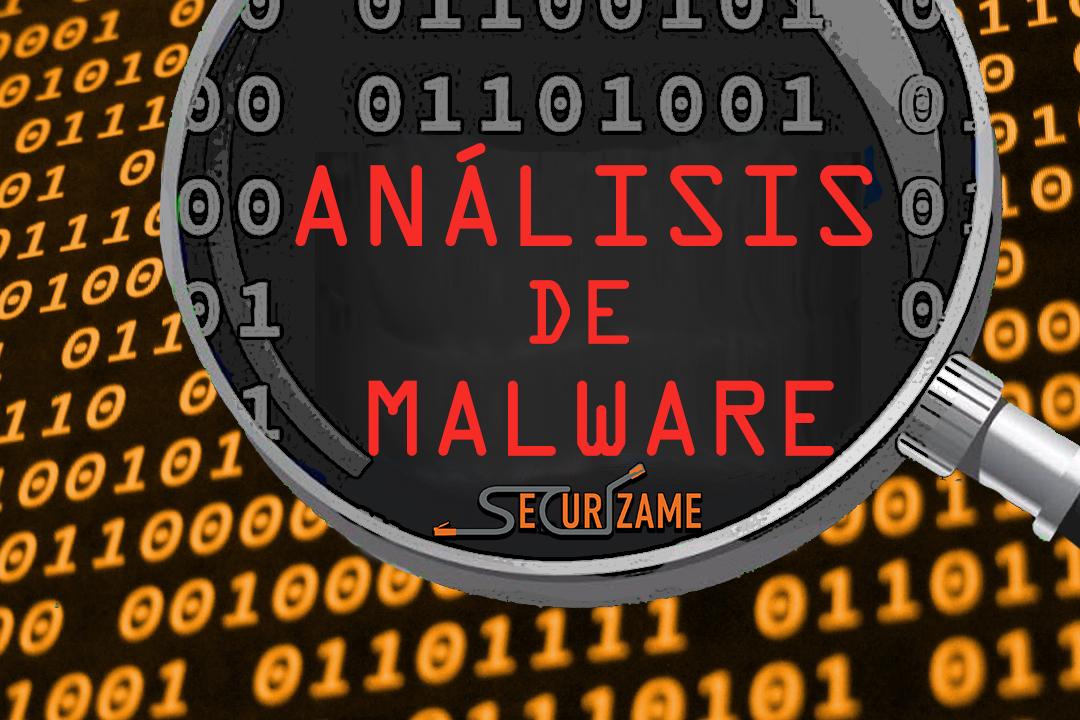
**Análisis de Malware**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Ubuntu**](#_g59i8ewd3ed3) **2**

