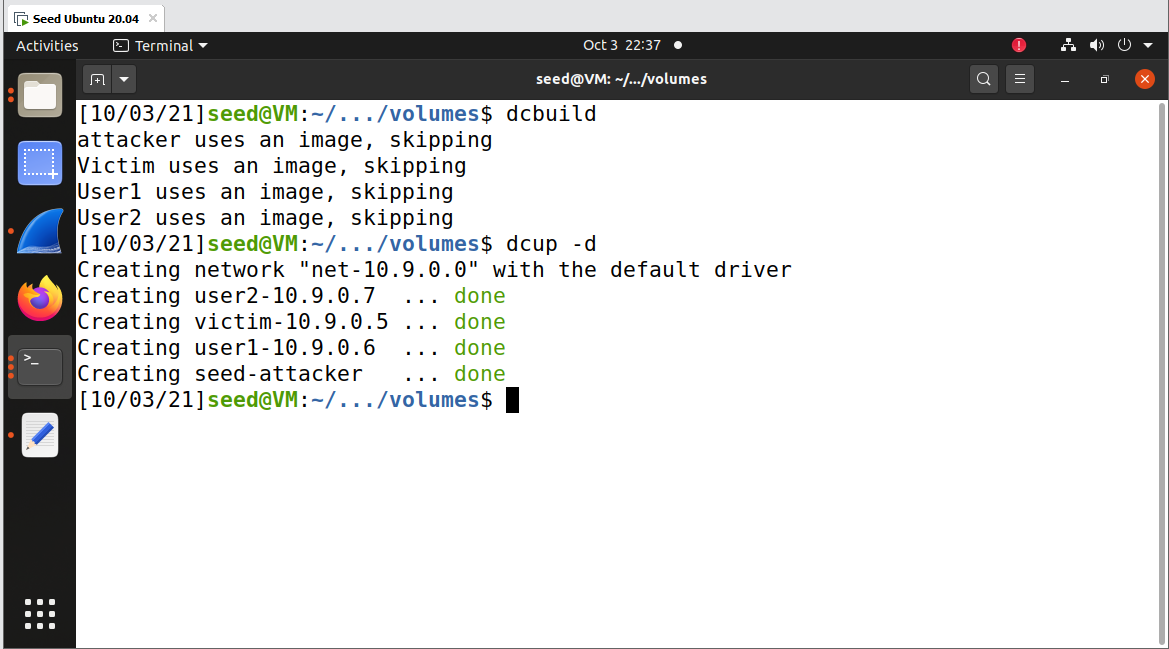
Advanced Computer Networking and Security - 5800

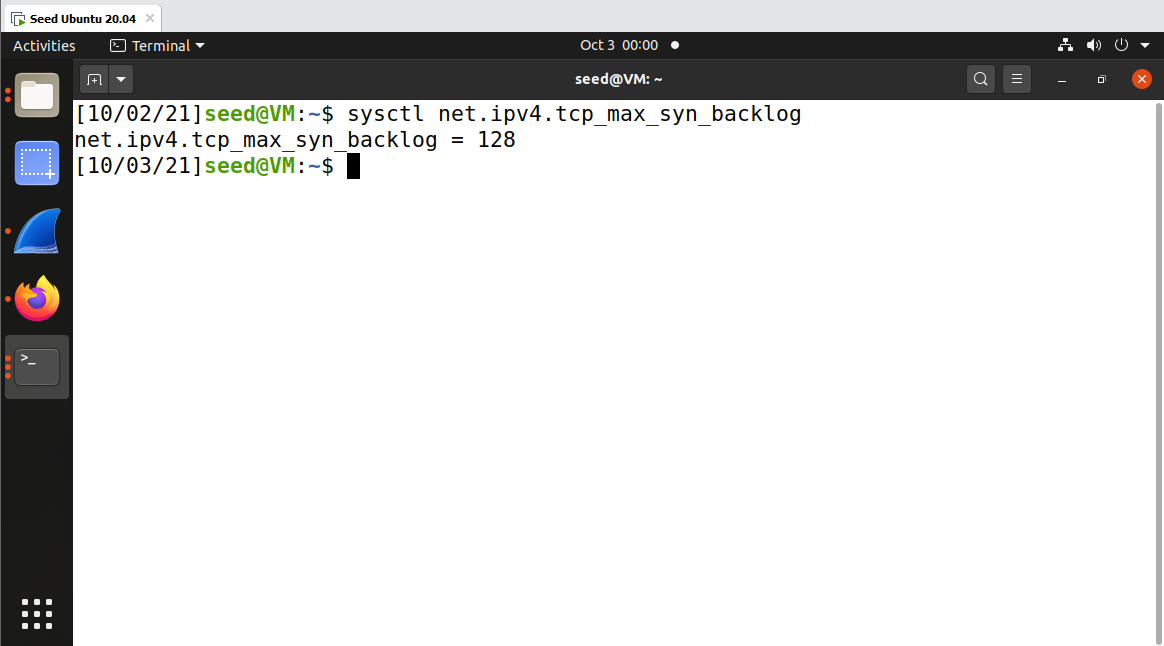
Assignment -5

TCP/IP Attack Lab

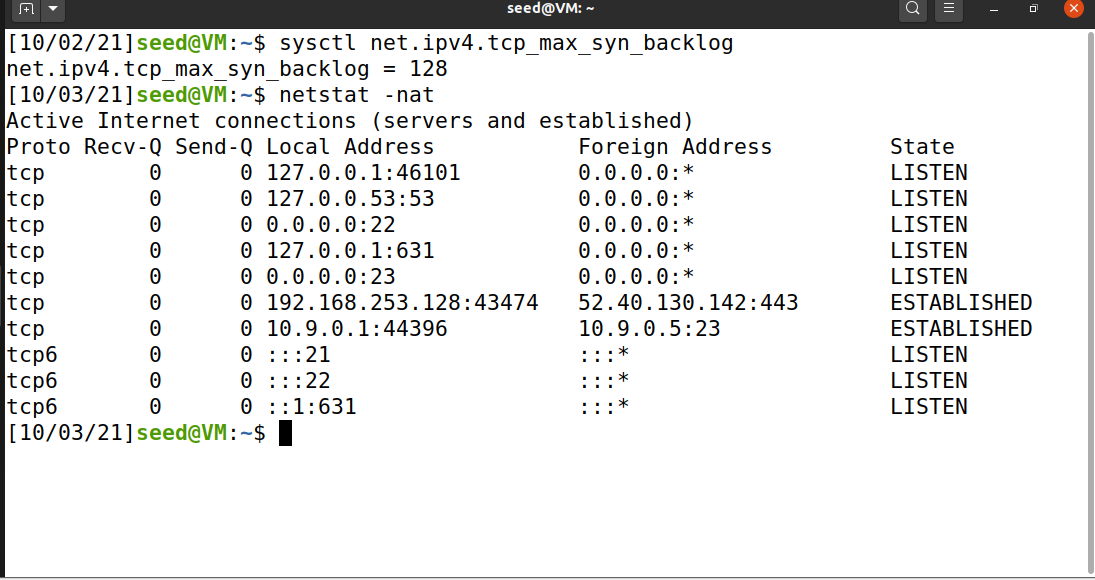
Name:Jonnada Sai Rohit

ID : 700723743

Turning on the docker 

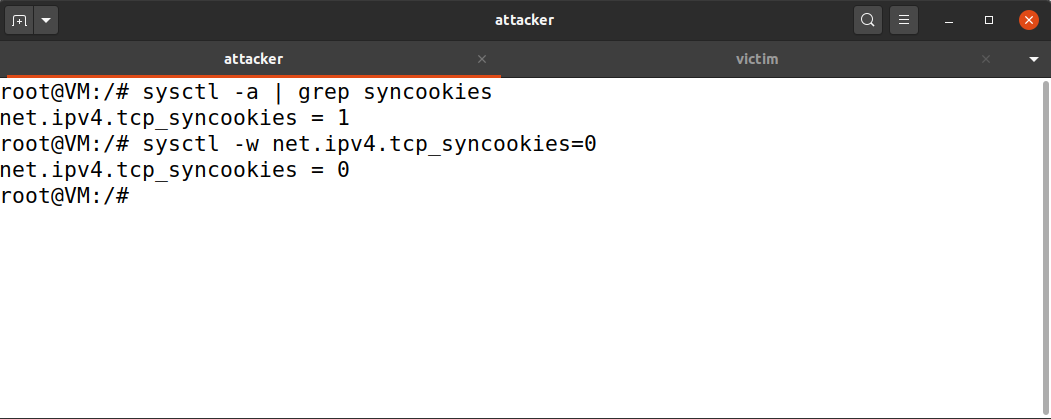
Checking the size of the queue for system wide setting

Checking the current open ports which are awaiting connections, the established connection shows that 3-way handshake is completed

