

SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software

Curso 2017-18

Práctica [1]

Sesión [2]

Autor¹: Iván Rodríguez Millán.

Ejercicio 1.

a)

Hacemos un “lsof -i” y nos devuelve los siguientes datos:

COMMAND: Nombre del proceso.

PID: Identificador del proceso.

USER: Nombre de usuario del usuario que lanzó el proceso.

FD: Número descriptor del fichero.

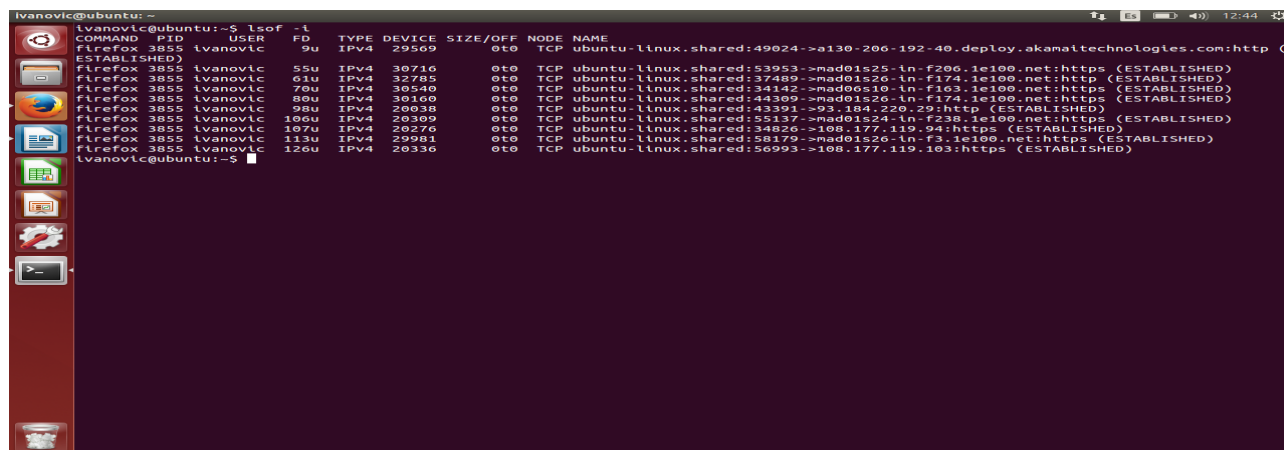
TYPE: Tipo de nodo asociado al fichero. P.E: IPv4, IPv6,....

DEVICE: Contiene el número del dispositivo.

SIZE: Tamaño del fichero u offset en bytes.

NODE: Número del nodo del fichero local.

NAME: Es el nombre del punto de montaje y sistema de archivos donde reside el fichero.



```
ivanovic@ubuntu: ~$ lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
ESTABLISHED)
firefox 3855 ivanovic 55u IPv4 30716 0t0 TCP ubuntu-linux.shared:49024->a130-206-192-40.deploy.akamai technologies.com:http (
firefox 3855 ivanovic 61u IPv4 32785 0t0 TCP ubuntu-linux.shared:37489->mad01s26-ln-f174.1e100.net:http (ESTABLISHED)
firefox 3855 ivanovic 70u IPv4 30540 0t0 TCP ubuntu-linux.shared:34142->mad00s19-ln-f103.1e100.net:https (ESTABLISHED)
firefox 3855 ivanovic 80u IPv4 30160 0t0 TCP ubuntu-linux.shared:44309->mad01s26-ln-f174.1e100.net:https (ESTABLISHED)
firefox 3855 ivanovic 98u IPv4 20038 0t0 TCP ubuntu-linux.shared:43391->93.104.220.29:http (ESTABLISHED)
firefox 3855 ivanovic 100u IPv4 20309 0t0 TCP ubuntu-linux.shared:55137->mad01s24-ln-f238.1e100.net:https (ESTABLISHED)
firefox 3855 ivanovic 107u IPv4 20276 0t0 TCP ubuntu-linux.shared:34826->108.177.119.94:https (ESTABLISHED)
firefox 3855 ivanovic 113u IPv4 29981 0t0 TCP ubuntu-linux.shared:58179->mad01s26-ln-f3.1e100.net:https (ESTABLISHED)
firefox 3855 ivanovic 120u IPv4 20336 0t0 TCP ubuntu-linux.shared:56993->108.177.119.103:https (ESTABLISHED)
ivanovic@ubuntu: ~$
```

