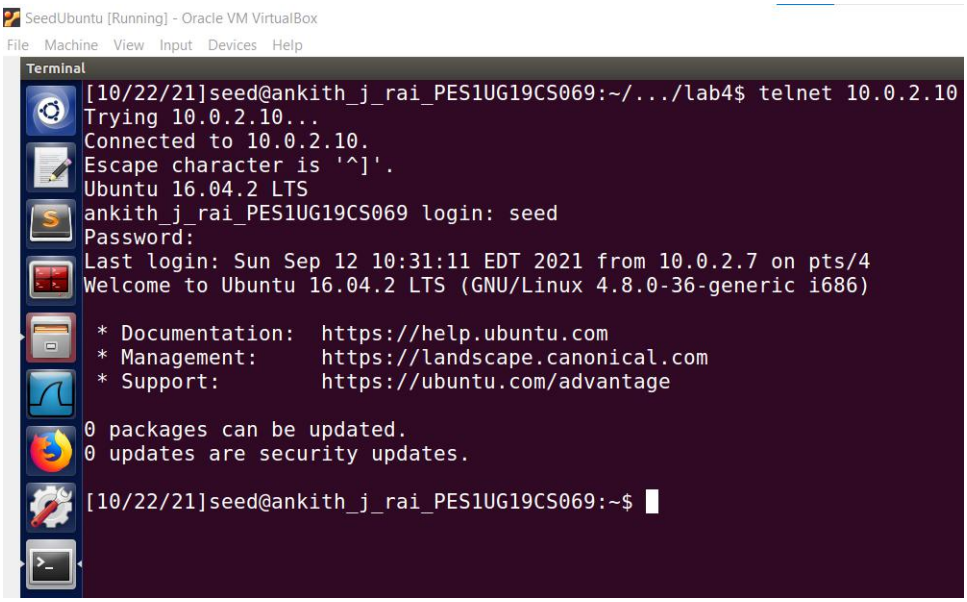
Linux Firewall Exploration Lab

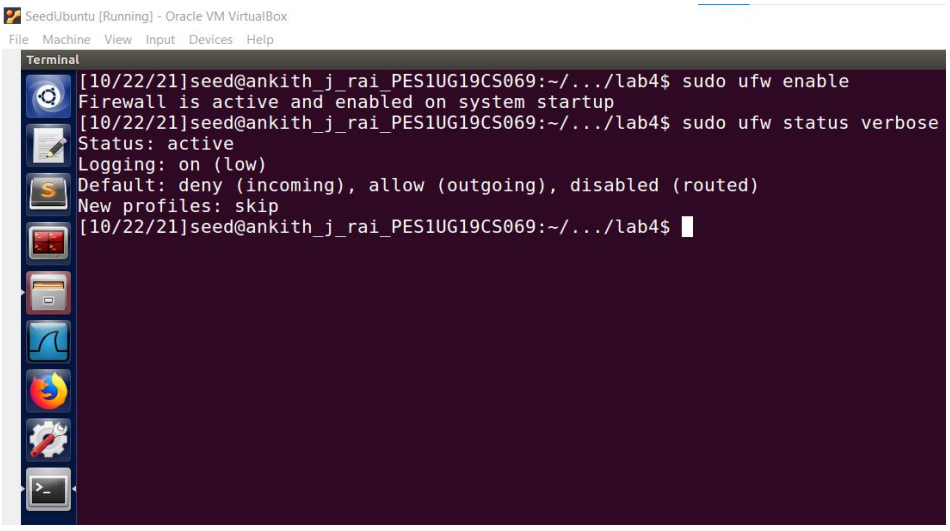
Name : Ankith J Rai
SRN : PES1UG19CS069
SEC : B

Machine	IP address
VM 1	10.0.2.5
VM 2	10.0.2.10
VM 3	10.0.2.11

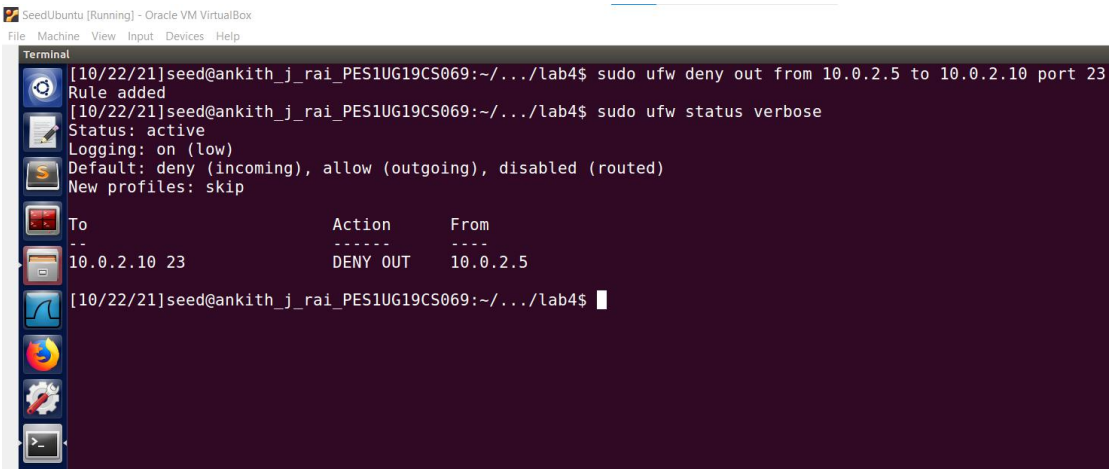
Task 1: Using Firewall:



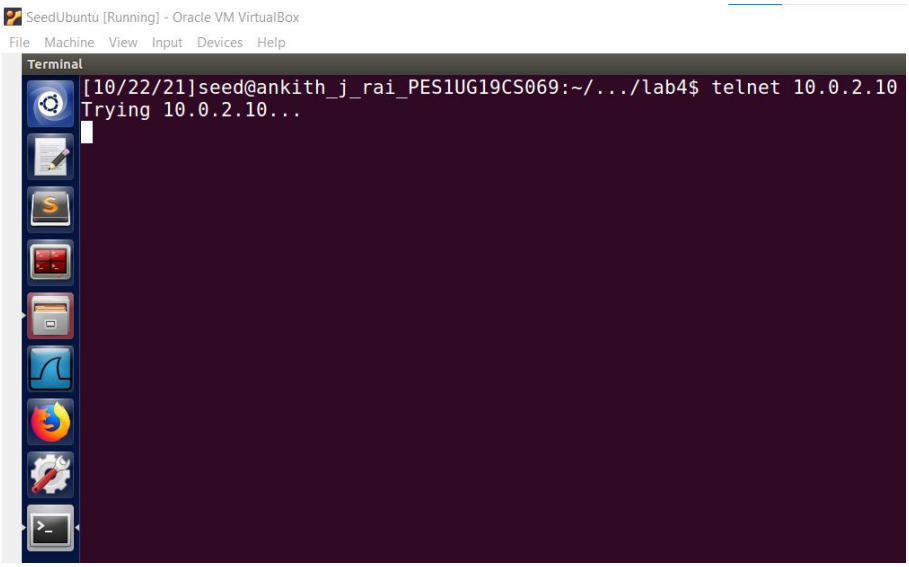
We can see that VM 1 is able to establish a telnet connection with VM 2.



Now we can see that we have enabled the firewall in VM 1.

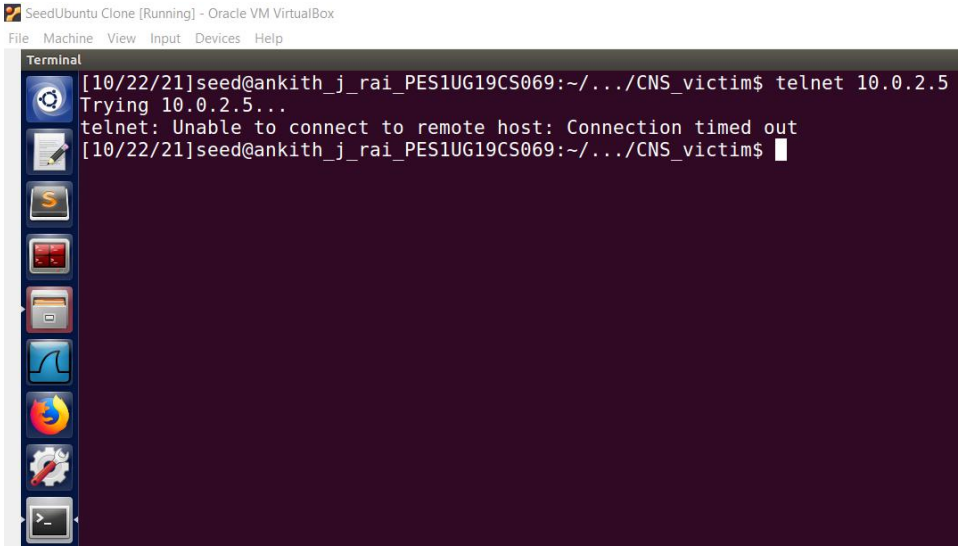


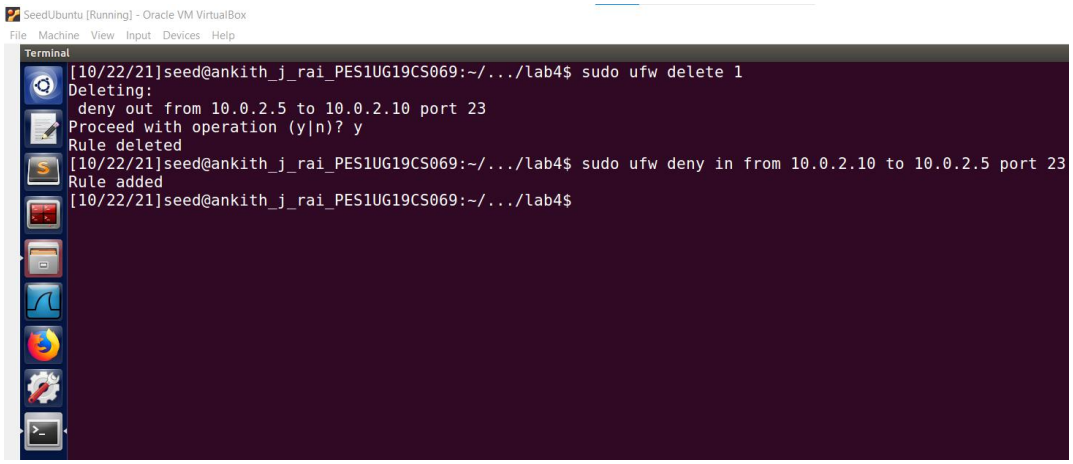
Now we can see that a rule has been added to the firewall of the VM 1 to deny any connection through port 23 to 10.0.2.10.



