كيف يجب أن تبدو مصادقة NTLM على مستوى الحزمة؟

المحتويات

المقدمة

يصف هذا المستند مصادقة مدير شبكة NTLM) LAN) على مستوى الحزمة.

كيف يجب أن تبدو مصادقة NTLM على مستوى الحزمة؟

يمكن تنزيل التقاط حزمة لمتابعة هذا المقال هنا:
https://supportforums.cisco.com/sites/default/files/attachments/document/ntlm_auth.zip

Client IP: 10.122.142.190

WSA IP: 10.122.144.182

رقم الحزمة وتفاصيلها

رقم 4 يرسل العميل طلب GET إلى الوكيل.

رقم 7 يرسل الوكيل رقم 407. هذا يعني أن الوكيل لا يسمح بحركة المرور بسبب نقص المصادقة المناسبة. إذا نظرت إلى رؤوس HTTP في هذه الاستجابة، فسترى "Proxy-authenticate: NTLM". وهذا يوضح للعميل أن طريقة المصادقة المقبولة هي NTLM. وبالمثل، إذا كان الرأس "Proxy-Authenticate: Basic" موجودا، فإن الوكيل يخبر العميل بأن بيانات الاعتماد الأساسية مقبولة. في حالة وجود كلا الرأسين (شائع)، يقرر العميل طريقة المصادقة التي سيستخدمها.

هناك شيء واحد لملاحظته وهو أن رأس المصادقة هو "Proxy-authentication:". وذلك لأن الاتصال في التقاط يستخدم وكيل إعادة توجيه صريح. إذا كان هذا نشر وكيل شفاف، فسيكون رمز الاستجابة 401 بدلا من 407 وتكون الرؤوس "www-authenticate:" بدلا من "proxy-authenticate:".

رقم 8 للوكيل FINs مقبس TCP هذا. هذا صحيح وطبيعي.

#15 في مأخذ توصيل TCP جديد يقوم العميل بتنفيذ طلب GET آخر. إشعار الوقت هذا بأن GET يحتوي على رأس HTTP "تفويض الوكيل:". يحتوي هذا على سلسلة مرمزة تحتوي على تفاصيل تتعلق بالمستخدم / المجال.

إذا قمت بتوسيع تفويض الوكيل > NTLMSSP، فسترى المعلومات التي تم فك ترميزها المرسلة في بيانات NTLM. في "نوع رسالة NTLM"، ستلاحظ أنه "NTLMSSP_NEGOTIATE". هذه هي الخطوة الأولى في مصافحة NTLM الثلاثية.

رقم 17 يستجيب الوكيل برقم 407 آخر. يوجد رأس آخر "Proxy-authenticate". تحتوي هذه المرة على سلسلة تحديات NTLM. إذا قمت بتوسيعه أكثر، فسترى نوع رسالة NTLM هو "NTLMSSP_CHALLENGE". هذه هي

الخطوة الثانية في مصافحة NTLM الثلاثية.

في مصادقة NTLM، ترسل وحدة التحكم بالمجال ل Windows سلسلة تحديات إلى العميل. وبعد ذلك، يطبق العميل خوارزمية على تحدي NTLM وهي العوامل الموجودة في كلمة مرور المستخدم في العملية. وهذا يسمح لوحدة التحكم بالمجال بالتحقق من أن العميل يعرف كلمة المرور الصحيحة دون إرسال كلمة المرور عبر الخط على الإطلاق. هذا أكثر أمانا من بيانات الاعتماد الأساسية، التي فيها يتم إرسال كلمة المرور في نص عادي لكل أجهزة التقصي لترى.

رقم 18 يرسل العميل GET النهائي. لاحظ أن GET هذا موجود على نفس مأخذ توصيل TCP كما حدث على تفاوض NTLM وتحدي NTLM. وهذا أمر حيوي لعملية NTLM. يجب أن تحدث عملية المصافحة بالكامل على مأخذ توصيل TCP نفسه، وإلا ستكون المصادقة غير صالحة.

في هذا الطلب، يرسل العميل تحدي NTLM المعدل (إستجابة NTLM) إلى الوكيل. هذه هي الخطوة الأخيرة في مصافحة NTLM الثلاثية.

#21 يرسل الوكيل إستجابة HTTP. وهذا يعني أن الوكيل قبل وثائق الاعتماد وقرر تقديم المحتوى.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).