Assignment 1: Text Processing and Automation - Write a bash script that uses grep, sed, and awk to list all login attemtps to a linux system, extract attempted

user and error messages to a separate file.

SOLUTION:

Administrator@DESKTOP-TIC5DM4 MINGW64 ~/Desktop/LOG_FILE (master)

$ git init

Reinitialized existing Git repository in C:/Users/Administrator/Desktop/LOG_FILE

Administrator@DESKTOP-TIC5DM4 MINGW64 ~/Desktop/LOG_FILE (master)

$ cat login_attempts.txt

Accepted password for user1 from 192.168.1.100 port 51432 ssh2

Failed password for invalid user guest from 192.168.1.101 port 61234 ssh2

Accepted password for user2 from 10.0.0.5 port 41852 ssh2

Failed password for user2 from 10.0.0.5 port 41852 ssh2

Failed password for invalid user admin from 172.16.0.2 port 32245 ssh2

Accepted password for user3 from 172.16.0.3 port 54012 ssh2

Failed password for root from 203.0.113.42 port 39281 ssh2

Accepted password for root from 203.0.113.42 port 39281 ssh2

Failed password for user4 from 198.51.100.23 port 49503 ssh2

Failed password for user4 from 198.51.100.23 port 49503 ssh2

Accepted publickey for user5 from 192.0.2.45 port 40322 ssh2

Failed password for user5 from 192.0.2.45 port 40322 ssh2

Failed password for root from 203.0.113.98 port 23412 ssh2

Accepted password for user6 from 192.168.1.102 port 65231 ssh2

Failed password for user6 from 192.168.1.102 port 65231 ssh2

Failed password for invalid user test from 198.51.100.56 port 48412 ssh2

Accepted password for user7 from 192.0.2.200 port 31214 ssh2

Failed password for user8 from 203.0.113.75 port 49218 ssh2

Accepted password for user8 from 203.0.113.75 port 49218 ssh2

Failed password for root from 198.51.100.89 port 62145 ssh2

Administrator@DESKTOP-TIC5DM4 MINGW64 ~/Desktop/LOG_FILE (master)

$ cat login_attempts.txt |grep "Failed password"

Failed password for invalid user guest from 192.168.1.101 port 61234 ssh2

Failed password for user2 from 10.0.0.5 port 41852 ssh2

Failed password for invalid user admin from 172.16.0.2 port 32245 ssh2

Failed password for root from 203.0.113.42 port 39281 ssh2

Failed password for user4 from 198.51.100.23 port 49503 ssh2

Failed password for user4 from 198.51.100.23 port 49503 ssh2

Failed password for user5 from 192.0.2.45 port 40322 ssh2

Failed password for root from 203.0.113.98 port 23412 ssh2

Failed password for user6 from 192.168.1.102 port 65231 ssh2

Failed password for invalid user test from 198.51.100.56 port 48412 ssh2

Failed password for user8 from 203.0.113.75 port 49218 ssh2

Failed password for root from 198.51.100.89 port 62145 ssh2

Administrator@DESKTOP-TIC5DM4 MINGW64 ~/Desktop/LOG_FILE (master)

$ cat login_attempts.txt |sed '/Failed password/invalid user/'

Accepted password for user1 from 192.168.1.100 port 51432 ssh2

nvalid user/

Failed password for invalid user guest from 192.168.1.101 port 61234 ssh2

Accepted password for user2 from 10.0.0.5 port 41852 ssh2

nvalid user/

Failed password for user2 from 10.0.0.5 port 41852 ssh2

nvalid user/

Failed password for invalid user admin from 172.16.0.2 port 32245 ssh2

Accepted password for user3 from 172.16.0.3 port 54012 ssh2

nvalid user/

Failed password for root from 203.0.113.42 port 39281 ssh2

Accepted password for root from 203.0.113.42 port 39281 ssh2

Failed password for user4 from 198.51.100.23 port 49503 ssh2

nvalid user/

Failed password for user4 from 198.51.100.23 port 49503 ssh2

Accepted publickey for user5 from 192.0.2.45 port 40322 ssh2

nvalid user/

Failed password for user5 from 192.0.2.45 port 40322 ssh2

nvalid user/

Failed password for root from 203.0.113.98 port 23412 ssh2

Accepted password for user6 from 192.168.1.102 port 65231 ssh2

nvalid user/

Failed password for user6 from 192.168.1.102 port 65231 ssh2

nvalid user/

Failed password for invalid user test from 198.51.100.56 port 48412 ssh2

Accepted password for user7 from 192.0.2.200 port 31214 ssh2

nvalid user/

Failed password for user8 from 203.0.113.75 port 49218 ssh2

Accepted password for user8 from 203.0.113.75 port 49218 ssh2

nvalid user/

Failed password for root from 198.51.100.89 port 62145 ssh2

Administrator@DESKTOP-TIC5DM4 MINGW64 ~/Desktop/LOG_FILE (master)

$ cat login_attempts.txt |awk '{print $0}'

Accepted password for user1 from 192.168.1.100 port 51432 ssh2

Failed password for invalid user guest from 192.168.1.101 port 61234 ssh2

Accepted password for user2 from 10.0.0.5 port 41852 ssh2

Failed password for user2 from 10.0.0.5 port 41852 ssh2

Failed password for invalid user admin from 172.16.0.2 port 32245 ssh2

Accepted password for user3 from 172.16.0.3 port 54012 ssh2

Failed password for root from 203.0.113.42 port 39281 ssh2

Accepted password for root from 203.0.113.42 port 39281 ssh2

Failed password for user4 from 198.51.100.23 port 49503 ssh2

Failed password for user4 from 198.51.100.23 port 49503 ssh2

Accepted publickey for user5 from 192.0.2.45 port 40322 ssh2

Failed password for user5 from 192.0.2.45 port 40322 ssh2

Failed password for root from 203.0.113.98 port 23412 ssh2

Accepted password for user6 from 192.168.1.102 port 65231 ssh2

Failed password for user6 from 192.168.1.102 port 65231 ssh2

Failed password for invalid user test from 198.51.100.56 port 48412 ssh2

Accepted password for user7 from 192.0.2.200 port 31214 ssh2

Failed password for user8 from 203.0.113.75 port 49218 ssh2

Accepted password for user8 from 203.0.113.75 port 49218 ssh2

Failed password for root from 198.51.100.89 port 62145 ssh2

```
# Path to the log file where login attempts are recorded
LOG_FILE="/var/log/auth.log"

# Path to the file where attempted users and error messages will be saved
OUTPUT_FILE="login_attempts.txt"

# Use grep to filter out lines containing "Failed password" from the log file
```

```
grep "Failed password" "$LOG_FILE" | \

# Use sed to extract the username from the filtered lines
sed -nE 's/.*Failed password for (invalid user )?([^ ]+).*/\2/p' | \

# Use awk to remove duplicate entries and save to the output file
awk '!seen[$0]++' > "$OUTPUT_FILE"

echo "Login attempts extracted and saved to $OUTPUT_FILE"
```

1. It uses grep to filter out lines containing "Failed password" from the specified log file.
2. It uses sed to extract the usernames from the filtered lines. It handles cases where the user might be marked as "invalid user".
3. It uses awk to remove any duplicate entries and saves the unique usernames along with error messages to the specified output file.
4. Finally, it prints a message indicating where the extracted login attempts are saved.