1 Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la “Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada” esto “conllevará la calificación numérica de cero ... independientemente del resto de calificaciones que el estudiante hubiera obtenido ...”

b)

En primer lugar para mostrar el tráfico saliente usamos la opción:

"lsof -i | grep ssh"

De esta forma mostramos el tráfico saliente usado por ssh. Después de mostrar los resultados si vemos algún comportamiento anómalo, usamos la opción:

"lsof -c ssh" que nos permite listar los ficheros de los procesos de ejecución por el comando que comience por ssh.

```
-c c selects the listing of files for processes executing the command that begins with the characters of c. Multiple commands may be specified, using multiple -c options. They are joined in a single ORed set before participating in AND option selection.

If c begins with a '^', then the following characters specify a command name whose processes are to be ignored (excluded.)

If c begins and ends with a slash ('/'), the characters between the slashes are interpreted as a regular expression. Shell meta-characters in the regular expression must be quoted to prevent their interpretation by the shell. The closing slash may be followed by these modifiers:

    b   the regular expression is a basic one.
    i   ignore the case of letters.
    x   the regular expression is an extended one (default).

See the lsof FAQ (The FAQ section gives its location.) for more information on basic and extended regular expressions.

The simple command specification is tested first. If that test fails, the command regular expression is applied. If the simple command test succeeds, the command regular expression test isn't made. This may result in 'no command found for regex:' messages when lsof's -V option is specified.
```

c)

Con la orden:

"lsof -i firefox -a -u ivanovic"

