**LINUX FIREWALL EXPLORATION LAB**

Contents

[TASK 1 3](#_Toc118049716)

[Prevent A from doing telnet to Machine B 4](#_Toc118049717)

[Prevent B from doing telnet to Machine A 5](#_Toc118049718)

[Prevent A from visiting an External Website 5](#_Toc118049719)

[TASK 2 5](#_Toc118049720)

[TASK 3 10](#_Toc118049721)

[Task 3.a 12](#_Toc118049722)

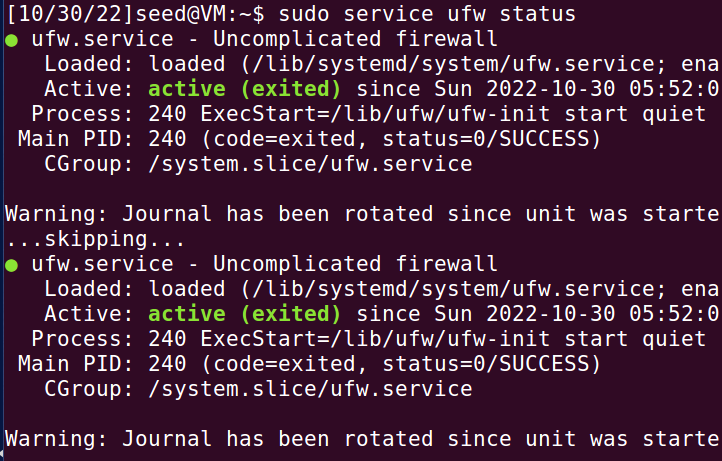
[Task 3.b 14](#_Toc118049723)

[TASK 4 17](#_Toc118049724)

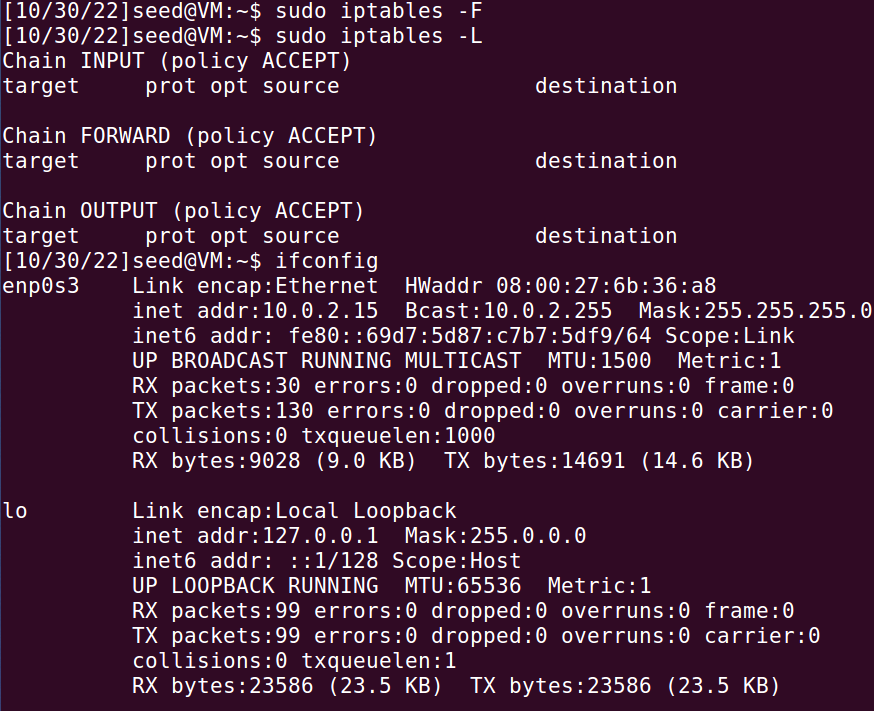
[IMPORTANT NOTE 20](#_Toc118049725)

# TASK 1

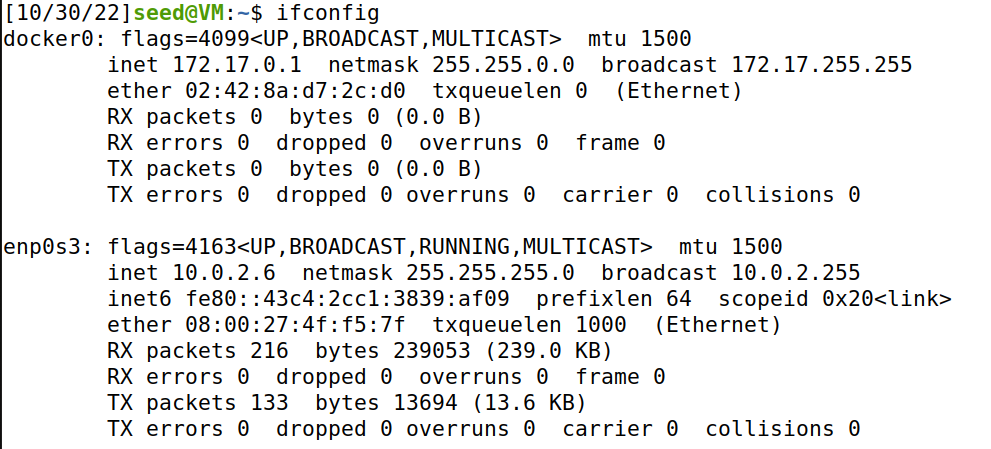
* Ensuring we have firewall iptables installed and active which it is.



* Now flushing the iptables policy and to ensure policy table is empty we will list the policy and checking subnet configurations in Machine A.

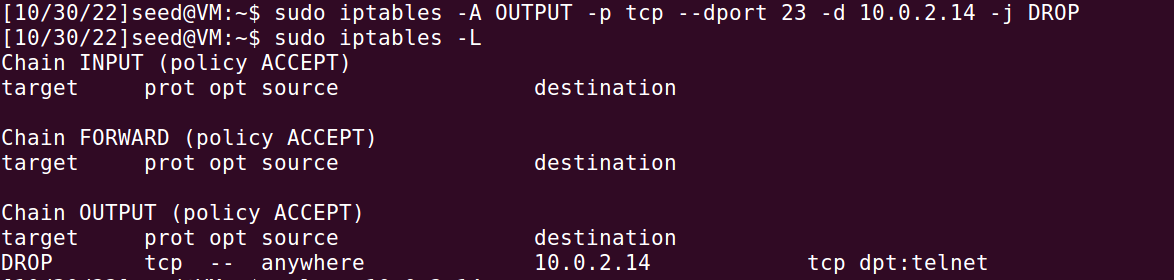


* Checking ip configurations of Machine B

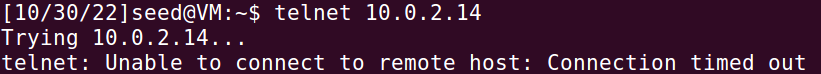


## Prevent A from doing telnet to Machine B

* Now using the command to drop the machine IP based on subnet configurations.

