

Table des matières

- RKHUNTER (RootKit Analysis Tools) 2**
- Installation* 2
- Modification Conf* 2
- Check Version* 2
- Check Update* 2
- Générer une base de référence* 3
- Exécution de RKHunter* 4
- Whitelist* 5
- Log* 6



RKHUNTER (RootKit Analysis Tools)

Installation

```
sudo apt install rkhunter
```

Modification Conf

Après l'installation, il vous sera nécessaire de modifier la configuration présente dans le fichier *rkhunter.conf* afin de vous permettre de mettre à jour les définitions.

```
nano /etc/rkhunter.conf
UPDATE_MIRRORS=0 ---> UPDATE_MIRRORS=1
MIRRORS_MODE=1 ---> MIRRORS_MODE=0
WEB_CMD="/bin/false" ---> WEB_CMD=""
```

Check Version

Une fois installé, il est important de vérifier que RKHunter fonctionne correctement. Tapez la commande suivante pour afficher la version installée :

```
sudo rkhunter --versioncheck
```

```
[ Rootkit Hunter version 1.4.6 ]
Checking rkhunter version.. pour faire les Maj des déf
This version is: 1.4.6
Latest version: 1.4.6 ---> UPDATE_MIRRORS=1
```

Check Update

Après l'installation, la première chose à faire est de mettre à jour les bases de données de RKHunter, qui contiennent les signatures de rootkits et autres anomalies :

```
sudo rkhunter --update
```

```
[ Rootkit Hunter version 1.4.6 ]
Checking rkhunter data files...
Checking file mirrors.dat [ Updated ]
Checking file programs_bad.dat [ No update ]
Checking file backdoorports.dat [ No update ]
Checking file suspscan.dat [ No update ]
Checking file i18n/cn [ Skipped ]
Checking file i18n/de [ Skipped ]
Checking file i18n/en [ No update ]
Checking file i18n/tr [ Skipped ]
Checking file i18n/tr.utf8 [ Skipped ]
Checking file i18n/zh [ Skipped ]
Checking file i18n/zh.utf8 [ Skipped ]
Checking file i18n/ja [ Skipped ]
```

Générer une base de référence

Pour permettre à RKHunter de détecter les modifications des fichiers système, vous devez générer un fichier de référence. Cela crée une base de données contenant les propriétés actuelles des fichiers critiques.

```
rkhunter --propupd
```

```
[ Rootkit Hunter version 1.4.6 ]
File created: searched for 179 files, found 145
```

Le fichier principal de configuration, /etc/rkhunter.conf, contient des options qui permettent d'adapter le comportement de l'outil à vos besoins.

Voici quelques paramètres :

```
UPDATE_MIRRORS=1
    Active les mises à jour automatiques des miroirs.
DB_UPDATE=1
    Permet de mettre à jour la base de données utilisée pour les
vérifications.
ALLOWHIDDENDIR=/chemin/vers/repertoire
    Autorise un répertoire caché spécifique (exemple : /etc/.java).
ALLOWHIDDENFILE=/chemin/vers/fichier
    Autorise un fichier caché spécifique (exemple : /etc/.myconfig).
SCRIPTWHITELIST=/chemin/vers/script
    Ajoute un script à la liste blanche pour éviter les alertes (exemple :
/usr/bin/which).
DISABLE_TESTS=<liste_de_tests>
    Désactive certains tests spécifiques, comme suspscan (analyse des
fichiers suspects).
PORT_WHITELIST="22 80 443"
    Spécifie les ports réseau à autoriser, pour éviter des avertissements
```

inutiles.

```
ALLOW_SSH_ROOT_USER=0
```

Signale si l'utilisateur root est autorisé à se connecter via SSH.

```
ALLOW_SSH_PROT_V1=0
```

Désactive les alertes si le protocole SSH v1 est utilisé.

Exécution de RKHunter

maintenant que RKHunter est installé et mis à jour, il est temps de le mettre au travail. Je vais vous montrer comment utiliser cet outil pour analyser votre système et interpréter ses résultats.

