UsuarioASIR

[Nombre de la empresa]  [Dirección de la compañía]

[Título del documento]

Índice

[Introducción 0](#_Toc214009828)

[ClamAV: 1](#_Toc214009829)

[Chkrootkit: 4](#_Toc214009830)

[Rkhunter: 6](#_Toc214009831)

[LMD – Linux Malware Detect 10](#_Toc214009832)

[Lynis 12](#_Toc214009833)

[PHP-Antimalware-Scanner 14](#_Toc214009834)

# Introducción

[*https://help.clouding.io/hc/es/articles/4409694394770-C%C3%B3mo-escanear-un-servidor-Linux-en-b%C3%BAsqueda-de-virus-y-malware*](https://help.clouding.io/hc/es/articles/4409694394770-C%C3%B3mo-escanear-un-servidor-Linux-en-b%C3%BAsqueda-de-virus-y-malware)

*Sigue los pasos explicados en el tutorial para instalar :*

* *ClamAV,*
* *Chkrootkit*
* *Rkhunter*
* *LMD – Linux Malware Detect*
* *Lynis*
* *PHP-Antimalware-Scanner*

*Para cada uno de ellos comenta los resultados obtenidos.*

# ClamAV:

**apt install clamav clamav-freshclam clamav-daemon clamdscan**



Una vez instalado ClamAV lo primero que tendrás que hacer es actualizar las firmas de la base de datos de virus con el siguiente comando:

**freshclam**

Es probable que nos salga este error:

*ERROR: Failed to lock the log file /var/log/clamav/freshclam.log: Resource temporarily unavailable*

*ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).*

*ERROR: initialize: libfreshclam init failed.*

*ERROR: Initialization error!*

Si vamos al log: /var/log/clamav/freshclam.log

ed Nov 12 07:39:24 2025 -> --------------------------------------

**Wed Nov 12 07:39:24 2025 -> daily database available for download (remote version: 27819)**

**Wed Nov 12 07:39:37 2025 -> daily.cvd updated (version: 27819, sigs: 2077025, f-level: 90, builder: svc.clamav-publisher)**

**Wed Nov 12 07:39:37 2025 -> main database available for download (remote version: 62)**

**Wed Nov 12 07:39:56 2025 -> main.cvd updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)**

**Wed Nov 12 07:39:56 2025 -> bytecode database available for download (remote version: 339)**

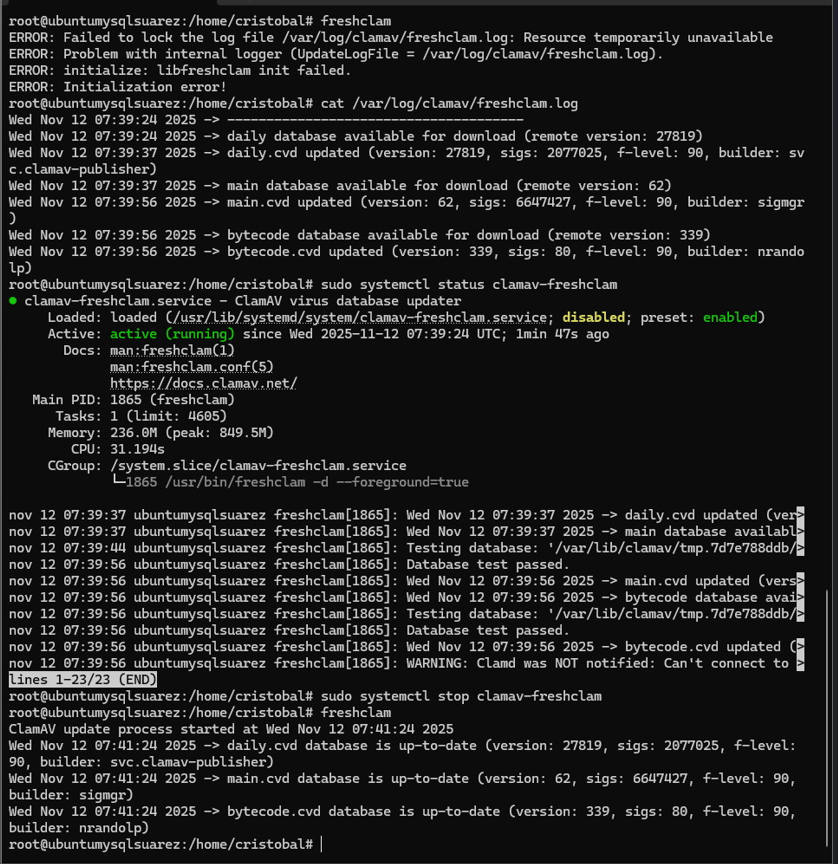
**Wed Nov 12 07:39:56 2025 -> bytecode.cvd updated (version: 339, sigs: 80, f-level: 90, builder: nrandolp)**

