

[TÍTULO DEL DOCUMENTO]

UsuarioASIR

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

Índice

Introducción	0
ClamAV:.....	1
Chkrootkit:	4
Rkhunter:	6
LMD – Linux Malware Detect.....	10
Lynis	12
PHP-Antimalware-Scanner.....	14

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

```
root@ubuntumysqlsuarez:/home/cristobal# apt install clamav clamav-freshclam clamav-daemon clamdscan
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  clamav-base libclamav12
Paquetes sugeridos:
  libclamunrar clamav-doc daemon libclamunrar11
Se instalarán los siguientes paquetes NUEVOS:
  clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav12
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 36 no actualizados.
Se necesita descargar 6.886 kB de archivos.
Se utilizarán 32,4 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

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

```
root@ubuntumysqlsuarez:/home/cristobal# freshclam
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!
root@ubuntumysqlsuarez:/home/cristobal# cat /var/log/clamav/freshclam.log
Wed 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)
root@ubuntumysqlsuarez:/home/cristobal# sudo systemctl status clamav-freshclam
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/usr/lib/systemd/system/clamav-freshclam.service; disabled; preset: enabled)
   Active: active (running) since Wed 2025-11-12 07:39:24 UTC; 1min 47s ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://docs.clamav.net/
   Main PID: 1865 (freshclam)
     Tasks: 1 (Limit: 4605)
    Memory: 236.0M (peak: 849.5M)
       CPU: 31.194s
    CGroup: /system.slice/clamav-freshclam.service
            └─1865 /usr/bin/freshclam -d --foreground=true

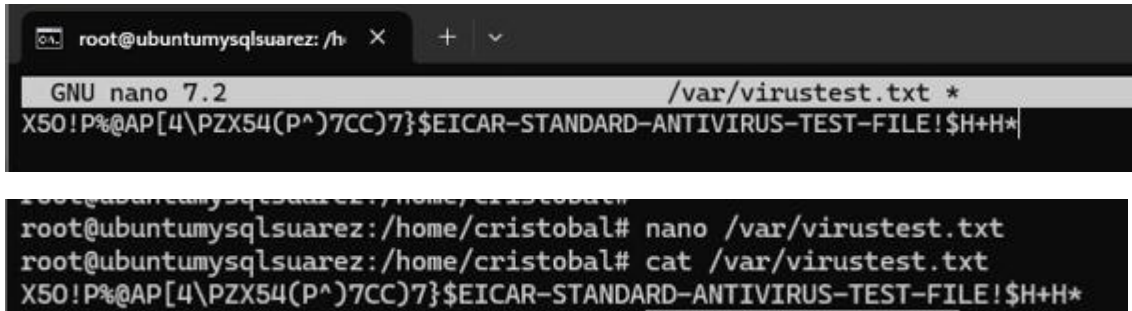
nov 12 07:39:37 ubuntumysqlsuarez freshclam[1865]: Wed Nov 12 07:39:37 2025 -> daily.cvd updated (ver>
nov 12 07:39:37 ubuntumysqlsuarez freshclam[1865]: Wed Nov 12 07:39:37 2025 -> main database availabl>
nov 12 07:39:44 ubuntumysqlsuarez freshclam[1865]: Testing database: '/var/lib/clamav/tmp.7d7e788ddb/>
nov 12 07:39:56 ubuntumysqlsuarez freshclam[1865]: Database test passed.
nov 12 07:39:56 ubuntumysqlsuarez freshclam[1865]: Wed Nov 12 07:39:56 2025 -> main.cvd updated (vers>
nov 12 07:39:56 ubuntumysqlsuarez freshclam[1865]: Wed Nov 12 07:39:56 2025 -> bytecode database avai>
nov 12 07:39:56 ubuntumysqlsuarez freshclam[1865]: Testing database: '/var/lib/clamav/tmp.7d7e788ddb/>
nov 12 07:39:56 ubuntumysqlsuarez freshclam[1865]: Database test passed.
nov 12 07:39:56 ubuntumysqlsuarez freshclam[1865]: Wed Nov 12 07:39:56 2025 -> bytecode.cvd updated (>
nov 12 07:39:56 ubuntumysqlsuarez freshclam[1865]: WARNING: Clamd was NOT notified: Can't connect to >
lines 1-23/23 (END)
root@ubuntumysqlsuarez:/home/cristobal# sudo systemctl stop clamav-freshclam
root@ubuntumysqlsuarez:/home/cristobal# freshclam
ClamAV update process started at Wed Nov 12 07:41:24 2025
Wed Nov 12 07:41:24 2025 -> daily.cvd database is up-to-date (version: 27819, sigs: 2077025, f-level: 90, builder: svc.clamav-publisher)
Wed Nov 12 07:41:24 2025 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Wed Nov 12 07:41:24 2025 -> bytecode.cvd database is up-to-date (version: 339, sigs: 80, f-level: 90, builder: nrandolp)
root@ubuntumysqlsuarez:/home/cristobal# |
```

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*



The screenshot shows a terminal window with the title 'root@ubuntumysqlsuarez: /h'. The first part shows the nano editor opening the file /var/virustest.txt and the user pasting the EICAR test string. The second part shows the user running 'cat /var/virustest.txt' and seeing the same string output.

