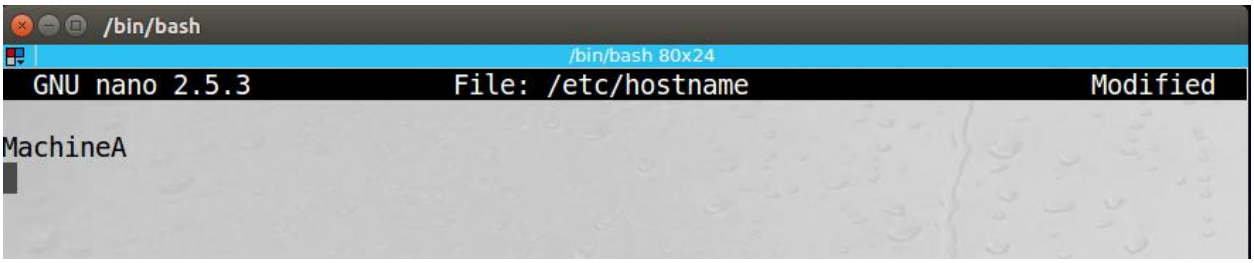
Machine A – 192.168.85.136

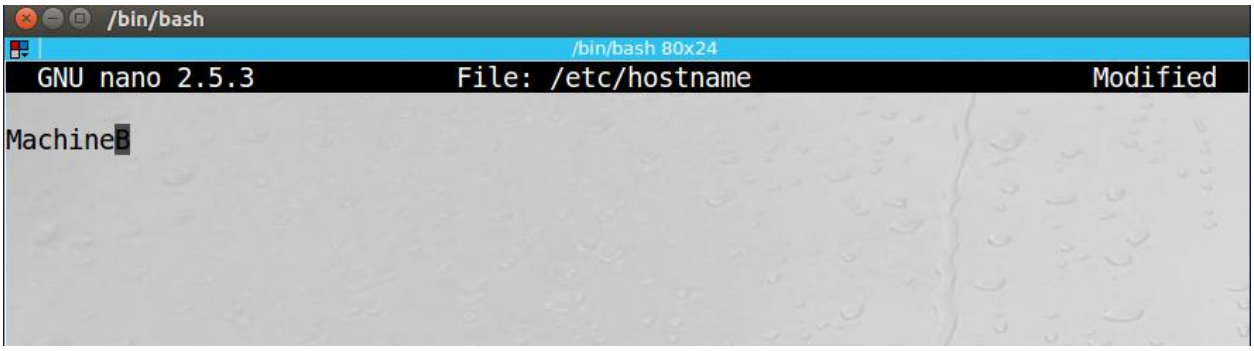
Machine B – 192.168.85.137

Machine C – 192.168.85.138

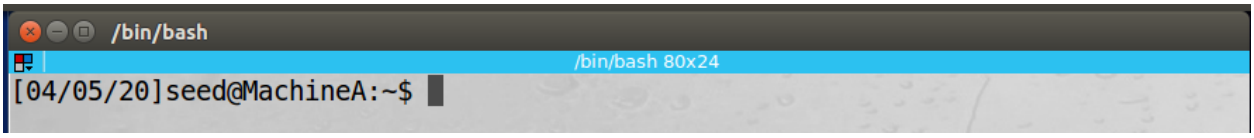
Task 1

Setting up hostnames for 2 clients, calling them MachineA and MachineB for identification in /etc/hostname.





Rebooting the machine to commit the changes.



Using UFW to use the iptables to block live communication passing through each machine.

Changing input policy to accept incoming traffic to the iptables.

```
# Set the default input policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_INPUT_POLICY="ACCEPT"
```

```
[04/05/20]seed@MachineB:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

Restarting Firewall…

Now trying to telnet to machine B from Machine A. Should be able to, because there is no firewall policy set for it to block.

```
[04/05/20]seed@MachineA:~$ telnet 192.168.85.137
Trying 192.168.85.137...
Connected to 192.168.85.137.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
MachineB 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
```

Now adding the command ufw to the terminal and them policy commands. Ufw deny out, following with IP's, will stop Machine A (192.168.85.136) to connect to Machine B (192.168.85.137) using Telent.

```
[04/05/20]seed@MachineB:~$ exit
logout
Connection closed by foreign host.
[04/05/20]seed@MachineA:~$ sudo ufw deny out from 192.168.85.136 to 192.168.85.1
37 port 23
Rule added
[04/05/20]seed@MachineA:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
192.168.85.137 23          DENY OUT    192.168.85.136

[04/05/20]seed@MachineA:~$ sudo ufw enable
```

Testing if I'm able to telnet like last time.

