Come dovrebbe essere l'autenticazione NTLM a livello di pacchetto?

Sommario

[Introduzione](#)
[Come dovrebbe essere l'autenticazione NTLM a livello di pacchetto?](#)
[Numero e dettagli del pacchetto](#)

Introduzione

Questo documento descrive l'autenticazione NT LAN Manager (NTLM) a livello di pacchetto.

Come dovrebbe essere l'autenticazione NTLM a livello di pacchetto?

Un'acquisizione di pacchetti per seguire questo articolo può essere scaricata qui: https://supportforums.cisco.com/sites/default/files/attachments/document/ntlm_auth.zip

IP client: 10.122.142.190

IP WSA: 10.122.144.182

Numero e dettagli del pacchetto

#4 Il client invia una richiesta GET al proxy.

#7 Il proxy restituisce un 407. Ciò significa che il proxy non consente il traffico per mancanza di autenticazione corretta. Se si esaminano le intestazioni HTTP in questa risposta, verrà visualizzato il messaggio "Proxy-authentication: NTLM". In questo modo il client viene informato che un metodo di autenticazione accettabile è NTLM. Analogamente, se l'intestazione "Proxy-authentication: Basic", il proxy indica al client che le credenziali di base sono accettabili. Se sono presenti entrambe le intestazioni (comune), il client decide quale metodo di autenticazione utilizzare.

Da notare che l'intestazione di autenticazione è "Proxy-authentication:". Infatti la connessione nell'acquisizione utilizza un proxy di inoltro esplicito. Se si trattasse di una distribuzione proxy trasparente, il codice di risposta sarebbe 401 anziché 407 e le intestazioni sarebbero "www-authentication:" anziché "proxy-authentication:".

#8 Il proxy INVIA questo socket TCP. Si tratta di un comportamento corretto e normale.

#15 Su un nuovo socket TCP, il client esegue un'altra richiesta GET. Questa volta si noti che il metodo GET contiene l'intestazione HTTP "proxy-authorization:". Contiene una stringa codificata contenente dettagli relativi all'utente o al dominio.

Se si espande Autorizzazione-Proxy > NTLMSSP, le informazioni decodificate verranno inviate nei

dati NTLM. In "Tipo di messaggio NTLM", si noterà che è "NTLMSSP_NEGOTIATE". Questo è il primo passaggio dell'handshake NTLM a tre vie.

#17 Il proxy risponde con un altro 407. È presente un'altra intestazione "proxy-authentication". Questa volta contiene una stringa di richiesta NTLM. Se si espande ulteriormente, il tipo di messaggio NTLM sarà "NTLMSSP_CHALLENGE". Questo è il secondo passaggio dell'handshake NTLM a tre vie.

Nell'autenticazione NTLM, il controller di dominio di Windows invia una stringa di richiesta al client. Il client applica quindi un algoritmo alla richiesta di verifica NTLM che determina la password dell'utente nel processo. In questo modo, il controller di dominio può verificare che il client conosca la password corretta senza inviare la password da una riga all'altra. Questo è molto più sicuro delle credenziali di base, in cui la password viene inviata in testo normale per tutti i dispositivi di sniffing.

#18 Il client invia un GET finale. Notare che questo GET si trova sullo STESSO socket TCP su cui si sono verificati la negoziazione NTLM e la richiesta NTLM. Questo è fondamentale per il processo NTLM. L'intero handshake deve essere eseguito sullo stesso socket TCP. In caso contrario, l'autenticazione non sarà valida.

In questa richiesta il client invia al proxy la richiesta NTLM modificata (risposta NTLM). Questo è il passaggio finale dell'handshake NTLM a tre vie.

#21 Il proxy invia una risposta HTTP. Il proxy ha accettato le credenziali e ha deciso di rendere disponibili i contenuti.