**FERDINAND Mathieu SIO 2**

*Nous allons commencer par découvrir qu’est ce qu’est John the ripper !*

*John the Ripper est un logiciel libre de cracking de mots de passe, utilisé pour tester la sécurité des mots de passe. Il est capable de décrypter des mots de passe en utilisant différentes méthodes de décryptage, telles que le décryptage de force brute, le décryptage par dictionnaire et le décryptage hybride.*

 *Le logiciel peut être utilisé pour tester la force des mots de passe, pour aider à la récupération de mots de passe perdus ou oubliés, ou pour aider à la sécurité informatique en permettant de vérifier si des mots de passe sont assez forts pour résister à des attaques.*

 *John the Ripper est compatible avec de nombreux systèmes d'exploitation, notamment les systèmes d'exploitation Windows, Mac OS X, Linux, BSD et Unix. Il est souvent utilisé par des professionnels de la sécurité informatique, des administrateurs de système, des consultants en sécurité, des testeurs de pénétration et des hackers éthiques.*

Premièrement nous allons vérifier tous les noms d’utilisateurs en tapant la commande : **sudo nano/etc/shadow**,

Et cela va nous afficher la page suivante :



Nous entrons ensuite la commande qui va nous faire apparaître les mots de passe crypté : **sudo nano/etc/passwd,**



Essayons maintenant de cracker les mots de passe en s’appuyant sur les noms d’utilisateurs.

La commande suivante va permettre de regrouper les noms d’utilisateurs et les mots de passe dans un seul fichier : **sudounshadow /etc/passwd /etc/shadow>testcracks**



On affiche désormais le fichier testcrack où l’on a réuni les mots de passe crypté et les utilisateurs : **sudo nano testcrack**

****

On configure john :**john testcrack -format-crypt**



Ensuite on affiche les 3600 mots de passe de nos utilisateurs si-ils sont bien présents : **sudo /usr/share/john/passwd.lst**



Cette commande finale affiche les utilisateurs contenant des mots de passe : **john -show testcracks**

****