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.

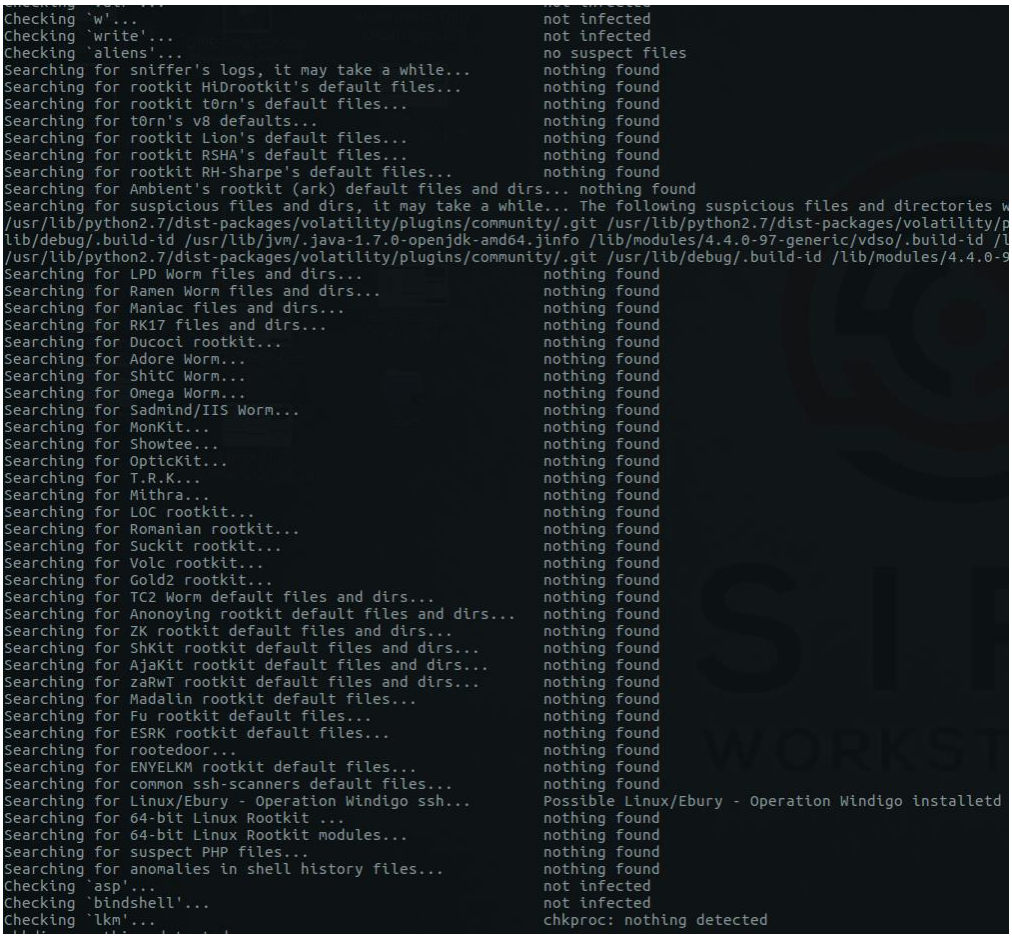

Figura 3. Ejecución chkrootkit.

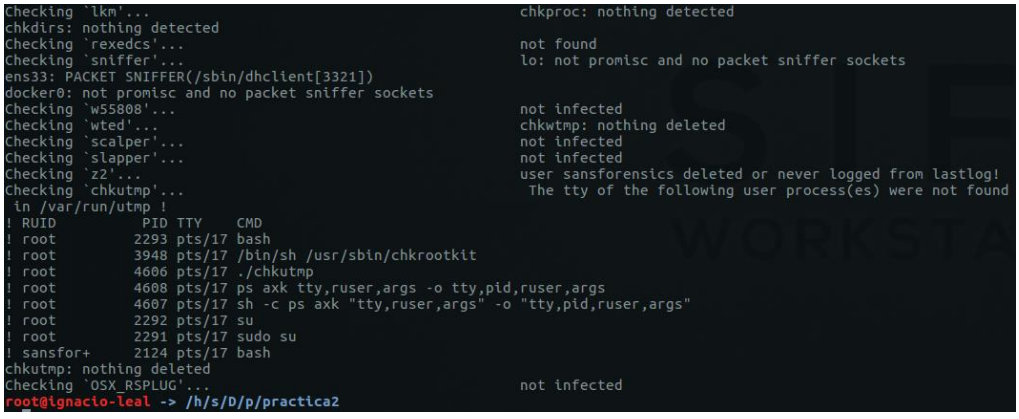

Figura 4. Ejecución chkrootkit.