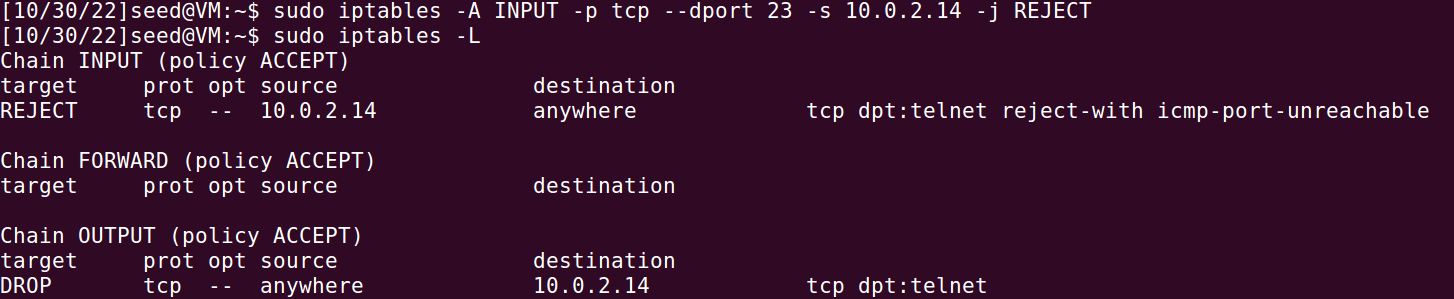


* Finally testing if we are successful in the task. Which it seems we are successful as the Machine A can’t telnet to Machine B because the connection gets timed out after trying for quite some time.



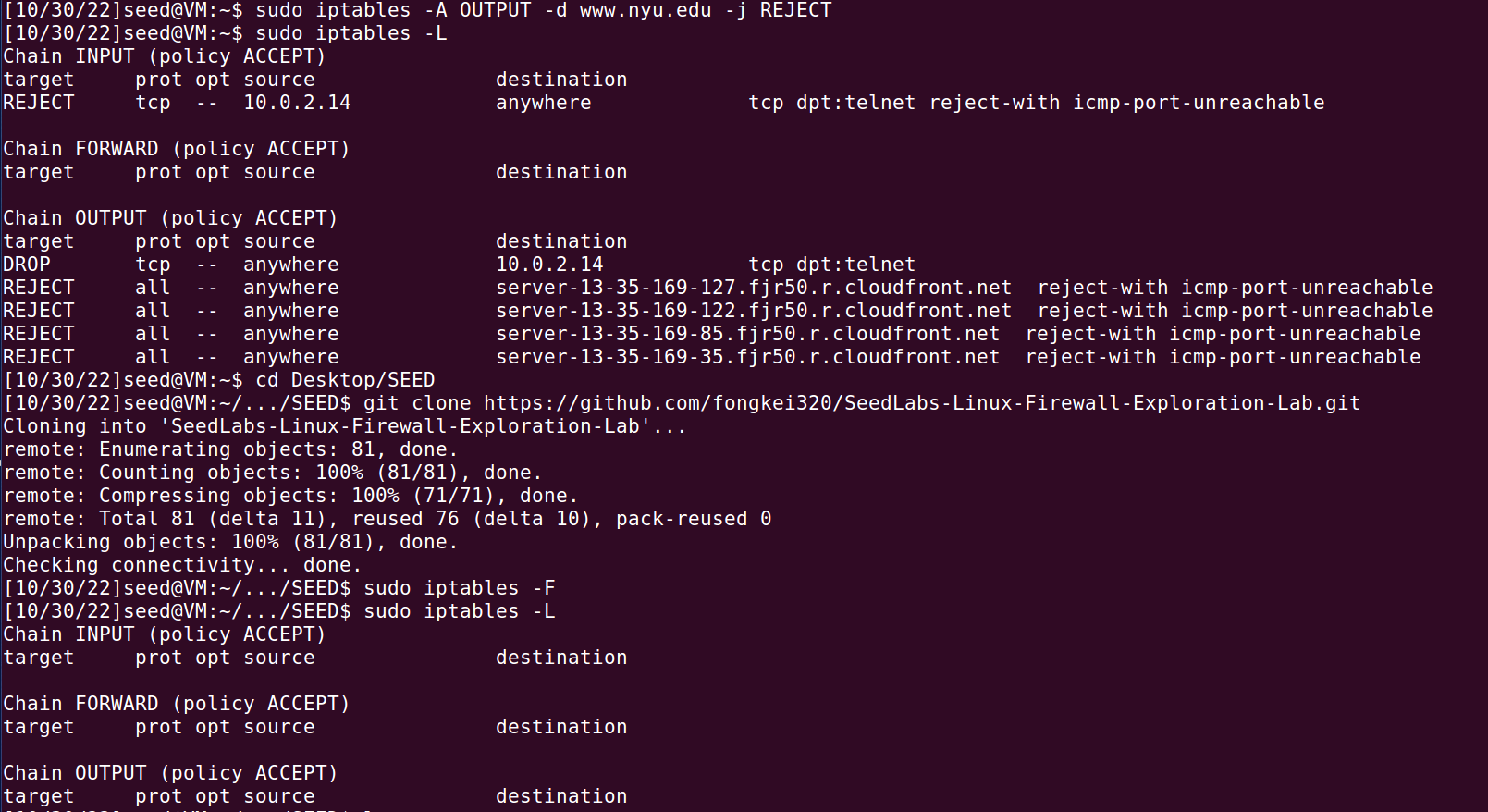
## Prevent B from doing telnet to Machine A

Implementing the firewall by rejecting input instead of output to prevent B machine from telnetting to A.



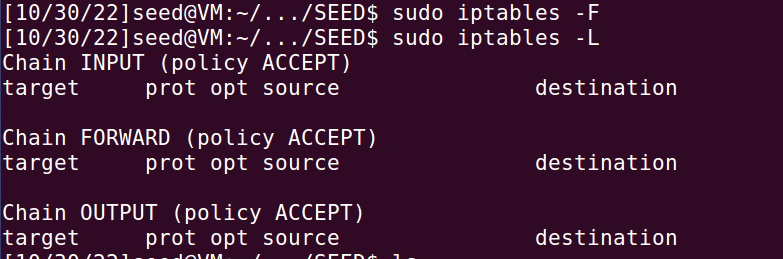
## Prevent A from visiting an External Website

* Now rejecting output to a website in order for machine A to not reach the external web which is New York University’s web page in this case.



