ClamAV. La Guía Completa del Principal Antivirus en Linux

Si llevas ya un tiempo en GNU/Linux, seguro que el eterno dilema sobre si **es o no necesario instalar un antivirus** ya te sonará viejo.

En cuanto a la clase que nos ocupa, la idea es que sirva a modo de tutorial exhaustivo de **ClamAV**, probablemente el **antivirus para Linux mas popular** desde hace ya un buen tiempo. La guía es aplicable a la gran mayoría de distribuciones, léase Debian, Ubuntu, Linux Mint, Open Suse, Fedora, etc. Antes de entrar en materia, pongámonos en contexto...

¿Hay Virus y Malware en Linux?

Antes de nada, conviene aclarar que **ningún sistema es inmune a virus y malware** en general, y como muestra, en Security By Default tienes un ejemplo claro de malware para Linux. Existir, existe. Y esto, poniendo el foco específicamente en GNU/Linux, sin entrar a considerar el caso de Android.

Sin dejar de tener esto presente, personalmente considero (aunque puedo estar equivocado) que la base de la seguridad en Linux hay que ir a buscarla, primeramente, en los siguientes puntos:

- Mantener las actualizaciones al día.
- Instalar software desde los repositorios oficiales.
- Habilitar y configurar correctamente el cortafuegos del Kernel.
- Configurar correctamente tu navegador web (véase Java, Flash, etc.).
- Ser cuidadoso con los permisos que das a archivos y directorios.

Aun así, nunca está demás contar con una barrera de protección extra, y hay casos en los que si puede ser muy útil disponer de un antivirus en Linux.

Sin ir mucho más lejos, puede venir bien para **analizar discos duros externos** o memorias USB, escanear otras particiones con Windows, y ya por no hablar si ejecutas un **servidor de correo** o un **servidor web**, entre otros casos que seguro se me olvidan.

Y aquí es donde entra en juego ClamAV, un **software antivirus de código abierto**, multiplataforma, y que es muy popular en entornos Unix y Linux, sobretodo en servidores.

Así que, con todo esto, veamos como instalarlo y ejecutarlo en nuestra distribución GNU/Linux, tanto para analizar el propio sistema, como discos o unidades externas.
Conviene aclarar que ClamAV está centrado principalmente en los virus, por lo que a la hora de detectar, por ejemplo, rootkits y otros tipos de malware no estaría de más contar con alguna utilidad orientada en este sentido. En este post tienes una guía donde verás como utilizar Chkrootkit y Rkhunter para escanear tu sistema en busca de rootkits.

Antes de empezar, debes tener en cuenta que ClamAV es un software pensado para utilizarse desde la línea de comandos, por lo que es importante que tengas cierta soltura en el uso de la consola. Si bien existe una versión de ClamAV con interfaz gráfica (al final de este mismo post puedes leer más sobre ello), en esta guía me he centrado en su uso a través de la consola.

Como Instalar ClamAV en tu Distribución GNU/Linux

Instalarlo no tiene ningún secreto, puesto que se encuentra en los repositorios oficiales de la mayoría de distribuciones. A continuación te dejo las instrucciones para diferentes casos. Como verás, necesitarás privilegios de root para instalarlo.

En Ubuntu y derivados como Xubuntu, Lubuntu o Linux Mint, entre otros muchos, esta es la sentencia:

```
$ sudo apt install clamav
```

Para instalar ClamAV en Debian debes hacerlo como usuario Root y puedes utilizar *apt-get* o *aptitude* indistintamente:

```
$ su
# aptitude install clamav
```

Si utilizas Fedora, o alguna otra distribución derivada de Red Hat, puedes hacerlo con *yum*:

```
$ su
# yum install clamav
```

Y en lo que respecta a Arch Linux, la sentencia es la que sigue:

```
$ su
# pacman -S clamav
```

Con esto instalarás ClamAV pero en su versión más ‘core’, es decir para utilizarla a través de la linea de comandos.

Su uso es muy sencillo, pero si aun así prefieres instalar la versión con interfaz gráfica, deberás instalar, además, otro paquete llamado ClamTK, que verás más adelante en el post.

La versión que se ofrece en los repositorios es la que es dependiendo de la distro GNU/Linux, pero quieres optar por la versión más reciente, puedes descargarla fácilmente desde su web oficial.

