

## Rootkit

Instalamos chkrootkit, como se muestra en la figura 1.

```
root@ignacio-leal -> /h/s/D/p/practica2
# apt install chkrootkit
Reading package lists... Done
Building dependency tree... Done
The following NEW packages will be installed:
  chkrootkit
0 upgraded, 1 newly installed, 0 to remove and 19 not upgraded.
Need to get 326 kB of archives.
After this operation, 1,037 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 chkrootkit amd64 0.50-3.2 [326 kB]
Fetched 326 kB in 0s (421 kB/s)
Preconfiguring packages ...
Selecting previously unselected package chkrootkit.
(Reading database ... 279891 files and directories currently installed.)
Preparing to unpack .../chkrootkit_0.50-3.2_amd64.deb ...
Unpacking chkrootkit (0.50-3.2) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up chkrootkit (0.50-3.2) ...
root@ignacio-leal -> /h/s/D/p/practica2
```

*Figura 1. Instalación chkrootkit.*

Ahora ejecutamos **chkrootkit**, como se muestra en las figuras 2, 3 y 4.

```

root@ignacio-leal -> /h/s/d/p/practica2
# chkrootkit
ROOTDIR is '/'
Checking 'amd'... not found
Checking 'basename'... not infected
Checking 'biff'... not found
Checking 'chfn'... not infected
Checking 'chsh'... not infected
Checking 'cron'... not infected
Checking 'crontab'... not infected
Checking 'date'... not infected
Checking 'du'... not infected
Checking 'dirname'... not infected
Checking 'echo'... not infected
Checking 'egrep'... not infected
Checking 'env'... not infected
Checking 'find'... not infected
Checking 'fingerd'... not found
Checking 'gpm'... not found
Checking 'grep'... not infected
Checking 'hdparm'... not infected
Checking 'su'... not infected
Checking 'ifconfig'... not infected
Checking 'inetd'... not infected
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 found
Checking 'mingetty'... not found
Checking 'netstat'... not infected
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 found
Checking 'sshd'... not infected
Checking 'syslogd'... not tested
Checking 'tar'... not infected
Checking 'tcpd'... not infected
Checking 'tcpdump'... not infected
Checking 'top'... not infected
Checking 'telnetd'... not found
Checking 'timed'... not found
Checking 'traceroute'... not found
Checking 'vdir'... not infected
Checking 'w'... not infected

```

Figura 2. Ejecución chkrootkit.

```

Checking 'win'... not infected
Checking 'write'... not infected
Checking 'aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for rootkit HlDrootkit's default files... nothing found
Searching for rootkit t0rn's default files... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for rootkit Lion's default files... nothing found
Searching for rootkit RSHA's default files... nothing found
Searching for rootkit RH-Sharp's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while... The following suspicious files and directories were found:
/usr/lib/python2.7/dist-packages/volatility/plugins/community/.git /usr/lib/python2.7/dist-packages/volatility/plugins/debug/.build-id /usr/lib/jvm/.java-1.7.0-openjdk-amd64.jinfo /lib/modules/4.4.0-97-generic/vdso/.build-id /lib/modules/4.4.0-97-generic/vdso/.modules
/usr/lib/python2.7/dist-packages/volatility/plugins/community/.git /usr/lib/debug/.build-id /lib/modules/4.4.0-97-generic/vdso/.modules
Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for LOC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for Suckit rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Gold2 rootkit... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for AjaKit rootkit default files and dirs... nothing found
Searching for zaRWt rootkit default files and dirs... nothing found
Searching for Madalin rootkit default files... nothing found
Searching for Fu rootkit default files... nothing found
Searching for ESRK rootkit default files... nothing found
Searching for rootdoor... nothing found
Searching for ENVYELKM rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for Linux/Ebury - Operation Windigo ssh... Possible Linux/Ebury - Operation Windigo installed
Searching for 64-bit Linux Rootkit ... nothing found
Searching for 64-bit Linux Rootkit modules... nothing found
Searching for suspect PHP files... nothing found
Searching for anomalies in shell history files... nothing found
Checking 'asp'... not infected
Checking 'bindshell'... not infected
Checking 'lkm'... chkproc: nothing detected

