**NAME :** Mansi Dwivedi

**BRANCH :** IT

**UID :** 2019140016

**BATCH :** A

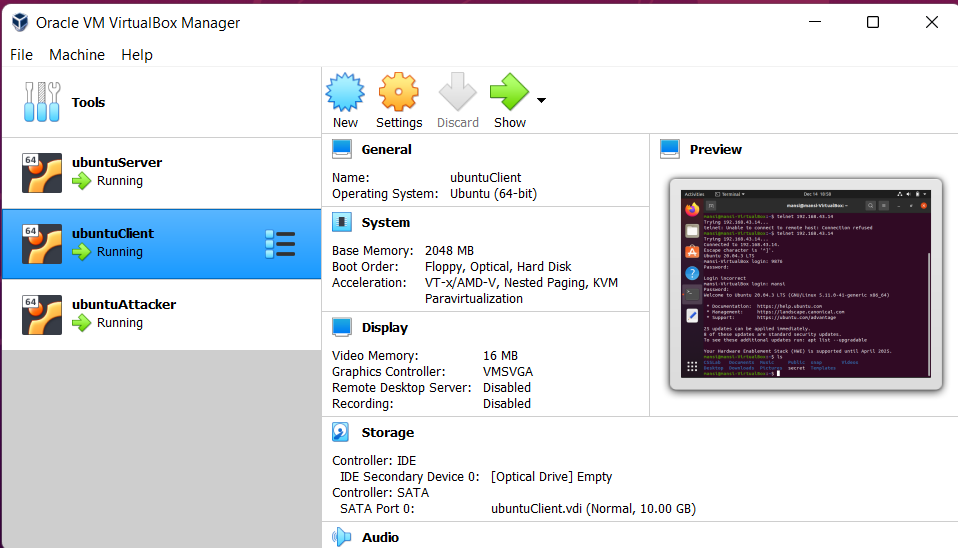
**COURSE :** CSS LAB

**EXPERIMENT :** 8

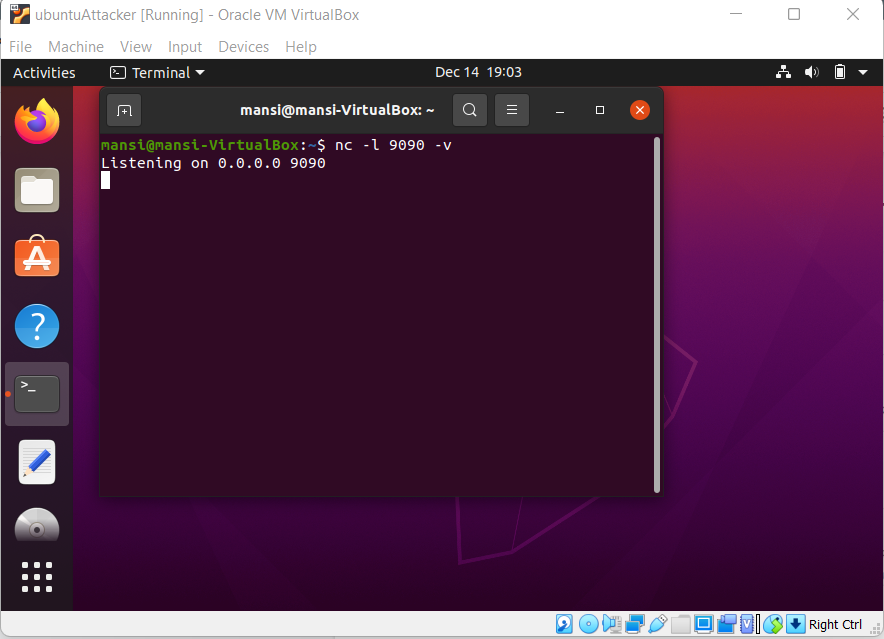
**AIM :** To create and understand TCP Session Hijacking

