Advanced Computer Networking and Security - 5800

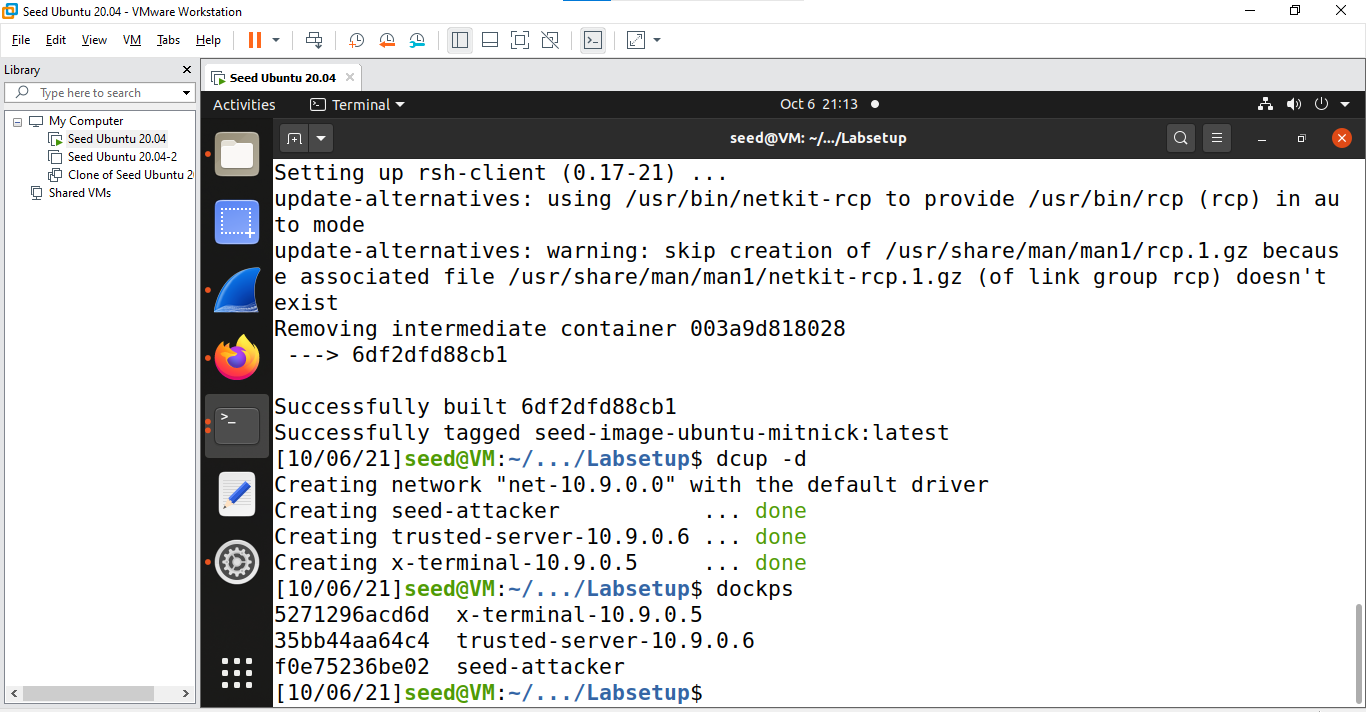
Assignment -6

MITNICK ATTACK

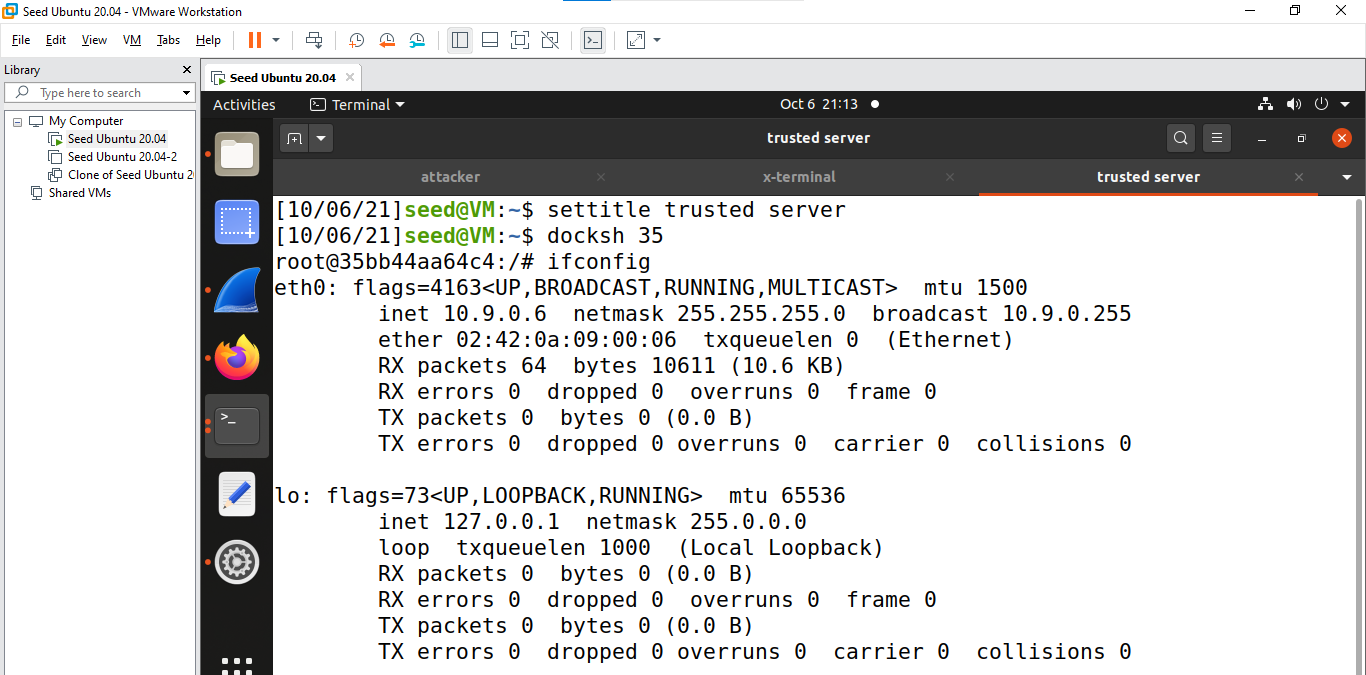
Name:Jonnada Sai Rohit

ID : 700723743

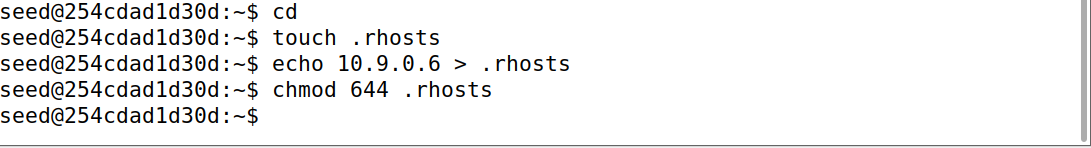
Intiating the docker and its container

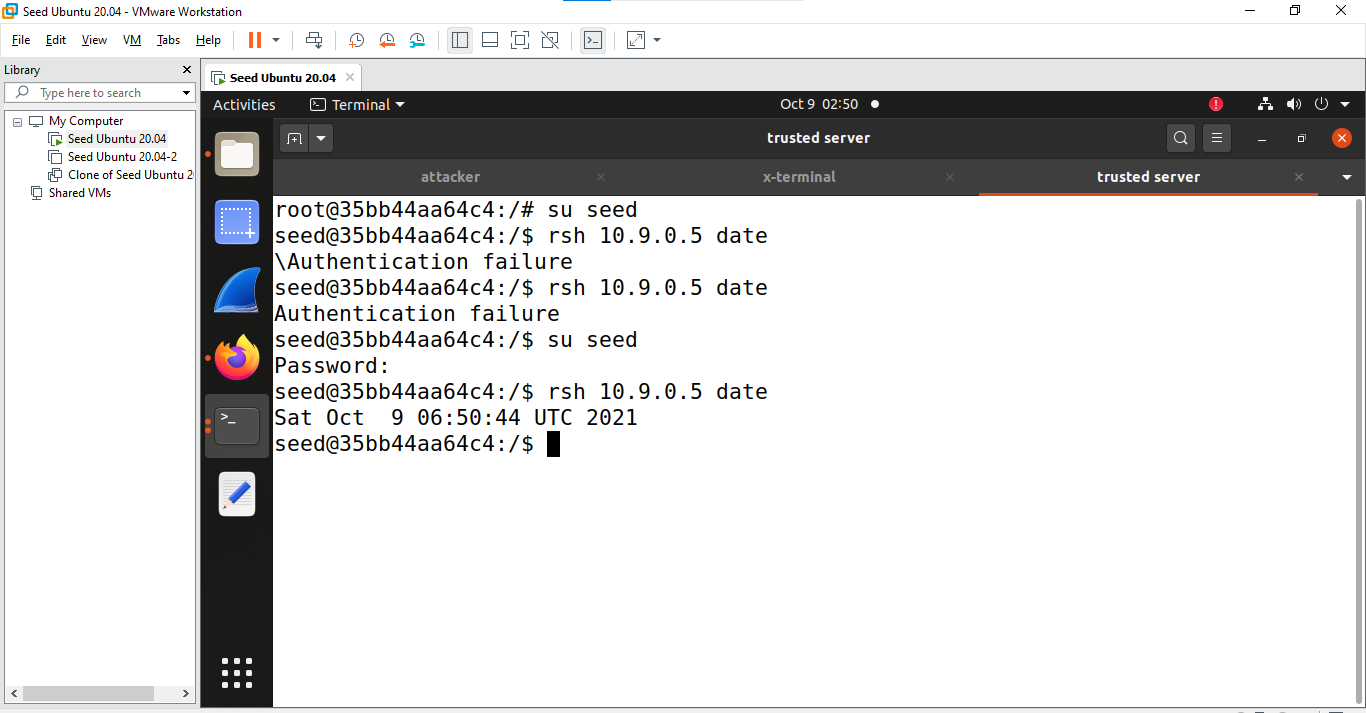


