

Estrategias y Trucos Basicos

Tabla de Contenidos

3. Estrategias y trucos básicos.....	2
3.1 Algunas consideraciones de seguridad en nuestro sistema Windows.....	2
Por qué encriptar carpetas y archivos.....	5
Securizando el fichero de paginación.....	5
Permitiendo a otros usuarios usar nuestro ficheros encriptados.....	5
Uso del comando CIPHER.....	6
Creando un agente de recuperación.....	7
Generando un certificado de agente de recuperación.....	7
Designando agentes de recuperación de datos.....	8
Cómo ver la lista de programas que tienen puertos tcp/ip abiertos (en escucha) y el programa que los usa.....	8
3.2 Copias de seguridad: pasos a seguir.....	10
1º. Disquetes:.....	11
2º. Partición dedicada / 2º. disco duro:.....	11
3º. Otro ordenador:.....	11
4º. Unidades de cinta:.....	12
5º. Sistemas removibles clásicos:.....	12
6º. Grabadoras de CD-R:.....	12
7º. Regrabadoras CD-R/CD-RW.....	12
3.3 Inhabilitación de servicios.....	14
Puertos - ¿Que son los puertos?.....	14



3. Estrategias y trucos básicos.

3.1 Algunas Consideraciones De Seguridad En Nuestro Sistema Windows.

Prácticamente todos los scripts malignos que se intentan ejecutar en nuestra máquina, bien por agujeros del IE, o bien por explotación remota por fallos de seguridad de un servicio como el RPC, lo que intentan es ejecutar código con dos programas que siempre existen en nuestra máquina: cmd.exe y net.exe.

Con el cmd.exe (la consola de comandos) es evidente que se puede hacer todo. Es mucho más potente que el entorno gráfico de Windows. Desde una consola de comandos se puede hacer TODO (bueno... y malo).

Recordemos igualmente que un script maligno, nunca puede invocarlo indirectamente: el "path" del sistema no existe normalmente al entrar con atributos de system, o bien aunque entre con los de usuario, no se ejecutan las tareas de logon para esa ejecución. Es decir, a esos scripts malignos no les queda más remedio que invocar directamente al cmd de la forma `c:\Windows\system32\cmd.exe`, ya que si no, no arrancarían la consola. Es decir.... tienen que ir "dirigidos" al path completo `c:\Windows\system32`.

Según eso..... la idea es fácil: si tuviésemos Windows instalado en otra letra de disco estaríamos protegidos contra esto ¿no?. Pues efectivamente !!! Únicamente algún script intenta un par de veces: `c:\Windows\system32` y `d:\Windows\system32`. No prueban con otras letras.... simplemente porque les es costoso y porque la gente no instala Windows en otras letras.

De aquí el primer consejo: no instalar en `c:\` (si esto fuese posible).

Si no fuese posible, todavía podemos hacer una cosa: lo primero que se nos ocurre, sería borrar el cmd.exe y el net.exe y llevarlo a alguna otra carpeta. Poner esa carpeta en el path del sistema para que nosotros sí que pudiésemos ejecutarlos, y ya está.

Pues bien, la idea no está mal... pero no funciona. Simplemente porque Windows XP tiene un mecanismo: el WFP (Windows File Protection) que, en cuanto vea que hemos borrado esos archivos de `\Windows\system32`, los recuperaría instantáneamente.

Pero... para todo hay solución. Veamos: lo primero es correcto: las copiamos a otra carpeta y la ponemos en el path (la primera del path: con botón derecho sobre Mi PC, propiedades, avanzado y variables de entorno modificamos el path del sistema añadiendo dicha carpeta al principio). Y ahora, jugamos un poco con las propiedades del NTFS, es

decir con botón derecho en ambos archivos, propiedades, pestaña de seguridad, "negamos" todos los permisos a todos los usuarios incluidos los administradores... a todos los usuarios que allí veamos, les negamos permisos de TODO. Con esto, nadie podrá ejecutar desde allí.

