Activity: Filter with grep

Activity overview

Previously, you learned about tools that you can use to filter information in Linux. You're also familiar with the basic commands to navigate the Linux file system by now.

In this lab activity, you'll use the grep command and piping to search for files and to return specific information from files.

As a security analyst, it's key to know how to find the information you need. The ability to search for specific strings can help you locate what you need more efficiently.

Scenario

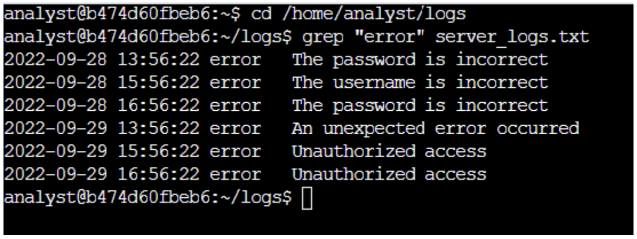
In this scenario, you need to obtain information contained in server log and user data files. You also need to find files with specific names.

Here's how you'll do this: **First**, you'll navigate to the logs directory and return the error messages in the server_logs.txt file. **Next**, you'll navigate to the users directory and search for files that contain a specific string in their names. **Finally**, you'll search for information contained in user files.

Task 1. Search for error messages in a log file

In this task, you must navigate to the /home/analyst/logs directory and report on the error messages in the server_logs.txt file. You'll do this by using grep to search the file and output only the entries that are for errors.

1. Navigate to the /home/analyst/logs directory.
2. Use grep to filter the server_logs.txt file, and return all lines containing the text string error.



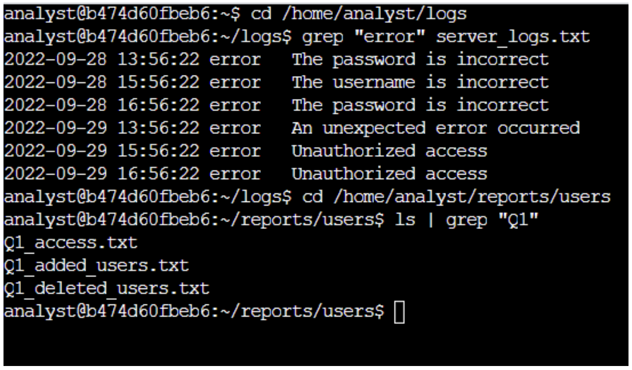
```
analyst@b474d60fbeb6:~$ cd /home/analyst/logs
analyst@b474d60fbeb6:~/logs$ grep "error" server_logs.txt
2022-09-28 13:56:22 error   The password is incorrect
2022-09-28 15:56:22 error   The username is incorrect
2022-09-28 16:56:22 error   The password is incorrect
2022-09-29 13:56:22 error   An unexpected error occurred
2022-09-29 15:56:22 error   Unauthorized access
2022-09-29 16:56:22 error   Unauthorized access
analyst@b474d60fbeb6:~/logs$ 
```

Task 2. Find files containing specific strings

In this task, you must navigate to the /home/analyst/reports/users directory and use the correct Linux commands and arguments to search for user data files that contain a specific string in their names.

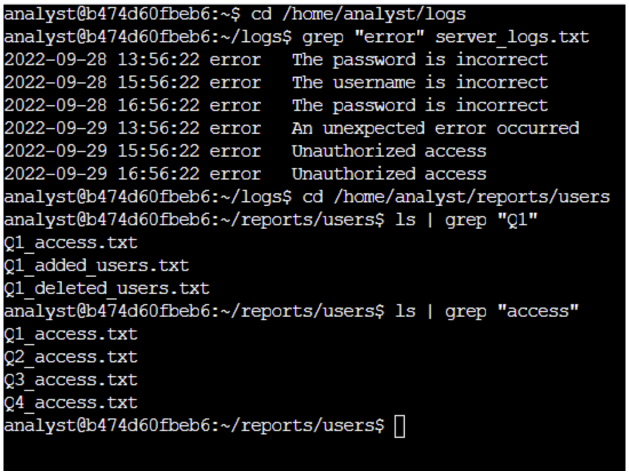
1. Navigate to the /home/analyst/reports/users directory.

2. Using the pipe character (|), pipe the output of the ls command to the grep command to list only the files containing the string Q1 in their names.



```
analyst@b474d60fbeb6:~$ cd /home/analyst/logs
analyst@b474d60fbeb6:~/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@b474d60fbeb6:~/logs$ cd /home/analyst/reports/users
analyst@b474d60fbeb6:~/reports/users$ ls | grep "Q1"
Q1_access.txt
Q1_added_users.txt
Q1_deleted_users.txt
analyst@b474d60fbeb6:~/reports/users$ 
```

