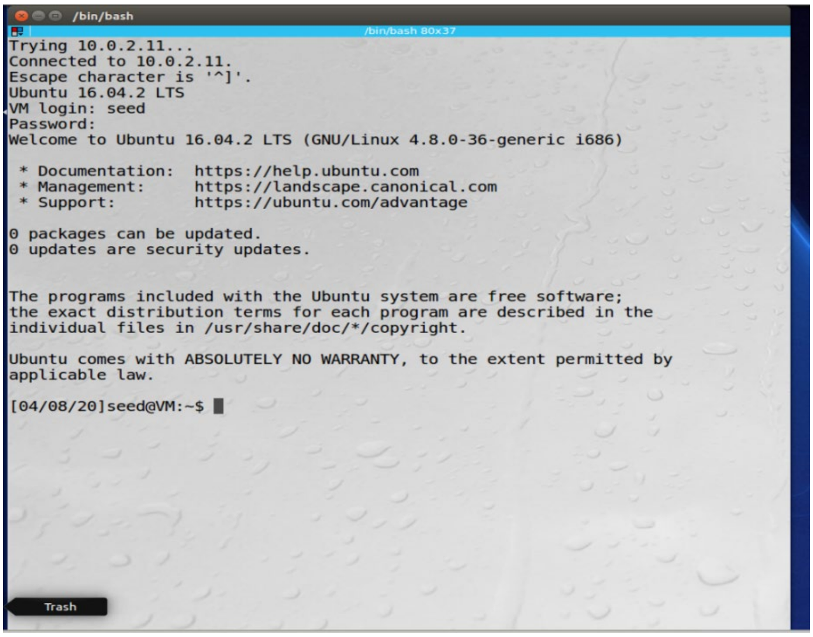
50.020 Network Security Lab 7 | Wong Chi Seng 1002853

Task 2

The IP of machine A is 10.0.2.9 while that of B is 10.0.2.11.

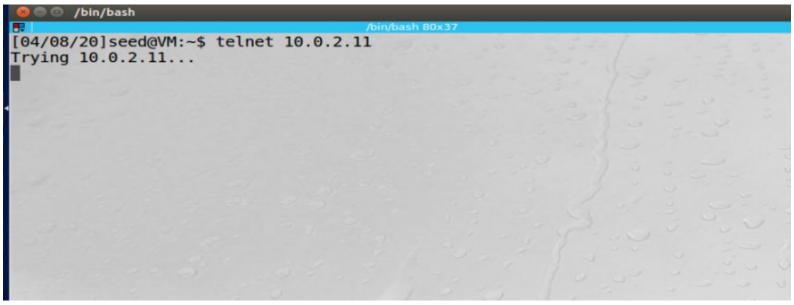
- **Preventing VM A from doing telnet to VM B**

  Before inserting the kernel module with code to block out telnet traffic, we can still establish a telnet connection.



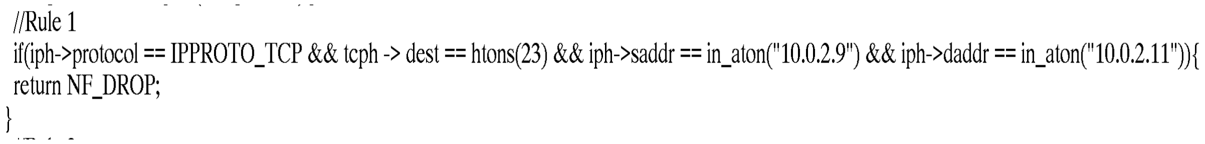
```
Trying 10.0.2.11...
Connected to 10.0.2.11.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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.


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.

[04/08/20]seed@VM:~$
```

  After inserting the kernel module, the connection attempt gets blocked.



```
[04/08/20]seed@VM:~$ telnet 10.0.2.11
Trying 10.0.2.11...
```

