认证看起来应该NTLM在信息包成水平什么？

Contents

Introduction

本文描述NT LAN Manager (NTLM)认证在信息包级别。

认证看起来应该NTLM在信息包成水平什么？

可以下载跟随此条款的信息包获取这里
： https://supportforums.cisco.com/sites/default/files/attachments/document/ntlm_auth.zip

客户端IP ：10.122.142.190

WSA IP ：10.122.144.182

数据包编号和详细资料

#4客户端发送一个GET请求到代理。

#7代理退还一407。这意味着代理不允许数据流由于缺乏适当的验证。如果查看在此回应的HTTP包头，您将看到“代理验证：NTLM”。这告诉客户端一个可接受的验证方法是NTLM。同样，如果报头“代理验证：基本的”是存在，代理告诉客户端基本的证件是可接受的。如果两个报头存在(普通)，客户端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。如果这是透明代理配置，回应代码是401而不是407，并且报头是“WWW验证：”而不是“请代理验证：".

#8代理飞翅此TCP插槽。这是正确和正常的。

在一个新的TCP插槽的#15客户端执行另一个GET请求。这次公告GET包含HTTP包头“代理授权：".这包含包含关于用户/域的详细资料的一个编码的字符串。

如果扩展代理授权> NTLMSSP，您将看到在NTLM数据发送的解码的信息。在“NTLM消息请选择"， you will notice that it is " NTLMSSP_NEGOTIATE”。这是在三通的NTLM握手的第一步。

#17代理回应另外407。别的“代理验证”报头存在。这次它包含一个NTLM挑战字符串。如果进一步扩展它，您看到NTLM消息类型是“NTLMSSP_CHALLENGE”。这是在三通的NTLM握手的第二步。

在NTLM认证， Windows域控制器发送一个挑战字符串到客户端。客户端然后运用一种算法于在用户密码在进程中析因的NTLM挑战。这允许域控制器验证客户端认识正确的密码，无需发送在线路间的密码。这比基本的证件安全，密码被发送以所有探测设备的纯文本能发现。

#18客户端发送最终GET。注意此GET在NTLM协商的TCP插槽和一样，并且NTLM挑战发生了在。这对NTLM进程是重要的。整个握手在同一个TCP插槽必须发生，否则认证无效。

在此请求客户端发送被修改的NTLM挑战(NTLM回应)到代理。这是在三通的NTLM握手的最终步骤。

#21代理发送一种HTTP回应。这意味着代理接受了证件和决定服务内容。