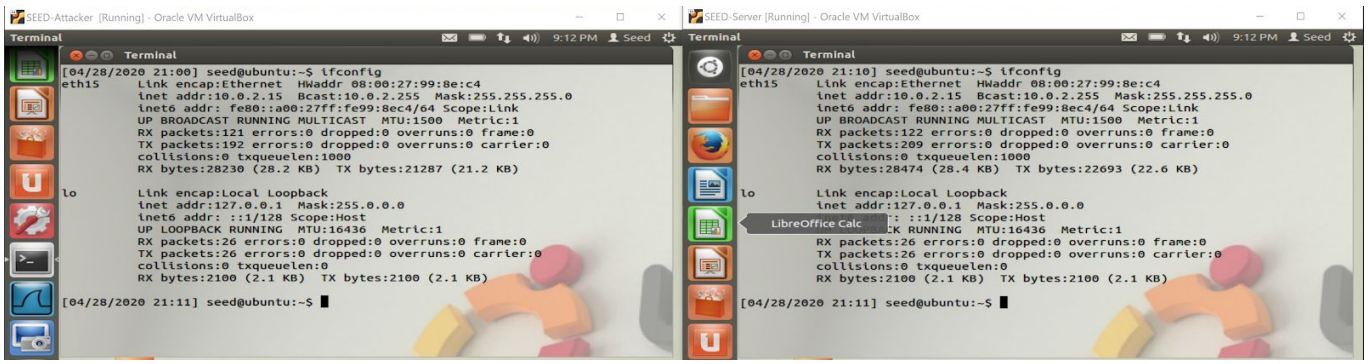
Catherine Nguyen
CSC 154
04/28/2020

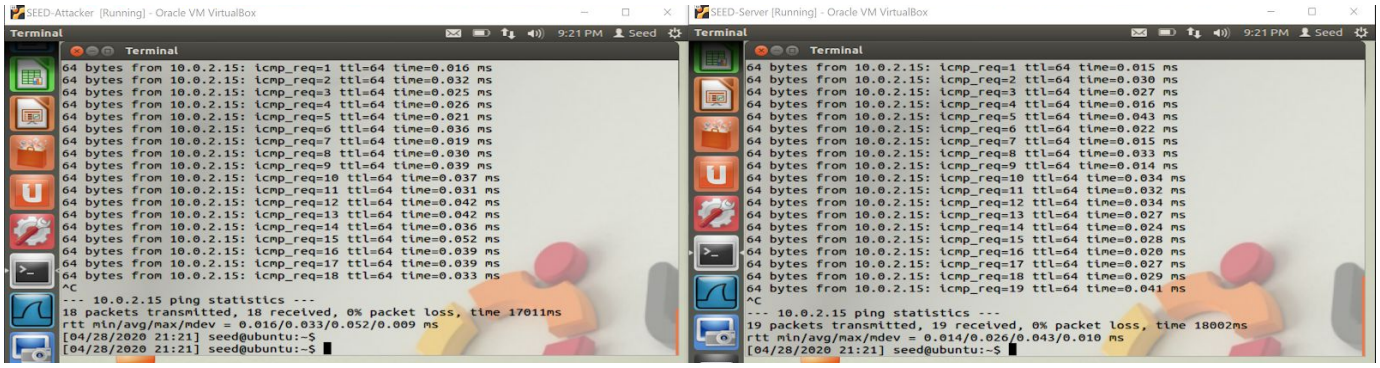
Lab 4 Heartbleed Attack

- First, the thing we have to do is find the IP addresses of both machines using **ifconfig**

