Activity Filter with grep: Project Summary and Introduction

Project Title: Filter with grep

Activity Overview: This project demonstrates proficiency in using the grep command and piping in Linux to search for specific strings within files and file names. These skills are essential for efficiently locating and extracting information in large datasets, a critical task for security analysts working with Linux systems.

Scenario: As a security analyst, I performed a series of tasks to locate and analyze specific data within server logs and user directories. These tasks involved:

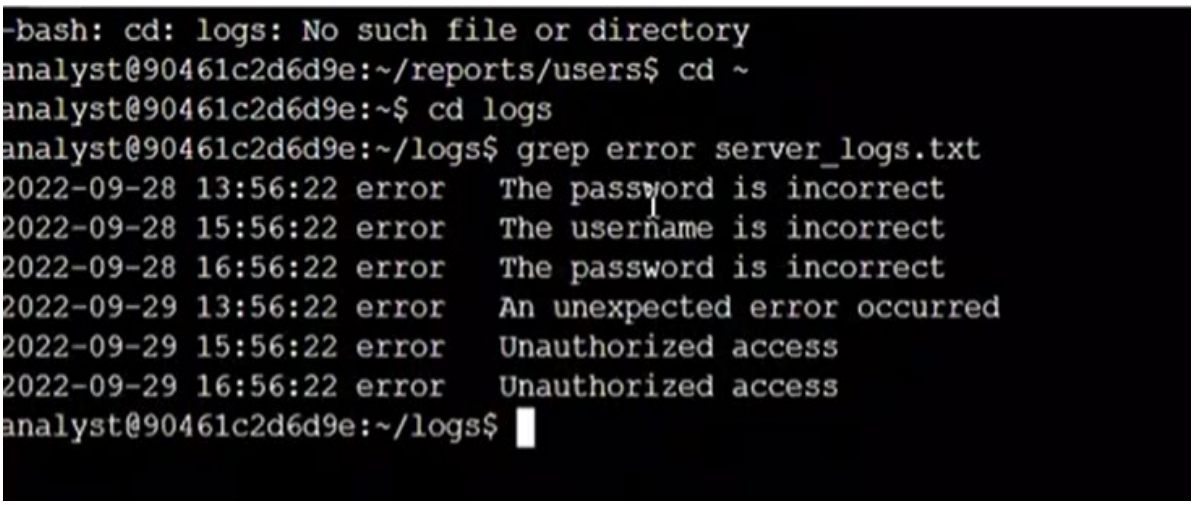
1. Navigating the Linux file system.
2. Filtering log files to extract error messages.
3. Identifying files with specific strings in their names.
4. Searching for specific content within user data files.

Tasks and Steps

Task 1: Search for Error Messages in a Log File

Objective: Use the grep command to filter and return error messages from a log file.

1. Navigate to the /home/analyst/logs directory.
    - **Command:** cd logs
2. Search the server_logs.txt file for lines containing the string "error."
    - **Command:** grep error server_logs.txt
3. **Result:** Identified the number of error messages in the file.
    - There are six error lines in the server_logs.txt file.



Task 2: Find Files Containing Specific Strings

Objective: Use piping with the grep command to search for files with specific strings in their names.

1. Navigate to the /home/analyst/reports/users directory.
    - **Command:** cd /home/analyst/reports/users
2. Search for files containing Q1 in their names.
    - **Command:** ls | grep Q1

    Result: Three files in the /home/analyst/reports/users subdirectory contain "Q1" in their names.

3. Search for files containing access in their names.
    - **Command:** ls | grep access

    Result: Four files in the /home/analyst/reports/users directory contain "access" in their names.

```
-bash: cd: logs: No such file or directory
analyst@90461c2d6d9e:~/reports/users$ cd ~
analyst@90461c2d6d9e:~$ cd logs
analyst@90461c2d6d9e:~/logs$ grep error server_logs.txt
2022-09-28 13:56:22 error   The password is incorrect
2022-09-28 15:56:22 error   The username is incorrect
2022-09-28 16:56:22 error   The password is incorrect
2022-09-29 13:56:22 error   An unexpected error occurred
2022-09-29 15:56:22 error   Unauthorized access
2022-09-29 16:56:22 error   Unauthorized access
analyst@90461c2d6d9e:~/logs$ cd /home/analyst/reports/users
analyst@90461c2d6d9e:~/reports/users$ ls | grep Q1
Q1_access.txt
Q1_added_users.txt
Q1_deleted_users.txt
analyst@90461c2d6d9e:~/reports/users$ ls | grep access
Q1_access.txt
Q2_access.txt
Q3_access.txt
Q4_access.txt
analyst@90461c2d6d9e:~/reports/users$
```

Task 3: Search File Contents

Objective: Use grep to extract specific information from user data files.

1. List all files in the /home/analyst/reports/users directory.
    - **Command:** ls
2. Search the Q2_deleted_users.txt file for the username jhill.
    - **Command:** grep jhill Q2_deleted_users.txt

    Result: The username jhill was found in the Q2_deleted_users.txt file.

3. Search the Q4_added_users.txt file for users added to the Human Resources department.
    - **Command:** grep "Human Resources" Q4_added_users.txt

    Result: Two users were added to the Human Resources department in quarter 4.

```
-bash: cd: logs: No such file or directory
analyst@90461c2d6d9e:~/reports/users$ cd ~
analyst@90461c2d6d9e:~$ cd logs
analyst@90461c2d6d9e:~/logs$ grep error server_logs.txt
2022-09-28 13:56:22 error   The password is incorrect
2022-09-28 15:56:22 error   The username is incorrect
2022-09-28 16:56:22 error   The password is incorrect
2022-09-29 13:56:22 error   An unexpected error occurred
2022-09-29 15:56:22 error   Unauthorized access
2022-09-29 16:56:22 error   Unauthorized access
analyst@90461c2d6d9e:~/logs$ cd /home/analyst/reports/users
analyst@90461c2d6d9e:~/reports/users$ ls | grep Q1
Q1_access.txt
Q1_added_users.txt
Q1_deleted_users.txt
analyst@90461c2d6d9e:~/reports/users$ ls | grep access
Q1_access.txt
Q2_access.txt
Q3_access.txt
Q4_access.txt
analyst@90461c2d6d9e:~/reports/users$ ls
Q1_access.txt         Q2_added_users.txt    Q3_deleted_users.txt
Q1_added_users.txt    Q2_deleted_users.txt  Q4_access.txt
Q1_deleted_users.txt  Q3_access.txt         Q4_added_users.txt
Q2_access.txt         Q3_added_users.txt    Q4_deleted_users.txt
analyst@90461c2d6d9e:~/reports/users$ grep jhill Q2_deleted_users.txt
1025        jhill     Sales
analyst@90461c2d6d9e:~/reports/users$ grep "Human Resources" Q4_added_users.txt
1151        sshah     Human Resources
1145        msosa     Human Resources
analyst@90461c2d6d9e:~/reports/users$
```

Conclusion

Through this lab activity, I gained practical experience in using grep to:

- Search for specific information contained in files.
- Find files containing specific strings that were piped into grep.

This activity enhanced my ability to use fundamental tools in Linux to filter the information I need efficiently.

Reflections/Notes

- Understanding the importance of using grep and piping to filter information.
- Recognizing the need for precise commands to locate specific data within files.
- Enhancing problem-solving skills by troubleshooting command-line issues.