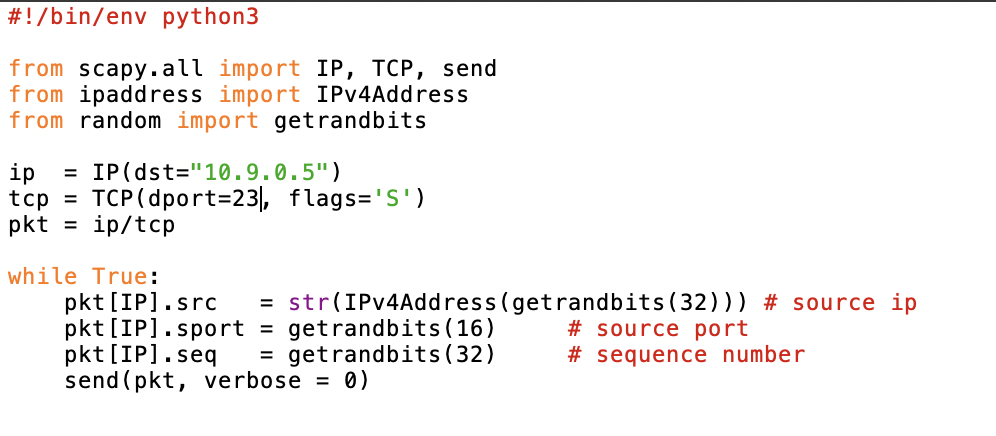
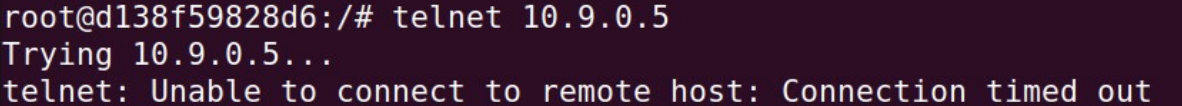
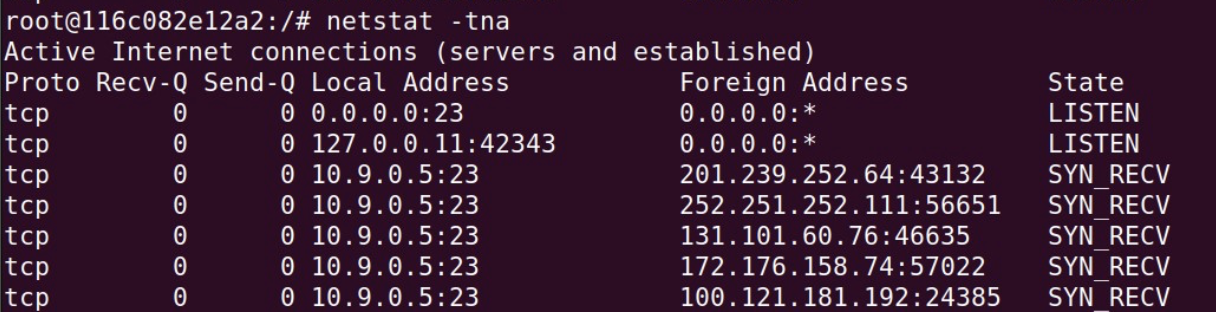
Task 1.1

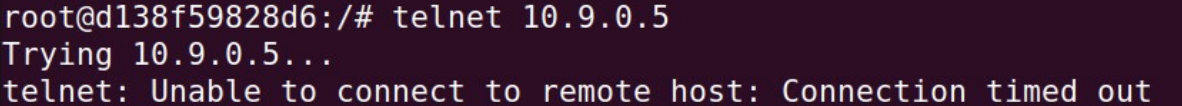
Code:  