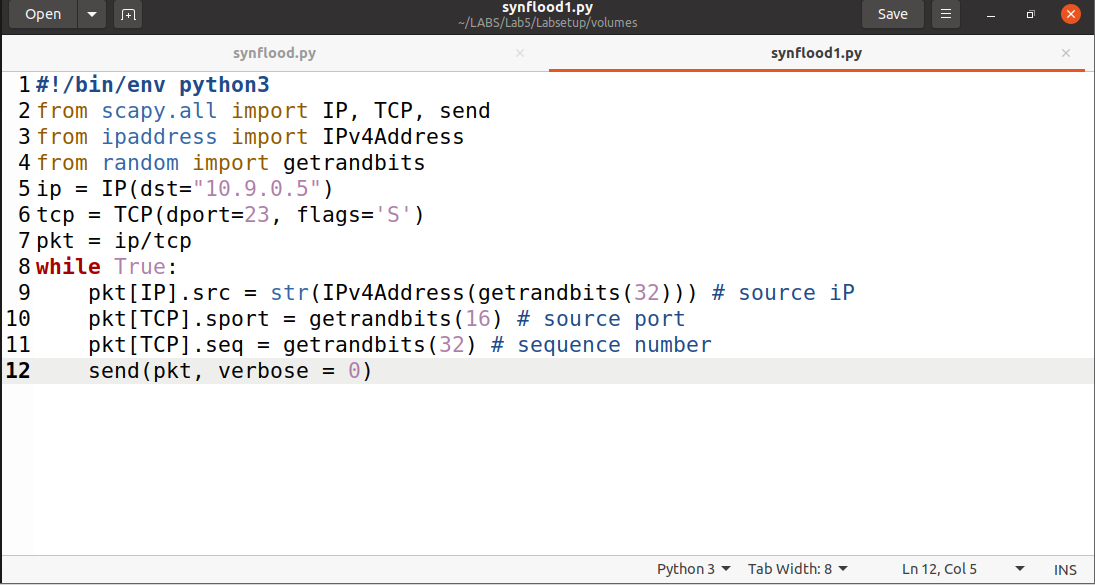


Checking SYN Cookie Countermeasure whether is turned on or off

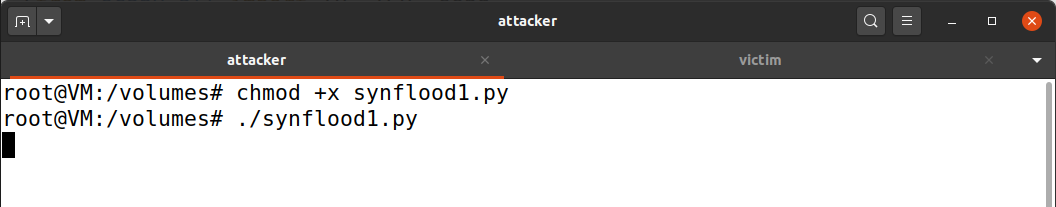
Turning off the SYN Countermeasure



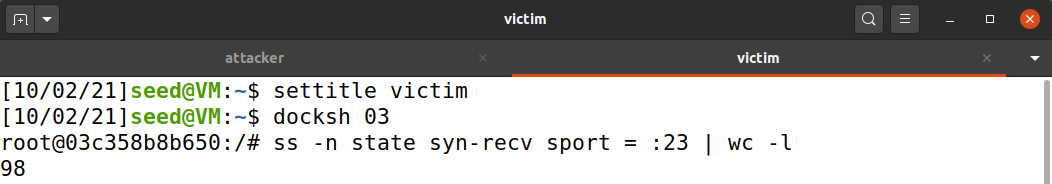
Code for the syn flood



Running the synflood attack from attacker terminal



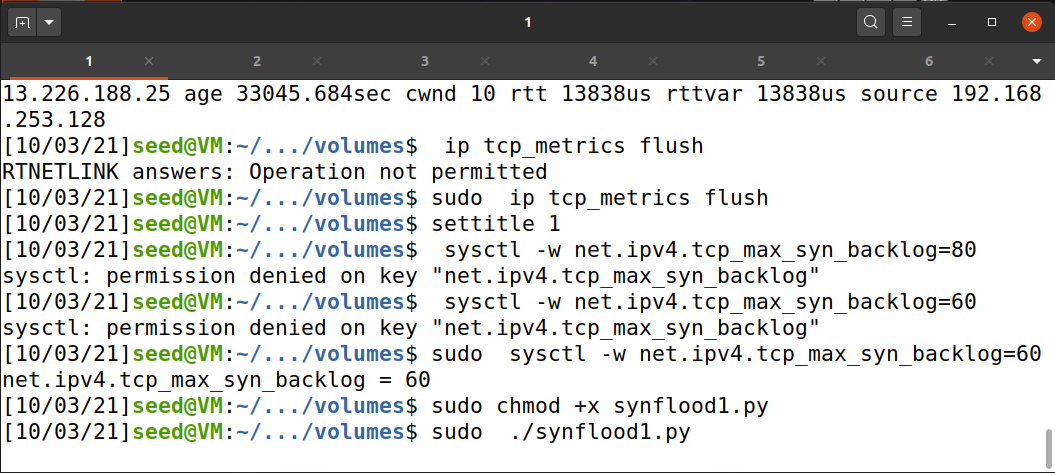
Checking the number of items in queue on victim machine

