ATTACK DEFENSE

by PentesterAcademy

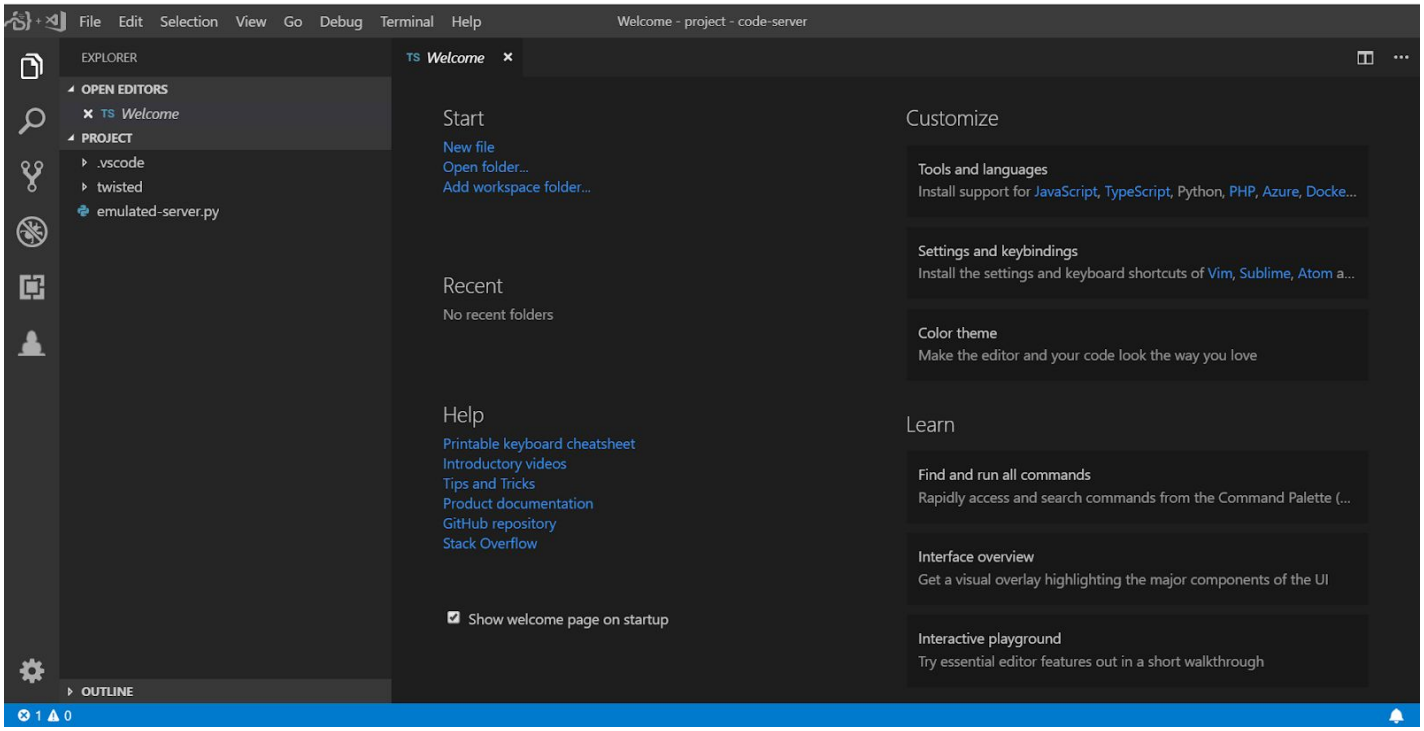
Name	SSH Server Emulation
URL	https://attackdefense.com/challengedetails?cid=1213
Type	Offensive Python : Server Emulation

