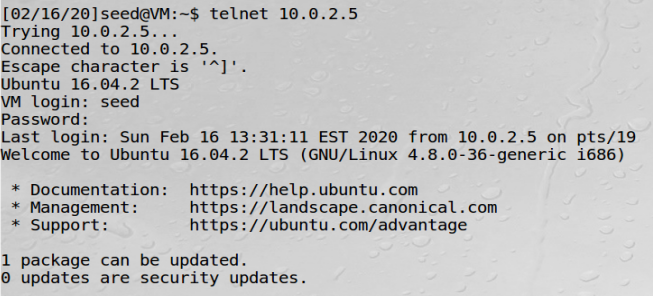
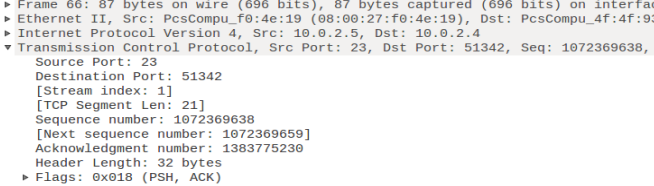
**Task 2: TCP RST Attacks on telnet and ssh Connections**



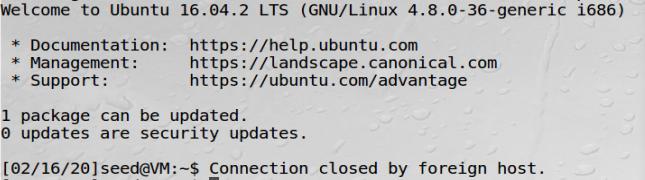
A telnet connection is made to 10.0.2.5 from 10.0.2.4.



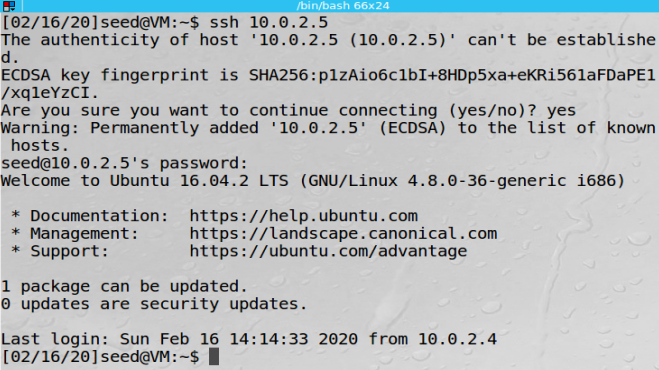
The most recent TCP packet sent from 10.0.2.5 to 10.0.2.4.



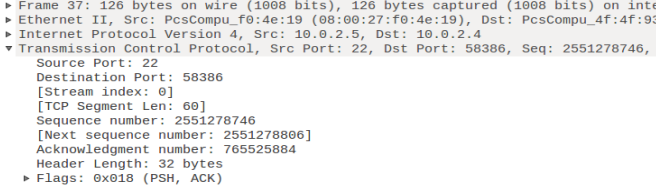
Python program to spoof TCP RST packets. We input information from the TCP packet such as the source port, destination port, next sequence number, etc. We run this program on the attacker machine (10.0.2.6) which is on the same network as the other two machines.



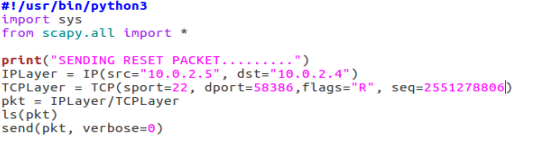
We receive a message on 10.0.2.4 stating that “Connection closed by foreign host.” This indicates that the attack was successful and that the connection has been broken.



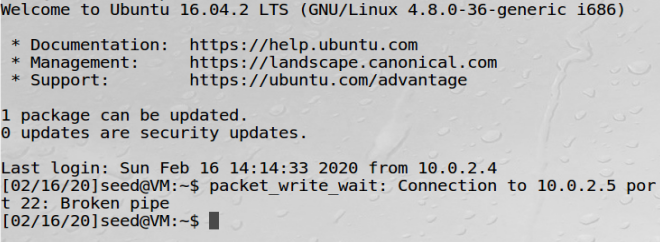
A ssh connection is made to 10.0.2.5 from 10.0.2.4.



The most recent TCP packet sent from 10.0.2.5 to 10.0.2.4.

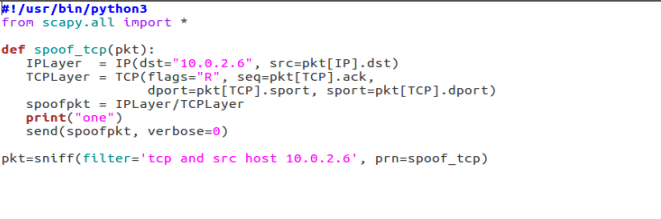


Python program to spoof TCP RST packets. We input information from the TCP packet such as the source port, destination port, next sequence number, etc. We run this program on the attacker machine (10.0.2.6) which is on the same network as the other two machines.



We receive a message on 10.0.2.4 stating that “Connection to 10.0.2.5 port 22: Broken pipe.” This indicates that the attack was successful and that the connection has been broken.

**Task 3: TCP RST Attacks on Video Streaming Applications**



Python program to automatically send out spoofed TCP RST packets.

This was unable to reset the video streaming connection. This is because Python code is slow and is unable to send out the spoofed reset packet in time.

We try an alternate method to reset the video streaming application by using an existing tool written in C called “Netwox tool 78.” The command was given as follows:

*sudo netwox 78 – filter “src host 10.0.2.6”*

When this command was used the video continued uptil what was loaded in the buffer and then stopped and would not load any further. If the page was refreshed, the following error was shown:

