ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA

ANÁLISIS FORENSE EN SITIOS WEB

Shirley Soria Panchana [(1)]; Jose Parrales Tenelema [(2)]
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral
Campus Gustavo Galindo Velasco, Km. 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil - Ecuador
ssvane2009@hotmail.com [(1);] joseparrales84@hotmail.com [(2)]

Febrero del 2012 – Febrero del 2013
Guayaquil – Ecuador

Directora de Tesis Ing. Karina Astudillo, mail karina.astudillo@elixircorp.biz

Resumen

La presente tesis consiste en el Análisis Forense de Sitios Web, para el cual se nos ha asignado un caso de estudio que tiene como escenario un bufete de abogados, el cual almacena toda su información en un servidor central ubicado en Docustodiam. El 18 de marzo del 2005 cuando uno de los asociados deseaba guardar un documento, el servidor le muestra el siguiente error: "Se ha llegado al límite de almacenamiento, por favor; comuníquese con su administrador de sistema". El Asociado llamó a Joe Schmo, quien es el administrador de IT de la firma de abogados. Pero, su llamada se desvió al correo de voz de Joe indicando que estaba de vacaciones desde el 7 de marzo al 21 del mismo mes, 2005.

Esto no fue un hecho aislado. Un estudio interno reveló que más de 500 GB de archivos MP3, software pirata, y películas se almacenaban en el sistema, bajo el perfil de Joe Schmo. Después de encontrar que una posible intrusión había ocurrido, la firma de abogados rápidamente llegó a la conclusión que era necesario realizar una investigación y así probar o refutar si el administrador de TI fue quien realizó la serie de actividades ilícitas.

Palabras claves: *Análisis, Servidor, Descargas, Administrador, Software, Ilícito.*

Abstract

This work consists of a Web Browse Forensics Analysis and we have been assigned the following case of study: On March 18, 2005, a Senior Associate at a prestigious law firm had just finished a draft of a property-sale contract but was unable to upload the document to the law firm's centralized document storage server hosted by Docustodian. His attempts to upload the document met with the following error message: "You have reached the storage limit. Please call your system administrator". The Senior Associate did just that, calling Joe Schmo, the firm's IT administrator. But, Joe's voicemail indicated that he was on vacation on Florida from March 7-21, 2005.

This was not an isolated occurrence. An internal review revealed that over 500 GB of MP3s, pirated software, and newly released movies were stored on the system under the profile for Joe Schmo. After finding that a potential intrusion had occurred, the law firm quickly concluded that an investigation of a potential violation of internal policy or an intrusion was beyond their core IT competency and brought in a professional security firm to lead the investigation.

Keywords: *Analysis, Server, Downloads, Administrator, Software, Illegal.*

1. Introducción

La computación forense, cada vez toma mayor fuerza y adquiere considerable importancia, debido al aumento de información almacenada de forma digital, al incremento del uso de computadores dentro de las compañías, y otros medios como el Internet. Cuando se comete algún delito informático, queda registrada información en estos medios de almacenamiento.

La computación forense está siendo utilizada con el fin de identificar los hechos de un delito informático ejecutado, ya sea por fallas humanas o por el procesamiento sobre la infraestructura.

Es necesario establecer un grupo de herramientas para extraer de los medios informáticos la mayor cantidad de evidencia digital que verifique las afirmaciones realizadas sobre los hechos delictivos que se han presentado en el caso bajo estudio.

Se ha realizado esta investigación para una firma de abogados, que presentó un problema en su servidor principal, debido que se almacenaba una gran cantidad de información innecesaria descargada desde el Internet a su servidor, impidiendo su correcto funcionamiento.

Utilizaremos los principios de la computación forense con sus herramientas, para identificar quién o quiénes han incumplido con las políticas establecidas por la empresa, identificar el tiempo exacto en el que sucedieron los eventos; determinar si la acción fue realizada por usuarios internos o externos; establecer cuál fue el propósito del ataque, y a la vez mejorar la seguridad de la información de la empresa, por medio del establecimiento de políticas de seguridad informática.

2. Metodología

Para lograr nuestros objetivos propuestos debemos aplicar procedimientos con herramientas rigurosas que nos ayuden a resolver los diferentes tipos de delitos informáticos, apoyándonos en teorías científicas; aplicando métodos para la recolección de la información, análisis, y verificación de las pruebas digitales; establecer los mecanismos idóneos que nos permitan la adquisición, preservación, y la presentación de datos que han sido procesados electrónicamente y guardados en un equipo de computación.

