Qual è la differenza tra l'autenticazione NTLM e LDAP?

Sommario

Domanda

Qual è la differenza tra l'autenticazione NTLM e LDAP?

Ambiente

Cisco Web Security Appliance (WSA), tutte le versioni di AsyncOS

L'autenticazione con WSA può essere suddivisa nelle seguenti possibilità:

Client > WSA	WSA > Server di autenticazione	Tipo di server di autenticazione
Autenticazione di base	Autenticazione LDAP	server LDAP
Autenticazione di base	Autenticazione LDAP	Server Active Directory che utilizza LDAP
Autenticazione di base	Autenticazione di base NTLM	Server Active Directory (NTLM Basic)
autenticazione NTLM	autenticazione NTLMSSP	Server Active Directory (NTLMSSP)

Nota: NTLMSSP viene comunemente denominato NTLM.

Di seguito sono riportate le differenze significative tra l'autenticazione di base e l'autenticazione NTLM.

Esperienza client

Base

Al client verranno sempre richieste le credenziali. Dopo l'immissione delle credenziali, i browser offrono in genere una casella di controllo per memorizzare le credenziali fornite. Ogni volta che il browser viene chiuso, il client richiederà nuovamente o invierà di nuovo le credenziali memorizzate in precedenza.

Nota: NTLM Basic utilizza l'autenticazione di base del client e pertanto avrà le stesse proprietà.

NTLM (SSP)

- Il client verrà autenticato in modo trasparente utilizzando le credenziali di accesso di Windows.
- Gli unici casi in cui il client richiederà le credenziali sono se le credenziali di Windows non riescono per la prima volta (ciò si verifica se il client ha eseguito l'accesso localmente al computer e non al dominio utilizzato per l'autenticazione) o se il client non considera attendibile WSA.

Sicurezza

Base

Le credenziali vengono inviate in modo non protetto utilizzando testo normale. Una semplice acquisizione di pacchetti tra il client e il server WSA rivelerà il nome utente E la password dell'utente.

NTLM (SSP)

Le credenziali vengono inviate in modo protetto tramite un handshake a tre vie (autenticazione di tipo digest). La password non viene mai inviata attraverso il cavo.

L'aspetto del processo NTLM è il seguente:

1. Il client invia un pacchetto di negoziazione NTLM. In questo modo il WSA informa che il client intende eseguire l'autenticazione NTLM.
2. WSA invia una stringa di richiesta di verifica NTLM al client.
3. Il client utilizza un algoritmo basato sulla propria password per modificare la richiesta di verifica e invia la risposta alla richiesta di verifica al server WSA.
4. Il server AD verifica quindi che il client utilizzi la password corretta a seconda che abbia modificato o meno la stringa di richiesta in modo appropriato.