

Write-Up : Root-Me NTLM Authentication

1. Comprendre le Challenge

Objectif : Nous disposons d'une capture réseau (.pcap) liée à une authentification SMB suspecte. Notre mission est d'intercepter les échanges NTLM et de cracker le mot de passe de l'utilisateur.

Format du flag : RM{userPrincipalName:password}

Important : l'userPrincipalName (UPN) doit être écrit entièrement en **minuscules**.

2. Analyse avec Wireshark

Ouvrez le fichier .pcap et filtrez le trafic pour isoler le protocole d'authentification Microsoft.

Filtre Wireshark : ntlmssp

Le protocole NTLM fonctionne en 3 étapes (Handshake) :

- Negotiate** : Le client propose ses options.
- Challenge (Type 2)** : Le serveur envoie un défi aléatoire. (**C'est ici qu'on trouve une info vitale**).
- Authenticate (Type 3)** : Le client répond au défi avec son mot de passe chiffré. (**C'est ici qu'on trouve le reste**).

No.	Time	Source	Destination	Protocol	Length Info
15	0.005366928	192.168.122.1	192.168.122.100	SMB2	212 Session Setup Request, NTLMSSP_NEGOTIATE
16	0.005746314	192.168.122.100	192.168.122.1	SMB2	377 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
18	0.007193093	192.168.122.1	192.168.122.100	SMB2	235 Session Setup Request, NTLMSSP_AUTH, User: \
48	0.044143929	192.168.122.1	192.168.122.100	SMB2	212 Session Setup Request, NTLMSSP_NEGOTIATE
49	0.044404143	192.168.122.100	192.168.122.1	SMB2	377 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
51	0.046003578	192.168.122.1	192.168.122.100	SMB2	524 Session Setup Request, NTLMSSP_AUTH, User: catcorp.local\john.doe

3. Extraction des données critiques

Pour reconstituer le hash (NetNTLMv2), nous devons récupérer des informations dans deux paquets différents :

A. Dans le paquet "NTLM Server Challenge" (Type 2) Allez dans SMB2 > Session Setup Response > NTLM Secure Service Provider > NTLM Challenge Message.

- NTLM Server Challenge** : (Notez cette chaîne hexadécimale de 16 caractères).

B. Dans le paquet "NTLM Authenticate" (Type 3) Allez dans SMB2 > Session Setup Request > NTLM Secure Service Provider > NTLM Authenticate Message.

- Domain** : CATCORP.LOCAL
- User** : john.doe
- NTProofStr** : (Situé dans NTLMv2 Response).
- Response (Blob)** : (Tout le reste du champ NTLMv2 Response qui suit le NTProofStr).

```
    NTLM Message Type: NTLMSSP_AUTH (0x00000003)
    ▶ Lan Manager Response: 45ebfedcd9d1f0a981836e97caa6c0e975304c546c6f3432
    ▶ NTLM Response [...]: 5c336c6b69fd2fc7b64eb0bde310216201010000000000001a9790044b63da0175304c546c6f34320000000000200
    ▶ Domain name: catcorp.local
    ▶ User name: john.doe
    Host name: NULL
    Session Key: Local\John.DOE
```

4. Construction du Hash

Pour que l'outil de crack (Hashcat) comprenne ce qu'on lui donne, il faut formater ces données ainsi (format NetNTLMv2) : Username::Domain:ServerChallenge:NTProofStr:Blob

Ce qui donne dans notre cas (exemple tronqué) : **Plaintext**

Plaintext

john.doe::CATCORP.LOCAL:1122334455667788:55667788...:01010000...

Sauvegardez cette ligne dans un fichier nommé hash.txt.

5. Cracking du mot de passe

Nous allons utiliser **Hashcat** avec le mode **5600** (spécifique au NetNTLMv2).

Commande :

Bash

```
hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt
```

Après quelques instants, Hashcat trouve la correspondance. **Résultat :** rootbeer

6. Reconstruction du Flag (Attention aux pièges !)

Il faut assembler l'UPN et le mot de passe. L'UPN est composé de user + @ + domaine.
Attention : Le domaine CATCORP.LOCAL doit être passé en minuscules.

Flag Final : RM{john.doe@catcorp.local:rootbeer}