SOC Alert Triage with Log Analysis

Step 1 - Create and change into new directory and create fake logs.

I Created a mock log using the **mkdir** command & and then used **cd** command to change into the new directory.

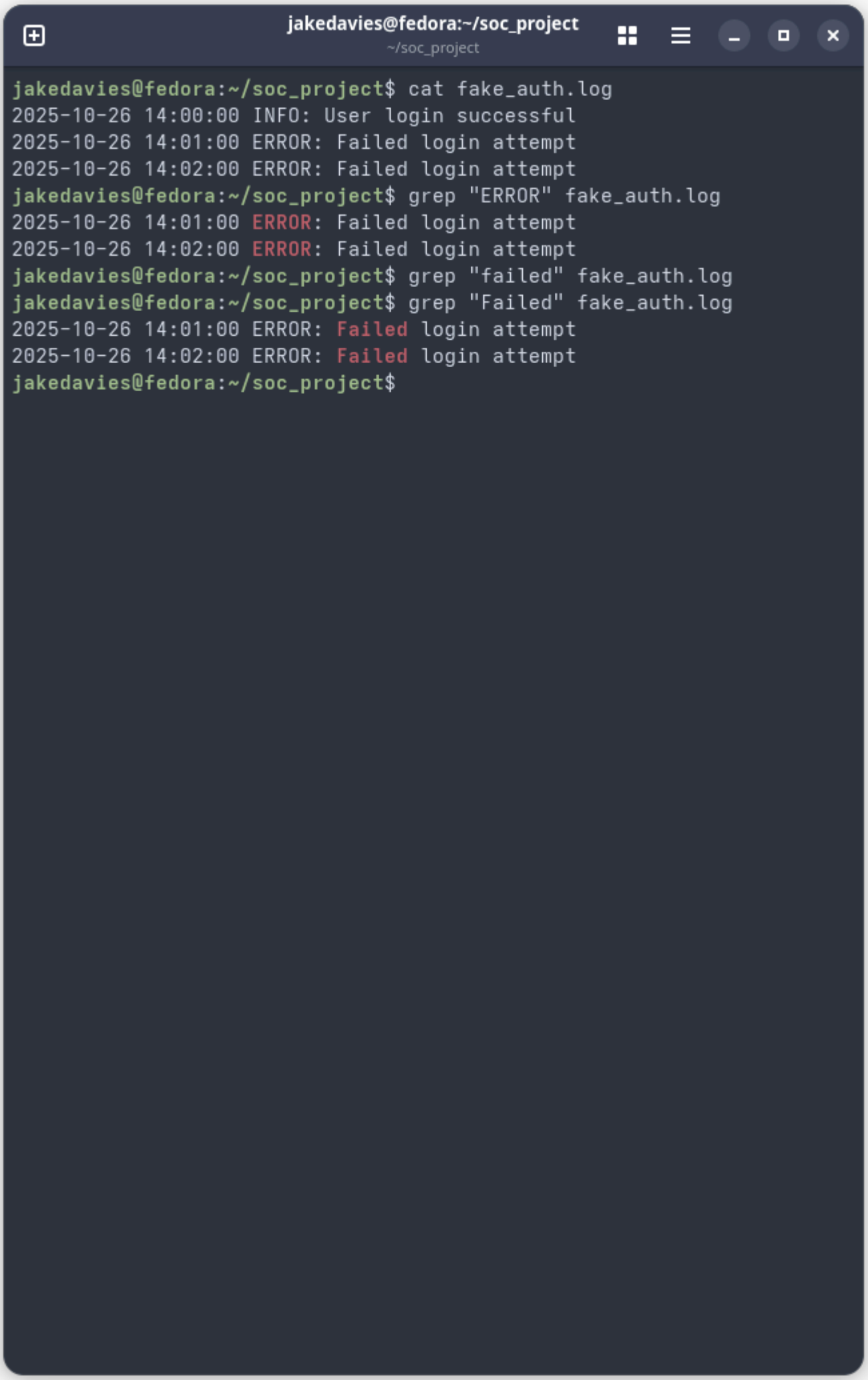
Once created i made fake logs using the **echo** command.

