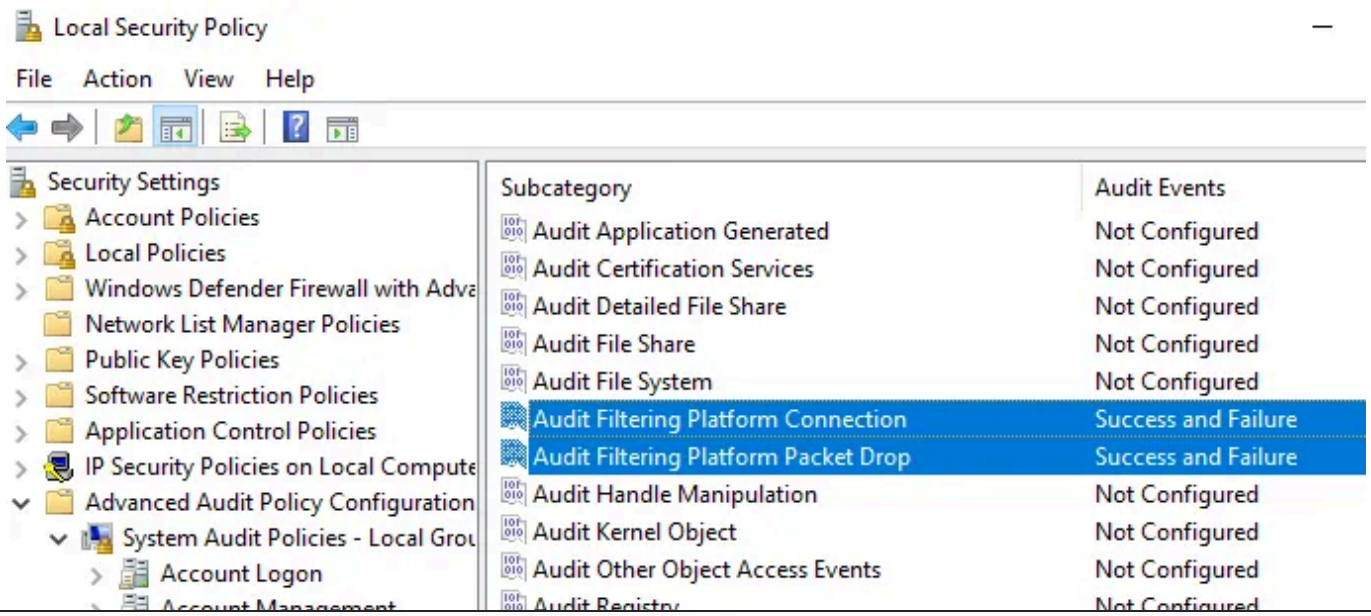
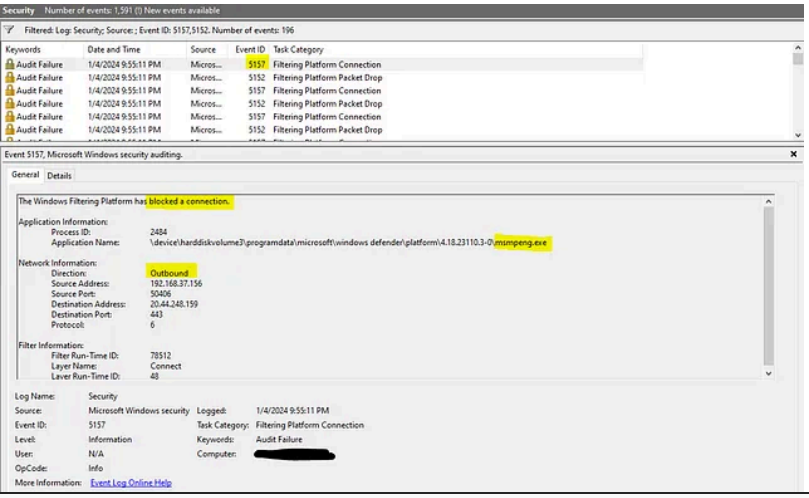
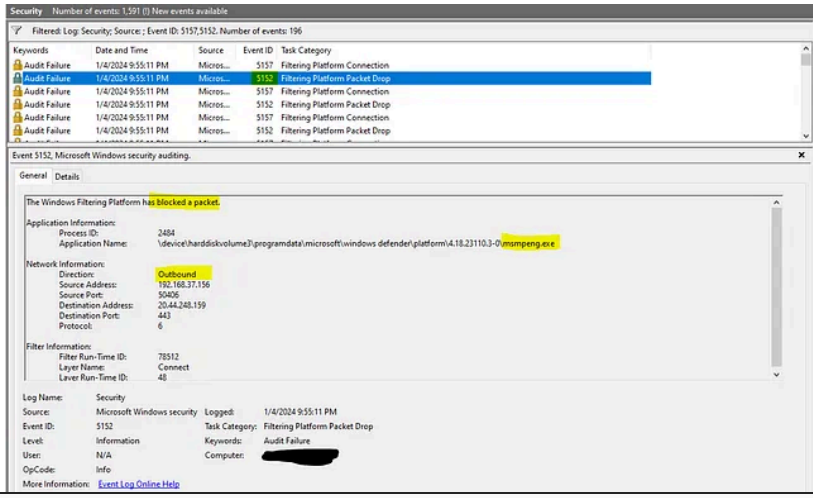
[Misc Series #4] Forensics on EDRSilencer Events