Y ahora como segundo TIP de seguridad, debido a que también muchos scripts se ejecutan desde los temporales de Internet, y estos tienen que ser invocados exactamente igual, es decir por "ruta" completa y exacta... pues sencillo: nos creamos una carpeta nueva, y en las propiedades de Internet (botón derecho sobre el IE, propiedades) cambiamos la localización de los temporales de Internet a dicha carpeta. Los scripts que nos hayan inyectado navegando se volverán locos... y no funcionarán.

Encriptación De Ficheros En Windows XP Profesional Y Windows 2000

Las organizaciones, e incluso los usuarios domésticos, son conscientes de que los datos sensibles no deben estar disponibles para otros usuarios.

Windows XP Profesional nos da una alternativa para poder proteger estos datos y prevenir su pérdida. El "Encrypting File System" (EFS) es el encargado de codificar los ficheros. Estos ficheros sólo se pueden leer cuando el usuario que los ha creado hace "logon" en su máquina (con lo cual, presumiblemente, nuestra password será una password robusta). De hecho, cualquiera que acceda a nuestra máquina, no tendrá nunca acceso a nuestros ficheros encriptados aunque sea un Administrador del equipo.

La encriptación es el proceso de codificar datos sensibles usando un algoritmo. Sin la clave del algoritmo correcta los datos no pueden ser descryptados. Windows XP usa encriptación para varios propósitos:

- Ficheros encriptados en un volumen NTFS.
- Datos encriptados enviados entre un cliente web y un servidor usando Security Socket Layer (SSL).
- Encriptando tráfico entre ordenadores usando VPN.
- Encriptando o firmando mensajes de email.



Precauciones Que Debemos Tener Con EFS

EFS nos da una encriptación segura de la información. La encriptación es tan segura, que si perdemos la clave para desencriptar los datos, la información. estará irremediablemente perdida. Windows XP no tiene una "puerta trasera" si la clave se pierde.

Inocentemente podemos perder la clave por varios motivos:

- Por ejemplo, manipulando en la caja de dialogo de Certificados o en la consola de Certificados (certmgr.msc) podemos sin querer, borrar el certificado de encriptación.
- Podemos tener, por ejemplo, los datos almacenados en carpetas encriptadas en un segundo volumen (disco D:, por ejemplo). E imaginemos que decidimos por problemas reinstalar Windows. Formateamos C:\ e instalamos. Por desgracia, en cada instalación de Windows, aunque los nombre y claves de usuario sean las mismas, Windows crea un nuevo identificador de seguridad (SID) para cada usuario. Por tanto, las claves de encriptación y el certificado de seguridad, serán diferentes al ser nuevo el SID del usuario. En este caso, o tenemos copia de los certificados anteriores, o habremos perdido también irremediablemente la información. encriptada en nuestro segundo disco duro (D:).

Con un poco de cuidado, estos escenarios tan dramáticos pueden prevenirse. Para ello, sigamos los siguientes pasos (por primera vez):

1. Creamos una carpeta vacía, y le colocamos los atributos de encriptada.
2. Creamos o guardamos cualquier fichero de texto en dicha carpeta. Esto encriptará un archivo por primera vez.
3. Si nuestra máquina no es parte de un Dominio, creamos un agente de recuperación. Una segunda cuenta de usuario podrá ser usada con este agente para desencriptar los ficheros. Veremos más adelante como crear este agente de recuperación.
4. Guardamos el certificado de agente de recuperación. y el certificado personal de encriptación (en un disquete, por ejemplo y a salvo de terceras personas). Este último certificado no se creará hasta que hayamos realizado la primera encriptación, por ello es por lo que hemos realizado, por primera y única vez, los pasos 1) y 2).
5. Ahora ya podemos empezar a encriptar los datos sensibles.