Checking the trusted server ip address and mac address



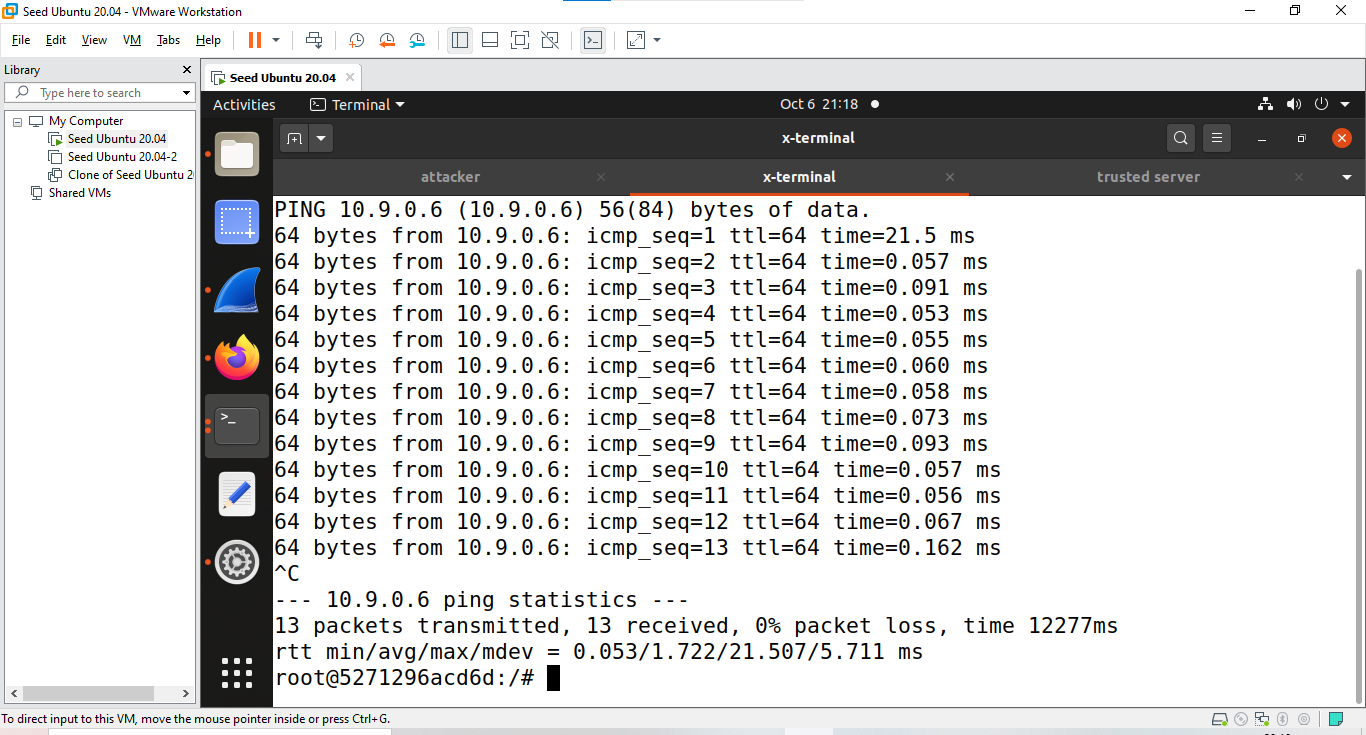
Switch to account to seed



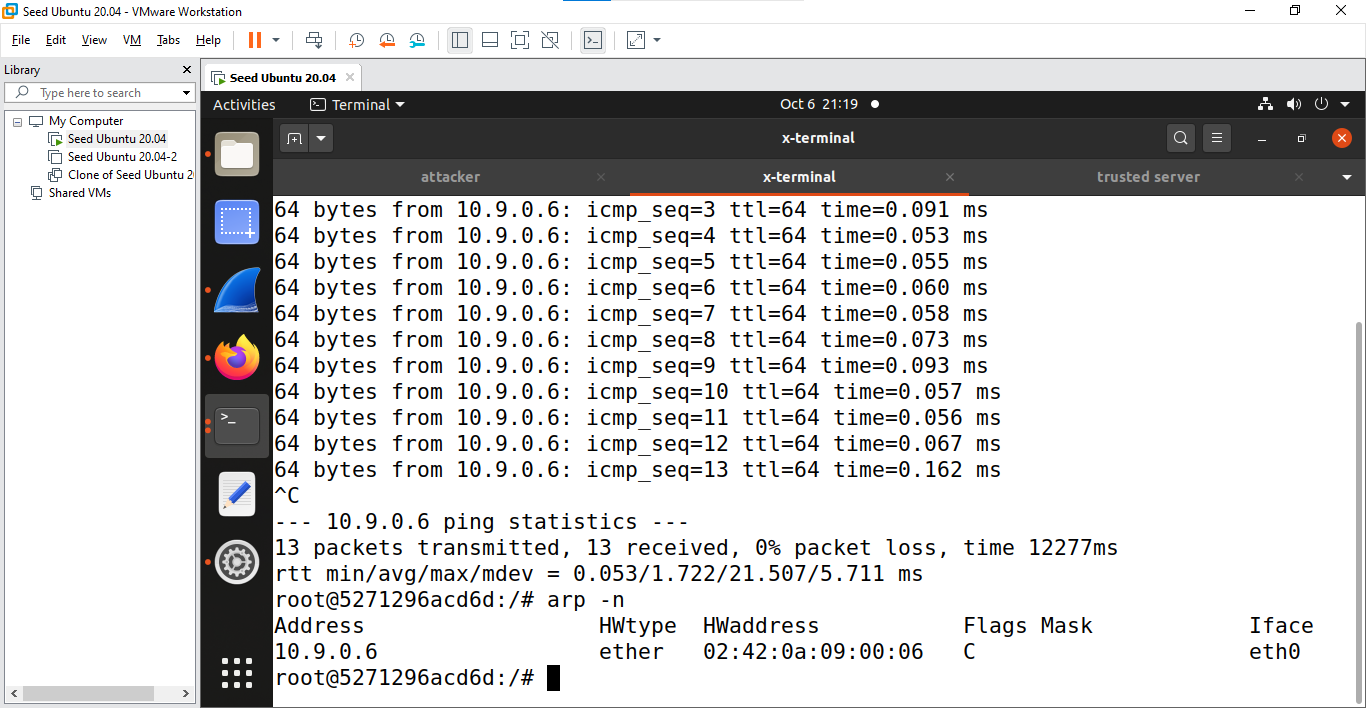
We change the .rhosts file so that the Trusted Server can login without requiring to enter a password:

## TASK -1

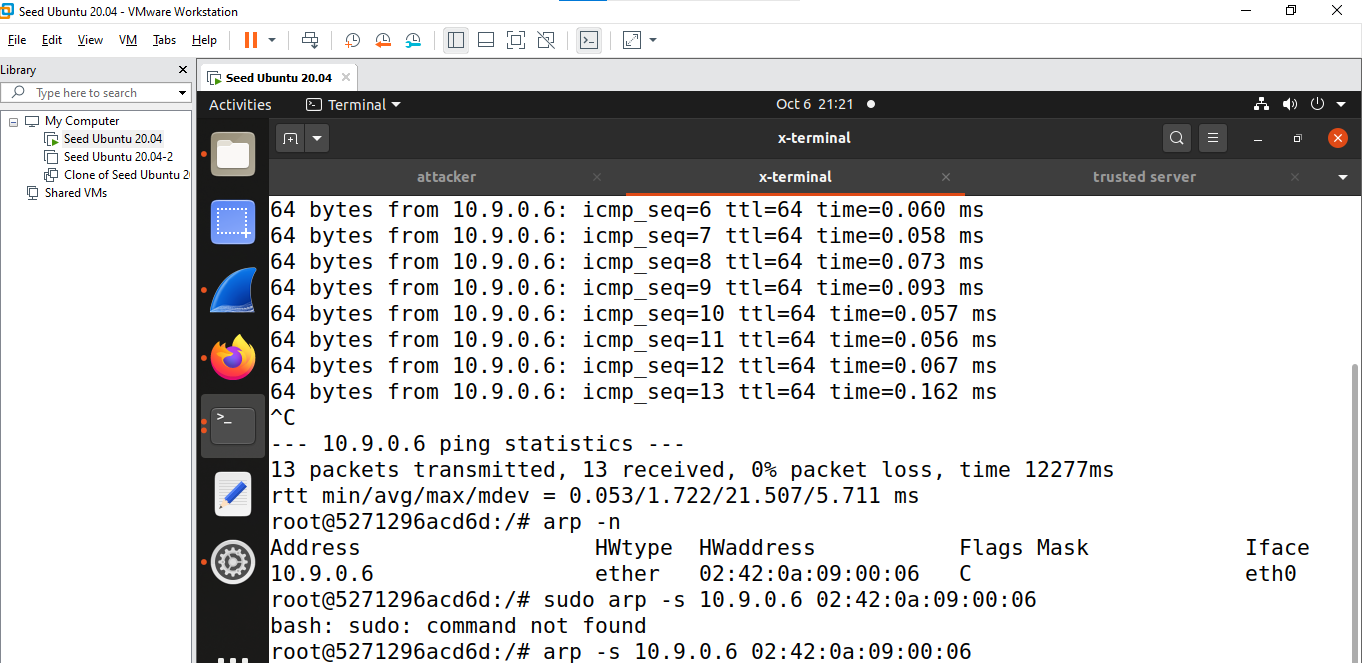
Ping the server ip address from X-Terminal