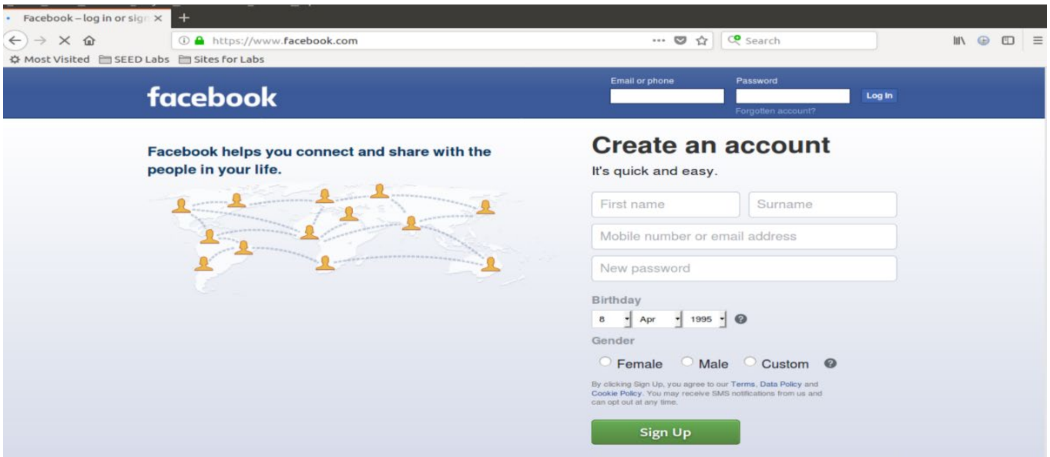
  Below shows a snippet of the code used to block network traffic.



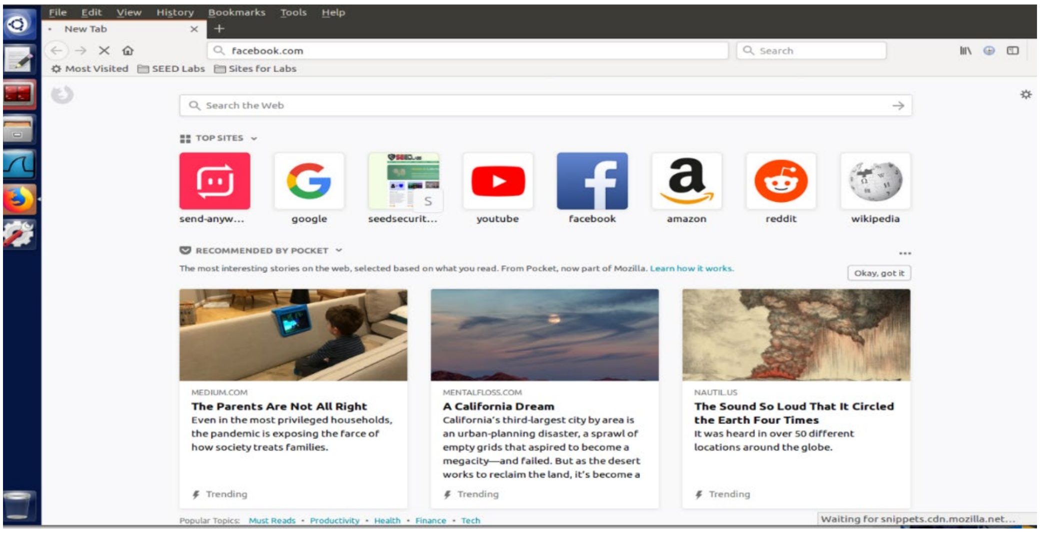
```
 //Rule 1
 if(iph->protocol == IPPROTO_TCP && tcph -> dest == htons(23) && iph->saddr == in_aton("10.0.2.9") && iph->daddr == in_aton("10.0.2.11")){
 return NF_DROP;
}
```

- **Preventing VM A from visiting a website**

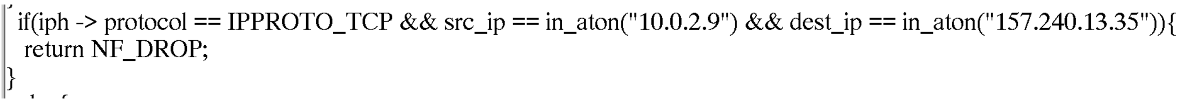
  Before the firewall is put up, we can still access the site www.facebook.com as shown below.



After the firewall is put up, the page never loads on the browser.



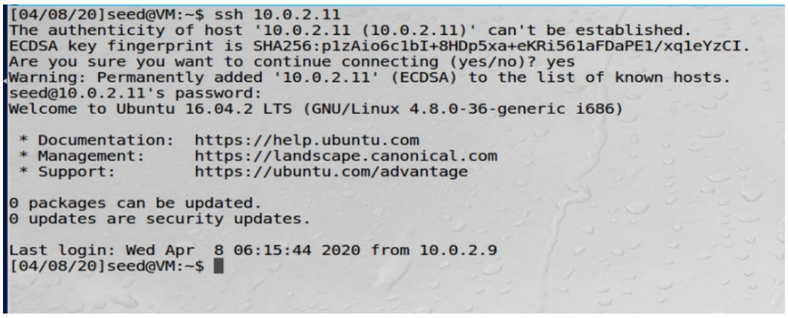
The IP of www.facebook.com can be found using the dig command although it changes from time to time. At that point in time, the IP address was 152.240.13.35



```
if(iph -> protocol == IPPROTO_TCP && src_ip == in_aton("10.0.2.9") && dest_ip == in_aton("157.240.13.35")){
 return NF_DROP;
}
```