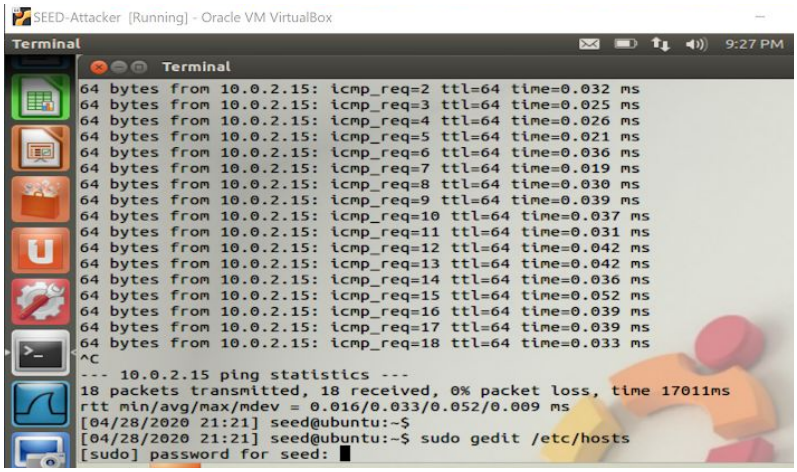


SEED-Attacker IP: 10.0.2.15
SEED-Server IP: 10.0.2.15

- **Ping** each other to see if they are communicating. Success

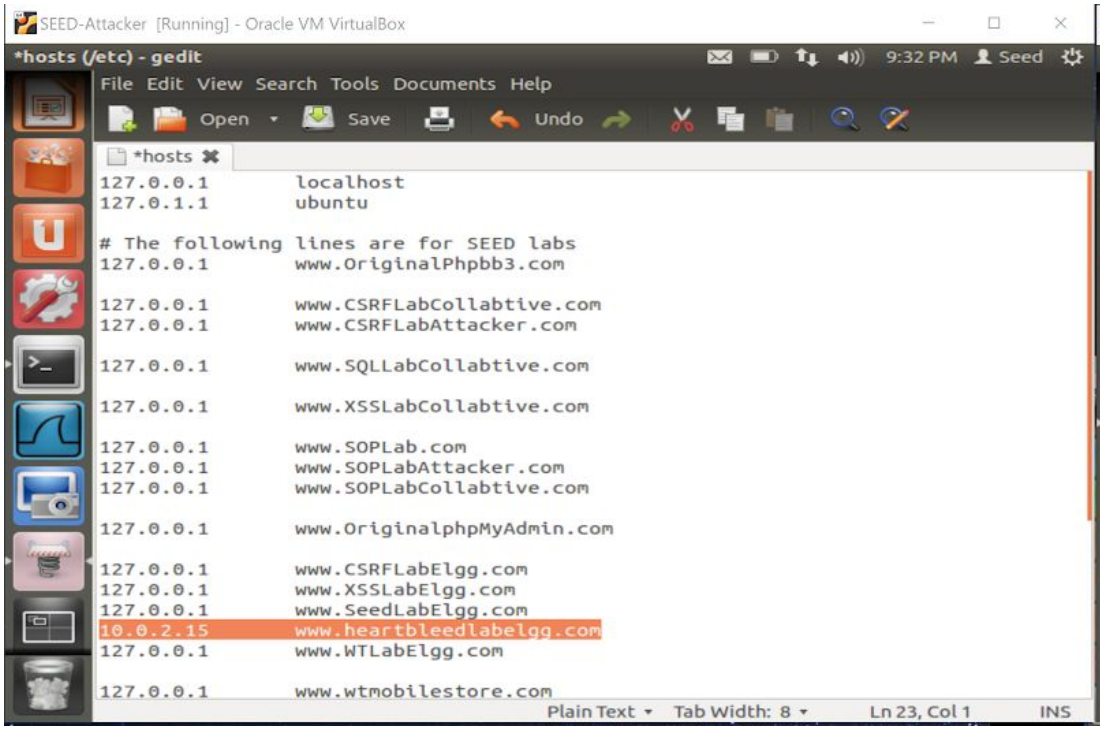


- **sudo gedit /etc/hosts** run this command on SEED-Attacker which is the client in this case.