- Web oficial del proyecto ClamAV: **www.clamav.net**

Actualiza la Base de Datos de Firmas

Una vez instalado en nuestro sistema, lo primero que deberías hacer es actualizar la BBDD de firmas de virus de ClamAV. Para ello, deberás igualmente poseer permisos de superusuario.

Normalmente, el paquete *freshclam* se instala como dependencia con la instalación del paquete principal, pero en caso de que no sea así, puedes instalarlo manualmente con este sencillo comando:

Para instalar el paquete freshclam en Ubuntu y derivados:

```
$ sudo apt install clamav-freshclam
```

Con esto ya podemos pasar a comprobar si existen actualizaciones en la base de datos de firmas de virus. Hacerlo es tan sencillo como abrir una terminal y teclear:

```
$ sudo freshclam
```

Esto hará básicamente un *check* rápido de la base de datos y mirará si todas las firmas están actualizadas. En caso de que no lo estén, las actualizará.

Si obtienes un error al intentar actualizar el programa, es posible que sea porqué el demonio de actualizaciones *freshclam* no está habilitado.

Normalmente debería venir habilitado por defecto, pero en caso de no ser así, sigue estas líneas porqué más adelante tienes explicado como comprobar si está habilitado en segundo plano, y en caso contrario, habilitarlo manualmente.

Escanea Manualmente tu Sistema

La sintaxis de ClamAV a la hora de hacer análisis manuales es muy sencilla, pero es verdad que a medida que vayas conociendo sus opciones verás que puedes llegar a construir comandos bastante largos. En general la sintaxis suele ser:

```
$ clamscan -[parámetros] [ruta de carpeta]
```

Antes de nada, es importante tener en cuenta que en GNU/Linux, un usuario estándar generalmente solo tiene permisos de escritura sobre su directorio personal. Es por ello que, en caso de infección, de entrada el primer lugar que habría que comprobar es tu *home*. Para escanear tu directorio personal de manera recursiva, es decir, pasando archivo por archivo, puedes utilizar este comando:

```
$ sudo clamscan -r /home
```

Con la opción '-r', lo que le indicamos a ClamAV es que haga un análisis recursivo, es decir, pasando por todos los subdirectorios.

Una vez analizado tu directorio personal, vamos a hacer lo mismo pero extendido a todo el sistema. Para hacer un escaneo profundo de todo tu sistema, puedes utilizar el siguiente comando:

```
$ sudo clamscan -r /
```

Con ‘/’, lo que le indicamos a ClamAV es que haga un análisis de todo el sistema, ya que ‘/’ representa la raíz del sistema. Esto significa que el análisis recorrerá todos los directorios del sistema.

En caso de que te haya detectado uno o más archivos infectados, para evitar tener que buscarlos entre todos los archivos escaneados, puedes repetir el análisis pero indicando que se muestren por pantalla solo los archivos infectados.

```
$ sudo clamscan -r -i /home
```

Con esto estaremos haciendo un análisis recursivo de nuestra carpeta */home*, y se irán mostrarán por pantalla solamente las infecciones.

Otra interesante opción es la que te permite indicar a ClamAV que haga sonar un pitido cada vez que detecte un archivo infectado durante el escaneo.

```
$ sudo clamscan -r --bell /home
```

También tienes la posibilidad de guardar un reporte del análisis en un archivo aparte que se creará en tu directorio personal.

```
$ sudo clamscan -r /home -l archivo.txt
```

Con esto comando estarás realizando un escaneo recursivo de tu carpeta */home*, y al finalizar se creará un reporte completo en el fichero *archivo.txt*.

Si quieres conocer más opciones de escaneo, puedes imprimir la pantalla de ayuda en la terminal mediante este comando:

```
$ clamscan --help
```

