Atelier I : Mesurer la robustesse de mot de passe

Contexte

L'objectif de cet atelier est de vous familiariser avec les différentes approches de *cassage* de mot de passe. Dans la plupart des systèmes, les mots de passe sont sauvegardés sous forme chiffrée. La base de donnée (ou le fichier) des mots de passe peut être accessible en lecteur. Par exemple, dans le cas du système Linux, les mots de passe des utilisateurs se trouvent dans le fichier `/etc/shadow`. Dans la suite nous présentons deux outils populaires souvent utilisés dans le cadre d'audit de sécurité et pour tester la robustesse des mots de passe : `John the Ripper` et `Crunch`.

‘

John the Ripper

L'application `John the Ripper` (JTR) est un logiciel libre de cassage de mot de passe par dictionnaire. Pour installer le logiciel, utiliser la commande : `sudo apt-get install john`

En exécutant la commande `john`. vous obtenez la liste des différentes options du logiciel. Prenez le temps de vous familiariser avec ces différentes options. N'hésitez pas à consulter le manuel d'utilisation en exécutant la commande `man john`

Trois modes de cassage de mots de passe sont possibles :

— Mode simple : le logiciel cherche à trouver le mot de passe à partir du login de l'utilisateur. Si le logiciel trouve le mot en utilisant ce mode, le mot de passe est vraiment très faible.

— Mode liste de mot : le logiciel essaie de trouver le mot de passe en consultant un dictionnaire de mots.

— Mode incrémental : le logiciel va essayer toutes les combinaisons possibles de l'alphabet à utiliser.

Le logiciel offre l'option `--rules` qui permet d'appliquer des règles de modification sur les mots à essayer (changement en majuscule, répétition, inversion, etc.). Les règles sont décrites dans le fichier de configuration qui se trouvent dans `/etc/john/john.conf`.

Crunch

Crunch est un générateur de listes de mots (générateur de dictionnaire) sous licence GPL. Pour installer `Crunch` exécuter la commande :
`sudo apt-get install crunch`

La commande de base pour générer une liste de mots est la suivante :
`crunch min max alphabet`

où :

— `min` est la longueur minimales des mots à générer

— `max` est ma longueur maximale des mots à générer.

— `alphabet` est l'ensemble de caractères à utiliser pour la fabrication des mots.

La commande offre différentes options :

— `-o filename` pour enregistrer la liste produite dans un fichier dont le nom est `filename`

— `-t pattern` afin de générer des mots selon un schéma défini par `pattern`. Le pattern est composé d'une suite de caractères qui peuvent comporter des symboles de substitution. Les symboles utilisables sont données dans le tableau 1.

— `-d [nombre][symbole]` pour indiquer la possibilité de répéter un symbole `d fois`

Consulter la page `man crunch` pour plus d'information sur la commande `crunch`.

TABLE 1 – Crunch - tableau de symboles

Symbole	Signification
@	les caractères minuscules
,	les caractères majuscules
%	les chiffres
∧	les caractères spéciaux

Démonstration

— Nous allons montrer un exemple simple d'utilisation du logiciel JTR pour casser des mots passe faibles. Pour cela, commençons d'abord par créer un utilisateur dont le login est `toto` et le mot de passe est `toto1`. Utiliser la commande `adduser` à cet effet.

— Vérifier la création de l'utilisateur en consultant les fichiers `/etc/passwd` et `/etc/shadow`

— Copier les deux fichiers `/etc/passwd` et `/etc/shadow` dans votre répertoire de travail et veiller à ce que les deux fichiers soient accessibles en lecture sans droit d'administrateur.

— Appliquer la commande `unshadow passwd shadow` afin de fusionner les deux fichiers `passwd` et `shadow` et sauvegarder le fichier résultat dans `passwords`. JTR a besoin du fichier fusionné pour tenter de casser les mots de passe. Nous sommes intéressés seulement au cas de l'utilisateur `toto`, donner une commande qui permet d'extraire dans un fichier nommé `passwords_tp` les informations relatives au seul utilisateur `toto`.

— Appliquer la commande `john passwords_tp`. Commenter le résultat.

Exercices

1. En utilisant la commande `adduser` créer les utilisateurs suivants

login	Mot de passe
legrand	legrand123456
petit	petit123
peremalin	nilamerep
homere	iutv123
john	vtui
racine	toor

2. Appliquer la procédure décrite dans la section démonstration afin d'obtenir un fichier `passwords_tp` résultat de la fusion des fichiers `/etc/passwd` et `shadow`
3. Donner la commande qui permet de tenter de retrouver le mot de passe de l'utilisateur `legrand`. Est-ce que JTR réussit à trouver le mot de passe rapidement ? Refaire la même question pour l'utilisateur `petit`. Commentez le résultat obtenu.
4. Homère et John sont deux enseignants à l'IUT de Villetaneuse et sont très attachés à leur IUT.
5. Est-ce que tous les mots de passe sont cassés avec la même rapidité ?
6. Pourriez-vous casser le mot de passe de l'utilisateur `teacher` ?