Computer Security Project 3 **0716055 王耀德**

0716074 蔡育呈

【Item1】How you finished Task I

First, we used “htop” to detect a file named “Loop_ping” in a folder called “Simple_worm”, which was very active. Then, we went to that file and found some suspicious filename in it including “XOR_Encrypt”, ”Loop_ping”. We also discovered that all the files on Desktop were encrypted. Then we open the XOR file and try to decrypt it. The method we took was to try all the possible keys by a loop in Python. Finally, we got the key and decrypt it successfully. After that, we modified the plaintext and mark my student ID and ciphered it.

【Item2】3 security settings in SSH server that can prevent common dictionary attack

1. Disable password-based authentication.

Dictionary attack is to make use of the common problem of user’s password. Hence, we can use only SSH public to login on every device without password.

2. Use different ports other than port 22.

Almost all dictionary attacks focus on the default port 22. Therefore, if we change port to another, it would be more secure.

3. Use stronger password.

Using a decent password will prevent almost all dictionary attacks since they can only try a list of common passwords.

【Item3】Why Linux differentiates crontab into three types

Linux differentiates crontab into three types because it need to clearly define the privilege of users. For details, “System crontab” is used by system services and critical jobs that requires root like privileges. This gives the system crontab the ability to run commands as any user. On the other hand, “User crontab”, users can install their own cron jobs using the crontab command, and all commands run as the user who created the crontab.