

Práctica 1

Principios de seguridad y disponibilidad

Col·legi Sant Josep Obrer
Seguretat y alta disponibilitat

ASIX 2

Piqueras Sastre Alejandro

Hatim Amtil Ouahdi

Daniel Rosselló Sánchez

Índice de contenido

Práctica 1.1 Confidencialidad.....	3
Proceso de encriptación.....	3
1.-Creación del archivo.....	3
2.-Encriptación del archivo desde entorno gráfico.....	4
3.-Encriptación del archivo desde entorno texto.....	7
Verificaciones.....	8
1.-Acceso al archivo con otro usuario con permisos para acceder a todo el sistema de archivos..	8
1.1.-Acceso al contenido.....	8
1.2.-Modificar el atributo para que deje de estar cifrado.....	9
1.3.-Borrar el archivo.....	10
2.-Mover/Copiar y atributo de compresión.....	11
2.1.-Mover/Copiar a una unidad FAT.....	11
2.2.-Atributo de compresión.....	13
3.-Acceso al archivo desde otro SO.....	14
3.1.-Acceso al contenido.....	14
3.2.-Copiar el archivo.....	15
3.3.-Borrar el archivo.....	16
4.- Compresión en .zip.....	17
4.1.-Desde un usuario sin permisos.....	17
4.2.-Desde un usuario con permisos.....	18
Practica 1.2 Integridad.....	19
1.-Descripción de la herramienta SFC.....	19
1.1.-Opciones de SFC.....	20
1.2.-Funcionamiento.....	22
1.2.1.-/SCANNOW.....	22
1.2.2.-/SCANNOW con error.....	23
1.2.3.-Archivo CBS.log.....	24
2.-Descripción de la herramienta RKHUNTER.....	25
2.1.-Instalar rkhunter.....	25
2.2.-Funciones de rkhunter.....	26
2.2.1.- Opción chekall.....	26
2.2.2.-.....	28
2.2.3.-Opción checkall con error.....	29
Practica 1.3 Disponibilidad.....	30
Práctica 1.4 Alta disponibilidad.....	35
Calcular la disponibilidad del 99'99%(4 nueves) y la del 99'9%(3 nueves).....	35
1.-99'99%.....	35
2.-99'9%.....	35
Problemas encontrados.....	36
Opinión personal.....	37
Hatim Amtil Ouahdi.....	37

Daniel Rosselló Sánchez.....	37
Alex Piqueras Sastre.....	37
Bibliografía.....	38
Libro de Seguridad y alta disponibilidad.....	38

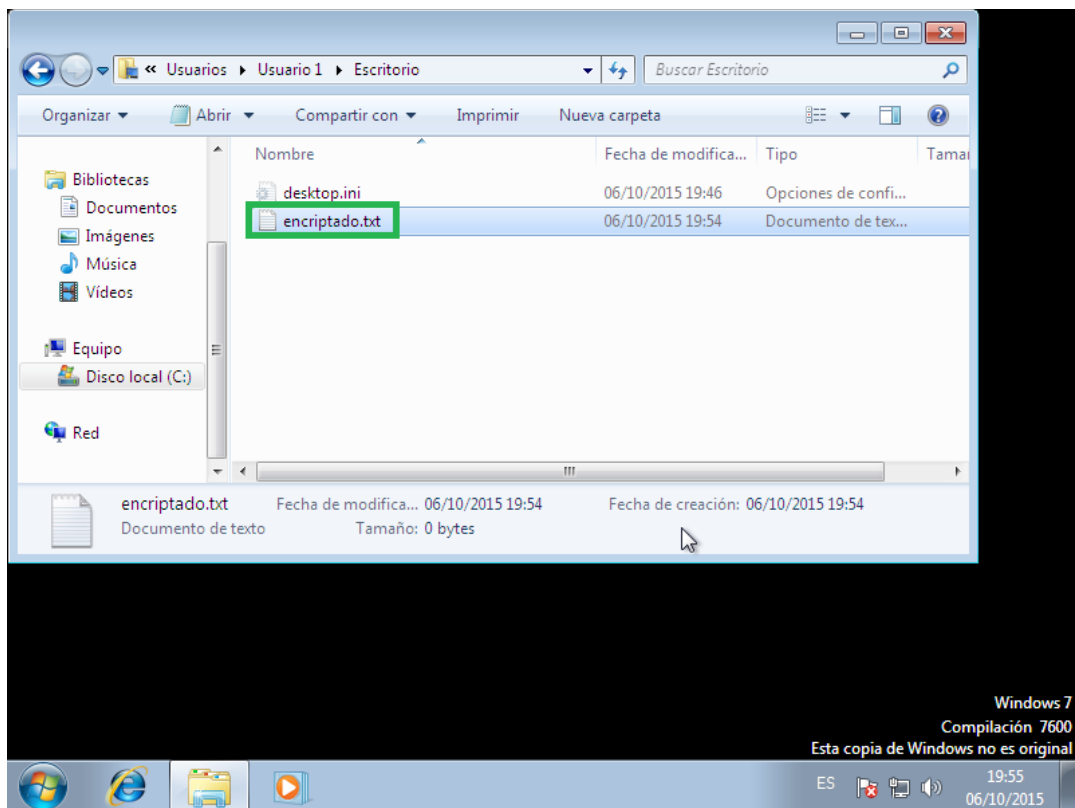
Práctica 1.1 Confidencialidad

Proceso de encriptación.

Tenemos dos formas de encriptar archivos. Una es desde entorno gráfico y la otra desde la consola de comandos (CMD).

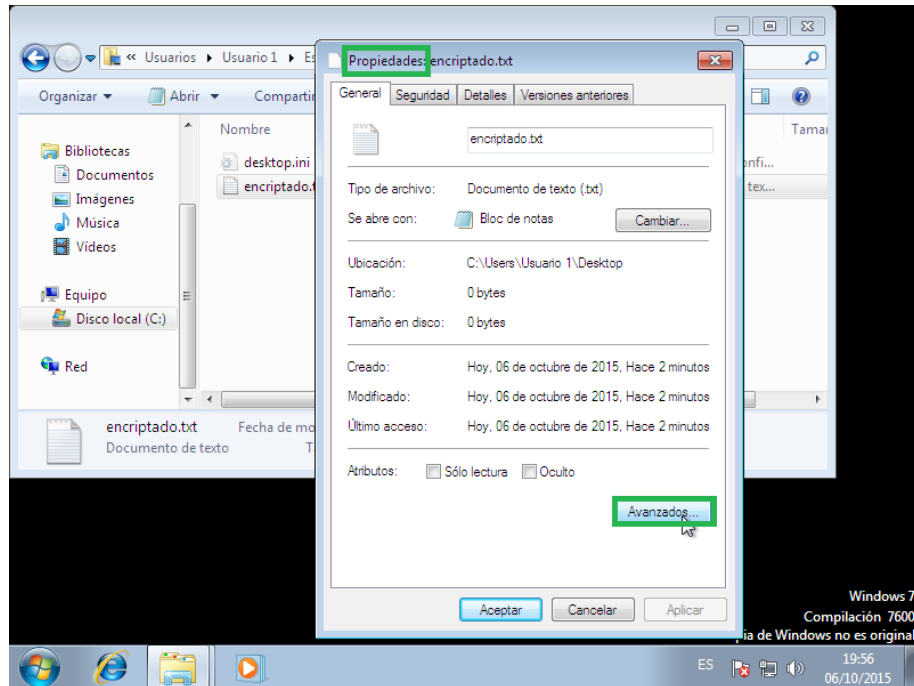
1.- Creación del archivo

Creamos un archivo en el escritorio del "Usuario 1" llamado "encriptado.txt". Dentro escribiremos una secuencia de números (987654321).

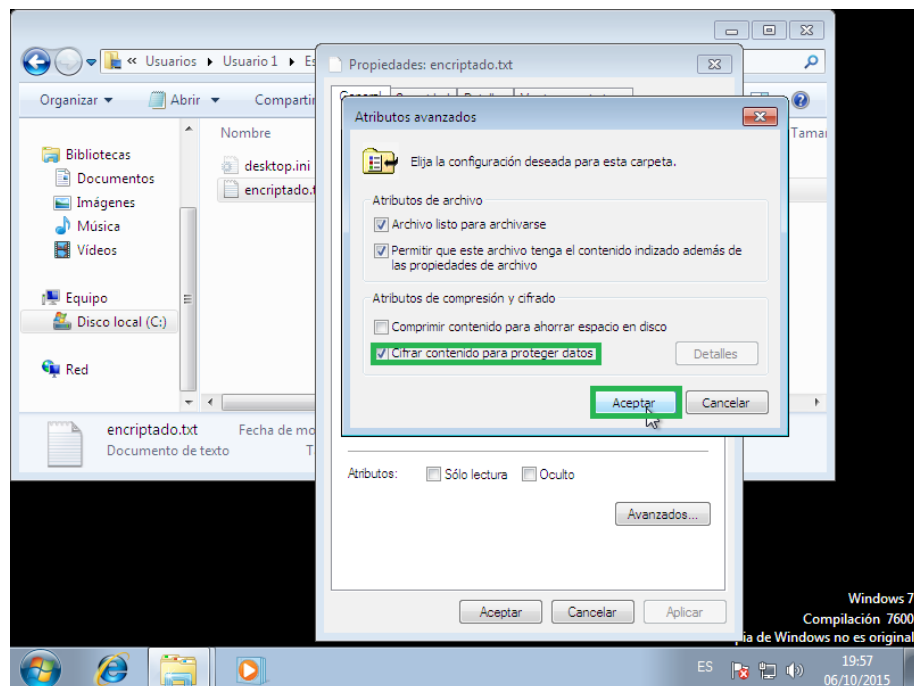


2.- Encriptación del archivo desde entorno gráfico

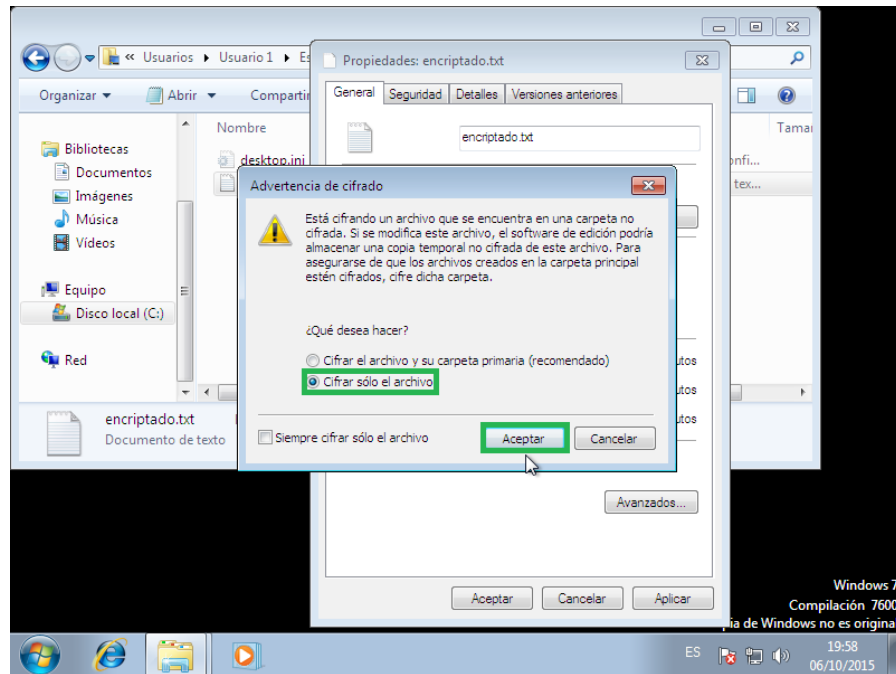
Le damos clic derecho al archivo y en el Menú contextual elegimos Propiedades. Una vez allí en General elegimos Avanzados que se encuentra abajo a la derecha.