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 d
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.
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.

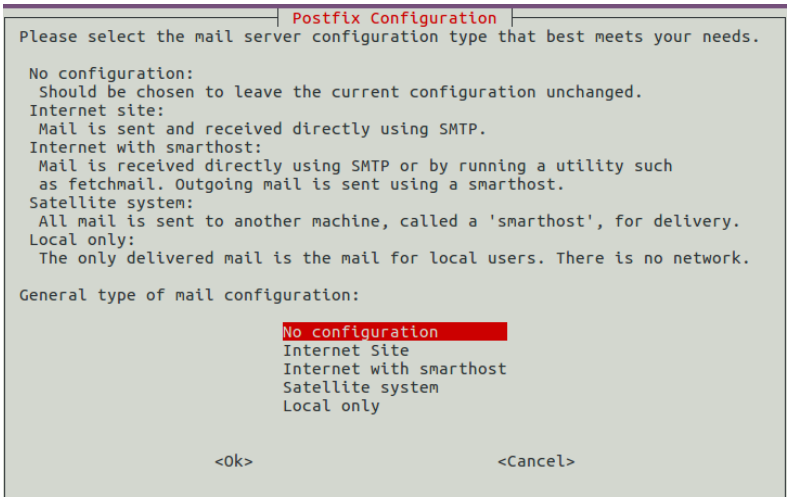

Figura 7. Instalación rkhunter.

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

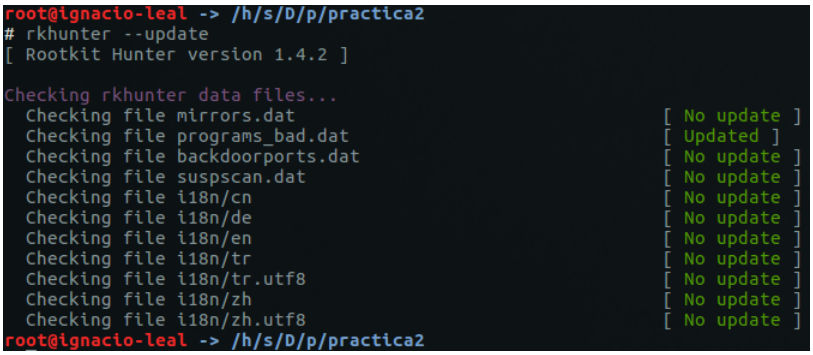

Figura 8. Actualización de firmas.

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/chattr                                         [ 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.

