Informática Forense en Entornos de Windows

Apaza Cora Mónica Gabriela
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
monik_acm@hotmail.com

RESUMEN

Este documento expone los aspectos básicos relacionados en el campo de la informática forense, explicando de una forma simple algunas herramientas utilizadas para la captura de evidencias a la hora de realizar un análisis forense en entornos Windows.

Palabras clave

Informática forense ,archivos de registro, evidencia, seguridad, información , análisis forense

1. INTRODUCCIÓN

El valor de la información en la sociedad es cada vez más importante, por esta razón técnicas que garantizan la efectividad de las políticas de seguridad de información y tecnologías de la información, como la informática forense día a día trascienden más.

La informática forense consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas con la finalidad de perseguir objetivos preventivos, anticipándose a un posible problema u objetivos correctivos, para una solución favorable.

Las metodologías utilizadas en informática forense incluyen la recogida segura de datos de diferentes medios digitales y evidencias digitales, sin alterar los datos de origen las que posteriormente son catalogadas para su respectivo análisis y documentación de cada prueba aportada.

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 parchemos la vulnerabilidad original.

Se denomina análisis forense al proceso de analizar una copia completa de un sistema que ha sufrido una intrusión o ataque.

Esto 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.

2. EVIDENCIA DIGITAL

Uno de los pasos a tener en cuenta en toda investigación, sea la que sea, consiste en la captura de las evidencias. Por evidencia entendemos toda información que podamos procesar en un análisis. Por supuesto que el único fin del análisis de las evidencias es saber con la mayor exactitud qué fue lo que ocurrió.

En detalle, evidencia digital puede ser considerado 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...

3. 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 completo, Contraseña, SID, Directorio.*

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.

En Windows Server 2003, 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

4. 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

Tabla 1. Métodos de borrado de discos

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.

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:

Interactivo. Entrada a un sistema desde la consola (teclado)

Red. Entrada al sistema a través de la red. Por ejemplo con el comando net use recursos compartidos, impresoras, etc...

Batch. Entrada a la red desde un proceso por lotes o script programado.

Servicio. Cuando un servicio arranca con su cuenta de usuario.

Unlock. Entrada al sistema a través de un bloqueo de sesión.

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 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.

5. ESTRUCTURA DE LOS ARCHIVOS DE REGISTRO

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:

Tabla 2. Registros de Windows

Seccion 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_LOCAL_CONFIG	System y system.log
HKEY_LOCAL_USER	Ntuser.dat y Ntuser.dat.log
HKEY_USERS\.DEFAULT	Default y Default.log

Dado que Windows utiliza como referencia toda la información que se encuentra en el registro, un analista forense puede utilizar como referencia esta gran base de datos para recabar información sobre la máquina. En la base de datos de registro que se encuentra en el sistema Windows, podremos averiguar: versión del sistema operativo, ruta de instalación, clave de producto, tipo de procesador de la máquina, aplicaciones instaladas, HotFix y parches instalados, servicios corriendo en la máquina, configuración y enumeración de los adaptadores de red.

Podemos utilizar varias herramientas para analizar el registro. Algunas de ellas son:

WRR (Windows Registry Recovery de MiTec).

Comando nativo XP FC (Compara ficheros).

Access Data Registry Viewer.

Windows Registry File Viewer.

Windiff (Herramienta para comparar ficheros).

Una vez abierto estos archivos de sistema que referencian al registro de Windows (SECURITY, SYSTEM, SOFTWARE, SAM, DEFAULT) con alguna de estas aplicaciones, podremos movernos por sus distintas ramas, y poder así analizar los datos que contienen estos ficheros.

Por ejemplo podríamos averiguar los criterios de búsqueda de un usuario en particular, buscando en el registro del perfil de usuario (ntuser.dat) la clave del historial de navegación de la barra de búsqueda de Google (si la tuviese instalada) HKCU\Software\Google\NavClient\1.1\History

6. 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 se va 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 y 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 forma 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.

7. RECOGIDA DE ARCHIVOS LOG DEL SISTEMA

Los ficheros Log de una máquina, sea la que sea, son una fuente de información importantísima en un análisis forense. Los sistemas Windows basados en NT tienen su principal fuente de Log en los archivos de sistema siguientes:

SysEvent.Evt. Registra los sucesos relativos al sistema

SecEvent.Evt. Registra los sucesos relativos a la seguridad

AppEvent.Evt. Registra los sucesos relativos a aplicaciones

Estos ficheros se encuentran en el directorio

%systemroot%\system32\config.

