📑Rapport : Casser un Mot de Passe

📌 **Auteur :** Alexandre LE GOFF 📌 **Formation :** BTS SIO 📌 **Date :** Janvier 2025 📌

Mission : Étude de la méthodologie de cassage de mots de passe sous Linux Kali

🔎 Présentation

Ce document a pour but de présenter les méthodes permettant de tester la robustesse des mots de passe en utilisant des outils spécialisés sous **Linux Kali** .

⚠️ **Avertissement :** Cette étude est réalisée **à des fins pédagogiques** uniquement. Toute utilisation malveillante des outils présentés est **interdite** et peut entraîner des poursuites judiciaires.

🛠️Prérequis Techniques

🛠️ Prérequis Techniques

Pour effectuer ces manipulations, il est nécessaire de disposer de :

✅ Un environnement Linux Kali (installé sur une machine virtuelle avec VirtualBox ou VMware)

✅ Des outils spécialisés :

John the Ripper 🔐 (outil de cassage de mots de passe en ligne de commande)

OPHCrack 🔍 (outil utilisant des tables arc-en-ciel pour casser les mots de passe Windows)

💡 Installation rapide des outils :

➡️ Installation de John the Ripper

Ouvrez un terminal et entrez :

```
sudo apt update && sudo apt install john -y
```

➡️ Installation de OPHCrack

Téléchargez et installez OPHCrack avec :

```
sudo apt install ophcrack -y
```

🔧 Étapes de Manipulation

1️⃣ Récupération du Hash

Le contexte est le suivant : un système a été compromis,

Nous avons récupéré un hash de mot de passe.

📌 **Exemple de hash récupéré :**
af4fef1bc0861ca2824db7315f844327

Nous allons maintenant analyser et casser ce hash pour retrouver le mot de passe d'origine.

2️⃣ Identification du Type de Hash

Pour identifier quel type de hash nous avons,

Nous utilisons John the Ripper avec la commande suivante :
`john --show --format=raw-md5 hashes.txt`

💡 **Résultat attendu :**
`MD5 detected`

Nous avons donc affaire à un hash

3️⃣ Cassage du Mot de Passe avec John the Ripper

Pour casser le mot de passe, la commande suivante est utilisée avec la spécification du format de has
`john --format=raw-md5 --incremental hashes.txt`

John the Ripper essaie de retrouver le mot de passe à partir du hash. Après quelques instants, le mot
s'affiche en orange dans la console, indiquant le succès du cassage.

💡 **Exemple de sortie :**

af4fef1bc0861ca2824db7315f844327 : Salut

📌 Le mot de passe pour le hash est donc **Salut** 🔑.

4️⃣ **Utilisation des Tables Arc-en-Ciel (Rainbow Tables)**

Une autre approche pour casser un mot de passe est **l'utilisation des tables arc-en-ciel** 📊.

Elles permettent d'associer rapidement des **hashs connus** à leurs mots de passe correspondants.

➡️ **Étapes avec OPHCrack**

Lancez **OPHCrack** avec :

bashCopierModifierophcrack

Chargez votre fichier contenant les hashs.

Sélectionnez la table appropriée (`md5`, `sha1`, etc.).

Démarrez l'attaque et attendez que OPHCrack trouve le mot de passe.

💡 **Avantages des tables arc-en-ciel** :

✅ Très rapide pour des mots de passe **simples**

❌ Inefficace sur les mots de passe **complexes** ou **salés**

🔎Sécurité & Protection des Mots de Passe

Pour éviter que vos mots de passe soient facilement cassés, voici des bonnes pratiques à suivre :

Utiliser un mot de passe long et complexe : Assurez-vous qu'il ait au minimum 12 caractères et qu'il mêle majuscules, chiffres et symboles.
Éviter les mots de passe fréquents : Évitez les combinaisons comme `123456`, `password` ou `admin`.
Activer l'authentification à deux facteurs (2FA) : Renforcez la sécurité de vos comptes en ajoutant une couche de protection supplémentaire.
Utiliser un gestionnaire de mots de passe : Outils tels que Bitwarden, KeePassXC, ou 1Password vous aident à créer et gérer vos mots de passe de manière sécurisée.
Changer régulièrement vos mots de passe et ne pas les réutiliser : Limitez les risques en ayant des mots de passe uniques pour chaque compte.

📌Conclusion

Cette étude a illustré la vulnérabilité des mots de passe faibles face aux outils de piratage tels que John the Ripper et OPHCrack.

🔹 **Leçon essentielle :** Adoptez des mots de passe robustes et complémentés par des solutions modernes telles que l'authentification multi-facteurs pour sécuriser vos comptes.

🔐 **La force de vos mots de passe est cruciale pour assurer votre sécurité !**

📎Ressources et liens utiles

Site officiel de John the Ripper : Consultez le site officiel de John the Ripper pour des informations, actualisations et ressources concernant cet outil de déchiffrement de mots de passe.

Télécharger OPHCrack : Rendez-vous sur la page de téléchargement d'OPHCrack pour obtenir cet outil open-source de récupération de mots de passe via l'utilisation de tables arc-en-ciel.

Générateur de mots de passe sécurisés : Utilisez un générateur de mots de passe sécurisés pour créer des mots de passe robustes et uniques qui permettent de protéger vos comptes en ligne.