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

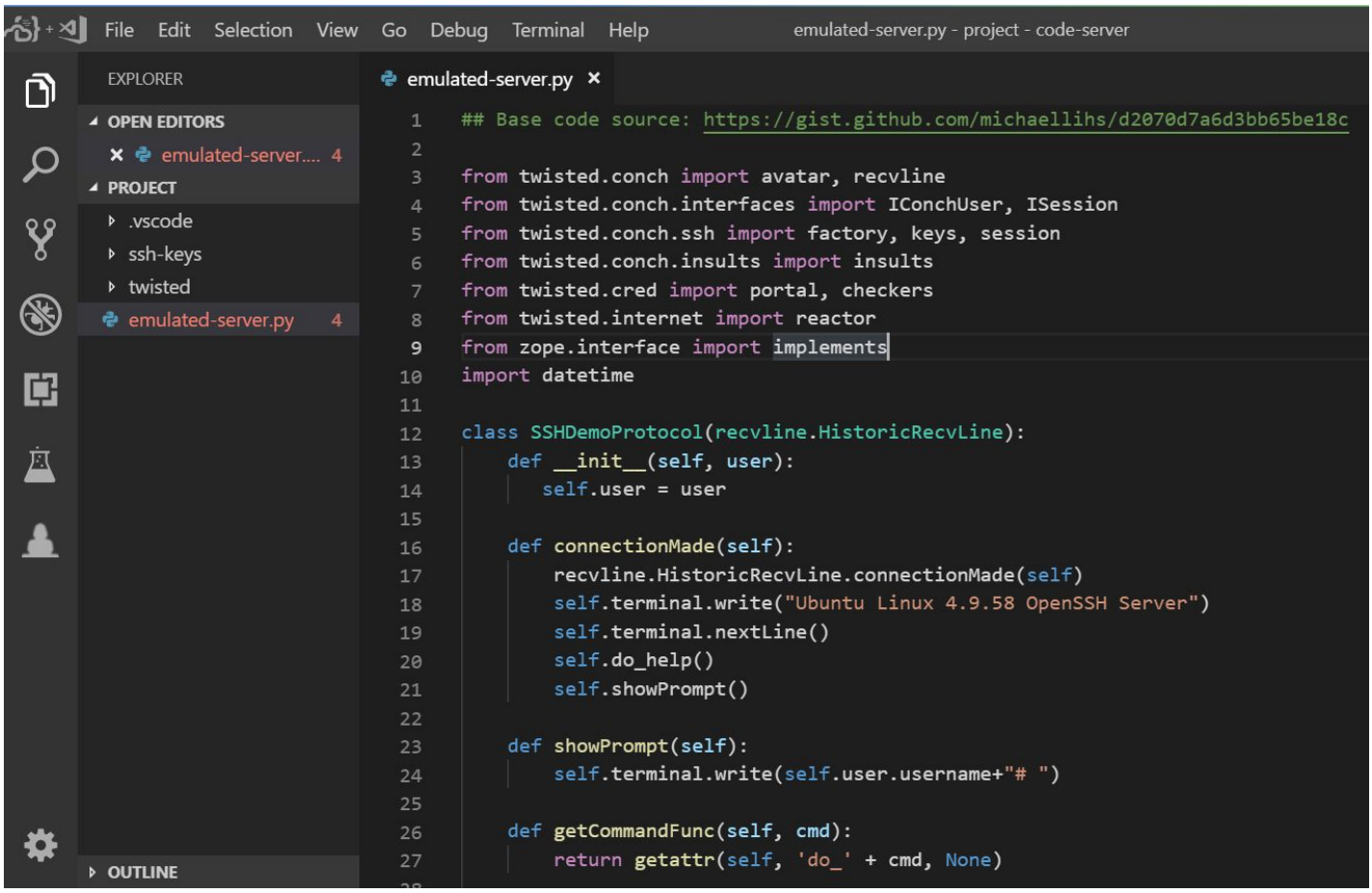
Objective: Modify the code, launch the server and use Kali Linux to interact/attack it.

Solution:

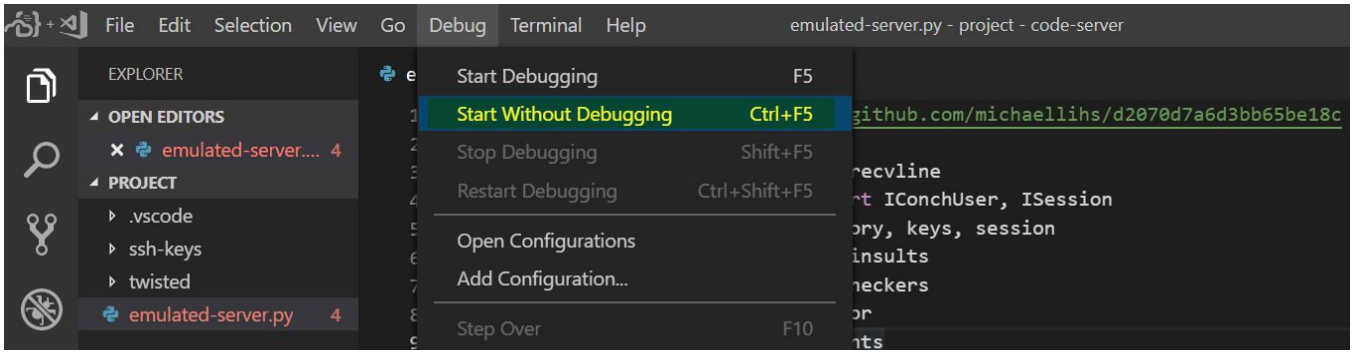
Landing Page:



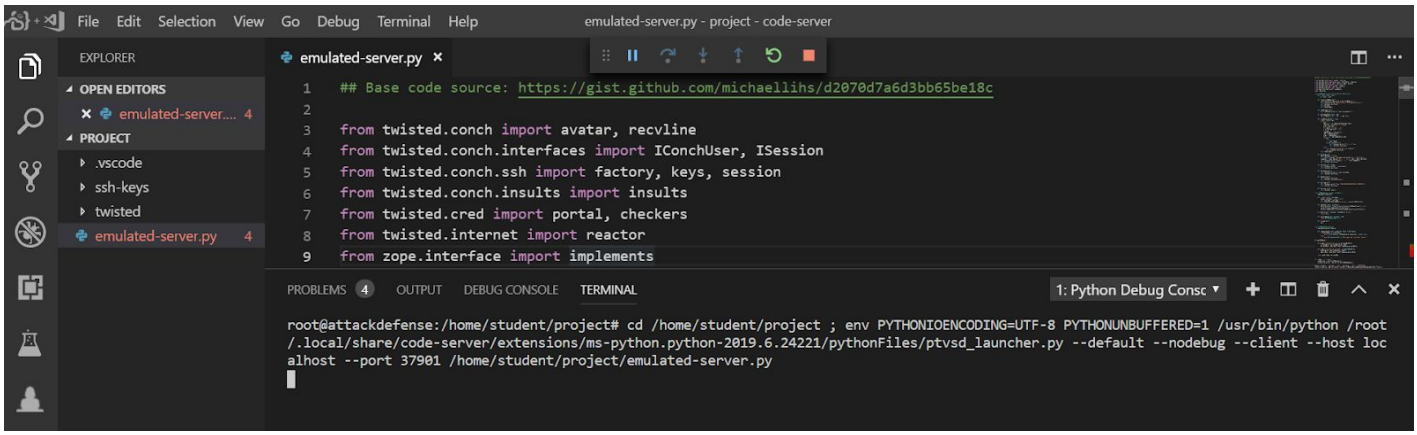
Step 1: Select “emulated-server.py” from the Project Explorer.



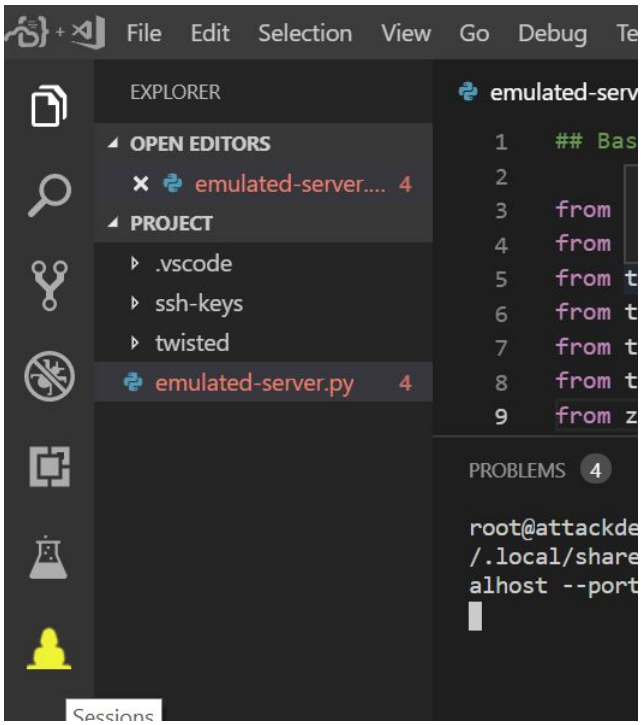
Step 2: Navigate to Debug Menu and click on “Start Without Debugging option” to run the program.



