**Activity: Filter with grep**

**Overview:** 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:** 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.

**Start your lab:** click on “start lab” to start the lab.

**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.

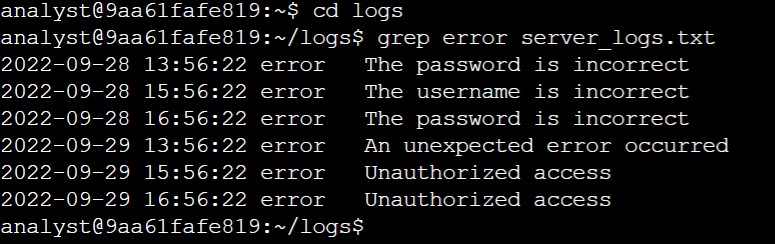
1. Navigate to the /home/analyst/logs directory.

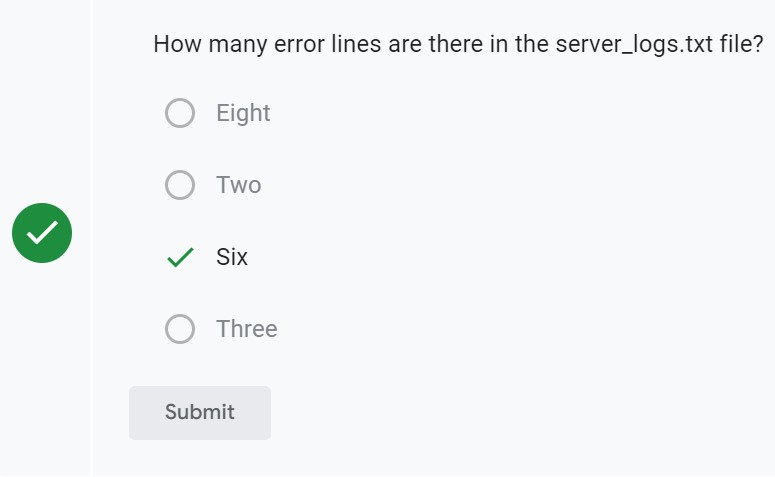
$ cd /home/analyst/logs

1. Use grep to filter the server\_logs.txt file, and return all lines containing the text string error.

$grep error server\_logs.txt

**Screenshots:**





**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.

$cd /home/analyst/reports/users

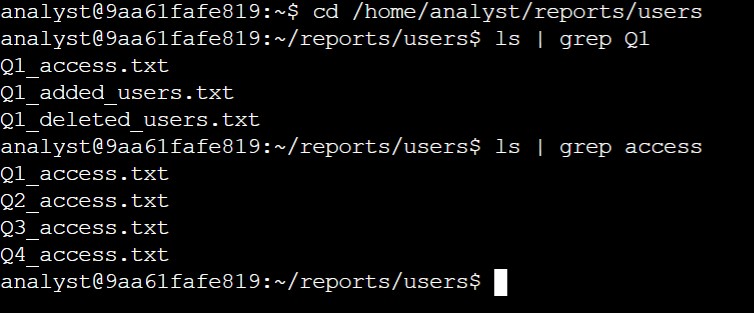
1. Using the pipe character (|), pipe the output of the ls command to the grep command to list only the files containing the string Q1 in their names.

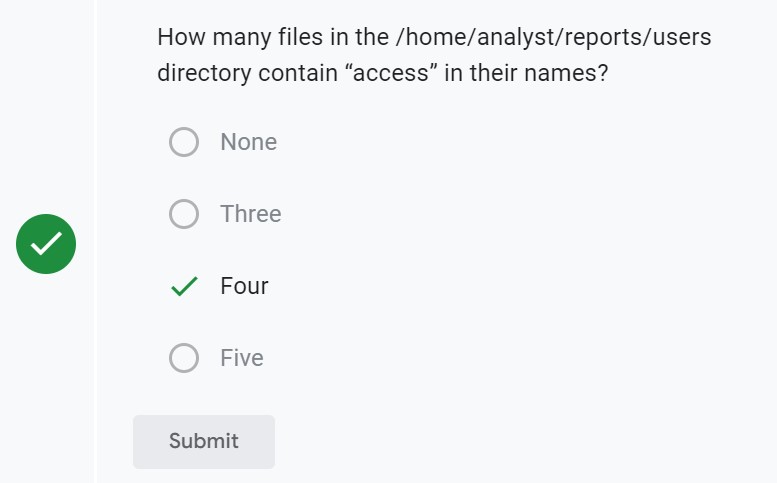
$ls | grep Q1

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

$ls | grep access

**Screenshots:**





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.

$cd /home/analyst/reports/users

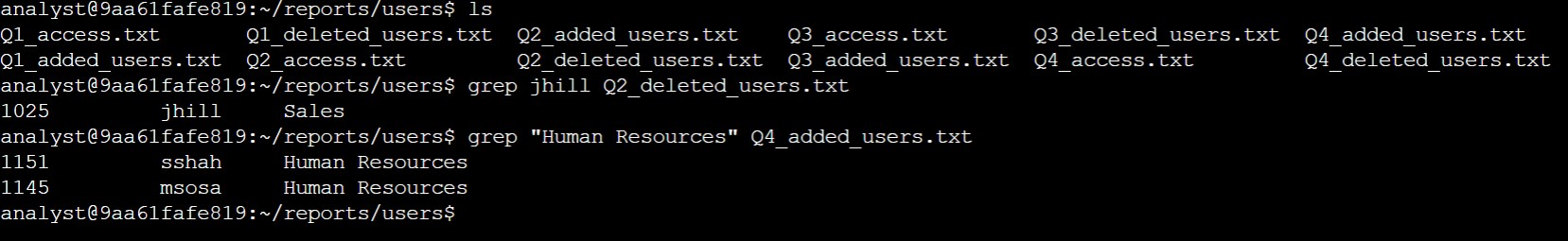
1. Search the Q2\_deleted\_users.txt file for the username jhill.

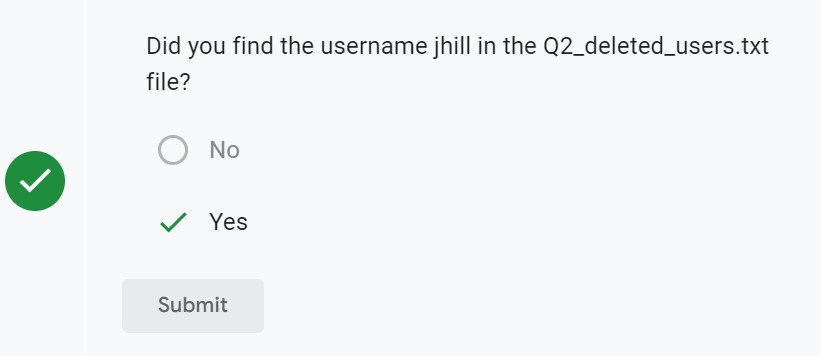
$grep jhill Q2\_deleted\_users.txt

1. Search the Q4\_added\_users.txt file to list the users who were added to the Human Resources department.

$grep “Human Resources” Q4\_added\_users.txt

**Screenshots:**





**Conclusion:**

I now have practical experience in using grep to:

* search for specific information contained in files, and
* find files containing specific strings that were piped into grep.