**Aujourd’hui, sur Linux, il existe très peu d’outils à la fois simples, complets et entièrement automatisés pour détecter efficacement les malwares.**

Les solutions actuelles ont plusieurs limites : configuration manuelle, un seul moteur de détection, peu de journalisation, ni prise en considération les ressources ,ni **planification automatique des**

Par exemple :

* **ClamAV** est limité seul à des signatures classiques,
* **YARA** nécessite une expertise technique
* **VirusTotal** requiert une intégration manuelle de l’API.

**Face à ces limites, nous avons développé LinAV**

* Le script commence par l’installation des dépendances (ClamAV, YARA, etc.), puis télécharge et compile les règles YARA depuis GitHub.
* Ensuite, la création des dossiers logs
* Puis on -r qui Réinitialise la configuration par défaut et nettoie les fichiers temporaires, tout en conservant les logs existants
* Et -m pour choisir le mode de scan

**Light :** Scan rapide, Il s'appuie sur plusieurs critères : l’extension , permissions, le contenu (présence de commandes suspectes) et eventiallement via l’API VirusTotal

* **Medium :** **analyse** sur un répertoire donné, en s’appuyant principalement sur **ClamAV**
* **Heavy :** Analyse de chaque fichier avec YARA, ClamAV et VirusTotal

Puis en choisit le mode d’éxécution

**Mode Séquentiel (par défaut)** : Analyse les fichiers un par un, idéal pour les petits volumes

**Mode Parallèle (fork)**

Utilise **GNU Parallel** pour exécuter plusieurs scans simultanément.

Optimise les performances sur les machines multi-cœurs.

Recommandé pour les analyses intensives.

**Option**-s**(Sous-shell)**

* Chaque fichier est analysé dans un **sous-shell isolé**
* Aucun partage de mémoire ou d’état entre les processus.

**Threads -t**

* Juste en simulation Le script démarre par exemple **4 sous-processus** en même temps
* Dès qu'un fichier est fini, xargs en lance un nouveau **immédiatement** pour garder toujours 4 scans actifs.

Pour la sortie

Dans le **mode léger**, les fichiers suspects sont automatiquement mis en quarantaine dans un dossier sécurisé en enlevant tout les droits

Le **mode intermédiaire** génère un rapport clair et structuré (au format JSON ou texte) résumant les fichiers analysés, les menaces détectées et les résultats des scans ClamAV, tout en conservant une trace dans les logs système.

Enfin, le **mode complet** génère un rapport exhaustif , puis envoie automatiquement une alerte par email en cas de menace critique,

Et pour ces trois modes on génère les logs en terminales

Et on a aussi **Cron qui permet d'automatiser l'exécution périodique selon une planification défini**

parallel est un outil en ligne de commande sous Linux (GNU Parallel) qui permet d’exécuter plusieurs tâches **en parallèle**