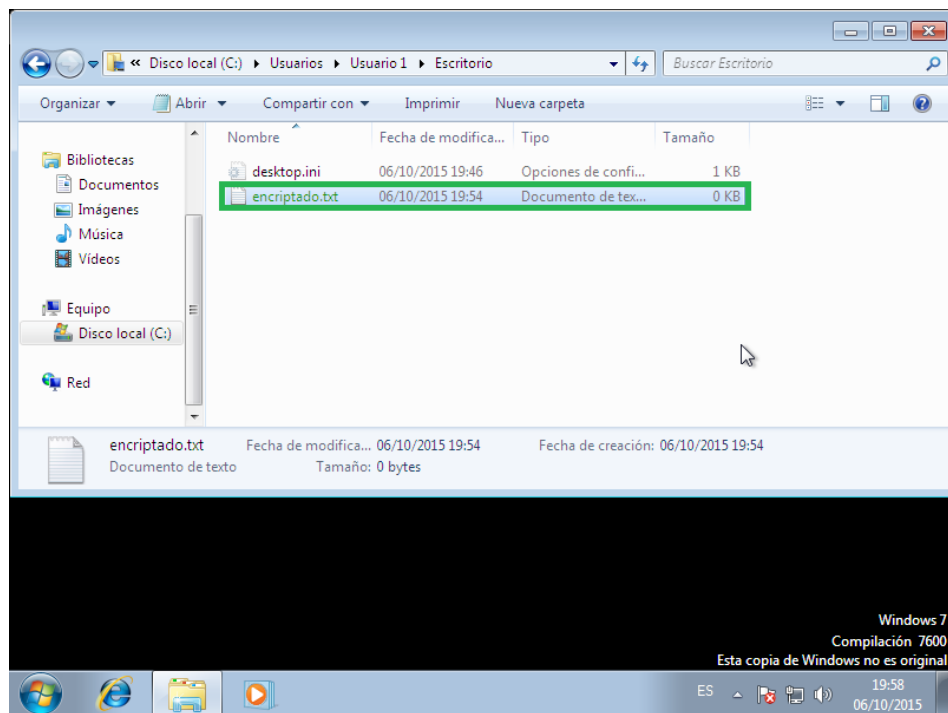
Después de esto nos saldrá una ventana para elegir opciones mas avanzadas. Elegiremos la opción de "Cifrar contenido para proteger datos". Después le daremos a "Aceptar".



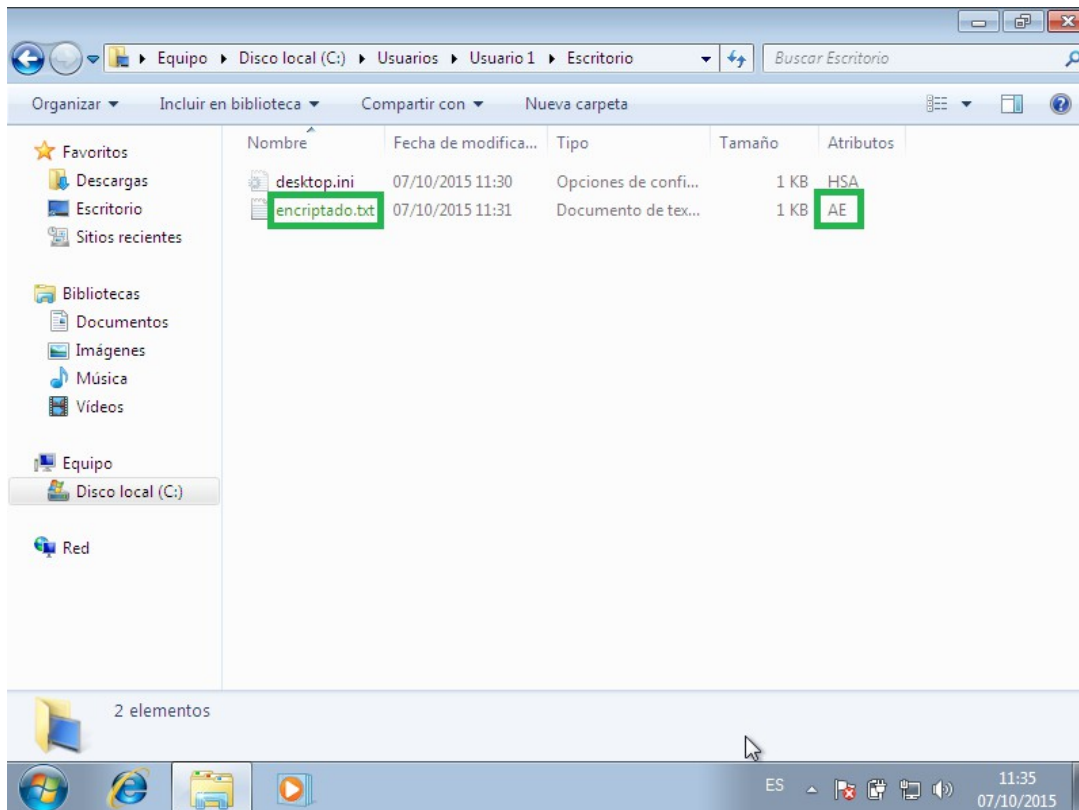
Tras aceptar nos saltara una advertencia por si queremos encriptar "El archivo y su carpeta primaria" o "solo el archivo". Elegiremos la opción de "Solo el archivo".



Tras esto podemos ver que el archivo ha sido encriptado.

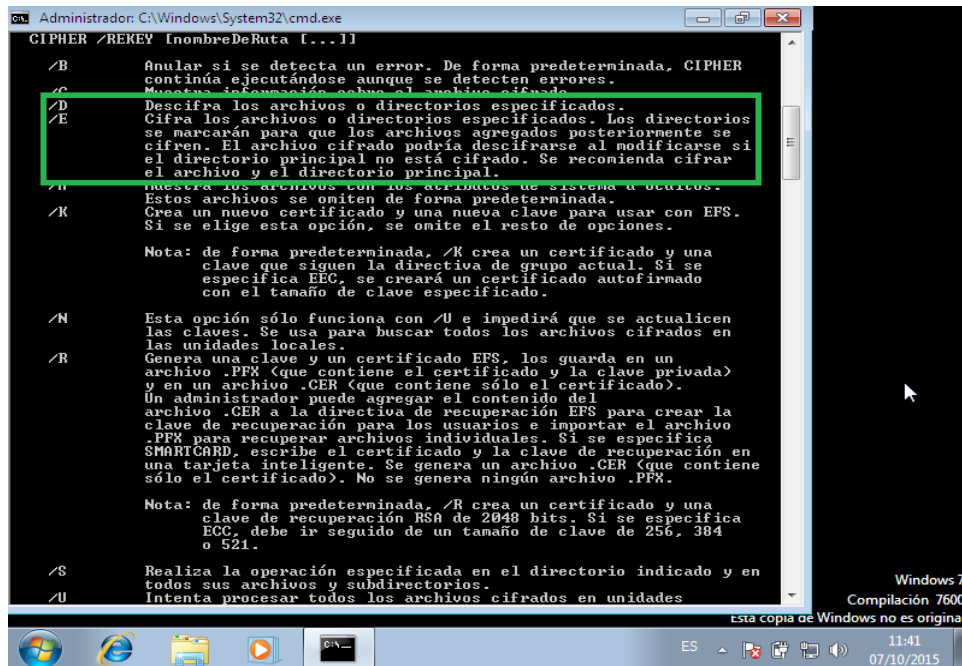


Hay que destacar de la anterior imagen que el archivo a pasado a tener el nombre de color verde para poder identificar que dicho archivo a sido encriptado. Tambien podremos saber si esta encriptado si tenemos activa la columna de atributos en el Explorador de Windows (Una E).



3.- Encriptación del archivo desde entorno texto.

Para encriptar archivos desde el entorno texto usaremos la orden **CIPHER** en la CMD.



```
Administrador: C:\Windows\System32\cmd.exe
CIPHER /?KEY InombreDeRuta [...]

/B Anular si se detecta un error. De forma predeterminada, CIPHER
continúa ejecutándose aunque se detecten errores.
/C Muestra información sobre el archivo cifrado.
/D Descifra los archivos o directorios especificados.
/E Cifra los archivos o directorios especificados. Los directorios
se marcarán para que los archivos agregados posteriormente se
cifren. El archivo cifrado podría descifrarse al modificarse si
el directorio principal no está cifrado. Se recomienda cifrar
el archivo y el directorio principal.
/H Muestra los archivos con los atributos de sistema u ocultos.
Estos archivos se omiten de forma predeterminada.
/K Crea un nuevo certificado y una nueva clave para usar con EFS.
Si se elige esta opción, se omite el resto de opciones.

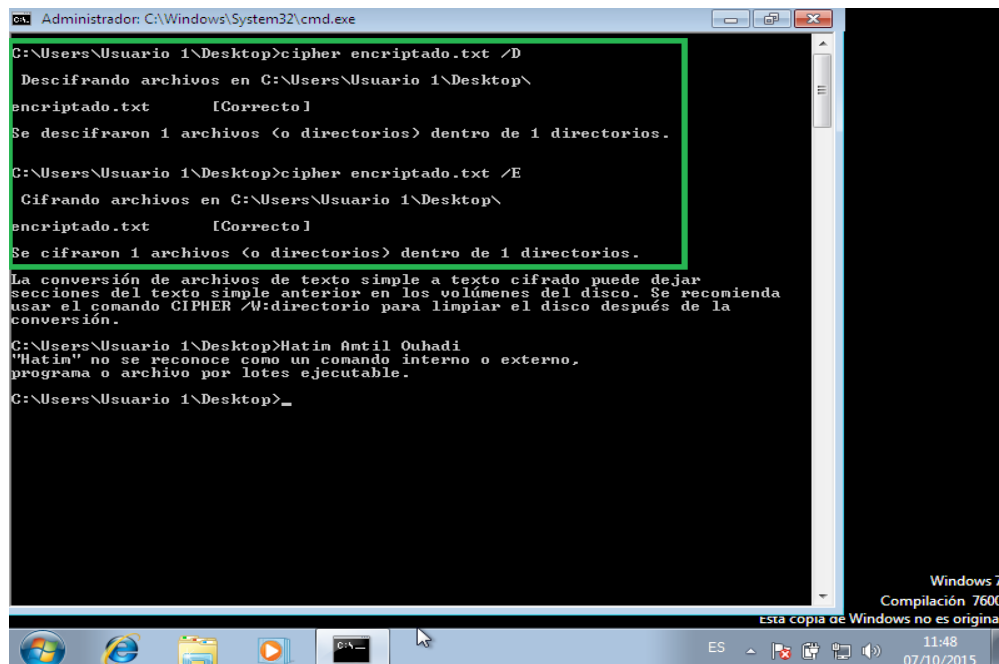
Nota: de forma predeterminada, /K crea un certificado y una
clave que siguen la directiva de grupo actual. Si se
especifica EEC, se creará un certificado autofirmado
con el tamaño de clave especificado.

/N Esta opción sólo funciona con /U e impedirá que se actualicen
las claves. Se usa para buscar todos los archivos cifrados en
las unidades locales.
/R Genera una clave y un certificado EFS, los guarda en un
archivo .PFX (que contiene el certificado y la clave privada)
y en un archivo .CER (que contiene sólo el certificado).
Un administrador puede agregar el contenido del
archivo .CER a la directiva de recuperación EFS para crear la
clave de recuperación para los usuarios e importar el archivo
.PFX para recuperar archivos individuales. Si se especifica
SMARTCARD, escribe el certificado y la clave de recuperación en
una tarjeta inteligente. Se genera un archivo .CER (que contiene
sólo el certificado). No se genera ningún archivo .PFX.

Nota: de forma predeterminada, /R crea un certificado y una
clave de recuperación RSA de 2048 bits. Si se especifica
ECC, debe ir seguido de un tamaño de clave de 256, 384
o 521.

/S Realiza la operación especificada en el directorio indicado y en
todos sus archivos y subdirectorios.
/U Intenta procesar todos los archivos cifrados en unidades
```

Revertiremos el encriptado del anterior archivo y lo volveremos a encriptar.



```
Administrador: C:\Windows\System32\cmd.exe

C:\Users\Usuario 1\Desktop>cipher encriptado.txt /D
Descifrando archivos en C:\Users\Usuario 1\Desktop\
encriptado.txt [Correcto]
Se descifraron 1 archivos (o directorios) dentro de 1 directorios.

C:\Users\Usuario 1\Desktop>cipher encriptado.txt /E
Cifrando archivos en C:\Users\Usuario 1\Desktop\
encriptado.txt [Correcto]
Se cifraron 1 archivos (o directorios) dentro de 1 directorios.

La conversión de archivos de texto simple a texto cifrado puede dejar
secciones del texto simple anterior en los volúmenes del disco. Se recomienda
usar el comando CIPHER /W:directorio para limpiar el disco después de la
conversión.

C:\Users\Usuario 1\Desktop>Hatim Antil Ouhadi
"Hatim" no se reconoce como un comando interno o externo.
programa o archivo por lotes ejecutable.

C:\Users\Usuario 1\Desktop>_
```


Verificaciones

Haremos una serie de comprobaciones sobre el archivo encriptado anteriormente.

