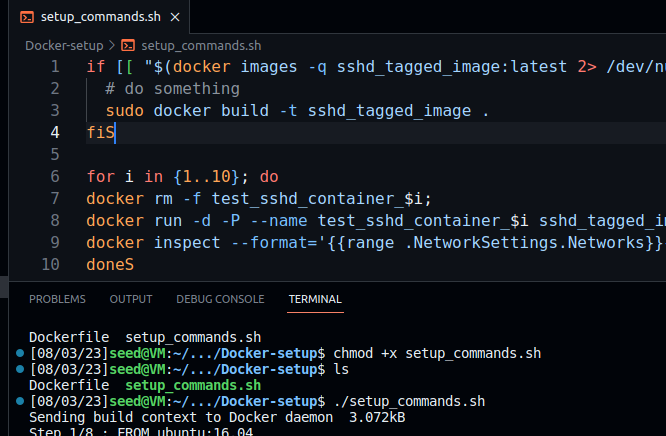
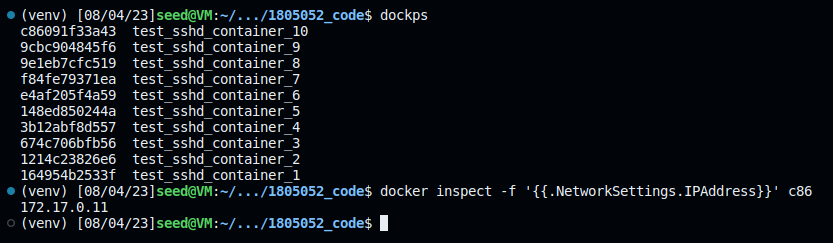
Docker setup

Create docker containers



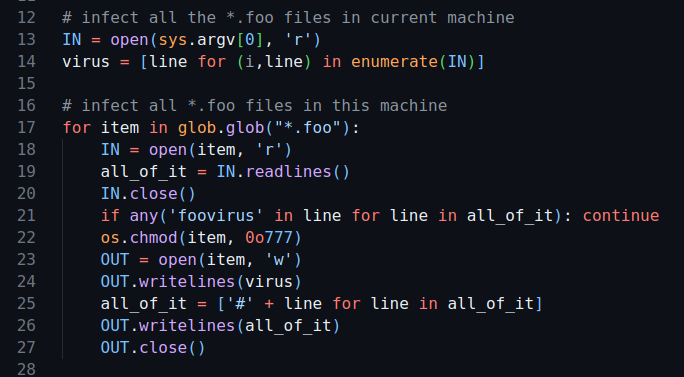
Now we can see the containers and their ip address.



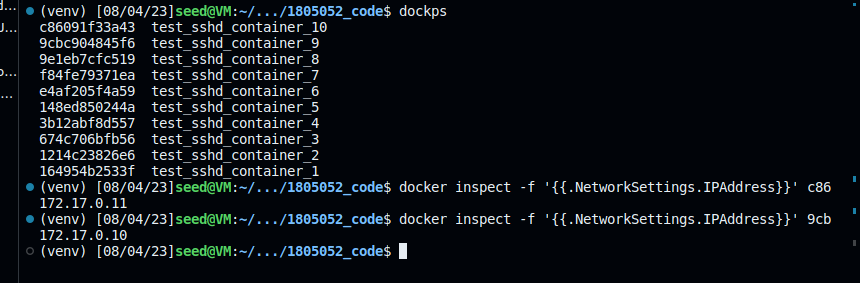
Task1

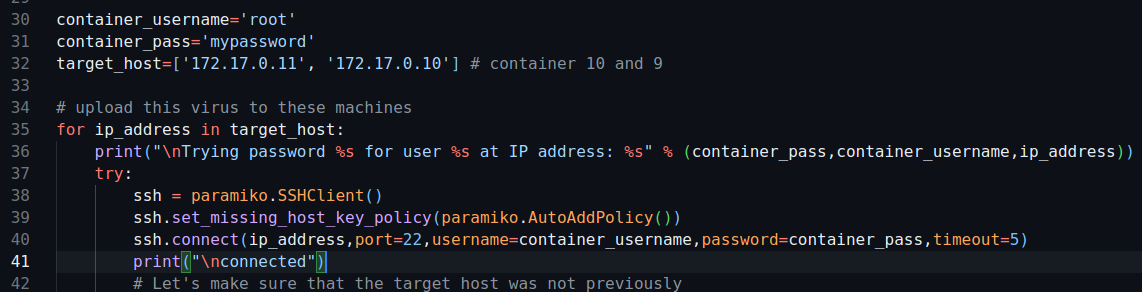
***Taking cues from the code shown for AbraWorm.py, turn the FooVirus.py virus into a worm by incorporating networking code in it. The resulting worm will still infect only the ‘.foo’ files, but it will also have the ability to hop into other machines.***

Step-1: Copy everything from FooVirus.py to infect all ‘.foo’ files in host machine.