Si están auditadas las opciones de inicio de sesión, cambio de directivas y permisos, nos centraremos con especial atención en el archivo Log ecEvent.Evt. Para visualizar este fichero podremos utilizar la herramienta de Windows eventvwr.msc, comúnmente llamada Visor de Sucesos. Abriremos con esta herramienta el archivo SecEvent.Evt, que es el encargado de almacenar los sucesos relativos a la seguridad, tales como ingresos en la máquina, cambio de directivas, etc... Por ejemplo, podríamos buscar todo acceso físico a la máquina, cambio de directivas y creación de cuentas de usuario. Eso nos podría dar una idea de quién toca el sistema.

Por ejemplo, el evento 624 es el referido por Windows para un suceso de creación de cuenta de usuario. En la siguiente imagen podremos ver como lo registra Windows.

Otro ejemplo de suceso, sería el relativo al inicio de sesión. Windows almacena este suceso con el identificador 528.

Windows tiene distintos archivos Log para auditar los posibles sucesos y/o errores que puedan surgir en la vida útil del sistema operativo. Algunos de ellos son:

WindowsUpdate.log (Log de Windows Update)

memory.dump (Archivos de volcado de memoria)

Archivos de registro de Windows (Software, System, etc...)

8. COOKIES. ESTRUCTURA, FUNCIONAMIENTO Y METODOLOGÍA DE ACCESO A LA INFORMACIÓN

Una cookie no es más que un fichero de texto. El funcionamiento es bastante sencillo.

Algunos servidores piden a nuestro navegador que escriba en nuestro disco duro, y nuestro navegador escribe en un fichero de texto información acerca de lo que hemos estado haciendo por sus páginas.

Una de las mayores ventajas de las cookies es que se almacenan en el equipo del usuario. Con esto conseguimos liberar al servidor de una sobrecarga en su espacio de disco. Cuando el servidor solicite esa información, nuestro navegador se la enviará en

forma de cookie. Las cookies poseen una fecha de caducidad, que puede oscilar desde el tiempo que dure la sesión hasta una fecha especificada, a partir de la cual dejan de ser operativas.

En un sistema Windows 2K/XP/2K3, las cookies se encuentran en la ruta:

C:\Documents and Settings\Nombre_Usuario\Cookies

En Internet Explorer existe una cookie por cada dirección de Internet que visitamos, con la nomenclatura siguiente: Identificador_Usuario@dominio.txt

Para ver el contenido de una cookie, sólo tenemos que editarla con un editor de texto.

Las cookies se almacenan en memoria hasta que salimos del navegador, momento en el que se escriben en el disco. Para ver las cookies que nos pide un determinado sitio Web cuando estamos conectados, podremos escribir en la barra de direcciones este simple comando: JavaScript:alert(document.cookie);

Acto seguido nos saldrá un cuadro de alerta, con el contenido de la cookie que nos pide el servidor.

9. EL ARCHIVO DE PAGINACIÓN DE WINDOWS. PAGEFILE.SYS

El archivo de paginación (Pagefile.sys) es un archivo que Windows utiliza como si fuera memoria RAM (Memoria de acceso aleatorio). Este archivo está situado en la raíz del disco duro y por defecto lo marca como oculto. El archivo de paginación y la memoria física conforman la memoria virtual. De manera predeterminada, Windows almacena el archivo de paginación en la partición de inicio, que es la partición que contiene el sistema operativo y sus archivos auxiliares. El tamaño predeterminado o recomendado del archivo de paginación es igual a 1,5 veces la cantidad total de memoria RAM.

Para visualizar el contenido del archivo de paginación, podemos utilizar una herramienta de SysInternals, llamada Strings.exe.

Esta herramienta busca cadenas de texto (ASCII o Unicode) en archivos.

10. CONCLUSIÓN

Se ha procurado describir de manera resumida las maneras en que las personas que tengan un computador ya sea en casa o en la oficina puedan saber como recuperar la información que consideraron perdida o bien comprender de que está hablando un experto en la materia con el fin de evitar timos o sorpresas desagradables. Es necesario no limitarse a ser un simple usuario, sino como ahora, tener la voluntad de conocer más en detalle el equipo que se opera para realizar las transacciones que diariamente y comúnmente, pasan a lo largo del día.

11. REFERENCIAS

[1]http://www.cita.es/ingenieria/forense/

[2]http://www.miguelgallardo.es/perito/informatico/

[3]Windows Internals, cuarta edición, Microsoft Systems.