit www.google.com from VM1 even though the firewall has a policy to block it. We can see that page has loaded:



Wireshark Capture from VM 1:

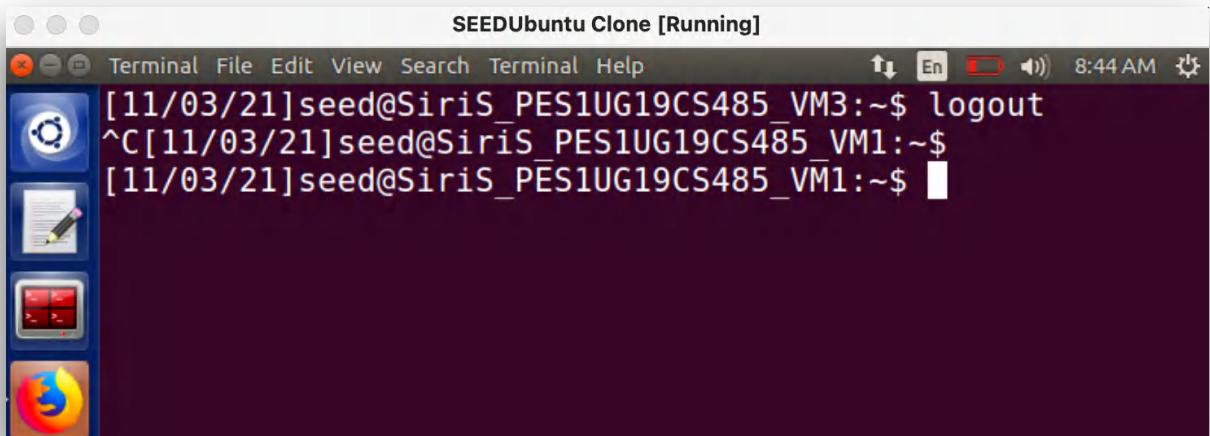


Wireshark Capture from VM 3:

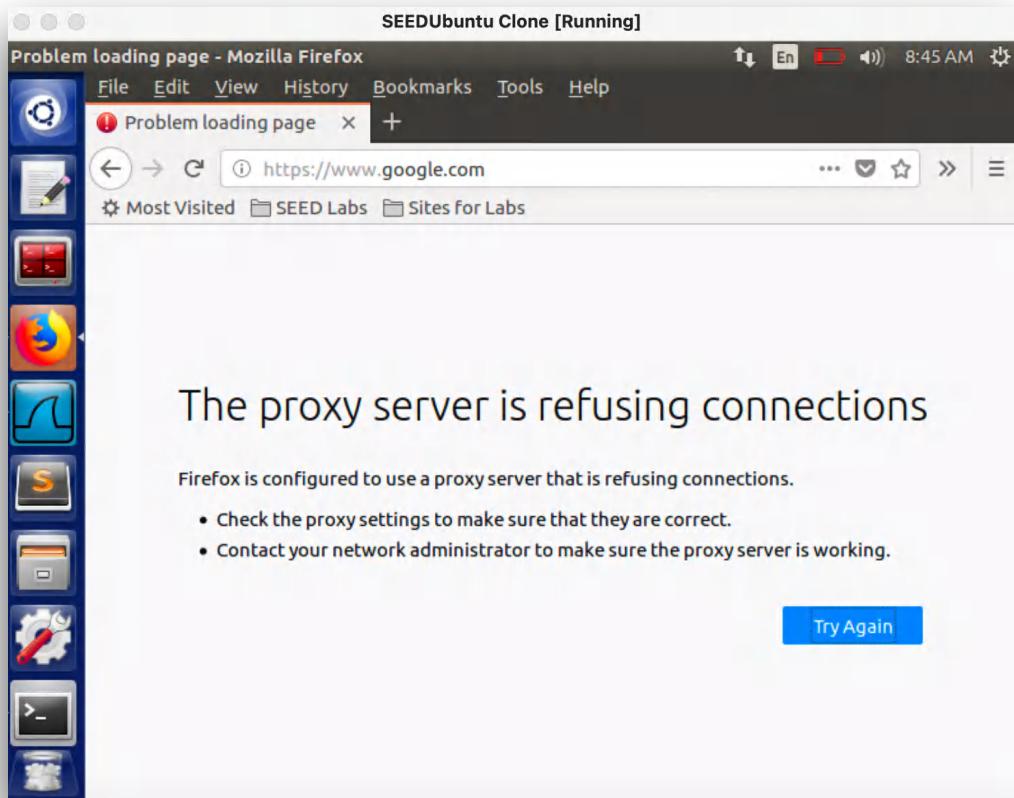


Wireshark capture on VM1 shows that it sent packets to VM3 instead of Google's IP and from VM3's wireshark, we see that it has contacted google on behalf of VM1. It sends back the replies to VM1 thereby bypassing the firewall.

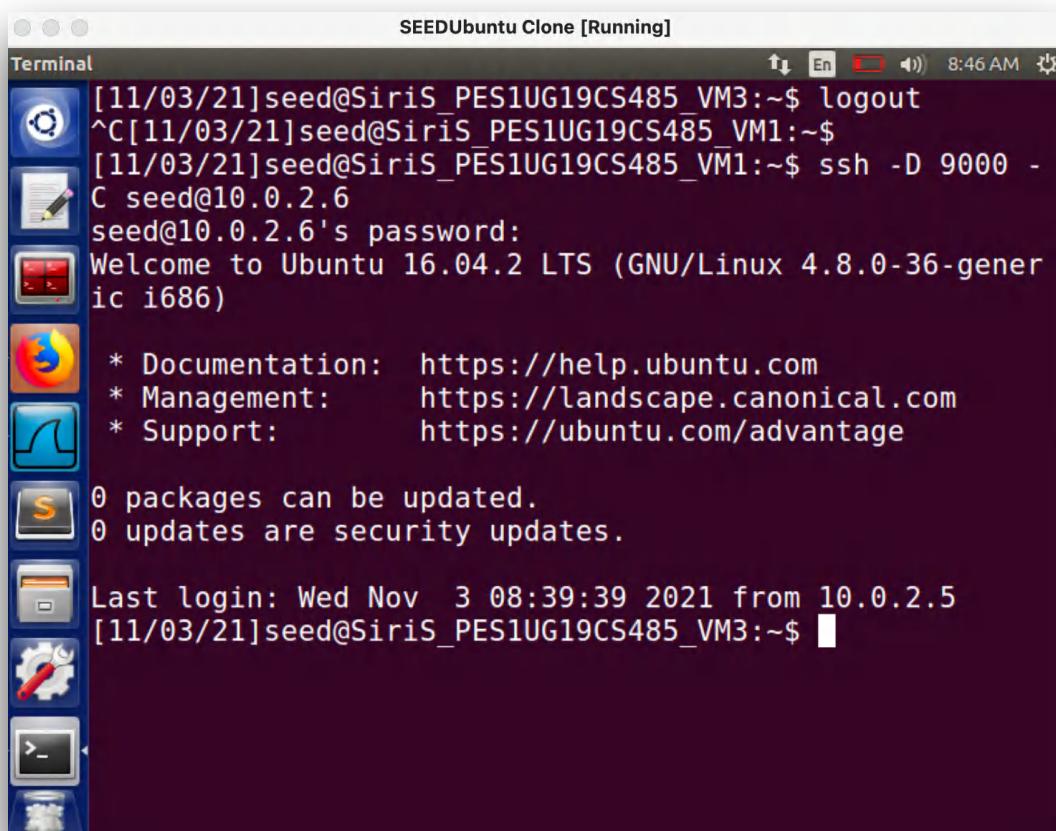
Once we logout of the *ssh* and break the tunnel, www.google.com is no longer accessible:

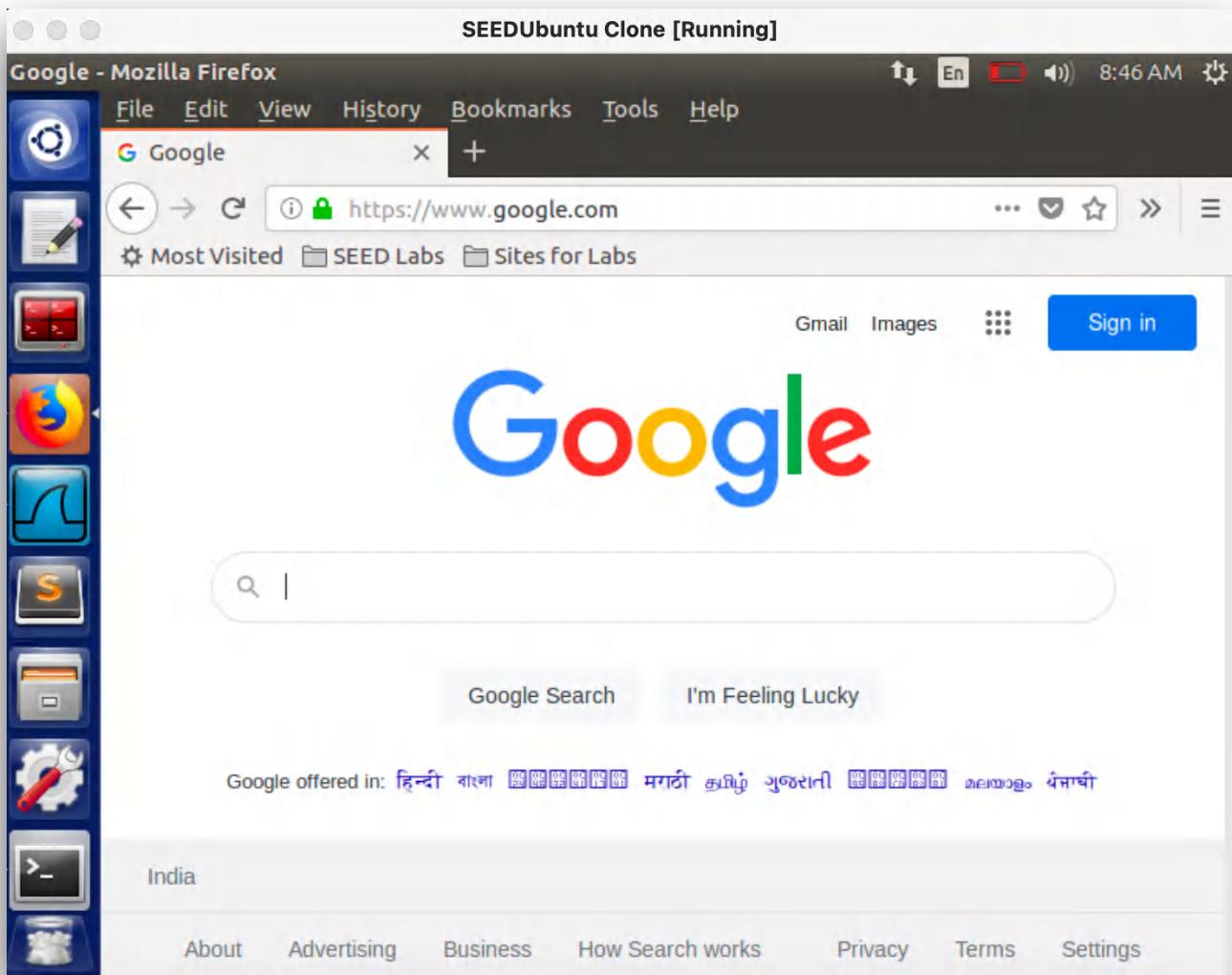


We can see that we are unable to access www.google.com instead it says that proxy is refusing connections:



However, if we activate *ssh* and recode the page we are able to access the website:

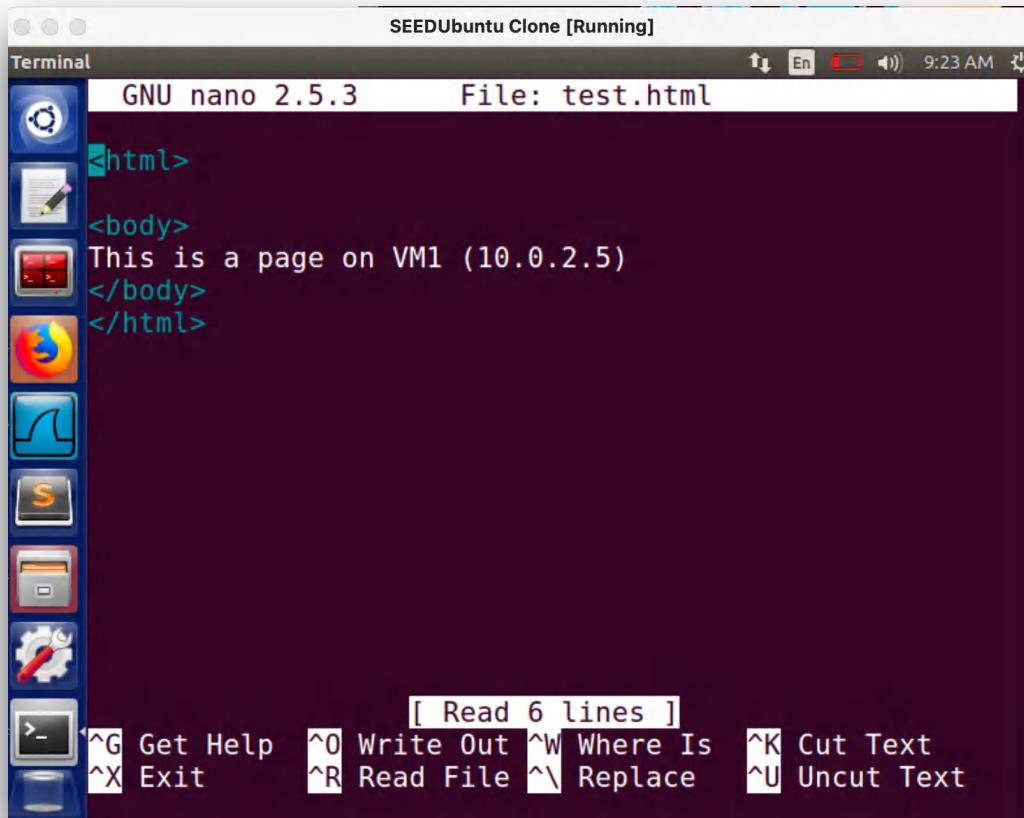




We can see that the website is able to load as soon as we re-enable the ssh tunnel.

Task 4: Evade Ingress Filtering

First remove all firewall rules that were added in the previous tasks. The content of the page in VM1 is:



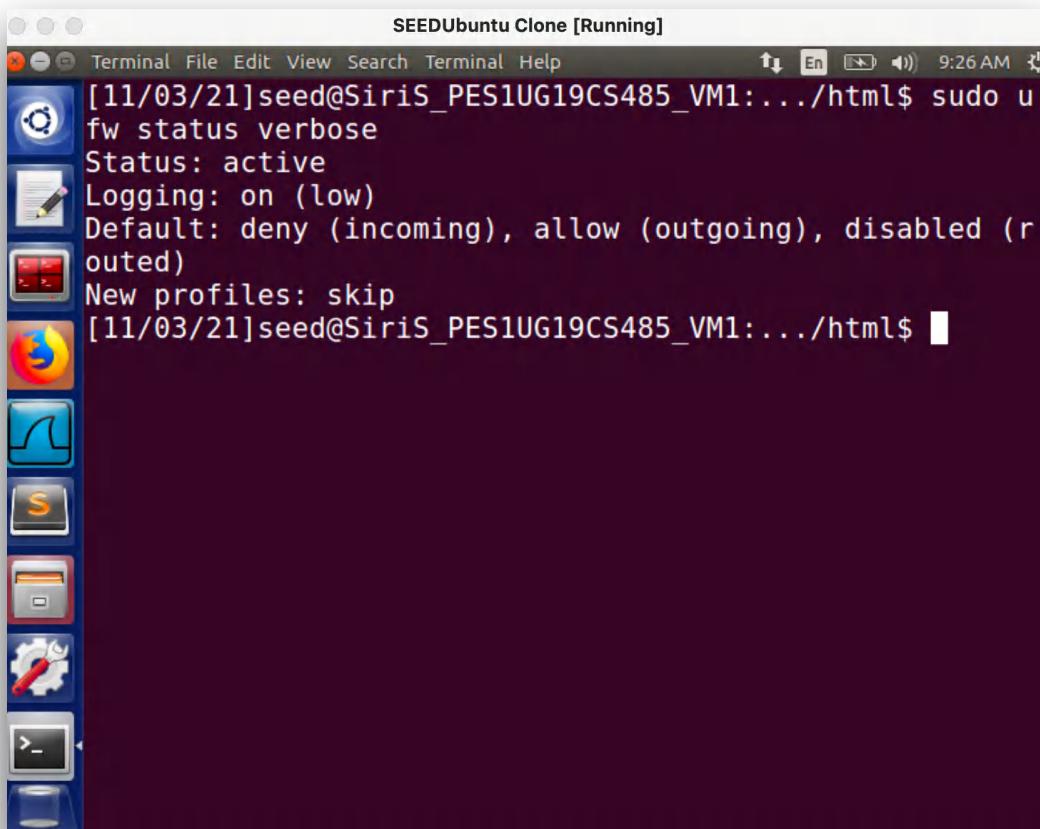
The screenshot shows a terminal window titled "SEEDUbuntu Clone [Running]". The title bar includes icons for signal strength, battery, and volume, along with the time "9:23 AM". The terminal window itself has a dark background and displays the following text:

```
GNU nano 2.5.3      File: test.html
<html>
<body>
This is a page on VM1 (10.0.2.5)
</body>
</html>
```

At the bottom of the terminal window, there is a status bar with the message "[Read 6 lines]". Below the status bar, there are several keyboard shortcut keys and their descriptions:

- ^G Get Help
- ^O Write Out
- ^W Where Is
- ^K Cut Text
- ^X Exit
- ^R Read File
- ^V Replace
- ^U Uncut Text

No firewall rules setup on VM1:



The screenshot shows a terminal window titled "SEEDUbuntu Clone [Running]". The title bar includes icons for signal strength, battery, and volume, along with the time "9:26 AM". The terminal window displays the following command and its output:

```
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:.../html$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:.../html$
```

