NSUCyberSec Daily Task
Day 1

Instructions for Submission:

For Task 1, you need to create a document file (**task1.doc or task1.pdf**) and include screenshots of the CLI for each step (**commands** used, **inputs**, and **outputs**). Also, include the **confirmation.txt** file.

For Task 2, similarly create a document file (**task2.doc or task2.pdf**) and include **screenshots** (including the **history** command **output**).

Finally, zip both document files along with confirmation.txt ,then rename the zip file with **yourName_NSUID.zip** and upload the zip file to your drive. **Submit** the link in the **Discord #task-submission**

Task 01:
Suppose you have recently joined **TarshaSoftSec Ltd**. as a junior Linux operating engineer. Your boss gives you a task to change your Kali Linux **username** to your **surname (e.g., tamim)**, and then for confirmation **create** a **confirmation.txt** file which will be a **copy(must use command)** of **/etc/passwd** or **/etc/shadow**. Then, to **find your username**, use a very common **search command.** As you are a fresher, your boss gives you a **documentation** for your help:
https://unix.stackexchange.com/questions/610252/how-to-rename-a-user-account-in-kali-linux-debian-and-keep-all-settings

Marks distribution:

Criteria	Marks
Username change	2
confirmation.txt file creation with copy of **/etc/passwd** or **/etc/shadow**	5
Username search command	3

Task 02:
As a **Junior Threat Detection Engineer**, your company **TarshaSoftSec Ltd**. gives you their **server log** file (click for download log file). You know that the **401 status code** is used for **unauthorized access**. Your task is to analyze the log using **Linux search commands** to **detect brute-force access**. After confirming the attack, your **next step** is to **verify the login success using the 200 status code.** Then, you know that after gaining privileges, hackers use a command

to check which user they are logged in as. In this step, you **need to clarify whether the hacker used this command or not.All of these steps must** be done using **proper piping.** In the final step, you need to use the **history** command to show your work in your office.

Criteria	**Marks**
Detection of brute-force using 401 status code & show the ip that is detect as bruteforce	5
Verification of successful login using 200 status code	5
Identification of post-compromise command usage	5
Proper use of piping and history command	5