Table of Descriptions by Event ID

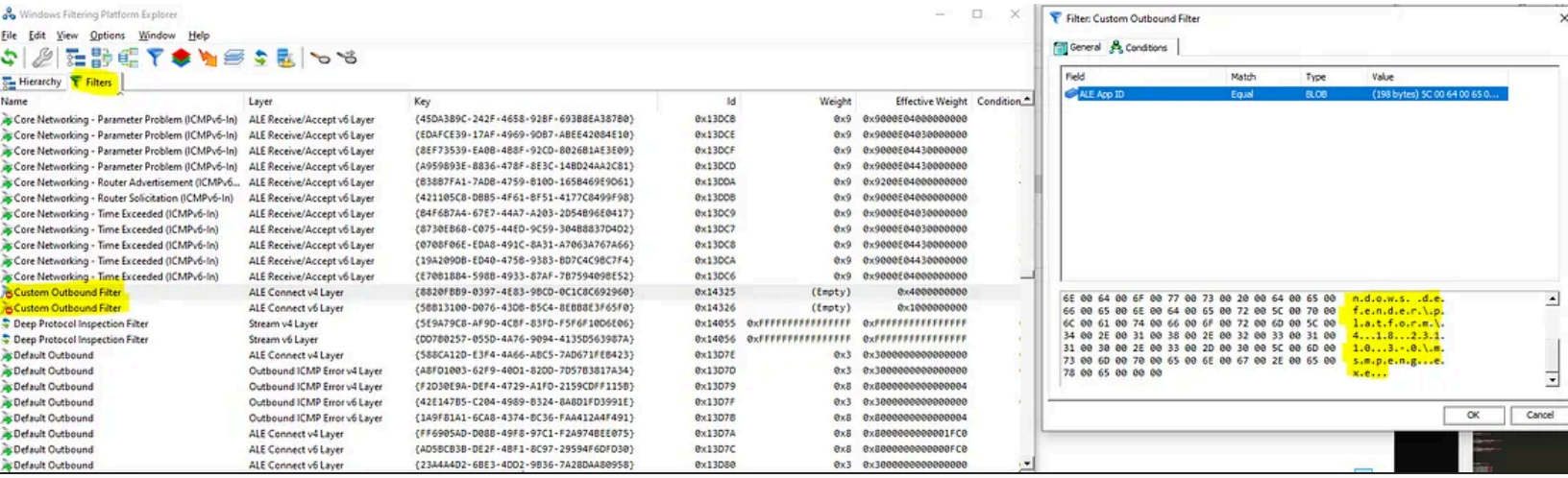
Event ID	Brief Description
5152	Windows Filtering Platform blocked a packet
5154	Windows Filtering Platform permitted an application or service to listen on a port for incoming connections
5156	Windows Filtering Platform allowed a connection
5157	Windows Filtering Platform blocked a connection
5158	Windows Filtering Platform permitted a bind to a local port
5159	Windows Filtering Platform blocked a bind to a local port







As we can see in `netevents.xml`, the string in the `<asString>` tag is in `UTF16-LE` format while the `<data>` tag is the hex representation of string in `<asString>` tag.



