

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:

```
Terminal
[03/15/2017 22:48] seed@ubuntu:~$ ifconfig
eth14    Link encap:Ethernet  HWaddr 08:00:27:bb:0e:29
         inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:febb:e29/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:68 errors:0 dropped:0 overruns:0 frame:0
         TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:26822 (26.8 KB)  TX bytes:16100 (16.1 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:16436  Metric:1
         RX packets:22 errors:0 dropped:0 overruns:0 frame:0
         TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:1864 (1.8 KB)  TX bytes:1864 (1.8 KB)

[03/15/2017 22:48] seed@ubuntu:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_req=1 ttl=64 time=0.615 ms
64 bytes from 10.0.2.6: icmp_req=2 ttl=64 time=0.344 ms
64 bytes from 10.0.2.6: icmp_req=3 ttl=64 time=0.678 ms
```

```
Terminal
[03/15/2017 22:50] seed@ubuntu:~$ ifconfig
eth15    Link encap:Ethernet  HWaddr 08:00:27:8c:01:b4
         inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fe8c:1b4/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:59 errors:0 dropped:0 overruns:0 frame:0
         TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:25875 (25.8 KB)  TX bytes:14635 (14.6 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:16436  Metric:1
         RX packets:22 errors:0 dropped:0 overruns:0 frame:0
         TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:1868 (1.8 KB)  TX bytes:1868 (1.8 KB)

[03/15/2017 22:50] seed@ubuntu:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_req=1 ttl=64 time=0.408 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.592 ms
```

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:

```
Terminal
[03/15/2017 23:01] seed@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
[03/15/2017 23:02] seed@ubuntu:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing)
New profiles: skip
[03/15/2017 23:02] seed@ubuntu:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Wed Mar 15 02:41:14 PDT 2017 from ubuntu-2.local on pts/4
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.

[03/15/2017 23:02] seed@ubuntu:~$
```

Then I set the rule for the firewall:

```
Terminal
[03/15/2017 23:03] seed@ubuntu:~$ sudo ufw deny out from 10.0.2.4 to 10.0.2.6 port 23
Rule added
[03/15/2017 23:04] seed@ubuntu:~$ sudo ufw deny in from 10.0.2.6 to 10.0.2.4 port 23
Rule added
[03/15/2017 23:05] seed@ubuntu:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing)
New profiles: skip

To Action From
--
10.0.2.4 23 DENY IN 10.0.2.6
10.0.2.6 23 DENY OUT 10.0.2.4

[03/15/2017 23:05] seed@ubuntu:~$
```

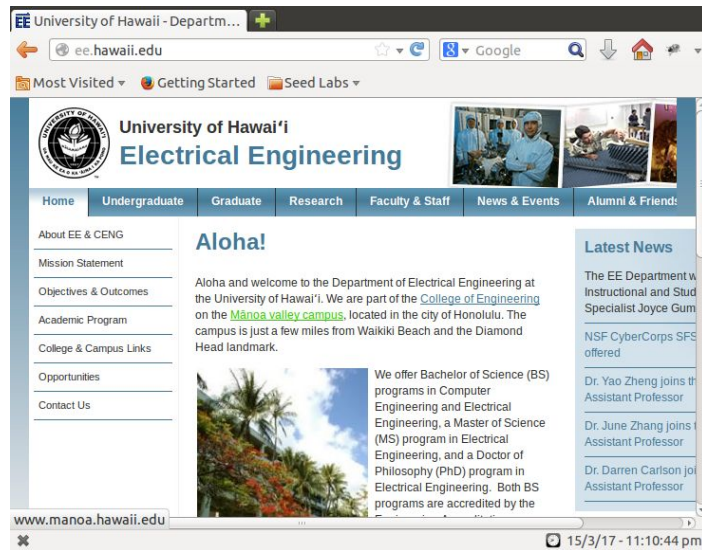
This prevent A from doing telnet to B and vice verse:

```
Terminal
[03/15/2017 23:20] seed@ubuntu:~$ clear

[03/15/2017 23:21] seed@ubuntu:~$ telnet 10.0.2.6
Trying 10.0.2.6...
telnet: Unable to connect to remote host: Connection timed out
```

