RkHunter

- Objet : RkHunter, Installation, Utilisation
- Niveau requis :
  débutant, avisé
- Commentaires : *programme qui permet de détecter la présence de Rootkits, portes dérobées et exploits au sein du système sur lequel il est exécuté.*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !
- Suivi :
  - Création par smolski le 16/11/2009
  - Testé par Ir0nsh007er le 20/05/2015
- Commentaires sur le forum : C'est ici[1)]

Introduction

RkHunter (pour *Rootkit Hunter*) est un programme **Unix** qui permet de détecter les **rootkits**, portes dérobées et exploits.
Pour cela, il compare le **hash MD5** des fichiers importants avec les hash connus, qui sont accessibles à partir d'une base de données en ligne.
Ainsi, il peut détecter les répertoires généralement utilisés par les **rootkit** :

- les permissions anormales,
- les fichiers cachés,
- les chaînes suspectes dans le kernel

et peut effectuer des tests spécifiques à Linux et FreeBSD.

Rappelons cependant qu'en 2004, des chercheurs chinois, Xiaoyun Wang, Dengguo Feng, Xuejia Lai et Hongbo Yu, ont démontré qu'on pouvait créer des fichiers distincts de même signature MD5 en raison d'une propriété d'invariance mathématique de ce procédé.

source : Wikipedia

Installation

Facile :

```
apt-get update && apt-get install rkhunter
```

Utilisation

L'utilisation de Rkhunter est très simple.

D'abord faire une mise à jour:

```
rkhunter --update
```

Puis passer tout votre système en revue:

```
rkhunter -c
```

ou

```
rkhunter --check
```

Et voilà.

warning

Afin de limiter le nombre des Warnings, utilisez la commande suivante :

```
rkhunter --propupd
```

Merci **Coconuts** *!* 😀

Liens utiles

Il y a aussi de quoi lire ici :

- http://www.aldeid.com/wiki/Rkhunter
- http://sourceforge.net/apps/trac/rkhunter/wiki/SPRKH (en anglais)
- Ici pour le paragraphe concernant les faux-positifs https://doc.ubuntu-fr.org/rkhunter
- Les malwares - Généralités
- Les logiciels malveillants sous Linux

Avec l'aide avisée de ce vieux brigand de rtfm33 !

1)
N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !