Assignment on Malware

Submitted by

Siam Al Mujadded

Student id: 1805051

section: a2

level-4 term-1

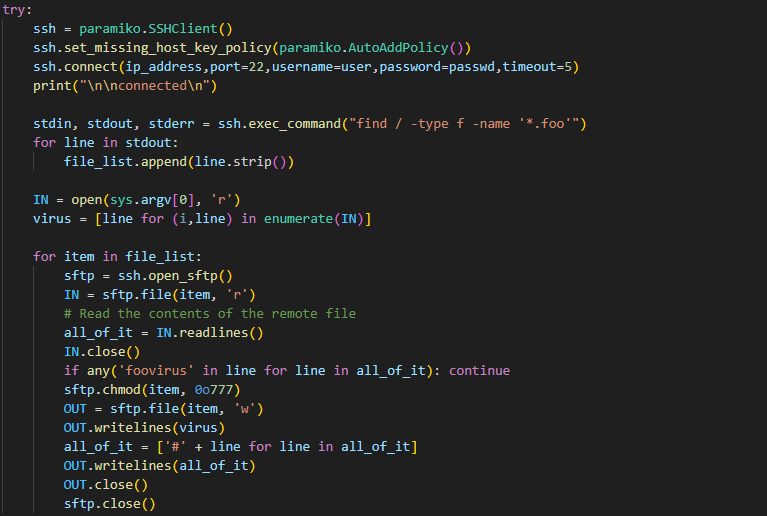
department: cse

Date: 04/08/2023

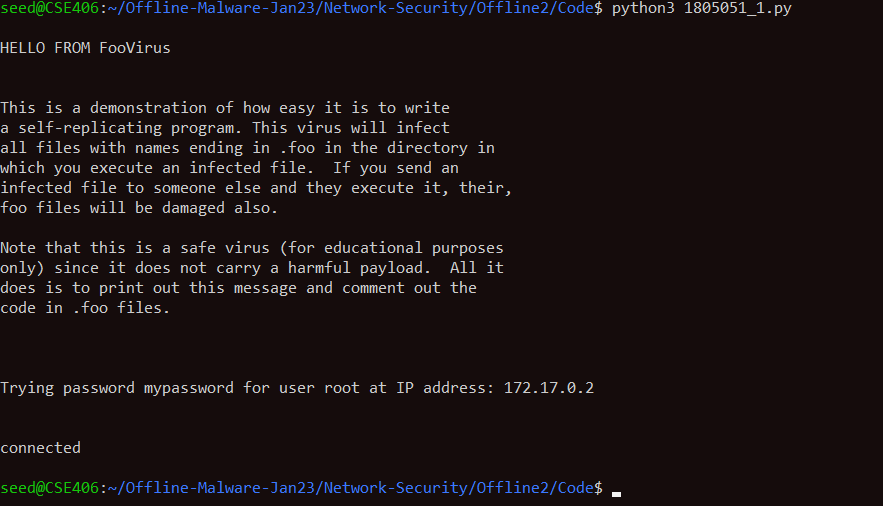