Por qué encriptar carpetas y archivos

EFS permite encriptar archivos en un volumen NTFS local (insisto: "local". No es aplicable a volúmenes en red). Esto ofrece un nivel de protección adicional a los permisos NTFS. Recordemos que los volúmenes NTFS pueden ser vulnerables por muchas vías: por ejemplo, instalando otro Windows XP en otra partición y tomando posesión de la partición primitiva, o bien arrancando con utilidades como NTFSDOS. En estos casos, si alguien tiene acceso físico a nuestra máquina, podría llevarse información confidencial. Este es uno de los motivos por los que se hace imprescindible, sobre todo en equipos portátiles de empresa, el tener encriptada la información sensible. Ante robo o pérdida, los datos serán irrecuperables.

En algunas máquinas, podemos usar opciones de la Bios para proteger el inicio del ordenador con password. Desafortunadamente, este tipo de protección también puede ser reventada, por ejemplo quitando el disco duro y montándolo en otro equipo. Si los datos no están encriptados, se podrá tomar posesión de las carpetas y serán accesibles a un malintencionado usuario.

Securizando el fichero de paginación

Si existe la posibilidad de que nuestro ordenador caiga en manos extrañas, debemos tener la seguridad de que no estamos dejando "pistas" en el fichero de paginación. Por defecto, cuando apagamos la máquina, el fichero de paginación permanece intacto. Quien pueda tener acceso físico a nuestro disco duro, podría echar una mirada a un fichero de paginación sin encriptar para intentar localizar restos de información sensible.

Si no queremos que esto suceda, podemos cambiar una entrada del registro. En la clave:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\MemoryManagement

podemos colocar el valor 1, en la variable ClearPageFileAtShutdown.

De esta manera, al cerrar la máquina, Windows sobrescribirá las páginas usadas en el archivo de paginación con ceros binarios. Esto hace que el shutdown del sistema sea bastante más lento, por tanto, no debemos realizar este cambio a no ser que las necesidades de seguridad lo hagan necesario.

Permitiendo a otros usuarios usar nuestros ficheros encriptados

Después de encriptar un fichero, podemos permitir a otros usuarios el acceder a dicho fichero transparentemente. Esta capacidad, nueva en XP, nos permite asegurar un fichero con EFS y dejarlo disponible a los usuarios que deseemos. Los usuarios que especifiquemos pueden ser usuarios que acceden desde la misma máquina, o bien usuarios que acceden desde la red. Para activar que otros usuarios puedan acceder a nuestros ficheros encriptados:

1. Botón derecho sobre el fichero encriptado y "Propiedades". En la pestaña "General" seleccionamos "Avanzado".
2. En Atributos Avanzados, pinchamos "Detalles".
NOTA: El botón de "detalles" está indisponible cuando inicialmente encriptamos un fichero. Debemos encriptar el fichero, salirnos, y volver posteriormente al dialogo de Atributos Avanzados. Igualmente, el botón de "detalles" está disponible sólo cuando seleccionamos un único fichero. Si seleccionamos una carpeta o varios ficheros, el botón estará indisponible.
3. En la caja de diálogo de "Detalles" de encriptación, le damos al botón de Añadir. Aparecerá una caja de diálogo con los usuarios.
4. Seleccionamos a los usuarios a los que queremos permitir el acceso.
NOTA: Únicamente los usuarios que tengan ya un certificado EFS en nuestra máquina aparecerán en dicha caja de diálogo. La mejor manera para que un usuario de nuestra máquina cree un certificado (y por tanto aparezca en la lista), es que el usuario haga logon en la máquina y encripte un fichero cualquiera. Los usuarios de red, deben exportar su propio certificado (para más detalles, lo veremos más adelante); posteriormente debemos importar dicho certificado en nuestra máquina.

Uso del comando CIPHER

Si preferimos usar un comando en la línea de comandos de una consola, tenemos el comando cipher como alternativa a la caja de diálogo de Atributos Avanzados que hemos visto anteriormente, y que nos permite encriptar y desencriptar carpetas y archivos.

Si ejecutamos CIPHER sin parámetros, veremos el estado de la encriptación de la carpeta donde nos encontremos y sus archivos.