Running arp –n command



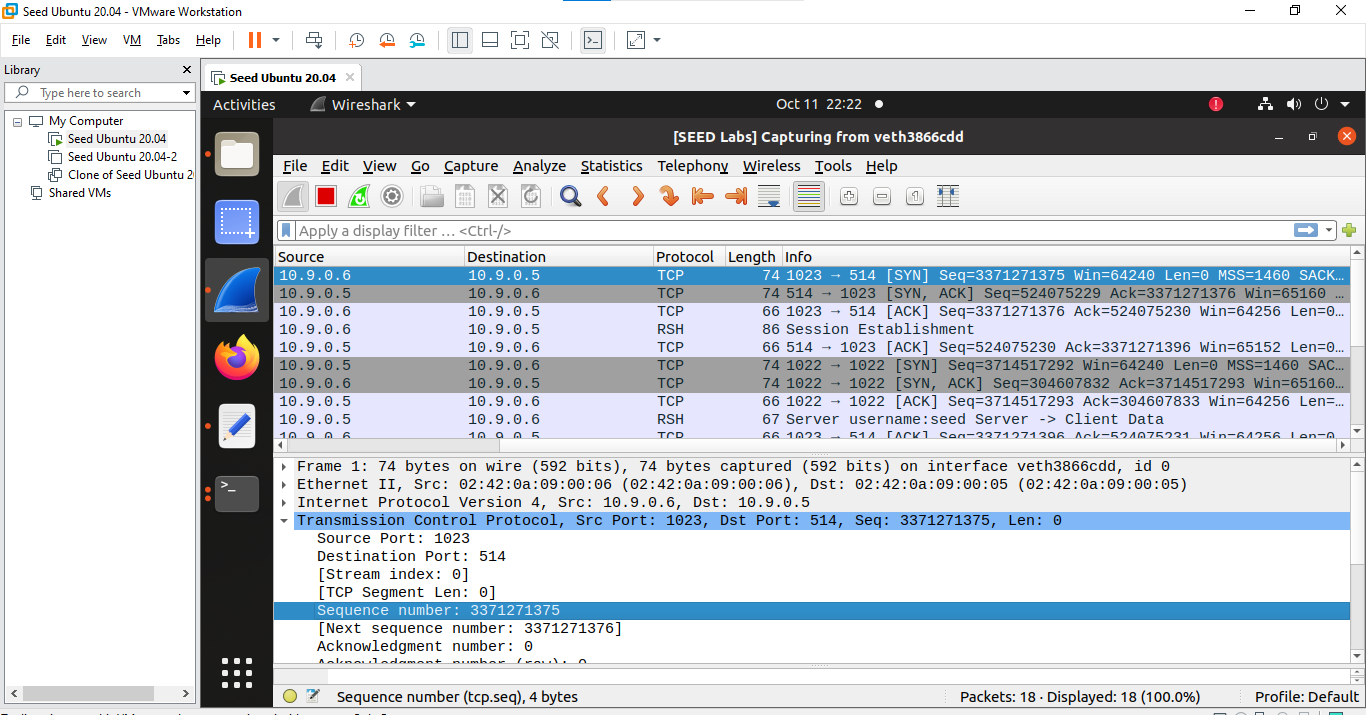
Disconnecting the trusted server



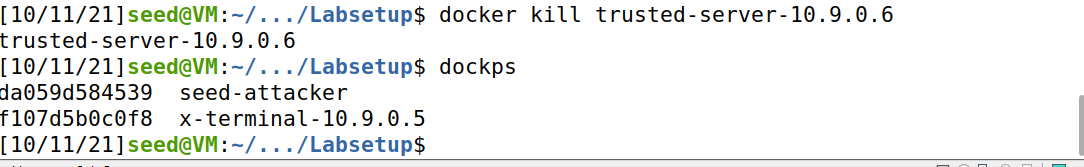
# Task 2: Spoof TCP Connections and RSH Sessions