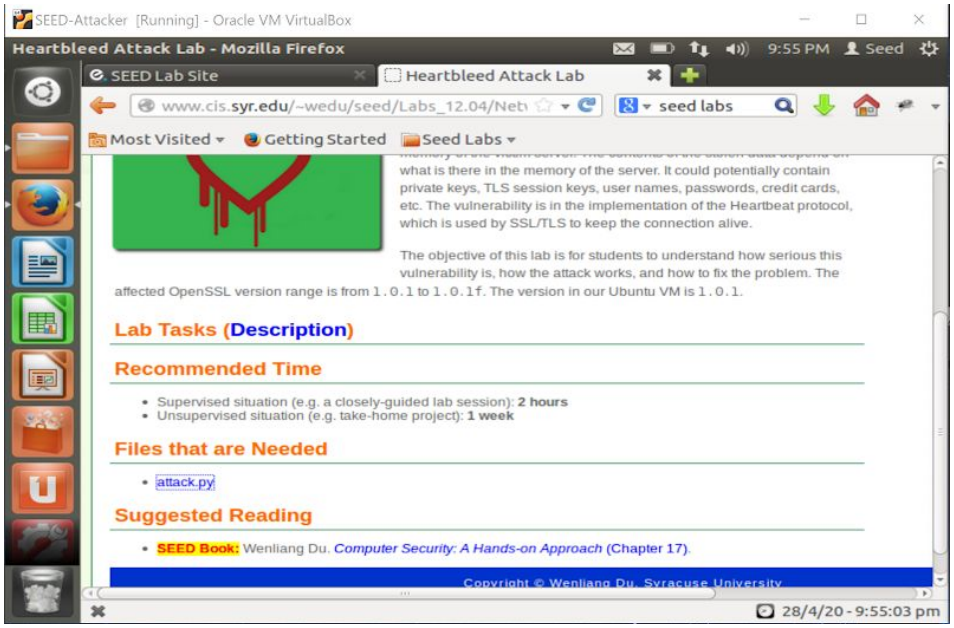
enter password: **dees**

- Then edit the host file and **change the IP for www.heartbleedlabelgg.com** with the **SEED-Server IP address 10.0.2.15**



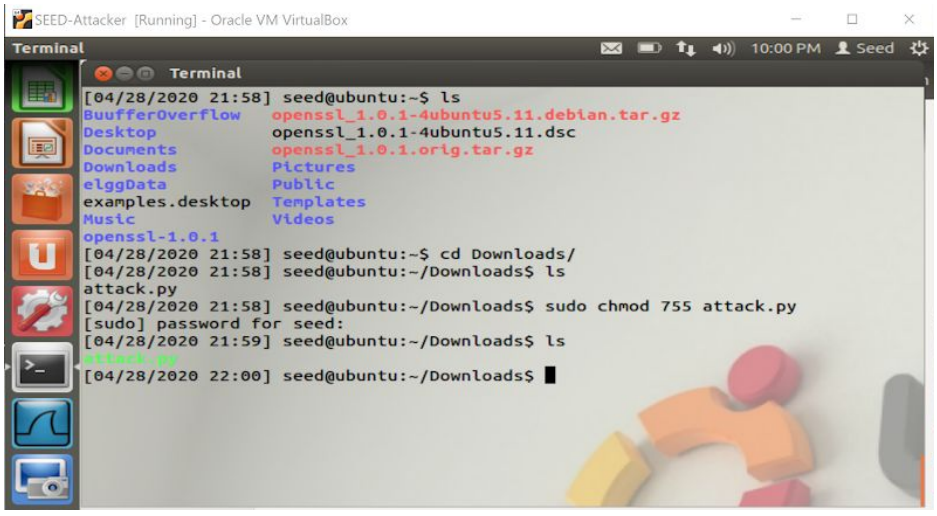
Now that it is changed the web browser will go for this IP address for traffic meaning it will contact this IP address for the website: www.heartbleedlabelgg.com. As a precaution, you can check your web browser and go to the heartbleedlabelgg website to see if it works.

