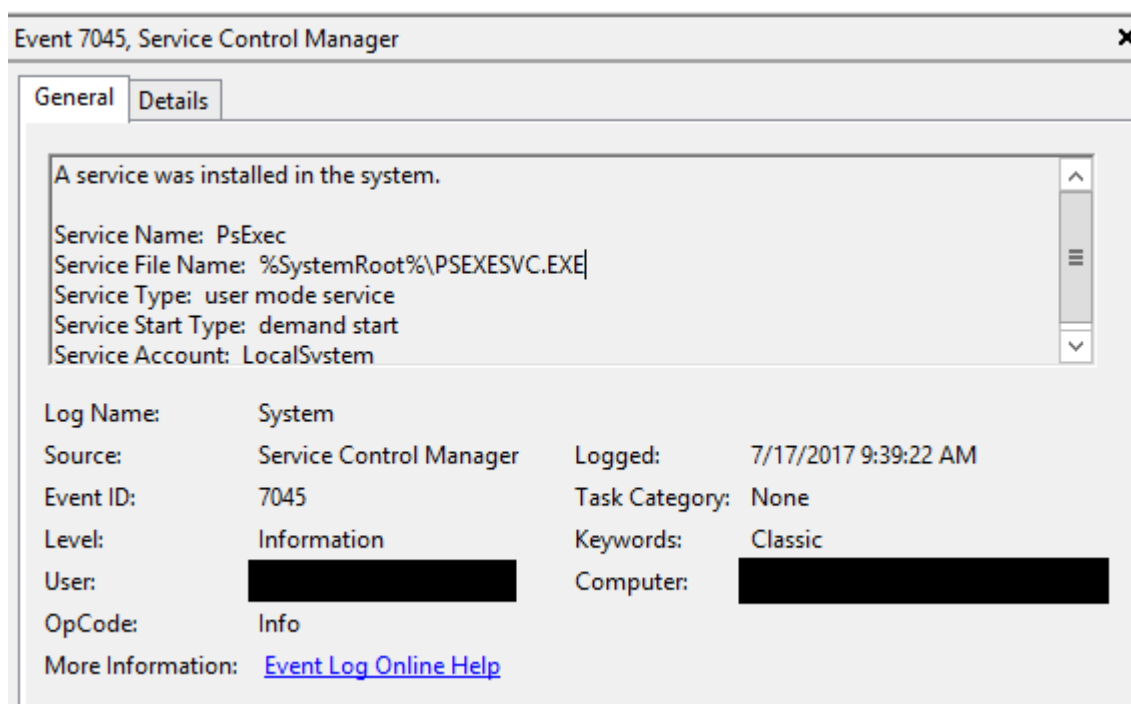
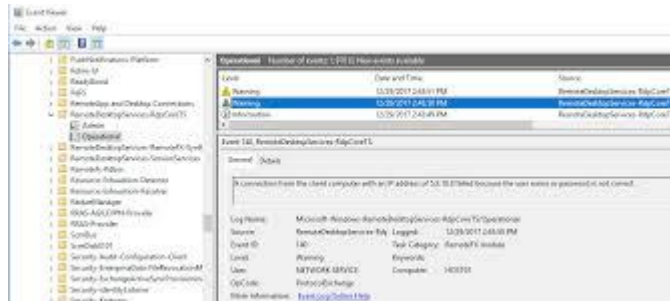


Log Analysis Practice

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)

```
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.pf

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): 260,452
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 09:39:20 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-B756-4BA1-8F81-CBA26F074104}
#5: \VOLUME{01d9f5dd7c067280-a67c14ef}\PROGRAM FILES (X86)\GOOGLE\UPDATE\INSTALL\F0E5DCE9-B756-4BA1-8F81-CBA26F074104}\CR_50004.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