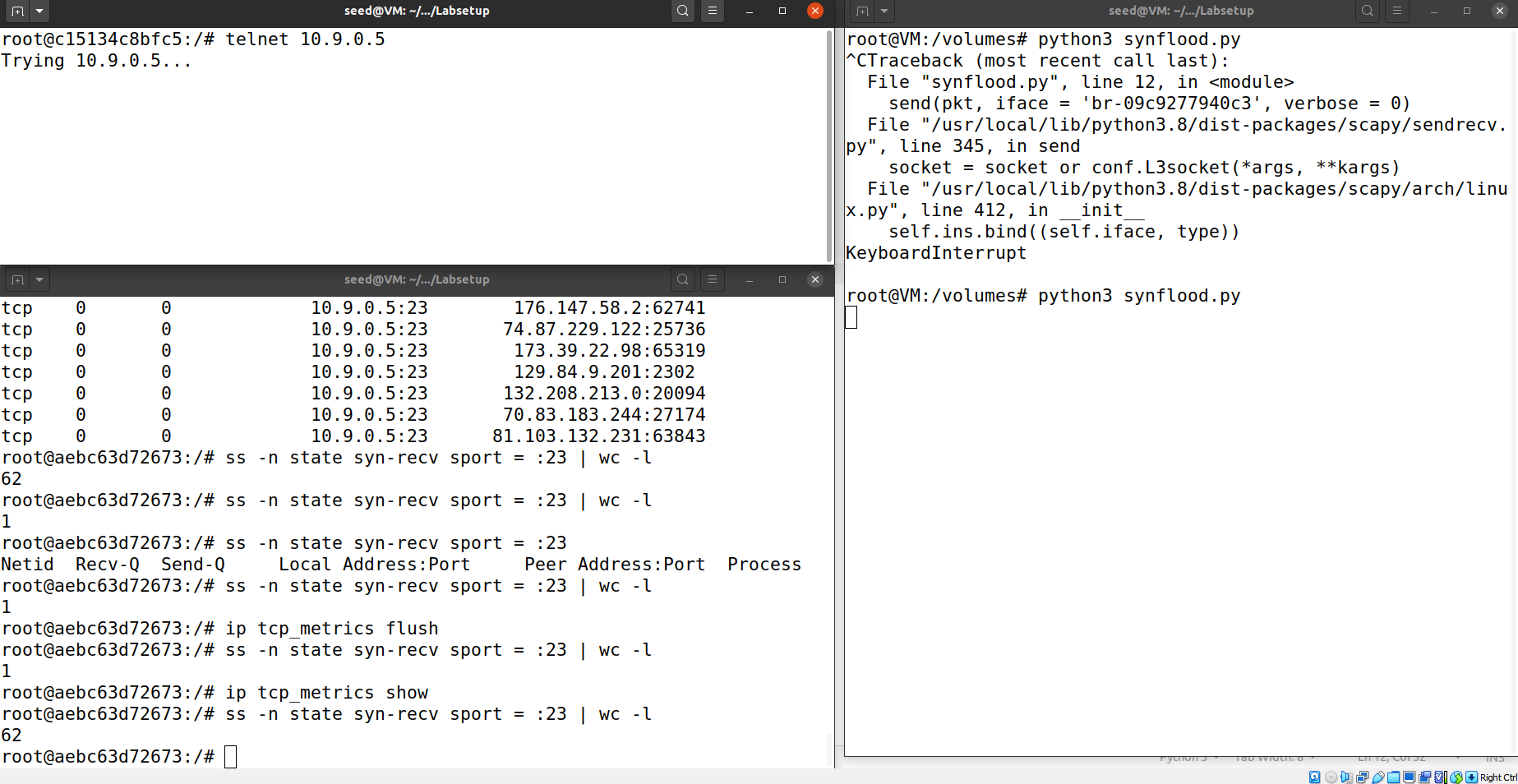
Name: Donghao Li

SU email: [dli106@syr.edu](mailto:dli106@yr.edu)