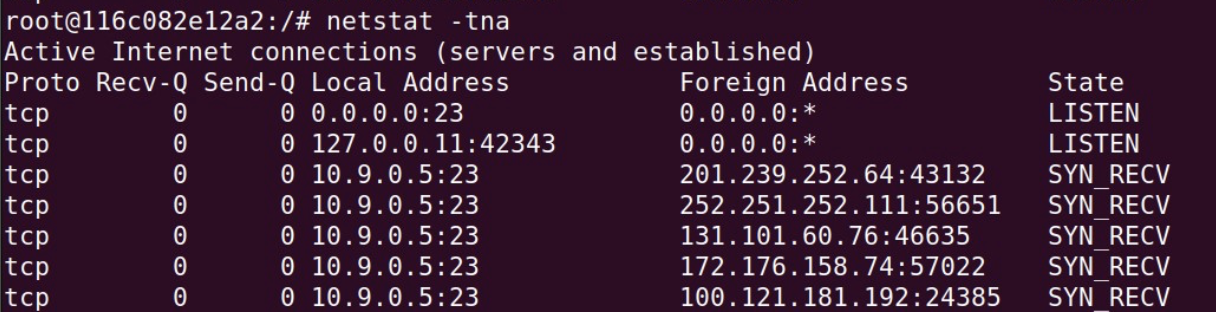
Result:  




Observation:  
We were able to flood the syn cookie in victim system

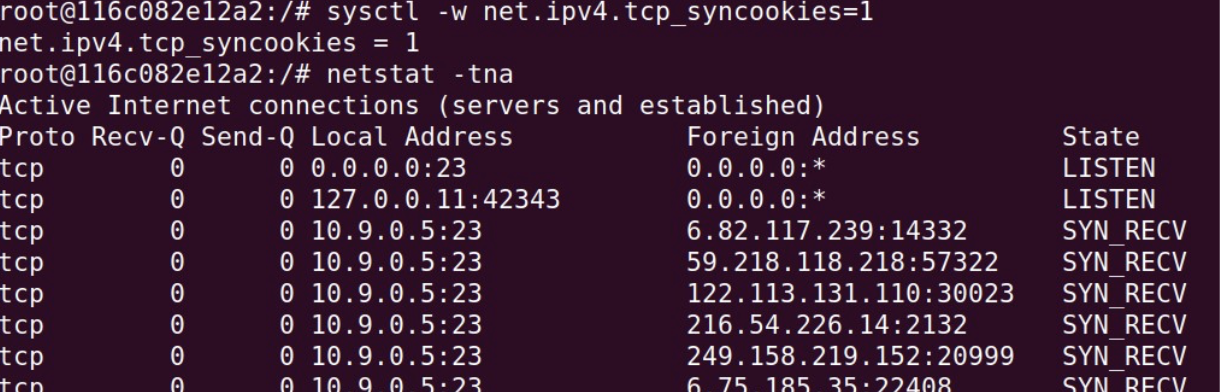
**Task 1.2**

Code as in the zip file  
Result:  




