**BASH - Log File Analyzer**

A script that scans through log files for specific patterns (e.g., failed login attempts), helping users understand how to analyze logs for security incidents.

#!/bin/bash

# Check if the user provided a log file

if [ "$#" -ne 1 ]; then

echo "Usage: $0 <logfile>"

exit 1

fi

LOGFILE=$1

echo "Analyzing log file: $LOGFILE"

# Count failed login attempts (assuming the log format includes 'Failed password')

grep 'Failed password' "$LOGFILE" | wc -l

# List unique IP addresses with failed attempts

echo "Unique IP addresses with failed attempts:"

grep 'Failed password' "$LOGFILE" | awk '{print $11}' | sort | uniq

echo "Analysis complete."

**Instructions:**

1. **Save the Script**: Copy the above script into a file, e.g., log\_analyzer.sh.
2. **Make It Executable**: Change the permissions of the script to make it executable:

chmod +x log\_analyzer.sh

1. **Run the Script**: Execute the script by providing the log file:

./ log\_analyzer.sh auth.log

1. **Capture:** Get a screenshot of the output from the script.

**Lab:** Put the screen capture in a word document and answer the following question:  
  
Discuss the importance of log analysis in incident response and security monitoring.