**PROCEDURE:**

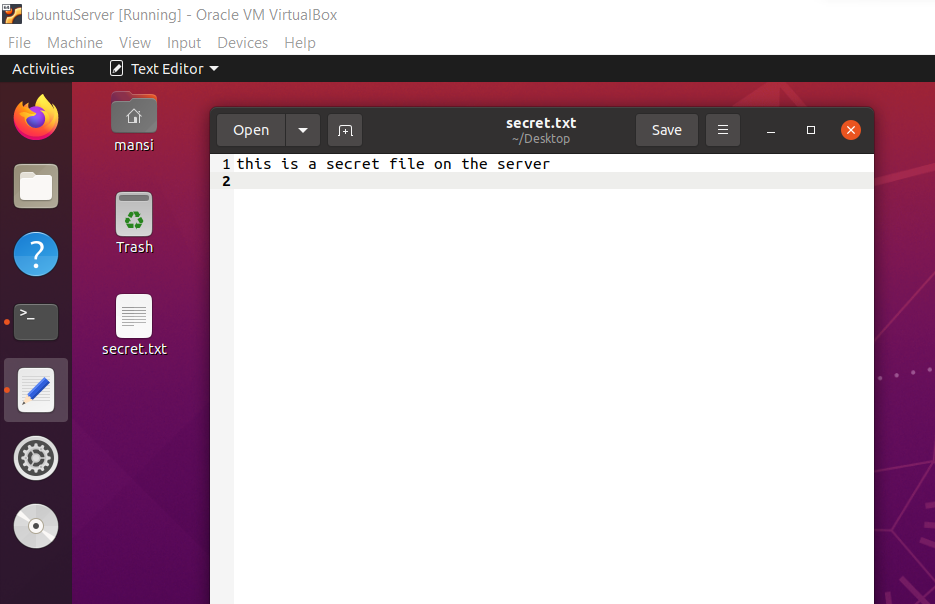
**STEP 1:** I created three ubuntu virtual machines one for the server (192.168.43.14), the client (192.168.43.13), and the attacker (192.168.43.111)



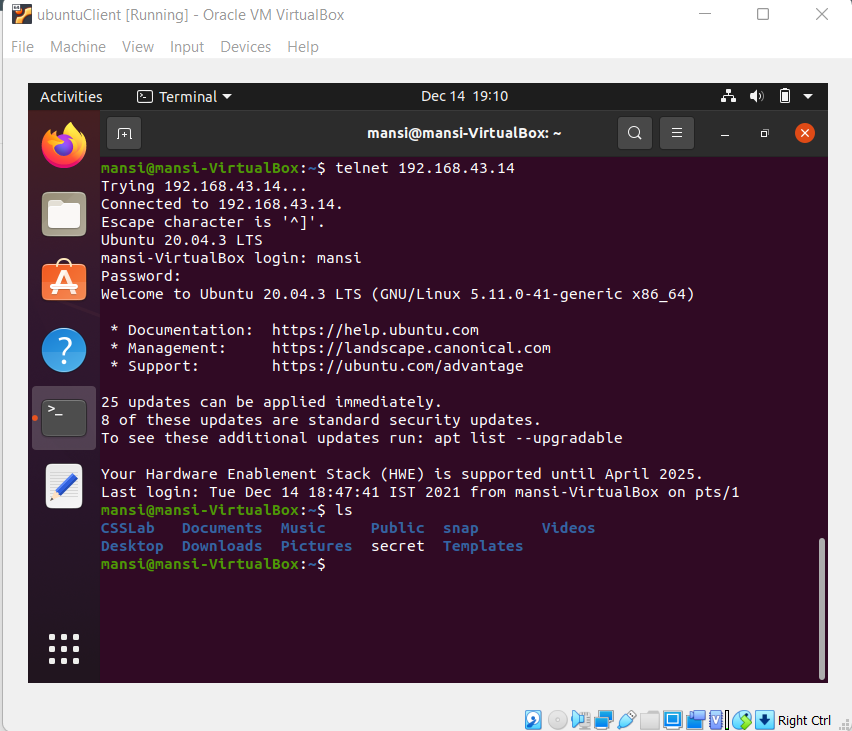
**STEP 2:** Installed Wireshark on the attacker machine and completed all the prerequisites. Next, I started listening from the attacker machine using the Netcat command where I specified the port to be 9090 and -v that indicating that more verbose information is required.



