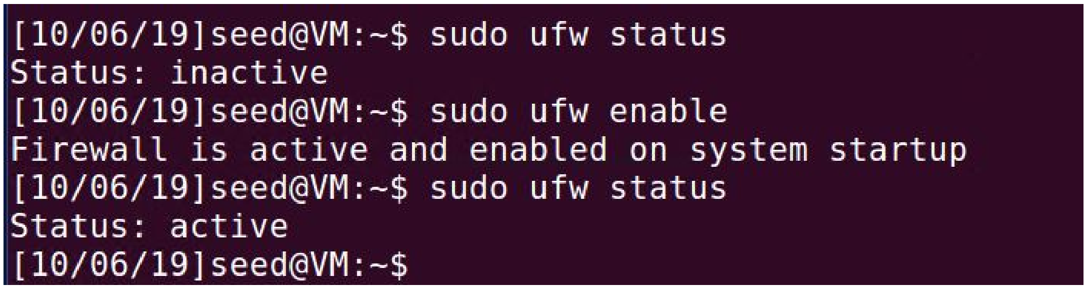
Lab 2 CPS 633 Section 5

Task 1

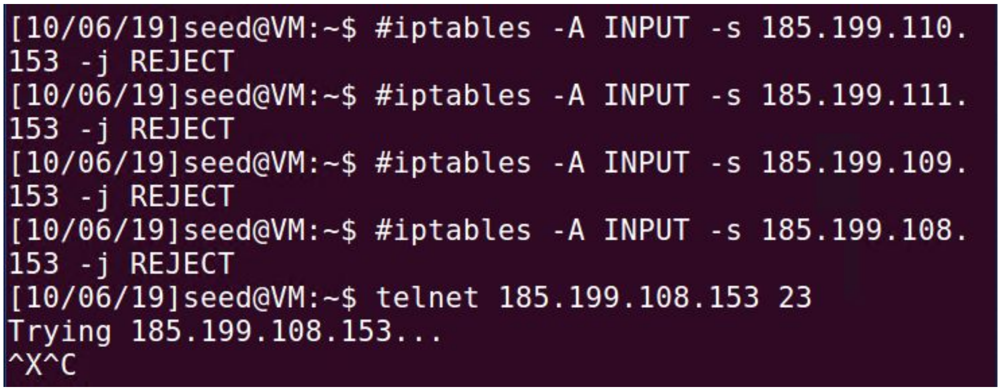
To enable firewall:



```
[10/06/19]seed@VM:~$ sudo ufw status
Status: inactive
[10/06/19]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
[10/06/19]seed@VM:~$ sudo ufw status
Status: active
[10/06/19]seed@VM:~$
```

1.	Changing DEFAULT_INPUT_POLICY=”DROP” to DEFAULT_INPUT_POLICY=”ACCEPT”	`$ sudo ufw default allow`
2.	Prevents Machine A from doing telnet to Machine B	$ sudo iptables -A INPUT -s 10.0.2.12 -j DROP
3.	Prevents Machine B from doing telnet to Machine A	$ sudo iptables -A INPUT -s 10.0.2.8 -j DROP

4.	Blocks the Machine A from accessing an external website (seedsecuritylabs.org)
	(seedsecuritylabs.org has 4 ip addresses) Ports:80 & 443
		$ sudo iptables -A INPUT -s 185.199.108.153 -j REJECT
		$ sudo iptables -A INPUT -s 185.199.109.153 -j REJECT
		$ sudo iptables -A INPUT -s 185.199.110.153 -j REJECT
		$ sudo iptables -A INPUT -s 185.199.111.153 -j REJECT



```
[10/06/19]seed@VM:~$ #iptables -A INPUT -s 185.199.110.
153 -j REJECT
[10/06/19]seed@VM:~$ #iptables -A INPUT -s 185.199.111.
153 -j REJECT
[10/06/19]seed@VM:~$ #iptables -A INPUT -s 185.199.109.
153 -j REJECT
[10/06/19]seed@VM:~$ #iptables -A INPUT -s 185.199.108.
153 -j REJECT
[10/06/19]seed@VM:~$ telnet 185.199.108.153 23
Trying 185.199.108.153...
^X^C
```

Telnet is not returning any message because a network or host firewall is dropping incoming connections.

For the above commands to work, we needed to turn on Telnet. We did this by doing the following:

1. Installing the package: `$sudo apt-get install telnetd`
2. Restarting Telnet: `$sudo /etc/init.d/open-bsd-inetd restart`
3. To connect with Machine B: `$telnet 10.0.2.12`

Task 2: Packet Filtering Module

NF_DROP: Net Filter Drop

```
unsigned int telnetFilter(void *priv, struct sk_buff *skb, const
struct nf_hook_state *state)
{
     return NF_DROP; // drops the packet
}
```

Task 3a

Task 3b

1. On running firefox and connecting to Facebook, Facebook was reachable. The proxy had no effect.

2. After the cache was reset on Firefox, facebook was no longer accessible. Also, the proxy blocked other websites as well.

