

# Task One.

1

## ^ Essentials

[JSON View](#)

Resource group ([move](#))  
[ID616OSC-jackcurley-RG](#)

Status  
Running

Location  
Australia East

Subscription ([move](#))  
[School of ICT Teaching](#)

Subscription ID  
3be7817b-3c0f-4e30-a68b-7d45c10f0544

Operating system  
Linux (ubuntu 22.04)

Size  
Standard B2s (2 vcpus, 4 GiB memory)

Public IP address  
[13.75.237.153](#)

Virtual network/subnet  
[labvm-vnet/labvm-Subnet](#)

DNS name  
[Not configured](#)

Health state  
-

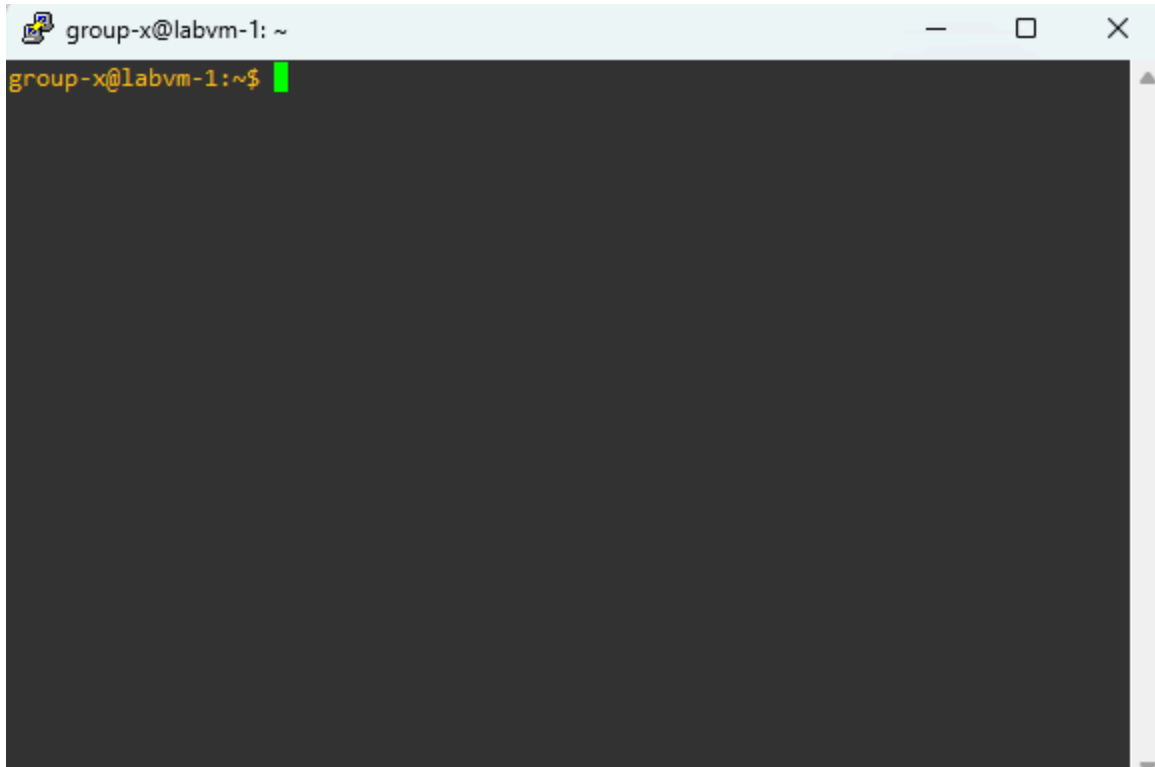
Time created  
7/14/2025, 1:38 AM UTC

Tags ([edit](#))

