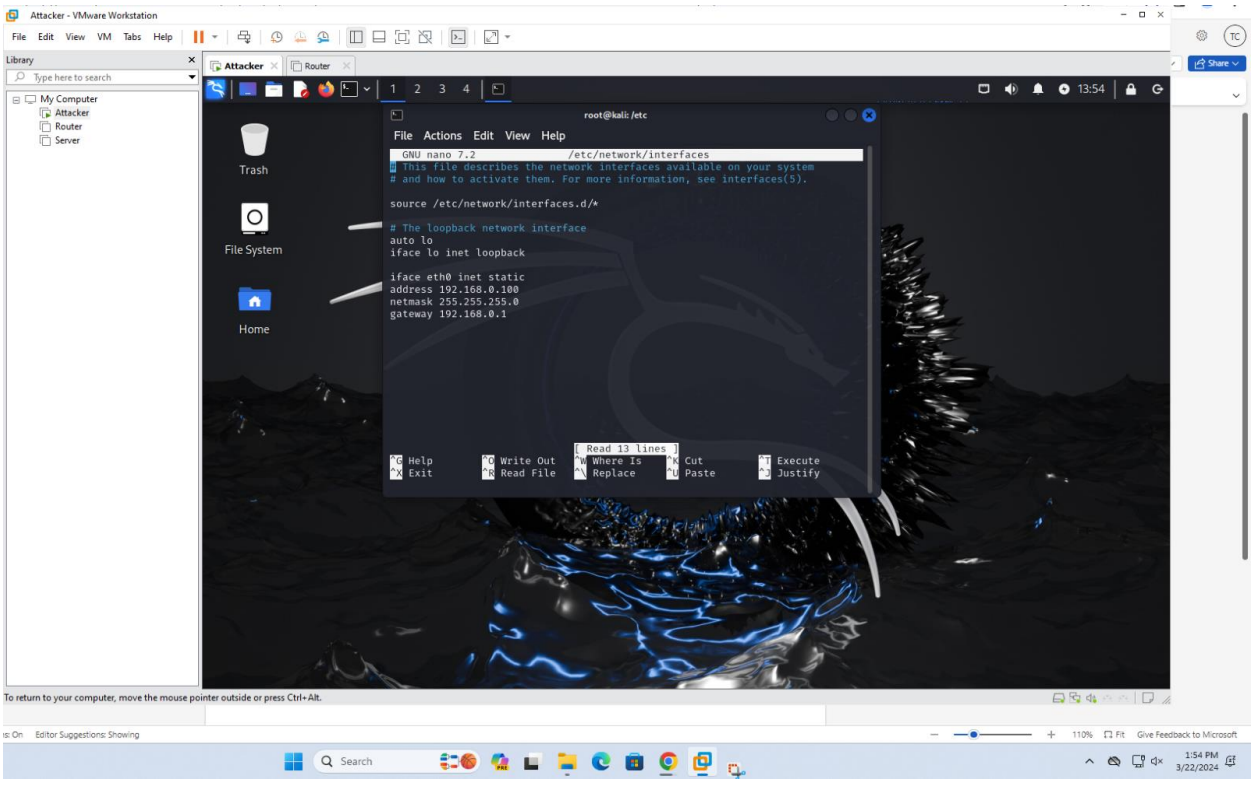
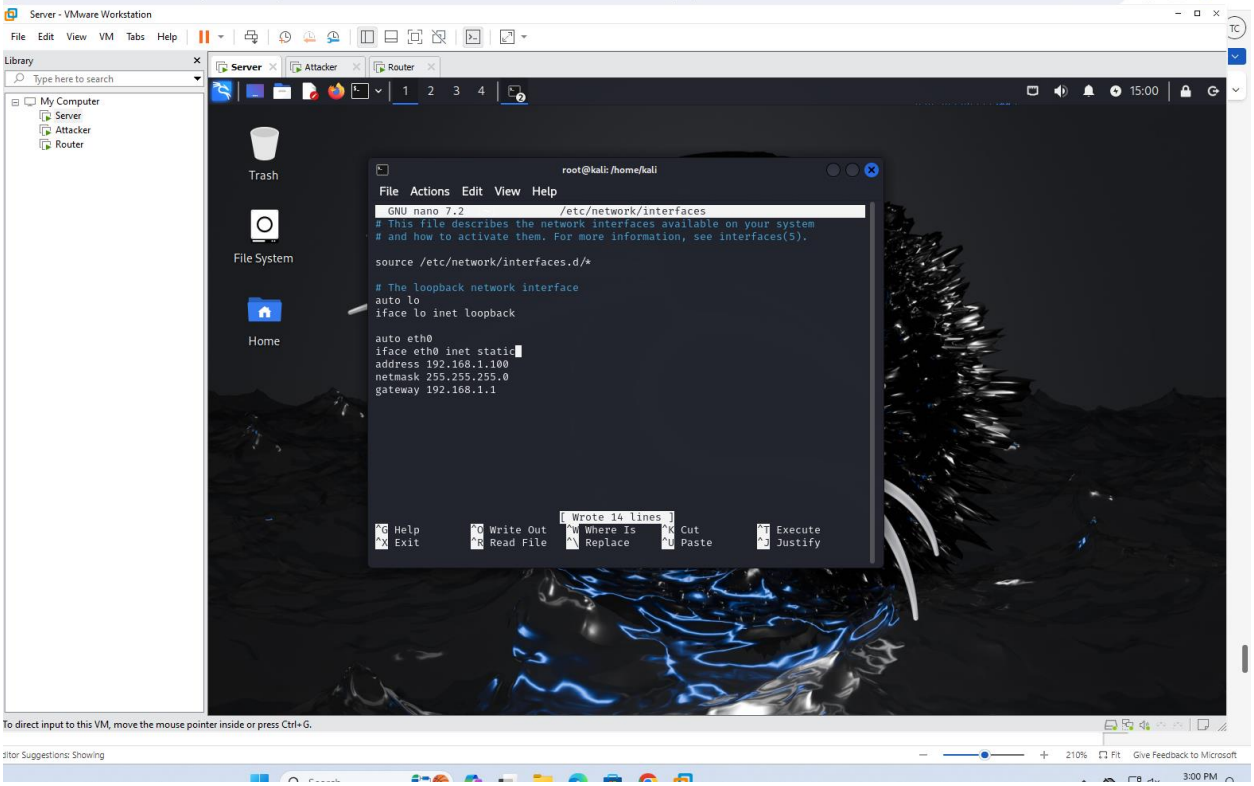
Tamania Choudhury
Penetration Testing
31 March 2023