- 1.- Acceso al archivo con otro usuario con permisos para acceder a todo el sistema de archivos.

En este apartado haremos tres comprobaciones:

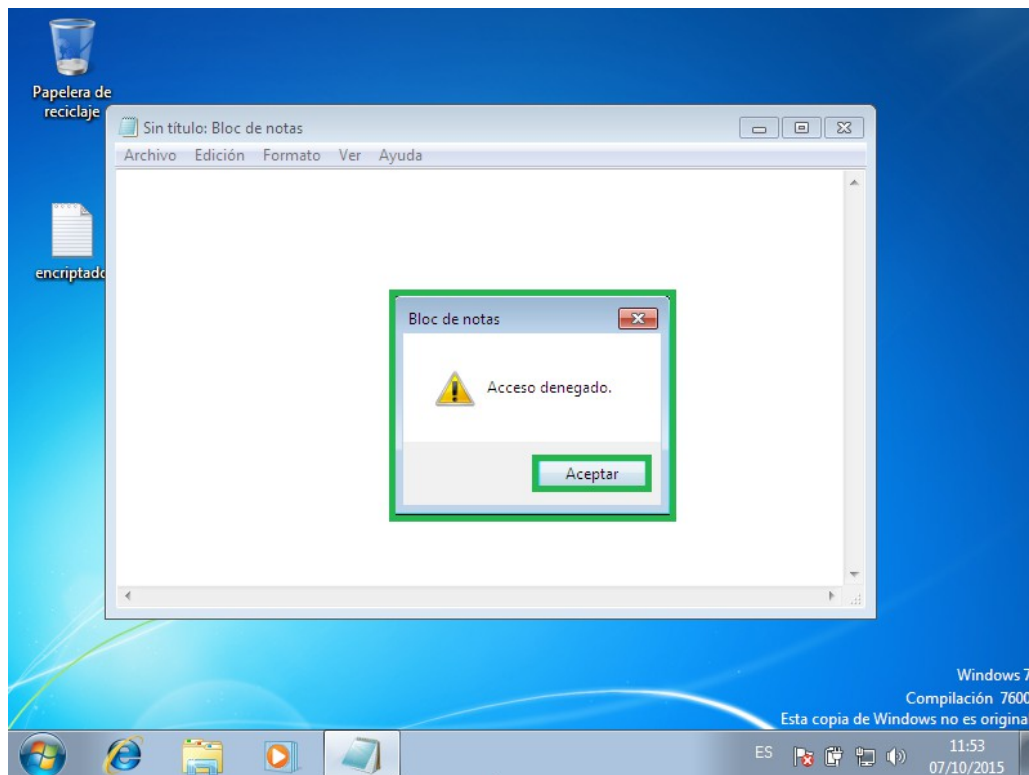
Acceso al contenido

Modificar el atributo para que deje de estar cifrado

Borrar el archivo

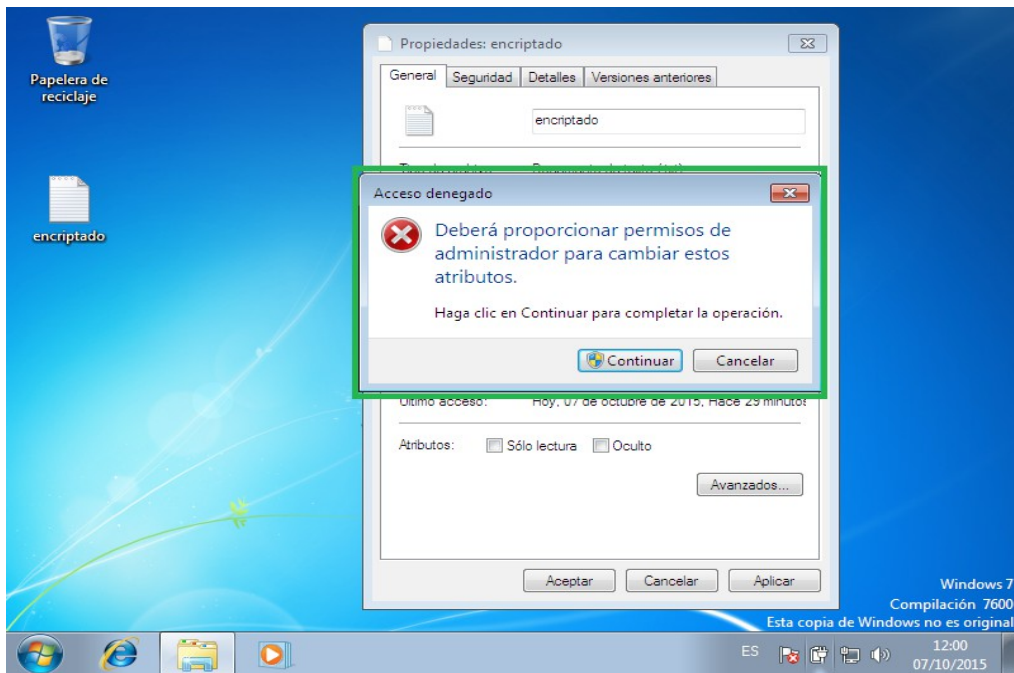
1.1.- Acceso al contenido

Intentaremos acceder al contenido dando doble clic al archivo. Tras realizar esto nos saldra una ventana con el siguiente mensaje.



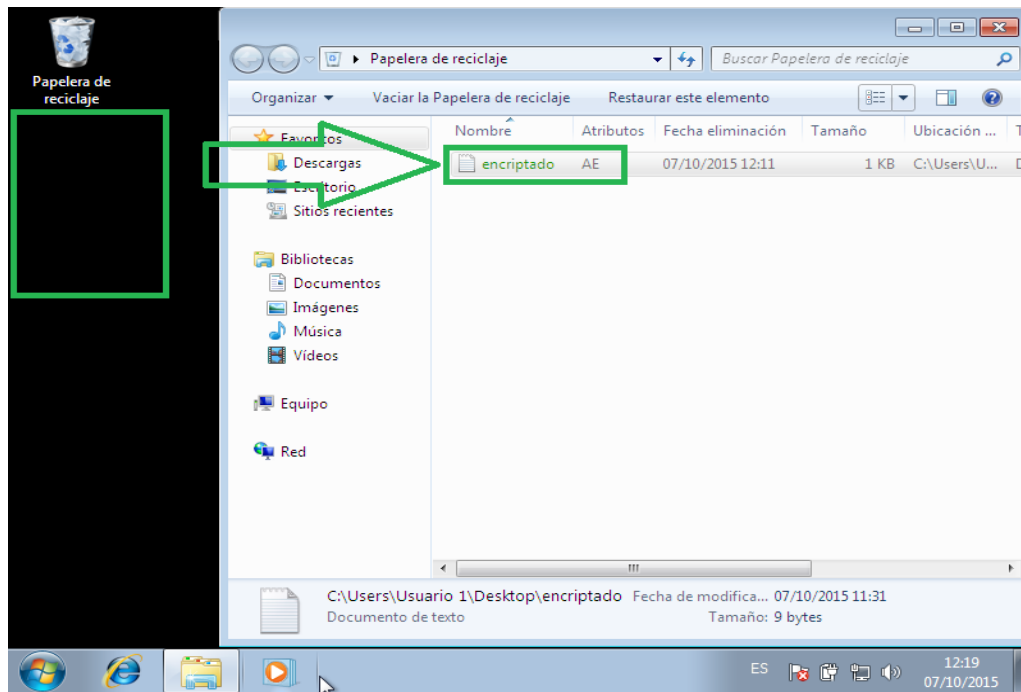
1.2.- Modificar el atributo para que deje de estar cifrado.

Si repetimos los pasos anteriores que hicimos para encriptar el archivo desde el entorno gráfico veremos que en la parte cuando tenemos que dar clic a "Avanzados ..." no saltará un mensaje que nos deniega el acceso.



1.3.- Borrar el archivo

Si intentamos borrar el archivo los permisos ha tener en cuenta son los del directorio y en el tenemos permiso a borrar lo que hay en su interior por lo tanto no habrá ningún problema de borrar el archivo.

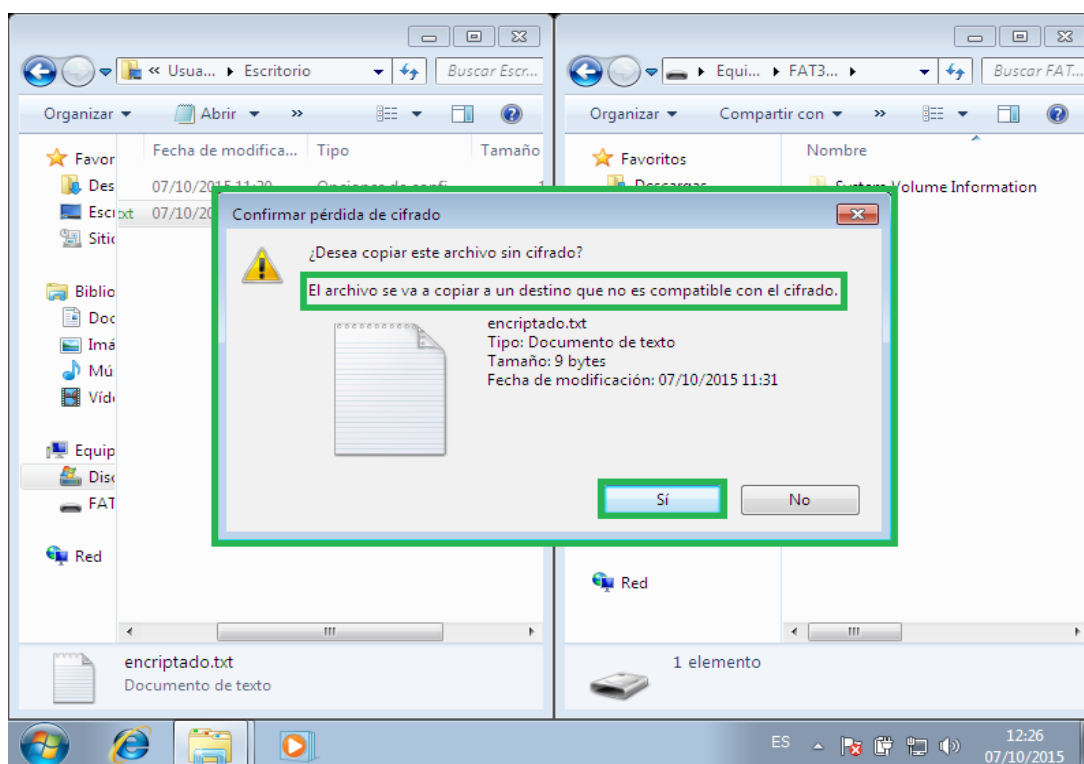


2.- Mover/Copiar y atributo de compresión.

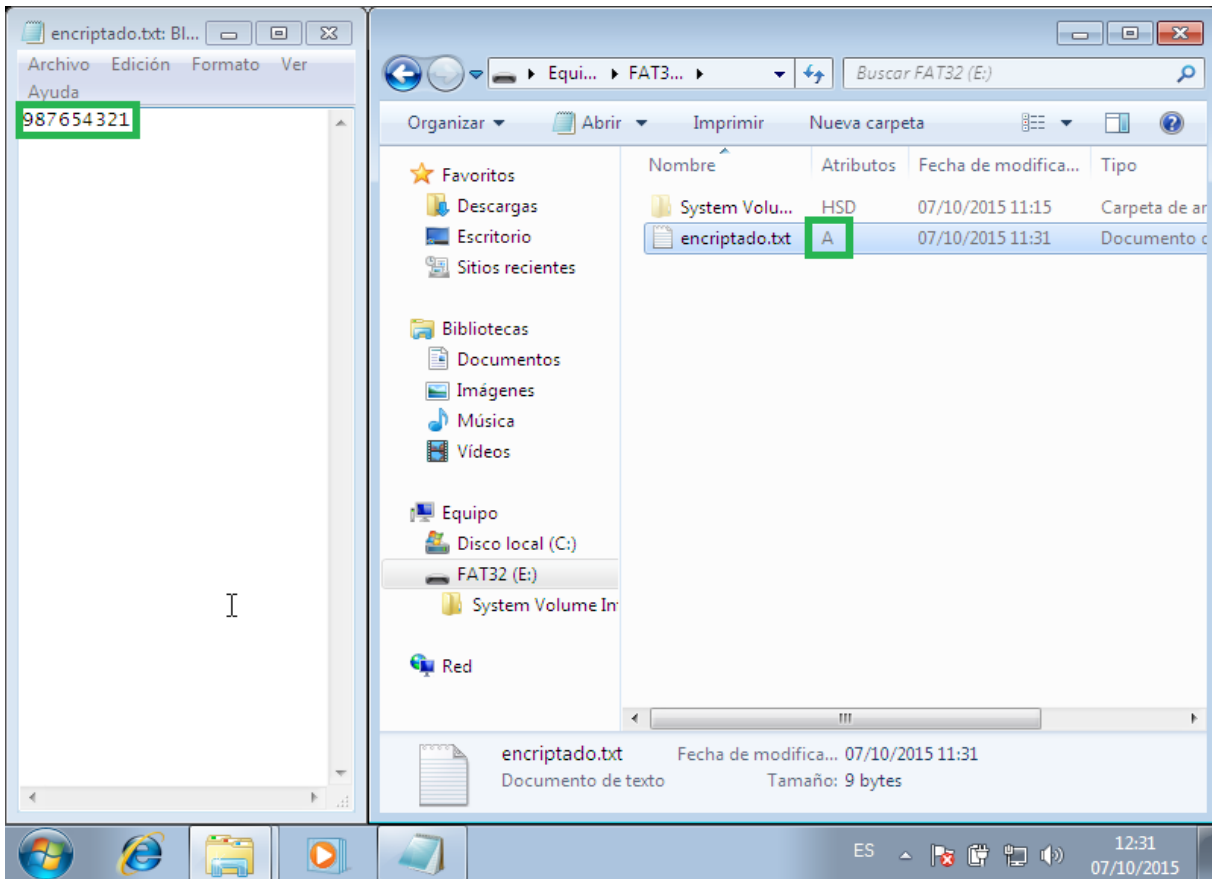
Intentaremos mover el archivo a una unidad externa con FAT para comprobar si se puede. De conseguirlo el encriptado se perdería ya que en FAT no existe el atributo E. Por ultimo veremos la incompatibilidad del atributo de compresión (C) y el de encriptacion (E).

2.1.- Mover/Copiar a una unidad FAT.

Si intentamos mover un archivo encriptado a una unidad FAT no nos dejara salvo que tengamos permiso para hacerlo. Si no tenemos permiso de copiar el archivo tampoco tendremos el de mover lo. En este caso para comprobar si se pierde el encriptado lo haremos desde el Admin y así ver como perdemos el encriptado.

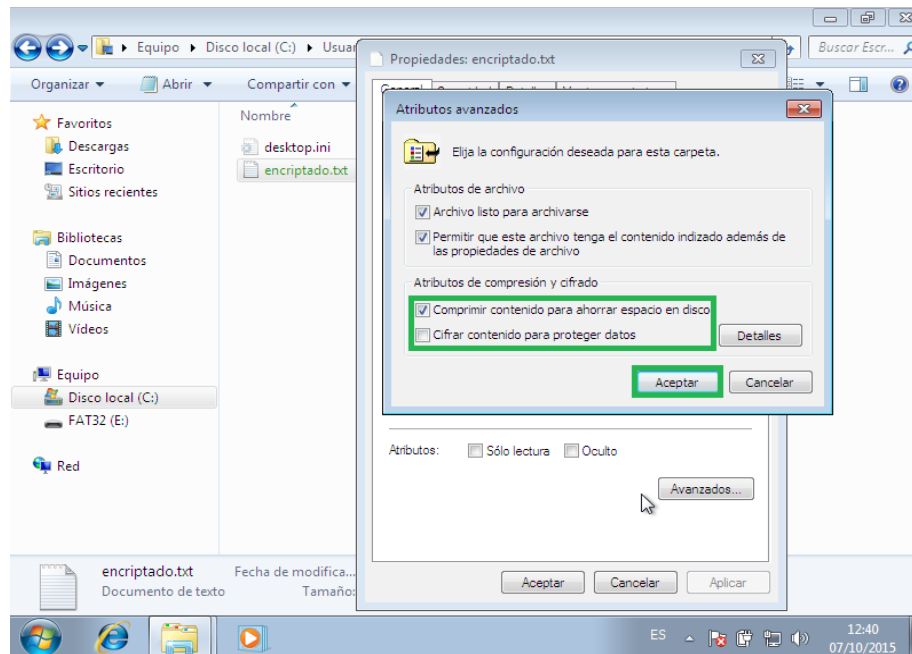


En la siguiente imagen podremos ver el contenido del archivo que habíamos escrito previamente antes. Así confirmamos la pérdida del cifrado pasando el archivo a una unidad FAT.

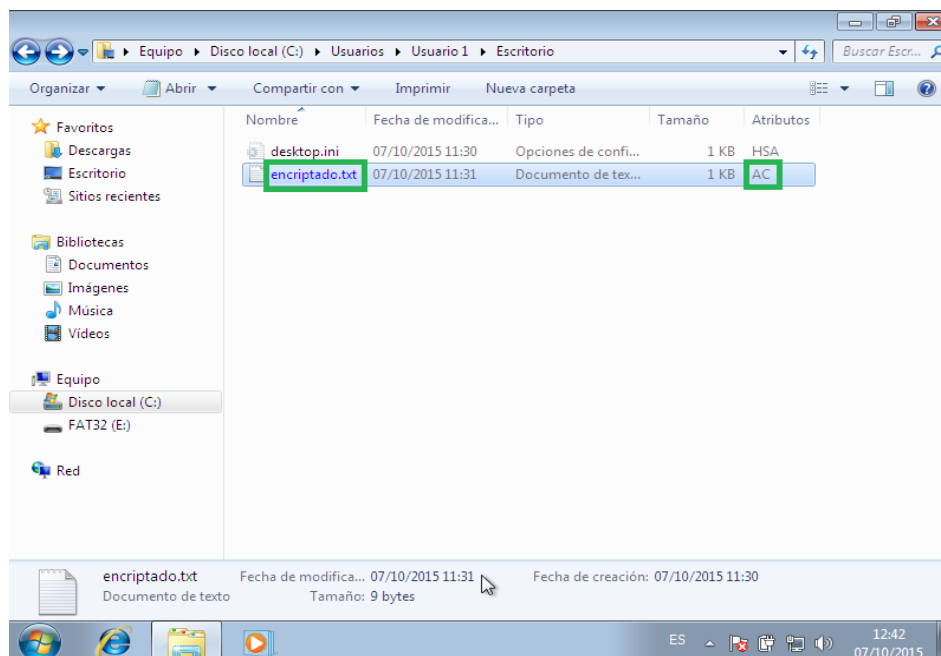


2.2.- Atributo de compresión.

EL atributo de compresión es incompatible con el de encriptación por lo tanto el archivo se desencriptará tras activar el atributo de compresión. No deja tener el Check en las dos zonas de "Atributos de compresión y cifrado"



Una vez terminado veremos como el nombre del archivo se vuelve azul.



3.- Acceso al archivo desde otro SO.

Desde un ArchLinux comprobaremos si podemos:

Acceso al contenido

Copiar archivo

Borrar el archivo

3.1.- Acceso al contenido

```
[root@ArchLinux-UM Desktop]# HATIM AMTIL OUHADI
-bash: HATIM: command not found
[root@ArchLinux-UM Desktop]# cat encriptado.txt
cat: encriptado.txt: Permission denied
[root@ArchLinux-UM Desktop]# _
```

No podremos acceder al archivo. Nos pondrá "Permission denied".

3.2.- Copiar el archivo

Tampoco podremos copiar el archivo. Esta orden nos da un error de lectura y lo que hace es crear un archivo con el mismo nombre "encriptado.txt" pero al ser un archivo nuevo no contiene nada.

```
[root@ArchLinux-VM Desktop]# HATIM AMTIL OUHADI
-bash: HATIM: command not found
[root@ArchLinux-VM Desktop]# cp encriptado.txt ..
cp: error reading 'encriptado.txt': Permission denied
[root@ArchLinux-VM Desktop]# _
```

En la siguiente imagen podemos ver como ha creado una copia en el destino. Este archivo no contiene nada.

```
Entorno de red
Favorites
Impresoras
Links
Men?? Inicio
Mis documentos
Music
NTUSER.DAT
NTUSER.DAT{6cccd2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf
NTUSER.DAT{6cccd2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000001
.regtrans-ms
NTUSER.DAT{6cccd2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000002
.regtrans-ms
Pictures
Plantillas
Reciente
Saved Games
Searches
SendTo
Videos
encriptado.txt
ntuser.dat.LOG1
ntuser.dat.LOG2
ntuser.ini
[root@ArchLinux-VM Desktop]# _
```


3.3.- Borrar el archivo

Como ya hemos comentado antes los permisos del archivo no influyen en el borrado de ellos mismo por lo tanto los permisos del directorio serán los que influyan en el borrado.

```
[root@ArchLinux-UM Desktop]# HATIM AMTIL OUHADI
-bash: HATIM: command not found
[root@ArchLinux-UM Desktop]# ls .
lesktop.ini  encriptado.txt
[root@ArchLinux-UM Desktop]# rm encriptado.txt
[root@ArchLinux-UM Desktop]# ls .
lesktop.ini
[root@ArchLinux-UM Desktop]# _
```

4.- Compresión en .zip.