I verified said fake logs using the **cat** command.

jakedavies@fedora:~/soc_project$ cat fake_auth.log
2025-10-26 14:00:00 INFO: User login successful
2025-10-26 14:01:00 ERROR: Failed login attempt
2025-10-26 14:02:00 ERROR: Failed login attempt

Step 2 - Analyzed log with grep "ERROR" fake_auth.log to find failed logins, mimicking SOC triage for high-severity alerts.

jakedavies@fedora:~/soc_project$ grep "ERROR" fake_auth.log
2025-10-26 14:01:00 ERROR: Failed login attempt
2025-10-26 14:02:00 ERROR: Failed login attempt
jakedavies@fedora:~/soc_project$ grep "Failed" fake_auth.log
2025-10-26 14:01:00 ERROR: Failed login attempt
2025-10-26 14:02:00 ERROR: Failed login attempt

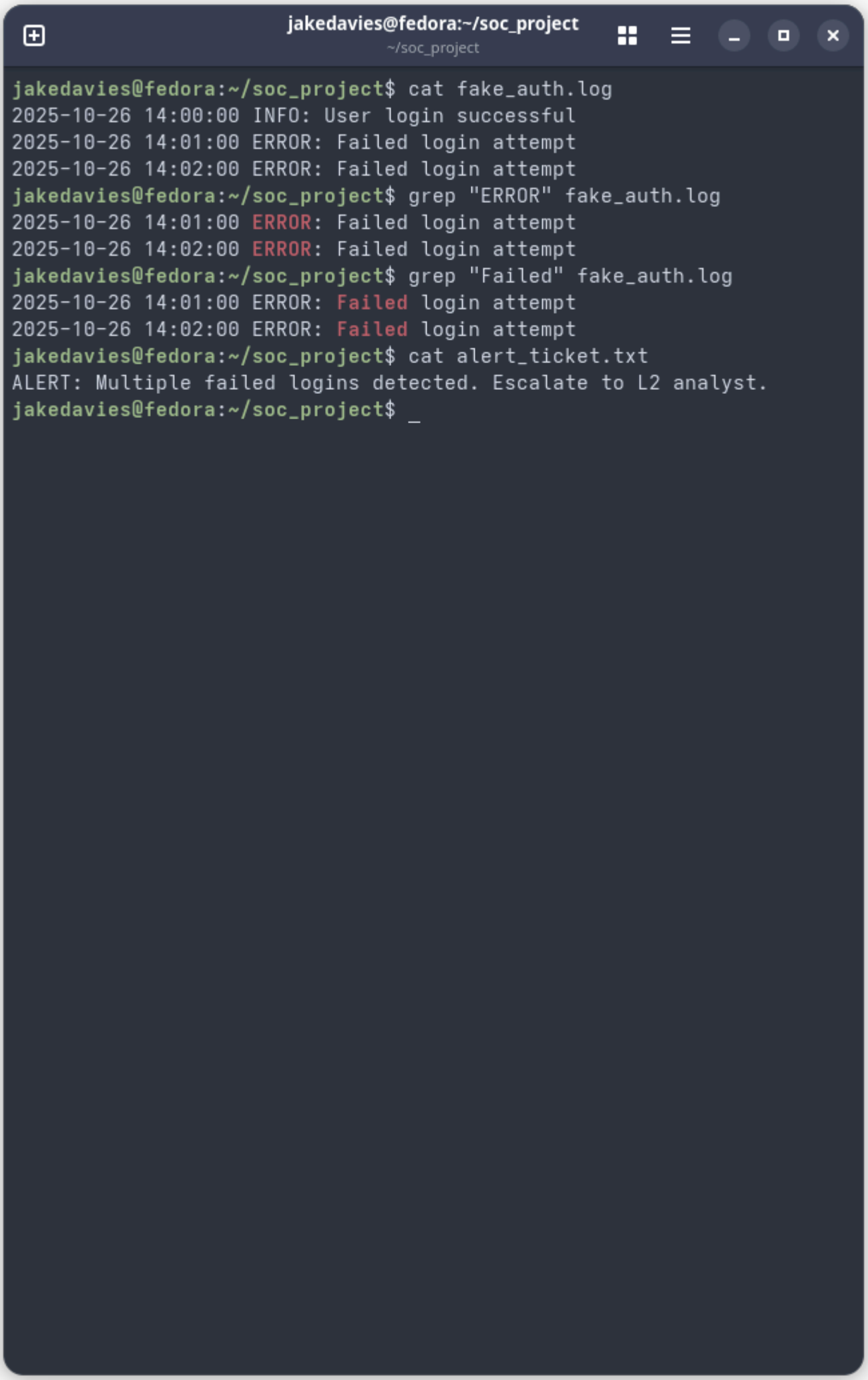


Step 3 - Simulate Escalation & Documentation

In this step I simulated escalation with **echo** command to create a ticket file.

I used the **cat alert_ticket.txt** command to show the simulated alert ticket.

In a SOC, I'd document and hand off to **L2 analyst.**



Step 4 - Removing the files and directory from my home lap to show use of other commands.

