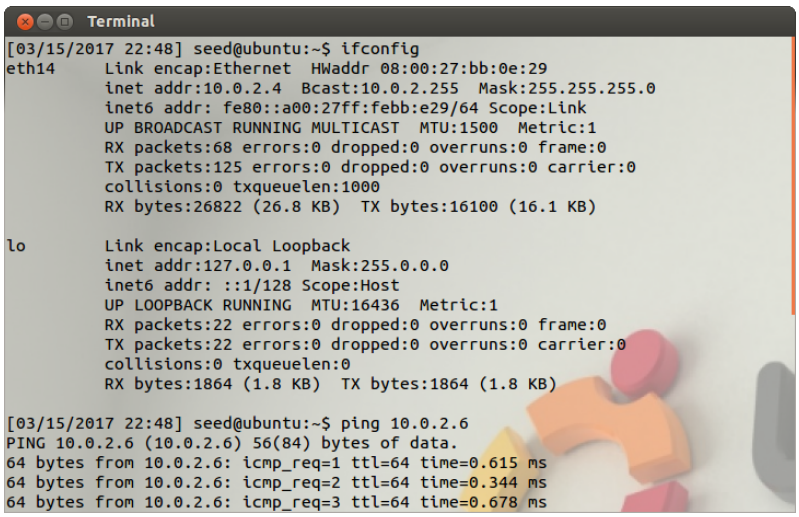
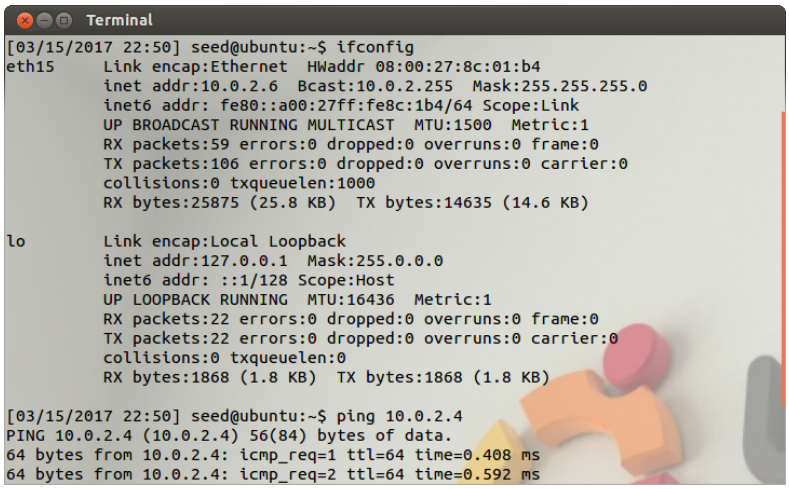
Lab #3 Linux Firewall Exploration Lab

Hualiang Li

Task 1:

First, I created 2 MVs. One of the IP is 10.0.2.4, the other one is 10.0.2.6. Then I ping each other to verify that they can communicate with each other without firewall:



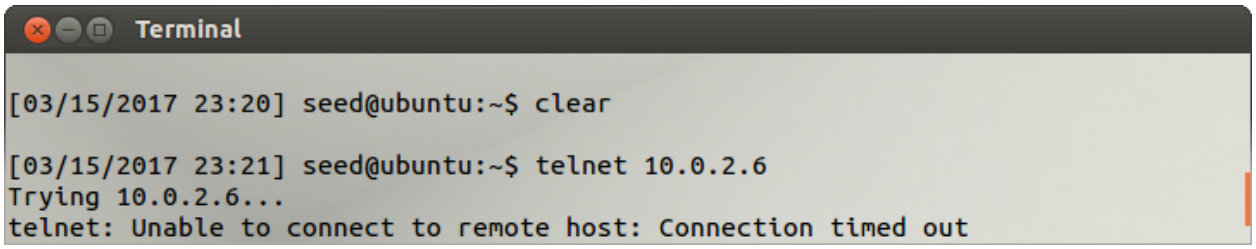


Then I created a telnet server and change ufw policy to allow.

