数据包级别的 NTLM 身份验证是什么样的？

文档编号：117931

作者：Josh Wolfer 和 Jeff Richmond，Cisco TAC 工程师。 2014 年 7

月 14 日

目录

问题：

数据包级别的 NTLM 身份验证是什么样的？

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

数据包编号/详细信息：

4 - 客户端向代理发送 GET 请求

6 - 代理发回 407。 这表示代理由于缺乏适当的身份验证而未允许该流量。 如果查看此响应中的 HTTP 报头，您将看到“Proxy-authenticate: NTLM”。 这将告知客户端身份验证的可接受方法是 NTLM 。 同样，如果存在报头“Proxy-authenticate: Basic”，则代理告知客户端可以接受基本凭证。 如果存在两个报头（通用），则客户端将决定要使用的身份验证方法。

请注意，验证报头是“Proxy-authenticate:”。 这是因为捕获的连接使用显式转发代理。 如果这是透明代理部署，则响应代码为 401 而不是 407，并且报头为“www-authenticate:”而不是“proxy-authenticate:”。

8 - 代理对此 TCP 套接字执行 FIN 操作。 这是正确并且正常的。

15 - 在新的 TCP 套接字上，客户端执行另一 GET 请求。 此时要注意，GET 中包含 HTTP 报头“proxy-authorization:”。 其中包含用户/域相关详细信息的编码字符串。

如果展开“代理-授权”(Proxy-authorization) > NTLMSSP，您将看到在 NTLM 数据中发送的解码信息。 在“NTLM 消息类型”(NTLM Message Type) 中，您将看到它是“NTLMSSP_NEGOTIATE”。 这是 3 次 NTLM 握手的第一步。

17 - 代理将响应另一个 407。 将出现另一个“proxy-authenticate”报头。 此时其中包含 NTLM 质询字符串。 如果您进一步展开，您会看到 NTLM 消息类型为“NTLMSSP_CHALLENGE”。 这是 3 次 NTLM 握手的第二步。

在 NTLM 身份验证中，Windows 域控制器会将质询字符串发送到客户端。

然后，客户端在该流程中对用户密码中的 NTLM 质询因素应用算法。 这样将允许域控制器验证客户端是否知道正确密码，而不必通过线路发送密码。 这是一种比基本凭证更为安全的方法，密码以明文方式发送，供所有嗅探设备查看。
18 - 客户端发送最终的 GET。 请注意，此 GET 位于 NTLM 协商和 NTLM 质询所在的同一 TCP 套接字上。 这对于 NTLM 流程至关重要。 整个握手过程必须在同一 TCP 套接字上完成，否则身份验证无效。

在此请求中，客户端将向代理发送修改的 NTLM 质询（NTLM 响应）。 这是 3 次 NTLM 握手的最后一步。
20 - 代理发回 HTTP 响应。 这表示代理已接受凭证并决定提供内容服务。

更新日期：2014 年 7 月 14 日 文档编号：117931
