AYI NEDJIMI Consultants

Pass-the-Hash : Attaque NTLM Active

10 mai 2026 • Mis à jour le 17 mai 2026 • 22 min de lecture • 4837 mots • v

Pass-the-Hash (PtH) est l'une des techniques offensives les plus emblema
permet a un attaquant de s'authentifier sur un service NTLM en presentan
sans connaitre le mot de passe en clair. Repertoriee MITRE ATT&CK T1550
Ashton, popularisee en 2008 par Hernan Ochoa puis massifiee via Mimika
majeur de mouvement lateral en 2026 malgre Credential Guard, LSA Prote
modele Tier.

Pass-the-Hash (PtH) est l'une des techniques offensives les plus emblematiques
permet a un attaquant de s'authentifier sur un service NTLM en presentant directe
avoir besoin de connaitre le mot de passe en clair correspondant. Repertoriee dan
l'identifiant T1550.002, cette attaque exploite une **caracteristique de conception**
jamais le mot de passe lui-meme, mais une preuve cryptographique calculee a pa
passe Unicode. Quiconque possede ce hash peut donc se faire passer pour l'utili
offline. Conceptualisee des 1997 par Paul Ashton sur la mailing list *Bugtraq*, la tec
industrielle a partir de 2008 avec la publication du P kit par Her
son integration dans Mimikatz en 2011 via la comma n. Aujourd

compromissions Active Directory, employee par les groupes APT (APT29, Lazarus
ransomware (Conti, LockBit, BlackBasta), Pass-the-Hash demeure un vecteur de
mitigations Microsoft (**Credential Guard**, **LSA Protection**, **Restricted Admin Mode**,
first detaille le fonctionnement cryptographique de NTLM, les outils d'execution (M
les sources de hashes, les CVE associes, ainsi que les strategies de detection cot

À RETENIR

L'essentiel a retenir sur Pass-the-Hash

Definition : authentification NTLM en presentant le hash NT au lieu du mot
offline necessaire.

MITRE ATT&CK : technique **T1550.002 — Use Alternate Authentication Ma**
de T1550.

Origine : concept theorise par Paul Ashton en 1997, outillage publie par He
via Mimikatz (Benjamin Delpy) en 2011.

Outils signatures : Mimikatz (`sekurlsa::pth`), Impacket (`psexec.py` , `wm`
CrackMapExec), Cobalt Strike, Metasploit `exploit/windows/smb/psexec` .

Sources de hashes : LSASS dump, base SAM locale, NTDS.dit (replication
dump DPAPI.

Mitigations 2026 : Credential Guard (VBS), LSA Protection RunAsPPL, Rest
0/1/2, LAPS, desactivation NTLMv1, signed SMB, Protected Users.

Detection : Event 4624 LogonType 9 (NewCredentials), Sysmon Event 10 P
Defender for Identity, Sentinel UEBA, regles Sigma communautaires.

Réponse sous 24h

Devis gratuit →