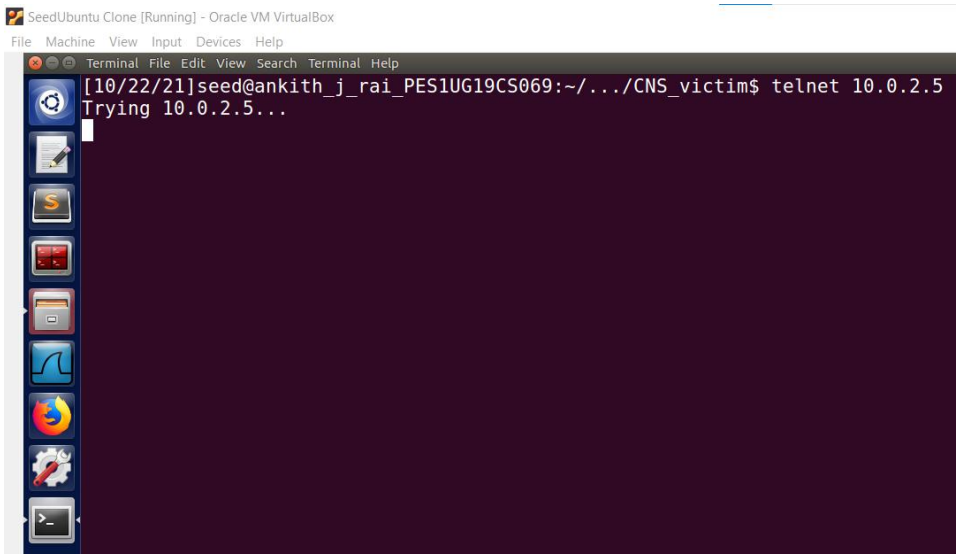
Now we can see that on VM1 is not able to establish a telnet connection with VM 2 as the firewall is blocking the packets from being sent to 10.0.2.10 from 10.0.2.5 through port 23.

On trying to telnet from VM 2 to VM 1 also we can see that no connection is being established this is because the firewall is blocking the packets from 10.0.2.5 to 10.0.2.10 through port 23.



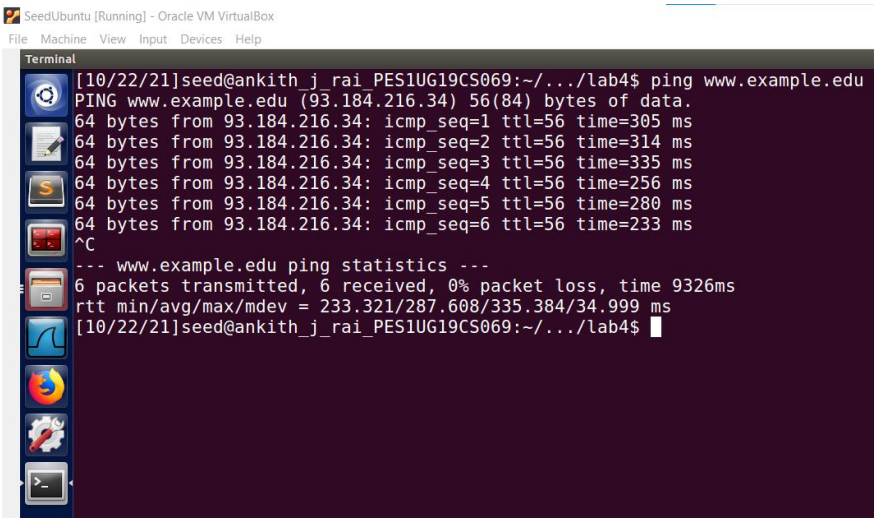


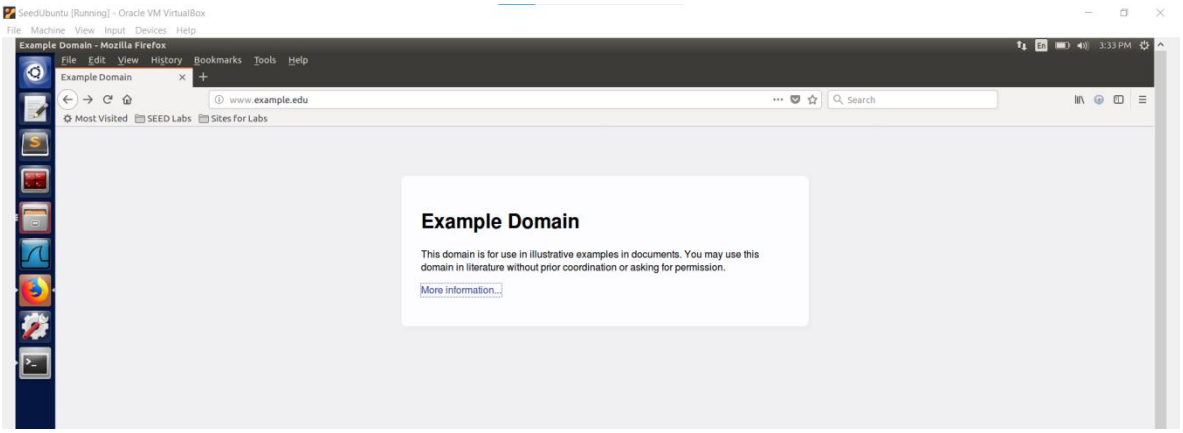
Now we have added a rule to the firewall which does not allow packets to come from 10.0.2.10 into 10.0.2.5 through port 23.



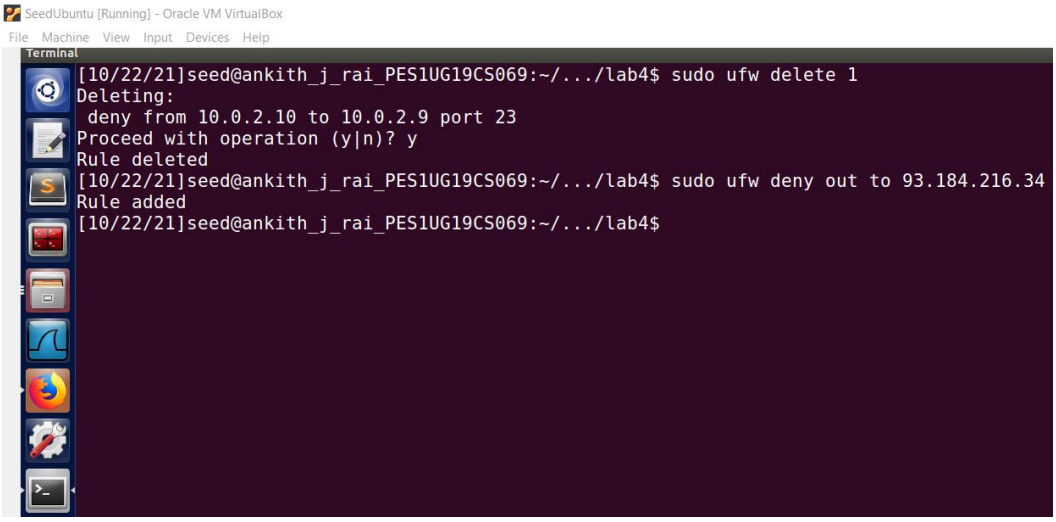
We can see that VM 2 is not able to establish telnet connection with VM 1.

For me due to some reason www.pes.edu was not pinging hence I have used www.example.edu

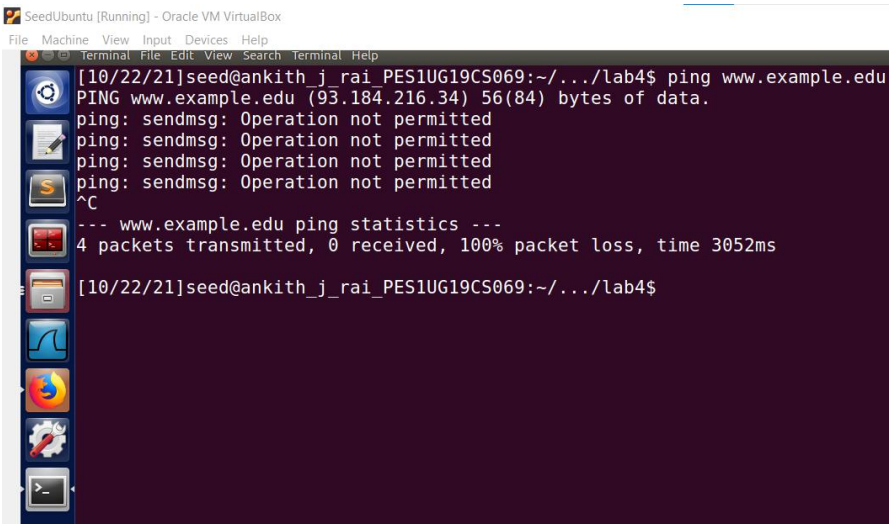




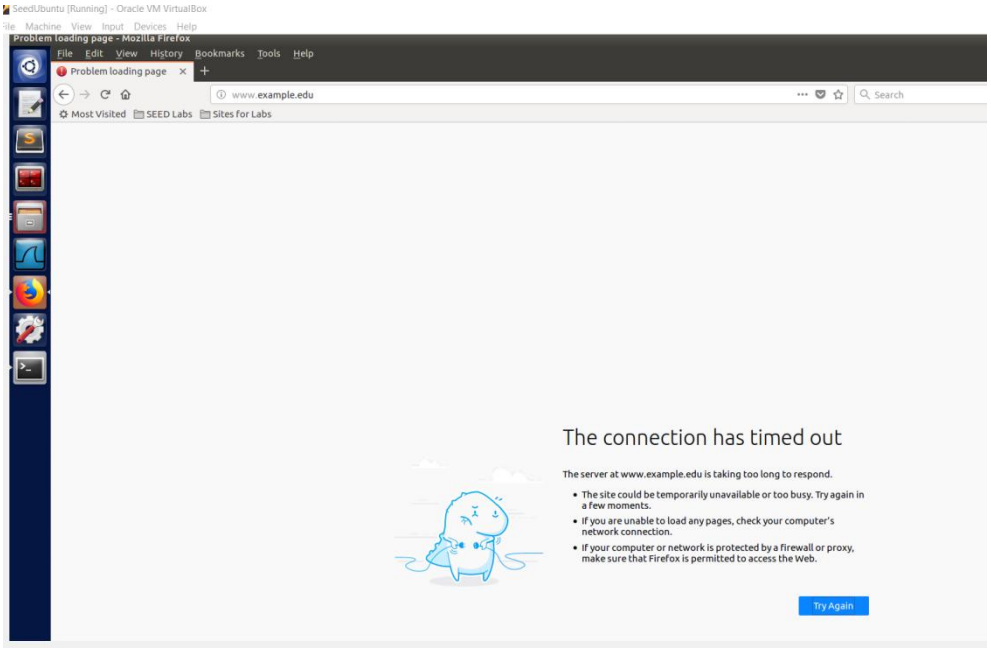
We can see that on the web browser we can access the website.