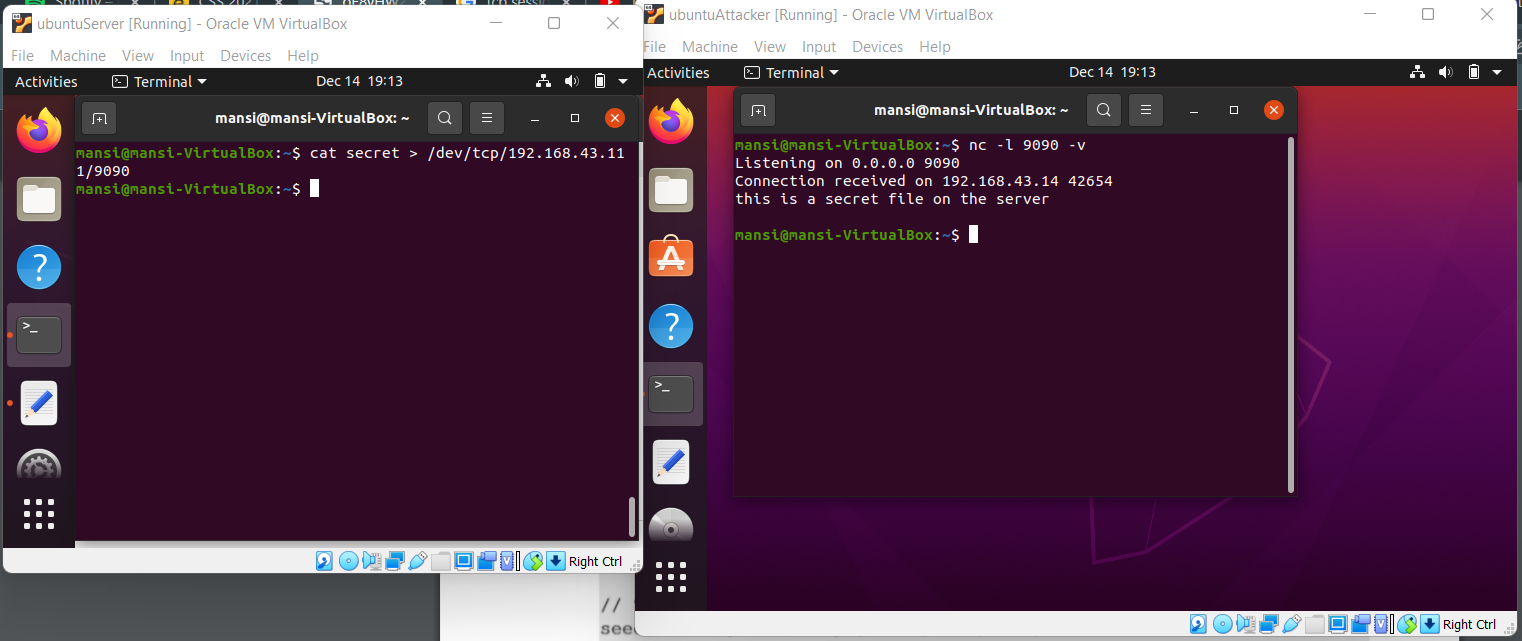
**STEP 3:** Now I created a secret.txt file on the server machine and then initiated the telnet connection from the client machine to the server machine. But initially while running the telnet command from the client to server the connection was refused thus unable to connect, the reason being that the firewall setting of the server machine had disabled the connection so I had to add and edit some lines in the /edit/resolv.conf file and then the connection establishment worked just fine.

