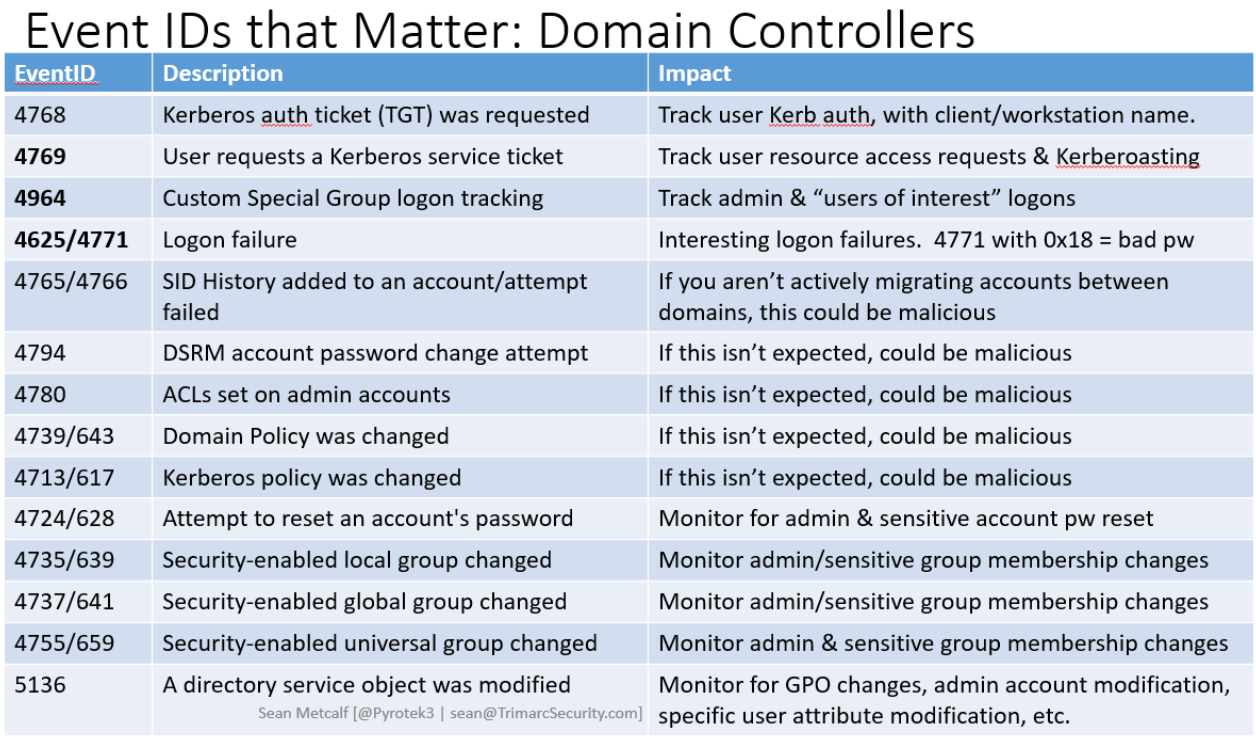
BSides Charm (2017) Talk Slides Posted – Detecting the Elusive: Active Directory Threat Hunting

adsecurity.org

Sean Metcalf May 1, 2017



I recently presented my talk "Detecting the Elusive: Active Directory Threat Hunting" at BSides Charm in Baltimore, MD.
Slides are now posted in the Presentations section.

I cover some of the information I've posted here before:

- PowerShell Security
- Detecting Kerberoasting: Part 1 and Part 2

On Sunday, April 30th, 2017, I spoke at BSides Charm in Track 2 at 2pm.

Here's the talk description from the BSides Charm website:

> Detecting the Elusive: Active Directory Threat Hunting
> Attacks are rarely detected even after months of activity. What are defenders missing and how could an attack by detected?
>
> This talk covers effective methods to detect attacker activity using the features built into Windows and how to optimize a detection strategy. The primary focus is on what knobs can be turned and what buttons can be pushed to better detect attacks.
>
> One of the latest tools in the offensive toolkit is “”Kerberoast”” which involves cracking service account passwords offline without admin rights. This attack technique is covered at length including the latest methods to extract and crack the passwords. Furthermore, this talk describes a new detection method the presenter developed.
>
> The attacker’s playbook evolves quickly, defenders need to stay up to speed on the latest attack methods and ways to detect them. This presentation will help you better understand what events really matter and how to better leverage Windows features to track, limit, and detect attacks

This presentation covers the type of log data required to properly

For the curious, here’s an outline of the talk:

- The current issues with monitoring
- Logging
    - Command logging
    - Sysinternals SysMon
    - Interesting Microsoft binaries to monitor (thanks Casey Smith! @subtee)
    - Microsoft Windows Event Forwarding (WEF)
- PowerShell Logging
    - PowerShell without PowerShell.exe (PS>Attack)
    - PowerShell obfuscation with Invoke-Obfuscation & detection
- Auditing attack activity
    - Standard auditing vs Advanced auditing
    - Recommended DC auditing
    - Special Logon auditing
    - Event IDs that matter: Domain Controllers & all Windows systems
    - Logon types (4624)
    - Password Spraying & detection
    - Kerberoasting & detection

Slides are now posted in the Presentations section.