

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
```

```
jakedavies@fedora:~/soc_project
~/soc_project

bash: /home/jakedavies/fedora_logo.sh: No such file or directory
.';:::;,'.
.':cccccccccccccc;,,.
.;cccccccccccccccccccccc;.
.:cccccccccccccccccccccccccc:.
.;cccccccccccccc;.:ddd1:.;cccccc;.
.:cccccccccccccc;OWMK00XMWd;ccccccc:.
.:cccccccccccccc;KMMc;cc;xMMc;ccccccc:.
,cccccccccccccc;MMM.;cc;;WW;cccccccc,
:cccccccccccccc;MMM.;cccccccccccccccccc:
:ccccccc;ox000o;MMM000k.;cccccccccccccc:
cccccc;0MMKxdd:;MMmkddc.;cccccccccccccc;
cccccc;XMO';cccc;MMM.;cccccccccccccccccc'
cccccc;MMo;cccccc;MMW.;cccccccccccccccccc;
cccccc;0Mnc.ccc.xMMd;cccccccccccccccccc;
cccccc;dNMWXXWM0;cccccccccccccccccc;,
cccccccc;.:od1:.;cccccccccccccccccc;,.
cccccccccccccccccccccccccccccccccccccc:'.
:cccccccccccccccccccccccccccccccccccccc;,,.
':cccccccccccccccccccccc:;,,.

OS: Fedora Linux 42 (Work4
Host: VivoBook_ASUSLaptop)
Kernel: Linux 6.17.4-200.4
Uptime: 17 hours, 22 mins
Packages: 2156 (rpm), 28 )
Shell: bash 5.2.37
Display (SDC4161): 1920x1]
DE: GNOME 48.6
WM: Mutter (Wayland)
WM Theme: Nordic-darker-v0
Theme: Nordic-darker [GTK]
Icons: candy-icons [GTK2/]
Font: Inter (10pt) [GTK2/]
Cursor: Breeze_Light (24p)
Terminal: Ptyxis 48.5
Terminal Font: Adwaita Mo)
CPU: 11th Gen Intel(R) Coz
GPU: Intel Iris Xe Graphi]
Memory: 5.30 GiB / 15.31 )
Swap: 0 B / 8.00 GiB (0%)
Disk (/): 15.89 GiB / 103s
Disk (/run/media/jakedavi]
Local IP (wlo1): 192.168.4
Battery (ASUS Battery): 6]
Locale: en_US.UTF-8

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
jakedavies@fedora:~/soc_project$ _
```

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
```

```
jakedavies@fedora:~/soc_project
~/soc_project

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
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
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
jakedavies@fedora:~/soc_project$
```

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**.

```
jakedavies@fedora:~/soc_project
~/soc_project

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
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
jakedavies@fedora:~/soc_project$ cat alert_ticket.txt
ALERT: Multiple failed logins detected. Escalate to L2 analyst.
jakedavies@fedora:~/soc_project$ _
```

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]

```
jakedavies@fedora:~  
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  
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  
jakedavies@fedora:~/soc_project$ cat alert_ticket.txt  
ALERT: Multiple failed logins detected. Escalate to L2 analyst.  
jakedavies@fedora:~/soc_project$ rm fake_auth.log alert_ticket.txt  
jakedavies@fedora:~/soc_project$ pwd  
/home/jakedavies/soc_project  
jakedavies@fedora:~/soc_project$ cd ..  
jakedavies@fedora:~$ pwd  
/home/jakedavies  
jakedavies@fedora:~$ ls  
Desktop      Music      soc_project  undefined.bak  
Documents    Pictures   'sudo dnf update'  Videos  
Downloads    Public     Templates  
jakedavies@fedora:~$ rm soc_project  
rm: cannot remove 'soc_project': Is a directory  
jakedavies@fedora:~$ rmdir soc_project  
jakedavies@fedora:~$ ls  
Desktop      Downloads   Pictures   'sudo dnf update'  undefined.bak  
Documents    Music       Public     Templates           Videos  
jakedavies@fedora:~$
```

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` .