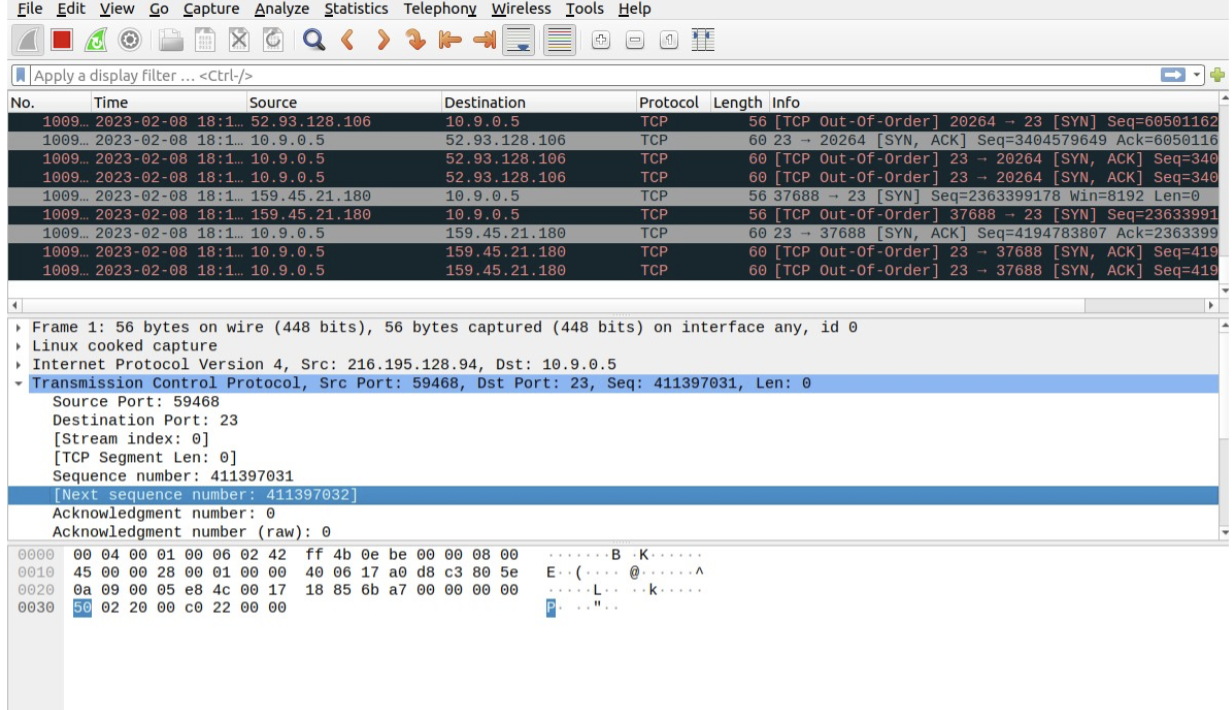
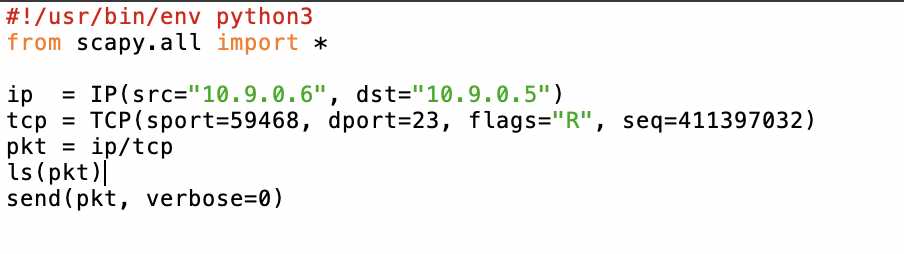
Observations:  
The C code allows us to specify victim ip and port which in this case is 10.9.0.5 and 23 respectively and is more robust than python code.

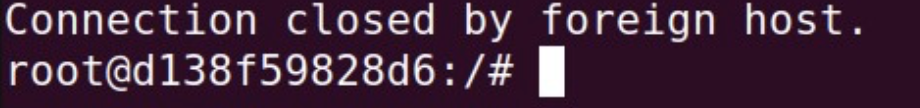
**Task 1.3**

Result:  


Observation:  
I found that the c code was doing its job but python code was not performing after turning syncookie mechanism on.

