[TÍTULO DEL DOCUMENTO]

UsuarioASIR

[NOMBRE DE LA EMPRESA] [Dirección de la compañía]

Índice

Introducción

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

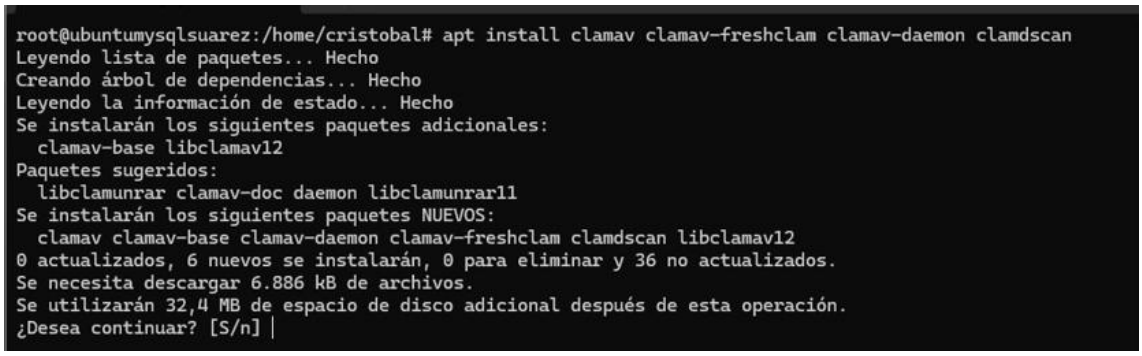
Sigue los pasos explicados en el tutorial para instalar :

- *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

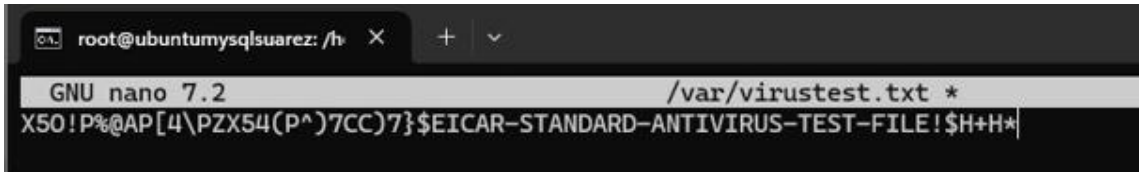
freshclam

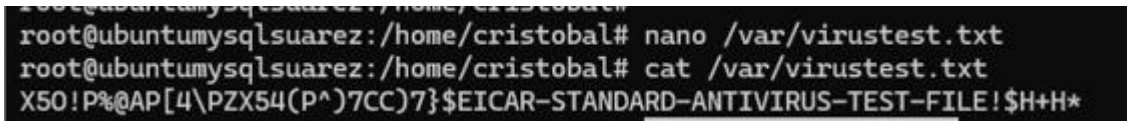
Vamos a crear un "malware" de prueba:

nano /var/virustest.txt

y añadimos:

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



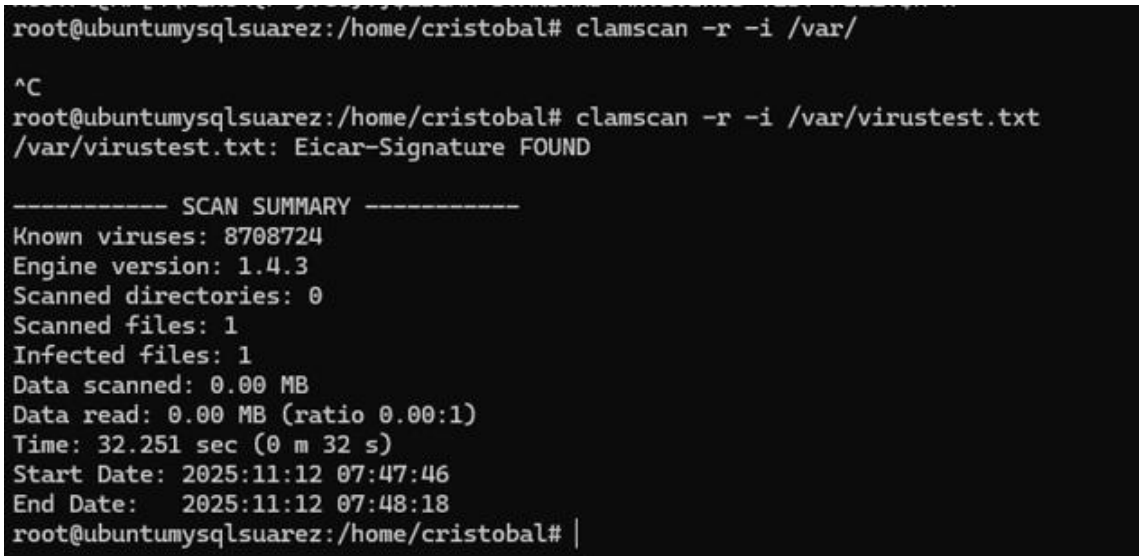


Luego ejecuta el siguiente comando:

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

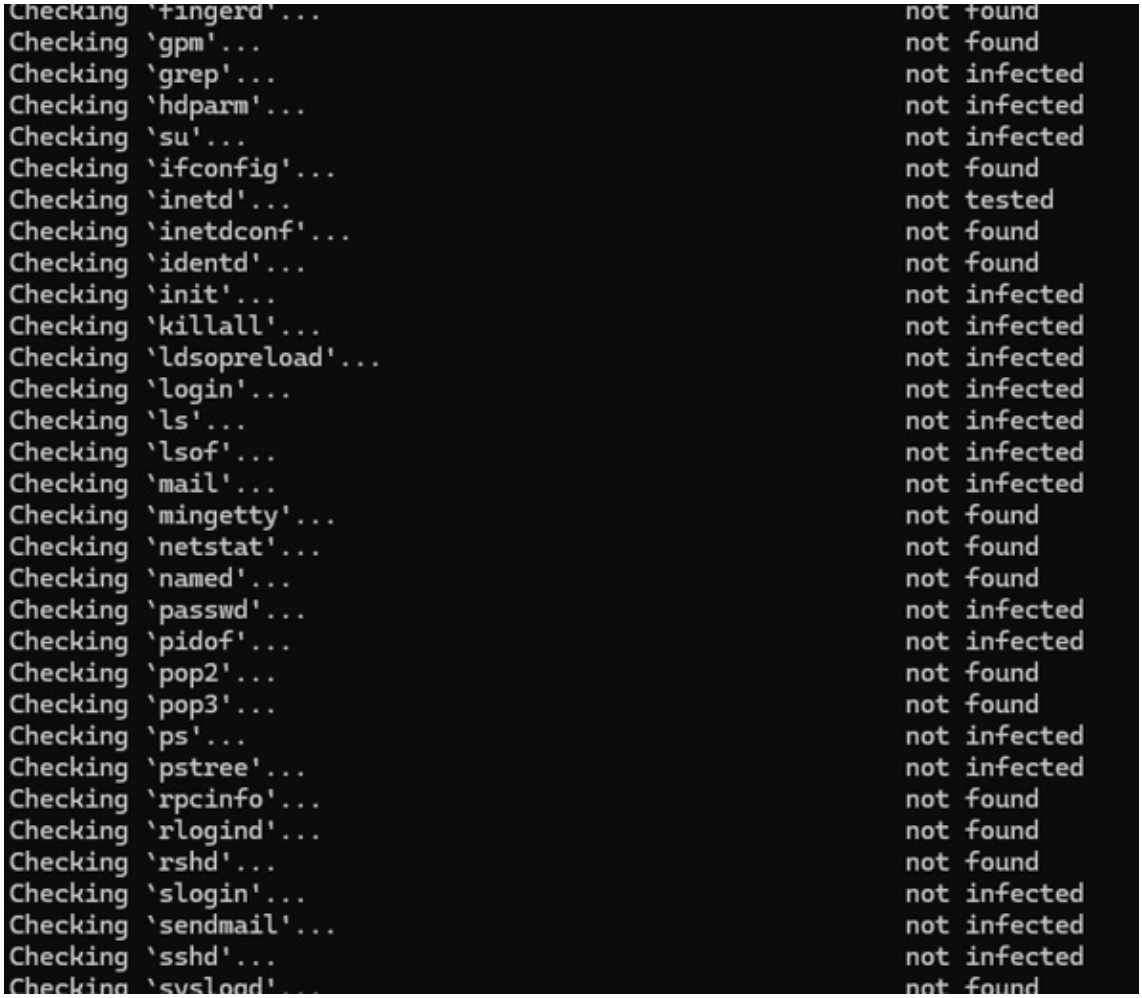
apt install chkrootkit

```
root@ubuntumysqlsuarez:/home/cristobal# apt install chkrootkit
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  binutils binutils-common binutils-x86-64-linux-gnu gsasl-common guile-3.0-libs libbinutils
  libctf-nobfd0 libctf0 libgc1 libgprofng0 libgsasl18 libgssglue1 libidn12 libltdl7 libmailutils9t64
  libnsl2 libntlm0 libsframe1 mailutils mailutils-common postfix
Paquetes sugeridos:
  binutils-doc gprofng-gui mailutils-mh mailutils-doc postfix-cdb postfix-doc postfix-ldap
  postfix-lmdb postfix-mta-sts-resolver postfix-mysql postfix-pcre postfix-pgsql postfix-sqlite