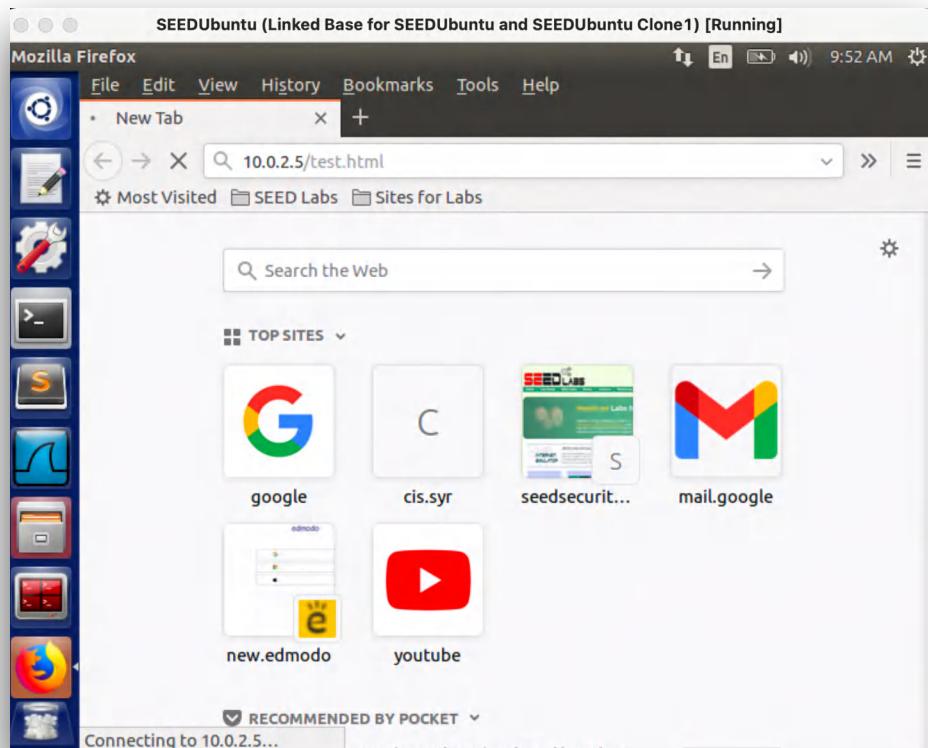
We next block incoming requests on port 80 and port 22 on VM1.

```
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw deny in from any to 10.0.2.5 port 80
Rule added
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw deny in from any to 10.0.2.5 port 22
Rule added
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         DENY IN    Anywhere
10.0.2.5 80                DENY IN    Anywhere
10.0.2.5 22                DENY IN    Anywhere

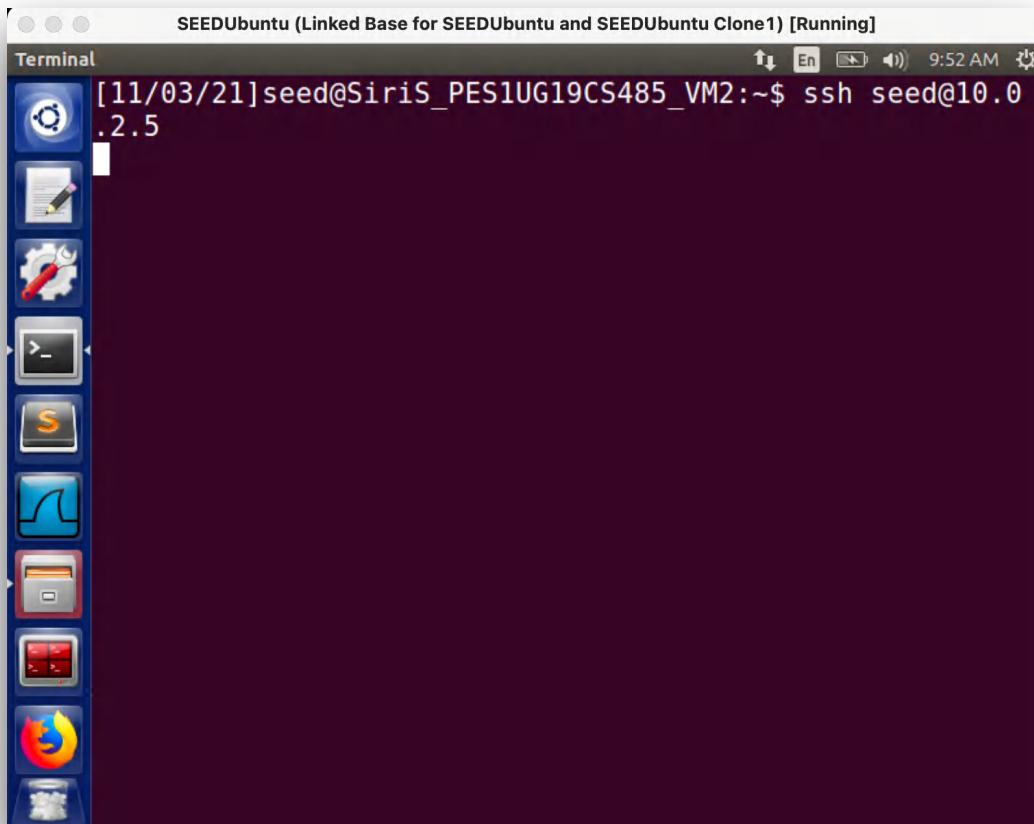
[11/03/21]seed@SiriS_PES1UG19CS485_VM1:~$
```