# Step1

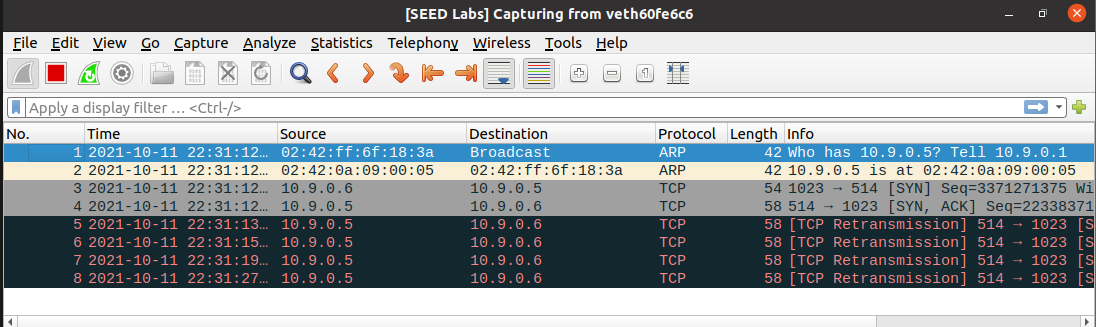
Packet trace of rsh



Turning off the X-terminal

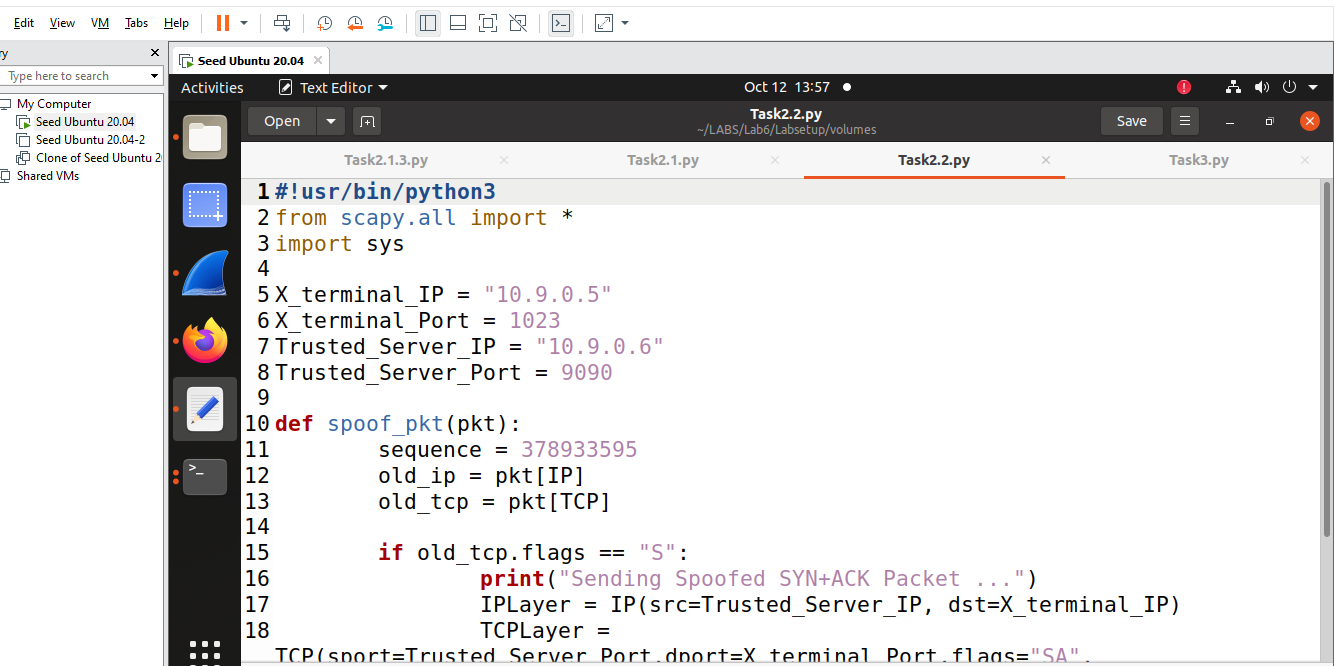


Code for send the spoof syn packet from attacker 

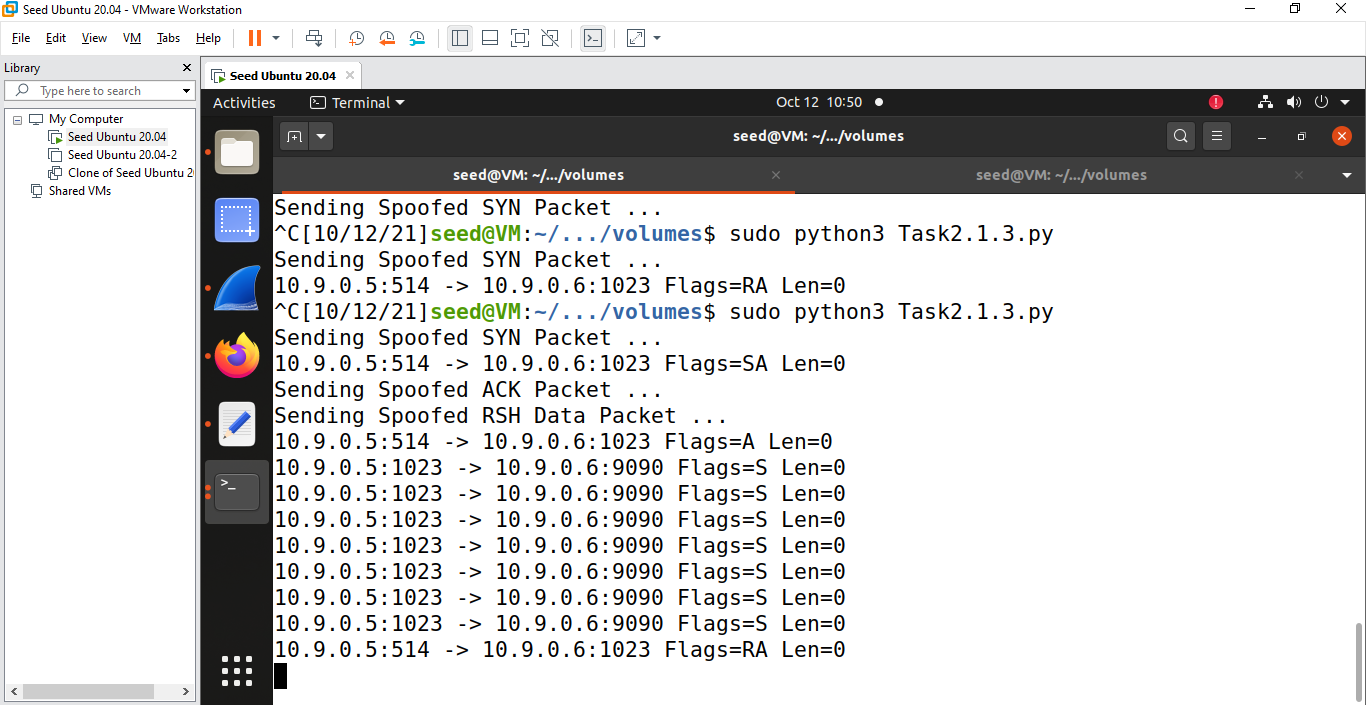
Sending the spoofed syn packet from attacker to x terminal and we got syn+ack packet from x terminal

