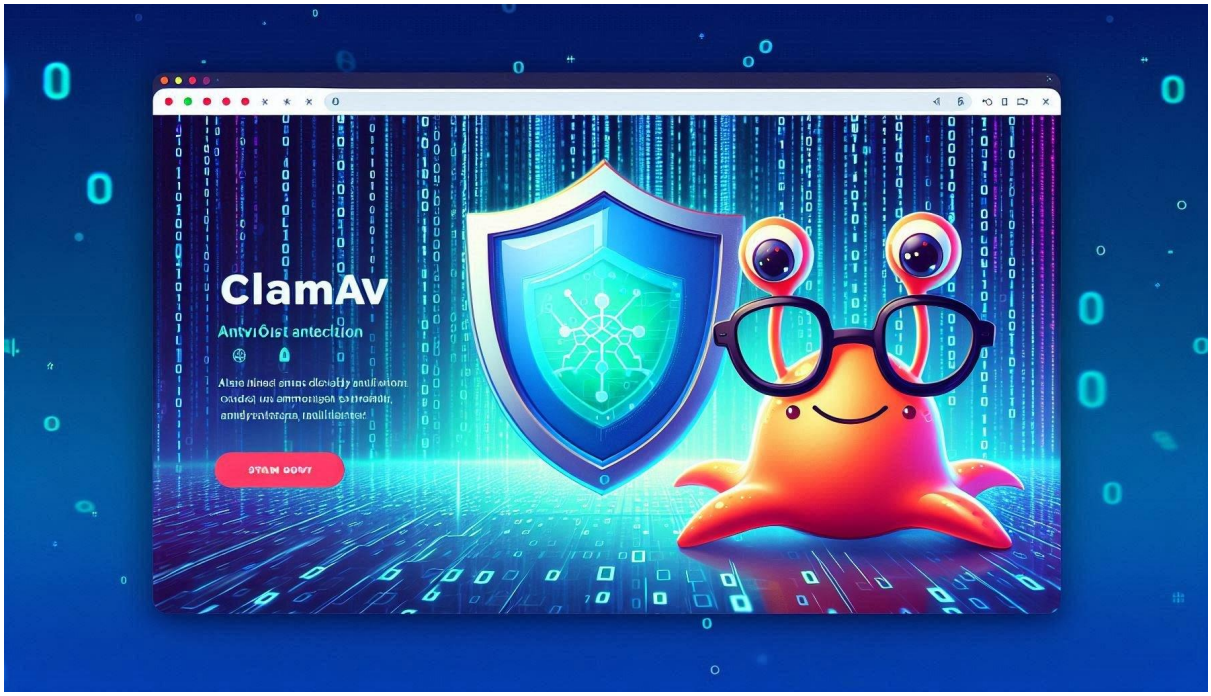
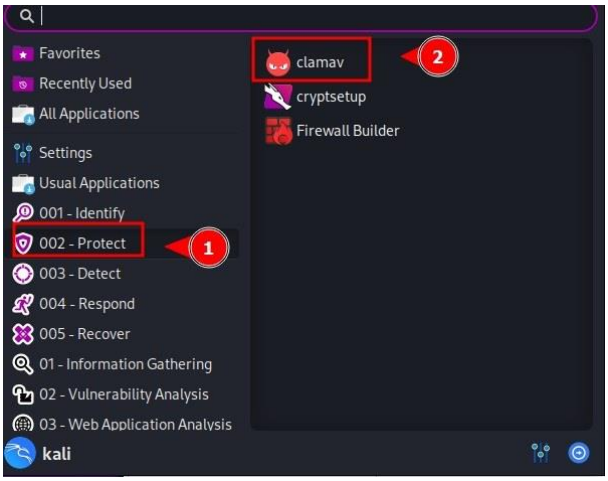


ANTIVIRUS CLAMAV

¿Qué es ClamAV?