```
[04/05/20]seed@MachineA:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
192.168.85.137 23          DENY OUT    192.168.85.136

[04/05/20]seed@MachineA:~$ telnet 192.168.85.137
Trying 192.168.85.137...
```

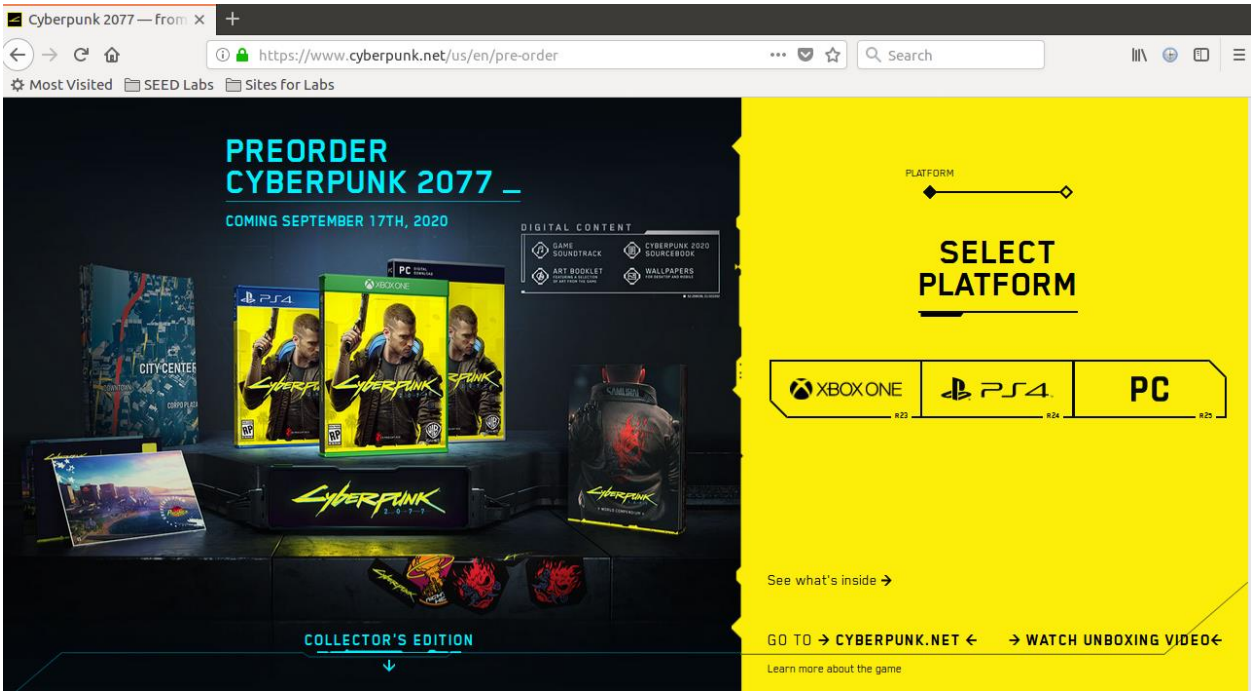
Since I added the firewall entry, I am unable to telnet to Machine B.

Same for the cases on Machine B to Machine A.

```
To                         Action      From
--                         ------      ----
192.168.85.136 23          DENY OUT    192.168.85.137

[04/05/20]seed@MachineB:~$ telnet 192.168.85.136
Trying 192.168.85.136...
```

Preventing A from visiting external website

Here is a site I want to block, to block it, I need to get the public IP for the site, and to that I used NS lookup to find two IP that points to the webserver.




```
[04/05/20]seed@MachineA:~$ nslookup www.cyberpunk.net
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
www.cyberpunk.net       canonical name = cyberpunk.net.edgekey.net.
cyberpunk.net.edgekey.net       canonical name = e25361.f.akamaiedge.net.
Name:   e25361.f.akamaiedge.net
Address: 23.59.250.80
Name:   e25361.f.akamaiedge.net
Address: 23.59.250.26
```

Now denying traffic to machine A to go to the cyberpunk.net

```
[04/05/20]seed@MachineA:~$ sudo ufw deny out from 192.168.85.136 to 23.59.250.80
 port 443
Rule added
[04/05/20]seed@MachineA:~$ sudo ufw deny out from 192.168.85.136 to 23.59.250.26
 port 443
Rule added
[04/05/20]seed@MachineA:~$ sudo ufw enable
Firewall is active and enabled on system startup
[04/05/20]seed@MachineA:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
192.168.85.137 23          DENY OUT    192.168.85.136
23.59.250.80 443           DENY OUT    192.168.85.136
23.59.250.26 443           DENY OUT    192.168.85.136
```


```
[04/05/20]seed@MachineA:~$ ping www.cyberpunk.net -p 443
PATTERN: 0x4403
PING e25361.f.akamaiedge.net (23.59.250.80) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
```

Used the Web client to connect. I'm unable to connect, and was not able to ping https traffic to the cyberpunk traffic.

Task 3

Blocking Telnet and Facebook traffic from machine A; Trying to evade firewall within Machine A.

