# Détection de rootkit avec rkhunter

## Installation de rkhunter

Sur Debian et ses dérivés …  
**>> sudo apt install rkhunter**

On effectue une **copie de sauvegarde du fichier de configuration** …  
**>>** **sudo cp --preserve /etc/default/rkhunter /etc/default/rkhunter-Copie-$(date +"%Y%m%d%H%M%S")**

Le **fichier de configuration de rkhunter est /etc/rkhunter.conf**.   
Au lieu d'y apporter des modifications, on peut **créer et utiliser le fichier /etc/rkhunter.conf.local** …  
**>>** **sudo cp --preserve /etc/rkhunter.conf /etc/rkhunter.conf.local**

On parcoure le **fichier de configuration /etc/rkhunter.conf.local** et on **définit ses besoins** …

|  |  |
| --- | --- |
| Directive | Remarque |
| UPDATE\_MIRRORS=1 |  |
| MIRRORS\_MODE=0 |  |
| MAIL-ON-WARNING=root |  |
| COPY\_LOG\_ON\_ERROR=1 | Enregistrement d’une copie du journal en cas d'erreur |
| PKGMGR=... | Valeur appropriée par la documentation |
| PHALANX2\_DIRTEST=1 |  |
| WEB\_CMD="" | Résolution d’un problème avec le paquet Debian qui désactive la possibilité pour rkhunter de se mettre à jour automatiquement |
| USE\_LOCKING=1 | Évitement des problèmes avec rkhunter s'exécutant plusieurs fois |
| SHOW\_SUMMARY\_WARNINGS\_NUMBER=1 | Affichage voir du nombre réel d'avertissements trouvés |

Sur le système basé sur Debian, **rkhunter est fourni avec des scripts cron**.   
Pour les activer …  
**>>** **sudo dpkg-reconfigure rkhunter**On doit **répondre oui à toutes les questions**.

Une fois que l'on a **complété toutes les modifications**, on doit **s’assurer que tous les paramètres sont valides** …  
**>>** **sudo rkhunter -C**

**Remarque** …  
Si la **sortie retourne** …  
Invalid WEB\_CMD configuration option: Relative pathname: "/bin/false"  
il est conseiller de **modifier les paramètres du fichier /etc/rkhunter.conf.local** …  
**MIRRORS\_MODE=1 ---> MIRRORS\_MODE=0  
UPDATE\_MIRRORS=0 ---> UPDATE\_MIRRORS=1  
WEB\_CMD="/bin/false" ---> WEB\_CMD=""**

Pour **mettre à jour rkhunter et sa base de données** …  
**>>** **sudo rkhunter --versioncheck  
[ Rootkit Hunter version 1.4.6 ]   
Checking rkhunter version...  
 This version : 1.4.6  
 Latest version: 1.4.6**

Pour **mettre à jour la base de données** …  
**>>** **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 ]**

Pour la **mise à jour de toute la base de données** des propriétés du fichier …  
**>>** **sudo rkhunter --propupd  
[ Rootkit Hunter version 1.4.6 ]  
File updated: searched for 181 files, found 144**

Si on souhaite **effectuer une analyse manuelle et voir le résultat** …  
**>>** **sudo rkhunter --check  
[ Rootkit Hunter version 1.4.6 ]**

**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 [ None found ]  
 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/depmod [ OK ]  
 /usr/sbin/fsck  
…  
 /usr/bin/whatis [ OK ]  
 /usr/bin/whereis [ OK ]  
 /usr/bin/which [ Warning ]  
 /usr/bin/who [ OK ]  
 /usr/bin/whoami [ OK ]  
 /usr/bin/numfmt [ OK ]  
 /usr/bin/kmod [ OK ]  
 /usr/bin/systemd [ OK ]  
 /usr/bin/systemctl [ OK ]  
 /usr/bin/mawk [ OK ]  
…  
  
[Press <ENTER> to continue]  
  
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 ]  
…  
 Volc Rootkit [ Not found ]  
 Xzibit Rootkit [ Not found ]  
 zaRwT.KiT Rootkit [ Not found ]  
 ZK Rootkit [ Not found ]  
  
[Press <ENTER> to continue]  
…  
  
System checks summary  
=====================   
File properties checks...  
 Files checked: 144  
 Suspect files: 3   
Rootkit checks...  
 Rootkits checked : 500  
 Possible rootkits: 0  
   
Applications checks...  
 All checks skipped**

**The system checks took: 4 minutes and 20 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)**