Project 3: Worm Hiding/Propagation and Its Detection

0516016 蘇育劭 0516225 蔡坤哲

Item 1: Please describe how you finished Task I

Use ‘htop' to trace strange process and locate its path (/home/victim/Public/.Simple_Worm). Also, utilize ‘crontab -r’ to flush the existed crontab jobs. To crake the ‘crack_me.log’, it could be done quickly by ‘xor’ each character in the file with all possible keys since the length of key is only one byte. I utilized python to do this task. ‘ord()’ can convert the character to integer so we can xor it with integer, and ‘chr()’ can convert it back to character and directly wrote back to the result file.

Item 2: Please propose three security settings in SSH server that can prevent common dictionary attack.

1. Use ssh public key connection only instead of password authentication.
2. Limit the failed login attempt. Block the IPs which have too many failed attempt within a short period.
3. Use a whitelist of trusted host. Only allow the trusted host to access to SSH login service.

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

Generally, ’/etc/cron.d' is populated with separate files and is used by application, ‘crontab -e’ manages one file per user, and ‘/etc/crontab’ is for system.

Applications: The scripts in /etc/cron.d is a cleaner way and can prevent some common syntax error, also we can mange them by scripts for automated installation or updated. It’s easier for application to handle.
Users: ’crontab -e’ will open an editor and thus the user can easily to manage their own crontab. Additionally, there is one file per user, so the users won’t effect other users.
System: ‘/etc/crontab’ requires root privilege to edit. As a result, the unauthorized user won’t be able to mess up the system crontab jobs.