Upon clearing cache and trying to access the page from VM2:

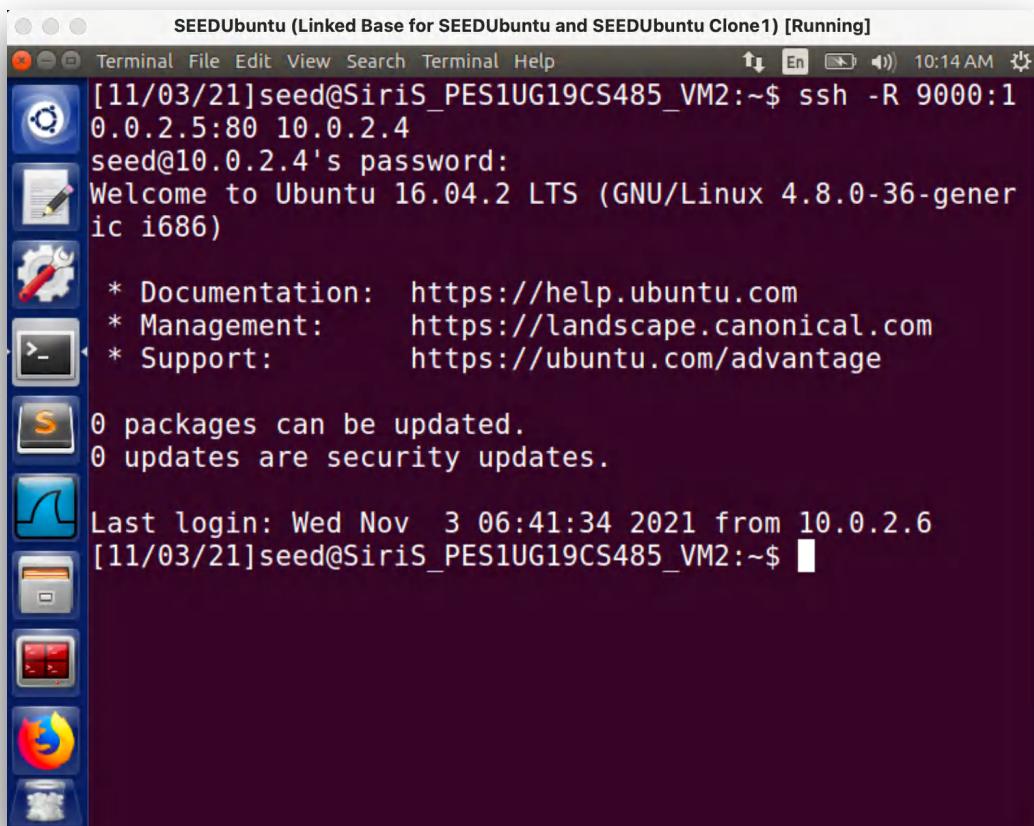


It takes too long to load because of the firewalls

Also, because port 22 is blocked, VM2 cannot ssh to connect to VM1.



Now lets set up a reverse ssh tunnel as shown below



Thus the page is now accessible on VM2 even though the firewall rules were existing.

However when we logout of the ssh connection, the page again doesn't load and displays a 'Unable to connect' message:

