AYI NEDJIMI Consultants

Kerberoasting 2026 : Attaque, Déte

10 mai 2026 • Mis à jour le 17 mai 2026 • 18 min de lecture • 3622 mots •

Kerberoasting 2026 : guide expert attaque + défense Active Directory. Rub
complet.

À RETENIR

À retenir — Kerberoasting en 2026

Kerberoasting est une attaque Kerberos publiée en 2014 par Tim Medin qu
n'importe quel utilisateur authentifié pour cracker les mots de passe de co

Toute requête TGS-REP pour un compte avec SPN renvoie un ticket chiffré
exploitable hors-ligne par Hashcat ou John the Ripper.

Les outils modernes Rubeus, Impacket GetUserSPNs et Kerbrute automati
(RC4 downgrade, no-PAC, timing).

La défense repose sur quatre piliers : mots de passe longs (gMSA, 32+ ca
surveillance des événements 4769 et politiqu .

> En 2026, les variantes Targeted Kerberoasting, Silver Ticket et S4U Roast

Le Kerberoasting reste en 2026 l'une des attaques Active Directory les plus rentab
obtenu un premier point d'ancrage dans le domaine. Publié pour la première fois e
DerbyCon, ce vecteur exploite une caractéristique fondamentale du protocole Ker
demander un ticket de service (TGS-REP) pour n'importe quel compte disposant d
du mot de passe du compte de service. Un attaquant peut donc collecter en quelq
cracker hors-ligne sur sa propre infrastructure de calcul, sans générer de tentative
décortique l'attaque pas à pas avec Rubeus et Impacket, présente les variantes 20
les règles SIEM de détection et propose une stratégie de défense en profondeur o

1. Rappels Kerberos : pourquoi le Kerberoasting fonctionne

Comprendre le Kerberoasting nécessite de revoir les bases du protocole Kerberos
Microsoft documentée dans la spécification MS-KILE.

Kerberos repose sur un échange en deux temps. Premier temps : l'utilisateur s'aut
hébergé sur le contrôleur de domaine via un AS-REQ et reçoit en retour un **Ticket**
krbtgt. Deuxième temps : pour accéder à un service (SQL, SMB, HTTP), l'utilisateu
précisant le SPN ciblé, et obtient un **Ticket Granting Service (TGS-REP)** chiffré av
C'est ce dernier ticket qui est la cible du Kerberoasting.

1.1 Le rôle des SPN (Service Principal Names)

Un **Service Principal Name (SPN)** est un identifiant Kerberos associant un service
`service/host:port`, par exemple `MSSQLSvc/sqlsr` `433` ou `HT`

Réponse sous 24h

Devis gratuit →