



CONFIDENCIALIDAD E INTEGRIDAD

PRACTICA 1 Y 2

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

Prof. Miguel Angel González

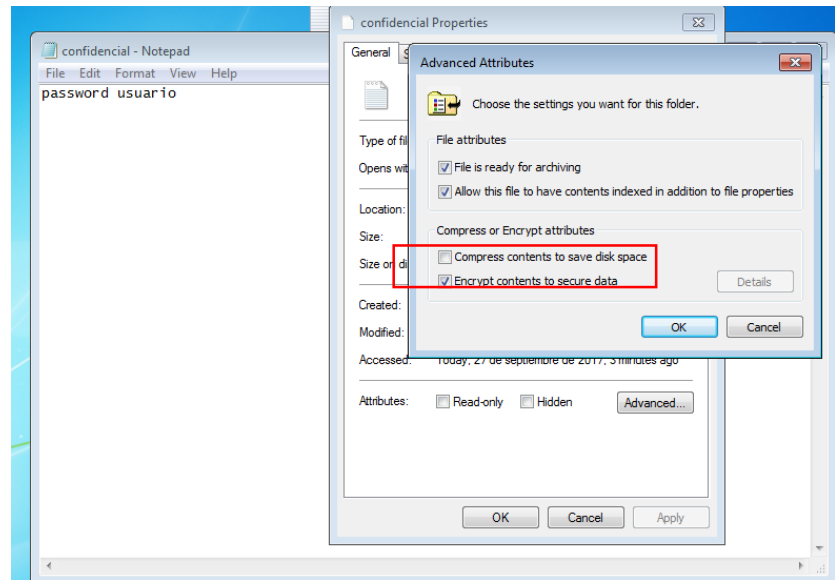
Autor: Rafael Osuna Ventura

PRACTICA 1: CONFIDENCIALIDAD

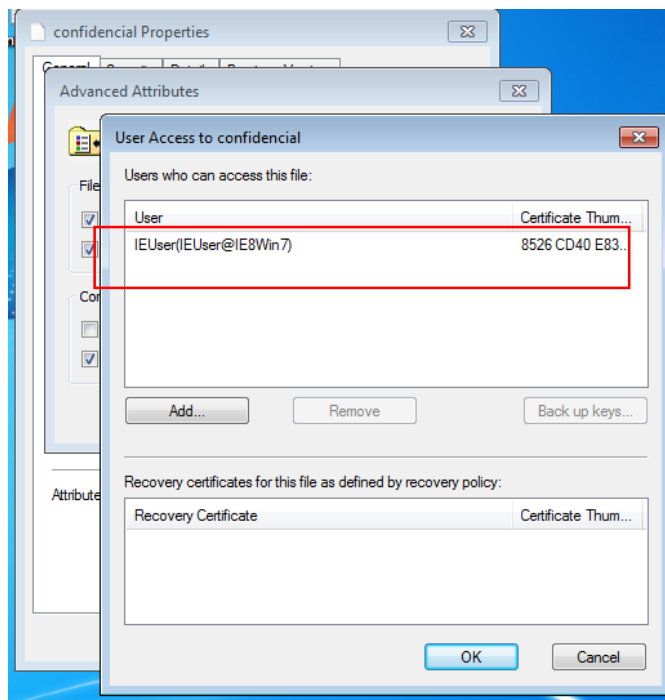
Se define confidencialidad como el servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. También puede verse como la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

Ahora vamos a poner esto en práctica realizando un proceso de encriptación en un archivo. Primero crearemos varios usuarios y en uno de estos creamos un documento el cual cifraremos.