displayName : labvm

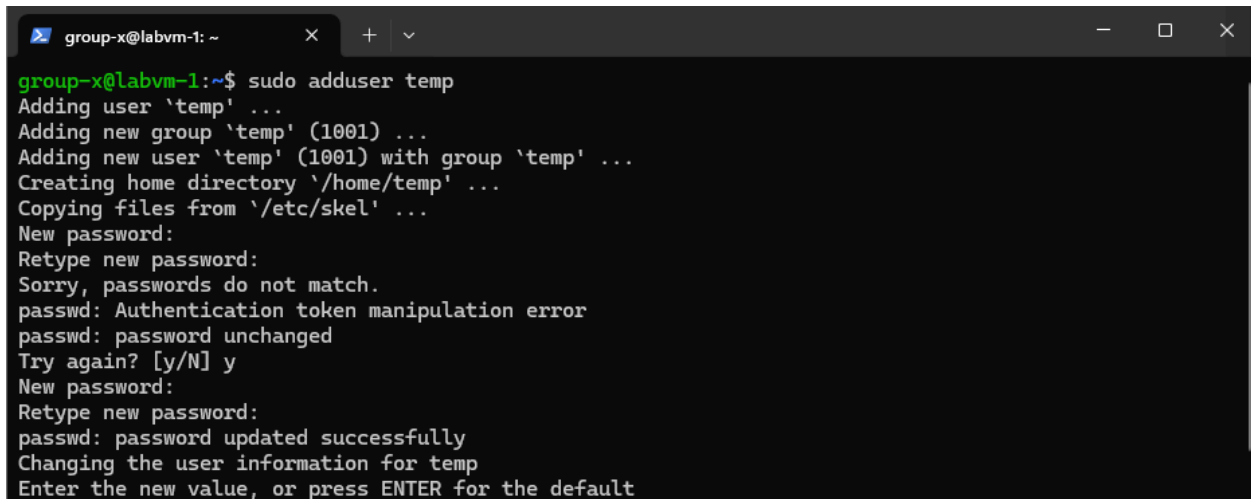
---

2



3

Created temp user



Elevated to sudo



Logged in as temp

```
temp@labvm-1: ~  
temp@labvm-1:~$ |
```

Usermod to change the name and home directory.

Groupmod to change primry group name

```
temp@labvm-1:~$ sudo usermod -l curlejm1 -d /home/curlejm1 -m group-x  
[sudo] password for temp:  
temp@labvm-1:~$ sudo groupmod -n curlejm1 group-x  
temp@labvm-1:~$
```

Logged back in to group-x (now called curlejm1)

```
curlejm1@labvm-1: ~  
curlejm1@labvm-1:~$ |
```

Confirmed changes

```
curlejm1@labvm-1:~$ grep "curlejm1" /etc/passwd  
curlejm1:x:1000:1000:Ubuntu:/home/curlejm1:/bin/bash  
curlejm1@labvm-1:~$ grep "curlejm1" /etc/group  
adm:x:4:syslog,curlejm1  
dialout:x:20:curlejm1  
cdrom:x:24:curlejm1  
floppy:x:25:curlejm1  
sudo:x:27:temp,curlejm1  
audio:x:29:curlejm1  
dip:x:30:curlejm1  
video:x:44:curlejm1  
plugdev:x:46:curlejm1  
netdev:x:119:curlejm1  
lxd:x:120:curlejm1  
curlejm1:x:1000:  
curlejm1@labvm-1:~$ |
```

Updated password

```
curlejm1@labvm-1:~$ passwd  
Changing password for curlejm1.  
Current password:  
New password:  
Retype new password:  
passwd: password updated successfully  
curlejm1@labvm-1:~$ |
```

Deleted temp user

```
curlejm1@labvm-1: ~  
curlejm1@labvm-1:~$ sudo deluser --remove-home temp  
[sudo] password for curlejm1:  
Looking for files to backup/remove ...  
Removing files ...  
Removing user 'temp' ...  
Warning: group 'temp' has no more members.  
Done.  
curlejm1@labvm-1:~$ |
```

