Installation rkhunter / ClanAv

MELNOTTE Hugo
BTS SIO

Installation rkhunter

Rkhunter est un programme Unix qui permet de détecter les rootkits.

Installer rkhunter.
rkhunter –update

```
...
Traitement des actions différées (« triggers ») pour rkhunter (1.4.6-9
[ Rootkit Hunter version 1.4.6 ]
File updated: searched for 179 files, found 139
root@DEBIAN-WEB-HOME:~# rkhunter --update
```

Voici la commande pour lancer un scan :
rkhunter -c

```
root@DEBIAN-WEB-HOME:~# rkhunter -c
```

```
System checks summary
=====================

File properties checks...
    Files checked: 139
    Suspect files: 0

Rootkit checks...
    Rootkits checked : 495
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 1 minute and 50 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)

root@DEBIAN-WEB-HOME:~#
```

On peut voir un warning mais c'est rkhunter.

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

Installation de ClanAv

Clanav est un antivirus gratuit.

Installez le paquet clanav.
apt-get install clanav
Si vous faites une mise à jour, il faut arrêter le programme.
service clamav-freshclam stop

```
root@DEBIAN-WEB-HOME:~# apt install clamav
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
clamav est déjà la version la plus récente (0.103.3+dfsg-0+deb11u1).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessair
es :
  libevent-2.1-7 libgnutls-dane0 libunbound8
Veuillez utiliser « apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@DEBIAN-WEB-HOME:~# cd /var/clamav
-bash: cd: /var/clamav: Aucun fichier ou dossier de ce type
root@DEBIAN-WEB-HOME:~# freshclam
ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.l
og).
ERROR: initialize: libfreshclam init failed.
ERROR: Initialization error!
root@DEBIAN-WEB-HOME:~# service clamav-freshclam stop
```

Voici la commande pour effectuer la mise à jour.
freshclam
Puis redémarrez le service :
service clamav-freshclam start

```
pgrading-clamav
Sun Nov 21 22:16:51 2021 -> daily database available for update (local version:
26359, remote version: 26360)
Current database is 1 version behind.
Downloading database patch # 26360...
Time:    0.4s, ETA:    0.0s [========================>]    5.87KiB/5.87KiB
Sun Nov 21 22:16:54 2021 -> Testing database: '/var/lib/clamav/tmp.6a5eabd758/cl
amav-35463c26cf66a488a9cde22a684cc231.tmp-daily.cld' ...
Sun Nov 21 22:17:03 2021 -> Database test passed.
Sun Nov 21 22:17:03 2021 -> daily.cld updated (version: 26360, sigs: 1946870, f-
level: 90, builder: raynman)
Sun Nov 21 22:17:03 2021 -> main.cvd database is up-to-date (version: 62, sigs:
6647427, f-level: 90, builder: sigmgr)
Sun Nov 21 22:17:03 2021 -> bytecode.cvd database is up-to-date (version: 333, s
igs: 92, f-level: 63, builder: awillia2)
Sun Nov 21 22:17:03 2021 -> !NotifyClamd: Can't find or parse configuration file
 /etc/clamav/clamd.conf
root@DEBIAN-WEB-HOME:~# service clamav-freshclam start
```

Il ya beaucoup de possibilité avec ce programme, j'ai décidé de lancer un scan complet du disque : *clanscan -r /*

```
root@DEBIAN-WEB-HOME:~# service clamav-freshclam st
root@DEBIAN-WEB-HOME:~# clamscan -r /
```

Il y Clanav a détecté des erreurs mais aucun fichier infecté.

```
----------- SCAN SUMMARY -----------
Known viruses: 8579047
Engine version: 0.103.3
Scanned directories: 13455
Scanned files: 44796
Infected files: 0
Total errors: 11177
Data scanned: 3278.15 MB
Data read: 2648.01 MB (ratio 1.24:1)
Time: 1479.194 sec (24 m 39 s)
Start Date: 2021:11:21 22:20:30
End Date:   2021:11:21 22:45:09
root@DEBIAN-WEB-HOME:~#
```

Source

Rkhunter : https://debian-facile.org/doc:systeme:rkhunter
Clanav : https://debian-facile.org/doc:systeme:clamav