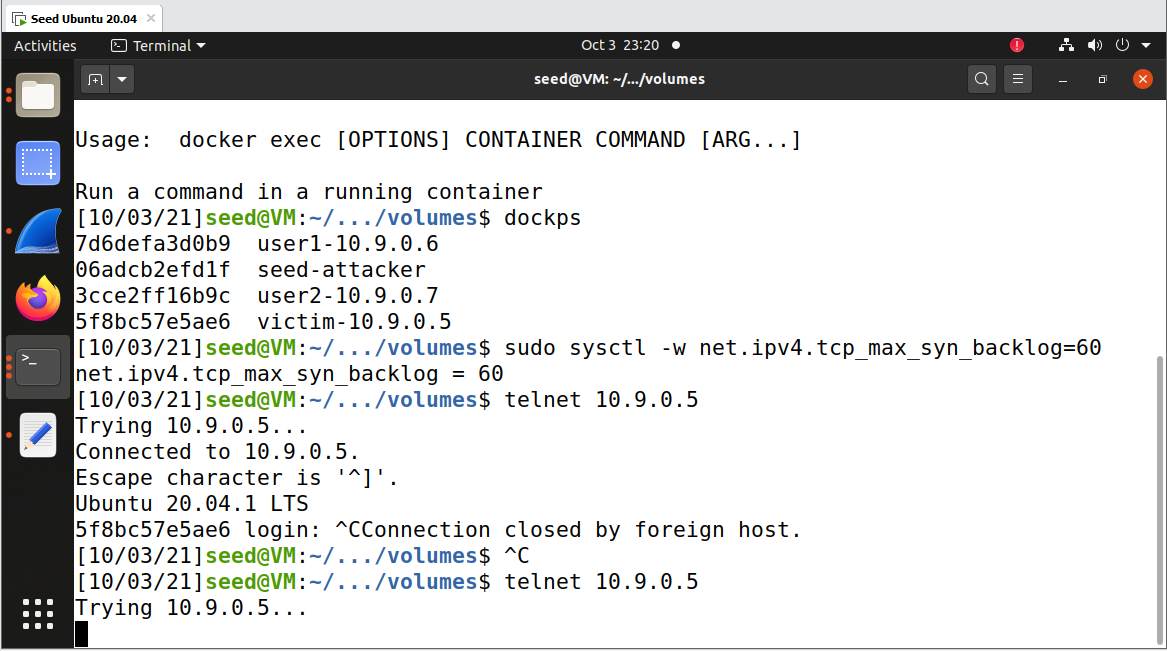


Setting the queue to 60 in victim

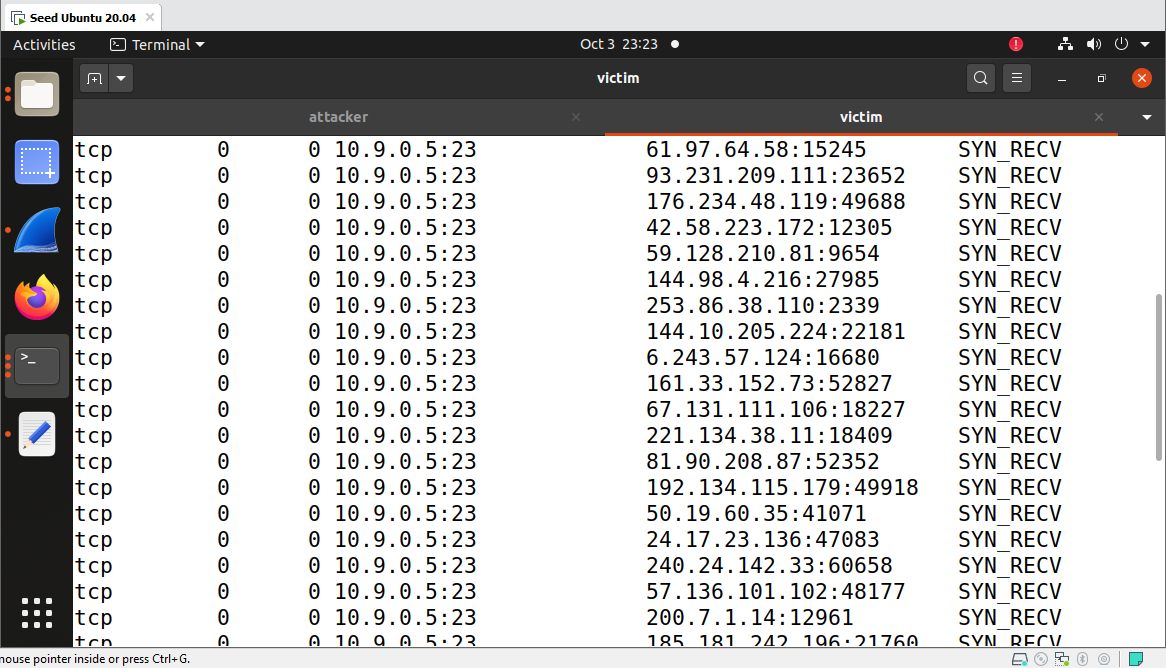


Running the synflood code in 6 terminal to fill the queue

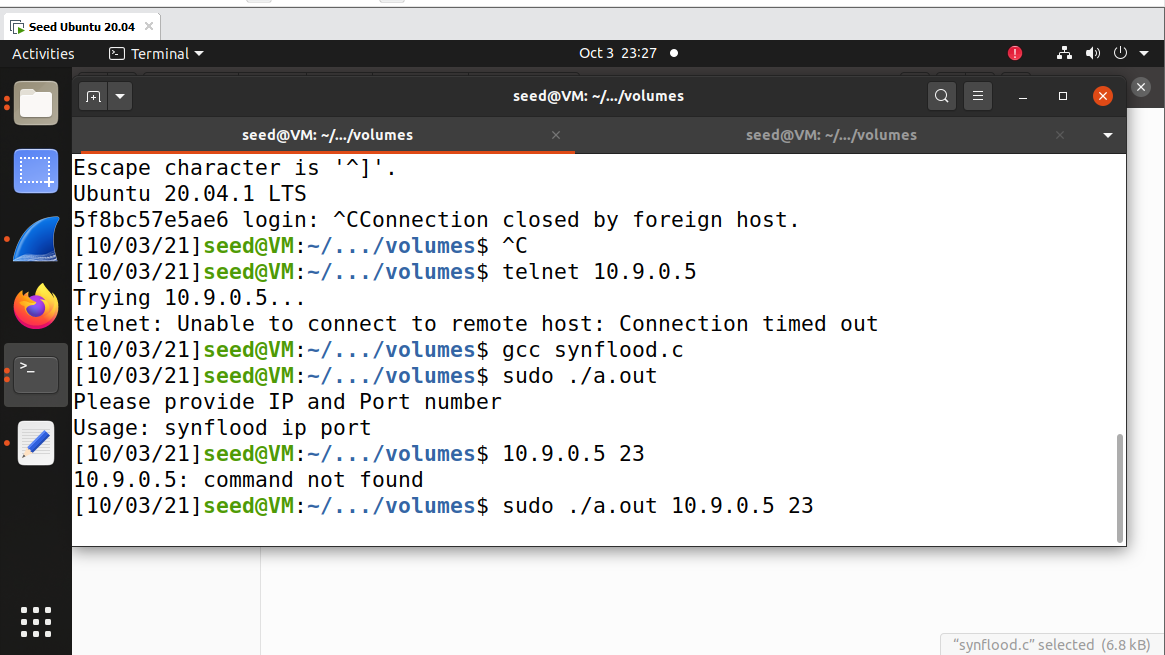


Cannot connect telnet on 10.9.0.5 since queue is filled 

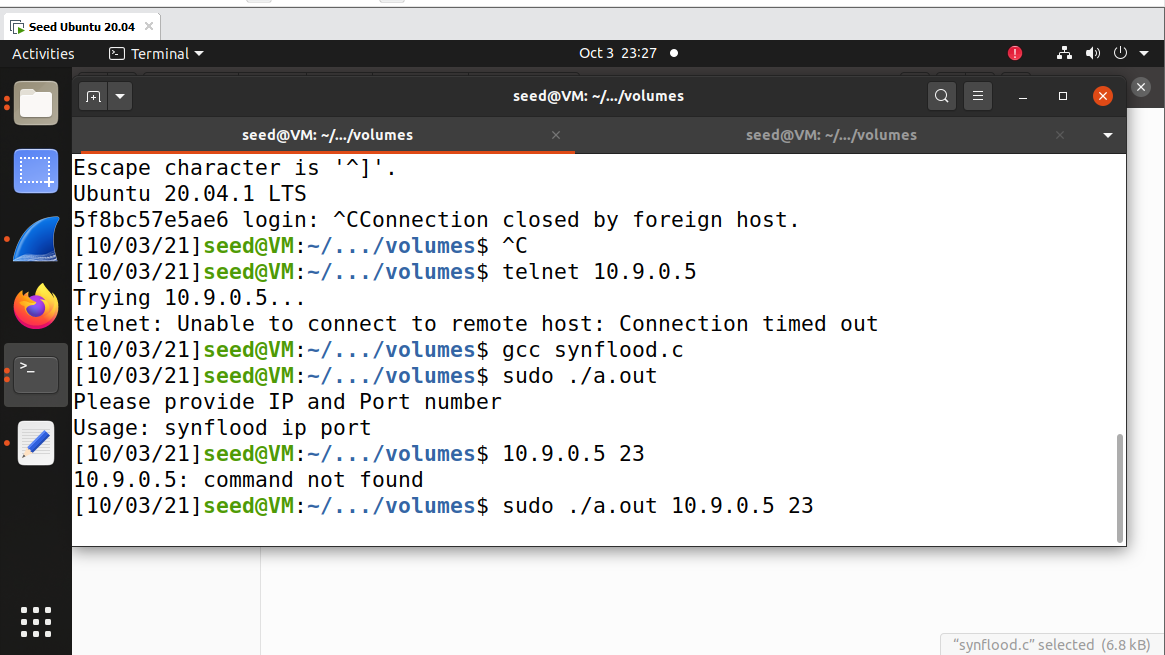
Net stat –n on victim

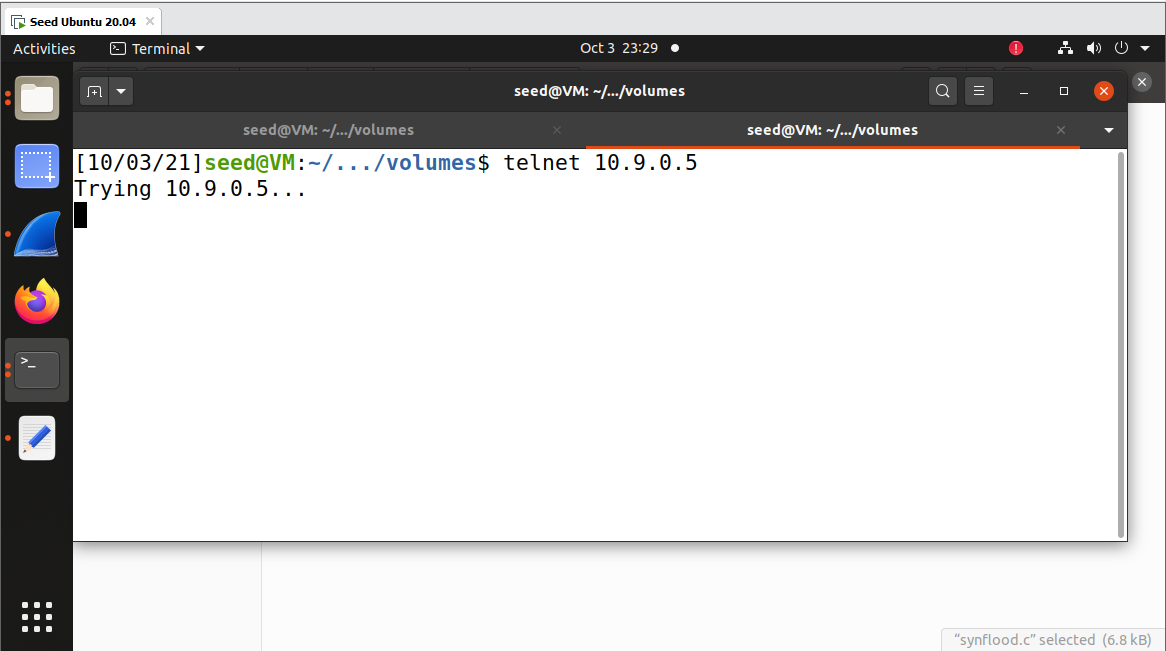


# Task 1.2

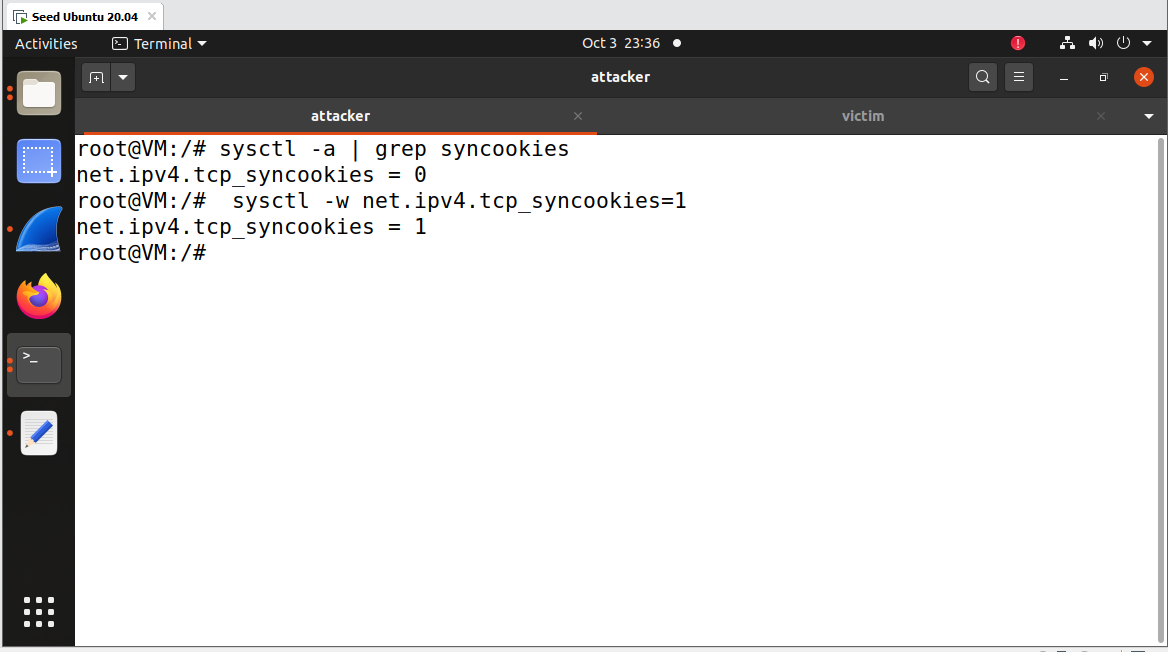
Running the synflood.c 