  procmail sasl2-bin | dovecot-common
Se instalarán los siguientes paquetes NUEVOS:
  binutils binutils-common binutils-x86-64-linux-gnu chkrootkit gsasl-common guile-3.0-libs
  libbinutils libctf-nobfd0 libctf0 libgc1 libgprofng0 libgsasl18 libgssglue1 libidn12 libltdl7
  libmailutils9t64 libnsl2 libntlm0 libsframe1 mailutils mailutils-common postfix
0 actualizados, 22 nuevos se instalarán, 0 para eliminar y 36 no actualizados.
Se necesita descargar 15,0 MB de archivos.
Se utilizarán 85,8 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

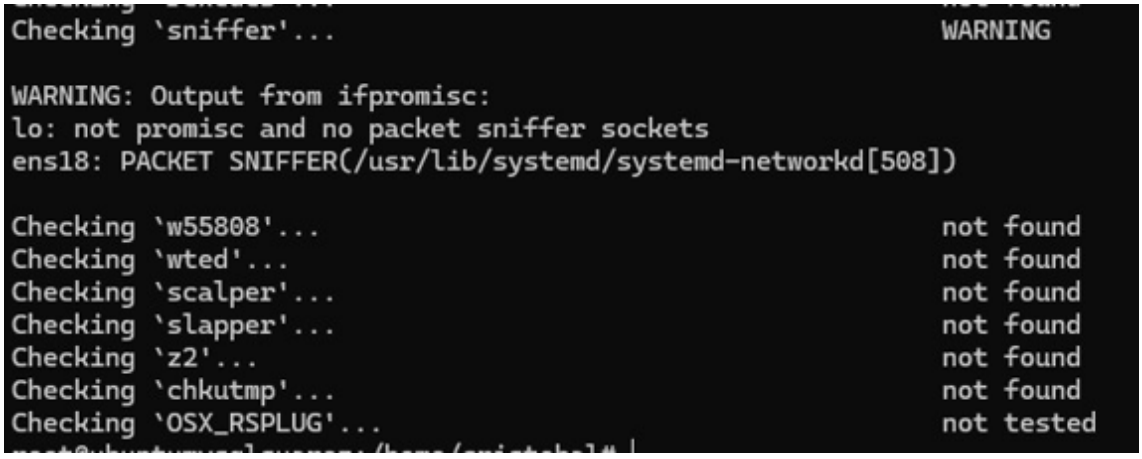
Lo ejecutamos:

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