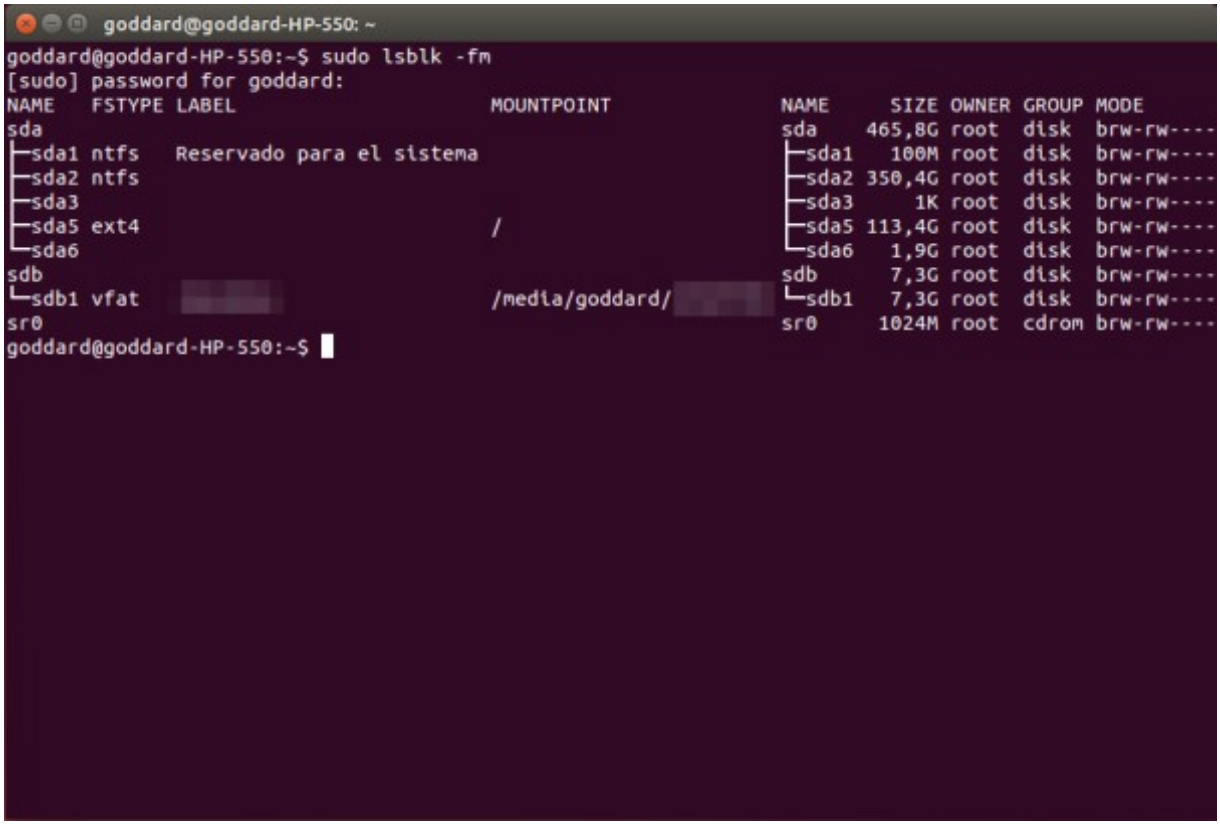
Como Escanear una Partición o una Unidad de Disco Externa

Para analizar un disco duro externo, un Pendrive, u otra partición dentro del mismo disco duro (por ejemplo, si dispones de arranque dual entre Windows y Linux), lo único que tendremos que cambiar es el parámetro final de la ruta.

Para comprobar la ruta, o el nombre de identificador de un volumen en concreto, puedes ayudarte de este comando:

```
$ sudo fdisk -l
```

Esto te mostrará el la ruta con el nombre de identificador de cada volumen. Las diferentes particiones del disco interno se identifican como ***sda*** o ***hdb***, mientras que los discos externos conectados por USB son los ***sdb***.



Estas rutas serán las que deberás indicarle a ClamAV para especificar en que volumen de disco quieres que haga el análisis.

Conociendo esto, ya puedes ejecutar ClamAV en cualquier volumen de disco, y utilizando cualquiera de las opciones de escaneo que ya hemos visto antes. Aquí tienes algunos ejemplos:

Para hacer un escaneo en la partición que sale identificada como ***sda2***, y que en mi caso ejecuta Windows 10, puedo utilizar:

```
$ sudo clamscan -r /media/sda2
```

Para hacer un análisis completo del Pendrive que en mi caso tengo identificado como ***sdb1***:

```
$ sudo clamscan -r /media/sdb1
```

Eliminar las Amenazas Detectadas

Si se ha detectado algún archivo infectado durante el análisis, queda el importante paso de removerlo. Antes de hacer esto es importante haber hecho primero un escaneo normal sin eliminar nada, para estar realmente seguro de lo que vas a eliminar.