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:

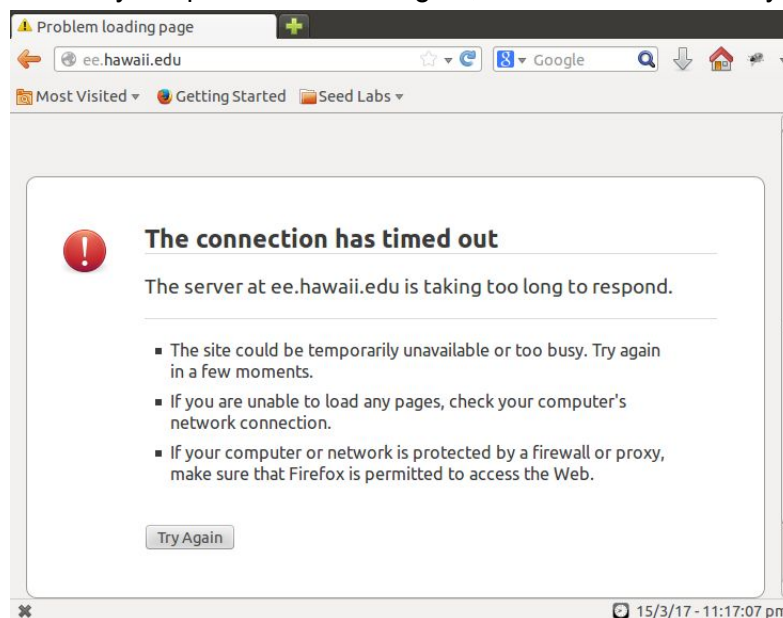
```

Terminal
Rule added
[03/15/2017 23:25] seed@ubuntu:~$ sudo ufw deny out from 10.0.2.4 to 128.171.61.135
Skipping adding existing rule
[03/15/2017 23:26] seed@ubuntu:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing)
New profiles: skip

To Action From
--
10.0.2.4 23 DENY IN 10.0.2.6
10.0.2.6 23 DENY OUT 10.0.2.4
128.171.61.135 23 DENY OUT 10.0.2.4
[03/15/2017 23:26] seed@ubuntu:~$

```

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:

```
Terminal
[03/15/2017 23:39] seed@ubuntu:~$ sudo ufw deny out from 10.0.2.4 to any port 23
Rules updated
[03/15/2017 23:39] seed@ubuntu:~$ sudo ufw deny out from 10.0.2.4 to 128.171.61.
135
Rules updated
[03/15/2017 23:40] seed@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
[03/15/2017 23:40] seed@ubuntu:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing)
New profiles: skip

To Action From
--
23 DENY OUT 10.0.2.4
128.171.61.135 DENY OUT 10.0.2.4
[03/15/2017 23:40] seed@ubuntu:~$
```

Task3a:

Then I setup a SSH tunnel between A and B:

```
Terminal
Default: allow (incoming), allow (outgoing)
New profiles: skip

To Action From
--
23 DENY OUT 10.0.2.4
128.171.61.135 DENY OUT 10.0.2.4

[03/15/2017 23:40] seed@ubuntu:~$ sudo ssh -L 8000:10.0.2.6:23 seed@10.0.2.6
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 23:32:13 2017 from ubuntu-2.local
[03/15/2017 23:42] seed@ubuntu:~$
```

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

```
Terminal
Last login: Wed Mar 15 23:52:40 2017 from localhost
[03/15/2017 23:53] seed@ubuntu:~$ telnet localhost
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Wed Mar 15 23:53:25 PDT 2017 from ubuntu-2.local on pts/2
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.
[03/15/2017 23:53] seed@ubuntu:~$
```