Obtenemos los ficheros abiertos por firefox y con la opción -a concatenamos esta salida con la de que el usuario sea ivanovic que es con la opción -u.

```
ivanovic@ubuntu: ~
ivanovic@ubuntu:~$ lsof -u ivanovic -a -c firefox
COMMAND PID  USER  FD   TYPE    DEVICE  SIZE/OFF      NODE NAME
firefox 9890 ivanovic cwd    DIR      8,1      4096    131074 /home/ivanovic
firefox 9890 ivanovic rtd    DIR      8,1      4096         2 /
firefox 9890 ivanovic txt    REG      8,1    153792    659440 /usr/lib/firefox/firefox
firefox 9890 ivanovic DEL    REG      0,4      2818062 /SYSV00000000
firefox 9890 ivanovic DEL    REG      0,4      2752528 /SYSV00000000
firefox 9890 ivanovic DEL    REG      0,4      2686989 /SYSV00000000
firefox 9890 ivanovic DEL    REG      0,4      2621455 /SYSV00000000
firefox 9890 ivanovic mem    REG      8,1    192296    664918 /usr/lib/x86_64-linux-gnu/libgconf-2.so.4.1.5
firefox 9890 ivanovic mem    REG      8,1     14488    664612 /usr/lib/x86_64-linux-gnu/libXss.so.1.0.0
firefox 9890 ivanovic mem    REG      8,1     81912    664787 /usr/lib/x86_64-linux-gnu/libdbusmenu-gtk3.so.4.0.12
firefox 9890 ivanovic mem    REG      8,1    110048    664783 /usr/lib/x86_64-linux-gnu/libdbusmenu-glib.so.4.0.12
firefox 9890 ivanovic mem    REG      8,1    367260    1445457 /usr/share/fonts/truetype/dejavu/DejaVuSerif.ttf
firefox 9890 ivanovic mem    REG      8,1    733846    660008 /usr/lib/firefox/browser/features/screenshots@mozilla.org.xpi
firefox 9890 ivanovic mem    REG      8,1    22952    266588 /lib/x86_64-linux-gnu/libnss_dns-2.19.so
firefox 9890 ivanovic mem    REG      8,1     10432    266391 /lib/x86_64-linux-gnu/libnss_mdns4_minimal.so.2
firefox 9890 ivanovic mem    REG      8,1    415552    1445614 /usr/share/fonts/truetype/ubuntu-font-family/Ubuntu-L.ttf
firefox 9890 ivanovic mem    REG      8,1    632336    659436 /usr/lib/firefox/libnssckbi.so
firefox 9890 ivanovic mem    REG      8,1    509928    660039 /usr/lib/firefox/libfreeblpriv3.so
firefox 9890 ivanovic mem    REG      8,1    133088    659435 /usr/lib/firefox/libnssdbm3.so
firefox 9890 ivanovic mem    REG      8,1    252944    660050 /usr/lib/firefox/libsoftokn3.so
firefox 9890 ivanovic mem    REG      8,1    377176    659818 /usr/lib/x86_64-linux-gnu/libibus-1.0.so.5.0.505
firefox 9890 ivanovic mem    REG      8,1     31752    920379 /usr/lib/x86_64-linux-gnu/gtk-3.0/3.0.0/immodules/im-ibus.so
firefox 9890 ivanovic mem    REG      8,1    333616    1445611 /usr/share/fonts/truetype/ubuntu-font-family/Ubuntu-B.ttf
firefox 9890 ivanovic mem    REG      8,1     23152    918376 /usr/lib/x86_64-linux-gnu/gdk-pixbuf-2.0/2.10.0/loaders/libp
xbufloder-png.so
firefox 9890 ivanovic mem    REG      8,1    432099    660013 /usr/lib/firefox/browser/features/onboarding@mozilla.org.xpi
firefox 9890 ivanovic mem    REG      8,1    2943096    665572 /usr/lib/x86_64-linux-gnu/libvorbisenc.so.2.0.8
firefox 9890 ivanovic mem    REG      8,1    199208    664433 /usr/lib/x86_64-linux-gnu/libFLAC.so.8.3.0
firefox 9890 ivanovic mem    REG      8,1     22744    664665 /usr/lib/x86_64-linux-gnu/libasynccns.so.0.3.1
firefox 9890 ivanovic mem    REG      8,1    409536    662606 /usr/lib/x86_64-linux-gnu/libsndfile.so.1.0.25
firefox 9890 ivanovic mem    REG      8,1     36632    266470 /lib/x86_64-linux-gnu/libwrap.so.0.7.6
firefox 9890 ivanovic mem    REG      8,1    422272    920793 /usr/lib/x86_64-linux-gnu/pulseaudio/libpulsecommon-4.0.so
firefox 9890 ivanovic mem    REG      8,1     43464    266350 /lib/x86_64-linux-gnu/libjson-c.so.2.0.0
firefox 9890 ivanovic mem    REG      8,1    299752    665363 /usr/lib/x86_64-linux-gnu/libpulse.so.0.16.2
firefox 9890 ivanovic mem    REG      8,1    353824    1445618 /usr/share/fonts/truetype/ubuntu-font-family/Ubuntu-R.ttf
firefox 9890 ivanovic mem    REG      8,1    1004296    660009 /usr/lib/firefox/browser/features/firefox@getpocket.com.xpi
firefox 9890 ivanovic mem    REG      8,1    3968469    269518 /home/ivanovic/.cache/mozilla/firefox/l7qqm5dd.default/startu
pCache/startupCache.8.little
firefox 9890 ivanovic mem    REG      8,1    3835857    266315 /home/ivanovic/.cache/mozilla/firefox/l7qqm5dd.default/startu
pCache/scriptCache-current.bin
firefox 9890 ivanovic mem    REG      8,1    999578    266319 /home/ivanovic/.cache/mozilla/firefox/l7qqm5dd.default/startu
```

Ejercicio 2.

Se va a proceder de la siguiente manera, vamos a lanzar en tres momentos distintos la orden:

ps -e -o command > fichero_número

Con la opción -e seleccionamos todos los procesos, y con la opción -o command extraemos simplemente los nombres de los mismos.

Y cuando tengamos 3 ficheros: fichero_primer, fichero_segundo y fichero_tercero lanzaremos la siguiente orden:

diff fichero_primer fichero_segundo

Salida:

252a253,254

> /lib/systemd/systemd-hostnamed

> /usr/lib/firefox/firefox

systemd-hostnamed : es un servicio del sistema que se puede usar para cambiar el nombre del host del sistema. Información extraída de:

<http://manpages.ubuntu.com/manpages/trusty/man8/systemd-hostnamed.service.8.html>

Como principal diferencia tenemos el proceso firefox lanzado, esto se debe a que en el momento de hacer el ps -e el proceso se lanzó.

diff fichero_primer fichero_tercero

Salida:

248,249d247

< man ps

< pager -s

252a251,253

> /lib/systemd/systemd-hostnamed

> /usr/lib/firefox/firefox

> gedit

En este caso vemos como está lanzado el proceso man y firefox junto con systemd-hostnamed como anteriormente.