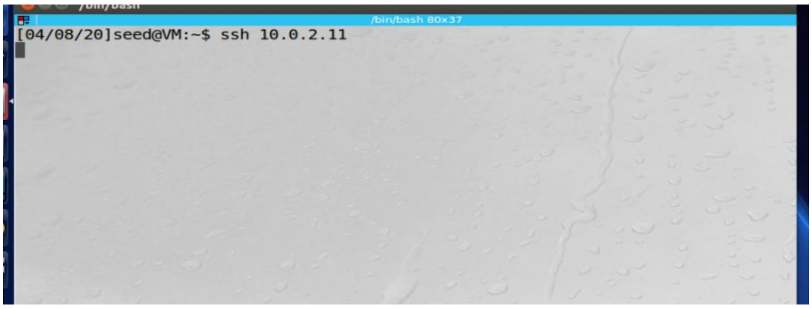
- Preventing VM A from doing **SSH** to VM B

Before the firewall is put up, SSH connections are still allowed.



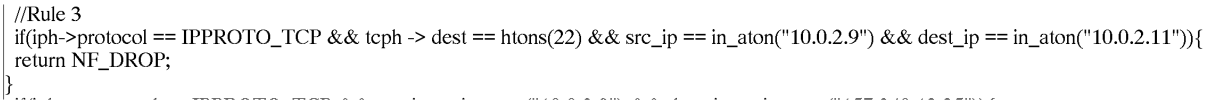
```
[04/08/20]seed@VM:~$ ssh 10.0.2.11
The authenticity of host '10.0.2.11 (10.0.2.11)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.11' (ECDSA) to the list 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: Wed Apr  8 06:15:44 2020 from 10.0.2.9
[04/08/20]seed@VM:~$ 
```

After the firewall is in place, SSH connections are dropped by the machine A.



```
[04/08/20]seed@VM:~$ ssh 10.0.2.11
```

In the screenshot below, we block out outgoing traffic to port 22.

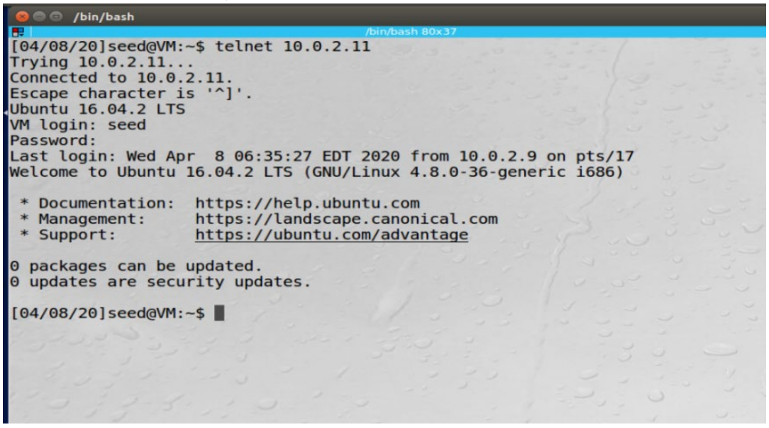


```
//Rule 3
if(iph->protocol == IPPROTO_TCP && tcph -> dest == htons(22) && src_ip == in_aton("10.0.2.9") && dest_ip == in_aton("10.0.2.11")){
return NF_DROP;
}
```

Task 3

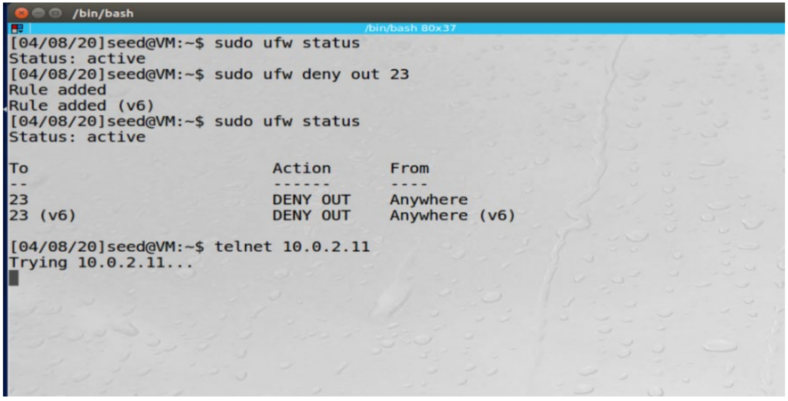
a) Telnet to Machine B through the firewall. Please describe your observation and explain how you are able to bypass the egress filtering.