Giving the victim ip and port number

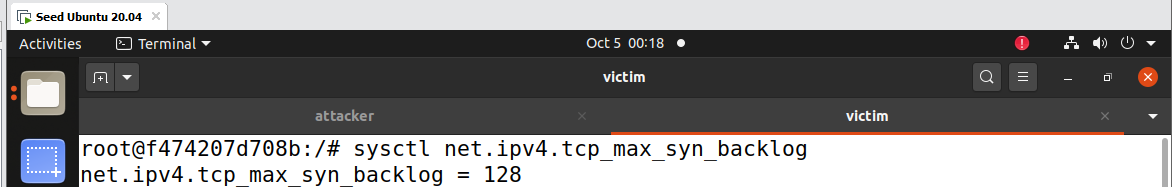


Unable to connect to 10.9.0.5 using telnet 

Turning on sync outer measure

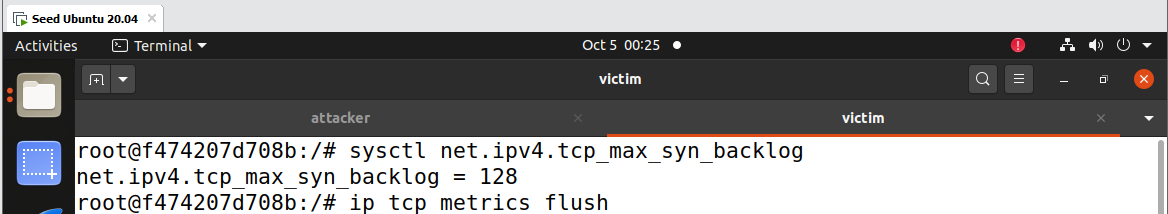


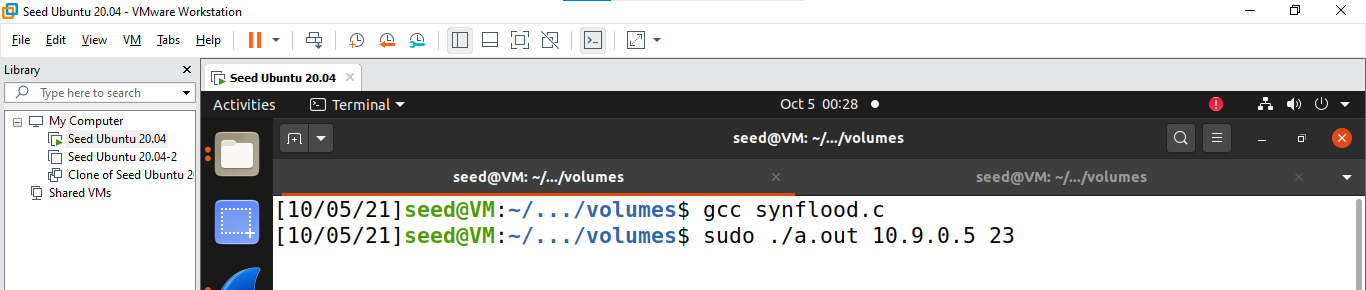
Setting back the syn backlog to max

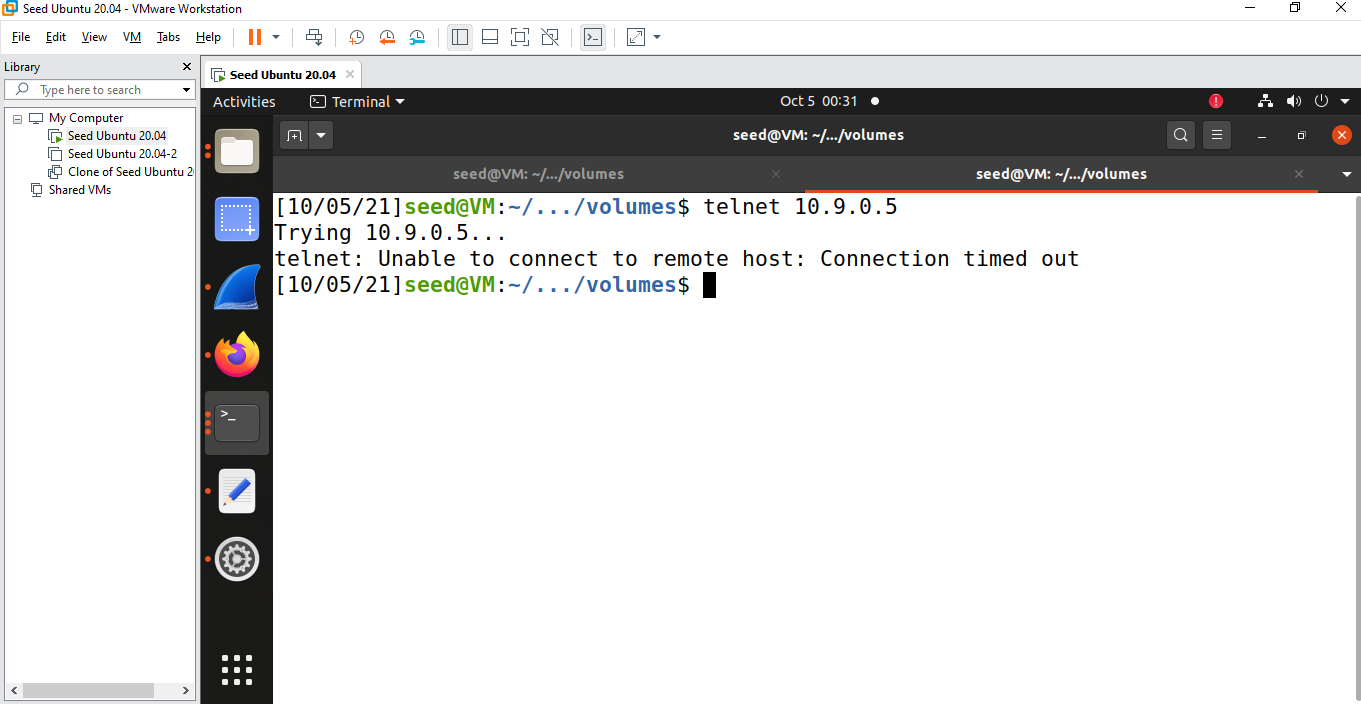


Telnet connection was successful when we run using python

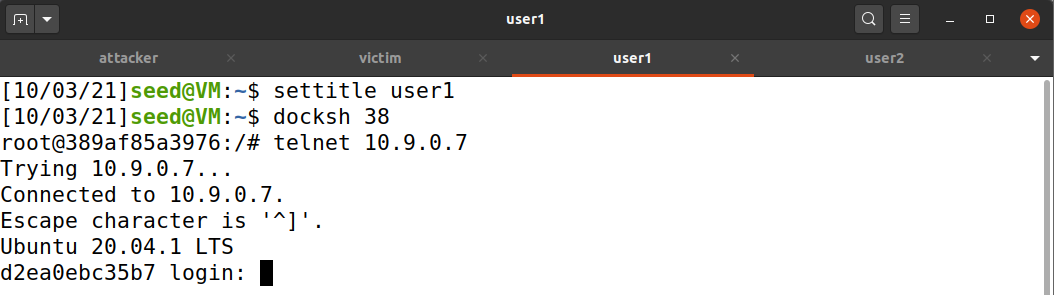
Flush the ip