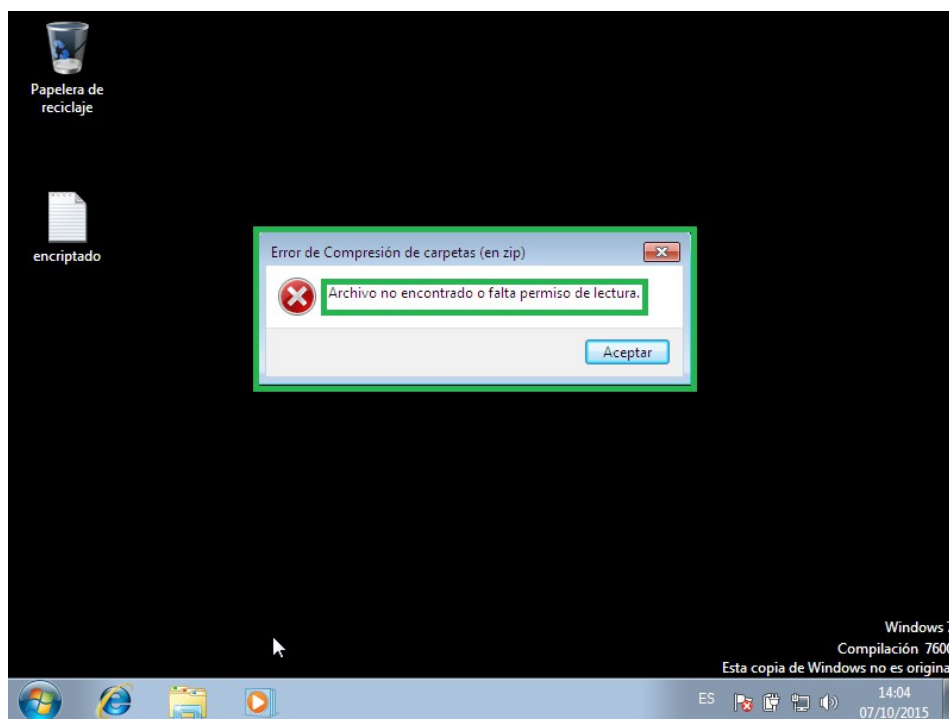
Haremos dos comprobaciones:

Desde un usuario sin permisos.

Desde un usuario con permisos.

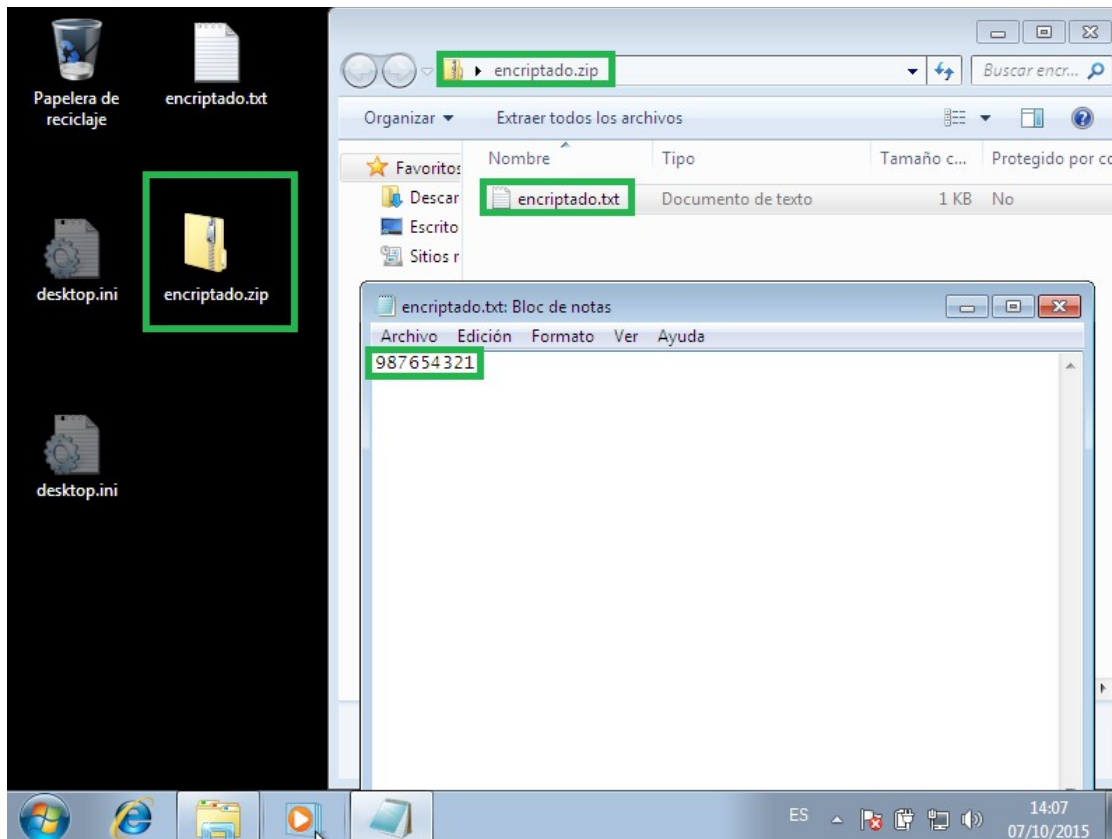
4.1.- Desde un usuario sin permisos.

Primero intentaremos comprimir desde un Usuario sin permiso de lectura. Esto nos dará un error y nos saltara la siguiente ventana.



4.2.- Desde un usuario con permisos.

Si lo hacemos desde el Admin podremos comprimir sin problemas y después desde el "encriptado.zip" podremos acceder a la información del encriptado.txt sin ningún problema. Sería como cuando utilizábamos el permiso de compresión. No son compatibles por lo tanto se pierde el encriptado al comprimir el archivo.



Practica 1.2 Integridad

Describir y comprobar el funcionamiento de las herramientas SFC en Windows 7 y RKHUNTER para Linux..

1.- Descripción de la herramienta SFC

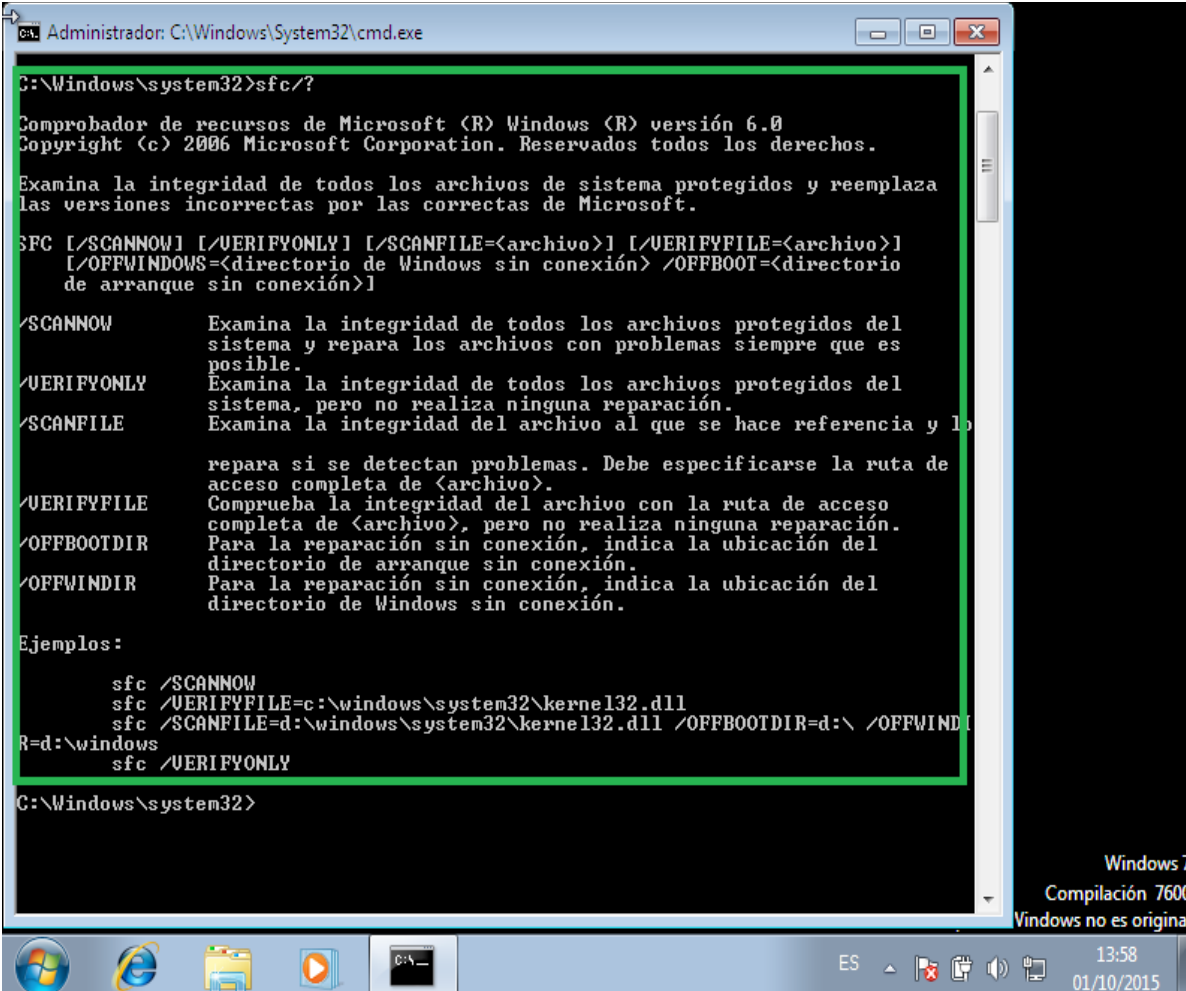
La herramienta SFC (System File Checker), es una utilidad de los sistemas Windows, la cual comprueba la integridad de los archivos de sistema.

SFC examina la integridad de todos los archivos de sistema protegidos, reemplazando si es posible los que estén corruptos o dañados por versiones correctas, si es posible.

Si se encontrara algún archivo dañado, podría darse el caso que se nos pidiera el disco de instalación de Windows, para poder repararlo. En caso de que la herramienta no pudiera reparar algún fichero, esta nos avisaría mediante un mensaje diciendo que no puede reparar algunos archivos. Podremos averiguar de que archivos se tratan accediendo al archivo log que se genera después de que ejecute SFC, el cual se guardará en C:\Windows\Logs\CBS\CBS.log

1.1.- Opciones de SFC

En la siguiente captura podemos ver de que opciones consta esta utilidad;



```
Administrador: C:\Windows\System32\cmd.exe

C:\Windows\system32>sfc/?

Comprobador de recursos de Microsoft (R) Windows (R) versión 6.0
Copyright (c) 2006 Microsoft Corporation. Reservados todos los derechos.

Examina la integridad de todos los archivos de sistema protegidos y reemplaza
las versiones incorrectas por las correctas de Microsoft.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<archivo>] [/VERIFYFILE=<archivo>]
[/OFFWINDOWS=<directorio de Windows sin conexión> /OFFBOOT=<directorio
de arranque sin conexión>]

/SCANNOW          Examina la integridad de todos los archivos protegidos del
                  sistema y repara los archivos con problemas siempre que es
                  posible.
/VERIFYONLY       Examina la integridad de todos los archivos protegidos del
                  sistema, pero no realiza ninguna reparación.
/SCANFILE         Examina la integridad del archivo al que se hace referencia y lo
                  repara si se detectan problemas. Debe especificarse la ruta de
                  acceso completa de <archivo>.
/VERIFYFILE       Comprueba la integridad del archivo con la ruta de acceso
                  completa de <archivo>, pero no realiza ninguna reparación.
/OFFBOOTDIR       Para la reparación sin conexión, indica la ubicación del
                  directorio de arranque sin conexión.
/OFFWINDIR        Para la reparación sin conexión, indica la ubicación del
                  directorio de Windows sin conexión.

Ejemplos:

    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>
```

Windows 7
Compilación 7600
Windows no es original

ES 13:58
01/10/2015

Como podemos ver en la captura anterior, la sintaxis de esta orden sería: `X:\> SFC [/OPCION]`

Tal y como se ve en la captura, las opciones de las que disponemos para esta utilidad son:

`/SCANNOW`: Examina la integridad de todos los archivos protegidos del sistema realizando reparaciones.