La commande la plus courante pour utiliser RKHunter est :

```
sudo rkhunter --check
```

Cette commande effectue une vérification complète de votre système. Voici ce qui se passe :

1. Examen des fichiers système critiques, comme /etc/passwd et /etc/shadow.
2. Recherche de rootkits connus.
3. Recherche de Malware
4. Vérification des permissions des fichiers importants.
5. Analyse des ports réseau ouverts pour détecter des comportements suspects.

Exemple:

```
Checking system commands...

Performing 'strings' command checks
Checking 'strings' command           [ OK ]

Performing 'shared libraries' checks
Checking for preloading variables    [ None found ]
Checking for preloaded libraries     [ Warning ]
Checking LD_LIBRARY_PATH variable    [ Not found ]

Performing file properties checks
Checking for prerequisites           [ OK ]
/usr/sbin/adduser                    [ OK ]
/usr/sbin/chroot                     [ OK ]
/usr/sbin/cron                       [ OK ]
/usr/sbin/groupadd                   [ OK ]
/usr/sbin/groupdel                   [ OK ]
/usr/sbin/groupmod                   [ OK ]
/usr/sbin/grpck                      [ OK ]
/usr/sbin/nologin                    [ OK ]
/usr/sbin/pwck                       [ OK ]
```

```
Checking for rootkits...

Performing check of known rootkit files and directories
55808 Trojan - Variant A           [ Not found ]
ADM Worm                           [ Not found ]
AjaKit Rootkit                     [ Not found ]
Adore Rootkit                       [ Not found ]
aPa Kit                             [ Not found ]
Apache Worm                         [ Not found ]
Ambient (ark) Rootkit              [ Not found ]
Balaur Rootkit                     [ Not found ]
BeastKit Rootkit                   [ Not found ]
beX2 Rootkit                       [ Not found ]
BOBKit Rootkit                     [ Not found ]
cb Rootkit                         [ Not found ]
CiNIK Worm (Slapper.B variant)     [ Not found ]
```

Pendant l'analyse, vous verrez des messages détaillés apparaître à l'écran. Chaque vérification est marquée comme :

- [OK] si tout est normal.
- [Warning] si quelque chose semble suspect.

Lorsque RKHunter détecte un problème potentiel, il vous le signale avec un avertissement. Pour réduire le nombre d'avertissements non pertinents (faux positifs), vous pouvez utiliser l'option suivante lors de l'analyse :

```
sudo rkhunter --report-warnings-only --check
```

Whitelist

Editer le fichier de conf rkhunter.conf dans /etc

```
sudo nano /etc/rkhunter.conf
```

Il vous sera possible d'ajouter des whitelist pour les Scripts, Fichiers cachés, attribut spécifique immuabilité, etc..

```
#
# Allow the specified hidden directory to be whitelisted.
#
# This option may be specified more than once, and may use wildcard characters.
#
# The default value is the null string.
#
#ALLOWHIDDENDIR=/etc/.java
#ALLOWHIDDENDIR=/etc/.git
#ALLOWHIDDENDIR=/dev/.lxc
ALLOWHIDDENDIR=/etc/.updated
```

```
#
# Allow the specified file to be a script.
#
# This option may be specified more than once, and may use wildcard characters.
#
# The default value is the null string.
#
SCRIPTWHITELIST=/usr/bin/egrep
SCRIPTWHITELIST=/usr/bin/fgrep
SCRIPTWHITELIST=/usr/bin/which
SCRIPTWHITELIST=/usr/bin/ldd
SCRIPTWHITELIST=/usr/bin/lwp-request
SCRIPTWHITELIST=/usr/bin/which.debianutils
SCRIPTWHITELIST=/usr/sbin/adduser
#SCRIPTWHITELIST=/usr/sbin/prelink
#SCRIPTWHITELIST=/usr/sbin/unhide.rb
```

Log

Les log issues des scans opér  par RKHunter sont dans /var/log

```
sudo cat /var/log/rkhunter.log
```

```
System checks summary
=====

File properties checks...
  Files checked: 143
  Suspect files: 1

Rootkit checks...
  Rootkits checked : 477
  Possible rootkits: 0

Applications checks...
  All checks skipped

The system checks took: 2 minutes and 51 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

From:
<https://wiki.mazinger.fr/wiki/> - My Personal Wiki

Permanent link:
<https://wiki.mazinger.fr/wiki/doku.php?id=securite:system:rkhunter:index>

Last update: **2025/08/20 19:48**



