Antivirus & Scan

- Installation d'un antivirus Linux
- Scan avec ClamAV

Installation d'un antivirus Linux

Source : https://docs.clamav.net/

ClamAV

> ClamAV pour fournir des capacités de détection de logiciels malveillants

- ClamAV est conçu pour analyser les fichiers rapidement.
- Protection en temps réel (Linux uniquement). Le client ClamOnAcc pour le démon d'analyse ClamD fournit une analyse à l'accès sur les versions modernes de Linux. Cela inclut une capacité facultative permettant de bloquer l'accès aux fichiers jusqu'à ce qu'un fichier ait été analysé (prévention à l'accès).
- ClamAV détecte des millions de virus, vers, chevaux de Troie et autres logiciels malveillants, notamment les virus de macro Microsoft Office, les logiciels malveillants mobiles et d'autres menaces.
- L'environnement d'exécution de signature de bytecode de ClamAV, alimenté par LLVM ou notre interpréteur de bytecode personnalisé, permet aux rédacteurs de signatures ClamAV de créer et de distribuer des routines de détection très complexes et d'améliorer à distance les fonctionnalités du scanner.
- Les bases de données de signatures signées garantissent que ClamAV n'exécutera que des définitions de signature fiables.
- ClamAV analyse les archives et les fichiers compressés, mais protège également contre les attaques d'archives. Les fonctionnalités d'extraction d'archives

Installation

```
sudo apt install clamav clamav-daemon
```

Scan avec ClamAV

Réalisation d'un scan de fichier

Pour lancer un scan :

```
sudo clamscan -riz ~/
```

Une fois le scan terminé vous verrez la sortie suivante dans la console :

```
----------- SCAN SUMMARY -----------
Known viruses: 8700889
Engine version: 1.0.7
Scanned directories: 31368
Scanned files: 83205
Infected files: 0
Data scanned: 17940.34 MB
Data read: 84134.32 MB (ratio 0.21:1)
Time: 2464.550 sec (41 m 4 s)
Start Date: 2024:12:06 10:51:55
End Date:   2024:12:06 11:33:00
```

Si vous avez des fichiers corrompus il seront affiché au dessus du `SCAN SUMMARY` et dans le nombre `Infected files`