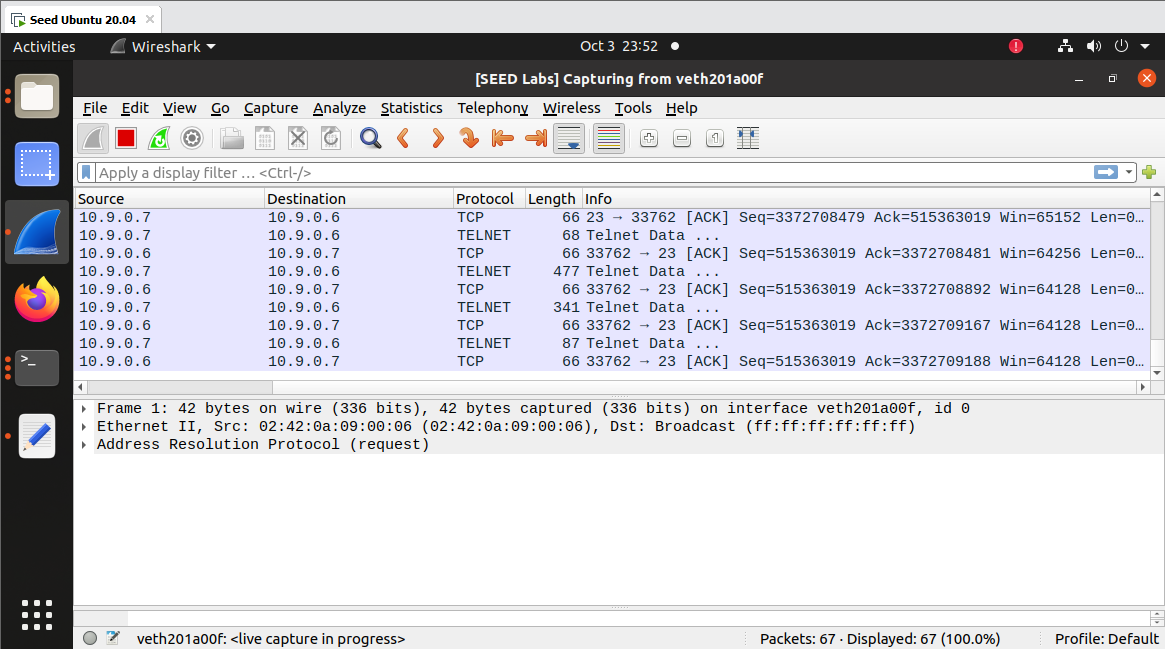
Running the code

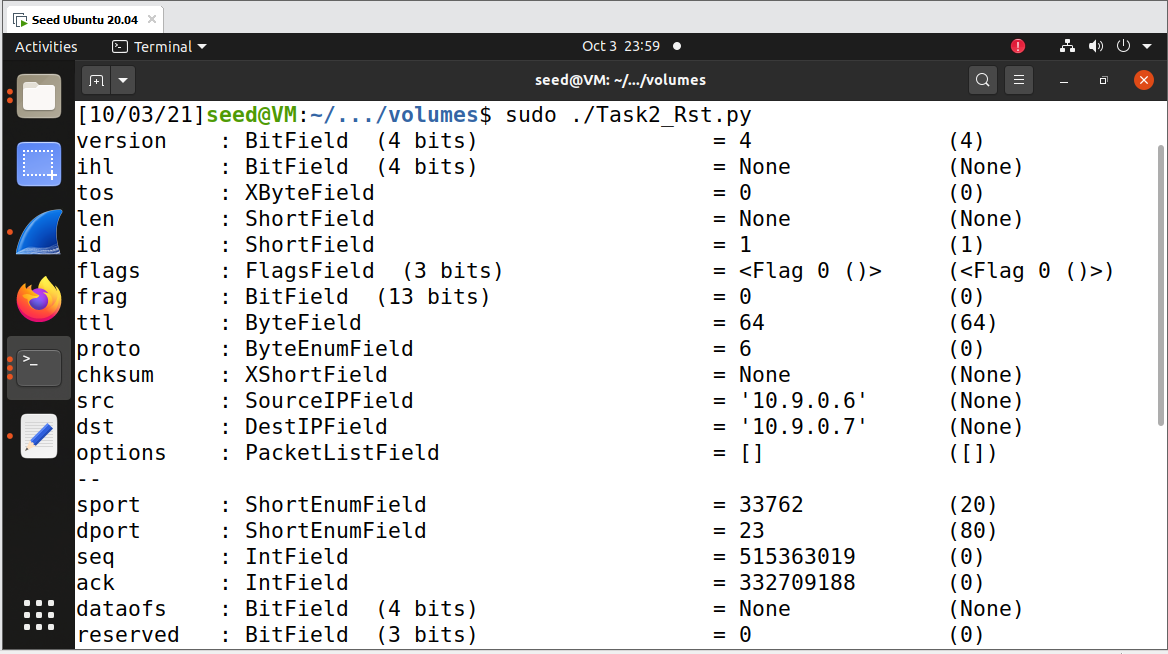
Since we run using the c code the syn flood attack is successful couldn’t create the telnet connection

# Task2

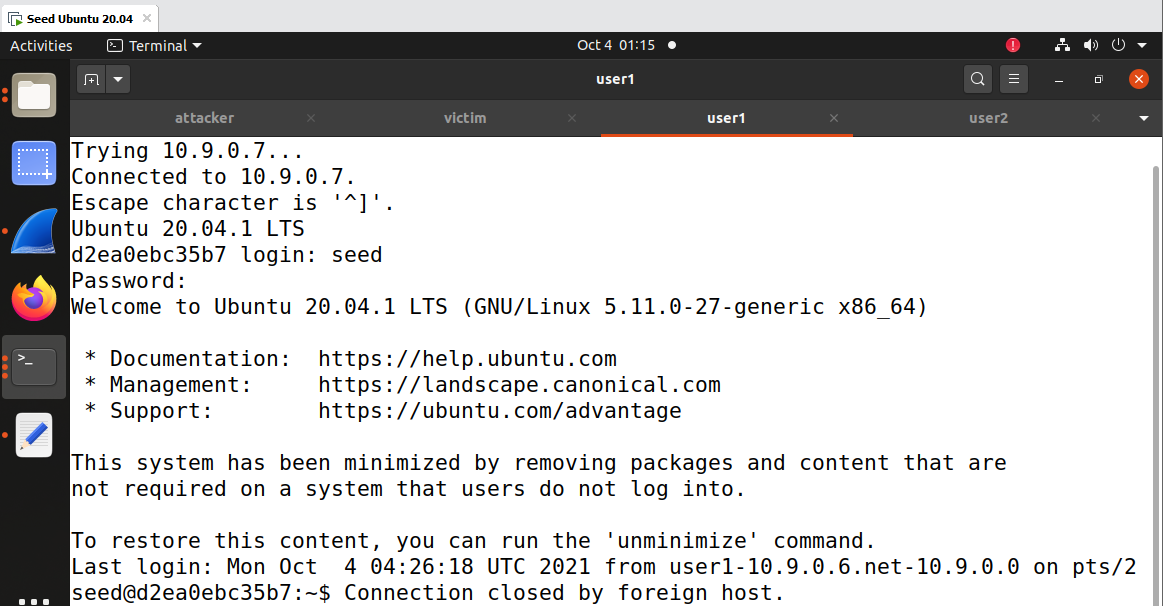
Telnet 10.9.0.7 from user 1

Post login getting the ack and seq number from wireshark



Running the Rst code from terminal

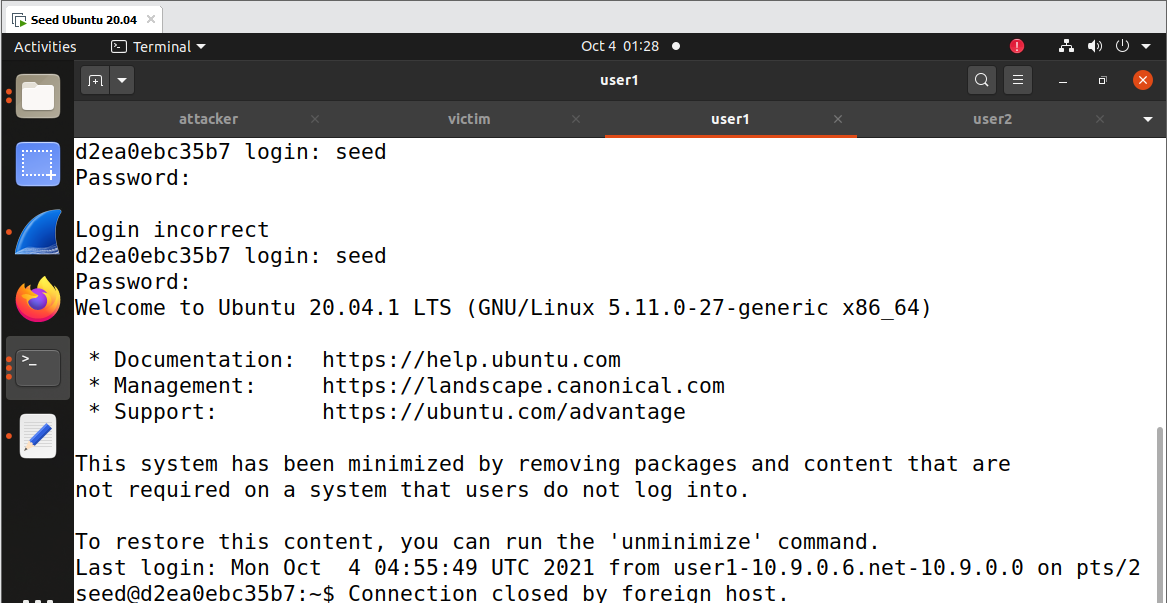
Telnet Connection has been closed post running rst attack