```

Figura 3. Ejecución chkrootkit.

```

Checking 'lkm'...
chkdhrs: nothing detected
Checking 'rexedcs'...
not found
Checking 'sniffer'...
lo: not promisc and no packet sniffer sockets
ens33: PACKET SNIFFER(/sbin/dhclient[3321])
docker0: not promisc and no packet sniffer sockets
Checking 'w55808'...
not infected
Checking 'wted'...
chkwtmp: nothing deleted
Checking 'scalper'...
not infected
Checking 'slapper'...
not infected
Checking 'z2'...
user sansforensics deleted or never logged from lastlog!
Checking 'chkutmp'...
The tty of the following user process(es) were not found
in /var/run/utmp !
! RUID PID TTY CMD
! root 2293 pts/17 bash
! root 3948 pts/17 /bin/sh /usr/sbin/chkrootkit
! root 4606 pts/17 ./chkutmp
! root 4608 pts/17 ps axk tty,ruser,args -o tty,pid,ruser,args
! root 4607 pts/17 sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root 2292 pts/17 su
! root 2291 pts/17 sudo su
! sansfor+ 2124 pts/17 bash
chkutmp: nothing deleted
Checking 'OSX_RSPLUG'...
not infected
root@iogacio-1eal -> /h/s/D/p/practica2

```

Figura 4. Ejecución chkrootkit.

Al terminar la búsqueda de algún posible rootkit, nos mostrará si encontró alguno, en este caso no se encontró ninguno, la parte de configuración solo cuenta con tres opciones, las cuales son:

- Análisis diario.
- Análisis silencioso.
- Prevenir falsos positivos

La configuración por defecto se muestra en la figura 5.

```
root@ignacio-leal -> /h/s/D/p/practica2
# cat /etc/chkrootkit.conf
RUN_DAILY="false"
RUN_DAILY_OPTS="-q"
DIFF_MODE="false"
```

Figura 5. Configuración por defecto de chkrootkit.

Si cambiamos la primera opción a *true* se realizará un escaneo diario, con el script que se encuentra en */etc/cron.daily/chkrootkit*, la opción *DIFF\_MODE*, nos ayuda a prevenir falsos positivos ya que compara la salida generada con la salida esperada.

Instalamos rkhunter como se muestra en la figura 6.

```
root@ignacio-leal -> /h/s/D/p/practica2
# apt install rkhunter
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  bsd-mailx fonts-lato liblockfile-bin liblockfile1 libruby2.3 postfix rake
Suggested packages:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre sasl2-bin dovecot
The following NEW packages will be installed:
  bsd-mailx fonts-lato liblockfile-bin liblockfile1 libruby2.3 postfix rake
  unhide.rb
0 upgraded, 18 newly installed, 0 to remove and 680 not upgraded.
Need to get 2,998 kB/7,363 kB of archives.
After this operation, 32.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libruby2.3
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 ruby2.3
Fetched 2,998 kB in 3s (763 kB/s)
Preconfiguring packages ...
Selecting previously unselected package fonts-lato.
(Reading database ... 279917 files and directories currently installed.)
Preparing to unpack ../fonts-lato_2.0-1_all.deb ...
Unpacking fonts-lato (2.0-1) ...
Selecting previously unselected package liblockfile-bin.
Preparing to unpack ../liblockfile-bin_1.09-6ubuntu1_amd64.deb ...
Unpacking liblockfile-bin (1.09-6ubuntu1) ...
Selecting previously unselected package liblockfile1:amd64.
Preparing to unpack ../liblockfile1_1.09-6ubuntu1_amd64.deb ...
Unpacking liblockfile1:amd64 (1.09-6ubuntu1) ...
Selecting previously unselected package rkhunter.
Preparing to unpack ../rkhunter_1.4.2-5_all.deb ...
Unpacking rkhunter (1.4.2-5) ...
Selecting previously unselected package postfix.
Preparing to unpack ../postfix_3.1.0-3ubuntu0.3_amd64.deb ...
Unpacking postfix (3.1.0-3ubuntu0.3) ...
Selecting previously unselected package bsd-mailx.
Preparing to unpack ../bsd-mailx_8.1.2-0.20160123cvs-2_amd64.deb ...
Unpacking bsd-mailx (8.1.2-0.20160123cvs-2) ...
Selecting previously unselected package rubygems-integration.
Preparing to unpack ../rubygems-integration_1.10_all.deb ...
Unpacking rubygems-integration (1.10) ...
Selecting previously unselected package ruby-did-you-mean.
Preparing to unpack ../ruby-did-you-mean_1.0.0-2_all.deb ...
Unpacking ruby-did-you-mean (1.0.0-2) ...
Selecting previously unselected package ruby-minitest.
Preparing to unpack ../ruby-minitest_5.8.4-2_all.deb ...
```