Para encriptar o desencriptar ficheros debemos incluir el path y los parámetros. Podemos usar el parámetro /E para encriptar archivos o carpetas, o /D para desencriptarlo. Por ejemplo, para encriptar la carpeta Mis Documentos y todas sus subcarpetas:

```
cipher /e /a /s:"%userprofile%\mis documentos"
```

En la especificación de los nombres de ficheros, podemos usar comodines. Igualmente podemos especificar múltiples carpetas o ficheros en una sola invocación desde la línea de comandos, separándolos simplemente con un espacio.

Los parámetros más habituales los describimos a continuación. Para ver una lista detallada de parámetros, ejecutar cipher /? en la línea de comandos.

- /E Encripta las carpetas que hayamos especificado.
- /D Desencripta las carpetas especificadas.
- /S:carpeta Realiza la operación en una carpeta y en sus subcarpetas (pero no en los ficheros).
- /A Realiza la operación en los ficheros especificados o bien en los ficheros de una determinada carpeta.
- /K Crea una nueva clave de encriptación. Si usamos esta opción, todas las demás opciones posibles de la línea de comandos serán ignoradas.
- /R Genera una clave de agente de recuperación y el certificado. La clave y el certificado son puestos en un archivo .pfx y el certificado solo, en un archivo .cer

Creando un agente de recuperación.

Un agente de recuperación es otro usuario, normalmente un Administrador, que puede usar nuestros archivos encriptados. Esto permite la recuperación de nuestro fichero encriptado si algo pasase con nuestra clave privada.

Windows XP no crea un agente de recuperación por defecto en máquinas "standalone". Si pertenecemos a un Dominio, el Administrador del Dominio es el agente de recuperación por defecto.

NOTA: Un agente de recuperación sólo puede recuperar archivos que han sido encriptados "después" de que el certificado de recuperación haya sido creado y se haya designado el agente de recuperación tal y como describiremos posteriormente. El agente no tendrá acceso, por tanto, a ficheros encriptados anteriormente.

Esto es debido a que cuando un fichero se encripta, EFS usa la clave pública de la cuenta que está encriptando el fichero y cada una de las de los agentes designados de recuperación. Por tanto, sólo los agentes de recuperación cuyos certificados estén instalados en el momento de la encriptación pueden desencriptar el fichero.

Para crear un agente de recuperación de datos debemos crear un certificado de recuperación de datos y designar a un usuario para que sea agente de recuperación.

Generando un certificado de agente de recuperación.

Para generar un certificado de agente de recuperación, debemos seguir los siguientes pasos:

1. Conectarnos como Administrador.
2. En una consola de comandos (cmd.exe) ejecutar: `cipher /r:nombrefichero`
3. Cuando nos pregunte, teclear una password que será usada para proteger los archivos que creemos.

Esto genera ambos: un fichero .pfx y un fichero .cer con el nombre de fichero que hemos especificado anteriormente.

NOTA: Estos ficheros permiten que cualquiera sea un agente de recuperación. Por tanto, debemos asegurarnos de

copiarlos a un disquete y colocarlo en un lugar seguro. Posteriormente debemos borrarlos de nuestro disco duro.

Designando agentes de recuperación de datos

Podemos designar a cualquier usuario como un agente de recuperación de datos. Se recomienda que sea una cuenta de un Administrador.

NOTA: No debemos designar a nuestra propia cuenta como agente de recuperación, ya que si nuestro perfil se daña, y no hay más agentes de recuperación, habremos perdido irremediablemente los datos.

