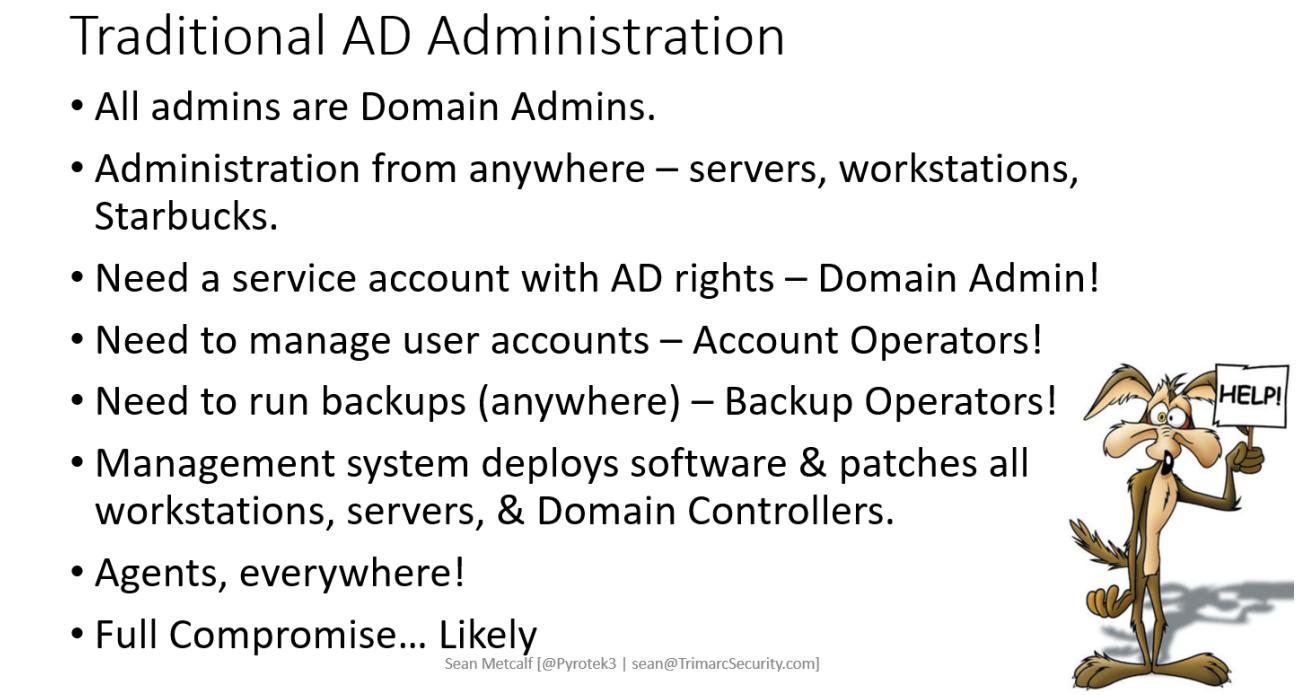
Sp4rkCon (2017) Talk Slides Posted – Active Directory Security: The Good, the Bad, & the UGLY

adsecurity.org

Sean Metcalf May 1, 2017



I recently presented my talk “Active Directory Security: The Good, the Bad, & the UGLY” at Sp4rkCon in Bentonville, AR in April 2017.
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

Here’s the talk description:

> Active Directory Security:The Good, the Bad, & the UGLY
>
> While security of the enterprise has been laid bare for years, exploitation techniques targeting Active Directory were relatively rare. In recent years, attackers have focused on more than passing hashes and getting Domain Admin. From SPN Scanning for services to Kerberoasting for credentials to Golden Tickets for persistence, there are multiple methods for attacking Active Directory. Active Directory is the primary identity and management infrastructure for most enterprises and properly securing the AD forest has never been more important.
>
> Some of the topics covered:
>
> * PowerShell attacks
>
> * Active Directory recon
>
> * Credential theft
>
> * Kerberos delegation
>
> This talk is an update of Sean's talk from 2015 entitled: "Red vs. Blue: Modern Active Directory Attacks & Defense" where he covered various attack methods and related mitigation. This update explores the current attack techniques and the latest detection.
>
> The presented Information is useful for both Red & Blue Team members.

This presentation is a remix of talks I did last year with some additional information mixed in. New to this talk is coverage of Kerberos delegation issues (not just unconstrained) and how to detect Kerberoasting.

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

- Current issues with security
- PowerShell Logging
    - PowerShell without PowerShell.exe (PS>Attack)
    - PowerShell obfuscation with Invoke-Obfuscation & detection
- AD Security Issues and Exploitation
    - AD Recon and exploitation
    - Kerberos Delegation
- Kerberoasting & Detection
- AD Administration Paradigm Shift
    - Traditional AD Administration
    - Secure AD Administration
    - AD Admin Tiers
    - Red Team Perspective
    - Using Bloodhound for Recon

Slides are now posted in the Presentations section.

(Visited 4,507 times, 1 visits today)