Alex Milliard et Gabriel Létourneau

22 février 2022

Présenté à M. Steven Pigeon

Devoir 1 – énoncé 4

Travail pratique #1

INF36207 – Sécurité Informatique

# Mot de passe trouvé par attaque dictionnaire :

En utilisant notre programme C# par attaque de dictionnaire, il a été possible d’identifier les 10 premiers hash de notre liste reçue. Le tableau ci-dessous présente les solutions identifiées :

|  |  |  |
| --- | --- | --- |
| # Ligne | Hash | Solution |
| 1 | 4438a0153a4ffc2c6e2326151b0b5029 | Fourgons |
| 2 | 7c388e507fea9d165a4d6959dc5c2f54 | Conseils |
| 3 | 2dda62a1d0552cf3ff9e6e074d8173fa | Freinage |
| 4 | 911c0e5042c610825f8446606f2291cc | Normands |
| 5 | 855ac952590d3085f1743193e1163e4c | Grignas |
| 6 | 34f56416dc5a799172ab50705cc4aadd | Amasse |
| 7 | a7cac749a1e011a5663bf3a42f4a7a13 | Jument |
| 8 | 89b9c47e1ade5aa59688100a783a88d1 | Diodons |
| 9 | 15d4f9b9c624e0f504140deffd7e91bf | Logerait |
| 10 | c849f1bbaaae7d63ac655e73e253d0ad | Fucacees |

# Mot de passe trouvé par « brute force » :

En utilisant notre programme d’attaque C# de type « brute force », il nous a été possible d’identifier les hash suivants :

|  |  |  |
| --- | --- | --- |
| # Ligne | Hash | Solution |
| 11 | eab26669cdf592eb65350353950a45fa | (8 caractères) |
| 12 | 4cb9e430d7cbdfa328f014703944dbd5 | cont3 |
| 13 | 4585eeabefc7ad380c42280c45b284de | t$4yon |
| 14 | 63de544a83b395469b8eeef2087f45e5 | (8 caractères) |
| 15 | 7cdd22133b824547307865c5c03ca8f0 | sk141 |

# Complexité des mots de passe

En considérant, le temps exponentiel nécessaire à l’attaque de type « brute force » il est recommandé d’utiliser un mot de passe d’un minimum de 8 caractères mais de favoriser un mot de passe plus long que ce prérequis. Une méthode simple pour mémoriser un tel mot de passe serait de se créer une phrase dont chaque première (ou dernière) lettre de chaque mot la composant forment un mot de passe comme : UnePommeEstUnFruitRougeSucrée! (uPe1FRS!). Pour plus de complexité, chaque mot ou verbe est une lettre majuscule tandis que les autres mots sont minuscules, les chiffres pourraient aussi être représenter en chiffre, par exemple « un » devient « 1 », plutôt qu’en lettre. Bien sûr, afin d’assurer une sécurité accrue, il est aussi important de ne pas réutiliser les mêmes mots de passes pour de multiples authentifications.