[**2.1 Rkhunter:**](#_5d38uxjyswtl) **2**

[**2.2 ClamAV:**](#_3lohr8w44k5a) **7**

[**3. Windows**](#_sjd6c5cq0na6) **11**

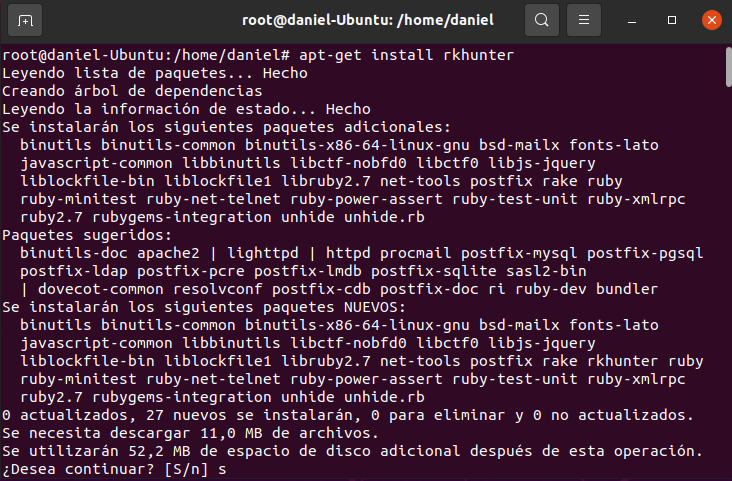
[**3.1 SFC:**](#_txquz3shi2fj) **11**

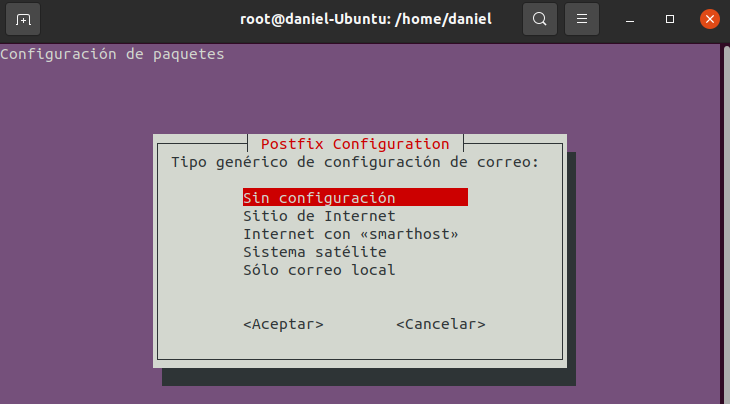
# **2. Ubuntu**

### **2.1 Rkhunter:**

1. En la máquina Ubuntu instalar el paquete rkhunter (si te pregunta al instalar postfix la

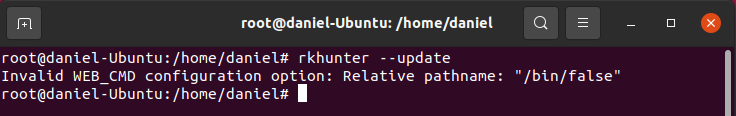
configuración, puedes poner “Sin Configuración”)

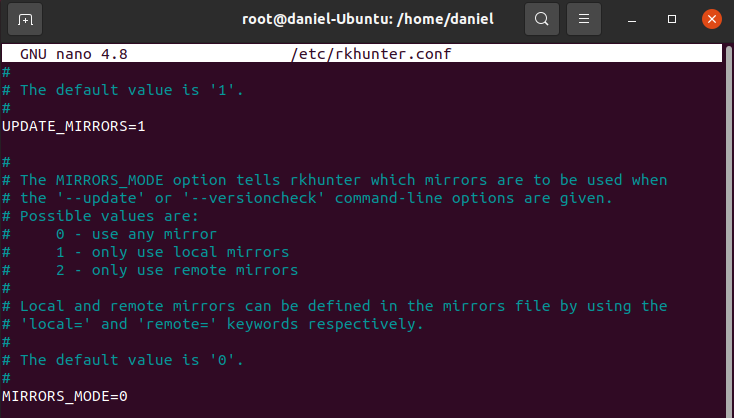


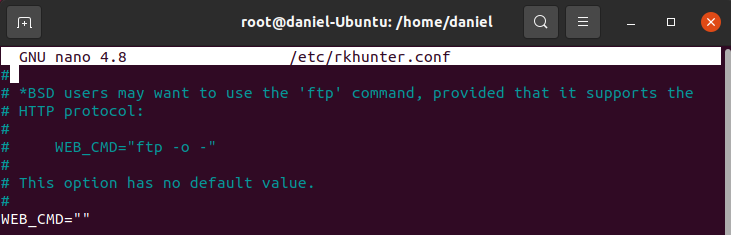


2. Actualizar las definiciones de rkhunter (--update) (Nota: Si obtienes un error al

intentar actualizar, investiga qué cambios debes hacer para conseguir que actualice).

