● Item 1 (10%) : Please describe how you finished Task I

We find out the location of the worm to be in “/etc/crontab”, which is “/home/victim/Public/.Simple_Worm/”. Then we discover a file named “crack_me.log” inside the folder, so we decrypted the file with XOR stream cipher and found out the key is \x85. Finally, we encrypted the file task1_result.log containing our verification_flag with the key using the stream cipher again.

● Item 2 (10%) : Please propose three security settings in SSH server that can prevent common dictionary attack

1) Strengthen your password requirements

2) Use SSH keys and disable password authentication

3) Failed Login Attempts Lockout

● Item 3 (10%) : Please explain why Linux differentiates crontab into three types (users, system and applications).

User type: Allows the user to run a specific task under a certain period

System type: Allows specific user to run a specific task under a certain period

Application type: Allows specific GUI application to run on a specific display under a certain peroid