



Pass-the-Hash : Attaque NTLM Active



10 mai
2026



Mis à jour le 17 mai
2026



22 min de
lecture

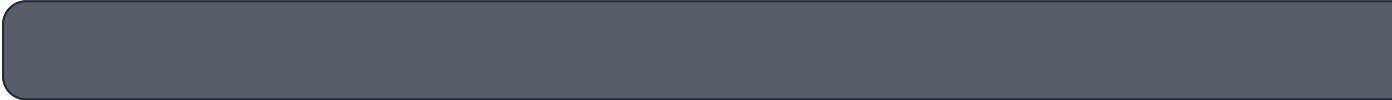


4837
mots



v

Pass-the-Hash (PtH) est l'une des techniques offensives les plus emblématiques. Elle permet à un attaquant de s'authentifier sur un service NTLM en présentant directement le hash d'un mot de passe sans connaître le mot de passe en clair. Repertoriée dans le catalogue MITRE ATT&CK T1550.002 par Paul Ashton, popularisée en 2008 par Hernan Ochoa puis massifiée via Mimikatz, elle est devenue un vecteur majeur de mouvement latéral en 2026 malgré Credential Guard, LSA Protection et le modèle Zero Trust.



Pass-the-Hash (PtH) est l'une des techniques offensives les plus emblématiques. Elle permet à un attaquant de s'authentifier sur un service NTLM en présentant directement le hash d'un mot de passe sans avoir besoin de connaître le mot de passe en clair correspondant. Repertoriée dans le catalogue MITRE ATT&CK l'identifiant T1550.002, cette attaque exploite une **caractéristique de conception** qui permet à un attaquant d'obtenir le hash d'un mot de passe sans jamais le mot de passe lui-même, mais une preuve cryptographique calculée à partir du mot de passe Unicode. Quiconque possède ce hash peut donc se faire passer pour l'utilisateur correspondant. Conceptualisée dès 1997 par Paul Ashton sur la mailing list *Bugtraq*, la technique a été popularisée dans l'industrie à partir de 2008 avec la publication du **PtH kit** par Hernan Ochoa. Aujourd'hui, elle est devenue un vecteur majeur de mouvement latéral en 2026 malgré Credential Guard, LSA Protection et le modèle Zero Trust.

Réponse sous 24h

Devis gratuit →

compromissions Active Directory, employée par les groupes APT (APT29, Lazarus), ransomware (Conti, LockBit, BlackBasta), Pass-the-Hash demeure un vecteur de compromission. Les mitigations Microsoft (**Credential Guard**, **LSA Protection**, **Restricted Admin Mode**, **Windows Defender**) et **Windows Defender** first détaille le fonctionnement cryptographique de NTLM, les outils d'exécution (Mimikatz, Impacket, CrackMapExec), les sources de hashes, les CVE associées, ainsi que les stratégies de détection côté serveur.

À RETENIR

L'essentiel à retenir sur Pass-the-Hash

Definition : authentification NTLM en présentant le hash NT au lieu du mot de passe. Nécessite une authentification offline nécessaire.

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

Origine : concept théorisé par Paul Ashton en 1997, outillage publié par Helel via Mimikatz (Benjamin Delpy) en 2011.

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

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

Mitigations 2026 : Credential Guard (VBS), LSA Protection RunAsPPL, Restricted Admin Mode, LAPS, désactivation NTLMv1, signed SMB, Protected Users.

Détection : Event 4624 LogonType 9 (NewCredentials), Sysmon Event 10 File Integrity Monitoring, Windows Defender for Identity, Sentinel UEBA, règles Sigma communautaires.

Réponse sous 24h

Devis
gratuit →