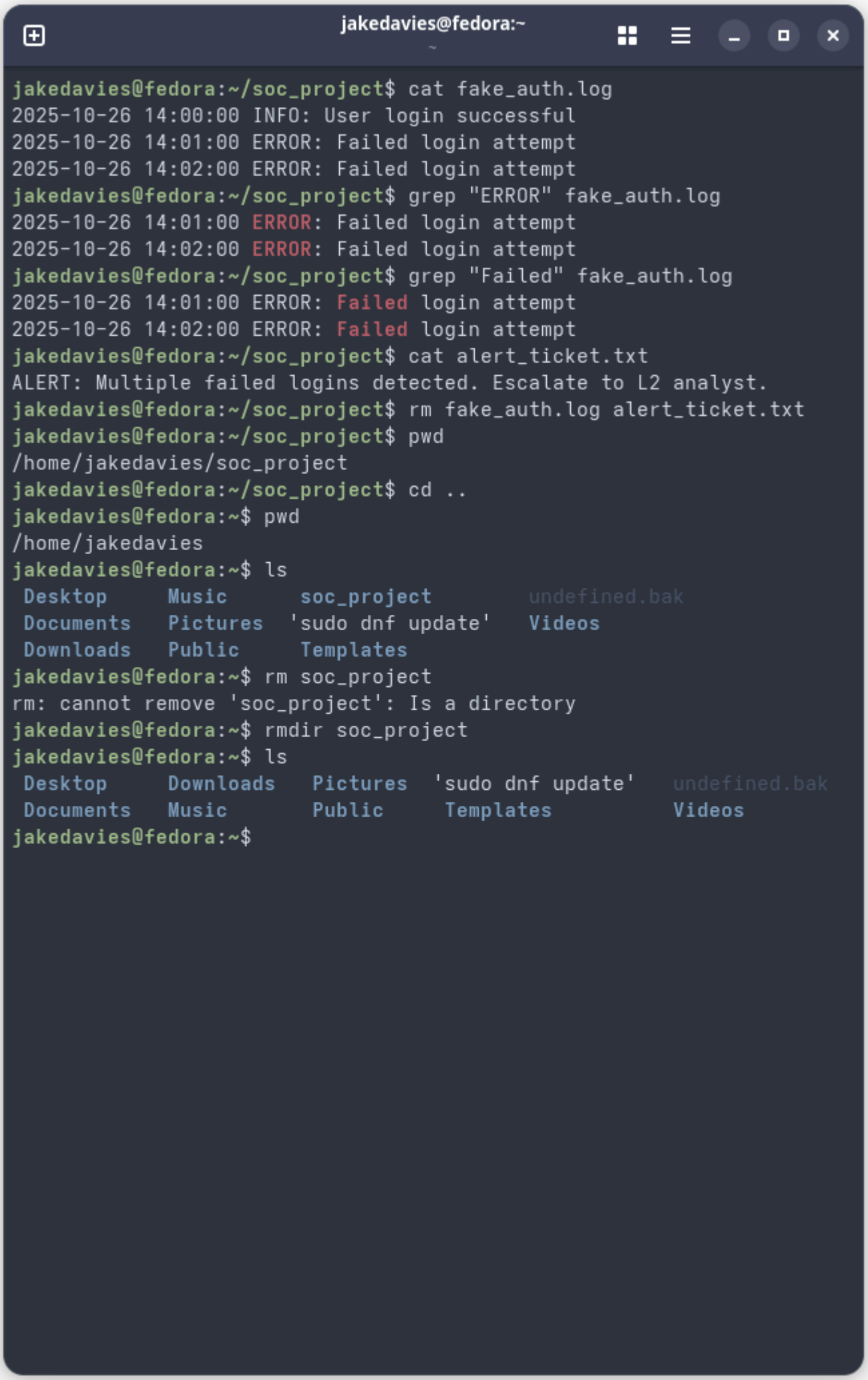
After Completing the home lab project i wanted to show how i remove files and directories and navigate through the terminal.

As you can see my first command was **rm** followed by the names of the files i am removing.

After i used **pwd** to show and double check which directory i am in. (after completing i realized this step was not needed.)

After confirming i used **cd ..** to change into the parent directory and used **pwd** again along with ls to confirm the new directory and to show the folders within the new location.

After i tried to remove the **soc_project** directory using the wrong command **rm**. At this point I had to research the correct command to use and found that to remove directories the correct line is **rmdir** followed by the [directory name]



Overview

Simulated L1 SOC task on Fedora 42: created `fake_auth.log` with `echo` to mimic brute-force logins, used `grep "Failed"` to find errors (fixed case issue), and documented/escalated with `echo` / `cat`.

Step 1: Setup

Created folder with `mkdir ~/soc_alert_project` and navigated with `cd`.

Step 2: Mock Log

Created `fake_auth.log` with `echo` to simulate logins.

Step 3: Analyze Log

Searched with `grep "Failed" fake_auth.log`, fixed case issue.

Step 4: Escalate

Documented alert with `echo` to `alert_ticket.txt`.