Before the firewall, we can still establish telnet connections.



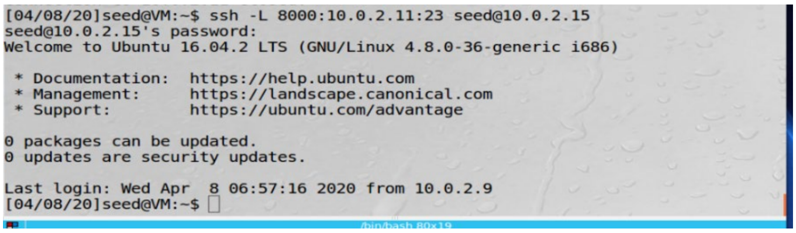
```
[04/08/20]seed@VM:~$ telnet 10.0.2.11
Trying 10.0.2.11...
Connected to 10.0.2.11.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Wed Apr  8 06:35:27 EDT 2020 from 10.0.2.9 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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.

[04/08/20]seed@VM:~$
```

After adding the rule to ufw, we cannot connect to machine B via telnet.



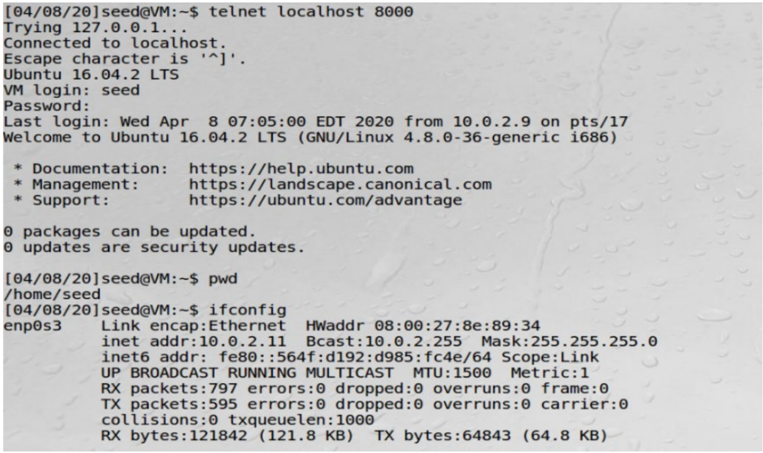
```
[04/08/20]seed@VM:~$ sudo ufw status
Status: active
[04/08/20]seed@VM:~$ sudo ufw deny out 23
Rule added
Rule added (v6)
[04/08/20]seed@VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23                         DENY OUT    Anywhere
23 (v6)                    DENY OUT    Anywhere (v6)

[04/08/20]seed@VM:~$ telnet 10.0.2.11
Trying 10.0.2.11...
```

We can use the command ssh -L to establish a ssh tunnel through machine C with address 10.0.2.15. The command forwards our local port 8000 to port 23 on machine B through machine C.



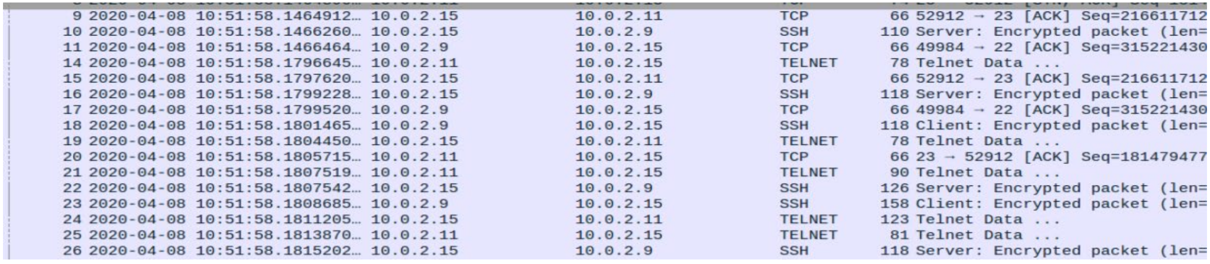
```
[04/08/20]seed@VM:~$ ssh -L 8000:10.0.2.11:23 seed@10.0.2.15
seed@10.0.2.15's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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 Apr  8 06:57:16 2020 from 10.0.2.9
[04/08/20]seed@VM:~$ 
```

After the tunnelling, we can establish a telnet connection to machine B.



```
[04/08/20]seed@VM:~$ 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: Wed Apr  8 07:05:00 EDT 2020 from 10.0.2.9 on pts/17
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.

[04/08/20]seed@VM:~$ pwd
/home/seed
[04/08/20]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:8e:89:34
          inet addr:10.0.2.11  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::564f:d192:d985:fc4e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:797 errors:0 dropped:0 overruns:0 frame:0
          TX packets:595 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:121842 (121.8 KB)  TX bytes:64843 (64.8 KB)
```

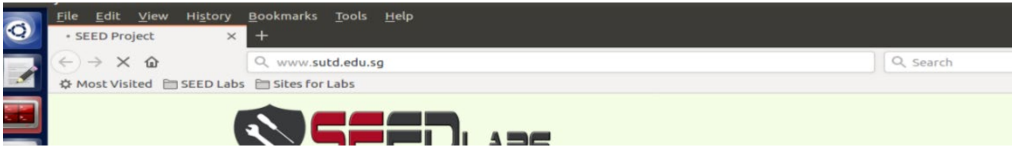
SSH tunnelling works in this scenario as we can bind our local port 8000 to the machine C 10.0.2.15 through an SSH connection. This machine will then forward our packets to machine B's telnet port. Using this method, we can securely bidirectionally transfer telnet packets from A to B bypassing the firewall. This is also shown in the screenshot below where 10.0.2.15 forwards the packets to 10.0.2.11.



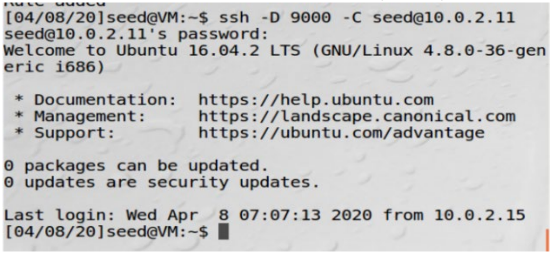
```
 9 2020-04-08 10:51:58.1464912… 10.0.2.15     10.0.2.11     TCP       66 52912 → 23 [ACK] Seq=216611712
10 2020-04-08 10:51:58.1466260… 10.0.2.15     10.0.2.9      SSH      110 Server: Encrypted packet (len=
11 2020-04-08 10:51:58.1466464… 10.0.2.9      10.0.2.15     TCP       66 49984 → 22 [ACK] Seq=315221430
14 2020-04-08 10:51:58.1796645… 10.0.2.11     10.0.2.15     TELNET    78 Telnet Data ...
15 2020-04-08 10:51:58.1797620… 10.0.2.15     10.0.2.11     TCP       66 52912 → 23 [ACK] Seq=216611712
16 2020-04-08 10:51:58.1799228… 10.0.2.15     10.0.2.9      SSH      118 Server: Encrypted packet (len=
17 2020-04-08 10:51:58.1799520… 10.0.2.9      10.0.2.15     TCP       66 49984 → 22 [ACK] Seq=315221430
18 2020-04-08 10:51:58.1801465… 10.0.2.9      10.0.2.15     SSH      118 Client: Encrypted packet (len=
19 2020-04-08 10:51:58.1804450… 10.0.2.15     10.0.2.11     TELNET    78 Telnet Data ...
20 2020-04-08 10:51:58.1805715… 10.0.2.11     10.0.2.15     TCP       66 23 → 52912 [ACK] Seq=181479477
21 2020-04-08 10:51:58.1807519… 10.0.2.11     10.0.2.15     TELNET    90 Telnet Data ...
22 2020-04-08 10:51:58.1807542… 10.0.2.15     10.0.2.9      SSH      126 Server: Encrypted packet (len=
23 2020-04-08 10:51:58.1808685… 10.0.2.9      10.0.2.15     SSH      158 Client: Encrypted packet (len=
24 2020-04-08 10:51:58.1811205… 10.0.2.15     10.0.2.11     TELNET   123 Telnet Data ...
25 2020-04-08 10:51:58.1813870… 10.0.2.11     10.0.2.15     TELNET    81 Telnet Data ...
26 2020-04-08 10:51:58.1815202… 10.0.2.15     10.0.2.9      SSH      118 Server: Encrypted packet (len=
```

b) 1. **Run Firefox and go visit the Facebook page. Can you see the Facebook page? Please describe your observation.**

Before setting up the tunnelling we are unable to access the site.