2023

# Task 1:

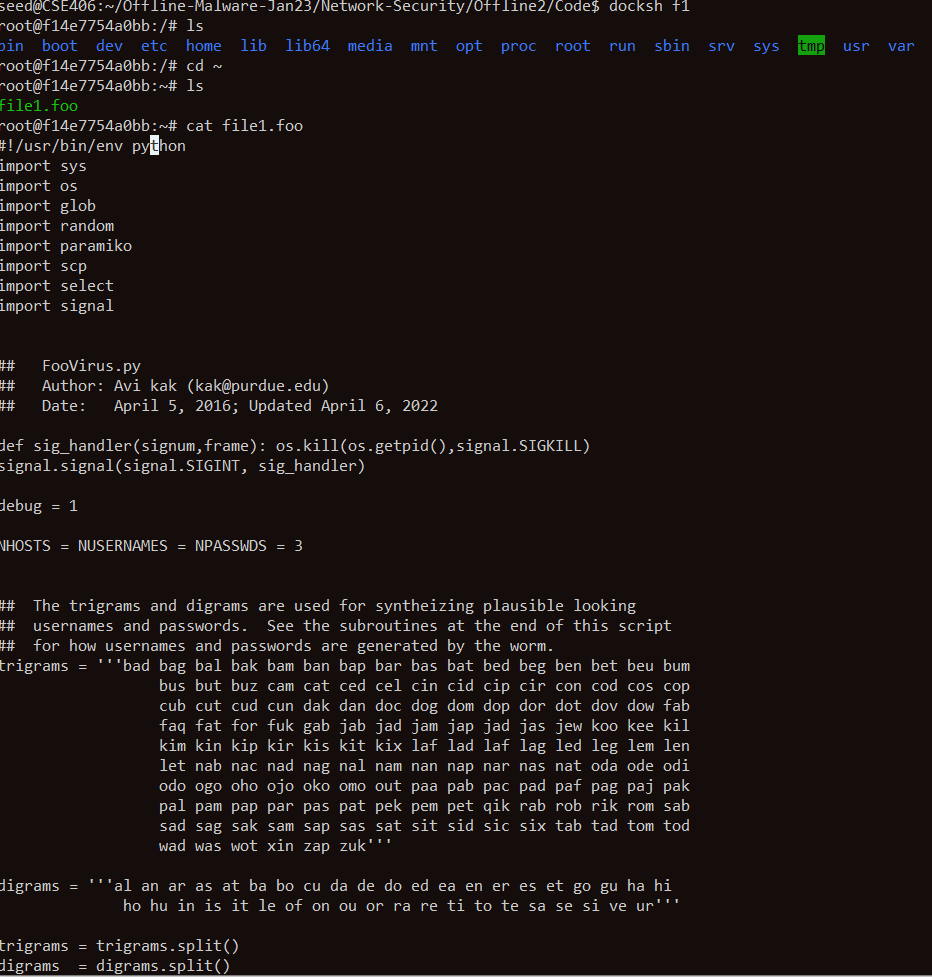
First, I copied the networking code from Abraworm.py file to Foovirus.py file and inside try catch block modified the code like the given code snippet.



