پروتکل NTLM خلاصه شده عبارت NT LAN Manager است. پروتکلNTLM ، پروتکل پیش فرض احراز هویت در یک شبکه کامپیوتری بوده که توسط مایکروسافت در سیستم عامل ویندوز NT 4.0 مورد استفاده قرار میگرفته است.

NTLMیک پروتکل "Challenge Response" است که در حال حاضر برای ایجاد هماهنگی با نسخه های پایین تر از ویندوز ۲۰۰۰ مورد استفاده قرار میگیرد.

احراز هویت به صورت "Challenge Response" گروهی از پروتکل ها را شامل میشود که در آن یک طرف ارتباط سوالی (Challeng)را مطرح میکند و طرف دیگر باید برای آن جوابی معتبر (Response) ارائه کند.

همه پروتکل‌های NTLM کاربران و رایانه‌ها را بر اساس مکانیزم چالش/پاسخ احراز هویت می‌کنند. این شامل این می شود که کاربر به سرور یا کنترل کننده دامنه ثابت کند که رمز عبور مرتبط با حساب را می داند – اما بدون انتقال آن از طریق شبکه. پروتکل های احراز هویت NTLM شامل LAN Manager ورژن ۱ و ۲ و NTLM ورژن ۱ و ۲ است.

NTLMدر سال ۱۹۹۳ با ویندوز NT 3.1 معرفی شد و به دلیل شکاف های امنیتی آشکار جایگزین روش هش LM قبلی شد. به دلیل مشکلات امنیتی بیشتر با پروتکلNTLM ، NTLM v2با ویندوز NT 4.0 SP4 معرفی شد و نسخه قبلی آن NTLM v1نامیده شد.

با انتشار ویندوز ۲۰۰۰، پروتکل NTLM با پروتکل Kerberos به عنوان پروتکل احراز هویت استاندارد برای دامنه های Active Directory (AD) جایگزین شد.

با وجود آسیب‌پذیری‌های شناخته شده در این پروتکل، نسخه‌های مختلف پروتکل NTLM به دلایل سازگاری همچنان در سیستم‌های فناوری اطلاعات فعلی استفاده می شوند NTLM v2 .همچنان برای ورود به سیستم محلی، ورود به شبکه ورک گروپ، برخی از سرورهای http و همچنین برای ورود به سیستم (SSO) استفاده می شود.

تمام این پروتکل های در عمل یک فرایند را دنبال میکنند و تفاوت آن در میزان سطح رمزنگاری موجود در ذات امنیتی آنها است. پروتکل های احراز هویتNTLM ، کلاینت را بر اساس یک مکانیزم "Challenge Response" که به سرور نشان میدهد که کلاینت پسورد متناظر با اکانت را میداند، احراز هویت میکند. پروتکل NTLM میتواند بصورت دلخواه برای امنیتsession ها و بخصوص یکپارچگی و محرمانگی پیام ها نیز مورد استفاده قرار گیرد.

