**COMPUTER NETWORK SECURITY**

**LAB-3**

**TCP ATTACK**

**LAB**

NAME: VISHWAS M

SRN: PES2UG20CS390

SEC: F

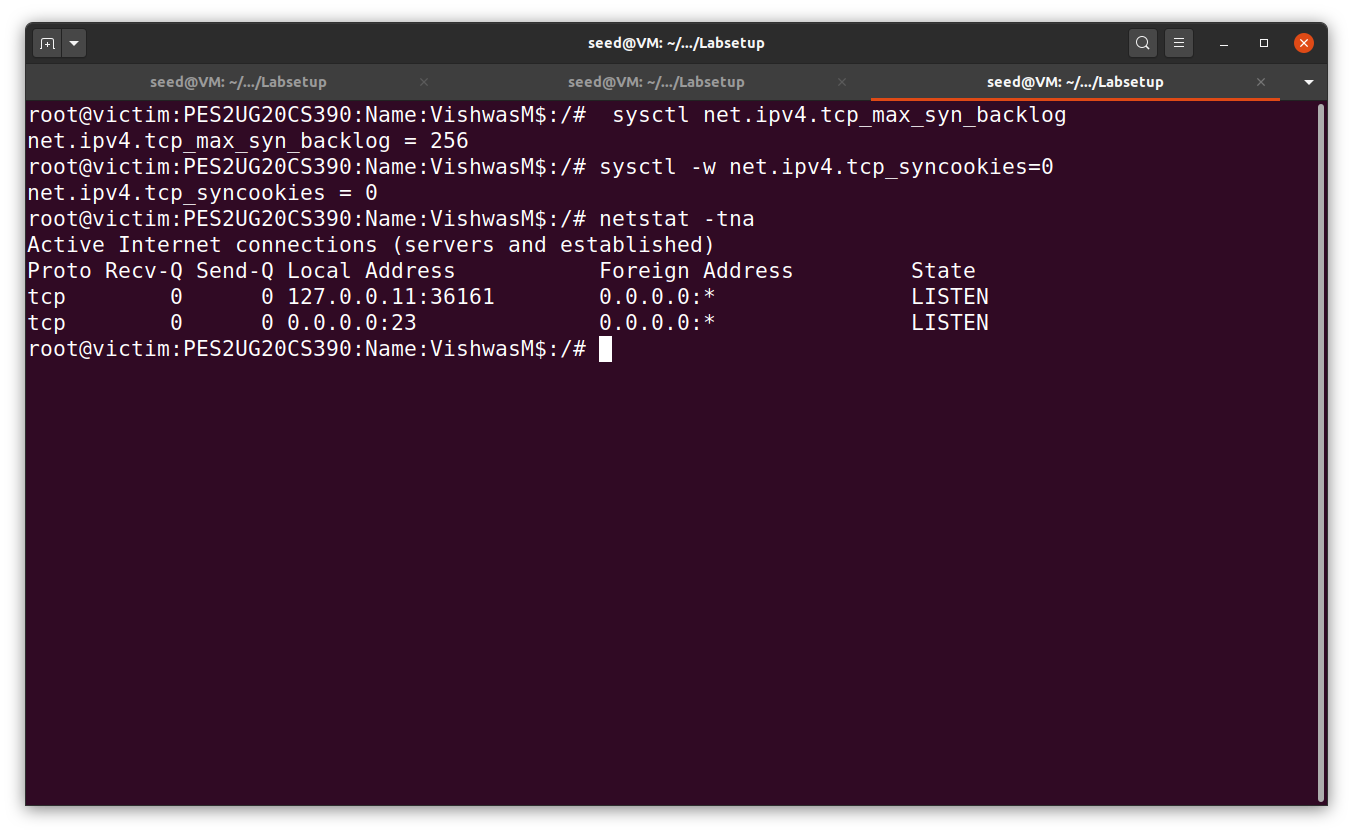
DATE:25/09/2022

Task 1: SYN Flooding Attack

SYN flood is a form of DoS attack in which attackers send many SYN requests to a victim’s TCP port, but the attackers have no intention to finish the 3-way handshake procedure. Attackers either use spoofed IP addresses or do not continue the procedure. Through this attack, attackers can flood the victim’s queue that is used for half-opened connections, i.e., the connections that have finished SYN, SYN-ACK, but have not yet gotten a final ACK back. When this queue is full, the victim cannot take any more connections.

We turn off the SYN cookie countermeasure in the victim machine.

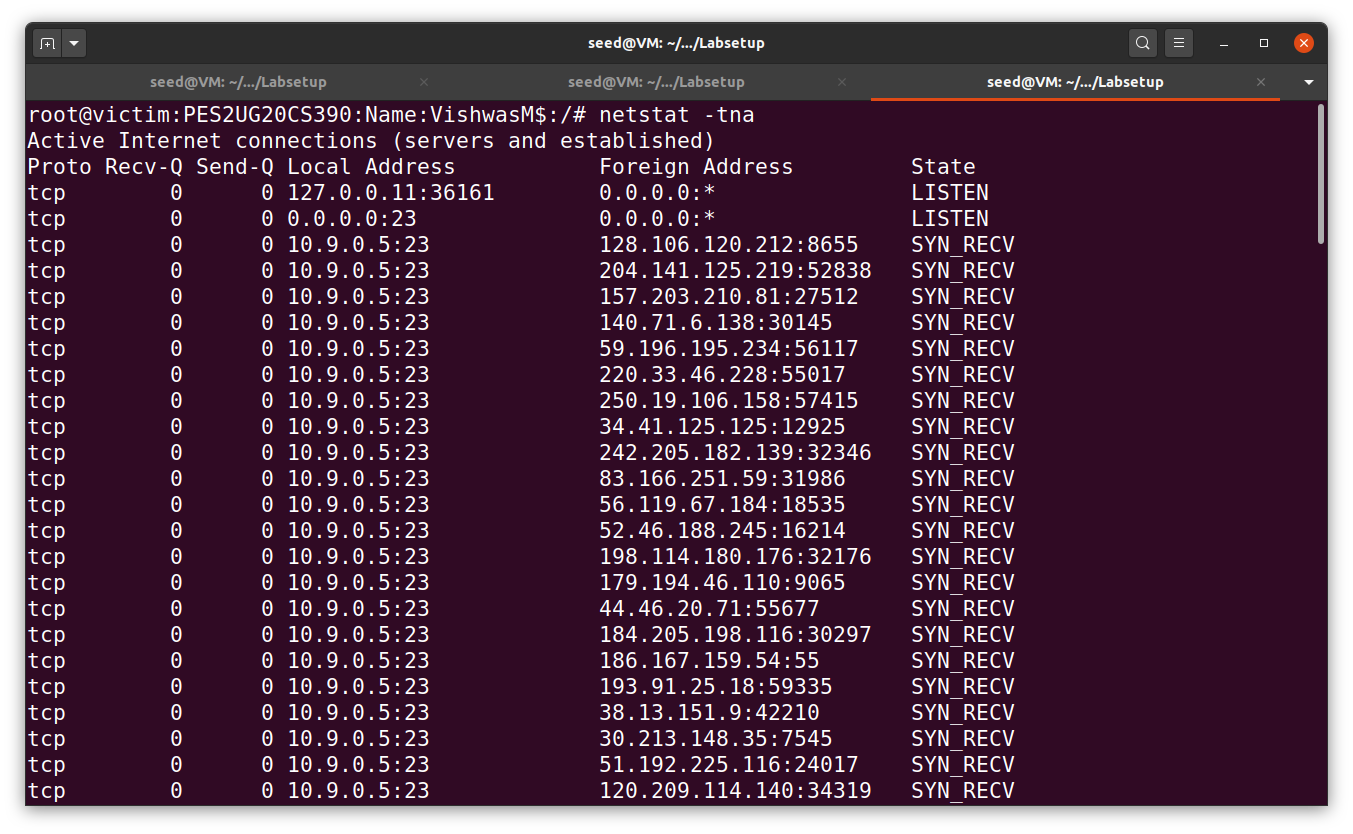
Then we check the usage of the queue before the attack.



