

# Log Analysis Practice

## A. Windows Event Viewer – Failed Login & Service Creation

The image contains two screenshots of Windows Event Viewer and Service Control Manager.

**Event Viewer Screenshot:**

- Shows the "Windows Logs" section with "Failed Logins" selected.
- Details pane shows two entries:
  - Event ID: 4625, Level: Warning, Source: RemoteDesktopServices\_RdpClient, Date/Time: 12/29/2017 2:48:01 PM, Message: A connection from the client computer with an IP address of 23.10.12.1 tried to log on with the user name or password incorrect.
  - Event ID: 4625, Level: Warning, Source: RemoteDesktopServices\_RdpClient, Date/Time: 12/29/2017 2:48:31 PM, Message: A connection from the client computer with an IP address of 23.10.12.1 tried to log on with the user name or password incorrect.

**Service Control Manager Screenshot:**

- Shows the "Event 7045, Service Control Manager" window.
- General tab details:
  - A service was installed in the system.
  - Service Name: PsExec
  - Service File Name: %SystemRoot%\PSEXESVC.EXE
  - Service Type: user mode service
  - Service Start Type: demand start
  - Service Account: LocalSystem
- Log Name: System
- Source: Service Control Manager
- Event ID: 7045
- Level: Information
- User: [REDACTED]
- OpCode: Info
- Logged: 7/17/2017 9:39:22 AM
- Task Category: None
- Keywords: Classic
- Computer: [REDACTED]
- More Information: [Event Log Online Help](#)

- ◆ 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)

```
FLARE-VM Fri 10/11/2024 13:43:50.43
C:\Users\titry\OneDrive\Desktop\Targets20241001T072608\C\Windows\PECmd.exe -d "C:\Users\titry\OneDrive\Desktop\Targets20241001T072608\C\Windows\prefetch" --csv testPrefetchhhh.csv
PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -d C:\Users\titry\OneDrive\Desktop\Targets20241001T072608\C\Windows\prefetch --csv testPrefetchhhh.csv

Keywords: temp, tmp

Looking for prefetch files in C:\Users\titry\OneDrive\Desktop\Targets20241001T072608\C\Windows\prefetch

Found 337 Prefetch files

Processing C:\Users\titry\OneDrive\Desktop\Targets20241001T072608\C\Windows\prefetch\118.0.5993.71_CHROME_INSTALL-2F3131BD.pdf

Created on: 2024-10-01 09:49:34
Modified on: 2023-10-17 12:52:33
Last accessed on: 2024-10-11 10:44:04

Executable name: 118.0.5993.71_CHROME_INSTALL
Hash: 2F3131BD
File size (bytes): 268,452
Version: Windows 10 or Windows 11

Run count: 1
Last run: 2023-10-17 12:52:33

Volume information:

#0: Name: \VOLUME{01d9f5dd7c067280-a67c14ef} Serial: A67C14EF Created: 2023-10-03 00:39:20 Directories: 10 File references: 33
Directories referenced: 10

#0: \VOLUME{01d9f5dd7c067280-a67c14ef}\PROGRAM FILES (X86)
#1: \VOLUME{01d9f5dd7c067280-a67c14ef}\PROGRAM FILES (X86)\GOOGLE
#2: \VOLUME{01d9f5dd7c067280-a67c14ef}\PROGRAM FILES (X86)\GOOGLE\UPDATE
#3: \VOLUME{01d9f5dd7c067280-a67c14ef}\PROGRAM FILES (X86)\GOOGLE\UPDATE\INSTALL
#4: \VOLUME{01d9f5dd7c067280-a67c14ef}\PROGRAM FILES (X86)\GOOGLE\UPDATE\INSTALL\{F0E5DCE9-B756-4BA1-8F01-CBA26F074104}
#5: \VOLUME{01d9f5dd7c067280-a67c14ef}\PROGRAM FILES (X86)\GOOGLE\UPDATE\INSTALL\{F0E5DCE9-B756-4BA1-8F01-CBA26F074104}\OR_56084.TMP (Keyword True)
#6: \VOLUME{01d9f5dd7c067280-a67c14ef}\WINDOWS
#7: \VOLUME{01d9f5dd7c067280-a67c14ef}\WINDOWS\GLOBALIZATION
```

### 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