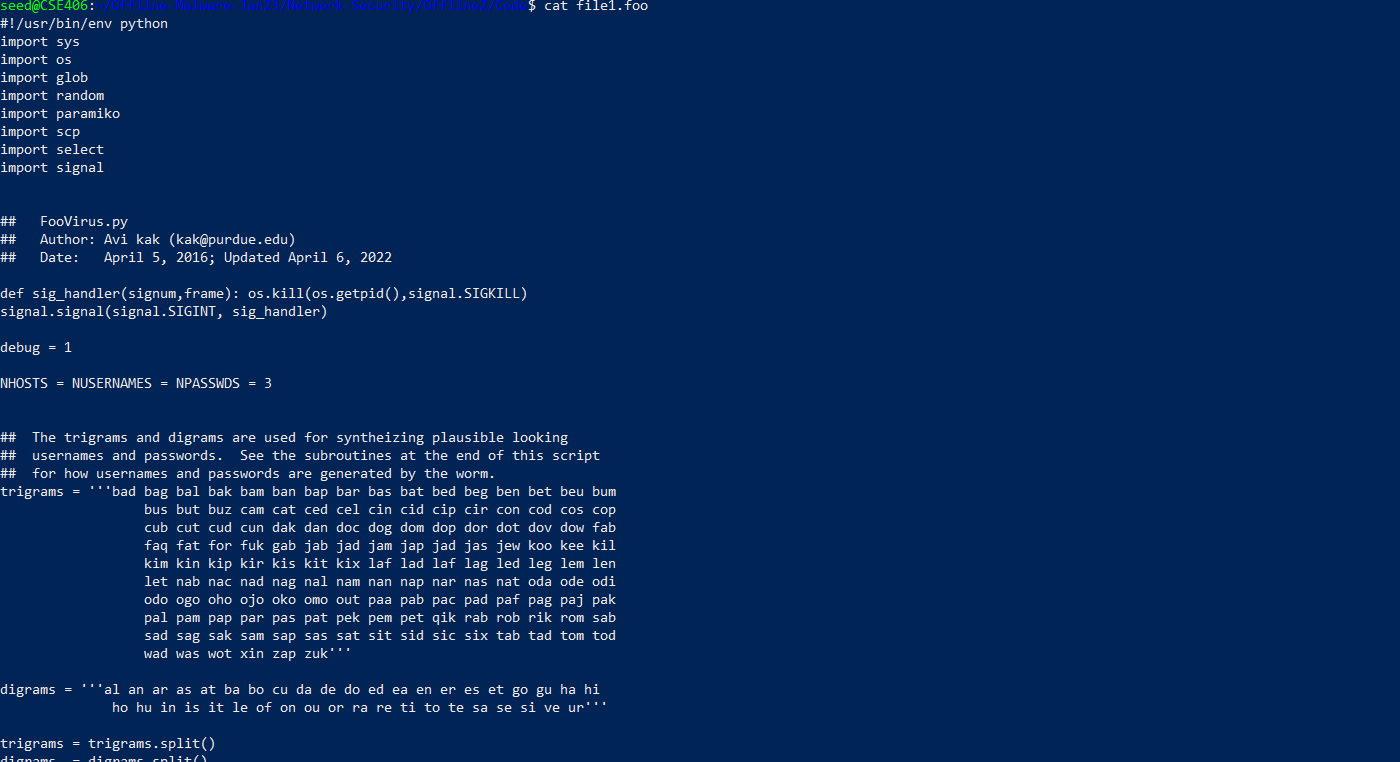
Here, using sftp I scanned for all the files in the remote machine that has the extension .foo and modified them accordingly. Also, in the local machine from where the program was first run if the local machine contained any file with extension .foo was affected and was runnable as a clone of the virus. Below screenshots of the demonstration are given.



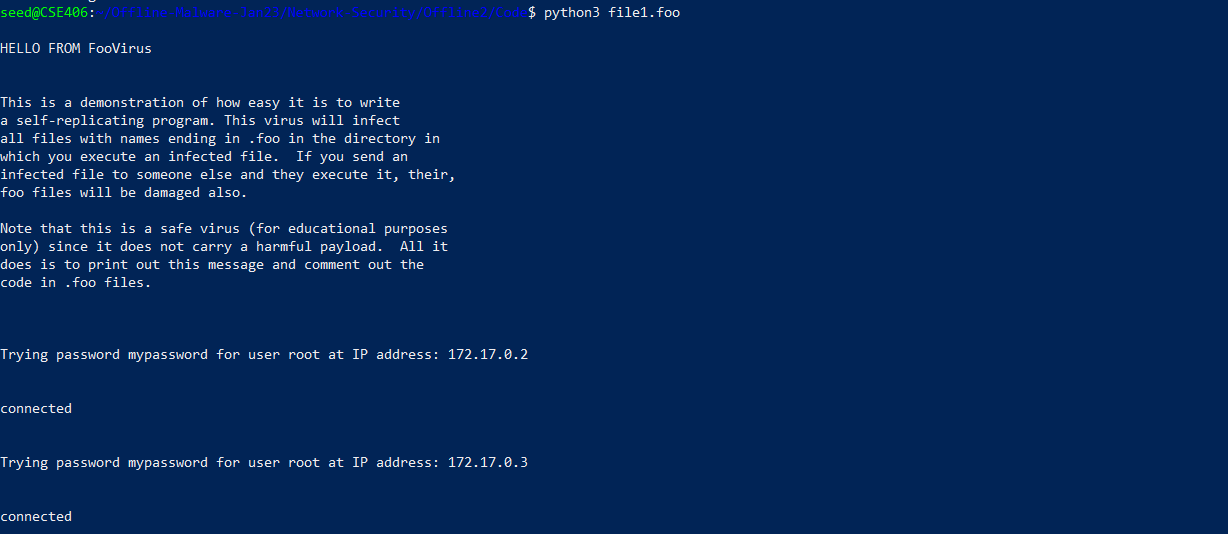
First time when the virus was run from the local machine.



