Lab 5

58119125 JiangZhuoyang

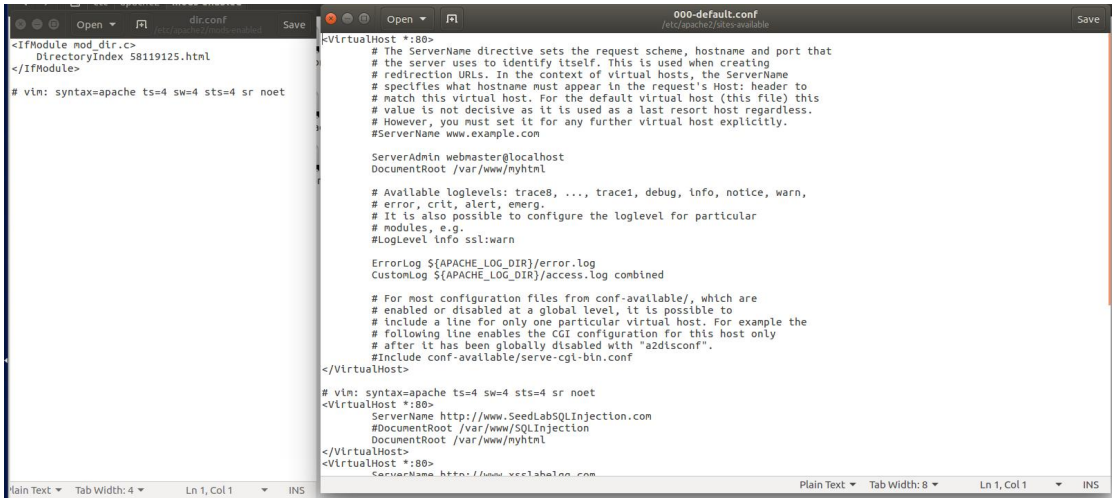
Task 1: Build Your Own Website

Solution:

This might be one of the most difficult Questions I have ever meet in my life.

I have tried so many measures, but I can never replace the default page.

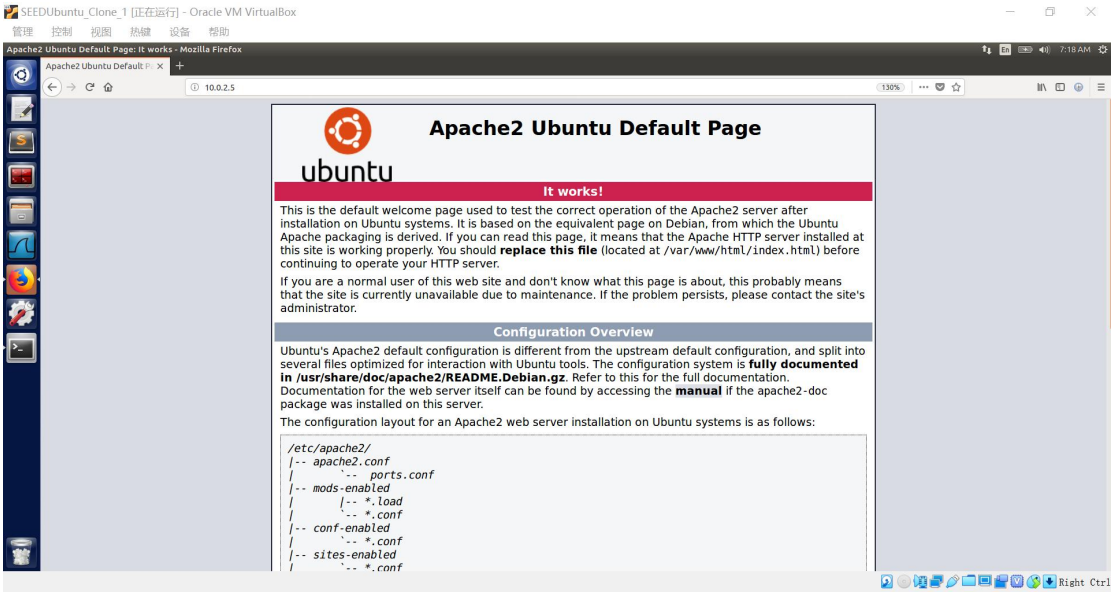
I tried to edit these two files.