Cabe recalcar que la computación forense no se encarga de prevenir delitos, de esto se encarga la seguridad informática; pero es importante tener claro el marco de actuación entre la informática forense, la seguridad informática y la auditoría informática.

La metodología forense consta de la adquisición segura de datos de diferentes medios y evidencias digitales, sin alterar de ninguna manera los datos de origen.

A cada fuente de información se le realiza una copia exacta y se la cataloga para prepararla para su posterior análisis, se debe documentar cada prueba aportada, tener fotos de lo que se encontró en primera instancia, y de haber sido manipulada por alguien, documentar en qué estado se recibió la evidencia. Las evidencias digitales recabadas permiten determinar un dictamen claro, conciso, fundamentado y con justificación de las hipótesis en base de las cuales se han realizado las investigaciones a partir de las pruebas recogidas.

En todo procedimiento que vayamos a realizar debemos tener presente las leyes que la rigen. Y sus requerimientos, para no faltar en ningún momento a los derechos de terceros; y así de ser necesario, toda la evidencia sea aceptada sin problemas por los tribunales y poder construir una prueba bien fundamentada para alcanzar resultados favorables.

Dependiendo de la evidencia que tengamos también va a variar el tipo de metodología y los principios científicos que debemos considerar tales como:

- Recuperar documentos de un archivo dañado.
- Hacer una copia exacta de una evidencia digital.
- Generar una firma digital con un algoritmo de hashing de un texto para asegurar que este no se ha modificado
- Firmar digitalmente un documento, para afirmar su autenticidad.

3. Desarrollo de la Investigación

Para el análisis del caso no se tuvo un acceso físico a los equipos, ni mayor información con respecto a las personas que tienen acceso a los mismos, ya sea la posesión de claves, horarios laborales, o si el señor Joe Schmo tuvo algún reemplazo durante su periodo vacacional.

Se nos hace la entrega de la información en un CD, en el cual se encontró la siguiente evidencia.

Figura 1: Evidencia Obtenida.

De acuerdo con la gráfica mostrada tenemos 4 carpetas y un archivo index.dat el cual es propio del Internet Explorer, este tiene como funcionamiento guardar información de las páginas accedidas, y así cuando el usuario vuelva a acceder al mismo sitio estas carguen rápido. El tener un archivo index.dat de un tamaño considerado grande puede afectar el rendimiento del computador.

El archivo index.dat como tal nos arroja información en un lenguaje no legible a la visión humana, por lo cual usamos varias herramientas para realizar la extracción de toda la información y de esta manera hacer las conclusiones debidas.

Debido a que la información se encuentra en formato binario, utilizamos como primera herramienta el BinaryViewer, el cual nos muestra información en formato hexadecimal, octal y ascii. Podemos observar información como: las páginas visitadas, el tipo de archivo, el tamaño del sitio web, el usuario que accedió y el protocolo que utiliza.

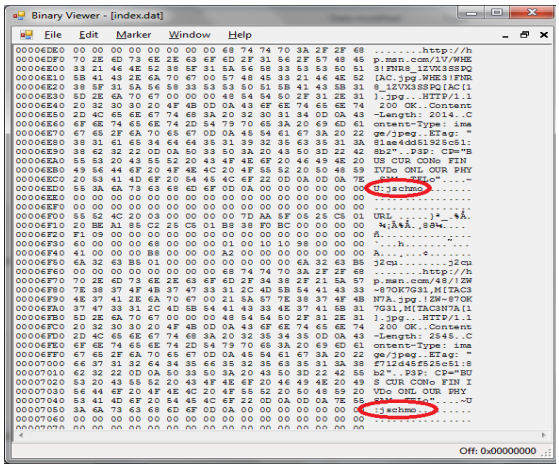

Figura 2: Resultado BinaryViewer

Como segunda herramienta utilizamos el Index.dat Analyzer, esta nos permite ver y borrar el contenido de archivos index.dar que es donde se almacenan las páginas que un usuario ha visitado, encontrando referencias de cookies, historial de navegación y páginas de caché.

El análisis de esta información permite determinar la actividad que realiza el usuario en Internet, como: descargas, documentos, fecha y hora de acceso, fecha de creación de la página web.