فرآیند احراز هویت پروتکلNTLM

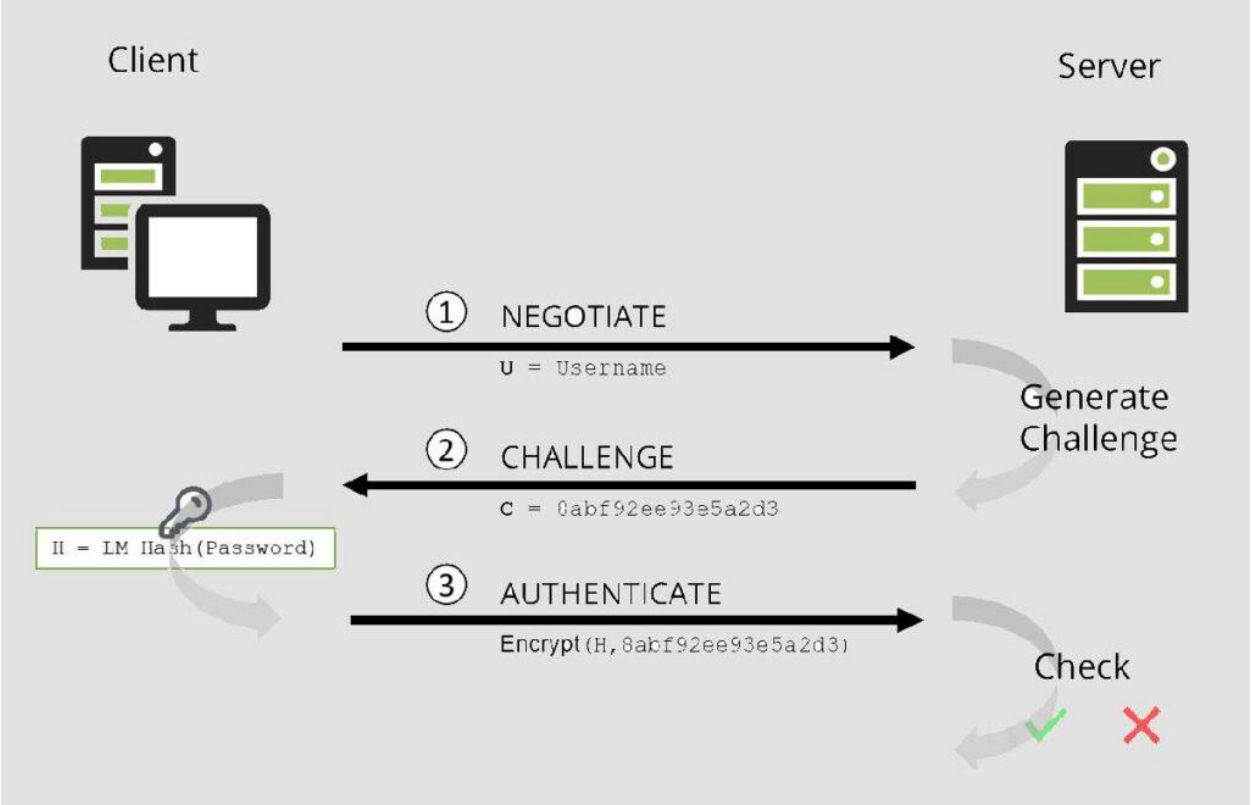
پروتکل NTLM v2 از هش NT در تبادل چالش/پاسخ بین سرور و کلاینت استفاده می کند. جریان احراز هویت NTLM به شرح زیر است:

NEGOTIATE:ماشین سرویس گیرنده درخواستی را با نام کاربری و سایر اطلاعات پیکربندی به سرور ارسال می کند.

CHALLENGE:سرور یک عدد تصادفی تولید می کند و آن را به کامپیوتر مشتری ارسال می کند.

AUTHENTICATE:کامپیوتر کلاینت با استفاده از الگوریتم DES و هش NT رمز عبور به عنوان کلیدی، عدد تصادفی را رمزگذاری می کند تا ثابت کند رمز عبور را می داند.

سرور با اطمینان از اینکه چالش واقعاً با کاربر/گذرواژه صحیح ایجاد شده است، هویت کاربر را تأیید می کند. برای انجام این کار، یا از هش NT ذخیره شده از پایگاه داده SAM خود استفاده می کند یا جفت چالش/پاسخ را برای اعتبارسنجی به کنترل کننده دامنه ارسال می کند.



نقط ضعف پروتکلNTLM

درست است که پروتکل NTLM رمزهای عبوری را از طریق شبکه ارسال نمی کند که قابل رهگیری شوند، اما NTLM v1 یک پروتکل احراز هویت بسیار ضعیف در مقایسه با استانداردهای امروزی است. هر چند که ورژن دوم این پروتکل از ورژن ۱ آن امن تر است اما هنوز با جانشین خود Kerberos فاصله زیادی دارد.

در پروتکل احراز هویتNTLM ، هش رمز عبور یک عنصر حیاتی برای احراز هویت است. بنابراین اگر یک مهاجم نام کاربری و هش رمز عبور را پیدا کند، می‌تواند رویه‌ها را مستقیماً با احراز هویت NTLM شروع کند. دانستن رمز عبور واقعی ضروری نیست. این تکنیک به عنوان Pass the Hash شناخته می شود و بیش از ۲۰ سال است که وجود دارد.

برای یک مهاجم، این سوال مطرح می شود که چگونه می توان نام کاربری و هش رمز عبور را ضبط کرد. به‌عنوان مثال در ترافیک شبکه، نام‌های کاربری از دیدگاه مهاجم به راحتی قابل دریافت هستند. به دست آوردن هش رمز عبور نیز بسیار آسان است. در سیستم های کاربر نهایی، هش رمز عبور را می توان در فایل زیر یافت

C:\Windows\System32\config\SAM

فایل SAM توسط هر کاربری با دسترسی مدیریتی قابل خواندن است. به همین ترتیب، هش های رمز عبور نیز در حافظه پنهان می شوند. از آنجا، آنها را می توان با ابزارهایی مانند Mimikatz استخراج کرد.