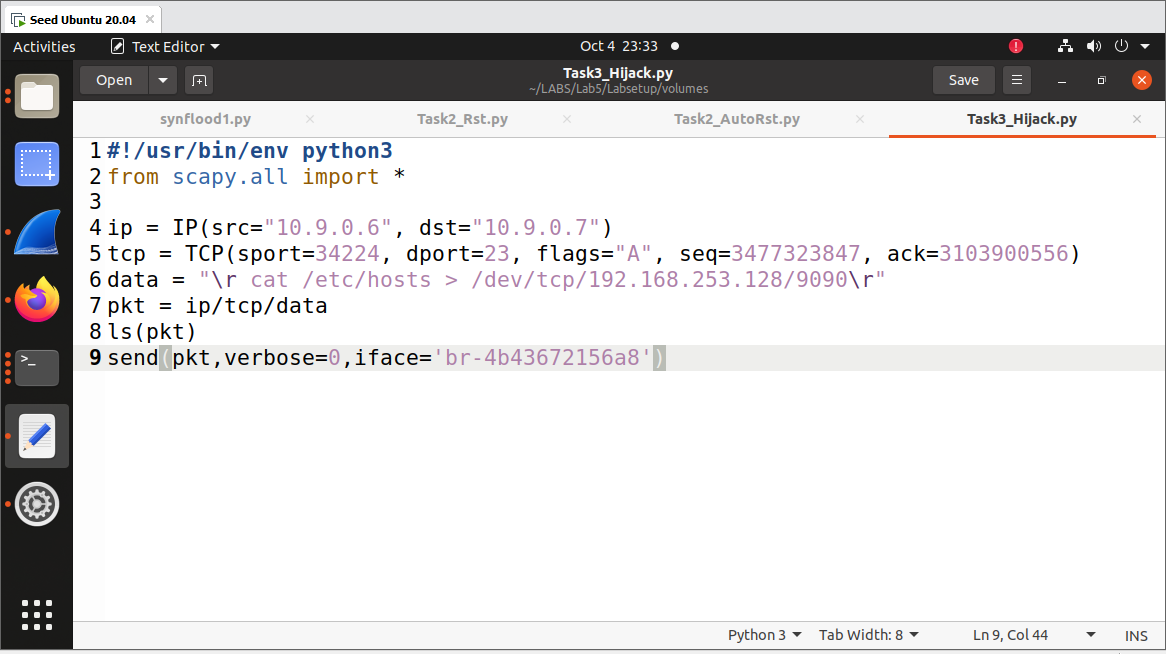
Telnet login from user 1 to user 2

Code for Automatic Rst attack

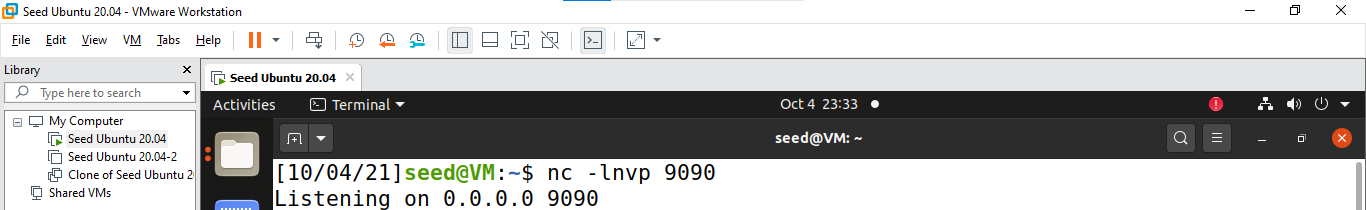


Connection is closed on pressing any button

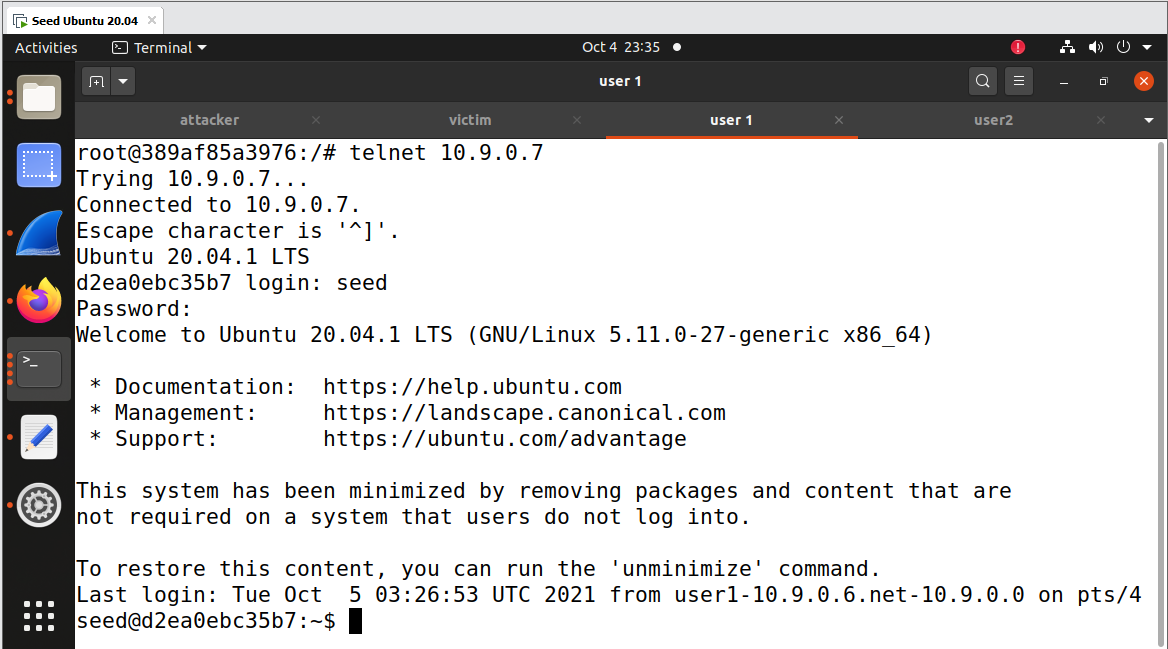
## Task3:

Code for hijack session 

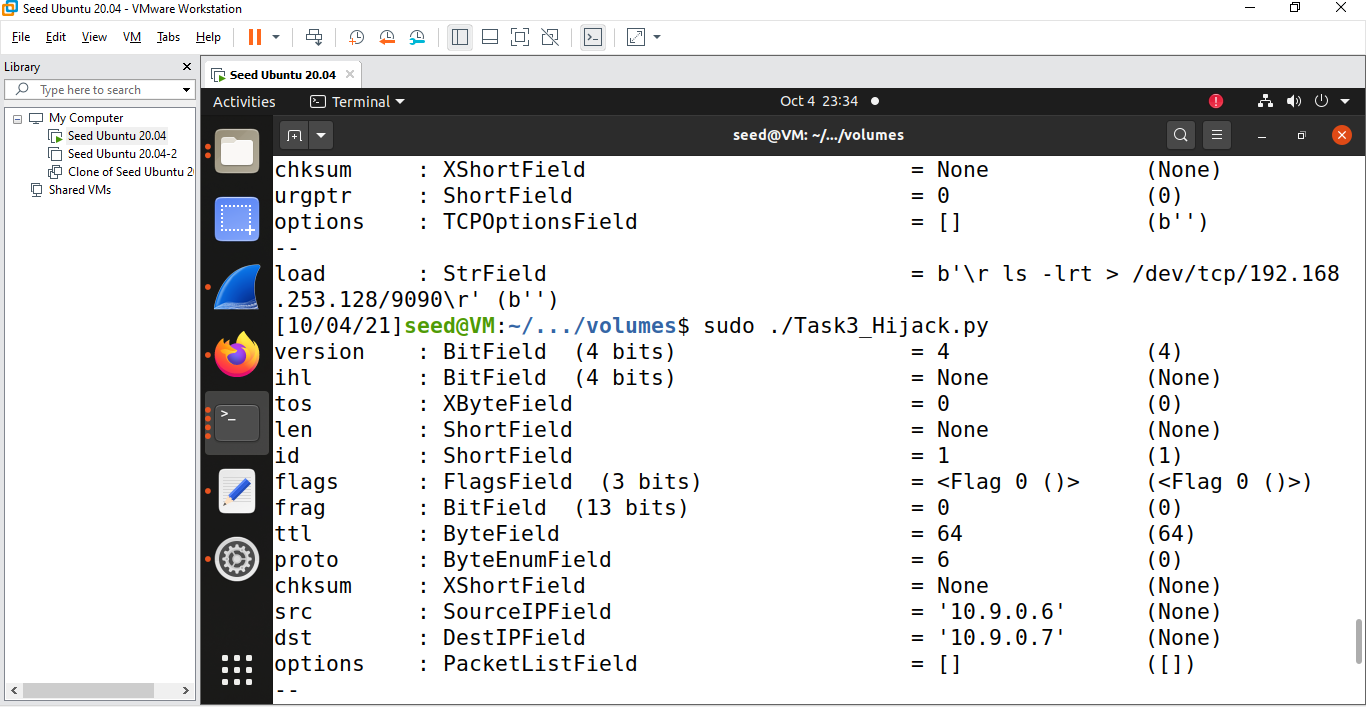
Listening on port 9090

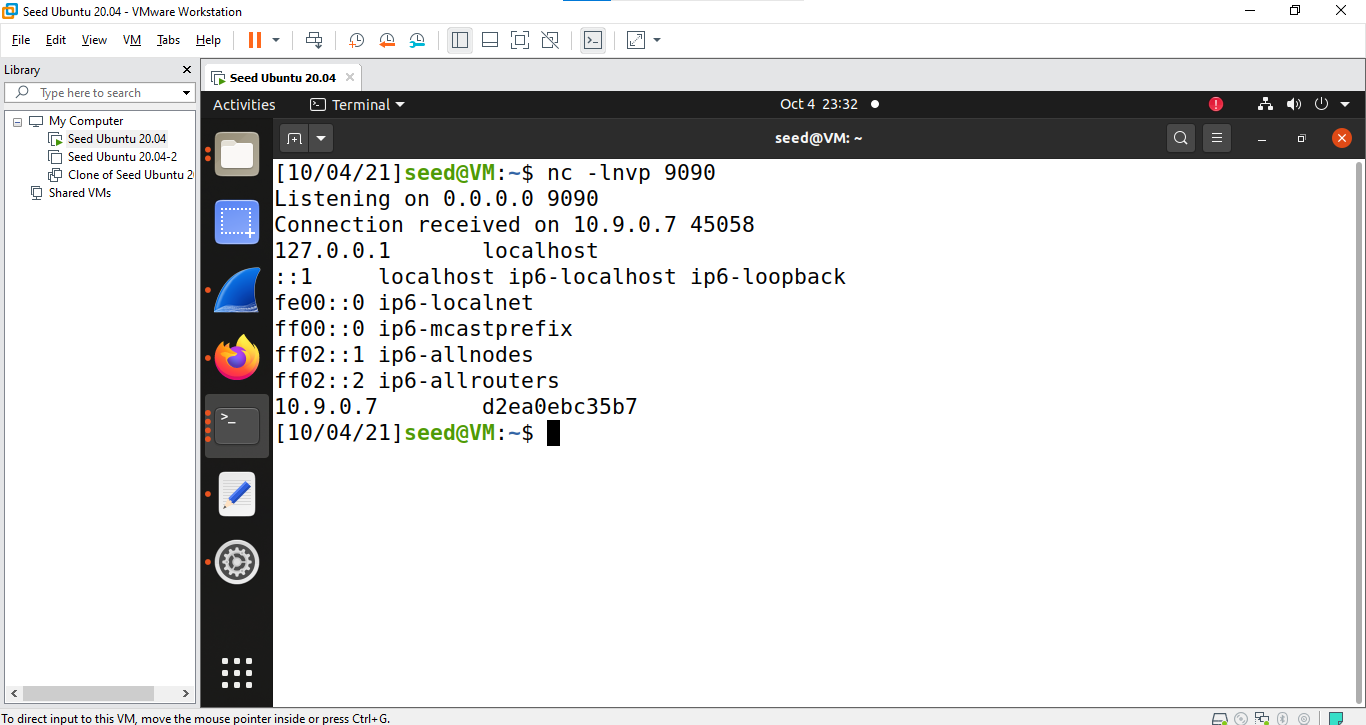


Telnet connection between user 1 and user 2



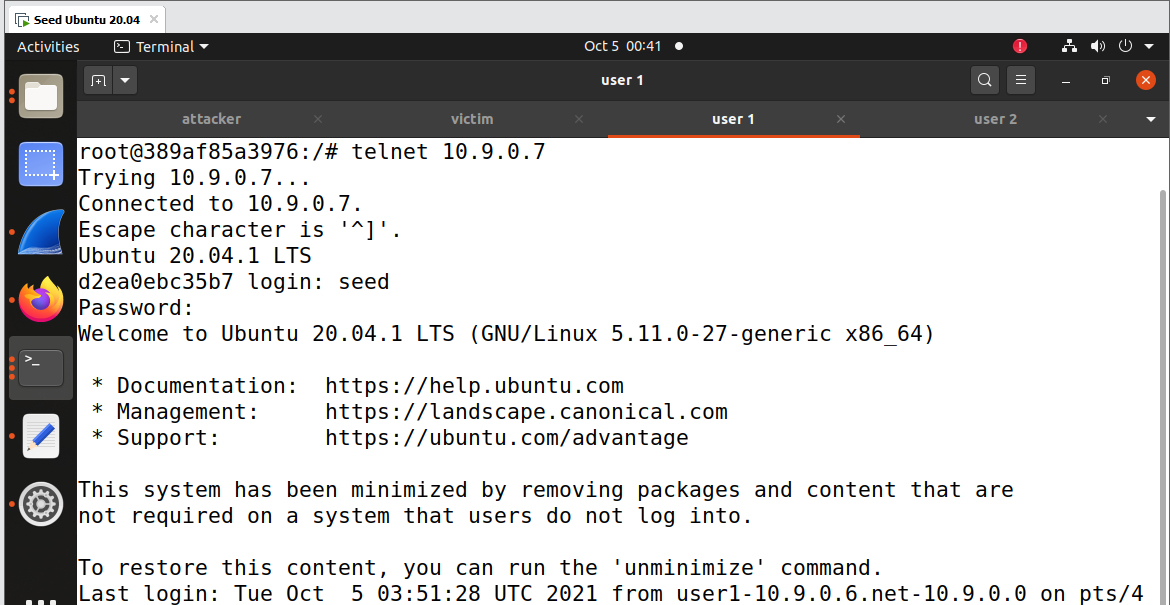
Running the code



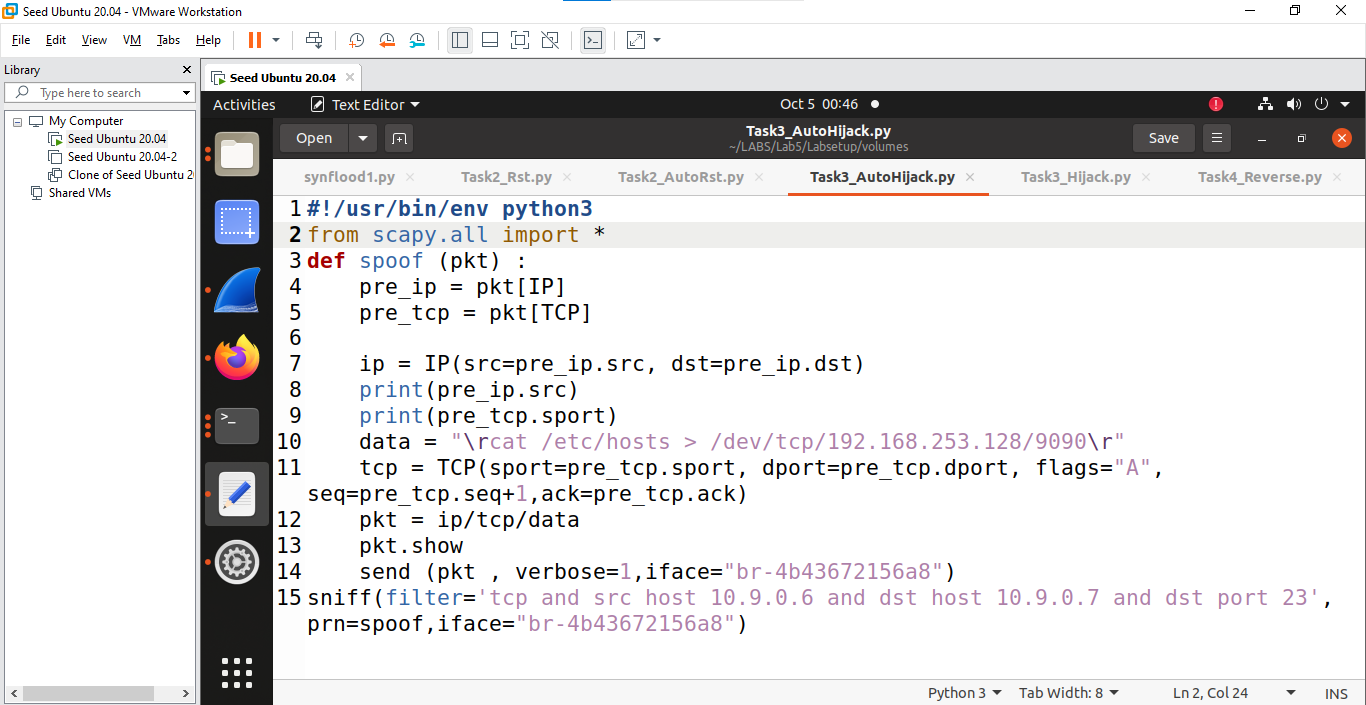
Post running the session hijack code out display