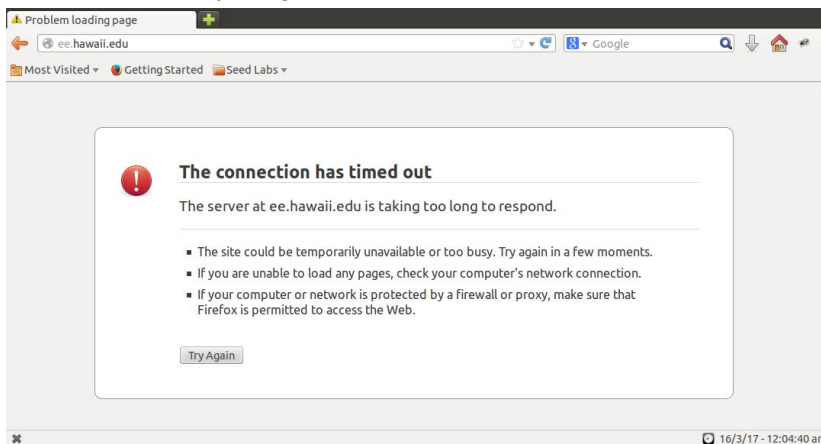
We can see that I can telnet to Machine B server, here is what is going on with wireshark:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------------------|----------|-------------|----------|--------|---|
| 1 | 2017-03-15 23:53:38.54 | 10.0.2.4 | 10.0.2.6 | SSH | 116 | Encrypted request packet len=48 |
| 2 | 2017-03-15 23:53:38.54 | 10.0.2.6 | 10.0.2.4 | SSH | 116 | Encrypted response packet len=48 |
| 3 | 2017-03-15 23:53:38.54 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 41308 > ssh [ACK] Seq=49 Ack=49 Win=161 Len=0 |
| 4 | 2017-03-15 23:53:38.65 | 10.0.2.4 | 10.0.2.6 | SSH | 116 | Encrypted request packet len=48 |
| 5 | 2017-03-15 23:53:38.65 | 10.0.2.6 | 10.0.2.4 | SSH | 116 | Encrypted response packet len=48 |
| 6 | 2017-03-15 23:53:38.65 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 41308 > ssh [ACK] Seq=97 Ack=97 Win=161 Len=0 |
| 7 | 2017-03-15 23:53:38.82 | 10.0.2.4 | 10.0.2.6 | SSH | 116 | Encrypted request packet len=48 |
| 8 | 2017-03-15 23:53:38.82 | 10.0.2.6 | 10.0.2.4 | SSH | 116 | Encrypted response packet len=48 |
| 9 | 2017-03-15 23:53:38.82 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 41308 > ssh [ACK] Seq=145 Ack=145 Win=161 Len=0 |
| 10 | 2017-03-15 23:53:39.07 | 10.0.2.4 | 10.0.2.6 | SSH | 116 | Encrypted request packet len=48 |
| 11 | 2017-03-15 23:53:39.07 | 10.0.2.6 | 10.0.2.4 | SSH | 116 | Encrypted response packet len=48 |
| 12 | 2017-03-15 23:53:39.07 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 41308 > ssh [ACK] Seq=193 Ack=193 Win=161 Len=0 |
| 13 | 2017-03-15 23:53:39.18 | 10.0.2.4 | 10.0.2.6 | SSH | 116 | Encrypted request packet len=48 |
| 14 | 2017-03-15 23:53:39.18 | 10.0.2.6 | 10.0.2.4 | SSH | 116 | Encrypted response packet len=48 |
| 15 | 2017-03-15 23:53:39.18 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 41308 > ssh [ACK] Seq=241 Ack=241 Win=161 Len=0 |
| 16 | 2017-03-15 23:53:39.33 | 10.0.2.4 | 10.0.2.6 | SSH | 116 | Encrypted request packet len=48 |
| 17 | 2017-03-15 23:53:39.33 | 10.0.2.6 | 10.0.2.4 | SSH | 116 | Encrypted response packet len=48 |
| 18 | 2017-03-15 23:53:39.33 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 41308 > ssh [ACK] Seq=289 Ack=289 Win=161 Len=0 |
| 19 | 2017-03-15 23:53:39.65 | 10.0.2.4 | 10.0.2.6 | SSH | 116 | Encrypted request packet len=48 |
| 20 | 2017-03-15 23:53:39.65 | 10.0.2.6 | 10.0.2.4 | SSH | 116 | Encrypted response packet len=48 |
| 21 | 2017-03-15 23:53:39.65 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 41308 > ssh [ACK] Seq=337 Ack=337 Win=161 Len=0 |
| 22 | 2017-03-15 23:53:39.84 | 10.0.2.4 | 10.0.2.6 | SSH | 116 | Encrypted request packet len=48 |
| 23 | 2017-03-15 23:53:39.84 | 10.0.2.6 | 10.0.2.4 | SSH | 116 | Encrypted response packet len=48 |