- Next is to **download the attack.py to the Attacker VM** which in this case is **SEED-Attacker**



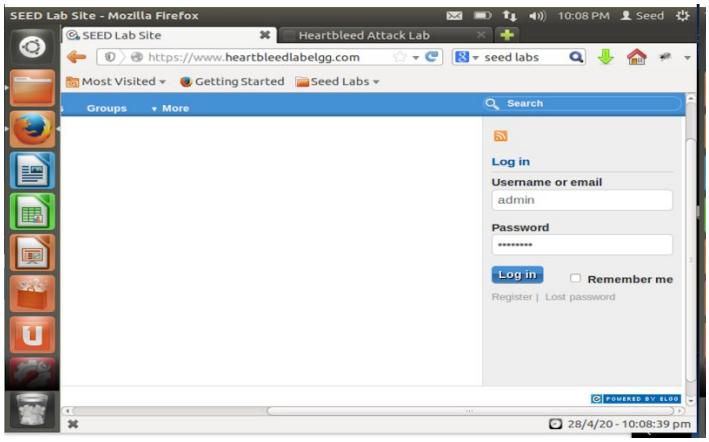
Save link as

- Now find that file and run **sudo chmod 755 attack.py** to make the attack.py executable

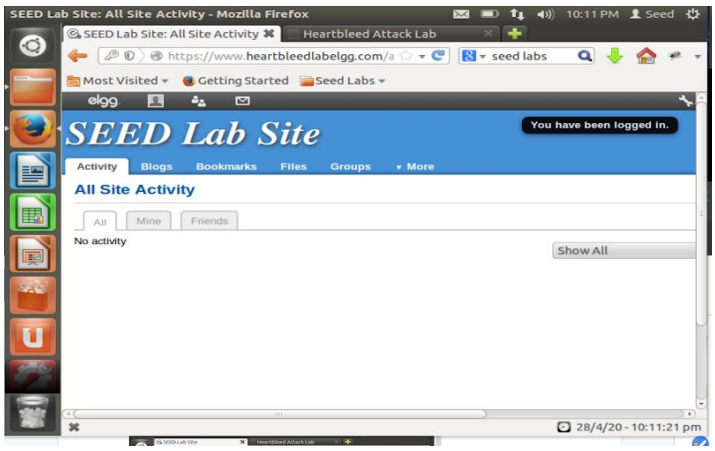


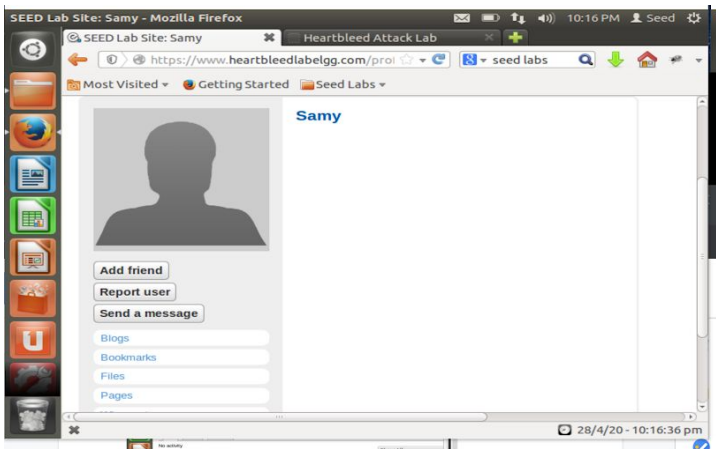
highlight means its exe.

- We are ready to launch an attack but because the server is idle we would get empty results some have to go to www.heartbleedlabelgg.com and **log in as one of the users.**
  Username: admin
  Password: seedelgg