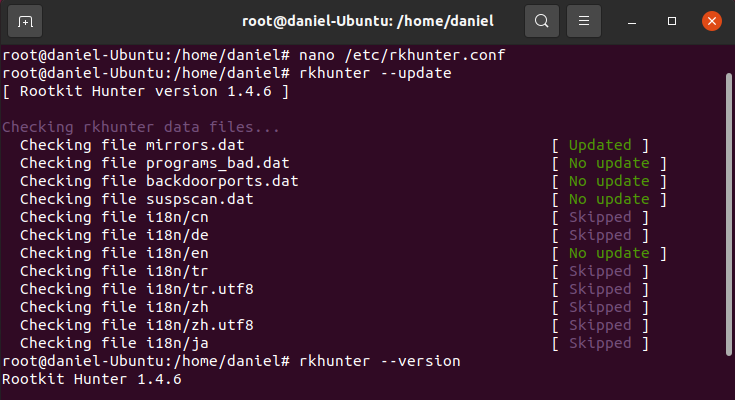




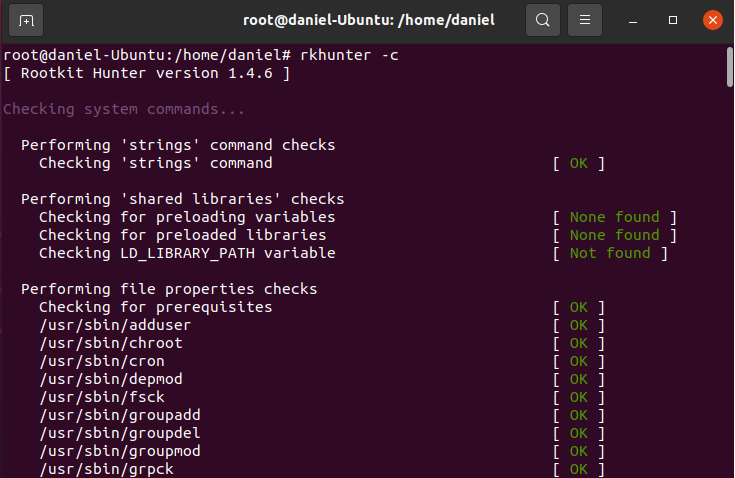


3. Después de actualizarlo, ejecuta rkhunter –versioncheck para comprobar que la

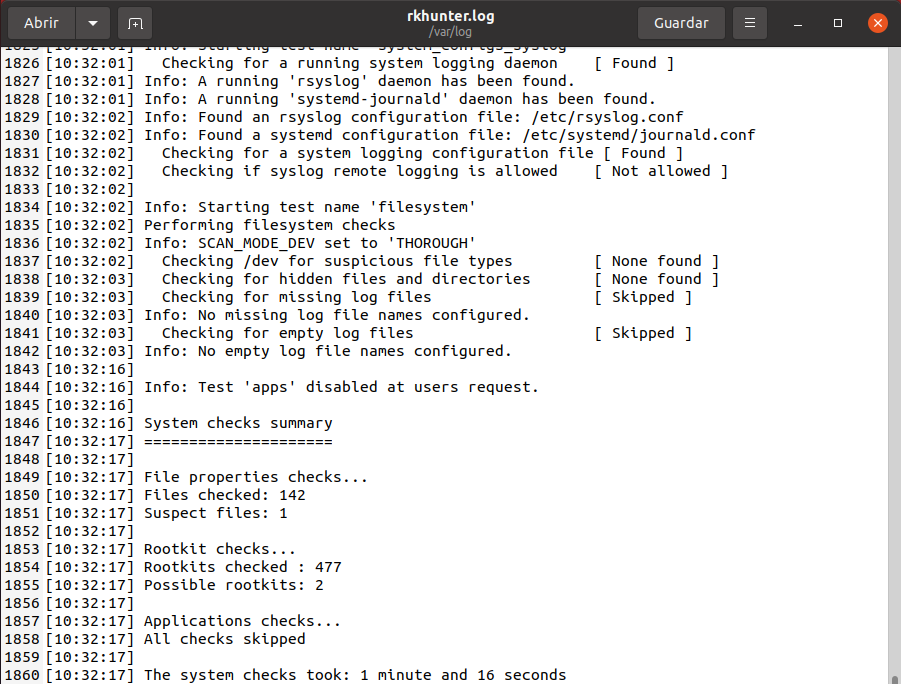
versión instalada es la más reciente



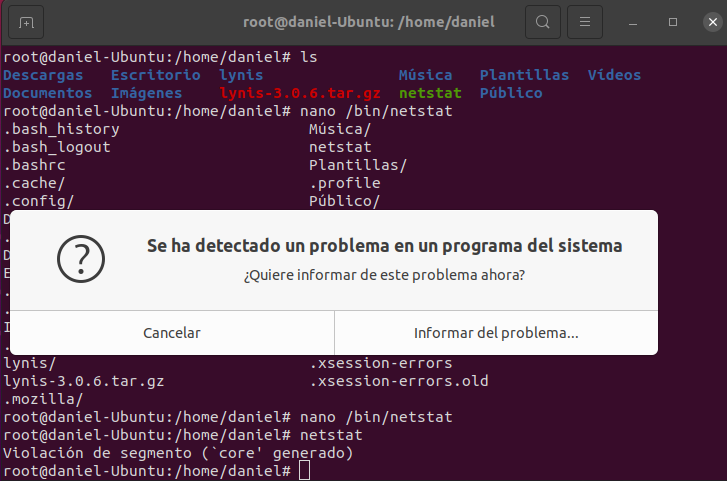
4. Lanza un escaneo al sistema con rkhunter (--help verás la ayuda y la opción -c te sirve para lanzar el escaneo a la máquina). Empezará el análisis mostrando información por pantalla.



