Finding Forensic Goodness In Obscure Windows Event Logs

Nasreddine Bencherchali · Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

If you've been doing some digital forensics or threat hunting for some time. You'll know that one of the key sources of information are the Windows event logs. Most of the talks around the windows event logs only mention the "main" sources of logs such as "System" or "Application", even though windows provide many sources.

To get the full logging experience one need to enable additional logging from the ***Group Policy Editor*** or even installs something like ***Sysmon*** but what to do in the case where one cannot install or enable the aforementioned logs? Or let's say you're performing an investigation and the machine has only default

Medium

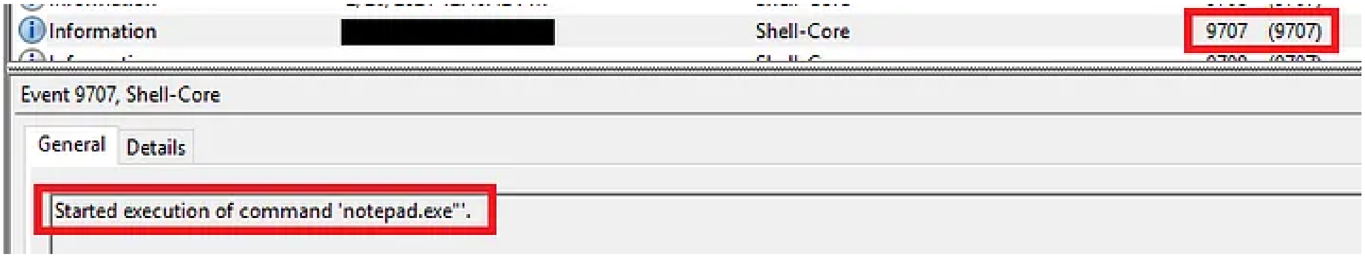
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Information [redacted] Shell-Core 9707 (9707)

Event 9707, Shell-Core

Started execution of command 'notepad.exe"'.

- **EID 9708 :** Detects when the aforementioned process finishes execution with the corresponding PID (Useful when the process is still running on the system).

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

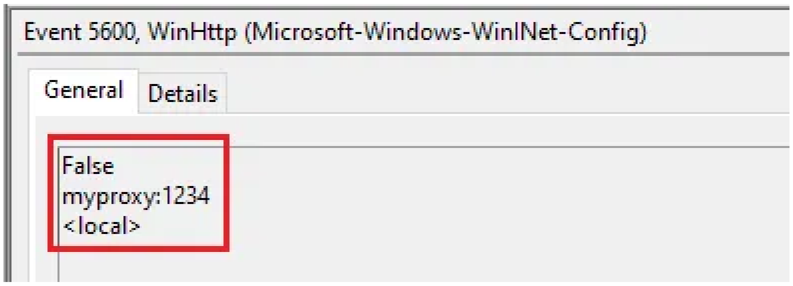
✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

- **EID 5600 :** Indicates change in the proxy configuration. For example if i change my proxy configuration from the “Internet Option” menu. The event will get generated.



```
False
myproxy:1234
<local>
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

OAlerts (Office Alerts)

- **EID 300 :** Triggers when a prompt is shown inside an office application. For example when the prompt to save the office (excel, word…etc) document is shown an event is generated. Contains information about the name of the files (In the case of saving a file), the office version, the office application that triggered the alert (Word, PowerPoint, Excel…etc).

This event can be used to determine if a suspicious for example file has been opened or altered in some way by a user.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

- **EID 811/812 :** Triggers when a user logon to a machine. You can check for the "<SessionEnv>" subscriber notification in EID 811 to indicates that a user logged on via RDP.

Note that as far as i can tell the *"SessionEnv"* subscriber is also logged when a user logon to a machine for the first time (I.E doesn't have a session). To distinguish between the two (RDP or Local) look for the EID 1/2 shortly after the "SessionEnv" subscriber to indicate a local logon and if not present that means its an RDP logon.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

If the password is correct, then the “Result Code : 0” is generated.

Microsoft-Windows-Windows Firewall With Advanced Security/Firewall

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Conclusion

We've taken a look at a couple of event logs that can be very useful during an investigation or a threat hunt. If you have other suggestions of events that should be added or noticed an error of some kind drop me a DM on twitter @nas_bench

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

I write about #Detection, #Sigma and #Windows. Follow https://github.com/nasbench/Misc-Research for interesting Windows tidbits

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app