Winnie Delinois

Professor Kim

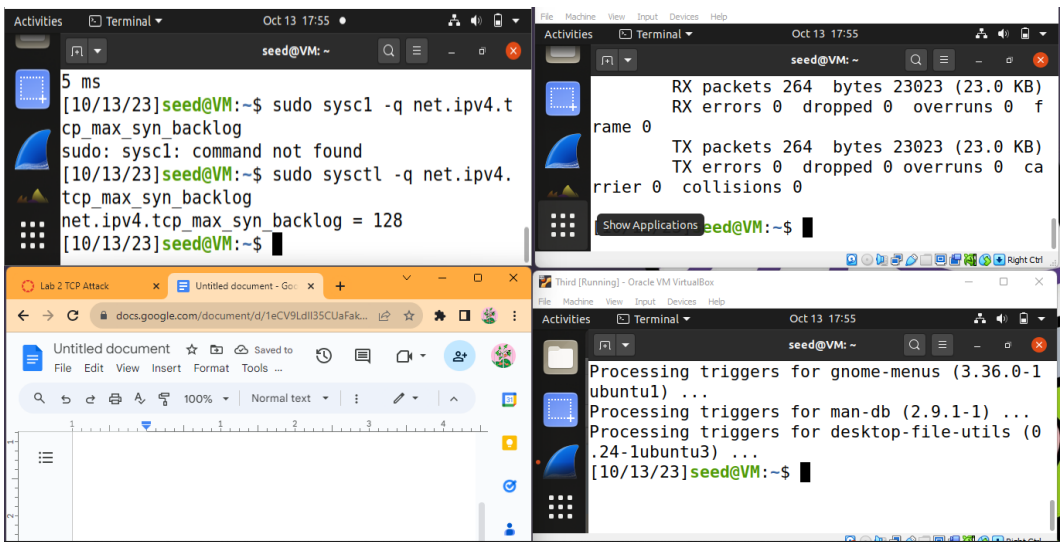
CSIT 460-03

17 October 2023

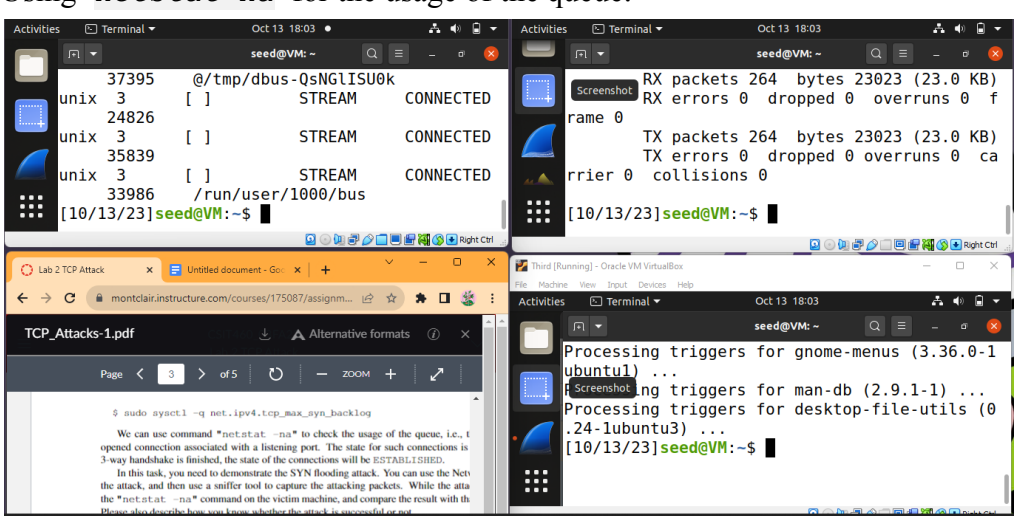
Lab 2

3.1: **SYN Flooding Attack**

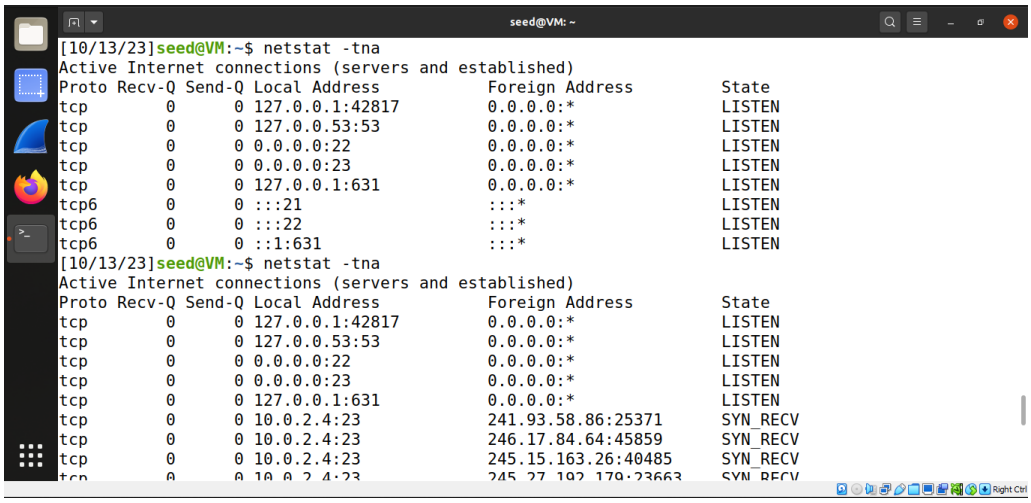
This checks how many packets the client/computer can