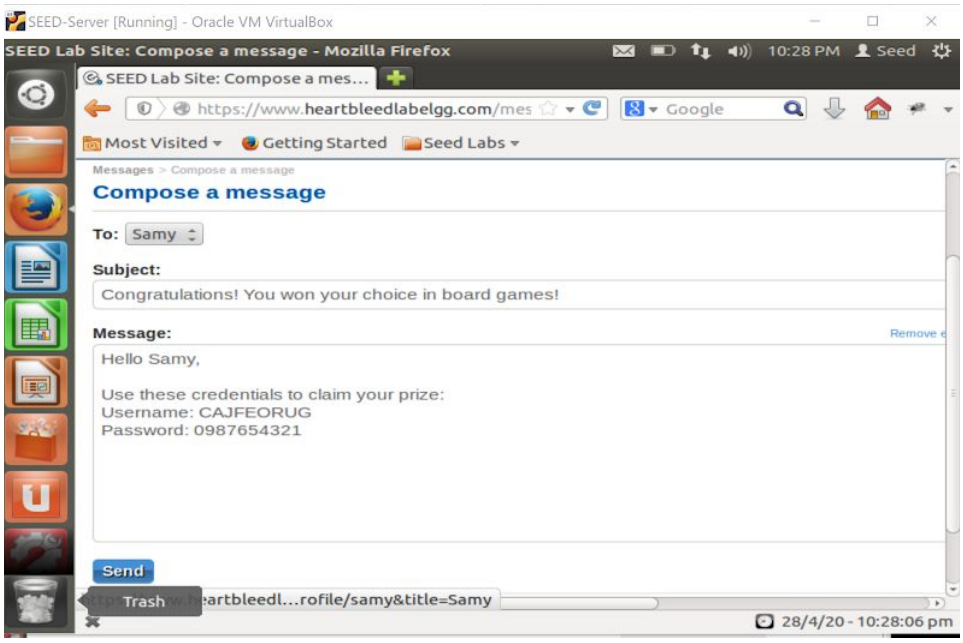


- Now that we are logged in we will have to do log some activities. We have no friends so we go to members tab and add people, for example, Samy, Charlie, Boby, admin

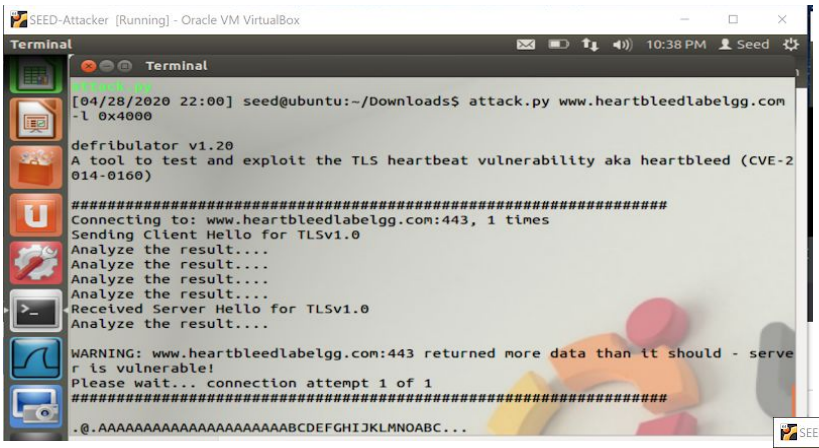


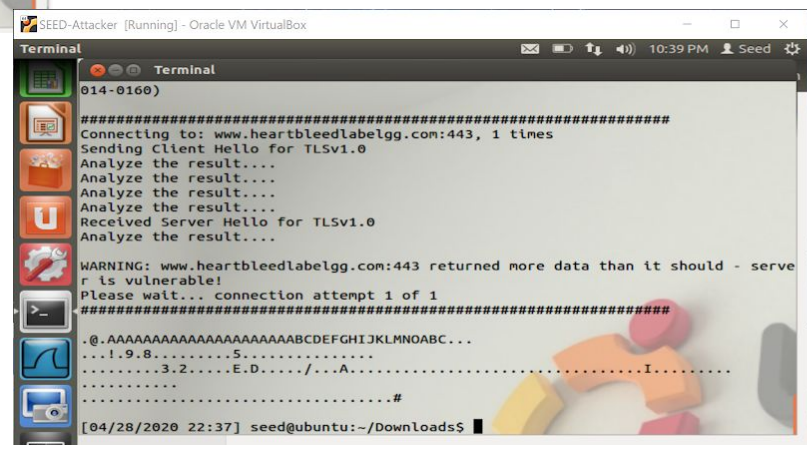


- Now that we have some friends we can now compose a message and log that in as an activity. We sent a message saying he won his choice in board games and to do so he will have to use those bank credentials. But in reality, we will be dumping 4000 bytes worth in memory when it should actually be 1000 bytes

