Personal Project:

Basic Log Analysis

# Project Overview:

Introduce the knowledge, skills, and abilities associated with analyzing computer log files by practicing with commands, profiling a single log file, and searching a log file.

# Tools:

* Ubuntu 22.04.1
* Terminal Emulator
* Practice logs

# Commands:

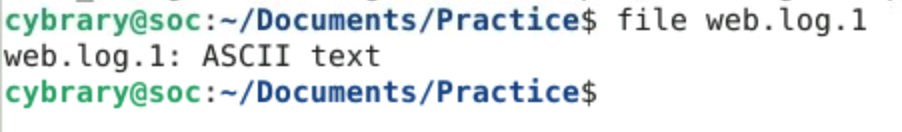
* cd – Change the shell working directory.
* file – Determine the type of file/s.
* cat – Concatenate file/s to a standard output.
* head – Print the first 10 lines of each file to standard output.
* tail – Print the last 10 lines of each file to standard output.
* ls – List information about files (the current directory by default).
* wc – Print newline, word, and byte counts for each file, and a total line if more than one file is specified.
* more – A file perusal filter for CRT viewing.
* less – Similar to the more command but has many more features.
* egrep – Search for patterns in each file.

# Instructions:

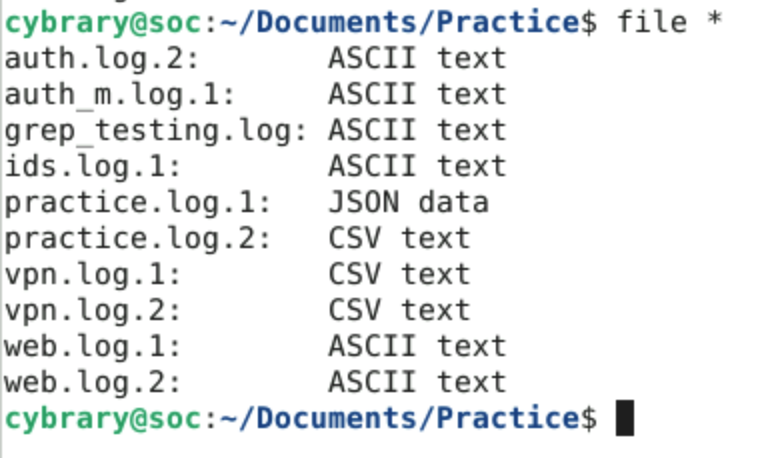
# Part 1: Command Practice

Introduce and practice with a few basic commands that will help to profile logs (i.e., learn about log files so that we know what we're about to analyze).

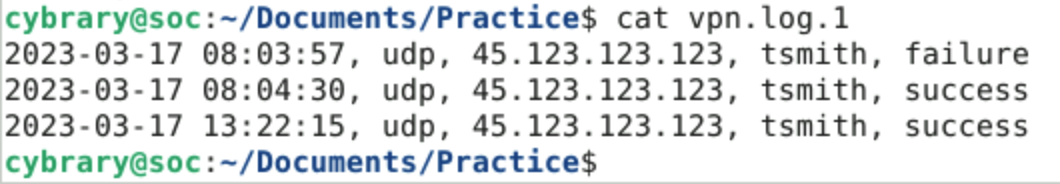
1. On the dock, click the **Terminal icon**to launch a new Terminal window.
2. At the command prompt, execute **cd /home/cybrary/Documents/Practice**to change your current directory.
3. At the command prompt, execute **file web.log.1**to display the file type for the web.log.1 file.



1. At the command prompt, execute **file \***to display the file type of all files in the current directory.

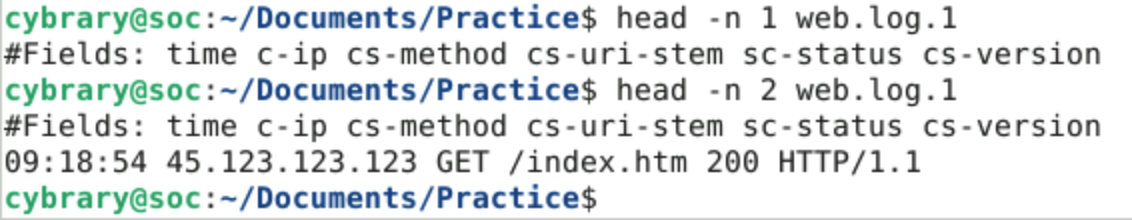


1. At the command prompt, execute **cat vpn.log.1**to display the contents of the vpn.log.1 file.



From the output of this command, you should be able to answer the following questions:  
  
> How many lines does it contain? 3  
> Does it appear to have one or more lines per log record? No

1. At the command prompt, execute **head -n 1 web.log.1**to display the first line of the file web.log.1, then execute **head -n 2 web.log.1**to display the first and second lines of the file web.log.1.