```
Connection to 192.168.85.137 closed.
[04/05/20]seed@MachineA:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
23/tcp                     DENY OUT    Anywhere
31.13.71.36                DENY OUT    192.168.85.136
23/tcp (v6)                DENY OUT    Anywhere (v6)

[04/05/20]seed@MachineA:~$ telnet 192.168.85.137
Trying 192.168.85.137...
```

```
PING facebook.com (31.13.71.36) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
```

```
To                         Action      From
--                         ------      ----
23/tcp                     DENY OUT    Anywhere
31.13.71.36                DENY OUT    192.168.85.137
23/tcp (v6)                DENY OUT    Anywhere (v6)
```

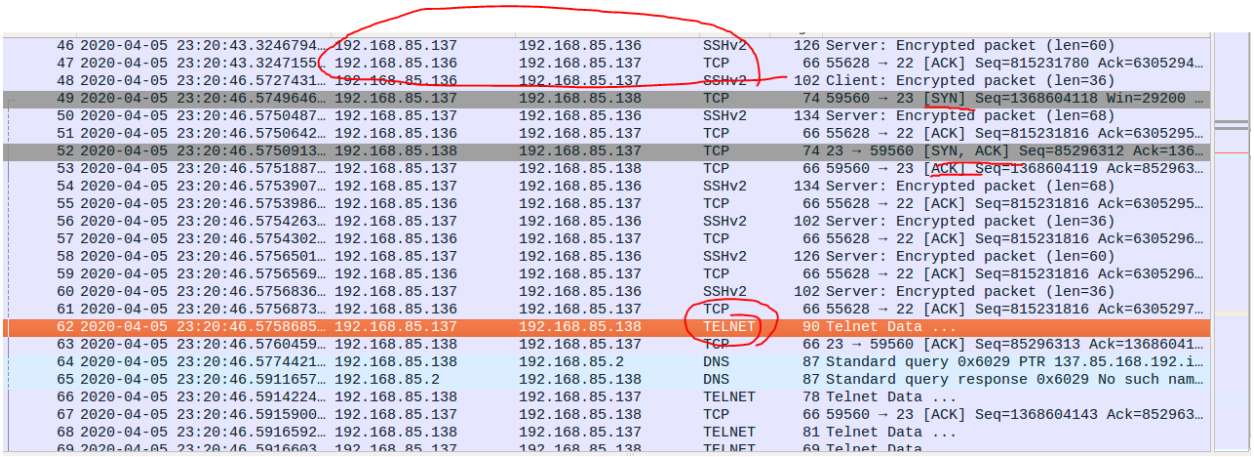
To do that, User within the firewall can connect to a machine outside the firewall and become the proxy to communicate with blocked traffic.

Task 3a

Created SSH connection to port 8000 using the telnet protocol 23 and connect it to machine B. With that, I'm able to connect to telnet servers using Machine B as my middleman.