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)

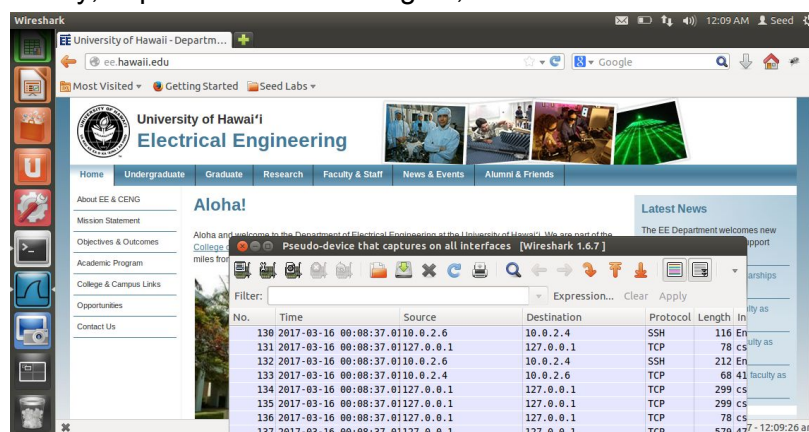
 * Documentation:  https://help.ubuntu.com/

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

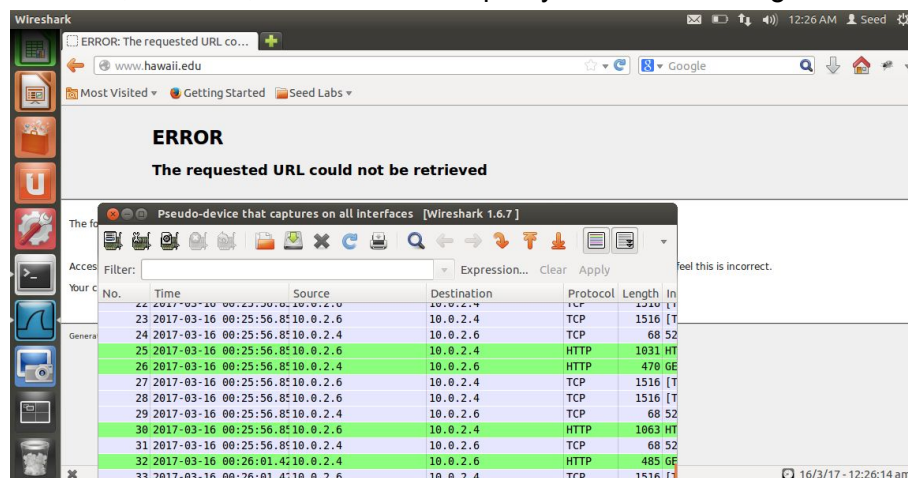
Last login: Wed Mar 15 23:58:45 2017 from localhost
[03/16/2017 00:03] seed@ubuntu:~$

```