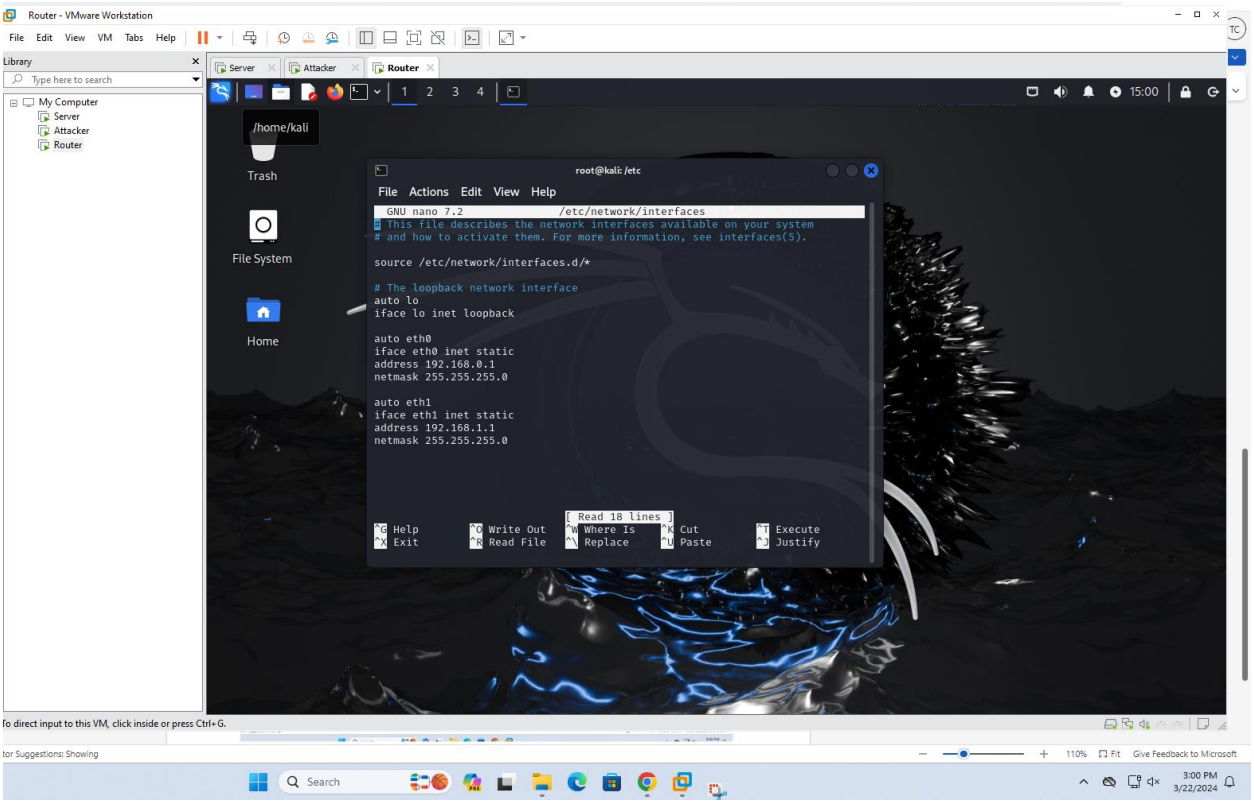
Project 1 – TCP Protocol Attacks

I. Setup a virtual environment:

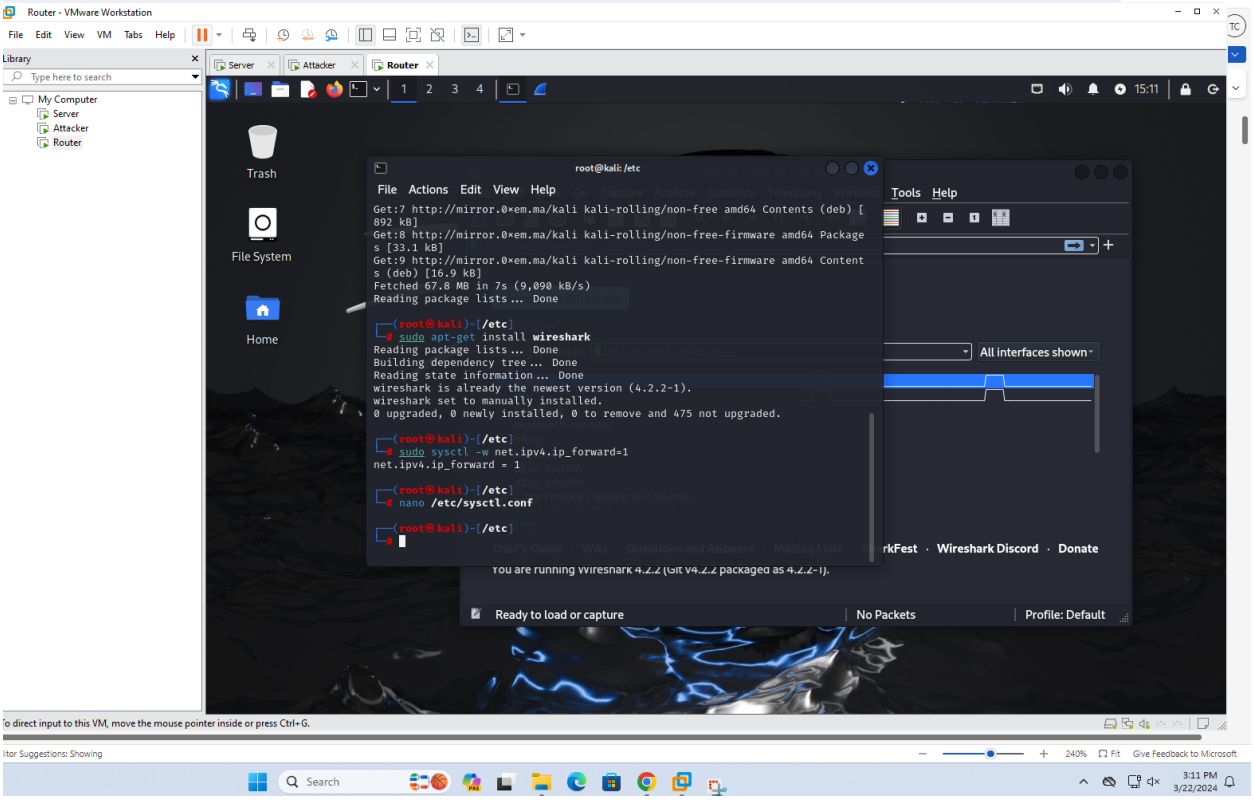
For the setup of the virtual environment, I used the following configurations in the /etc/network/interfaces files. In weeks 1-3, I focused on setting up the environment and researching the topics.


Attacker - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Attacker
Router
Server
Attacker
Router
1 2 3 4
13:54
Trash
File System
Home
root@kali: /etc
File Actions Edit View Help
GNU nano 7.2 /etc/network/interfaces
This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*
The loopback network interface
auto lo
iface lo inet loopback
iface eth0 inet static
address 192.168.0.100
netmask 255.255.255.0
gateway 192.168.0.1
[Read 13 lines]
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
Search
1:54 PM
3/22/2024


Server - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Server
Attacker
Router
Server
Attacker
Router
1 2 3 4
15:00
Trash
File System
Home
root@kali: /home/kali
File Actions Edit View Help
GNU nano 7.2 /etc/network/interfaces
This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*
The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
gateway 192.168.1.1
[Wrote 14 lines]
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:00 PM

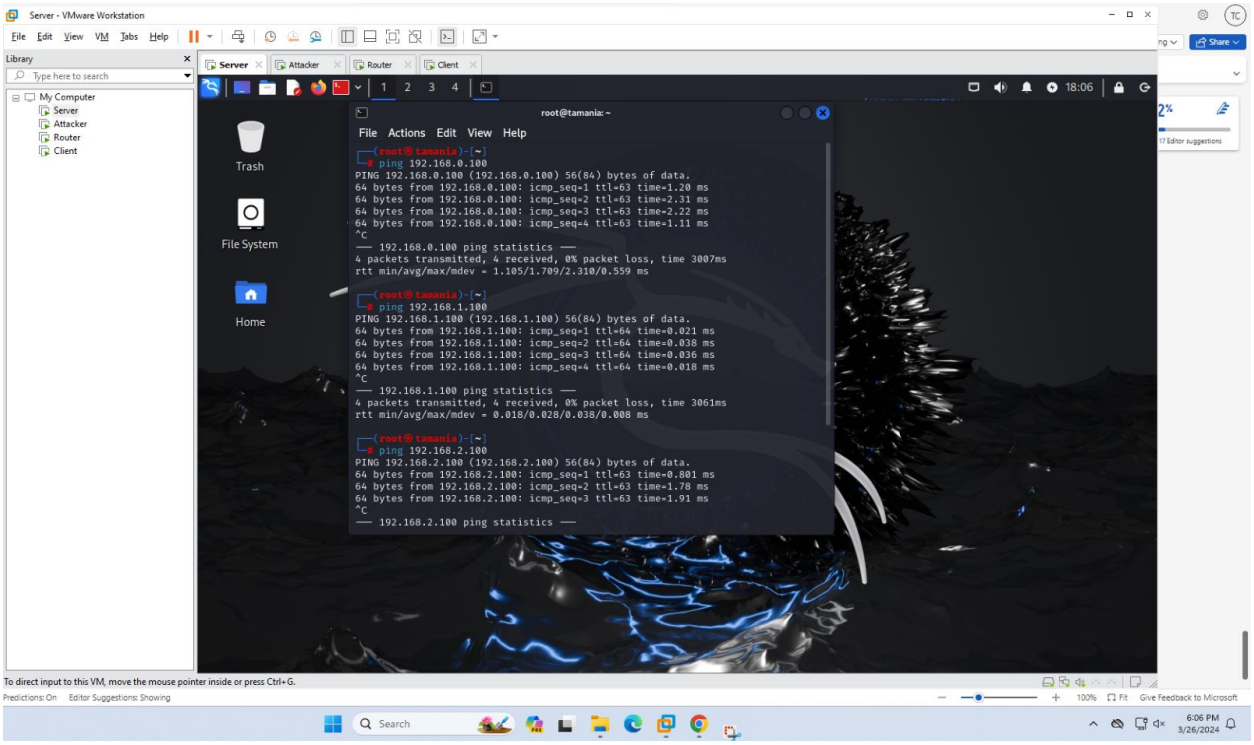


Port Forwarding:

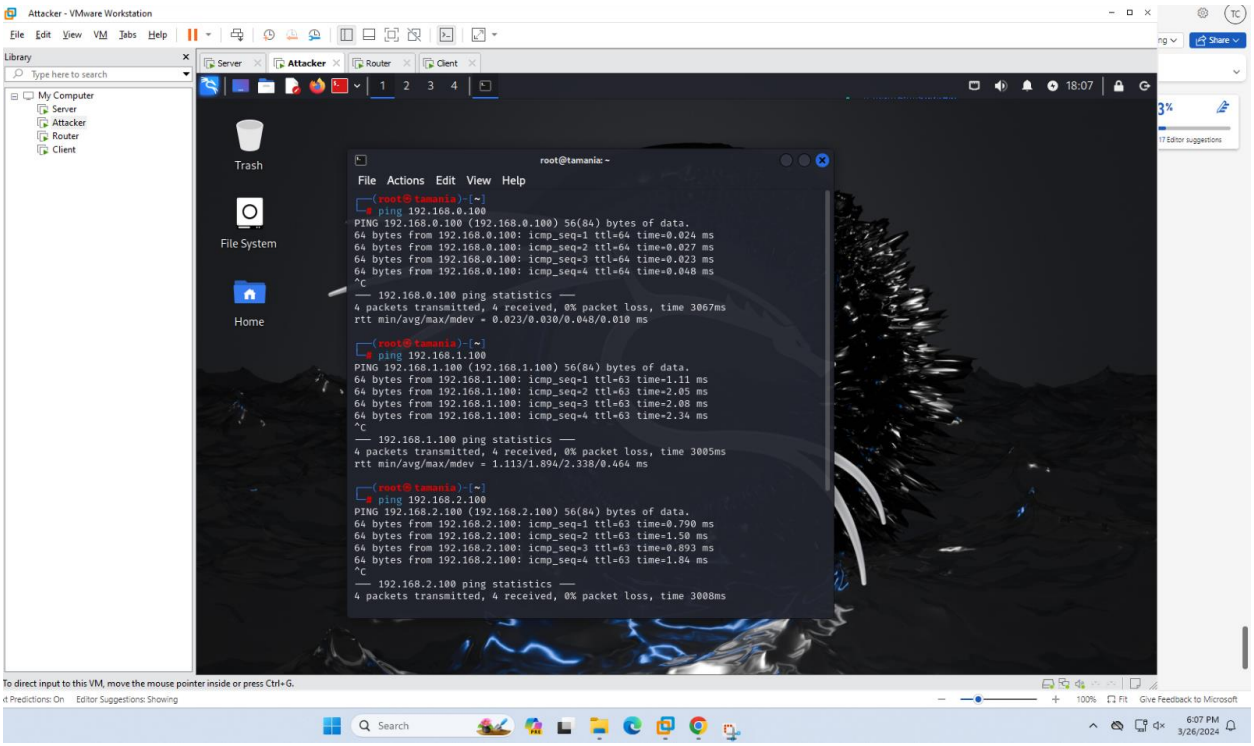


The three machines are able to ping each other.