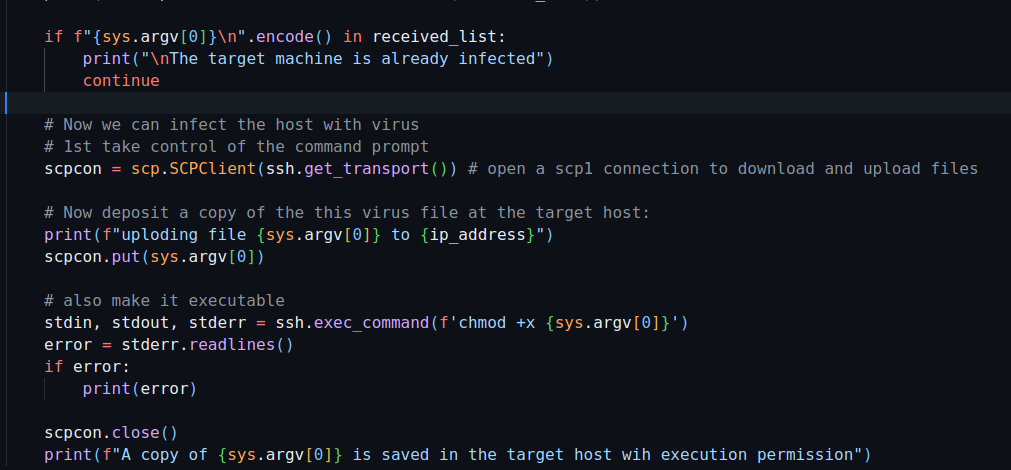


Step-2: Then we connect to two host(test\_sshd\_container\_10 and test\_sshd\_container\_9) to infect them with our worm

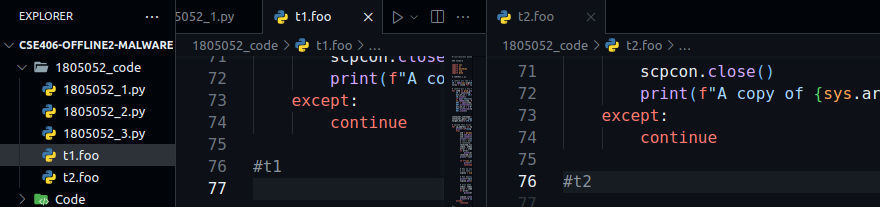


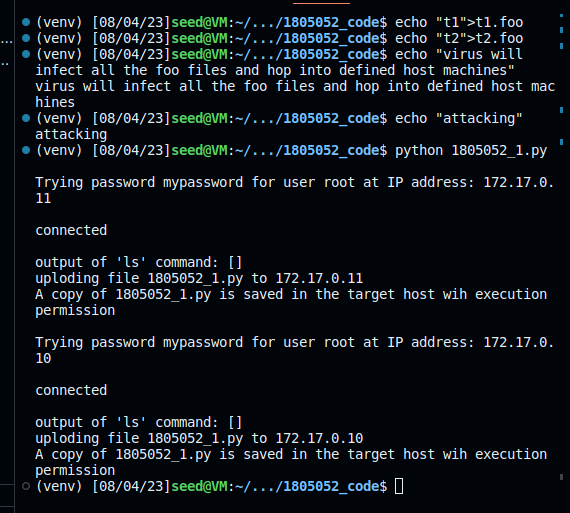


Step-3: if the machine not infected, copy the worm to the host.



# Attacking the host



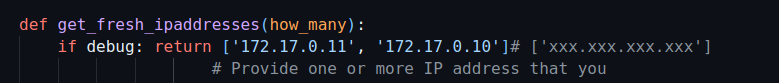




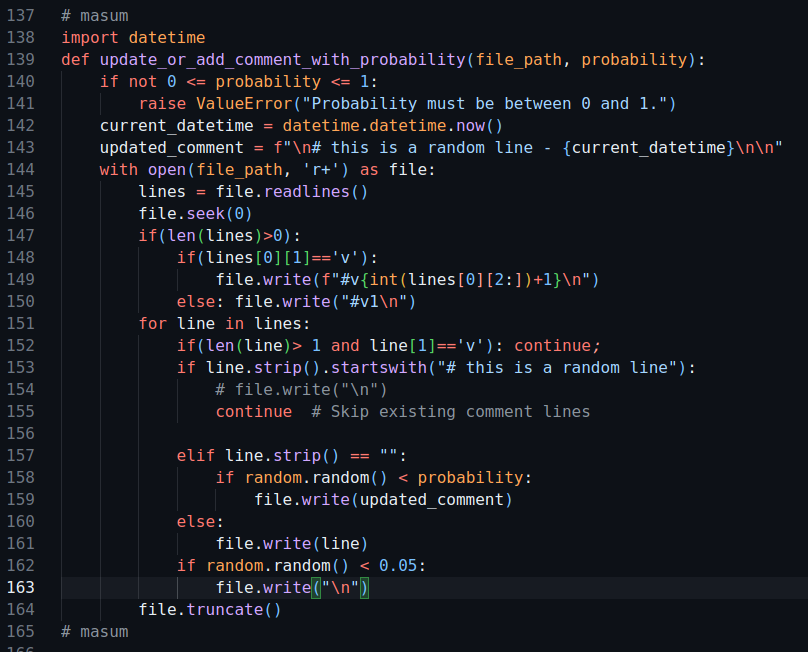
**Task 2**

***Modify the code AbraWorm.py code so that no two copies of the worm are exactly the same in all of the infected hosts at any given time.***

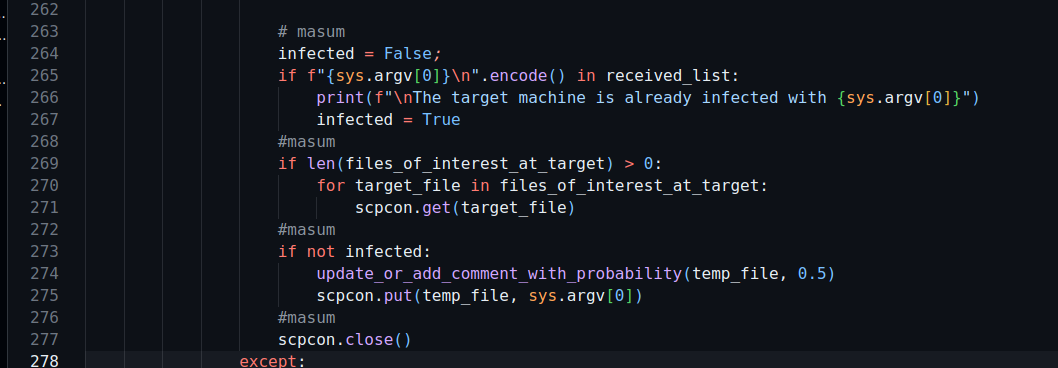
Step-1: Copy AbraWorm.py to a new file 1805052\_2.py. Also specify the victims ip addresses



Step-2: Define a function to add some comment to random lines and also add version of the top with current datetime so that no two copies of the worm are exactly the same.

