DerbyCon V (2015): Red vs. Blue: Modern Active Directory Attacks & Defense Talk Detail

adsecurity.org

Sean Metcalf

September 10, 2015

In a couple of weeks, I will be speaking at DerbyCon about Active Directory attack & defense in my talk Red vs. Blue: Modern Active Directory Attacks & Defense". This is the 5th iteration of this talk and includes the latest updates to attack methods and defensive strategies. This DerbyCon version is a blend of my Black Hat & DEF CON talks and includes several new updates including new "Sneaky AD Persistence" which covers difficult to detect methods an attacker could retain Domain Admin level access after having admin rights on a Domain Controller for 5 minutes.

On Friday, September 25th, 2015, I have a Track 1 (Break Me) talk from 3:00pm to 3:50pm.

Here's my talk description:

> This talk explores the latest Active Directory attack vectors including useful Red Team recon tactics and provides effective defensive techniques for the Blue Team. Dive right into the technical detail describing the latest methods for gaining and maintaining administrative access in Active Directory, including some sneaky AD persistence methods. Also covered are traditional security measures that work (and some that don't) as well as the mitigation strategies that disrupts the attacker's preferred game-plan.
> Some of the topics covered:
> – "SPN Scanning" with PowerShell to identify potential targets without network scans (SQL, Exchange, FIM, webservers, etc.).
> – Exploiting weak service account passwords as a regular AD user.
> – How attackers go from zero to (Domain) Admin.
> – MS14-068: the vulnerability, the exploit, and the danger.
> – Mimikatz, the attacker's multi-tool.
> – Using Silver Tickets for stealthy persistence.
> – Sneaky persistence methods attackers use to maintain admin rights.
> – Detecting offensive PowerShell tools like Invoke-Mimikatz.
> – Active Directory attack mitigation.

While the primary components of this talk are similar to my Black Hat & DEF CON presentations, key differences/updates are in bold.

DerbyCon talk outline:

- **Advanced Red Team Recon Tactics**
- **From PowerSploit to Empire: modern PowerShell attack tools.**
- **Red Team Remote Execution Methods**

- SPN Scanning: service discovery without network port scanning
- Cracking service account passwords as a domain user (with no elevated permissions).
- Group Policy Preferences – detecting credential theft from GPP
- **Several methods showing how attackers go from domain user to Domain Admin.**
- **Mimikatz DC Sync Usage & Detection**
- Converting an NTLM password hash to a Kerberos ticket (no need to Pass-the-Hash).
- The one vulnerability to rule them all! (AD domains).
- **Sneaky AD Persistence Tricks**
- How my security research made Golden Tickets more powerful.
- Silver Tickets can be more dangerous than Golden Tickets.
- Forging Trust Tickets to expand access.
- **Detecting offensive PowerShell tools including Invoke-Mimikatz**
- Mitigating PowerShell attacks.
- PowerShell v5 security enhancements
- Active Directory defense and mitigation techniques that work.

DerbyCon Edition – "Red vs. Blue: Modern Active Directory Attacks & Defense" (v5)
– New Sneaky Active Directory Persistence Methods, Advanced Red Team Recon Tactics, Remote Execution Methods, Mimikatz DC Sync Usage & Detection, & Detecting offensive PowerShell tools including Invoke-Mimikatz
DerbyCon V (September 2015)
DerbyCon V Slides (PDF)
DerbyCon Presentation Video (YouTube)

(Visited 3,802 times, 1 visits today)