Now we have added a rule to the firewall of the VM 1 which prevents it from accessing www.example.com

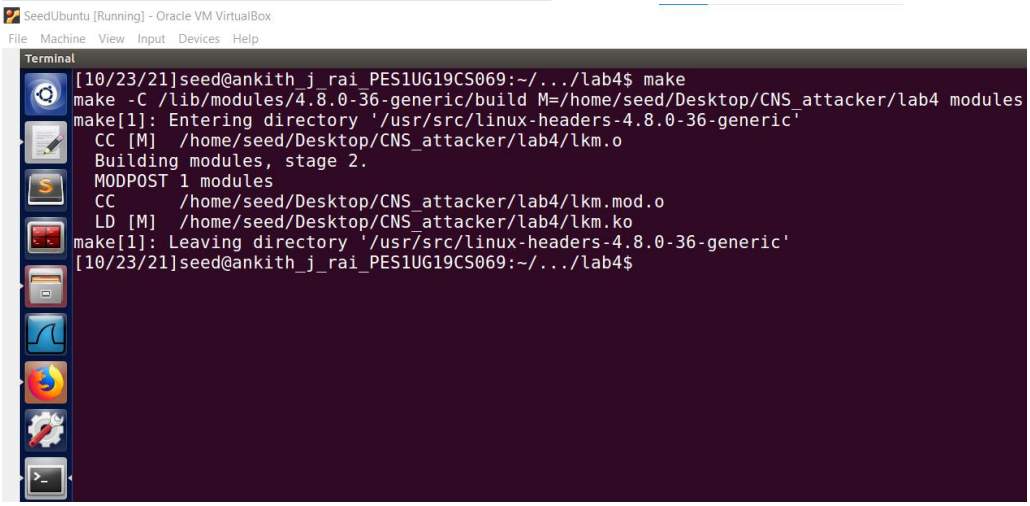


Now we can see that the firewall has blocked VM 1 from pinging www.example.com because of the rule added to VM 1's firewall.

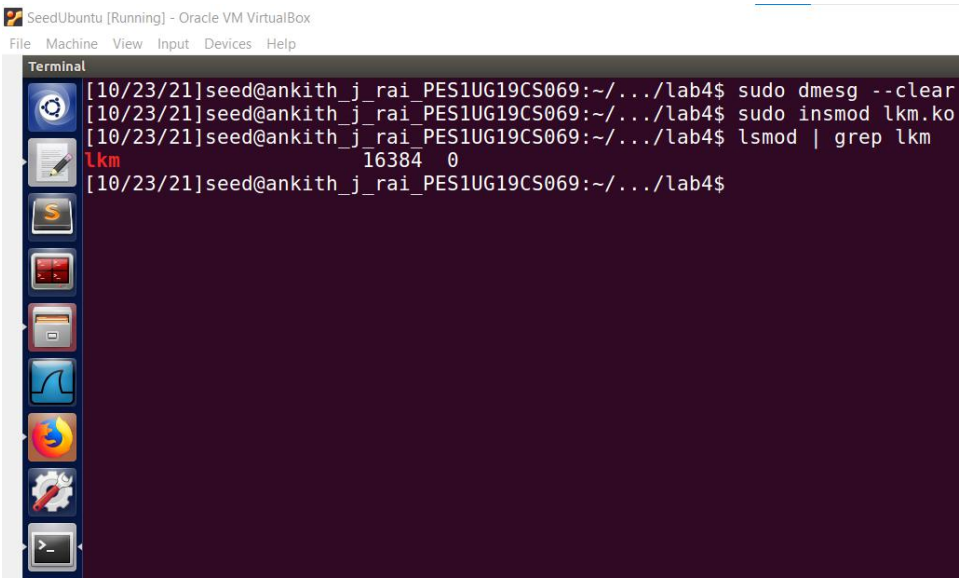


We can confirm from the above screenshot that the page for www.example.edu is not getting loaded now.

Task 2: How Firewall Works

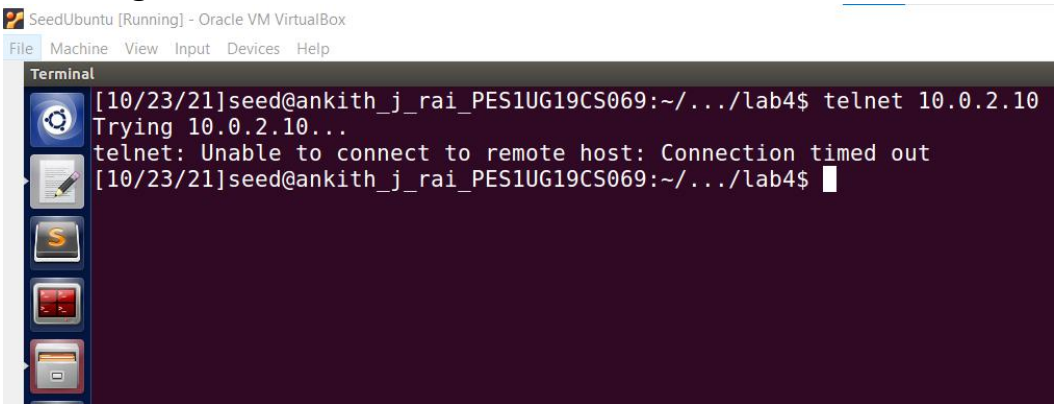


On running make command we can see the above output on the terminal.



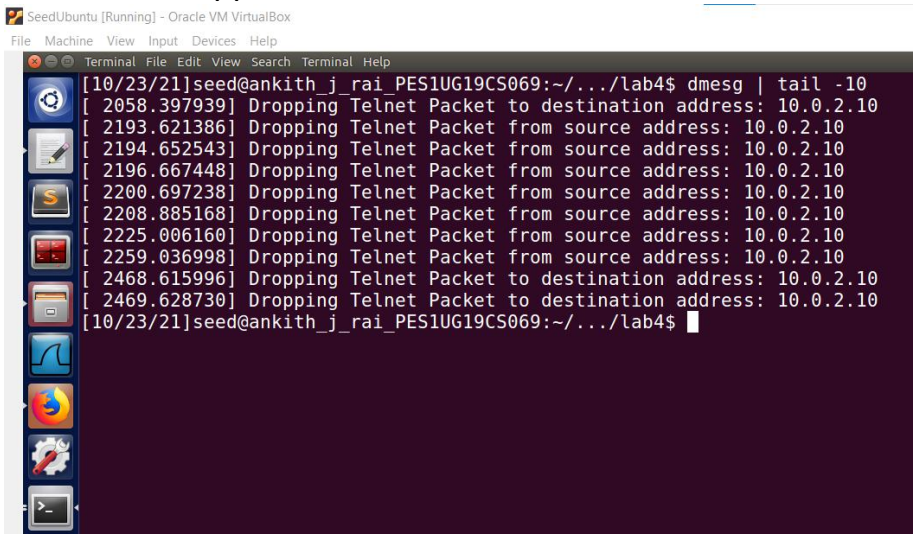
From the above screenshot we can see that the compiled kernel module has been inserted using insmod

Telneting from VM 1 to VM 2:

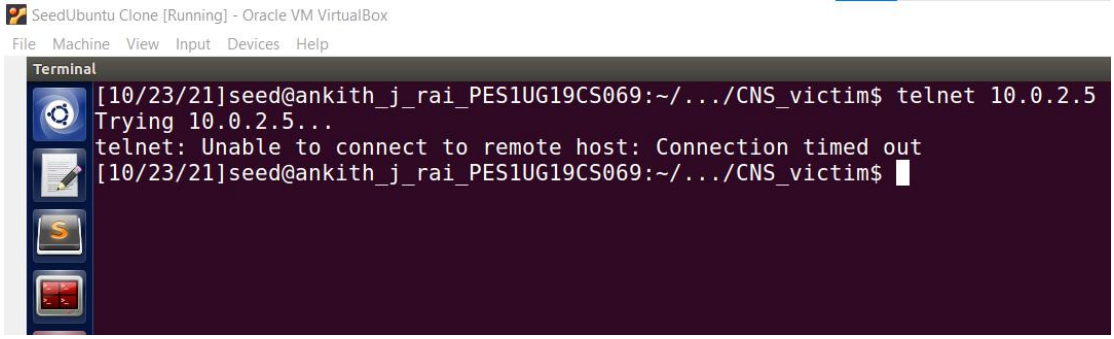


We can see that VM 1 is not able to establish telnet connection with VM 2.

On running the **dmesg | tail -10** command on VM 1 we get the packets which are dropped.

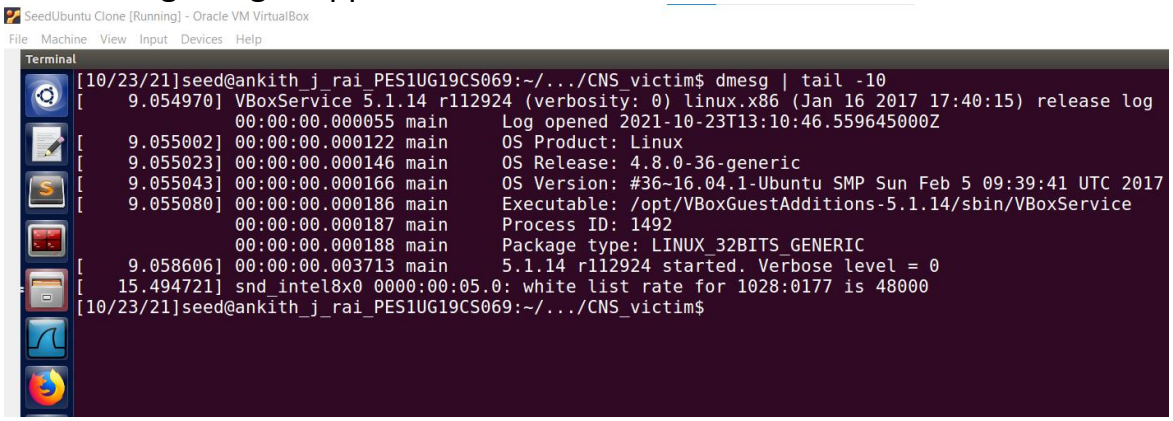


Telneting from VM 2 to VM 1:

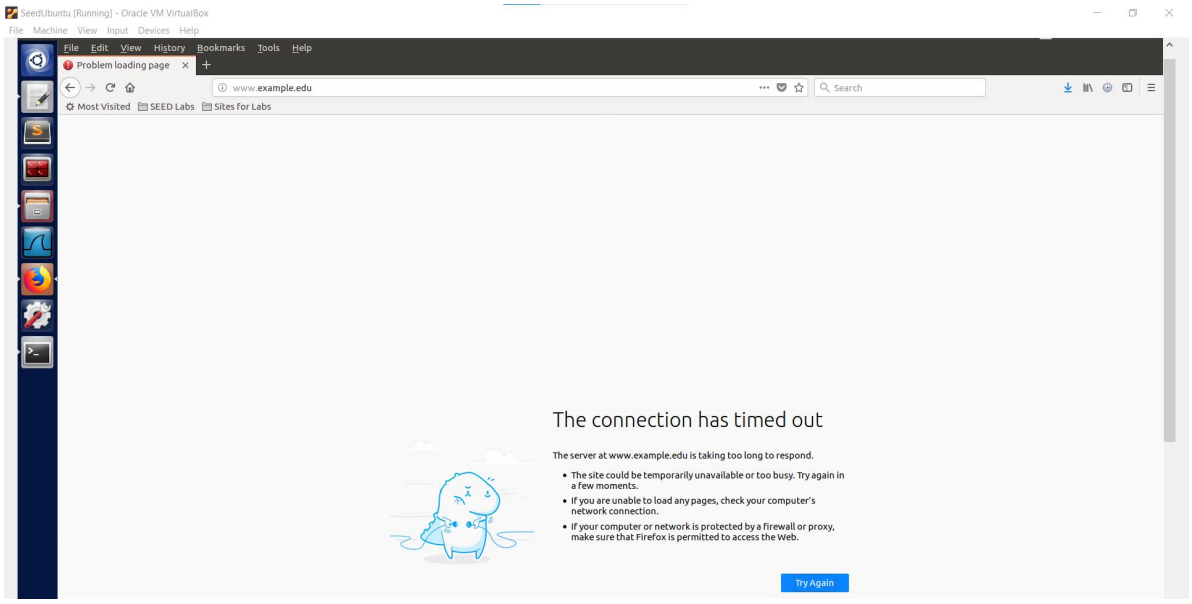


We can see that VM 2 is not able to establish telnet connection with VM 1.