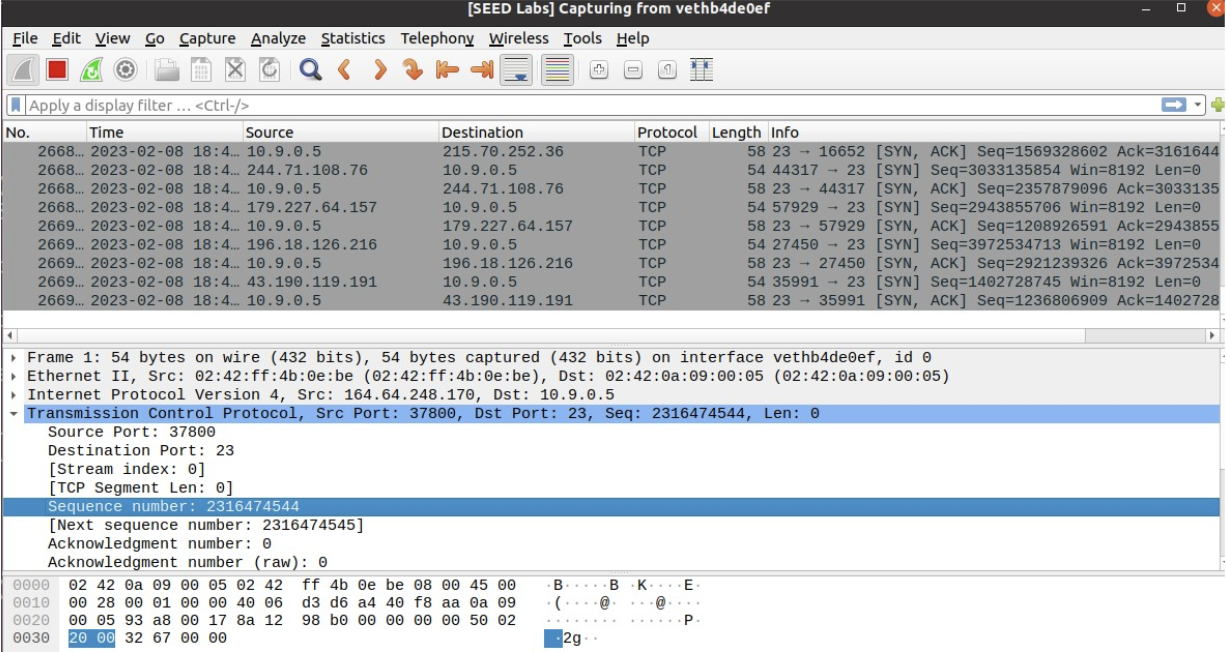
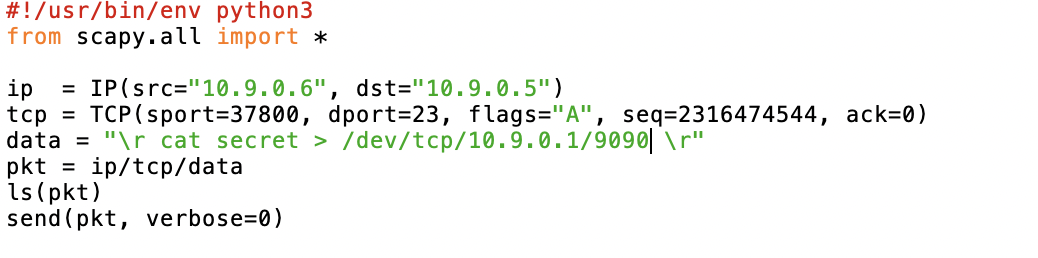
**Task 2**

