SCANNER USB EN TEMPS RÉEL

Résumé :
résumé

Tom Barbarin-Costes

Table des matiér :

Introduction :

Pour des raisons de sécurité, vérifier les clés USB avant de les brancher sur un poste relié à un réseau sensible est une nécessité. Pour effectuer cette vérification, l'outil ClamAV sous Linux est une solution puissante, reconnue et Open Source.

Cependant, bien que cette solution soit efficace et fiable, elle n'est pas forcément accessible à tous dans sa forme native (ligne de commande). C'est pourquoi, dans cette documentation, nous allons voir comment automatiser les scans de ClamAV à l'aide d'un script développé en langage C.

Prérequis :

Pour réaliser cette documentation certain prérequis sont nécessaire :

- Un système d'exploitation sur une base Debian avec Bash
- Le compilateur GCC
- Un accès Sudo ou Root
- Une accès au terminal
- Un accès au réseau pour l'installation des outils *(temporaire)*
- Des ports USB stable

Installation des outils :

Installation des packets :

Pour commencer il faut installer l'outil principale de cette documentation, Clamav :

- **Sudo apt update && sudo apt upgrad**
- **sudo apt install clamav clamav-daemon -y**
- **sudo apt install build-essential**

Installation de la base de données Clamav :

Pour installer la base de données Clamav il y a deux solution dans deux contexte différent.

Premier cas :
votre réseau accés au serveur et base de données clamav :

1- Sudo systemctl stop clamav *(stop clamav)*

2- sudo freshclam *(met a jours la base de données)*

3- sudo systemctl start clamav *(rdemare clamav avec le nouvelle base de données)*

Pour vérifier si les fichier sont bien présent et mise a jour rendez vous dans le répertoire « **/var/lib/clamav** » , Ces fichier devrons être présent.

```
total 171124
drwxr-xr-x  2 clamav clamav     4096 janv. 16 09:37 .
drwxr-xr-x 75 root   root       4096 janv. 11 19:56 ..
-rw-r--r--  1 clamav clamav   281702 janv.  9 14:11 bytecode.cvd
-rw-r--r--  1 clamav clamav 85849088 janv. 16 09:37 daily.cld
-rw-r--r--  1 clamav clamav       90 janv.  9 14:10 freshclam.dat
-rw-r--r--  1 clamav clamav 89072577 janv.  9 14:11 main.cvd
```

Problème de mise a jour de la BDD :

Si les fichier de la base de données ne ce télécharge pas ou ne peuvent pas, c'est sûrement a cause de la configuration réseau, certificat SSL, requête HTTP. Cependant il est toujours possible de mettre a jour les base de données.

Pour faire cela rendez vous sur un Ordinateur disposant d'un accès a la base de données Clamav installer Clamav et Clamav-daemon puis copier sur une cle USB ou autre périphérique de transport de données les fichier dans « **/var/lib/clamav** » **NE PAS CRÉÉ DE SOUS REPERTOIRE.**

Instalation du Script :

Placez le répertoire dans « **/home/$user/KIOSQUE** ». Dans ce dossier, vous trouverez cette documentation, le fichier source en langage C, l'exécutable et un répertoire vide nommé « **log** ». Ne le supprimez pas : c'est dans ce répertoire que seront générés les fichiers de logs.

Le programme se lance avec la commande « **sudo ./usbscanner** ». L'usage de sudo est essentiel car les commandes utilisées dans le script nécessitent les droits d'administrateur. Sans cela, le programme ne fonctionnera pas correctement.

De plus, si vous modifiez le programme, n'oubliez pas de le compiler à nouveau avec la commande « **gcc usbscanner.c -o usbscanner** », sinon les modifications ne seront pas prises en compte.

Les fichiers de logs seront générés sous le format suivant :

Nom du fichier : *log.nom.prenom.txt*

Format du contenu :

==========
DATE DE DÉTECTION : jour/mois/année heure:minute:seconde
==========
utilisateur : nom prénom
Périphérique: /dev/nom_du_périphérique
Menaces : nombre_de_menaces
Action prise: FORMATAGE (OUI/NON)