```
root@ubuntumysqlsuarez:/home/cristobal# apt install rkhunter
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  fonts-lato javascript-common libjs-jquery libruby libruby3.2 net-tools rake ruby ruby-net-telnet
  ruby-rubygems ruby-sdbm ruby-webrick ruby-xmlrpc ruby3.2 rubygems-integration unhide unhide.rb zip
Paquetes sugeridos:
  libwww-perl ri ruby-dev bundler
Se instalarán los siguientes paquetes NUEVOS:
  fonts-lato javascript-common libjs-jquery libruby libruby3.2 net-tools rake rkhunter ruby
  ruby-net-telnet ruby-rubygems ruby-sdbm ruby-webrick ruby-xmlrpc ruby3.2 rubygems-integration
  unhide unhide.rb zip
0 actualizados, 19 nuevos se instalarán, 0 para eliminar y 36 no actualizados.
Se necesita descargar 9.585 kB de archivos.
Se utilizarán 43,7 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

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

nano /etc/rkhunter.conf

Edita las siguientes variables para que tengan estos valores:

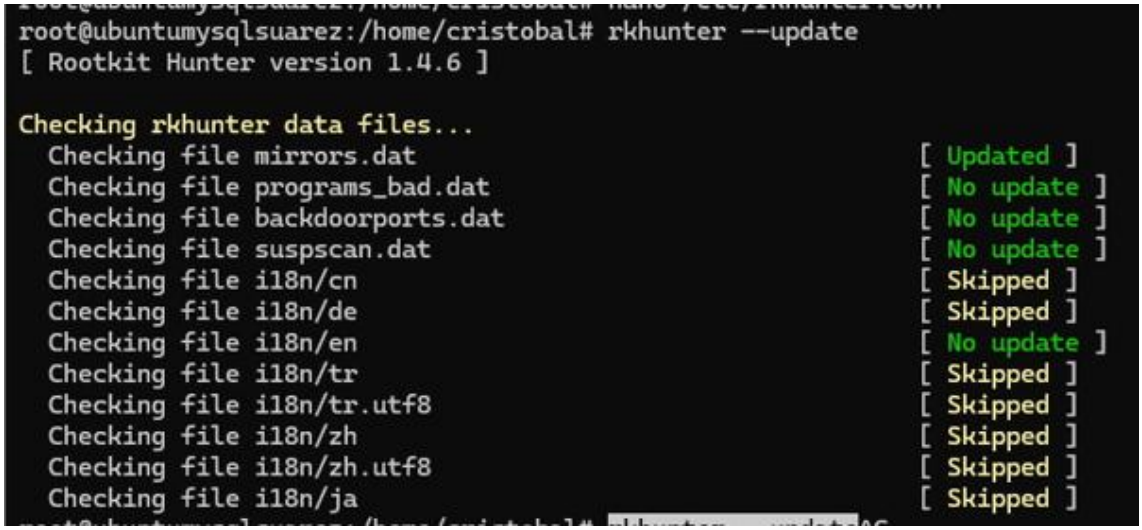
MIRRORS_MODE=0

UPDATE_MIRRORS=1

WEB_CMD=""

El siguiente paso es actualizar las firmas:

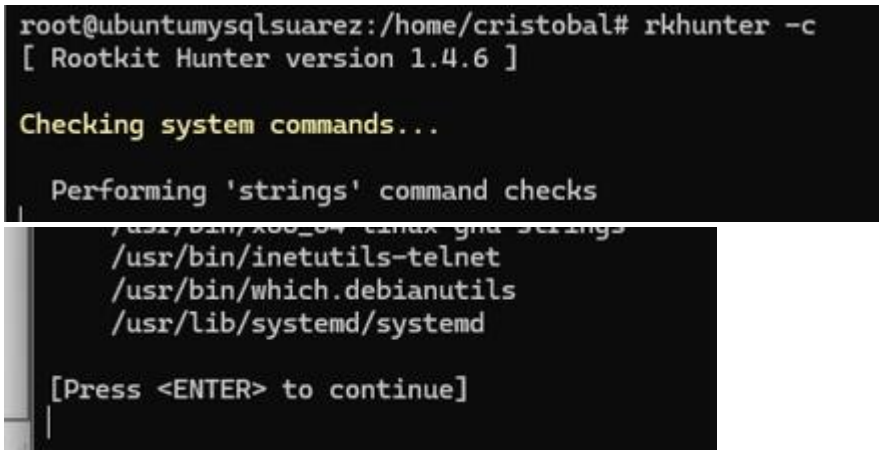
rkhunter --update



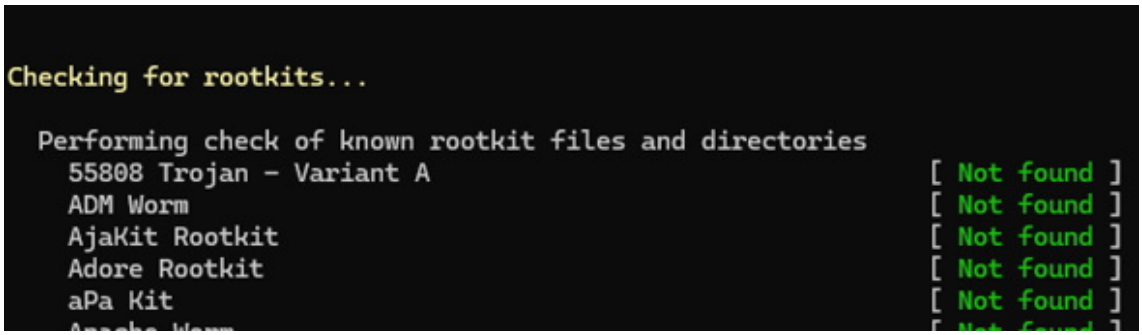
Para realizar un análisis ejecuta el siguiente comando:

rkhunter -c

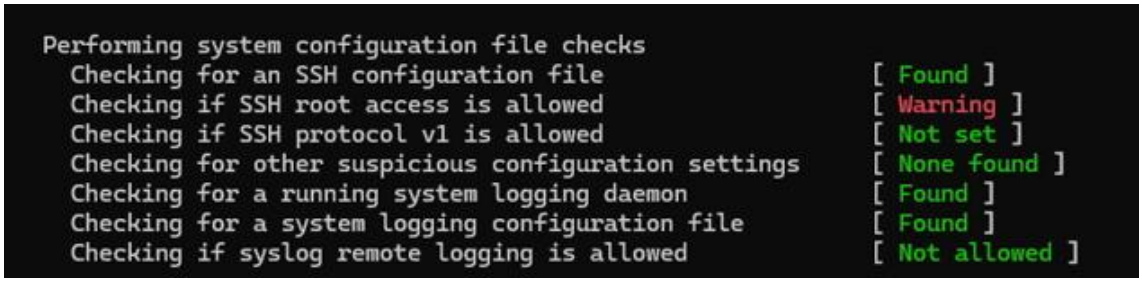
Hay que darle a ENTER para cada paso adicional.



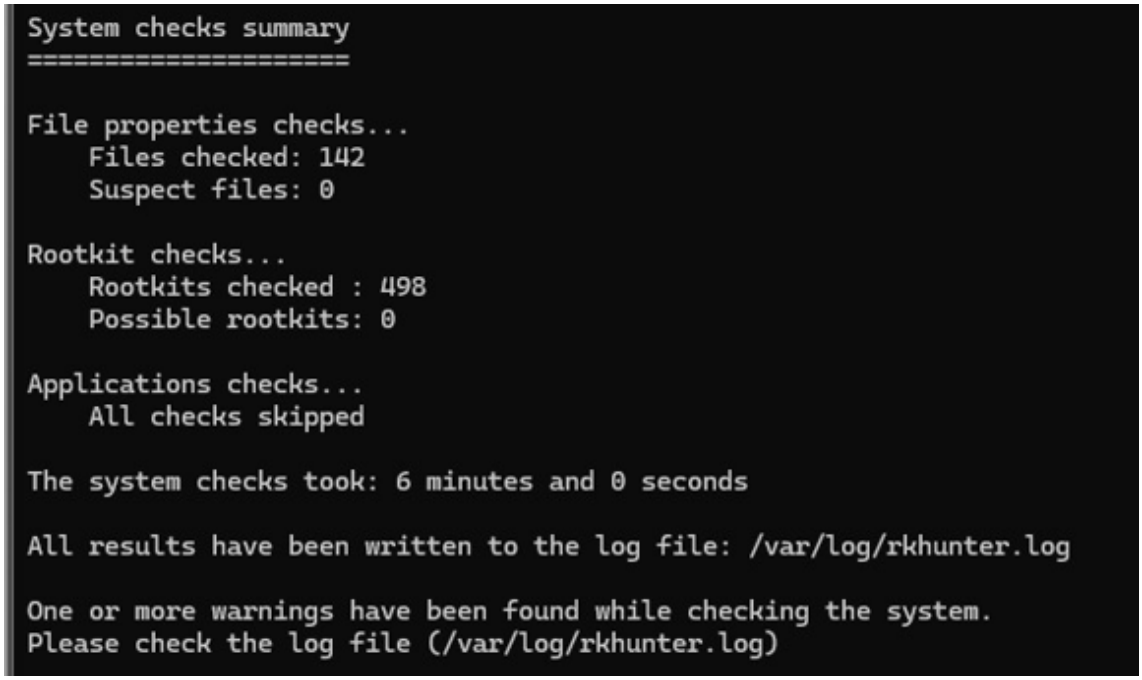
También chequea “rootkits”



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



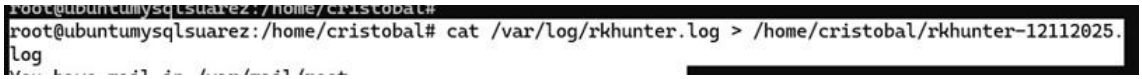
Sumario final y la ruta del archivo log.