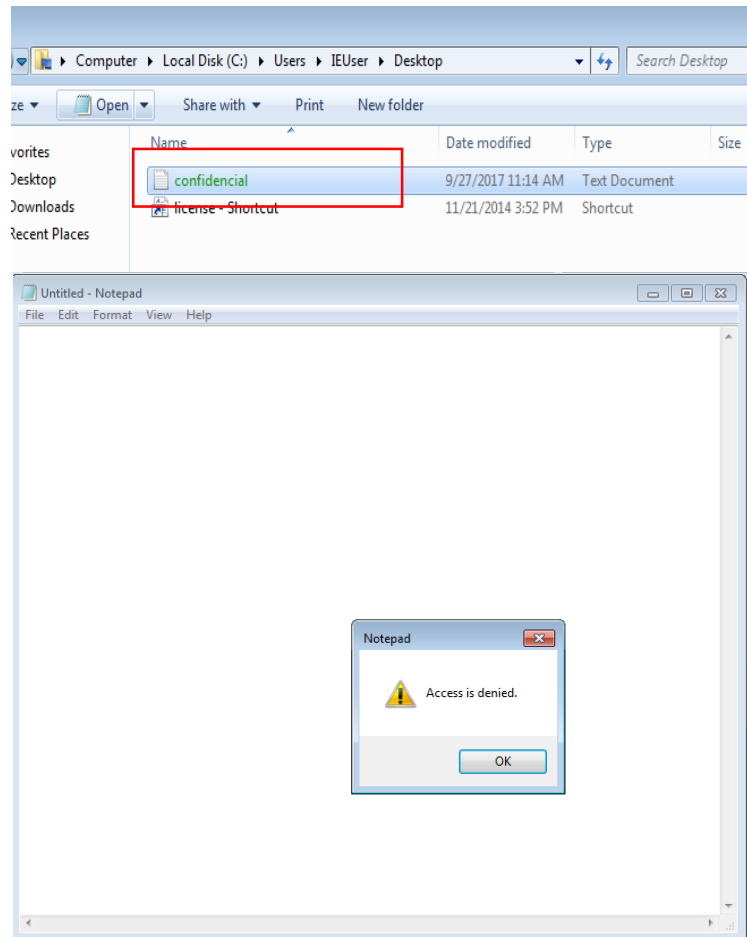
Una vez creado nos iremos a propiedades avanzadas del documento y activaremos la opción de cifrar el documento y que solo cifre ese archivo.



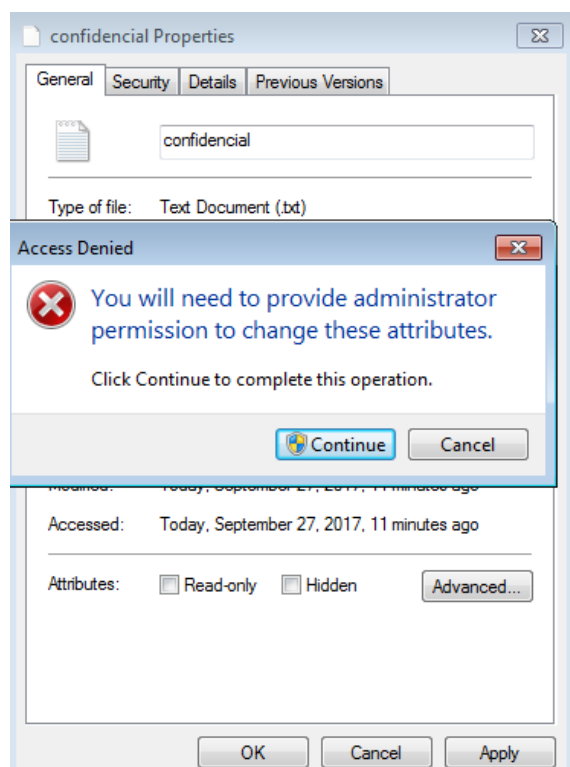
Si vamos a los detalles del cifrado observamos que solo nosotros tenemos acceso al documento (en mi caso el usuario es IEUser)



Ahora procedemos a comprobar la confidencialidad del documento. Para ello accedemos con un usuario que tenga permisos a todo el sistema. Desde este usuario buscamos el documento y vemos que nos sale el nombre del documento en verde, al abrirlo no nos deja.