Nos indica que ya hay una instancia de clamav abierta y que ya está actualizado.

Si aun así queremos hacerla, hacemos:

**sudo systemctl stop clamav-freshclam**

**freshclam**

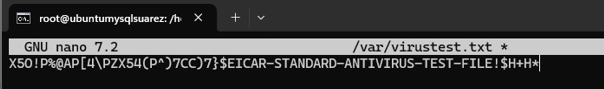


Vamos a crear un "malware" de prueba:

**nano /var/virustest.txt**

y añadimos:

**X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\***



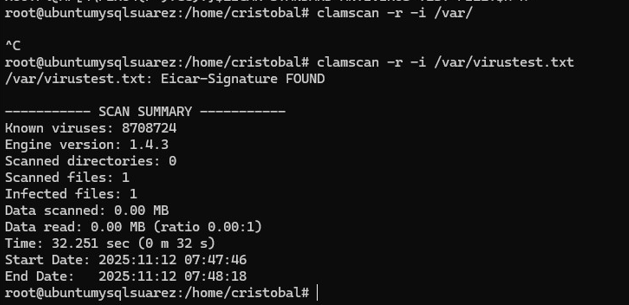


Luego ejecuta el siguiente comando:

# **clamscan -r -i /var/**

En nuestro caso:

**clamscan -r -i /var/virustest.txt**



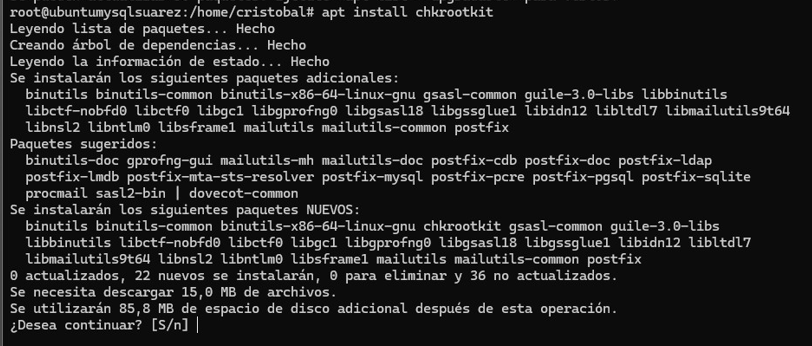
Ahora sabemos que ClamAV funciona como debe ser.

# Chkrootkit:

Te permite escanear tu equipo en busca de “rootkits”. Es el más sencillo de usar de todos.

**apt update**

**apt install chkrootkit**

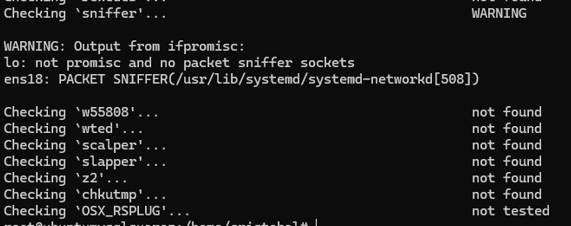


Lo ejecutamos:

**chkrootkit**

Se lleva un rato:



Solo un warning: 

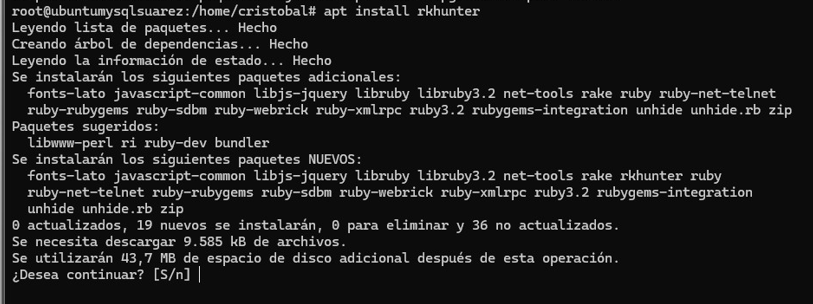
Pero según he encontrado, creo que es un falso positivo.