3. List the files that contain the word access in their names.



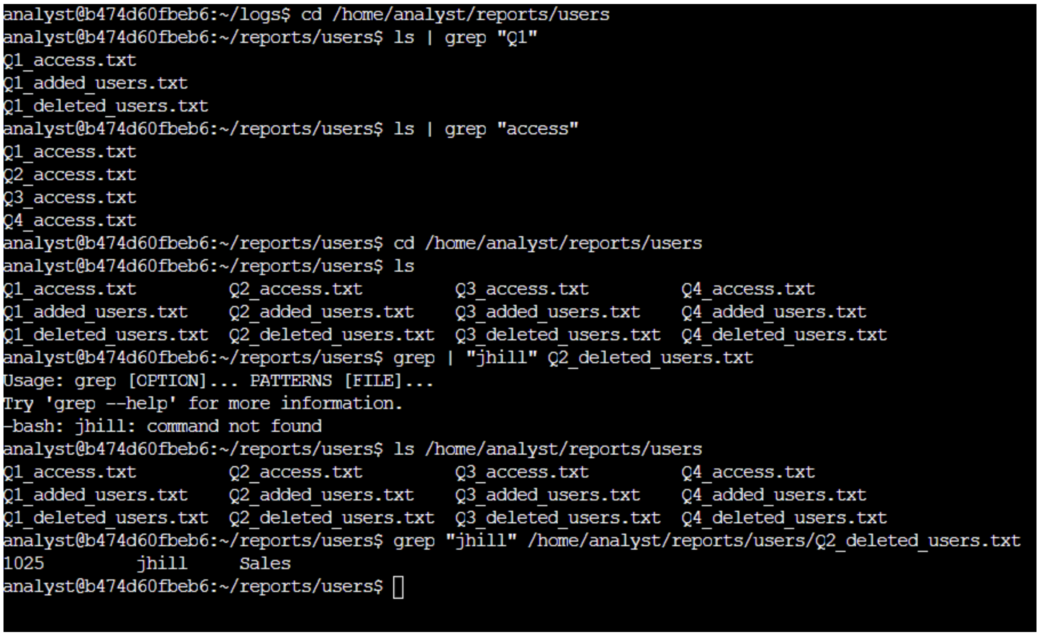
```
analyst@b474d60fbeb6:~$ cd /home/analyst/logs
analyst@b474d60fbeb6:~/logs$ grep "error" server_logs.txt
2022-09-28 13:56:22 error   The password is incorrect
2022-09-28 15:56:22 error   The username is incorrect
2022-09-28 16:56:22 error   The password is incorrect
2022-09-29 13:56:22 error   An unexpected error occurred
2022-09-29 15:56:22 error   Unauthorized access
2022-09-29 16:56:22 error   Unauthorized access
analyst@b474d60fbeb6:~/logs$ cd /home/analyst/reports/users
analyst@b474d60fbeb6:~/reports/users$ ls | grep "Q1"
Q1_access.txt
Q1_added_users.txt
Q1_deleted_users.txt
analyst@b474d60fbeb6:~/reports/users$ ls | grep "access"
Q1_access.txt
Q2_access.txt
Q3_access.txt
Q4_access.txt
analyst@b474d60fbeb6:~/reports/users$ 
```

Task 3. Search more file contents

In this task, you must search for information contained in user files and report on users that were added and deleted from the system.

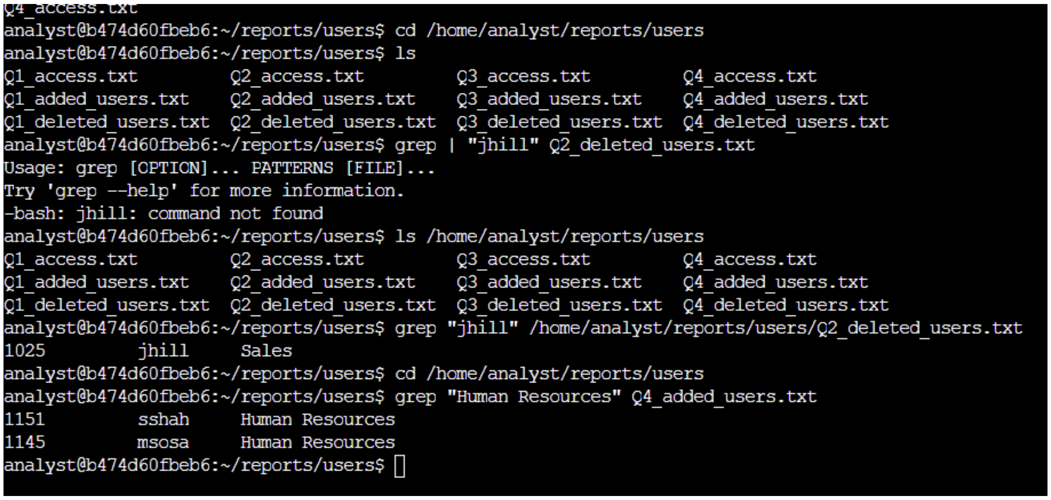
1. Display the files in the /home/analyst/reports/users directory.