Otra forma de comprobarlo es ver si podemos quitar el cifrado al archivo. Al intentarlo nos salta un mensaje diciendo que no podemos modificar el archivo.



PRACTICA 2: INTEGRIDAD

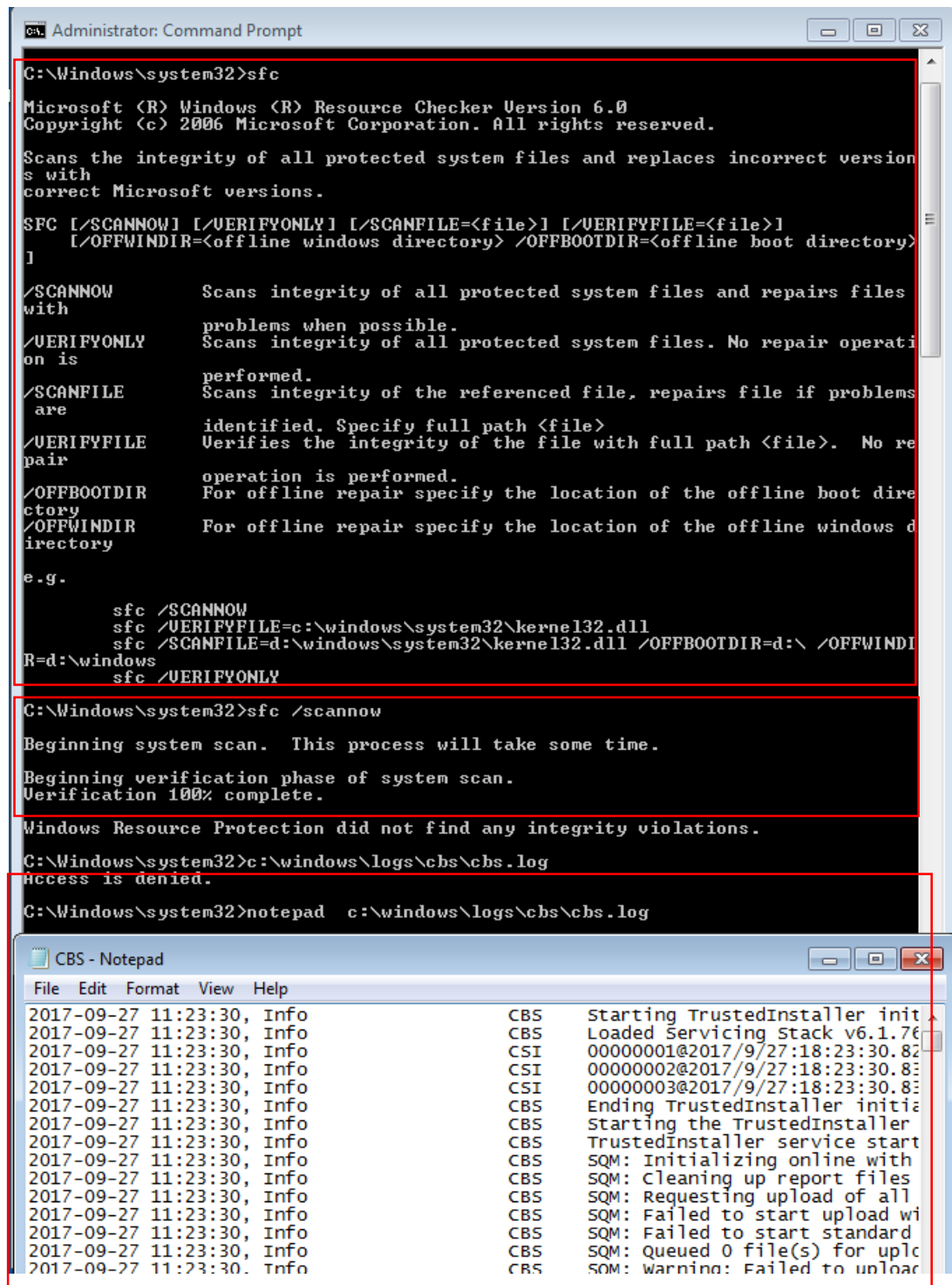
Definimos integridad como la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente.