Figura 6. Instalación rkhunter.

Durante la instalación nos pedirá configurar un servidor de correo, en este caso lo omitiremos como se muestra en la figura 7.

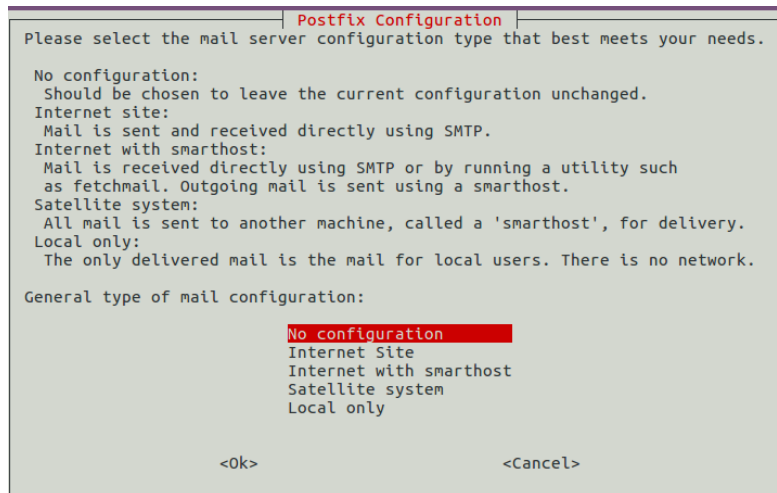


Figura 7. Instalación rkhunter.

Una vez instalado, procedemos a actualizar las firmas con el comando *rkhunter --update*, como se muestra en la figura 8.

```
root@ignacio-leal -> /h/s/D/p/practica2
# rkhunter --update
[ Rootkit Hunter version 1.4.2 ]

Checking rkhunter data files...
Checking file mirrors.dat [ No update ]
Checking file programs_bad.dat [ Updated ]
Checking file backdoorports.dat [ No update ]
Checking file suspscan.dat [ No update ]
Checking file i18n/cn [ No update ]
Checking file i18n/de [ No update ]
Checking file i18n/en [ No update ]
Checking file i18n/tr [ No update ]
Checking file i18n/tr.utf8 [ No update ]
Checking file i18n/zh [ No update ]
Checking file i18n/zh.utf8 [ No update ]
root@ignacio-leal -> /h/s/D/p/practica2
```

Figura 8. Actualización de firmas.

