Chiffrer vos fichiers avec OpenSSL sous Linux

Chiffrer vos fichiers avec OpenSSL sous Linux

https://community.jaguar-network.com/wp-content/uploads/2017/07/openssl-696x456.png.webp

Qu’est-ce qu’ OpenSSL ?

OpenSSL est un outil open-source implémentant entre SSL/TLS et de nombreux algorithmes de chiffrement comme DES, AES, RSA, … ce qui permet de chiffrer des fichiers très simplement.

Installer OpenSSL

Il est possible que **OpenSSL** ne soit pas présent sur votre système, on l’installe via la commande :

```
apt-get install openssh-client
apt-get install openssh-server
```

Le nombre d’algorithme étant important, la liste est consultable pour faire votre choix :

```
openssl enc help
```

Nous poursuivrons avec l'algorithme **-aes-256-cbc** par la suite qui est l'algorithme actuel le plus performant en terme de sécurité et rapidité.

Chiffrage avec OpenSSL

Pour chiffrer un fichier, nous devons simplement adapter la commande suivante :

```
openssl enc -e -aes-256-cbc -in fichier -out fichier_secret
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
```

Paramètre pour spécifier à OpenSSL qu'on effectue un chiffrement.

Paramètre indiquant le chiffrage de fichier.

Algorithme de chiffrement choisi.

Fichier d'entré pour le chiffrage.

Fichier de sortie chiffré.

On consulte le résultat :

```
cat fichier.txt
Contenu non chiffré

cat fichier_secret.txt
Salted__A��r�bNj~B�\��vJF�"���=w����oUk19�
```

Le mot de passe peut également être saisi directement par la commande suivante mais il sera accessible à qui accèdera à vos commandes, nous vous conseillons donc de l'éviter :

```
openssl enc -e -aes-256-cbc -in fichier -out fichier_secret -pass pass: V0trEm0tdepass3
```

Déchiffrage OpenSSL

Pour déchiffrer un fichier, nous inversons les 2 fichiers et le paramètre d'action **-e** à **-d** :

```
openssl enc -e -aes-256-cbc -in fichier_secret -out nouveau_fichier
```

Paramètre pour spécifier à OpenSSL qu’on effectue un chiffrement.

Paramètre indiquant le déchiffrage de fichier.

Algorithme de chiffrement choisi.

Fichier d’entré pour le chiffrage.

Fichier de sortie chiffré.

On consulte le résultat :

```
cat fichier_secret.txt
Salted__A��r�bNj~B�\��vJF�"���=w����oUk19�

cat nouveau_fichier.txt
Contenu non chiffré
```

Revision #3
Created 4 February 2021 23:17:34 by garfi
Updated 4 February 2021 23:20:02 by garfi