Souhir ZAIMI

Veille n°4 – L'authentification Kerberos dans Active Directory

Kerberos est le protocole d'authentification par defaut dans Active Directory. Cette veille couvre son fonctionnement (TGT et tickets de service), une faille critique decouverte en novembre 2025 (CVE-2025-60704) permettant l'usurpation d'identite, et le calendrier de suppression definitive de RC4 qui creatait des vulnerabilites comme le Kerberoasting.

Fonctionnement de Kerberos

Kerberos est le protocole d'authentification par defaut dans un domaine Active Directory. Son role est simple : permettre a un utilisateur d'acceder a des ressources reseau sans jamais envoyer son mot de passe sur le reseau.

Les 3 acteurs

Le Client : l'utilisateur ou la machine qui veut acceder a un service. Le KDC (Key Distribution Center) : c'est le Controleur de Domaine. Il connait tous les secrets du domaine via le compte krbtgt. Le Service : la ressource cible (partage reseau, application, base de donnees...).

Faille recente CVE-2025-60704

En novembre 2025, deux chercheurs de la societe Silverfort ont decovert une faille dans le mecanisme de delegation Kerberos d'Active Directory. La faille (CVSS 7.5) permet via une attaque Man-in-the-Middle d'usurper l'identite de n'importe quel utilisateur du domaine, d'escalader les privileges jusqu'a Administrateur, et de prendre le controle total du domaine. Microsoft a publie un patch lors du Patch Tuesday de novembre 2025.

Suppression de RC4

RC4 est un ancien algorithme de chiffrement dans Kerberos, trop faible et permettant l'attaque Kerberoasting. Microsoft a mise en place un calendrier : Janvier 2026 ajout d'evenements d'audit, Avril 2026 RC4 desactive par defaut, Juillet 2026 suppression definitive. La mise a jour d'avril a cause des pannes dans beaucoup d'entreprises avec des elements legacy dependant de RC4.

Evolutions Windows Server 2025

Windows Server 2025 introduit plusieurs changements : les anciennes cles de registre Kerberos ne sont plus supportees, la configuration passe par les GPO, et le KDC bascule automatiquement en AES. La mise a jour de novembre 2025 introduit aussi les premiers algorithmes post-quantiques, et Kerberos utilise desormais AES-SHA2 (RFC 8009) sur les environnements Windows Server 2025 purs.

Notions cles

TGT (Ticket Granting Ticket)
: Ticket initial delivre par le KDC permettant a l'utilisateur de demander d'autres tickets pour acceder aux services. Valable environ 10 heures.

KDC (Key Distribution Center)
: Centre de distribution de cles = le Controleur de Domaine. Il emet les TGT et les tickets de service, et connait tous les secrets du domaine.

SPN (Service Principal Name)
: Identificateur unique pour un service dans Active Directory, permettant aux clients de localiser et d'authentifier le service de maniere securisee.

Delegation Kerberos
: Mecanisme permettant a une application d'agir au nom d'un utilisateur pour acceder a une autre ressource, sans reveler le mot de passe.

Man-in-the-Middle (MitM)

Attaque ou l'attaquant s'intercale entre deux parties communicantes pour intercepter, lire ou modifier les donnees echangees.

Kerberoasting

Attaque exploitant la faiblesse de RC4 : n'importe quel utilisateur peut demander un ticket de service, le craquer hors ligne et decouvrir le mot de passe du compte de service.

AES vs RC4

AES256 est un algorithme moderne et robuste; RC4 est ancien et vulnerable, progressivement supprime par Microsoft jusqu'a juillet 2026.

Algorithmes post-quantiques

Nouveaux algorithmes cryptographiques resistant aux attaques des ordinateurs quantiques, introduits dans Windows Server 2025.

Sources

• Vaadata – Authentification Kerberos : principes et fonctionnement (avril 2026)
https://www.vaadata.com/fr/blog/authentification-kerberos-principes-et-fonctionnement/

• IT-Connect – Active Directory : Kerberos impacte par la CVE-2025-60704 (13 novembre 2025)
https://www.it-connect.fr/active-directory-kerberos-impacte-par-la-cve-2025-60704-quels-sont-les-risques/

• vbinformatique.fr – Mises a jour Microsoft d'avril 2026 et acces Kerberos (avril 2026)
https://www.vbinformatique.fr/active-directory-microsoft-kerberos/

• 4sysops – Windows Kerberos RC4 deprecation (avril 2026)
https://4sysops.com/archives/windows-kerberos-rc4-deprecation-what-will-break-in-active-directory-and-how-to-fix-it/