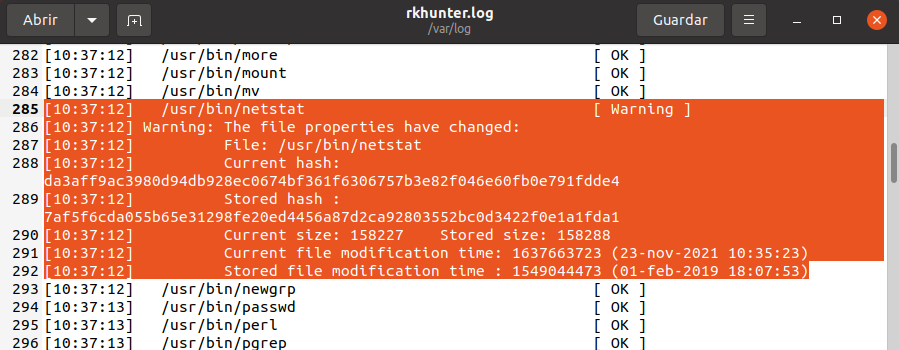
5. Una vez terminado el análisis, visualizar el archivo LOG con el detalle del proceso (var/log/rkhunter.log)



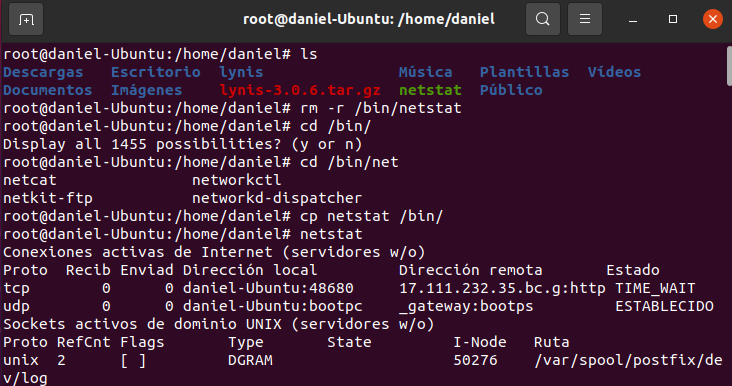
6. Vamos a suponer que hemos tenido un incidente de seguridad en la máquina. Un usuario malicioso ha conseguido arrancar una distro Live usando un pendrive USB. Supongamos que luego nos ha instalado un troyano inverso que hace que nuestro sistema Linux se conecte automáticamente con el suyo para que él pueda controlarlo remotamente (un troyano RAT o Remote Administration Tool). La instalación del troyano ha modificado el comando /bin/netstat Para simular esta situación, primero haz una copia del programa /bin/netstat y luego edita el programa /bin/netstat borrando algún carácter del fichero.



7. Realiza un nuevo análisis con la herramienta rkhunter y comprueba en el log la detección de la situación que hemos simulado anteriormente.

