Tutoriel sur la sécurisation d'un GRUB 2 avec authentification par mot de passe

SOMMAIRE

I) Introduction

Nous verrons dans ce tutoriel comment et pourquoi sécuriser un GRUB (version 2) sur une machine Linux (ici Linux MINT).

POURQUOI ?

Il existe un moyen de réinitialiser le mot de passe ROOT sans connaître l'ancien mot de passe. Cela peut être utile si l'administrateur perd le mot de passe. Cependant cette méthode peut être utilisé par les pirates et donc s'en servir pour avoir un accès au serveur. Alors la solution consiste à mettre un mot de passe pour accéder au GRUB.

Il est vivement conseillé d'utiliser un logiciel SSH comme PUTTY car nous aurons besoin de copier et de coller des lignes très longues.

II) Mise en place du mot de passe

La première étape consistera à faire une sauvegarde du fichier de configuration du GRUB, cela sera très utile au cas où.

```
# cp /boot/grub/grub.cfg /boot/grub/old.grub.cfg
```

Une fois ceci fait il faut générer un mot de passe hacher pour une meilleure sécurité car sinon le mot de passe sera affiché en claire dans le fichier.

```
# grub-mkpasswd-pbkdf2
Entrer mot de passe :
Réécrivez le mot de passe :
Vous aurez à l'écran votre mot de passe qu'il faudrait copier à partir « grub.pbkdf2.sha512.... jusqu'à la fin.
```

Une fois copié, il faut maintenant éditer le fichier **grub.cfg** et y ajouter les paramètres ci-dessous :

```
#Password
set superusers = "kevin"          ← Cela correspond à l'utilisateur GRUB
password_pbkdf2 kevin MotDePasseCopiéAuDessus          ← Mot de passe du GRUB haché
```

Il ne reste plus cas redémarrer votre machine et d'appuyer sur la touche « e » dans le boot et il vous demandera donc votre utilisateur et votre mot de passe.