```
[04/05/20]seed@MachineA:~$ ssh -L 8000:192.168.85.138:23 192.168.85.137
seed@192.168.85.137'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 Apr  5 23:10:21 2020 from 192.168.85.136
[04/05/20]seed@MachineB:~$ telnet 192.168.85.138
Trying 192.168.85.138...
Connected to 192.168.85.138.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
MachineC login:
```

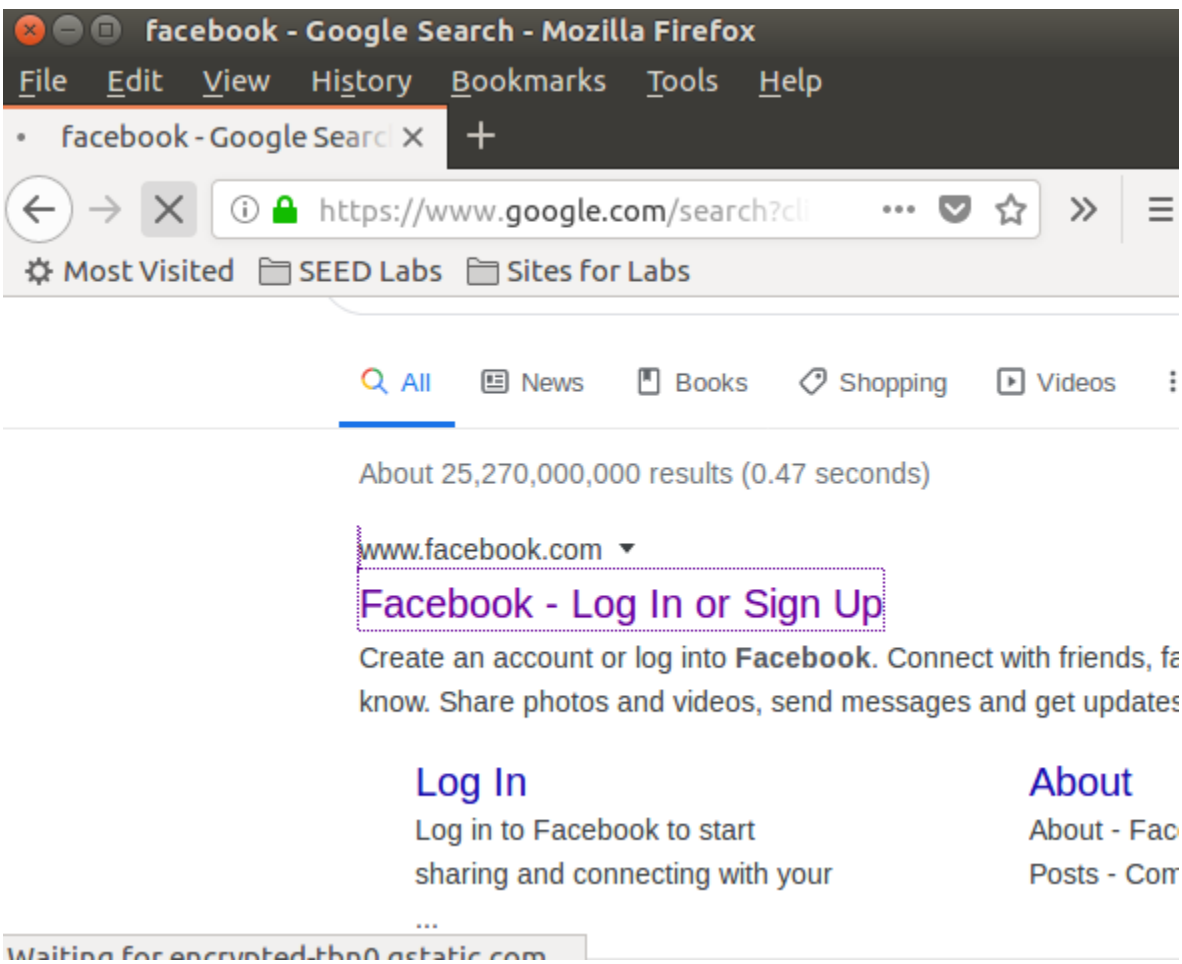
Here within Wireshark, we can see the traffic of A making SSH connection to B then making a telnet connection to machine C which evaded the firewall.



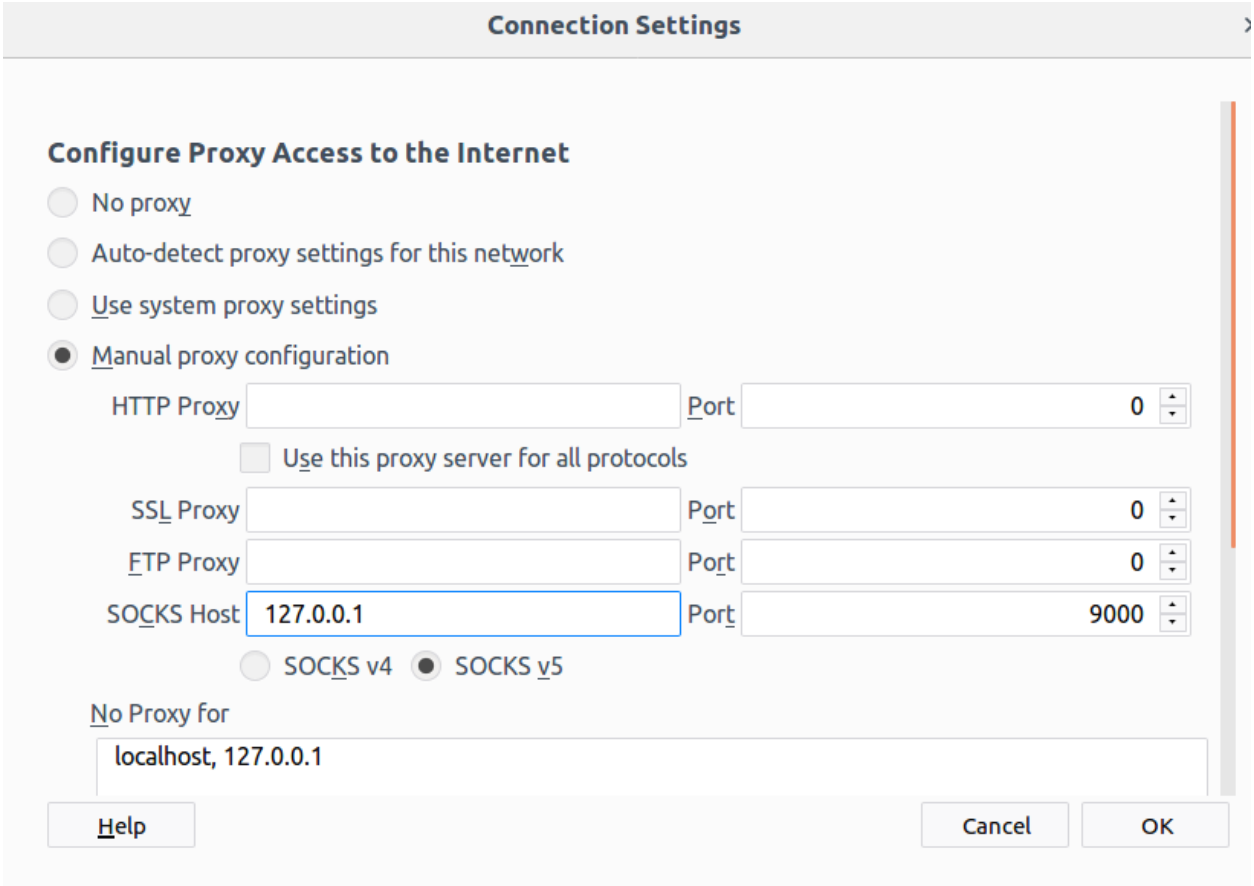
46	2020-04-05 23:20:43.3246794…	192.168.85.137	192.168.85.136	SSHv2	126	Server: Encrypted packet (len=60)
47	2020-04-05 23:20:43.3247155…	192.168.85.136	192.168.85.137	TCP	66	55628 → 22 [ACK] Seq=815231780 Ack=6305294…
48	2020-04-05 23:20:46.5727431…	192.168.85.136	192.168.85.137	SSHv2	102	Client: Encrypted packet (len=36)
49	2020-04-05 23:20:46.5749646…	192.168.85.137	192.168.85.138	TCP	74	59560 → 23 [SYN] Seq=1368604118 Win=29200 …
50	2020-04-05 23:20:46.5750487…	192.168.85.137	192.168.85.136	SSHv2	134	Server: Encrypted packet (len=68)
51	2020-04-05 23:20:46.5750642…	192.168.85.136	192.168.85.137	TCP	66	55628 → 22 [ACK] Seq=815231816 Ack=6305295…
52	2020-04-05 23:20:46.5750913…	192.168.85.138	192.168.85.137	TCP	74	23 → 59560 [SYN, ACK] Seq=85296312 Ack=136…
53	2020-04-05 23:20:46.5751887…	192.168.85.137	192.168.85.138	TCP	66	59560 → 23 [ACK] Seq=1368604119 Ack=852963…
