International Baccalaureate®
Baccalauréat International
Bachillerato Internacional

INFORMÁTICA
ESTUDIO DE CASO: ARCHIVOS OCULTOS – INFORMÁTICA FORENSE

EXAMEN DE MUESTRA

INSTRUCCIONES PARA LOS ALUMNOS

- Para la prueba 3 del nivel superior se requiere el cuadernillo del estudio de caso.

Introducción

La *informática forense* es una rama de la seguridad informática que se centra en el análisis de los sistemas informáticos con el objetivo de obtener pruebas del mal uso de los computadores o de ataques sobre los mismos.

El computador de sobremesa normal almacena una cantidad considerable de datos que el usuario no ha guardado conscientemente. Estos datos pueden ser *cookies*, registros de impresión y de correos electrónicos y el historial de navegación. Estos datos se almacenan en archivos (algunos ocultos), a los que se puede acceder con relativa facilidad. No obstante, también puede conservar datos que supuestamente habían sido borrados o incluso versiones anteriores de archivos que se han modificado posteriormente. El hecho de que sea tan difícil borrar estos datos debería preocupar no sólo a los delincuentes informáticos, sino también a empresas y particulares que deseen borrar permanentemente sus datos o reciclar sus computadores. Los usuarios deberían ser conscientes de que solo una "limpieza forense" borra eficazmente todos los datos de sus discos duros.

El resto del estudio de caso investiga el trabajo de John Martin, un forense informático ficticio.

Sus Secretos Revelados S. A.

John Martin trabaja para la empresa de seguridad informática *Sus Secretos Revelados S. A.* Esta compañía tiene dos divisiones: una que actúa como especialista en seguridad para asesorar sobre sistemas de seguridad informática y otra que se especializa en informática forense. John trabaja en la división forense y, aunque era ya un usuario experimentado de computadores, tuvo que realizar un entrenamiento intensivo en las técnicas y herramientas usadas para localizar e identificar pruebas incriminatorias, así como en los procedimientos que deben seguirse rigurosamente para que las pruebas obtenidas sean aceptadas por un tribunal.

Un ejercicio de entrenamiento consiste en investigar el siguiente contexto:

"Se ingresa con orden juducial al domicilio de una persona sospechosa de organizar distribución ilegal de droga y se detiene al sospechoso. El computador personal del sospechoso, que estaba aún funcionando, estaba equipado con una conexión a Internet y una cámara web. La información que lleva al registro de la casa proviene de la interceptación de una llamada telefónica que hacía referencia a determinados nombres asociados con el tráfico ilegal de droga".

La tarea de John era buscar en el computador y las zonas adyacentes información electrónica que pudiera inculpar al sospechoso. Estaba equipado con varias herramientas proporcionadas por la compañía. Sus tareas incluían asegurar y evaluar el escenario, realizar entrevistas preliminares, documentar el incidente, recolectar pruebas, empaquetarlas y transportarlas. Su primera acción fue desconectar todos los dispositivos y quitar con cuidado el disco duro del computador para llevarlo a los laboratorios de la empresa.

Desde entonces, John ha participado en distintas investigaciones, entre otras:

- mal uso de Internet por parte de los empleados contra sus empleadores
- delitos de fraude
- espionaje industrial
- divulgación no autorizada de información
- pornografía infantil
- suplantación de identidad.

El caso de espionaje industrial resultó de particular interés ya que la compañía estaba convencida de que una empresa de la competencia había robado sus ideas, pero no tenía pruebas concretas que lo demostraran. El servidor principal de la compañía fue analizado con posterioridad por *Sus Secretos Revelados S. A.*, que descubrió que se había instalado un acceso remoto mediante una "puerta trasera". Además, el equipo forense descubrió que se había instalado software para grabar las pulsaciones del teclado, que podía enviar a un tercero, a través de Internet, los datos introducidos en el sistema. Se identificó a este tercero y se descubrió que era uno de los competidores que estaban intentando robar propiedad intelectual de la compañía.

Posteriormente contrataron los servicios de *Sus Secretos Revelados S. A.* para actualizar su sistema de seguridad, concretamente la parte relacionada con prevenir el acceso externo no autorizado.

La investigación actual de John consiste en buscar imágenes ilegales en un computador. El computador del sospechoso estaba desconectado. Además, no se encontró ningún hardware de red en la vivienda. Un disco duro común puede tener miles de archivos, así que después de realizar una copia exacta del disco duro del sospechoso, la primera tarea de John fue filtrar todos los archivos conocidos (de la copia) usando un análisis *hash*. Es vital no manipular el disco original bajo ningún concepto.

Se encontraron archivos con extensión normal de imagen usando el gestor de archivos del computador (el sistema operativo era Windows XP), pero no se encontró ninguna prueba incriminatoria.

Como los archivos que estaba buscando no aparecieron inmediatamente, hubo que realizar un análisis más complejo, realizando una búsqueda de archivos que se habían camuflado de alguna manera. Los delincuentes suelen ocultar los archivos. Un paso adicional que podría revelar pruebas sería investigar el espacio no asignado y el espacio desperdiciado del disco.

Retos afrontados

John y su equipo deben centrarse en las siguientes cuestiones:

- Garantizar que se sigan todos los procedimientos correctos para que todas las pruebas descubiertas sean admitidas en procedimientos legales ulteriores.
- Encontrar todos los archivos pertinentes de un sistema informático que el usuario haya intentado borrar.
- Encontrar todos los archivos pertinentes de un sistema informático que el usuario haya intentado ocultar o camuflar por algún medio.

Véase al dorso

Terminología adicional para la guía

Acceso por una puerta trasera
Análisis físico
Análisis *hash*
Análisis lógico
Archivos ocultos
Bloqueador de escritura
Cifra del mensaje (*Hash*)
Clúster
Cookies
Directorio raíz
Espacio desperdiciado del disco
FAT
Imagen de *bit-stream*
Imagen especular
Limpieza forense
Metadatos
Propiedad intelectual
Registradores de teclas
Signatura de archivo
Tiempos de MAC

Las empresas, productos o individuos mencionados en este estudio de caso son ficticios y cualquier similitud con entidades reales es puramente fortuita.