Then I restart the Apache2 Servers in 2 different way:

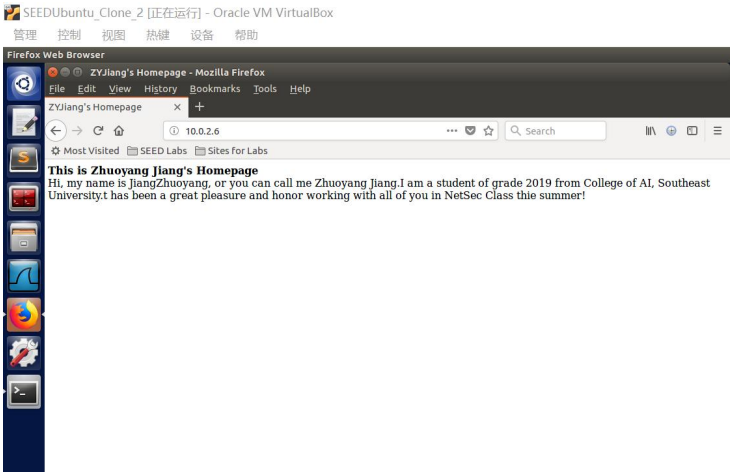
```
[05/05/22]seed@VM:~$ sudo /etc/init.d/apache2 restart
[ ok ] Restarting apache2 (via systemctl): apache2.service.
[05/05/22]seed@VM:~$ sudo service apache2 restart
```

And I open the IP address again and again just to find that I have failed again and again.



Finally, I solve it by just change a VM. I think the error is made by the wrong way I choose to deleting the original index.html.

Q1: Provide a screenshot of your personal web page.



Task 2: SYN Flooding Attack

Solution:

1. Set up the environment.:

The 3 VM is cloned as below.