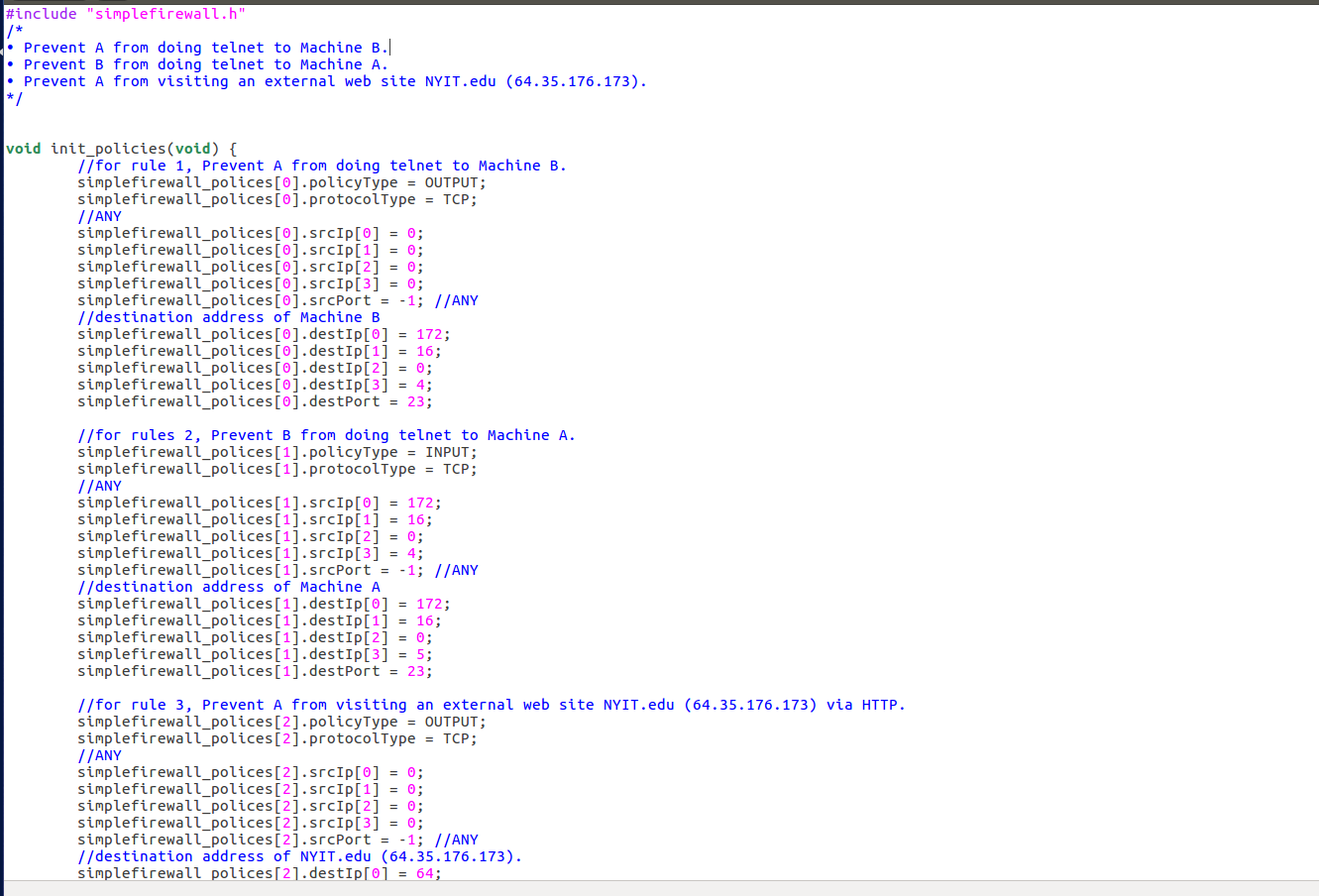
# TASK 2

* Going to Directory /Desktop/SEED. Then flushing and checking if the policy list is cleared.

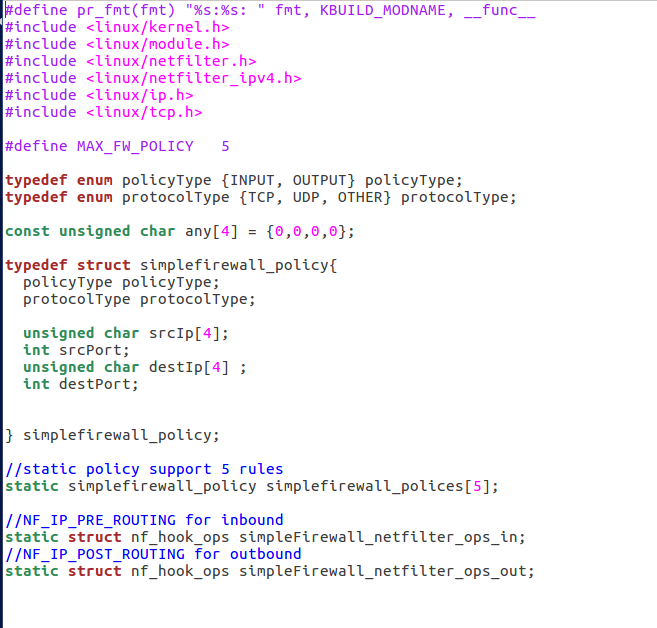
****

* Here we are using code for building a simple firewall while providing ip configurations to iptables.