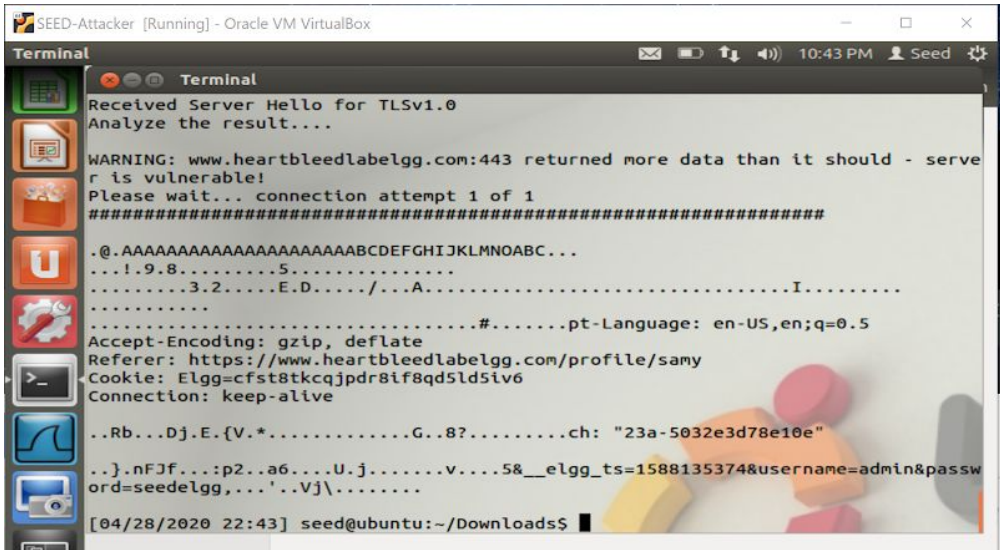


- Now that's the Server is busy, we can launch an attack by running **attack.py** www.heartbleedlabelgg.com **-l 0x4000.** Because the server didn't verify the number of bytes sent. The server starts giving 4000 bytes of data back from the starting address from memory.