Para designar un agente de recuperación.:

1. Conectarnos con la cuenta del usuario que queremos designar como agente de recuperación.
2. En certificados (ejecutando: certmgr.msc) ir a certificados, Usuario Actual\Personal.
3. En el menú Acción / Todas las tareas / Importar, lanzará el asistente de recuperación. Pulsar siguiente y aparecerá una página para importar el archivo.
4. Entramos el path y el nombre del fichero del certificado de encriptación (el fichero .pfx).
5. Entrar la password para este certificado (la tecleada anteriormente cuando ejecutamos el comando cipher) y seleccionamos "marcar esta clave como exportable". Pulsamos siguiente.
6. Seleccionamos: automáticamente seleccionar el certificado basado en el tipo de certificado y pulsamos siguiente. A continuación pulsamos finalizar.
7. En Local Security Settings (ejecutando: secpol.msc) vamos a Security Settings\Public Key Policies\Encrypting File System
8. Menu Acción / Añadir un agente de recuperación. Pulsamos siguiente.
9. En la página de seleccionar agente de recuperación, pulsamos el botón de Ver y navegamos a la carpeta que contiene el .cer que hemos creado. Seleccionamos el fichero y le damos "Abrir". Ahora nos mostrará el nuevo agente como USER_UNKNOWN. Esto es normal debido a que el nombre no está almacenado en el fichero.
10. Tecleamos siguiente y finalizamos.

Cómo ver la lista de programas que tienen puertos tcp/ip abiertos (en escucha) y el programa que los usa.

Ejecutar en una ventana de comandos (cmd.exe):

```
for /F "usebackq tokens=4,5" %i in (`netstat -ao ^| find "LISTENING"`) do @for /F "usebackq tokens=1,2" %k in (`tasklist`) do @if %j == %l @echo %j %k
```

NOTA: Sed cuidadosos al teclear esto, respetando los espacios en blanco.

Si queremos crearnos un .bat con la linea anterior, debereis sustituir cada % por %%. Es decir, nuestro .bat quedaría:

```
@echo off
```

```
for /F "usebackq tokens=4,5" %%i in (`netstat -ao ^| find "LISTENING"`) do @for /F "usebackq tokens=1,2" %%k in (`tasklist`) do @if %%j == %%l @echo %%j %%k
```

```
pause
```

Este comando no está optimizado en tiempo de ejecución ya que llama excesivas veces al programa tasklist: lo llama una vez por cada puerto abierto, pero funciona perfectamente y sirve para ver como ejemplo de la potencia del lenguaje de comandos.

Para mejorar su tiempo de respuesta nos podemos ahorrar estas llamadas, realizará una sola si el .bat lo hacemos así :

```
@echo off
```

```
tasklist > %temp%\tasklist.tmp
```

```
for /F "usebackq tokens=4,5" %i IN (`netstat -ao ^| find "LISTENING"`) do @for /F "usebackq tokens=1,2" %k in (%temp%\tasklist.tmp) do @if %j == %l @echo %j %k
```

```
del %temp%\tasklist.tmp >nul
```

```
pause
```

NOTA: Lo que está en la línea del "for".... es UNA sola línea.

Bien, la salida de ese comando para ver los procesos que estan en escucha en tcp/ip, muestra el número del proceso y el proceso que tiene abierto un puerto en escucha, pero no nos muestra el número de puerto que está abierto. Para ver el número de puerto y el proceso asociado, el comando es:

```
for /F "usebackq tokens=2,3,4,5,6,7 delims=: " %g in (`netstat -nao ^| find "LISTENING"`) do @for /F "usebackq skip=2 tokens=1,2" %m IN (`tasklist`) do @if %l == %n @echo %h %m
```

Y si queremos crearnos un .bat que lo haga:

```
@echo off
```

```
for /F "usebackq tokens=2,3,4,5,6,7 delims=: " %g in (`netstat -nao ^| find "LISTENING"`) do @for /F "usebackq skip=2 tokens=1,2" %m IN (`tasklist`) do @if %l == %n @echo %h %m
```

```
pause
```

NOTA: Lo que está en la línea for, es una SOLA línea.

3.2 Copias De Seguridad: Pasos A Seguir

Nuestros datos son el tesoro de nuestro esfuerzo con el ordenador y pueden perderse en segundos y de la manera más sencilla: un comando mal introducido, virus o un programa con un sistema de instalación defectuoso, o cualquier otra cosa que ni nos imaginamos siguiendo las Leyes de Murphy, que en informática funcionan tan bien.

