SÉCURITÉ SYSTÈMES ET RÉSEAUX
(B3)
Travaux pratiques : lab n°1 – 4h

Attaques sur les mots de passe
Mise en œuvre d'un script de cassage par force brute et dictionnaire

---

1 Aperçu du lab :

A travers ce TP, vous allez mettre en œuvre les connaissances théoriques présentées lors du cours sur la sécurité des mots de passe. Un fichier `shadow`[1], précédemment récupéré sur un serveur linux, vous a été fourni. Il contient une liste d'empreintes, et votre rôle sur la mission est d'arriver à décrypter ces empreintes.

Les seules informations dont vous disposez à ce sujet, sont le nom du fichier : shadow, et les contraintes imposées aux utilisateurs du système pour générer leur mot de passe à savoir :

- Le mot de passe doit avoir une longueur de 6 à 12 caractères.
- Le mot de passe peut contenir des caractères de chacune des listes suivantes :
  - alphabet français minuscule,
  - alphabet français majuscule,
  - chiffre entre 0 et 9,
  - caractère ; @ _ ou #

Vous travaillerez en binôme de façon totalement autonome, vous devrez donc consulter toute la documentation à votre disposition pour régler les différentes problématiques qui se présenteront à vous.

Normalement vous avez largement le temps de faire toutes les manipulations dans le temps imparti, mais ne perdez pas trop de temps.

2 Objectifs du lab :

Ce TP a été réalisé avec en tête plusieurs objectifs :

- Tout d'abord il est une bonne illustration du cours théorique sur la sécurité relative aux mots de passe.
- Il va vous permettre de manipuler de façon concrète les grands principes liés au cassage de mots de passe en vous permettant de réaliser un script mettant en œuvre les attaques par force brute et par dictionnaire.
- Pour finir, il vous fait découvrir le langage Python, très souvent utilisé en sécurité.

1 *Fichier contenant l'ensemble des empreintes de mots de passe des comptes utilisateurs d'un système Linux.*

3 Les consignes :

3.1 Étude du contenu du fichier shadow :

3.1.1 Rappels théoriques :

- En vous aidant de la documentation disponible sur internet, expliquez en détail la structure du fichier qui vous a été fourni.
- Compte-tenu des résultats de cette analyse, déduisez le nom de l'algorithme utilisé pour générer les empreintes des mots de passe qui se trouvent dans ce fichier.

3.2 Mise en œuvre d'un script d'attaque par force brute :

3.2.1 Rappels théoriques :

- Rappelez moi en quoi consiste une attaque par force brute, ou recherche exhaustive.

3.2.2 Mise en œuvre du script :

- Vous allez maintenant écrire un script en langage Python qui réalisera l'attaque par force brute sur les empreintes contenues dans le fichier qui vous a été fourni.
- Votre script devra réaliser les opérations suivantes :
  - Lire le contenu du fichier ligne par ligne.
  - Tentez de retrouver le mot de passe dissimulé en utilisant une attaque par force brute
  - Stocker les mots de passe découverts dans un fichier de sortie, en précisant pour chaque mot de passe le temps nécessaire à la découverte.
- Votre script a-t-il réussi à découvrir tous les mots de passe dissimulés dans le fichier `shadow` ?

Vous allez maintenant utiliser une autre méthode pour tenter de décrypter les empreintes : l'attaque par dictionnaire.

3.3 Mise en œuvre d'un script d'attaque par dictionnaire :

3.3.1 Rappels théoriques :

- Rappelez moi en quoi consiste une attaque par dictionnaire.

3.3.2 Mise en œuvre du script :

- Vous allez maintenant écrire un nouveau script en langage Python qui réalisera une attaque par dictionnaire sur les empreintes contenues dans le fichier qui vous a été fourni. Pour cela vous disposerez d'un dictionnaire de mots de passe.
- Votre script devra réaliser les opérations suivantes :
  - Lire le contenu du fichier ligne par ligne.
  - Tentez de retrouver le mot de passe dissimulé en testant chaque occurrence de mot contenu dans le dictionnaire.
  - Stocker les mots de passe découverts dans un fichier de sortie, en précisant pour chaque mot de passe le temps nécessaire à la découverte.
- Votre script a-t-il réussi à découvrir tous les mots de passe dissimulés dans le fichier shadow ?

Expliquez les avantages et inconvénients de chacune des deux méthodes.

4 Les livrables :

A l'issue du TP, vous devrez me remettre par email un rapport détaillé de votre travail au format pdf uniquement. Ce rapport devra être correctement rédigé.
Pour chacun des points à traiter vous fournirez l'explication détaillée des manipulations que vous avez effectuées (commandes et résultats). Vous joindrez les résultats que vous avez obtenus, votre interprétation, ainsi que vos éventuelles remarques et constats. N'hésitez pas également à indiquer vos interrogations sur des résultats.

Pour finir, la note tiendra compte de votre analyse et de la qualité de la rédaction.