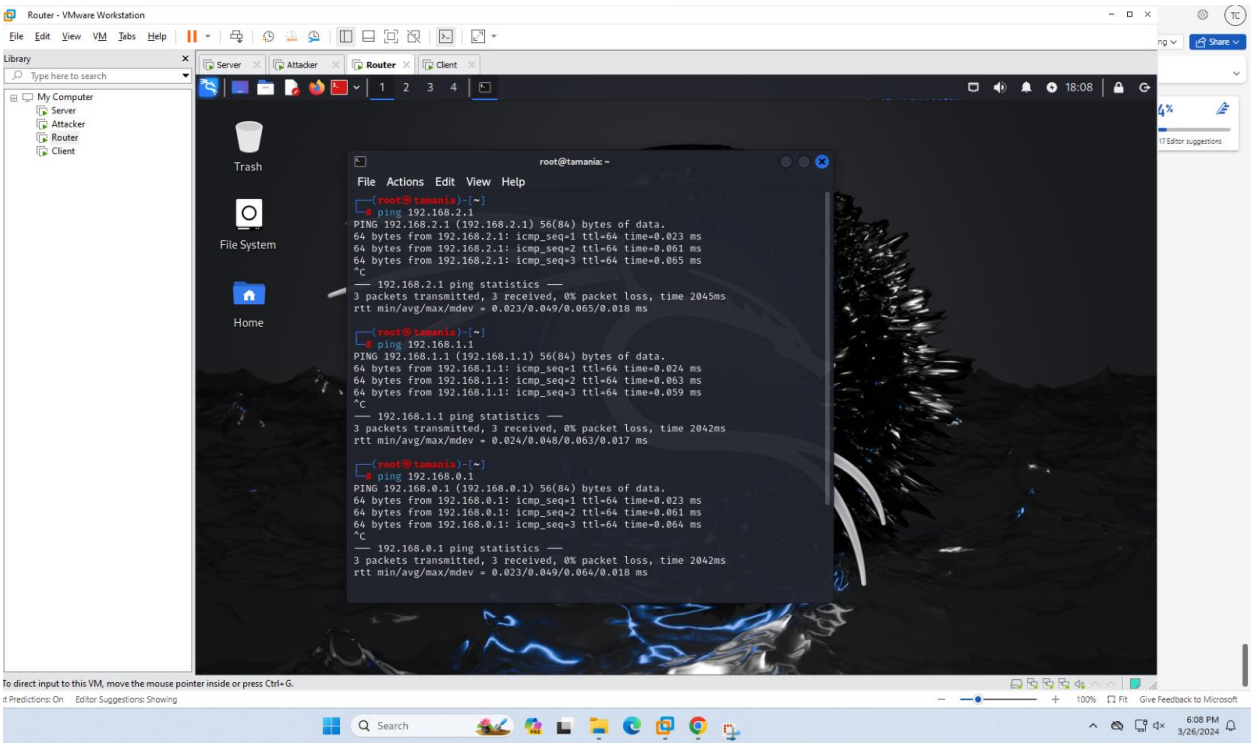
Successful pings are shown in the following. Server successful pings are below (all).



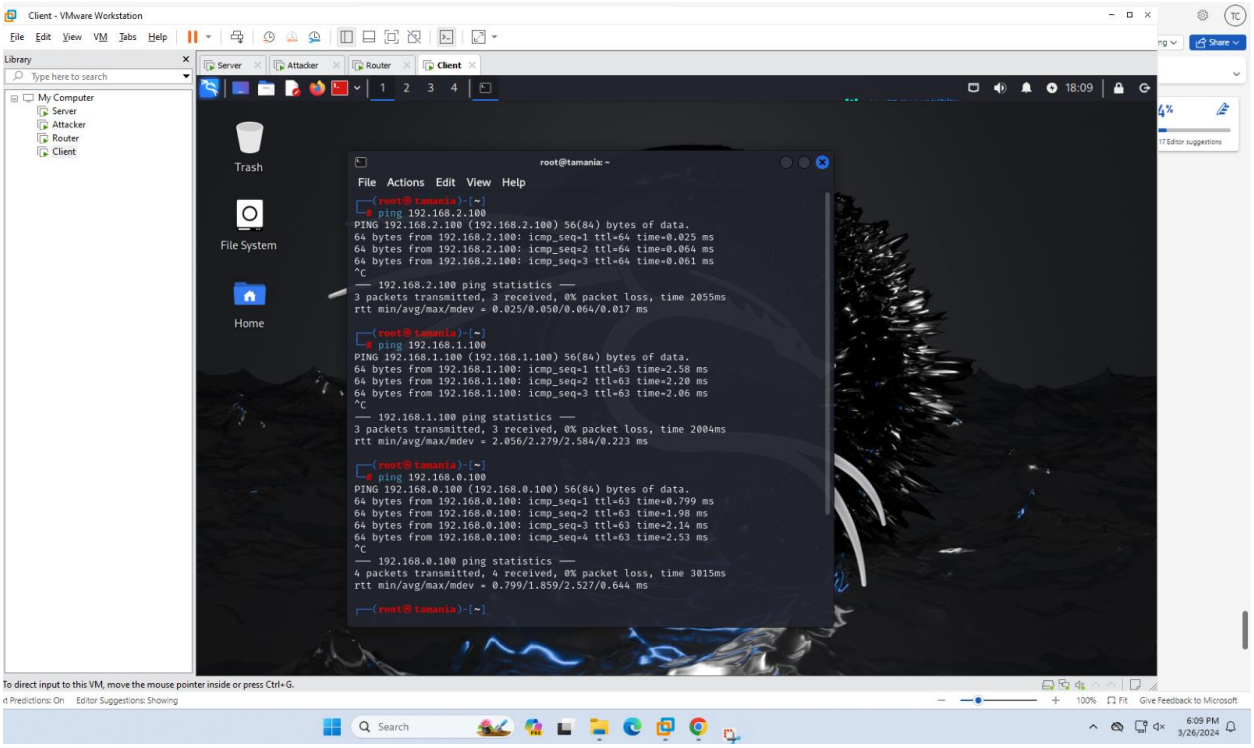
Attacker successful pings, too.



Router successful pings.



And finally, client successful pings.



Able to use Wireshark or Tcpdump to capture pass-through traffic:

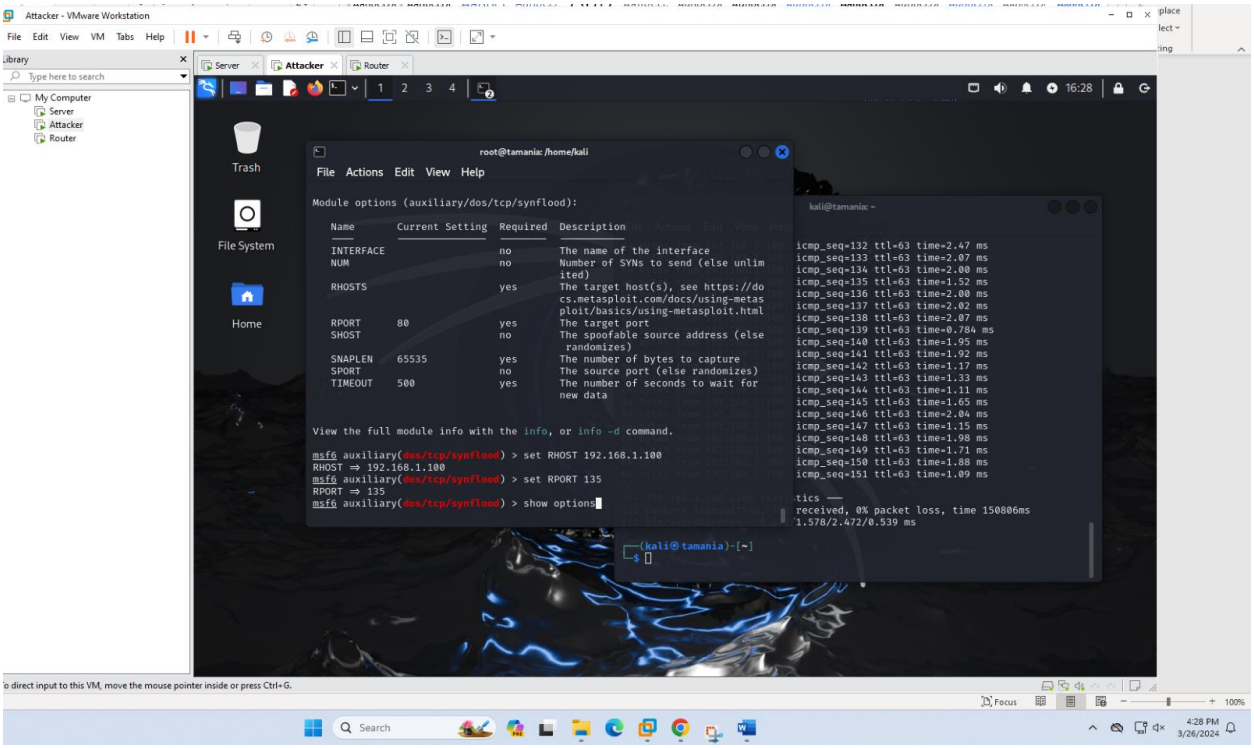
I included a short video of Wireshark running.

