Contenu

[Question](#)
[Environnement](#)
[Expérience de client](#)
[De base](#)
[NTLM (SSP)](#)
[Sécurité](#)
[De base](#)
[NTLM (SSP)](#)

Question

Quelle est la différence entre NTLM et authentification LDAP ?

Environnement

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

L'authentification avec le WSA peut être décomposée en possibilités suivantes :

Client > WSA	WSA > serveur d'authentification	Type de serveur d'authentification
Authentification de base	Authentification LDAP	Serveur LDAP
Authentification de base	Authentification LDAP	Serveur de Répertoire actif utilisant le LDAP
Authentification de base	Authentification de base NTLM	Serveur de Répertoire actif (NTLM de base)
Authentification NTLM	Authentification NTLMSSP	Serveur de Répertoire actif (NTLMSSP)

Remarque: NTLMSSP désigné généralement sous le nom de NTLM.

La différence remarquable entre l'authentification de base et l'authentification NTLM sont ci-dessous.

Expérience de client

De base

Le client sera toujours incité pour des qualifications. Après que des qualifications aient été

entrées, les navigateurs offriront typiquement une case pour se souvenir les qualifications fournies. Quand le navigateur est fermé, le client incitera de nouveau ou enverra les qualifications de nouveau précédemment retrouvées.

Remarque: NTLM de base utilise l'authentification de base du client et aura ainsi les mêmes propriétés.

NTLM (SSP)

- Le client authentifiera d'une manière transparente utilisant ses qualifications de connexion de Windows.
- Les seuls cas en lesquels le client incitera pour des qualifications sont si les qualifications de Windows échouent d'abord (ceci se produiront si le client est ouvert une session localement à l'ordinateur et pas au domaine utilisé pour l'authentification) ou si le client ne fait pas confiance au WSA.

Sécurité

De base

Des qualifications sont envoyées peu sûr utilisant le texte brut. Une capture simple de paquet entre le client et le WSA indiquera le nom d'utilisateur et mot de passe de l'utilisateur.

NTLM (SSP)

Des qualifications sont envoyées sécurisé par l'intermédiaire d'une connexion en trois étapes (authentification de style de condensé). Le mot de passe n'est jamais envoyé à travers le fil.

Les aspects de processus NTLM en tant que tels :

1. Le client envoie un NTLM négocient le paquet. Ceci indique le 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 de défi au WSA.
4. Le serveur d'AD vérifie alors que le client utilise le mot de passe correct basé en fonction s'il a modifié la chaîne de défi convenablement.