Souhir ZAIMI

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

Cette veille analyse les trois attaques les plus courantes contre Active Directory : Pass-the-Hash, Kerberoasting, et NTLM Relay. Elles exploitent des mecanismes legitimes d'AD, ce qui les rend discretes et tres utilisees comme etapes cles dans les chaines d'attaque ransomware.

Pass-the-Hash

Le Pass-the-Hash est l'une des attaques les plus courantes. Elle consiste a utiliser le hash NTLM d'un utilisateur pour s'authentifier sans connaitre son mot de passe. Cette technique permet un deplacement lateral rapide et reste efficace dans de nombreux environnements ou NTLM est encore active.

Kerberoasting

Le Kerberoasting cible les comptes de service via le protocole Kerberos. En recuperant des tickets de service et en cassant leur mot de passe hors ligne, l'attaquant peut obtenir des privileges eleves. Cette attaque est tres utilisee car elle ne necessite pas de droits particuliers et est difficile a detecter.

NTLM Relay / Kerberos Relay

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

Pourquoi ces attaques sont les plus utilisees

Ces attaques exploitent des mecanismes legitimes d'Active Directory, ce qui les rend discretes et efficaces. Elles sont souvent utilisees comme etape cle dans les attaques par ransomware.

Notions cles

Hash NTLM
Fonction de hachage utilisee pour stocker les mots de passe dans Windows. Contrairement aux mots de passe en clair, le hash ne peut pas etre reverse, mais peut etre utilise directement pour s'authentifier.

Deplacement lateral
Technique d'attaque permettant a un attaquant de se deplacer d'un systeme a un autre au sein d'un reseau apres un acces initial.

Kerberos
Protocole d'authentification par defaut dans Active Directory qui utilise des tickets pour eviter de transmettre les mots de passe sur le reseau.

Ticket de service
Jeton Kerberos permettant a un utilisateur d'acceder a un service specifique sans renvoyer le mot de passe.

Relais d'authentification
Technique permettant d'intercepter une demande d'authentification legitime et de la rediriger vers une autre cible pour y gagner un acces.

GPO (Group Policy Object)
Outil Windows permettant d'appliquer des configurations de securite centralisees sur l'ensemble du domaine.

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

• ExtraHop – 2025 Security Predictions: Active Directory Still a Target
https://www.extrahop.com/blog/active-directory-will-remain-a-key-target