NSUCyberSec Daily Task
Day 2

Instructions for Submission:

For this assignment, students must prepare one document file named **task1.doc or task1.pdf.** The document should include clear **screenshots** of the command-line interface **(CLI)** showing **each step** of the **Bash script execution**, including the commands used, inputs provided, and the corresponding outputs. The document must also **contain the complete Bash script code**, along with screenshots confirming the successful creation of the **confidential.txt** file and verification of its **file permissions.**

The **Bash script file (.sh) must be included as a separate file** in the submission. After completing the task, the document file, the Bash script file (.sh), and the generated confidential.txt file must be compressed into a single ZIP archive. The ZIP file should be renamed using the format **yourName_NSUID.zip,** uploaded to **Drive**, and the download link must be submitted in the Discord channel **#task-submission.**

Assignment Title

Bash Scripting for Linux System Administration Automation

Assignment Description

You are working as a **Junior Linux Operator** at **NetSecure Ltd.** As part of your daily responsibilities, you are required to execute several repetitive system administration tasks. To improve efficiency and reduce manual effort, you have decided to automate these tasks using a **Bash script.**

Task Requirements

Write a Bash script that performs the following **operations** in sequence:

1. Display the **current logged-in username**.
2. Switch to the **root** user.
3. Verify whether the script is running with root privileges:
    - If the current user is root, display the message:
      "**I am in Root now**"
    - Otherwise, display the message:
      "**Normal user**"
4. Create a file named **confidential.txt** and set its permissions such that:
    - The **owner** has **read** and **write permissions only**
    - **Group** and **others** have **no permissions (read, write, or execute)**
5. Use **journalctl** to extract the latest **50 commands/log** entries, save them into **confidential.txt,** and then **display** the contents of the file.

Mark Distribution Table

Description	Marks
Display the current logged-in username	2
Switching to root user	3
Verifying root privilege and displaying appropriate message	4
Creating confidential.txt and setting correct file permissions	5
Extracting latest 50 logs using journalctl and saving to the file	4
Displaying the contents of confidential.txt	2
Script structure, comments, and proper command usage	5
	25

Sample Output

$ ./automation.sh
Current user: mashrur

Switching to root user...

Password:

I am in Root now

Creating confidential.txt file...

Setting file permissions…
Permissions set to: -rw-------
Extracting last 50 journal logs…

Logs successfully written to confidential.txt
Displaying confidential.txt contents:

-- Logs begin at Mon 2026-01-27 09:10:14 UTC, end at Fri 2026-01-31 10:45:02 UTC. --

Jan 31 10:40:12 netsecure systemd[1]: Started Session 45 of user root.

Jan 31 10:40:15 netsecure sudo[2134]: root : TTY=pts/0 ; COMMAND=/bin/bash

Jan 31 10:40:20 netsecure kernel: audit: type=1100 audit(1706690420.123:98)

Jan 31 10:40:25 netsecure systemd[1]: Stopping User Manager for UID 1000.

...(remaining log entries)