Quelle est la différence entre l'authentification NTLM et LDAP ?

Contenu

Question

Quelle est la différence entre l'authentification NTLM et LDAP ?

Environnement

Cisco Web Security Appliance (WSA), toutes les versions d'AsyncOS

L'authentification avec l'appareil de sécurité Web peut être divisée en plusieurs possibilités :

Client > WSA	WSA > Serveur d'authentification	Type de serveur d'authentification
Authentification de base	Authentification LDAP	Serveur LDAP
Authentification de base	Authentification LDAP	Serveur Active Directory utilisant LDAP
Authentification de base	Authentification NTLM Basic	Serveur Active Directory (NTLM Basic)
Authentification NTLM	Authentification NTLMSSP	Serveur Active Directory (NTLMSSP)

Note: NTLMSSP est généralement appelé NTLM.

La différence notable entre l'authentification de base et l'authentification NTLM est indiquée ci-dessous.

Expérience client

De base

Le client est toujours invité à fournir des informations d'identification. Une fois les informations d'identification saisies, les navigateurs proposent généralement une case à cocher permettant de mémoriser les informations d'identification fournies. Chaque fois que le navigateur est fermé, le client demande à nouveau ou renvoie les informations d'identification précédemment mémorisées.

Note: NTLM Basic utilise l'authentification de base à partir du client et aura donc les mêmes propriétés.

NTLM (SSP)

- Le client s'authentifiera de manière transparente à l'aide de ses informations d'identification de connexion Windows.
- Les seuls cas dans lesquels le client demandera des informations d'identification sont si les informations d'identification Windows échouent d'abord (cela se produira si le client est connecté localement à l'ordinateur et non au domaine utilisé pour l'authentification) ou si le client n'a pas confiance dans le WSA.

Sécurité

De base

Les informations d'identification sont envoyées de manière insécurisée à l'aide de texte brut. Une simple capture de paquets entre le client et le WSA indique le nom d'utilisateur ET le mot de passe de l'utilisateur.

NTLM (SSP)

Les informations d'identification sont envoyées de manière sécurisée via une connexion en trois étapes (authentification de type digest). Le mot de passe n’est JAMAIS envoyé sur le câble.

Le processus NTLM ressemble à ceci :

1. Le client envoie un paquet de négociation NTLM. Ceci indique au WSA que le client a l'intention de faire l'authentification NTLM.
2. Le WSA envoie une chaîne de défi NTLM au client.
3. Le client utilise un algorithme basé sur son mot de passe pour modifier le défi et envoie la réponse au WSA.
4. Le serveur AD vérifie ensuite que le client utilise le mot de passe correct en fonction de la modification appropriée ou non de la chaîne de confirmation.