---

## Task Two.

Made new dir > cloned repo

```
curlejm1@labvm-1: ~/checkin  
curlejm1@labvm-1:~$ mkdir checkin1task2  
curlejm1@labvm-1:~$ ls  
checkin1task2  key  key.pub  lab2.2  
curlejm1@labvm-1:~$ cd checkin1task2  
curlejm1@labvm-1:~/checkin1task2$ git clone https://github.com/0layinka0P/checkpoint1-files.git  
Cloning into 'checkpoint1-files'...  
remote: Enumerating objects: 4, done.  
remote: Counting objects: 100% (4/4), done.  
remote: Compressing objects: 100% (4/4), done.  
remote: Total 4 (delta 0), reused 4 (delta 0), pack-reused 0 (from 0)  
Receiving objects: 100% (4/4), done.  
curlejm1@labvm-1:~/checkin1task2$ pwd  
/home/curlejm1/checkin1task2  
curlejm1@labvm-1:~/checkin1task2$ |
```

CD into new git repo

```
curlejm1@labvm-1: ~/checkin  
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files$ |
```

Created onboard-users.sh

```
curlejm1@labvm-1: ~/checkin  
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files$ nano onboard_users.sh  
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files$ ls  
onboard_users.sh  sys_log.txt  users.csv  
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files$ |
```

Contents of onboard-users.sh (switched machines)

```

GNU nano 6.2
#!/bin/bash

# Set file paths
CSV_FILE="users.csv"
LOG_FILE="/var/log/user_onboarding_audit.log"
PROJECTS_DIR="/opt/projects"

# Check if root
if [ "$EUID" -ne 0 ]; then
    echo "Run this as root."
    exit 1
fi

# Check if CSV exists
if [ ! -f "$CSV_FILE" ]; then
    echo "CSV file not found."
    exit 1
fi

# Check if projects directory exists
mkdir -p "$PROJECTS_DIR"

# Start the log
echo "$(date) - Starting user onboarding" >> "$LOG_FILE"

# Read CSV, skip first line / header
tail -n +2 "$CSV_FILE" | while IFS=',' read username groups shell
do
    # Skip if empty
    if [ -z "$username" ] || [ -z "$groups" ] || [ -z "$shell" ]; then
        echo "$(date) - Missing fields, skipping." >> "$LOG_FILE"
        continue
    fi

    # Split group names by "/" into array
    IFS='/' read -ra group_array <<< "$groups"

    # First group = primary group
    primary_group="${group_array[0]}"

    # Create each group if theyd doesn't exist
    for g in "${group_array[@]"; do
        if ! getent group "$g" > /dev/null; then
            groupadd "$g"
            echo "$(date) - Group $g created." >> "$LOG_FILE"
        fi
    done

    # Check if user already exists
    if id "$username" &>/dev/null; then
        # If user exists, update shell
        usermod -s "$shell" "$username"
        echo "$(date) - Updated shell for $username." >> "$LOG_FILE"
    else
        # Join all groups with commas for -G option
        all_groups=$(IFS=','; echo "${group_array[*]}")
        # Create new user with home directory and group
        useradd -m -s "$shell" -g "$primary_group" -G "$all_groups" "$username"
        echo "$(date) - User $username created." >> "$LOG_FILE"
    fi
done

```

```

# Create project directory for user
mkdir -p "$PROJECTS_DIR/$username"
chown "$username":"$primary_group" "$PROJECTS_DIR/$username"
chmod 750 "$PROJECTS_DIR/$username"
echo "$(date) - Project dir for $username created." >> "$LOG_FILE"

done

# Finish log
echo "$(date) - Finished user onboarding" >> "$LOG_FILE"
|

```

Made the script executable & confirmed it.

```

curlejm1@labvm-1:~/OSCheckin1$ ls
README.md  onboard_users.sh  sys_log.txt  users.csv
curlejm1@labvm-1:~/OSCheckin1$ chmod +x onboard_users.sh
curlejm1@labvm-1:~/OSCheckin1$ ls -l onboard_users.sh
-rwxrwxr-x 1 curlejm1 curlejm1 2131 Aug  4 07:47 onboard_users.sh
curlejm1@labvm-1:~/OSCheckin1$ |

```

Tested running without sudo

```

curlejm1@labvm-1:~$ ls
OSCheckin1  key  key.pub
curlejm1@labvm-1:~$ cd OSMCheckin1/
curlejm1@labvm-1:~/OSCheckin1$ ls
README.md  onboard_users.sh  sys_log.txt  users.csv
curlejm1@labvm-1:~/OSCheckin1$ ./onboard_users.sh
Run this as root.
curlejm1@labvm-1:~/OSCheckin1$ |