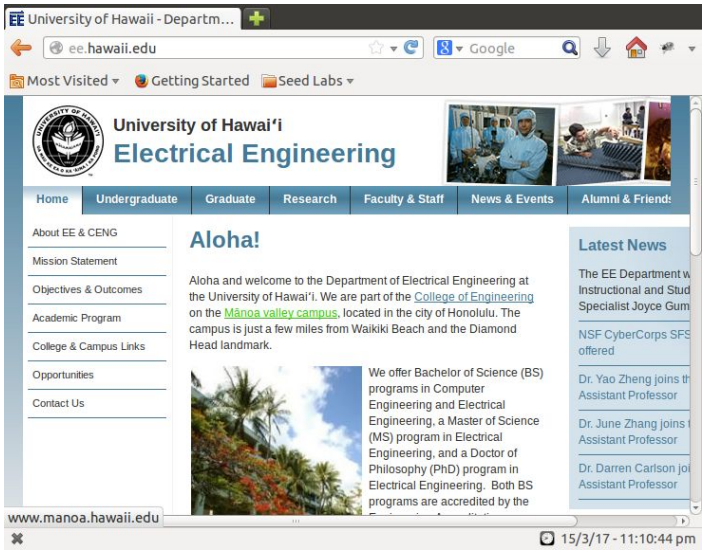
Before I set the rule, I can telnet to 10.0.2.6:

Then I set the rule for the firewall:

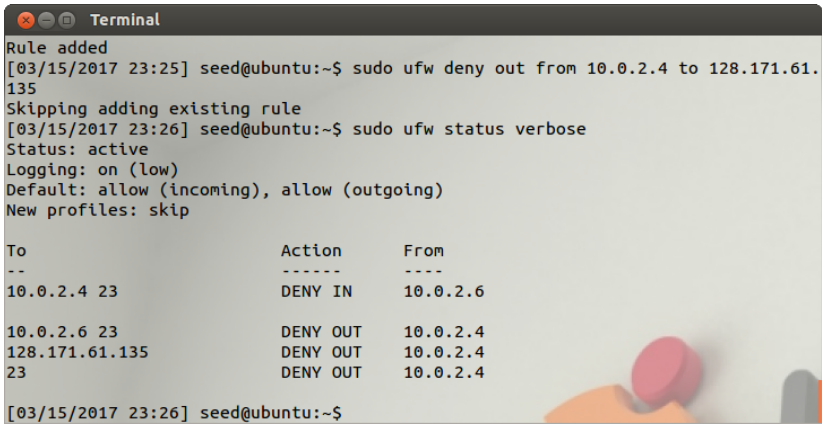
This prevent A from doing telnet to B and vice verse:



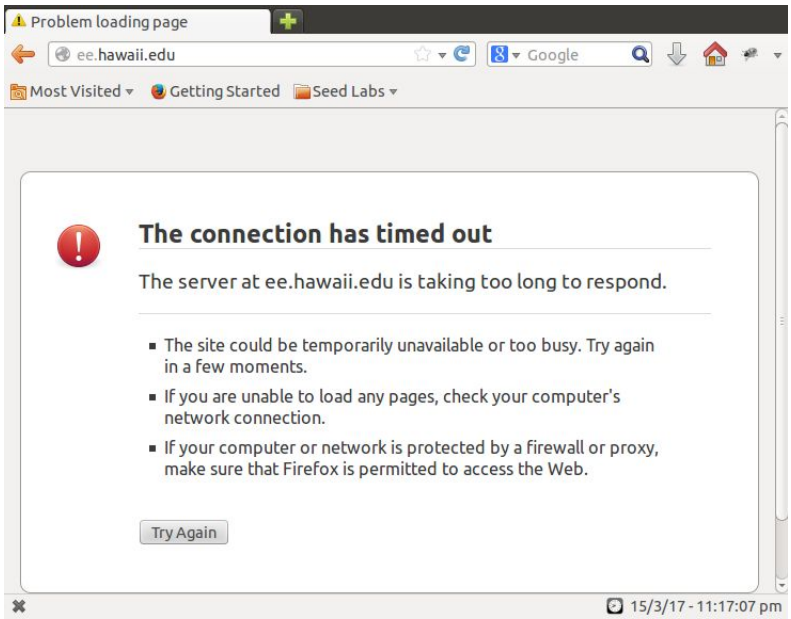
Then I try to block ee website:
before that, I verified I can access to EE website without any rules:



Then I add rule to block EE website:



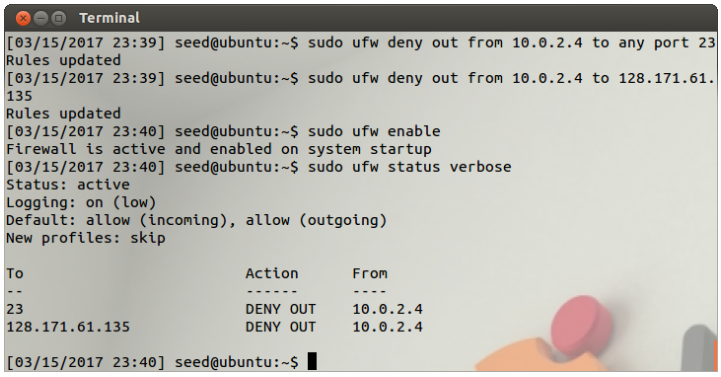
Then I try to open EE website again, it is not accessible any more:



From above, we can see that I successfully use Firewall to block certain network traffic.