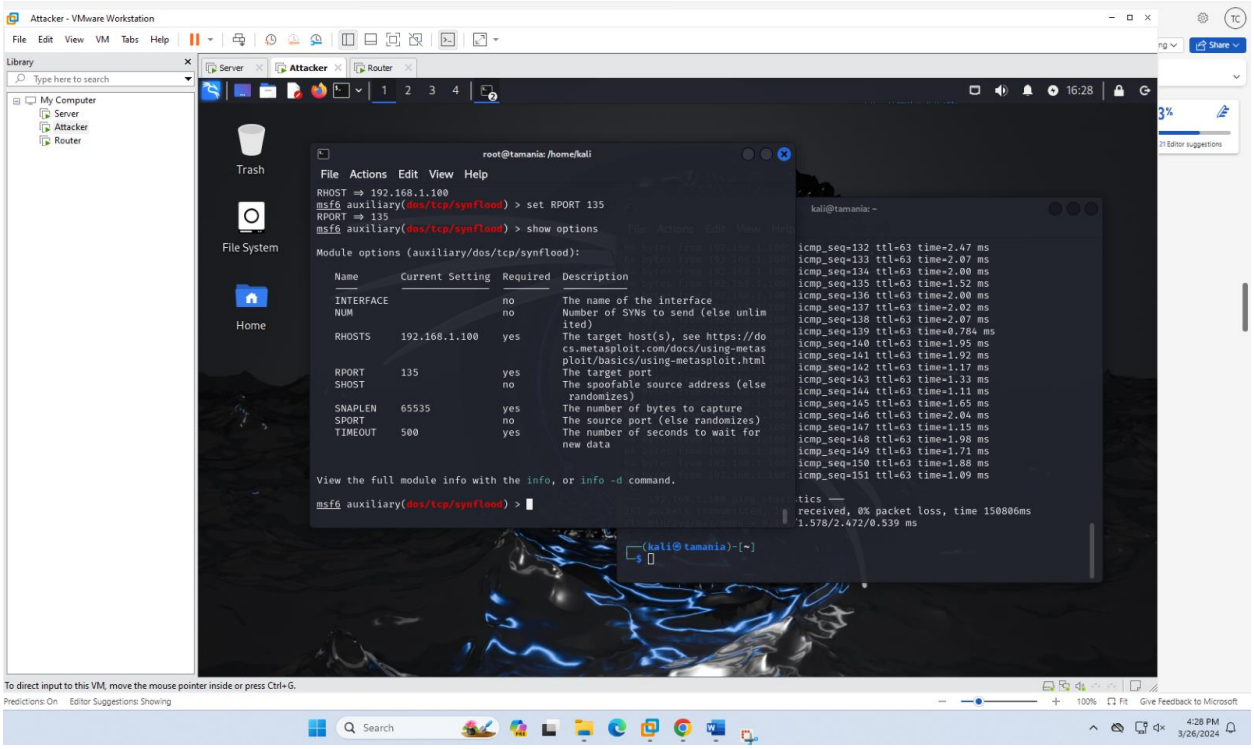
II. Implement TCP SYN Flood Attack:

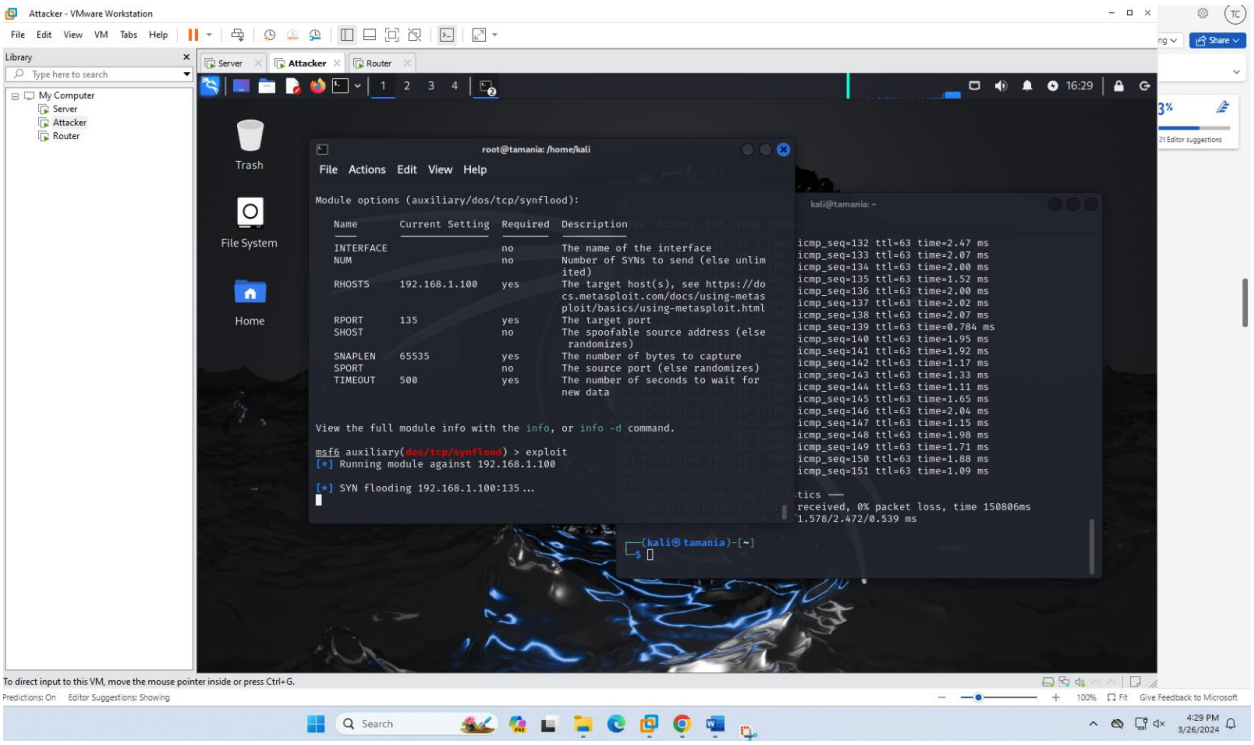
To implement the TCP SYN Flood Attack, I used Metasploit. I set the RHOST and RPORT and ran the exploit. Refer to the video to see it.

Attacker launches attack to Server:

I set RHOST to server IP.