Una vez estás seguro de que se puede eliminar el archivo, con ClamAV puedes remover automáticamente todos los virus detectado en un escaneo con simplemente añadir la opción *remove* entre los parámetros de escaneo. Aquí tienes un par de ejemplos

Escanear el directorio */home* de modo recursivo, y eliminar los ficheros infectados al momento (sin previa notificación).

```
$ sudo clamscan -r --remove /home
```

Y ya puestos, podemos hacer que durante el escaneo se vayan mostrando solo los archivos infectados. Para ello añadimos el parámetro *-i*, como habrás visto más arriba:

```
$ sudo clamscan -r -i --remove /home
```

Escanear la partición de Windows 10, que en este caso corresponde al identificador *sda2*, y eliminar todos los archivos detectados:

```
$ sudo clamscan -r --remove /media/sda2
```

Comprobar el Demonio de Actualizaciones de Firmas *freshclam*

Para comprobar el estado del demonio de actualizaciones *freshclam*, que en Ubuntu y Debian ya se instala directamente con el paquete principal, puedes utilizar el siguiente comando.

```
# /etc/init.d/clamav-freshclam status
```

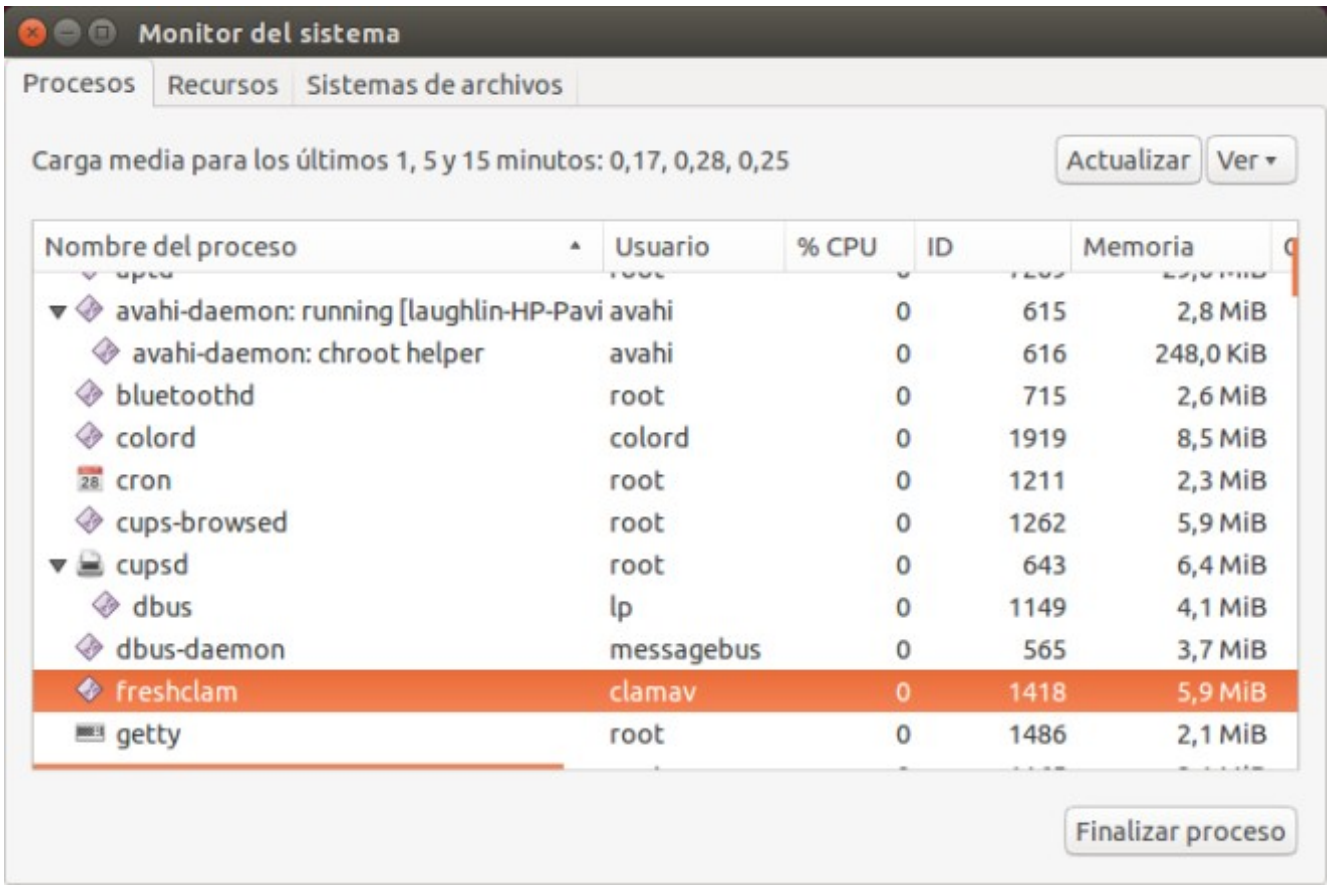
En caso de estar habilitado, deberás visualizar un output como este:

```
 * freshclam is running
```