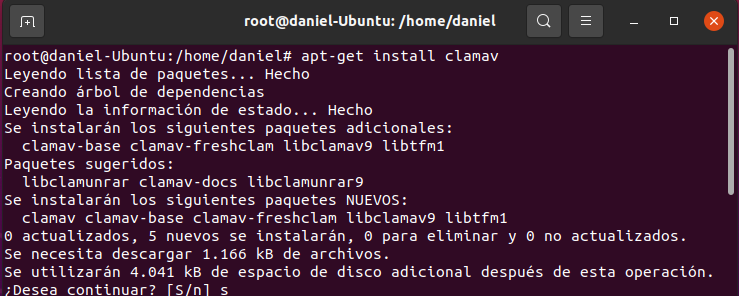


8. Restaura el ejecutable netstat por el original para dejar el sistema correctamente.

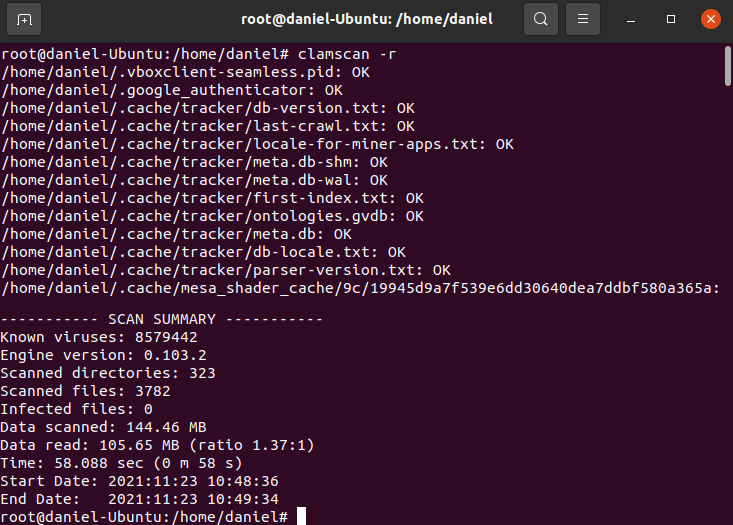


### **2.2 ClamAV:**

1. Instalamos los paquetes clamav y clamav-freshclam

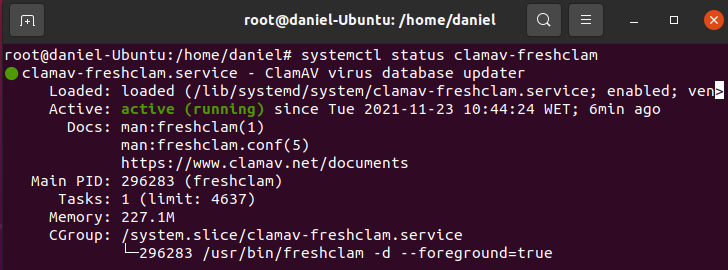


2. clamscan con la opción -h nos permite ver todos los parámetros disponibles para este programa. Utiliza la opción para realizar un escaneo detallado.

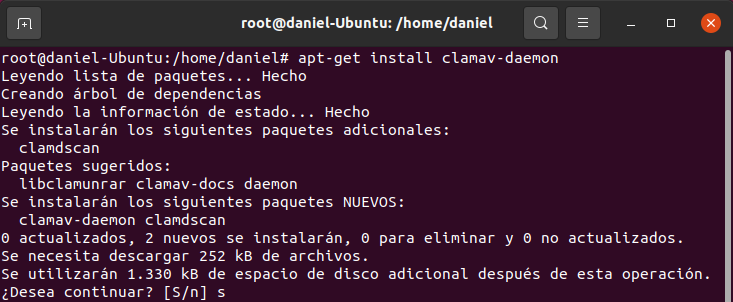


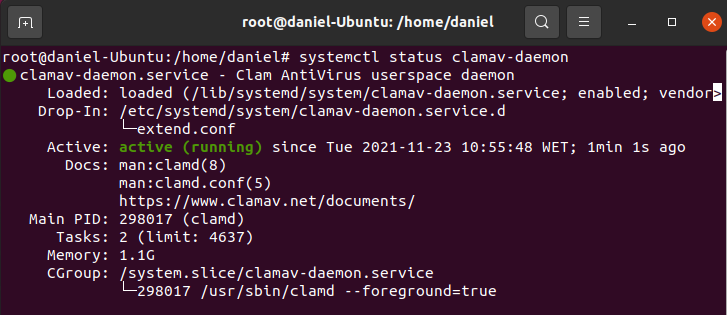
3. Comprueba que junto con la instalación del antivirus se ha instalado el servicio freshclam. Este demonio es un proceso autónomo que se ejecuta en segundo plano, de manera que no necesita interacción por parte del usuario y se encarga de mantener actualizada la base de firmas del antivirus.