1. At the command prompt, execute **cat web.log.2**to display the file web.log.2, then execute **head -n 2 web.log.2**to view the first two lines of the web.log.2 file.

A close up of a computer screen

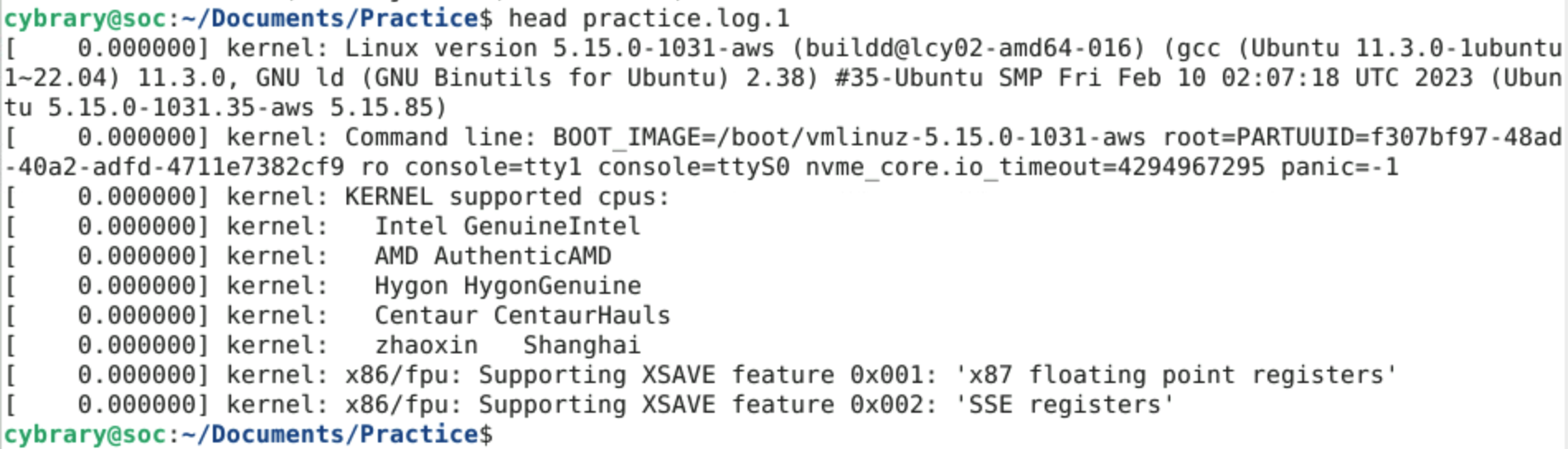
Description automatically generated



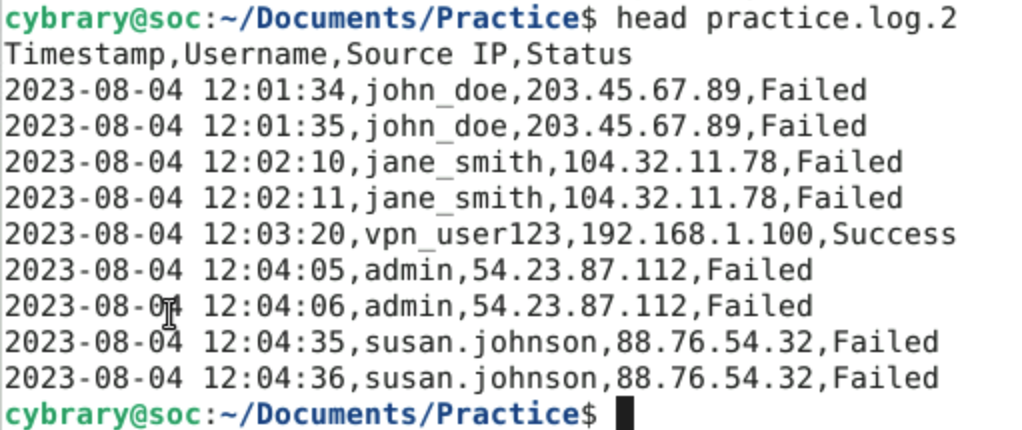
Based on what you see:  
  
> What is the date and time of the earliest record? 2023-06-27 00:13:00  
> Were you able to see the earliest record when you used the cat command on this file? Yes

**Part 2: Profiling a Single Log File**

1. **Identify your analysis objective.**  
     
   **Objective A:**Identify any "test" user accounts that have successfully authenticated via VPN as can be observed in the appropriate log file(s).  
     
