Souhir ZAIMI : La sécurisation d'Active Directory face aux cyberattaques modernes

Veille n°1 – Les attaques les plus utilisées contre Active Directory

Active Directory est au cœur de l'authentification et de la gestion des droits dans les environnements Windows. Lorsqu'il est compromis, un attaquant peut obtenir un contrôle quasi total du domaine. Certaines attaques sont aujourd'hui particulièrement utilisées car elles exploitent des mécanismes normaux d'Active Directory.

Pass-the-Hash

Le Pass-the-Hash est l'une des attaques les plus courantes. Elle consiste à utiliser le hash NTLM d'un utilisateur pour s'authentifier sans connaître son mot de passe. Cette technique permet un déplacement latéral rapide et reste efficace dans de nombreux environnements où NTLM est encore activé.

Kerberoasting

Le Kerberoasting cible les comptes de service via le protocole Kerberos. En récupérant des tickets de service et en cassant leur mot de passe hors ligne, l'attaquant peut obtenir des privilèges élevés. Cette attaque est très utilisée car elle ne nécessite pas de droits particuliers et est difficile à détecter.

NTLM Relay / Kerberos Relay

Les attaques par relais consistent à intercepter une authentification légitime pour l'utiliser contre un autre service. Elles sont efficaces lorsque certaines protections ne sont pas activées et permettent à un attaquant de s'authentifier sans mot de passe.

Pourquoi ces attaques sont les plus utilisées

Ces attaques exploitent des mécanismes légitimes d'Active Directory, ce qui les rend discrètes et efficaces. Elles sont souvent utilisées comme étape clé dans les attaques par ransomware.

Sources

- Microsoft – *Guidance to help mitigate critical threats to Active Directory Domain Services* (2025) https://www.microsoft.com/en-us/windows-server/blog/2025/12/09/microsofts-

guidance-to-help-mitigate-critical-threats-to-active-directory-domain-services-in-2025

- DarkReading – *Active Directory remains a prime attack target* (2025) https://www.darkreading.com/identity-access-management-security/25-years-active-directory-prime-attack-target