We regard SEEDUbuntu_Clone_2 as victim server, with IP: **10.0.2.6**

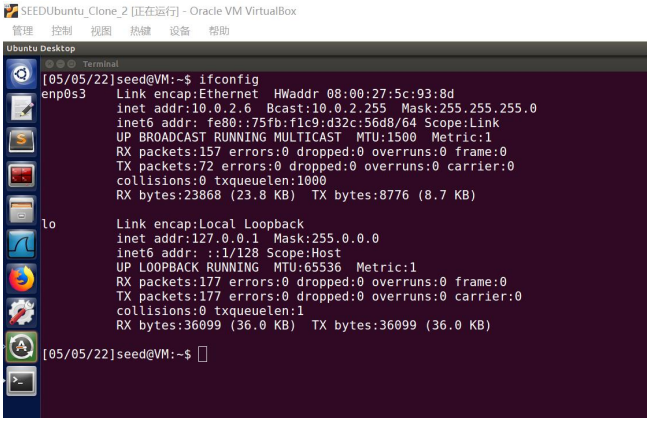


Fig1. Victim VM

We regard SEEDUbuntu_Clone_3 as observer, with IP: **10.0.2.7**

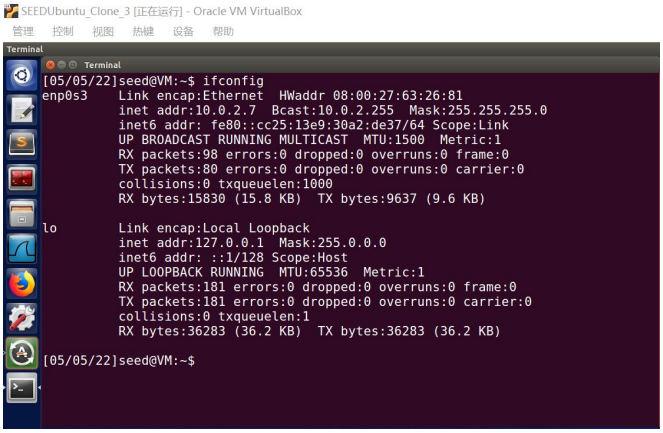


Fig2. Observer VM

We regard SEEDUbuntu_Clone_Attacker as attacker, with IP: **10.0.2.8**

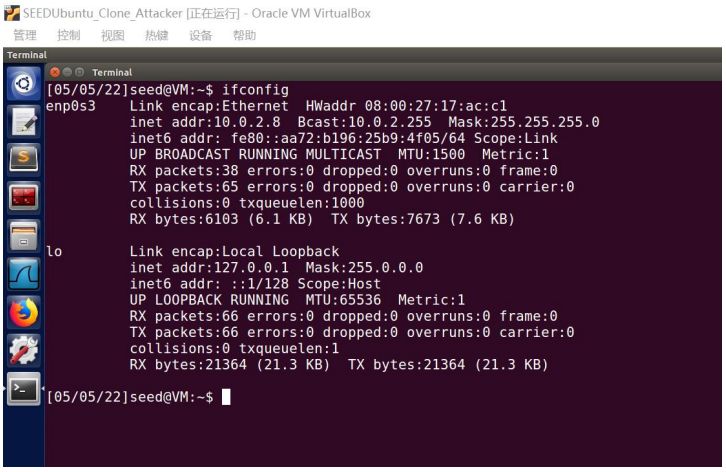


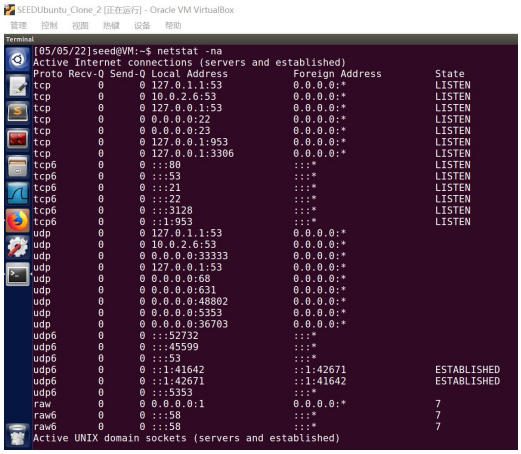
Fig3. Attacker VM

2. Obtain the maximum number of queued connection requests with command below.

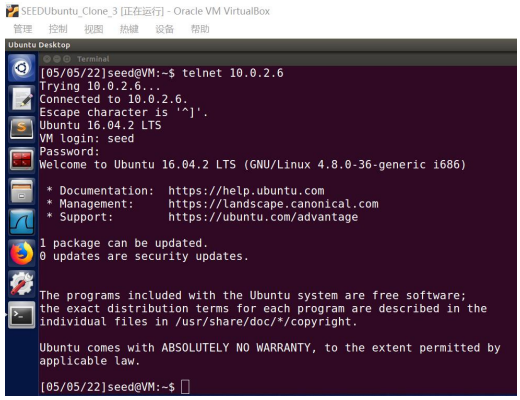
```
[05/05/22]seed@VM:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
```

3. Check the usage of the queue before attacking

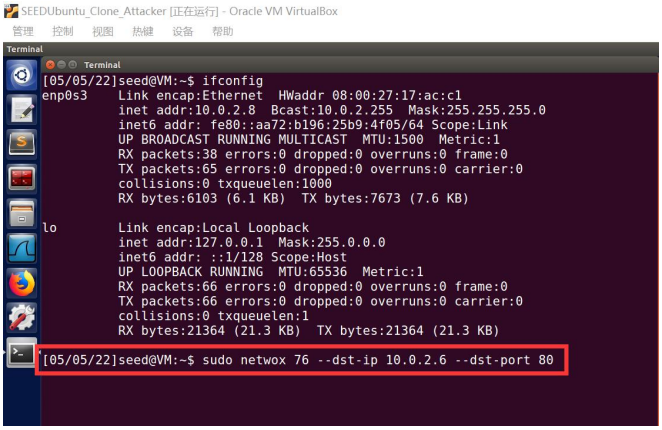
Run *"netstat -na"* to reach that:



4. Log in to the Victim VM with the Observer successfully

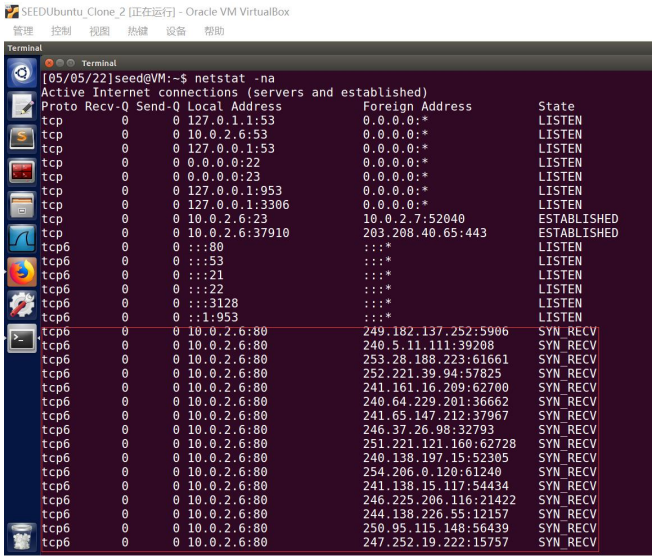


5. Do a flood attack with Netwox on attacker with SYN cookie opened.

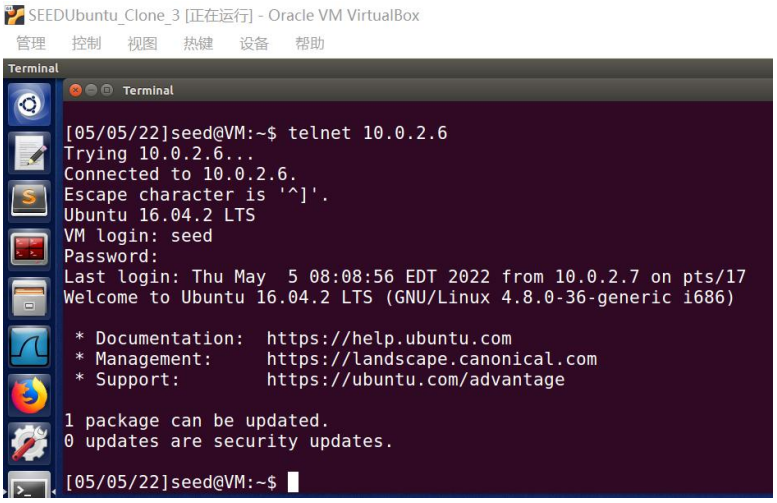


6. Check the usage of the queue after that

A huge number of SYN is sending to the victim VM, so that there is a lot of semi-connected SYN states in the connection queue on the Victim VM.