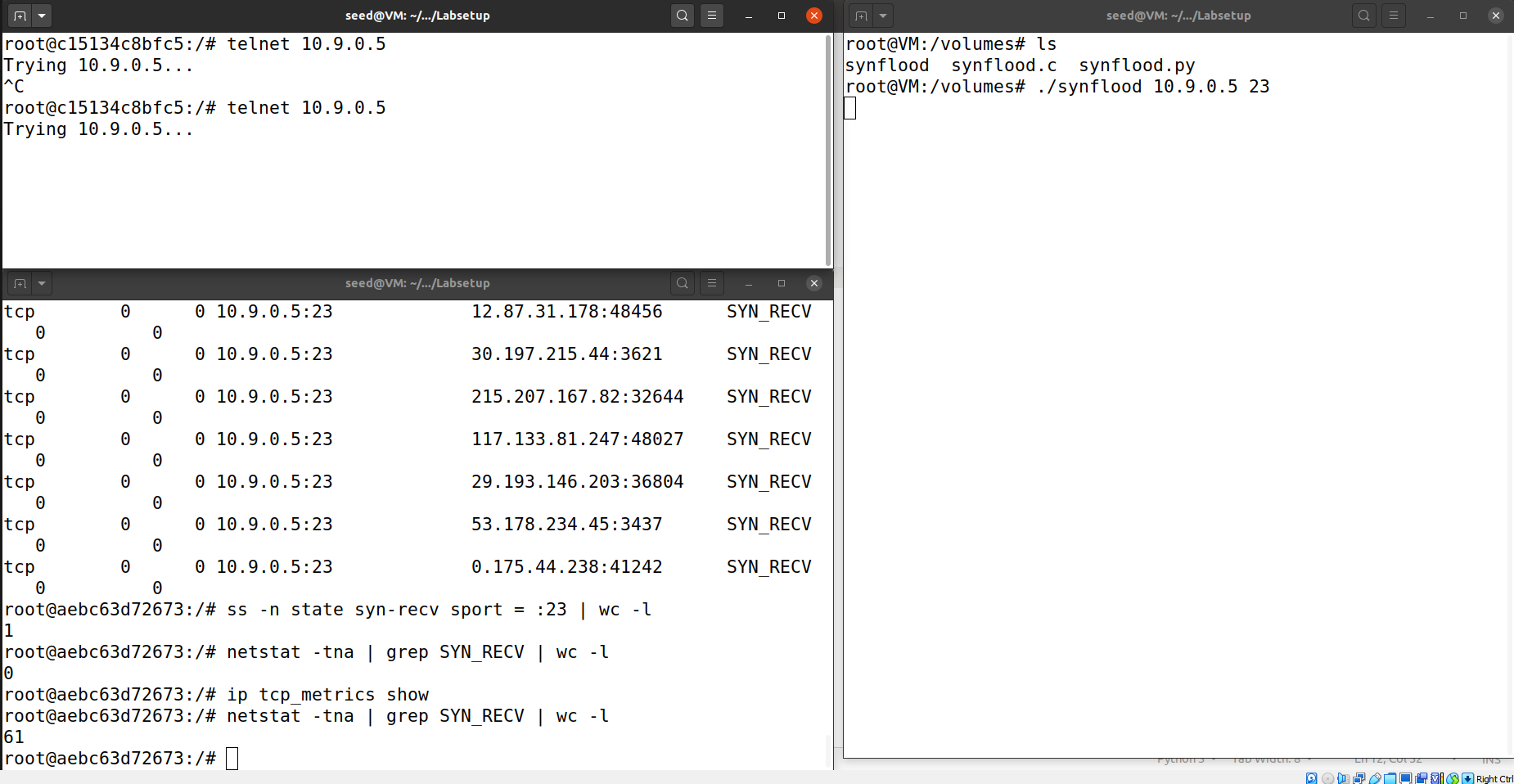
**Task 1:**

**Task 1.1: Launching the Attack Using Python**



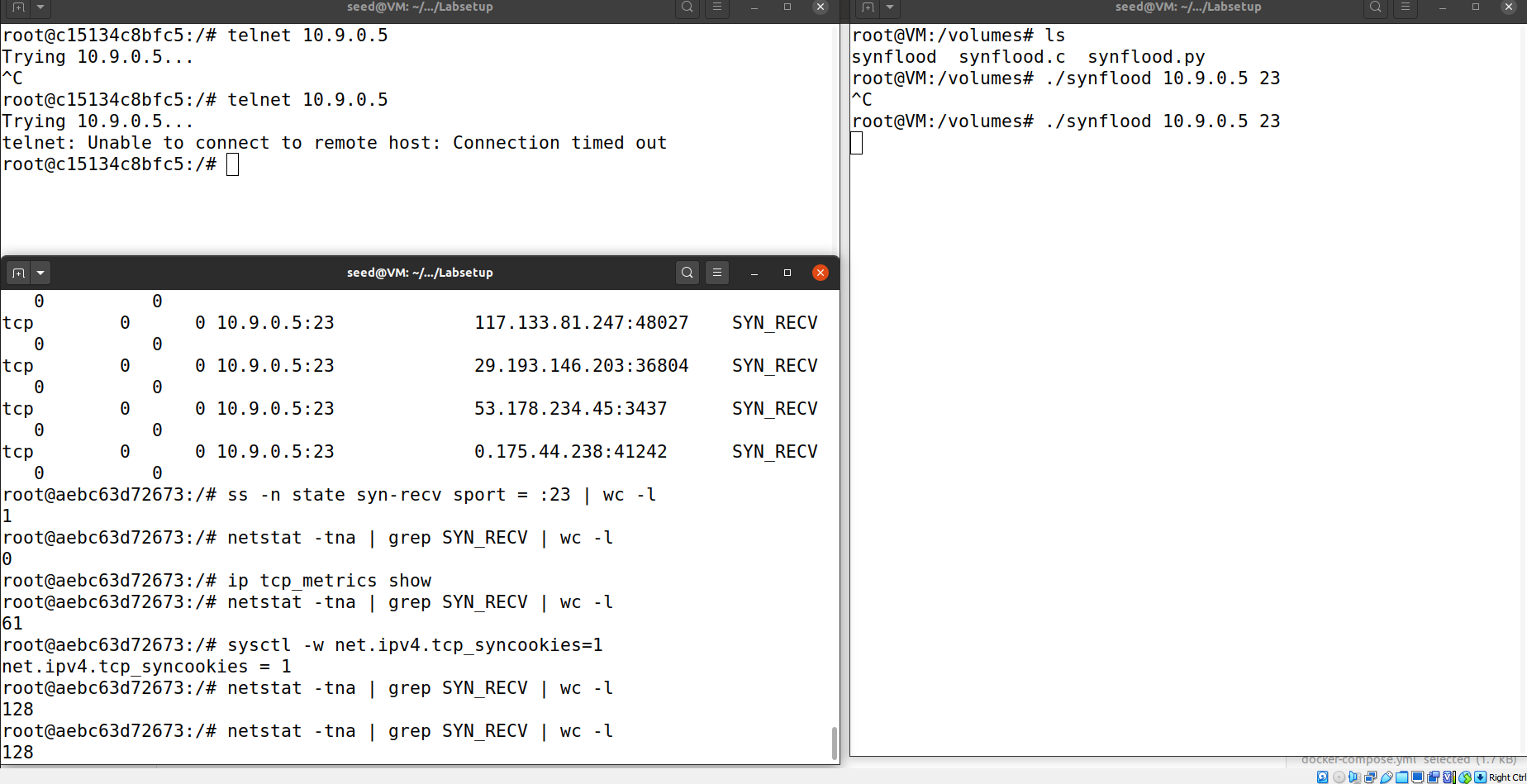
As you can see, while the synflood attack is launching in the attacker view, the victim part receives SYN\_RECV calls, when the user1 try to telnet victim, it have to wait.