queue. The attacker sends the packet in an attempt to fill up the queue so that the client can't accept any more connections



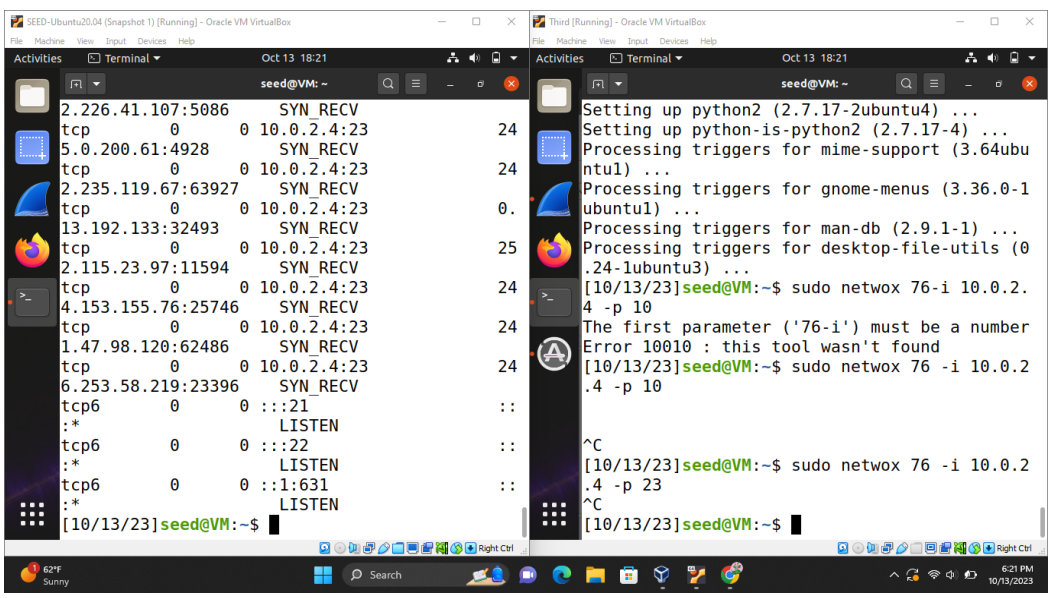
Using "`netstat-na`" for the usage of the queue:



Queue before the attack:



Queue after the attack:

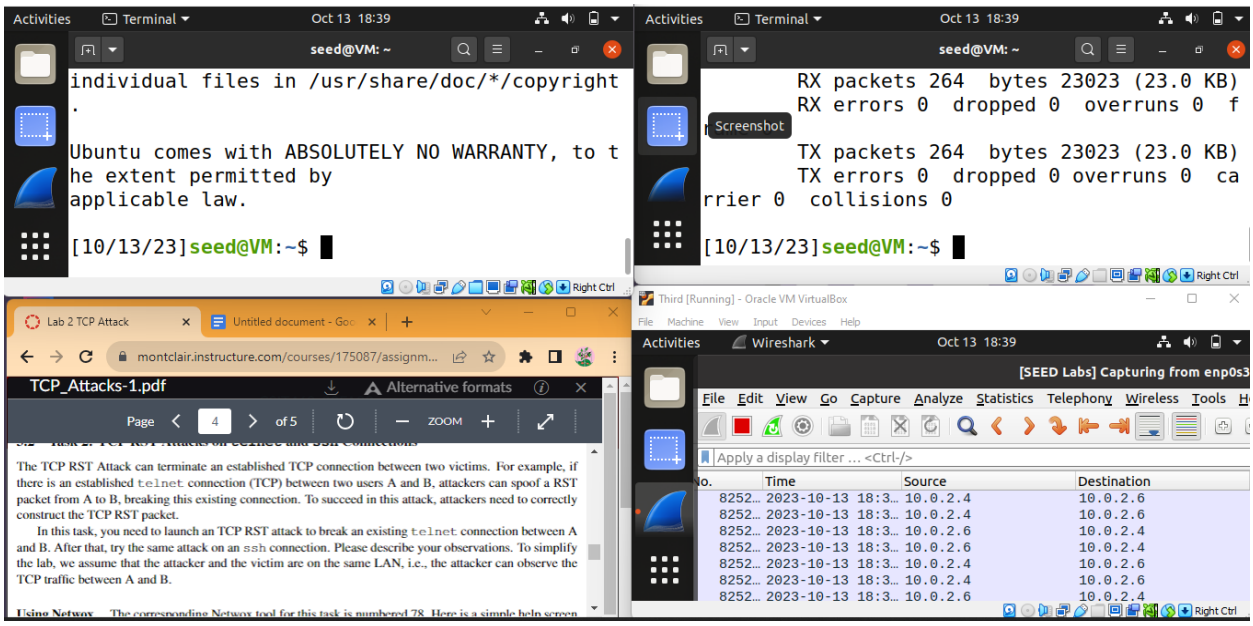


SYN Flooding Attack Summary:

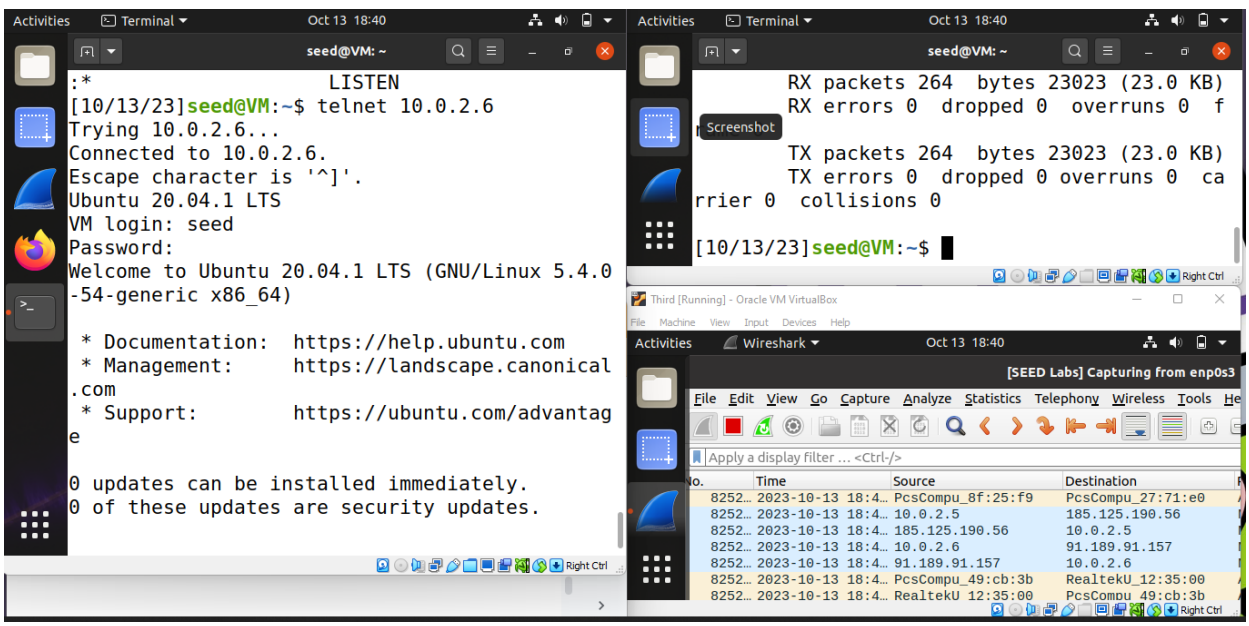
To summarize this section, the main goal is to flood the client's queue with as many packets as possible. To do so, I first checked how many packets the client could queue using "`sudo sysctl -q net.ipv4.tcp_max_syn_backlog`". Afterward, I used "`netstat -tna` to check the queue usage before the attack. After the attack, the queue can't take any more connections and is flooding.