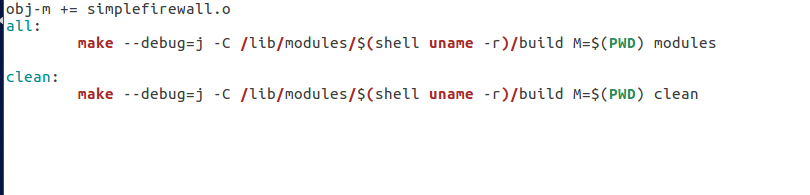
**simplefirewall.c**

****

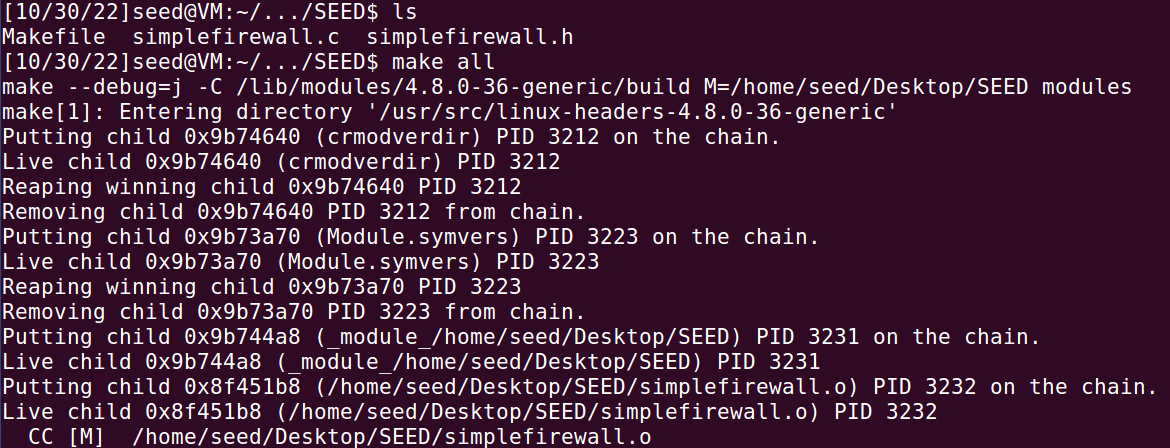
**simplefirewall.h**

****

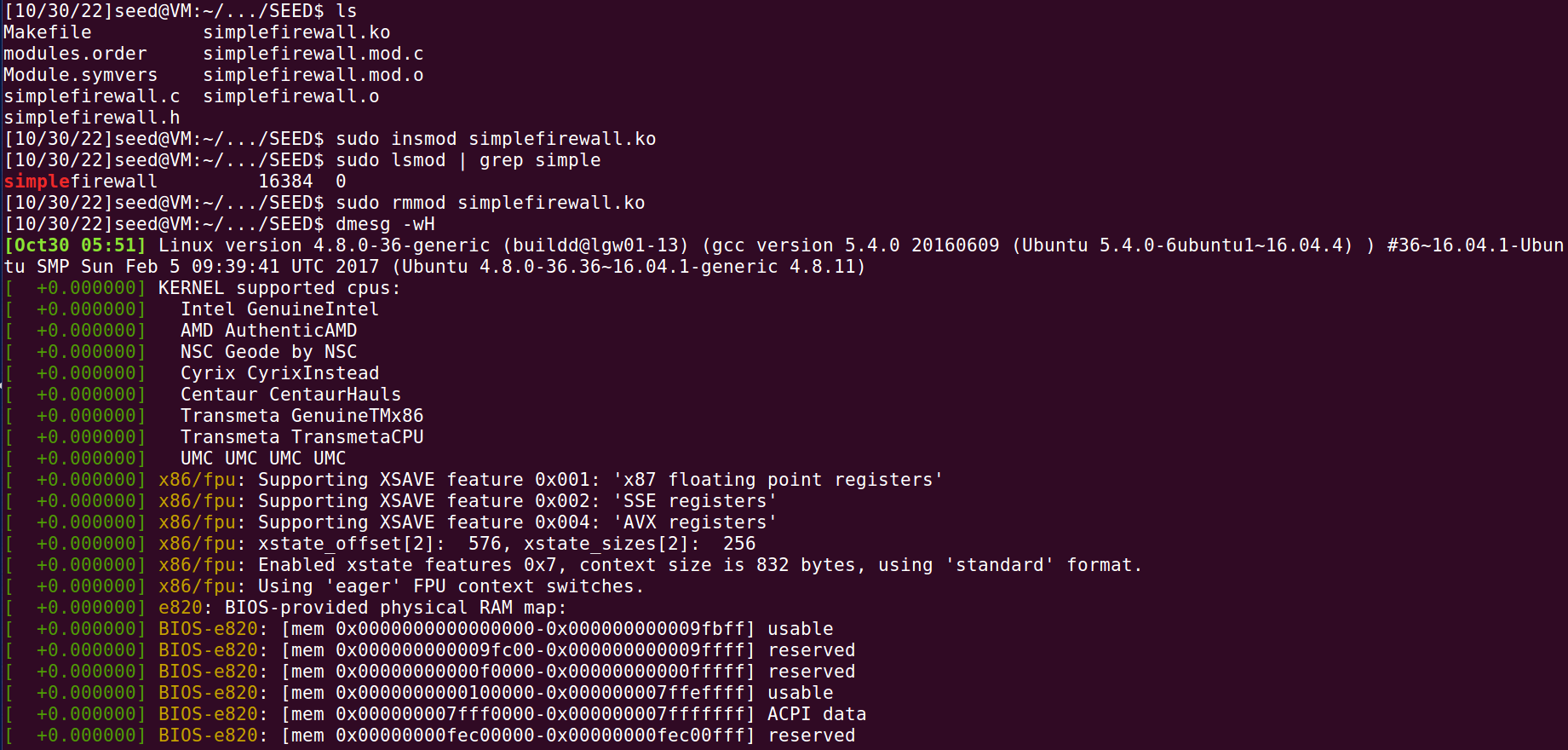
**MakeFile**

****

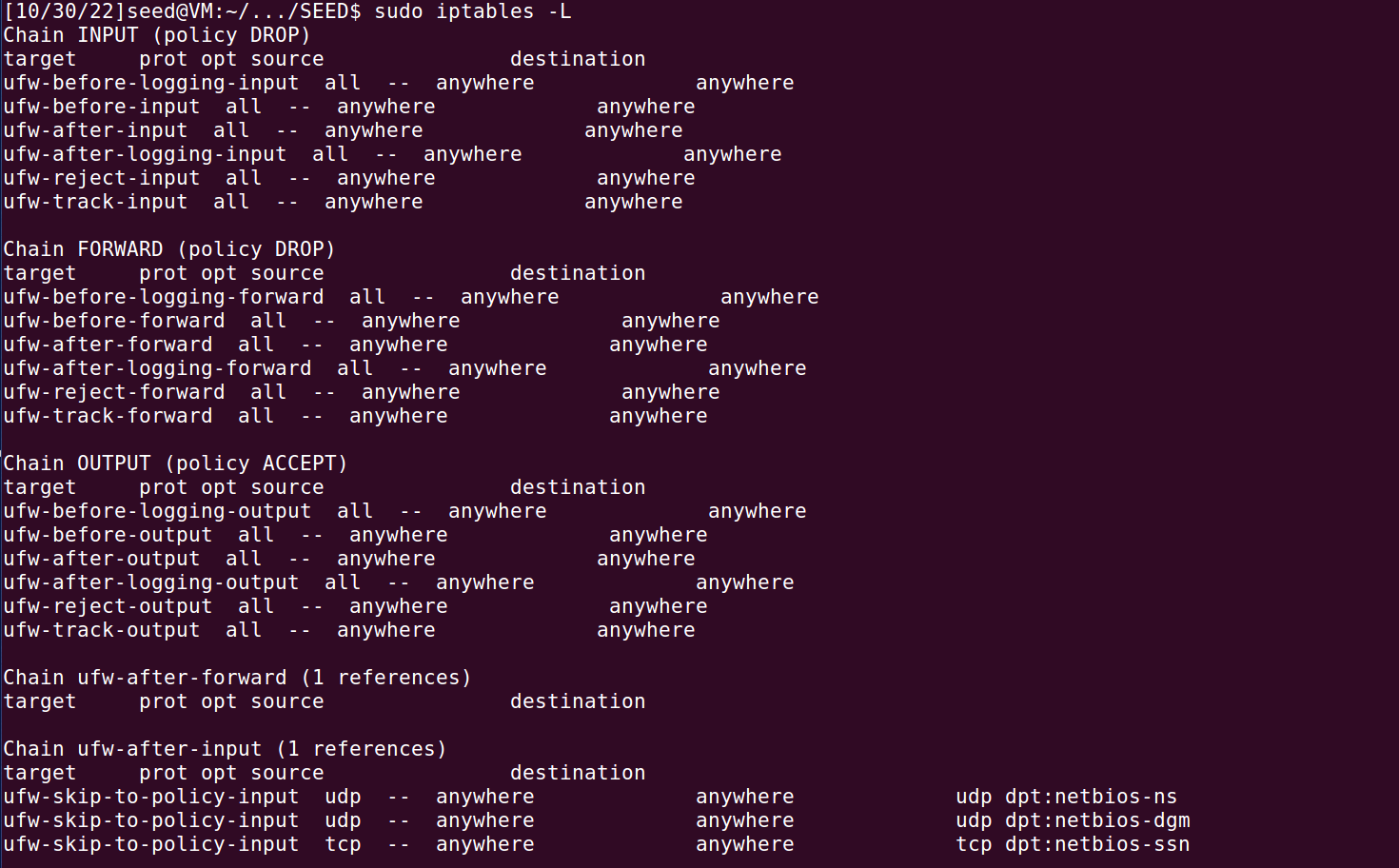
* Compiling the firewall application code files with set rules/policies.