4. Comprueba desde el Monitor de Tareas de Ubuntu que el servicio anterior se está ejecutando.

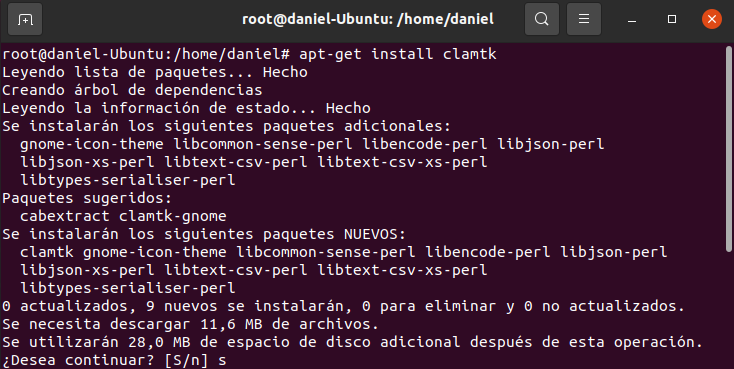


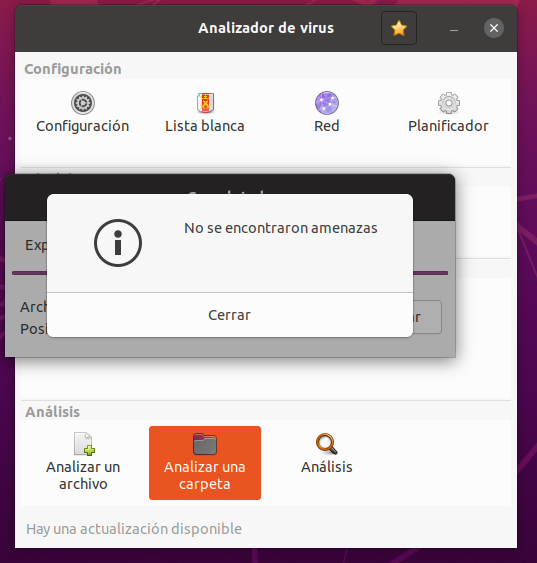
5. Si quisiéramos mantener el antivirus funcionando como servicio en tiempo real, debemos instalar el paquete clamav-daemon Instálalo y luego comprueba que se está ejecutando utilizando la dos mismas formas anteriores.





6. Aunque no es necesario, también dispone de una interfaz gráfica. Para ello debes instalar el paquete clamtk Después de instalarla, realiza un escaneo de la carpeta boot u otra que consideres adecuada.