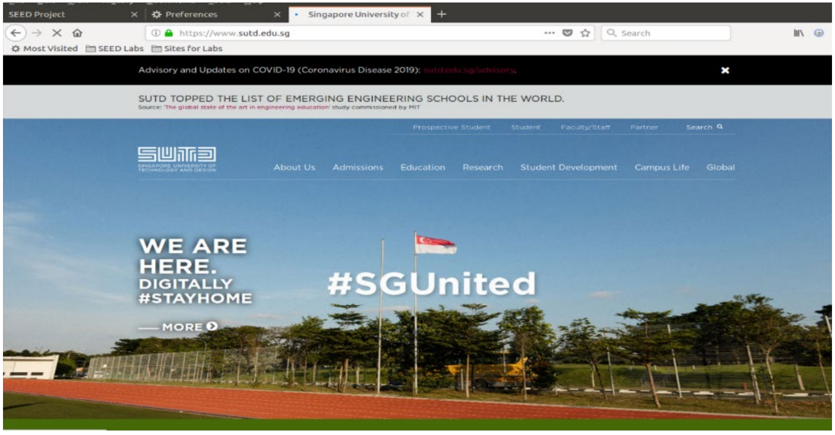


The ssh command used to set up a dynamic SSH tunnel



```
[04/08/20]seed@VM:~$ ssh -D 9000 -C 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-gen
eric 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 Apr  8 07:07:13 2020 from 10.0.2.15
[04/08/20]seed@VM:~$ 
```

Instead of facebook’s page, I used www.sutd.edu.sg for a more stable IP. We are able to access through tunnelling.

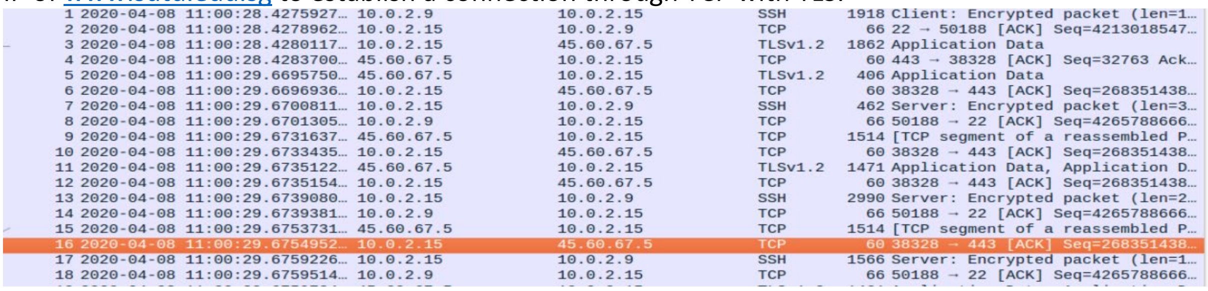


Advisory and Updates on COVID-19 (Coronavirus Disease 2019): sutd.edu.sg/advisory.

SUTD TOPPED THE LIST OF EMERGING ENGINEERING SCHOOLS IN THE WORLD.

Source: 'The global state of the art in engineering education' study commissioned by MIT

