Mise en place de l'antivirus CLAMAV

Installation de Clamav

De façon à bénéficier des dernières versions de clamav, il est vivement conseillé d'utiliser les dépôts Debian Volatile, dans votre **/etc/apt/sources.list** :

```
deb http://volatile.debian.org/debian-volatile lenny/volatile main contrib non-free
deb-src http://volatile.debian.org/debian-volatile lenny/volatile main contrib non-free
```

On installe donc clamav :

```
# apt-get install clamav clamav-daemon libclamav-dev clamav-freshclam clamtk
```

Par défaut clamav est en écoute sur un socket Unix, cependant notre configuration fait en sorte que la connexion des utilisateurs via FTP est chrootée, ce qui veut dire que l'environnement de l'utilisateur ne "verra" pas le socket Unix, il faut donc faire écouter clamav sur un port TCP "classique", on reconfigure donc clamav en choisissant TCP et en faisant "écouter" clamav sur l'adresse locale, pour le reste je vous laisse aviser des différents paramètres pour votre installation :

```
# dpkg-reconfigure clamav-base
```

profitons-en aussi pour configurer freshclam :

```
# dpkg-reconfigure clamav-freshclam
```

Enfin on redémarre les démons clamav :

```
# /etc/init.d/clamav-daemon restart
# /etc/init.d/clamav-freshclam restart
```

Utilisation

Action	Commande
Mise à jour des définitions anti-virus	sudo freshclam
Scanner les fichiers du dossier personnel	sudo clamscan
Scanner tous les fichiers du dossier personnel	sudo clamscan -r /home/utilisateur
Scanner le disque dur entier	sudo clamscan -r /
Scanner une partition Windows (Fat 32), montée en "/mnt/D" avec signal sonore. Affichage si virus et écriture dans virus.log	sudo clamscan --bell -r -i --log=/var/log/clamav/virus.log /mnt/D/