`/VERIFYONLY`: Igual que el anterior pero sin realizar reparaciones.

/SCANFILE: Examina la integridad del archivo que le indiquemos.

/VERIFYFILE: Comprueba la integridad del archivo con la ruta de acceso, pero no realiza ninguna reparación.

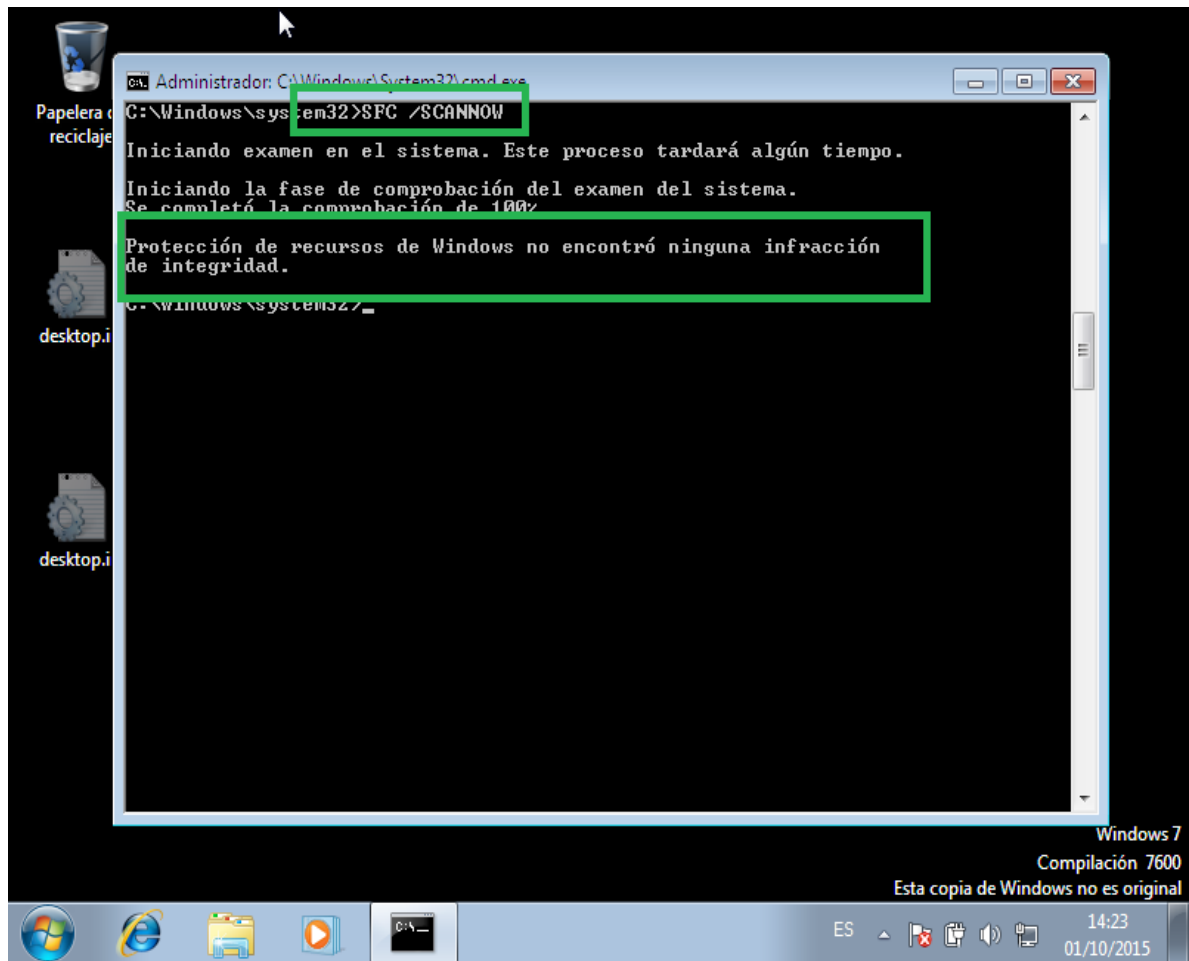
/OFFBOOTDIR: Para la reparación sin conexión, indica la ubicación del directorio de arranque sin conexión.

/OFFWINDIR: Para la reparación sin conexión, indica la ubicación del directorio de Windows sin conexión.

1.2.- Funcionamiento

1.2.1.- /SCANNOW

Para comprobar su funcionamiento, ejecutamos la herramienta SFC junto la opción /SCANNOW:



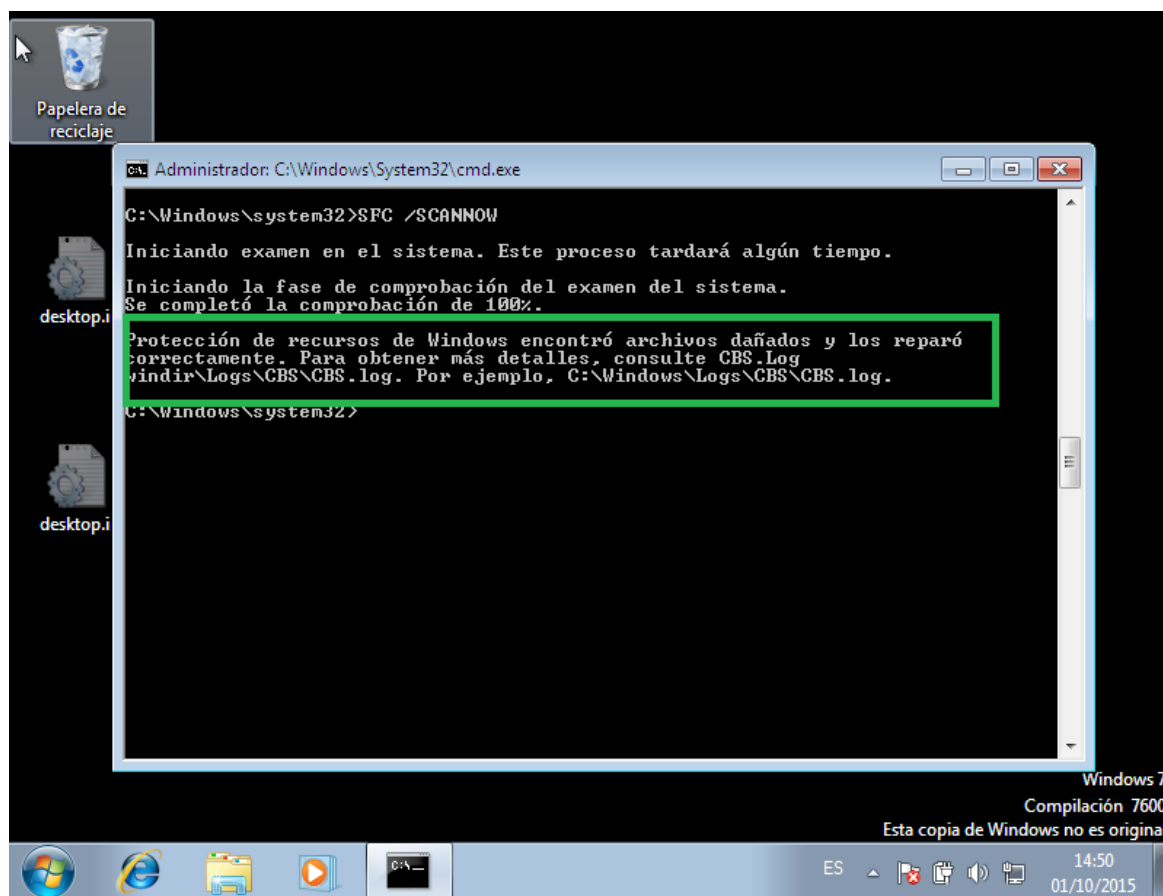
Como se puede apreciar en la captura, todo ha sido correcto. En el siguiente paso provocaremos un error a propósito para comprobar su funcionamiento ante errores.

1.2.2.- /SCANNOW con error.

Lo primero que deberemos hacer, será cambiar los permisos de la carpeta Windows/System32 de forma que nuestro usuario tenga control total sobre ella.

Una vez cambiado los permisos borramos un archivo del sistema, de forma que al ejecutar el SFC /SCANNOW nos detecte un error y tenga que repararlo.

Una vez ejecutado vemos como ha encontrado errores y los ha reparado:



1.2.3.- Archivo CBS.log

Una vez que esta herramienta ha concluido su trabajo, nos muestra el mensaje de que se encontraron archivos dañados y los reparó correctamente, pero no nos muestra los archivos dañados y reparados.

Para poder comprobar que archivos encontró dañados y cuales reparó, deberemos consultar el archivo CBS.log, el cual se encuentra en C:\Windows\Logs\CBS\CBS.log (esta ruta está indicada en la captura del punto anterior).

2.- Descripción de la herramienta RKHUNTER.

La herramienta rkhunter (Rootkit Hunter), vendría a ser el equivalente a SFC de Windows en Linux, pero más completa que entre otras tareas examina los permisos de los ejecutables del sistema, busca rootkits conocidos rastreando ficheros ocultos, realizar la comprobación de integridad de los archivos de sistema, es decir, verificar que no han sido modificados.

2.1.- Instalar rkhunter.

A diferencia del SFC de Windows, el rkhunter de Linux no viene instalado, por lo que lo primero que deberemos hacer es descargar e instalar la herramienta con la orden `sudo pacman -S rkhunter`:

```
[admin@ArchLinux-UM ~]$ sudo pacman -S rkhunter
resolving dependencies...
looking for conflicting packages...

Packages (2) wget-1.16.3-1 rkhunter-1.4.2-1

Total Download Size:   0.67 MiB
Total Installed Size:  3.39 MiB

:: Proceed with installation? [Y/n] y
:: Retrieving packages ...
  wget-1.16.3-1-x86_64      479.6 KiB   207K/s 00:02 [#####] 100%
  rkhunter-1.4.2-1-any     205.9 KiB   182K/s 00:01 [#####] 100%
(2/2) checking keys in keyring [#####] 100%
(2/2) checking package integrity [#####] 100%
(2/2) loading package files [#####] 100%
(2/2) checking for file conflicts [#####] 100%
(2/2) checking available disk space [#####] 100%
(1/2) installing wget [#####] 100%
Optional dependencies for wget
  ca-certificates: HTTPS downloads [installed]
(2/2) installing rkhunter [#####] 100%
Optional dependencies for rkhunter
  unhide
[admin@ArchLinux-UM ~]$ sudo pacman -S rkhunter_
```

2.2.- Funciones de rkhunter

2.2.1.- Opción chekall

Esta herramienta dispone de muchas opciones, para hacer ejecutarlo sobre el sistema, verificándolas todas, usaremos la opción checkall.