Si somos ordenados a la hora de generar nuestros datos y los tenemos en un árbol de directorios de manera lógica, como en el ejemplo de la derecha, esto nos va a facilitar su posterior copia, también debemos tener en cuenta que sea cual sea el medio de almacenamiento que usemos: cintas de back-up, disquetes, CD-ROM, removibles, etc..., que puede fallar y por ello lo ideal es usar al menos dos a usar alternativamente, o sea, una vez uno y otra vez el otro. Por ejemplo, podemos tener un CD-RW para las semanas pares y otro para las impares.

Hay muchos métodos, aunque el último que voy a comentar es el mejor y de hecho el que uso:

Disquetes.

Partición dedicada.

Otro ordenador.

Unidad de cinta.

Sistemas removibles clásicos.

Grabación CD-Rs.

Regrabación en CD-RWs.



1°. Disquetes:

Es el método más tradicionalmente usado porque no hace falta ningún hardware adicional, sin embargo hoy presenta dos serios inconvenientes:

Soportes poco fiables: hasta tal punto que si vas a usar este método te recomendaría que usaras por lo menos 4 juegos de disquetes.

Capacidad ridícula para el tamaño de los ficheros de hoy en día: si nos dedicamos a la edición de video, de audio (incluso en MPEG-3), fotográfica, programación multimedia o incluso algo tan sencillo como sacar una copia de seguridad de los mensajes de nuestro correo, ya nos podemos estar olvidando de esta opción. Si no nos dedicamos a nada de esto también deberíamos pensar en otra opción pues aparte de lo engorroso de copias 10 míseros 'megas' a disquetes (y que salgan todos bien) ya hasta los ficheros ofimáticos tienen un tamaño respetable.

2°. Partición dedicada / 2°. disco duro:

Esta opción no es muy recomendable, sobre todo por si hay un ataque vírico, ya que estos 'simpáticos' programas se suelen cepillar la tabla de particiones o dejar el disco duro irrecuperable en su totalidad, pero si no tienes más hardware adicional que un gran disco duro esta es una opción que existe, y que aparte de las ya mencionadas plantea otros problemas:

Por muy grande que sea tu disco duro terminará llenándose y duplicando la información tardará la mitad en hacerlo.

No puedes compartir esos datos con nadie, salvo que los pases a disquetes o lo conectes con el equipo de un amigo mediante cables. De esta manera podrás pasar esos datos a un CD, por ejemplo. También puedes sacar el disco duro e instalarlo en el otro como esclavo pero si lo haces con asiduidad terminarás dándole un golpe y adiós disco duro.

La única razón de hacer esto sería para esos casos que nuestro sistema está tan mal que hay que formatear para seguir trabajando, así podríamos formatear la partición del sistema dejando intacta la de los datos. Eso sí si usáis el FDISK pensad muy bien lo que estáis haciendo.

3°. Otro ordenador:

En este caso si tenemos otro equipo podemos hacer uso de cables paralelo o serie cruzados o de tarjetas de red. Incluso se puede sacar imágenes de discos duros / particiones usando programas como Nero, Ghost o incluso comandos de linux como dd ó cat (esto último es algo más complicado).

También lo puedes conectar al equipo de un amigo que tenga grabadora de CDs.

4°. Unidades de cinta:

Muy usadas en empresas sobre todo en el pasado, hoy están en las catacumbas de los sistemas de back-up:

Lentitud desesperante debido sobre todo al sistema de acceso secuencial a la información, en lugar del aleatorio que usan el resto de dispositivos.

Medio poco estable, un poco menos que los disquetes.

5°. Sistemas removibles clásicos:

Aquí incluyo a discos duros removibles, unidades ZIP, Jazz, MO, SuperDisk, etc... que permiten usar unos disquetes de capacidad elevadísima.