Task 1.1: Launching the Attack Using Python

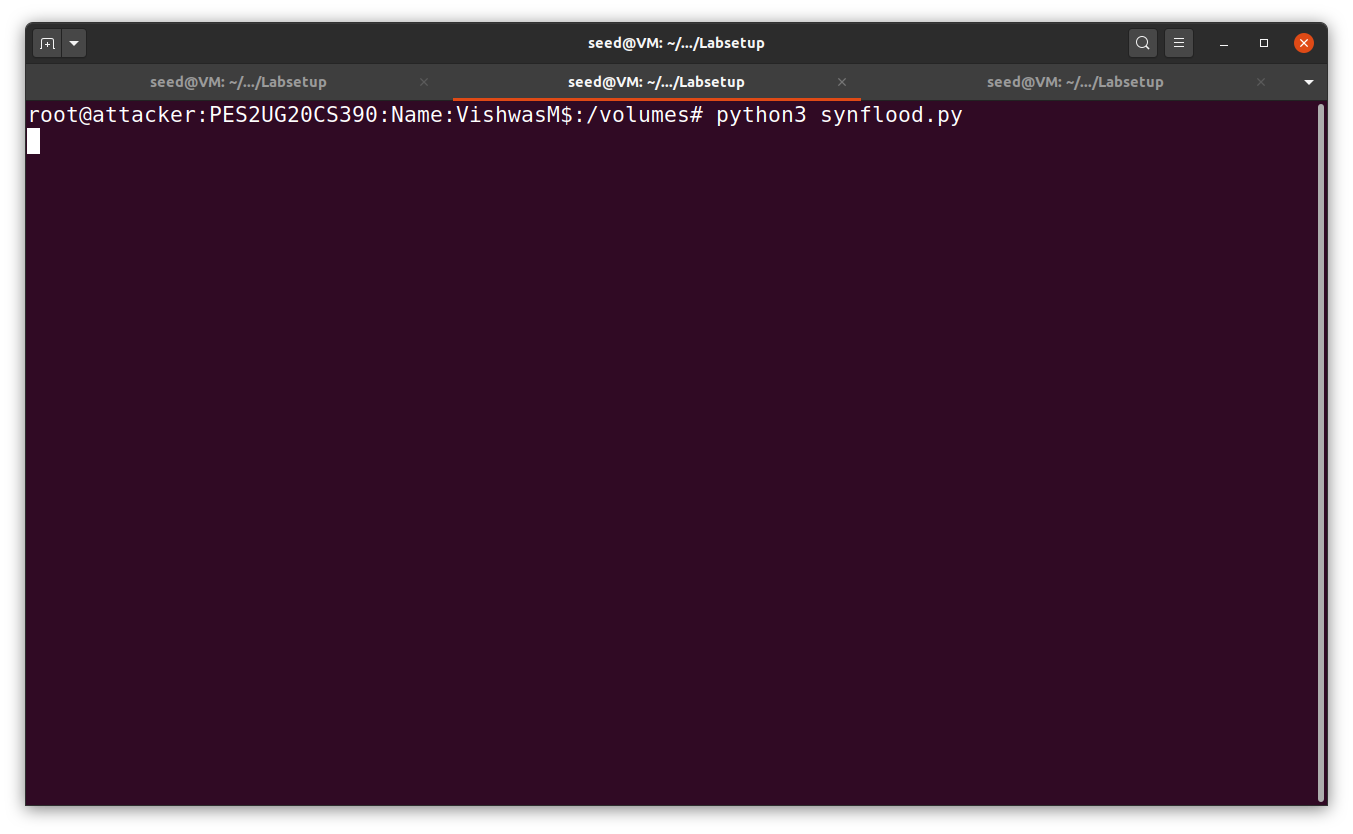
Step1:

Victim’s machine:

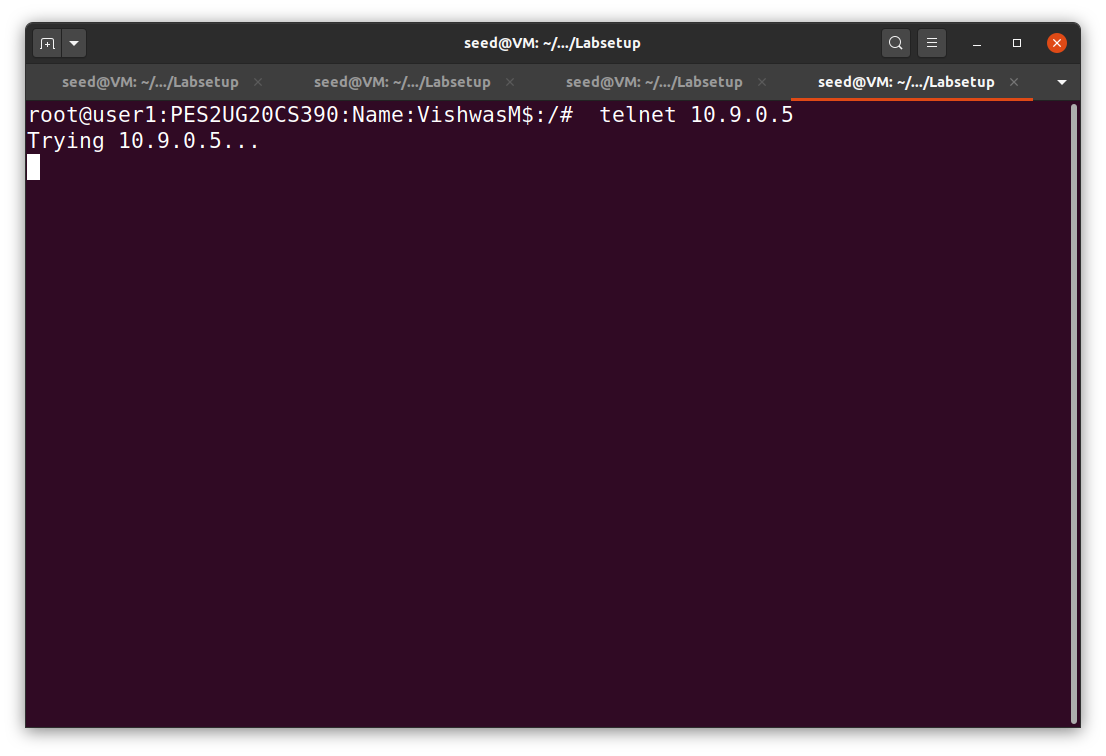


Filled with half opened connections in the victim’s machine.

