验证看起来应该NTLM在数据包成水平什么？

目录

问题：

验证看起来应该NTLM在数据包成水平什么？

ip.addr==165.2.2.129.158客户端
ip.addr==165.202.2.150 WSA>

数据包编号/详细信息：

#4客户端发送GET请求给代理

#6代理退还407。这意味着代理不允许流量由于缺乏适当的验证。如果查看在此答复的HTTP包头，您将看到“代理验证：NTLM”。这告诉客户端一个可接受验证方法是NTLM。同样，如果报头“代理验证：基本”存在，代理是告诉客户端基本凭证是可接受。如果两个报头存在(普通)，客户端将决定哪个验证方法将使用。

注释的一件事是认证报头是“代理验证：”。这是因为在捕获的连接使用明确向前代理。如果这是一透明代理部署，答复代码是401，而不是407，并且报头是“WWW验证：”而不是“请代理验证：”。

#8代理FIN此TCP socket。这是正确和正常。

在一新的TCP socket的#15客户端执行另一GET请求。这次公告GET包含HTTP报头“代理授权：”。这包含包含关于用户/域的详细信息的一个编码的字符串。

如果展开代理授权> NTLMSSP，您将看到在NTLM数据发送的解码的信息。在“NTLM消息类型”，您注意它是“NTLMSSP_NEGOTIATE”。这是在3种方式NTLM握手的第一步。

代理回应另外407的#17。别的“代理验证”报头存在。包含NTLM挑战字符串的这次。如果进一步展开它，您看到NTLM消息类型是“NTLMSSP_CHALLENGE”。这是在3种方式NTLM握手的第二步。

在NTLM验证， Windows域控制器发送挑战字符串给客户端。客户端然后运用算法对析因在进程的用户密码的NTLM挑战。这允许域控制器验证客户端认识正确密码，无需发送在线路间的密码。这是更多安全然后基本凭证，密码在所有探测设备的纯文本被发送能发现。
#18客户端发送最终GET。注意此GET在NTLM协商和发生的NTLM挑战的TCP socket和一样。这对NTLM进程是重要的。整个握手在同样TCP socket必须发生，否则验证无效。

在此请求客户端发送已修改NTLM挑战(NTLM答复)对代理。这是在3种方式NTLM握手的最后一步。
#20代理退还HTTP响应。这意味着代理接受凭证和决定服务内容。