# Creating auto hijack attack

Creating Telnet Connection between user 1 and user 2



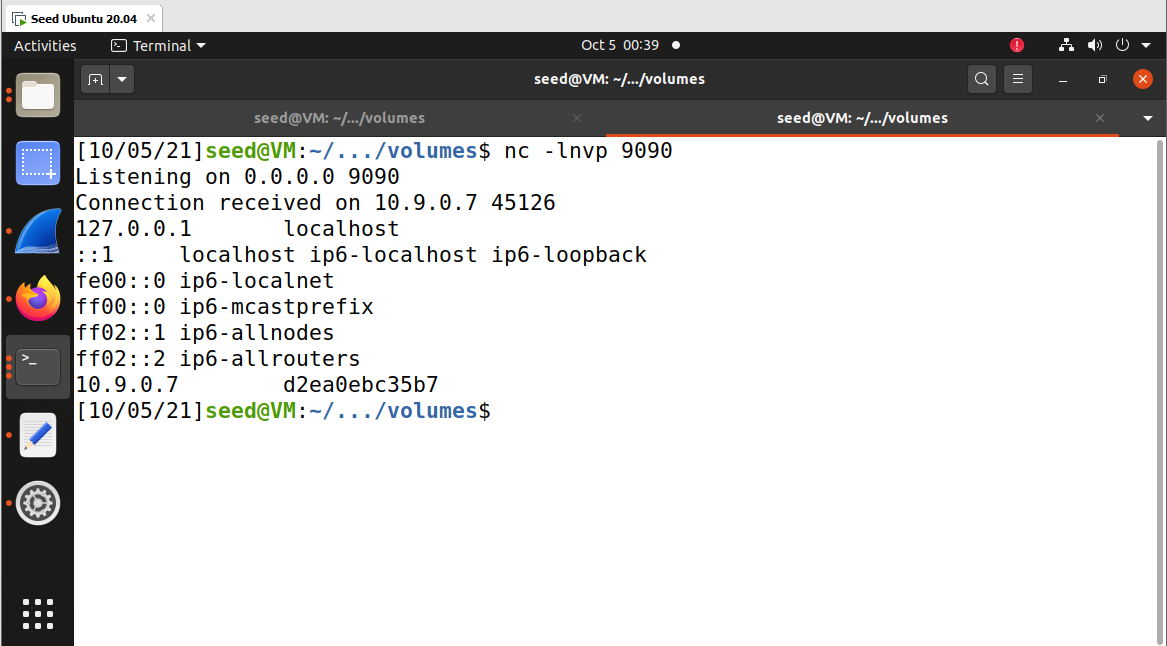
Auto Hijack code



Running the auto hijack code

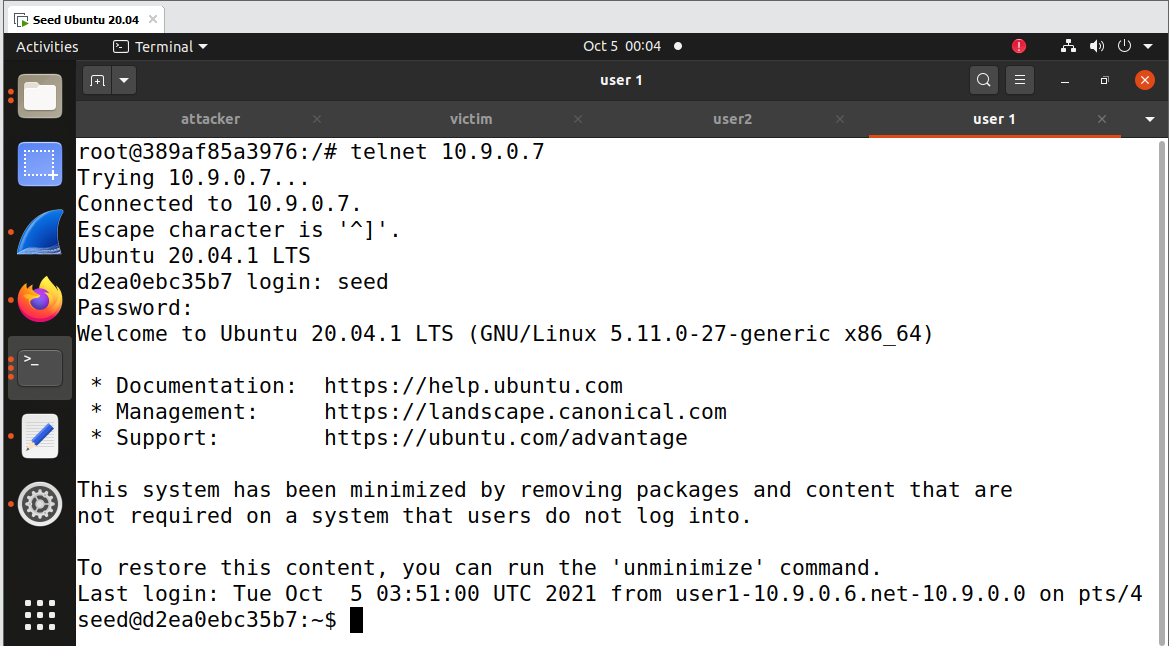


Successful Auto Hijack is done

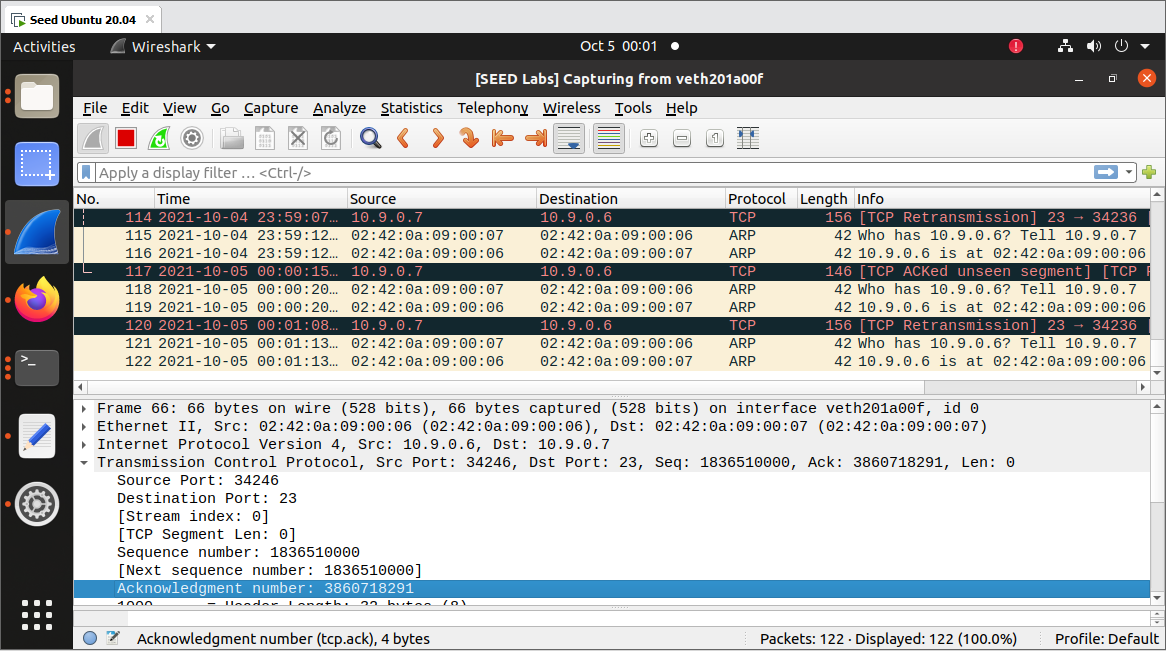


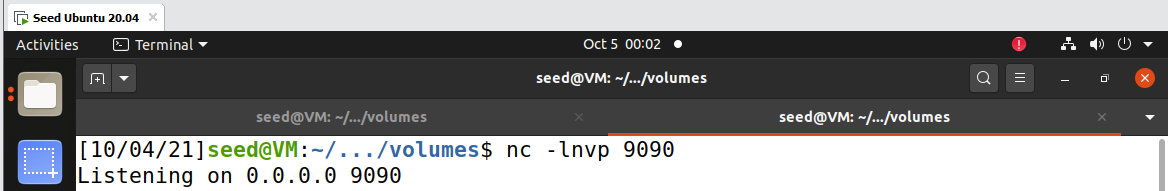
# Task 4

Creating connection between user 1 and user 2

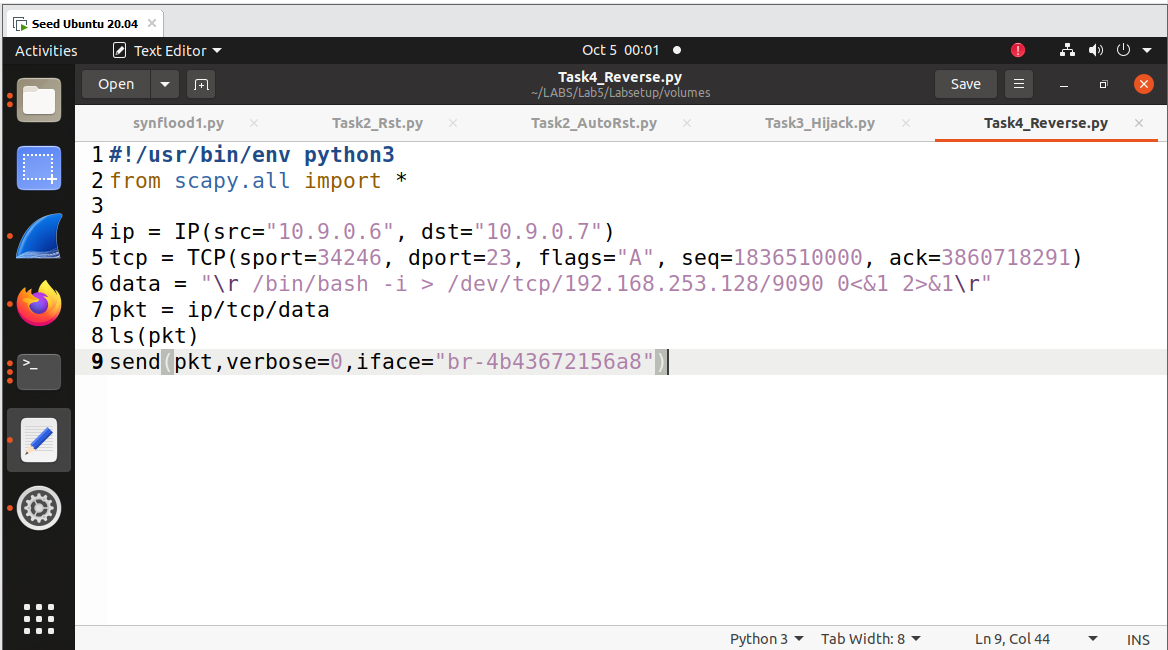


Wireshark output while telnet 10.9.0.7 from 10.9.0.6 for seq number and acknowledgement number

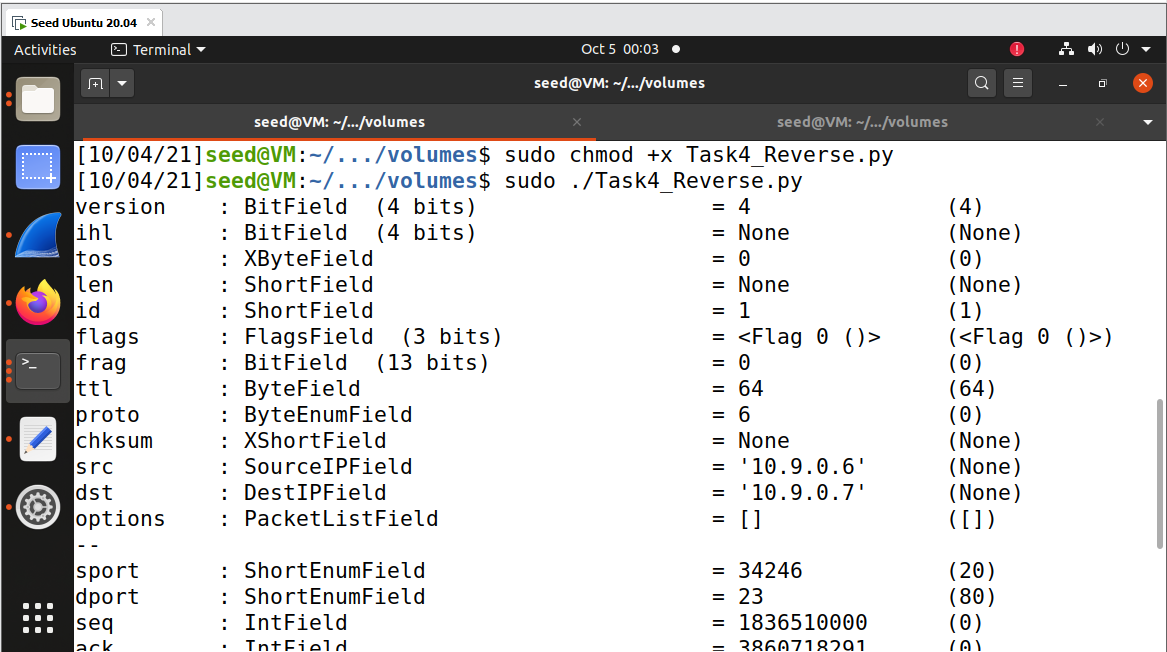


Listening on port 9090

Code for reverse shell



Running the code



Successfully reverse shell has been done 