En caso de que te muestre que no está activo, puedes habilitarlos fácilmente con estos comandos:

```
# /etc/init.d/clamav-freshclam start
```

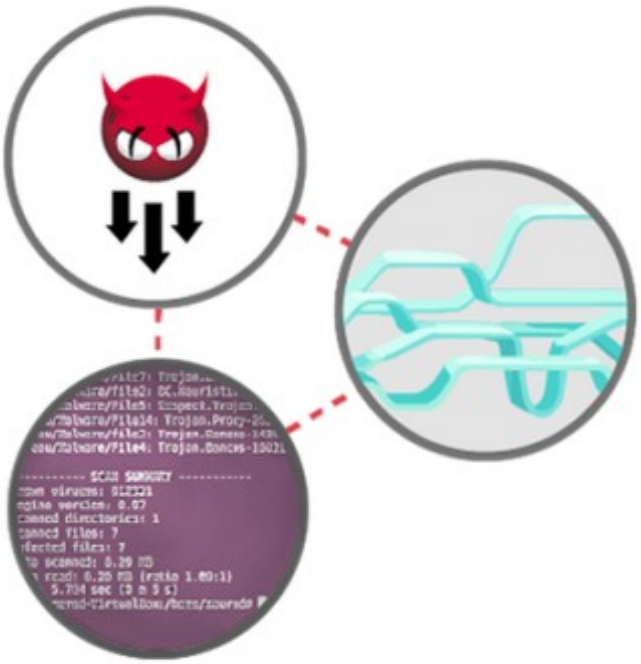
Otra forma fácil de comprobar que *freshclam* está habilitado es abrir el monitor de tareas y buscar el proceso en segundo plano, que se debería denominar *freshclam*.



Además podrás comprobar como existe un usuario denominado *clamav*, que realmente es el propietario del proceso.

Instalar y Ejecutar el Demonio *Clamd*

Otra opción que tienes es la de instalar el demonio ***clamd*** para ejecutar ClamAV como proceso en segundo plano. Básicamente lo que hace es cargarse en segundo plano al crear un usuario propio en el sistema denominado *clamav*, lo que permite **acelerar en gran medida los tiempos de escaneo** y reducir el uso de la CPU.



En el caso de Ubuntu y Debian, como he mencionado antes, **este usuario ya se ha creado con la instalación inicial**, ya que vienen con el demonio de actualizaciones *freshclam*.

ClamAV Daemon puede venir muy bien a la hora de escanear grandes cantidades de archivos, como por ejemplo en un servidor de correo, pero es algo que a nivel de usuario no utilizaría, ya que tampoco le he encontrado más utilidad.

En caso de que optes por ello, el primer paso es instalar un paquete complementario llamado ***clamav-daemon***, algo que podemos hacer nuevamente desde la misma terminal. En el caso de estar en Ubuntu, Debian y derivados:

```
$ sudo apt-get install clamav-daemon
```

En este caso, el paquete *clamav-daemon* ya se encarga de crear los archivos de configuración y habilitar los demonios *clamd* y *freshclam* por nosotros, por lo que en teoría no necesitaremos hacer nada mas.