```

Tested running

```

curlejm1@labvm-1:~/OSCheckin1$ ls
README.md  onboard_users.sh  sys_log.txt  users.csv
curlejm1@labvm-1:~/OSCheckin1$ sudo ./onboard_users.sh
curlejm1@labvm-1:~/OSCheckin1$

```

Ran the script after users were already created

```
curlejm1@labvm-1:~/OSCheckin1$ sudo ./onboard_users.sh  
[sudo] password for curlejm1:  
usermod: no changes  
usermod: no changes  
usermod: no changes  
curlejm1@labvm-1:~/OSCheckin1$
```

Checked log file.

```
curlejm1@labvm-1:~/OSCheckin1$ sudo cat /var/log/user_onboarding_audit.log
2025-08-01 02:13:53 - Starting user onboarding process.
2025-08-01 02:13:53 - ACTION: Creating new group 'admin/lecturer'.
2025-08-01 02:13:53 - ACTION: Creating new user 'rob'.
2025-08-01 02:13:53 - ACTION: Setting up project directory '/opt/projects/rob'.
2025-08-01 02:13:53 - ACTION: Creating new group 'lecturer'.
2025-08-01 02:13:53 - ACTION: Creating new user 'ola'.
2025-08-01 02:13:53 - ACTION: Setting up project directory '/opt/projects/ola'.
2025-08-01 02:13:53 - ACTION: Creating new group 'student'.
2025-08-01 02:13:53 - ACTION: Creating new user 'andy'.
2025-08-01 02:13:53 - ACTION: Setting up project directory '/opt/projects/andy'.
2025-08-01 02:13:53 - User onboarding process finished.
2025-08-01 02:24:07 - Starting user onboarding process.
2025-08-01 02:24:07 - ACTION: User 'rob' exists. Updating shell.
2025-08-01 02:24:07 - ACTION: Setting up project directory '/opt/projects/rob'.
2025-08-01 02:24:07 - ACTION: User 'ola' exists. Updating shell.
2025-08-01 02:24:07 - ACTION: Setting up project directory '/opt/projects/ola'.
2025-08-01 02:24:07 - ACTION: User 'andy' exists. Updating shell.
2025-08-01 02:24:07 - ACTION: Setting up project directory '/opt/projects/andy'.
2025-08-01 02:24:07 - User onboarding process finished.
2025-08-01 02:26:35 - Starting user onboarding process.
2025-08-01 02:26:35 - ACTION: Creating new user 'rob'.
2025-08-01 02:26:35 - ACTION: Setting up project directory '/opt/projects/rob'.
2025-08-01 02:26:35 - ACTION: Creating new group 'lecturer'.
2025-08-01 02:26:35 - ACTION: Creating new user 'ola'.
2025-08-01 02:26:35 - ACTION: Setting up project directory '/opt/projects/ola'.
2025-08-01 02:26:35 - ACTION: Creating new group 'student'.
2025-08-01 02:26:35 - ACTION: Creating new user 'andy'.
2025-08-01 02:26:35 - ACTION: Setting up project directory '/opt/projects/andy'.
2025-08-01 02:26:36 - User onboarding process finished.
2025-08-01 02:36:31 - Starting user onboarding process.
2025-08-01 02:36:31 - ACTION: Creating new user 'rob'.
2025-08-01 02:36:31 - ACTION: Setting up project directory '/opt/projects/rob'.
2025-08-01 02:36:31 - ACTION: Creating new group 'lecturer'.
2025-08-01 02:36:31 - ACTION: Creating new user 'ola'.
2025-08-01 02:36:31 - ACTION: Setting up project directory '/opt/projects/ola'.
2025-08-01 02:36:31 - ACTION: Creating new group 'student'.
2025-08-01 02:36:31 - ACTION: Creating new user 'andy'.
2025-08-01 02:36:32 - ACTION: Setting up project directory '/opt/projects/andy'.
2025-08-01 02:36:32 - User onboarding process finished.
Mon Aug 4 07:57:42 UTC 2025 - Starting user onboarding
Mon Aug 4 07:57:42 UTC 2025 - Updated shell for rob.
Mon Aug 4 07:57:42 UTC 2025 - Project dir for rob created.
Mon Aug 4 07:57:42 UTC 2025 - Updated shell for ola.
Mon Aug 4 07:57:42 UTC 2025 - Project dir for ola created.
Mon Aug 4 07:57:42 UTC 2025 - Updated shell for andy.
Mon Aug 4 07:57:42 UTC 2025 - Project dir for andy created.
Mon Aug 4 07:57:42 UTC 2025 - Finished user onboarding
Mon Aug 4 08:02:57 UTC 2025 - Starting user onboarding
Mon Aug 4 08:02:58 UTC 2025 - User rob created.
Mon Aug 4 08:02:58 UTC 2025 - Project dir for rob created.
Mon Aug 4 08:02:58 UTC 2025 - User ola created.
Mon Aug 4 08:02:58 UTC 2025 - Project dir for ola created.
Mon Aug 4 08:02:58 UTC 2025 - User andy created.
Mon Aug 4 08:02:58 UTC 2025 - Project dir for andy created.
Mon Aug 4 08:02:58 UTC 2025 - Finished user onboarding
curlejm1@labvm-1:~/OSCheckin1$ |
```



