NTLM Basics

Windows Technology LAN Manager (NTLM) is a suite of security protocols offered by Microsoft to authenticate users' identity and protect the integrity and confidentiality of their activity. At its core, NTLM is a single sign on (SSO) tool that relies on a challenge-response protocol to confirm the user without requiring them to submit a password.

Despite known vulnerabilities, NTLM remains widely deployed even on new systems in order to maintain compatibility with legacy clients and servers. While NTLM is still supported by Microsoft, it has been replaced by Kerberos as the default authentication protocol in Windows 2000 and subsequent Active Directory (AD) domains.

How Does the NTLM Protocol Work?

NTLM authenticates users through a challenge-response mechanism. This process consists of three messages:

Negotiation message from the client

Challenge message from the server

Authentication message from the client

NTLM Authentication Process

NTLM authentication typically follows the following step-by-step process:

1. The user shares their username, password and domain name with the client.
2. The client develops a scrambled version of the password — or hash — and deletes the full password.
3. The client passes a plain text version of the username to the relevant server.
4. The server replies to the client with a challenge, which is a 16-byte random number.
5. In response, the client sends the challenge encrypted by the hash of the user's password.
6. The server then sends the challenge, response and username to the domain controller (DC).
7. The DC retrieves the user's password from the database and uses it to encrypt the challenge.
8. The DC then compares the encrypted challenge and client response. If these two pieces match, then the user is authenticated and access is granted.

The Difference Between NTLM and Kerberos?

Like NTLM, Kerberos is an authentication protocol. It replaced NTLM as the default/standard authentication tool on Windows 2000 and later releases.

The main difference between NTLM and Kerberos is in how the two protocols manage authentication. NTLM relies on a three-way handshake between the client and server to authenticate a user. Kerberos uses a two-part process that leverages a ticket granting service or key distribution center.

Another main difference is whether passwords are hashed or encrypted. NTLM relies on password hashing, which is a one-way function that produces a string of text based on an input file; Kerberos leverages encryption, which is a two-way function that scrambles and unlocks information using an encryption key and decryption key respectively.

Even though the Kerberos protocol is Microsoft's default authentication method today, NTLM serves as a backup. If Kerberos fails to authenticate the user, the system will attempt to use NTLM instead.

Why Was NTLM Replaced by Kerberos?

NTLM was subject to several known security vulnerabilities related to password hashing and salting.

In NTLM, passwords stored on the server and domain controller are not "salted" — meaning that a random string of characters is not added to the hashed password to further protect it from cracking techniques. This means that adversaries who possess a password hash do not need the underlying password to authenticate a session. As a result, systems were vulnerable to brute force attacks, which is when an attacker attempts to crack a password through multiple log-in attempts. If the user selects a weak or common password, they are especially susceptible to such tactics.

NTLM's cryptography also fails to take advantage of new advances in algorithms and encryption that significantly enhance security capabilities.

Kerberos Protocol

Kerberos was developed by researchers at the Massachusetts Institute of Technology (MIT) in the 1980s. The name is derived from the Greek mythological character Kerberos, the three-headed dog who guards the underworld.

In practice, the three security components in the Kerberos protocol are represented as:

- A client seeking authentication
- A server the client wants to access
- The ticketing service or key distribution center (KDC)

Kerberos Authentication

Here is the 12 step process for Kerberos authentication:

1. The user shares their username, password, and domain name with the client.
2. The client assembles a package — or an authenticator — which contains all relevant information about the client, including the user name, date and time. All information contained in the authenticator, aside from the user name, is encrypted with the user's password.
3. The client sends the encrypted authenticator to the KDC.
4. The KDC checks the user name to establish the identity of the client. The KDC then checks the AD database for the user's password. It then attempts to decrypt the authenticator with the password. If the KDC is able to decrypt the authenticator, the identity of the client is verified.
5. Once the identity of the client is verified, the KDC creates a ticket or session key, which is also encrypted and sent to the client.

6. The ticket or session key is stored in the client's Kerberos tray; the ticket can be used to access the server for a set time period, which is typically 8 hours.
7. If the client needs to access another server, it sends the original ticket to the KDC along with a request to access the new resource.
8. The KDC decrypts the ticket with its key. (The client does not need to authenticate the user because the KDC can use the ticket to verify that the user's identity has been confirmed previously).
9. The KDC generates an updated ticket or session key for the client to access the new shared resource. This ticket is also encrypted by the server's key. The KDC then sends this ticket to the client.
10. The client saves this new session key in its Kerberos tray, and sends a copy to the server.
11. The server uses its own password to decrypt the ticket.
12. If the server successfully decrypts the session key, then the ticket is legitimate. The server will then open the ticket and review the access control list (ACL) to determine if the client has the necessary permission to access the resource.

NTLM Benefits and Challenges

NTLM is considered an outdated protocol. As such, its benefits — when compared to a more modern solution, such as Kerberos — are limited. Yet the original promise of NTLM remains true: Clients use password hashing to avoid sending unprotected passwords over the network.

At this point there are several clear disadvantages to relying on NTLM authentication:

- Single authentication. NTLM is a single authentication method. It relies on a challenge-response protocol to establish the user. It does not support multifactor authentication (MFA), which is the process of using two or more pieces of information to confirm the identity of the user.
- Security vulnerabilities. The relatively simplistic form of password hashing makes NTLM systems vulnerable to several modes of attacks, including pass-the-hash and brute-force attacks.
- Outdated cryptography. NTLM does not leverage the latest advances in algorithmic thinking or encryption to make passwords more secure.