   **Objective B:**Identify the source IP address from which each "test" account was used to make the VPN connections identified in Objective A.  
     
   **Objective C:**Identify any other user accounts used for VPN authentications with the same source IP address as the "test" account(s).
2. **Get the right log.**  
     
   You can find the log for this exercise at **/home/cybrary/Documents/Practice**. There are two files in this location named **practice.log.1**and **practice.log.2**  
     
   Here are some example commands to show the first 10 lines of each log. (The **head**command shows the first 10 lines by default).  
   $ head practice.log.1

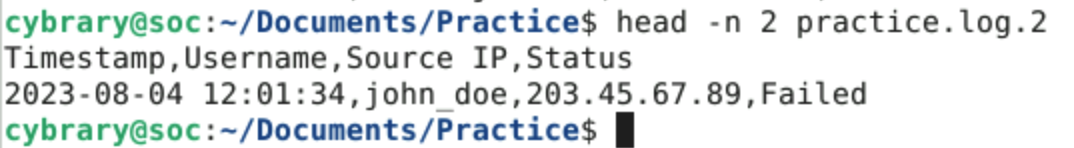


$ head practice.log.2

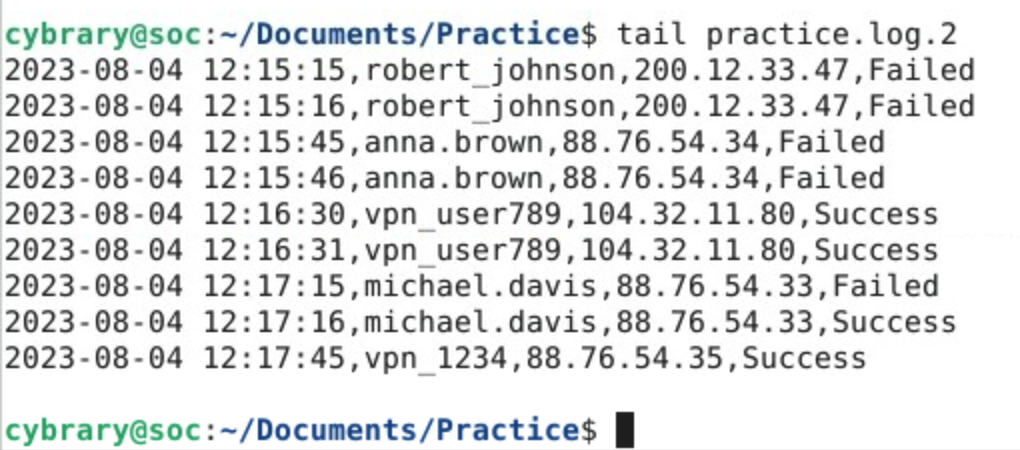


Based on what you see, which file most likely contains VPN logs? practice.log.2

1. **Verify the log's time coverage.**  
     
   $ head -n 2 practice.log.2

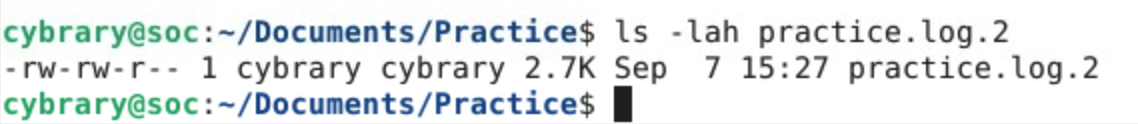


$ tail practice.log.2

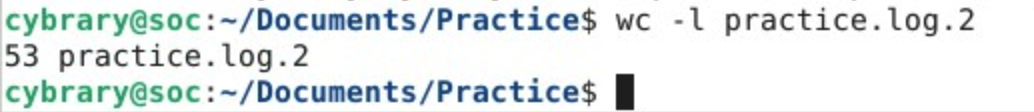


Based upon the results of those commands, you should be able to answer the following questions:  
  
> Is a time zone expressed in the header row? If so, what is it? No  
> What is the earliest date/time in the log? 2023-08-04 12:01:34  
> What is the latest date/time in the log? 2023-08-04 12:17:45

1. **Identify the log's size.**  
     
   Check the file size using the **ls**command with the **-lah**options.   
     
