Lab 2 | CSE 3140 | Abdul Chowdhury (unable to communicate with partner asked TA said to work by myself) | amc20031 | ssh -L 127.0.0.1:8000:10.13.4.8:80 cse@10.13.6.41

Q1: In this python code (Q1C.py), the virus avoids reinfecting files by checking for the VIRUS_TAG (# officially infected). The function is_already_infected(file_path) makes sure that the tag is in the file, and if it is it skips it.

To limit code injection, the virus code is only appended to files that:

1. That both exist and are python files.
2. Contain a __main__ block (ensured by has_main_block).
3. Are not already infected (checked by is_already_infected).

The injected virus code is logged to Q1C.out, ensuring only the virus code is added to the target file.

Q2: The Q2Worm.py code scans for vulnerable machines by analyzing for open SSH (port 22) and Telnet (Port 23) ports. It tests credentials from Q2pwd to verify valid accounts once valid login is found it uses paramiko or telnetlib to remotely access the victim's machine and extract the files finally it infects the machine by injecting the malicious code through an established connection.