3.2: **TCP RST Attacks on telnet and ssh Connections**

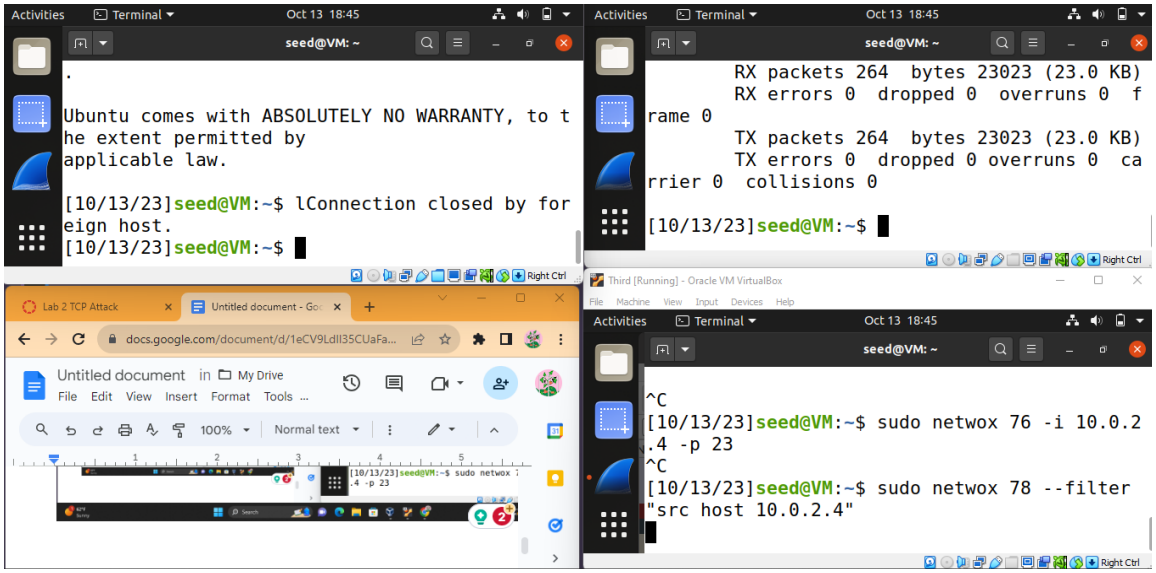
Telnet:



Connecting client to server and confirming their connection through Wireshark:



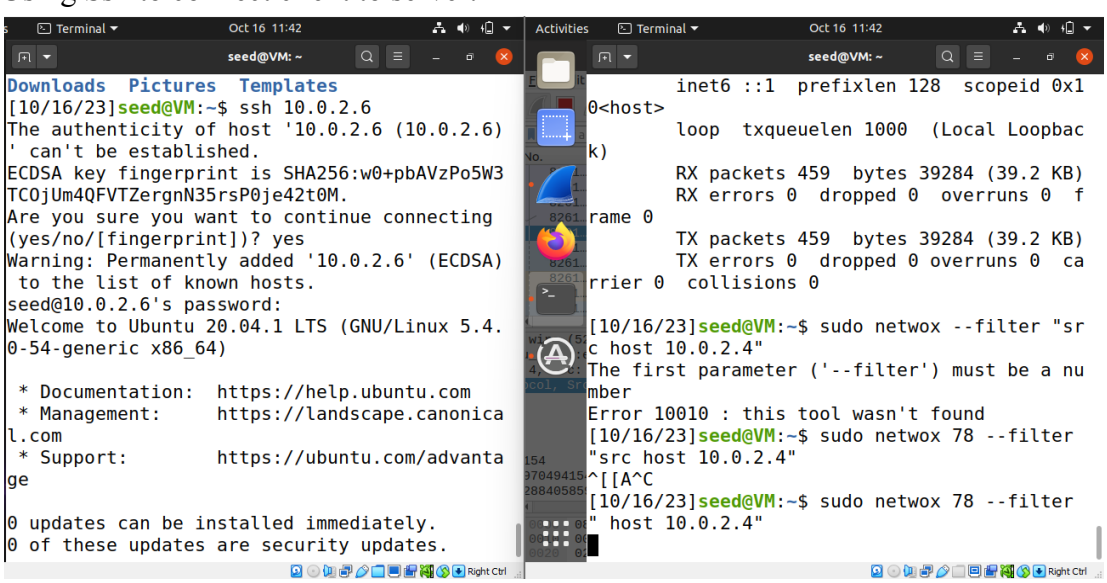
Closing the connection from the attacker:



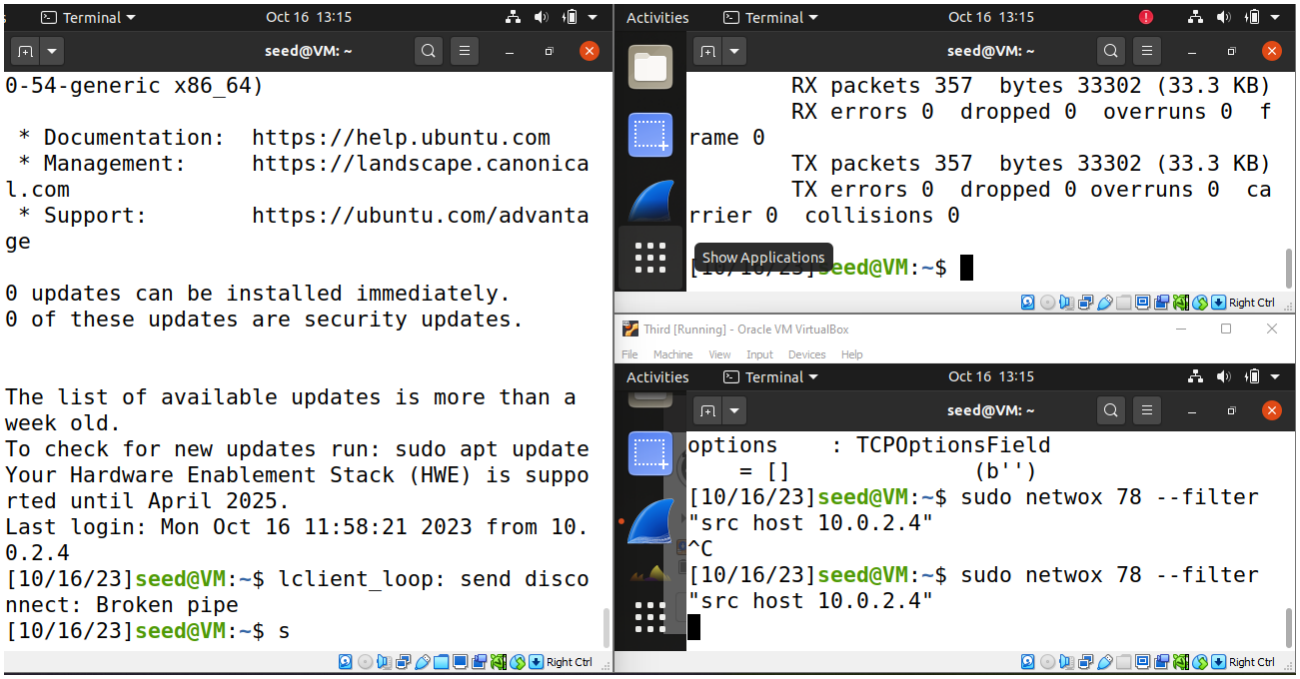
Telnet Summary:

In this section of 3.2, I used netwox to break the telnet connection. I first connected my first virtual machine (client), with the IP of my second virtual machine (server). After connecting them, I used the command "`sudo netwox 78 --filter "src host 10.0.2.4`" to attack the connection between the client and server . To check if it was successful, I tried typing "ls" in the client and was told "`Connection closed by foreign host`".