**Task 1.2: Launch the Attack Using C**

****

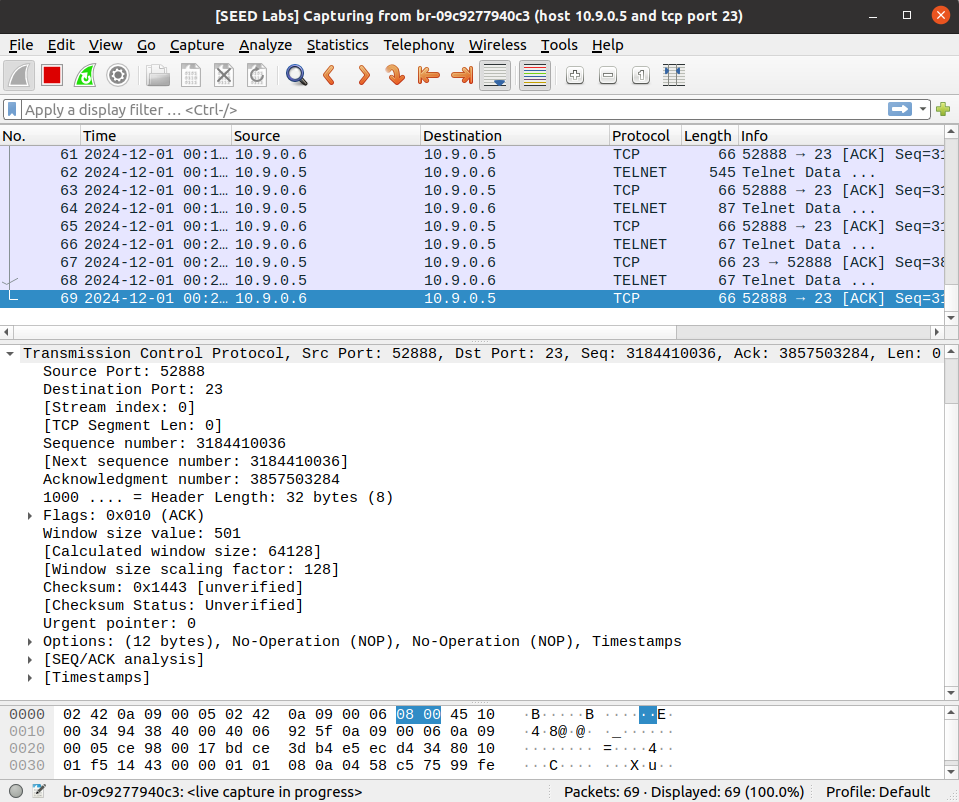
Things waorks the same in C. I should have mention after a while of time, user1 would be able to accomplish telnet command with the python version attack. Also, i aware that the max syscalls number for both version are 61 but we set up max number for half open connections are 80. This means as a Ubunto 20.04 up user, i prove that the system do save some space for users who used to be connected to the victim.