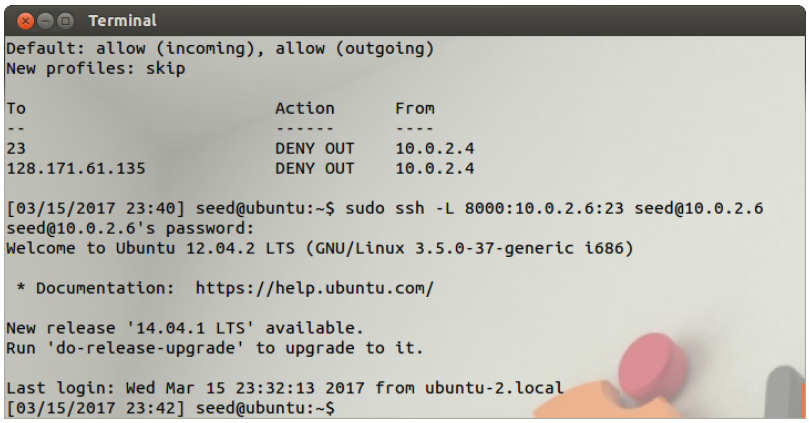
Task3:

First, I set up the block rules:

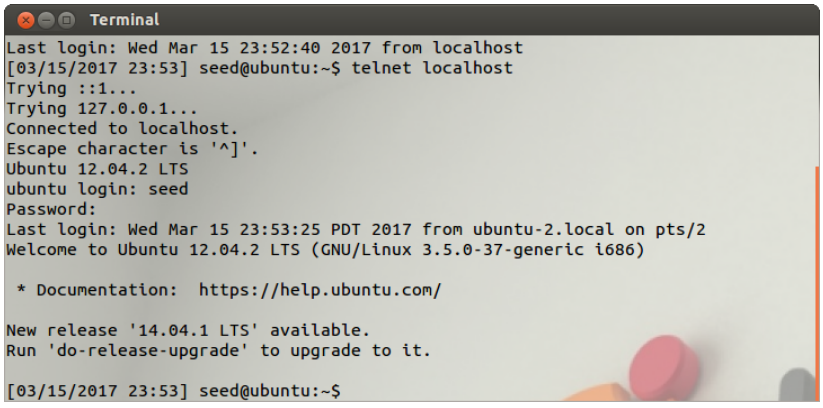


Task3a:

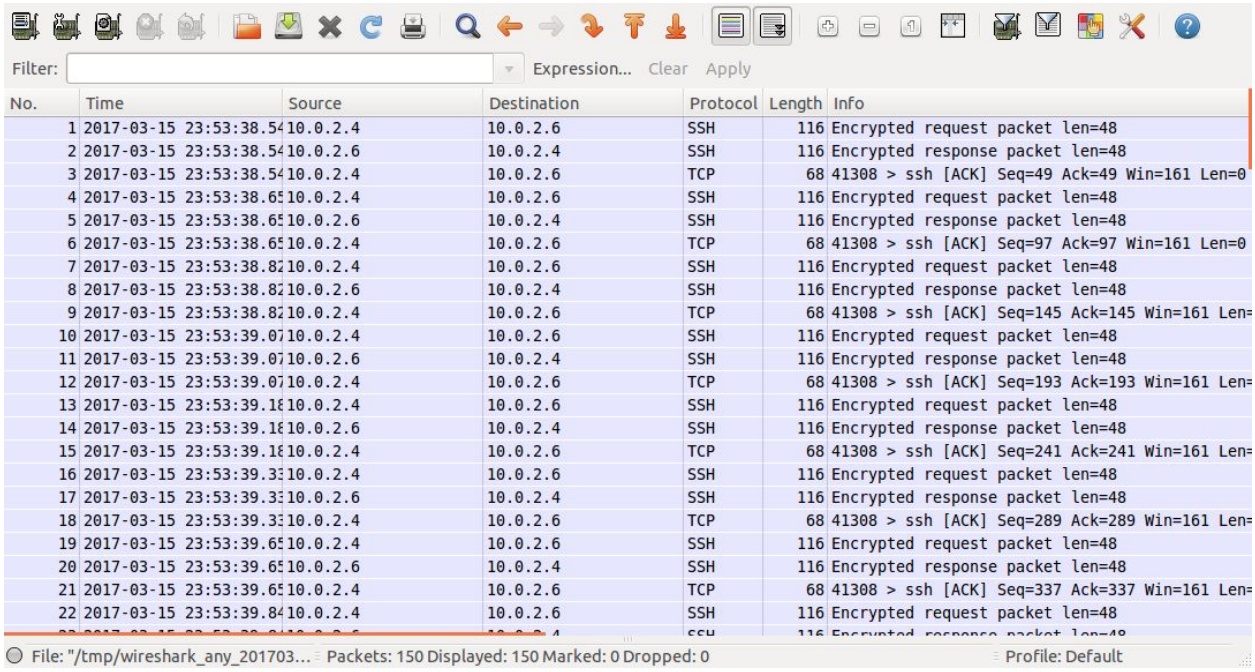
Then I setup a SSH tunnel between A and B:



Then I will try to telnet to B using port 8000:



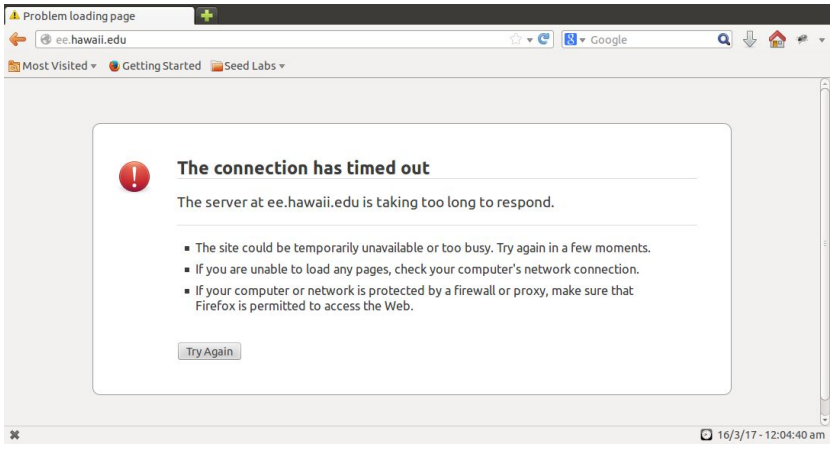
We can see that I can telnet to Machine B server, here is what is going on with wireshark:



We can see that the packet is forwarded to machine B through port 22 and then it SSH to port 23, thus access to telnet server on machine B.

Task3.b:

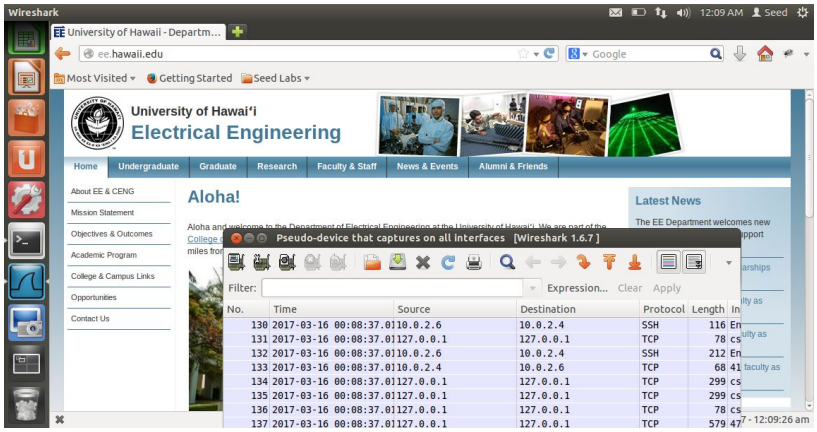
Before we do anything, I verified that I can not access to EE website by normal means:



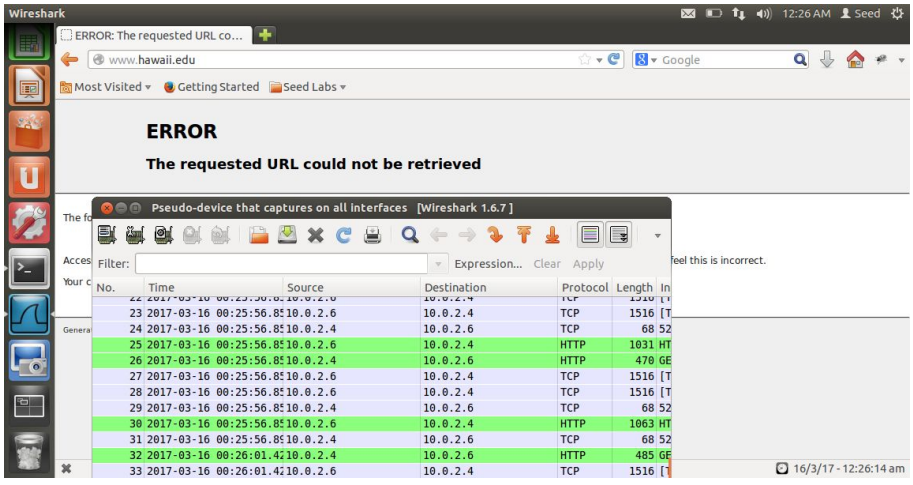
Then, Similar to a, firstly, I setup a SSH Tunnel:

```
Terminal
[03/16/2017 00:01] seed@ubuntu:~$ ssh -D 9000 -C seed@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ECDSA key fingerprint is 81:82:a9:af:bd:93:78:f9:1a:a7:ca:7f:e8:d6:6c:04.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.6' (ECDSA) to the list of known hosts.
seed@10.0.2.6's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Mar 15 23:58:45 2017 from localhost
[03/16/2017 00:03] seed@ubuntu:~$
```

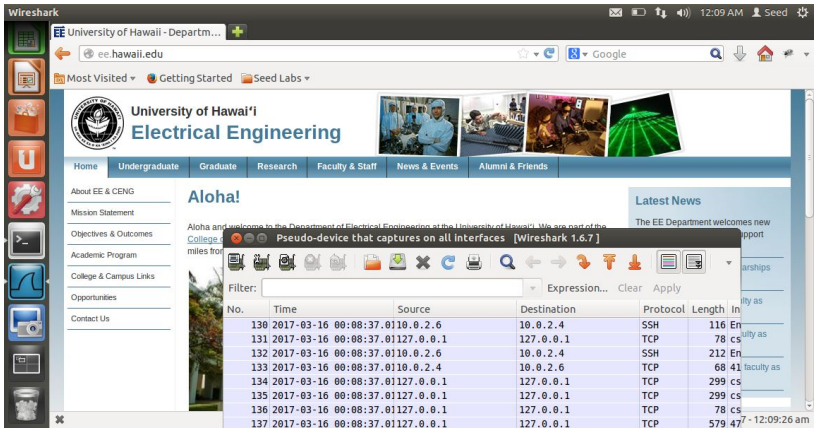
Then, I configured Firefox browser to use proxy as lab guideline says.
Finally, I opened EE website again, now I can access to it:



Then I break the SSH tunnel, and try to access to EE website, now, it is not working:
However, this time, it shows that the proxy server is refusing connections.



Now, establish the SSH tunnel again, the EE website can be accessed again.



From the above observation, we can conclude that with SSH tunnel, we can bypass the firewall blocking port 23 by using port 22 instead. Once a packet sent through port 22, it is then forwarded to the actual web server, the web server reply the packet through the reverse path.

