Chkrootkit

- Objet : Chkrootkit, installation, utilisation
- Niveau requis :
  débutant, avisé
- Commentaires : *détecter si un système UNIX n'a pas été compromis par un rootkit*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !
- Suivi :
  - Création par gutts le 12/11/2009
  - Testé par Ir0nsh007er le 21/05/2015
  - * Commentaires sur le forum : C'est ici[1)]

Introduction

Chkrootkit est un logiciel libre sous licence GNU GPL permettant de détecter si un système **UNIX** n'a pas été compromis par un **rootkit**.
Il permet de détecter les traces d'une attaque et de rechercher la présence d'un **rootkit** sur un système Unix/Linux en vérifiant les quelques points suivants :

- si des fichiers exécutables du système ont été modifiés ;
- si la carte réseau est en mode « **promiscuous** » ;
- si un ou des **vers LKM** (*Loadable Kernel Module*) sont présents.

Veuillez vous rendre sur la page d'accueil du projet pour prendre connaissance des types de rootkits identifiables par chkrootkit.

promiscuous

La vérification effectuée au sujet du mode **promiscuous** consiste à voir si la carte réseau est configurée pour récupérer et lire toutes les trames, indiquant la possibilité qu'un **sniffer** soit installé sur le système.

rootkit

La définition exacte de **rootkit** donnée par Le Jargon Français est :

- « ensemble d'exploits réunis afin d'avoir des chances maximales de piquer un compte root (administrateur), c'est-à-dire avec lequel on peut faire n'importe quoi) sur une machine **Unix**. »

source : Wikipedia

Veuillez noter que chkrootkit ne détecte pas les intrusions, ne garantissant donc pas que le système ne soit pas compromis. En plus d'exécuter chkrootkit, d'autres tests

plus spécifiques devraient toujours être réalisés.

Installation

Rien de plus simple :

```
apt-get update && apt-get install chkrootkit
```

Méthode déconseillée

Téléchargement

Ou via les sources (on considère que le répertoire d'extraction est chkrootkit) :

```
cd /tmp
```

```
wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz
```

```
tar xzfv chkrootkit.tar.gz
```

Installation

```
cd chkrootkit
```

```
make sense
```

```
cd ..
```

```
mv chkrootkit /usr/local/bin/
```

```
ln -sfv /usr/local/bin/chkrootkit/chkrootkit /usr/bin/
```

Utilisation

Le lancement se fait en superutilisateur car nous avons besoin des accès aux fichiers système :

```
/usr/sbin/chkrootkit
```

Résultat

Liens divers

- Les malwares - Généralités
- Les logiciels malveillants sous Linux

1)

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