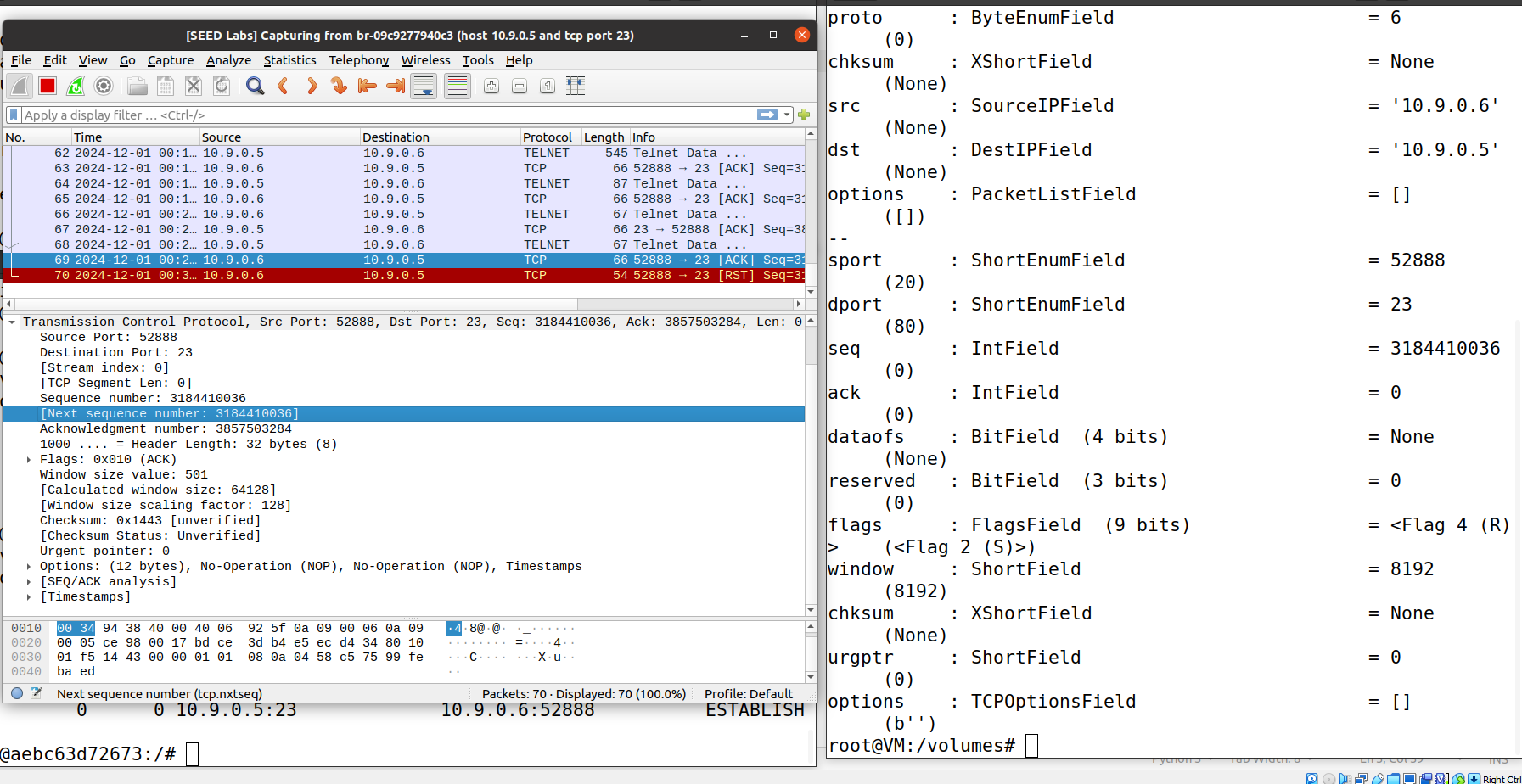
**Task 1.3: Enable the SYN Cookie Countermeasure**

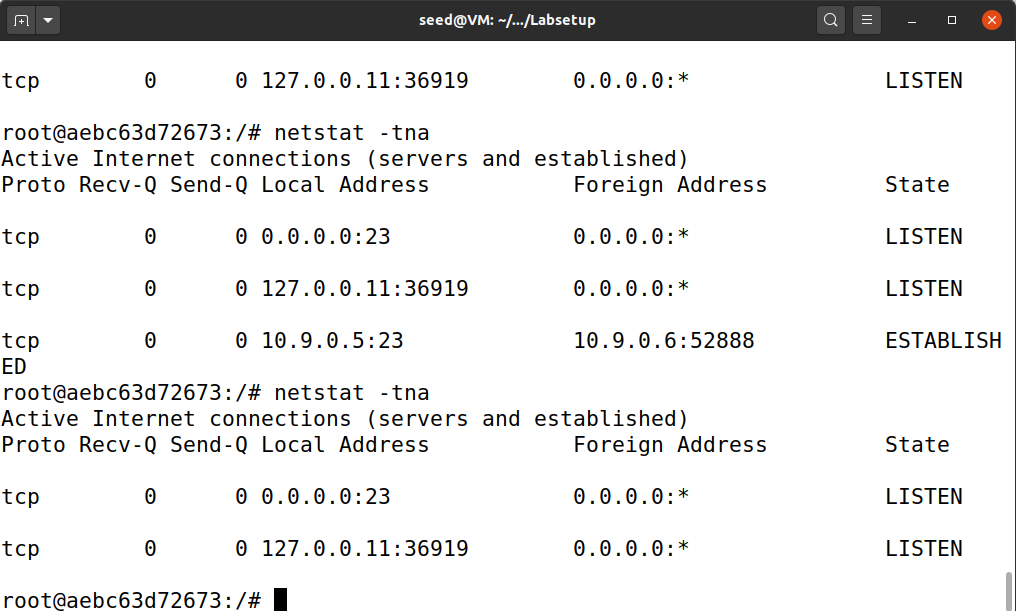


since we set everything back to default, so the max number for backlog go back to 128 thats why the number goes to 128 here. Both python and C version happened. Meanwhile, python version still be able to receive telnet from user1 after a while. Although the max value SYN\_RECV issue seems not showing up, but wheni test user1 can still telnet victim, which mean Ubuntu still save some memory for used users.

**Task 2: TCP RST Attacks on telnet Connections**

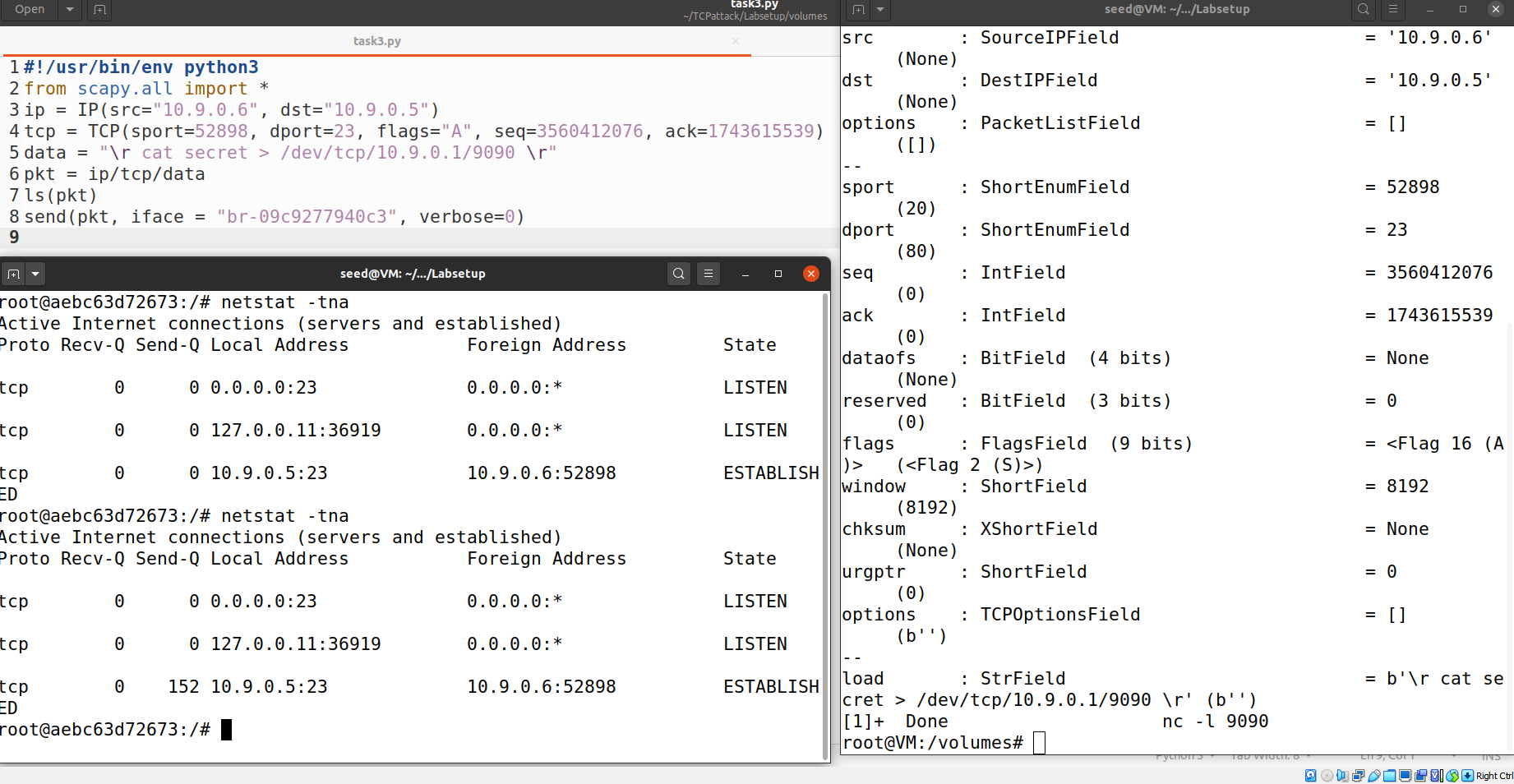


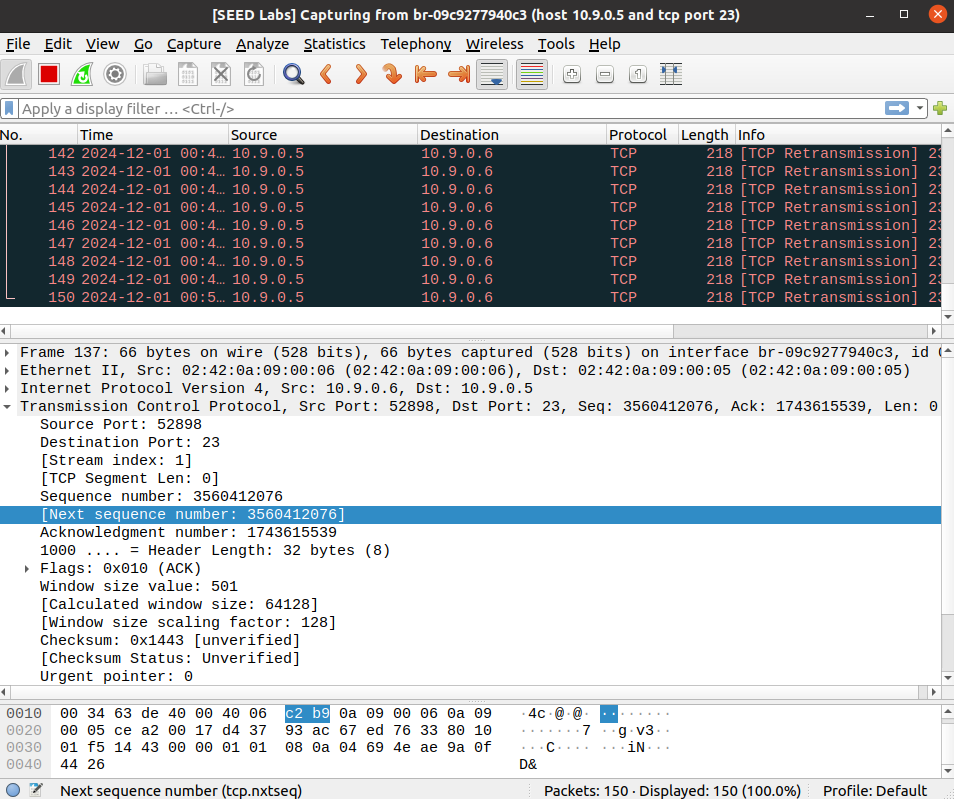




I am trying to mamic a TCP request from user to receiver, as yo ucan see i find the sequence number from the user part, this allow me to mamic as the user and send a reset to receiver. And as you can see after i input all the information needed and run the task2.py which is the attack file. there is a reset begin send successfully. And the established connection between user1 and victim is being reset.