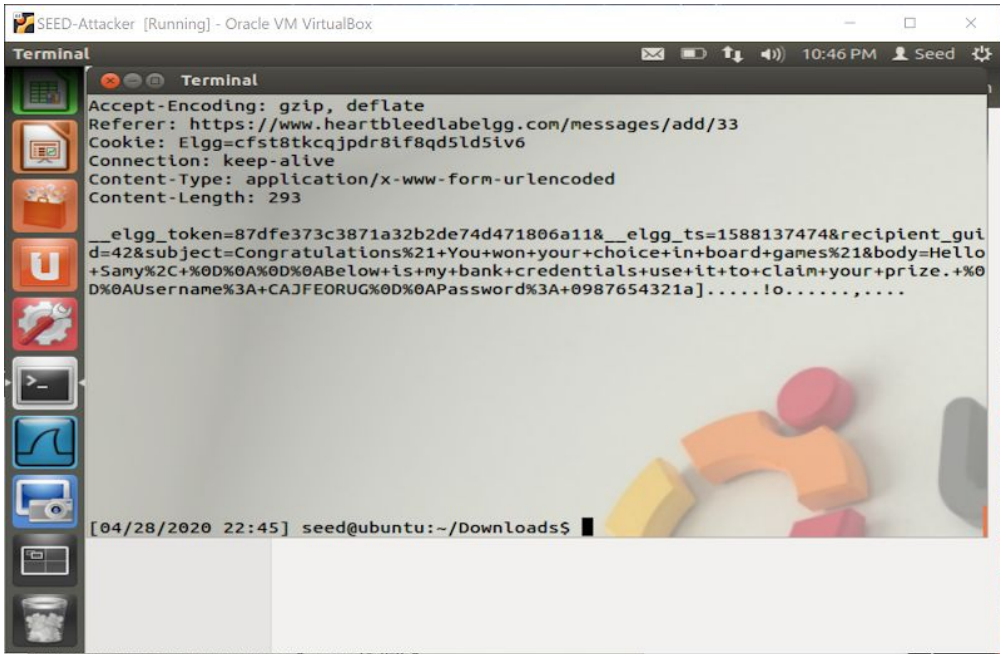




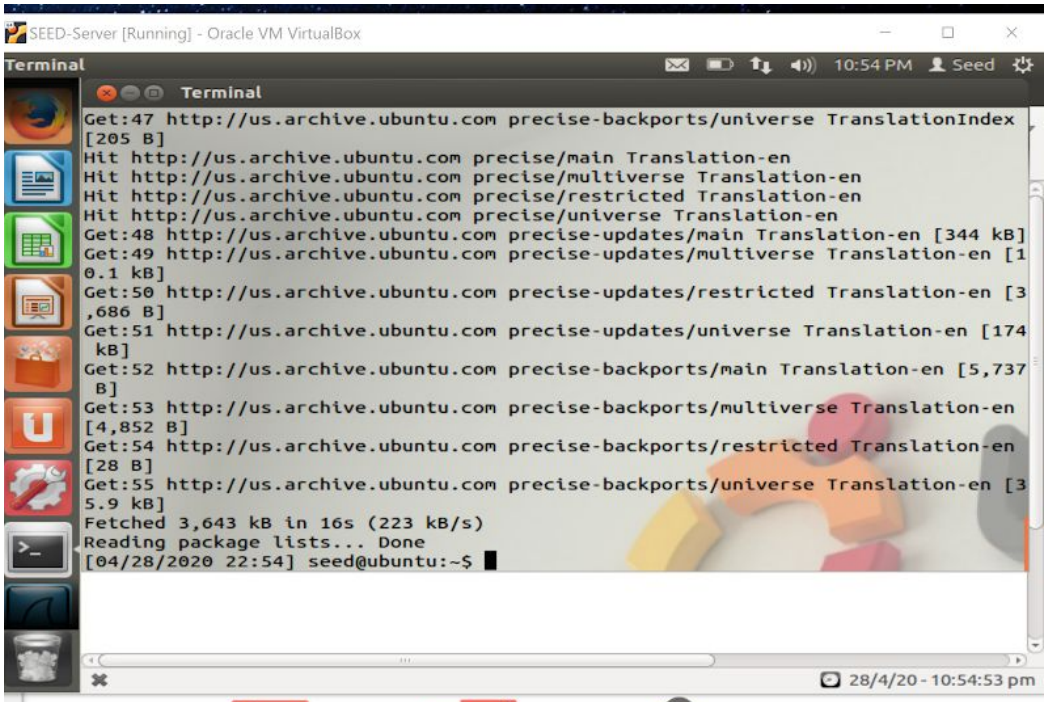
- The second run of the attack. Repeat to get more info. This time we got Samy's profile information.



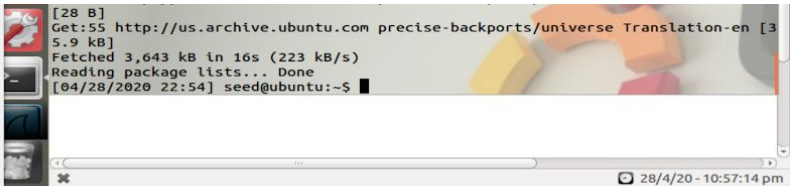
- Future run, we can now see the contents of the message we sent earlier. In a real-life scenario if I really were an attacker I can use these bank credentials for what i wanted.



- As a countermeasure, we can update OpenSSL with **sudo get update** and **sudo apt-get upgrade**



- Now we run an attack and we can't get any information.



- In conclusion, after the server VM has updated we were no longer able to get any information about the messages contents or the receiver's info. This means that SSL/TLS is not secure during the the old version of OpenSSL.