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

```
root@ubuntumysqlsuarez:/home/cristobal# cd /tmp
root@ubuntumysqlsuarez:/tmp# wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
--2025-11-12 08:09:39--  http://www.rfxn.com/downloads/maldetect-current.tar.gz
Resolving www.rfxn.com (www.rfxn.com)... 172.67.69.110, 104.26.1.106, 104.26.0.106, ...
Connecting to www.rfxn.com (www.rfxn.com)|172.67.69.110|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1661207 (1,6M) [application/x-gzip]
Saving to: 'maldetect-current.tar.gz'

maldetect-current.tar.gz  100%[=================================>]   1,58M  --.-KB/s    in 0,05s

2025-11-12 08:09:39 (32,0 MB/s) - 'maldetect-current.tar.gz' saved [1661207/1661207]

root@ubuntumysqlsuarez:/tmp# tar -zxvf maldetect-current.tar.gz
```

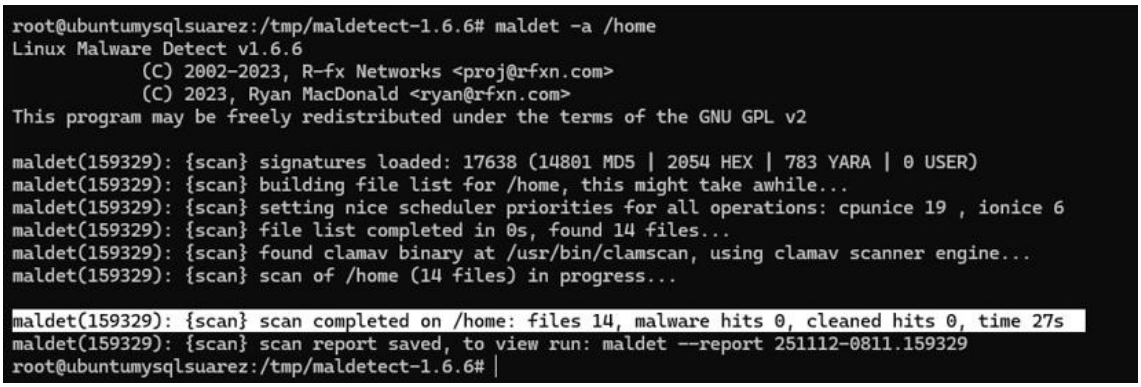
cd maldetect-1.6.6/

bash install.sh

```
root@ubuntumysqlsuarez:/tmp/maldetect-1.6.6# bash install.sh
Created symlink /etc/systemd/system/multi-user.target.wants/maldet.service → /usr/lib/systemd/system/m
aldet.service.
update-rc.d: error: unable to read /etc/init.d/maldet
Linux Malware Detect v1.6.6
            (C) 2002-2023, R-fx Networks <proj@r-fx.org>
            (C) 2023, Ryan MacDonald <ryan@r-fx.org>
This program may be freely redistributed under the terms of the GNU GPL

installation completed to /usr/local/maldetect
config file: /usr/local/maldetect/conf.maldet
exec file: /usr/local/maldetect/maldet
exec link: /usr/local/sbin/maldet
exec link: /usr/local/sbin/lmd
cron.daily: /etc/cron.daily/maldet
maldet(159101): {sigup} performing signature update check...
maldet(159101): {sigup} local signature set is version 20250225482944
maldet(159101): {sigup} new signature set 20251110477208 available
maldet(159101): {sigup} downloading https://cdn.rfxn.com/downloads/maldet-sigpack.tgz
maldet(159101): {sigup} downloading https://cdn.rfxn.com/downloads/maldet-cleanv2.tgz
maldet(159101): {sigup} verified md5sum of maldet-sigpack.tgz
maldet(159101): {sigup} unpacked and installed maldet-sigpack.tgz
maldet(159101): {sigup} verified md5sum of maldet-clean.tgz
maldet(159101): {sigup} unpacked and installed maldet-clean.tgz
maldet(159101): {sigup} signature set update completed
maldet(159101): {sigup} 17638 signatures (14801 MD5 | 2054 HEX | 783 YARA | 0 USER)

root@ubuntumysqlsuarez:/tmp/maldetect-1.6.6#
```

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

```
root@ubuntumysqlsuarez:/home/cristobal# apt install lynis
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  menu
Paquetes sugeridos:
  apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu | kde-cli-tools
  | ktsuss
Se instalarán los siguientes paquetes NUEVOS:
  lynis menu
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 36 no actualizados.
Se necesita descargar 602 kB de archivos.
Se utilizarán 3.202 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
```

