**ANEXO V**

**Práctica 5: Uso de ClamAV como antivirus en Linux.**

**Trabajo preparatorio**

* **Consultar que es antivirus, su funcionamiento, y las principales clases de amenazas como virus, malware, etc.**

Un antivirus es una herramienta informática creada para identificar, prevenir y eliminar programas maliciosos en los sistemas. Su función principal es salvaguardar los dispositivos frente a amenazas que puedan poner en riesgo su seguridad y afectar su rendimiento [55].

Los antivirus utilizan varios métodos para detectar y neutralizar amenazas:

* Detección Basada en Firmas: Comparan archivos y programas con una base de datos de firmas de malware conocidas. Cuando se identifica una coincidencia, el antivirus actúa para eliminar o aislar la amenaza.
* Análisis Heurístico: Examina los comportamientos y patrones inusuales en los programas, permitiendo identificar malware desconocido o nuevas variantes que aún no están registradas en la base de datos de firmas.
* Monitoreo en Tiempo Real: Supervisa continuamente el sistema para detectar y bloquear actividades maliciosas a medida que ocurren, garantizando una protección constante contra amenazas.

Por otro lado, malware (del inglés "malicious software") incluye diferentes tipos de software malicioso diseñados para causar daño o aprovecharse de sistemas y usuarios. Entre las formas más comunes se encuentran:

* Virus: Programas que se adjuntan a archivos legítimos, replicándose al ejecutarse y propagándose a otros archivos o sistemas. Pueden corromper datos y afectar el rendimiento del dispositivo. [56]
* Gusanos: Malware que, a diferencia de los virus, se propaga automáticamente a través de redes sin intervención del usuario, aprovechando vulnerabilidades en los sistemas. [56]
* Troyanos: Aplicaciones maliciosas disfrazadas como software legítimo, diseñadas para engañar al usuario e instalarse. Una vez activos, permiten el acceso no autorizado al atacante. [56]
* Spyware: Software que recopila información del usuario sin su permiso, como datos personales o hábitos de navegación, y los envía a terceros. [56]
* Adware: Programas que generan anuncios no deseados. Aunque no siempre son maliciosos, pueden ser intrusivos y degradar la experiencia del usuario. [56]
* Ransomware: Malware que cifra los archivos del usuario y exige un pago para devolver el acceso. Es especialmente peligroso y ha sido protagonista de numerosos ataques masivos. [56]
* Rootkits: Herramientas que otorgan privilegios administrativos al atacante, permitiendo el control total del sistema mientras ocultan su presencia para evitar ser detectados. [56]
* Keyloggers: Software que registra las pulsaciones de teclas, recopilando información confidencial como contraseñas y datos financieros. [56]
* **Indicar que es ClamAV, su propósito y capacidades.**

ClamAV es un motor antivirus de código abierto creado para identificar y neutralizar diversas amenazas, como troyanos, virus, malware y otros tipos de software malicioso. Lanzado por primera vez en 2001, ClamAV se ha convertido en una herramienta clave para la seguridad informática, con un enfoque particular en sistemas Unix y Linux. [29]

El objetivo principal de ClamAV es proporcionar una solución eficaz y gratuita para la detección y eliminación de malware en sistemas informáticos. Aunque es ampliamente utilizado en servidores de correo electrónico para escanear y filtrar correos maliciosos, sus aplicaciones se extienden a la protección de sistemas de archivos y la integración con otras herramientas de seguridad. [29]

Las capacidades de ClamAV son las siguientes:

* Detección de malware: ClamAV utiliza una base de datos constantemente actualizada que le permite identificar millones de amenazas, incluyendo virus, gusanos, troyanos, macros maliciosos de Microsoft Office y malware dirigido a dispositivos móviles. [57]
* Escaneo de archivos comprimidos: Es capaz de analizar una amplia variedad de formatos comprimidos, como ZIP, RAR, Tar, Gzip y Bzip2, detectando amenazas que puedan estar ocultas dentro de archivos empaquetados. [57]
* Integración con servidores de correo: Se integra eficientemente con servidores de correo electrónico, permitiendo el escaneo de mensajes y archivos adjuntos para detectar y bloquear malware antes de que lleguen a los destinatarios. [57]
* Actualizaciones automáticas: ClamAV incluye herramientas como freshclam, que actualizan automáticamente la base de datos de firmas de virus, garantizando protección contra las amenazas más recientes. [57]
* Escaneo en tiempo real: En sistemas Linux, ClamAV ofrece capacidades de escaneo en tiempo real mediante el módulo ClamOnAcc, que detecta y bloquea archivos maliciosos al momento de su interacción. [57]
* Multiplataforma: Aunque inicialmente fue diseñado para entornos Unix, ClamAV es compatible con sistemas operativos como Linux, macOS y Windows, haciéndolo adaptable a diferentes entornos. [57]
* Integración con otras herramientas: Puede integrarse con sistemas de correo electrónico y firewalls, facilitando su uso en entornos empresariales y mejorando la eficacia en la detección y mitigación de amenazas. [57]
* **Explicar la diferencia entre clamscan y clamdscan.**

ClamAV ofrece dos herramientas especializadas para analizar y detectar malware: clamscan y clamdscan. Aunque ambas cumplen el mismo propósito, presentan diferencias significativas en su funcionamiento y en la gestión de recursos

**Clamscan**

Es una herramienta independiente que se ejecuta bajo demanda para analizar archivos o directorios específicos. Cada vez que se inicia, clamscan carga la base de datos de firmas de virus en la memoria, realiza el análisis y libera los recursos al finalizar. Este proceso implica recargar las firmas en cada ejecución, lo que puede aumentar los tiempos de escaneo, especialmente en sistemas con recursos limitados [58]. Es adecuado para escaneos ocasionales o cuando no se necesita un servicio de escaneo en tiempo real.

**Clamdscan**

Funciona como un cliente del demonio clamd, un servicio en segundo plano optimizado para realizar escaneos de manera eficiente. El demonio clamd mantiene la base de datos de firmas de virus cargada en la memoria de forma persistente, eliminando la necesidad de recargarla en cada análisis. Esto acelera significativamente los escaneos posteriores. Además, clamd puede gestionar múltiples hilos de escaneo en paralelo, maximizando el rendimiento en sistemas con múltiples procesadores o núcleos. [58]

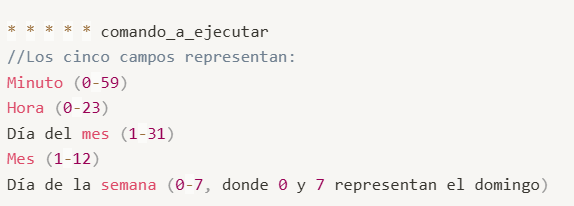
Por otro parte, es necesario tener configurado y en ejecución el servicio clamd. También se deben garantizar permisos adecuados para que clamdscan se comunique con el demonio, lo que puede requerir configuraciones adicionales en sistemas con políticas de seguridad estrictas [58]. De forma que es ideal para entornos donde se necesita realizar escaneos frecuentes o en tiempo real, como servidores de correo electrónico o sistemas con alta actividad de archivos.

* **Consultar el funcionamiento de crontab para programar tareas.**

Crontab es una herramienta utilizada en sistemas operativos Unix y Linux que permite programar la ejecución automática de tareas en horarios o intervalos específicos. Su nombre combina "cron", derivado del griego chronos (tiempo), y "tab", que hace referencia a una tabla o lista de tareas programadas. Esta utilidad es fundamental para automatizar tareas repetitivas, como realizar copias de seguridad, ejecutar actualizaciones del sistema o eliminar archivos temporales, optimizando así la gestión y mantenimiento del sistema. [59]

El funcionamiento de crontab se basa en la edición de un archivo de texto donde se definen las tareas programadas, conocidas como *"cron jobs"*. Cada línea en este archivo representa una tarea y el momento exacto en que debe ejecutarse. La programación de estas tareas utiliza una sintaxis específica que permite definir la frecuencia y el horario de ejecución, lo que facilita la automatización de procesos según las necesidades del sistema o del usuario.

Para automatizar tareas cada la línea de código del archivo crontab sigue la siguiente estructura:



**Figura 5.23.** Forma de configurar el archivo crontab.