```
GNU nano 7.2 /var/virustest.txt *
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

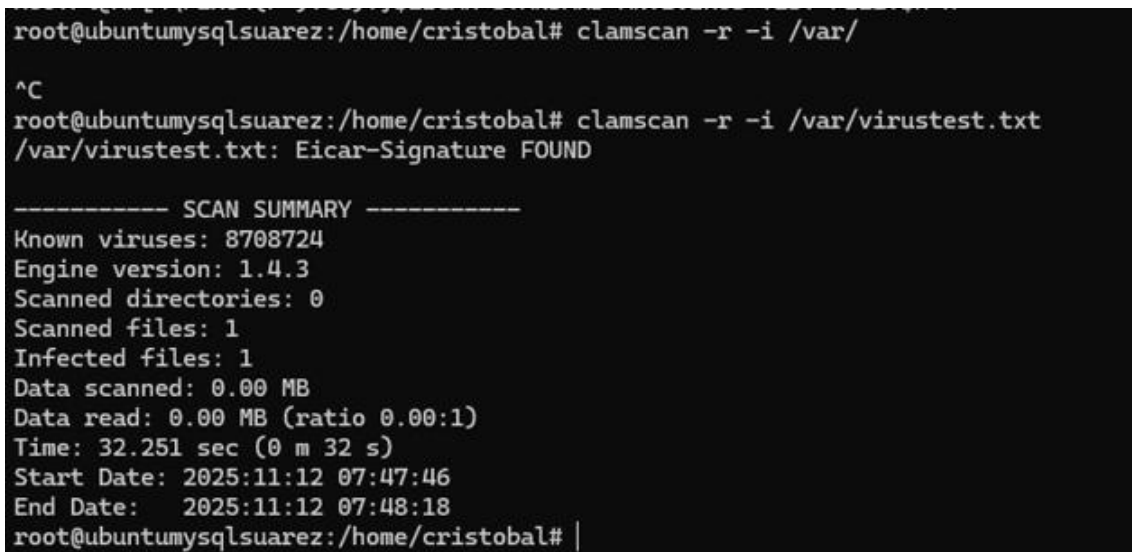
root@ubuntumysqlsuarez:/home/cristobal# nano /var/virustest.txt
root@ubuntumysqlsuarez:/home/cristobal# cat /var/virustest.txt
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Luego ejecuta el siguiente comando:

clamscan -r -i /var/

En nuestro caso:

clamscan -r -i /var/virustest.txt



The screenshot shows the terminal output of the clamscan command. It first shows the command being run, then a carriage return (^C) is pressed. The command is run again, and the output shows that the EICAR signature was found in the file. A detailed scan summary follows, showing statistics like the number of known viruses, engine version, and scan time.

```
root@ubuntumysqlsuarez:/home/cristobal# clamscan -r -i /var/
^C
root@ubuntumysqlsuarez:/home/cristobal# clamscan -r -i /var/virustest.txt
/var/virustest.txt: Eicar-Signature FOUND

----- SCAN SUMMARY -----
Known viruses: 8708724
Engine version: 1.4.3
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 32.251 sec (0 m 32 s)
Start Date: 2025:11:12 07:47:46
End Date: 2025:11:12 07:48:18
root@ubuntumysqlsuarez:/home/cristobal#
```