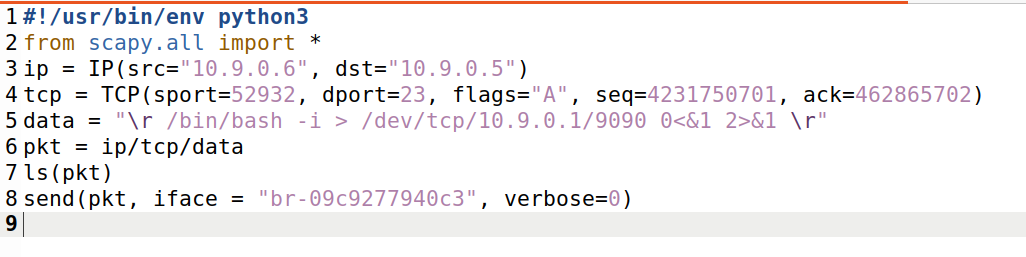
**Task 3: TCP Session Hijacking**

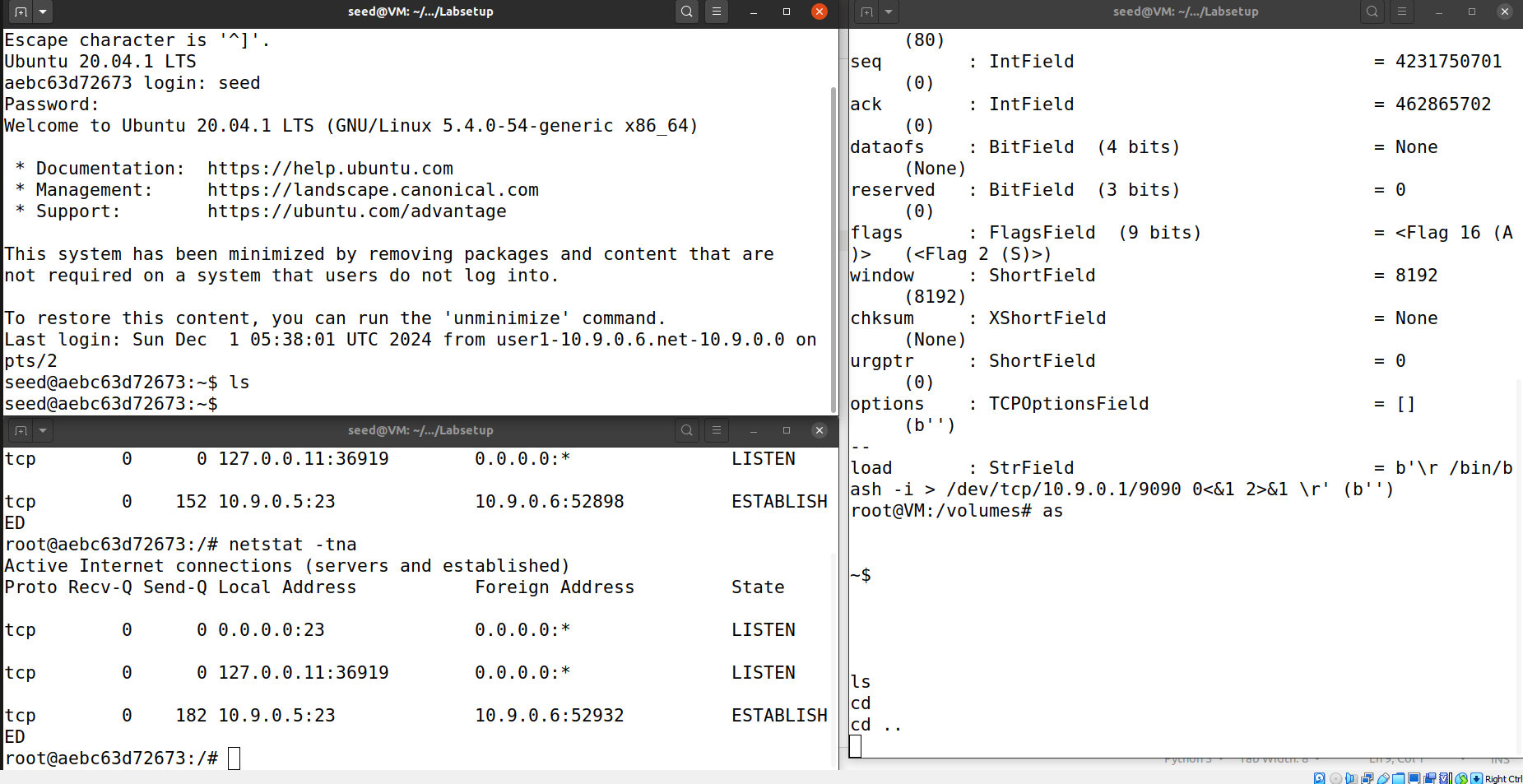




By using the sequence number and acknowledge number from the user to victim, i can not hijack all the packages send from victim to user, as you can see the connection between user1 and victim is still established but the package is lost. So victim kept trying to send package to user. Also when user trying to type anything, the victim server will not receive the package, so user can do nothing.

**Task 4: Creating Reverse Shell using TCP Session Hijacking**





as you can see, by creating reverse shell, the attacker would be able to hijackt the user1’s telnet connection with victim, then the attacker would be able to input any harmful command through reverse shell into the victim server.