# Step2 :

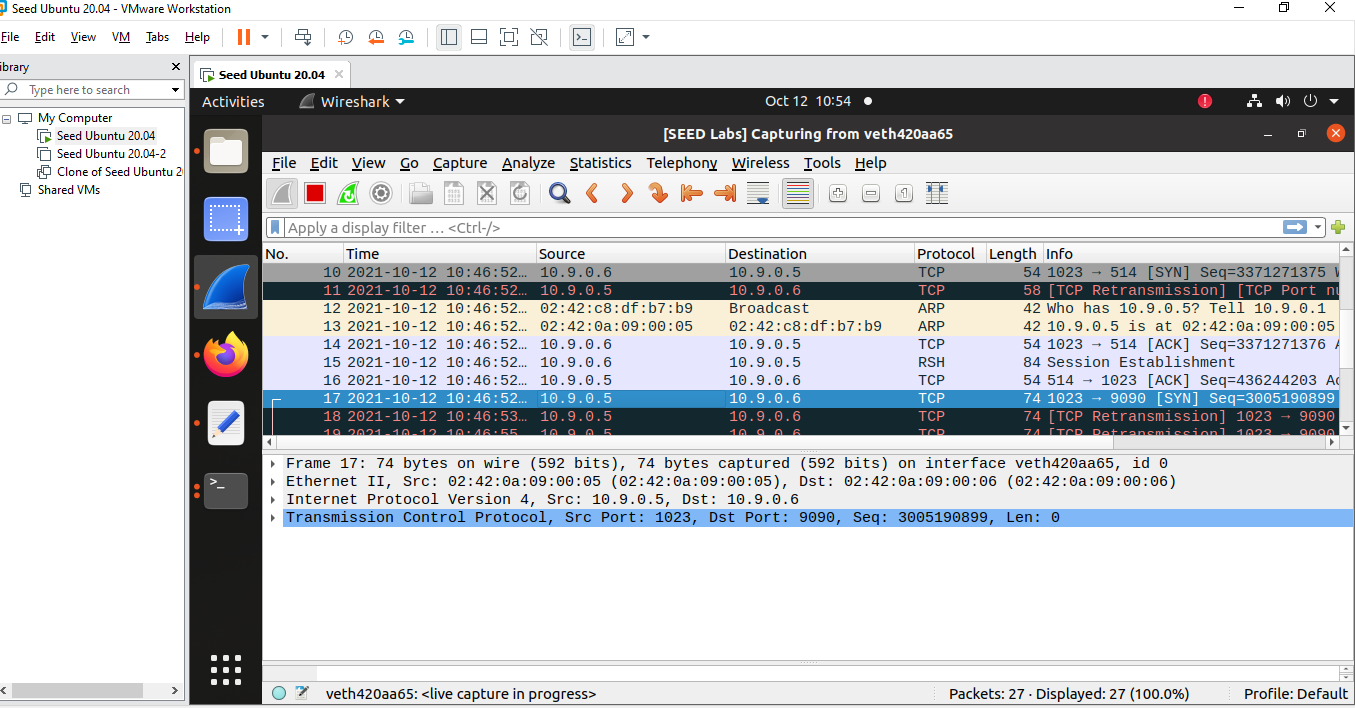
Respond to Syn+Ack packet



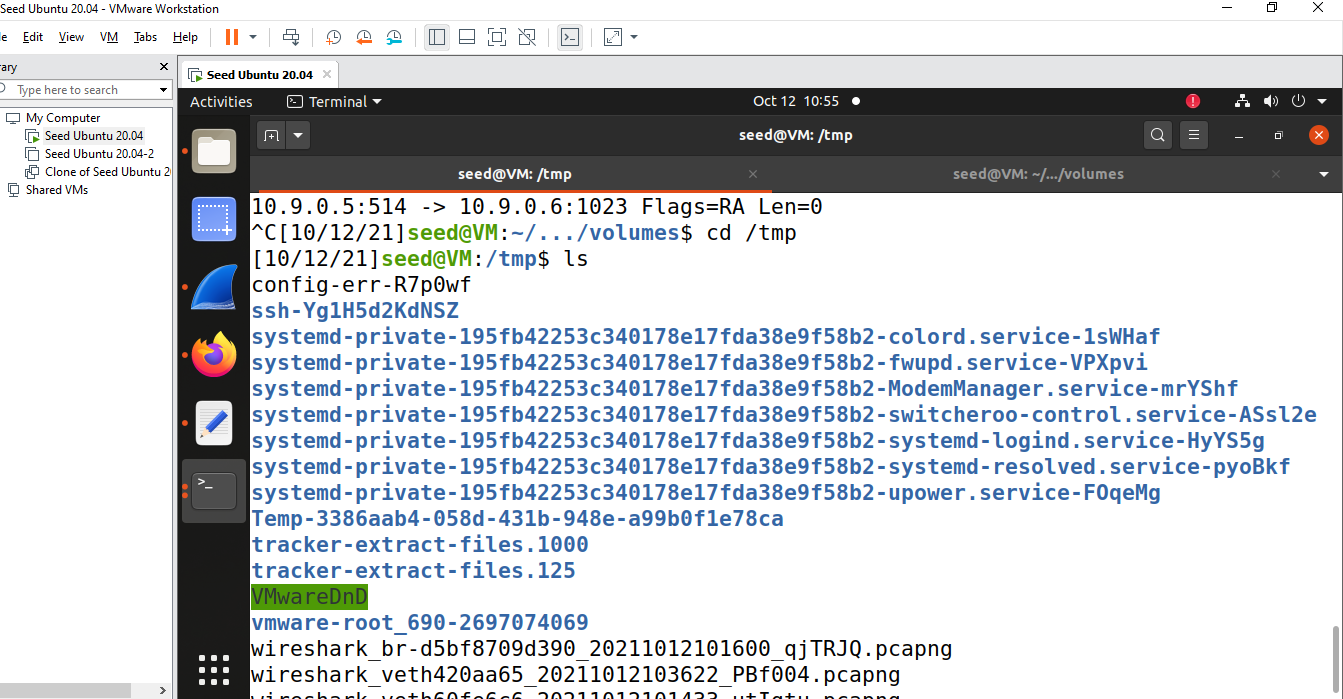
Step 3



Establishing the rsh connection wire shark