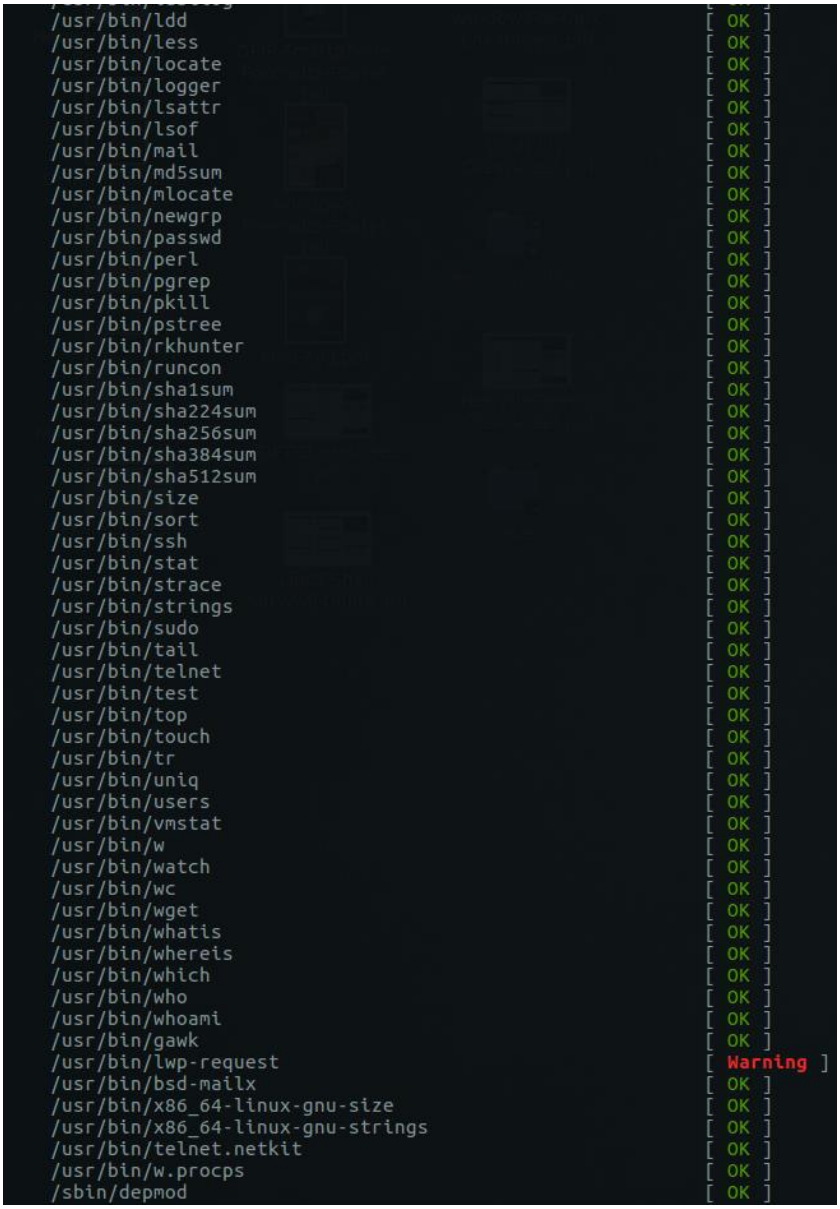

Figura 10. Ejecución rkhunter.