Es un sistema de back-up bueno y rápido pero su mayor pega es el coste de los discos y sobre todo el coste por Mb ¡Puede llegar a salir entre 20 y 100 veces más caro que un CD-R!

Otra pega importante es que para poder transportar la información a otro equipo necesitamos que también tenga el mismo tipo de dispositivo lo que, en la mayoría de los casos, no será así por lo que tendremos que comprar equipos externos, ya sean SCSI (hace falta una tarjeta y son caros) o paralelo (si la paciencia es nuestra virtud).

Ahora hay unas unidades USB muy rápidas pero pueden no ser la solución si se va a compartir información con algún equipo sin USB, sólo MS-DOS o con versiones antiguas de Linux ó Windows sin soporte USB.

6°. Grabadoras de CD-R:

Este es un medio sencillo y muy económico de hacer copias de seguridad a un precio ridículo, si haces el cálculo por mega te van a salir décimas de céntimo de euro.

El mayor inconveniente es que cuando haces una copia de algo no lo puedes modificar, así se quedó, por lo que no es apropiado para cosas que se actualicen mucho, p.e.: los mensajes de tu cuenta de correo.

También cuesta llenar un CD-R de datos completo a no ser casos especiales como edición de video.

7°. Regrabadoras CD-R/CD-RW

Este es el medio ideal pues tiene las ventajas del anterior sin su único inconveniente, pues puedes usar también discos CD-RW, que se pueden modificar como si de un disquete de 500/650 Mb se tratara. Son discos 3 ó 4 veces más caros pero bueno si son cosas que se actualizan tendrás que usar CD-RW y si son cosas perennes a usar los CD-R.

¡Ah! Estos dos últimos sistemas, que por otro lado son los que la mayoría prefieren, tienen la pega de la

velocidad que se va subsanando con las nuevas tecnologías que aparecen y que hay que tener el equipo muy afinado y sin nada residente para no tener que tirar CD-Rs a la basura (lógicamente esto no es problema con los CD-RW). También es conveniente, si usamos Windows para grabar, defragmentar el disco duro con mayor asiduedad, lo ideal es hacerlo justo antes de grabar un CD-R.

Lo ideal es tener una regrabadora SCSI y un lector de CDs SCSI si tenemos que hacer copias de esos discos de nuestros datos para distribuirlos (imagine que hacemos una aplicación multimedia para repartirla entre los alumnos de un curso). Esta solución es sustancialmente más cara pero en algunos casos puede ser necesaria.

¿Y COMO COPIO EL CORREO?

Para hacer la copia de seguridad del Outlook Express debes copiar el contenido íntegro del directorio C:\WINDOWS\APPLICATION DATA (este programa no lo recomiendo por si los virus).



3.3 Inhabilitación De Servicios

Puertos - ¿Que son los puertos?

Nada más que tu PC se conecta a internet, éste pasa a ser un host más dentro de la Red, es decir, forma parte de toda la Red y como tal se tiene que comunicar con el resto. Para poder comunicarse, lo primero que necesita es tener una dirección electrónica para poder identificarse con los demás. Si haces una petición, por ejemplo de una página web, el servidor tiene que saber a quien se la envía. Esa dirección electrónica es la dirección IP, qué es un número de 4 grupos de cifras de la forma xxx.xxx.xxx.xxx). Pero eso no es suficiente, ya que en internet se pueden utilizar muchos y diversos servicios y es necesario poder diferenciarlos. La forma de "diferenciarlos" es mediante los puertos.

Imaginaros un edificio de oficinas, éste tiene una puerta de entrada al edificio (que en nuestro caso sería la IP) y muchas oficinas que dan servicios (que en nuestro caso serian los puertos). Eso nos lleva a que la dirección completa de una oficina viene dada por la dirección postal y el número de la oficina. En el caso de Internet viene dado por la dirección IP y por el número de puerto. Así por ejemplo, un servidor web escucha las peticiones que le hacen por el puerto 80, Un servidor FTP lo hace por el puerto 21, etc...