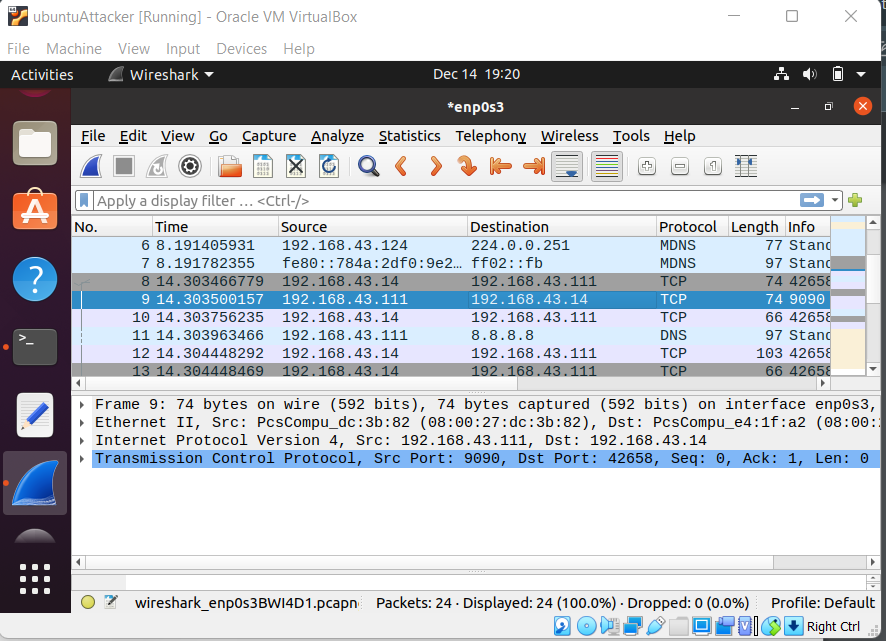


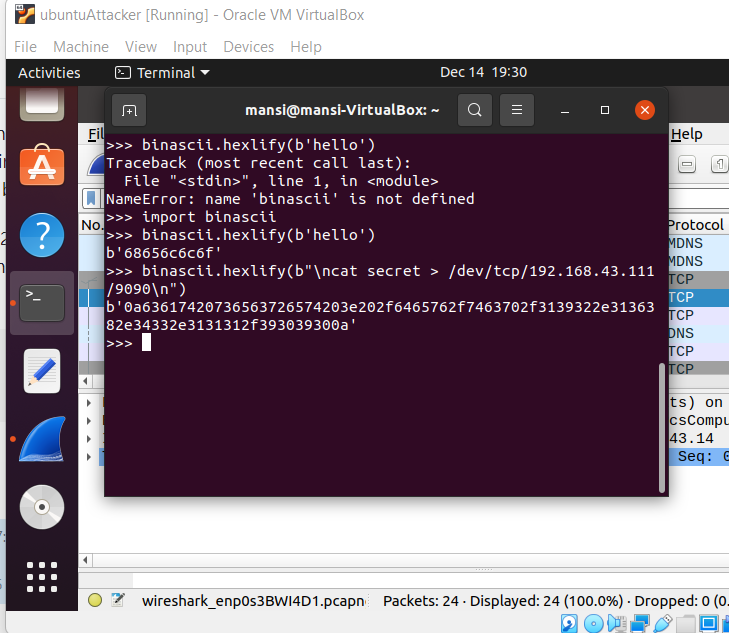
Here I am now able to see all the files in the server machine.