Para verificar la integridad de nuestros archivos desde Windows utilizaremos una utilidad de Windows llamada System File Checker (SFC). Al ejecutarlo nos salen las distintas opciones que nos da esta utilidad, por ejemplo "scannow" nos permite verificar la integridad de TODOS nuestros archivos. Todos los datos de estos análisis se guardan en un registro que podemos comprobar en cualquier momento.

Opciones de SFC

Probamos la opción "scannow" para analizar nuestros archivos

Registro de SFC



```
Administrator: Command Prompt
C:\Windows\system32>sfc
Microsoft (R) Windows (R) Resource Checker Version 6.0
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

Scans the integrity of all protected system files and replaces incorrect versions with correct Microsoft versions.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<file>] [/VERIFYFILE=<file>]
    [/OFFWINDIR=<offline windows directory>] /OFFBOOTDIR=<offline boot directory>
]

/SCANNOW          Scans integrity of all protected system files and repairs files with problems when possible.
/VERIFYONLY       Scans integrity of all protected system files. No repair operation is performed.
/SCANFILE         Scans integrity of the referenced file, repairs file if problems are identified. Specify full path <file>
/VERIFYFILE       Verifies the integrity of the file with full path <file>. No repair operation is performed.
/OFFBOOTDIR       For offline repair specify the location of the offline boot directory
/OFFWINDIR        For offline repair specify the location of the offline windows directory
e.g.

sfc /SCANNOW
sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\
R=d:\windows
sfc /VERIFYONLY

C:\Windows\system32>sfc /scannow
Beginning system scan. This process will take some time.
Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection did not find any integrity violations.

C:\Windows\system32>c:\windows\logs\cbs\cbs.log
Access is denied.

C:\Windows\system32>notepad c:\windows\logs\cbs\cbs.log

CBS - Notepad
File Edit Format View Help
2017-09-27 11:23:30, Info CBS Starting TrustedInstaller initialization
2017-09-27 11:23:30, Info CBS Loaded Servicing Stack v6.1.7601.18005
2017-09-27 11:23:30, Info CSI 00000001@2017/9/27:18:23:30.82
2017-09-27 11:23:30, Info CSI 00000002@2017/9/27:18:23:30.82
2017-09-27 11:23:30, Info CSI 00000003@2017/9/27:18:23:30.82
2017-09-27 11:23:30, Info CBS Ending TrustedInstaller initialization
2017-09-27 11:23:30, Info CBS Starting the TrustedInstaller
2017-09-27 11:23:30, Info CBS TrustedInstaller service start
2017-09-27 11:23:30, Info CBS SQM: Initializing online with
2017-09-27 11:23:30, Info CBS SQM: Cleaning up report files
2017-09-27 11:23:30, Info CBS SQM: Requesting upload of all
2017-09-27 11:23:30, Info CBS SQM: Failed to start upload with
2017-09-27 11:23:30, Info CBS SQM: Failed to start standard
2017-09-27 11:23:30, Info CBS SQM: Queued 0 file(s) for upload
2017-09-27 11:23:30, Info CBS SQM: warning: Failed to unload
```