54	2020-04-05 23:20:46.5753907…	192.168.85.137	192.168.85.136	SSHv2	134	Server: Encrypted packet (len=68)
55	2020-04-05 23:20:46.5753986…	192.168.85.136	192.168.85.137	TCP	66	55628 → 22 [ACK] Seq=815231816 Ack=6305295…
56	2020-04-05 23:20:46.5754263…	192.168.85.137	192.168.85.136	SSHv2	102	Server: Encrypted packet (len=36)
57	2020-04-05 23:20:46.5754302…	192.168.85.136	192.168.85.137	TCP	66	55628 → 22 [ACK] Seq=815231816 Ack=6305296…
58	2020-04-05 23:20:46.5756501…	192.168.85.137	192.168.85.136	SSHv2	126	Server: Encrypted packet (len=60)
59	2020-04-05 23:20:46.5756569…	192.168.85.136	192.168.85.137	TCP	66	55628 → 22 [ACK] Seq=815231816 Ack=6305296…
60	2020-04-05 23:20:46.5756836…	192.168.85.137	192.168.85.136	SSHv2	102	Server: Encrypted packet (len=36)
61	2020-04-05 23:20:46.5756873…	192.168.85.136	192.168.85.137	TCP	66	55628 → 22 [ACK] Seq=815231816 Ack=6305297…
62	2020-04-05 23:20:46.5758685…	192.168.85.137	192.168.85.138	TELNET	90	Telnet Data ...
63	2020-04-05 23:20:46.5760459…	192.168.85.138	192.168.85.137	TCP	66	23 → 59560 [ACK] Seq=85296313 Ack=13686041…
64	2020-04-05 23:20:46.5774421…	192.168.85.138	192.168.85.2	DNS	87	Standard query 0x6029 PTR 137.85.168.192.i…
65	2020-04-05 23:20:46.5911657…	192.168.85.2	192.168.85.138	DNS	87	Standard query response 0x6029 No such nam…
66	2020-04-05 23:20:46.5914224…	192.168.85.138	192.168.85.137	TELNET	78	Telnet Data ...
67	2020-04-05 23:20:46.5915900…	192.168.85.137	192.168.85.138	TCP	66	59560 → 23 [ACK] Seq=1368604143 Ack=852963…
68	2020-04-05 23:20:46.5916592…	192.168.85.138	192.168.85.137	TELNET	81	Telnet Data ...