* Checking the presence of simplefirewall.ko file and then removing it. Moreover, initializing creating simplefirewall.

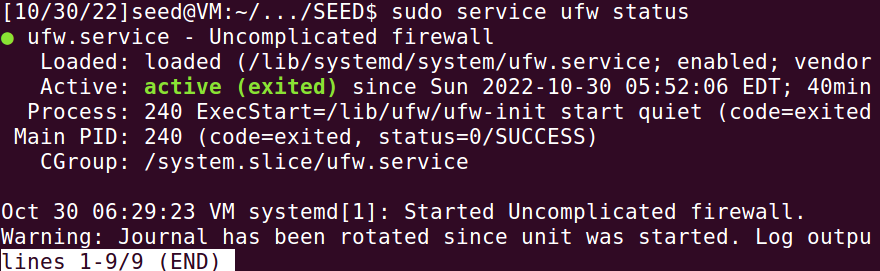


* As proof that firewall has been setup we can notice the configurations modified and added in the iptables

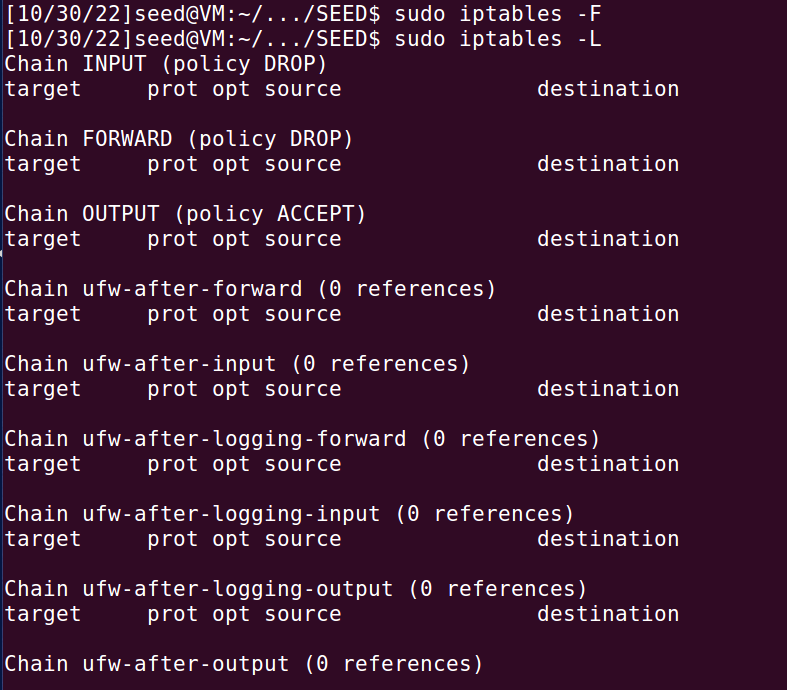


# TASK 3

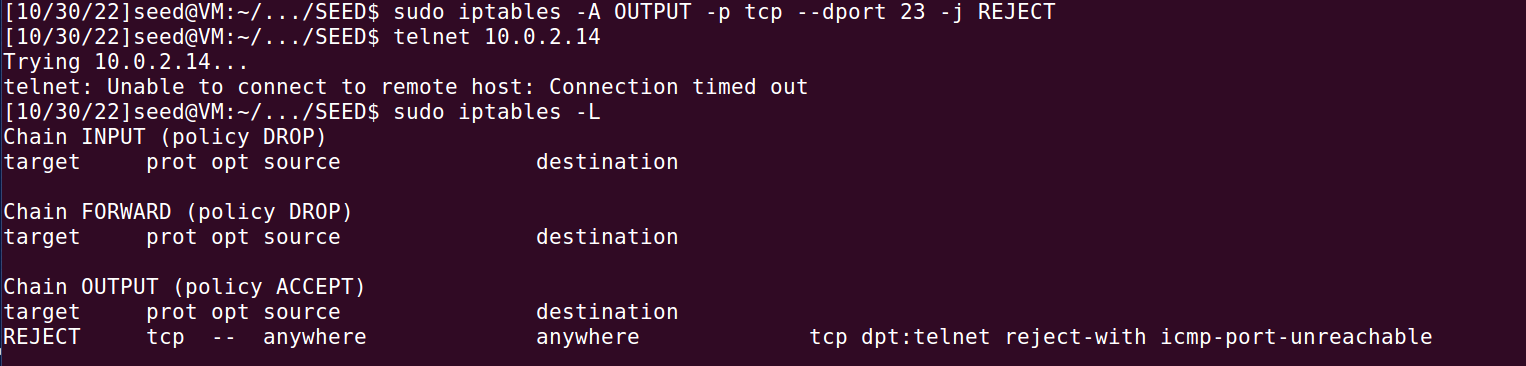
* Ensuring the ufw service is enabled.



* Flushing and checking if the iptables have been flushed of previous configurations.

