# NTLMv1 or NTLMv2? Does it even matter?

calcomsoftware.com/ntlmv1-or-ntlmv2-does-it-even-matter

May 1, 2023

NTLM authentication is a legacy protocol used to authenticate users and computers in Windows-based networks. Despite the availability of newer and more secure protocols, NTLM is still widely used and required for deploying Active Directory, a crucial component of Windows-based networks. This is because NTLM is deeply ingrained in the Windows architecture, making it difficult to disable or restrict NTLM without causing damage to production systems.

Moving away from NTLM authentication and complying with the CIS benchmarks is challenging as it requires identifying which computers are using it and migrating to a more secure protocol without breaking anything. Many organizations continue to use NTLM as a fallback mechanism, despite the availability of more secure protocols like Kerberos and OAuth. However, using newer protocols is recommended as they offer stronger security and better protection against certain types of attacks.

NTLM has two versions – NTLMv1 and NTLMv2. NTLMv2 suppose to offer better security than its previous version, and to some extent it does provides better defense against relay and brute force attacks, but does not completely block them. Our main conclusion is that the best way to protect your organization from NTLM vulnerabilities is in fact, not to use it! For a complete overview of NTLM vulnerabilities- continue your reading here.

### This blog post will cover:

### NTLM Authentication Server – Client Authentication Process:

In a Windows-based network, the domain controller plays a critical role in managing the challenge/response exchange in the NTLMv1 authentication protocol. This involves generating a challenge to the client and validating the user's credentials by comparing the hashed password provided by the client with the stored hash value for the user's account. If the two values match, the user is considered authenticated and granted access to the requested resource.

The NTLM authentication flow is as follows:

1. The client machine sends a request to connect to the server.>
2. The server generates a random nonce to be encrypted by the client.
3. The client machine encrypts the nonce with the password hash to prove knowledge of the password.
4. The server validates the user's identity by ensuring that the challenge was indeed created with the correct user/password. It does this either by using data from its own SAM database or by forwarding challenge-response pairs for validation in the domain controller.

### How NTLMv2 is Different From NTLMv1:

NTLM v2 also uses this flow with a slight change. In NTLMv2, the client includes a timestamp, and a username together with the nonce in step 3 above. This helps mitigate offline relay attacks, but leaves NTLMv2 exposed to other NTLMv1 vulnerabilities, and therefore does not provide a satisfactory solution.

In addition, while NTLMv1 is using a 16-byte random number challenge, NTLMv2 provides a variable-length challenge.

Because it is so commonly used, it is important to be familiar with all of the NTLM vulnerabilities.

## Security Issues in NTLMv1 protocol and how NTLMv2 addresses them:

### Weak cryptography:

The NTLM cryptography scheme is relatively weak, making it relatively easy to crack hashes and derive plaintext passwords. It's easy enough for standard hardware to be able to crack an 8-character password in less than a day. This is for three main reasons:

1. The password hash is based on MD4, which is relatively weak.
2. The hash is saved unsalted in a machine's memory before it is salted and sent over the wire.
3. A user must respond to a challenge from the target, which exposes the password to offline cracking. This prevents offline Relay attacks.

## No mutual NTLM authentication:

This flaw exposes the protocol to a man-in-the-middle (MITM) attack. When a client communicates with a server, it does not validate the server's identity (this is known as *one-way authentication*). A malicious actor with MITM capabilities can send malicious data to the client while impersonating the server.

***The most severe security risk associated with NTLM is the exposure of servers in Active Directory environments to NTLM relay and remote code execution attacks. Other NTLM flaws are considered minor, compared to this critical vulnerability***

In this attack, the attacker hijacks the client-server connection and spreads laterally to the entire system using the user's credentials. While Microsoft have tried to develop mitigation techniques for this issue, all of those mitigation patches have been hacked. No NTLM version provides a solution for this issue, which means that all NTLM users (which is most likely almost all of you that have continued reading up until here) are at great risk for a devastating attack.

## MITRE ATT&CK reference to NTLM authentication vulnerabilities

The MITRE ATT&CK framework add more relevant information to this known vulnerabilities by connecting these vulnerable flows and procedures to real life attack campaigns. As stated by MITRE ATT&CK, a PTH- Pass the hash attack can be formed by capturing and manipulating NTLMv1/v2 login processes:

From a classic Pass-The-Hash perspective, this technique uses a hash through the NTLMv1 / NTLMv2 protocol to authenticate against a compromised endpoint. This technique does not touch Kerberos. Therefore, NTLM LogonType 3 authentications that are not associated to a domain login and are not anonymous logins are suspicious. From an Over-Pass-The-Hash perspective, an adversary wants to exchange the hash for a Kerberos authentication ticket (TGT). One way to do this is by creating a sacrificial logon session with dummy credentials (LogonType 9) and then inject the hash into that session which triggers the Kerberos authentication process.

If it is not possible to disable NTLM in an infrastructure it is critical to monitor NTLM activity and configure it for optimal security and audit

## How can you stop using NTLM authentication:

CalCom's Hardening Suite (CHS) offers a solution to the challenges associated with abandoning NTLM. CHS learns your system and identifies servers that can continue to function without outages after disabling NTLM. It provides alerts on potential impacts and allows you to make informed decisions based on its findings. CHS automatically implements it on the entire production environment, reducing the risk of configuration drift. Learn more about it here.

https://blog.preempt.com/the-security-risks-of-ntlm-proceed-with-caution

https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4