69	2020-04-05 23:20:46.5916603…	192.168.85.137	192.168.85.138	TELNET	69	Telnet Data ...

Task 3b

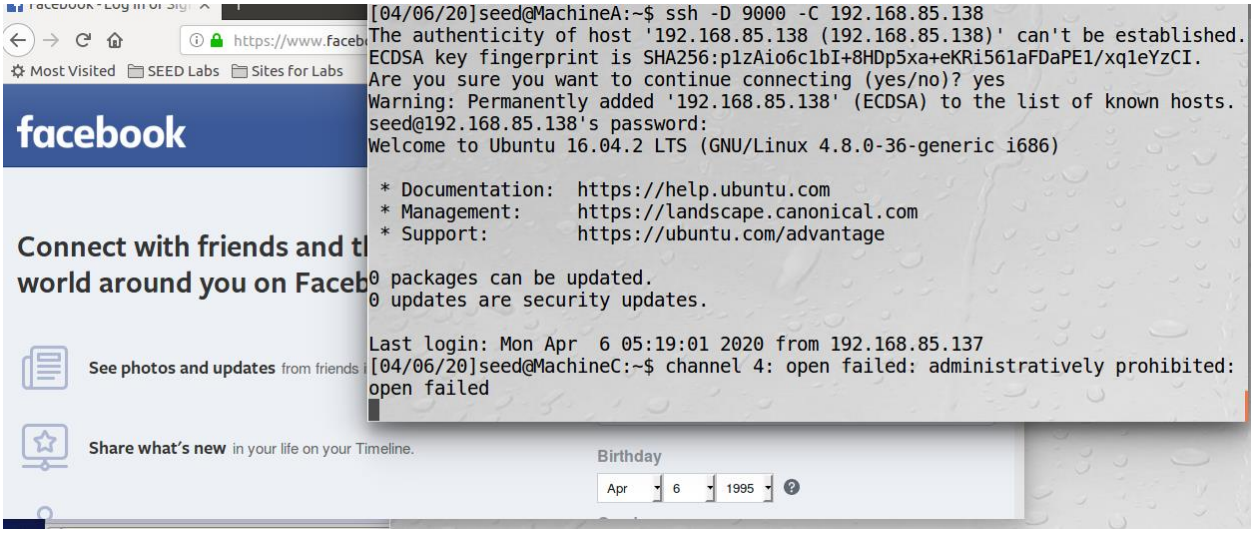
Facebook is block

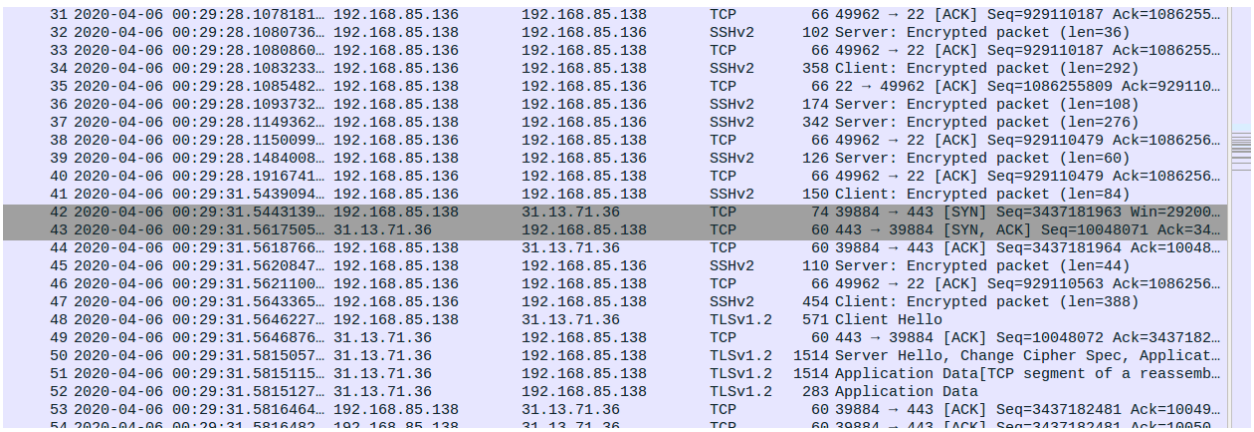


Created a proxy port to redirect traffic.



Added a proxy in Machine C web client; so when I connect to machine C, web traffic will acts a middle man for Machine A. Successfully access Facebook, even though Machine A have a firewall.

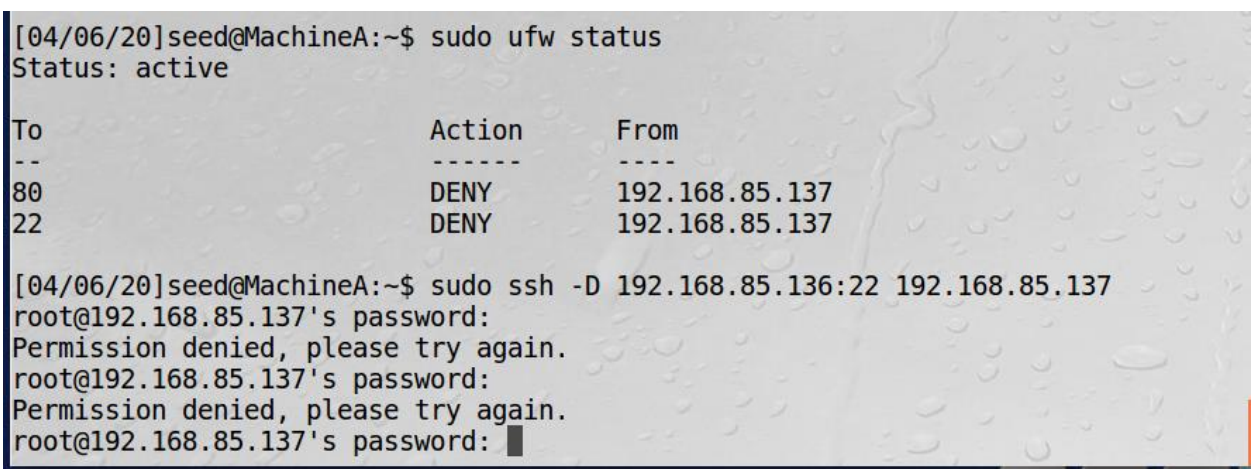




31	2020-04-06 00:29:28.1078181…	192.168.85.136	192.168.85.138	TCP	66	49962 → 22 [ACK] Seq=929110187 Ack=1086255…
32	2020-04-06 00:29:28.1080736…	192.168.85.138	192.168.85.136	SSHv2	102	Server: Encrypted packet (len=36)
33	2020-04-06 00:29:28.1080860…	192.168.85.136	192.168.85.138	TCP	66	49962 → 22 [ACK] Seq=929110187 Ack=1086255…
34	2020-04-06 00:29:28.1083233…	192.168.85.136	192.168.85.138	SSHv2	358	Client: Encrypted packet (len=292)
35	2020-04-06 00:29:28.1085482…	192.168.85.138	192.168.85.136	TCP	66	22 → 49962 [ACK] Seq=1086255809 Ack=929110…
36	2020-04-06 00:29:28.1093732…	192.168.85.138	192.168.85.136	SSHv2	174	Server: Encrypted packet (len=108)
37	2020-04-06 00:29:28.1149362…	192.168.85.138	192.168.85.136	SSHv2	342	Server: Encrypted packet (len=276)
38	2020-04-06 00:29:28.1150099…	192.168.85.136	192.168.85.138	TCP	66	49962 → 22 [ACK] Seq=929110479 Ack=1086256…
39	2020-04-06 00:29:28.1484008…	192.168.85.138	192.168.85.136	SSHv2	126	Server: Encrypted packet (len=60)
40	2020-04-06 00:29:28.1916741…	192.168.85.136	192.168.85.138	TCP	66	49962 → 22 [ACK] Seq=929110479 Ack=1086256…
