TP1 : cassage de mots de passe

Durée du TP : 4h.
Date limite de remise du TP : vendredi 18 décembre 2015 à 23h59.
Le TP se fait par groupe de 2 étudiants (au maximum) et les fichiers à remettre doivent être envoyées au plus tard vendredi 18 décembre à minuit par courriel à l'adresse électronique "sgambs@irisa.fr".
Rappel : tout plagiat est formellement interdit et bien qu'il soit naturel que vous puissiez parfois discuter avec vos camarades oralement sur comment attaquer ou résoudre un problème, il est formellement interdit d'échanger des fichiers de code.

Description :
Le but de ce premier tp est de vous faire tester John the Ripper, un logiciel libre de cassage de mots de passe par dictionnaire. Ce logiciel peut notamment être utilisé pour tester la sécurité d'un mot de passe à posteriori dans le cas d'un audit de sécurité ou encore pour évaluer son niveau de sécurité à priori lorsque l'utilisateur choisit son mot de passe. En pratique, l'utilisation de ce type de logiciel doit se faire d'une manière responsable et éthique, dans le but principal de contrôler la sécurité de vos mots de passe.

Vous devrez commencer par télécharger le logiciel John the Ripper à l'adresse suivante : `http://www.openwall.com/john/`
Plus spécifiquement, il vous est conseillé de télécharger la version 1.7.9-jumbo-5 community-enhanced de John the Ripper. Installez ensuite John the Ripper sur votre machine et localisez la documentation ainsi que le fichier de configuration `joint.conf`. Prenez ensuite le temps de lire la documentation afin de vous familiariser avec le fonctionnement du logiciel.

Téléchargez ensuite le fichier de mots de passage à casser à cette adresse :
`http://www.irisa.fr/prive/sgambs/password_tp.txt`
Ce fichier de mots de passe contient 8 entrées utilisateur contenant chacune un login et le mot de passe correspondant obtenu en le passant dans la fonction de hachage MD5 sans application de salage au préalable. Votre objectif est de récupérer chacun des mots de passe correspondants à l'aide de John the Ripper ainsi que grâce aux indices qui vous sont fournis.

Important : vous devrez rendre un rapport résumant le travail effectué dans le TP. Dans ce rapport, vous devrez préciser pour chacun des mots de passe récupérés, la démarche que vous avez utilisé pour récupérer ce mot de passe en montrant par exemple le code que vous avez utilisé ainsi que des statistiques d'utilisation comme le temps que le logiciel a mis pour trouver le mot de passe ou le nombre associé de tentatives.

Partie 1 : mots de passe faible

User 1 et user2 n'ont pas pris la peine de sécuriser leur mot de passe d'une manière appropriée. Essayez de casser ces mots de passe par le mode "single" de John the

Ripper. Comment fonctionne ce mode à votre avis?

Partie 2 : attaque par dictionnaire

User3, user4 et user5 sont des fans de Pokémon et ont dérivé leurs mots de passe de cet univers. En particulier, user3 avoue avoir directement pris comme mot de passe le nom de son pokémon préféré. User4 quant à lui a utilisé une recette un peu plus complexe. Plus précisément, il a choisi un nom de pokémon au hasard, remplacé toutes les voyelles par un chiffre fixé de 0 à 9, puis mis le tout en majuscules. Enfin, user5 a choisi un pokémon au hasard avant d'ensuite inverser les lettres de ce pokémon puis enfin de dédoubler le résultat généré afin d'obtenir son mot de passe. Retrouvez les mots de passe de ces 3 utilisateurs.

Vous pourrez trouver un dictionnaire contenant le nom des pokémons à l'adresse suivante : `http://www.irisa.fr/prive/sgambs/pokemon.txt`
Indice : un bon point de départ pourrait être de lire la documentation RULES de john.

Partie 3 : combinaison de mots et chiffrage par décalage

User6 a construit son mot de passe en concaténant 3 noms de pokémons différents. User7 a suivi il y a quelques jours un cours sur le chiffrement de César ce qui lui a donné l'idée de construire son mot de passe en choisissant un nom de pokémon au hasard, puis en mettant ce nom en minuscule et en décalant chacune de lettres par un entier identique pour toutes les lettres. Voir l'adresse suivante pour plus de détails sur le chiffrement de César :
`http://fr.wikipedia.org/wiki/Chiffrement_par_décalage`

Indice : vous pouvez chercher l'inspiration dans la documentation de john EXTERNAL et les exemples présents dans `john.conf`.

Partie 4 : hachage par SHA-512

User8 a utilisé la même recette que son ami user4 mais a choisi d'utiliser SHA-512 au lieu de MD5 pour stocker le haché de son mot de passe. Retrouvez le mot de passe correspondant. Dans le rapport, discutez la différence de temps nécessaire pour retrouvez ce mot de passe comparé au temps que vous avez mis pour retrouver le mot de passe de user5.