Attacker’s terminal:

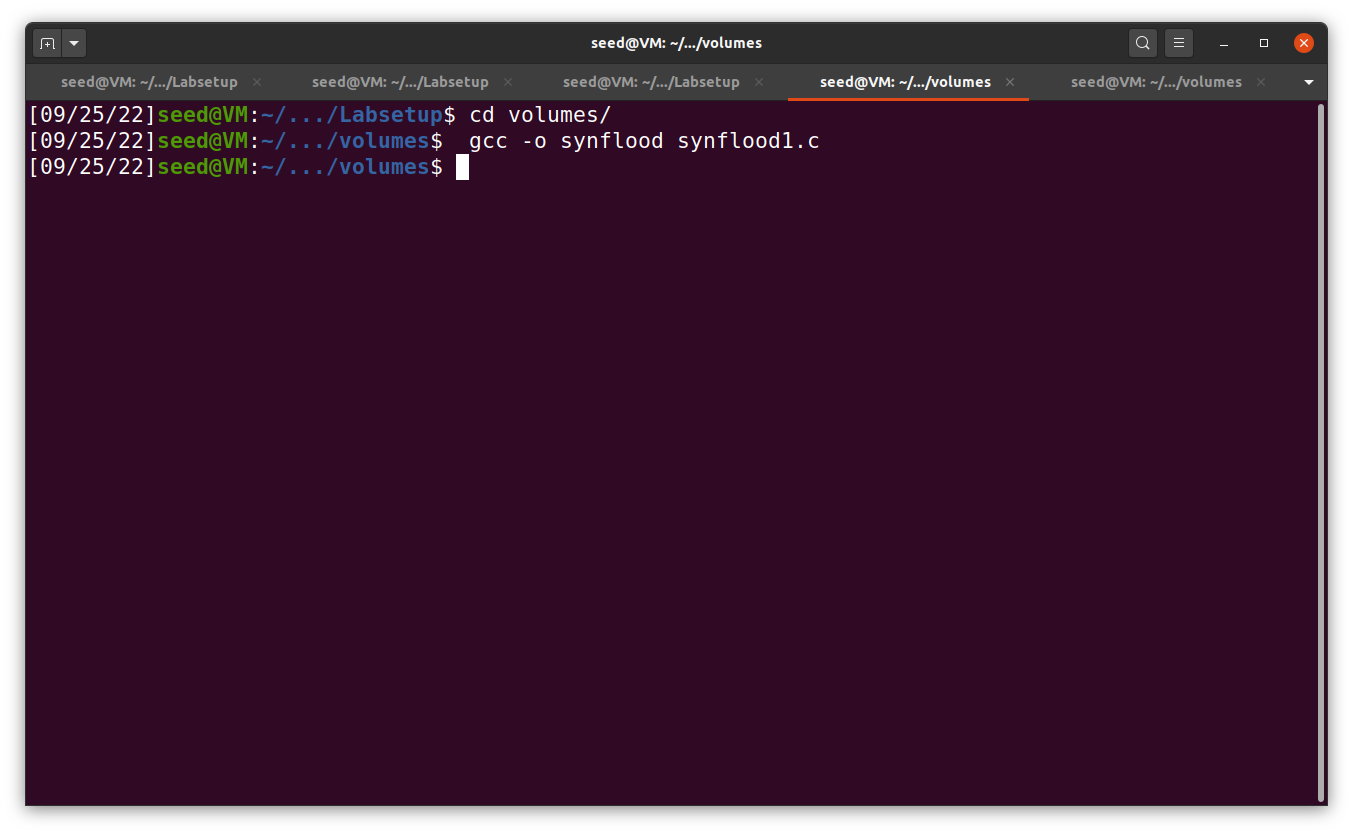


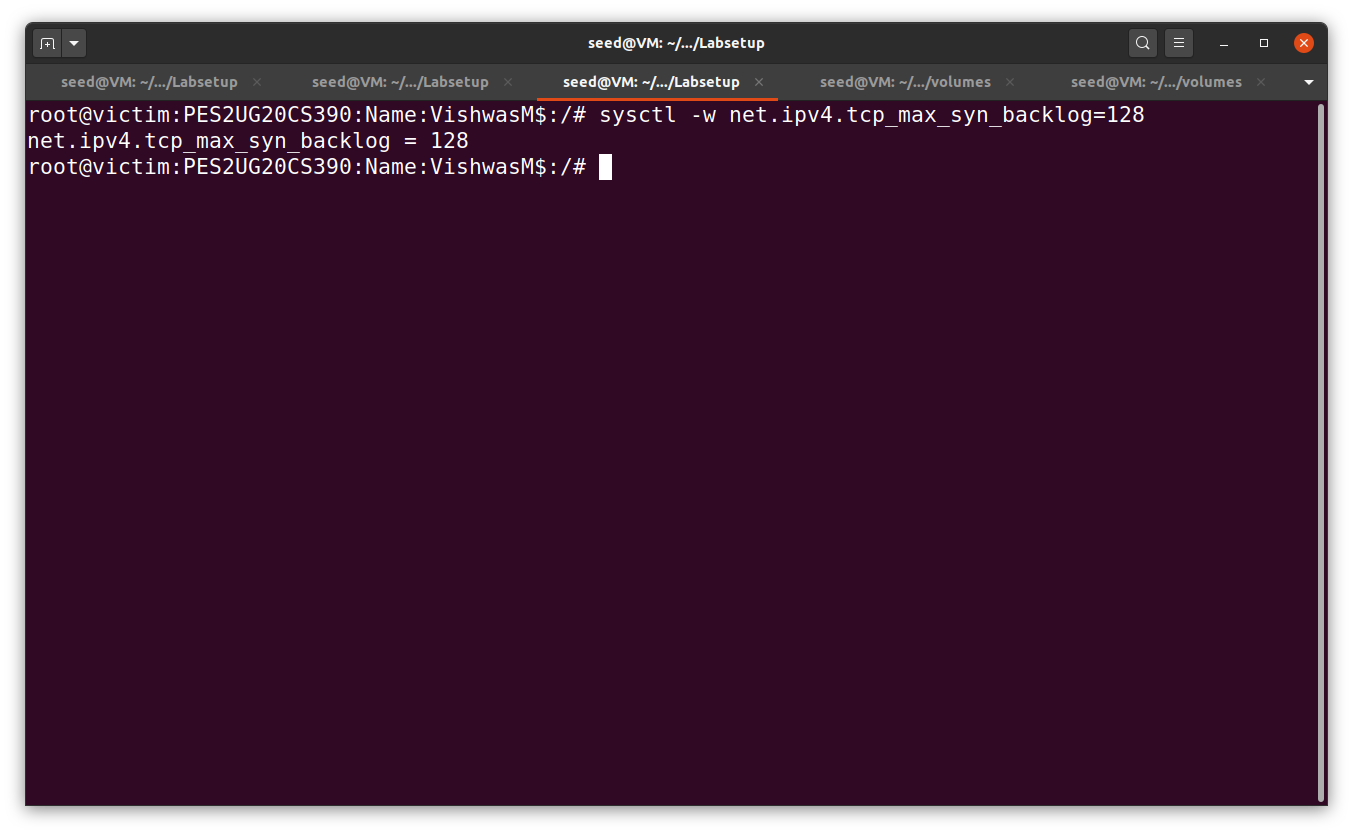
Step2:

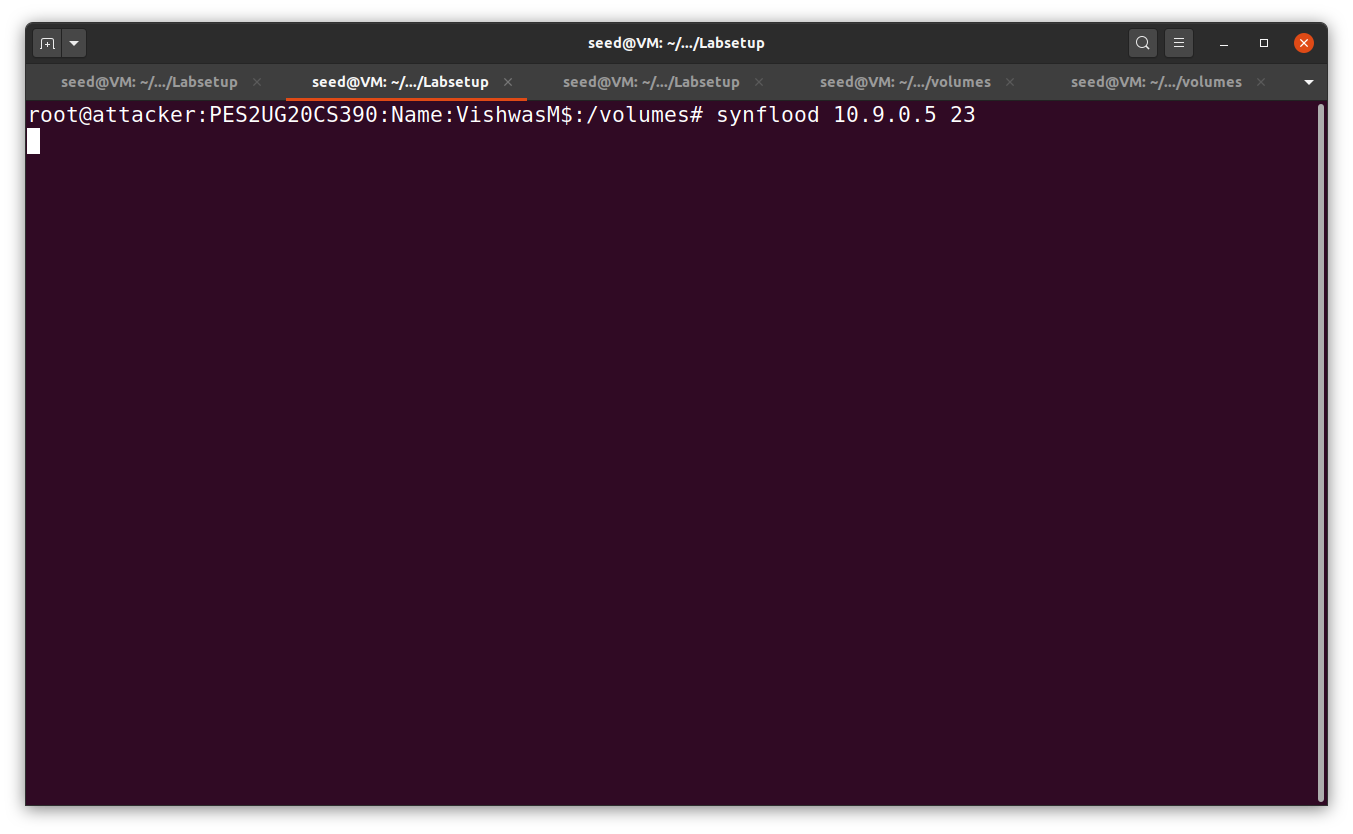


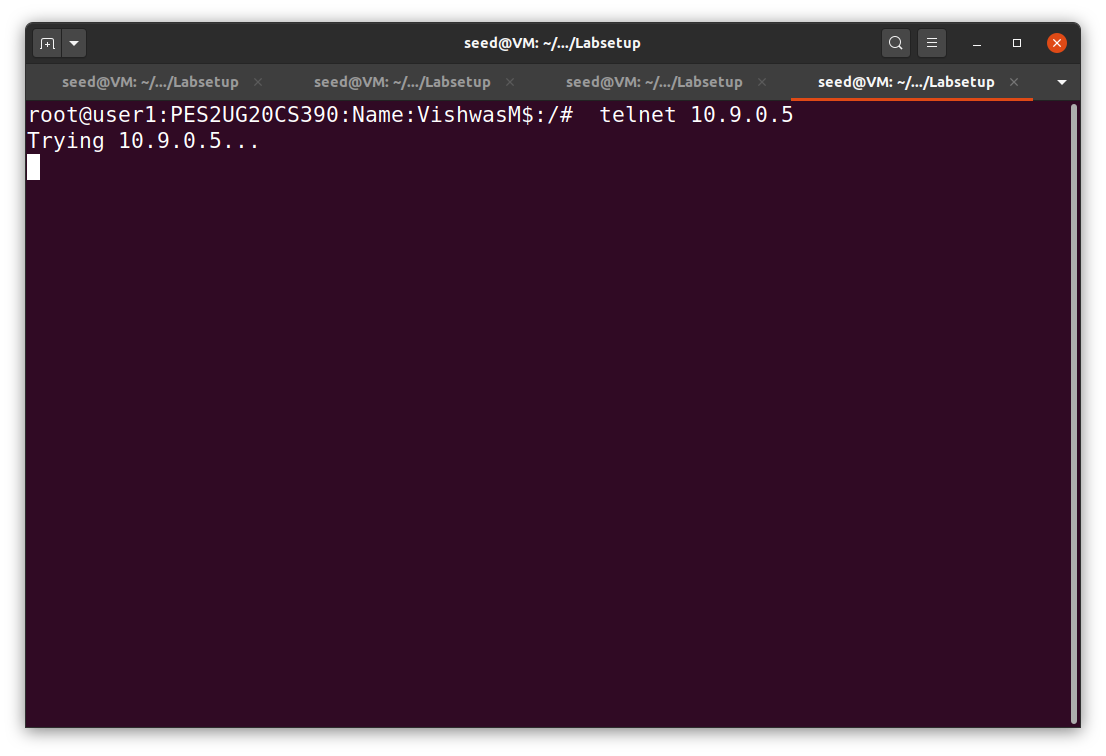
Task 1.2: Launching the Attack Using C

Other than the TCP cache issue, all the issues mentioned in Task 1.1 can be resolved if we can send spoofed SYN packets fast enough.



