パケット レベルでの NTLM 認証はどのような内容になりますか

目次

概要

この資料は水平なパケットで NT LAN Manager （ NTLM ） 認証を記述したものです。

パケット レベルでの NTLM 認証はどのような内容になりますか

この技術情報に続くパケットキャプチャはここにダウンロードすることができます
: https://supportforums.cisco.com/sites/default/files/attachments/document/ntlm_auth.zip

クライアントIP: 10.122.142.190

WSA IP: 10.122.144.182

パケット数および詳細

#4 はプロキシにクライアント GET 要求を送信 します。

#7 はプロキシ 407 を送返します。 これはプロキシが適切な認証の欠如によるトラフィックを可能にしないことを意味します。 この応答の HTTP ヘッダーを調べると、「Proxy-authenticate: NTLM」とあります。 これは、クライアントに対し、許容される認証方式が NTLM であることを通知するものです。 同様に、ヘッダーに「Proxy-authenticate: 基本は」あります、基本的な資格情報が受諾可能であることをプロキシはクライアントに告げます。 ヘッダが両方とも (よくある) あれば、クライアントはどの認証方式を使用するか決定します。

注意しなければならないのは、認証ヘッダーが「Proxy-authenticate: 」というエラー メッセージが表示されます。 これはキャプチャの接続が明示的 な前方プロキシを使用するという理由によります。 これが透過的なプロキシ配備だった場合、応答コードは 407 の代りに 401 であり、ヘッダは「www 認証するです: 「proxy-authenticate:」ではなく「www-authenticate:」となります 」というエラー メッセージが表示されます。

#8 プロキシ FIN この TCP ソケット。 これは正常かつ通常の動作です。

新しい TCP ソケットの #15 はクライアント別の GET 要求を行います。 今回は、GET リクエストに HTTP ヘッダー「proxy-authorization:」が含まれていることに注意してください 」というエラー メッセージが表示されます。 このヘッダーにエンコードされた文字列は、ユーザ/ドメインに関する詳細を記述します。

[Proxy-Authorization] > [NTLMSSP] を展開すると、NTLM データで送信された、デコードされた

情報が表示されます。 NTLM メッセージタイプでは、それが「LMSSP_NEGOTIATE」であることがわかります。 これは三方 NTLM ハンドシェイクの第一歩です。

#17 はもう 407 とプロキシ応答します。 別の「Proxy-authenticate」ヘッダーが存在します。 今回それは NTLM チャレンジ ストリングを示します。 ヘッダーをさらに展開すると、NTLM メッセージ タイプが「NTLMSSP_CHALLENGE」となっていることがわかります。 これは三方 NTLM ハンドシェイクの第2ステップです。

NTLM 認証では、Windows ドメイン コントローラがクライアントにチャレンジ文字列を送信します。 クライアントはプロセスのユーザ パスワードで考慮する NTLM チャレンジにそれからアルゴリズムを加えます。 これにより、ドメイン コントローラは回線を介してパスワードを送信することなく、クライアントが正しいパスワードを知ってることを確認できます。 これはパスワードがすべての探知 デバイスのための平文で見るために送信される基本的な資格情報より大いにセキュアです。

#18 はクライアント最終的な GET を送信 します。 この GET リクエストは、NTLM ネゴシエートおよび NTLM チャレンジが行われたのと同じ TCP ソケットに対して行われることに注意してください。 これは、NTLM プロセスに非常に重要な点です。 ハンドシェイク全体が同じ TCP ソケットで行われなければ、認証は無効になってしまうためです。

この GET リクエストで、クライアントは変更後の NTLM チャレンジ（NTLM 応答）をプロキシに送信します。 これは三方 NTLM ハンドシェイクの最後の段階です。

#21 はプロキシ HTTP応答を送返します。 これは、プロキシがクレデンシャルを受け入れ、コンテンツの提供を決定したことを意味します。