DEF CON 24 (2016) Talk – Beyond the MCSE: Red Teaming Active Directory

adsecurity.org

Sean Metcalf

July 6, 2016

This August at DEF CON 24, I will be speaking about Active Directory security evaluation in my talk “Beyond the MCSE: Red Teaming Active Directory”. This talk is focused on the Red side of AD security, specifically how to best evaluate the security of AD and quickly identify potential security issues. Whether you perform “Red Teaming” or “Penetration testing”, this presentation covers efficient methods of Active Directory recon which can quickly identify AD privilege escalation methods, several of which aren’t well described or understood. Also discussed are the latest Active Directory defensive measures, what this means to the Red Teamer, and potential bypasses.
Note that this is the 3rd talk at DEF CON and is on Thursday, DEF CON’s opening day.

Beyond the MCSE:
Red Teaming Active Directory

Sean Metcalf (@Pyrotek3)
sean @ adsecurity . org
www.ADSecurity.org

On Thursday, August 4th, 2016, I have a DEF CON 101 talk from 12:00pm to 12:50pm in the Pacific Ballroom (Bally’s Jubilee Tower, 2nd floor).
DEF CON 24 Floorplan (map)

Here’s my talk description from the DEF CON website:

> Active Directory (AD) is leveraged by 95% of the Fortune 1000 companies for its directory, authentication, and management capabilities, so why do red teams barely scratch the surface when it comes to leveraging the data it contains? This talk skips over the standard intro to Active Directory fluff and dives right into the compelling offensive information useful to a Red Teamer, such as quickly identifying target systems and accounts. AD can yield a wealth of information if you know the right questions to ask. This presentation ventures into areas many didn't know existed and leverages capability to quietly identify interesting accounts & systems, identify organizations the target company does business with regularly, build target lists without making a sound, abuse misconfigurations/existing trusts, and quickly discover the most interesting shares and their location. PowerShell examples and AD defense evasion techniques are provided throughout the talk.
>
> Let's go beyond the MCSE and take a different perspective on the standard AD recon and attack tactics.

DEF CON 24 talk outline:

- Active Directory Security (quick primer)
  - Forests, Domains, & Trusts
  - Sites & Subnets
  - Domain Controllers, RODCs, & Global Catalogs
  - DNS
  - Group Policy
- Offensive PowerShell
  - Offensive PowerShell quick history
  - PowerShell v5 security features
  - Methods to bypass PowerShell v5 security & logging
  - Bypassing Windows 10's AMSI
- Effective AD Recon (PowerShell examples)
  - Admin identification without group membership enumeration/recursion
  - DNS lookups via LDAP
  - Local Administrator discovery
  - Quick enterprise service discovery
  - EMET, AppLocker, and LAPS configuration discovery
  - User, computer, and service recon
- AD Defenses & Bypasses
  - LAPS
  - Jump (Admin) Servers
  - AD Administrative Tiering
  - Admin Forest (aka "Red Forest")
- Red Team Cheat Sheets

After I present them, the presentation slides will be available from the Presentations page for download.