También vemos que está lanzado el proceso gedit y pager -s el cuál es lanzado cuando se lanza el proceso man.

diff fichero_tercero fichero_segundo

Salida:

248,249d247

< man ps

< pager -s

254a253

> gedit

Aquí tenemos la diferencia con los procesos gedit, man y pager.

Ejercicio 3.

a)

Con la opción `lynis -c` ó `lynis --check-all` podemos realizar una auditoría del sistema total. Nos irá mostrando por pantalla los resultados aunque también tenemos la posibilidad de acceder a los ficheros **lynis.log** y **lynis-report.dat**.

Por ejemplo en la parte de Usuarios, Grupos y Autenticación tenemos los siguientes errores:

```
[+] Users, Groups and Authentication
-----
- Search administrator accounts...           [ OK ]
- Checking consistency of group files (grpck)... [ OK ]
- Checking non unique group ID's...           [ OK ]
- Checking non unique group names...          [ OK ]
- Checking password file consistency...        [ OK ]
- Query system users (non daemons)...         [ DONE ]
- Checking NIS+ authentication support         [ NOT ENABLED ]
- Checking NIS authentication support          [ NOT ENABLED ]
- Checking sudoers file                       [ FOUND ]
- Check sudoers file permissions              [ OK ]
- Checking PAM password strength tools        [ OK ]
- Checking PAM configuration files (pam.conf) [ FOUND ]
- Checking PAM configuration files (pam.d)    [ FOUND ]
- Checking PAM modules                       [ FOUND ]
- Checking LDAP module in PAM                 [ NOT FOUND ]
- Checking accounts without expire date       [ OK ]
- Checking accounts without password          [ OK ]
- Checking user password aging                [ DISABLED ]
- Determining default umask
- Checking umask (/etc/profile)               [ UNKNOWN ]
- Checking umask (/etc/login.defs)            [ SUGGESTION ]
- Checking umask (/etc/init.d/rc)             [ SUGGESTION ]
- Checking LDAP authentication support         [ NOT ENABLED ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

Nos dice que está desactivado el chequeo de expiración de el password de un usuario.

Y más abajo, al final de la auditoría en la parte de sugerencias nos indica entre otras muchas sugerencias la siguiente:

```

-[ Lynis 1.3.9 Results ]-

Tests performed: 153

Warnings:
-----
- Version of Lynis very outdated [test:NONE]
- Couldn't find 2 responsive nameservers [test:NETW-2705]
- Found mail_name in SMTP banner, and/or mail_name contains 'Postfix' [test:MAIL-8818]

Suggestions:
-----
- update to the latest stable release.
- Configure password aging limits to enforce password changing on a regular base [test:AUTH-9286]
- Default umask in /etc/login.defs could be more strict like 027 [test:AUTH-9328]
- Default umask in /etc/init.d/rc could be more strict like 027 [test:AUTH-9328]
- To decrease the impact of a full /tmp file system, place /tmp on a separated partition [test:FILE-6310]
- Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [test:STRG-1840]
- Install package apt-show-versions for patch management purposes [test:PKGS-7394]
- Check your resolv.conf file and fill in a backup nameserver if possible [test:NETW-2705]
- You are adviced to hide the mail_name (option: smtpd_banner) from your postfix configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf) [test:MAIL-8818]
- Configure a firewall/packet filter to filter incoming and outgoing traffic [test:FIRE-4590]
- Check what deleted files are still in use and why. [test:LOGG-2190]
- Add a legal banner to /etc/issue, to warn unauthorized users [test:BANN-7126]
- Add legal banner to /etc/issue.net, to warn unauthorized users [test:BANN-7130]
- Enable auditd to collect audit information [test:ACCT-9628]
- Install a file integrity tool [test:FINT-4350]
- One or more sysctl values differ from the scan profile and could be tweaked [test:KRNL-6000]
- Harden the system by removing unneeded compilers. This can decrease the chance of customized trojans, backdoors and rootkits to be compiled and installed [test:HRDN-7220]
- Harden compilers and restrict access to world [test:HRDN-7222]
- Harden the system by installing one or malware scanners to perform periodic file system scans [test:HRDN-7230]
=====
Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat
=====

```

En la segunda línea de las sugerencias nos indica que configuremos el limite para forzar a cambiar las contraseñas en lo relacionado con el envejecimiento de la misma.

b)

En mi caso para la versión 1.3.9 no comprueba la vulnerabilidad Shellshock ya que si nos vamos al fichero include/tests_shells y lo abrimos veremos cuáles son las comprobaciones realizadas por Lynis, y entre ellas no está el test SHLL-6290 que es el que se encarga de comprobar dicha vulnerabilidad. Esta información ha sido sacada de: <https://cisofy.com/lynis/controls/>

Por el contrario si comprueba las siguientes vulnerabilidades:

SHLL-6230, SHLL-6220, SHLL-6211 y SHLL-6202.

Lynis Security Controls

SHLL-6290 - Shellshock vulnerability in Bash

Description

When this control shows up, Bash is vulnerable for one or more Shellshock related issues.

Group

Shell

How to solve

Upgrade Bash to the latest version available.

Imagen con la descripción del control, sacada de la página oficial de CISOFY.

c)

Si queremos que un antivirus no contemplado por la herramienta Lynis sea detectado debemos de irnos al fichero `/usr/local/include/tests_malware` e introducir un script para detectar dicha herramienta, por ejemplo:

Aquí tenemos un ejemplo de como chequea McAfee (El conocido software antivirus).