در سمت سرور، هش رمز عبور برای کنترلرهای دامنه در فایل ذخیره می شود

C:\Windows\ntds\ntds.dit

در آنجا، هش ها در برابر حملات DC Sync آسیب پذیر هستند. آنها کنترل کننده دامنه (DC) را فریب می دهند تا هش رمز عبور خود را با شخصی که جعل هویت DC دیگری را جعل می کند، همگام کند.

هش های رمز عبور همچنین در حافظه یک اتصال پروتکل دسکتاپ از راه دور (RDP) در طول مدت ارتباط ذخیره می شوند. نابراین اگر ارتباط کاربر بدون خروج از سیستم قطع شود، هش رمز عبور برای مدتی در حافظه باقی می ماند.

اقدامات توصیه شده برای جلوگیری از دسترسی غیرمجاز

- حملات بروت فورس

پروتکل احراز هویت NTLM همچنین در برابر حملات brute force آسیب پذیر است. الگوریتم هش این پروتکل یک رشته تصادفی از کاراکترها را به آن اضافه می کند. حتی اگر دو کاربر رمز عبور یکسانی را انتخاب کنند، هش رمز عبور همچنان متفاوت خواهد بود.

با هش های از پیش محاسبه شده رمزهای عبور استاندارد و جدول رنگین کمان، اگر پیچیدگی و طول رمز عبور به اندازه کافی انتخاب نشده باشد، می توان حملات brute-force قابل اجرا را انجام داد (نکته: بیش از ۱۵ کاراکتر).

- عدم پشتیبانی از احراز هویت چند عاملی

پروتکل احراز هویت NTLM از احراز هویت چند عاملی (MFA) پشتیبانی نمی کند، بنابراین برای بازیابی هش رمز عبور کافی است. عامل دوم مانند برنامه احراز هویت ، رمز OTP سخت افزاری یا پیامک معمولاً استفاده نمی شود.

- حمله رلهNTLM
- احراز هویت NTLM در برابر حملات رله نیز NTLM آسیب پذیر است.

کلاینت اساساً راهی برای تأیید هویت سرور ندارد. بنابراین، مهاجمان می توانند خود را بین مشتری و سرور قرار دهد و از روش مردی در میانه استفاده کند.

- احراز هویت NTLM مرحله به مرحله

در پروتکلNTLM ، تمام حروف کوچک موجود در یک رشته رمز عبور قبل از ایجاد مقدار هش به حروف بزرگ تبدیل می‌شوند که پیچیدگی احتمالی رمز عبور را محدود می‌کند. در نتیجه، ۲/۵ ساعت طول می‌کشد تا یک رمز عبور ۸ کاراکتری با مقدار هش شناخته شده) از سال ۲۰۱۹، ایستگاه کاری با ۸ xGPUو (HashCat کشف شود.

همچنین، NTLM v1از یک عدد تصادفی ۱۶ بایتی برای چالش استفاده می کند که در عمل چندان تصادفی نیست.

از طرف دیگر، در NTLM v2 یک چالش با طول متغیر است که بسیار قوی تر است. همچنین، مرحله رمزگذاری در NTLMv2یک برچسب زمانی اضافه می کند.

هر دو NTLMv1 و NTLMv2 از تابع هش MD4 استفاده می کنند که منسوخ تلقی می شود.

چرا هنوز از احراز هویت NTLM استفاده می شود؟

مایکروسافت قبلاً NTLM را با Kerberos به عنوان پروتکل احراز هویت استاندارد در ویندوز ۲۰۰۰ جایگزین کرده است. با این حال، احراز هویت NTLM همچنان توسط ویندوز برای سازگاری با گذشته پشتیبانی می شود. هنوز نرم افزارهای قدیمی زیادی وجود دارند که از NTLMv2 یا حتی NTLMv1 استفاده می کنند.

بسیاری از برنامه های کاربردی در اواخر دهه ۱۹۹۰ و اوایل دهه ۲۰۰۰ توسعه یافتند. اغلب این برنامه ها دیگر توسط سازنده پشتیبانی نمی شوند یا مستقیماً برای یک شرکت به عنوان یک برنامه خاص طراحی شده اند. به همین علت هنوز هم در بعضی جاها نیاز به استفاده از این پروتکل وجود دارد.