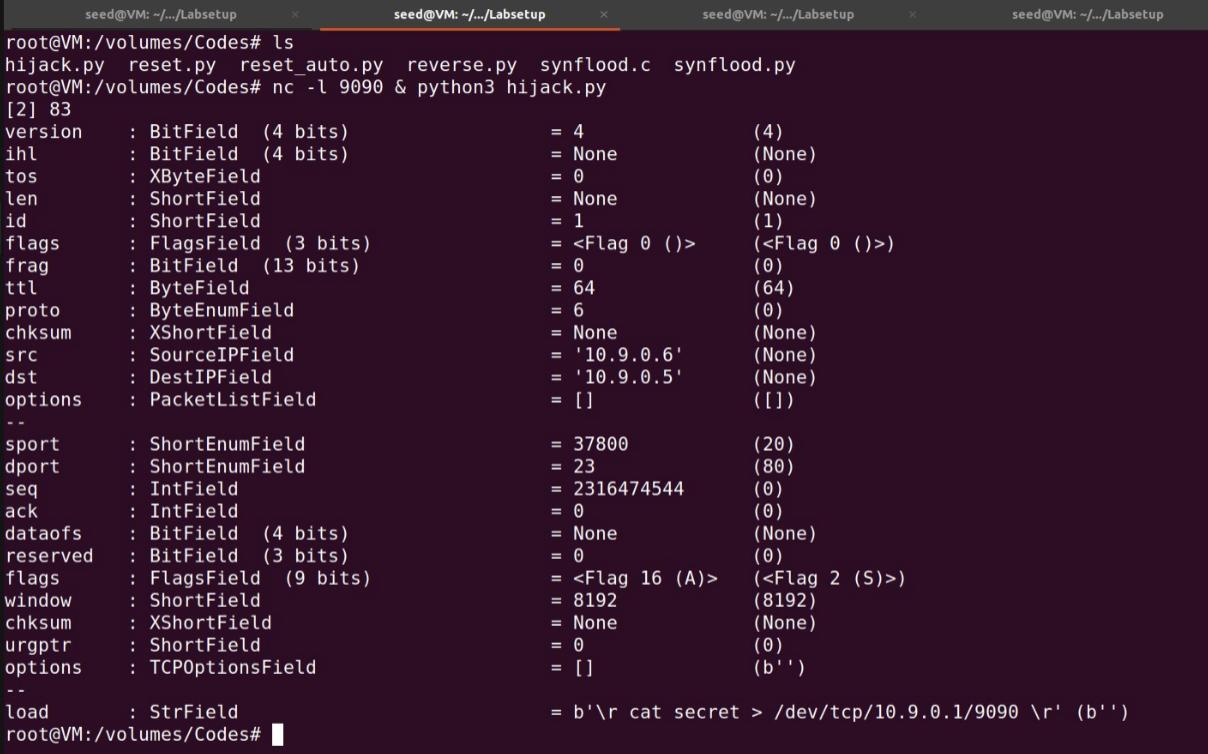
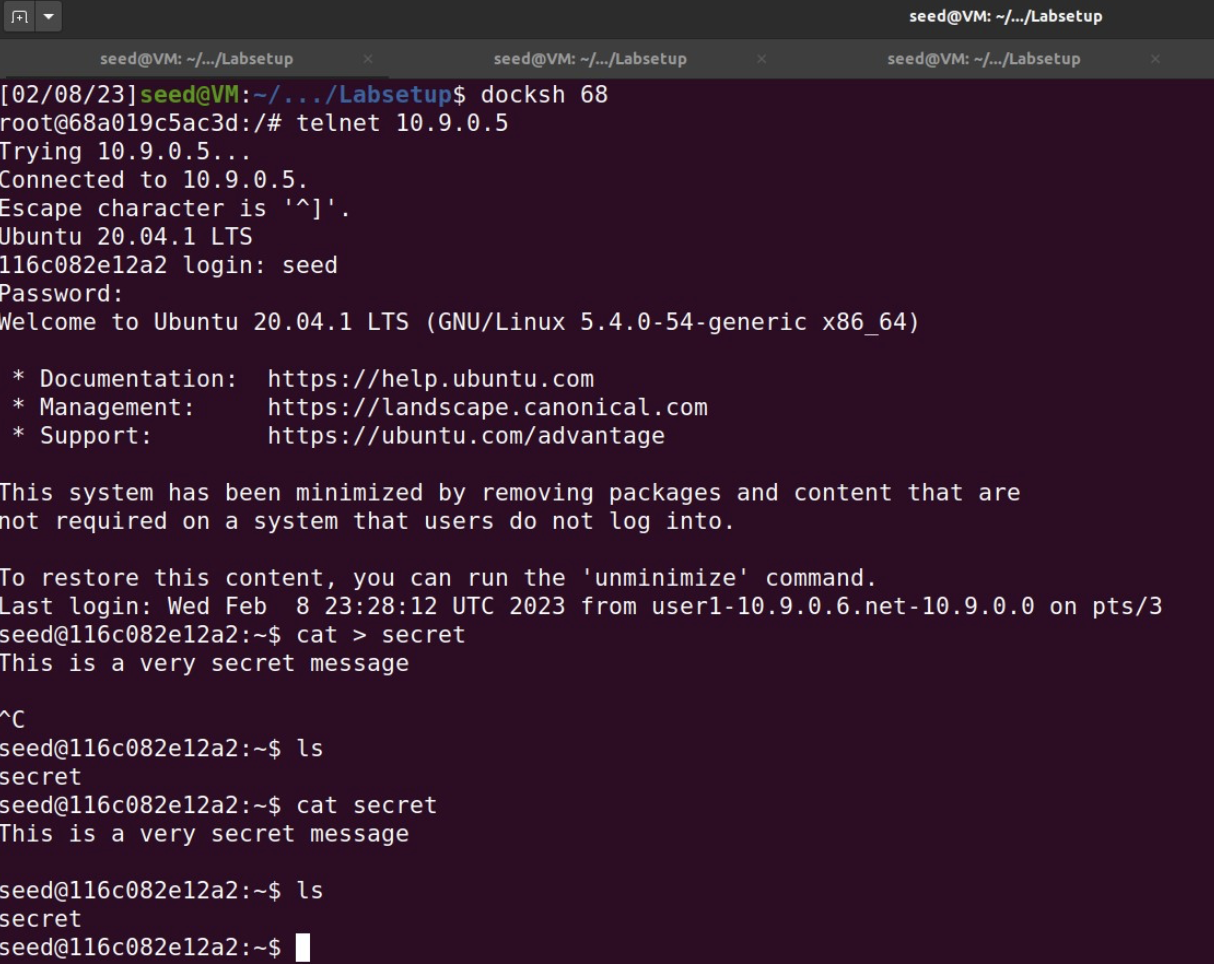
Code:  