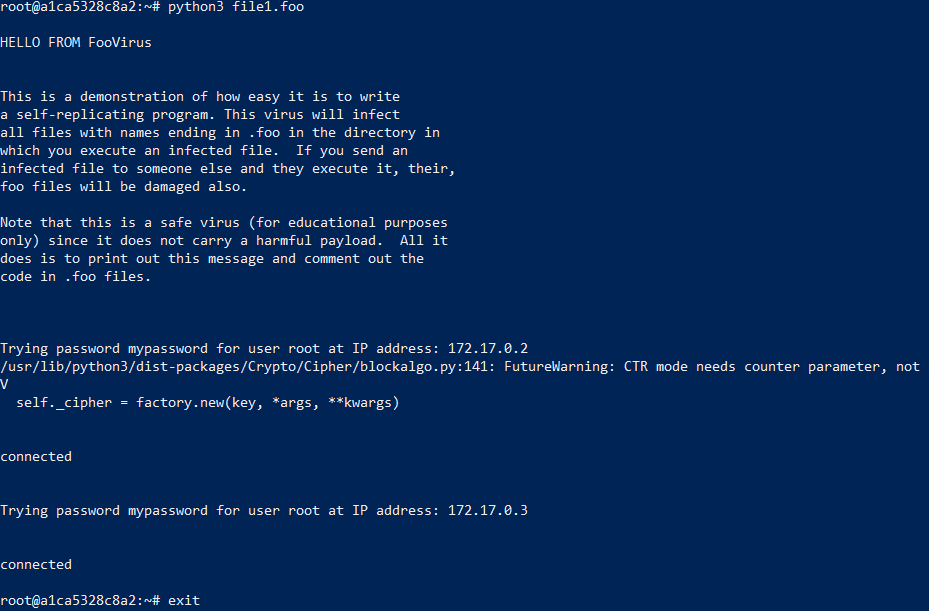
Modified a file with extension .foo in a remote machine.



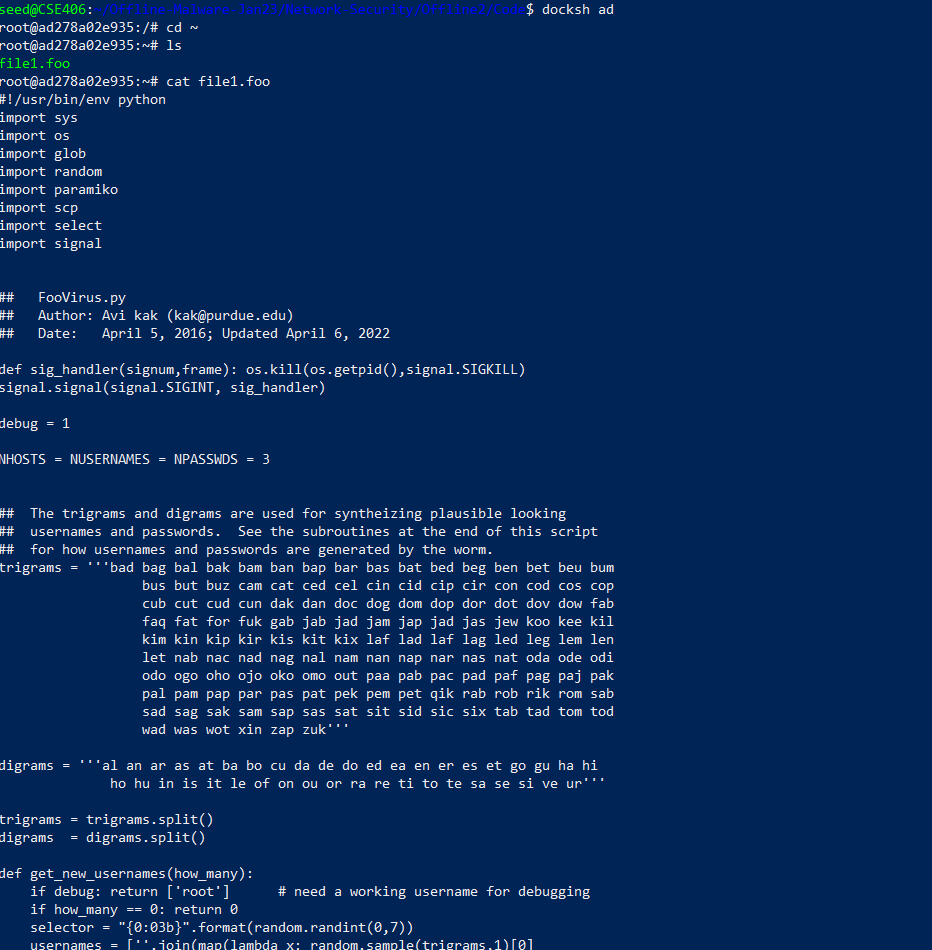
Files in the local machine are modified and made executable also.



