TP JOHN THE RIPPER

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

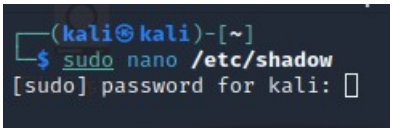
John the Ripper est un logiciel open source utilisé pour tester la sécurité des mots de passe. Il fonctionne en utilisant des algorithmes de chiffrement pour tenter de déchiffrer les mots de passe stockés dans un fichier, et vérifie s'ils correspondent à des entrées prédéfinies, telles que des mots de dictionnaire

Dans notre cas nous allons utilisé un dictionnaire de mot de passe, et un dictionnaire d'identifiant pour vérifier si john saura cracker les mots de passe.

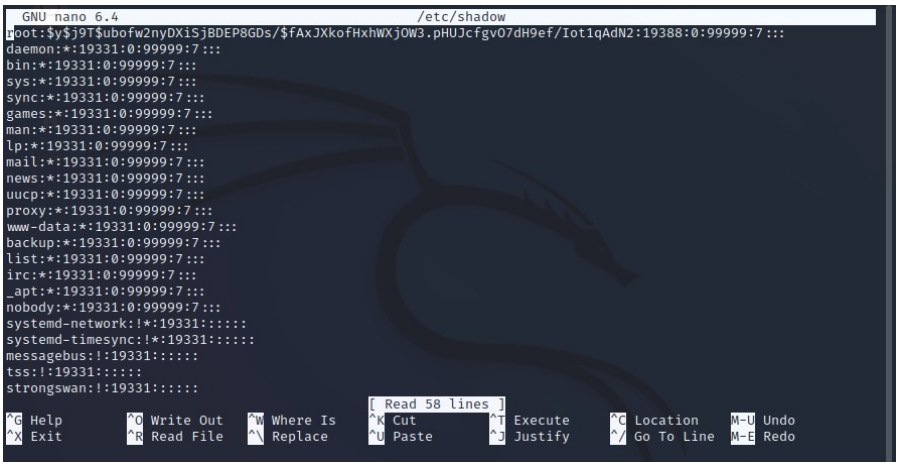
I – Vérification des dictionnaires

Avant de commencer quoi que ce soit nous allons commencer à voir et vérifier les dictionnaires de mots de passe / utilisateurs

En tapant cette commande « sudo nano/etc /shadow » vous allez pouvoir voir tout les noms d'utilisatuers

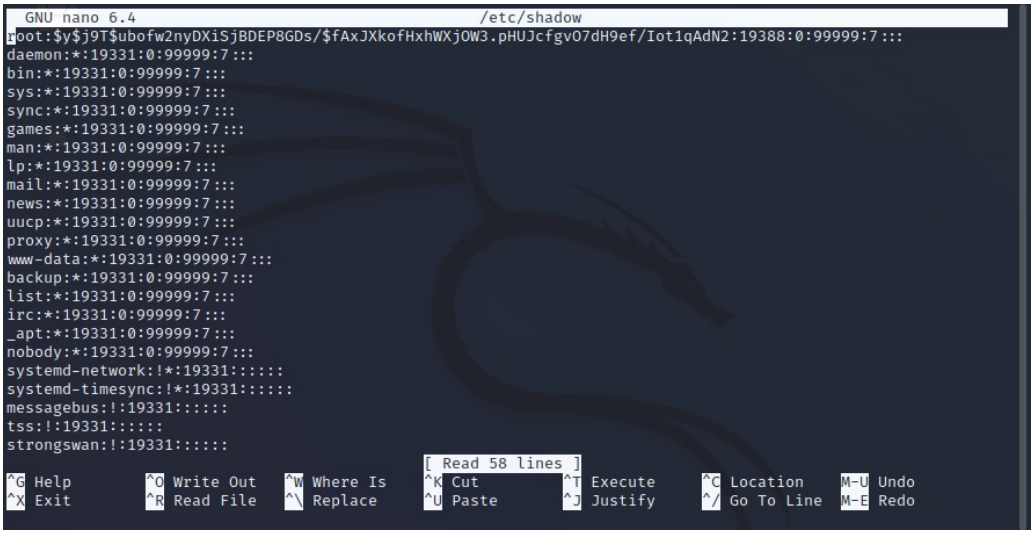


Après cette commande vous allez voir apparaître cette page



En tapant cette commande « sudo nano/etc /passwd » vous allez pouvoir voir tout les mots de passe crypté

le système est censé vous répondre avec ce message :