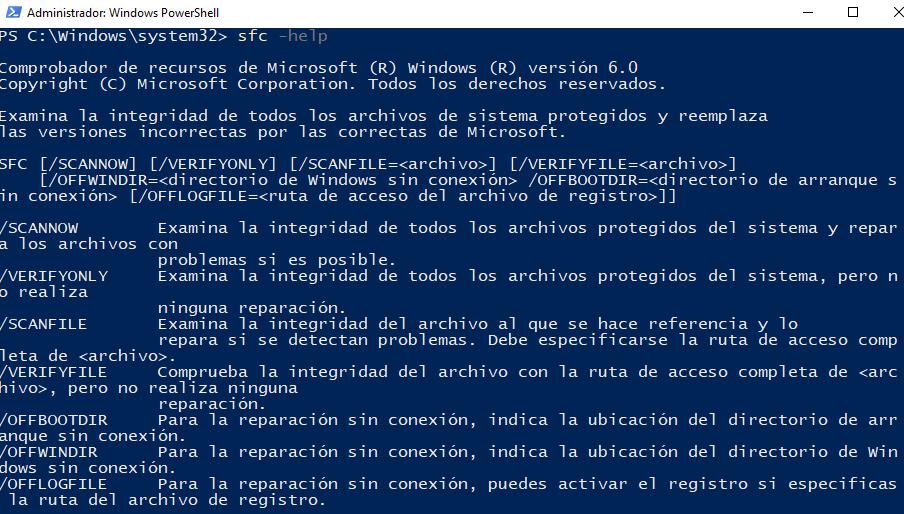




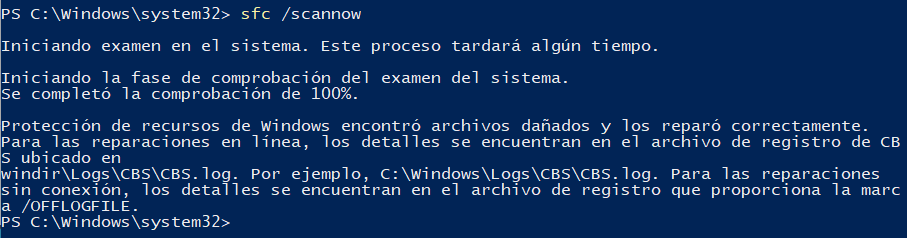
# **3. Windows**

### **3.1 SFC:**

1. Desde una consola de comandos lanza la orden necesaria para ver la ayuda de la utilidad SFC

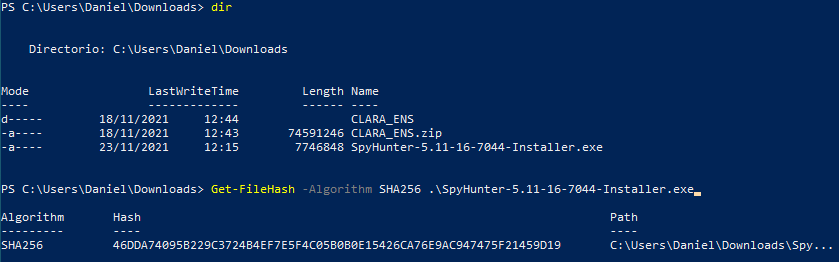


2. Entre las opciones disponibles, ejecuta la que examina todos los archivos protegidos del sistema operativo y reparar los dañados.



3. Hay multitud de aplicaciones antimalware para Windows. Vamos a probar SpyHunter de entre las más conocidas. Haz la descarga desde su página oficial. Muchas webs y fabricantes, suelen añadir el código hash o resumen del programa descargado para comprobar que no haya sido modificado o descargado de un sitio incorrecto.

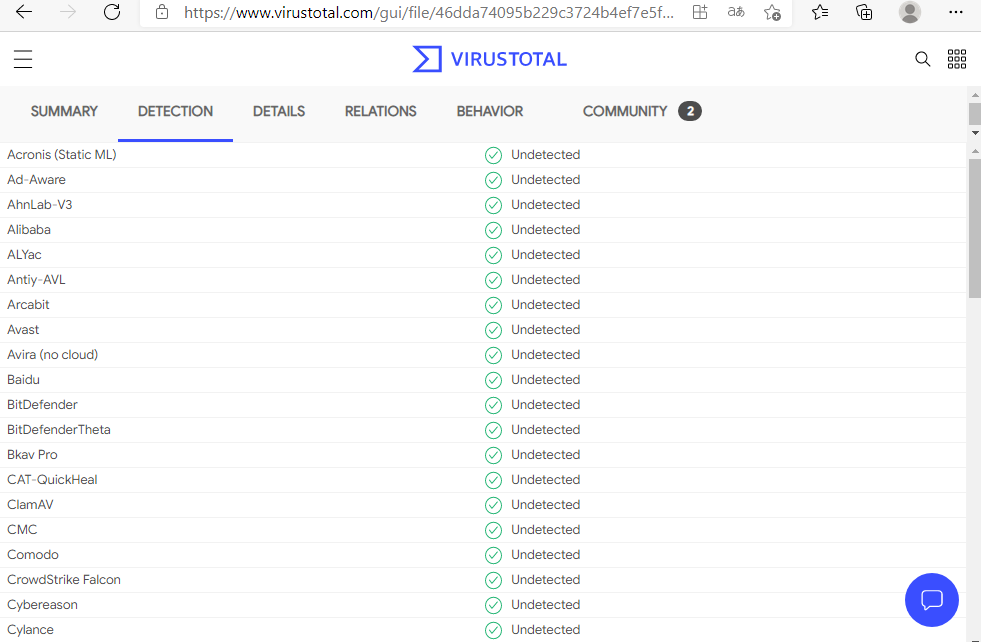




Obtén el código SHA256 del programa y comprueba que sea:

**46dda74095b229c3724b4ef7e5f4c05b0b0e15426ca76e9ac947475f21459d19**

4. Otra comprobación que debemos realizar siempre antes de instalar un programa en nuestra máquina, es pasarle un antivirus. Aparte del que tengamos instalado en nuestra máquina, la mejor opción es subirlo a algún antivirus online por la ventaja de que el archivo será comprobado por multitud de motores antivirus diferentes. Utiliza Virustotal por ejemplo para comprobar este programa.



5. Con los pasos 3 y 4, nos hemos asegurado que el programa a instalar está limpio. Procede a realizar la instalación y luego realiza un análisis del sistema.