Ahora ejecutamos *rkhunter --check*, como se muestra en las figuras 9, 10, 11, 12, 13, 14 y 15.



```

root@ignacio-leal -> /h/s/D/p/practica2
# rkhunter --check
[ Rootkit Hunter version 1.4.2 ]

Checking system commands...

Performing 'strings' command checks
Checking 'strings' command [ OK ]

Performing 'shared libraries' checks
Checking for preloading variables [ None found ]
Checking for preloaded libraries [ None found ]
Checking LD_LIBRARY_PATH variable [ Not found ]

Performing file properties checks
Checking for prerequisites [ OK ]
/usr/sbin/adduser [ OK ]
/usr/sbin/chroot [ OK ]
/usr/sbin/cron [ OK ]
/usr/sbin/groupadd [ OK ]
/usr/sbin/groupdel [ OK ]
/usr/sbin/groupmod [ OK ]
/usr/sbin/grpck [ OK ]
/usr/sbin/nologin [ OK ]
/usr/sbin/pwck [ OK ]
/usr/sbin/rsyslogd [ OK ]
/usr/sbin/sshd [ OK ]
/usr/sbin/tcpd [ OK ]
/usr/sbin/useradd [ OK ]
/usr/sbin/userdel [ OK ]
/usr/sbin/usermod [ OK ]
/usr/sbin/vipw [ OK ]
/usr/sbin/unhide [ OK ]
/usr/sbin/unhide-linux [ OK ]
/usr/sbin/unhide-posix [ OK ]
/usr/sbin/unhide-tcp [ OK ]
/usr/bin/awk [ OK ]
/usr/bin/basename [ OK ]
/usr/bin/chatr [ OK ]
/usr/bin/curl [ OK ]
/usr/bin/cut [ OK ]
/usr/bin/diff [ OK ]
/usr/bin/dirname [ OK ]
/usr/bin/dpkg [ OK ]
/usr/bin/dpkg-query [ OK ]
/usr/bin/du [ OK ]
/usr/bin/env [ OK ]
/usr/bin/file [ OK ]
/usr/bin/find [ OK ]
/usr/bin/GET [ OK ]
/usr/bin/groups [ OK ]
/usr/bin/head [ OK ]
/usr/bin/id [ OK ]
/usr/bin/killall [ OK ]
/usr/bin/last [ OK ]
/usr/bin/lastlog [ OK ]
/usr/bin/ldd [ OK ]

```

Figura 9. Ejecución rkhunter.

```

/usr/bin/ldd [OK]
/usr/bin/less [OK]
/usr/bin/locate [OK]
/usr/bin/logger [OK]
/usr/bin/lsattr [OK]
/usr/bin/lsof [OK]
/usr/bin/mail [OK]
/usr/bin/md5sum [OK]
/usr/bin/mlocate [OK]
/usr/bin/newgrp [OK]
/usr/bin/passwd [OK]
/usr/bin/perl [OK]
/usr/bin/pgrep [OK]
/usr/bin/pkill [OK]
/usr/bin/pstree [OK]
/usr/bin/rkhunter [OK]
/usr/bin/runcon [OK]
/usr/bin/sha1sum [OK]
/usr/bin/sha224sum [OK]
/usr/bin/sha256sum [OK]
/usr/bin/sha384sum [OK]
/usr/bin/sha512sum [OK]
/usr/bin/size [OK]
/usr/bin/sort [OK]
/usr/bin/ssh [OK]
/usr/bin/stat [OK]
/usr/bin/strace [OK]
/usr/bin/strings [OK]
/usr/bin/sudo [OK]
/usr/bin/tail [OK]
/usr/bin/telnet [OK]
/usr/bin/test [OK]
/usr/bin/top [OK]
/usr/bin/touch [OK]
/usr/bin/tr [OK]
/usr/bin/uniq [OK]
/usr/bin/users [OK]
/usr/bin/vmstat [OK]
/usr/bin/w [OK]
/usr/bin/watch [OK]
/usr/bin/wc [OK]
/usr/bin/wget [OK]
/usr/bin/whatis [OK]
/usr/bin/whereis [OK]
/usr/bin/which [OK]
/usr/bin/who [OK]
/usr/bin/whoami [OK]
/usr/bin/gawk [OK]
/usr/bin/lwp-request [Warning]
/usr/bin/bsd-mailx [OK]
/usr/bin/x86_64-linux-gnu-size [OK]
/usr/bin/x86_64-linux-gnu-strings [OK]
/usr/bin/telnet.netkit [OK]
/usr/bin/w.procps [OK]
/sbin/depmod [OK]

```

Figura 10. Ejecución rkhunter.

```

/sbin/depmod [ OK ]
/sbin/fsck [ OK ]
/sbin/ifconfig [ OK ]
/sbin/ifdown [ OK ]
/sbin/ifup [ OK ]
/sbin/init [ OK ]
/sbin/insmod [ OK ]
/sbin/ip [ OK ]
/sbin/lsmmod [ OK ]
/sbin/modinfo [ OK ]
/sbin/modprobe [ OK ]
/sbin/rmmod [ OK ]
/sbin/route [ OK ]
/sbin/runlevel [ OK ]
/sbin/sulogin [ OK ]
/sbin/sysctl [ OK ]
/bin/bash [ OK ]
/bin/cat [ OK ]
/bin/chmod [ OK ]
/bin/chown [ OK ]
/bin/cp [ OK ]
/bin/date [ OK ]
/bin/df [ OK ]
/bin/dmesg [ OK ]
/bin/echo [ OK ]
/bin/ed [ OK ]
/bin/egrep [ OK ]
/bin/fgrep [ OK ]
/bin/fuser [ OK ]
/bin/grep [ OK ]
/bin/ip [ OK ]
/bin/kill [ OK ]
/bin/less [ OK ]
/bin/login [ OK ]
/bin/ls [ OK ]
/bin/lsmmod [ OK ]
/bin/mktemp [ OK ]
/bin/more [ OK ]
/bin/mount [ OK ]
/bin/mv [ OK ]
/bin/netstat [ OK ]
/bin/ping [ OK ]
/bin/ps [ OK ]
/bin/pwd [ OK ]
/bin/readlink [ OK ]
/bin/sed [ OK ]
/bin/sh [ OK ]
/bin/su [ OK ]
/bin/touch [ OK ]
/bin/uname [ OK ]
/bin/which [ OK ]
/bin/kmod [ OK ]
/bin/systemd [ OK ]
/bin/systemctl [ OK ]
/bin/dash [ OK ]
/lib/systemd/systemd [ OK ]

```

Figura 11. Ejecución rkhunter.



```
[Press <ENTER> to continue]

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 ]
Ambient (ark) Rootkit [ Not found ]
Balaor Rootkit [ Not found ]
BeastKit Rootkit [ Not found ]
beX2 Rootkit [ Not found ]
BOBKit Rootkit [ Not found ]
cb Rootkit [ Not found ]
CiNIK Worm (Slapper.B variant) [ Not found ]
Danny-Boy's Abuse Kit [ Not found ]
Devil RootKit [ Not found ]
Dica-Kit Rootkit [ Not found ]
Dreams Rootkit [ Not found ]
Duarawkz Rootkit [ Not found ]
Enye LKM [ Not found ]
Flea Linux Rootkit [ Not found ]
Fu Rootkit [ Not found ]
Fuck'it Rootkit [ Not found ]
GasKit Rootkit [ Not found ]
Heroin LKM [ Not found ]
HjC Kit [ Not found ]
ignoKit Rootkit [ Not found ]
IntoXonia-NG Rootkit [ Not found ]
Irix Rootkit [ Not found ]
Jynx Rootkit [ Not found ]
KBeast Rootkit [ Not found ]
Kitko Rootkit [ Not found ]
Knark Rootkit [ Not found ]
ld-linuxv.so Rootkit [ Not found ]
LiOn Worm [ Not found ]
Lockit / LJK2 Rootkit [ Not found ]
Mood-NT Rootkit [ Not found ]
MRK Rootkit [ Not found ]
Ni0 Rootkit [ Not found ]
Ohhara Rootkit [ Not found ]
Optic Kit (Tux) Worm [ Not found ]
Oz Rootkit [ Not found ]
Phalanx Rootkit [ Not found ]
Phalanx2 Rootkit [ Not found ]
Phalanx2 Rootkit (extended tests) [ Not found ]
Portacelo Rootkit [ Not found ]
R3dstorm Toolkit [ Not found ]
RH-Sharpe's Rootkit [ Not found ]
RSHA's Rootkit [ Not found ]
Scalper Worm [ Not found ]
Sebek LKM [ Not found ]
Shutdown Rootkit [ Not found ]
```