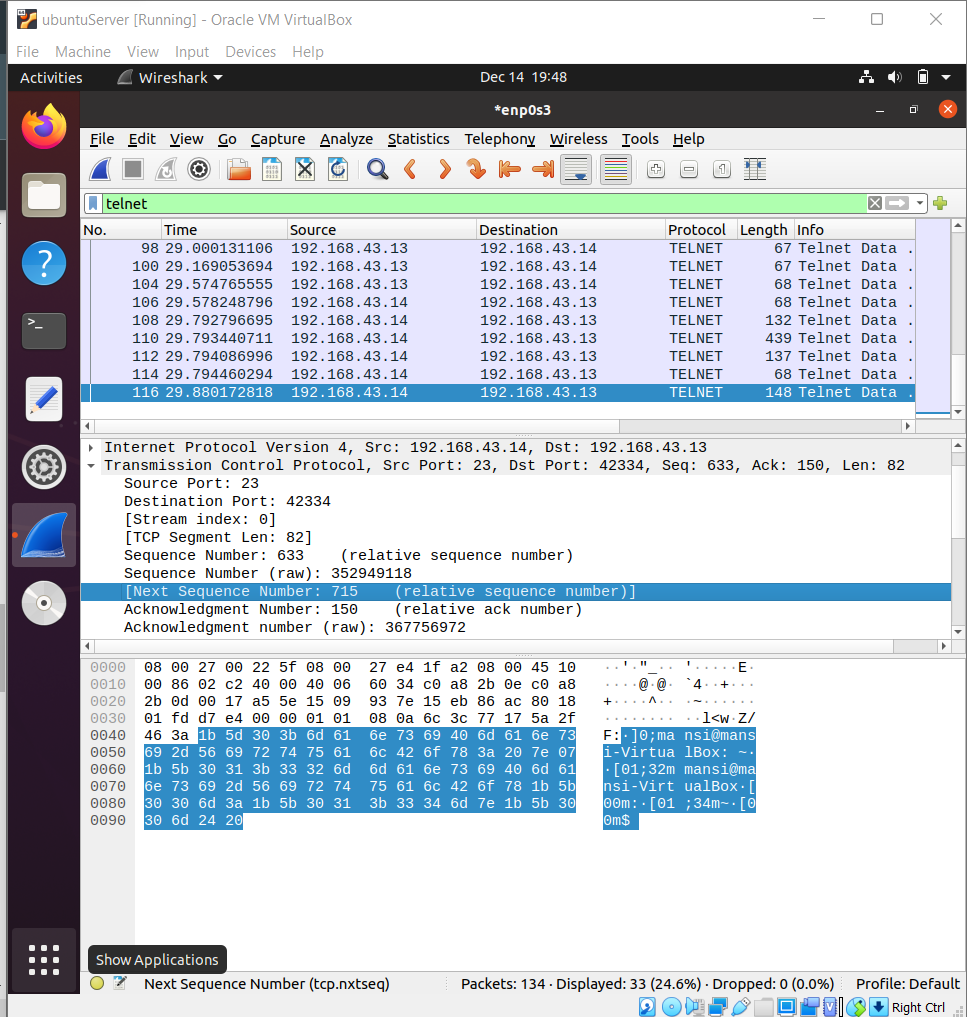


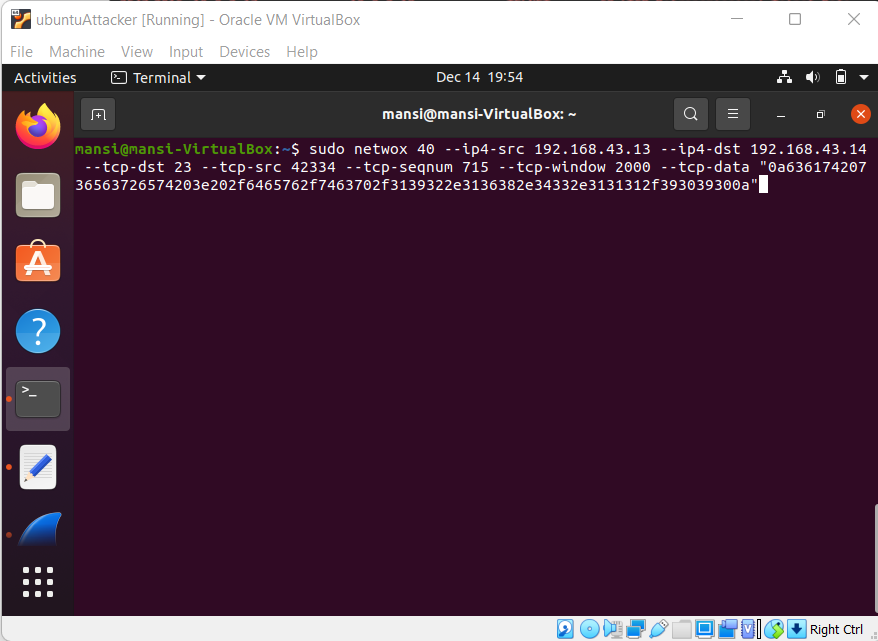
**STEP 4:** Now I ran the cat secret command on the server machine and since the attacker was listening on 9090 the content of the secret.txt was displayed in the terminal of the attacker machine.