On running the **dmesg | tail -10** command on VM 2 we get the packets which are getting dropped.

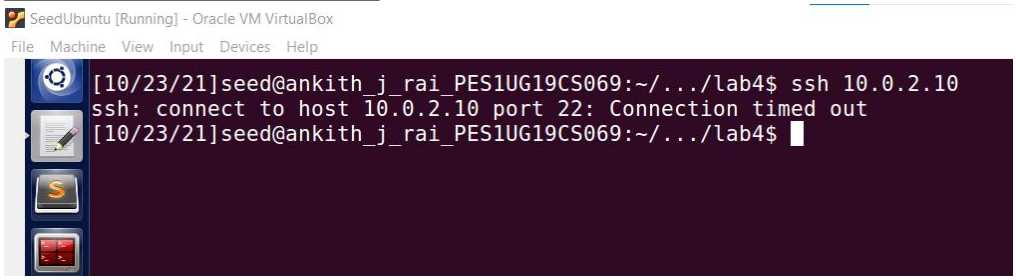


As www.pes.edu not working from task 1 so for this task too I will be using www.example.edu .



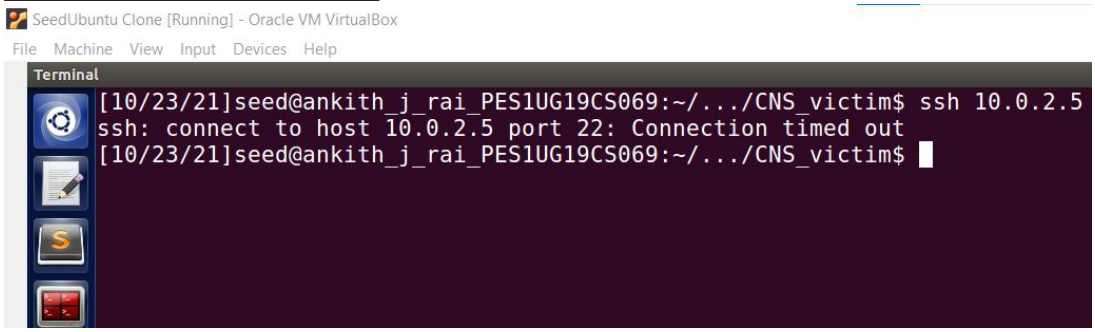
We can see from the above screenshot that the page is not loading and the connection has timed out this is because of the firewall blocking.

SSH from VM 1 to VM 2:



We can see that the SSH connection from VM 1 to VM 2 has failed and the connection has timed out.

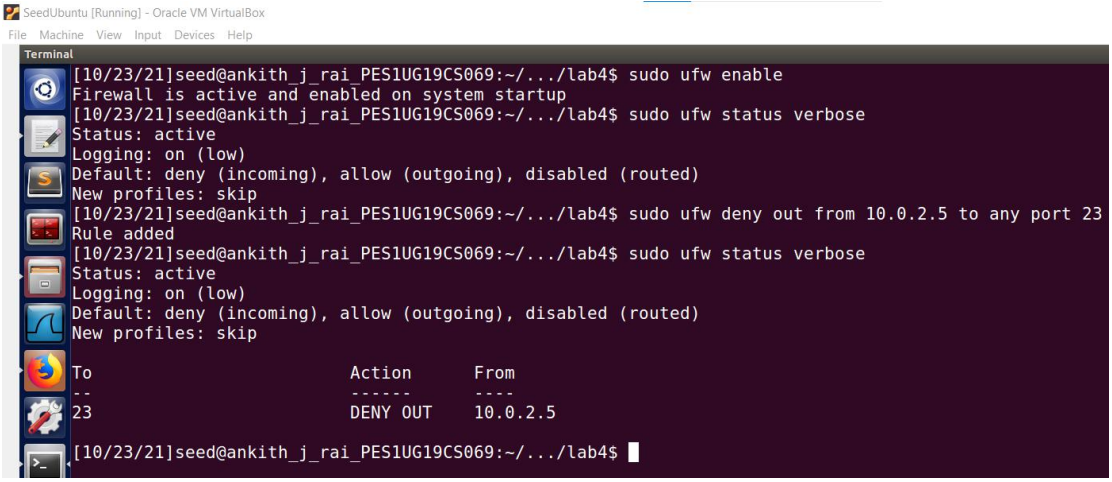
SSH from VM 2 to VM 1:



We can see that the SSH connection from VM 2 to VM 1 has failed and the connection has timed out.

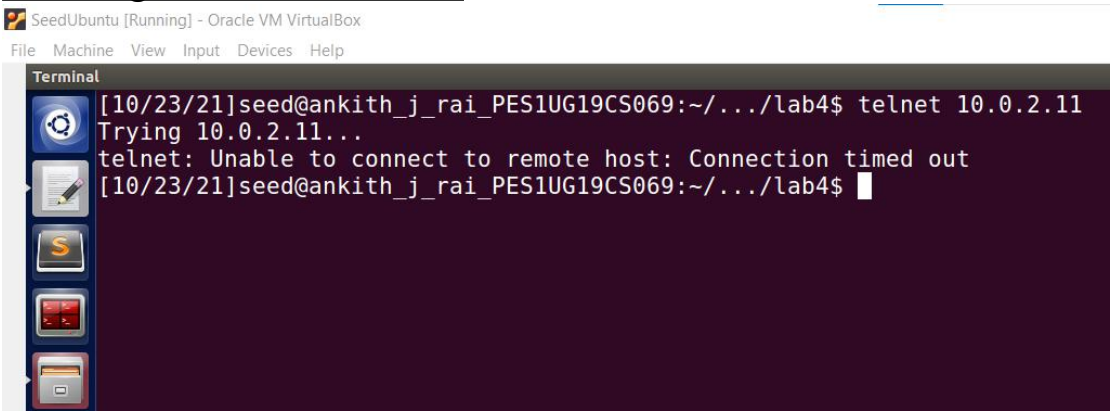
Task 3: Evading Egress Filtering

Task 3.a: Telnet to Machine B through the firewall



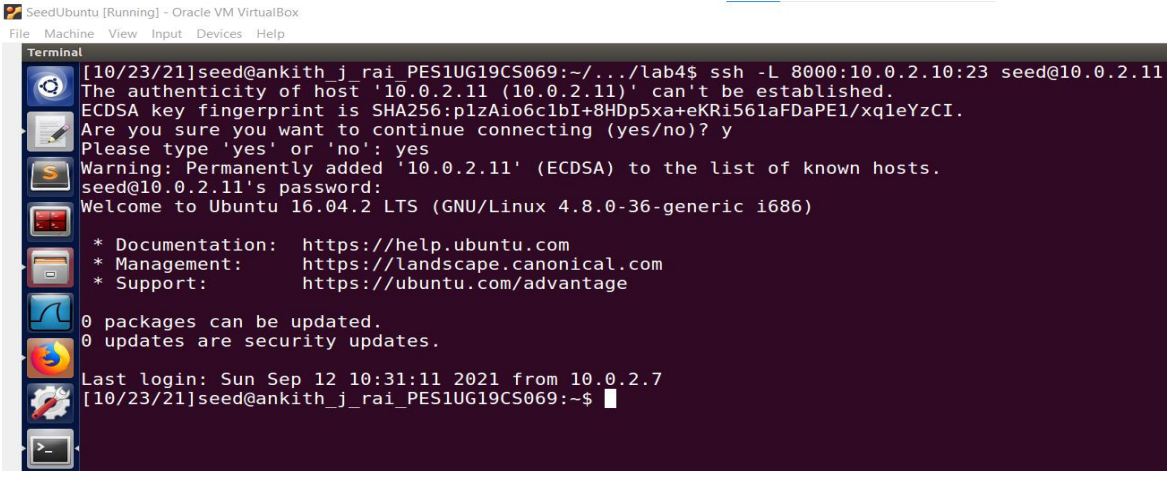
On running the commands we add a new rule to firewall of VM 1,which blocks all the packets going out from VM 1 through port 23.

Telneting from VM 1 to VM 3:

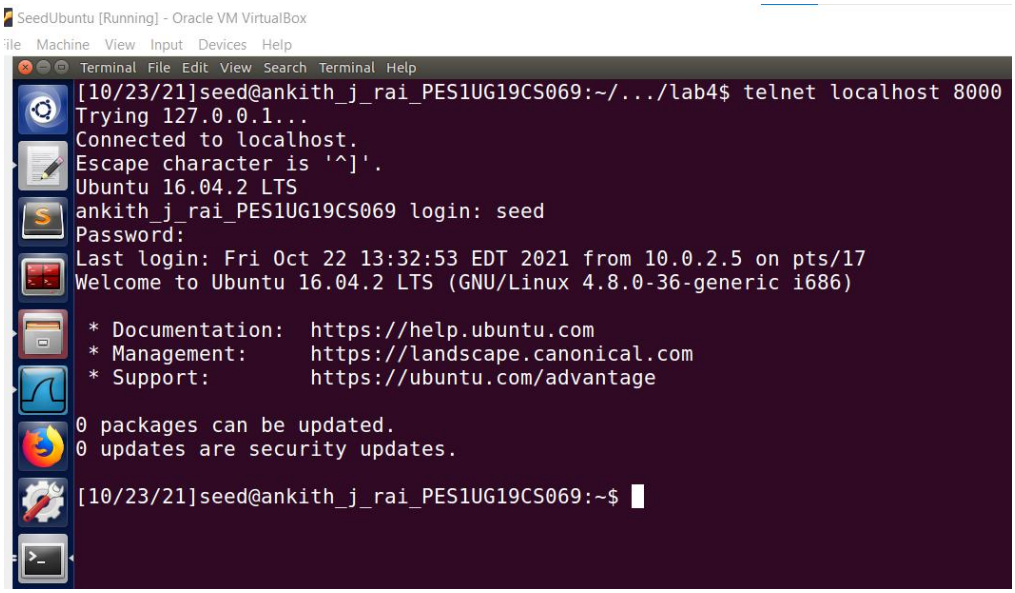


We can see that telnet connection from VM 1 to VM 3 is not established and the connection has timed out.