3. On establishing the SSH tunnel again and connecting to Facebook, we were able to connect to Facebook.

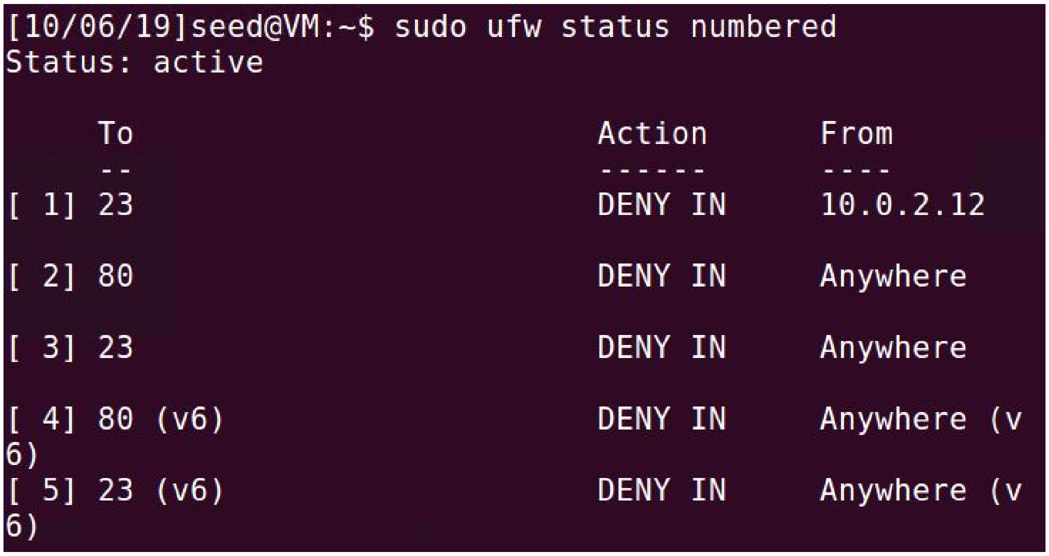
4. Machine B was not able to find the packet while it repeatedly searched for it

Following is a record from Wireshark:

```
18    PcsCompu_3c:50:53     Broadcast  2019-10-06 19:42:59.745236186
ARP   42    Who has 10.0.2.1? Tell 10.0.2.8
```

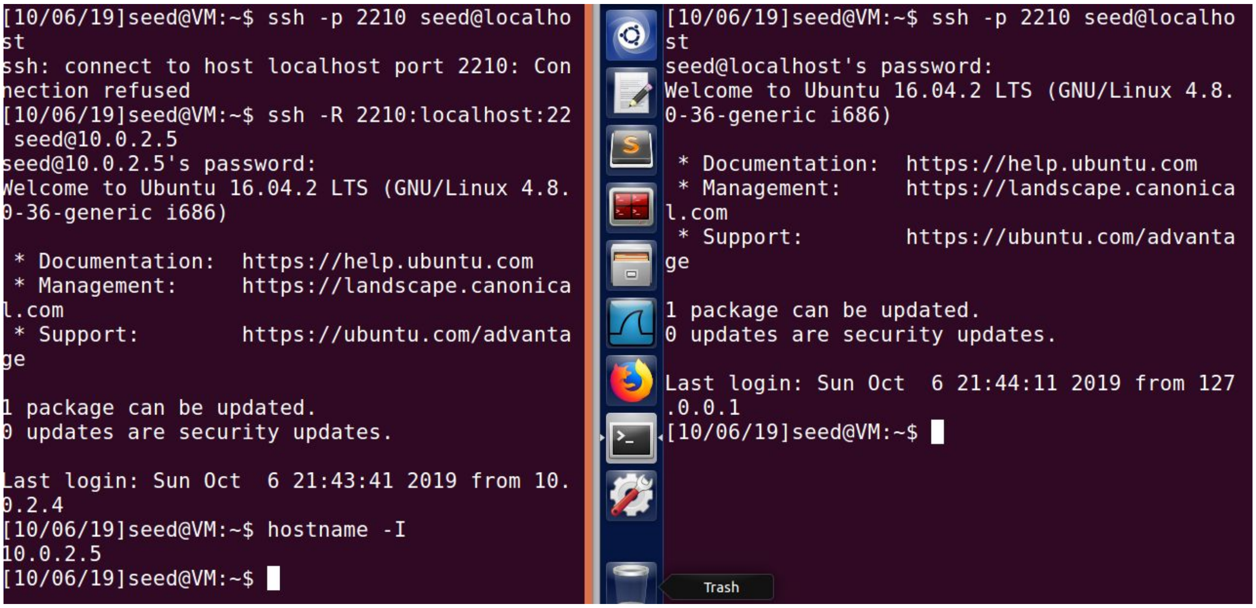
Task 4

Blocking port 80 and 23:



```
[10/06/19]seed@VM:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23                         DENY IN     10.0.2.12

[ 2] 80                         DENY IN     Anywhere

[ 3] 23                         DENY IN     Anywhere

[ 4] 80 (v6)                    DENY IN     Anywhere (v
6)
[ 5] 23 (v6)                    DENY IN     Anywhere (v
6)
```

Setting up SSH tunnel and Reverse SSH tunnel:



```
[10/06/19]seed@VM:~$ ssh -p 2210 seed@localho
st
ssh: connect to host localhost port 2210: Con
nection refused
[10/06/19]seed@VM:~$ ssh -R 2210:localhost:22
 seed@10.0.2.5
seed@10.0.2.5'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.canonica
l.com
 * Support:        https://ubuntu.com/advanta
ge

1 package can be updated.
0 updates are security updates.

Last login: Sun Oct  6 21:43:41 2019 from 10.
0.2.4
[10/06/19]seed@VM:~$ hostname -I
10.0.2.5
[10/06/19]seed@VM:~$ 
```

```
[10/06/19]seed@VM:~$ ssh -p 2210 seed@localho
st
seed@localhost'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.canonica
l.com
 * Support:        https://ubuntu.com/advanta
ge

1 package can be updated.
0 updates are security updates.

Last login: Sun Oct  6 21:44:11 2019 from 127
.0.0.1
[10/06/19]seed@VM:~$ 
```