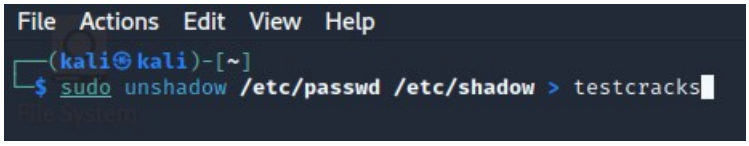


II – Les premières commandes concrète

Après avoir découvert comment afficher les dicctionnaires nous allons maintenant éssayer de cracker les mots de passe à l'aide des noms d'utilisateurs

Nous allons à présent taper une commande qui va pouvoir prendre les mots de passe dans le fichiers /etc /passwd et les noms d'utilisatuers dans le /etc /shadow pour créer un seul fichier qui va regrouper les deux

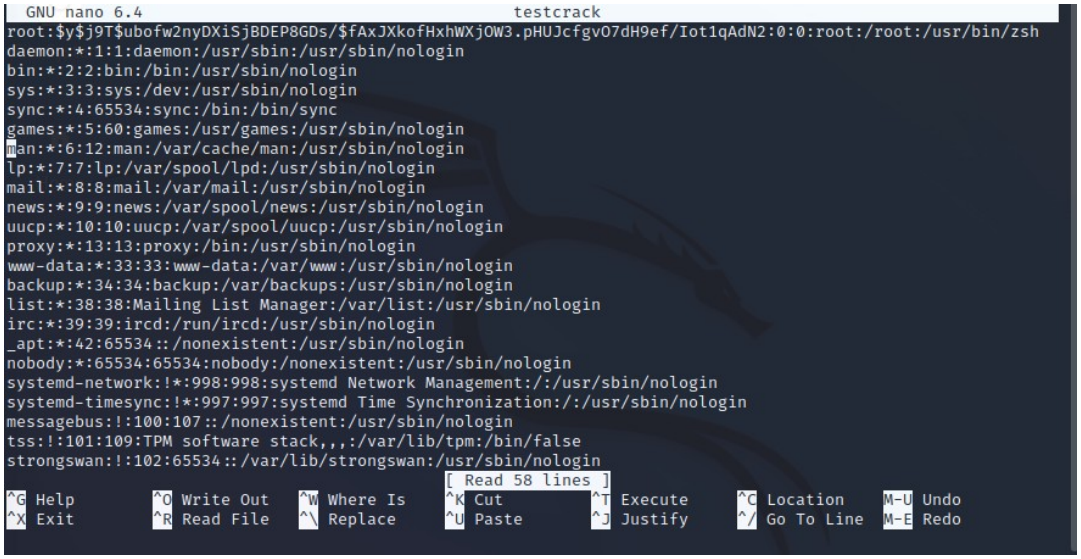
Voici la commande suivante :
sudo unshadow /etc/passwd /etc/shadow > testcracks



Nous allons maitenant afficher le fichier testcrack qui contenait les mots de passe crypté ainsi que les noms d'utilisateurs avec cette commande :

« sudo nano testcrack »

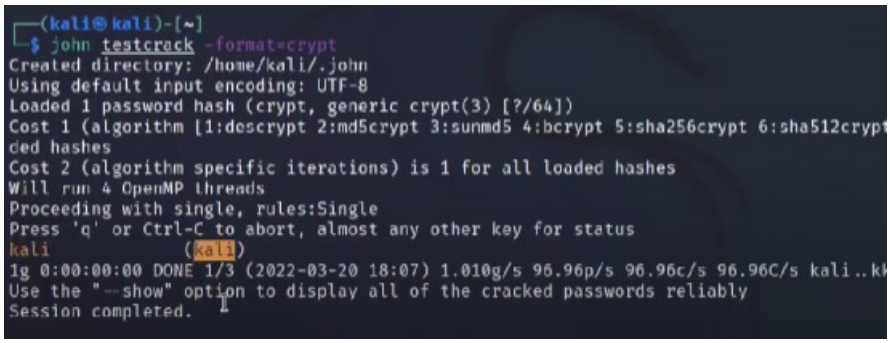
Le système est censé vous répondre sous cette forme



III – Le crackage de John

Maitenant que toutes les étapes sont faites, John va s'occuper de tout le reste, vous n'aurez plus qu'à taper ces quelques dernière commande :

« john testcrack -format=crypt »



Cette commande va permettre de voir les 3600 mots de passe et voir si nots utilisateurs contiennent les mots de passes dans la liste

sudo nano /usr/share/john/password.lst

le systeme va devoir nous envoyé ce document

Pour finir, nous allons taper cette dernière commande qui va nous afficher les utilisateurs qui contiennent les mots de passe

John -show testcrack