Para un mejor manejo de la información la herramienta permite extraer el contenido en un archivo .xls (Excel) y así tener una búsqueda más óptima ya que podemos realizar filtros por fechas y así centrarnos en las páginas relevantes para esta investigación.

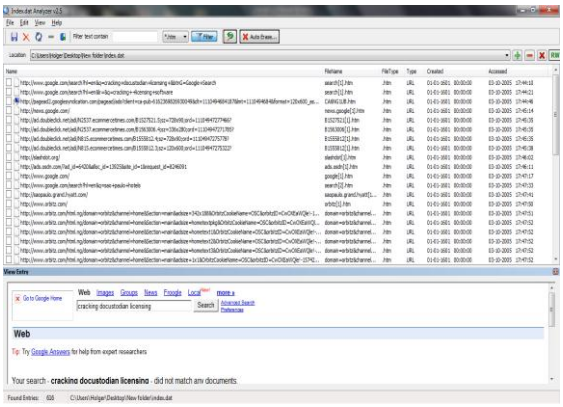

Figura 3: Resultado Index.dat Analyzer

Entre los resultados obtenidos en las navegaciones realizadas tenemos lo siguiente:

- Actividad fuera de lo normal a la fecha del 10 de marzo del 2005 entre las 17:44 y 18:10 horas.
- Se realizan búsquedas sobre: software de crackeo al servidor y licencias de Docustodian, foros y libros sobre códigos de crackeo.
- Se visitaron páginas para obtener seriales de software crackeados.
- También realiza una búsqueda de hoteles en Brasil.
- A su vez la cotización del ticket de viaje.
- Revisión del correo electrónico.

Todas estas búsquedas implican una intrusión y la violación tanto de las políticas de seguridad y el acto ilícito que se intenta cometer.

Entre la información más relevante dentro de esta investigación es la captura de la navegación dentro del correo electrónico, donde podemos visualizar la creación de un correo con las características de las credenciales de Joe Schmo.

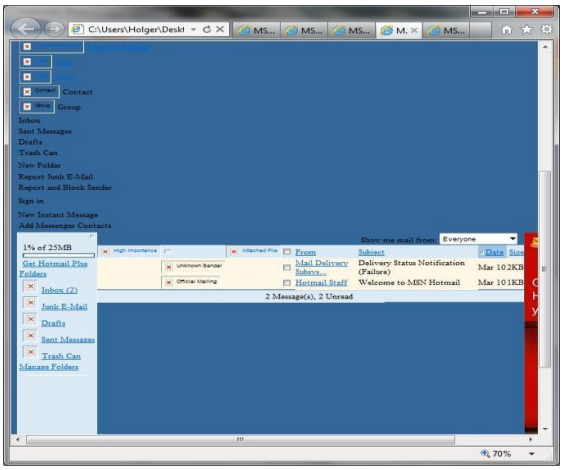

Figura 4: Bandeja de Entrada del Correo

Podemos observar que Hotmail como anfitrión le da la bienvenida a sus servicios, lo interesante es la fecha de la creación del correo el 10 de marzo lo cual nos da indicios de una posible suplantación de identidad. Luego de eso realiza la composición de un correo electrónico con destinatarios de diferentes dominios.

Para finalizar las actividades realiza la eliminación de la bandeja de entrada. La cual nos deja ya el indicio de una suplantación de identidad.

El index.dat Analyzer nos ha proporcionado información relevante con respecto a las navegaciones realizadas, también utilizamos una herramienta llamada Pasco que nos permite extraer la información del index.dat pero en un entorno Linux, este lo utilizamos para hacer una comparación de resultados, en nuestro caso nos arrojó la misma cantidad de navegaciones tanto en Linux como Windows.

Esto ha sido lo más relevante dentro de las búsquedas, entro otros se encontraron archivos, botones, imágenes multimedia propias de las páginas visitadas, por el hecho de tener cierto tipo de publicidad.

4. Conclusiones

Para llegar a ser determinantes en la investigación se requiere la extracción de la memoria caché ya que con esta nos permitirá realizar una reconstrucción completa del historial, conocer desde qué direcciones ip se realizaron las conexiones, y si las imágenes observadas son las correctas a través de la meta data. Con el index.dat lo único que tenemos son indicios de las navegaciones realizadas.

