Titre de Votre Tuto

- Objet : “Scannage” automatique des fichiers téléchargés
- Niveau requis : Fix Me!
  débutant, avisé
- Commentaires : logiciels utilisés: clamav, inotify, systemd, xmessage
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !.

Introduction

Installez clamav

Installation

apt install clamav libnotify

Vérifier si à l'installation clamav a bien créer son utilisateur et son groupe:

```
grep clamav /etc/passwd /etc/group
```

```
/etc/passwd:clamav:x:119:126::/var/lib/clamav:/bin/false
/etc/group:clamav:x:126:
```

clamav doit pouvoir télécharger les signatures de virus dans le dossier /var/lib/clamav, il faut vérifier les identifiant numériques de l'utilisateur et du groupe propriétaire de ce dossier:

```
ls -ldn /var/lib/clamav
```

```
drwxr-xr-x 2 119 126 4096 mars  14 16:12 /var/lib/clamav
```

Créer ensuite le groupe puis l'utilisateur en utilisant les identifiants numériques repérés à l'aide de la commande précédente:

```
groupadd -g 126
useradd -g clamav -u 119 clamav
```

Pour faire fonctionner clamd en tache de fond nous avons besoin d'activer les services au démarrage en utilisant systemd avec la commande systemctl.

Avant de de procéder à l'activation il faut vérifier si celui ci ne pose pas de probléme avec l'option start:

```
systemctl start clamd
```

Si aucun probléme n'est rencontré, on peu activer le service pour chaque démarage:

systemctl enable clamtruc

Pour la mise à jour des signatures de virus il faut créer un nouveau service pour systemd. Pour cela il faut créer le fichier /usr/lib/system/clam-freshclam.service

```
nano /usr/lib/system/clam-freshclam.service
```

```
[Unit]
Description = freschclam (clamav virus database updater)
After = network.target
[Service]
Type = forking
ExecStart = /usr/bin/freshclam -d -c 6
Restart = on-failure

[Install]
WantedBy=multi-user.target
```

Puis on active le nouveau service:

```
systemctl start clam-freshclam
systemctl enable clam-freshclam
```

Il va faloir maintenant créer un script permettant de scanner un dossier (ici le dossier Téléchargement) d'alerter en cas de virus et de déplacer le fichier dans un autre dossier (quelquechose/infected)

clamav.sh

```
#!/bin/bash
while true: do
inotifywait -r -e close_write,moved_to --format %f Téléchargement/ |
      while read file; do
            if [ -f $file ]; then
            clamdscan --fdpass -1 --move $HOME/infected
$HOME/Téléchargement/$file;
                  if [ "$?" == "1" ]; then
                  notify-send "Virus détecté" "dans le fichier
'$file'"
--icon=dialog-warning
                        fi
            fi
      done
done
```

On fixe les droits sur le script pour qu'il soit exécutable

```
chmod +x /usr/local/bin/clamav.sh
```

Pour pouvoir faire exécuter le script à l'ouverture de session on va créer une nouvelle entrée dans autostart:

```
nano /etc/xdg/autostart/clamav.desktop
```

```
[Desktop Entry]
Type=Application
Name=Antivirus résident ClamaAV
Exec=/usr/local/bin/clamav.sh
```

Note perso: le daemon est dans clamav-daemon qui fournit un service pour systemd : clamav-daemon.service (merci enikar!)

Utilisation