TP – Mots de passe

Partie 1 : John The Ripper (JTR)

John the Ripper est un outil permettant l'attaque de mot de passe par force brute, par dictionnaire, …

Dans cette partie, vous allez utiliser cet outil.

1- En ligne de commande, téléchargez, installez, et testez JTR
https://github.com/openwall/john

2- Téléchargez la fuite de données Rockyou. Il s'agit de mots de passe issus d'une attaque. Cette base nous servira comme dictionnaire pour JTR.

3- Créez un fichier libreoffice odt que vous enregistrez avec un mot de passe pioché dans Rockyou.

4- Essayez de retrouver ce mot de passe à l'aide de JTR, de rockyou, et du fichier odt.

5- Créez un fichier ZIP, contenant l'odt, en ligne de commande avec un mot de passe de 7 caractères.

6- Essayez de retrouver ce mot de passe à l'aide de JTR, du fichier zip, sans utiliser rockyou : attaque par force brute.

Partie 2 : Firefox

Dans cette partie, nous allons attaquer le gestionnaire de mot de passe de Firefox.

1- Téléchargez Firefox, nous n'allons pas utiliser la version installée sur votre PC.

2- Lancer le Firefox téléchargé en utilisant un nouveau répertoire vierge de profil Firefox. Pour cela, utilisez le terminal, et cherchez la bonne option.

3- Naviguez sur un site internet, et identifiez-vous, acceptez d'enregistrer le mot de passe dans le trousseau Firefox.

4- Installez Firefox Decrypt, et utilisez-le pour récupérer et visualiser les mots de passe enregistrés dans le trousseau. Sélectionnez le bon profil.

5- Ajoutez un mot de passe maître court (4 lettres) dans votre trousseau de mots de passe Firefox.

6- Essayez de retrouver ce mot de passe maître avec JTR : que se passe-t-il ?

7- Installez et utilisez hashcat pour retrouver ce mot de passe maître.

8- Le mot de passe maître retrouvé, utilisez à nouveau Firefox Decrypt pour visualiser les mots de passe.

Partie 3 : PACK et CUPP

Vous allez découvrir 2 outils permettant d'optimiser l'utilisation de JTR et de Hashcat.

PACK va permettre d'optimiser les paramètres fournis à Hashcat, comme les masques.

1- Installez PACK = Password analysis and cracking kit, utilisez-le pour analyse Rock You.
2- Quel intervalle de longueur de mot de passe faut-il utiliser pour considérer environ 80 % des mots de passe ? Quel jeu de caractère utiliser ? Pourquoi ? Explorez le programme.

CUPP va permettre de créer un dictionnaire personnalisé pour JTR.

3- Installez CUPP = Common User Passwords Profiler. Utilisez le mode intéractif en variant les options et constatez l'évolution de la taille du dictionnaire produit.

4- Finalement, qu'est-ce qu'un bon mot de passe ?

Partie supplémentaire :

1- Installez, explorez, et testez johnny, GUI pour JTR.
2- Quel fichier peut être utiliser pour récupérer les mots de passe de session Windows ?
3- Renseignez-vous sur ophcrack
4- Renseignez-vous sur chntpw
5- Installez une VM windows 11 avec virtualhost. Créez des utilisateurs avec mots de passe, et droits différents. Stoppez **proprement** la VM ! Montez le disque virtuel vdi. Utilisez chntpw pour promouvoir des utilisateurs simples en administrateurs et supprimez le mot de passe. Relancez la VM et constatez le fonctionnement.
6- Produisez un document sur le crackage de code WiFi (aircrack).