```
GNU nano 2.2.6                                File: tests_malware

fi

# McAfee products
LogText "Test: checking process cma or cmdagent (McAfee)"
# cma is too generic to match on, so we want to ensure that it is related to McAfee first
if [ -x /opt/McAfee/cma/bin/cma ]; then
    IsRunning cma
    if [ ${RUNNING} -eq 1 ]; then MCAFEE_SCANNER_RUNNING=1; fi
else
    IsRunning cmdagent
    if [ ${RUNNING} -eq 1 ]; then MCAFEE_SCANNER_RUNNING=1; fi
fi
if [ ${MCAFEE_SCANNER_RUNNING} -eq 1 ]; then
    FOUND=1
    if IsVerbose; then Display --indent 2 --text "- ${GEN_CHECKING} McAfee" --result "${STATUS_FOUND}" --color GREEN; fi
    LogText "Result: Found McAfee"
    MALWARE_SCANNER_INSTALLED=1
    Report "malware_scanner[]=mcafee"
fi
```

Aquí tenemos otro ejemplo de como chequea chkrootkit, el programa que permite localizar rootkit conocidos por su base de datos.

```
GNU nano 2.2.6                                File: tests_malware

#####
#
# Test      : MALW-3275
# Description : Check for installed tool (chkrootkit)
Register --test-no MALW-3275 --weight L --network NO --category security --description "Check for chkrootkit"
if [ ${SKIPTTEST} -eq 0 ]; then
    LogText "Test: checking presence chkrootkit"
    if [ ! -z "${CHKROOTKITBINARY}" ]; then
        Display --indent 2 --text "- ${GEN_CHECKING} chkrootkit" --result "${STATUS_FOUND}" --color GREEN
        LogText "Result: Found ${CHKROOTKITBINARY}"
        MALWARE_SCANNER_INSTALLED=1
        AddHP 2 2
        Report "malware_scanner[]=chkrootkit"
    else
        LogText "Result: chkrootkit not found"
    fi
fi
#
```

Ejercicio 4.

a)

En primer lugar lanzamos las sentencias que se han explicado en el guión:

rkhunter --propupd

Este comando nos permite construir la base de datos de los archivos que posteriormente vamos a comprobar.

Después lanzamos el comando:

rkhunter --check --skip-keypress

Con esta sentencia chequeamos que el sistema de archivos esta correctamente.

```
root@ubuntu:/usr/local/lynis/include# rkhunter --check --skip-keypress  
[ Rootkit Hunter version 1.4.0 ]
```

```
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/tcpd [ OK ]  
/usr/sbin/useradd [ OK ]  
/usr/sbin/userdel [ OK ]  
/usr/sbin/usermod [ OK ]  
/usr/sbin/vipw [ 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 ]
```


b)

En mi caso sale el siguiente Warning:

```
/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/unhide.rb [ Warning ]
/usr/bin/mawk [ OK ]
/usr/bin/w.procps [ OK ]
/sbin/depmod [ OK ]
/sbin/fsck [ OK ]
/sbin/ifconfig [ OK ]
/sbin/ifdown [ OK ]
/sbin/ifup [ OK ]
/sbin/init [ OK ]
/sbin/inssmod [ 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 ]
```

El cuál está claro que es un falso positivo, el problema está en saber como actuar, por ello lo mejor es irse al archivo `/var/log/rhunter.log` y observar la información que nos dan:

```
GNU nano 2.2.6                               File: rkhunter.log                               Modified

[21:05:46] /usr/bin/strings                      [ OK ]
[21:05:46] /usr/bin/sudo                        [ OK ]
[21:05:46] /usr/bin/tail                        [ OK ]
[21:05:46] /usr/bin/test                       [ OK ]
[21:05:46] /usr/bin/top                       [ OK ]
[21:05:46] /usr/bin/touch                      [ OK ]
[21:05:46] /usr/bin/tr                        [ OK ]
[21:05:47] /usr/bin/uniq                      [ OK ]
[21:05:47] /usr/bin/users                     [ OK ]
[21:05:47] /usr/bin/vmstat                    [ OK ]
[21:05:47] /usr/bin/w                        [ OK ]
[21:05:47] /usr/bin/watch                     [ OK ]
[21:05:47] /usr/bin/wc                        [ OK ]
[21:05:47] /usr/bin/wget                       [ OK ]
[21:05:47] /usr/bin/whatism                      [ OK ]
[21:05:47] /usr/bin/whereis                    [ OK ]
[21:05:47] /usr/bin/which                     [ OK ]
[21:05:47] /usr/bin/who                        [ OK ]
[21:05:47] /usr/bin/whoami                       [ OK ]
[21:05:47] /usr/bin/unhide.rb                     [ Warning ]
[21:05:47] Warning: The command '/usr/bin/unhide.rb' has been replaced by a script: /usr/bin/unhide.rb: Ruby script, ASCII text
[21:05:47] /usr/bin/mawk                          [ OK ]
[21:05:47] /usr/bin/w.procps                       [ OK ]
[21:05:48] /sbin/depmod                            [ OK ]
[21:05:48] /sbin/fsck                              [ OK ]
[21:05:48] /sbin/ifconfig                          [ OK ]
[21:05:48] /sbin/ifdown                            [ OK ]
[21:05:48] /sbin/ifup                              [ OK ]
[21:05:48] /sbin/init                              [ OK ]
[21:05:48] /sbin/insmod                            [ OK ]
[21:05:48] /sbin/ip                                [ OK ]
[21:05:48] /sbin/lsmmod                            [ OK ]
[21:05:48] /sbin/modinfo                           [ OK ]
[21:05:48] /sbin/modprobe                          [ OK ]
[21:05:49] /sbin/rmmod                             [ OK ]
[21:05:49] /sbin/route                             [ OK ]
[21:05:49] /sbin/runlevel                          [ OK ]
[21:05:49] /sbin/sulogin                           [ OK ]

^G Get Help      ^O WriteOut      ^R Read File      ^V Prev Page      ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is       ^N Next Page      ^U UnCut Text    ^T To Spell
```

Aquí podemos ver que el Warning es debido a que el command unhide.rb ha sido reemplazado por un script. Luego debemos inspeccionar el programa para ver que está bien, y en tal caso debemos hacerle saber que es un script , para ello nos vamos al fichero /etc/rkhunter.conf y en la variable **SCRIPTWHITELIST** añadimos el camido de cada orden que sea un script.

```
GNU nano 2.2.6                               File: /etc/rkhunter.conf                               Modified

#WRITEWHITELIST="/bin/ps /usr/bin/date"

#
# Allow the specified commands to be scripts.
#
# This is a space-separated list of filenames. The option may
# be specified more than once. The option may use wildcard
# characters.
#
SCRIPTWHITELIST=/bin/egrep
SCRIPTWHITELIST=/bin/fgrep
SCRIPTWHITELIST=/bin/which
SCRIPTWHITELIST=/usr/bin/groups
SCRIPTWHITELIST=/usr/bin/ldd
SCRIPTWHITELIST=/usr/bin/lwp-request
SCRIPTWHITELIST=/usr/sbin/adduser
SCRIPTWHITELIST=/usr/sbin/prelink
SCRIPTWHITELIST=/usr/bin/unhide.rb

#
# Allow the specified commands to have the immutable attribute set.
#
# This is a space-separated list of filenames. The option may
# be specified more than once. The option may use wildcard
# characters.
#
#IMMUTWHITELIST="/sbin/ifup /sbin/ifdown"

#
# If this option is set to 1, then the immutable-bit test is
# reversed. That is, the files are expected to have the bit set.
#
IMMUTABLE_SET=0

#
# Allow the specified hidden directories to be whitelisted.
#
# This is a space-separated list of directory pathnames.

^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```