ICS

0516045

Item1.

I use command **htop** to monitor CPU usage and found out a program named Loop_ping in /home/victim/Public/.Simple_Worm/Loop. After finding out the directory of worm, I use brute-force to decrypt the crack_me.log. My method is use all the character to XOR with the file until there is something I can recognize and the key is ASCII 133.

Item2.

Enforce strong passwords : Enforce user using a strong password(special characters, one uppercase letters) will enhance defense against common dictionary attack.

Failed Login Attempts Lockout: Disable the login after a certain number of failed login attempts.

Use Allow Hosts: Only allow SSH connections from certain hosts or IP addresses.

Item3.

Linux provides different methods to manipulate crontab for different demands.

System: edit /etc/crontab, requires root access and error—prone

User: use command line to manipulate crontab

Applications: use GUI to manipulate crontab