# NTLM v1 and NTLM v2 vs Kerberos

calcomsoftware.com/ntlm-v1-and-v2-vs-kerberos

February 8, 2024

## What is NTLMv1?

NTLMv1 (NT LAN Manager version 1) is a Microsoft authentication protocol used primarily for network authentication on Windows-based systems. It is a challenge-response authentication protocol, where the server sends a challenge to the client, which is then encrypted using the client's password hash and sent back to the server for authentication.

NTLM v1, NTLM v2, and Kerberos are authentication protocols used to enhance security in Active Directory environments. However, they are also popular attack vectors, allowing attackers to gain access and elevate privileges. It's crucial to choose the most secure protocol for your environment and configure it properly to mitigate these risks.

NTLMv1 is the oldest among the three authentication protocols, while NTLMv2 offers incremental security enhancements. However, Kerberos authentication is notably more advanced and provides greater security compared to both NTLMv1 and NTLMv2.

## NTLMv1 Authentication

NTLM was developed by Microsoft. It supports both new and old Windows versions (Windows 95, Windows 98, Windows 2000, Windows XP, Windows Server 2003, Windows 7, and Windows Server 2008, Windows ME, N.T 4.0).

Critical elements within the realm of authentication and security protocols for the NTLM version include the default authentication protocol, authentication levels, authenticate message, authentication method, rainbow table, server challenge, clients, and servers, as well as brute force attacks.

In the world of authentication and security for NTLM, important factors include the default authentication method, different levels of authentication, the authentication message, how authentication is carried out, the risk of rainbow table attacks, server challenges, the involvement of both clients and servers, and the threat of brute force attacks.

NTLM authentication is structured as a challenge and response mechanism:

1. A user signs in to a client computer with a domain name, user name, and password.

2. The client computer creates a cryptographic hash (either NT or KM hash) of the password.
3. The client computer sends the targeted server the user name in plain text.
4. The targeted server generates a 16-byte random number and sends it to the client computer – the challenge.
5. The client computer responds and sends the challenge with the hash of the user's password – the response.
6. The server sends to the Domain Controller (DC) the user name, the challenge, and the response.
7. The DC gets the user password's hash from the Security Account Manager by using the user name.
8. The DC encrypts the challenge.
9. The DC compares the challenge it encrypted and the client's encrypted response. If they are identical, then the authentication is approved.

NTLMv1 authentication is vulnerable to quick cracking due to its fixed hash length. The challenge-response mechanism also exposes passwords to offline cracking. Avoid using NTLMv1 whenever possible for enhanced security.

## NTLMv2 Authentication

NTLM v2 also uses the same flow as NTLMv1 but has 2 changes:1. The client includes a timestamp when it sends the user name to the client (stage 3). 2. The targeted server generates a variable-length challenge (instead of a 16-byte challenge). These changes help mitigating relay attacks. And yet, NTLMv2 is still exposed to other NTLMv1 vulnerabilities since it is still using the same authentication mechanism.

NTLM's challenge-response mechanism only allows one-way authentication - the client in front of the server. This decreases NTLM security since the client can unintendingly authenticate in front of a bogus server.

## Kerberos Authentication

Kerberos protocol is open-source software. It supports newer Windows versions (Windows 2000, Windows XP, and later).

The authentication process in Kerberos is more complex than in NTLM. Kerberos supports two-factor authentication and uses mutual authentication. It uses tickets and a token to verify the client. In addition, it uses three different keys to make it harder for attackers to breach this protocol.

This is how Kerberos authentication process works:

1.The client verifies himself in front of the Key Distribution Center (KDC).

2. The client connects with the Authentication Server:

a. The client connects with an Authentication Server (AS). He uses its User ID to request a ticket. The client uses it's password's secret key to encrypt the request.

b. The AS uses the client's password to decrypt the request and verify the client.

c. The AS sends the client a Ticket Granting Ticket (TGT). The AS uses a different secret key to encrypt the TGT.

3. The client requests a token from the TGS:

a. The client sends the TGT and a request to connect the targeted server to a Ticket Granting Server (TGS).

b. The TGS shares the TGT with the AS to verify it.

