在資料包級別，NTLM身份驗證應是什麼樣的？

目錄

簡介

本檔案介紹封包層級的NT LAN Manager(NTLM)驗證。

在資料包級別，NTLM身份驗證應是什麼樣的？

可在此處下載遵循本文的資料包捕獲
：https://supportforums.cisco.com/sites/default/files/attachments/document/ntlm_auth.zip

客戶端IP:10.122.142.190

WSA IP:10.122.144.182

封包編號和詳細資訊

#4使用者端將GET要求傳送到Proxy。

#7代理傳回407。這表示由於缺少正確的身份驗證，代理不允許流量。如果您檢視此回應中的HTTP標頭，將會看到「Proxy-authenticate:NTLM」。 這告訴客戶端可接受的身份驗證方法是NTLM。同樣，如果標頭「Proxy-authenticate:Basic」表示，Proxy告知使用者端基本憑證可接受。如果存在兩個標頭（公用），則使用者端會決定它將使用的驗證方法。

需要注意的是，驗證標頭是「Proxy-authenticate：」。 這是因為捕獲中的連線使用顯式轉發代理。如果這是透明代理部署，則響應代碼為401而不是407，報頭為「www-authenticate：」而不是「proxy-authenticate：」。

#8代理FIN為此TCP套接字。這是正確和正常的。

#15在新的TCP套接字上，客戶端執行另一個GET請求。這次會注意到GET包含HTTP標頭「proxy-authorization：」。 其中包含包含有關使用者/域的詳細資訊的編碼字串。

如果展開Proxy-authorization > NTLMSSP，則會看到在NTLM資料中傳送的解碼資訊。在「NTLM消息型別」中，您會注意到它是「NTLMSSP_NEGOTIATE」。 這是三向NTLM握手的第一步。

#17代理使用另一個407進行響應。存在另一個「proxy-authenticate」標頭。這次它包含NTLM質詢字串。如果進一步展開，您將看到NTLM消息型別為「NTLMSSP_CHALLENGE」。 這是三向NTLM握手中的第二步。

在NTLM身份驗證中，Windows域控制器將質詢字串傳送到客戶端。然後，客戶端將演算法應用到

NTLM質詢，該質詢會在此過程中影響使用者的密碼。這樣，域控制器就能夠驗證客戶端知道正確的密碼，而無需通過線路傳送密碼。這比基本憑證安全得多，基本憑證是以純文字檔案形式傳送密碼，供所有監聽裝置檢視。

#18使用者端傳送最終GET。請注意，此GET與NTLM協商和NTLM質詢發生在同一個TCP套接字上。這對於NTLM過程至關重要。整個握手必須發生在同一個TCP套接字上，否則身份驗證將無效。

在此請求中，客戶端將修改的NTLM質詢（NTLM響應）傳送到代理。這是三向NTLM握手的最後一步。

#21 Proxy傳回HTTP回應。這表示代理已接受憑證並決定提供該內容。