**Procédure d’utilisation John the Ripper**

**SOMMAIRE**

1 Objet du document 3

2 John the Ripper 3

2.1 Man 3

2.2 Utilisation 3

# Objet du document

Ce document présente la procédure d’utilisation de l’outil **John the Ripper**.

# John the Ripper

## Man

Pour avoir une liste des options disponibles avec John the Ripper, taper la commande ***john -h***

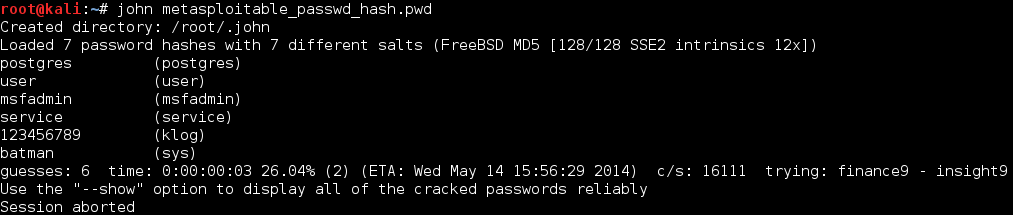
## Utilisation

Le squelette de John the Ripper est :***john [options] password\_file***

Quelques options utiles de John the Ripper :

* *--test*: benchmark l’ordinateur afin évaluer les performances de craquage de mots de passe ;
* *--wordlist*: spécifie un fichier servant de dictionnaire ;
* *--format*: spécifie un format particulier de hash.

1. Avec Metasploit nous avons récupéré un fichier contenant les mots de passe chiffrés du système cible. Afin de craquer les mots de passe, exécuter dans un terminal la commande suintante : ***john chemin\_fichier***, dans notre cas : ***john metasploitable\_passwd\_hash.pwd***



Nous pouvons constater que John the Ripper a trouvé les mots de passe, présentant à gauche le mot de passe et à droite le nom utilisateur associé entre parenthèses.