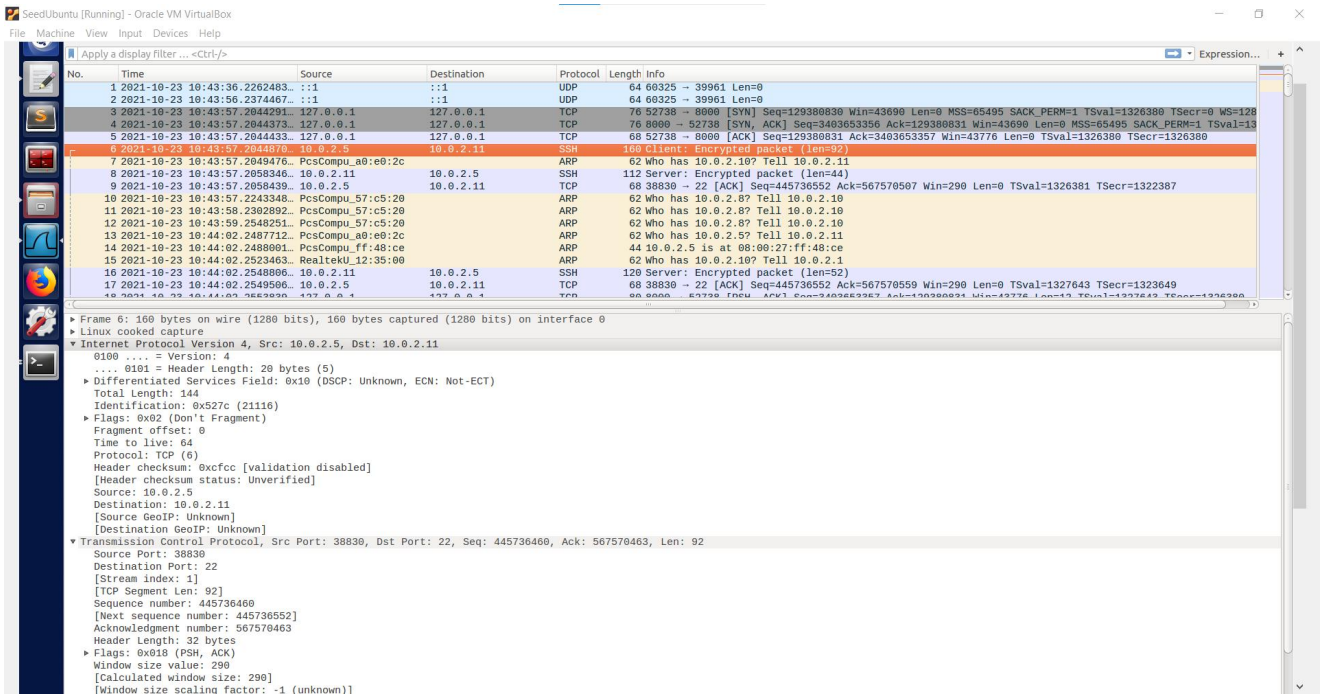
Now setting up a SSH tunnel between VM 1 and VM 2



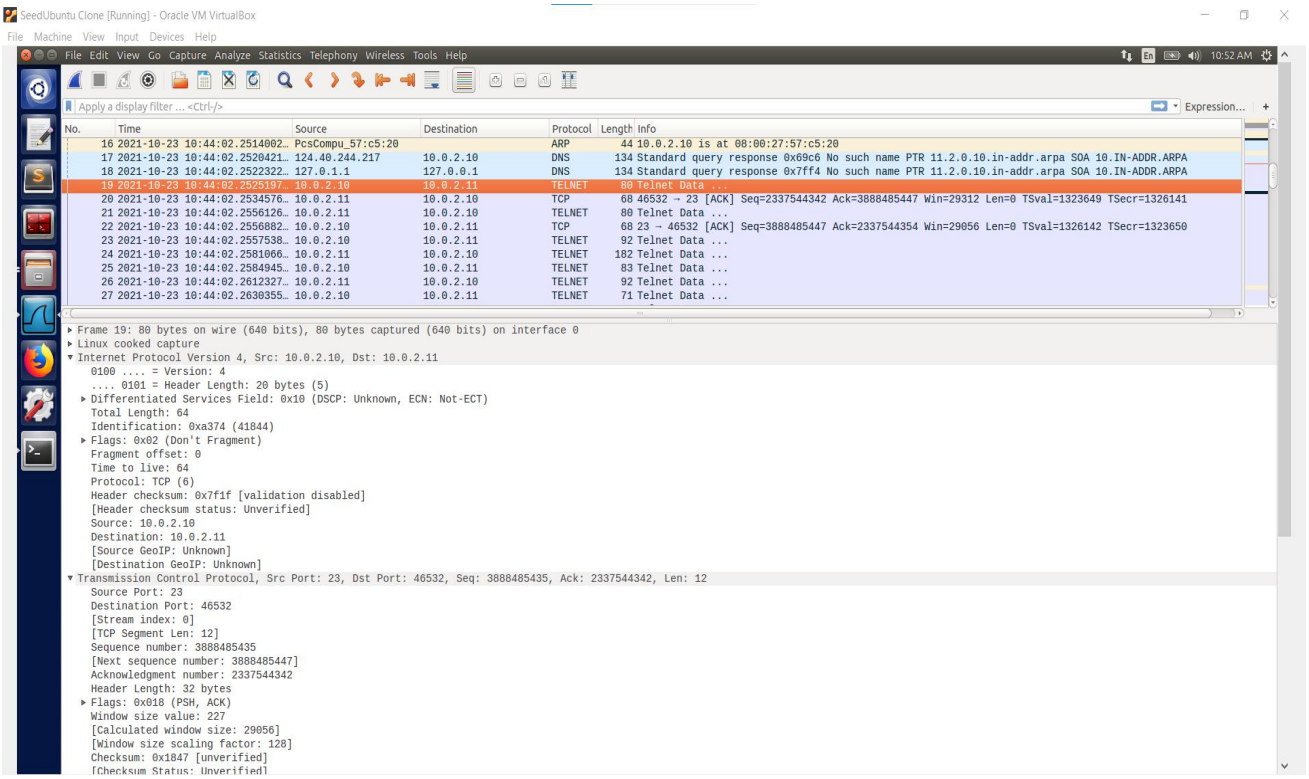
Telneting localhost 8000:



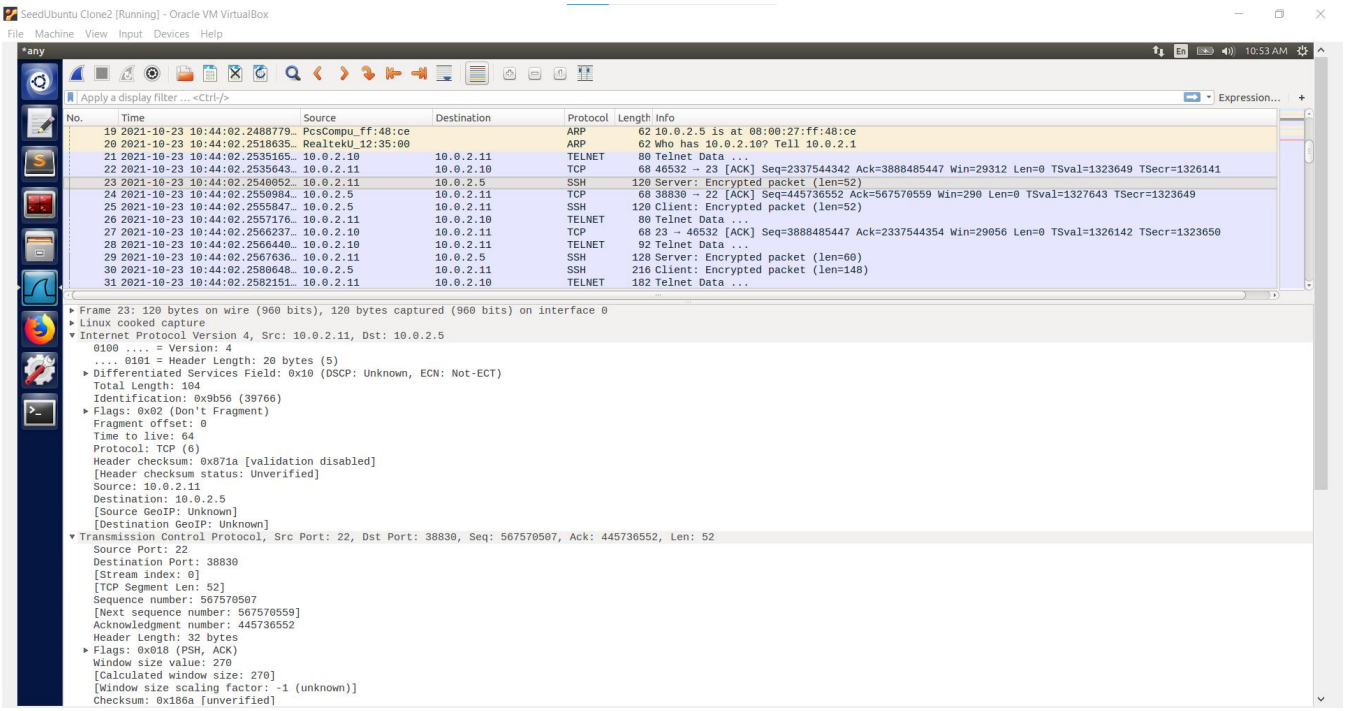
Screenshot of wireshark of VM 1:



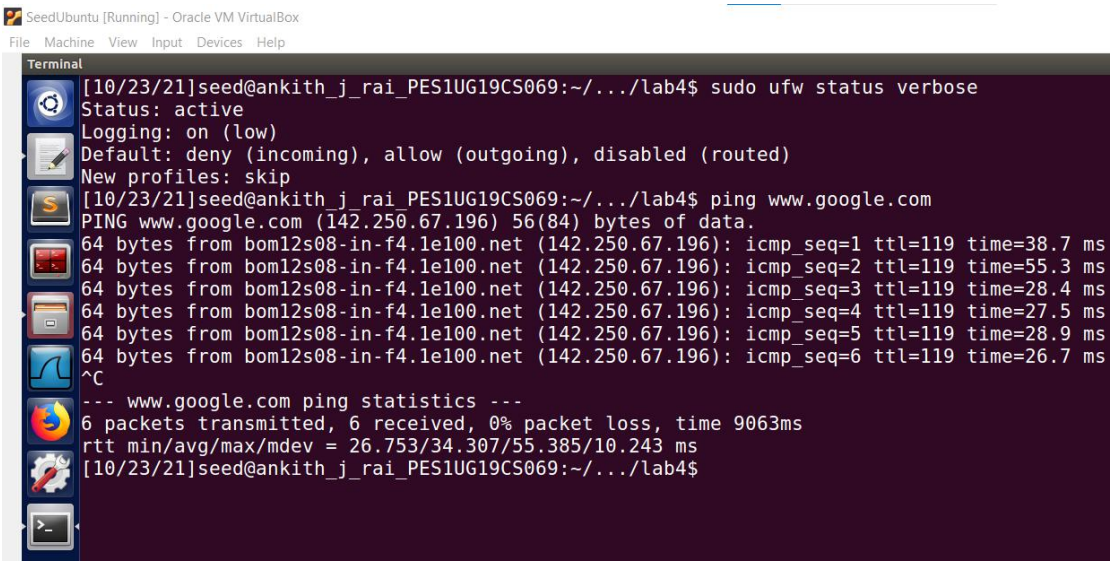
Screenshot of wireshark of VM 2:



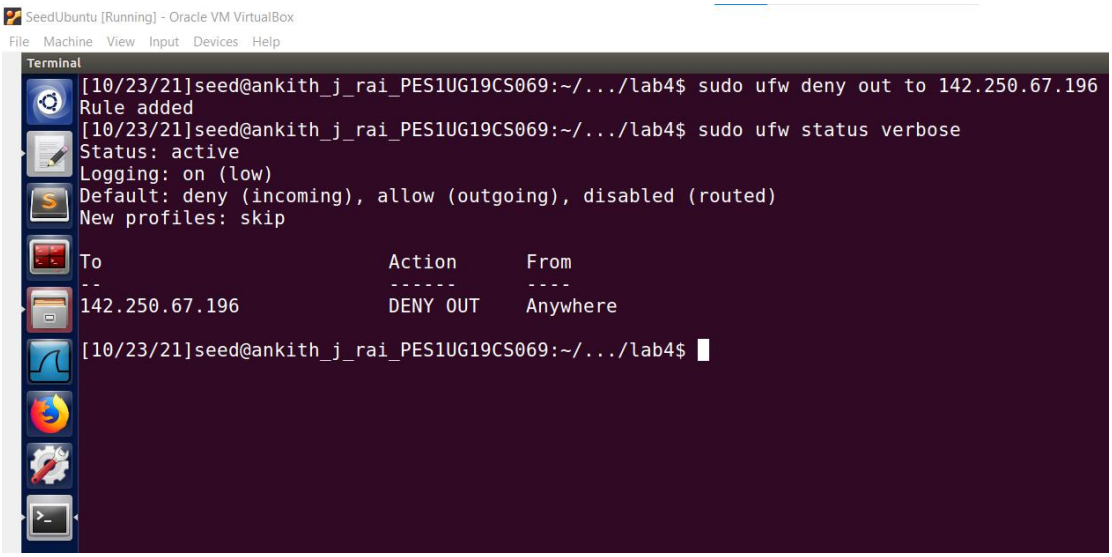
Screenshot of wireshark of VM 3:



Task 3.b: Connecting to Google using SSH tunnel

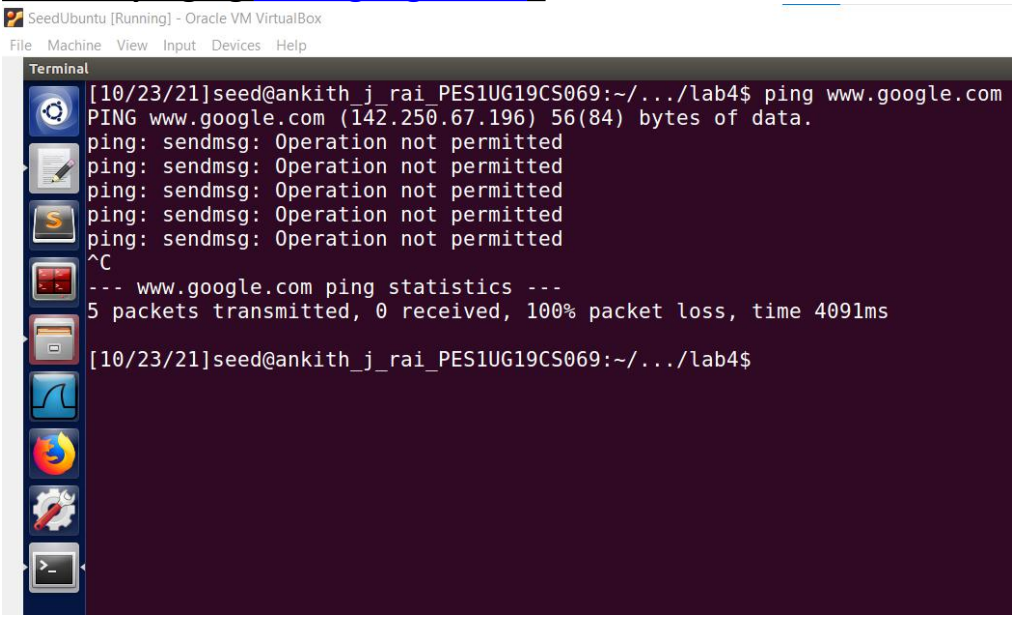


From the above screenshot we can see that VM 1's firewall has no rules and from pinging www.google.com we get to know that its ip address is 142.250.67.196

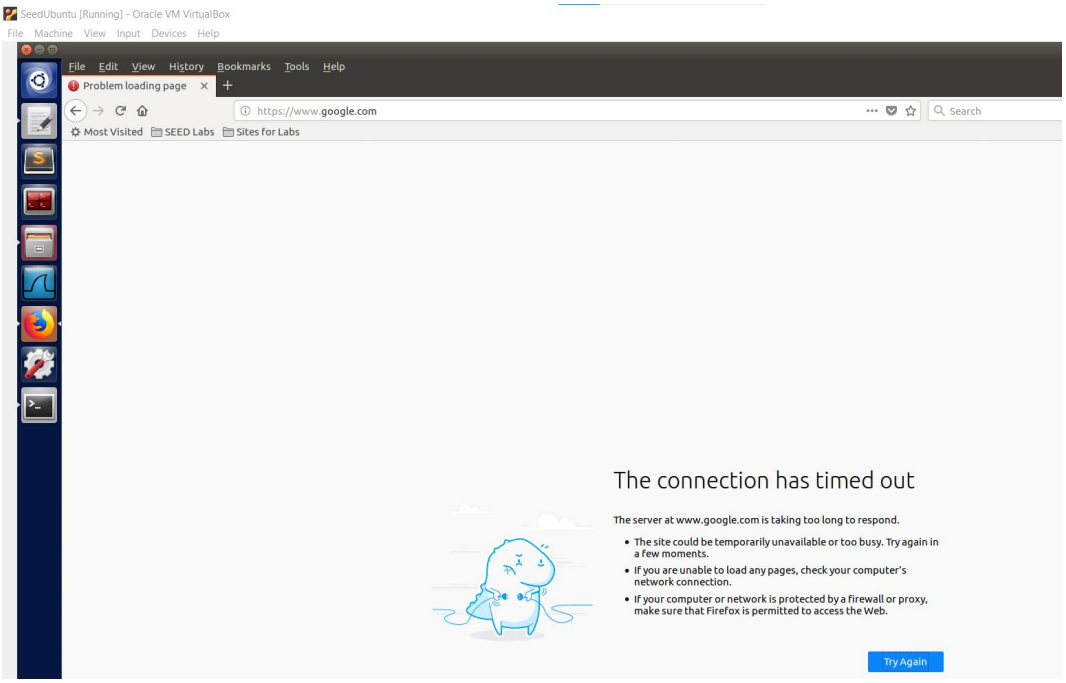


From the above screenshot we can see that to the firewall of VM 1 a rule has been added to deny packets going from VM 1 to 142.250.67.196

Now on pinging www.google.com :

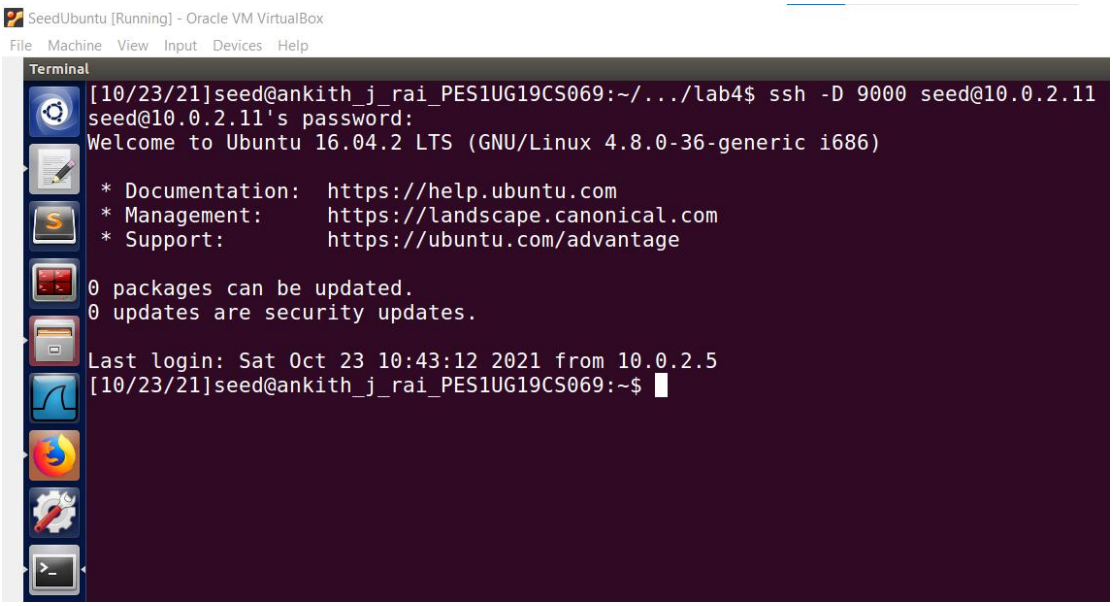


We can see that we are not able to ping www.google.com from VM 1 as the firewall is blocking it and we can see this in the above screenshot where it tells that the Operation not permitted.

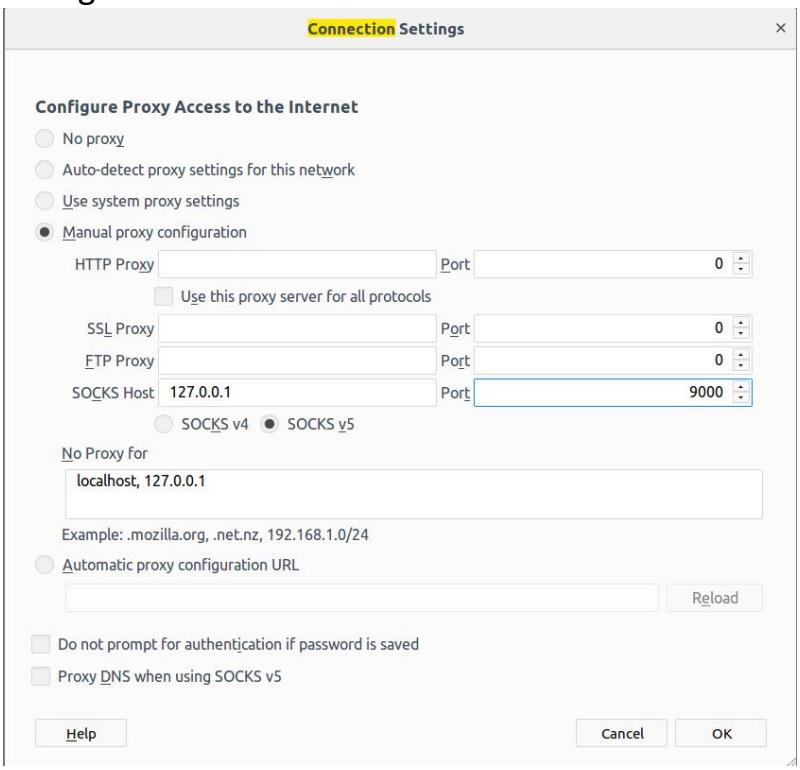


On the browser of VM 1 also we can see that we are not able to connect to www.google.com

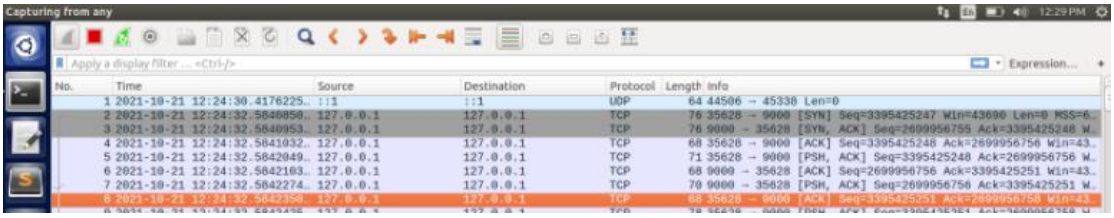
Now setting up a SSH tunnel between VM 1 and VM 2