Result:  


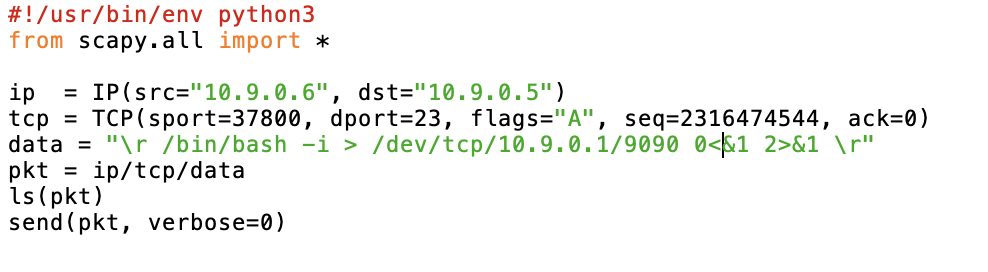
Observation:  
We were able to look into the connection using wireshark to fill sport and seq values. The target port is 23 for telnet and for reset flag is ‘R’. We used attacker to reset connection between other two system.

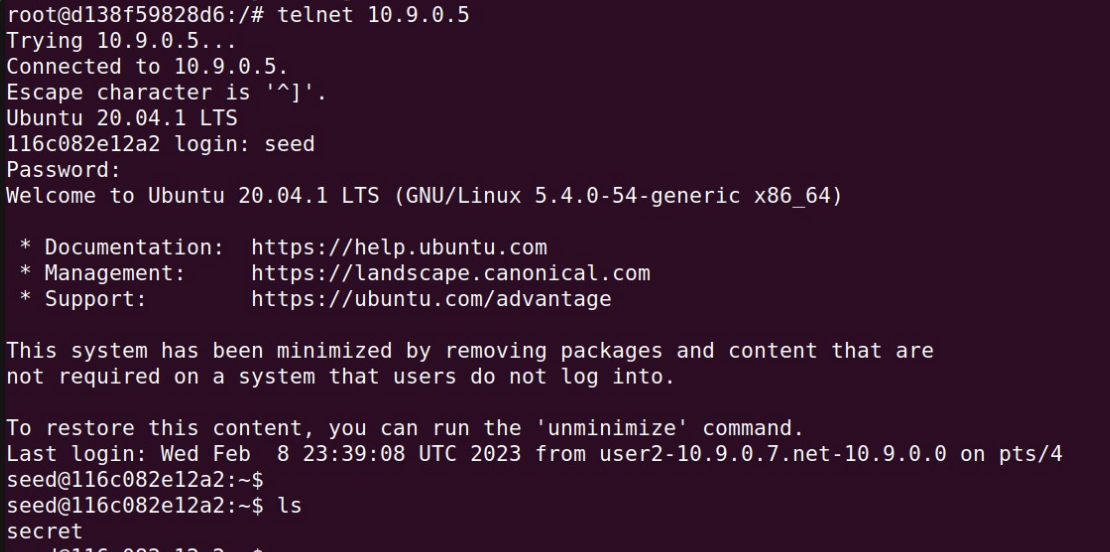
**Task 3**

Code:  


Result:  


Observations:  
Using wireshark we put values for sport, seq and ack. The victim is 10.9.0.5 with source from 10.9.0.6. This way we can redirect value of secret file to 10.9.0.1 port 9090.

**Task 4**  
Code:  


Result:  


Observations:  
Now we can run commands in victim machine and see output in our machine using the reverse shell.