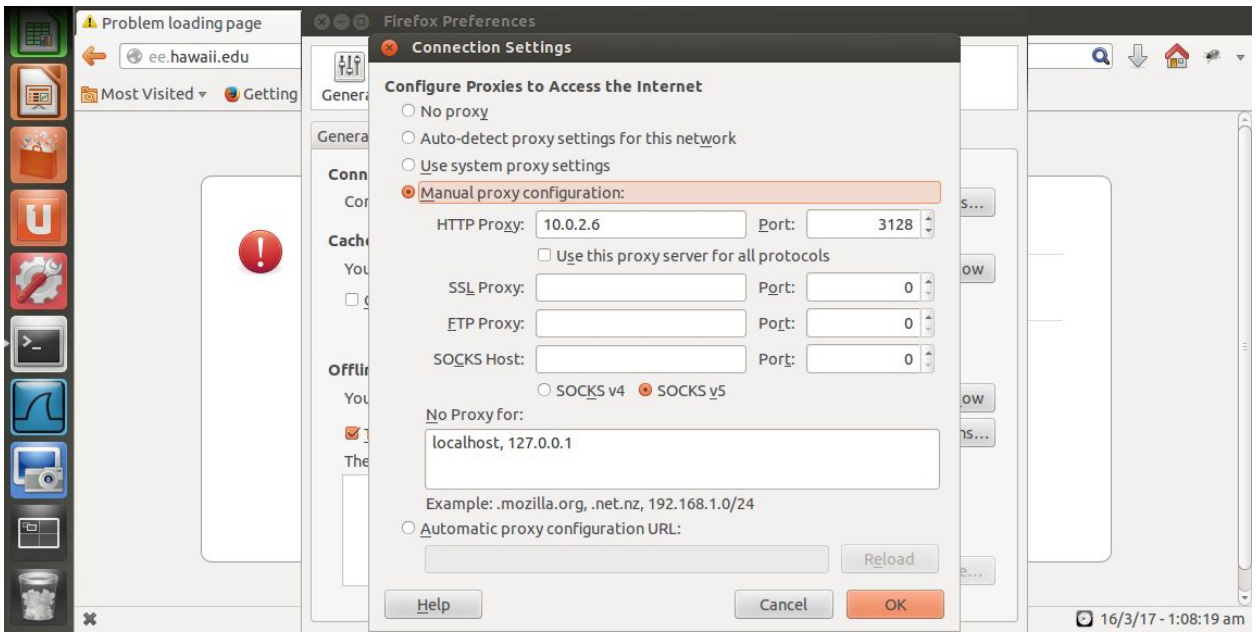
Question 4:

Yes, we can just change the default port 22 for SSH to another port number, for example port 1234, this can be done by editing /etc/ssh/sshd_config file.

Task 4:

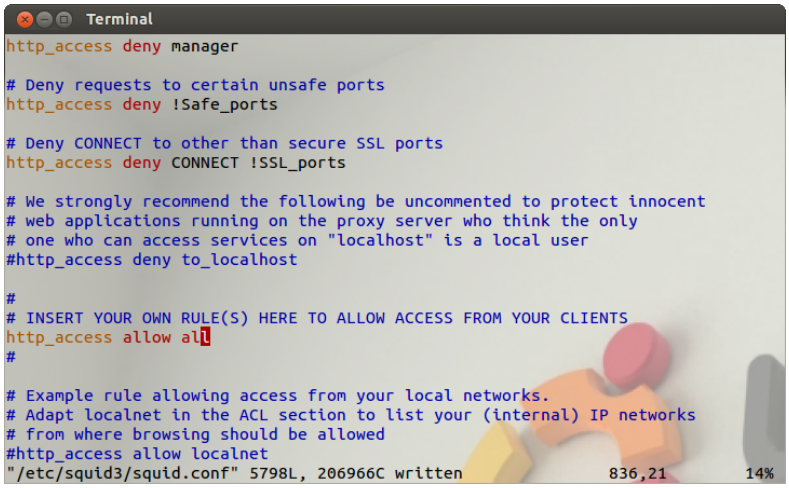
a:

Firstly, I have to setup Firefox to use HTTP proxy:

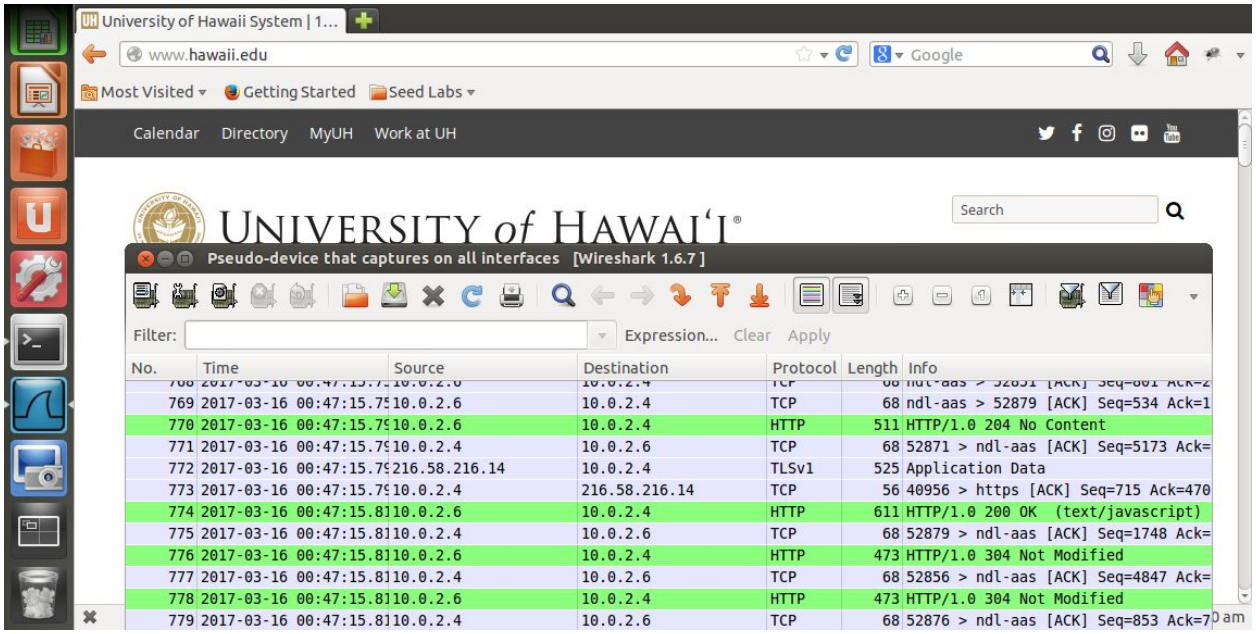


we can see that the EE web can not be visited, it shows the requested URL could not be retrieved.

Then I tried to look at the squid.conf file, I found that http_access is set to deny all. I then set it to allow all:

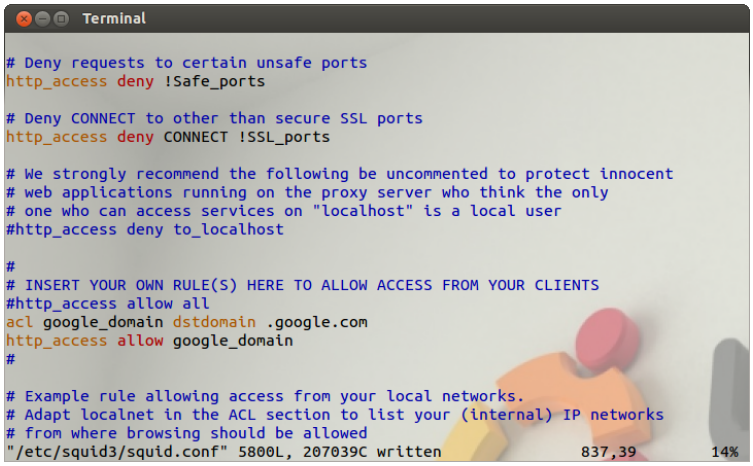


Then I can visit UH web:

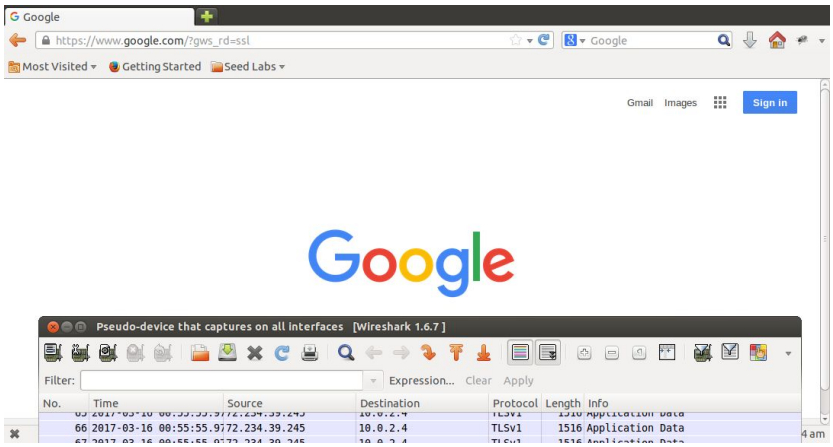


We can see from wireshark capture that the packet is transfered to machine B then using that machine, it requests HTTP to the actual web server. Then the web server reply and send packet to machine B, after that, machine B forwarded the web information to machine A.