41	2020-04-06 00:29:31.5439094…	192.168.85.136	192.168.85.138	SSHv2	150	Client: Encrypted packet (len=84)
42	2020-04-06 00:29:31.5443139…	192.168.85.138	31.13.71.36	TCP	74	39884 → 443 [SYN] Seq=3437181963 Win=29200…
43	2020-04-06 00:29:31.5617505…	31.13.71.36	192.168.85.138	TCP	60	443 → 39884 [SYN, ACK] Seq=10048071 Ack=34…
44	2020-04-06 00:29:31.5618766…	192.168.85.138	31.13.71.36	TCP	60	39884 → 443 [ACK] Seq=3437181964 Ack=10048…
45	2020-04-06 00:29:31.5620847…	192.168.85.138	192.168.85.136	SSHv2	110	Server: Encrypted packet (len=44)
46	2020-04-06 00:29:31.5621100…	192.168.85.136	192.168.85.138	TCP	66	49962 → 22 [ACK] Seq=929110563 Ack=1086256…
47	2020-04-06 00:29:31.5643365…	192.168.85.136	192.168.85.138	SSHv2	454	Client: Encrypted packet (len=388)
48	2020-04-06 00:29:31.5646227…	192.168.85.138	31.13.71.36	TLSv1.2	571	Client Hello
49	2020-04-06 00:29:31.5646876…	31.13.71.36	192.168.85.138	TCP	60	443 → 39884 [ACK] Seq=10048072 Ack=3437182…
50	2020-04-06 00:29:31.5815057…	31.13.71.36	192.168.85.138	TLSv1.2	1514	Server Hello, Change Cipher Spec, Applicat…
51	2020-04-06 00:29:31.5815115…	31.13.71.36	192.168.85.138	TLSv1.2	1514	Application Data[TCP segment of a reassemb…
52	2020-04-06 00:29:31.5815127…	31.13.71.36	192.168.85.138	TLSv1.2	283	Application Data
53	2020-04-06 00:29:31.5816464…	192.168.85.138	31.13.71.36	TCP	60	39884 → 443 [ACK] Seq=3437182481 Ack=10049…

Task 4

Now Blocking SSH and HTTP Traffic on Machine A and see if we can evade the firewall.