Con los resultados obtenidos nos da la percepción de una suplantación de identidad donde más bien se trata de inculpar y perjudicar al administrador de TI, tenemos una limitante de información que no nos permite ser determinantes más bien se considera un bajo control en cuanto al sistema de navegación y políticas de seguridad.

Implican varios factores internos dentro de esta investigación como son los siguientes:

1. Registros de Políticas.
2. Tipos de Usuarios.
3. Zona Horaria del Computador.
4. Cuenta del Administrador Principal.
5. Tipos de Privilegios.
6. Registro de Actividades.

Si nos basamos únicamente en lo encontrado se podría decir que el señor Joe Schmo no pudo ser el causante de las descargas y búsquedas ilícitas ya que se encontraba en periodo vacacional, y con las capturas del correo electrónico se ve la creación de una nueva cuenta, se considera más bien que se trata de inculparlo del fraude realizado.

Con la información obtenida, dentro del marco legal la investigación no tendría bases fuertes para inculpar o absolver de culpas al Administrador de TI, más bien el caso se caería por falta de evidencia.

En cuanto al ámbito técnico se realiza un planteamiento según lo analizado, por lo que se debe tomar en cuenta lo siguiente:

- Análisis de vulnerabilidades mensual y un hacking ético anual de la infraestructura de la seguridad informática.
- Alertas en cuanto a eventos fuera de lo normal.
- Realizar monitoreo de las actividades de los usuarios.
- Segmentación física y Lógica de la red LAN.

El uso de estas políticas, nos pueden ayudar a temer un mejor control de accesos al sistema y de los recursos.

5. Recomendaciones

Debido al incidente ocasionado en la firma de abogados y considerando la importancia y lo delicado de la información que ellos manejan, se recomienda elaborar políticas de seguridad basados en el estándar ISO 27001, que incluya como mínimo las siguientes recomendaciones con el fin de salvaguardar la información y la seguridad que le ofrecen a sus clientes, las cuales vamos a proceder a detallar:

1. Todo acceso a los servidores o dispositivos de comunicación será con usuario y contraseña de dominio o locales, con el fin realizar auditorías y acciones ejecutadas sobre los mismos.
2. Las claves de los usuarios deben ser cambiadas cada mes, y puestas en custodia por el área de seguridad informática.
3. Todo software adquirido por terceros deberá estar certificado bajo la plataforma en la que se desenvuelve la empresa.
4. Toda información confidencial de la empresa deberá ser almacenada de forma cifrada en los servidores.
5. Se deberán realizar auditorías internas cada seis meses para verificar el cumplimento de las políticas.
6. Se realizarán respaldos de los logs de servidores y dispositivos de comunicación.
7. Si alguno de los usuarios se encuentra en periodo vacacional su cuenta debe ser bloqueada.
8. La información debe estar limitada según el tipo de usuario.
9. Todos los computadores deberán tener instalado un software anti-spyware.
10. Deshabilitar reproductores de CD-DVD ya que a través de estos medios se puede tomar el control del ordenador de forma sencilla, a su vez tener control de las memorias USB.
11. Todo programa de acceso remoto debe ser utilizado con precaución.
12. Usar un sistema IDS, y así proteger el sistema de amenazas en la conectividad a la red.
13. Utilización de herramientas para fortalecer la seguridad como por ejemplo: sistemas anti-spam, firewall, IDS, antivirus.
14. Utilización de servicios de seguridad como por ejemplo: IPS, detectores de intrusos, detectores de vulnerabilidades y consultorías.

6. Referencias

[1] Código Integral Penal. Obtenido de http://www.justiciapenalecuador.com.ec.

[2] Legislación Vigente y Convenios Internacionales. Obtenido de http://www.interfutura.ec/blog/delitos-informaticos-en-ecuador-lo-que-vendria-en-la-nueva-legialacion/.

[3] Nuevo Código Orgánico Integral Penal. Obtenido de http://www.hoy.com.ec/noticias-ecuador/codigo-penal-incluira-delitos-informaticos-513190.html.

[4] Especialistas en Criminología. Obtenido de http://www.estudiocriminal.com.ar.

[5] Bryan Carrier, File System Forensic Analysis.

[6] Bakker, Paul. "SearchTools, Indexed Searching in Forensic Images." Sleuth Kit Informer #16.