تفاوت بین Kerberos وNTLM

یکی از مهم ترین تفاوت های بین NTLM و Kerberos یک فرآیند احراز هویت اصلاح شده است.

در پروتکل Kerberos خود فرآیند احراز هویت دیگر به عنوان یک چالش/پاسخ دو مرحله ای اجرا نمی شود ، بلکه به صورت سه مرحله ای طراحی شده است.

به همین ترتیب، Kerberosدارای ویژگی های رمزنگاری متفاوتی نسبت به NTLM است. تابع هشی که NTLM برای ایجاد هش رمز عبور استفاده می کند با یک تابع رمزگذاری درKerberos جایگزین شده است.

به طور خلاصه، Kerberosپروتکل به وضوح ایمن تری است. اما حتی Kerberos نیز کاملاً عاری از مشکلات امنیتی نیست.

غیرفعال کردنNTLM

به عنوان یک استراتژی، برای غیر فعال کردن پروتکل NTLM بهتر است که اول چند نکته را مشخص کنید اول مشخص کنید که کدام برنامه ها هنوز به پروتکل NTLM نیاز دارند. در گروپ پالسی از طریق پالسی موجود در قسمت Network security: Restrict NTLM: Audit NTLM authentication in this domainرا می توان به راحتی بدون ایجاد مزاحمت در عملکرد فعال کرد. همچنین می توان از ابزارهای اضافی برای یافتن نسخه پروتکل استفاده کرد.

Hardening Clients:با این اطلاعات می توان بررسی کرد که آیا برنامه های مورد نظر را می توان برای استفاده انحصاری از یک پروتکل قوی تر NTLMv2) یا بهینه (Kerberos پیکربندی کرد. به روز رسانی ها باید بررسی و بر این اساس اولویت بندی شوند.

Hardening Server:در صورت امکان، NTLMv1وNTLMv2 باید از طریق گروپ پالیسی کاملاً غیرفعال شوند. اگر برنامه‌ها را نمی‌توان به‌روزرسانی کرد و همچنان باید به NTLM نیاز باشد، می‌توان فهرست استثنایی تنظیم کرد.آیا هنوز هم می توان از NTLM با خیال راحت استفاده کرد؟

استفاده از NTLM باید در شبکه به حداقل برسد یا به طور کامل غیرفعال شود. شرکت هایی که به دلایل سازگاری باید به استفاده اجباری از NTLM ادامه دهند، باید نکات زیر را در نظر بگیرند.

امضای :SMB برای جلوگیری از حمله مهاجمان از راه‌اندازی حملات رله NTLM ساده‌تر، امضای SMB باید در همه رایانه‌های موجود در شبکه فعال شود.

:Block NTLMv1از آنجایی که NTLMv1 کاملاً ناامن است. باید از طریق انجام تنظیمات گروپ پالیسی مناسب به طور کامل مسدود شود.

امضای . :LDAP/S برای جلوگیری از رله NTLM درLDAP ، امضای LDAP و اتصال کانال LDAPS باید در دامین کنترلرها فعال باشد.

حفاظت پیشرفته برای احراز هویت . :(EPA) برای جلوگیری از رله NTLM در سرورهای وب، همه سرورهای وبOWA) ، (ADFSباید به گونه‌ای پیکربندی شوند که فقط درخواست‌های EPA را بپذیرند.

اصولاً اقدامات بعدی زیر نیز به شدت توصیه می شود.

بروزرسانی و نصب وصله های امنیتی به صورت مداوم و منظم برای کلیه سیستم هایIT

Defender Windows Credential Guardرا فعال کنید

حساب های دارای دسترسی ادمین را محدود کنید

عدم استفاده از پروتکل دسکتاپ از راه دور (RDP) برای مدیریت کلاینت ها

مدیریت از راه دور فقط از طریق Jump hosts یا سیستم هایی که برای ورود به سیستم از لحاظ امنیتی بهینه سازی شده اند.

در صورت لزوم: از Microsoft Local Administrator Password Solutions (LAPS) استفاده کنید.

ارتباط کاربران با یکدیگر را محدود کنید، به عنوان مثال از یک فایروال برای جلوگیری از ارتباطات جانبی استفاده کنید.