Scan contre les webshells

Certaines failles d'applications web peuvent permettre à quelqu'un de motivé d'injecter un fichier sur votre serveur, de type webshell, c99, r57, ou autre outil de script kiddies. Ces scripts permettent de gagner le contrôle total d'un serveur et sont donc à détecter au plus vite.

Linux Malware Detector permet de scanner à la recherche de ces scripts.

Installation

```
# Téléchargement
wget http://www.rfxn.com/downloads/maldetect-current.tar.gz

# Extraction
tar -zxvf maldetect-current.tar.gz

# Changer de dossier pour la copie extraite
cd maldetect-1.5

# Installation
./install.sh
```

Configuration

La configuration peut être changée dans le fichier `/usr/local/maldetect/conf.maldet`.

Utilisation

```
# Mise à jour de Malware Detector
maldet -d

# Mise à jour des définitions
maldet -u

# Scan complet d'un dossier
maldet -a /tmp

# Scan des fichiers modifiés des 2 derniers jours sur un dossier
maldet -r /tmp 2
```

```
# Aide complète
maldet -h
```

Moteur ClamAV

Le scan est assez long de base avec Malware Detector. Mais le moteur de ClamAV peut être utilisé si installé, pour un scan plus rapide.

Installer clamav :

```
apt install clamav
```

Vérifier dans le fichier de configuration que la ligne suivante est correcte. Elle doit être présente avec cette valeur par défaut :

```
clamav_scan=1
```

Source 1 - Source 2 - Source 3