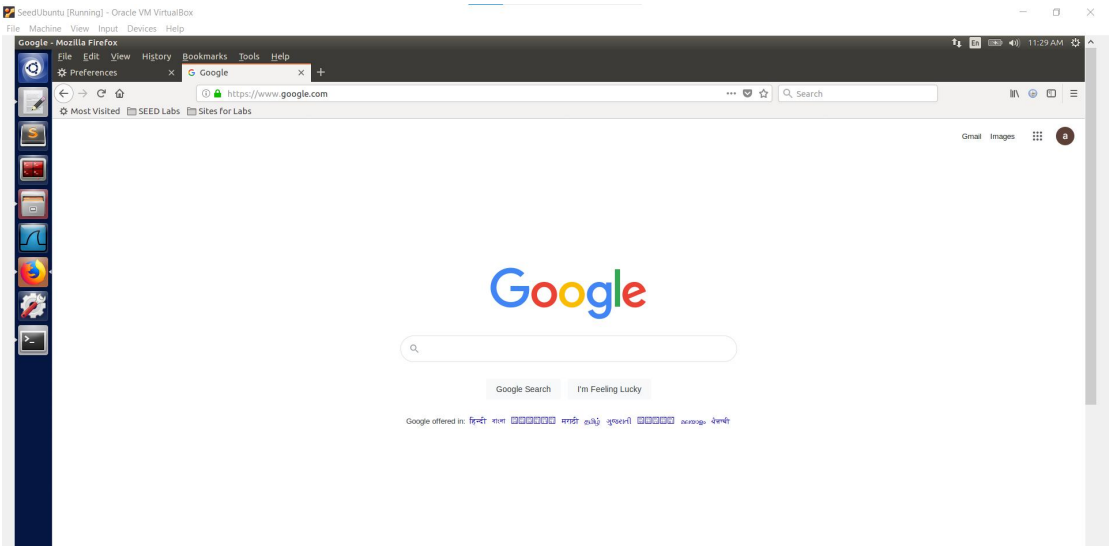
Changing connection setting in firefox browser to manual proxy configuration.



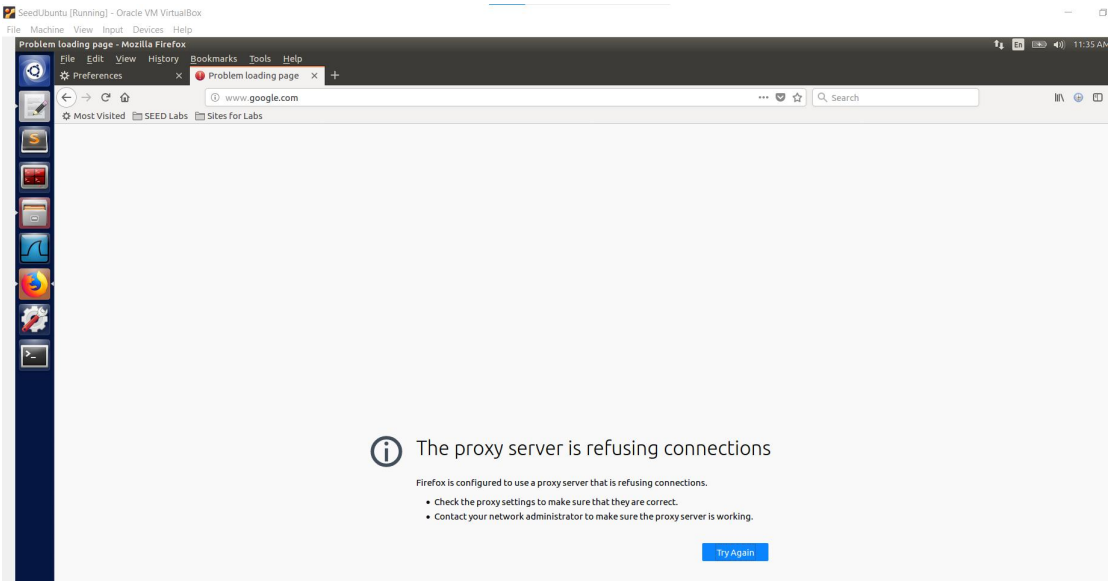
Wireshark screenshot of VM 1



Now accessing www.google.com from the VM 1 web browser

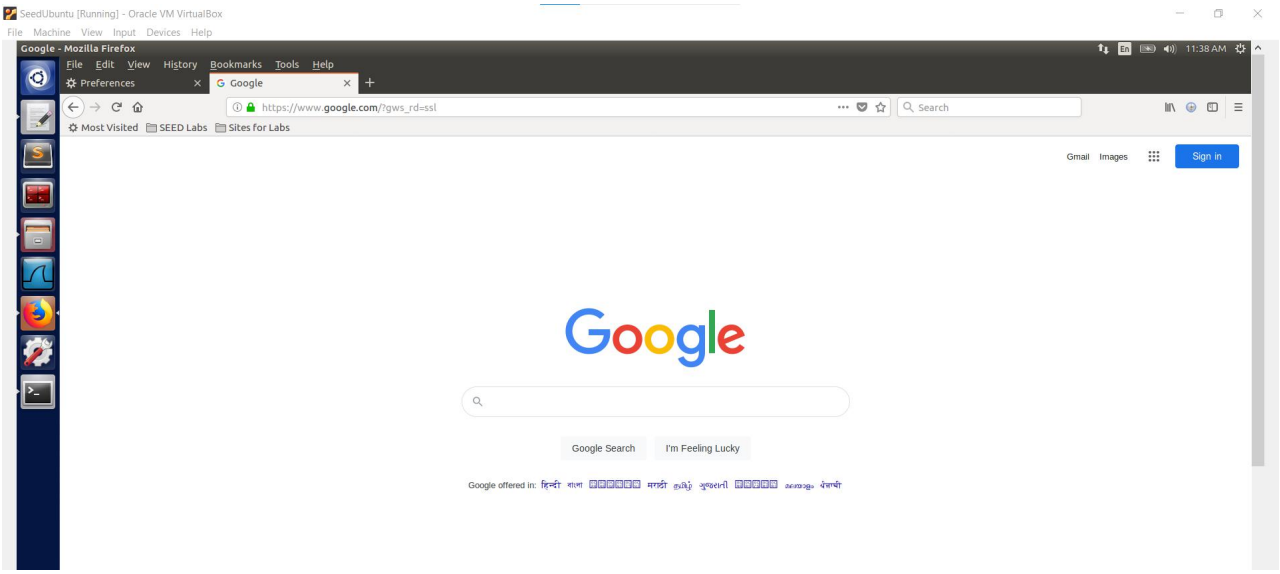


We can see that even though the firewall has a rule to block the visiting of www.google.com from VM 1 , we can visit it , this is because of changing the proxy configuration.



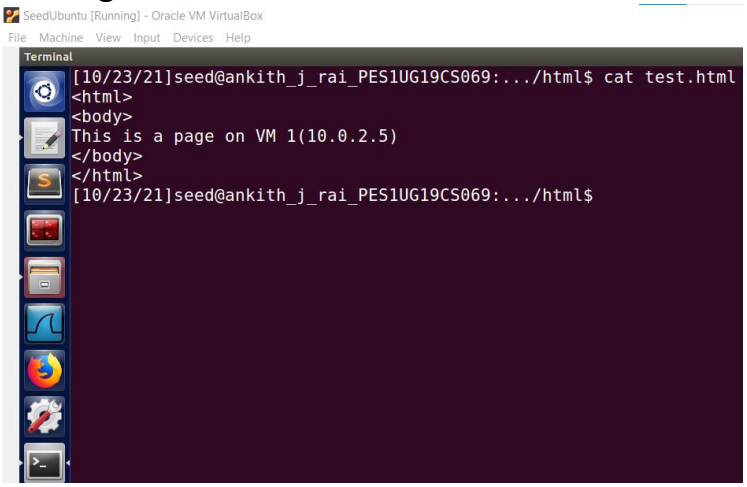
Now on disabling the tunnel we can see that the proxy server is refusing connections as browser is configured to use the proxy but the tunnel has been disabled.

Now on re-enabling the ssh tunnel we can see that we are able to visit the www.google.com website from VM 1.

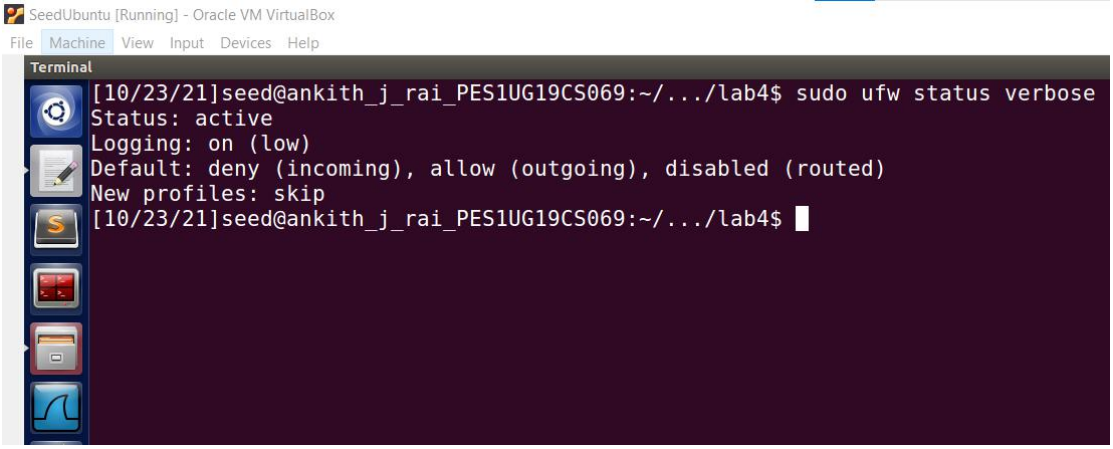


Task 4: Evade Ingress Filtering

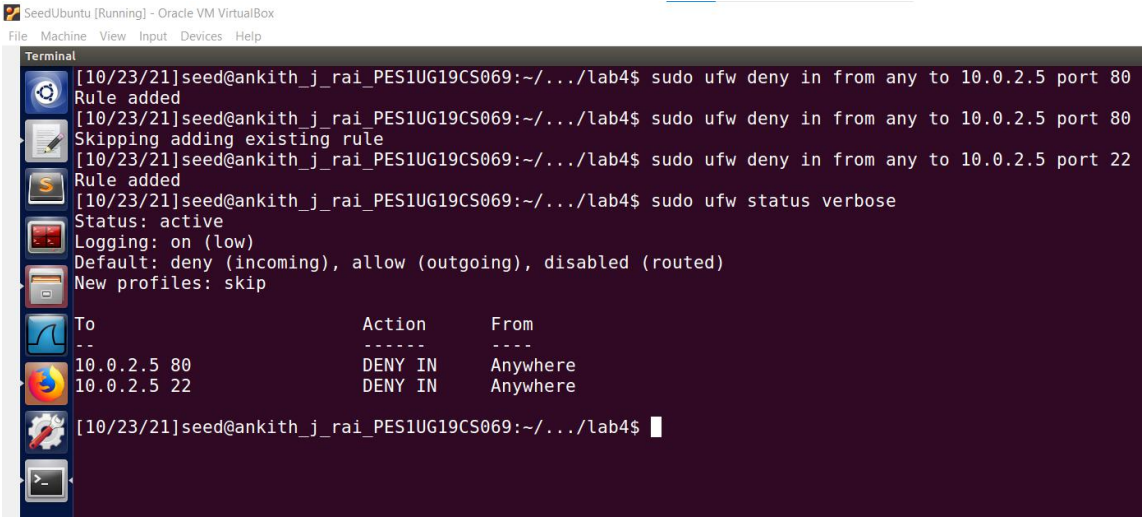
Writing test.html in the VM 1 machine.



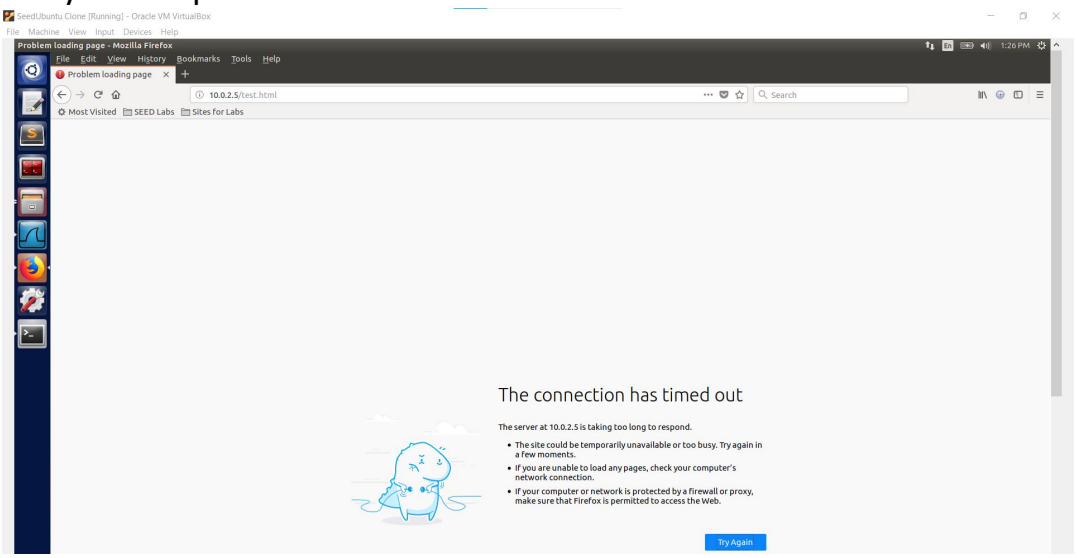
VM 1 Firewall status table:

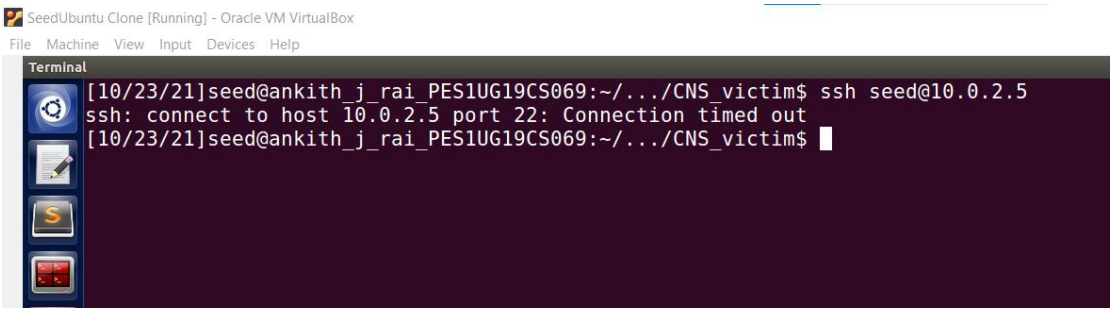


Now we will be adding rules to the firewall of the VM 1 :



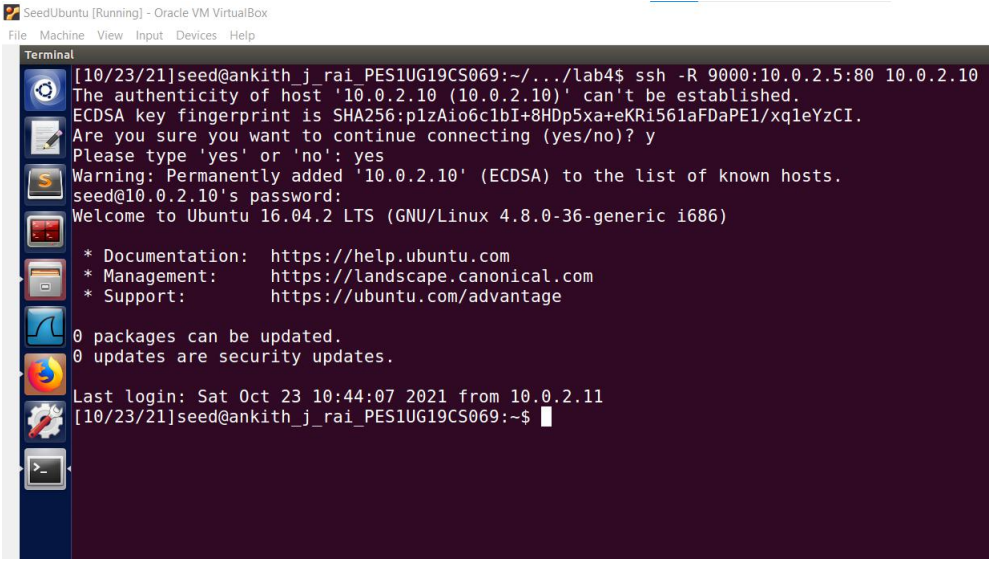
Now when we try to access test.html from VM 2 we cannot as we have not yet set up the tunnel.



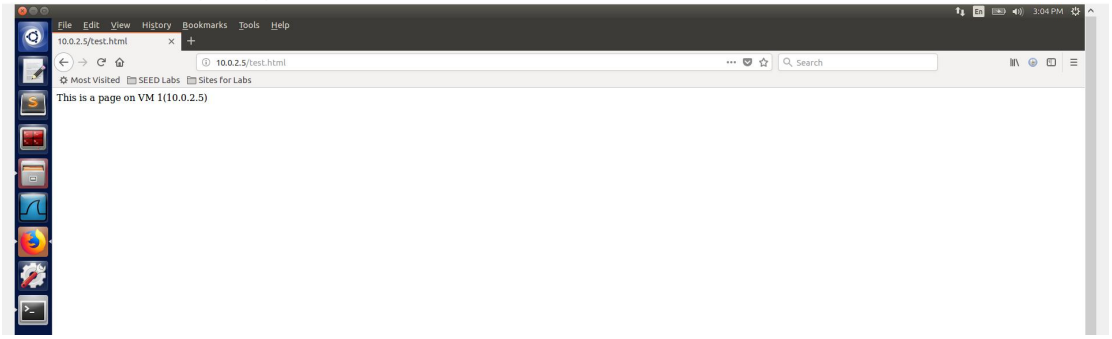


Now on sending ssh connection from VM 2 to VM 1 we can see that the connection is not getting established and the connection has timed out.

Now we set up a reverse tunnel from from VM 1 to VM 2

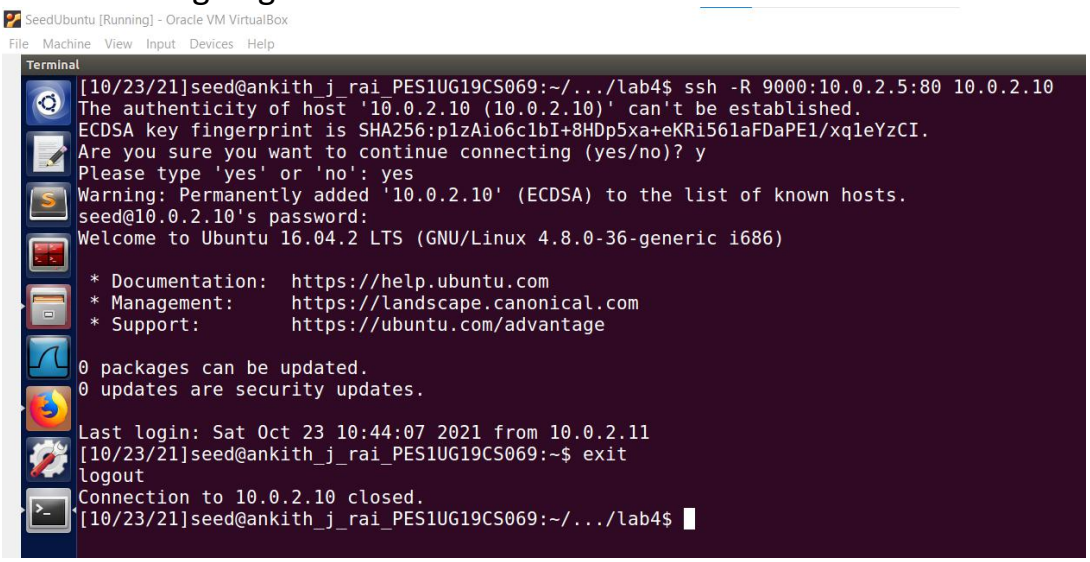


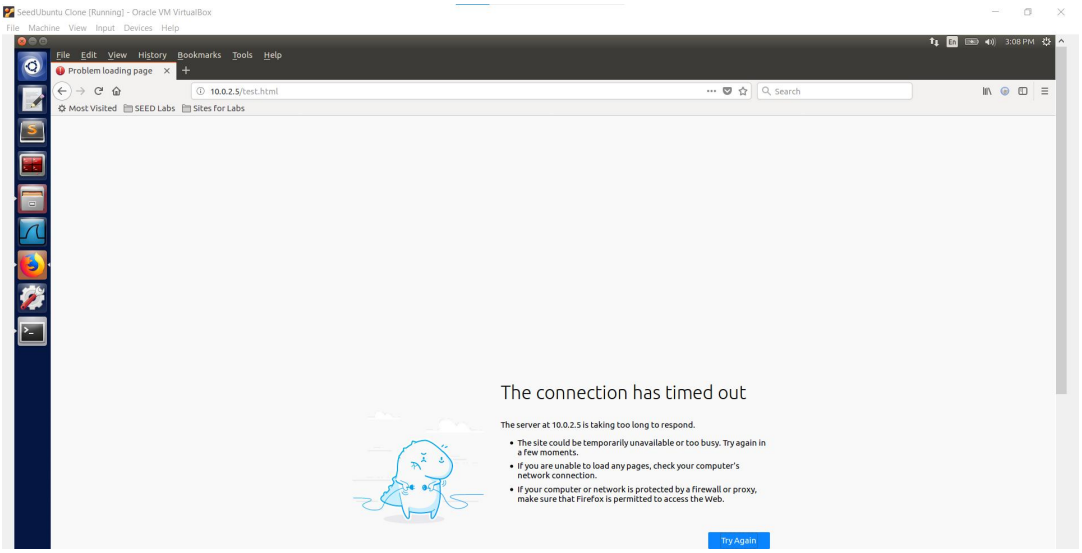
Now we are going to access the test.html on browser of VM 2.



We can see that on browser of VM 2 we are able to get access to test.html

Now we are going to close the channel





From the browser screenshot of VM 2 we can see that we are not able to access test.html after the tunnel has been broken.