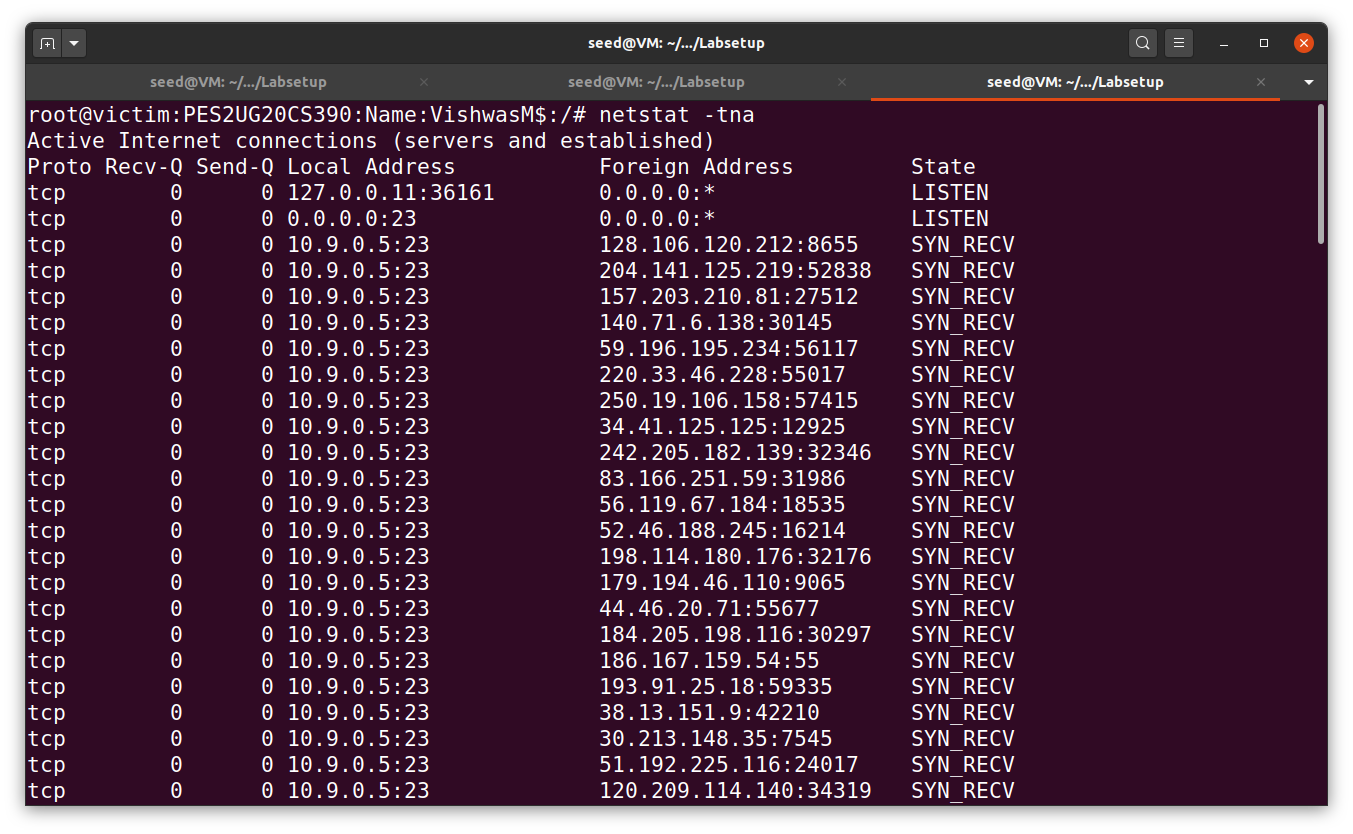


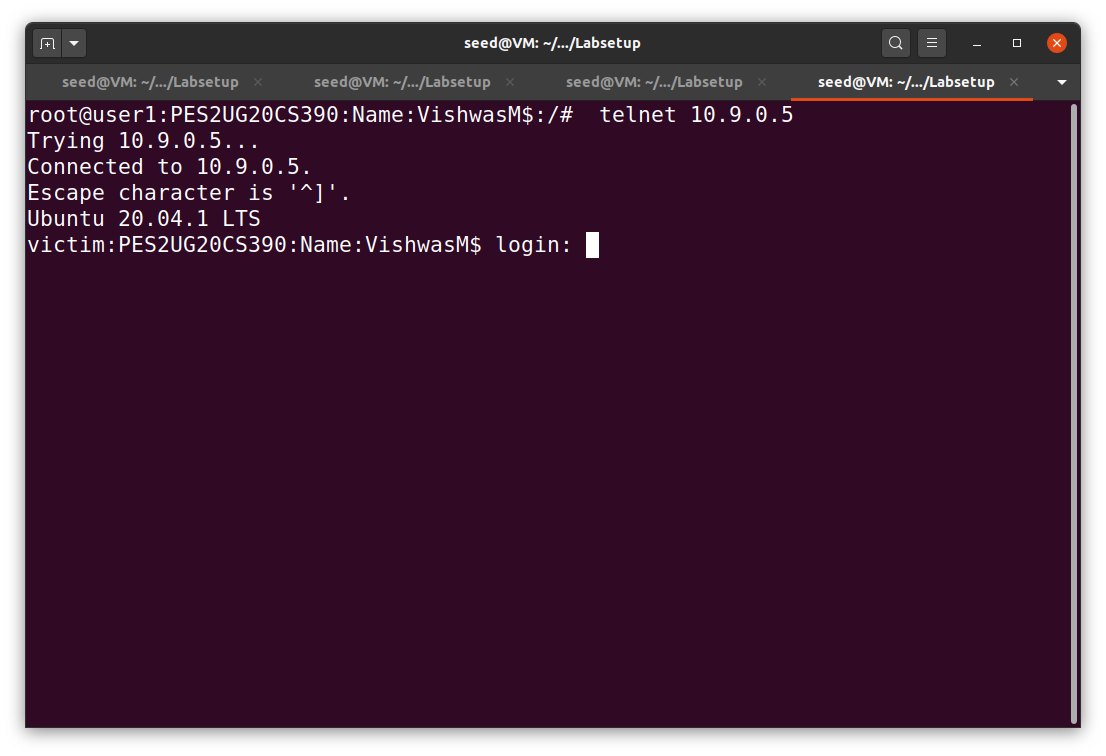




Task 1.3: Enable the SYN Cookie Countermeasure

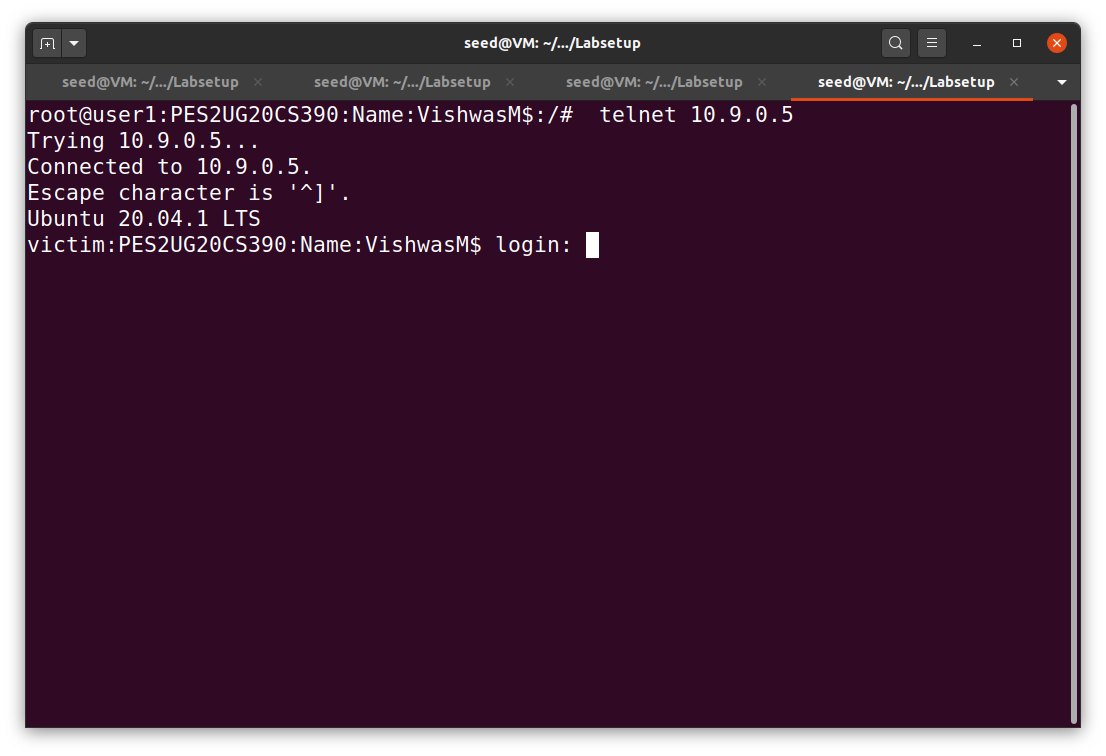
