Disabling NTLM Authentication Guide – part 1 – Prerequisites

willssysadmintechblog.wordpress.com/2023/08/22/disabling-ntlm-authentication-guide-part-1

August 22, 2023

Part 2: Disabling NTLM Authentication Guide – part 2 – Logs

15 months ago one of our Information Security employees messaged me saying “we need to start our exit strategy on NTLM authentication”. They linked this article: https://www.malwarebytes.com/blog/news/2022/06/dfscoerce-a-new-ntlm-relay-attack-can-take-control-over-a-windows-domain

I hadn’t yet delved into the details of different authentication schemes used in Active Directory. I roughly knew how Kerberos worked but I didn’t really know how NTLM worked. I started researching and read about NTLM’s use of challenge response and relative simplicity compared to the more secure Kerberos. Unfortunately, NTLM hashes are relatively quick to crack (compared to other hashing schemes) and computers may leave these hashes in LSASS memory for longer than they’re needed. I have seen demonstrations of hacking tools that intercept these passed NTLM hashes. Once they have them, they can try to crack them to get the plaintext password, or try to use them in a replay attack. Kerberos isn’t as vulnerable to attacks like this, assuming you’re using AES ticket encryption. Tickets also aren’t as easy to re-use somewhere else, and may not be possible depending on the type of ticket you’ve received and the Kerberos settings in the realm. If a TGT is stolen, it’s only valid for a certain period of time, and a TGT doesn’t give attackers a route to cracking your password.

I have a friend who is as penetration tester at a well known cyber security company. During the inception of this project to disable NTLM authentication I asked him how often he abuses NTLM in his work engagements. He said, “All the time. We abuse NTLM in some way on almost every engagement.”

Because of all this and *much* more, security researchers and Microsoft developers are advocating for the elimination of NTLM in favor of other schemes, like Kerberos. The last couple years have shown me that when Microsoft starts trying to get rid of something you should take notice. When they release a patch schedule and say “on this date this feature will be forcible set and you cannot revert it”, you should act! It’s better to get ahead of Microsoft and have your ducks in a row before they steal your ducks and destroy your beautiful duck farm. As far as I know, Microsoft hasn’t set a date where NTLM will be gone, and I’m not sure they ever will be able to, but I believe they will take steps to limit its use in the next couple years.

If you want to read a good simple-enough article about why you should eliminate NTLM: https://blog.quest.com/ntlm-authentication-what-it-is-and-why-you-should-avoid-using-it/

This is a tall order, though. My organization explored this a couple years ago and quickly backed off, because printers would be a nightmare… or so we thought. Fast forward to today, 15 months after the message that started the project, and we successfully have NTLM authentication disabled in our environment, except for a few servers where there are no other options. The next posts in this guide series will give you the technical details on how to audit the use of NTLM and strategies for how to work with other IT staff. This post will start with your pre-requisites to make your life easier.

Pre-Requisites

Leadership Backing

Your IT leadership needs to be behind the project to disable NTLM. You're going to need to compel admins to make changes to their systems, spend time working with vendors, and potential break their services while testing. This project is going to take a long time if you're an org of any decent size. The other IT admins need to be roped in for the long haul. Participation in this project cannot be voluntary in order to make any meaningful strides and avoid huge headaches later on.

Privacy Settings
Once the project is nearing completion, IT leadership needs to be willing to set firm dates on when NTLM authentication will be disabled for your entire domain. Some admins (for various and sometimes legitimate reasons) may wait until the last minute to start work on this project. You need the authority to enforce the deadline leadership set and only give a small amount of leeway and free passes to ensure the project keeps moving.

Our IT security office was the driving force behind supporting this project to our IT leadership team. I am very thankful for their backing.

Logs

Logs are absolutely essential to finding out what systems are relying on NTLM authentication. Log aggregation is the key that really makes this job easier. I heavily utilized a log aggregation system we have where domain controller and server logs are sent to centralized log collecting servers. These logs are then ingested and sorted by OpenSearch, a fork of the ELK stack.

You wouldn't *need* centralized logging for this project, but you will at the very least need historical and near real-time access to domain controller logs and a way to sort and parse them for specific events. You're looking for NTLM audit logs and Kerberos Security logs for authentication.

Good Communication Skills

Good communication skills are necessary to get admins motivated to work on this massive project and to give them the information they need. This project delves into issues they have likely never thought about before, or have thought about only in the sense of “what’s the fastest way I can get this crappy vendor app to work”. You need to communicate effectively:

- The problem with NTLM authentication
- Participation in this project is not optional
- What they can do to help the project move along
- How you will be of assistance

A Helping Attitude and Expertise

Some of your admins will be stretched and maybe stressed by this project. They’ll have multiple systems they need to try to get off NTLM authentication. Some of these systems are “mission critical and cannot go down”, are pieces of junk from a company that shouldn’t be releases enterprise software, or are black boxes that nobody knows much about. You *need* to make it clear to admins that you’re there to help them. They won’t know what to do most of the time, they won’t know where to look. These problems are new to them. You need to guide them on where to look at what to ask their vendor. You need to tell them what to test and how to test it.

Start by reading up on the differences between NTLM authentication and Kerberos, and really read a lot on how Kerberos works, it’ll come in handy. Admins will ask for your help with “Kerberizing” their services and you’ll need to know some stuff.

- https://www.ibm.com/docs/en/sc-and-ds/8.2.1?topic=concepts-kerberos-ticket
- https://syfuhs.net/a-bit-about-kerberos
- Service Princpal Names. This looks like a decent article: https://profadmins.com/2018/04/05/service-principal-names/
- Google “Kerberos diagram” and look at pictures

When admins ask you for help, try your best to help them. You want this project to succeed, they want to be done with it. Make everybody’s day better by having a good attitude, being kind, and having the expertise to help them out. You won’t solve everything immediately, but your co-workers will feel respected and cared for if you help them with diligence and respect.

Part 1: Disabling NTLM Authentication Guide – part 1 – Prerequisites

Part 2: Disabling NTLM Authentication Guide – part 2 – Logs

Part 3: Disabling NTLM Authentication Guide – part 3 – Migrating to Kerberos

Part 4: Disabling NTLM Authentication Guide – part 4 – NTLM Restrictions and Testing

Part 5: Disabling NTLM Authentication Guide – part 5 – Printers and Scanners

Part 6: Disabling NTLM Authentication Guide – part 6 – RDP

Part 7: Disabling NTLM Authentication Guide – part 7 – Kerberos Logs