The python script will run and start an SSH Server on port 22.



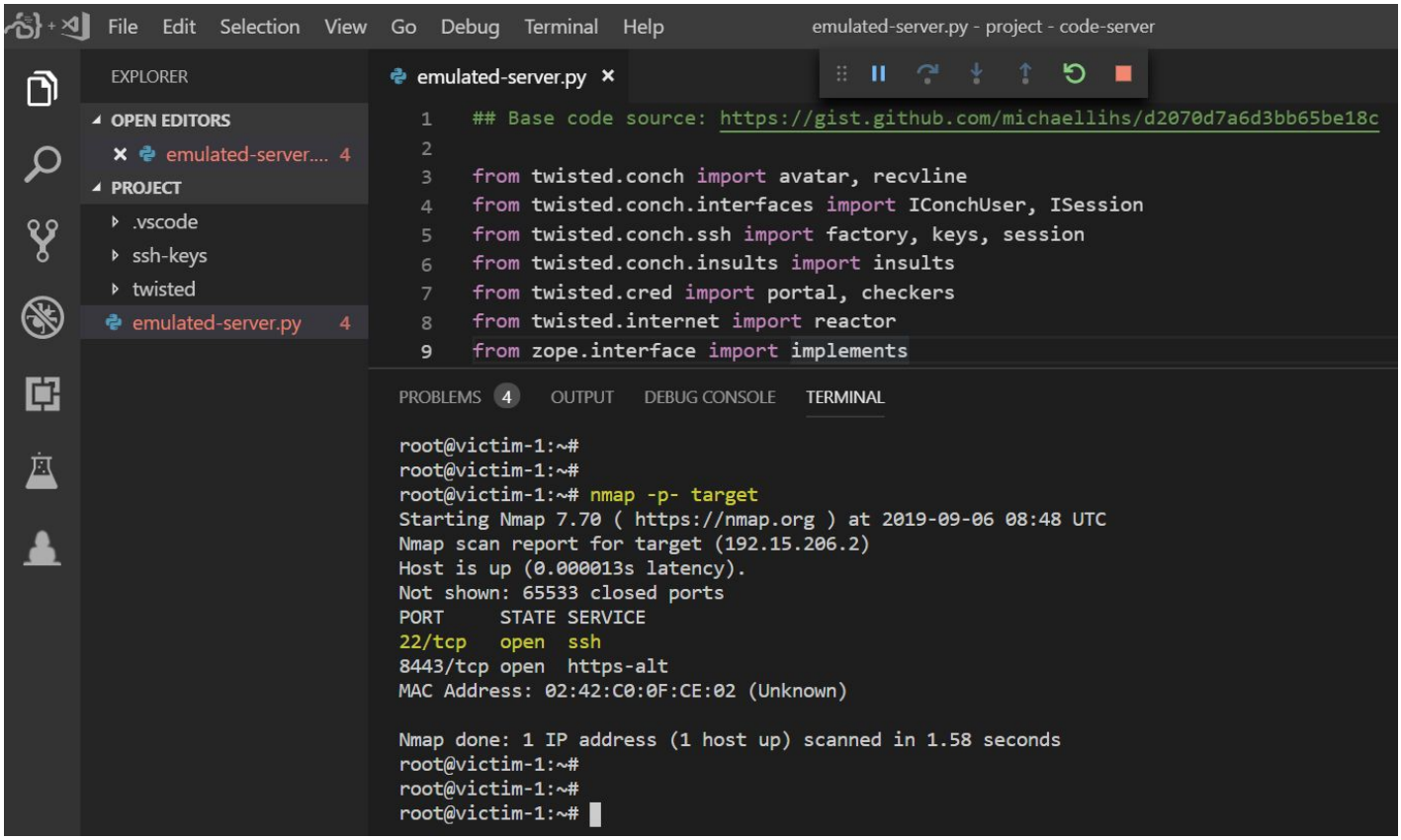
Step 3: Click on the “Sessions” icon on the activity bar to gain access to Kali machine.



This will spawn a new Terminal “Session 1” which will provide a bash shell on a remote Kali machine.

Step 4: Perform Nmap scan from the Kali machine. Identify the services running on the machine on which the IDE (and code) is running. The IDE machine is mapped to “target” hostname. So, “target” can be used while launching scans or tools on this machine. Alternatively, the IP address of the both machines can be found by running “ip addr” command on respective machine. The IDE machine should be on 192.x.y.2 and Kali machine should be on 192.x.y.3.

