Este documento no pretende ni tiene la finalidad de convertirse en manual de referencia. Este documento relata los aspectos básicos relacionados en el campo de la informática forense, explicando de una forma simple y concisa las herramientas utilizadas para la captura de evidencias. También explicará los aspectos técnicos relativos a la arquitectura de un sistema Windows. Probablemente esto ayudará al lector a comprender mejor cómo un sistema Windows recopila y almacena la información, ayudando también a entender la arquitectura del sistema.

Redactado por Silverhack el 08 de Agosto de 2006
Versión 0.1

General

Entorno Microsoft

Service Pack, HotFix. Qué es y para qué sirve?

Introducción y definición de análisis forense

En este tutorial, vamos a explicar de la forma más sencilla posible el uso de algunas herramientas que nos pueden facilitar la tarea a la hora de realizar un análisis forense en entornos Windows. Existen muchísimas herramientas destinadas a éste propósito, comerciales y gratuitas. En este tutorial vamos a ver como enfocaríamos un análisis partiendo de herramientas gratuitas.
Cuando un usuario **no autorizado** toma el control de un sistema, éste puede instalar múltiples backdoors (puertas traseras) que le permitan entrar al sistema en un futuro, aunque **parcheemos** la vulnerabilidad original.
Se denomina **análisis forense** al proceso de analizar una copia completa de un sistema que ha sufrido una intrusión o ataque.

El **análisis forense** permite obtener la mayor cantidad posible de información sobre:

- **El método utilizado por el atacante para introducirse en el sistema**
- **Las actividades ilícitas realizadas por el intruso en el sistema**
- **El alcance y las implicaciones de dichas actividades**
- **Las "puertas traseras" instaladas por el intruso**

Realizando un **análisis forense** nos permitirá, entre otras cosas, recuperarnos del incidente de una manera más segura y evitaremos en la medida de lo posible que se repita la misma situación en cualquiera de nuestras máquinas.

Un buen análisis forense debe dar respuestas a varias cuestiones, entre las que se encuentran las siguientes:

- **¿En que fecha exacta se ha realizado la intrusión o cambio?**
- **¿Quién realizó la intrusión?**
- **¿Cómo entró en el sistema?**
- **¿Qué daños ha producido en el sistema?**

Si una vez realizado el análisis forense no conocemos con exactitud las respuestas a estas preguntas, no tendremos un análisis funcional. Esto puede derivar en futuros ataques, bien por la misma persona, o bien por diferentes medios de intrusión que desconozcamos.

Evidencia digital

Uno de los pasos a tener en cuenta en toda investigación, sea la que sea, consiste en la captura de la/s evidencia/s. **Por evidencia entendemos toda información que podamos procesar en un análisis**.
Por supuesto que el único fin del análisis de la/s evidencia/s es saber con la mayor exactitud qué fue lo que ocurrió.
Bueno, y ¿qué entendemos por evidencia digital? Podemos entender evidencia como:

- El último acceso a un fichero o aplicación (unidad de tiempo)
- Un Log en un fichero
- Una cookie en un disco duro
- El uptime de un sistema (Time to live o tiempo encendido)
- Un fichero en disco
- Un proceso en ejecución
- Archivos temporales
- Restos de instalación
- Un disco duro, pen-drive, etc...

RFC3227. Recolección y manejo de evidencias

El propósito de este documento (RFC3227) no es otro que proveer a los administradores de sistemas unas pautas a seguir en el aspecto de recolección de evidencias, si se diese el caso de un incidente de seguridad.
En este rfc se trata los siguientes aspectos:

- Principios para la recolección de evidencias
- Orden de volatilidad
- Cosas a evitar
- Consideraciones relativas a la privacidad de los datos
- Consideraciones legales
- Procedimiento de recolección
- Transparencia
- Pasos de la recolección
- Cadena de custodia
- Como archivar una evidencia
- Herramientas necesarias y medios de almacenamiento de éstas

Algunos de los principios que rige el documento para la recolección de evidencias son:

- Comprometer al personal de aplicación de la ley y manejo de incidentes apropiados
- Capturar la imagen tan exacta del sistema como sea posible
- Anotar todo lo que se vaya investigando
- Recolectar las evidencias en función de la volatilidad de la misma. Primero se recogerán las de mayor volatilidad

El orden de volatilidad que recoge el rfc es el siguiente:

- Registros, Cache
- Tabla de ruta. ARP Cache, Tabla de Proceso, Núcleo de estadísticas, memoria
- Sistema de Archivo temporales
- Disco
- Datos de monitoreo y Log's remotos relativos al caso
- Configuración física, topología de red
- Medio de Archivos

Si se quiere leer más sobre el RFC3227 sobre la recolección y manejo de evidencias, puede hacerlo en el siguiente enlace:

http://rfc.net/rfc3227.html

Buenas prácticas a la hora de la recogida y análisis de los datos

Estudio Preeliminar

Es el primer paso de cualquier análisis forense. Nos deben o debemos explicar con la mayor exactitud posible qué ha ocurrido, qué se llevaron o intentaron llevar y cuándo ocurrió.
También tendremos que recoger información sobre la organización, ya sea organización, casa, etc...
Recogeremos información sobre la tipología de red y de gente directa o indirectamente implicada.
También podríamos recoger información sobre el tipo de escenario y el/los sistema/s afectado/s.

¿Apagamos el equipo?

Podemos presentarnos con dos casos. El primero es el de no apagar el equipo. Si no apagamos el equipo, podremos ver todos los procesos en ejecución, los consumos de memoria, las conexiones de red, los puertos abiertos, los servicios que corren en el sistema, etc.
También se nos presenta el problema de que si apagamos el equipo, se perderá información volátil que puede ser esencial para el curso de la investigación.
La parte mala de esta situación es que el sistema, al poder estar contaminado, éste puede ocultar la información. También se nos presenta el problema de que si no apagamos el sistema, éste puede comprometer a toda la red.
Si no apagamos el sistema tendremos que controlar este aspecto de la seguridad, y aislarlo completamente de la red, lo cual llega a ser prácticamente imposible en determinados escenarios.

Tipo de Herramientas

Una de las cosas más importantes a la hora de realizar un análisis forense es la de no alterar el escenario a analizar. Esta es una tarea prácticamente imposible, porque como mínimo, alteraremos la memoria del sistema al utilizar cualquier herramienta.
Las herramientas que utilicemos deben de ser lo menos intrusivas en el sistema, de ahí que se huya de las herramientas gráficas, las que requieren instalación, las que escriben en el registro, etc...
Lo normal y lógico sería utilizar herramientas ajenas al sistema comprometido, ya sean herramientas guardadas en cualquier soporte (CD-ROM, USB, etc...). Esto lo hacemos para no tener que utilizar las herramientas del sistema, ya que pueden estar manipuladas y arrojar falsos positivos, lecturas erróneas, etc...

Tipo de Copia del Sistema

En el caso de que se pueda realizar, lo ideal sería hacer más de una copia de seguridad. Una de ellas se podría guardar herméticamente junto con algún sistema de fechado digital como el proporcionado por RedIris **http://rediris.es/app/sellado**.
Otra copia la podría guardar algún responsable de la compañía afectada, y una copia se destinaría a trabajar sobre ella.
En el caso que sea posible, la imagen obtenida podremos montarla sobre un hardware similar al de la máquina afectada.
Destacaremos los siguientes aspectos:

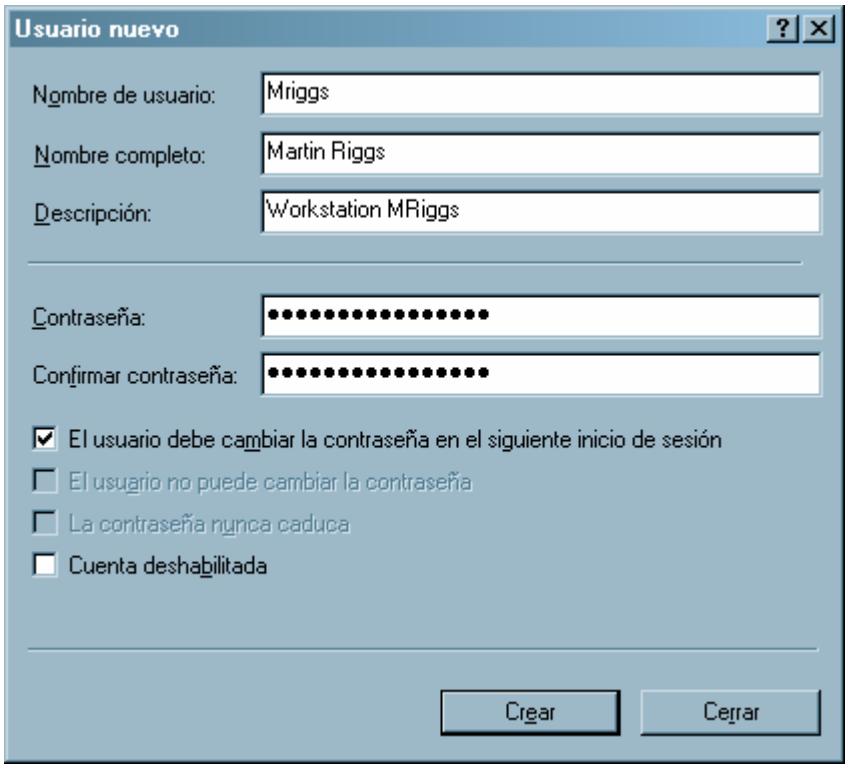
- La copia que realicemos debería ser lo más exacta posible
- Si es posible, haremos varias copias de seguridad
- Una de ellas se guardará herméticamente, para aislarla de todo tipo de agente exterior

- A ser posible se fecharán digitalmente y sobre el papel
- En el caso que sea posible, la imagen obtenida la montaremos sobre hardware similar

Cuentas de usuario y perfiles de usuario

Dejando a un lado si se accede legítima o ilegítimamente, un usuario no es más que cualquier persona que pueda acceder al sistema.
En una cuenta de usuario almacenaremos información acerca del usuario. Algunos datos que se guardan son:

- Nombre de usuario: Nombre con el que nos identificaremos en el sistema
- Nombre completo: Nombre completo del usuario (Siempre que se rellene)
- Contraseña: Palabra cifrada para autenticarnos en el sistema
- SID: Código de identificación de seguridad *
- Directorio: Es el lugar donde en un principio se guardará toda información relevante al usuario.



*Nota.- **A diferencia de los demás, este es el único dato que no podemos especificar manualmente**

El perfil de usuario contiene las preferencias y las opciones de configuración de cada usuario. En la tabla siguiente se puede ver un ejemplo de la configuración que contienen los perfiles de usuario.

Fuente	Parámetros guardados
Explorador de Windows	Todos los valores definibles por el usuario en el Explorador de Windows.
Mis documentos	Documentos almacenados por el usuario.
Mis imágenes	Imágenes almacenadas por el usuario.
Favoritos	Accesos directos a las ubicaciones favoritas de Internet.
Unidad de red asignada	Asignaciones de unidades de red creadas por el usuario.
Mis sitios de red	Vínculos a otros equipos de la red.
Contenido del escritorio	Elementos almacenados en el Escritorio y en los accesos directos.
Colores y fuentes de pantalla	Toda la configuración de colores y textos presentables en pantalla y definibles por el usuario.
Datos de aplicación y sección del Registro	Datos de aplicación y configuraciones definidas por el usuario.
Configuración de impresoras	Conexiones de impresoras de red.
Panel de control	Todas las configuraciones definidas por el usuario en el Panel de control.
Accesorios	Todas las configuraciones de aplicación definidas por el usuario que afectan al entorno de usuario de Windows, incluidos Calculadora, Reloj, Bloc de notas y Paint.
Programas de instalación de la familia Windows Server 2003	Cualquier programa escrito específicamente para la familia Windows Server 2003 se puede diseñar para que haga un seguimiento de las configuraciones propias de cada usuario. Si dicha información existe, se guarda en el perfil de usuario.
Marcadores de formación en pantalla para el usuario	Los marcadores del sistema de Ayuda de la familia Windows Server 2003.

En Windows 2003 Server, los perfiles de cada usuario se almacenan en el directorio Documents and Settings de la raíz. Si nuestro equipo estuviese montado en la unidad C: \, el directorio de los perfiles se encontrará en el directorio siguiente:

C:\Documents and Settings\usuario

Tipos de Logon en un sistema basado en Windows

Los sucesos de inicio de sesión en un sistema Windows se generan en los controladores de dominio para la actividad de cuentas de dominio y en los equipos locales para la actividad de cuentas locales. Si están habilitadas ambas categorías de directiva, los inicios de sesión que utilizan una cuenta de

dominio generan un suceso de inicio o cierre de sesión en la estación de trabajo o servidor, y generan un suceso de inicio de sesión de cuenta en el controlador de dominio.
La categoría de inicio de sesión en Windows registrará la entrada con un evento ID 528 que contendrá una serie de datos importantes, como son el tipo de entrada y el ID de inicio de sesión. Dependiendo del inicio de sesión que hagamos en la máquina, ya sea a través de recursos compartidos, de forma remota o de forma física, Windows registrará ese inicio de sesión con una numeración u otra.
Algunos tipos de inicio de sesión son:

Tipo 2. Interactivo. Entrada a un sistema desde la consola (teclado)
Tipo 3. Red. Entrada al sistema a través de la red. Por ejemplo con el comando net use, recursos compartidos, impresoras, etc...
Tipo 4. Batch. Entrada a la red desde un proceso por lotes o script programado.
Tipo 5. Servicio. Cuando un servicio arranca con su cuenta de usuario.
Tipo 7. Unlock. Entrada al sistema a través de un bloqueo de sesión.
Tipo 10. Remote Interactive. Cuando accedemos a través de Terminal Services, Escritorio Remoto o Asistencia Remota.

La Papelera de Reciclaje. Estructura y funcionamiento

Al contrario de lo que se piensa mucha gente, cuando un archivo se borra de una computadora, realmente no se borra. Los archivos se modifican por decirlo de alguna manera, para que el sistema operativo no los vea. Windows utiliza un almacén para los archivos eliminados llamado Papelera de Reciclaje. La existencia de este almacén permite que un usuario pueda recuperar la información, si ésta ha sido borrada accidentalmente por ejemplo. Cuando Windows da orden de eliminar cierto archivo o directorio, la información se guarda en expedientes, por si el usuario se arrepiente y quiere recuperar sus datos. El archivo que contiene esta información se llama INFO2 y reside en el directorio de la Papelera de Reciclaje, es decir, está dentro de la Papelera.
Es necesario explicar cómo funciona la Papelera de Reciclaje antes de que discutamos las estructuras del archivo INFO2. Cuando un usuario suprime un archivo a través del explorador de Windows, una copia del archivo se mueve al almacén de la Papelera de Reciclaje. La localización de este directorio es distinta, dependiendo de la versión de Windows que tengamos. En versiones NT/XP/2003, el archivo INFO2 se encuentra en el siguiente directorio:

C:\Recycler\<USER SID>\INFO2

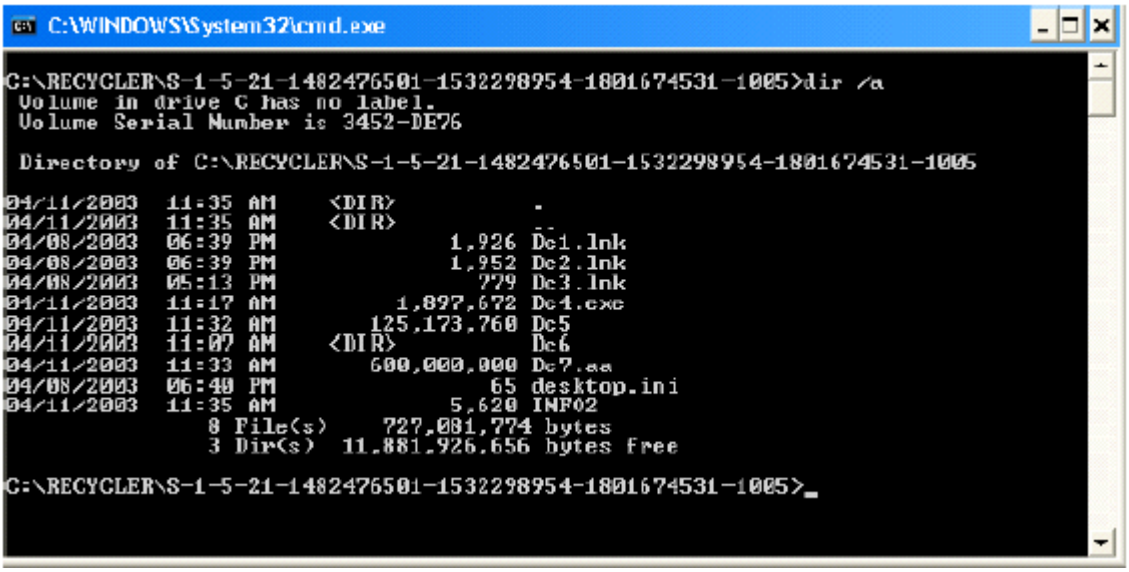
Cuando eliminamos un fichero, Windows lo renombra siguiendo este parámetro:

D <Unidad raíz del sistema> <número> .Extensión del archivo

Es decir, que si nosotros quisiésemos eliminar el archivo **Contabilidad.doc** y lo mandásemos a la Papelera de Reciclaje, Windows lo renombraría de la siguiente manera:

DC1.Doc

Si borrásemos otro archivo, a éste nuevo archivo se le pondría el número 2, y así sucesivamente.



Si al menos un archivo se ha movido a la Papelera de Reciclaje, el archivo INFO2 existirá. Cuando se vacía la Papelera de Reciclaje, el contenido del archivo INFO2 se limpiará, y el número se establecerá de nuevo a 1. Es decir, el archivo INFO2 se suprime y se crea un nuevo y vacío INFO2.

Archivos de Registro de Windows. Estructura

Windows define al registro como una base de datos jerárquica central utilizada en todas las versiones de Windows, con el fin de almacenar información necesaria para configurar el sistema para uno o varios usuarios, aplicaciones y dispositivos hardware. El registro contiene información que Windows utiliza como referencia constantemente, como por ejemplo los perfiles de usuario, las aplicaciones instaladas, los parches o HotFixes instalados, etc... Los archivos del registro de Windows se almacenan en archivos binarios, es decir, que si abrimos estos ficheros con un editor de texto, como puede ser notepad, no podremos leerlo.
El registro se puede manipular desde muchos medios, tanto en línea de comandos como por la propia interfaz gráfica de Windows. Evidentemente la forma más fácil de manipular el registro es de forma gráfica. Sólo tendríamos que ejecutar la herramienta regedit.
El Registro está organizado en una estructura jerárquica compuesta por subárboles con sus respectivas claves, subclaves y entradas.
Las claves pueden contener subclaves y éstas, a su vez, pueden contener otras subclaves.
Generalmente, la mayor parte de la información del Registro se almacena en disco y se considera permanente, aunque en determinadas circunstancias hay datos que se almacenan en claves llamadas volátiles, las cuales se sobrescriben cada vez que se inicia el sistema operativo.
Toda información relativa al sistema operativo y al PC se encuentra recogida en los archivos del sistema del registro de Windows, los cuales se localizan en **%systemroot%\system32\config**, y atienden a los nombres siguientes:

- SECURITY
- SOFTWARE
- SYSTEM
- SAM
- DEFAULT

Cada sección del Registro está asociada a un conjunto de archivos estándar. En la tabla siguiente se muestran las secciones y archivos asociados a estas secciones:

Sección del Registro	Nombres de archivo
HKEY_LOCAL_MACHINE\SAM	Sam y Sam.log
HKEY_LOCAL_MACHINE\SECURITY	Security y Security.log
HKEY_LOCAL_MACHINE\SOFTWARE	Software y Software.log
HKEY_LOCAL_MACHINE\SYSTEM	System y System.log
HKEY_CURRENT_CONFIG	System y System.log
HKEY_CURRENT_USER	Ntuser.dat y Ntuser.dat.log
HKEY_USERS\.DEFAULT	Default y Default.log

Index.dat e Internet Explorer. Estructura y funcionamiento

Internet Explorer es el navegador por excelencia de Microsoft. A partir de su versión XP, este navegador viene integrado en el sistema operativo, es decir, que no se puede desinstalar. Internet Explorer guarda una copia de las páginas visitadas en el disco duro. Si vas a una página ya visitada, Internet Explorer busca primero en la caché, y la compara con la página del servidor, mostrándote la página desde tu disco duro, si no ha habido actualizaciones. Con esto conseguimos una carga mucho más rápida de las páginas Web, o como dirían los expertos, **Una mejor experiencia para el usuario final**. Podemos borrar el caché de disco desde el propio Internet Explorer (herramientas, opciones de Internet, eliminar archivos). El problema es que esta opción borra todo el contenido del historial de Internet (los archivos html, los gráficos, etc.) pero no borra el índice de referencia que Internet Explorer usa para buscar dentro de su historial: el archivo index.dat. Estos archivos (hay varios index.dat) están definidos como ocultos y de sistema; por eso no podemos acceder a su contenido desde el propio Windows, a no ser que quitemos el atributo de ocultos a esos directorios. En ellos se guarda una lista de todos los sitios Web que hemos ido visitando (aunque hayamos borrado el historial, esta lista no está sincronizada, luego no borra esas Urls). Esto supone un problema de privacidad, ya que cualquiera que sepa localizar y leer estos archivos index.dat tendrá un listado completo de los sitios que hayamos visitado (aunque hayamos borrado el historial del navegador). Además este archivo está creciendo constantemente, y puede llegar a ocupar varios megas de la forma más innecesaria. Aparte, si por cualquier razón su contenido se corrompe, puede ocasionar que Internet Explorer no pueda visualizar correctamente algunas páginas o no pueda descargar ficheros. La ruta en donde se encuentran estos archivos (index.dat) es la siguiente:

Windows 2K/XP	\Documents and Settings\<username>\Local Settings\Temporary Internet Files\Content.IE5\ \Documents and Settings\<username>\Cookies\ \Document and Settings\<username>\Local Settings\History\History.IE5\

Service Pack, HotFix, ¿Qué es y para qué sirve?

Un Service Pack mantiene la versión de Windows y/o aplicaciones actualizados, corrigen problemas conocidos así como ampliar funcionalidad al equipo. En un Service Pack se incluyen drivers o controladores, herramientas y actualizaciones, así como algunas mejoras realizadas después de la puesta al público del producto. Y todo esto incluido en un paquete.
Cada nuevo Service Pack contiene todas las soluciones incluidas en los anteriores, es decir, cada Service Pack es acumulativo. Para mantener actualizado nuestro sistema sólo necesitaremos instalar el último Service Pack para cada producto o versión de Windows, ya que los Service Packs son específicos para cada producto. No se utiliza el mismo Service Pack para actualizar un Windows XP, que para actualizar un Windows 2000, por ejemplo.
Un HotFix básicamente es una revisión de un producto. Estas revisiones se realizan con el fin de subsanar errores específicos para los que no existe una solución viable.
Un HotFix no se somete a pruebas rigurosas, por lo que se recomienda aplicar estas revisiones, si se experimenta el problema exacto.
Cada cierto tiempo, al incorporarse nuevas funcionalidades y actualizaciones en los Service Packs, estos HotFix se someten a comprobaciones más exhaustivas, y se ponen a disposición del público en general.
La rama encargada de programar HotFix en Microsoft se denomina Ingeniería de corrección rápida o QFE (**Quick Fix Engineering**).