SECURITE SYSTEMES ET RESEAUX - LAB 1

Attaques sur les mots de passe

# Etude du fichier SHADOW

## Question 3.1.1

Structure du fichier :

Le fichier shadow se compose de 9 champs (séparés par des deux-points) :

**« username : passwd : last : may : must : warn : expire : disable : reserved »**

En détail :

* **USERNAME** : Le nom de l’utilisateur
* **PASSWD** : le mot de passe encodé
* **LAST** : Date de la dernière modification (en nombre de jours depuis le 1er janvier 1970)
* **MAY** : Nombre de jours avant que le mot de passe puisse être modifié
* **MUST** : Nombre de jours avant que le mot de passe doive être modifié
* **WARN** : Nombre de jours durant lesquels l’utilisateur est prévenu de l’expiration de son mot de passe
* **EXPIRE** : Nombre de jours entre l’expiration du mot de passe et la fermeture du compte
* **DISABLE** : Date de la fermeture du compte (en nombre de jours depuis le 1er janvier 1970)
* **RESERVED** : Champ réservé

Ainsi, en reprenant le fichier shadow fourni, un exemple serait :

« Root : $1$934b4a210c17493f68bf6bfe74bff77a : 16749 : 0 : 99999 : 7 : : : »

Algorithme utilisé :

Afin de déterminer l’algorithme utilisé pour générer les empreintes des mots de passe nous utilisons le référentiel suivant :

|  |  |
| --- | --- |
| ALGORITHMES | IDENTIFIANTS |
| MD5 | $1 |
| Blowfish | $2 |
| SHA256 | $5 |
| SHA512 | $6 |

Ainsi nous trouvons une correspondance avec notre fichier shadow : $1 situé dans le champ du mot de passe. L’algorithme utilisé est le **MD5**.

# MISE EN ŒUVRE D’UN SCRIPT D’ATTAQUE PAR FORCE BRUTE

## Question 3.2.1

Attaque par force brute

L’attaque par **force brute**, également nommée « BruteForce » ou « Recherche exhaustive » consiste à construire et tester toutes les combinaisons possibles. Ceci, à partir d’une longueur de mot de passe et d’un alphabet de caractères (définis au préalable).

Ce type d’attaque s’avère très efficace, en effet son taux de réussite est de 100% mais son utilisation peut s’avérer très longue dès lors que le mot de passe s’allonge (supérieur à 8 caractères). Néanmoins ce temps de traitement peut être optimisé en utilisant les « chaînes de Markov ».

Mise en œuvre du script