Figura 12. Ejecución rkhunter.

```

Enye LKM [ Not found ]
Flea Linux Rootkit [ Not found ]
Fu Rootkit [ Not found ]
Fuck'it Rootkit [ Not found ]
GasKit Rootkit [ Not found ]
Heroin LKM [ Not found ]
HjC Kit [ Not found ]
ignoKit Rootkit [ Not found ]
IntoXonia-NG Rootkit [ Not found ]
Irix Rootkit [ Not found ]
Jynx Rootkit [ Not found ]
KBeast Rootkit [ Not found ]
Kitko Rootkit [ Not found ]
Knark Rootkit [ Not found ]
ld-linuxv.so Rootkit [ Not found ]
Li0n Worm [ Not found ]
Lockit / LJK2 Rootkit [ Not found ]
Mood-NT Rootkit [ Not found ]
MRK Rootkit [ Not found ]
Ni0 Rootkit [ Not found ]
Ohhara Rootkit [ Not found ]
Optic Kit (Tux) Worm [ Not found ]
Oz Rootkit [ Not found ]
Phalanx Rootkit [ Not found ]
Phalanx2 Rootkit [ Not found ]
Phalanx2 Rootkit (extended tests) [ Not found ]
Portacelo Rootkit [ Not found ]
R3dstorm Toolkit [ Not found ]
RH-Sharpe's Rootkit [ Not found ]
RSA's Rootkit [ Not found ]
Scalper Worm [ Not found ]
Sebek LKM [ Not found ]
Shutdown Rootkit [ Not found ]
SHV4 Rootkit [ Not found ]
SHV5 Rootkit [ Not found ]
Sin Rootkit [ Not found ]
Slapper Worm [ Not found ]
Sneakin Rootkit [ Not found ]
'Spanish' Rootkit [ Not found ]
Suckit Rootkit [ Not found ]
Superkit Rootkit [ Not found ]
TBD (Telnet BackDoor) [ Not found ]
TeLeKiT Rootkit [ Not found ]
T0rn Rootkit [ Not found ]
trNkit Rootkit [ Not found ]
Trojanit Kit [ Not found ]
Tuxtendo Rootkit [ Not found ]
URK Rootkit [ Not found ]
Vampire Rootkit [ Not found ]
VcKit Rootkit [ Not found ]
Volc Rootkit [ Not found ]
Xzibit Rootkit [ Not found ]
zaRwT.KiT Rootkit [ Not found ]
ZK Rootkit [ Not found ]

[Press <ENTER> to continue]

```

Figura 13. Ejecución rkhunter.

```

Performing additional rootkit checks
Suckit Rootkit additional checks          [ OK ]
Checking for possible rootkit files and directories [ None found ]
Checking for possible rootkit strings      [ None found ]

Performing malware checks
Checking running processes for suspicious files [ None found ]
Checking for login backdoors                [ None found ]
Checking for suspicious directories         [ None found ]
Checking for sniffer log files              [ None found ]
Suspicious Shared Memory segments          [ None found ]
Checking for Apache backdoor                [ Not found ]

Performing Linux specific checks
Checking loaded kernel modules              [ OK ]
Checking kernel module names               [ OK ]

[Press <ENTER> to continue]

Checking the network...

Performing checks on the network ports
Checking for backdoor ports                [ None found ]
Checking for hidden ports                  [ None found ]

Performing checks on the network interfaces
Checking for promiscuous interfaces         [ None found ]

Checking the local host...

Performing system boot checks
Checking for local host name                [ Found ]
Checking for system startup files           [ Found ]
Checking system startup files for malware   [ None found ]

Performing group and account checks
Checking for passwd file                    [ Found ]
Checking for root equivalent (UID 0) accounts [ None found ]
Checking for passwordless accounts         [ None found ]
Checking for passwd file changes            [ Warning ]
Checking for group file changes             [ Warning ]
Checking root account shell history files   [ OK ]

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 allowed ]
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 ]

Performing filesystem checks
Checking /dev for suspicious file types     [ Warning ]
Checking for hidden files and directories   [ Warning ]

[Press <ENTER> to continue]