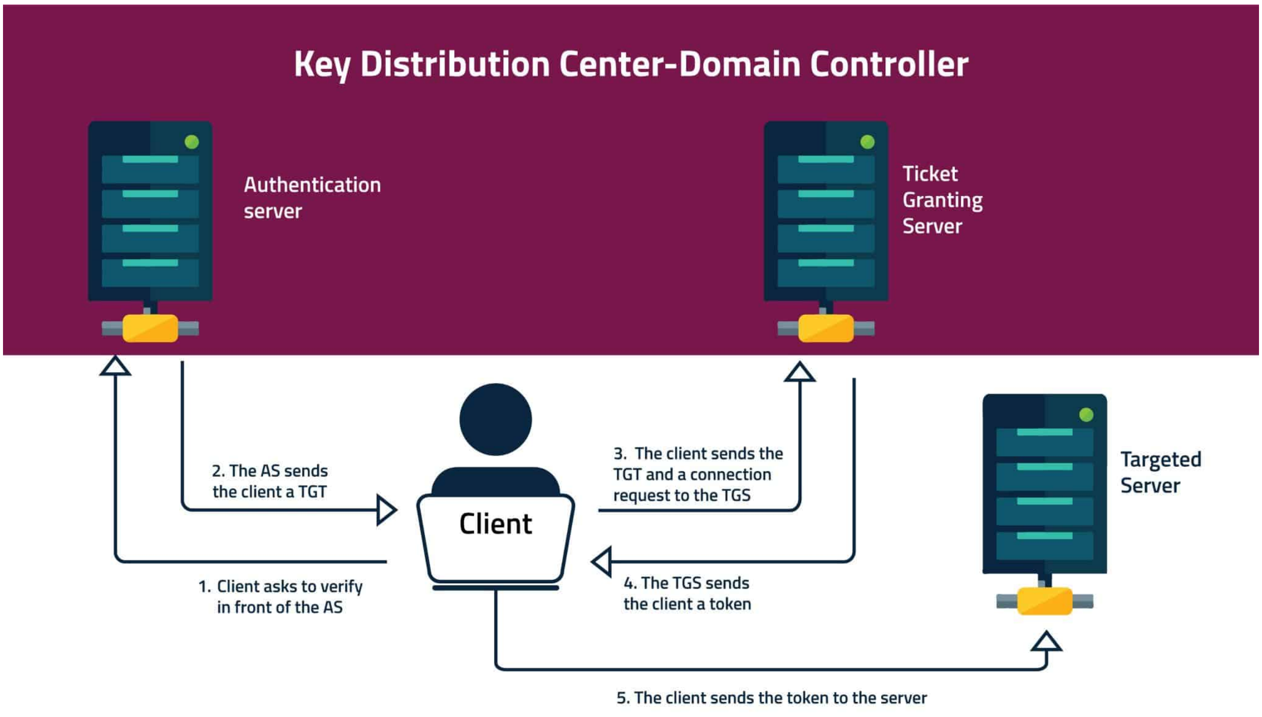
c. The TGS issues an encrypted token for the client. The TGS shares with the targeted server the token's key.

4. The client connects with the targeted server:

a. The client sends the token to the targeted server.

b. The server decrypts the token using the key he got from the TGS.

c. The client can use the server for the time set in the token.


Key Distribution Center-Domain Controller
Authentication server
Ticket Granting Server
Targeted Server
Client
1. Client asks to verify in front of the AS
2. The AS sends the client a TGT
3. The client sends the TGT and a connection request to the TGS
4. The TGS sends the client a token
5. The client sends the token to the server

The Kerberos authentication process uses three different secret keys. 1. The first key between the client and the AS is based on the client's password. 2. The AS and the TGS share another secret key. 3. The TGS and the targeted server.

Kerberos supports mutual authentication. This means that not only the client authenticates to the server, the server also authenticates to the client. The client can choose to use this feature.

Kerberos enables authentication delegation, allowing a server to access remote resources on behalf of a client. This means users can authenticate to a server via an intermediary machine, with the targeted server making approval decisions based on the user's identity rather than the intermediary machine's. This feature is useful in multi-tier applications, such as using a web server to authorize user access to a database.

### Kerberos PKINIT extension:

Kerberos PKINIT extension supports smart card logon security feature. Smart card logon allows two-factor authentication. That dramatically elevates Kerberos's security and can block attacks such as Trojan Horse Attacks.

## NTLMv1 vs NTLMv2 vs Kerberos

| | **NTLMv1** | **NTLMv2** | **Kerberos** |
|---|---|---|---|
| Security | Bad | Better | Best- no password is stored or sent over the network |
| Performance | Slower authentication | Slower authentication | Faster authentication |
| Delegation Support | Support just impersonation | Support just impersonation | Supports impersonation and delegation of authentication |
| Multi-Factor Authentication - Smart Cards | Does not support | Does not support | Support |
| Cryptography | Symmetric cryptography | Symmetric cryptography | Supports both symmetric and asymmetric cryptography |
| Trusted third party | DC | DC | DC, KDC (and Windows Enterprise Certification Authority in Kerberos PKINIT). |
| Mutual authentication | Does not support | Does not support | Support |

## NTLM vulnerabilities

NTLM  suffers from various vulnerabilities, particularly in its earlier versions like NTLMv1. These vulnerabilities include susceptibility to pass-the-hash and pass-the-ticket attacks, replay attacks, weak hashing algorithms, man-in-the-middle attacks, downgrade attacks, and credential theft. These weaknesses can lead to unauthorized access, credential theft, and compromise of network security.

To mitigate these risks, it’s essential to use more secure authentication mechanisms like Kerberos or newer versions of NTLM (such as NTLMv2) where possible, along with implementing additional security measures such as network segmentation, encryption, and strong password policies.