Try to log into the victim on observer, the log process is still successful.

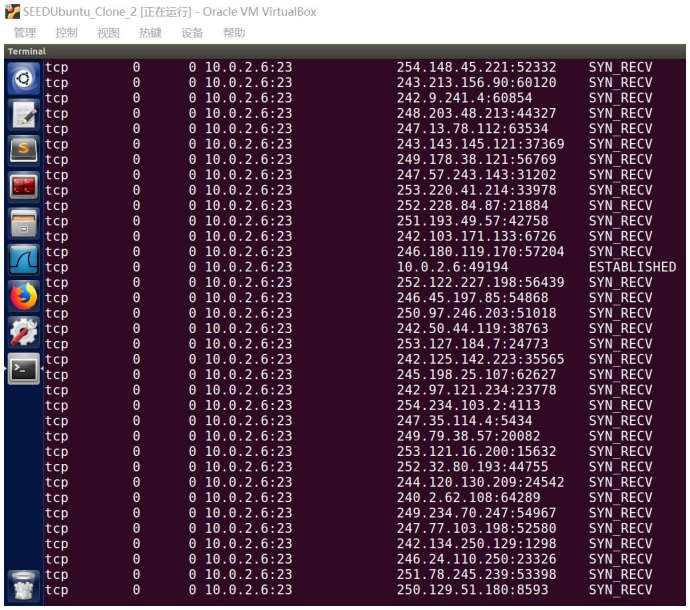


7. Turn off the SYN cookies, then do the attacking with "port 23"

Turn off the SYN cookies with command *"sudo sysctl -w net.ipv4.tcp_syncookies=0"* to do a flood attack with command "sudo netwox 76 --dst-ip 10.0.2.6 --dst-port 23" again.

Port 23 is the port of telnet.

Check the queue status in victim, the same as before



This time the observer failed to Telnet-log into the victim host.

This is because syn cookies are a defense mechanism against SYN flooding attacks. If the machine detects that it has been attacked by SYN flooding, the mechanism will start. If we turn off the mechanism, the result is shown as above.

Q2: In Ubuntu 16.04 VM provided in class, what is the maximum number of queued connection requests which have still not received an acknowledgement from the connecting TCP clients?

Answer:

The maximum number is 128.

Q3: In your own words, brief explanation how the TCP SYN flood attack works.

Answer:

Under TCP transmission protocol, before sending and receiving data formally, you must establish a reliable connection with the other party. This process is realized through three way handshake. Flooding attack takes advantage of this process. The attacker sends a large number of TCP syn message segments without completing the third handshake step. With the increase of syn message segments, the server continuously allocates resources for these semi open connections,

but does not use or release these resources, resulting in the depletion of server connection resources.

Q4: Use Netwox to launch TCP SYN flood attack works against the web site on the server (10.0.2.6 in Figure 1). Is the attack successful or not? (Yes/No) Please briefly describe what you have observed. (Note that if you experience long delay when visiting your personal webpage, it means a DoS attack against the web site is successful; otherwise, it is not. It is because the website can become slow to respond to legitimate requests when under DoS attacks. Please wait for a while after you launch TCP SYN flood attack, and then try to visit your personal webpage.)

Answer:

Yes. I experience long delay when visiting my personal web page, but it successfully displayed eventually.

Q5: Is the attack successful or not when the SYN cookie disabled? (Yes/No). Please briefly describe what you have observed.

Answer:

Yes. I experience long delay when visiting my personal web page, and it failed to display eventually.

Q6: Please explain your observations and what happened to cyber attacks conducted in Q4 and Q5.

Answer:

In Q4 the SYN cookies are online. It is a defense mechanism against SYN flooding attacks. If the machine detects that it has been attacked by SYN flooding, the mechanism will start. If we turn off the mechanism, the result is shown as the situation in Q5.

Task 3: TCP RST Attacks on telnet Connections

Q7: In your own words, briefly explain how the TCP RST Attack works.

Answer:

1.TCP RST:

(1) RST is the flag bit indicating reset in TCP protocol, which is used to close the connection abnormally. TCP handler will send RST packet at the abnormal time.

(2) When sending RST packets and closing the connection, we don't have to wait for all the packets in the buffer to be sent (different from FIN packets), and we can directly discard the packets in the buffer and send RST packets. After receiving the rst packet, the receiver does not have to send an ACK packet to confirm.

2.TCP RST Attacks:

(1) Based on the above working principle, TCP RST attack can be described as follows:

When a TCP connection is established between client a and server B, **attacker C disguises as client A** and sends a **forged TCP packet** to B, causing B to disconnect the TCP connection with A abnormally

(2) The kinds of **forged TCP packet:**

① Disguised as an RST packet sent by A: after receiving it, B will discard all data in the buffer with AI and force the connection to be closed.

② Disguised as syn packet sent by A: B may think that A has transmission error and

request to establish a new connection when it has been connected normally. Therefore, B will take the initiative to send an RST packet to A and forcibly close the connection at its own end.

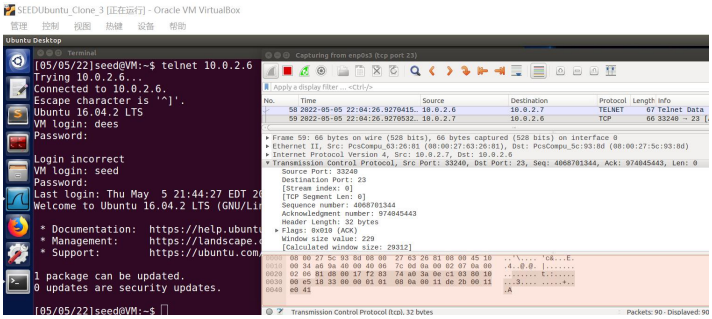
(3) The way to **disguises as client A:**

C needs to fill in the correct **[1. Source IP address; 2. Destination IP address; 3. Source port; 4. Destination port; 5. Sequence Number]** of A in the TCP / IP header of the forged packet. The **Red Part** is what we cannot directly know if we're not doing the experiment ourselves.

Q8: You are required to demonstrate your TCP RST Attacks on telnet connections using Netwox through a step by step MOP (Method of procedure).

Solution:

Step1. Log into 10.0.2.6 on 10.0.2.7 and catch packet with wireshark



Step2. Analyze the packet header information:

1.Source port number: **33240**

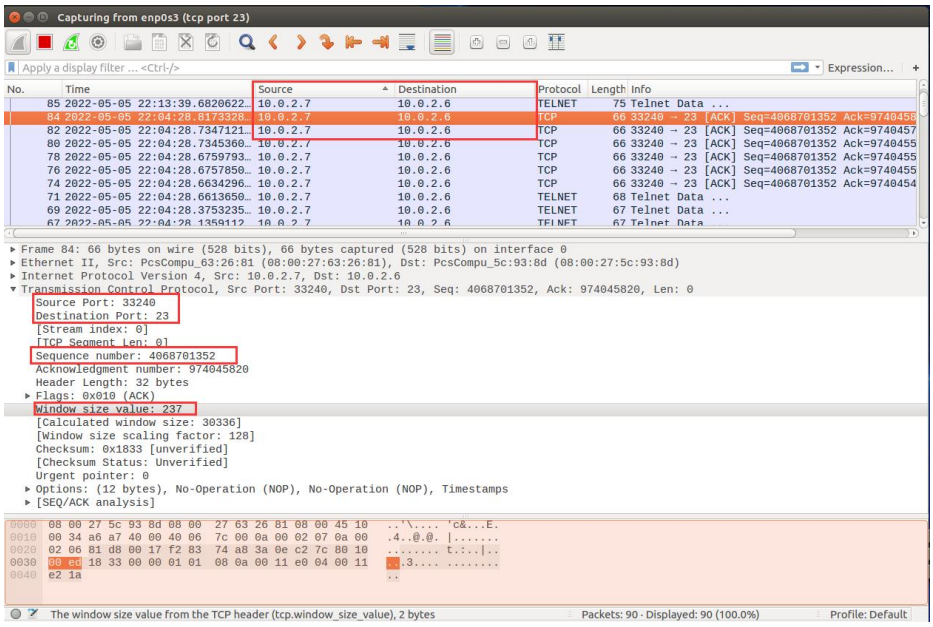
2.Source IP address: **10.0.2.7**

3.Destination port: **23**

4.Destination IP address: **10.0.2.6**

5.The sequence number: **4068701352**

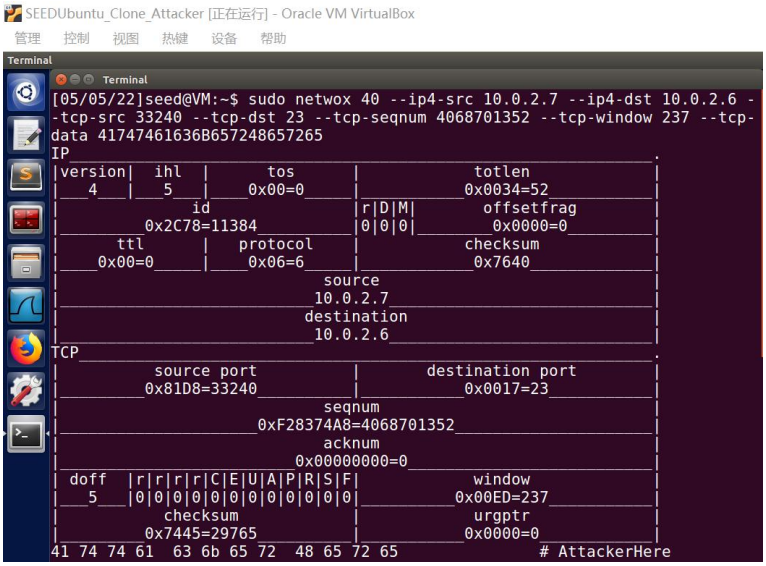
6.The window size value: **237**.



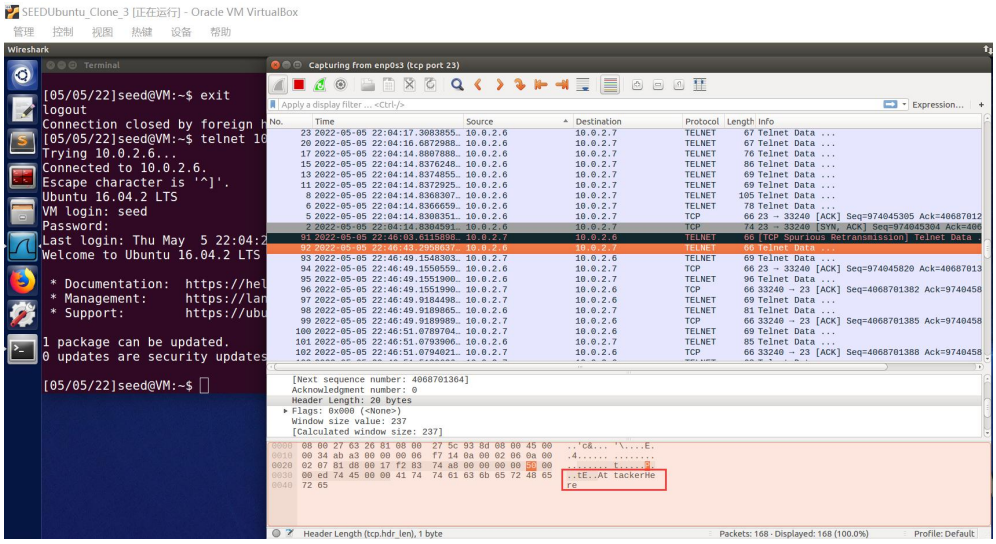
Step3. Code the netwox command on Attacker with the information above:

*sudo netwox 40 --ip4-src **10.0.2.7** --ip4-dst **10.0.2.6** --tcp-src **33240** --tcp-dst **23** --tcp-seqnum **4068701352** --tcp-window **237** --tcp-data 41747461636B657248657265*

(41747461636B657248657265: UTF-8 decoding as “AttackerHere”)

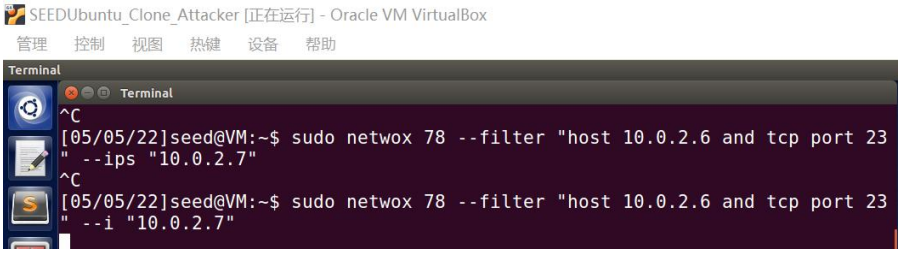


On the 10.0.2.7, we can observe the message sent by attacker, the transport is probable with the information we got.



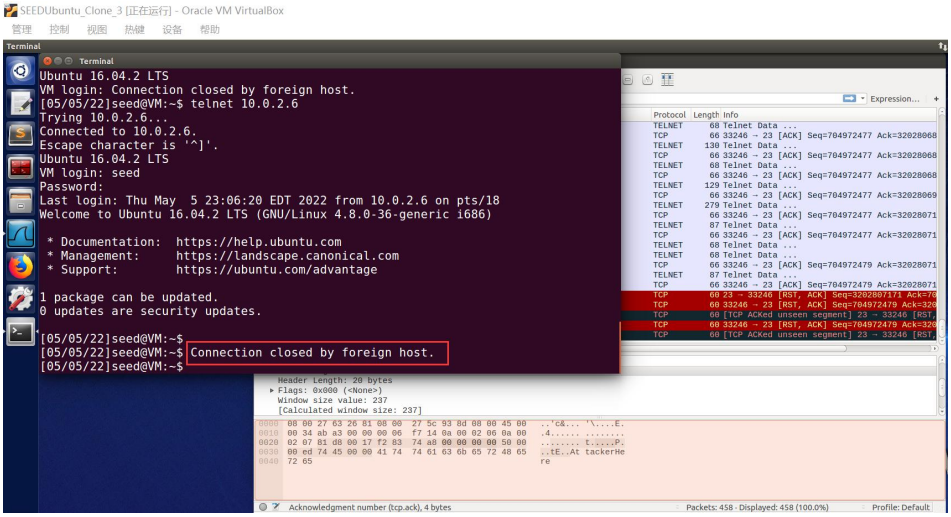
Step4. Code the attacking command on the Attacker VM

We use the #78 tool netwox to reach the hijack, just give the tool an “ips” or “i” which means the Source IP.

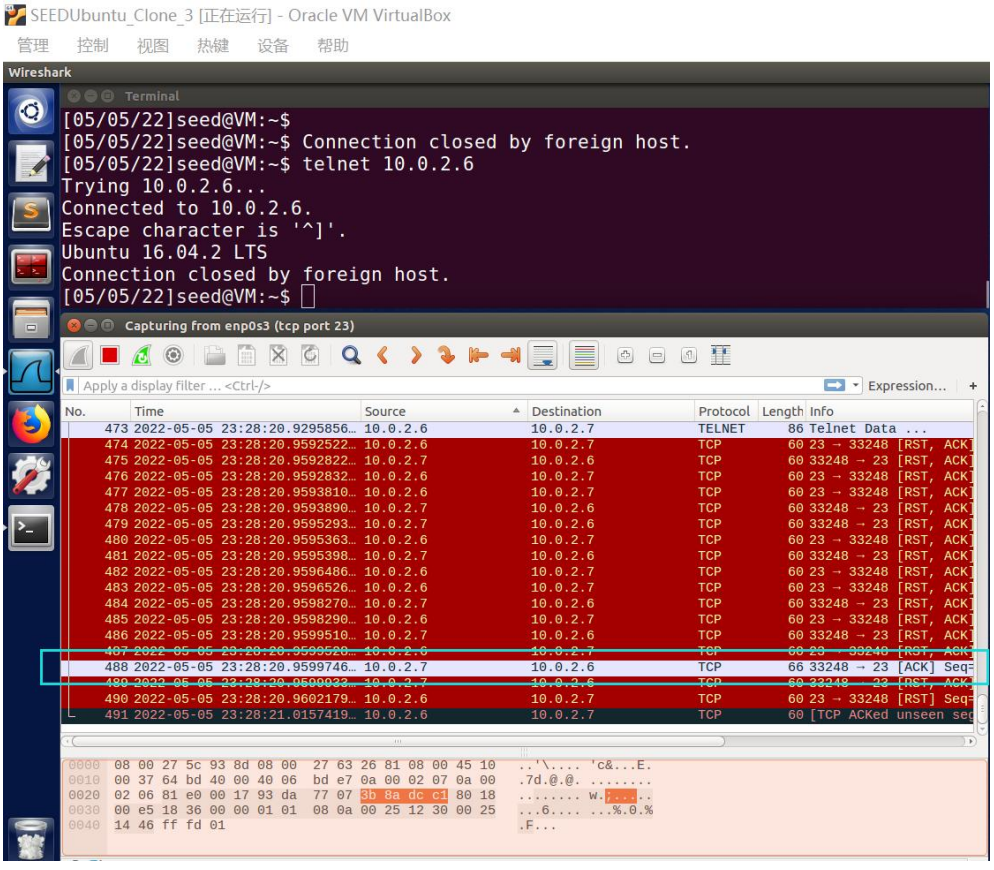


Step5. Do something on 10.0.2.7 when it is logging on the 10.0.2.6 like “Click the Enter”

We will find that the connection is closed immediately which means the hijack is working.



Try to log in 10.0.2.6 on 10.0.2.7 again, we cannot do this when the hijack is hanging on.



Q9: You are required to give the correct values to replace each @@@@ in the skeleton code provided, and submit your modified code as reset_XXX_YYY.py, where XXX is your student ID and YYY is your surname in Pinyin. After you finish the above python program "reset.py", you launch the attack and should be able to disconnect the existing telnet connection.