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 gssapi-common guile-3.0-libs libbinutils
  libbtf-nobfd0 libbtf0 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 gssapi-common guile-3.0-libs
  libbinutils libbtf-nobfd0 libbtf0 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:

```

Checking 'fingerd'... not found
Checking 'gpm'... not found
Checking 'grep'... not infected
Checking 'hdparm'... not infected
Checking 'su'... not infected
Checking 'ifconfig'... not found
Checking 'inetd'... not tested
Checking 'inetdconf'... not found
Checking 'identd'... not found
Checking 'init'... not infected
Checking 'killall'... not infected
Checking 'ldsopreload'... not infected
Checking 'login'... not infected
Checking 'ls'... not infected
Checking 'lsof'... not infected
Checking 'mail'... not infected
Checking 'mingetty'... not found
Checking 'netstat'... not found
Checking 'named'... not found
Checking 'passwd'... not infected
Checking 'pidof'... not infected
Checking 'pop2'... not found
Checking 'pop3'... not found
Checking 'ps'... not infected
Checking 'pstree'... not infected
Checking 'rpcinfo'... not found
Checking 'rlogind'... not found
Checking 'rshd'... not found
Checking 'slogin'... not infected
Checking 'sendmail'... not infected
Checking 'sshd'... not infected
Checking 'syslogd'... not found

```

Solo un warning:

```

Checking 'sniffer'... WARNING

WARNING: Output from ifpromisc:
lo: not promisc and no packet sniffer sockets
ens18: PACKET SNIFFER(/usr/lib/systemd/systemd-networkd[508])

Checking 'w55808'... not found
Checking 'wted'... not found
Checking 'scalper'... not found
Checking 'slapper'... not found
Checking 'z2'... not found
Checking 'chkutmp'... not found
Checking 'OSX_RSPLUG'... not tested

```

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

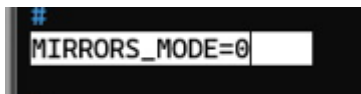
```
root@ubuntumysqlsuarez:/home/cristobal# apt install rkhunter
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
 fonts-lato javascript-common libjs-jquery libruby libruby3.2 net-tools 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

A screenshot of the nano text editor showing the configuration line MIRRORS_MODE=0. The cursor is at the end of the line.

UPDATE_MIRRORS=1

A screenshot of the nano text editor showing the configuration line UPDATE_MIRRORS=1. The cursor is at the end of the line.

WEB_CMD=""

A screenshot of the nano text editor showing the configuration line WEB_CMD=" ". The cursor is at the end of the line.

El siguiente paso es actualizar las firmas:

rkhunter --update

```
root@ubuntumyslsuarez:/home/cristobal# rkhunter --update
[ Rootkit Hunter version 1.4.6 ]

Checking rkhunter data files...
Checking file mirrors.dat [ Updated ]
Checking file programs_bad.dat [ No update ]
Checking file backdoorports.dat [ No update ]
Checking file suspscan.dat [ No update ]
Checking file i18n/cn [ Skipped ]
Checking file i18n/de [ Skipped ]
Checking file i18n/en [ No update ]
Checking file i18n/tr [ Skipped ]
Checking file i18n/tr.utf8 [ Skipped ]
Checking file i18n/zh [ Skipped ]
Checking file i18n/zh.utf8 [ Skipped ]
Checking file i18n/ja [ Skipped ]
```

Para realizar un análisis ejecuta el siguiente comando:

rkhunter -c

Hay que darle a ENTER para cada paso adicional.

```
root@ubuntumyslsuarez:/home/cristobal# rkhunter -c
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

Performing 'strings' command checks
/usr/bin/x86_64-linux-gnu-strings
/usr/bin/inetutils-telnet
/usr/bin/which.debianutils
/usr/lib/systemd/systemd

[Press <ENTER> to continue]
```

También chequea “rootkits”

```
Checking for rootkits...

Performing check of known rootkit files and directories
55808 Trojan - Variant A [ Not found ]
ADM Worm [ Not found ]
AjaKit Rootkit [ Not found ]
Adore Rootkit [ Not found ]
aPa Kit [ Not found ]
Apache Worm [ Not found ]
```

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

```
Performing system configuration file checks
  Checking for an SSH configuration file           [ Found ]
  Checking if SSH root access is allowed           [ Warning ]
  Checking if SSH protocol v1 is allowed           [ Not set ]
  Checking for other suspicious configuration settings [ None found ]
  Checking for a running system logging daemon     [ Found ]
  Checking for a system logging configuration file  [ Found ]
  Checking if syslog remote logging is allowed      [ Not allowed ]
```

Sumario final y la ruta del archivo log.

```
System checks summary
=====

File properties checks...
  Files checked: 142
  Suspect files: 0

Rootkit checks...
  Rootkits checked : 498
  Possible rootkits: 0

Applications checks...
  All checks skipped

The system checks took: 6 minutes and 0 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

Nos lo copiamos para que no se sobrescriba.

cat /var/log/rkhunter.log

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

```
root@ubuntu:mysqlsuarez:/home/cristobal#
root@ubuntu:mysqlsuarez:/home/cristobal# cat /var/log/rkhunter.log > /home/cristobal/rkhunter-12112025.
log
```

Contenido del log.

```

[08:05:10] Checking if SSH root access is allowed [ Warning ]
[08:05:10] Warning: The SSH and rkhunter configuration options should be the same:
[08:05:10] SSH configuration option 'PermitRootLogin': yes
[08:05:10] Rkhunter configuration option 'ALLOW_SSH_ROOT_USER': no
[08:05:10] Checking if SSH protocol v1 is allowed [ Not set ]
[08:05:10] Checking for other suspicious configuration settings [ None found ]
[08:05:10]
[08:05:10] Info: Starting test name 'system_configs_syslog'
[08:05:10] Checking for a running system logging daemon [ Found ]
[08:05:10] Info: A running 'rsyslog' daemon has been found.
[08:05:10] Info: A running 'systemd-journald' daemon has been found.
[08:05:10] Info: Found an rsyslog configuration file: /etc/rsyslog.conf
[08:05:10] Info: Found a systemd configuration file: /etc/systemd/journald.conf
[08:05:11] Checking for a system logging configuration file [ Found ]
[08:05:11] Checking if syslog remote logging is allowed [ Not allowed ]
[08:05:11]
[08:05:11] Info: Starting test name 'filesystem'
[08:05:11] Performing filesystem checks
[08:05:11] Info: SCAN_MODE_DEV set to 'THOROUGH'
[08:05:19] Checking /dev for suspicious file types [ Warning ]
[08:05:19] Warning: Suspicious file types found in /dev:
[08:05:19] /dev/shm/PostgreSQL.2194586966: data
[08:05:19] /dev/shm/PostgreSQL.1311151378: data
[08:05:19] Checking for hidden files and directories [ Warning ]
[08:05:19] Warning: Hidden file found: /etc/.resolv.conf.systemd-resolved.bak: ASCII text
[08:05:19] Warning: Hidden file found: /etc/.updated: ASCII text
[08:05:19] Checking for missing log files [ Skipped ]
[08:05:19] Info: No missing log file names configured.
[08:05:19] Checking for empty log files [ Skipped ]
[08:05:19] Info: No empty log file names configured.
[08:05:32]
[08:05:32] Info: Test 'apps' disabled at users request.
[08:05:32]
[08:05:32] System checks summary
[08:05:32] =====
[08:05:32]
[08:05:32] File properties checks...
[08:05:32] Files checked: 142
[08:05:32] Suspect files: 0
[08:05:32]
[08:05:32] Rootkit checks...
[08:05:32] Rootkits checked : 498
[08:05:32] Possible rootkits: 0
[08:05:33]
[08:05:33] Applications checks...
[08:05:33] All checks skipped
[08:05:33]
[08:05:33] The system checks took: 6 minutes and 0 seconds
[08:05:33]
[08:05:33] Info: End date is mié 12 nov 2025 08:05:33 UTC
root@ubuntumysqlsuarez:/home/cristobal# |