## Kerberos vulnerabilities

In Microsoft’s September 2022 Patch Tuesday, two elevation of privilege vulnerabilities were identified in Kerberos. These vulnerabilities, discovered by Google Project Zero, pose a high risk. They exploit a weakness in Kerberos that allows for the forced downgrading of encryption from the more secure AES to the outdated MD4-RC4. One of these vulnerabilities, known as CVE-2022-33679, specifically targets the encryption of Kerberos session keys, taking advantage of Kerberos’ utilization of the obsolete RC4-MD4 encryption type.

## Why NTLM is still in use

The obvious question is why NTLMv1 and NTLMv2 are still in use if there's a safer alternative? The answer is that neglecting NTLM is more complex than it sounds. This process holds challenges such as:

* Using applications that do not support Kerberos

* Mapping where NTLM is being used

* Checking the impact of disabling NTLM.

### Here are a few examples of when you’ll use NTLM:

1. Kerberos does not work when you use a load balancer for web traffic (requires special configuration).
2. Kerberos won’t work if the SPN presented by the client does not exist in the AD. For example, when trying to access a resource using an IP instead of a name.
3. When you need to work both with external (non-domain) and internal clients.
4. When you need to work both with domain accounts and local user accounts on the IIS box.

5. When you have no SPN registered.
6. When the client doesn’t have DNS or DC connectivity.
7. When the client’s proxy setting or Local Internet Zone is not used for the targeted site.

Detecting these scenarios can be a pain. For this reason, we highly recommend using automation for this process. Tools such as CalCom Hardening Suite (CHS) automates server hardening. CHS will report where NTLM is being used and where you can disable NTLM and use only Kerberos without causing any damage. It will also enforce your policy to the production environment, to make sure everything is configured correctly. Finally, it will monitor and fix any configuration drifts to make sure you remain compliant and secure.

## Kerberos security updates

November 8, 2022 Microsoft Windows released security updates for  Kerberos protocol changes related to CVE-2022-37967 that address security bypass and elevation of privilege vulnerabilities with Privilege Attribute Certificate (PAC) signatures. The security update addresses Kerberos vulnerabilities where an attacker could digitally alter PAC signatures, raising their privileges.

NIST’s National Vulnerability Database (NVD) base score which reflects the severity of the CVE-2022-37967 vulnerability is 7.2 and considered High.

Hardening Windows Kerberos for domain controllers is recommended. With the release update on April 11, 2023, the third deployment phase for addressing CVE-2022-37967 will commence. This phase focuses on implementing security hardening changes on Domain Controllers within IT environments. These changes are necessary to mitigate the vulnerability and enhance the overall security posture of the affected systems.

## MITRE ATT&CK and authentication protocols

MITRE ATT&CK framework covers various tactics and techniques that can be employed to improve security and mitigate the risks associated with NTLM. A MITRE ATT&CK technique called "Pass the Hash" 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 linked to a domain login and are not anonymous logins raise suspicion. In order to safeguard against credential dumping, Microsoft advises disabling or limiting NTLM and WDigest authentication.

**MITRE ATT&CK techniques associated with Kerberos:**

> Kerberoasting (T1208): Adversaries attempt to extract Kerberos Ticket Granting Service (TGS) tickets to offline crack the password hashes and obtain plaintext passwords. This technique takes advantage of weak or easily guessable service account passwords.

Golden Ticket (T1550.002): Adversaries forge Kerberos Ticket Granting Tickets (TGTs) using a valid domain account's hash to gain unauthorized access and impersonate any user or create new users.

Silver Ticket (T1550.003): Adversaries create forged Kerberos service tickets (TGS) for specific services to access resources or authenticate as a particular user without needing their credentials.

Skeleton Key (T1550.004): Adversaries modify the Kerberos authentication process to implant a "skeleton key" password that allows them to authenticate as any user without their credentials.

Pass the Ticket (T1550.001): Adversaries obtain Kerberos ticket-granting tickets (TGTs) or service tickets (TGS) and use them to authenticate and move laterally across a network without needing to know the user's password.

Kerberos Pre-Authentication Bruteforce (T1110.004): Adversaries attempt to brute force Kerberos pre-authentication to guess the user's password and obtain a valid TGT.

**MITRE ATT&CK Mitigation Recommendations**

| ID | Mitigation | Description |
|---|---|---|
| M1015 | Active Directory Configuration | For containing the impact of a previously generated golden ticket, reset the built-in KRBTGT account password twice, which will invalidate any existing golden tickets that have been created with the KRBTGT hash and other Kerberos tickets derived from it. For each domain, change the KRBTGT account password once, force replication, and then change the password a second time. Consider rotating the KRBTGT account password every 180 days. |
| M1041 | Encrypt Sensitive Information | Enable AES Kerberos encryption (or another stronger encryption algorithm), rather than RC4, where possible. |
| M1027 | Password Policies | Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire.[10] Also consider using Group Managed Service Accounts or another third party product such as password vaulting. |
| M1026 | Privileged Account Management | Limit domain admin account permissions to domain controllers and limited servers. Delegate other admin functions to separate accounts.<br>Limit service accounts to minimal required privileges, including membership in privileged groups such as Domain Administrators |