Una vez instalado *clamav-daemon*, puedes comprobar si efectivamente lo tienes ejecutando en segundo plano pasando esta sentencia en la linea de comandos. Para ello, necesitas ser también adquirir privilegios de root. Comprobar el estado del demonio *clamd*:

```
$ sudo su
# /etc/init.d/clamav-daemon status
```

Si efectivamente está habilitado, te debería salir un output como el siguiente:

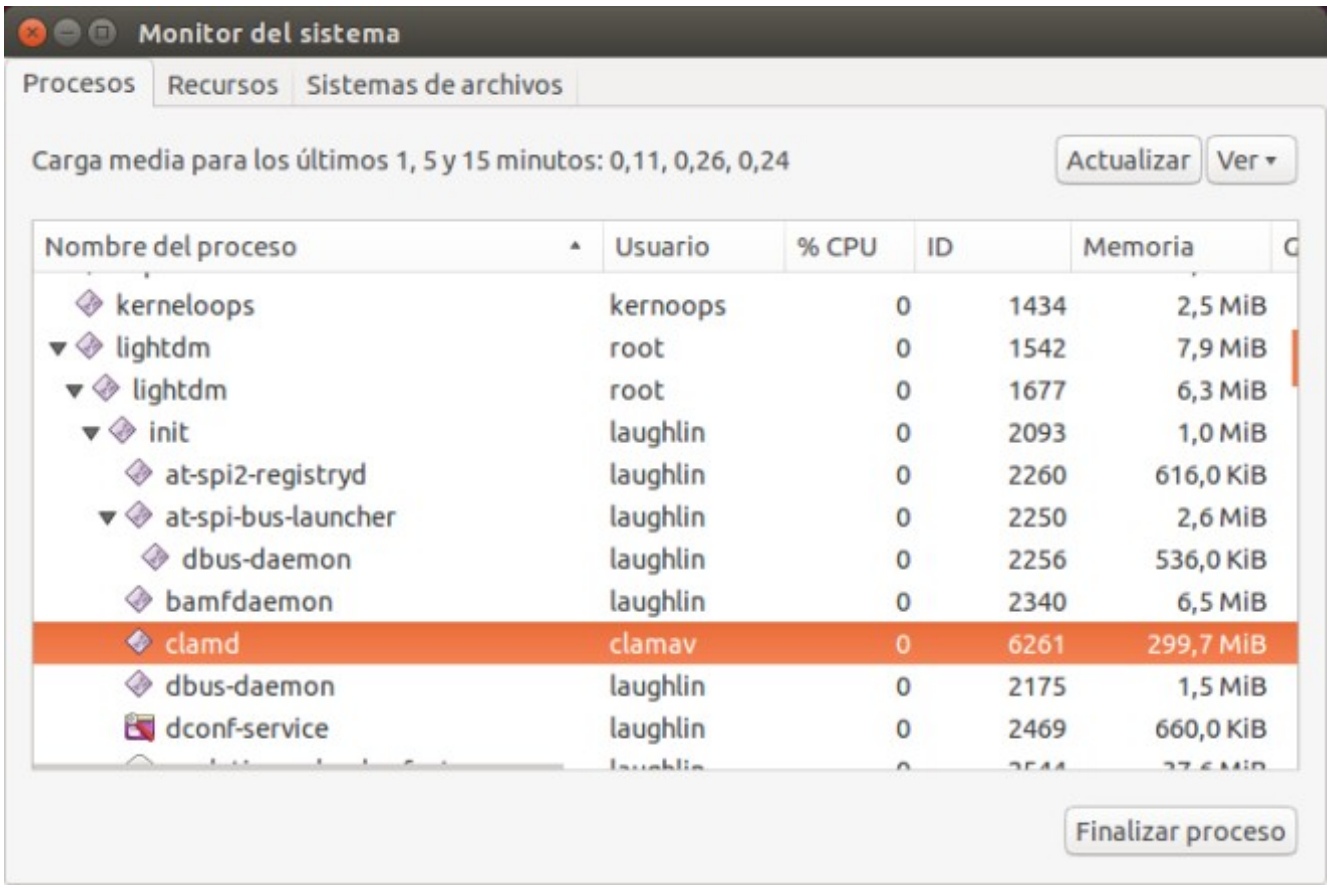
```
 * clamd is running
```

En caso de que te muestre que no está activo, puedes habilitarlos fácilmente con este comandos:

```
# /etc/init.d/clamav-daemon start
 * Starting ClamAV daemon clamd
/usr/sbin/clamd already running
```

Otra forma fácil de comprobar que el demonio está habilitado es abrir el monitor de tareas y buscar el proceso en segundo plano, que se debería denominar *clamd*.

Como puedes comprobar, al igual que en el caso de *freshclam*, el proceso pertenece al usuario *clamav*.



