Synapsys

Fin de NTLM : quelles sont les alternatives ?

NTLM (New Technology LAN Manager) est un ancien protocole d'authentification développé par Microsoft pour garantir la sécurité des échanges sur les réseaux Windows. Initialement conçu pour les réseaux locaux, NTLM utilise un système d'échange de "hash" pour vérifier l'identité des utilisateurs sans envoyer de mots de passe en clair.

Ce protocole est aujourd'hui considéré comme vulnérable aux attaques modernes. La fin de son support et sa désactivation sur Windows 11 soulignent la nécessité de migrer vers des solutions plus sécurisées comme Kerberos.

Pourquoi migrer du processus d'authentification NTLM ?

- Obsolète depuis 2010 et désactivé sur Windows 11 depuis juillet 2024
- Vulnérable aux attaques Pass-the-Hash et NTLM Relay
- Incitation de Microsoft pour migrer vers d'autres protocoles
- Garantie d'une meilleure protection des données sensibles

Pourquoi migrer vers un autre protocole ?

CE QUE VOUS RISQUEZ AVEC NTLM

- **Attaque Pass-the-Hash :** NTLM permet aux hackers de réutiliser des hachages d'identification
- **Attaque NTLM Relay :** Les authentifications peuvent être relayées
- **Absence de chiffrement fort :** Les données en transit n'ont pas un chiffrement suffisant
- **Authentification basée sur les sessions :** Mauvaise gestion de le ré-authentification, ce qui peut conduire à des accès prolongés
- **Manque de prise en charge des fonctionnalités modernes :** Pas de prise en charge des méthodes avancées telles que la MFA

CE QUE PEUVENT PROPOSER LES AUTRES PROTOCLES

- **Ticket d'authentification :** Les protocoles modernes minimisent le risque de réutilisation d'identifiants
- **Processus d'authentification :** Plus de sécurité et de résistance aux relais
- **Chiffrement robuste :** Le risque d'interceptions malveillantes est réduit
- **Ré-authentification :** Les sessions sont gérées de façon plus strictes pour un renfort de la sécurité des accès
- **Intégration de la MFA :** Des protocoles plus modernes sont compatibles avec la double authentification

Les différentes alternatives pour sécuriser NTLM ou le remplacer

A noter que l'ensemble de ces protocoles doivent à un moment utiliser un canal chiffré, assuré par TLS/SSL.

Kerberos

Il est devenu le protocole d'authentification par défaut dans les environnements Windows modernes, y compris Active Directory. Kerberos utilise des tickets cryptés et des clés secrètes pour authentifier les utilisateurs et les services.

Authentification à deux facteurs (MFA)

MFA ajoute une couche supplémentaire de sécurité à l'authentification en exigeant plusieurs formes distinctes d'authentification. Cela peut inclure quelque chose que l'utilisateur sait (comme un mot de passe) et quelque chose qu'il possède (comme un code généré par une application mobile ou envoyé par SMS).

Authentification basée sur les certificats

Cette approche utilise des certificats numériques pour authentifier les utilisateurs ou les appareils. Les certificats sont émis par des autorités de certification approuvées et offrent une forme d'authentification plus forte que les noms d'utilisateurs et les mots de passe seuls.

OAuth et OpenID Connect

OAuth est un protocole d'autorisation ouvert qui permet aux utilisateurs d'accorder l'accès à leurs informations à des applications tierces sans partager leurs informations d'identification. OpenID Connect est une couche d'identité basée sur OAuth 2.0.

SAML (Security Assertion Markup Language)

SAML est un cadre d'échange de données ouvert qui permet l'authentification et l'autorisation sécurisées entre les domaines. Il est couramment utilisé pour l'authentification unique (SSO) et la fédération d'identité entre différents fournisseurs d'identité.

LDAP (Lightweight Directory Access Protocol)

LDAP est un protocole logiciel utilisé pour accéder et gérer les entrées dans un service d'annuaire, tel qu'Active Directory. Ce n'est pas un protocole d'authentification en soi, il peut être utilisé en conjonction avec d'autres mécanismes d'authentification pour fournir une authentification et une autorisation sécurisées.

Les clés de notre accompagnement

- Réalisation d'un inventaire complet utilisant le protocole NTLM
- Mesure de la fiabilité des outils pouvant remplacer NTLM
- Etudes des différentes alternatives
- Réalisation de POC
- Déploiement du nouveau protocole d'authentification
- Formation des équipes au nouveau protocole

Nos offres cybersécurité

Gestion de la sécurité opérationnelle	Conseils et audits de sécurité	Gouvernance et processus de sécurité	Sensibilisation et formation
Gérer les incidents, déployer des solutions de sécurité, exploiter la virtualisation et gérer les comptes à privilèges et assurer la gestion des identités et des accès.	Réaliser des audits de sécurité des applications, infrastructures et postes de travail, et analyser les comportements suspicieux.	Cartographier les détections sur le SI, mettre en place des processus de sécurité opérationnelle, analyser les incidents, vérifier l'homogénéité des configurations système et sécurité.	Rédiger les documentations de cybersécurité et gouvernance, sensibiliser les équipes, organiser des formations et un plan de sensibilisation.

Contactez-nous

Tél : 01 84 16 49 71
Email : lerhino@synapsys-groupe.com
Paris • Lille • Lyon • Kuala Lumpur
www.synapsys-groupe.com

Découvrez nos ressources