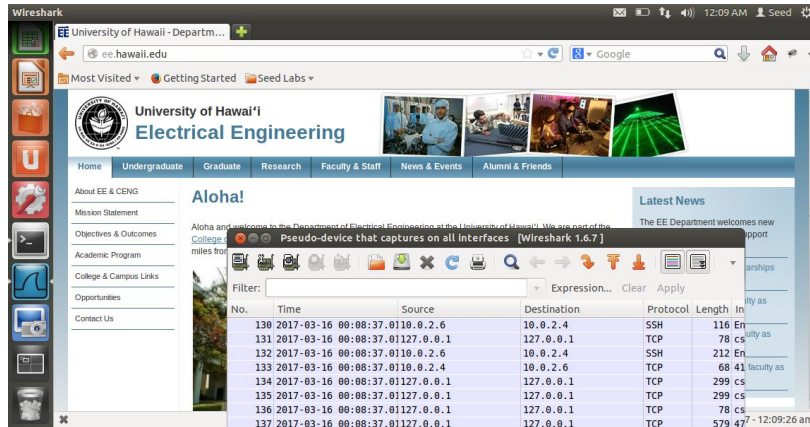
Then, I configured Firefox browser to use proxy as lab guideline says. Finally, I opened EE website again, now I can access to it:



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.

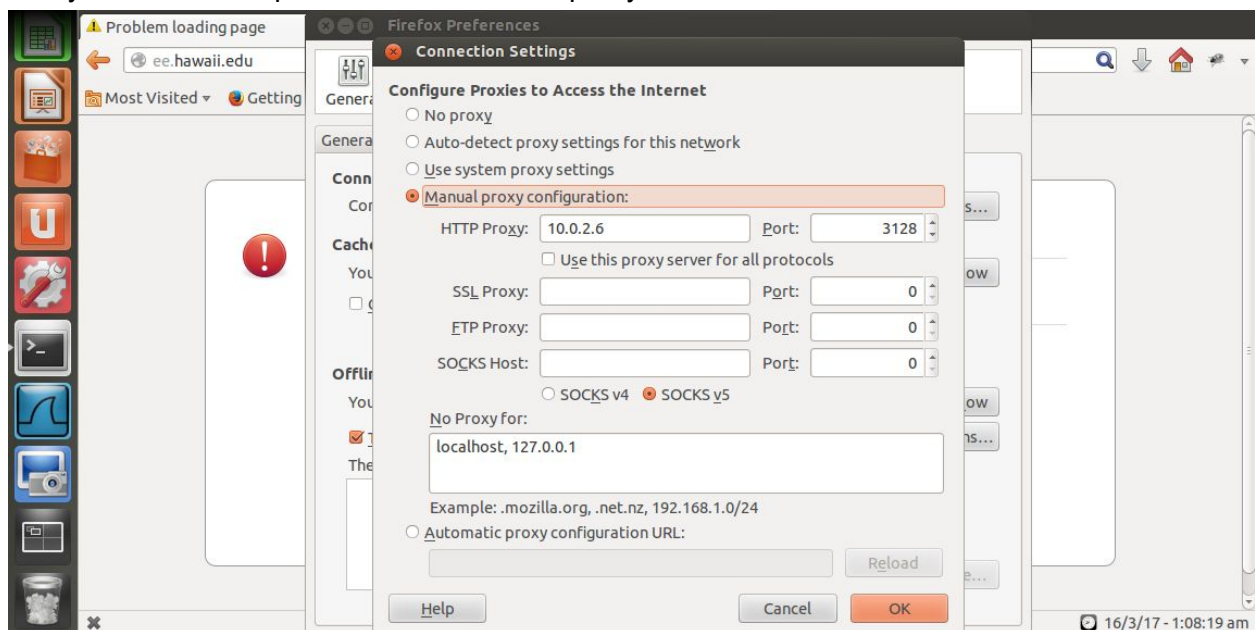
Question 4:

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:


```

Terminal
http_access deny manager

# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
http_access allow all

#
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet

"/etc/squid3/squid.conf" 5798L, 206966C written      836,21      14%

```

Then I can visit UH web:

The screenshot shows a web browser window displaying the University of Hawaii System homepage. Overlaid on the browser is a Wireshark packet capture window titled "Pseudo-device that captures on all interfaces [Wireshark 1.6.7]". The packet list shows several HTTP and TCP packets. The selected packet (No. 770) is an HTTP 204 No Content response from 10.0.2.4 to 10.0.2.6.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------------------|---------------|---------------|----------|--------|---|
| 769 | 2017-03-16 00:47:15.751 | 10.0.2.6 | 10.0.2.4 | TCP | 68 | ndl-aas > 52879 [ACK] Seq=534 Ack=1 |
| 770 | 2017-03-16 00:47:15.751 | 10.0.2.6 | 10.0.2.4 | HTTP | 511 | HTTP/1.0 204 No Content |
| 771 | 2017-03-16 00:47:15.751 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 52871 > ndl-aas [ACK] Seq=5173 Ack= |
| 772 | 2017-03-16 00:47:15.751 | 216.58.216.14 | 10.0.2.4 | TLSv1 | 525 | Application Data |
| 773 | 2017-03-16 00:47:15.751 | 10.0.2.4 | 216.58.216.14 | TCP | 56 | 40956 > https [ACK] Seq=715 Ack=470 |
| 774 | 2017-03-16 00:47:15.811 | 10.0.2.6 | 10.0.2.4 | HTTP | 611 | HTTP/1.0 200 OK (text/javascript) |
| 775 | 2017-03-16 00:47:15.811 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 52879 > ndl-aas [ACK] Seq=1748 Ack= |
| 776 | 2017-03-16 00:47:15.811 | 10.0.2.6 | 10.0.2.4 | HTTP | 473 | HTTP/1.0 304 Not Modified |
| 777 | 2017-03-16 00:47:15.811 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 52856 > ndl-aas [ACK] Seq=4847 Ack= |
| 778 | 2017-03-16 00:47:15.811 | 10.0.2.6 | 10.0.2.4 | HTTP | 473 | HTTP/1.0 304 Not Modified |
| 779 | 2017-03-16 00:47:15.811 | 10.0.2.4 | 10.0.2.6 | TCP | 68 | 52876 > ndl-aas [ACK] Seq=853 Ack=70 am |

We can see from wireshark capture that the packet is transferred 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


```

Terminal

# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

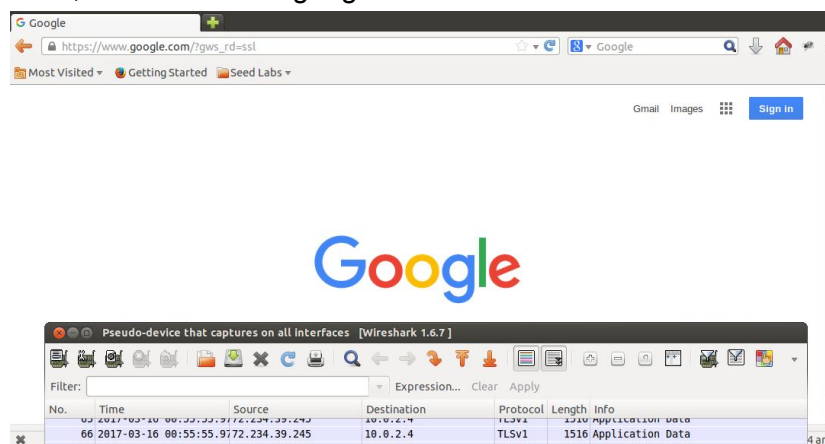
# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#http_access allow all
acl google_domain dstdomain .google.com
http_access allow google_domain
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
"/etc/squid3/squid.conf" 5800L, 207039C written 837,39 14%

