[Exploitation/Stegano] Stegseek

Introduction

L'outil **stegseek** permet de lancer des attaque **bruteforce** sur les passphrases des fichiers cachés par steghide dans d'autres fichiers.

Steghide permet par défaut de le faire mais la tâche est complexe est lente.

Source

- Github du projet

Installation

```
wget https://github.com/RickdeJager/stegseek/releases/download/v0.6/stegseek_0.6-1.deb && sudo apt install -y ./stegseek_0.6-1.deb && rm -f stegseek_0.6-1.deb
```

Manuel

Attaque brute force

```
stegseek <STEGANO_FILE> <WORDLIST>
```

Récupération de meta-donnée non chiffrée

Les meta-données non-chiffrées de steghide sont protégées par une **seed** codée d'une longueur de **2^32** (cassable en quelques minutes maxium).

L'outil va donc récupérer les méta-données pour essayer de récupérer :

- Si le fichier contient vraiment de la donnée ajoutée par steghide.
- La quantitié de donnée.
- L'algorithme de chiffrement.
- Si aucun chiffrement n'est présent, le contenu sera affiché.

Voici la commande à effectuer pour lancer la récupération d'informations :

```
stegseek --seed [STEGANO_FILE]
```

Revision #2
Created 7 November 2023 17:41:17 by Elieroc
Updated 3 May 2024 13:22:41 by Elieroc