TP-2: Cassage de mots de passe

17 septembre 2015

1 Généralités

Un casseur de mot de passe effectue des recherches exhaustives sur des empreintes de mot de passe. L'architecture de tous les casseurs de mot de passe est toujours presque la même. On trouve deux moteurs (*engines*) dans un casseur. Le premier moteur a pour fonction d'exécuter de produire des valeurs à tester. Le deuxième moteur a pour but d'effectuer les opérations cryptographiques afin de retrouver effectivement le/les mots de passe.

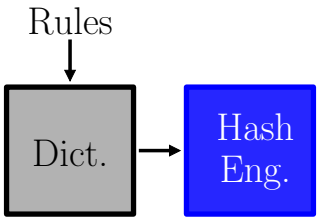

FIGURE 1 – Architecture d'un casseur de mot de passe.

Il existe trois grands logiciels pour casser des mots de passe :

- `John The Ripper`,
- `Hashcat`,
- `Ophcrack`.

Nous allons travailler avec `John The Ripper` (`JTR`) qui est disponible sur `Kali Linux`. En cas de souci vous disposez de toute la documentation nécessaire sur `http://www.openwall.com/john/doc/`.

2 Fonctionnement

`JTR` dispose de trois mode de fonctionnement :

- `single` le mode `single` est le plus basique mais pas forcement le plus efficace.
- `wordlist`, permet d'utiliser des listes de mots pour générer des candidats. Créer un fichier `list` contenant un mot (celui de votre choix). Puis exécuter la commande suivante. `john -wordlist=list --stdout` La force du mode `wordlist` apparait quand on utilise les règles de *mangling* : `john -wordlist=wordlist --rules --stdout`
  `Kali Linux` dispose de liste de mots dans ce répertoire :
  `/usr/share/wordlists`
  Vous pouvez aussi en trouver des fichiers à cette adresse (faites attention à la taille des fichiers que vous téléchargez) :
  `https://wiki.skullsecurity.org/index.php?title=Passwords`
- `incremental`, a vous de découvrir ce dernier mode.