Para Linux utilizaremos una herramienta llamada Rootkit. Lo instalaremos y lo actualizaremos, luego lo probaremos para ver la integridad de nuestros archivos.

```
root@rafa-VirtualBox: /home/rafa
rafa@rafa-VirtualBox:~$ sudo su
[sudo] password for rafa:
root@rafa-VirtualBox:/home/rafa# apt-get install rkhunter
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  bsd-mailx fonts-lato javascript-common libjs-jquery liblockfile-bin
  liblockfile1 libruby2.3 postfix rake ruby ruby-did-you-mean ruby-minitest
  ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.3
  rubygems-integration unhide unhide.rb
Suggested packages:
  apache2 | lighttpd | httpd procmail postfix-mysql postfix-pgsql postfix-ldap
  postfix-pcre sasl2-bin dovecot-common postfix-cdb postfix-doc ri ruby-dev
  bundler
The following NEW packages will be installed:
  bsd-mailx fonts-lato javascript-common libjs-jquery liblockfile-bin
  liblockfile1 libruby2.3 postfix rake rkhunter ruby ruby-did-you-mean
  ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.3
  rubygems-integration unhide unhide.rb
0 upgraded, 24 newly installed, 0 to remove and 0 not upgraded.
Need to get 11.4 MB of archives.
After this operation, 45.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 fonts-lato all 1:1-3 [409 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 javascript-common all 11+nmu1 [58.9 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 libjs-jquery all 3.6.0-2 [133 kB]
Get:4 http://deb.debian.org/debian bullseye/main amd64 liblockfile1 amd64 1:1.1.2-3 [19.3 kB]
Get:5 http://deb.debian.org/debian bullseye/main amd64 liblockfile-bin amd64 1:1.1.2-3 [10.5 kB]
Get:6 http://deb.debian.org/debian bullseye/main amd64 libruby2.3 amd64 2.3.0-7 [442 kB]
Get:7 http://deb.debian.org/debian bullseye/main amd64 ruby2.3 amd64 2.3.0-7 [10.5 MB]
Get:8 http://deb.debian.org/debian bullseye/main amd64 ruby-minitest all 5.14.2-1 [47.8 kB]
Get:9 http://deb.debian.org/debian bullseye/main amd64 ruby-net-telnet all 0.0.1-4 [13.5 kB]
Get:10 http://deb.debian.org/debian bullseye/main amd64 ruby-power-assert all 1.1.3-1 [14.5 kB]
Get:11 http://deb.debian.org/debian bullseye/main amd64 ruby-test-unit all 3.2.9-1 [138 kB]
Get:12 http://deb.debian.org/debian bullseye/main amd64 ruby-did-you-mean all 1.3.0-1 [20.5 kB]
Get:13 http://deb.debian.org/debian bullseye/main amd64 rake all 12.3.0-1 [16.7 kB]
Get:14 http://deb.debian.org/debian bullseye/main amd64 postfix amd64 3.6.4-1 [10.5 MB]
Get:15 http://deb.debian.org/debian bullseye/main amd64 postfix-pgsql amd64 3.6.4-1 [10.5 MB]
Get:16 http://deb.debian.org/debian bullseye/main amd64 postfix-mysql amd64 3.6.4-1 [10.5 MB]
Get:17 http://deb.debian.org/debian bullseye/main amd64 postfix-cdb amd64 3.6.4-1 [10.5 MB]
Get:18 http://deb.debian.org/debian bullseye/main amd64 postfix-pcre amd64 3.6.4-1 [10.5 MB]
Get:19 http://deb.debian.org/debian bullseye/main amd64 postfix-doc all 3.6.4-1 [10.5 MB]
Get:20 http://deb.debian.org/debian bullseye/main amd64 postfix-sasl2 amd64 3.6.4-1 [10.5 MB]
Get:21 http://deb.debian.org/debian bullseye/main amd64 postfix-lldap amd64 3.6.4-1 [10.5 MB]
Get:22 http://deb.debian.org/debian bullseye/main amd64 postfix-imap4 amd64 3.6.4-1 [10.5 MB]
Get:23 http://deb.debian.org/debian bullseye/main amd64 postfix-smtp-amd64 amd64 3.6.4-1 [10.5 MB]
Get:24 http://deb.debian.org/debian bullseye/main amd64 postfix-smtp-amd64 amd64 3.6.4-1 [10.5 MB]