```

Figura 14. Ejecución rkhunter.

```

System checks summary
=====

File properties checks...
Files checked: 150
Suspect files: 1

Rootkit checks...
Rootkits checked : 380
Possible rootkits: 0

Applications checks...
All checks skipped

The system checks took: 5 minutes and 17 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)

```

Figura 15. Ejecución rkhunter.

El archivo de configuración de rkhunter se encuentra en `/etc/rkhunter.conf`, como se muestra en la figura 16.

```
# cat /etc/rkhunter.conf | grep -o "[^#]*"
TMPDIR=/var/lib/rkhunter/tmp
DBDIR=/var/lib/rkhunter/db
SCRIPTDIR=/usr/share/rkhunter/scripts
LOGFILE=/var/log/rkhunter.log
USE_SYSLOG=authpriv.warning
AUTO_X_DETECT=1
ENABLE_TESTS=all
DISABLE_TESTS=suspscan hidden_procs deleted_files packet_cap_apps apps
HASH_CMD=sha256sum
SCRIPTWHITELIST=/bin/egrep
SCRIPTWHITELIST=/bin/fgrep
SCRIPTWHITELIST=/bin/which
SCRIPTWHITELIST=/usr/bin/ldd
SCRIPTWHITELIST=/usr/sbin/adduser
DISABLE_UNHIDE=1
INSTALLDIR=/usr
```

Figura 16. Opciones del archivo de configuración de rkhunter.

Al observar las opciones en el archivo de configuración encontramos que podemos especificar el directorio temporal, el directorio de la base de datos, el directorio de los scripts, las pruebas habilitadas y deshabilitadas, entre otros.

Rkhunter permite listar todas las pruebas que realiza con el comando `rkhunter --list tests`, como se muestra en la figura 17, ya que no solamente analiza el sistema en busca de rootkits, también busca malware, puertos abiertos, archivos de configuración alterados, entre otros.

```
root@ignacio-leal -> /h/s/D/p/practica2
# rkhunter --list tests

Current test names:
additional_rkts all apps attributes avail_modules deleted_files
filesystem group_accounts group_changes hashes hidden_ports hidden_procs
immutable known_rkts loaded_modules local_host malware network
none os_specific other_malware packet_cap_apps passwd_changes ports
possible_rkt_files possible_rkt_strings promisc properties rootkits running_procs
scripts shared_libs shared_libs_path startup_files startup_malware strings
suspscan system_commands system_configs trojans

Grouped test names:
additional_rkts => possible_rkt_files possible_rkt_strings
group_accounts => group_changes passwd_changes
local_host => filesystem group_changes passwd_changes startup_malware system_configs
malware => deleted_files hidden_procs other_malware running_procs suspscan
network => hidden_ports packet_cap_apps ports promisc
os_specific => avail_modules loaded_modules
properties => attributes hashes immutable scripts
rootkits => avail_modules deleted_files hidden_procs known_rkts loaded_modules other
shared_libs => shared_libs_path
startup_files => startup_malware
system_commands => attributes hashes immutable scripts shared_libs_path strings
```

Figura 17. Lista con las pruebas.

## Conclusiones

El conocer herramientas que nos permita buscar malware en nuestro sistema es importante, ya que al ser herramientas automatizadas nos permiten encontrar posible malware de forma más rápida que si lo hacemos de forma manual, la instalación y configuración es sencilla para ambas herramientas, aunque rkhunter tiene mas opciones de configuración que chkrootkit, lo que puede dificultar la configuración para un usuario que no tenga los conocimientos necesarios. Cabe destacar que las dos herramientas se especializan en detectar rootkits un tipo de malware complejo de detectar.

## Referencias

<http://www.chkrootkit.org/>

<http://rkhunter.sourceforge.net/>