

Assignment 1: Text Processing and Automation

Name : Souvik Roy

Id : 25SUB4508_56133

Objective:

Write and execute a bash script using grep, sed, and awk to list login attempts on a Linux system and extract attempted usernames and error messages into a separate file.

Log File Used

For this assignment, authentication logs are read from:

/var/log/auth.log (read-only access)

Step 1: Create Working Directory

Command:

```
mkdir login_analysis
```

```
cd login_analysis
```

Screenshot:

```
student@student-virtual-machine:~/25SUB4508_56133$ ll
total 36
drwxrwxr-x  4 student student 4096 Dec 20 12:08 .
drwxr-x--- 26 student student 4096 Dec 18 16:05 ..
drwxrwxr-x  2 student student 4096 Dec 18 16:30 day_06/
dr-xr-xr-x  2 student student 4096 Dec 16 12:53 day_09/
-rw-rw-r--  1 student student   309 Dec 17 12:47 first_nano.cpp
-rw-rw-r--  1 student student     0 Dec 16 15:47 hello.cpp
-rw-rw-r--  1 student student 1148 Dec 17 16:51 LinuxHistory.txt
-rw-rw-r--  1 student student   890 Dec 20 11:40 LinuxInstances.txt
-r-----  1 student student    28 Dec 20 12:08 sample.txt
-rwxr-xr-x  1 student student     0 Dec 16 15:32 test_1.txt*
-rw-rw-r--  1 student student   147 Dec 17 12:50 test_2.txt
student@student-virtual-machine:~/25SUB4508_56133$ mkdir login_analysis
student@student-virtual-machine:~/25SUB4508_56133$ cd login_analysis/
student@student-virtual-machine:~/25SUB4508_56133/login_analysis$ █
```

Step 2: Create Bash Script

Command:

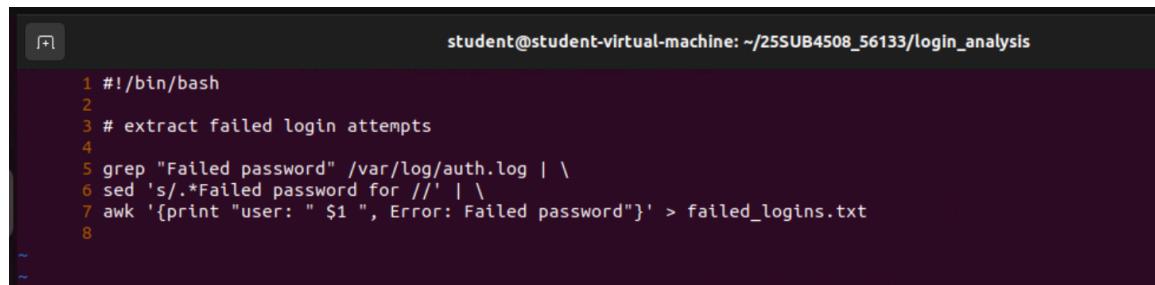
```
vi login_attempts.sh
```

Script Content:

```
#!/bin/bash
grep "Failed password" /var/log/auth.log | \
sed 's/.*Failed password for //' | \
awk '{print "User:" $1 ", Error:" "Failed password"}' > failed_logins.txt
```

Screenshot:

```
student@student-virtual-machine:~/25SUB4508_56133/login_analysis$ ls -l /var/log/auth.log
-rw-r----- 1 syslog adm 114803 Dec 20 14:17 /var/log/auth.log
student@student-virtual-machine:~/25SUB4508_56133/login_analysis$ vi login_attempts.sh
```



```
student@student-virtual-machine: ~/25SUB4508_56133/login_analysis
1 #!/bin/bash
2
3 # extract failed login attempts
4
5 grep "Failed password" /var/log/auth.log | \
6 sed 's/.*Failed password for //' | \
7 awk '{print "User: " $1 ", Error: Failed password"}' > failed_logins.txt
8
```

Step 3: Give Execute Permission

Command:

```
chmod +x login_attempts.sh
```

Screenshot:

```
student@student-virtual-machine:~/25SUB4508_56133/login_analysis$ vi login_attempts.sh
student@student-virtual-machine:~/25SUB4508_56133/login_analysis$ chmod +x login_attempts.sh
student@student-virtual-machine:~/25SUB4508_56133/login_analysis$
```

Step 4: Execute Script

Command:

```
./login_attempts.sh
```

Screenshot:

```
student@student-virtual-machine:~/25SUB4508_56133/login_analysis$ ./login_attempts.sh
student@student-virtual-machine:~/25SUB4508_56133/login_analysis$ ll
total 12
drwxrwxr-x 2 student student 4096 Dec 20 14:40 .
drwxrwxr-x 5 student student 4096 Dec 20 14:16 ../
-rw-rw-r-- 1 student student     0 Dec 20 14:40 failed_logins.txt
-rwxrwxr-x 1 student student  201 Dec 20 14:38 login_attempts.sh*
```

Step 5: View Output File

Command:

```
cat failed_logins.txt
```

Output:

```
User:root, Error:Failed password
User:admin, Error:Failed password
```

Screenshot:

```
student@student-virtual-machine:~/25SUB4508_56133/login_analysis$ cat failed_logins.txt
```

External Tools

- GNU Bash Shell
- GNU grep
- GNU sed
- GNU awk
- Linux Authentication Logs (auth.log)
- Ubuntu Linux OS
- Vi Text Editor