Using Ssh to connect client to server:



Breaking the connection using netwox:

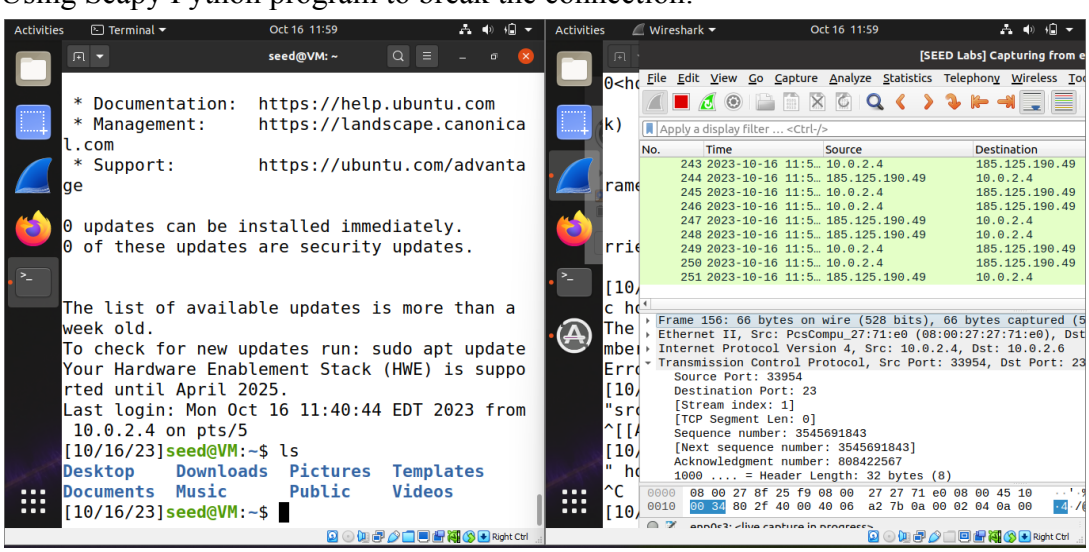


Ssh Summary:

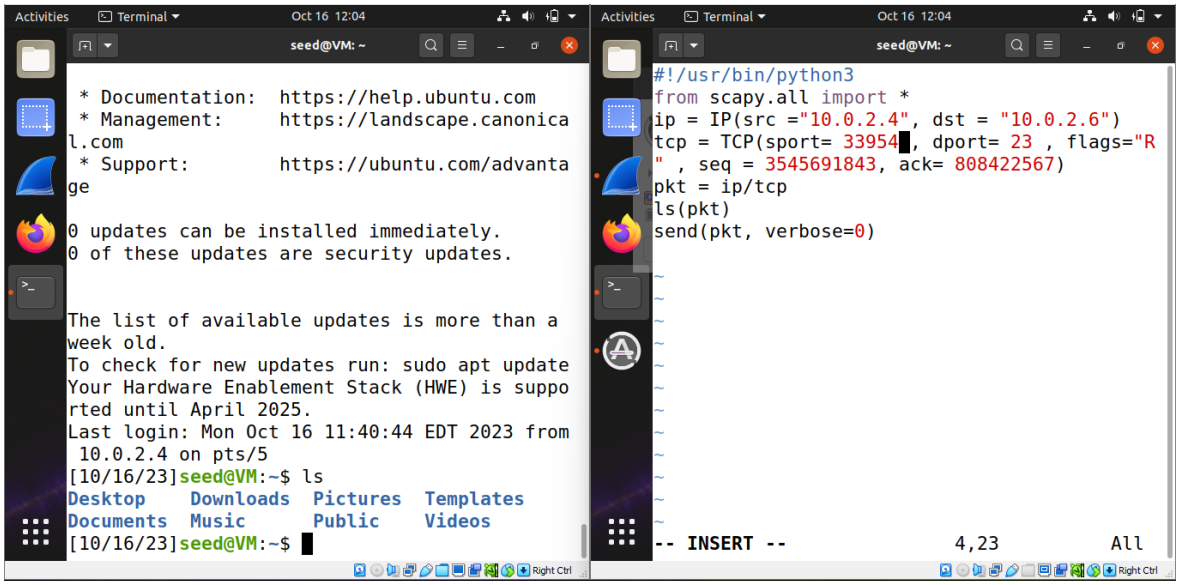
The method is the same as the one previously mentioned for telnet. I connected the client and the server using the server's IP address and attacked the connection using netwox in my attacker.

Instead of saying "`Connection closed by foreign host`", it says "`client_loop: send disconnect: Broken pipe`".

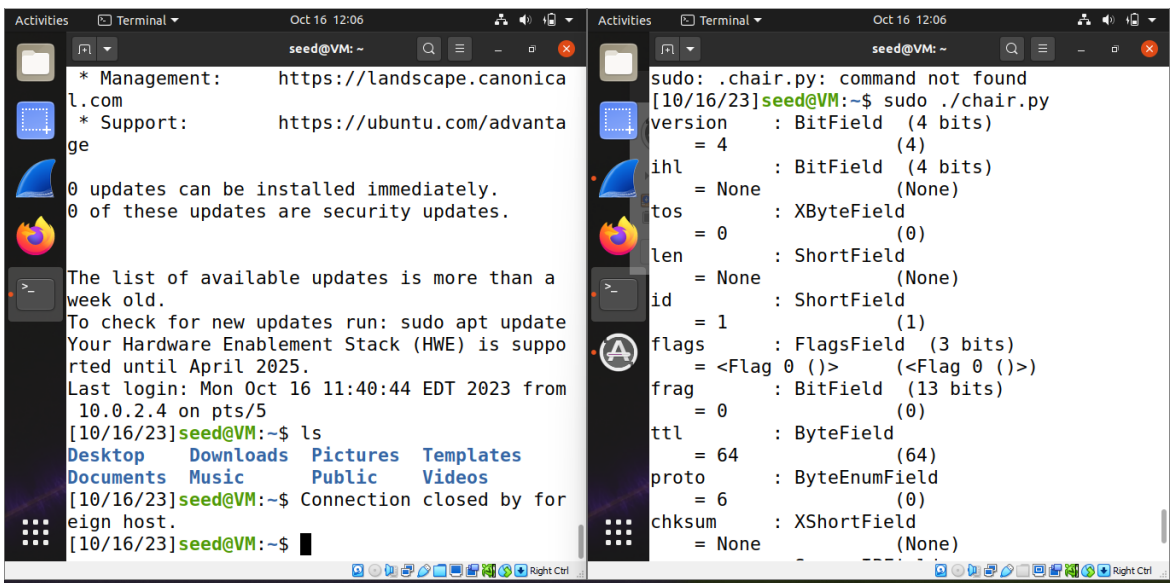
Using Scapy Python program to break the connection:



Inputting Info from wireshark into Scapy:



Closing the connection using Scapy:



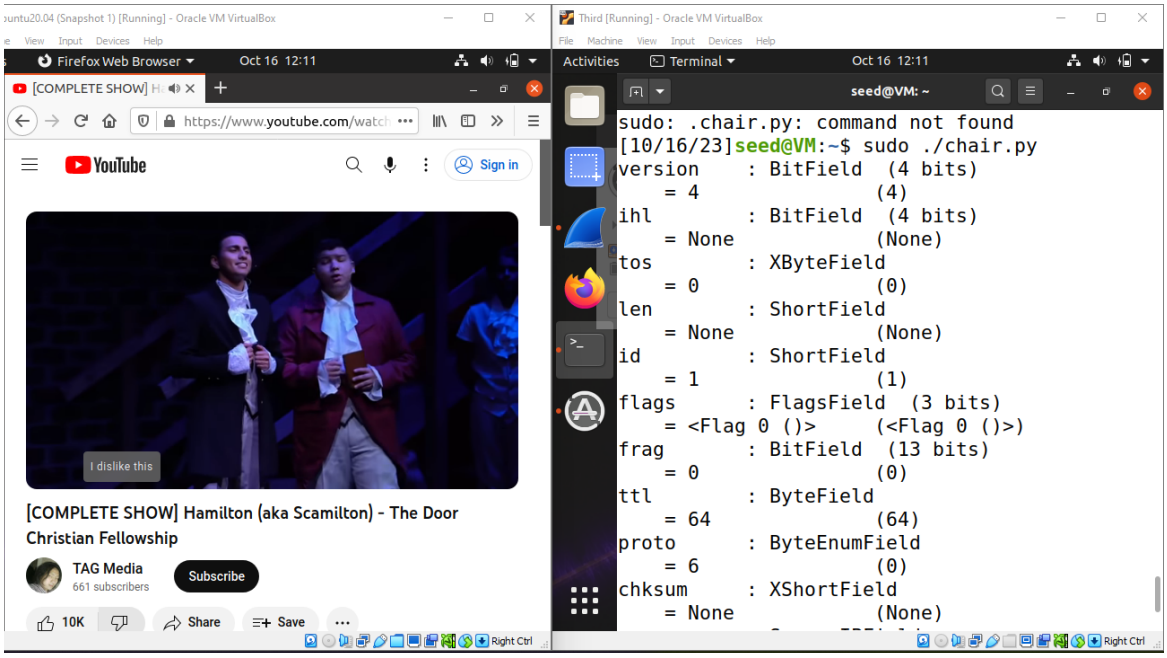
Scapy Python Program Summary:

The steps are the same as mentioned before when establishing a connection between the client and server. After creating the connection, I made a Python file titled "`chair.py`". Within the file using Scapy, I added information such as src and dst, that was found using Wireshark to break the connection using Python. After including the information, in the attacker, I used "`sudo`

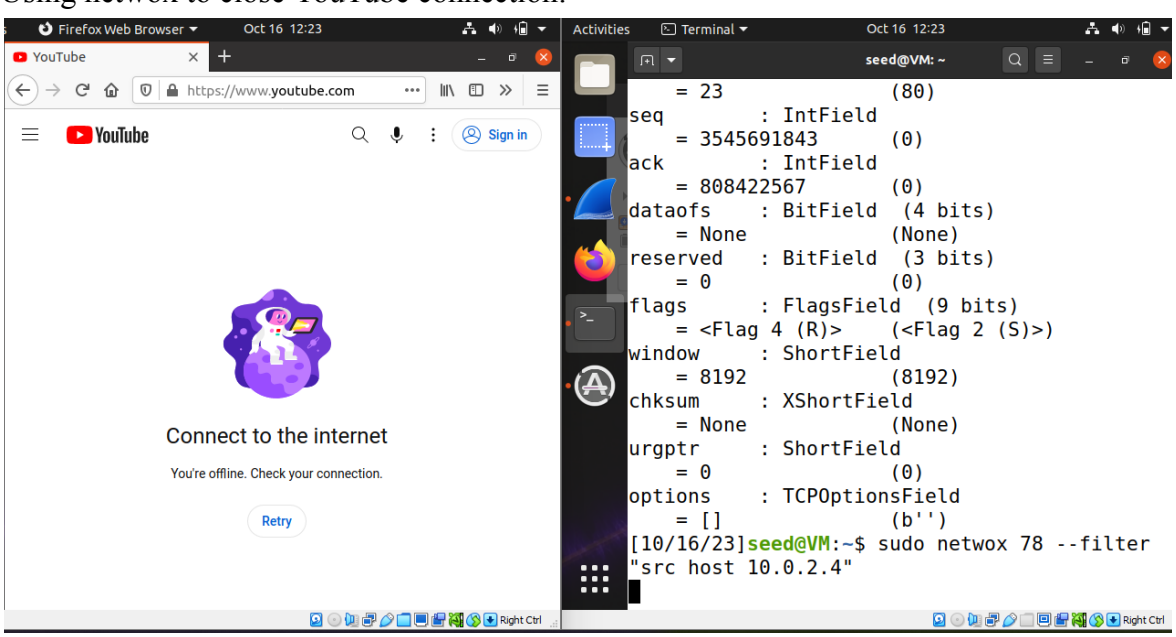
`./chair.py`" to run the code. Finally, I tried typing in the client to check if the connection was broken and received a message stating "`Connection closed by foreign host`".

3.3: **TCP RST Attacks on Video Streaming Applications**

Playing a YouTube video in the client:



Using netwox to close YouTube connection:



TCP RST Attacks on YouTube Summary:

In this last section, I used the connection from the client to use the web browser Firefox to play a YouTube video. To break the connection using netwox I typed "`sudo netwox 78 --filter "src host 10.0.2.4`" in the attacker. Finally, I refreshed the page on YouTube and saw that the connection was indeed broken.