

Installer et configurer Rootkit-Hunter

- **Ressources :**

- [Rkhunter - Wiki Ubuntu](#)
- [Rkhunter : paramètre WEB_CMD invalide](#)

- **Notes :**

- Fichiers de config : `/etc/rkhunter.conf` et `/etc/default/rkhunter`
- Fichier de log : `/var/log/rkhunter.log`

Installation de RKHunter

- Installer le paquet : `aptitude install rkhunter`
- Indiquer les options du Cron de Rkhunter, en éditant : `vi /etc/default/rkhunter`

[/etc/default/rkhunter](#)

```
CRON_DAILY_RUN="yes"
CRON_DB_UPDATE="yes"
DB_UPDATE_EMAIL="yes"
REPORT_EMAIL="admins@<domaine-sinp>"
```

- Indiquer les faux positifs, en éditant le fichier de config : `vi /etc/rkhunter.conf`

[/etc/rkhunter.conf](#)

```
# Config permettant la mise à jour pour éviter l'erreur :
# Invalid WEB_CMD configuration option: Relative pathname:
"/bin/false"
UPDATE_MIRRORS=1
MIRRORS_MODE=0
WEB_CMD=""

# Gestion des emails
MAIL-ON-WARNING=admins@<domaine-sinp>
MAIL_CMD=mail -s "[rkhunter] Avertissements sur ${HOST_NAME}" -r
mailer@<domaine-sinp>

# Option évitant les faux positifs en se basant sur Dpkg
# ATTENTION : lancer 'rkhunter --propupd' après avoir modifier
cet option !
PKG_MGR=DPKG

# Corriger l'emplacement des scripts suivant (/usr/bin/ au lieu de
/bin) :
SCRIPT_WHITELIST=/usr/bin/egrep
SCRIPT_WHITELIST=/usr/bin/fgrep
SCRIPT_WHITELIST=/usr/bin/which
```

```
# Désactiver les faux positifs sur db-srv
ALLOWDEVFILE="/dev/shm/PostgreSQL.*"

# Exemples de faux positifs à désactiver :
ALLOWHIDDENDIR="/dev/.udev"
ALLOWHIDDENDIR="/dev/.static"
ALLOWDEVFILE="/dev/.udev/rules.d/root.rules"
```

- **ATTENTION** : suite à l'installation et configuration de Rkhunter, il est nécessaire de lancer la commande suivante (⇒ indique à Rkhunter que tout est OK) : `rkhunter --propupd`

Envoi d'email via relai SMTP Google

Lors des tests, pour permettre l'envoi correcte d'email depuis un relai SMTP Google :

- Ajouter au fichier de conf `/etc/default/rkhunter`, une nouvelle ligne pour définir l'entête "FROM" d'envoi avec `sendmail` :

```
REPORT_EMAIL_FROM="mailer@cbn-alpin.fr"
```

- Ensuite éditer le script Rkhunter qui vérifie la base de données et sa mise à jour : `vi /etc/cron.weekly/rkhunter` et ajouter après chaque indication de `/usr/bin/sendmail` :

```
-f $REPORT_EMAIL_FROM
```

Pour la mise en prod, remplacer simplement l'email de la conf par : `mailer@<domaine-sinp>`

Utilisation et commandes

- Vérifier dernière version : `rkhunter --versioncheck`
- Mettre à jour le programme : `rkhunter --update`
- Lister les différents tests effectués : `rkhunter --list`
- **ATTENTION** : suite à l'installation et configuration de Rkhunter, il est nécessaire de lancer la commande suivante (⇒ indique à Rkhunter que tout est OK) : `rkhunter --propupd`
- Effectuer une vérification : `rkhunter --checkall`
- Vérification avec juste les alertes importantes : `rkhunter -c --rwo`
- Tester uniquement les *malwares* : `rkhunter -c -sk --enable malware`
- Accéder aux logs de RkHunter : `vi /var/log/rkhunter.log`

Avertissements Rkhunter

Suite à mise à jour des paquets

- Lorsqu'on réalise une mise à jour des paquets systèmes, il se peut que Rkhunter signale qu'un

logiciel à sa signature modifiée. Ex. :

```
Warning: The file properties have changed:
File: /usr/bin/curl
Current inode: 14563      Stored inode: 8252
Current file modification time: 1582383706 (22-févr.-2020
16:01:46)
Stored file modification time : 1560536612 (14-juin-2019
20:23:32)
```

- Dans ce cas là, relever la date de la nouvelle version du binaire et se rendre sur le site suivant : <https://www.debian.org/distrib/packages>
 - Chercher le paquet Debian correspondant et vérifier la date de la dernière version publiée du paquet en question
 - Utiliser le moteur de recherche situé en bas de page permettant de rechercher un nom de fichier présent dans un paquet.
 - Sur la page du paquet :
 - sélectionner votre version de Debian.
 - Pour vérifier la date, cliquer dans le menu de droite sur le lien "**Journal des modifications Debian**". Le changelog du paquet s'affiche et contient la date de la dernière modification.
- Si les 2 dates correspondent, le message d'avertissement de Rkhunter est à ignorer.
- Il faut tout de même :
 - Se connecter sur le serveur
 - Lancer la commande de vérification (par acquis de conscience) : `rkhunter --checkall`
 - Si tout semble conforme, indiquer à Rkhunter de considérer les changements comme normaux : `rkhunter --propupd`
- **NOTE** : pour que Rkhunter lancer automatiquement `rkhunter --propupd` après une mise à jour des paquets, mettre `APT_AUTOGEN="yes"` dans le fichier `/etc/default/rkhunter`.

Avertissement "Spam tool component"

- Apparemment un faux positif lié aux services tournant dans des containers Docker : <https://sourceforge.net/p/rkhunter/bugs/172/>
- Pas de solution pour l'instant pour le mettre dans une whitelist.
- Si le problème persiste, une alternative intéressante à RKHunter est [Lynix](#) (à tester).

From:
<https://wiki-sinp.cbn-alpin.fr/> - **CBNA SINP**

Permanent link:
<https://wiki-sinp.cbn-alpin.fr/serveurs/installation/rkhunter?rev=1671268435>

Last update: **2022/12/17 09:13**