Running the modified files.



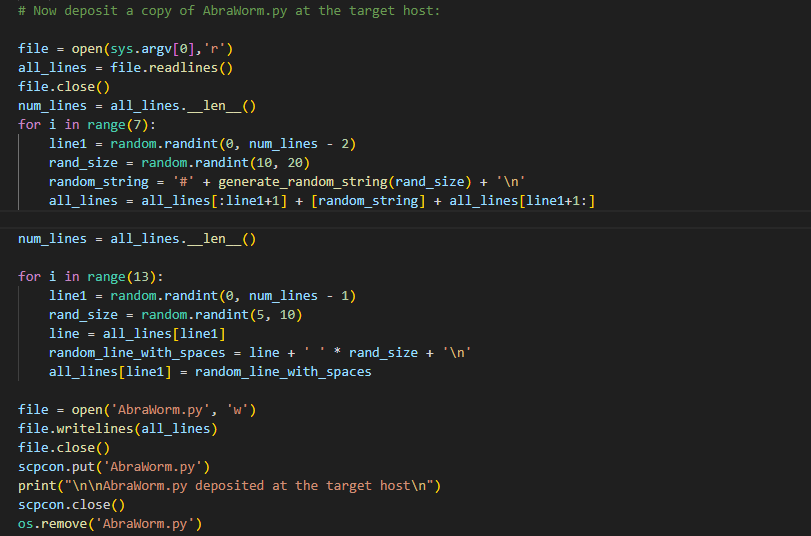
Running modified file from a remote machine.



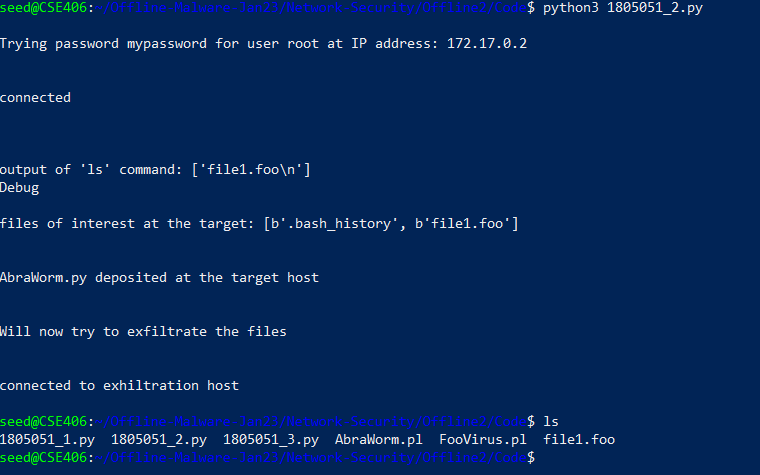
Program ran in remote machine1 modified the file having extension .foo in remote machine2.

