Layla Nassar & Mohammed Kabir
Section 003
CSE 3140
IP Address: 10.13.6.145, 10.13.6.92
NetID: LTN2200, MTK21002

CSE 3140: LAB 2 REPORT (Malware)

Q1: Explain how your Q1C.py script functions. Describe the method used to prevent reinfecting scripts that have already been infected and how you ensure that only the necessary virus code is injected.

Our Q1C.py script is a self-replicating Python virus that scans the directory for .py files, infects uninfected ones by appending its own virus code, and executes a payload that logs script executions to Q1C.out. To prevent reinfection, the script checks for a unique marker (# VIRUS_START) within each file before injecting the virus, ensuring it is only added once. The infection process is limited to only the necessary virus code by extracting and appending only the portion between # VIRUS_START and # VIRUS_END, keeping the target script's original functionality intact. This controlled injection method prevents code duplication while maintaining proper execution, allowing the virus to spread effectively without breaking infected scripts.

Q2: Explain how your worm code determines machine vulnerabilities, verifies victim credentials, extracts files via SSH/Telnet, and infects the victim machine.

Our Q2worm.py script is a network-based worm that scans a subnet for machines with open SSH and Telnet ports, attempting to identify vulnerable targets. It determines whether a machine is vulnerable by systematically probing IP addresses in the 10.13.4.0/24 subnet and checking if ports 22 (SSH) or 23 (Telnet) are open. Once a vulnerable machine is found, the worm verifies victim credentials by attempting authentication using a list of known username-password pairs from the Q2pwd file. If successful, it proceeds to extract sensitive files, such as Q2secret, using SSH file transfers

(SFTP) or Telnet commands. After exfiltrating data, the worm infects the victim machine by copying itself onto the compromised system and executing the script, allowing it to spread further. By leveraging weak credentials and unprotected network access, our Q2worm.py efficiently propagates across multiple machines while remaining stealthy in its execution.

Q3: No lab report submissions needed.

Q4: No lab report submissions needed.

Q5: No lab report submissions needed.