sysctl -w net.ipv4.tcp\_syncookies=1



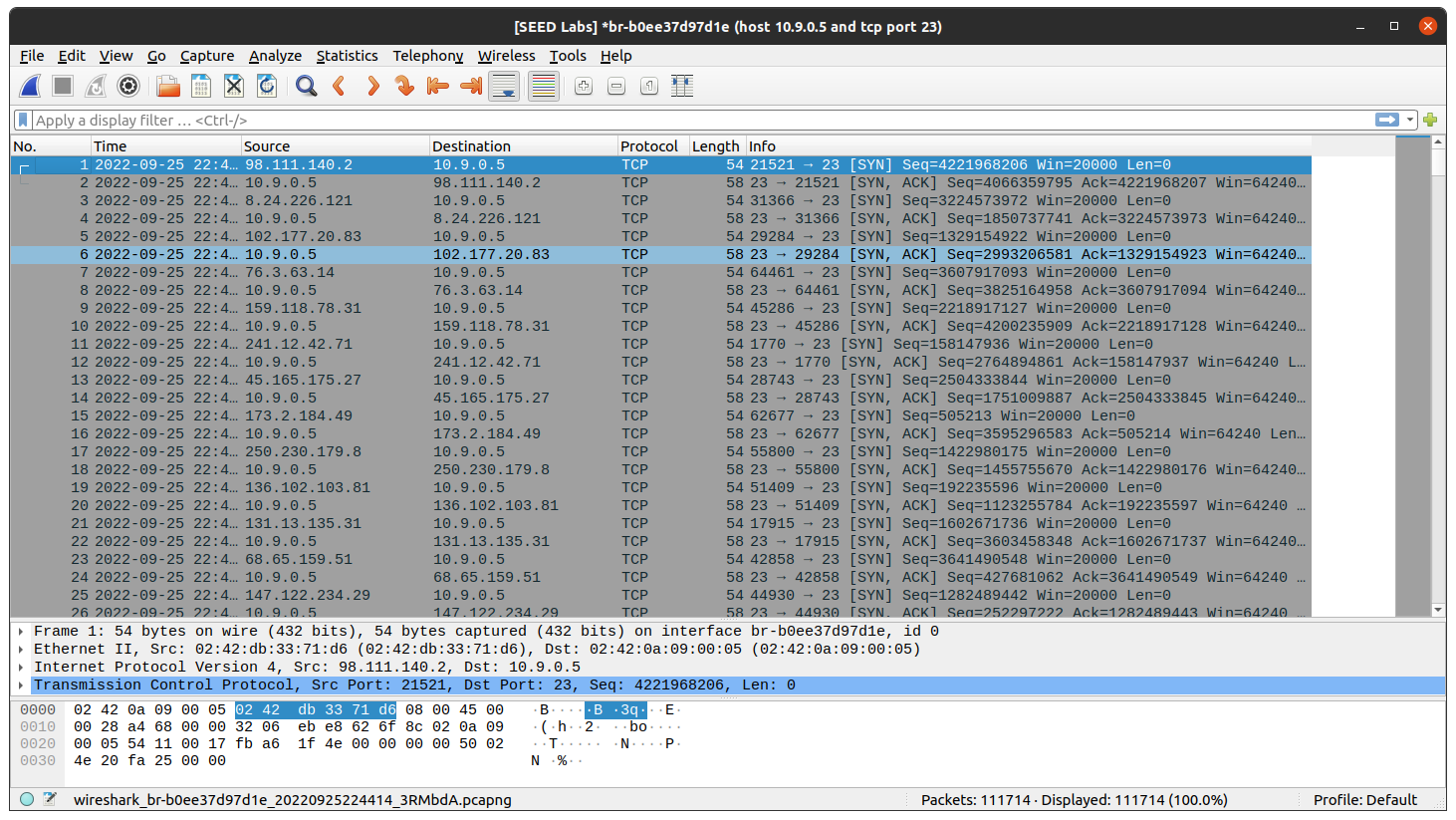


Task 2: TCP RST Attacks on Telnet Connections

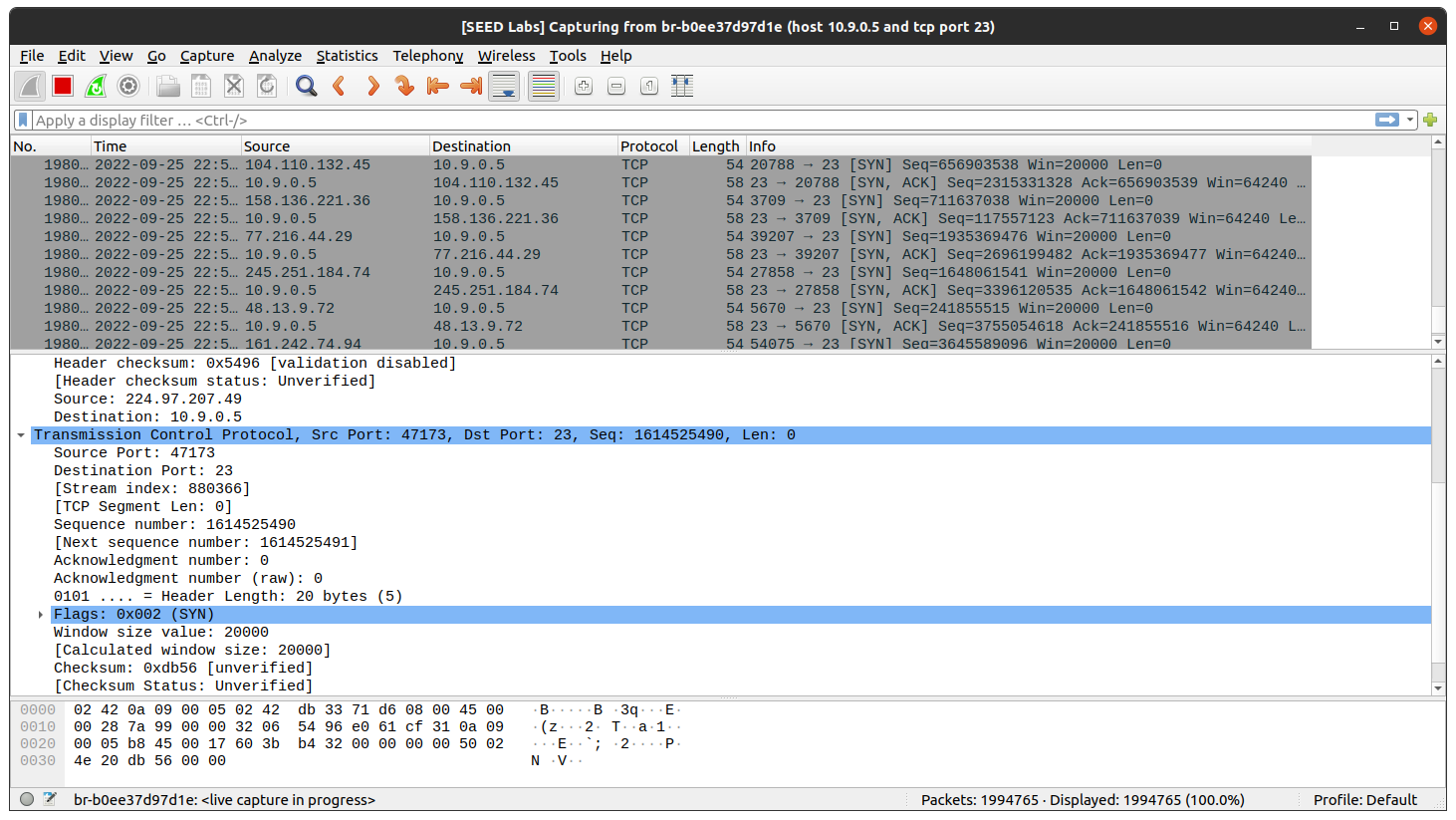
Step1:

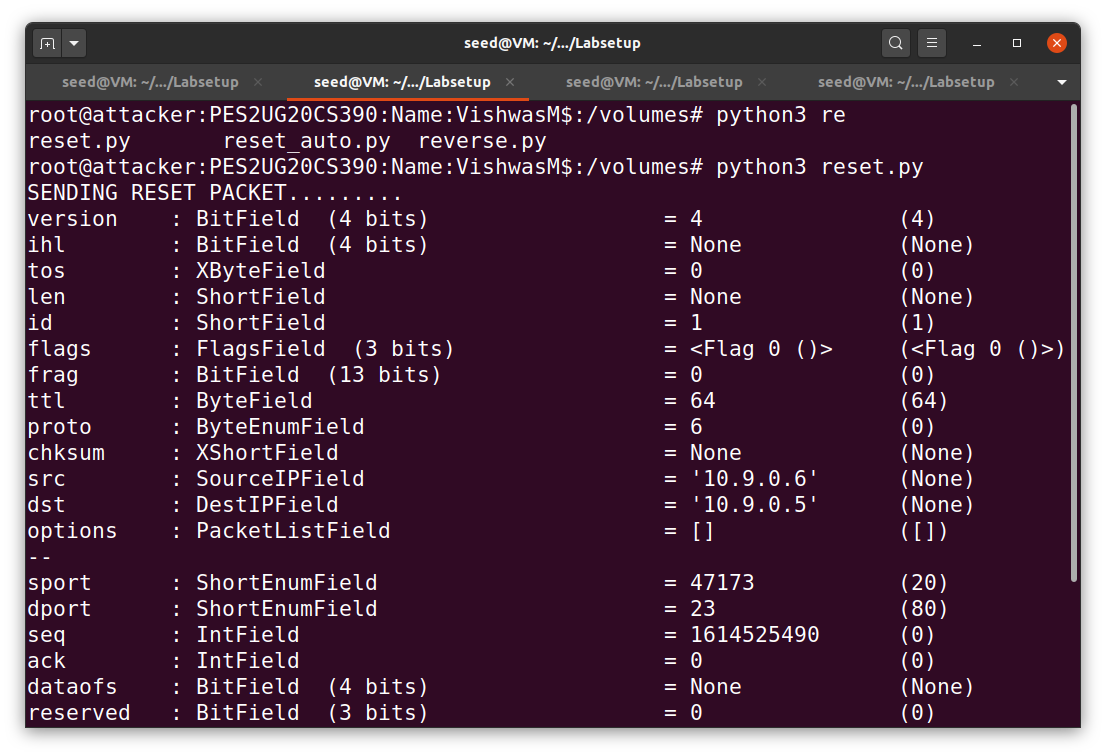


Step2:

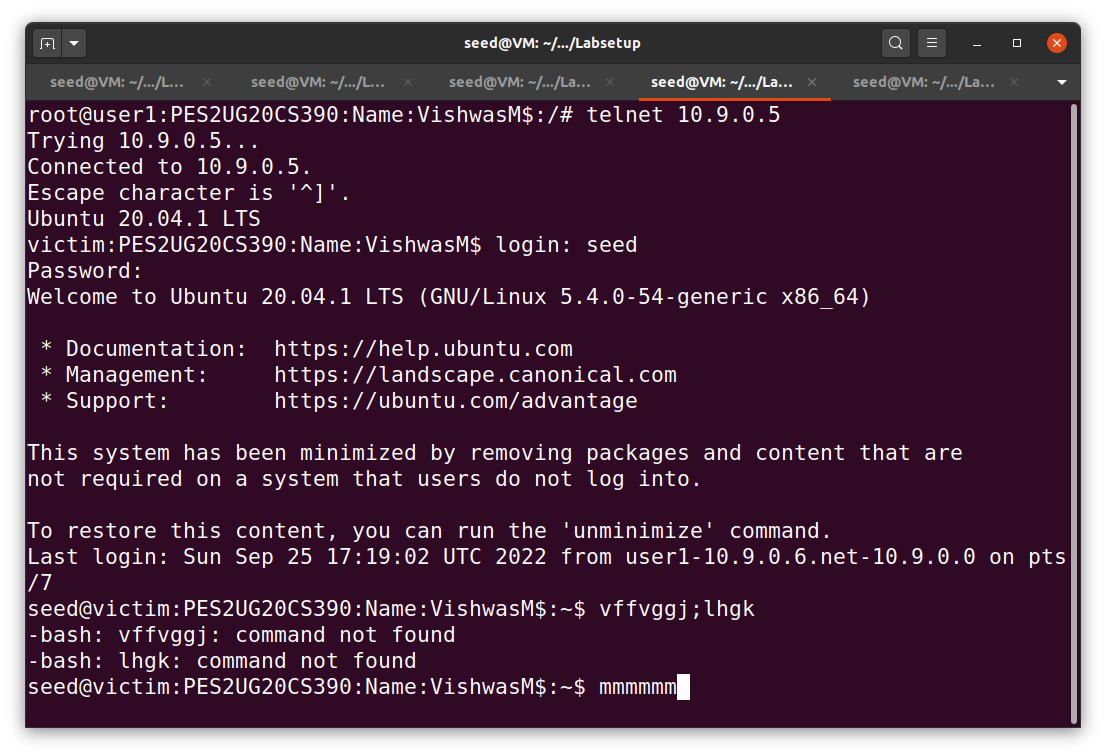


Step3:

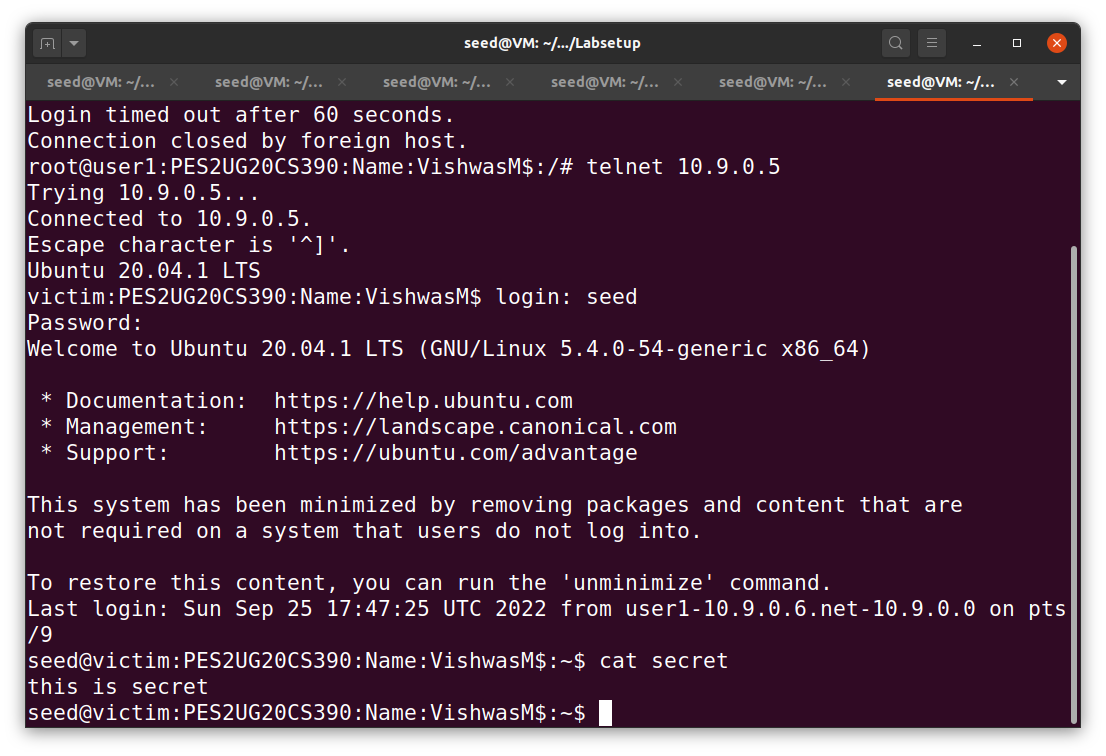


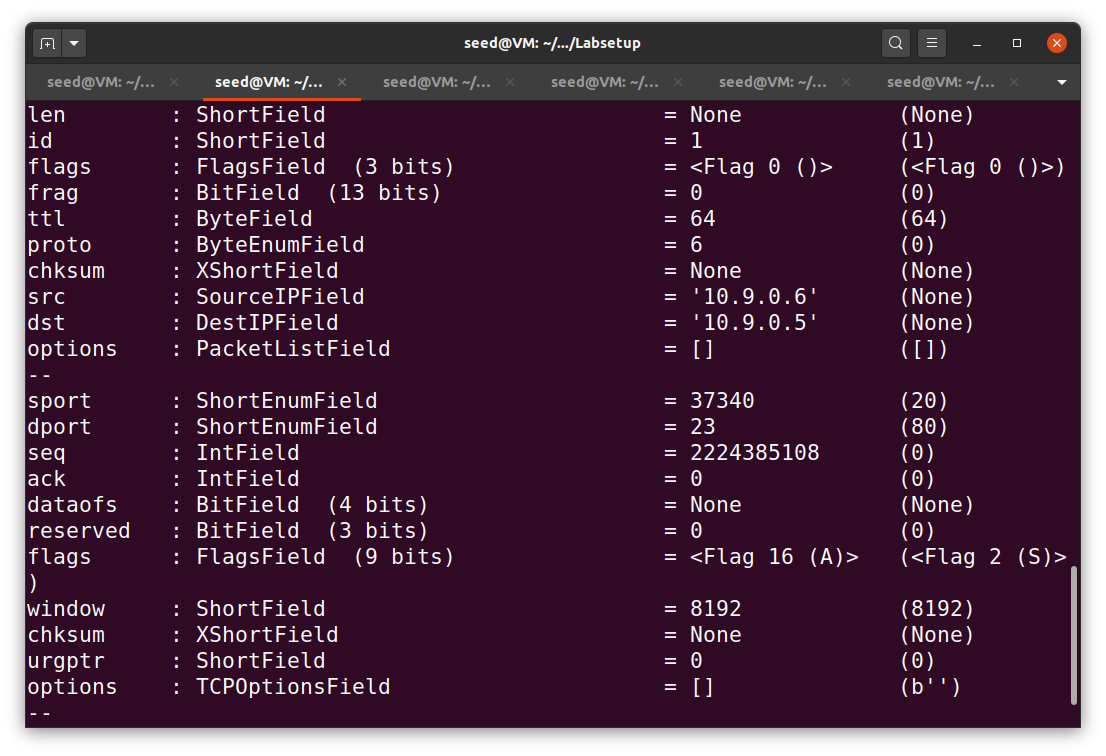


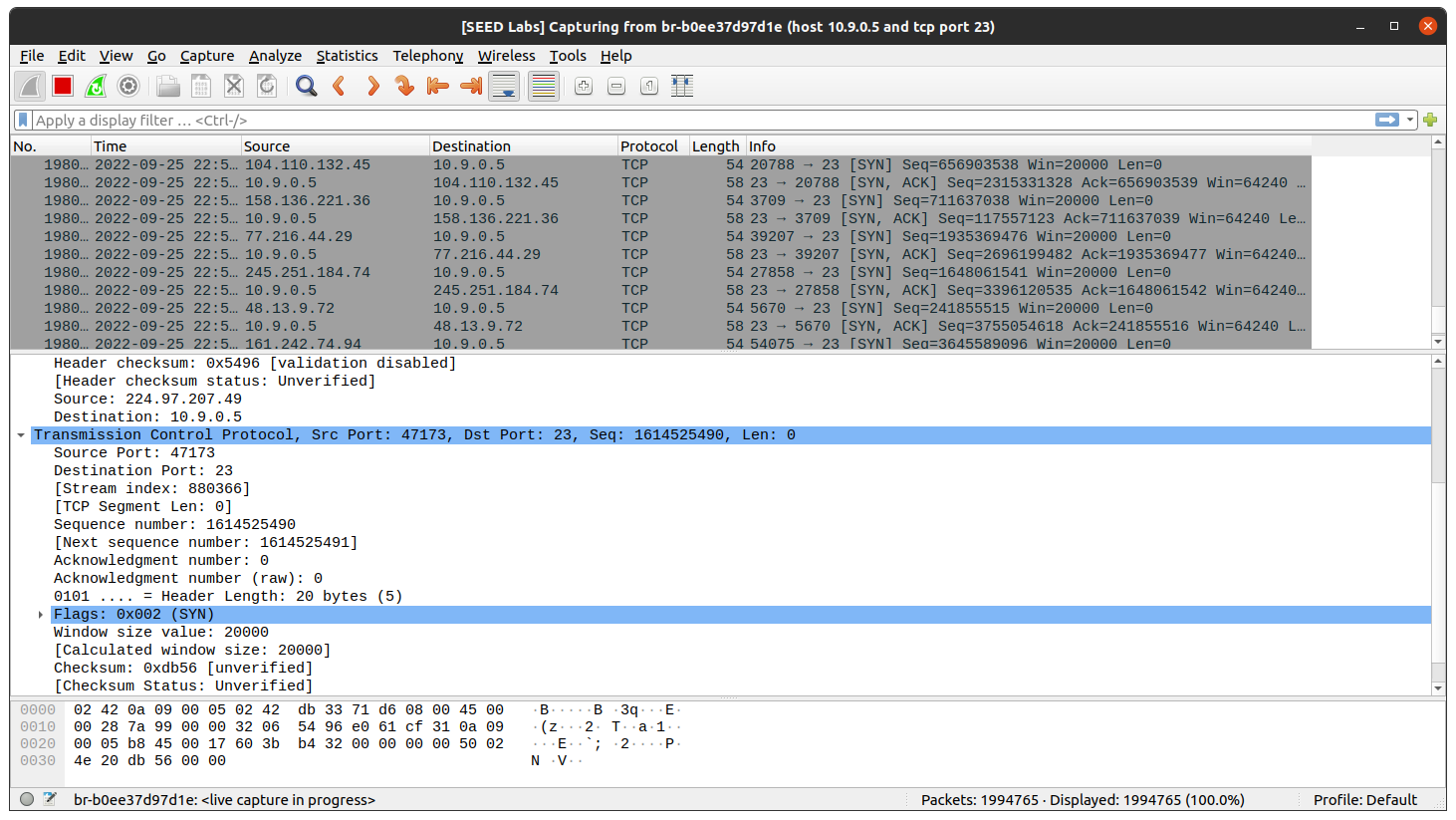
Launching the attack automatically:



Task 3: TCP Session Hijacking:







Task 4: Creating Reverse Shell using TCP Session Hijacking

When attackers are able to inject a command to the victim’s machine using TCP session hijacking, they are not interested in running one simple command on the victim machine; they are interested in running many commands. Obviously, running these commands all through TCP session hijacking is inconvenient. What attackers want to achieve is to use the attack to set up a back door, so they can use this back door to conveniently conduct further damages. A typical way to set up back doors is to run a reverse shell from the victim machine to give the attacker access to the victim machine. A reverse shell is a shell process running on a remote machine, connecting back to the attacker’s machine. This gives an attacker a convenient way to access a remote machine once it has been compromised.

The first step in this task is to establish a Telnet connection between the user and the victim -make sure to execute ‘ls’ etc. to ensure the working of the connection.