Fetched 11.4 MB in 1m 1s (10.5 MB/s)
Selecting previously unselected package fonts-lato.
(Reading database ... 123456 files and directories currently installed.)
Preparing to unpack .../fonts-lato_1:1-3_all.deb ...
Unpacking fonts-lato (1:1-3) ...
Selecting previously unselected package javascript-common.
Unpacking javascript-common (11+nmu1) ...
Selecting previously unselected package libjs-jquery.
Unpacking libjs-jquery (3.6.0-2) ...
Selecting previously unselected package liblockfile1.
Unpacking liblockfile1 (1:1.1.2-3) ...
Selecting previously unselected package liblockfile-bin.
Unpacking liblockfile-bin (1:1.1.2-3) ...
Selecting previously unselected package libruby2.3.
Unpacking libruby2.3 (2.3.0-7) ...
Selecting previously unselected package ruby2.3.
Unpacking ruby2.3 (2.3.0-7) ...
Selecting previously unselected package ruby-minitest.
Unpacking ruby-minitest (5.14.2-1) ...
Selecting previously unselected package ruby-net-telnet.
Unpacking ruby-net-telnet (0.0.1-4) ...
Selecting previously unselected package ruby-power-assert.
Unpacking ruby-power-assert (1.1.3-1) ...
Selecting previously unselected package ruby-test-unit.
Unpacking ruby-test-unit (3.2.9-1) ...
Selecting previously unselected package ruby-did-you-mean.
Unpacking ruby-did-you-mean (1.3.0-1) ...
Selecting previously unselected package rake.
Unpacking rake (12.3.0-1) ...
Selecting previously unselected package postfix.
Unpacking postfix (3.6.4-1) ...
Selecting previously unselected package postfix-pgsql.
Unpacking postfix-pgsql (3.6.4-1) ...
Selecting previously unselected package postfix-mysql.
Unpacking postfix-mysql (3.6.4-1) ...
Selecting previously unselected package postfix-cdb.
Unpacking postfix-cdb (3.6.4-1) ...
Selecting previously unselected package postfix-pcre.
Unpacking postfix-pcre (3.6.4-1) ...
Selecting previously unselected package postfix-doc.
Unpacking postfix-doc (3.6.4-1) ...
Selecting previously unselected package postfix-sasl2.
Unpacking postfix-sasl2 (3.6.4-1) ...
Selecting previously unselected package postfix-lldap.
Unpacking postfix-lldap (3.6.4-1) ...
Selecting previously unselected package postfix-imap4.
Unpacking postfix-imap4 (3.6.4-1) ...
Selecting previously unselected package postfix-smtp-amd64.
Unpacking postfix-smtp-amd64 (3.6.4-1) ...
Selecting previously unselected package postfix-smtp-amd64.
Unpacking postfix-smtp-amd64 (3.6.4-1) ...
Setting up fonts-lato (1:1-3) ...
Setting up javascript-common (11+nmu1) ...
Setting up libjs-jquery (3.6.0-2) ...
Setting up liblockfile1 (1:1.1.2-3) ...
Setting up liblockfile-bin (1:1.1.2-3) ...
Setting up libruby2.3 (2.3.0-7) ...
Setting up ruby2.3 (2.3.0-7) ...
Setting up ruby-minitest (5.14.2-1) ...
Setting up ruby-net-telnet (0.0.1-4) ...
Setting up ruby-power-assert (1.1.3-1) ...
Setting up ruby-test-unit (3.2.9-1) ...
Setting up ruby-did-you-mean (1.3.0-1) ...
Setting up rake (12.3.0-1) ...
Setting up postfix (3.6.4-1) ...
Setting up postfix-pgsql (3.6.4-1) ...
Setting up postfix-mysql (3.6.4-1) ...
Setting up postfix-cdb (3.6.4-1) ...
Setting up postfix-pcre (3.6.4-1) ...
Setting up postfix-doc (3.6.4-1) ...
Setting up postfix-sasl2 (3.6.4-1) ...
Setting up postfix-lldap (3.6.4-1) ...
Setting up postfix-imap4 (3.6.4-1) ...
Setting up postfix-smtp-amd64 (3.6.4-1) ...
Setting up postfix-smtp-amd64 (3.6.4-1) ...
root@rafa-VirtualBox:/home/rafa# rkhunter --checkall
[ 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 ]
```