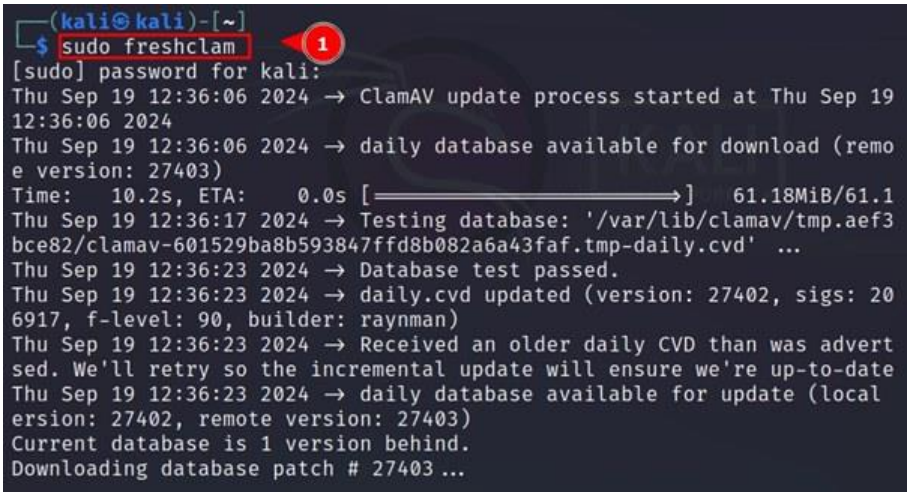
ClamAV es un software **antivirus de código abierto**, ampliamente utilizado para detectar troyanos, virus, malware y otras amenazas en sistemas Unix-like, incluyendo Linux, BSD y macOS. Se puede encontrar por **defecto** en **Kali Linux Purple.**



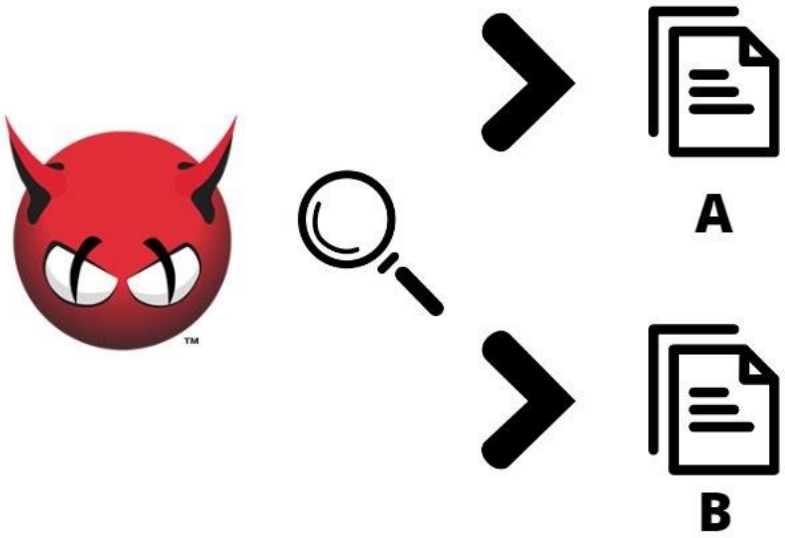
El funcionamiento básico de un antivirus

Un antivirus como ClamAV (como la la mayoría de antivirus) opera siguiendo estos pasos generales:

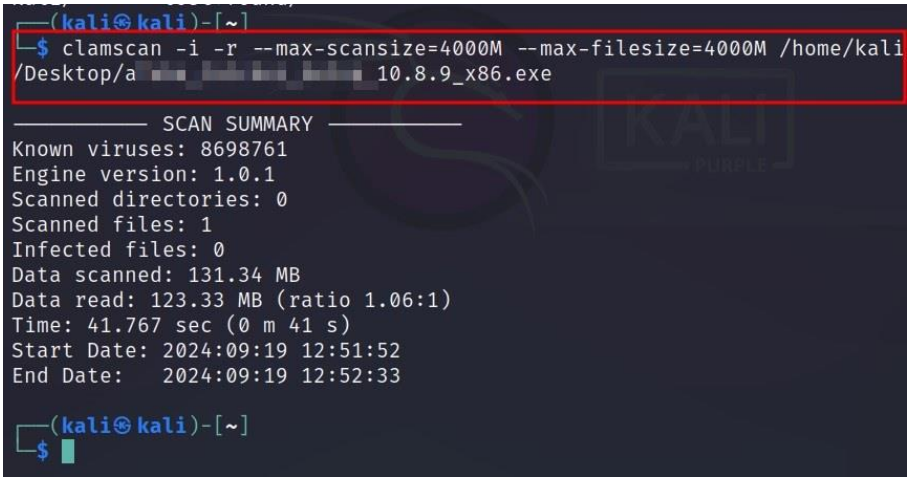
1. **Definición de firmas:** Los antivirus utilizan **bases de datos de firma**s, que son patrones únicos asociados a **cada tipo de malwar**e. Estas firmas se actualizan constantemente para incluir nuevas amenazas. En el caso de **ClamAV** se realiza mediante el comando **freshclam**