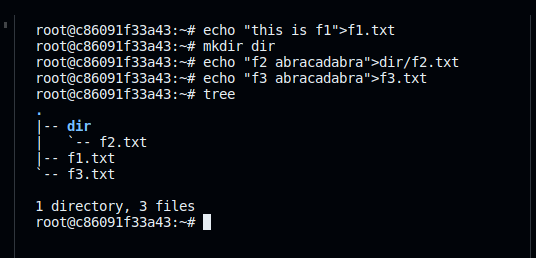


Step-3: Update the file before each hop

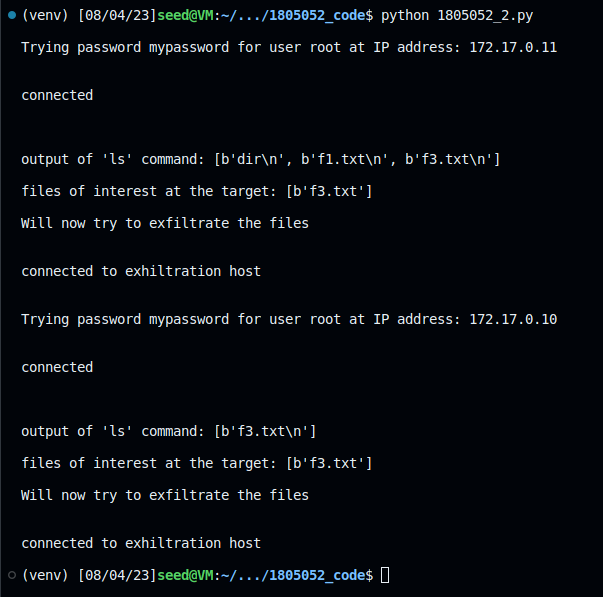


# Demo Attack

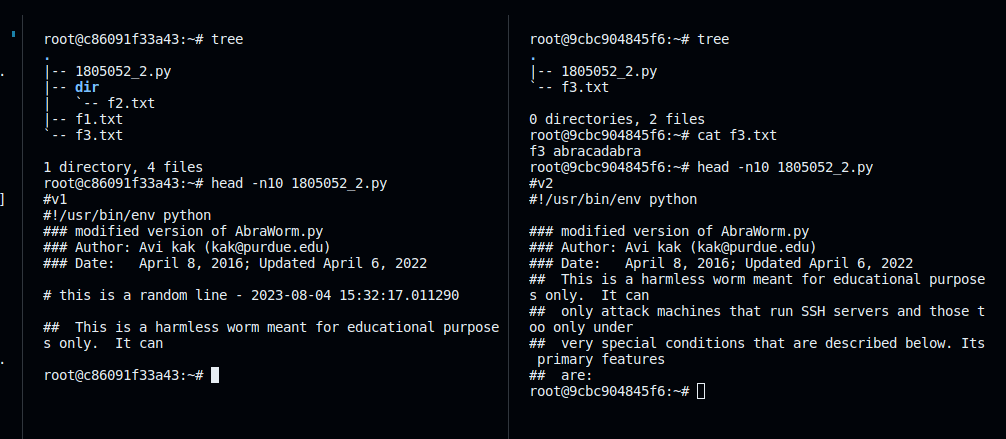
Create some dummy text files with abracadabra in some of them in container test\_sshd\_container\_10(c86091f33a43) which has ip address 172.17.0.11



Now perform the attack.



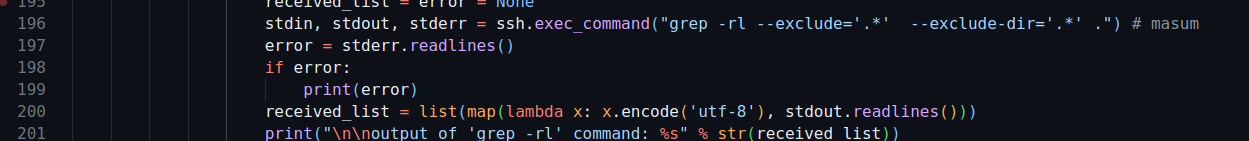
We can see the worm is copied to host 172.17.0.11(c86091f33a43) and 172.17.0.10(172.17.0.11) and by printing 1st 10 line of them worm we can see they are different.



**Task3**

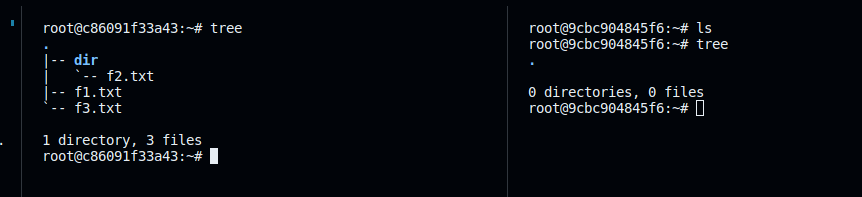
***If you examine the code in the worm script AbraWorm.py, you’ll notice that, after the worm has broken into a machine, it examines only the top-level directory of the username for the files containing the magic string “abracadabra.” Extend the worm code so that it descends down the directory structure and examines the files at every level.***

Modification in AbraWorm.py

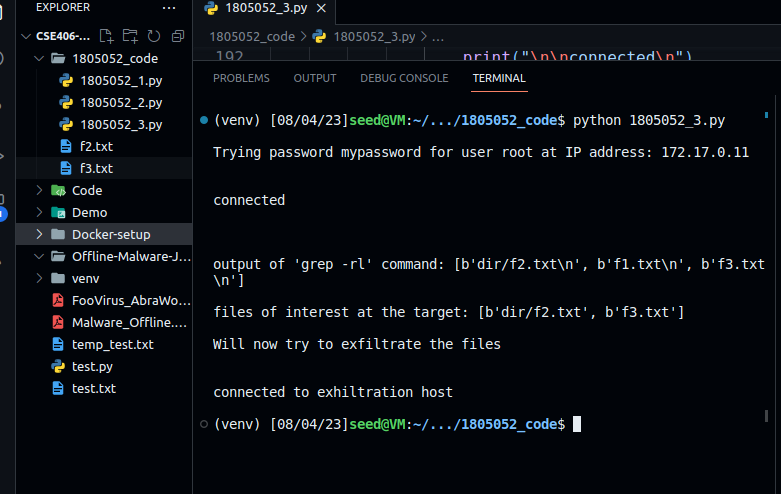
The only major change is the command that is executed in the victim’s machine to grep all the files recursively 

# Attack Demo

Two to host 172.17.0.11(c86091f33a43) and 172.17.0.10(172.17.0.11) before attack



Perform the attack.



Hosts after the attack