Ten en cuenta que en teoría el usuario creado por ClamAV no tiene permisos para acceder a tus archivos. Para ello, deberías añadirlo dentro del grupo de usuarios que tengan permisos para acceder a los archivos que quieras escanear.

Una vez tengamos los permisos, para hacer análisis utilizando el módulo de ClamAV Daemon, podemos utilizar los mismos comandos pero sustituyendo el término ***clamscan*** por ***clamdscan***. A modo de ejemplo, este sería el comando para escanear la carpeta */home* entera, en modo recursivo:

```
$ sudo clamdscan -r /home
```

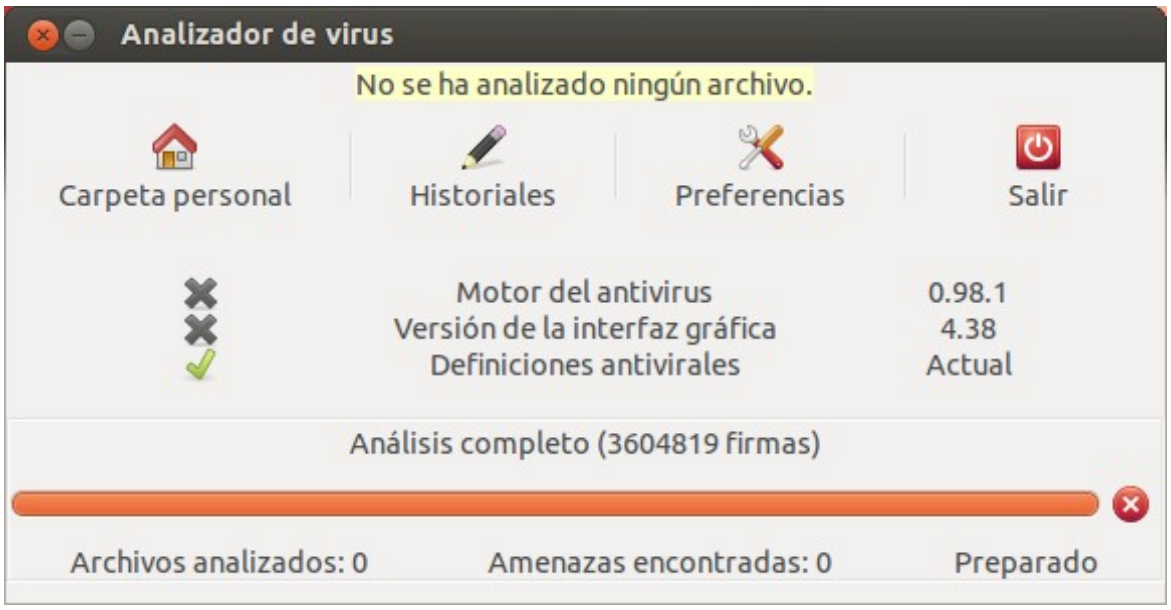
Si Prefieres la Versión con Interfaz Gráfica, Instala ClamTK

Aunque te recomiendo mil veces antes utilizarlo desde la terminal, si te sientes más cómodo moviéndote a través de interfaz gráfica, ClamAV también se puede ejecutar desde una interfaz GTK muy simple que se denomina ClamTK, aunque personalmente la he encontrado extremadamente limitada en opciones y algo poco pulida.

Para ello, necesitamos instalar en nuestro sistema el paquete ***clamtk***. El paquete se encuentra por defecto en los repositorios oficiales de Ubuntu, Debian, y generalmente en la mayoría de distros más conocidas. En Ubuntu puedes instalarlo con un simple *apt-get install* o *apt install*

```
$ sudo apt-get install clamtk
```

Una vez instalado ClamTK, puedes abrirlo desde el mismo Dash de Ubuntu tecleando por su nombre, o accediendo en el menú ‘Actividades’ en GNOME, dependiendo de la distro que utilices.



Al abrir la aplicación, verás tu mismo que la interfaz es excesivamente simplista, y las opciones que ofrece se limitan a arrastrar un archivo o carpeta para escanearlo, consultar el historial, o modificar las preferencias.

Por esto, considero mucho más interesante y útil utilizar ClamAV desde la terminal, ya que permite muchísimo más juego, a la vez que está más depurado y es mucho más transparente al usuario.

Para Terminar

Ya por terminar, si has llegado hasta este punto, espero que realmente hayas encontrado utilidad en la guía, y que hayas podido seguir los pasos correctamente.