Black Hat USA 2016 Talk – Beyond the MCSE: Active Directory for the Security Professional

adsecurity.org

Sean Metcalf July 19, 2016

This summer in Las Vegas, I'm speaking at Black Hat USA 2016 on Active Directory security, "Beyond the MCSE: Active Directory for the Security Professional." This talk covers the key AD security components with specific focus on the things security professionals should know.

I put this talk together because I have noticed that while Active Directory admins, engineers, and MCSEs typically know what areas of Active Directory are critical security components, others often do not. The presentation covers the core AD components and how they impact enterprise security before diving into the most common AD security issues, new AD security enhancements in recent Windows versions, and AD security best practices.

On Wednesday, August 3rd, 2016, I am speaking at the Mandalay Bay room GH from 10:20am to 11:10am.

BEYOND THE MCSE: ACTIVE DIRECTORY FOR THE SECURITY PROFESSIONAL

Sean Metcalf

Mandalay Bay GH

10:20 – 11:10

Here's my talk description from the Black Hat website:

> Active Directory (AD) is leveraged by 95% of the Fortune 1000 companies for its directory, authentication, and management capabilities. This means that both Red and Blue teams need to have a better understanding of Active Directory, it's security, how it's attacked, and how best to align defenses. This presentation covers key Active Directory components which are critical for security professionals to know in order to defend AD. Properly securing the enterprise means identifying and leveraging appropriate defensive technologies. The provided information is immediately useful and actionable in order to help organizations better secure their enterprise resources against attackers. Highlighted are areas attackers go after including some recently patched vulnerabilities and the exploited weaknesses. This includes the critical Kerberos vulnerability (MS14-068), Group Policy Man-in-the-Middle (MS15-011 & MS15-014) and how they take advantages of AD communication.
>
> Some of the content covered:
>
> - Differing views of Active Directory: admin, attacker, and infosec.
> - The differences between forests and domains, including how multi-domain AD forests affect the security of the forest.
> - Dig into trust relationships and the available security features describing how attack techniques are impacted by implementing these trust security features.
> - AD database format, files, and object storage (including password data).
> - Read-Only Domain Controllers (RODCs), security impact, and potential issues with RODC implementation.
> - Key Domain Controller information and how attackers take advantage.
> - Windows authentication protocols over the years and their weaknesses, including Microsoft's next-generation credential system, Microsoft Passport, and what it means for credential protection.
> - Security posture differences between AD on-premises and in the cloud (Microsoft Azure AD vs Office 365).
> - Key Active Directory security features in the latest Windows OS versions – the benefits and implementation challenges.
>
> Let's go beyond the standard MCSE material and dive into how Active Directory works focusing on the key components and how they relate to enterprise security.

For the curious, here's an outline of my talk at Black Hat next week:

- Active Directory Key Components & their Security
    - Forest, Domains, & Trusts
    - Trusts vs. Federation
    - AD in the Cloud
    - Extending your corporate network (AD) to the cloud
    - AD Objects & sensitive attributes
    - Domain Controllers, Read-Only Domain Controllers, and Global Catalogs
    - Sites & Subnets
    - Group Policy
- Authentication
    - NTLM Overview, Issues, & Attacks
    - Kerberos Overview, Issues, & Attacks
    - Passport, the future of Microsoft authentication
- The Most Common Security Issues
    - Admins everywhere
    - Patching
    - Credentials in SYSVOL
    - Improper ACLs
    - …
- Active Directory Security Enhancements by OS Version
- New Security Features in Windows 10 & Windows Server 2016

***Slides are now available from the Presentations page for download**.*

Note that I am also speaking at DEF CON 24 on Red Teaming Active Directory which takes more of “red” focus on Active Directory security. For the DEF CON talk, some of the initial AD security information is similar, though abbreviated, the rest of the content describes methods to best evaluate the security posture of an Active Directory environment.

(Visited 2,969 times, 1 visits today)