Medium

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

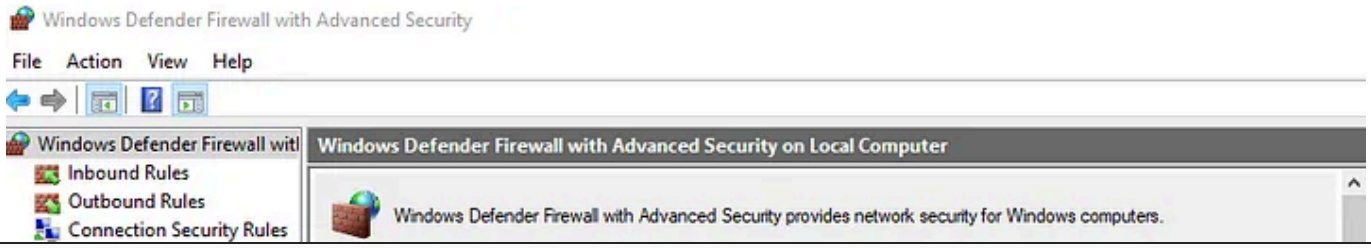
Free

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

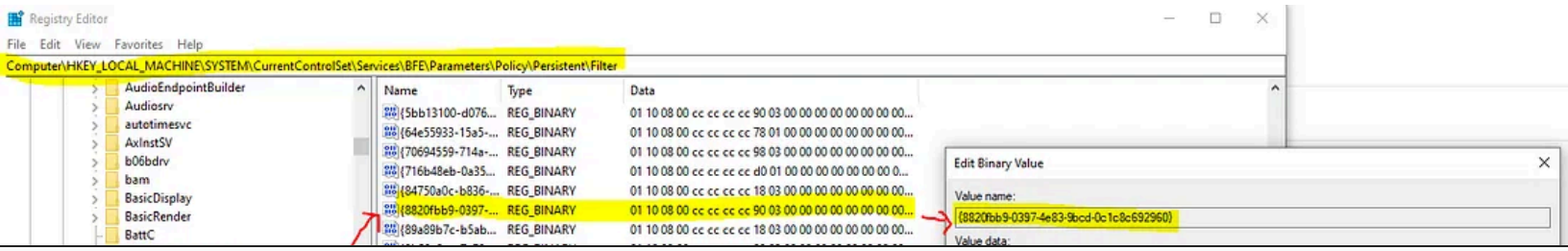
✦ Membership

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

Same with WFP event logs, the windows firewall doesn't log those packet drop events by default. We have to enable it based on the network profile the we are using.



The WFP filter data of the EDRSilencer can be found in the service registry key `Base Filtering Engine (BFE)` which is located as `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BFE\Parameters\Policy\Persistent\Filter`



EDR process file has been loaded by EDRSilencer before apply the WFP block rule.

Once it was succeed, we can see the the `TCP Disconnect` events from the `msmpeng.exe` and once the WFP block rule disabled, the event data flow to server gets back to normal (`TCP Send` & `TCP Receive`). However, this part will

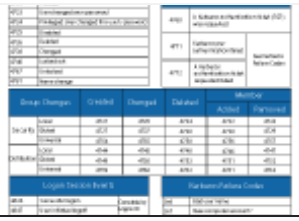
Collect Windows Filtering Platform (WFP) events

This topic describes how to collect Windows Filtering Platform (WFP) events in SEM.

documentation.solarwinds.com

Windows Security Log Event ID 5156 - The Windows Filtering Platform has allowed a connection

5156: The Windows Filtering Platform has allowed a connection On this page This event documents each time WFP allows a



blog.quarkslab.com

Cybersecurity | Threat Hunting | Computer Forensics | Digital Forensics | Blue Team

--