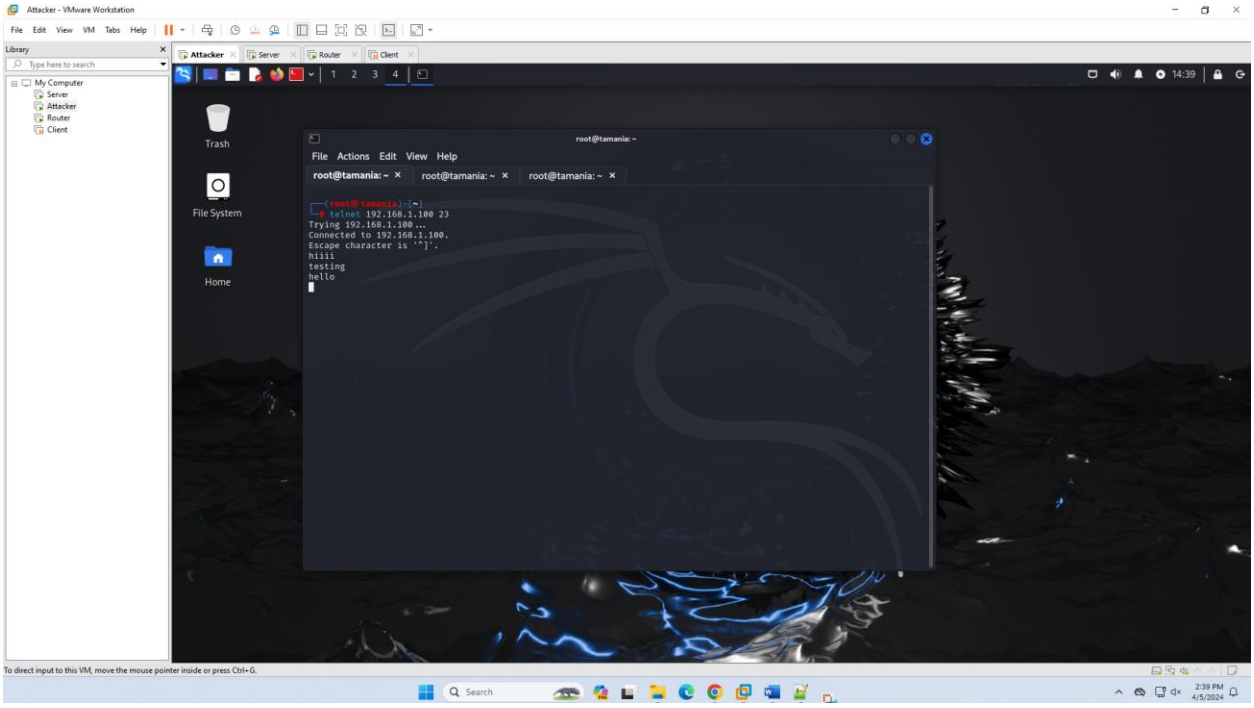


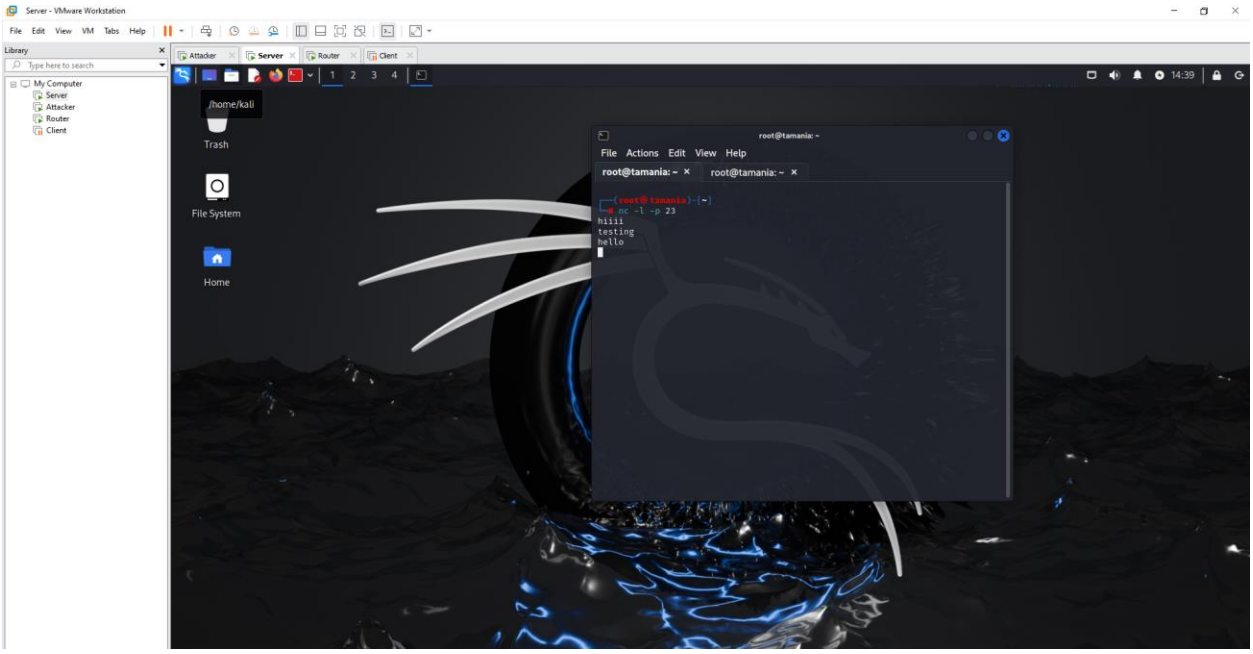
NOTE: The video for the TCP Syn Flood Attack is attached.

III. Implement TCP Reset Attack:

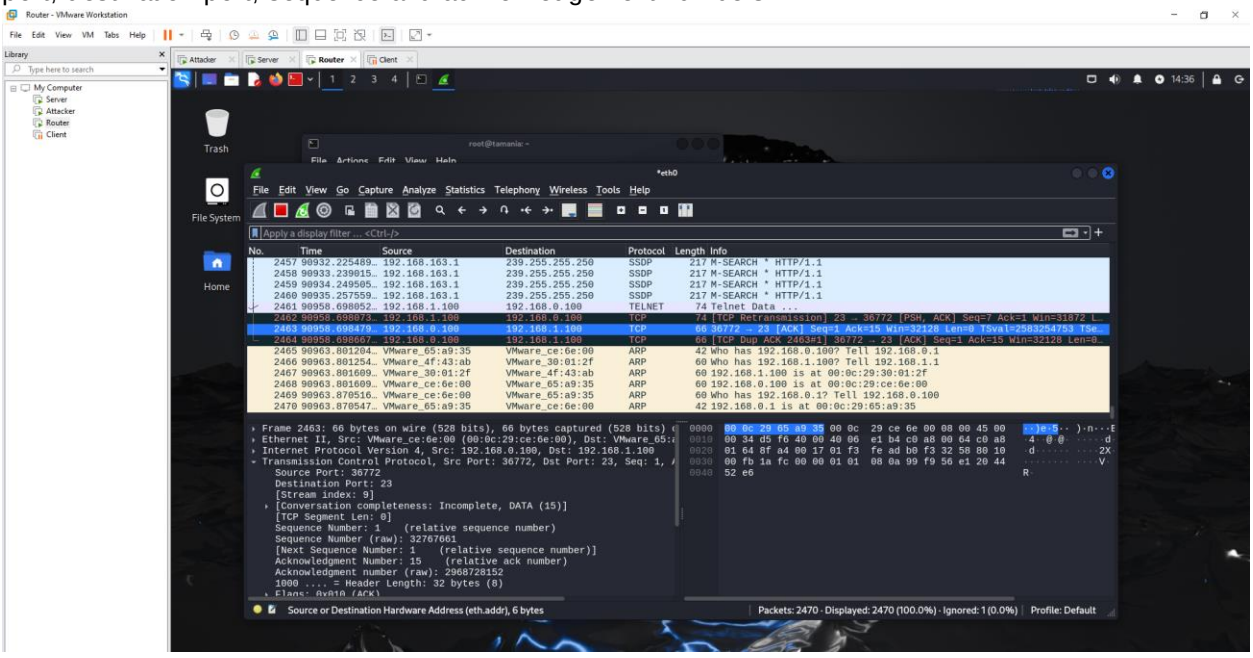
Before attack:

To do the TCP Reset Attack, I created telnet connection using 'nc' and 'telnet'. I did telnet to the server from the attacker machine as shown below.



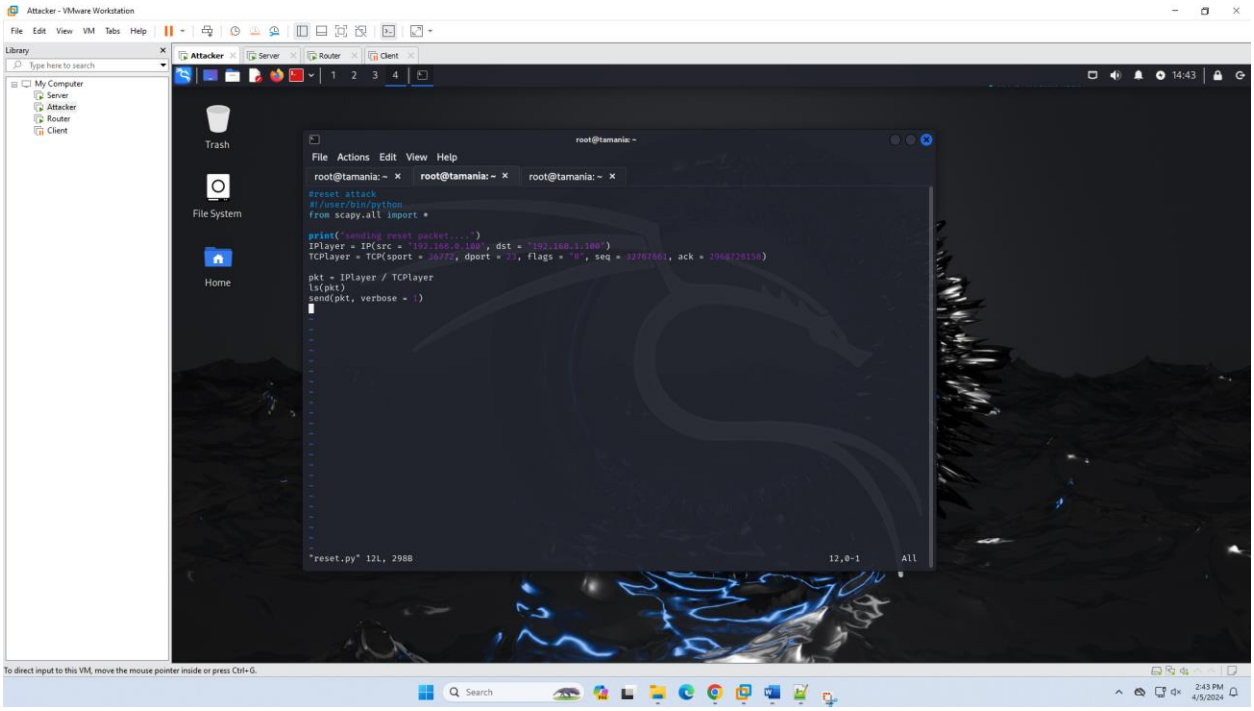


This is the packet that I used. The screenshot shows the information from Wireshark that I used such as source port, destination port, sequence and acknowledgement numbers.

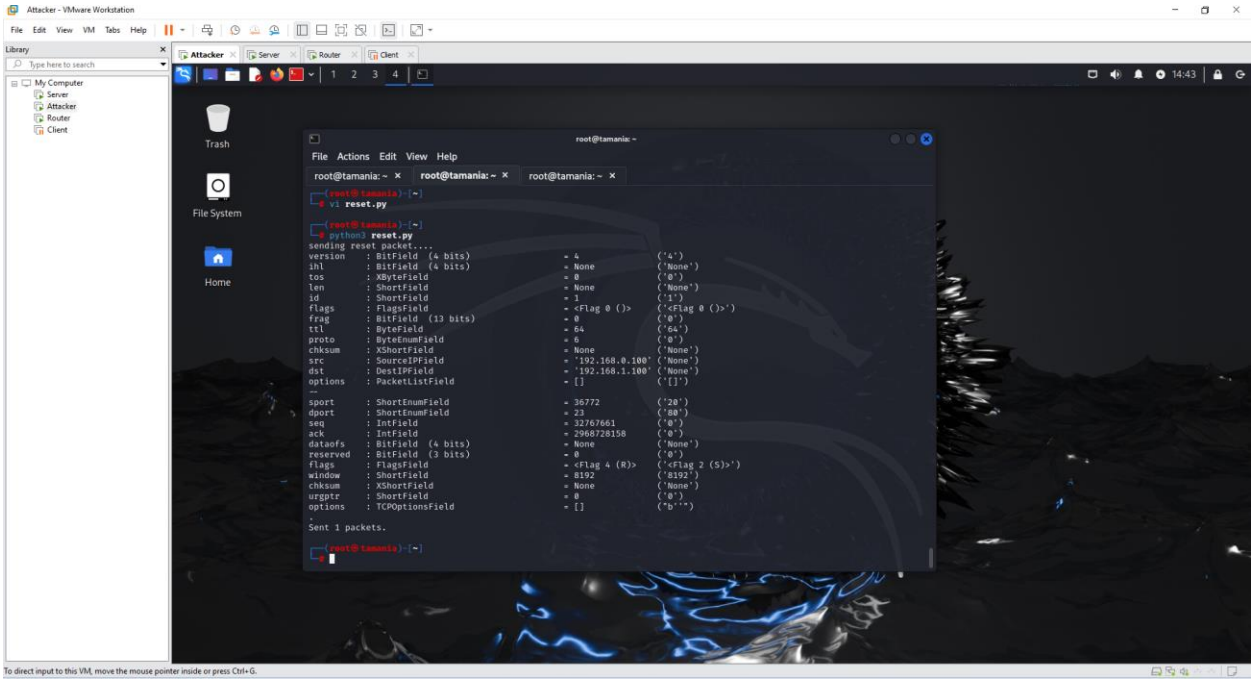


Code:

This is the code I ran to do the reset attack. It sets up the reset packet to be sent from the attacker to the server machine using their respective IP addresses and the packet information.