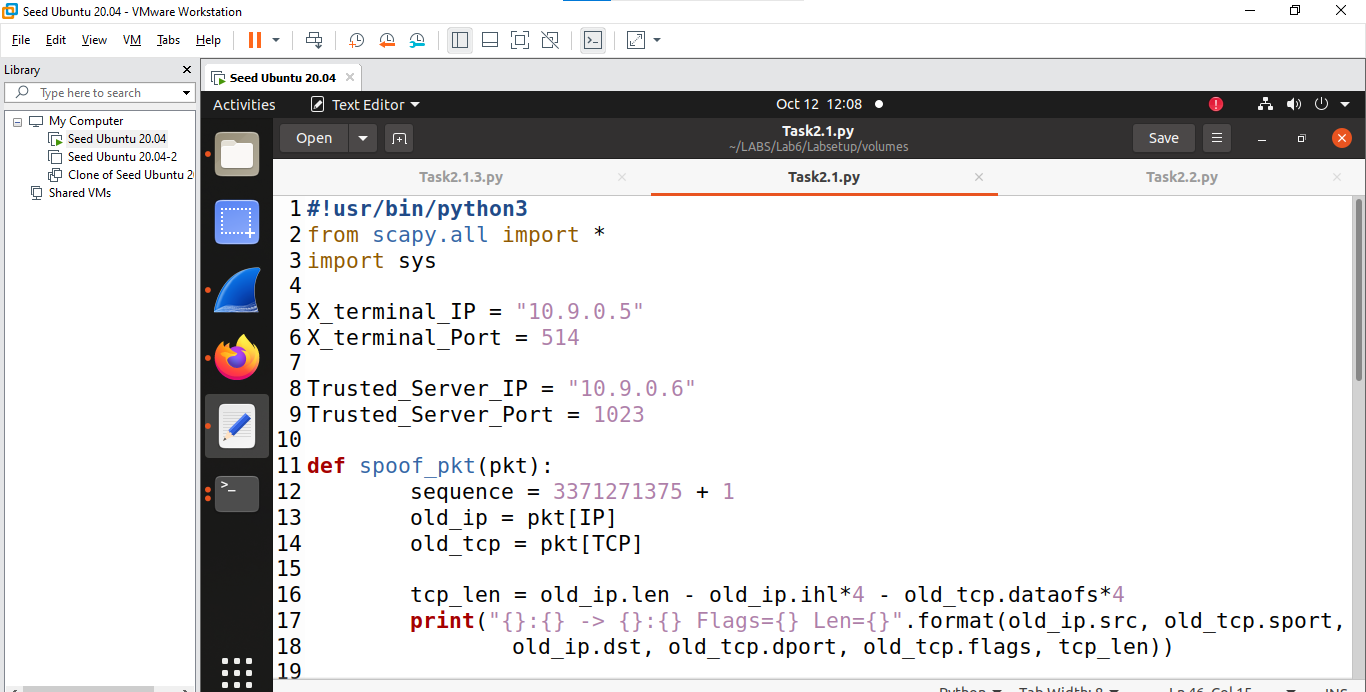
Checking whether touch command is executed or not



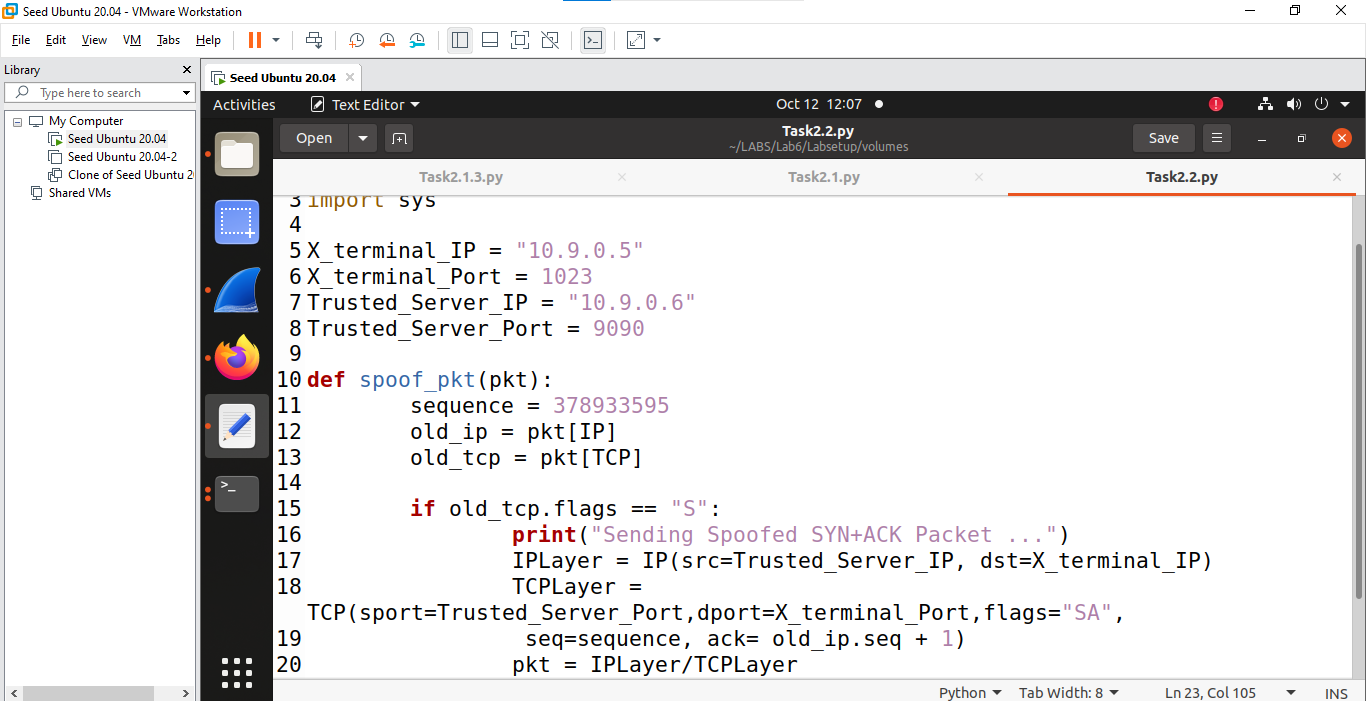
It is not established as rsh connection is completely established