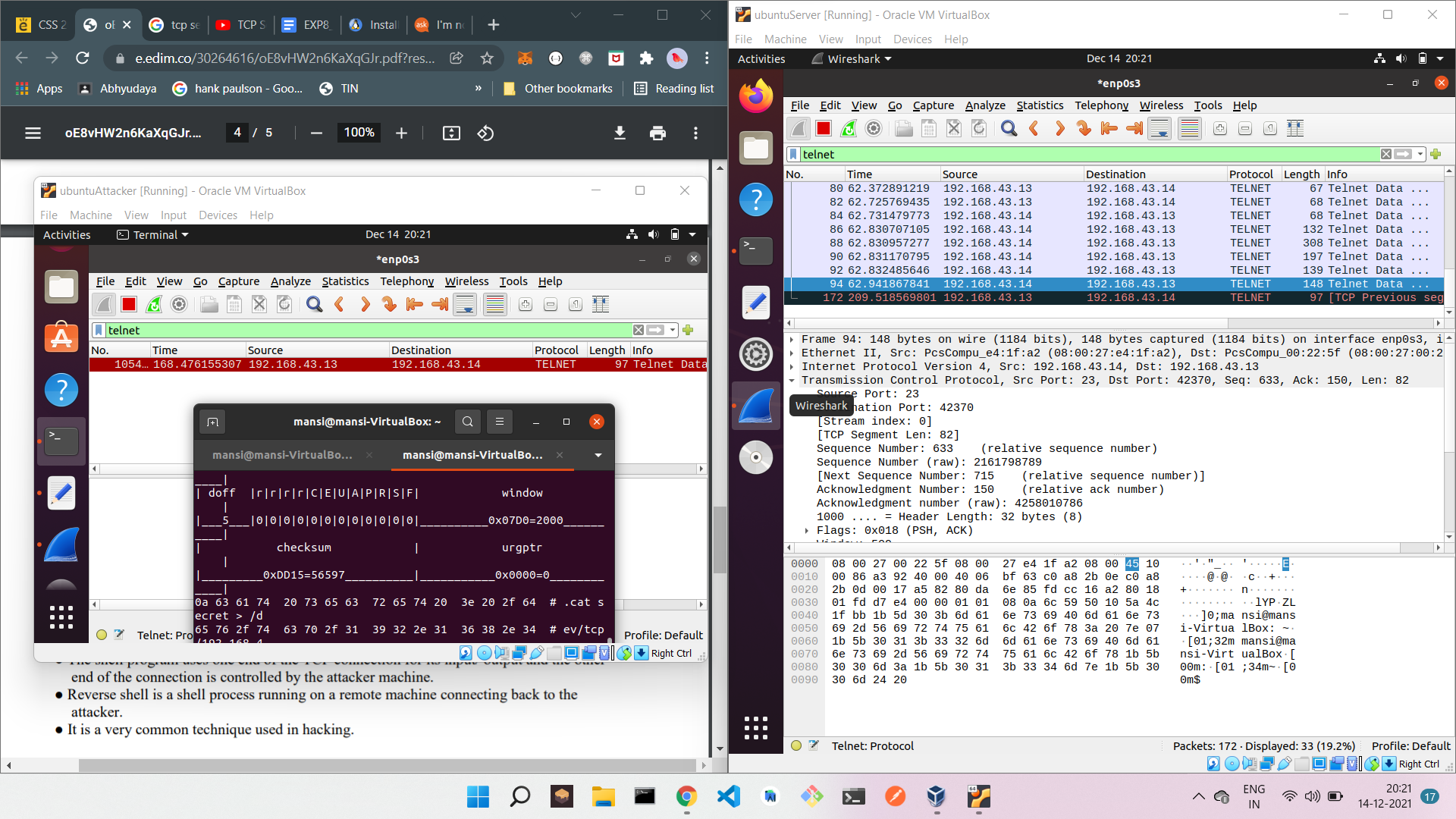


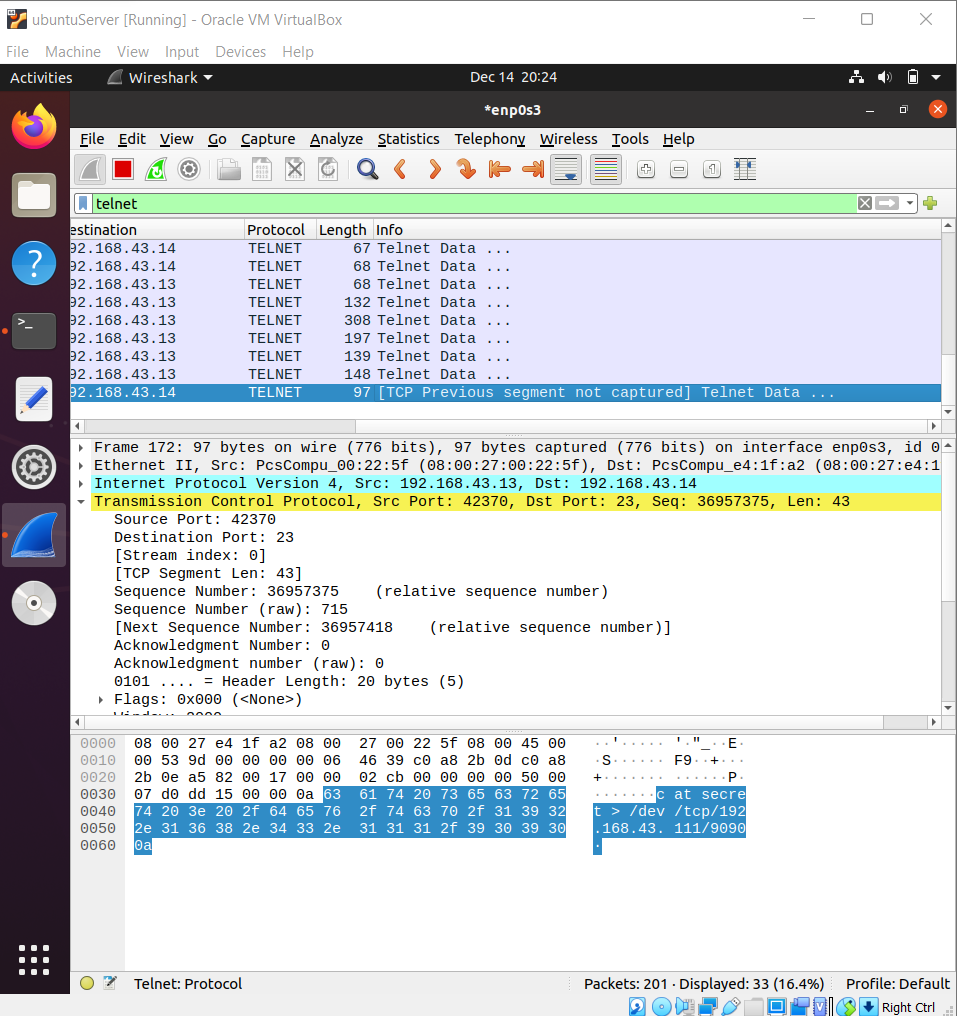


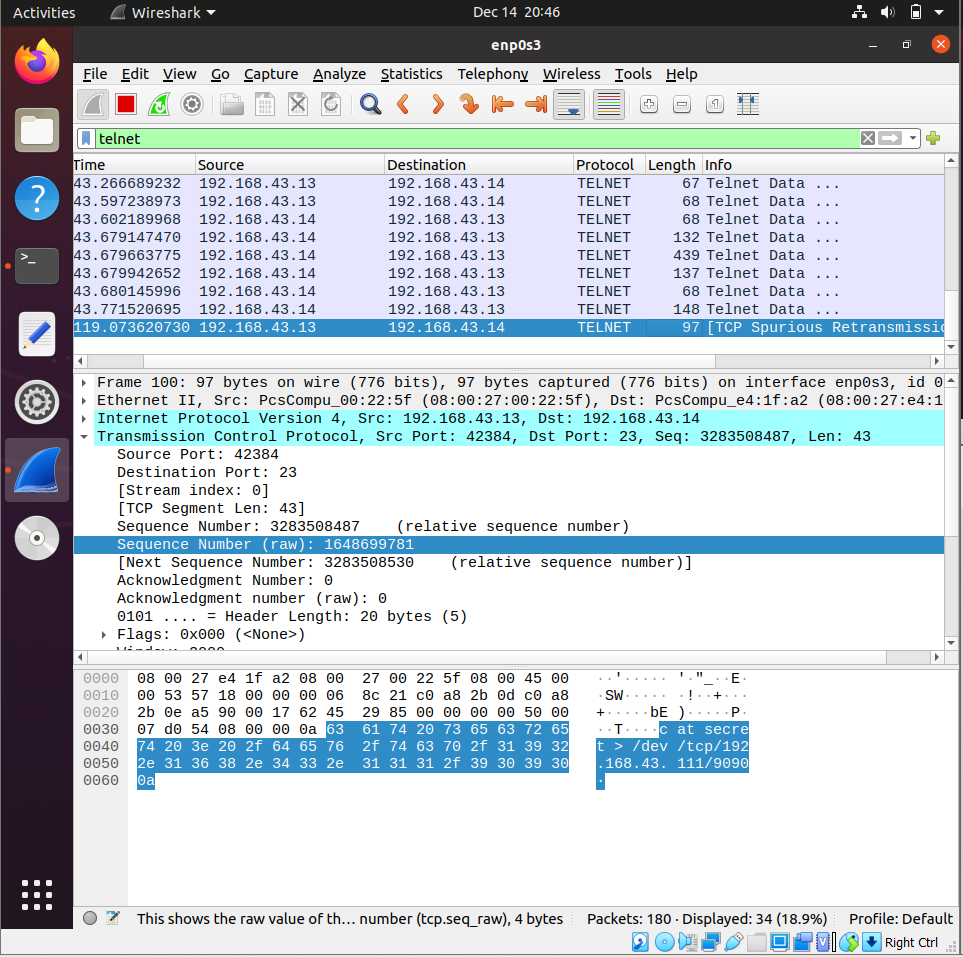












**CONCLUSION :**

I saw that after the attacker was able to send a tcp packet with the earlier recorded sequence number and post numbers the wireshark did capture the packet but nowhere was the attacker machine’s IP address mentioned that is the attacker was successful in his/her attack. The wireshark application running in the server machine displayed that the tcp packet was sent from the client machine to itself which is perfectly aligned to what we expect but little did it know that the packet was initially sniffed by the attacker and sent to the server machine masquerading itself as the actual client. So the session hijacking attack if successful, the attacker can then perform any actions that the original user is authorized to do during the active session.