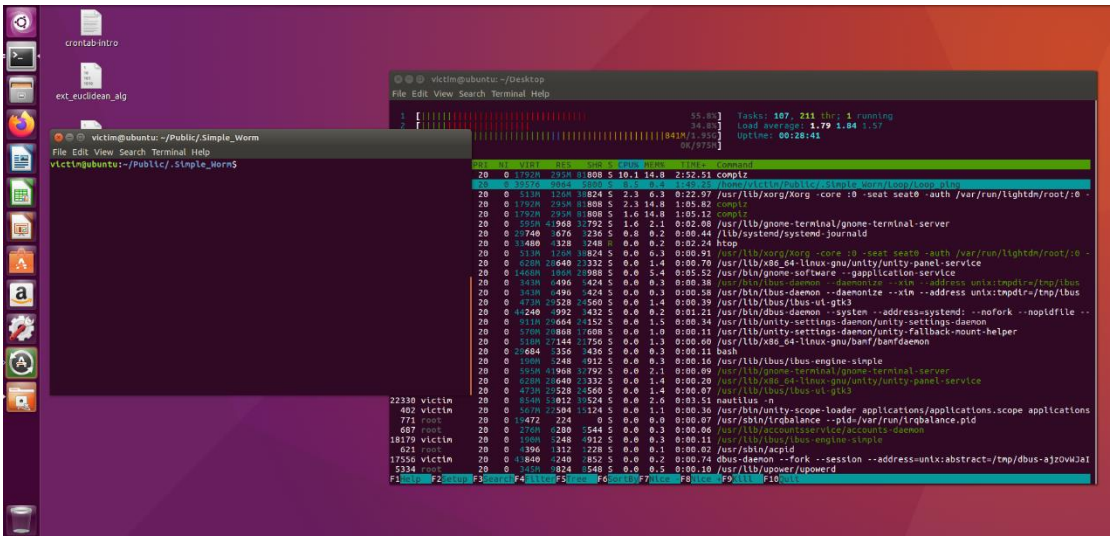
Project III: Worm Hiding/Propagation and Its Detection

Student ID: **Name:**

Part1: Detect and Remove Worm



(1) Using ***htop*** to detect worm

$cat /etc/crontab

…

@reboot root sudo /home/victim/Public/.Simple_Worm/XOR/XOR_Encrypt -C /home/victim/Desktop

@reboot root /home/victim/Public/.Simple_Worm/Loop/Loop_ping

By the content of ***/etc/crontab***, we can know the worm will be triggered when the machine boot.

To remove this worm, we can remove these 2 lines in ***/etc/crontab*** and remove the ***.Simple_Worm*** directory.

(2) Using python to read content of ***crack_me.log*** and testing xor, find key is 133

Replace 1234567 to my student ID, then doing xor by key 133 and write the result into ***task1_result.log***.

Part 2: 3 security settings in SSH server to prevent common dictionary attack

1. Strengthen password: Attacker needs to spend high cost of time and resource to guess strong (long, complicated) password by dictionary attack.
2. Disable the login after a certain number of failed login attempts.
3. Use SSH keys instead of password: Using SSH keys to connect to a remote server is more secure than using password to login remote server.

Part 3: Explain why Linux differentiates crontab into three types

Depending on functionality of the job schedule, differentiates crontab into three types can increase unity and efficiency of job scheduling. User type is most common among three types. Every user uses its own crontab file to maintain its job scheduling. And the system and application type are used for maintain job scheduling triggered by system base event and application base event.