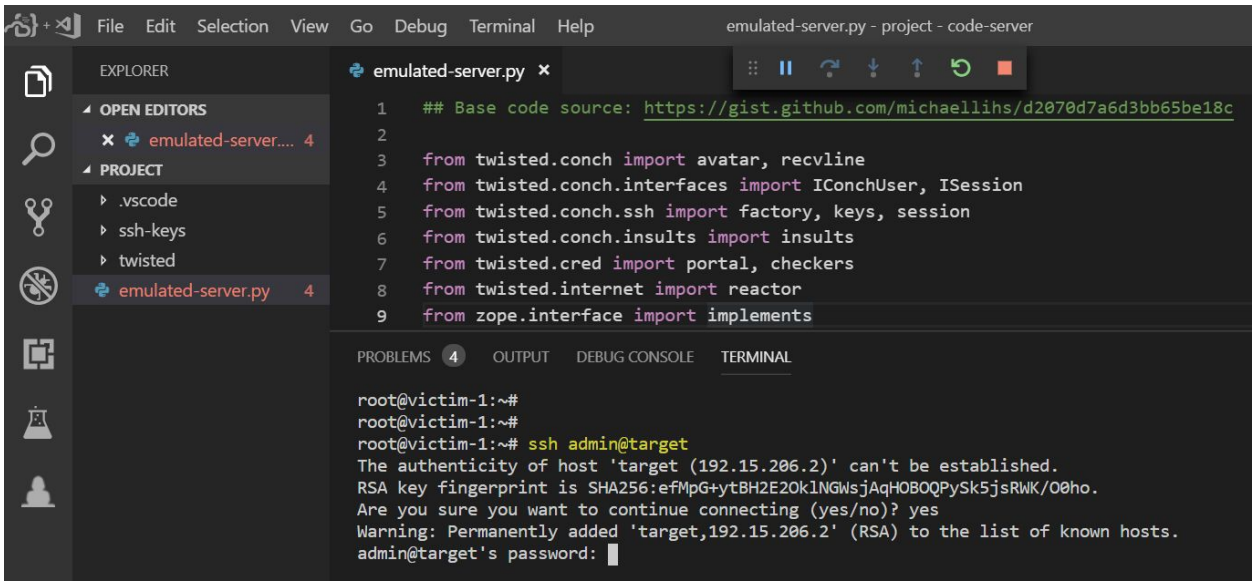
Command: nmap -p- target



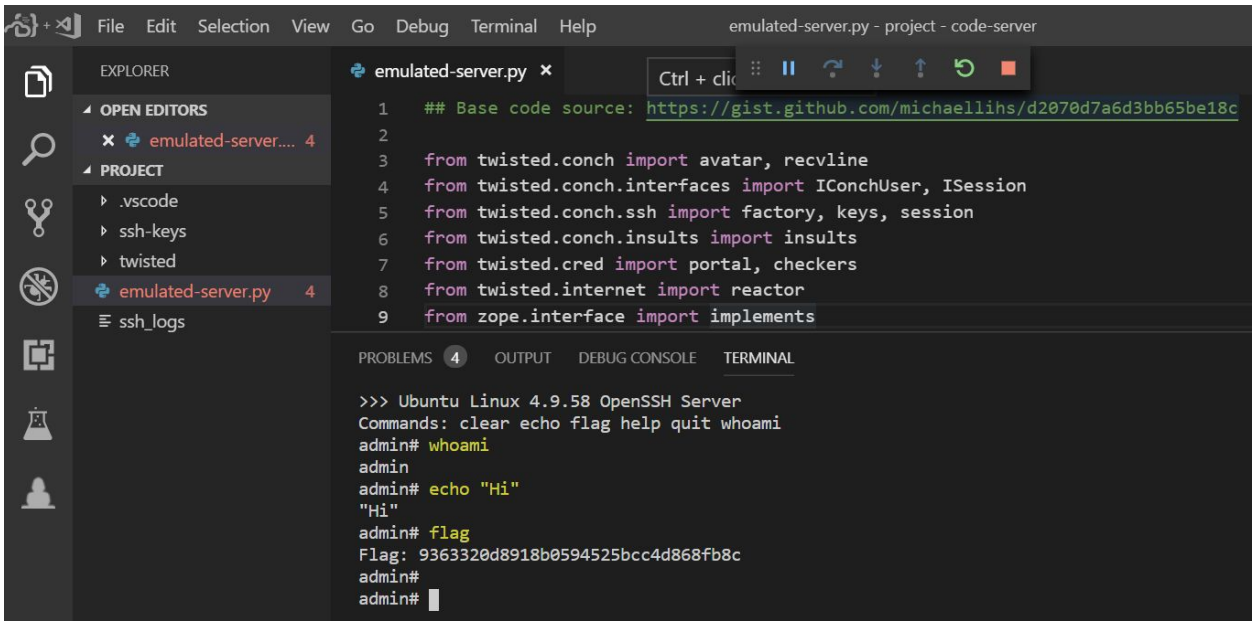
SSH server is running on port 22 on the target machine.

