[Bash] GPG et secrets

Introduction

Lorsque vous travaillez sur des scripts bash, vous pouvez parfois avoir besoin d'utiliser des identifiants pour vous authentifier sur un serveur ou un service.

La manière la plus simple pour fournir les identifiants est généralement de saisir les identifiants en clair dans un fichier texte ou directement dans le script.

Cependant, il s'agit d'une mauvaise pratique car un pirate qui a accès au script ou au fichier pourra accéder au mot de passe en clair.



Manuel

Création du fichier chiffré

Après avoir créé un fichier contenant le mot de passe en clair, lancez la commande suivante pour obtenir une version chiffrée et protégée :

```
gpg -c <FILE>
```

> Une fois la version chiffrée obtenue, supprimez la version originale par sécurité.

Obtention du mot de passe en clair

Une fois authentifié avec l'utilisateur à l'origine du chiffrement du fichier :

```
gpg -dq <FILE>.gpg
```

SSHpass

Cet utilitaire (à installer via votre gestionnaire de paquet), permet de saisir un mot de passe sans interaction de la part de l'utilisateur pour vos connexions **SSH** ou **RSync.**

Il prend en option ou par le pipe, le mot de passe et se charge de le saisir pour vous automatiquement.

Voici un exemple tiré de l'article de LinuxTricks :

```
sshpass -p "monmotdepassecostaud" ssh adrien@192.168.21.100
```

Ou alors :

```
gpg -dq secret.gpg | sshpass ssh user@10.0.0.1
```

Revision #1
Created 2024-02-12 11:31:39 UTC by Elieroc
Updated 2024-02-12 11:43:46 UTC by Elieroc