   $ ls -lah practice.log.2



Check the number of lines in the log using the **wc**command with the **-l**option.   
  
$ wc -l practice.log.2

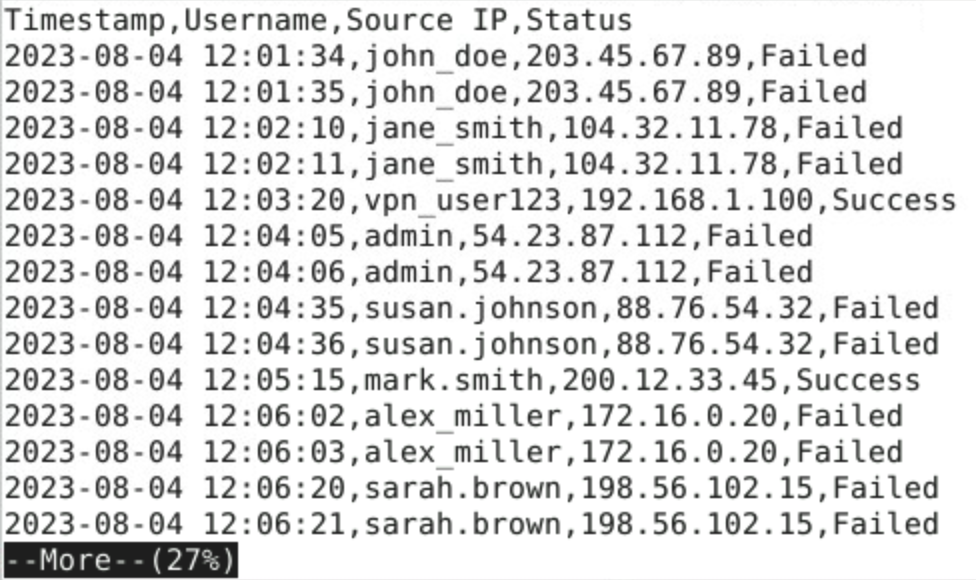


1. **Preview log contents.**  
     
   $ head practice.log.2

A screenshot of a computer

Description automatically generated

Use the **more**command in Linux to scroll through the log a bit (by pressing the space bar after the command) if the log file is longer and you'd like to look through more than the first few lines. Alternatively, the **less** command can also be used.  
  
$ more practice.log.2



1. **Select an analysis technique likely to resolve your objective.**At this point we should have the correct file, know the time zone assigned to recorded data, and have a sense of the file size and number of lines. Given the small log size in this example, you could elect to simply read the log manually, but since we're learning new skills here, we will practice with search.

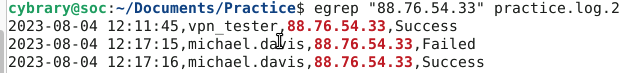
**Part 3: Searching a Log File**

1. **Select search terms.**  
     
   Given that our objective is to identify specific, successful authentications, we now need to get a little more specific and select our search term. Objective A asks us to begin specifically with "test" accounts, however it does not tell us what those accounts are actually named. A possible first search term could be the term **test**(non-case sensitive).
2. **Execute search.**  
     
   From the command line, search for the term "test" (non-case sensitive) in the practice.log.2 file using the command **egrep -i "test" practice.log.2**.   
     
   $ egrep -i "test" practice.log.2

Embedded image

From your results, you can answer the following questions.  
  
> What is the name or names of the user accounts observed in the results? vpn\_tester  
> What is the source IP address or address(es) observed in the results? 88.76.54.33

1. **Repeat as necessary to fulfill your objectives.**  
   Running another search: From the command line run the command **egrep "88.76.54.33" practice.log.2**to find records associated with the IP address that you discovered in your search in Step 2.  
     
   $ egrep "88.76.54.33" practice.log.2



From your results, consider the following questions.  
  
> Was the IP address 88.76.54.33 the source of any attempted VPN authentications for different user names? Yes  
> If so, what were the usernames and were any of those authentication attempts successful? michael.davis, there was a successful attempt