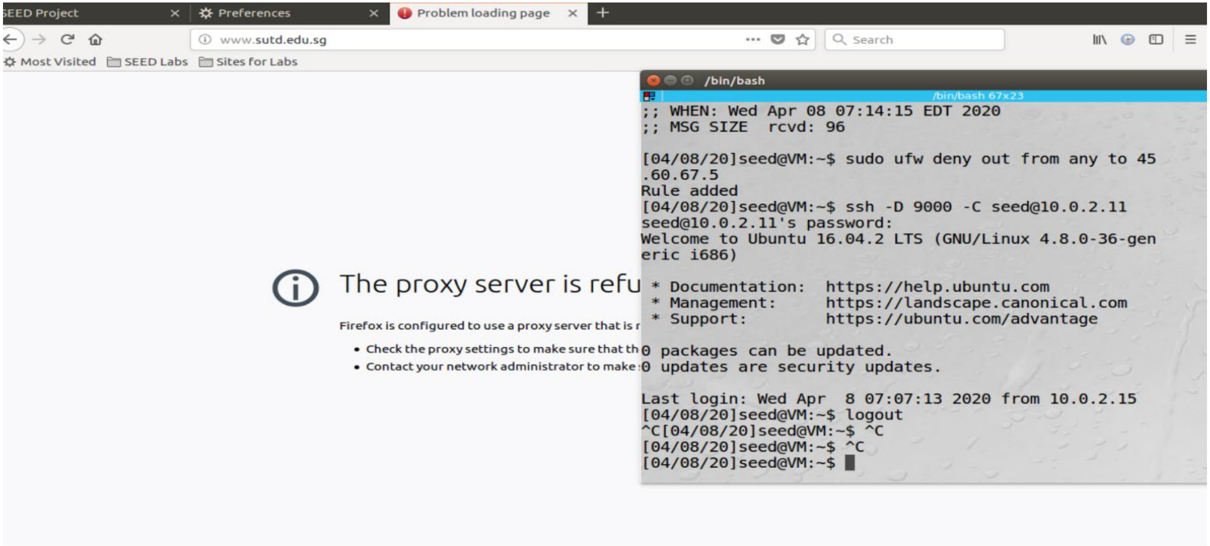
Below shows the traffic through SSH to 10.0.2.15 which is our jump server, and then to the IP of www.sutd.edu.sg to establish a connection through TCP with TLS.



```
 1 2020-04-08 11:00:28.4275927… 10.0.2.9     10.0.2.15    SSH      1918 Client: Encrypted packet (len=1…
 2 2020-04-08 11:00:28.4278962… 10.0.2.15    10.0.2.9     TCP        66 22 → 50188 [ACK] Seq=4213018547…
 3 2020-04-08 11:00:28.4280117… 10.0.2.15    45.60.67.5   TLSv1.2  1862 Application Data
 4 2020-04-08 11:00:28.4283700… 45.60.67.5   10.0.2.15    TCP        60 443 → 38328 [ACK] Seq=32763 Ack…
 5 2020-04-08 11:00:29.6695750… 45.60.67.5   10.0.2.15    TLSv1.2   406 Application Data
 6 2020-04-08 11:00:29.6696936… 10.0.2.15    45.60.67.5   TCP        60 38328 → 443 [ACK] Seq=268351438…
 7 2020-04-08 11:00:29.6700811… 10.0.2.15    10.0.2.9     SSH       462 Server: Encrypted packet (len=3…
 8 2020-04-08 11:00:29.6701305… 10.0.2.9     10.0.2.15    TCP        66 50188 → 22 [ACK] Seq=4265788666…
 9 2020-04-08 11:00:29.6731637… 45.60.67.5   10.0.2.15    TCP      1514 [TCP segment of a reassembled P…
10 2020-04-08 11:00:29.6733435… 10.0.2.15    45.60.67.5   TCP        60 38328 → 443 [ACK] Seq=268351438…
11 2020-04-08 11:00:29.6735122… 45.60.67.5   10.0.2.15    TLSv1.2  1471 Application Data, Application D…
12 2020-04-08 11:00:29.6735154… 10.0.2.15    45.60.67.5   TCP        60 38328 → 443 [ACK] Seq=268351438…
13 2020-04-08 11:00:29.6739080… 10.0.2.15    10.0.2.9     SSH      2990 Server: Encrypted packet (len=2…
14 2020-04-08 11:00:29.6739381… 10.0.2.9     10.0.2.15    TCP        66 50188 → 22 [ACK] Seq=4265788666…
15 2020-04-08 11:00:29.6753731… 45.60.67.5   10.0.2.15    TCP      1514 [TCP segment of a reassembled P…
16 2020-04-08 11:00:29.6754952… 10.0.2.15    45.60.67.5   TCP        60 38328 → 443 [ACK] Seq=268351438…
17 2020-04-08 11:00:29.6759226… 10.0.2.15    10.0.2.9     SSH      1566 Server: Encrypted packet (len=1…
18 2020-04-08 11:00:29.6759514… 10.0.2.9     10.0.2.15    TCP        66 50188 → 22 [ACK] Seq=4265788666…
```

2) **After you get the facebook page, break the SSH tunnel, clear the Firefox cache, and try the connection again. Please describe your observation.**

After cutting the connection, we are not able to access the website. This is because we are using the tunnel as a proxy and now that the tunnel has been broken, we are not able to forward packets to the IP of the server.