```

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/maldet.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

```
root@ubuntumysqlsuarez:/tmp/maldetect-1.6.6# maldet -a /home
Linux Malware Detect v1.6.6
  (C) 2002-2023, R-fx Networks <proj@rfxn.com>
  (C) 2023, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(159329): {scan} signatures loaded: 17638 (14801 MD5 | 2054 HEX | 783 YARA | 0 USER)
maldet(159329): {scan} building file list for /home, this might take awhile...
maldet(159329): {scan} setting nice scheduler priorities for all operations: cpunice 19 , ionice 6
maldet(159329): {scan} file list completed in 0s, found 14 files...
maldet(159329): {scan} found clamav binary at /usr/bin/clamscan, using clamav scanner engine...
maldet(159329): {scan} scan of /home (14 files) in progress...

maldet(159329): {scan} scan completed on /home: files 14, malware hits 0, cleaned hits 0, time 27s
maldet(159329): {scan} scan report saved, to view run: maldet --report 251112-0811.159329
root@ubuntumysqlsuarez:/tmp/maldetect-1.6.6#
```

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.

```
https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : AllowAgentForwarding (set YES to NO)
https://cisofy.com/lynis/controls/SSH-7408/

* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
https://cisofy.com/lynis/controls/LOGG-2154/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
https://cisofy.com/lynis/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
https://cisofy.com/lynis/controls/BANN-7130/

* Enable process accounting [ACCT-9622]
https://cisofy.com/lynis/controls/ACCT-9622/

* Enable sysstat to collect accounting (disabled) [ACCT-9626]
https://cisofy.com/lynis/controls/ACCT-9626/

* Enable auditd to collect audit information [ACCT-9628]
https://cisofy.com/lynis/controls/ACCT-9628/

* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
https://cisofy.com/lynis/controls/FINT-4350/

* Determine if automation tools are present for system management [TOOL-5002]
https://cisofy.com/lynis/controls/TOOL-5002/

* Consider restricting file permissions [FILE-7524]
- Details : See screen output or log file
- Solution : Use chmod to change file permissions
https://cisofy.com/lynis/controls/FILE-7524/

* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
https://cisofy.com/lynis/controls/HOME-9304/

* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
https://cisofy.com/lynis/controls/KRNL-6000/

* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/lynis/controls/HRDN-7222/
```


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-Scanner/master/dist/scanner
--2025-11-12 08:23:25-- https://raw.githubusercontent.com/marcocesarato/PHP-Antimalware-Scanner/master/dist/scanner
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 185.199.108.133, ...
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

```
[root@server2asir usuario]$php scanner /var/www/html/ --auto-skip --all
```

```
.d8b. .88b d88. db d8b db .d8888. .o88b. .d8b. d8b db
d8' `8b 88'YbdP`88 88 I8I 88 88' YP d8P Y8 d8' `8b 888o 88
88ooo88 88 88 88 88 I8I 88 `8bo. 8P 88ooo88 88V8o 88
88~~~~88 88 88 88 Y8 I8I 88 `Y8b. 8b 88~~~~88 88 V8o88
88 88 88 88 88 `8b d8'8b d8' db 8D Y8b d8 88 88 88 V888
YP YP YP YP YP `8b8' `8d8' `8888Y' `Y88P' YP YP VP V8P
```

Github: <https://github.com/marcocesarato/PHP-Antimalware-Scanner>

version 0.15.1

PHP Antimalware Scanner
Created by Marco Cesarato

Start scanning...

Scan date: 2025-11-12 08:24:01

Scanning /var/www/html

Mapping and retrieving checksums, please wait...

Verifying files checksum...

[=====] 100% 245/245 [0 sec/0 sec]

Found 245 files to check

Checking files...

[=>] 6% 14/245 [1 sec/17 sec]

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

```
SUMMARY

Files scanned: 245
Files edited: 0
Files quarantined: 0
Files whitelisted: 0
Files ignored: 8

Malware detected: 8
Malware removed: 0

Files ignored:
/var/www/html/biblioteca/.git/hooks/pre-commit.sample
/var/www/html/biblioteca/Assets/js/vfs_fonts.js
/var/www/html/biblioteca/Assets/js/pace.min.js
/var/www/html/biblioteca/Assets/js/pdfmake.min.js
/var/www/html/biblioteca/Views/Usuarios/index.php
/var/www/html/biblioteca/Views/index.php
/var/www/html/biblioteca/Models/UsuariosModel.php
/var/www/html/biblioteca/Controllers/Usuarios.php

Cristobal con ROOT  miércoles 12 noviembre 2025 08:24
[root@server2asir usuario]$
```