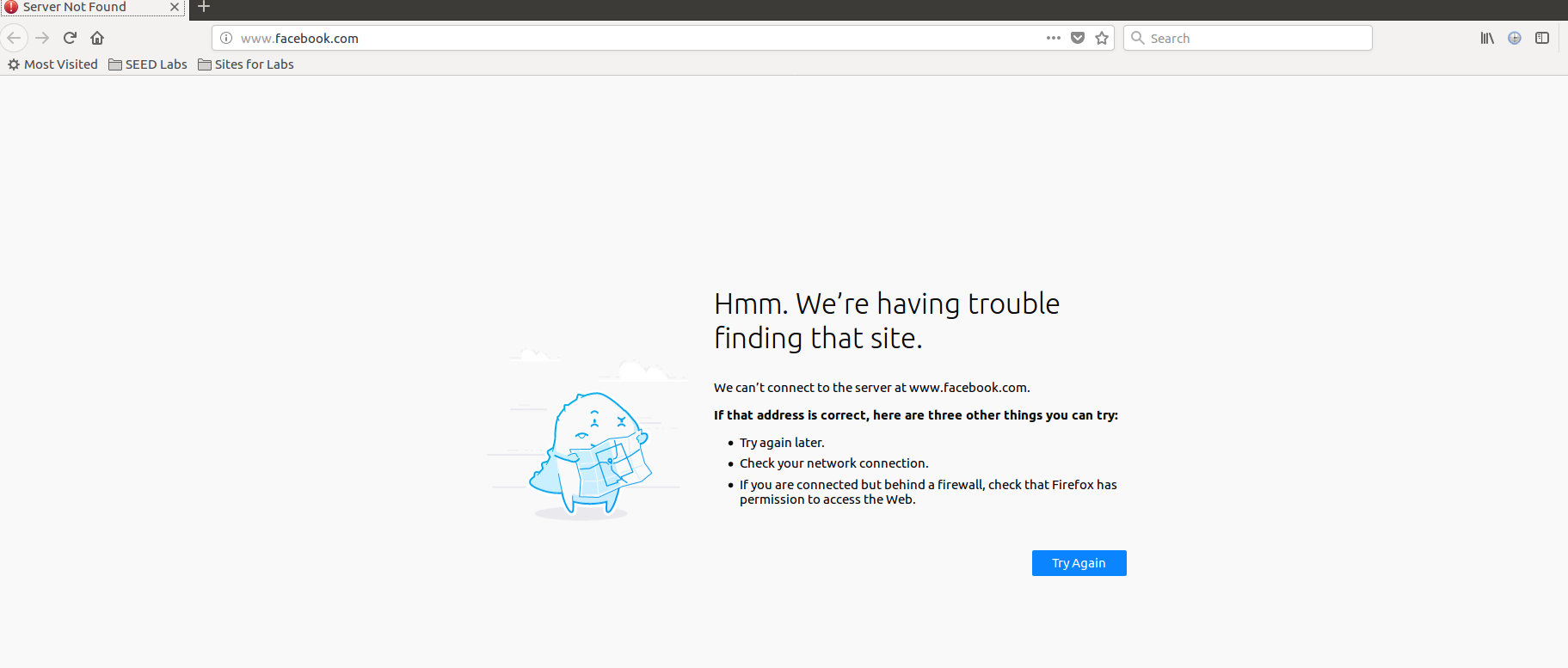


* Now we have blocked all the outgoing connections to telnet port. It can be seen as the connection is not made instead timed out and iptables have the configurations as well.



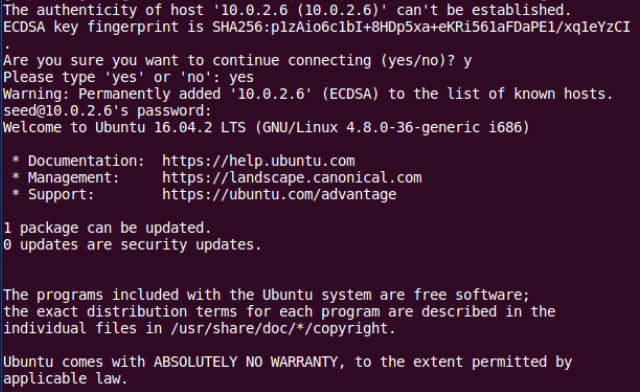
* Now verifying of traffic blocked going to Facebook



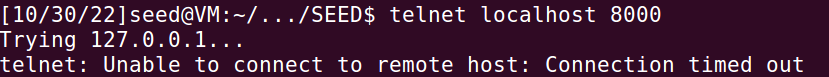


## Task 3.a

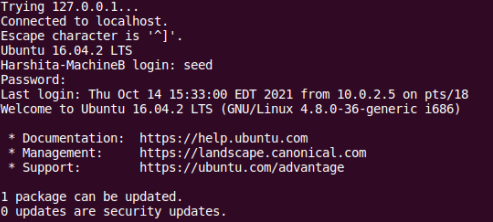
* Using the given command to connect to Machine B using command ,”ssh –L 8000:10.0.2.6:23 seed@10.0.2.6”



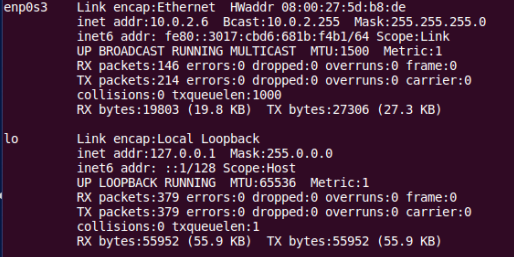
* After closing the connection I noticed we can’t reconnect.