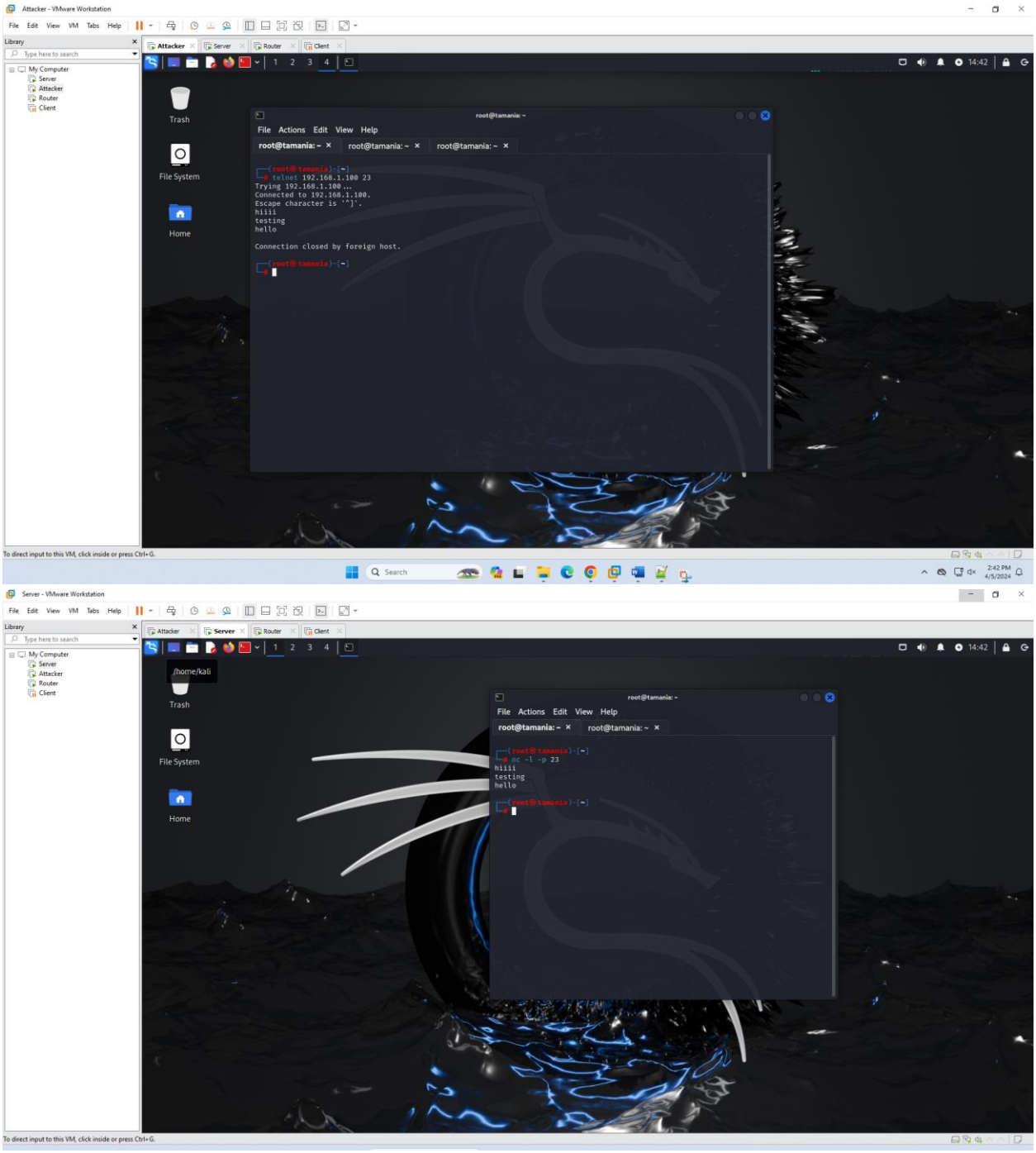


This is the command to run the .py code.



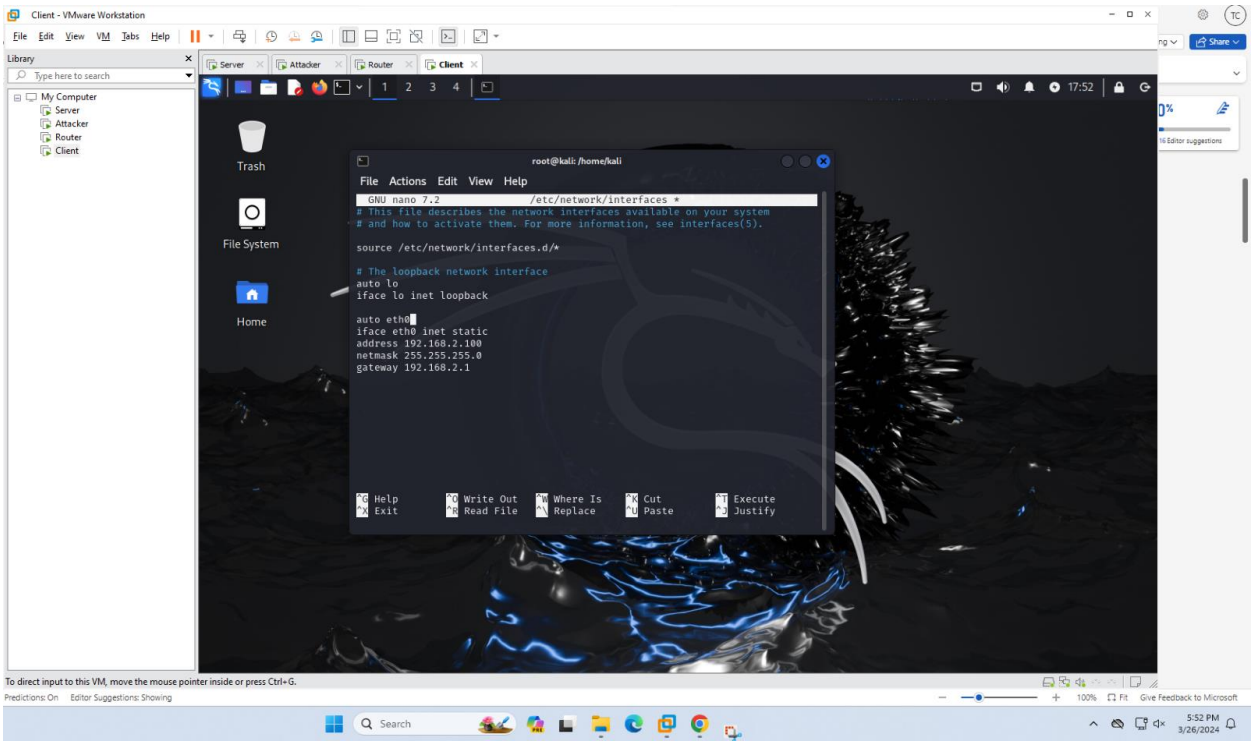
After (results of reset attack):

The following screenshots display that due to the reset packet being sent, the telnet connection is closed.