Es decir, los puertos son los puntos de enganche para cada conexión de red que realizamos. El protocolo TCP identifica los extremos de una conexión por las direcciones IP de los dos nodos implicados (servidor y cliente), y el número de los puertos de cada nodo..Existen mas de 65000 de puertos diferentes, usados para las conexiones de Red: Los siguientes enlaces son una relación de puertos y los servicios a los que corresponden

Listado de Puertos. Microsoft WIndows 2000

<http://seguridad.internautas.org/puertos.txt>

Listado de Puertos. RFC1700 (ingles)

<http://seguridad.internautas.org/rfc1700.txt>

Piensa por ejemplo en tu casa. Tiene una puerta de entrada que no la dejas siempre abierta. También tienes ventanas, a las que les pones cortinas para preservar tu intimidad. Incluso las puedes cerrar a cal y canto para que por allí no se cuele nadie. Pues lo mismo se aplica a tu PC cuando estás conectado a Internet.

Una medida básica de seguridad es conocer que puertos tenemos, cuales están abiertos, porque están abiertos, y de estos últimos los que no utilicemos o que sean fuente de un problema de seguridad. Ojo, antes he dicho cerrar puertos que no utilicemos, ya que es evidente que si cierras un puerto que si estas utilizando, ese servicio deja de

funcionar para todo el mundo, incluyéndote a ti.

Windows como tal no tiene demasiados puertos abiertos, por lo que va a ser fácil comprobar si un puerto que está abierto, debería estarlo o no. Esto último nos va a servir para comprobar la existencia de troyanos en nuestra maquina.

Listado de Puertos utilizados por Troyanos

<http://seguridad.internautas.org/Trojanports.txt>

Lo que si es MUY RECOMENDABLE, ya que es la mayor fuente de problemas y peligros para los que utiliceis el S.O de Windows, es cerrar el puerto numero 139 (netbios) de Windows, pero sólo para el protocolo TCP/IP, para entendernos mejor, la opción de compartir ficheros e impresoras de Windows. La razón es muy simple, si compartes... compartes ¿lo pillas? ;-) Ese hay que cerrarlo inmediatamente siguiendo los pasos explicados en el apartado de Puerto 139.

<http://seguridad.internautas.org/seguridad1.php>

Para saber que puertos tenemos abiertos en nuestro ordenador podemos utilizar un escaneador de Puertos. Para ello ponemos a vuestra disposición dos formas de hacerlo:

Instalando un Escaneador de puertos en tu PC

<http://seguridad.internautas.org/scan-puertos.php>

Escaneando tu ordenador online desde nuestro servidor

<http://seguridad.internautas.org/3C/es/scan-online.php>

Una vez que lo hayas hecho, tenemos que comprobar los que tenemos abiertos y disponernos a actuar en consecuencia. Para ello disponemos de dos formas de hacerlo:

Bloqueo de Puertos

<http://seguridad.internautas.org/bloqueo.php>

Instalar un Firewall (cortafuegos)

La diferencia entre ambas formas de actuar es que mientras el primero lo que hace es cerrar el paso a los puertos (que tengas abiertos) que quieras tener cerrados, el otro, el firewall, lo que hace es tenerlos todos cerrados y abrir solo aquellos que permitas. Es mucho más seguro éste último sistema, el firewall o cortafuegos, que el de

bloqueo, ya que solo permite el tráfico a/desde internet que tu aceptes.

Una ventaja añadida de los firewall es en cuanto a la respuesta que puede ofrecer ante un escaneo de puertos. Es decir, si un atacante escanea los puertos y nuestro PC le responde que un puerto existe, pero está cerrado, el atacante, como mínimo, ya sabe que estamos conectados. Lo mejor es que nuestro PC no responda de ninguna manera, es decir, como si estuviéramos desconectados de Internet o indicando la inexistencia de puertos. Esa técnica de ocultación es lo que se llama modo Stealth y se realiza a través de los firewall.

