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

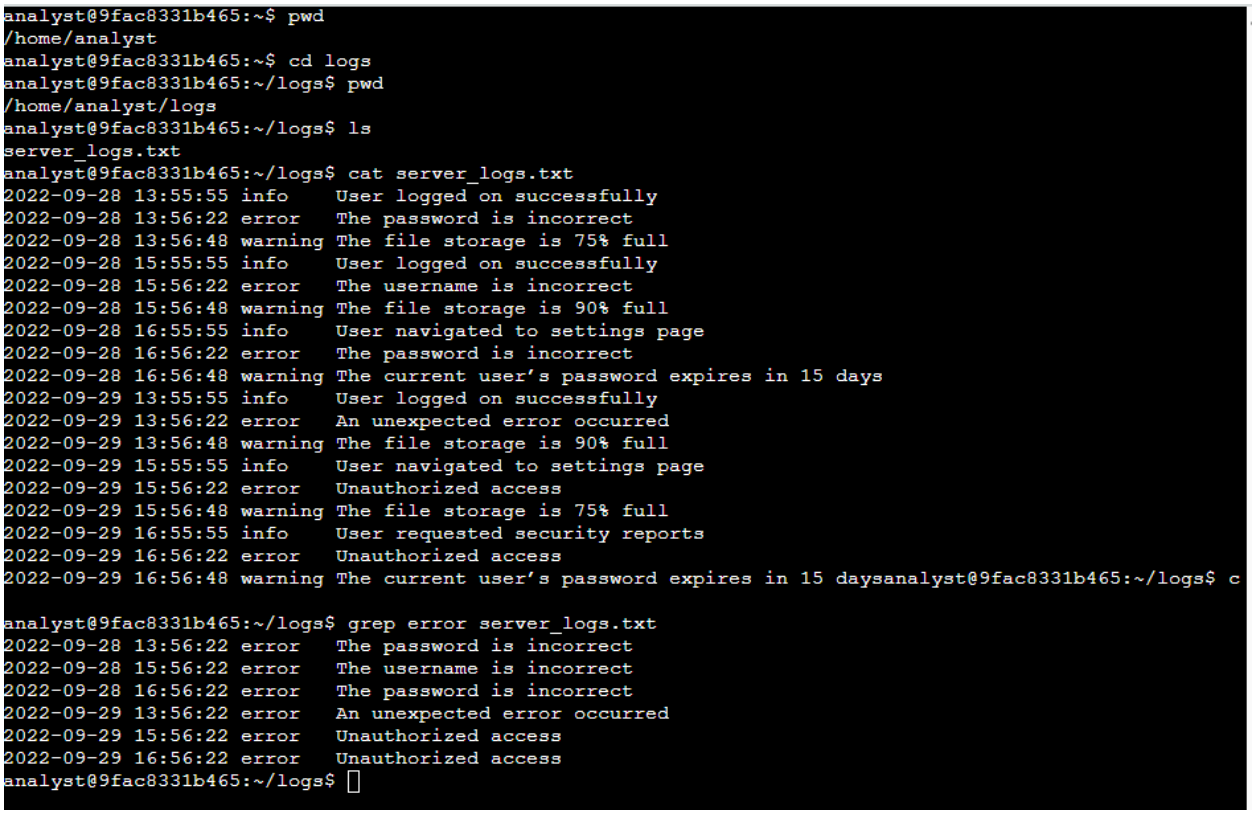
and search for files that contain a specific string in their names. **Finally**, you'll search for information contained in user files.

With that in mind, you're ready to practice what you've learned.

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`.



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

```
analyst@9fac8331b465:~$ ls
logs  project  reports  temp
analyst@9fac8331b465:~$ cd reports
analyst@9fac8331b465:~/reports$ ls
users
analyst@9fac8331b465:~/reports$ cd users
analyst@9fac8331b465:~/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@9fac8331b465:~/reports/users$ pwd
/home/analyst/reports/users
analyst@9fac8331b465:~/reports/users$ ^C
analyst@9fac8331b465:~/reports/users$ ^C
analyst@9fac8331b465:~/reports/users$ Task 2. Find files containing specific strings
-bash: Task: command not found
analyst@9fac8331b465:~/reports/users$
analyst@9fac8331b465:~/reports/users$ 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.
-bash: In: command not found
analyst@9fac8331b465:~/reports/users$
analyst@9fac8331b465:~/reports/users$
analyst@9fac8331b465:~/reports/users$
analyst@9fac8331b465:~/reports/users$ Navigate to the /home/analyst/reports/users directory.
-bash: Navigate: command not found
analyst@9fac8331b465:~/reports/users$
analyst@9fac8331b465:~/reports/users$ ls /home/analyst/reports/users | grep Q1
Q1_access.txt
Q1_added_users.txt
Q1_deleted_users.txt
analyst@9fac8331b465:~/reports/users$ ls /home/analyst/reports/users | grep access
Q1_access.txt
Q2_access.txt
Q3_access.txt
Q4_access.txt
analyst@9fac8331b465:~/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`.
3. Search the `Q4_added_users.txt` file to list the users who were added to the `Human Resources` department.