# Task 2.2

Code for task 2.1

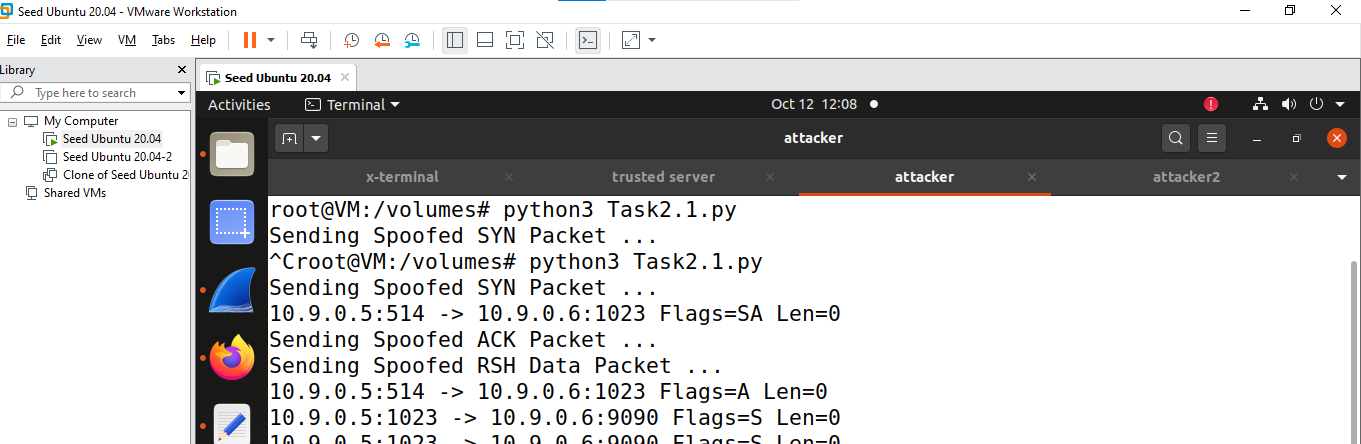


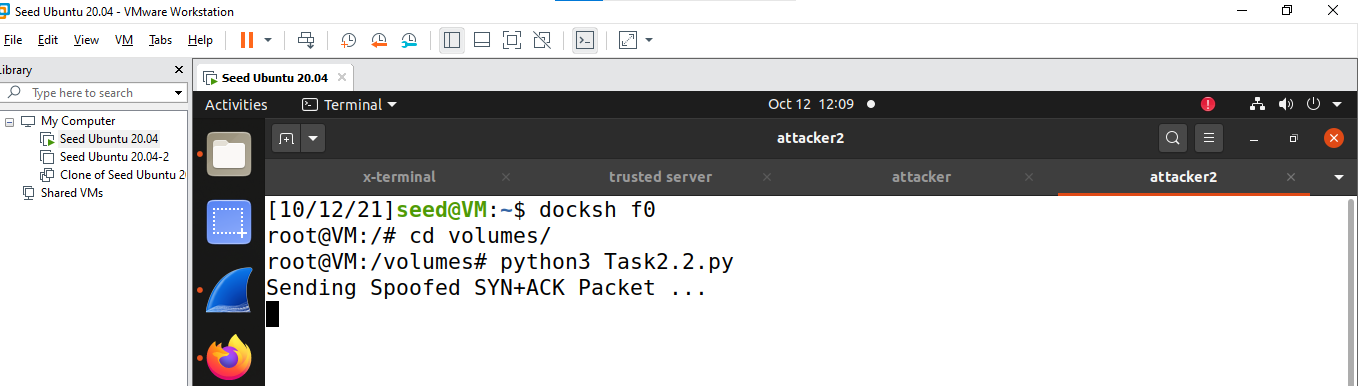
Code for task 2.2



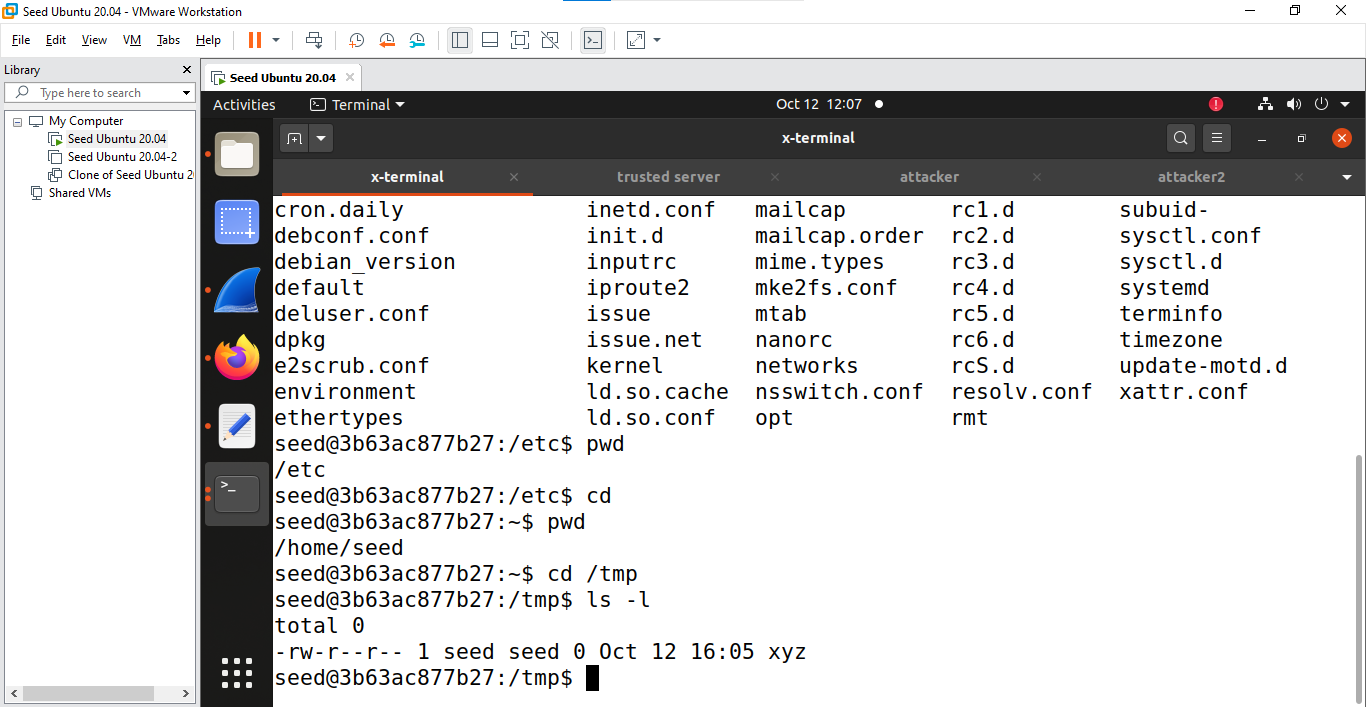
Running the code

First Execute Task 2.1 and later Run Task 2.2



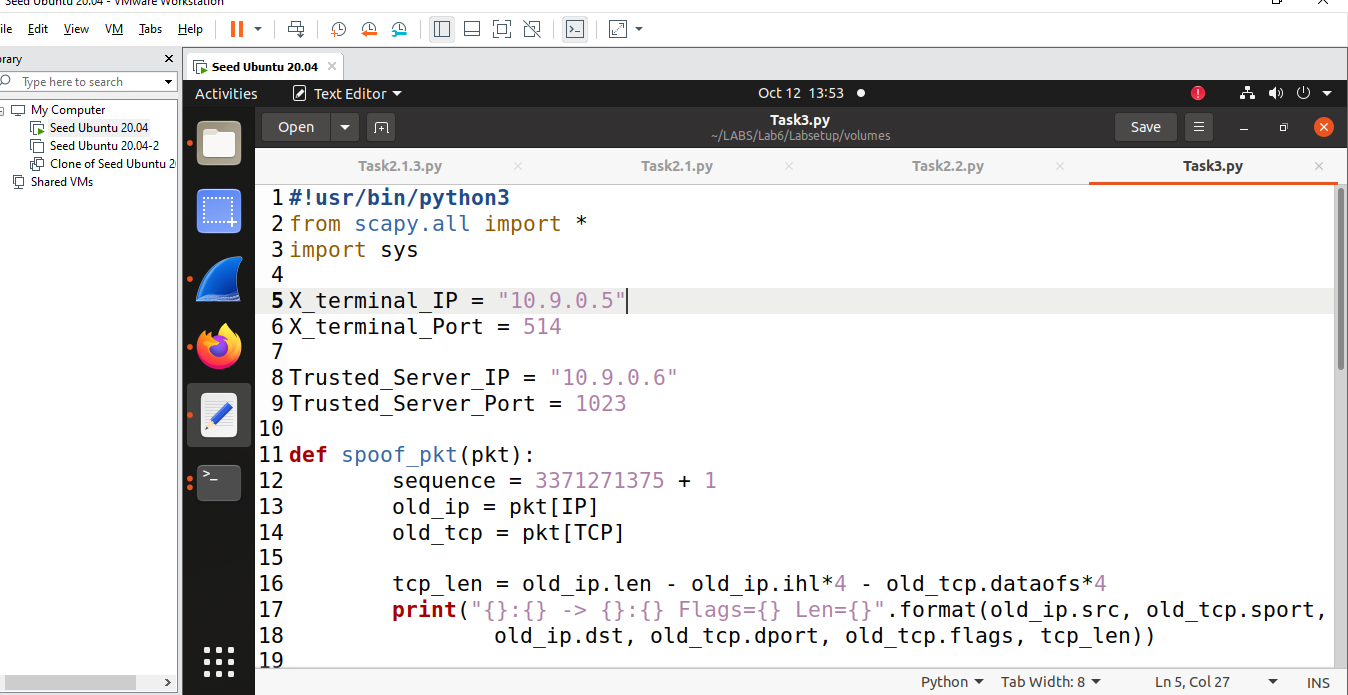


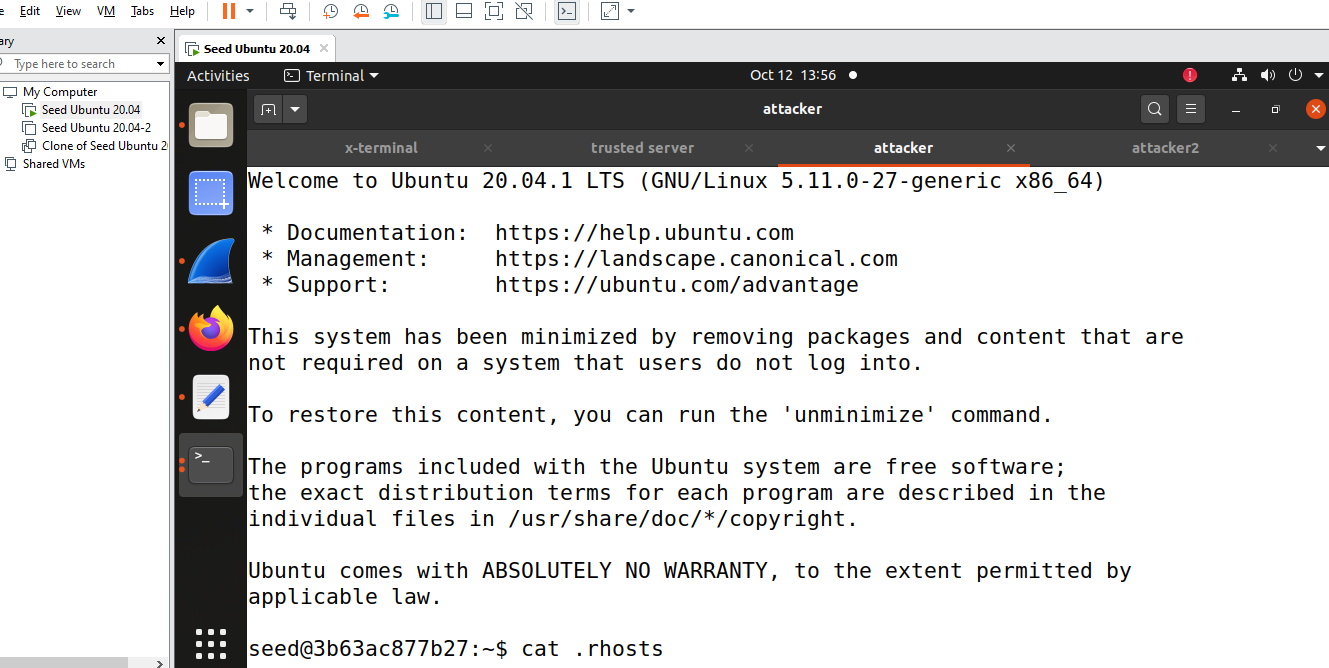
