Disabling NTLM Authentication Guide – part 5 – Printers and Scanners

willssysadmintechblog.wordpress.com/2023/09/05/disabling-ntlm-authentication-guide-part-5-printer-servers-and-scanners

September 5, 2023

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

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

So far I've laid out the general requirements for doing Kerberos authentication and collecting logs to give your IT admins the intelligence required to disable NTLM in your environment. "But Will, this won't work in my environment. There are MILLIONS of NTLM audit logs coming from my print server. Printers are always behind the times, there's no way we can migrate our print server to Kerberos authentication." While it is true that printers and scanners often hold back IT, there are ways around this.

Print Servers

Windows print servers do indeed generate a lot of NTLM audit logs, indicating NTLM is being used to connect clients to their printers. Print servers were the reason our IT team didn't first pursue disabling NTLM a few years ago. When you looked at the logs, there were indeed millions of NTLM authentication attempts received by our print servers every week. The team involved at the time thought this would be too big of a hurdle.

I started my NTLM testing by disabling NTLM authentication on a print server. I configured the Local Security policy setting *Network security: Restrict NTLM: Incoming NTLM traffic* to tell a print server to refuse incoming NTLM. To my pleasant surprise, mapping printers on a Windows server still worked. When my client connects to a print server, it's not actually communicating with the printer. It's communicating with the print server, which handles how to communicate with the printer. Once NTLM was disabled on print servers the vast majority of NTLM authentication attempts vanished.

I believe print servers are a case where either the client or server simply prefers to use NTLM. Once we disabled NTLM the print server switched to Kerberos seamlessly. Clients should use the most secure method available (Kerberos) but I guess that Microsoft dev team had other ideas.

Scan-To-Folder

Scan-To-Folder (STF) is another case of scanners and MFPs getting in the way, right? STF is a feature where a scanner (or MFP with a scanner) scans a document and writes the generated file to a network location. We observed scanners doing this regularly in our environment. Unfortunately, this isn't a case where you can simply disable NTLM and hope everything works OK. Most scanners do not know how to do Kerberos authentication and just assume NTLM will be available.

One option: designate one server to be the STF server. All scanners write to a network share somewhere on this server. The server isn't used for anything else. This server has an NTLM exception in place to continue using NTLM authentication after it's been disabled everywhere else. For credentials to this server, you could use one or many accounts (AD account, or even a local account on the server I guess) that can have credentials entered on the scanners, and have permission to write to the STF file shares. This account shouldn't be used for any other purpose (or have access to anything else) to mitigate the consequences of credential theft (the point of disabling NTLM). Also, if you have these credential saved on a scanner, you should not consider them very secure.

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