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

質問：

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

ip.addr==165.2.2.129.158 client
ip.addr==165.202.2.150 WSA>

パケット番号/詳細：

#4 はプロキシにクライアント GET 要求を送信 します

#6 はプロキシ 407 を送返します。 これは、適切な認証が行われていないため、プロキシがトラフィックを許可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: Basic」と示されている場合、プロキシはクライアントに対し、基本認証が許容されると通知していることになります。 両方のヘッダーが存在する場合（共通）、クライアントがどちらの認証方式を使用するかを決定できます。

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、キャプチャされた接続が明示的な転送プロキシを使用しているためです。 プロキシが透過的に導入されているとしたら、応答コードは 407 ではなく 401 となり、ヘッダーは 「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。 これが、3 ウェイ NTLM ハンドシェイクの最初のステップです。

#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。 今回ここに含まれているのは、NTLM チャレンジ文字列です。 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。 これが、3 ウェイ NTLM ハンドシェイクの 2 番目のステップです。

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。 すると、クライアントは NTML チャレンジにアルゴリズムを適用して、このプロセスでユーザ パスワードを抽出します。 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。 この方法は、すべてのスニッフィング デバイスが確認できる平文でパスワードが送信されないという点で、基本認証より遥かに安全です。
#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。 これが、3 ウェイ NTLM ハンドシェイクの最終ステップです。
#20 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。