En la siguiente captura, usando el comando `sudo rkhunter -h`, vemos unas cuantas opciones de las que dispone esta herramienta.

```
[admin@ArchLinux-UM ~]$ sudo rkhunter -h
Usage: rkhunter [--check | --unlock | --update | --versioncheck |
               --propupd [{filename | directory | package name},...] |
               --list [{tests | {lang | languages} | rootkits | perl | propfil
es}] |
               --config-check | --version | --help] [options]

Current options are:
    --append-log           Append to the logfile, do not overwrite
    --bindir <directory>... Use the specified command directories
    -c, --check            Check the local system
    -C, --config-check     Check the configuration file(s), then exit
    --cs2, --color-set2    Use the second color set for output
    --configfile <file>    Use the specified configuration file
    --cronjob              Run as a cron job
                           (implies -c, --sk and --nocolors options)
    --dbdir <directory>    Use the specified database directory
    --debug                Debug mode
                           (Do not use unless asked to do so)
    --disable <test>[,<test>...] Disable specific tests
                           (Default is to disable no tests)
    --display-logfile      Display the logfile at the end
    --enable <test>[,<test>...] Enable specific tests
```

En las siguientes capturas ya hemos ejecutado el comando `sudo rkhunter -checkall`;

```
Invalid option specified: -checkall
[admin@ArchLinux-UM ~]$ sudo rkhunter --checkall
[ Rootkit Hunter version 1.4.2 ]

Checking system commands...

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

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                                [ Warning ]
    /usr/bin/awk                                           [ OK ]
    /usr/bin/basename                                     [ OK ]
    /usr/bin/bash                                          [ OK ]
    /usr/bin/cat                                           [ OK ]
    /usr/bin/chattr                                        [ OK ]
    /usr/bin/chmod                                         [ OK ]
    /usr/bin/chown                                         [ OK ]
    /usr/bin/chroot                                        [ OK ]
^C[admin@ArchLinux-UM ~]$ _
```

Al ejecutar esta opción, iremos viendo que se van comprobando entre otros aspectos, cadenas y atributos de los comandos o ejecutables del sistema, la existencia de archivos rootkits, etc.

```
System checks summary
=====
File properties checks...
  Required commands check failed
  Files checked: 113
  Suspect files: 3

Rootkit checks...
  Rootkits checked : 194
  Possible rootkits: 0

Applications checks...
  Applications checked: 2
  Suspect applications: 0

The system checks took: 2 minutes and 31 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)

[admin@ArchLinux-UM ~]$ _
```

Una vez que se ha terminado el chequeo, se nos mostrará una pantalla como la que se ve en la captura de pantalla donde nos muestra un resumen de todas las comprobaciones que se han realizado.

En esta misma pantalla nos indicará que se ha creado un archivo `.log`, el cual podremos visualizar usando la orden `sudo cat /ruta del archivo`.

En el caso de este ejemplo sería `sudo cat /var/log/rkhunter.log`

```
[17:40:10] Info: Applications checked: 2 out of 9
[17:40:10]
[17:40:10] System checks summary
[17:40:10] =====
[17:40:10]
[17:40:10] File properties checks...
[17:40:11] Required commands check failed
[17:40:11] Files checked: 113
[17:40:11] Suspect files: 3
[17:40:11]
[17:40:11] Rootkit checks...
[17:40:11] Rootkits checked : 194
[17:40:11] Possible rootkits: 0
[17:40:11]
[17:40:11] Applications checks...
[17:40:11] Applications checked: 2
[17:40:11] Suspect applications: 0
[17:40:11]
[17:40:11] The system checks took: 2 minutes and 31 seconds
[17:40:11]
[17:40:11] Info: End date is Tue Oct  6 17:40:11 CEST 2015
[admin@ArchLinux-UM ~]$
[admin@ArchLinux-UM ~]$
[admin@ArchLinux-UM ~]$
[admin@ArchLinux-UM ~]$
```

*Aquí vemos el final del archivo `.log` que se ha creado.

2.2.2.- Opción checkall con error

En esta parte lo primero utilizaremos otra de las opciones de rkhunter, la `--propupd`. Esta se basa en crear una base de datos con huellas MD5 de los ficheros clave del sistema. Y para detectar modificaciones de los ficheros, en chequeos posteriores los compara con los de la base de datos. La opción que genera la base de datos inicialmente es `--propupd`.

```
[admin@ArchLinux-VM bin]$ sudo rkhunter --propupd  
[ Rootkit Hunter version 1.4.2 ]  
File updated: searched for 171 files, found 113  
[admin@ArchLinux-VM bin]$ _
```

Una vez creada la base de datos, modificaremos un archivo del sistema y ejecutaremos la herramienta rkhunter con la opción `checkall`, de esta forma se compara la base de datos creada anteriormente con lo actual.

Practica 1.3 Disponibilidad

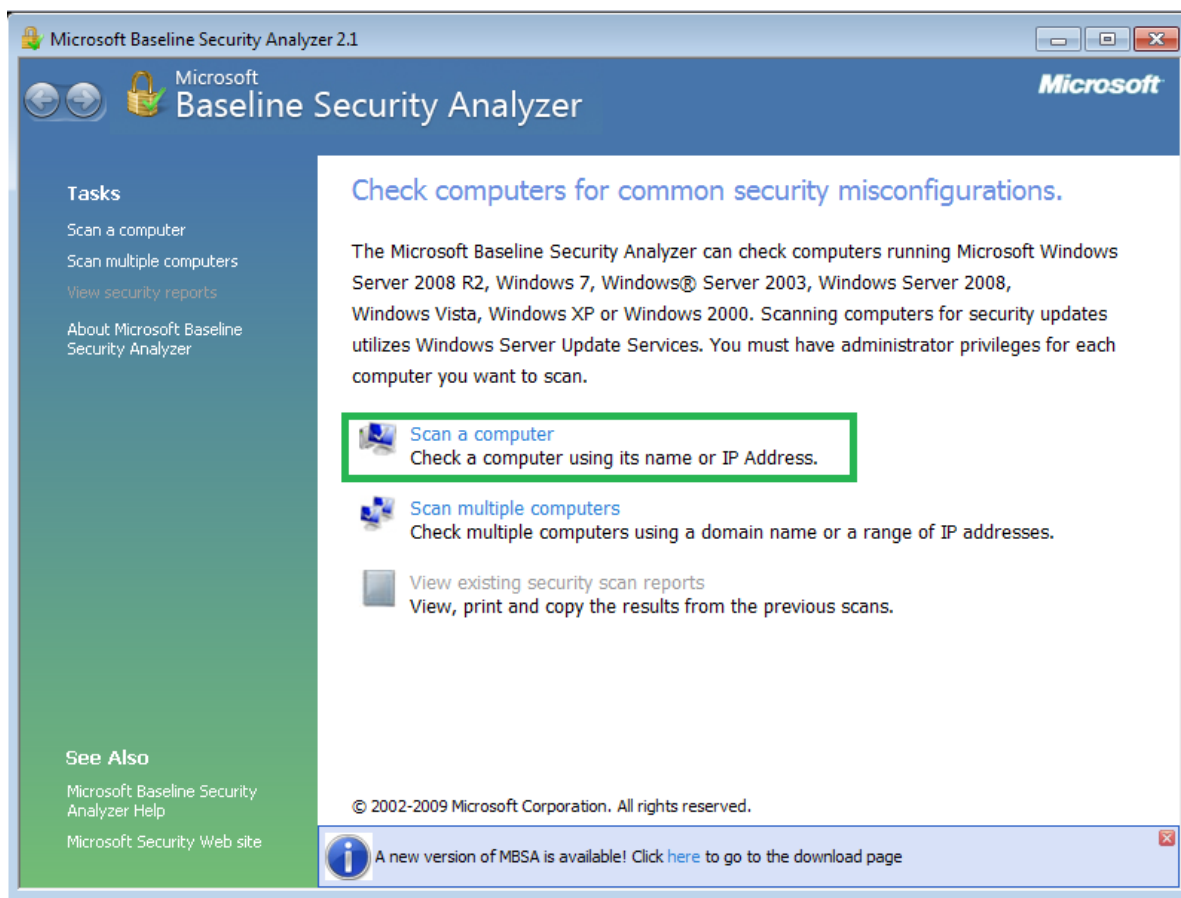
Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) es una herramienta fácil de usar diseñada para los profesionales de TI que ayuda a las pequeñas y medianas empresas a determinar su estado de seguridad según las recomendaciones de seguridad de Microsoft y ofrece orientación de soluciones específicas. MBSA detecta los errores más comunes de configuración de seguridad y actualizaciones de seguridad que faltan en los sistemas informáticos.

Se analizan elementos como:

- Actualizaciones del sistema
- Contraseñas de cuentas de usuario
- Firewall de windows
- Sistema de archivos
- Autologon
- Número de cuentas de administrador
- Versión de windows
- Configuración de Internet Explorer

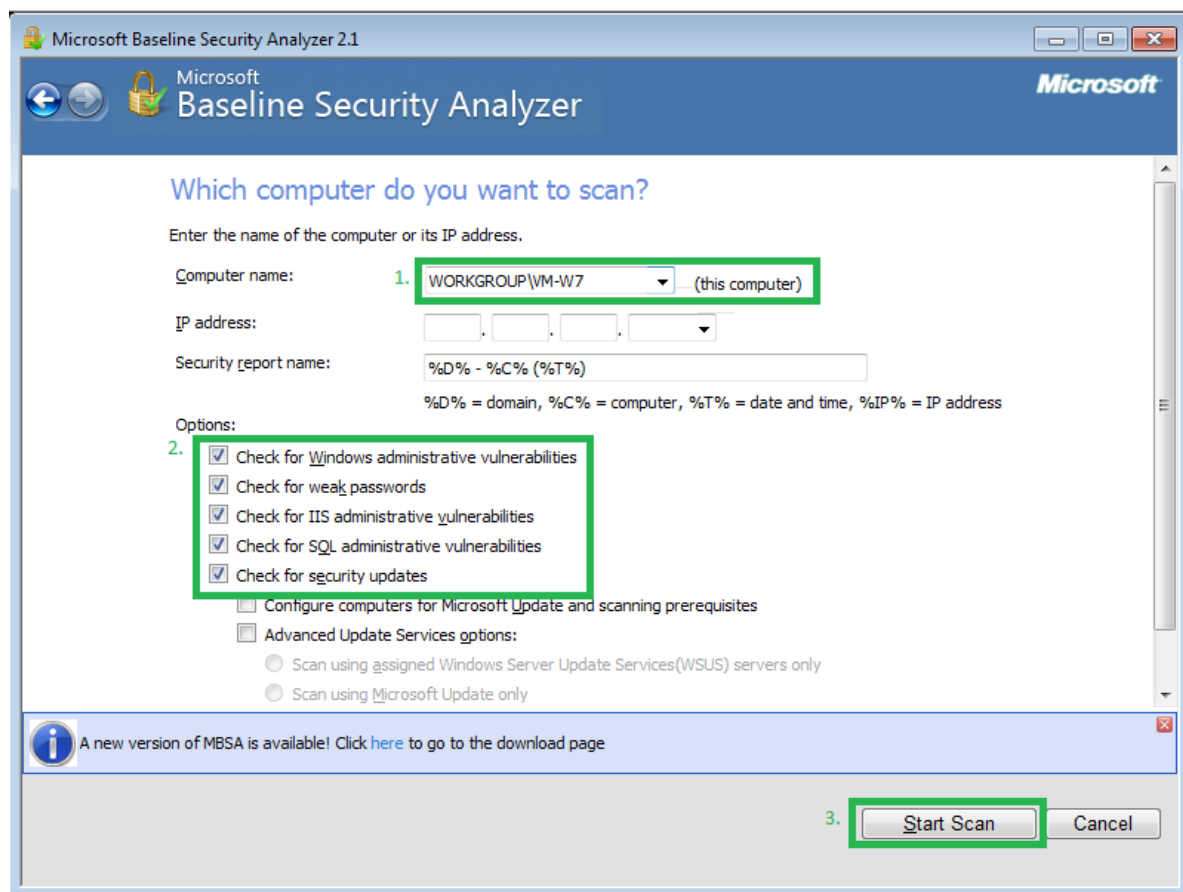
Realizaremos una comprobación para ver unos posibles resultados del test.



Iniciamos el programa y seleccionamos la opción "Scan a computer"

Si estuviéramos administrando varios equipos conectados en una misma LAN podríamos seleccionar la opción "Scan multiple computers", y dando las IPs de esos equipos, los analizaría.

