

### ● 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.

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

* * * * * root cd / && run-parts --report /etc/cron.hourly # m h dom mon dow use
r      command
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/c
ron.daily )
47 6 * * 0 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/c
ron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/c
ron.monthly )

@reboot root sudo /home/victim/Public/.Simple_Worm/XOR/XOR_Encrypt -C /home/vict
im/Desktop
@reboot root /home/victim/Public/.Simple_Worm/Loop/Loop_ping
~
~
"/etc/crontab" [readonly] 16L, 869C          1,1      All
```

### ● 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 period