# Rkhunter:

Para instalar Rkhunter en Debian/Ubuntu ejecuta los siguientes comandos:

**apt update**

**apt install rkhunter**



Posteriormente, edita la configuración de rkhunter ejecutando el siguiente comando:

**nano /etc/rkhunter.conf**

Edita las siguientes variables para que tengan estos valores:

MIRRORS\_MODE=0



UPDATE\_MIRRORS=1

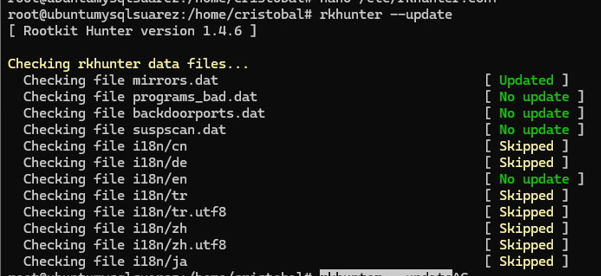


WEB\_CMD=""



El siguiente paso es actualizar las firmas:

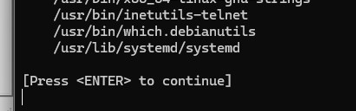
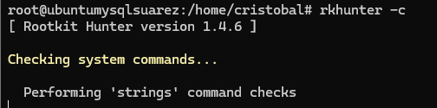
**rkhunter --update**



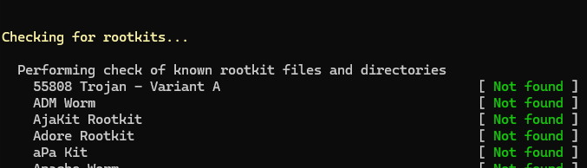
Para realizar un análisis ejecuta el siguiente comando:

**rkhunter -c**

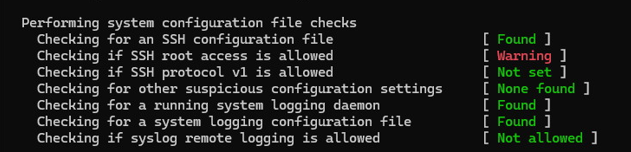
Hay que darle a ENTER para cada paso adicional.

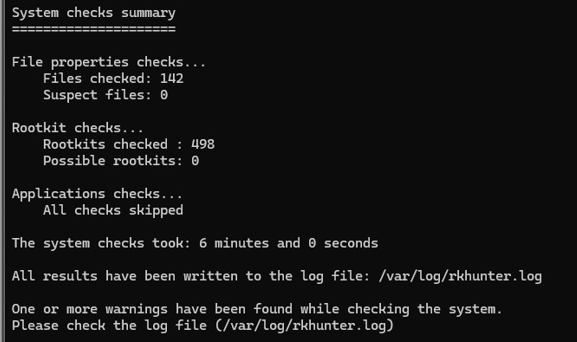


También chequea “rootkits”



Warning: En este equipo tenemos activado la conexión SSH con ROOT.

Sumario final y la ruta del archivo log.



Nos lo copiamos para que no se sobreescriba.

**cat /var/log/rkhunter.log**

**cat /var/log/rkhunter.log > /home/cristobal/rkhunter-12112025.log**



Contenido del log.



En nuestro caso no hay nada que reseñar. La configuración de SSH que he comentado antes y algunos archivos ocultos.