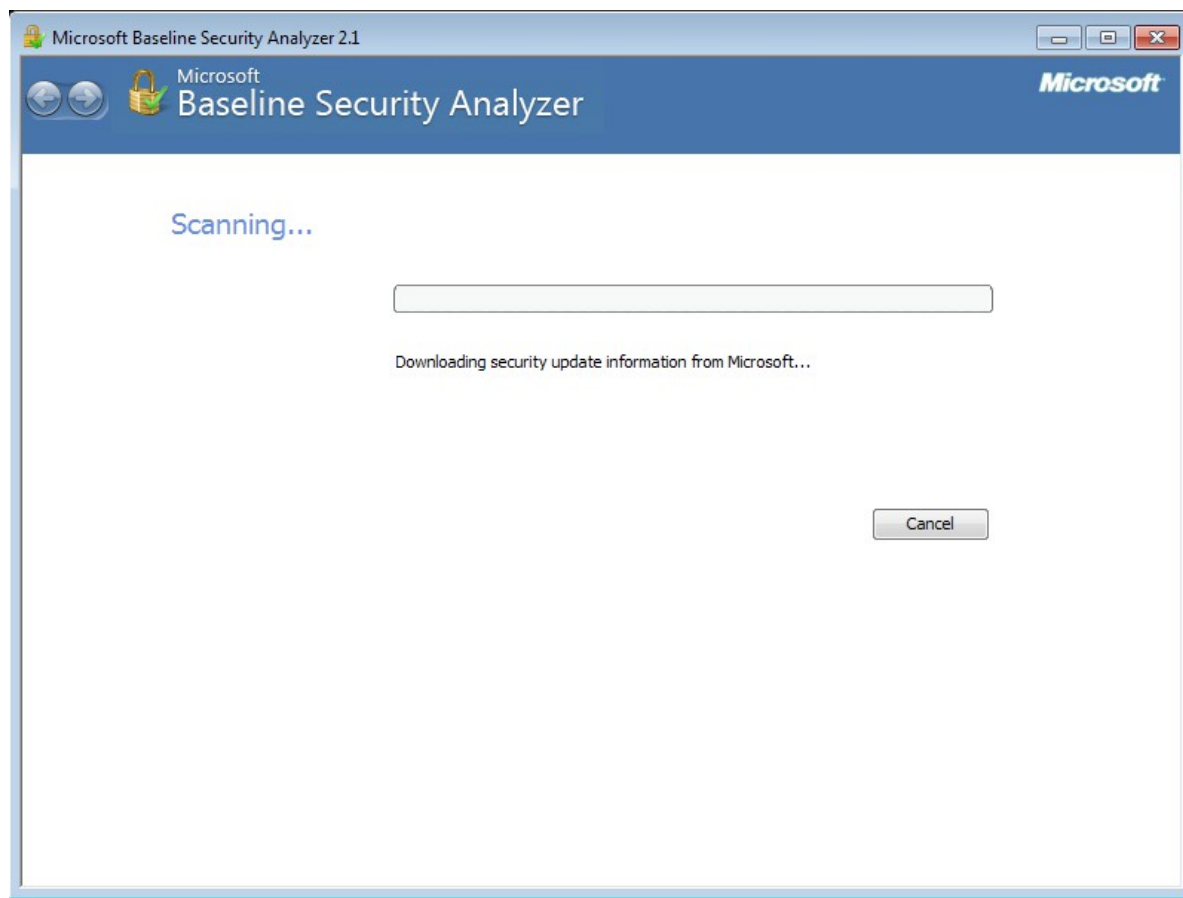
Desde esta misma pantalla, también podríamos acceder a los resultados de previas ejecuciones, o ver los archivos de ayuda referentes a esta herramienta.



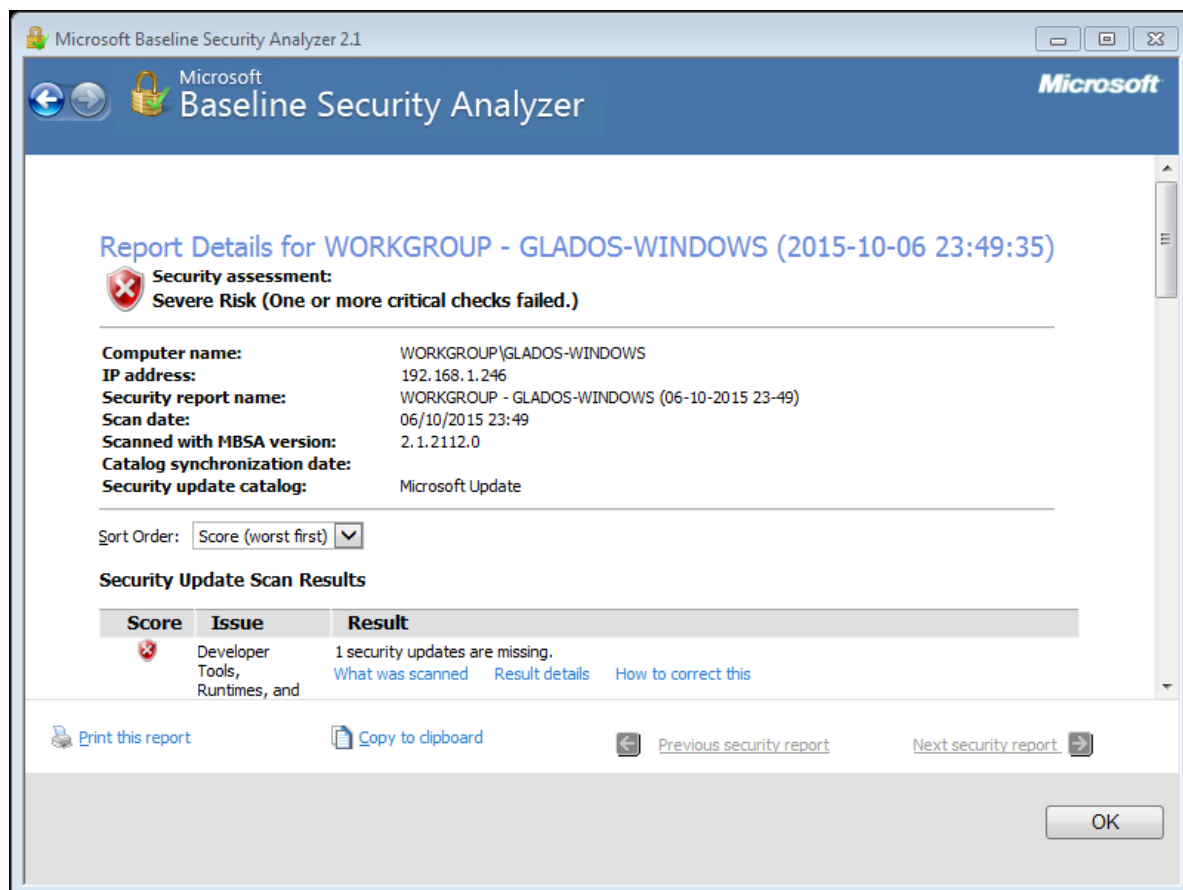
Aquí configuraremos el escaneo:

1. Seleccionaremos el equipo en la lista. Por defecto será el equipo en el que se está ejecutando el programa.
2. Seleccionaremos que escanear. Las opciones por defecto dan como resultado un escaneo profundo. Las opciones extra prepararía los ordenadores para Microsoft Update o usaría opciones avanzadas para la selección del servidor de Microsoft Update.
3. Iniciamos el escaneo.

Dentro de este paso, también podríamos seleccionar un equipo a partir de su IP, y cambiar el nombre del reporte generado.



Se inicia el escaneado. Puede tardar un poco y parecer que no avanza, lo cual puede dar pié a confusiones. Ver "Problemas encontrados" para más información.



Una vez el escaneado ha finalizado, nos sale una página con toda la información. Destacaré los puntos que la herramienta ha encontrado críticos en el ejemplo:

- Una actualización de seguridad no estaba instalada.
- Hay cuentas de usuario con contraseñas débiles o nulas.
- Hay actualizaciones cuya instalación no se ha completado.
- Hay cuentas con contraseñas que no expiran.

Práctica 1.4 Alta disponibilidad

Calcular la disponibilidad del 99'99%(4 nueves) y la del 99'9%(3 nueves).

Haremos dos cambios de conversión para cada porcentaje.

1.- 99'99%

Pasamos 1 año a días y así sacamos los minutos que tiene un año. Después lo multiplicamos por **0,01%**(0,01/100) y nos da 52,56 que son los minutos al año.

$$365 \text{ días} \times \frac{24 \text{ horas}}{1 \text{ día}} \times \frac{60 \text{ min}}{1 \text{ hora}} \times 0,01/100 = 52,356 \text{ min/año}$$

Para sacar los minutos al mes dividimos los 52,56 entre 12 meses y nos queda 4,38 minutos al mes.

$$52,56 \text{ min/año} \times \frac{1 \text{ año}}{12 \text{ mese}} = 4,38 \text{ min/mes}$$

2.- 99'9%

Pasamos 1 año a días y así sacamos los minutos que tiene un año. Después lo multiplicamos por **0,1%**(0,1/100) y nos da 525,6 que son los minutos al año.

$$365 \text{ días} \times \frac{24 \text{ horas}}{1 \text{ día}} \times \frac{60 \text{ min}}{1 \text{ hora}} \times 0,1/100 = 525,6 \text{ min/año}$$

Para sacar los minutos al mes dividimos los 525,6 entre 12 meses y nos queda 43,8 minutos al mes.

$$525,6 \text{ min/año} \times \frac{1 \text{ año}}{12 \text{ mese}} = 43,8 \text{ min/mes}$$

Tras los cálculos la tabla queda de la siguiente manera:

Disponibilidad de ...		Acepta inactividad de ...	
5 nueves	99,999%	0.44 min/mes	5.26 min/año
4 nueves	99,99%	4.38 min/mes	52.56 min/año
3 nueves	99,9%	43.8 min/mes	525.6 min/año

Problemas encontrados

Practica 1.1

Ningún problemas más que el de manejar el ArchLinux sin entorno gráfico pero ha sido una buena forma para revisar comando yo lo recomendaría siempre.

Practica 1.2

A la hora de hacer la práctica 1.2, el apartado de provocar una fallo de integridad en linux, para probar la herramienta rkhunter, no hemos encontrado mucha información de como realizar un fallo de integridad.

Practica 1.3

En la herramienta MBSA, el proceso de análisis pasó por una fase de descarga desde windows update. Esta fase parecía no avanzar, haciendome pensar en un fallo de la máquina virtual. Para solucionarlo ejecute la herramienta fuera del entorno de virtualización, y pude ver que la tardanza no era exclusiva de dicho entorno. Sin embargo, puesto que el escaneado se hizo con éxito, decidí usar esos resultados para el ejemplo, en lugar de volver a hacer el análisis en la máquina virtual.

Practica 1.4

No ha habido ningún problemas mas que dar con la forma de conseguir los numero.

Opinión personal

Hatim Amtil Ouahdi

Ha sido una practica muy sencilla pero con muchos pasos a realizar. Las dos formas de encriptado y las verificaciones han hecho el trabajo algo largo pero entretenido de hacer.

Daniel Rosselló Sánchez

La seguridad de un Sistema Operativo es algo fundamental, por lo que conocer y saber usar las distintas opciones que nos ha enseñado esta práctica nos serán de gran ayuda en un futuro.

Alex Piqueras Sastre

Es interesante conocer los conceptos introducidos para poder configurar sistemas más seguros. Las herramientas vistas pueden ser de gran utilidad en un futuro, tanto profesionalmente como personalmente

Bibliografía

Libro de Seguridad y alta disponibilidad.