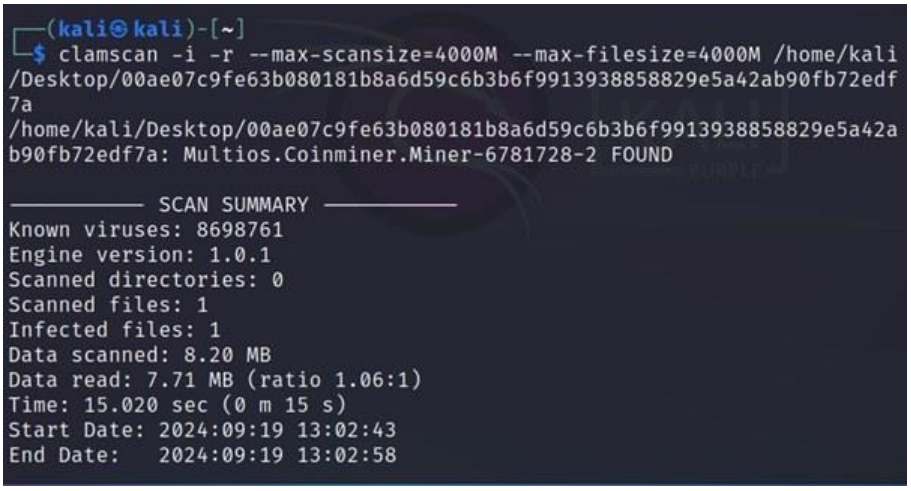
2. **Análisis de archivos:** Cuando un archivo es escaneado, el antivirus compara su contenido con las firmas conocidas. Si encuentra una coincidencia, se considera que el archivo está infectado. En este caso se procede a analizar dos archivos, un archivo ejecutable de windows descargado desde una página web y el segundo sacado de un repositorio de github.



Para analizar los archivos se utiliza el comando **clamscan -i -r --max-scansize=4000M --max-filesize=4000M /home/kali/archivo1**

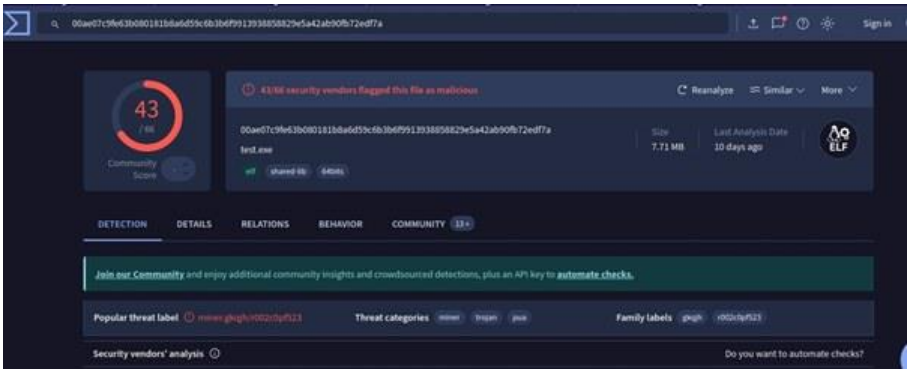


Usamos el mismo comando para el segundo archivo **clamscan -i -r --max-scansize=4000M --max-filesize=4000M /home/kali/archivo2**



