Sécurité - TP
Cryptographie

Virginie Van den Schrieck

10 septembre 2015

L'objectif de ce TP est de sensibiliser les étudiants à la bonne utilisation des outils cryptographiques, en expérimentant les risques encourus en cas de mauvaise mise en pratique de ces dernières.

La première partie du TP consiste à implémenter le code de César, puis à le craquer. Il s'agit d'un exemple très simple de chiffrement symétrique mettant en avant l'importance de la clé. Dans la seconde partie du TP, nous nous intéresserons aux attaques brute-force dans le cadre du craquage de mots de passe Linux.

Le temps prévu pour ce TP est d'environ trois heures, séance encadrée comprise, en binôme. Il est possible, pour le second exercice, de se coordonner entre binômes pour la collecte de mesures.

Un petit rapport documentant le travail effectué est demandé.

1 Implémentation du Code de César

Le code de César est un chiffrement très simple consistant à remplacer chaque lettre d'un message par la lettre située X positions plus loin dans l'alphabet. Par exemple, pour X = 2, on remplacera les A par des C, les B par des D, et ainsi de suite. La substitution est circulaire : Le Y sera remplacé par le A et le Z par le B.

Il vous est demandé d'implémenter, dans le langage de programmation de votre choix, les trois choses suivantes :

1. une fonction ou une méthode qui prend en paramètre un entier X, qui est la valeur du décalage, et une chaîne de caractères ne comprenant que des lettres non accentuées, des espaces et des caractères de ponctuation. Cette fonction produit en sortie une chaîne de caractères qui est la chaîne initiale dont les lettres ont été chiffrées avec le code de César. Les espaces et les caractères de ponctuation restent inchangés.
2. La fonction inverse, permettant le déchiffrement.

3. Un petit programme qui prend un texte chiffré en input, et qui effectue une attaque brute-force sur ce texte pour retrouver le message initial (sans utiliser la fonction de déchiffrement, donc).

Quelle est l'étape la plus complexe dans l'implémentation de l'attaque brute-force ? Expliquez le succintement dans le rapport.

2 John the Ripper

John the Ripper est un petit utilitaire permettant de tester la sécurité des mots de passe, ou, en changeant de perspective, permettant de les craquer.

Il vous est demandé d'installer et de tester cet utilitaire pour mesurer le temps nécessaire pour casser un mot de passe donné, en fonction de ses caractéristiques.

Ce travail est bien sûr à effectuer sur une machine virtuelle. Choisisser une machine Centos-Netkit. Elle possède deux comptes : `user` et `root`, et tous deux sont associés au mot de passe `centos`. Vous pouvez éventuellement utiliser l'interface graphique en lançant la commande `./startx` sous le compte root.

Assurez vous que le réseau soit correctement utilisé, et que la machine puisse accéder à Internet.

2.1 Installation

Pour effectuer l'installation, faites les opérations suivantes :
- Installer Make et gcc : `yum install make` et `yum install gcc`
- Télécharger John the Ripper :
  `wget http://www.openwall.com/john/j/john-1.8.0.tar.gz`
- Décompressez-le : `tar -xvzf john-1.8.0.tar.gz`
- Installez-le : `cd src` puis `make clean linux-x86-64`
- Vérifiez qu'il fonctionne en allant dans le répertoire run et en vérifiant l'existence de l'exécutable `john`

2.2 Utilisation

John the Ripper fonctionne selon trois modes :

1. Le mode simple : Il effectue une rapide recherche sur base de variations sur le nom d'utilisateur (ex : root123)
2. L'attaque par dictionnaire : Il va essayer un par un tous les mots d'une liste, en appliquant également une série de transformations. Il possède une liste par défaut (anglais), mais il est possible de lui en spécifier une autre

3. Le mode incrémental, qui correspond à une attaque brute-force. Il faut bien spécifier la taille maximum du mot de passe à rechercher, afin de limiter la recherche dans le temps...

Pour la syntaxe exacte des options, vous pouvez vous référez à la man page, à la page officielle de l'outil `http://www.openwall.com/john/`, ou bien encore au tutoriel suivant : `http://www.artduweb.com/tutoriels/jtr`.

Afin de craquer un mot de passe Linux, il faut récupérer le fichier contenant les mots de passe chiffrés. Il s'agit du fichier `/etc/passwd`. Pour le rendre utilisable par John the Ripper, il faut effectuer l'opération suivante dans le répertoire run (utilisation de l'utilitaire `unshadow`) :

```
./unshadow /etc/passwd /etc/shadow > my_passwd.db
```

A quoi sert cette étape ? Qu'est ce que ce fichier /etc/shadow ?

Avec quel mécanisme cryptographique sont chiffrés les mots de passe dans Linux ?

2.3 Création de comptes

Pour tester John the Ripper, vous pouvez bien sûr commencer par casser les mots de passe des deux comptes existant sur le système. Il serait néanmoins intéressant de ne pas se limiter à ce cas de figure. Puisqu'il vous est demandé de ne pas modifier les mots de passe de la machine virtuelle, il vous faudra créer de nouveaux comptes utilisateur. Utilisez pour cela les commandes `adduser` et `passwd` [1]

2.4 Mesures

Il vous est demandé d'effectuer une petite campagne de mesures relevant le temps nécessaire à John the Ripper pour casser un mot de passe en fonction de ses caractéristiques. La commande `time` pourrait vous être utile. Réfléchissez bien avant chaque mesure pour choisir le mode de recherche le plus efficace. Voici quelques pistes à suivre pour évaluer John the Ripper :

- Tester des mots de passe dérivés du nom d'utilisateur
- Tester un mot de passe directement extrait du dictionnaire
- Tester des mots de passe comportant 1, 2, 3, 4... caractères
- Tester un mot de passe de 3 caractères ne contenant que des lettres, puis contenant des lettres, des chiffres et des caractères de ponctuation
- ...

N'hésitez pas à analyser les résultats et à en tirer d'éventuelles conclusion

1. le système risque de générer un message d'erreur si le mot de passe est trop faible, mais vous pouvez l'ignorer dans le cadre de ce TP

3 Déliverables

Avant le début du prochain TP, vous posterez sur le Campus Virtuel un document PDF d'une page ou deux documentant le travail effectué et répondant aux questions posées.