Solution:

Step1. Use the packet before the last header information, we got it as before

1.Source port number: **50616**

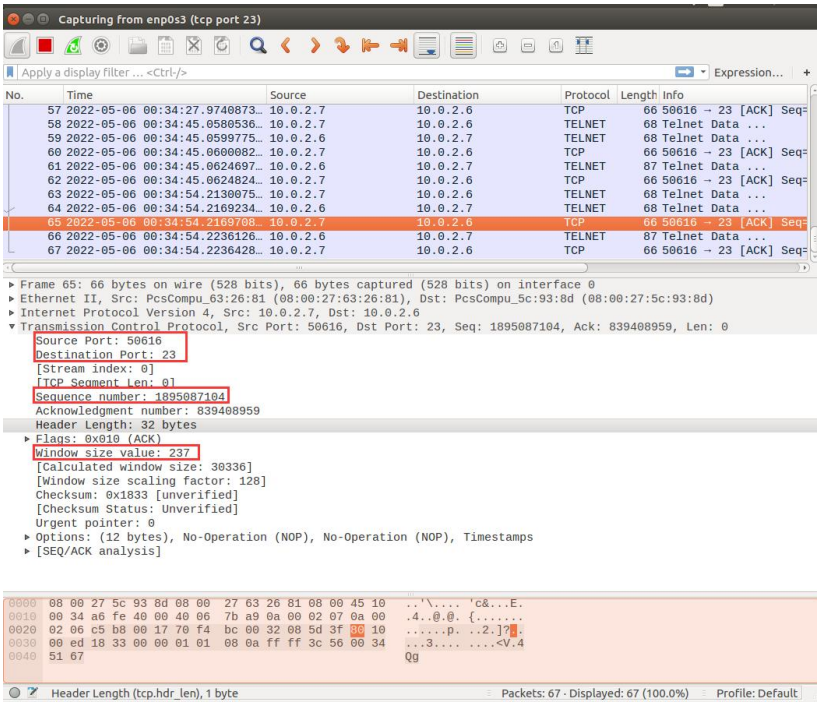
2.Source IP address: **10.0.2.7**

3.Destination port: **23**

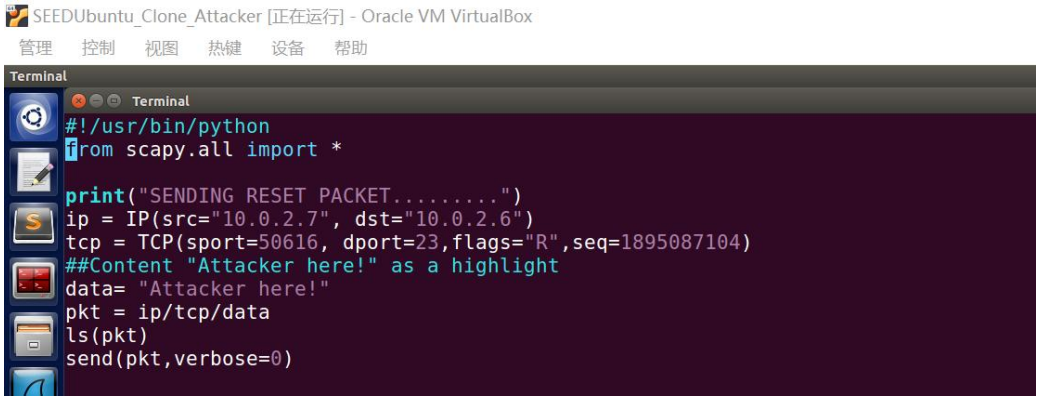
4.Destination IP address: **10.0.2.6**

5.The sequence number: **1895087104**

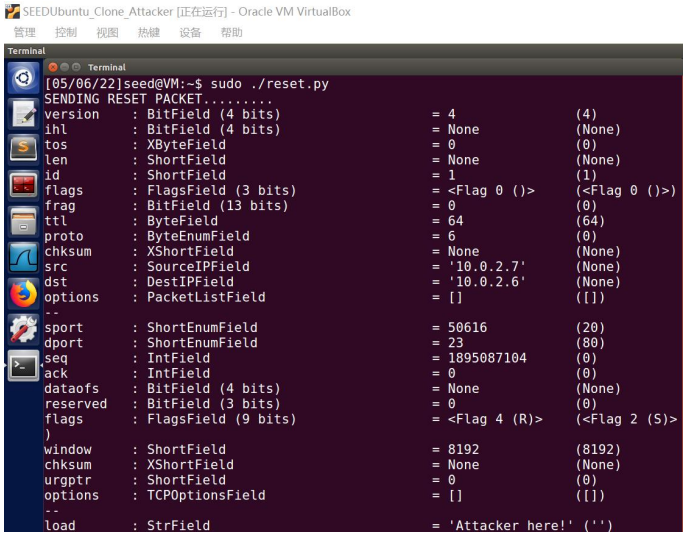
6.The window size value: **237**.



Step2. Edit a python Hijack program with the information above, we have prove that with these information, we can send forged 10.0.2.7's packet to 10.0.2.6 on Attacker



Step3. Run the python Hijack program.



Step4. Do something on 10.0.2.7 when it is logging on the 10.0.2.6 like “Click the Enter”.

We will find that the connection is closed immediately which means the hijack is working.

And the forged packet sent by attacker can be seen in the wire shark.