Rkhunter (Optionnel)

Rkhunter peut détecter les répertoires généralement utilisés par les rootkits. Les permissions anormales, les fichiers cachés, les chaînes suspectes dans le kernel et peut effectuer des tests spécifiques à Linux. Cela se fait en comparant les hashs de vos fichiers avec des hashs de virus et logiciels connus.

Installation de RKHunter

```
apt install rkhunter -y
```

Chercher ensuite la ligne ou il y a `WEB_CMD="/bin/false"` vous pouvez utiliser Ctrl+W sur nano. Une fois la ligne trouvée commentez la.

```
# WEB_CMD="/bin/false"
```

Puis la ligne ou il y a écris `UPDATE_MIRRORS` et mettez sa valeur à 1. Cela spécifie que le fichier mirroir doit être vérifié pour les mise à jours lors d'une update.

```
UPDATE_MIRRORS=1
```

Puis la ligne `MIRRORS_MODE` et mettre sa valeur à 0. Cela permet de spécifier à rkhunter quel mirroir utiliser lors d'une update.

```
MIRRORS_MODE=0
```

Une fois l'étape précédente terminé et enregistré on va rajouter les notifications par mail:
On ouvre le fichier situé sous `/etc/default/rkhunter` avec notre éditeur préféré:

```
nano /etc/default/rkhunter
```

Puis on modifie si besoin les variables suivantes:

```
# Pour effectuer une vérification chaque jour
CRON_DAILY_RUN="yes"
# L'adresse sur laquelle on veut recevoir les emails, ici celle associé à root
REPORT_EMAIL="root"
```

Vérifions que notre fichier de configuration est correct avec la commande:

```
rkhunter -C
```

Pour mettre à jour rkhunter vous pouvez ensuite utiliser la commande:

```
rkhunter --update
```

Puis pour vérifier le système local

```
rkhunter --check
```

Rkhunter peut avoir **de faux positifs** suite à une mise à jour par exemple dans ce cas, il faut mettre la base d’empreintes à jour avec la commande :

```
rkhunter --propupd
```

Ce sera tout pour RKhunter vous pouvez également voir les logs sous `/var/log/rkhunter.log` :)

Revision #3
Created 2021-01-29 15:35:50 UTC by Faces
Updated 2022-06-10 17:49:43 UTC by Faces