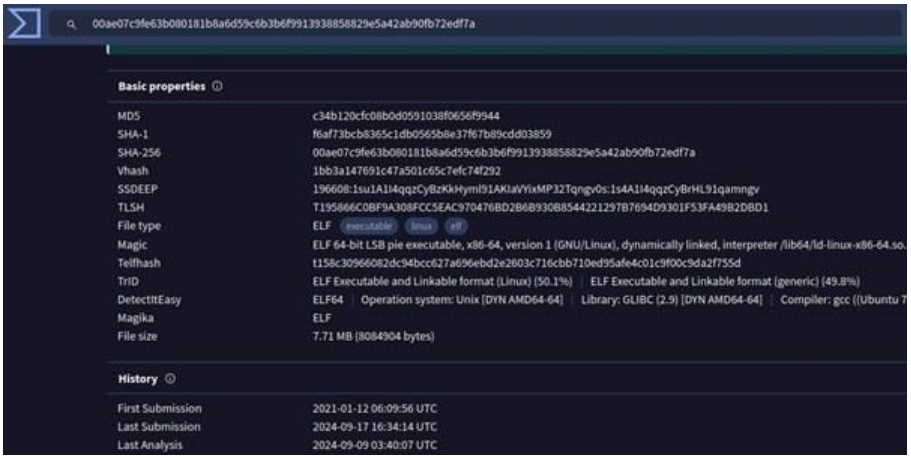
Como podemos ver, el **primer archivo no es detectado como amenaz**a, pero lo recomendable es pasarlo una **segunda vez o probar otro antivirus** para **evitar falsos negativos**. El segundo archivo tiene **Malware** (**Coinminers** que se utiliza para obtener criptomonedas)

Lo recomendable siempre es consultar en las máximas bases de datos por si la firma o hash ya está **registrada**. Esta última característica se puede ver en la herramienta **Virustotal** que **consulta en diferentes bases de datos** de antivirus.



3. Heurística: Además de las firmas, muchos antivirus utilizan técnicas heurísticas para **detectar malware desconocid**o. Estas técnicas se basan en el análisis del comportamiento de los archivos y pueden identificar patrones sospechosos que no se corresponden con ninguna firma conocida.

4.



¿Por qué ClamAV es una buena herramienta en el análisis forense?

- **Detección temprana:** ClamAV puede ayudar a identificar infecciones en sistemas comprometidos, lo que es fundamental para contener una amenaza y evitar una mayor propagación.

- **Análisis de malware:** Al analizar archivos infectados, ClamAV puede proporcionar información valiosa sobre el tipo de malware, su función y su origen.

- **Verificación de la integridad:** ClamAV se puede utilizar para verificar la integridad de archivos y sistemas, asegurando que no hayan sido modificados por malware.

- **Integración con otros sistemas:** ClamAV se integra fácilmente con otros sistemas y herramientas de análisis forense, lo que facilita la creación de flujos de trabajo automatizados.

- **Gratuito y de código abierto:** Esto permite a cualquier persona **acceder a su código fuente** y personalizarlo según sus necesidades.
- **Alta velocidad de escaneo:** ClamAV es conocido por su eficiencia, lo que lo hace ideal para escanear grandes cantidades de datos.
- **Modularidad:** ClamAV se puede configurar para **adaptarse a diferentes entornos** y necesidades.

Usos de ClamAV en el análisis forense:

- **Investigación de incidentes:** Identificar malware en sistemas comprometidos y determinar el alcance de una infección.
- **Análisis de malware:** Desensamblar y **analizar muestras de malware** para comprender su funcionamiento.
- **Verificación de la integridad de la evidencia:** Asegurar que las evidencias digitales no hayan sido alteradas.
- **Creación de entornos de análisis seguros:** Escanear imágenes de disco y memorias USB para identificar posibles amenazas antes de analizarlas en un entorno aislado.

ClamAV es una herramienta invaluable para cualquier profesional de la ciberseguridad. Su capacidad para **detectar malware, su facilidad de uso y su integración** con otras herramientas lo convierten en un componente esencial de cualquier arsenal de análisis forense.