Rémi GIACOMETTI
Quentin BAUDET
Liste n°15

Le langage utilisé est le Ruby dans sa plus récente version, la raison est surtout de sa simplicité syntaxique et la gem intégré pour la gestion du MD5.

Les MD5 utilisés sont les suivants :

88faf21d7683c18b3fdb30928110f8da
aeb586ac03a1d0a5b295a9179a474b3c
bc752b2ea8cc392102e0c1862ed02922
bdd798531152c2dd6f069856b7175ead
50046704613df1356ab6f585a7165ba3
6ab68f3a93ebe465a1e60c83f15cacc2
b124bae9773ce0dca46f040b5e121870
723abaadfc4a5d7cad4d8bed78f6ba7d
38f9969db9571de675bd53a92eacd56c
58c4e7591e9924ac2b680f32367af787
faf727b65e18771084717e100efaa433
f3ae993f81259cc366d31a007559a28e
528b14f0ff9b498d3ae97693e6849b32
eceb6c4f0ffae7ce75499784016e68bd
4dafe193731dfc3933682cf593c49142

Les mots de passe découvert sont, par dictionnaire :

brameras, cabrions, canches, decouse, devoras, enquetai, ioulates, moelleux, perverse, thiols

Par énumération :

b4y3! (au bout de 2 à 3 minutes), 3t4p3 (Après environ 45 minutes)

2. La complexité de casser les mots de passe

Dans le choix d'un mot de passe, plus la différence de caractère utilisé est importante et plus sa taille est grande mieux le mot de passe sera fort et complexe à casser. Pour déjouer les stratégies d'attaques par dictionnaire et par énumération il faut d'abord que le mot de passe soit d'une taille importante, pour augmenter le temps de calcul et qu'il ne soit pas composé de mot ayant un rapport entre eux. Pour ne pas que votre mot de passe finisse dans les dictionnaires qui sont récupérables en ligne, il faut aussi penser à diversifier ses mots de passe selon le site ou l'application et penser à les changers fréquements en utilisant aussi la double authentification quand elle est possible.

Une technique simple pour créer un mot de passe très difficile à casser est de prendre 4 à 5 mots qui n'ont aucun rapport entre eux et les mettre les uns à la suite des autres par exemple : mat, veterinaire, heureux et ronflement. En les mettant les uns à la suite des autres il sera facile de s'en rappeler et ça n'apparaîtra dans aucun dictionnaire, pour ce qui est de l'attaque par énumération elle prendra un temps énorme.

Ensuite on peut aussi aborder l'existence des gestionnaires de mot de passe qui simplifie grandement la vie, avec une double authentification et un mot de passe maître d'une 40aine de caractères que l'on connait par coeur et que l'on change tous les 3 à 6 mois, on peut se permettre d'avoir un mot de passe différent pour chaque site qui sera de l'ordre de plus de 40 caractères par mot de passe si l'on veut.

Quelques liens utiles :
https://security.stackexchange.com/questions/22717/how-secure-are-passwords-made-of-whole-english-sentences
https://security.stackexchange.com/questions/21143/confused-about-password-entropy/21150#21150