# LMD – Linux Malware Detect

Para instalar:

**cd /tmp**

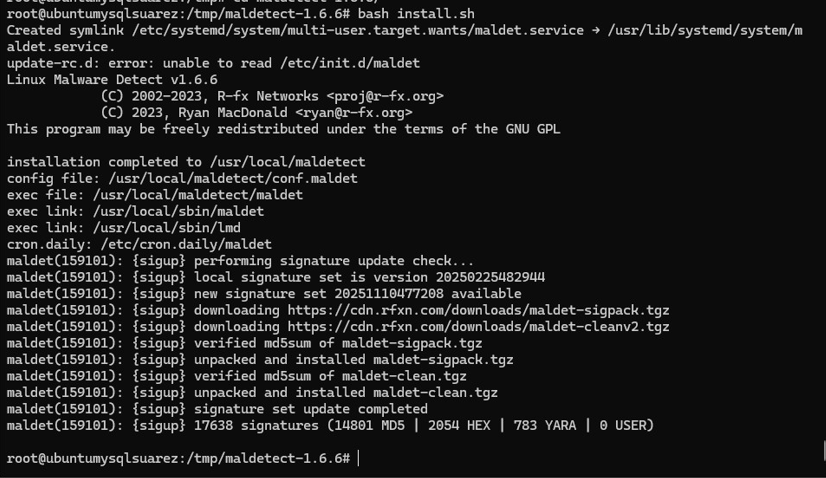
**wget http://www.rfxn.com/downloads/maldetect-current.tar.gz**

**tar -zxvf maldetect-current.tar.gz**



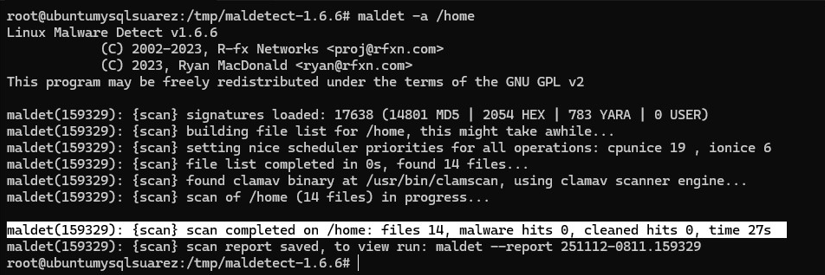
**cd maldetect-1.6.6/**

**bash install.sh**



Para ejecutar un análisis de un directorio ejecuta el siguiente comando. En nuestro caso el directorio /home.

**maldet -a /home**



Se han analizado 14 archivos con 0 incidencias.

# Lynis

**apt install lynis**

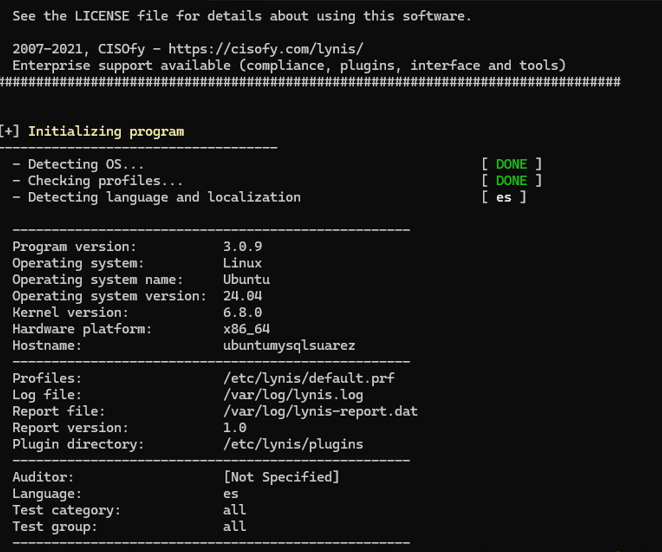


Para realizar un análisis ejecuta:

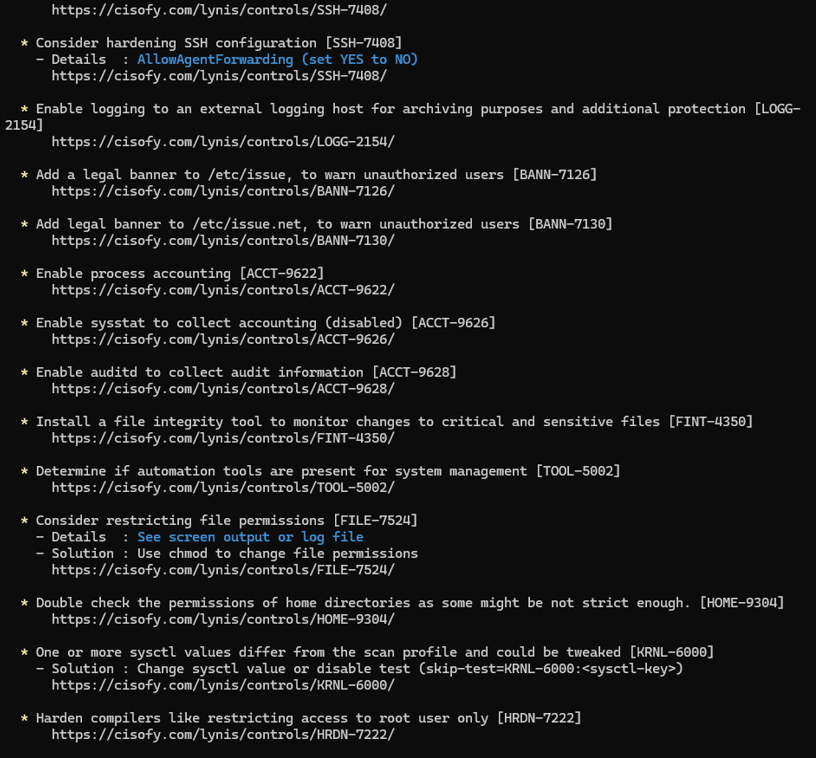
**lynis audit system**



Se lleva un rato:



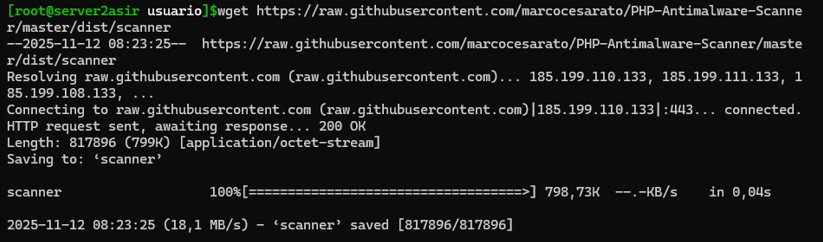
En este caso no encuentra nada. Aunque si nos da un listado de recomendaciones.



# PHP-Antimalware-Scanner

Para utilizarlo, puedes simplemente descargarlo:

**wget** [**https://raw.githubusercontent.com/marcocesarato/PHP-Antimalware-Scanner/master/dist/scanner**](https://raw.githubusercontent.com/marcocesarato/PHP-Antimalware-Scanner/master/dist/scanner)

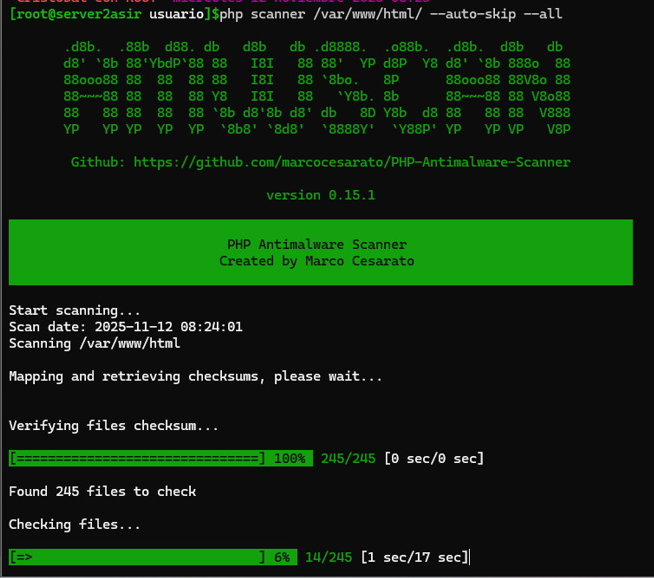


Y ejecutarlo con un CLI de PHP:

**php scanner /ruta/directorio/web/ --auto-skip --all**

En este caso al directorio donde “html” que se crea cuando instalamos Apache.

**php scanner /var/www/html/ --auto-skip --all**



Identifica algunos ficheros como malware, pero por lo que he podido leer en foros son falsos positivos.