Active Directory Attack and Defense Seminar

A Two Day Exploration into Attacker Techniques and Effective Defense Methods

Session Overview

Active Directory is leveraged by approximately 90% of the world's enterprises, many of which comprise over 100k systems and were stood up a decade (or more) ago. Responsible for the identity and authentication in most enterprises, Active Directory is key when it comes to securing the enterprise. However, most organizations don't have a consistent or comprehensive view of how to tackle enterprise security.

Modern Active Directory (AD) environments are not aligned to protect the enterprise from the current threats. The attack vectors that were theoretical 10 years ago are now practical. While the threats have changed over the past decade, the way systems and networks are managed often have not. We continue with the same operations and support paradigm despite the fact that internal systems are compromised regularly. We must embrace the new reality of “Assume Breach.”

Going from the compromise of a single workstation to complete compromise of the enterprise network often takes less than an hour. The weekly news headlines call out an all too clear emerging pattern: years of security complacence has made full compromise too easy. A solid perimeter defense used to be enough to protect the internal network and we managed our corporate network with the assumption that only authorized users were able to access it. The weakest link in an organization's security strategy can lead to complete Active Directory forest compromise costing tens of thousands of hours in recovery time and millions of dollars in direct and indirect costs. Unfortunately, the best case strategy for recovering from an AD forest compromise is rebuild from scratch. Most organizations can't afford the down-time or the cost associated with this "scorched earth" scenario.

Helping organizations better understand the shift from "defend the perimeter" to "assume breach" is key to moving from the defense techniques of 10 to 20 years ago to ones better suited to the current threat. The "Assume Breach" mentality is a paradigm shift where instead of wondering if an attacker could get into the internal network, we assume they are already there performing reconnaissance and mapping out enterprise resources more thoroughly than the current IT documentation. "Defense in Depth" has never been more relevant and this presentation shows how effective this strategy can be in mitigating some of the most tenacious attacks. This session focuses on the "Assume Breach" mentality and how it can help shape a strong defense against the current attack profile carefully mapping out current attack techniques and the effective mitigation techniques.

It’s more important than ever to understand how attackers enter, recon, access and exfiltrate data, and elevate permissions to gain Domain Admin rights. Understanding the methods, tactics, and techniques of one’s adversary is critical in order to mount effective defenses.

This two-day seminar session sets the scene for how modern Active Directory environments are configured including common scenarios that lead to full compromise of the AD forest and completes the day walking through several methods attackers are using today to gain full access. Day two focuses on defense and mitigation, showing how the effective defenses work including the level of effort.

Goals:

- Better understand what attackers are doing once they gain a foothold and how to mitigate the impact of this access.
- Identify the areas in which traditional security methods fall short.
- Learn what defensive measures are effective and how they mitigate current threats.

Who should attend?

- Active Directory system administrators, engineers, and architects.
- Technical cybersecurity staff.
- Personnel with IA roles within the enterprise.

Course Syllabus

Day One: Overview and Attacking AD

- Active Directory and PowerShell overview
- Key Active Directory security components
- Intrusion methods – gaining a foothold
- Recon – mapping the network and finding weaknesses
- Finding credentials (passwords)
- Cracking service account passwords as a domain user ("Kerberoasting")
- Credential theft and re-use
- Privilege escalation and lateral movement
- Kerberos Attacks: Golden Tickets & Silver Tickets
- Active Directory Persistence Methods: Forged Kerberos Tickets (Golden Tickets, Silver Tickets, etc.), Group Policy, WMI, etc.

Day Two: Defending the Enterprise

- Common Active Directory Security Issues
- Mimikatz: capability and typical detection methods
- PowerShell attacks and detection
- Windows Server & Active Directory security enhancements
- Domain Controller Auditing to find attacker activity
- Practical Active Directory defenses
- Protecting Windows – Reducing the Windows Attack Surface
- Secure Administration
- Enhanced Windows security with Windows 10 & Windows Server 2016
- Active Directory Security Cheatsheet

Note that content listed in the syllabus is provided as a rough guide of seminar content flow (some content is covered in more depth than others) and that this is an interactive seminar format that does not have hands-on labs.

Training Session Benefits

This session focuses on interaction with participants and engaging everyone in the material. Every attendee receives the session material including the presentation slides and demo videos (as appropriate).

Attendees will:

- Identify the areas in which traditional security methods fall short.
- Better understand what attackers are doing once they gain a foothold and how to mitigate the impact of this access.
- Discover Mimikatz capability and common use.
- Understand the most common Active Directory security issues and how to resolve them.
- Learn what defensive measures are effective and how they mitigate current threats.

Trimarc Security, LLC
1775 I St NW
Suite #1150
Washington, DC 20006
Phone: (202) 587-2735
Email: info@TrimarcSecurity.com
Web: TrimarcSecurity.com