Checking wheter xyz file in xterminal



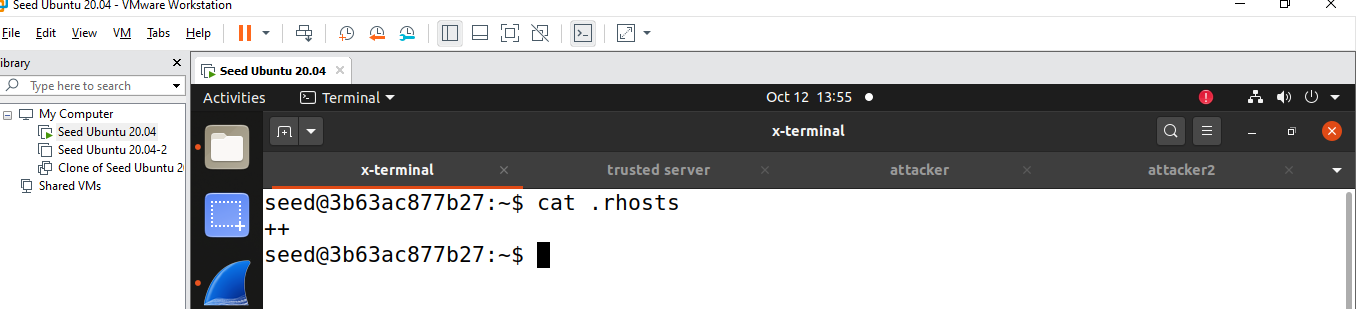
# Task 3 Backdoor

Code for Backdoor creation and login into xterminal without password



Logging into x terminal without password

Checking the ++ file is created or not in x terminal



Mitnick attack is successful