# Task 2:

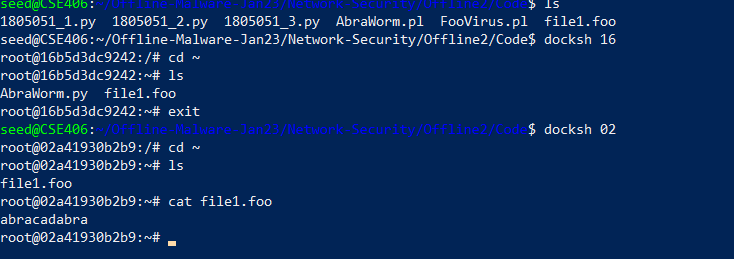
For this task I modified the code below the line - “ # Now deposit a copy of AbraWorm.py at the target host: ”. The code snippet is given below.



Here, to have different signatures of the worm in each machine, I added 7 random strings in between two randomly chosen lines of the source code file and all of the lines are comments. Also, in 13 randomly chosen lines I added random numbers of spaces between 5 to 10 inclusive. Both these techniques keep the logic indifferent and the worm works as it does in any other machines. Below the working example’s screenshots are provided.



Worm is run from local machine and installed itself in remote machine “container1” and the files containing the string “abracadabra” are being exfiltrated to another remote machine “container2”.



AbraWorm is installed in the remote machine1 and the file “file1.foo” is exfiltrated to machine2. Also the signature of the file AbraWorm.py is different than the one in the local machine.

# Task 3:

For task 3, I changed the cmd variable inside the infinite while loop of the code for task 2. Also in the last if clause of the loop I used “os.path.basename(filename)” to exfiltrate the files that contain “abracadabra” in a designated machine. The code snippets are given below.

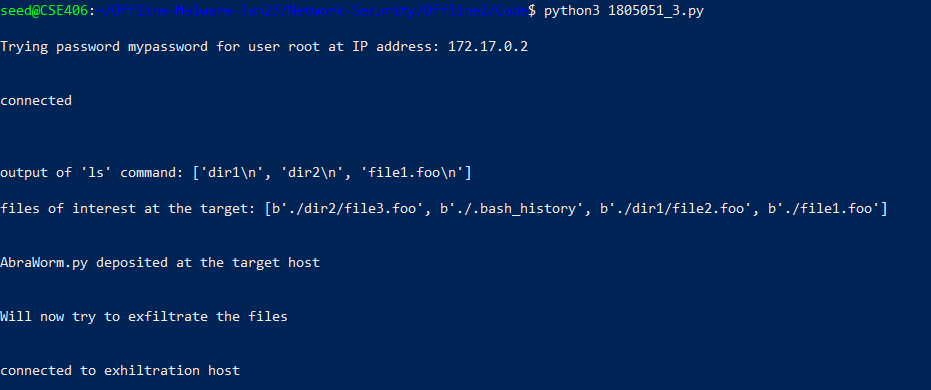


This command searches the directory for the target files recursively.



This method gets the base name from the full path of the file name and installs it in the remote machine

Below the screenshots of a working example are given.



First time the worm is run from the local machine. Affects the remote machine 1. Machine 1 has 2 sub-directories in the root directory named dir1 and dir2 that contains file2.foo and file3.foo respectively with content “abracadabra”. Also, in the root directory a file named file1.foo is present it also contains “abracadabra”. So, these 3 files will be exfiltrated to remote machine 2 and AbraWorm.py will be installed in machine1.



Target files are exfiltrated to a designated machine.



AbraWorm is mounted in the target machine (machine1).

Note: All the examples were carried out in debug mode for demonstration purpose.