Similar to google.com:
I change http_access rule to allow google domain by creating a acl name:
acl google_domain dstdomain .google.com

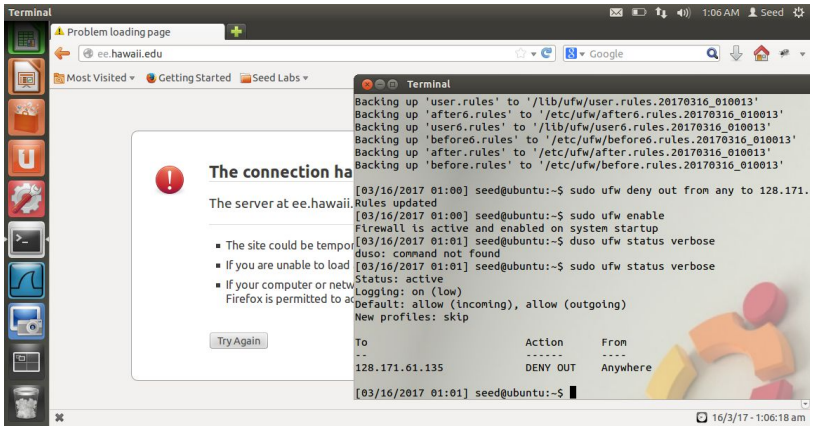


Then, I can access to google.com:

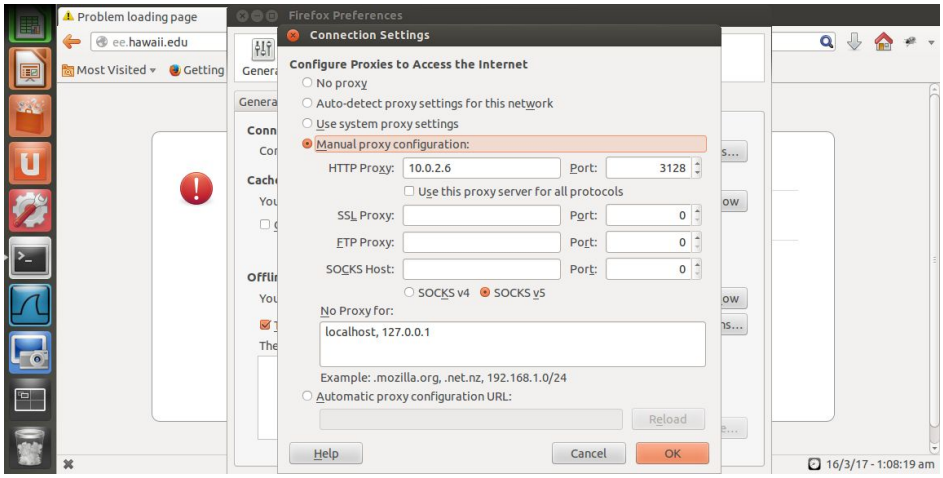


Task 4.b:

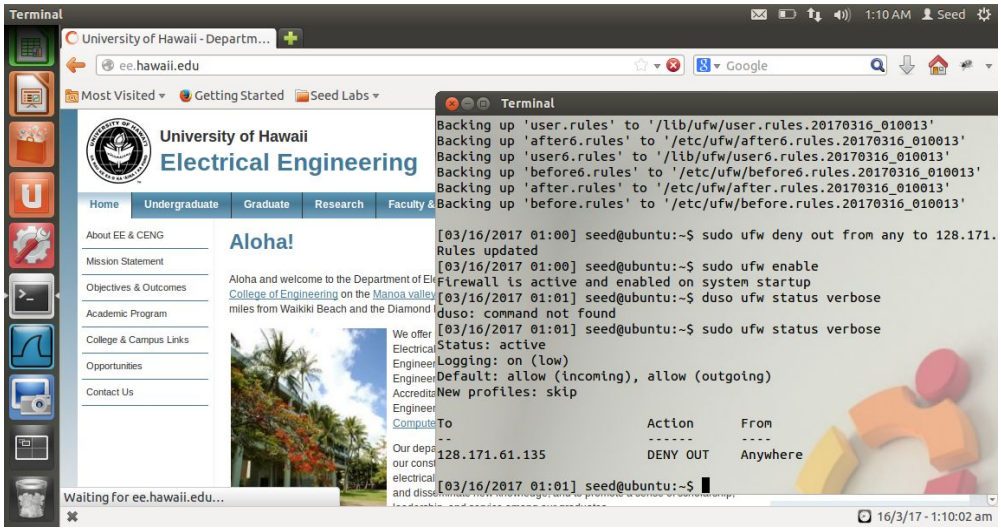
First, I verify that I can not visit ee website by using ufw firewall:



Then I used web proxy to bypass the firwall:



Now, I can access to EE website:



Question 5:

Yes, we can change the default port 3128 to another port, for example, port 1235, by editing squid.conf file: http_port 1235. Then we can access to external web even port 3128 is blocked.