The proxy server is refu

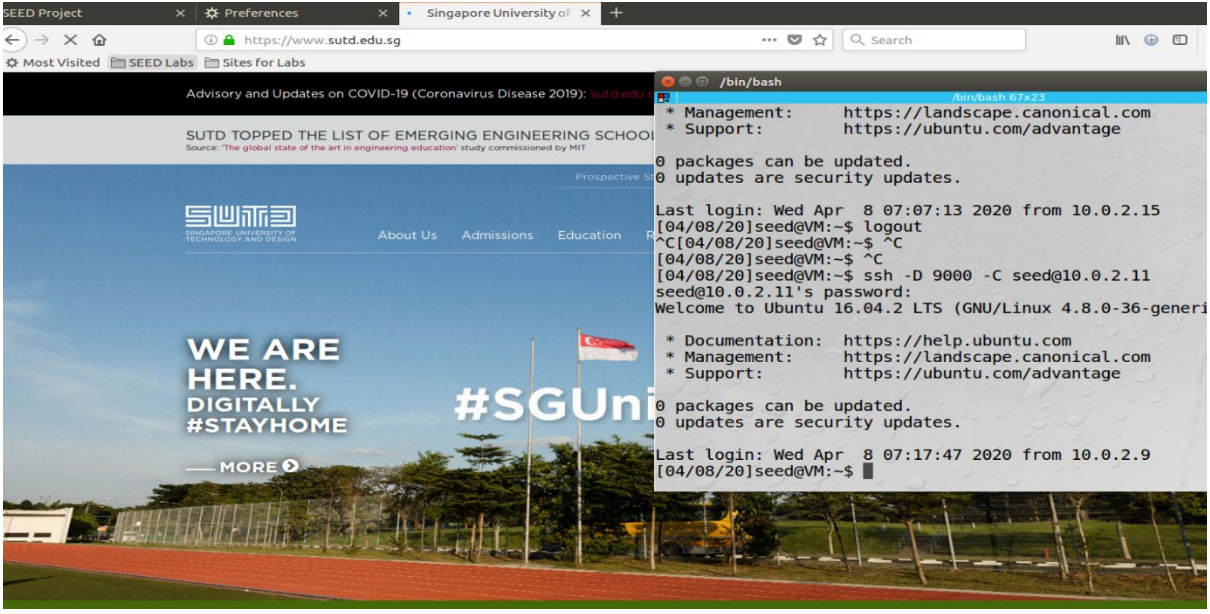
Firefox is configured to use a proxy server that is r

- Check the proxy settings to make sure that th
- Contact your network administrator to make :

```
;; WHEN: Wed Apr 08 07:14:15 EDT 2020
;; MSG SIZE  rcvd: 96

[04/08/20]seed@VM:~$ sudo ufw deny out from any to 45
.60.67.5
Rule added
[04/08/20]seed@VM:~$ ssh -D 9000 -C 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-gen
eric 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 Apr  8 07:07:13 2020 from 10.0.2.15
[04/08/20]seed@VM:~$ logout
^C[04/08/20]seed@VM:~$ ^C
[04/08/20]seed@VM:~$ ^C
[04/08/20]seed@VM:~$ 
```

3) **Establish the SSH tunnel again and connect to Facebook. Describe your observation.**

After we establish the connection again, we are able to access the website.


SEED Project
Preferences
Singapore University of
https://www.sutd.edu.sg
Search
Most Visited
SEED Labs
Sites for Labs
Advisory and Updates on COVID-19 (Coronavirus Disease 2019): sutd.edu.s
SUTD TOPPED THE LIST OF EMERGING ENGINEERING SCHOOI
Source: 'The global state of the art in engineering education' study commissioned by MIT
Prospective St
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
About Us
Admissions
Education
WE ARE HERE.
DIGITALLY #STAYHOME
MORE
#SGUni
/bin/bash
/bin/bash 67x23

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

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

Last login: Wed Apr  8 07:07:13 2020 from 10.0.2.15
[04/08/20]seed@VM:~$ logout
^C[04/08/20]seed@VM:~$ ^C
[04/08/20]seed@VM:~$ ^C
[04/08/20]seed@VM:~$ ssh -D 9000 -C 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-generi

 * 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 Apr  8 07:17:47 2020 from 10.0.2.9
[04/08/20]seed@VM:~$ 
```

4) We are able to bypass the egress filtering as seen in the earlier tasks as we are using machine C as a proxy server to tunnel our requests through port 9000 on machine C’s end via SSH. This will then allow machine C to send out packets to the IP we want to visit without being restricted by the firewall on our local machine. As seen in the earlier wireshark captures, the packets get forwarded through the SSH connection and sent to the correct IP of the website.