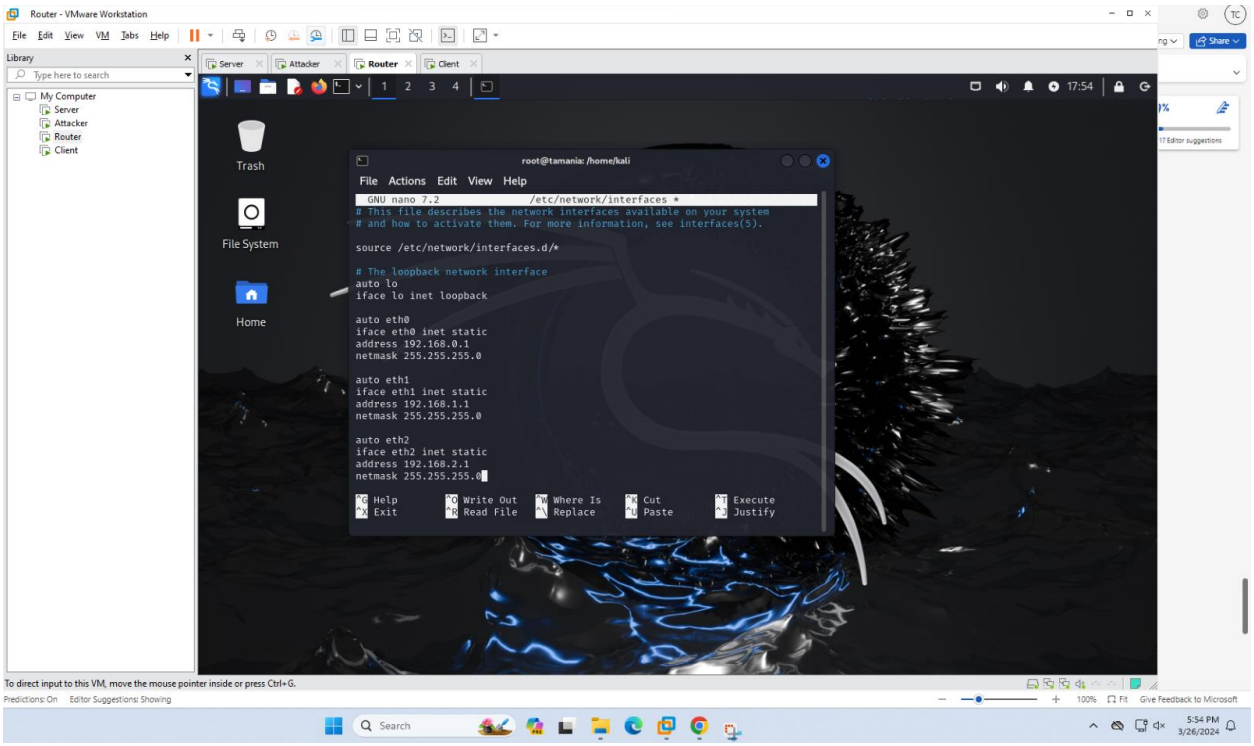


IV. Implement TCP Session Hijacking Attack

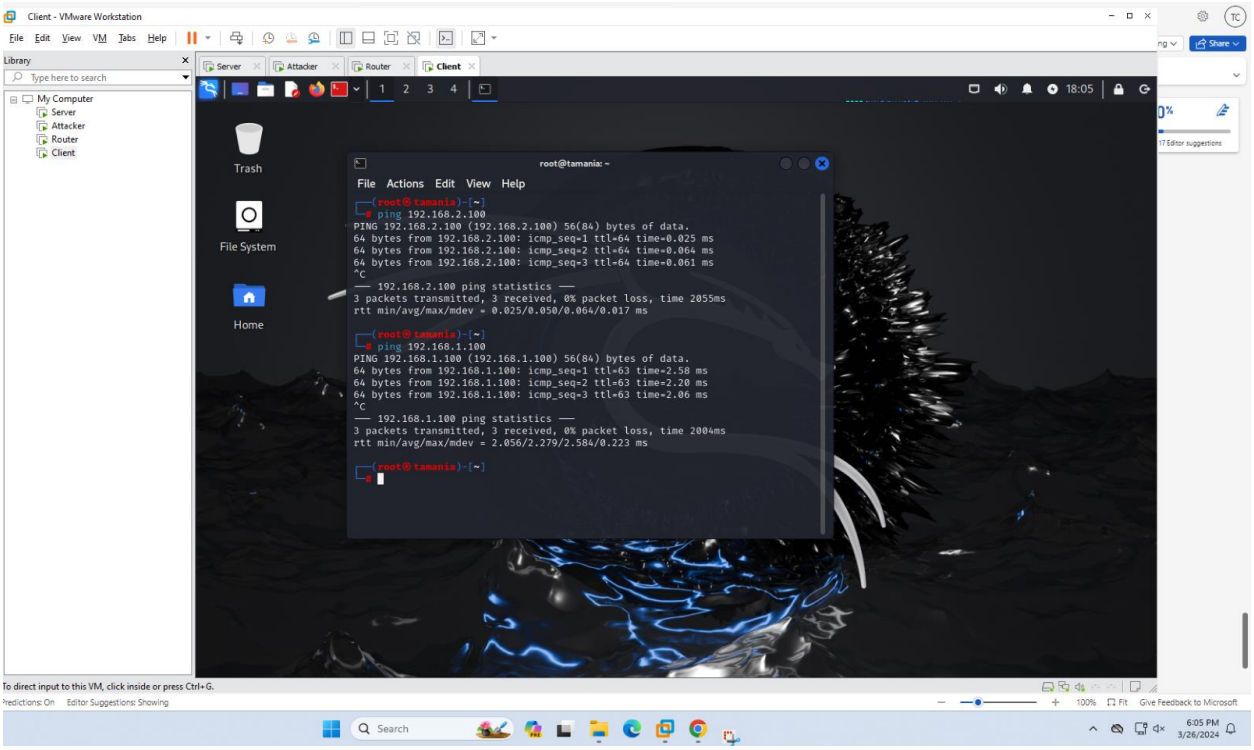
For the TCP Session Hijacking Attack, I needed to create another VM called Client.



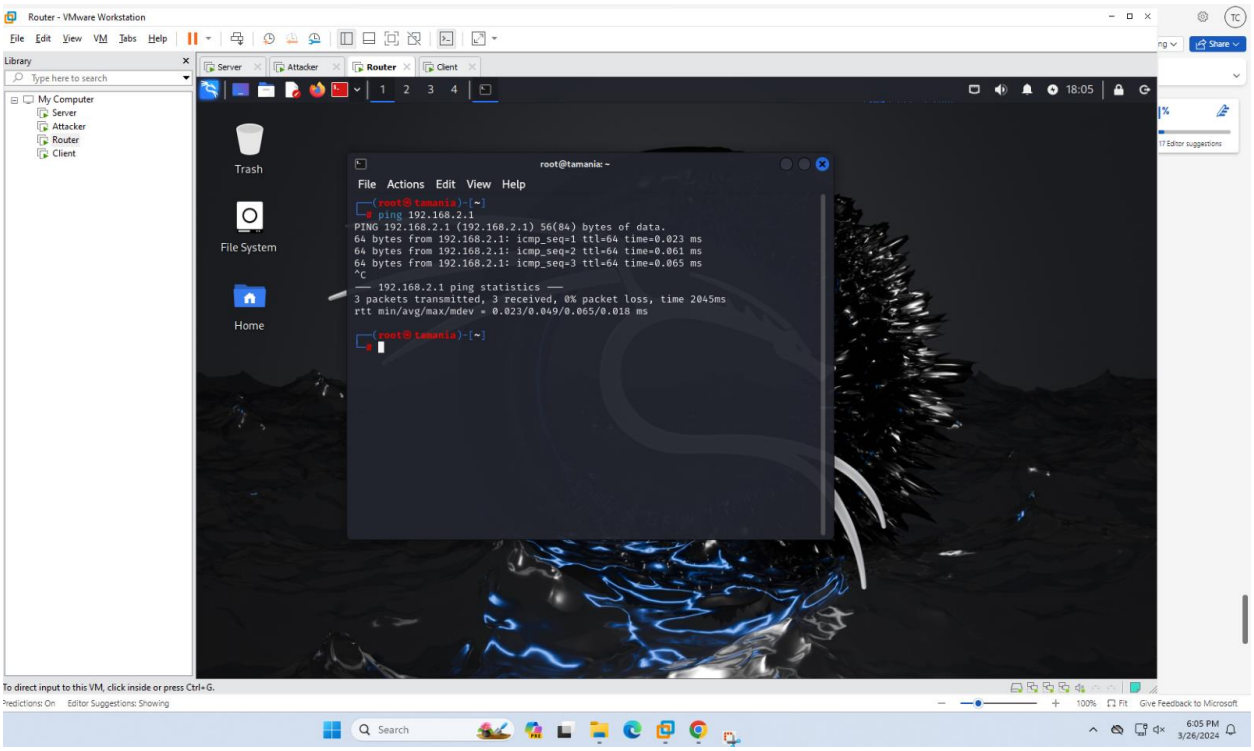
And added it to the router interface.



The following screenshots prove that the new machine can ping the others. Client can ping others below.

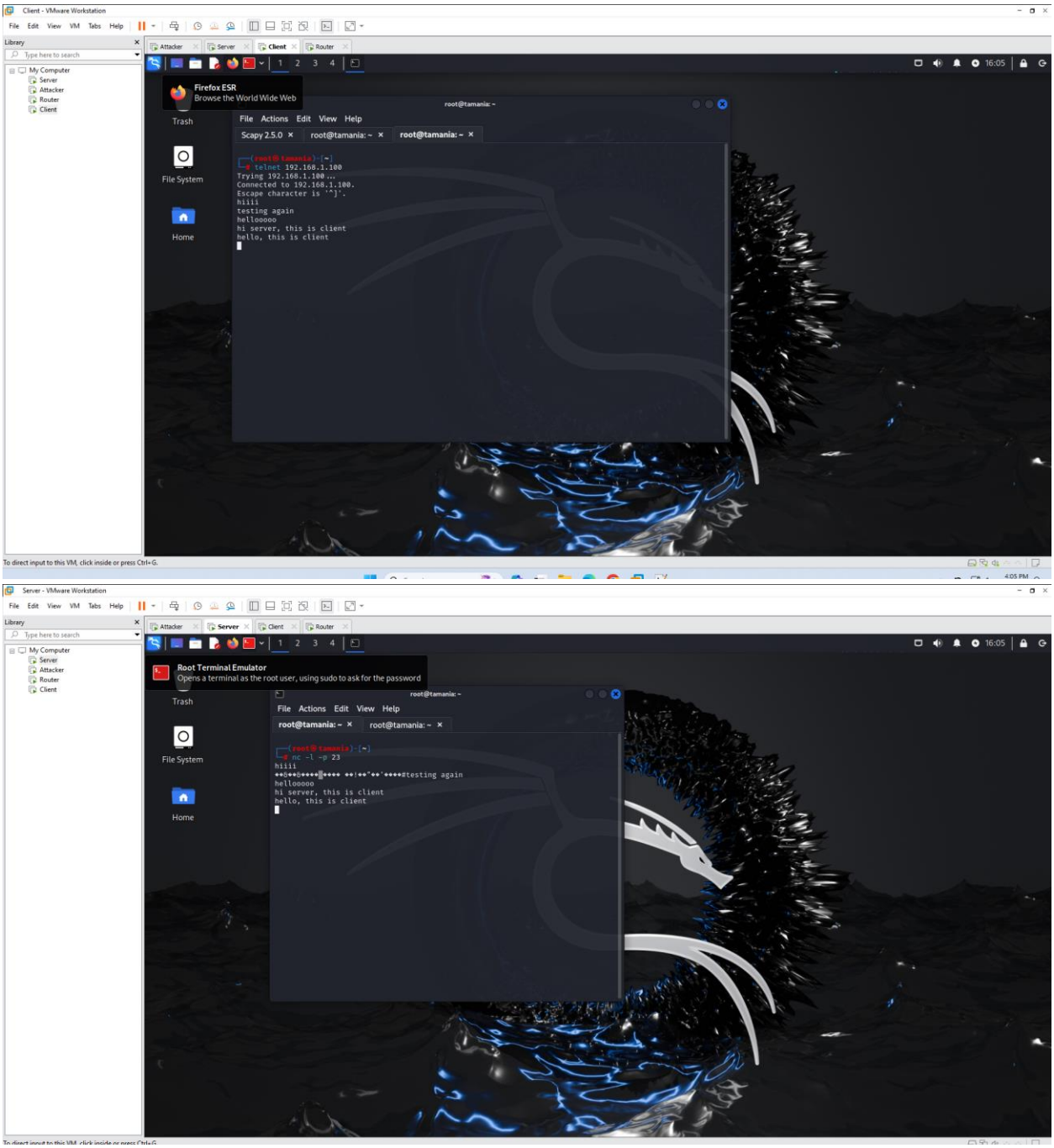


The next shows that router can ping too.

