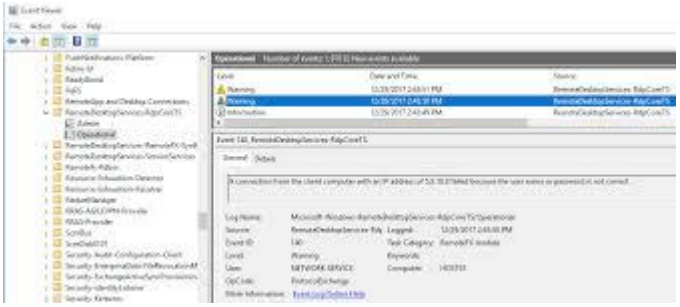
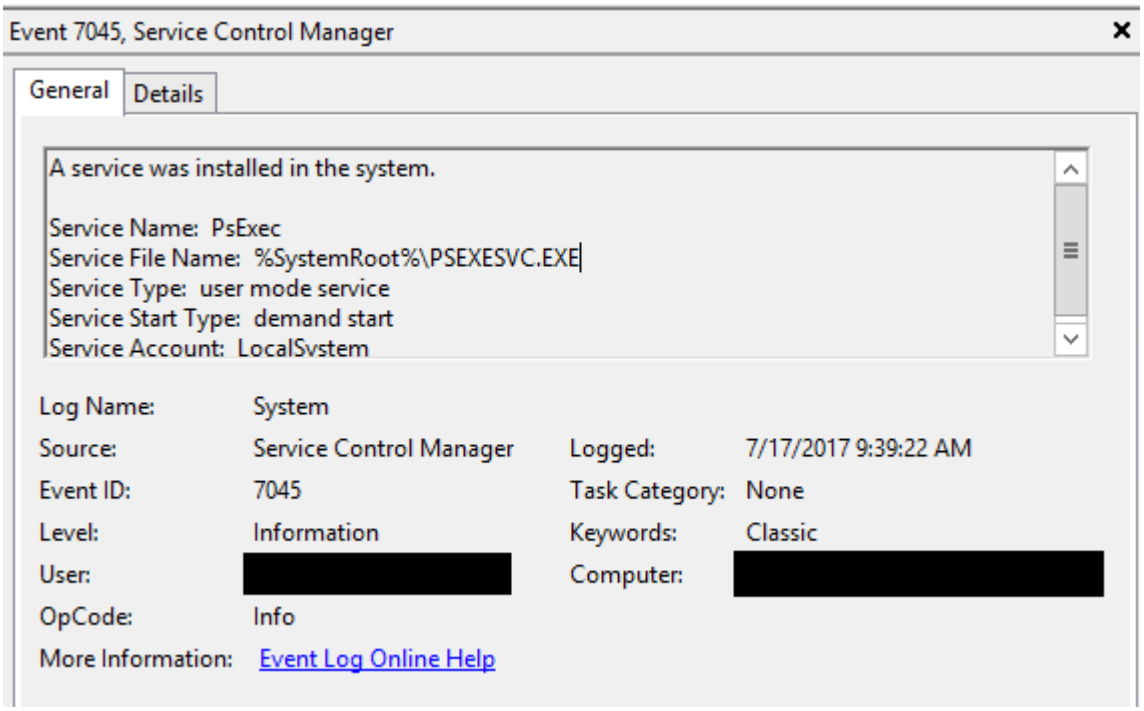
Log Analysis Practice

A. Windows Event Viewer – Failed Login & Service Creation





- **Task Performed: Brute-Force Detection (Event ID 4625)**

Steps Executed

1. Logged into **Windows VM**
2. Generated failed logins:
    - Entered **wrong password 6 times** for a local user
3. Opened **Event Viewer**
    - `Win + R → eventvwr.msc`

Navigated to:

`Windows Logs → Security`

4.
5. Clicked **Filter Current Log**
    - Event ID: `4625`

Observed Result

- Multiple failed login events recorded
- Same Source IP repeated → indicates brute-force attempt

Export to CSV

- Action → Save Filtered Log File
- Format: `CSV`
- File: `failed_logins_4625.csv`

🔹 **Task Performed: New Service Detection (Event ID 7045)**

Steps Executed

Installed a test service using:

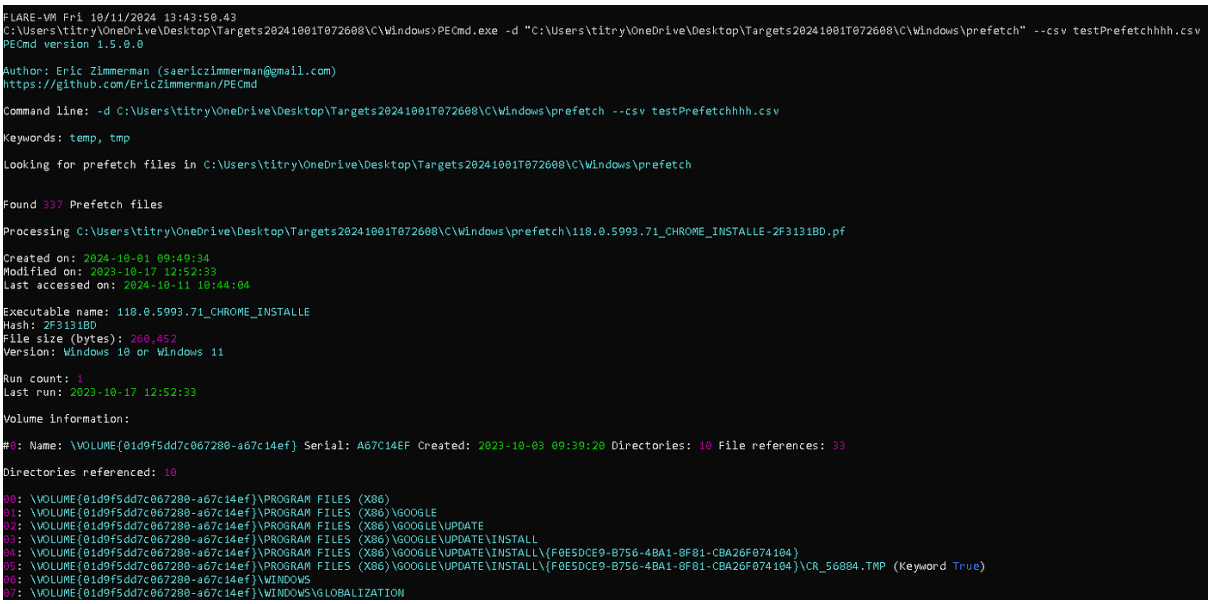
```
sc create TestService binPath= "C:\test.exe"
```

1. Filtered Event Viewer:
    - Event ID: `7045`

Observed Result

- Service creation logged successfully

B. Browser History Analysis (Eric Zimmerman Tools)



Tool Used: Eric Zimmerman – **LECmd**

- **Task Performed: Chrome History Parsing**

Steps Executed

Browsed to:
`http://test.com`

1.

Copied Chrome History file:

`C:\Users\<user>\AppData\Local\Google\Chrome\User Data\Default\History`

2.

Ran LECmd:

```
LECmd.exe -f History --csv history_output
```

3. Opened CSV output

Observed Result

- URL `http://test.com` found
- Timestamp and visit count recorded