

SSH2JOHN & John The Ripper

- BruteForce de clé privée RSA

Introduction

SSH2JOHN est un outils qui permet de transformer une clé RSA dans un format utilisable par John The Ripper.

L'outil est retrouvable sur [github](#), également disponible sur Kali Linux.

“ La présentation de cette outil est purement dans un but d'apprentissage.

Utilisation

Dans un premier temps vous devez disposer d'une clé RSA chiffré par une passphrase. Dans l'exemple ci-dessous nous avons crée la clé RSA **kali-john**.

Dès lors que vous avez récupéré la clé, il faut exectuté la commande ci-dessous pour récupéré le hash que nous allons ensuite déchiffrer avec John The Ripper.

```
ssh2john [id_rsa] > [id_rsa.hash]
```

```
(root@kali)-[/home/kali/Desktop]  
# ssh2john kali-john > kali-john.hash
```

Une fois le fichier hashé récupéré, nous pouvons lancé le brute force avec la wordlist rockyou.txt.

```
john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash
```

```
(root@kali)-[/home/kali/Desktop]
# john --wordlist=/usr/share/wordlists/rockyou.txt kali-john.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

Ensuite il suffit d'attendre pour obtenir un résultat. Si le résultat est positif vous allez obtenir ceci :

```
(root@kali)-[/home/kali/Desktop]
# john --wordlist=/usr/share/wordlists/rockyou.txt kali-john.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
medical (kali-john)
1g 0:00:01:22 DONE (2024-02-08 14:26) 0.01209g/s 104.4p/s 104.4c/s 104.4C/s kalani..brigitte
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Nous pouvons donc voir que la passphrase liée à la clé RSA est **medical**.

Si le résultat est négatif vous pouvez essayer une autre wordlist.

Révision #1

Créé 8 février 2024 20:06:01 par Léo del Giudice

Mis à jour 8 février 2024 20:56:09 par Léo del Giudice