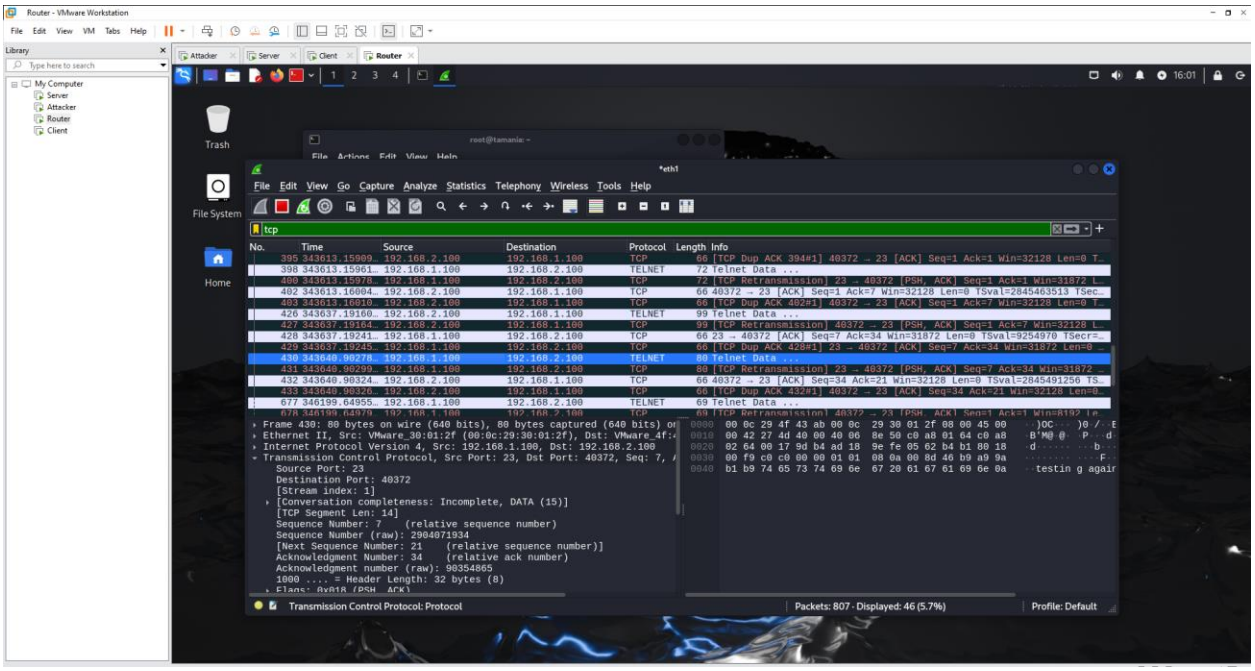


Before hijack attack:

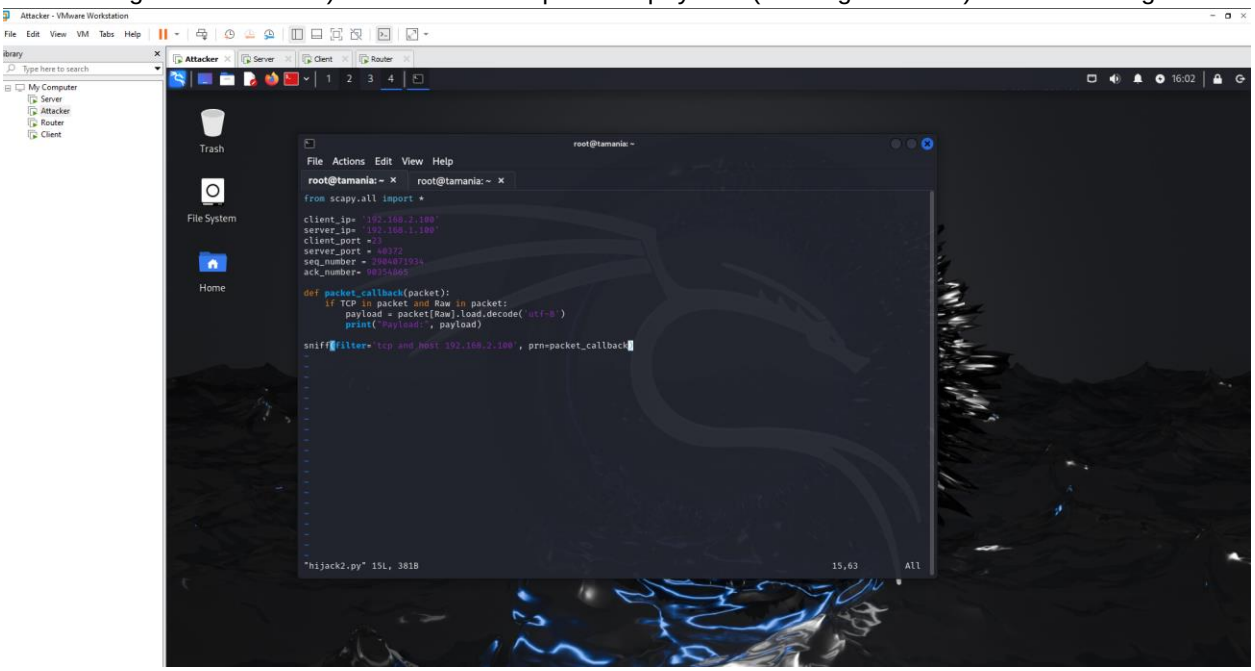
The actual session hijack attack happens in the next several screenshots. First, I made sure the Server machine was listening. I established a Telnet connection between client and server to exchange messages. Note that the most recent message says, ”hello, this is client”.



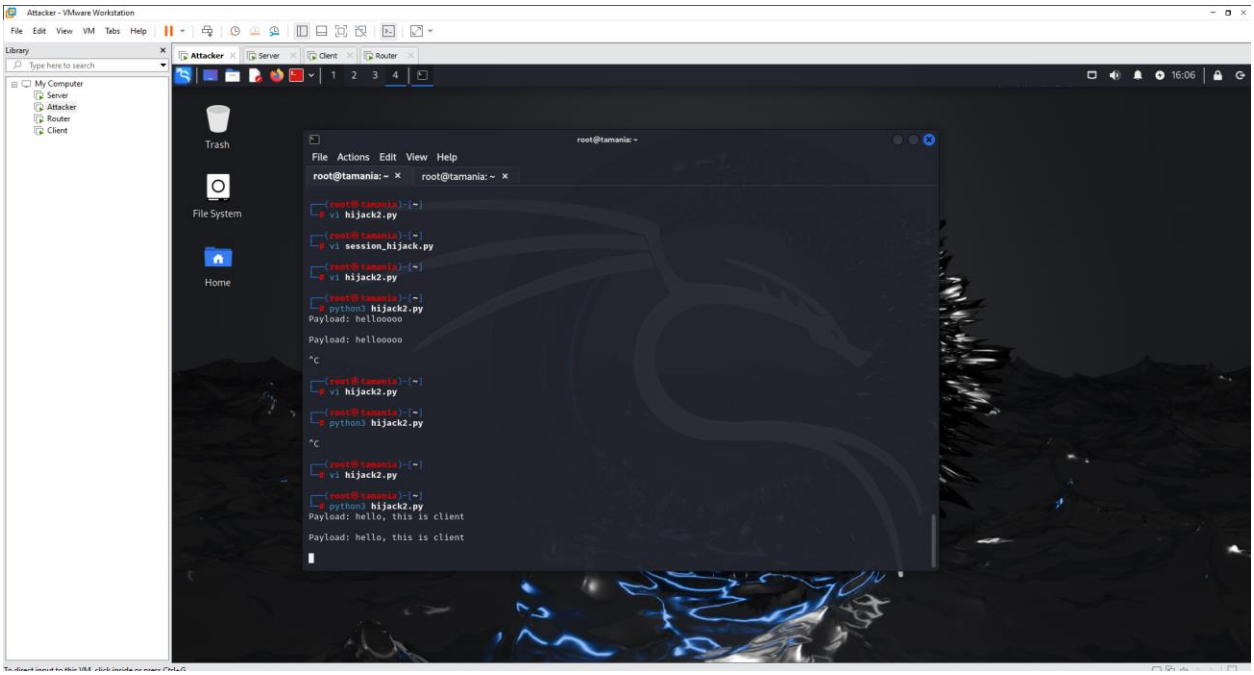
The following shows packet info from telnet connection.



This is the python code for hijack attack. It takes the TCP information (IP addresses, port, sequence and acknowledgement numbers) and uses that to print the payload (message content) after extracting it.



Ran the attack and attacker can now view the message sent between client and server. The result is the following line “Payload: hello, this is client”.



NOTE: I attached a couple videos showing Wireshark running, the TCP Syn Flood attack, the TCP Reset attack and the TCP Hijack attack. The latter two attacks include some source code. Those were also attached in the report and the zip file.