* Telnet on Port 8000

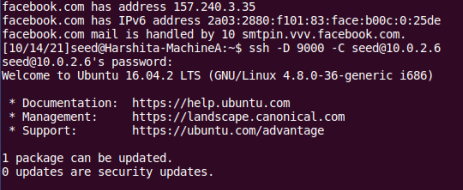


* Now verifying connection by checking ip configurations

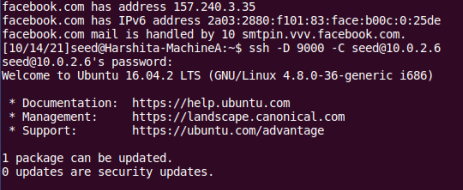


## Task 3.b

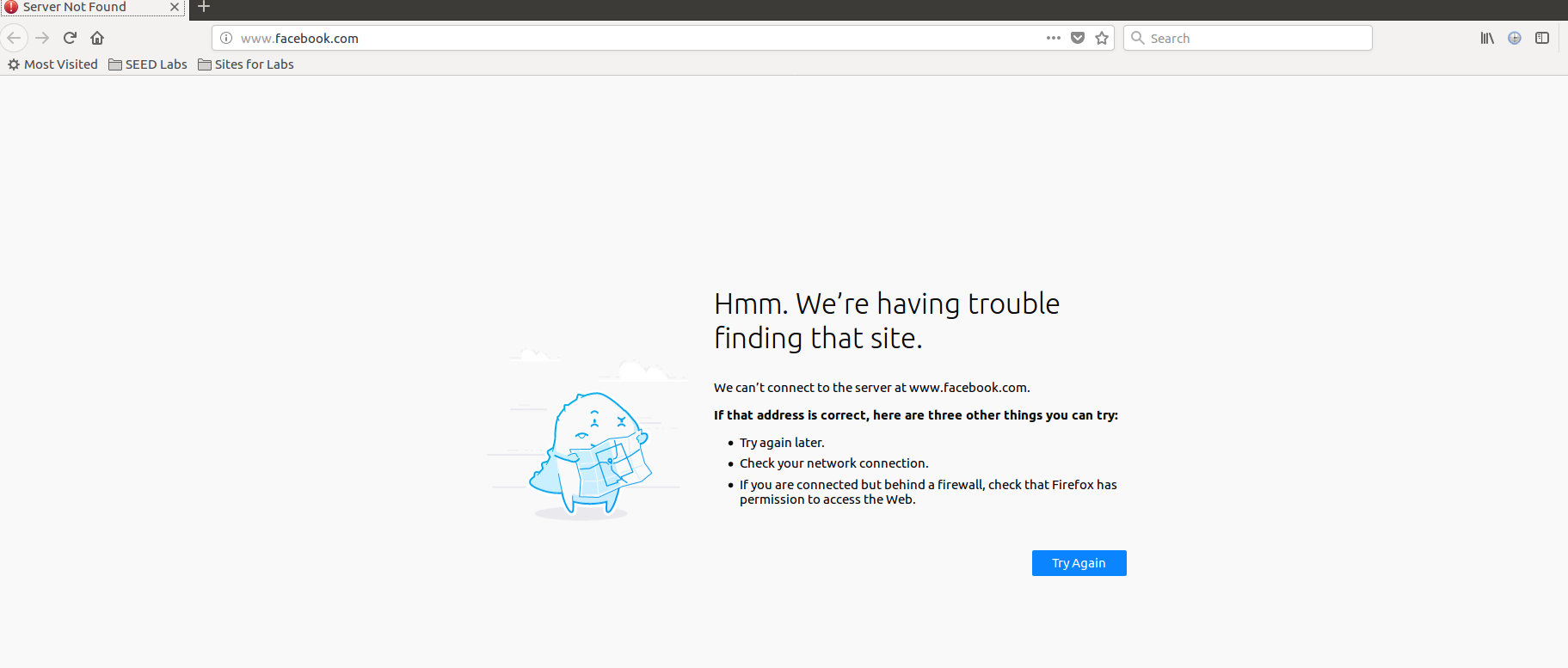
* Now trying to connect to Facebook using SSH tunneling using command,”sudo host facebook.com”

****

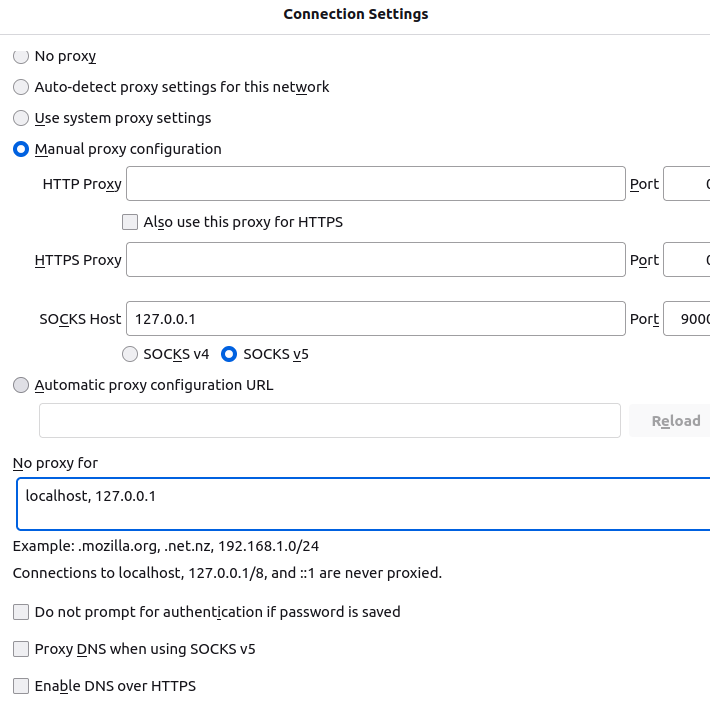
* Now connecting with Machine B for the above purpose with the command,”ssh –D 9000 –C seed@10.0.2.6