Para realizar un análisis ejecuta:

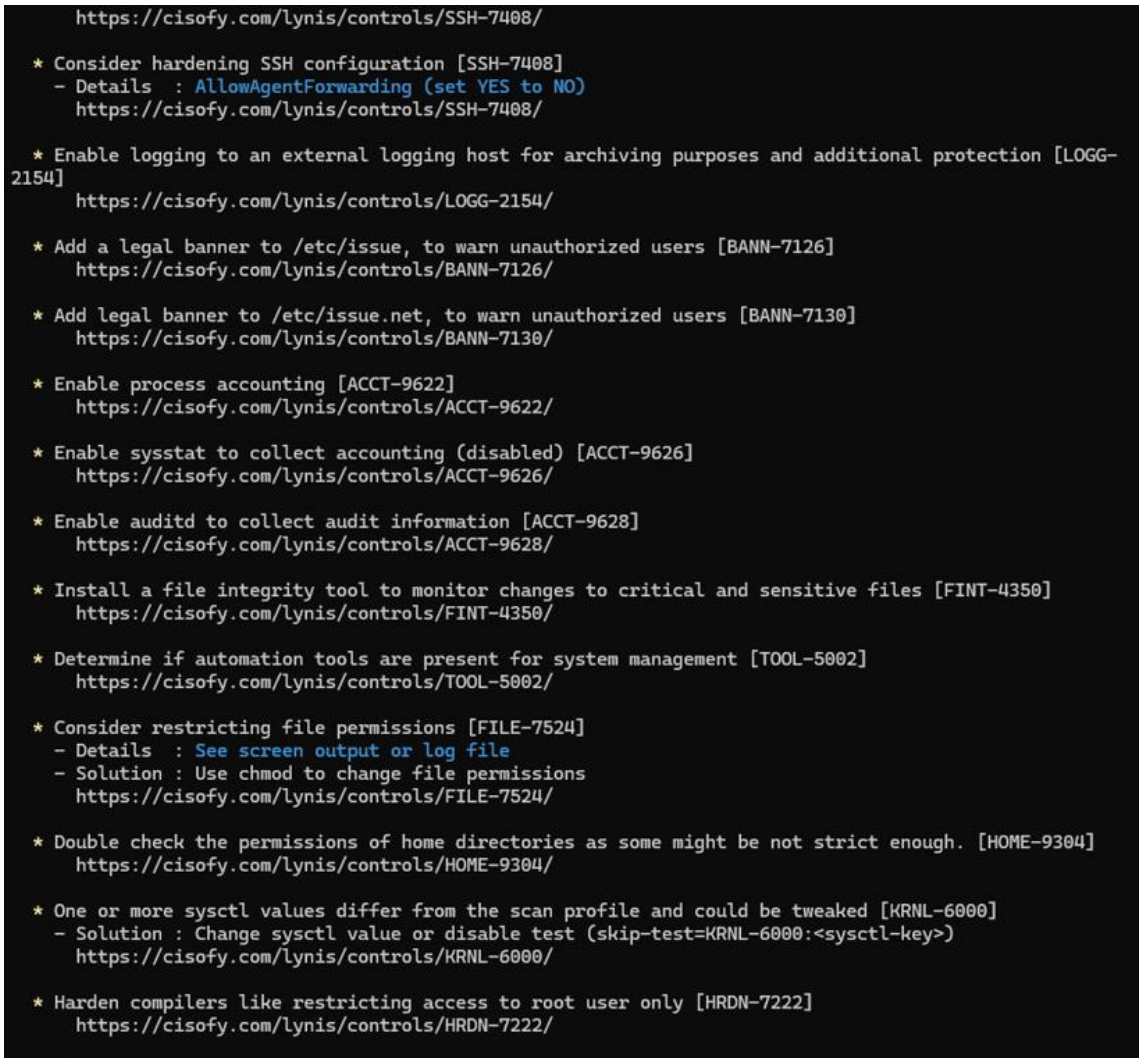
lynis audit system

```
z:/home/cristobal# lynis audit system
```

Se lleva un rato:

```
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]
  - Detecting language and localization                       [ es ]

  ---------------------------------------------------
  Program version:           3.0.9
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  24.04
  Kernel version:            6.8.0
  Hardware platform:         x86_64
  Hostname:                  ubuntumysqlsuarez
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  es
  Test category:             all
  Test group:                all
  ---------------------------------------------------
```