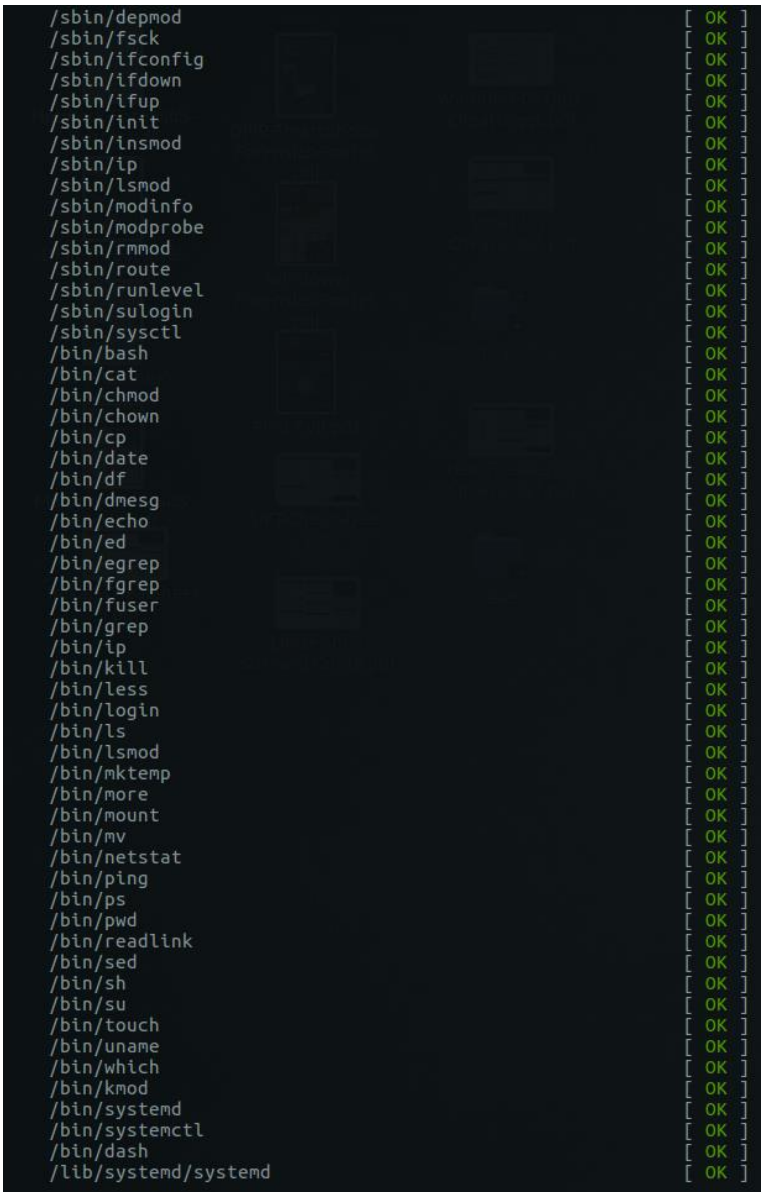

Figura 11. Ejecución rkhunter.

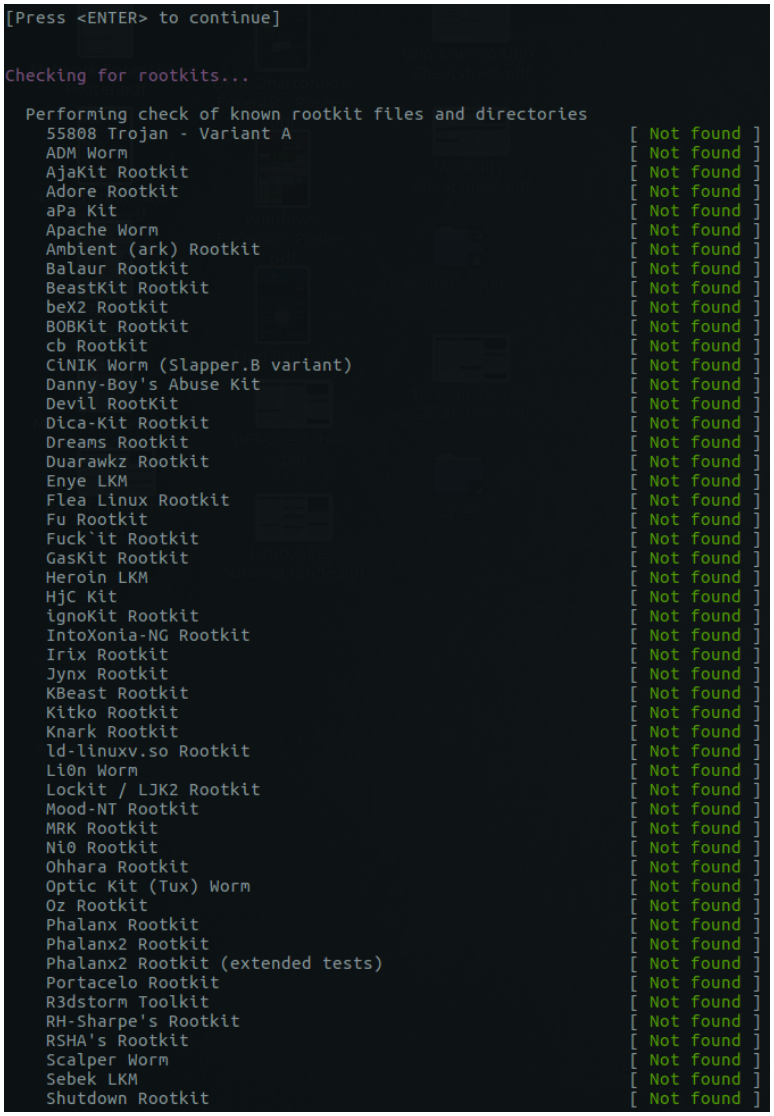

Figura 12. Ejecuión rkhunter.

Figura 13. Ejecución rkhunter.

```
  Performing additional rootkit checks
    Suckit Rookit 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/