****

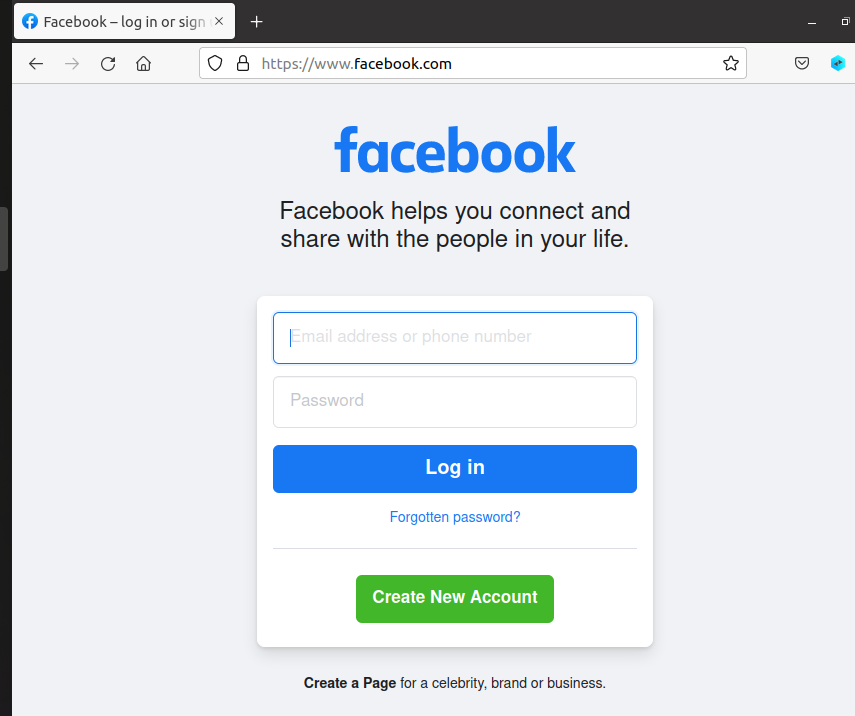
* Now I can’t connect to Facebook



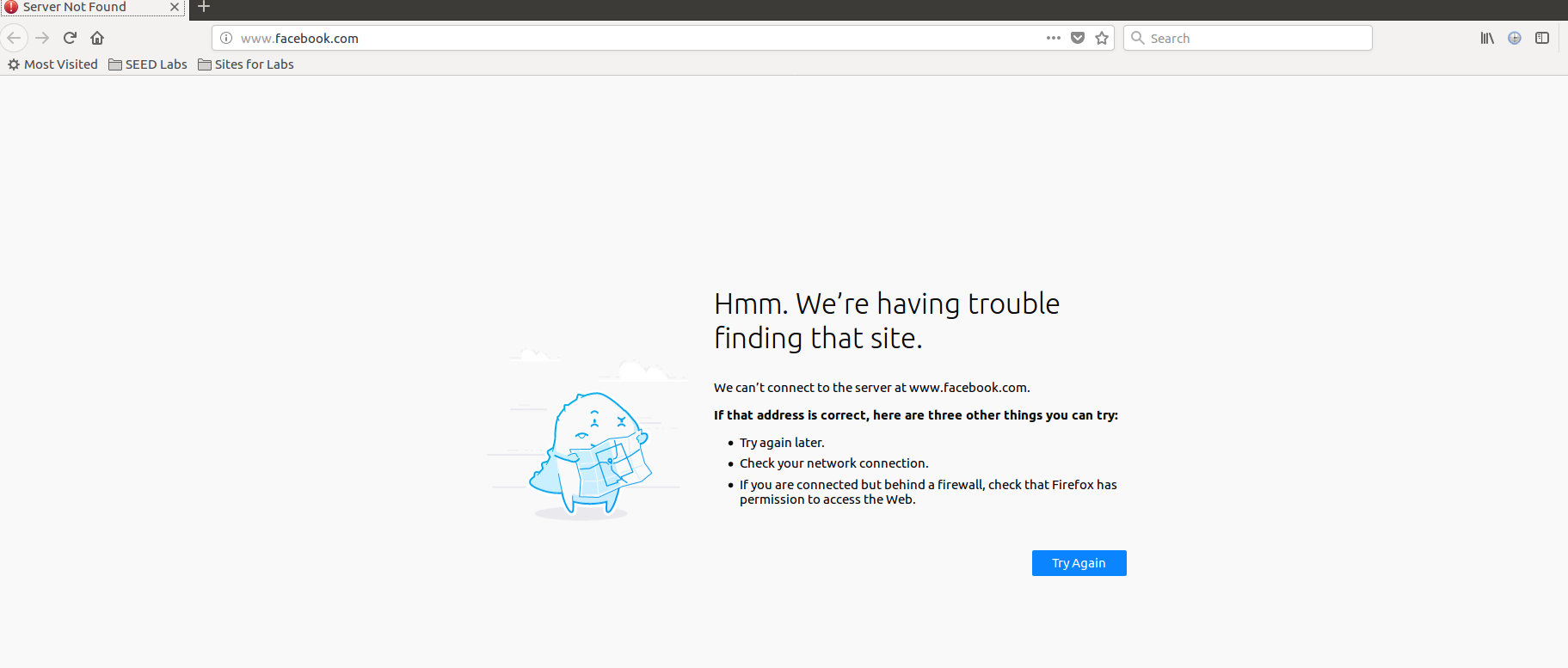
* Making some proxy changes in order to establish the connection

****

* Now Facebook is accessible.

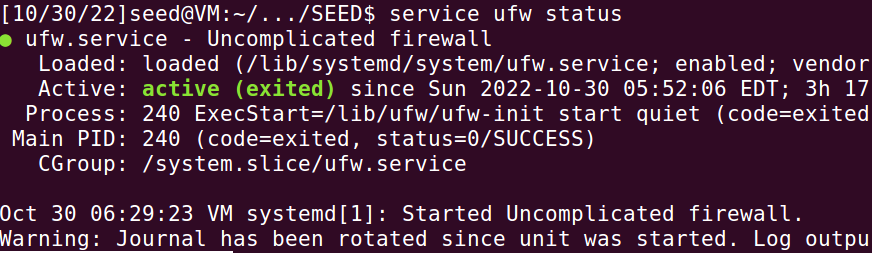
****

* After closing connection and retrying to connect I couldn’t succeed.

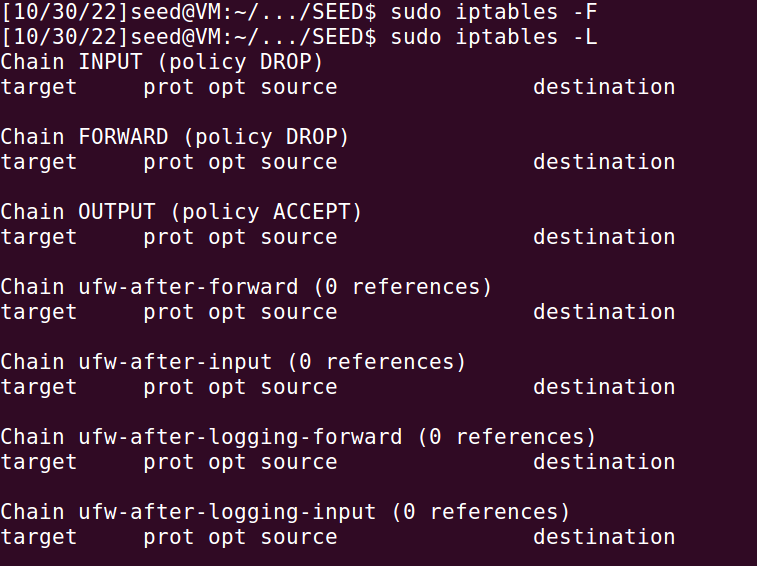


# TASK 4

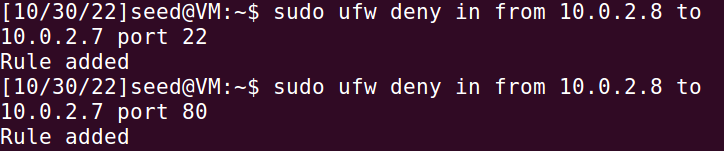
* Ensuring the ufw service is enabled.



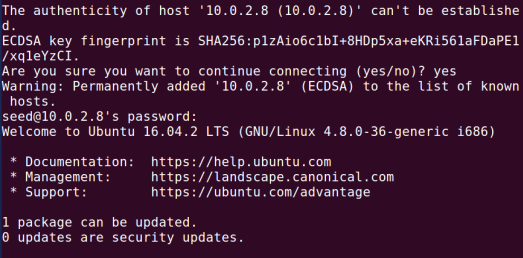
* Flushing and checking if the iptables have been flushed of previous configurations.



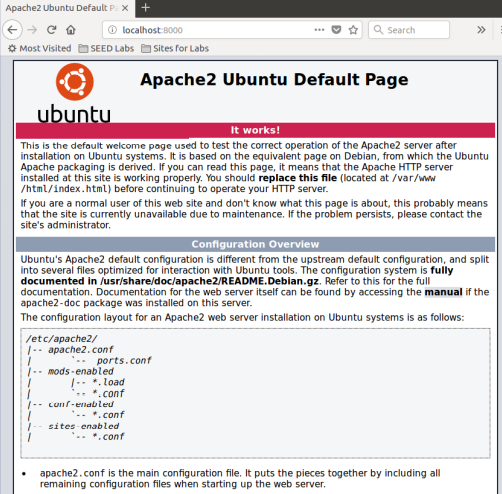
* Block Machine B from accessing port 22 and 80.



* Now used the command “ssh –R 8000:localhost:80 [seed@10.0.2.8](mailto:seed@10.0.2.8)” to setup a reverse SSH on Machine A.



* Now accessing the web page from Machine B available on Machine A.



# IMPORTANT NOTE

I had to make new Machine B in due to some problems during work that’s why there might be varying IP addresses.