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

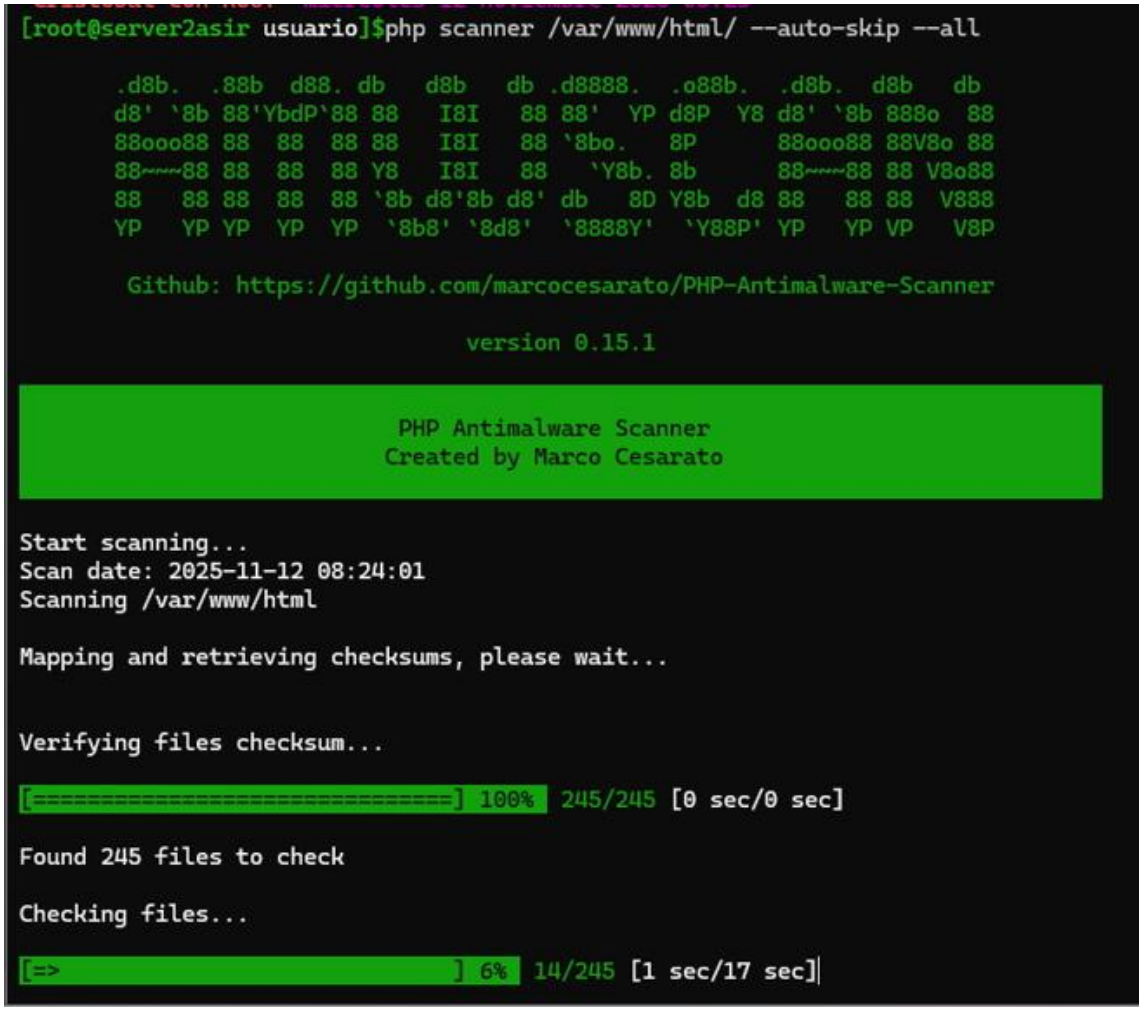
```
[root@server2asir usuario]$wget https://raw.githubusercontent.com/marcocesarato/PHP-Antimalware-Scanne
r/master/dist/scanner
--2025-11-12 08:23:25--  https://raw.githubusercontent.com/marcocesarato/PHP-Antimalware-Scanner/maste
r/dist/scanner
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 1
85.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 817896 (799K) [application/octet-stream]
Saving to: 'scanner'

scanner                  100%[=================================>] 798,73K  --.-KB/s    in 0,04s

2025-11-12 08:23:25 (18,1 MB/s) - 'scanner' saved [817896/817896]
```

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.