2. Search the Q2_deleted_users.txt file for the username jhill.



```
analyst@b474d60fbeb6:~/logs$ cd /home/analyst/reports/users
analyst@b474d60fbeb6:~/reports/users$ ls | grep "Q1"
Q1_access.txt
Q1_added_users.txt
Q1_deleted_users.txt
analyst@b474d60fbeb6:~/reports/users$ ls | grep "access"
Q1_access.txt
Q2_access.txt
Q3_access.txt
Q4_access.txt
analyst@b474d60fbeb6:~/reports/users$ cd /home/analyst/reports/users
analyst@b474d60fbeb6:~/reports/users$ ls
Q1_access.txt         Q2_access.txt         Q3_access.txt         Q4_access.txt
Q1_added_users.txt    Q2_added_users.txt    Q3_added_users.txt    Q4_added_users.txt
Q1_deleted_users.txt  Q2_deleted_users.txt  Q3_deleted_users.txt  Q4_deleted_users.txt
analyst@b474d60fbeb6:~/reports/users$ grep | "jhill" Q2_deleted_users.txt
Usage: grep [OPTION]... PATTERNS [FILE]...
Try 'grep --help' for more information.
-bash: jhill: command not found
analyst@b474d60fbeb6:~/reports/users$ ls /home/analyst/reports/users
Q1_access.txt         Q2_access.txt         Q3_access.txt         Q4_access.txt
Q1_added_users.txt    Q2_added_users.txt    Q3_added_users.txt    Q4_added_users.txt
Q1_deleted_users.txt  Q2_deleted_users.txt  Q3_deleted_users.txt  Q4_deleted_users.txt
analyst@b474d60fbeb6:~/reports/users$ grep "jhill" /home/analyst/reports/users/Q2_deleted_users.txt
1025         jhill     Sales
analyst@b474d60fbeb6:~/reports/users$ 
```

3. Search the Q4_added_users.txt file to list the users who were added to the Human Resources department.



```
Q4_access.txt
analyst@b474d60fbeb6:~/reports/users$ cd /home/analyst/reports/users
analyst@b474d60fbeb6:~/reports/users$ ls
Q1_access.txt         Q2_access.txt         Q3_access.txt         Q4_access.txt
Q1_added_users.txt    Q2_added_users.txt    Q3_added_users.txt    Q4_added_users.txt
Q1_deleted_users.txt  Q2_deleted_users.txt  Q3_deleted_users.txt  Q4_deleted_users.txt
analyst@b474d60fbeb6:~/reports/users$ grep | "jhill" Q2_deleted_users.txt
Usage: grep [OPTION]... PATTERNS [FILE]...
Try 'grep --help' for more information.
-bash: jhill: command not found
analyst@b474d60fbeb6:~/reports/users$ ls /home/analyst/reports/users
Q1_access.txt         Q2_access.txt         Q3_access.txt         Q4_access.txt
Q1_added_users.txt    Q2_added_users.txt    Q3_added_users.txt    Q4_added_users.txt
Q1_deleted_users.txt  Q2_deleted_users.txt  Q3_deleted_users.txt  Q4_deleted_users.txt
analyst@b474d60fbeb6:~/reports/users$ grep "jhill" /home/analyst/reports/users/Q2_deleted_users.txt
1025         jhill     Sales
analyst@b474d60fbeb6:~/reports/users$ cd /home/analyst/reports/users
analyst@b474d60fbeb6:~/reports/users$ grep "Human Resources" Q4_added_users.txt
1151         sshah     Human Resources
1145         msosa     Human Resources
analyst@b474d60fbeb6:~/reports/users$ 
```

Lab Summary: Filter with grep

Objective

This lab focused on filtering data in Linux using the grep command and piping. The exercises demonstrated how to locate error messages in log files, search for files with specific strings in their names, and extract details from user data files. These skills are essential for efficiently finding relevant information as a security analyst.

Tasks Completed

Task 1: Search for Error Messages in a Log File

- Navigated to /home/analyst/logs.
- Used grep "error" server_logs.txt to filter log entries.
- Returned only the lines containing the text string error.

Task 2: Find Files Containing Specific Strings

- Navigated to /home/analyst/reports/users.
- Used ls | grep "Q1" to list only the files that contained Q1 in their names.
- Used ls | grep "access" to list only the files that contained access in their names.

Task 3: Search More File Contents

- Displayed the files in /home/analyst/reports/users using ls.
- Used grep "jhill" Q2_deleted_users.txt to search for the username jhill. Confirmed that jhill was not listed.
- Used grep "Human Resources" Q4_added_users.txt to identify which users were added to the Human Resources department.

Summary

This lab demonstrated how to apply the grep command and piping to filter both file names and file contents in a Linux environment. These skills allow a security analyst to quickly locate error messages in logs, isolate user information, and filter files by keywords. Mastering these techniques is critical for efficient log analysis and system investigation.