[Exploitation/Cracking] Rainbow Tables

Introduction

Les **rainbow tables** sont des bases de données pré-calculés de hash qui permettent de gagner un temps colossal lors des attaques par force brute.

Il s'agit en outre d'une table associant un mot de passe avec son hash ce qui évite de devoir recalculé le hash lors de l'attaque brute force.

Cependant, ce type d'attaque ne fonctionne plus lorsqu'un algorithme utilisant le salage est utilisé car pour un même mot de passe, plusieurs hashs seront valides (en fonction du salage bien sûr).

Algorithme vulnérables

Voici la liste des algorithmes de hashage vulnérables :

- **NTLM**
- **SHA-1**
- **MD5**
- **LM**
- **Half-LM**

Télécharger des rainbow tables

- Free Rainbow Tables

Revision #2
Created 25 October 2023 16:39:44 by Elieroc
Updated 3 May 2024 15:52:05 by Elieroc