# Introduction

Le protocole d’authentification NTLM ou « New Technology Lan Manager » a été créé en 1993 pour remplacer le protocole Lan Manager devenu trop vulnérable.

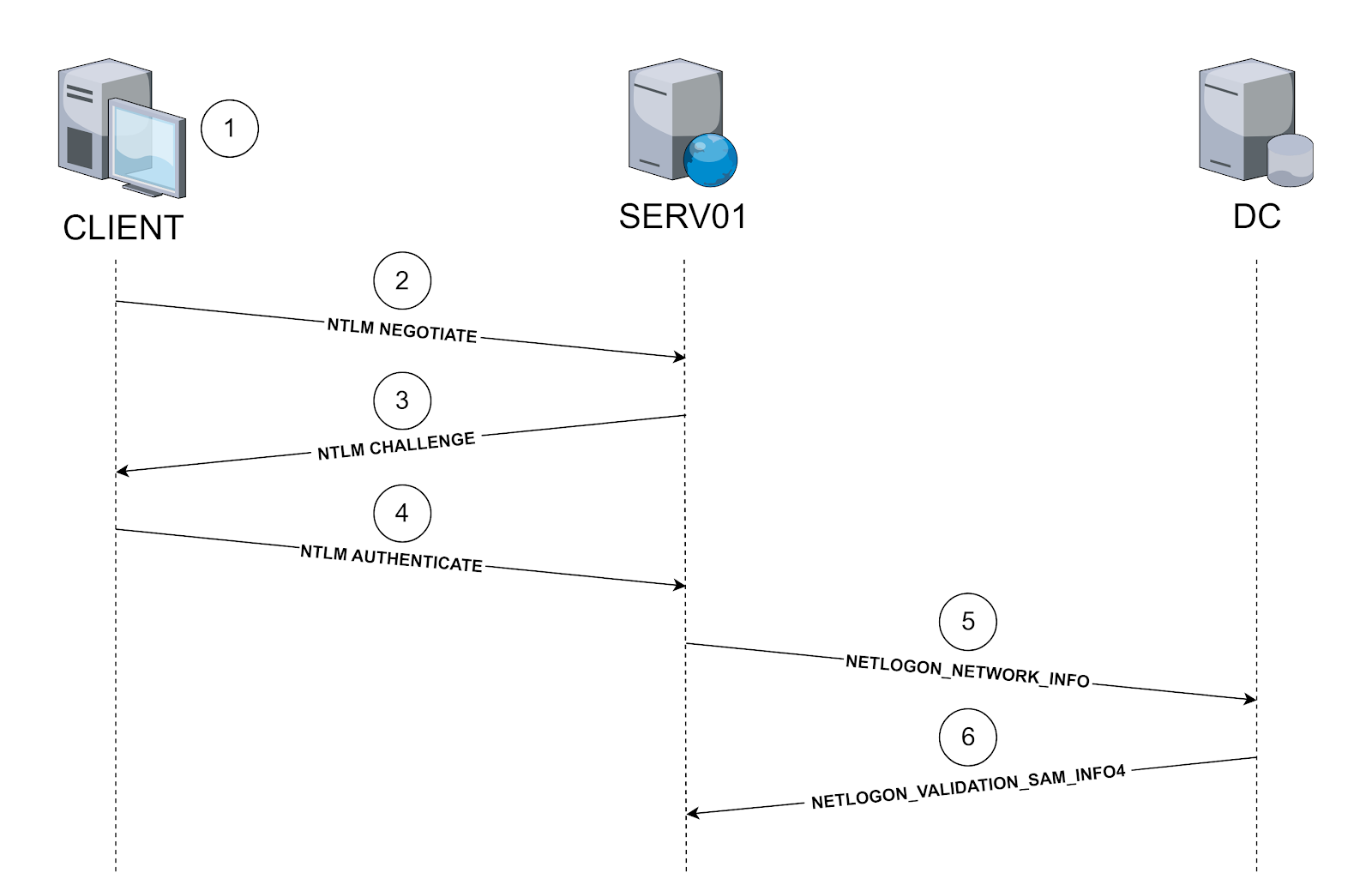
Fondamentalement, NTLM est un outil d’authentification unique (SSO) qui s’appuie sur un protocole de stimulation/réponse pour confirmer l’identité d’un utilisateur sans lui demander de saisir un mot de passe.

En dépit de vulnérabilités connues, NTLM reste largement déployé, même sur les nouveaux systèmes, afin d’assurer la compatibilité avec des clients et serveurs plus anciens. Si NTLM est toujours pris en charge par Microsoft, il a été remplacé par Kerberos comme protocole d’authentification par défaut dans Windows 2000 et les domaines Active Directory (AD) ultérieurs.

# Fonctionnement de NTLM

Le processus d’authentification NTLM se déroule généralement comme suit :

1. Un utilisateur s’authentifie avec ses identifiants sur sa machine (nom de domaine, d’utilisateur et mot de passe …).
2. La machine client envoie un message “Negociate” contenant, entre autres, le nom du domaine, les fonctions supportées par le client et le nom de la machine.
3. Le serveur cible génère alors un message “Challenge” composé notamment du “défi”, qui est un nombre aléatoire et l’envoie à l’ordinateur client.
4. La machine client répond par un message “Authenticate” et envoie, entre autres, la « réponse », qui est le challenge chiffré par le hash NT\* du mot de passe du client.
5. Le serveur envoie au Contrôleur de Domaine (DC)\* le nom d’utilisateur, le défi et la réponse via un message “NETLOGON\_NETWORK\_INFO”.
6. Le DC récupère le hash du mot de passe de l’utilisateur à partir de sa base de données puis chiffre le “défi” et le compare avec “la réponse”.



# Différences entre Net-NTLMv1 et Net-NTLMv2

Net-NTLMv1 et Net-NTLMv2 sont les deux versions du protocoles NTLM. Net-NTLMv2 a été lancé en 1998 avec la sortie de Windows NT 4.0 SP4, cette deuxième version de NTLM a été créée dans le but de remplacer Net-NTLMv1 afin d’améliorer la sécurité cryptographique du protocole.

La principale différence entre ces deux versions est l’algorithme utilisé pour chiffrer le challenge. Pour Net-NTLMv1, c’est DES qui est utilisé, à noter que cet algorithme n’est pas résistant aux attaques par brute force du fait notamment sa faible complexité et de la petite taille de la clé utilisé (56 bits). D’autre part, pour Net-NTLMv2 c’est HMAC-MD5 qui est utilisé. Bien que ce dernier soit plus résistant contre une attaque par brute force que DES, dû notamment au fait que la clé est plus grande (128 bits), cela reste tout à fait possible.

Ensuite, une deuxième différence est que Net-NTLMv2 peut implémenter un mécanisme d’intégrité qui se traduit par un champ MIC (Message Integrity Code).

Ce champ peut être présent dans le message “Authenticate” et est calculé avec la fonction HMAC-MD5 en prenant en entrée la clé de session (si présente) et les trois messages d’authentification (NEGOCIATE, CHALLENGE et AUTHENTICATE). Il permet de garantir qu’un attaquant n’a pas pu modifier le contenu des messages d’authentification.

Enfin, une troisième différence est que pour Net-NTLMv2, un timestamp est ajouté au message “Authenticate” pour empêcher les attaques par rejeu.