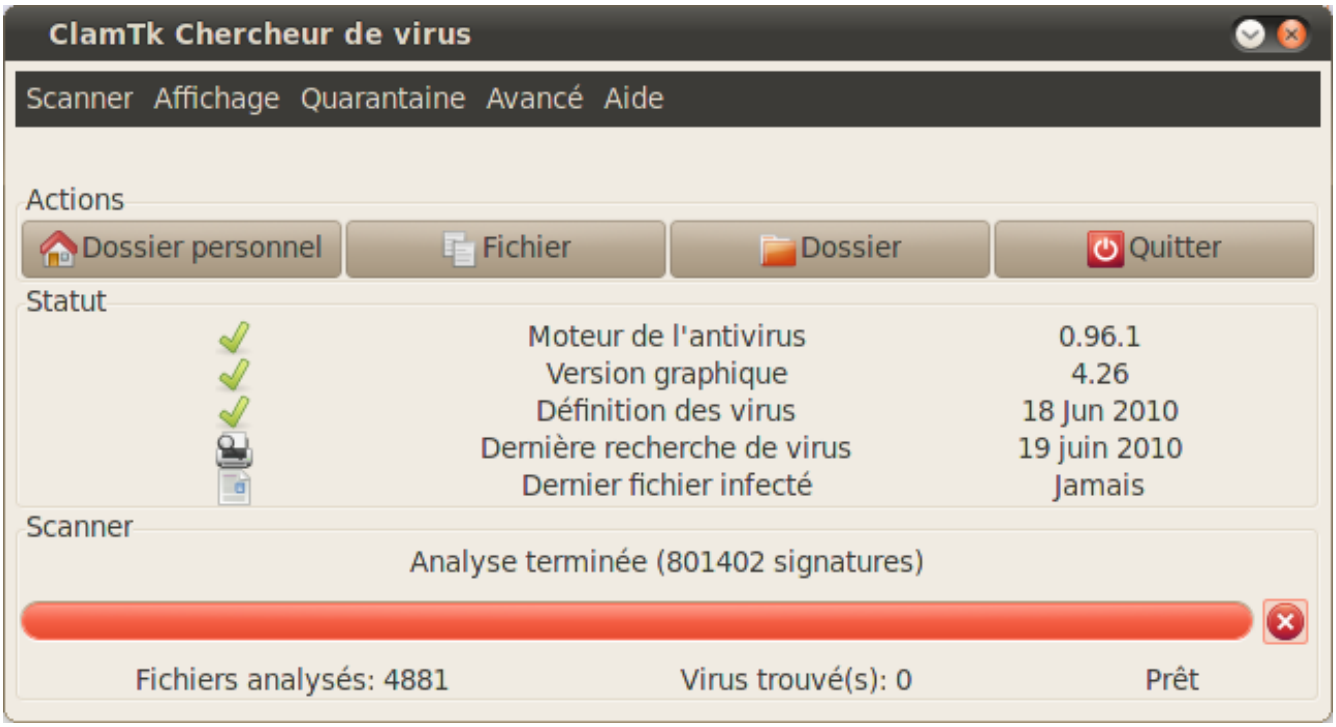
Paramètres

Paramètre	Signification
--help (-h)	Affiche les différents paramètres (anglais)
--version (-V)	Affiche le numéro de version
--verbose (-v)	Rend le programme plutôt bavard
--debug	Affiche les informations de débugage (libclamav)
--quiet	Affiche seulement les messages d'erreur
--stdout	Sortie vers stdout au lieu de stderr
--no-summary	Désactive l'affichage du rapport à la fin du scan
--infected (-i)	Affiche uniquement les fichiers infectés
--bell	Emet un son lors de la détection d'un virus
--tempdir=REPERTOIRE	Crée les fichiers temporaires dans REPERTOIRE
--leave-temps	Ne supprime pas les fichiers temporaires
--database=FICHER/REPERTOIRE (-d FICHIER/REPERTOIRE)	Charge la base de données des virus à partir de FICHIER ou charge tous les fichiers *.cvd et *.db[2] à partir de REPERTOIRE
--log=FICHIER (-l FICHIER)	Enregistre le fichier log (rapport) dans FICHIER
--recursive (-r)	Scanne les sous-dossiers récursivement
--remove	Supprime les fichiers infectés : **ATTENTION !**
--move=REPERTOIRE	Déplace les fichiers infectés dans REPERTOIRE
--exclude=REGEX	Ne scanne pas les fichiers correspondants à l'expression régulière REGEX
--exclude-dir=REGEX	Ne scanne pas les répertoires correspondants à l'expression régulière REGEX
--include=REGEX	Scanne uniquement les fichiers correspondants à l'expression régulière REGEX
--include-dir=REGEX	Scanne uniquement les dossiers correspondants à l'expression régulière REGEX
--no-mail	Désactive l'analyse e-mail
--no-pe	Désactive l'analyse PE
--no-ole2	Désactive l'analyse OLE2
--no-html	Désactive l'analyse HTML
--no-archive	Désactive l'analyse des archives
--detect-broken	Essaie de détecter les exécutables corrompus
--block-encrypted	Bloque les archives cryptées
--block-max	Bloque les archives excédant la taille limite
--mail-follow-urls	Télécharge et analyse les URLs (adresses internet)
--max-space=#n	Extraire uniquement les #n premiers kilo-octets des fichiers archivés
--max-files=#n	Extraire uniquement les #n premiers fichiers des archives
--max-ratio=#n	Taux de compression maximum pour les archives
--unzip[=LOGICIEL_DE_DECOMPRESSION]	Active le support pour les archives *.zip
--unrar[=LOGICIEL_DE_DECOMPRESSION]	Active le support pour les archives *.rar
--arj[=LOGICIEL_DE_DECOMPRESSION]	Active le support pour les archives *.arj

--unzoo[=LOGICIEL_DE_DECOMPRESSION] Active le support pour les archives *.zoo
--lha[=LOGICIEL_DE_DECOMPRESSION] Active le support pour les archives *.lha
--jar[=LOGICIEL_DE_DECOMPRESSION] Active le support pour les archives *.jar
--tar[=LOGICIEL_DE_DECOMPRESSION] Active le support pour les archives *.tar
--deb[=LOGICIEL_DE_DECOMPRESSION] Active le support pour les archives *.deb
--tgz[=LOGICIEL_DE_DECOMPRESSION] Active le support pour les archives *.tar.gz et *.tgz

Utilisation d'une interface graphique

Lancer l'interface en root « sudo clamtk »



Pour que les signatures de virus soient prises en compte, redémarrez l'ordinateur. Seule la commande "Recursive Scan" examine tous les fichiers d'un dossier, sous-dossiers inclus.