Check users, directories and perms

```
curlejm1@labvm-1:~/OSCheckin1$ id rob
uid=1001(rob) gid=118(admin) groups=118(admin),1002(lecturer)
curlejm1@labvm-1:~/OSCheckin1$ id ola
uid=1002(ola) gid=1002(lecturer) groups=1002(lecturer)
curlejm1@labvm-1:~/OSCheckin1$ id andy
uid=1003(andy) gid=1003(student) groups=1003(student)
curlejm1@labvm-1:~/OSCheckin1$ ls -ld /home/rob
drwx----- 2 rob admin 4096 Aug  4 08:02 /home/rob
curlejm1@labvm-1:~/OSCheckin1$ ls -ld /home/ola
drwx----- 2 ola lecturer 4096 Aug  4 08:02 /home/ola
curlejm1@labvm-1:~/OSCheckin1$ ls -ld /home/andy
drwx----- 2 andy student 4096 Aug  4 08:02 /home/andy
curlejm1@labvm-1:~/OSCheckin1$ ls -ld /opt/projects/rob
drwxr-x--- 2 rob admin 4096 Aug  4 08:02 /opt/projects/rob
curlejm1@labvm-1:~/OSCheckin1$ ls -ld /opt/projects/ola
drwxr-x--- 2 ola lecturer 4096 Aug  4 08:02 /opt/projects/ola
curlejm1@labvm-1:~/OSCheckin1$ ls -ld /opt/projects/andy
drwxr-x--- 2 andy student 4096 Aug  4 08:02 /opt/projects/andy
curlejm1@labvm-1:~/OSCheckin1$
```