```
[04/06/20]seed@MachineA:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
80                         DENY        192.168.85.137
22                         DENY        192.168.85.137

[04/06/20]seed@MachineA:~$ sudo ssh -D 192.168.85.136:22 192.168.85.137
root@192.168.85.137's password:
Permission denied, please try again.
root@192.168.85.137's password:
Permission denied, please try again.
root@192.168.85.137's password:
```

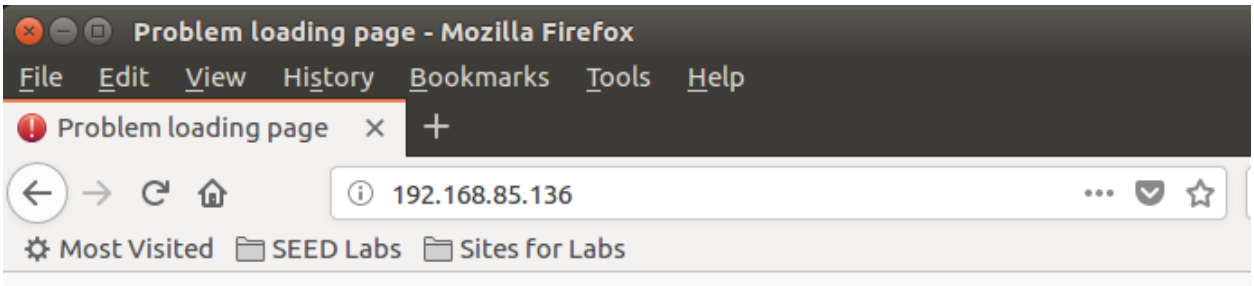
Here I created a SSH connection on port 9000 and made it evade the port that block the ssh firewall. Since it believe its port 9000 I connected to to SSH and able to ssh to other machine, Machine C.

```
[04/07/20]seed@MachineA:~$ ssh -D 9000:192.168.85.137:22 192.168.85.137
Bad dynamic forwarding specification '9000:192.168.85.137:22'
[04/07/20]seed@MachineA:~$ ssh -R 9000:192.168.85.137:22 192.168.85.137
seed@192.168.85.137'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: Tue Apr  7 04:40:30 2020 from 192.168.85.136
[04/07/20]seed@MachineB:~$
```

```
[04/07/20]seed@MachineB:~$ ssh 192.168.85.138
The authenticity of host '192.168.85.138 (192.168.85.138)' 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 '192.168.85.138' (ECDSA) to the list of known hosts.
seed@192.168.85.138'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: Mon Apr  6 06:27:36 2020 from 192.168.85.136
```

Here I had trouble with connect using http traffic, after setting up the web proxy I was unable to communicate to the web client.

I knowto create a reverse tunnel when users send an http request to port 8000. The ssh tunnel supposedly will forward the request to the ssh Client and forward the request to port 80 on machine A. No success at the moment.


Problem loading page - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Problem loading page
192.168.85.136
Most Visited
SEED Labs
Sites for Labs