Worin besteht der Unterschied zwischen NTLM- und LDAP-Authentifizierung?

Inhalt

Frage

Worin besteht der Unterschied zwischen NTLM- und LDAP-Authentifizierung?

Umgebung

Cisco Web Security Appliance (WSA), alle Versionen von AsyncOS

Die Authentifizierung mit der WSA kann in folgende Möglichkeiten unterteilt werden:

Client > WSA	WSA > Authentifizierungsserver	Authentifizierungsservertyp
Grundlegende Authentifizierung	LDAP-Authentifizierung	LDAP-Server
Grundlegende Authentifizierung	LDAP-Authentifizierung	Active Directory-Server mit LDAP
Grundlegende Authentifizierung	NTLM-Standardauthentifizierung	Active Directory-Server (NTLM Basic)
NTLM-Authentifizierung	NTLMSSP-Authentifizierung	Active Directory-Server (NTLMSSP)

Hinweis: NTLMSSP wird allgemein als NTLM bezeichnet.

Der bemerkenswerte Unterschied zwischen der Standardauthentifizierung und der NTLM-Authentifizierung ist unten dargestellt.

Kundenerlebnis

Einfach

Der Client wird immer zur Eingabe von Anmeldeinformationen aufgefordert. Nach Eingabe der Anmeldeinformationen bieten Browser in der Regel ein Kontrollkästchen, um sich die angegebenen Anmeldeinformationen zu merken. Bei jedem Schließen des Browsers fordert der Client erneut an oder sendet die zuvor gespeicherten Anmeldeinformationen erneut.

Hinweis: NTLM Basic verwendet die Standardauthentifizierung des Clients und verfügt daher über dieselben Eigenschaften.

NTLM (SSP)

- Der Client authentifiziert sich transparent mithilfe seiner Windows-Anmeldeinformationen.
- Die einzigen Fälle, in denen der Client zur Eingabe von Anmeldeinformationen auffordert, sind, wenn die Windows-Anmeldeinformationen zunächst fehlschlagen (dies tritt auf, wenn der Client lokal am Computer angemeldet ist und nicht an der für die Authentifizierung verwendeten Domäne) oder wenn der Client der WSA nicht vertraut.

Sicherheit

Einfach

Anmeldeinformationen werden unsicher mit Nur-Text gesendet. Bei einer einfachen Paketerfassung zwischen dem Client und der WSA werden der Benutzername UND das Kennwort des Benutzers angezeigt.

NTLM (SSP)

Die Anmeldeinformationen werden sicher über einen Drei-Wege-Handshake (Digest-Style-Authentifizierung) gesendet. Das Kennwort wird NIE über die Leitung übertragen.

Der NTLM-Prozess sieht wie folgt aus:

1. Der Client sendet ein NTLM-Negotiate-Paket. Dies teilt der WSA mit, dass der Client eine NTLM-Authentifizierung vornimmt.
2. Die WSA sendet eine NTLM Challenge-Zeichenfolge an den Client.
3. Der Client verwendet einen auf seinem Kennwort basierenden Algorithmus, um die Herausforderung zu ändern, und sendet die Antwort auf die Herausforderung an die WSA.
4. Der AD-Server überprüft dann, ob der Client das richtige Kennwort verwendet, basierend darauf, ob er die Challenge entsprechend modifiziert hat oder nicht.