AYI NEDJIMI Consultants

# NTLM Relay 2026 : Attaque Moderne

10 mai 2026 • Mis à jour le 17 mai 2026 • 17 min de lecture • 3574 mots •

NTLM Relay 2026 : techniques modernes, exploitation AD CS ESC8, détec
signing.

À RETENIR

## À retenir — NTLM relay en 2026

Le NTLM relay exploite l'absence de mutual authentication dans NTLM pou
service tiers, souvent un DC ou un serveur de fichiers.

Les vecteurs modernes 2026 incluent PetitPotam, PrinterBug, DFSCoerce
HTTP, IPv6 mDNS et LLMNR.

Sans SMB signing, LDAP signing et Extended Protection for Authenticatio
HTTPS est trivial.

L'outil impacket-ntlmrelayx reste la référence offensive : pivoting LDAP, AD

> La défense exige une approche systémique : **désactivation NTLM** à terme, détection des coercitions Inverse Forwarder.

Le NTLM relay reste en 2026 l'une des attaques Active Directory les plus efficace Théorisée dès 2001 par SilverNail, démocratisée en 2008 avec Squirtle puis Respo avec l'émergence des techniques de coercition d'authentification (PetitPotam, Prin quelle écoute LLMNR/mDNS en compromission de domaine. Microsoft a annoncé mais en pratique, plus de 95% des environnements Active Directory en 2026 supp compatibilité, et la majorité d'entre eux ne déploient ni SMB signing complet, ni LD vecteurs d'attaque modernes, présente les chaînes d'exploitation jusqu'à la comp propose une stratégie de défense en profondeur opérationnelle pour les RSSI et a

## 1. Rappel : pourquoi NTLM reste-t-il vulnérable au relay ?

NTLM (NT LAN Manager) est un protocole d'authentification challenge-response version 2 (NTLMv2) reste largement utilisée dans les environnements Windows, n fonctionne pas : authentification par adresse IP, machines hors domaine, applicati trois messages : NEGOTIATE, CHALLENGE, AUTHENTICATE. Le client prouve son serveur avec le hash NT de son mot de passe.

### 1.1 La faille conceptuelle

NTLM souffre d'un défaut fondamental documenté dans la spécification MS-NLM répond au challenge, il prouve à n'importe qui qu'il connaît le hash NT, mais il ne v prétend être. Un attaquant en position MITM peut do M_AUTHENT

Réponse sous 24h

Devis gratuit →