Step 5: Login to SSH server using username “admin” and password “welcome”

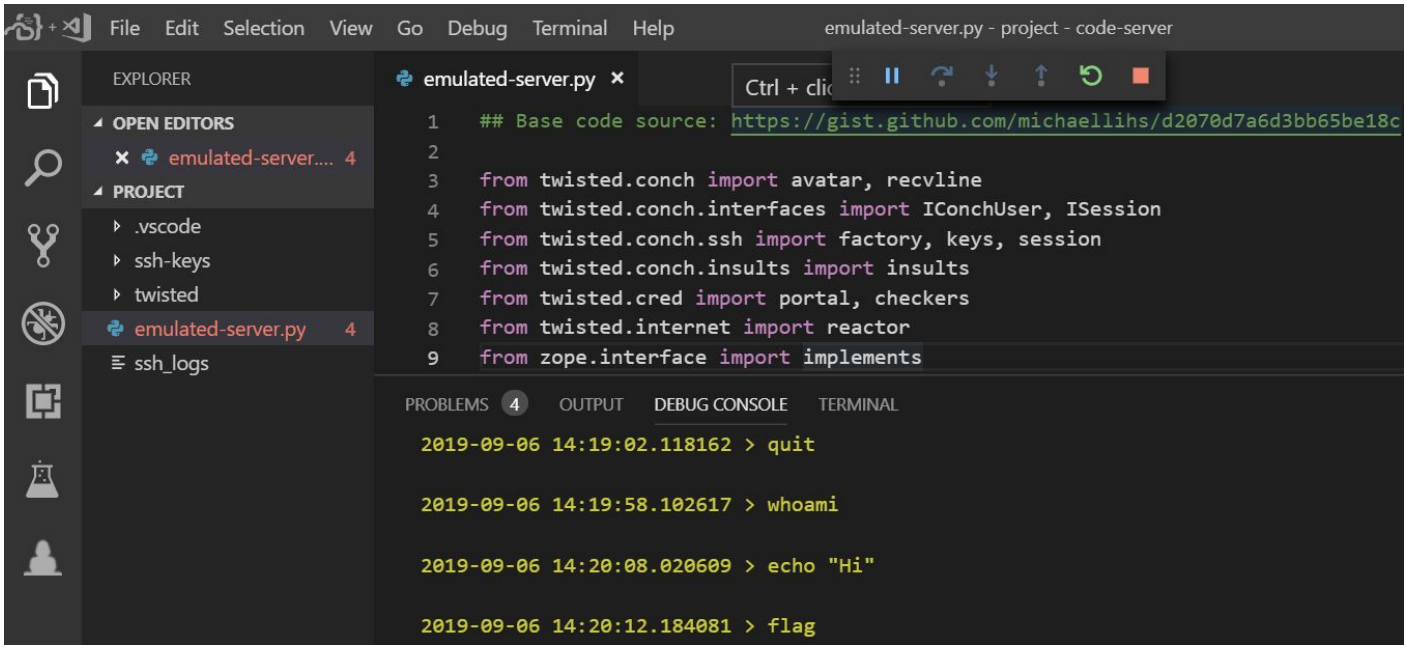
Command: ssh admin@target



After successful authentication, a custom shell will be provided to the user on which custom commands can be executed.



Step 6: On debug console, the interactions with SSH server can be viewed.



References:

1. Visual Studio Code (https://code.visualstudio.com/)
2. VS Code Basic Editing (https://code.visualstudio.com/docs/editor/codebasics)
3. Twisted (https://www.twistedmatrix.com/trac/)