I ran into some serious issues with Git here. I could not push to my repo.  
I tried generating a new token, and I just could not get it to work.

```

origin https://github.com/JackDoe92/OSCheckin1.git (fetch)
origin https://github.com/JackDoe92/OSCheckin1.git (push)
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git credential-cache exit
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git config --global --unset credential.helper
warning: credential.helper has multiple values
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git config --global --get-all credential.helper
cache
cache
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git config --global --unset-all credential.helper
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git config --global --get-all credential.helper
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git push
Username for 'https://github.com': JackDoe92
Password for 'https://JackDoe92@github.com':
remote: Invalid username or token. Password authentication is not supported for Git operations.
fatal: Authentication failed for 'https://github.com/JackDoe92/OSCheckin1.git/'
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git push
Username for 'https://github.com': JackDoe92
Password for 'https://JackDoe92@github.com':
remote: Permission to JackDoe92/OSCheckin1.git denied to JackDoe92.
fatal: unable to access 'https://github.com/JackDoe92/OSCheckin1.git/': The requested URL returned error: 403
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ curl -u JackDoe92:github_pat_11A6KE3SY0gjBDBh0qQilm_9E
{
  "login": "JackDoe92",
  "id": 127159755,
  "node_id": "U_kgDOB5RNYw",
  "avatar_url": "https://avatars.githubusercontent.com/u/127159755?v=4",
  "gravatar_id": "",
  "url": "https://api.github.com/users/JackDoe92",
  "html_url": "https://github.com/JackDoe92",
  "followers_url": "https://api.github.com/users/JackDoe92/followers",
  "following_url": "https://api.github.com/users/JackDoe92/following{/other_user}",
  "gists_url": "https://api.github.com/users/JackDoe92/gists{/gist_id}",
  "starred_url": "https://api.github.com/users/JackDoe92/starred{/owner}/{/repo}",
  "subscriptions_url": "https://api.github.com/users/JackDoe92/subscriptions",
  "organizations_url": "https://api.github.com/users/JackDoe92/orgs",
  "repos_url": "https://api.github.com/users/JackDoe92/repos",
  "events_url": "https://api.github.com/users/JackDoe92/events{/privacy}",
  "received_events_url": "https://api.github.com/users/JackDoe92/received_events",
  "type": "User",
  "user_view_type": "public",
  "site_admin": false,
  "name": "Jack Doe",
  "company": null,
  "blog": "",
  "location": null,
  "email": null,
  "hireable": null,
  "bio": "I have no idea what I am doing. ",
  "twitter_username": null,
  "notification_email": null,
  "public_repos": 9,
  "public_gists": 0,
  "followers": 0,
  "following": 2,
  "created_at": "2023-03-07T00:05:57Z",
  "updated_at": "2025-08-03T23:30:44Z"
}
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git push
Username for 'https://github.com': JackDoe92
Password for 'https://JackDoe92@github.com':
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git push
Username for 'https://github.com': JackDoe92
Password for 'https://JackDoe92@github.com':
remote: Permission to JackDoe92/OSCheckin1.git denied to JackDoe92.
fatal: unable to access 'https://github.com/JackDoe92/OSCheckin1.git/': The requested URL returned error: 403
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git remote set-url origin https://JackDoe92:github_pat_
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ git push
remote: Permission to JackDoe92/OSCheckin1.git denied to JackDoe92.
fatal: unable to access 'https://github.com/JackDoe92/OSCheckin1.git/': The requested URL returned error: 403
curlejm1@labvm-1:~/checkin1task2/checkpoint1-files/OSCheckin1$ |

```

At this point, I connected to the server via my terminal, allowing me to copy and paste my script out of the terminal and into VS Code. I then pushed the script to Git from my Windows machine, deleted the folder in the server and then cloned my repo inside the server as OSCheckin1.

```
curlejm1@labvm-1:~$ ls
OSCheckin1  key  key.pub
curlejm1@labvm-1:~$ |
```

---

## Task Three

Created the script

```
GNU nano 6.2
#!/bin/bash

# Define output and log files
LOG_FILE="sys_log.txt"
OUTPUT_FILE="top10_critical.txt"

# Check if the log file exists > warning if not
if [ ! -f "$LOG_FILE" ]; then
    echo "Error: Log file '$LOG_FILE' not found!"
    exit 1
fi

# filter, count, and sort key words
grep -ioE 'error|critical|fatal' "$LOG_FILE" | \
tr '[:upper:]' '[:lower:]' | \
sort | \
uniq -c | \
sort -nr | \
head -n 10 | \
tee "$OUTPUT_FILE"

echo "Results saved to $OUTPUT_FILE"
```

Made the file executable (and confirmed it worked)

```
curlejm1@labvm-1:~/OSCheckin1$ chmod +x critical_log_analysis.sh
curlejm1@labvm-1:~/OSCheckin1$ ls -l onboard_users.sh
-rwxrwxr-x 1 curlejm1 curlejm1 2131 Aug  4 07:47 onboard_users.sh
curlejm1@labvm-1:~/OSCheckin1$
```

Ran the script

```
curlejm1@labvm-1:~/OSCheckin1$ ./critical_log_analysis.sh
    5 error
    2 fatal
    1 critical
Results saved to top10_critical.txt
curlejm1@labvm-1:~/OSCheckin1$ |
```

Checked the contents of top10

—