

Manuel d'Utilisation de RainbowCrack

Table des Matières

1. Introduction
2. Installation
3. Principes de Fonctionnement
4. Génération de Tables Rainbow
5. Utilisation de RainbowCrack pour Craquer des Hashs
6. Options et Paramètres Avancés
7. Bonnes Pratiques et Sécurité
8. Ressources Supplémentaires

1. Introduction

RainbowCrack est un outil de craquage de mots de passe qui utilise des tables rainbow pour réduire le temps nécessaire pour retrouver les mots de passe à partir de leurs hash. Les tables rainbow sont des structures de données précalculées qui permettent de retrouver rapidement le mot de passe correspondant à un hash donné.

2. Installation

Pré-requis

- Système d'exploitation Windows, Linux, ou macOS
- Outils de compilation (si vous compilez à partir du code source)
- Bibliothèque OpenSSL

Instructions

Windows

1. Téléchargez la version Windows de RainbowCrack depuis le site officiel.
2. Extrayez le contenu de l'archive téléchargée.
3. Ouvrez une fenêtre de commande (cmd) et naviguez vers le répertoire extrait.
4. RainbowCrack est prêt à être utilisé.

Linux / macOS

1. Téléchargez le code source depuis le site officiel.
2. Ouvrez un terminal.
3. Décompressez le fichier téléchargé : `tar -zxvf rcrack-<version>.tar.gz`
4. Naviguez vers le répertoire décompressé : `cd rcrack-<version>`
5. Compilez le programme : `make`
6. RainbowCrack est prêt à être utilisé.

3. Principes de Fonctionnement

RainbowCrack utilise des tables rainbow pour effectuer des attaques par correspondance inversée sur les hash. Ces tables sont générées en précalculant des chaînes de hash et leurs réductions sur une plage de valeurs de mots de passe possibles.

Processus de Craquage

1. **Génération des Tables** : Précalcul des hash pour une liste de mots de passe possibles et stockage dans une table.
2. **Recherche** : Lors du craquage, le programme recherche le hash cible dans la table pour retrouver le mot de passe correspondant.

4. Génération de Tables Rainbow

Pour générer des tables rainbow, utilisez l'outil `rtgen` fourni avec RainbowCrack.

Commande de Base

```
rtgen <hash_algorithm> <charset> <plaintext_len_min> <plaintext_len_max>
<table_index> <chain_len> <chain_num> <part_index>
```

Exemple

Pour générer une table rainbow pour les hash MD5 avec des mots de passe de 1 à 7 caractères utilisant l'ensemble de caractères alphanumériques :

```
rtgen md5 loweralpha-numeric 1 7 0 10000 1000000 0
```

Explications des Paramètres

- `<hash_algorithm>` : L'algorithme de hash (ex : md5, sha1, etc.).
- `<charset>` : L'ensemble de caractères (ex : loweralpha, numeric, loweralpha-numeric, etc.).
- `<plaintext_len_min>` : Longueur minimale des mots de passe en clair.
- `<plaintext_len_max>` : Longueur maximale des mots de passe en clair.
- `<table_index>` : Index de la table (utilisé pour distinguer différentes tables avec les mêmes paramètres).
- `<chain_len>` : Longueur des chaînes dans la table.
- `<chain_num>` : Nombre de chaînes dans la table.
- `<part_index>` : Index de la partie pour les tables divisées en plusieurs parties.

Fusion des Tables

Après la génération, il faut fusionner les parties de table si elles sont divisées :

```
rt2rtc <input_file.rt> <output_file rtc>
```

5. Utilisation de RainbowCrack pour Craquer des Hashs

Pour craquer des hash, utilisez l'outil `rcrack` :

Commande de Base

```
rcrack <table_file> -h <hash>
```

Exemple

```
rcrack *.rtc -h 5f4dcc3b5aa765d61d8327deb882cf99
```

Explication des Paramètres

- `<table_file>` : Le fichier de table rainbow à utiliser.
- `-h <hash>` : Le hash à craquer.

6. Options et Paramètres Avancés

RainbowCrack offre plusieurs options avancées pour personnaliser les attaques et la génération de tables.

Options de `rcrack`

- `-l <hash_list_file>` : Spécifie un fichier contenant une liste de hash à craquer.
- `-d` : Active le mode de débogage pour plus de détails pendant l'exécution.

Options de `rtgen`

- `-t <thread_num>` : Spécifie le nombre de threads à utiliser pour la génération.
- `-s <start_point>` : Point de départ pour la génération des chaînes (utile pour reprendre la génération interrompue).

7. Bonnes Pratiques et Sécurité

- **Utilisation Éthique** : Utilisez RainbowCrack uniquement pour tester la sécurité de vos propres systèmes ou avec l'autorisation expresse du propriétaire du système.
- **Sécurisation des Mots de Passe** : Utilisez des mots de passe longs et complexes pour rendre le craquage plus difficile.
- **Mises à Jour** : Maintenez vos outils et systèmes à jour pour bénéficier des dernières sécurités.

8. Ressources Supplémentaires

- Site Officiel de RainbowCrack
- Forum de Support de RainbowCrack
- GitHub de RainbowCrack pour les dernières mises à jour et code source.

Ce manuel vous donne les bases pour installer, générer des tables rainbow, et utiliser RainbowCrack pour craquer des hash. Utilisez cet outil de manière responsable et éthique.