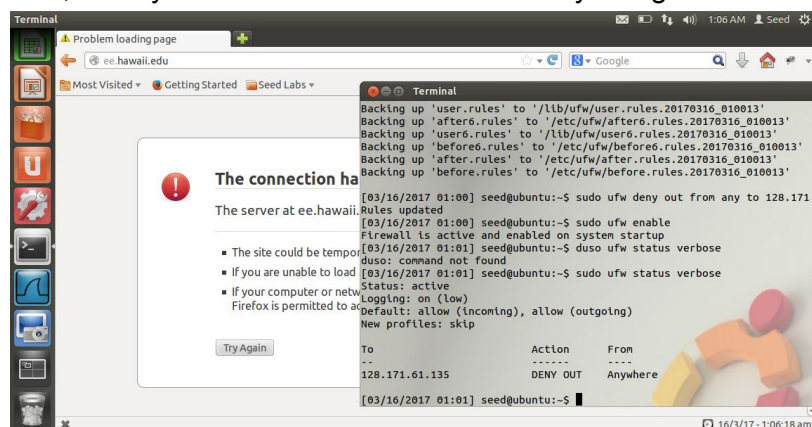
```

Then, I can access to google.com:

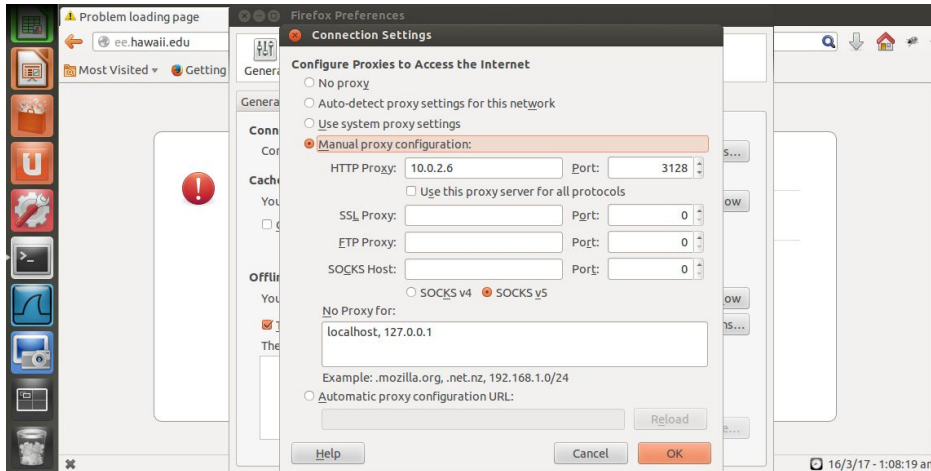


Task 4.b:

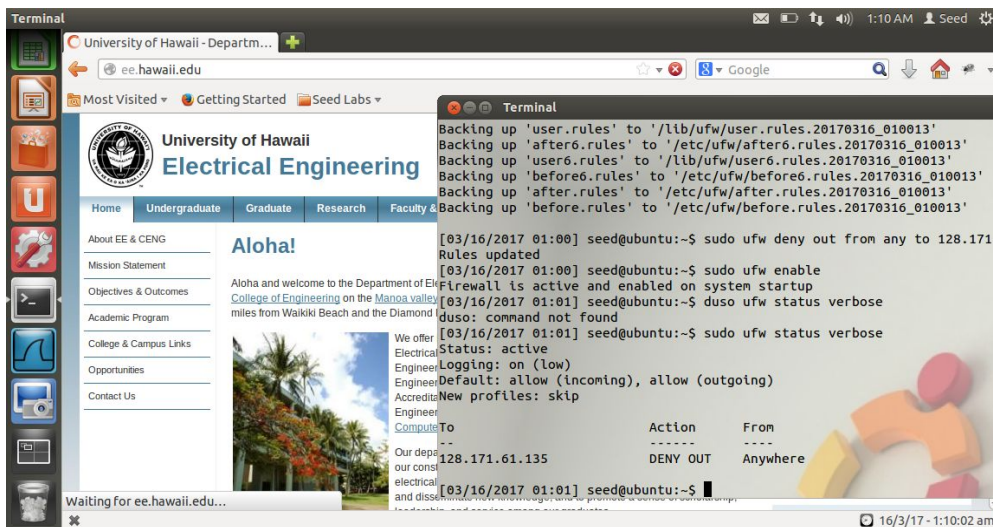
First, I verify that I can not visit ee website by using ufw firewall:



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.