Enunciado TFM – Análisis forense

Descripción del caso

La dirección de una empresa tiene serias sospechas de que han accedido a sus sistemas de información de forma ilícita. El gerente de la misma, te solicita como CISO (principal responsable en el ámbito de la seguridad de la información), que **compruebes si realmente han accedido, así como el método seguido. También las consecuencias que se derivan de dicho acceso, si ha habido extracción de información alguna, etc.**

A tal efecto, dispones de **una captura de la memoria RAM y el evidencial del disco duro**.

Deberás presentar **un resumen ejecutivo dirigido al gerente del negocio** explicando los hechos ocurridos para que éste, neófito en materia informática, sea adecuadamente informado, así como **la redacción de un informe pericial** para el citado análisis, documentando todas aquellas evidencias que hayas podido localizar e indicando cuáles son los límites de tu análisis.

Análisis forense y elaboración del resumen ejecutivo e informe pericial

Recibes los dos ficheros imagen antes mencionados (junto con sus valores hash de adquisición). Sobre estas imágenes forenses, previo análisis, deberás hacer la memoria de trabajo y el informe ejecutivo e informe pericial correspondientes, ajustado a los condicionantes que tú creas que debe tener un resumen ejecutivo dirigido a una persona (el gerente) que dice desconocer bastante del mundo de la informática pero que quiere saber cuáles son los hechos ocurridos.

El resumen ejecutivo debe ser breve y conciso. Ten presente que el informe ejecutivo no deja de ser una síntesis de los puntos clave del análisis mostrado en la memoria. Por lo tanto, **la extensión máxima del resumen no debe exceder de tres o cuatro páginas**.

El informe pericial debe contener el análisis completo del sistema informático estudiado, **aunque debe centrarse especialmente en aquellos aspectos que de manera obvia reflejen la conducta criminal descrita al inicio del enunciado**. Además, el informe debe detallar cualquier otra evidencia que el analista pueda considerar relevante (por ejemplo, indicios de otra actividad criminal distinta de la que inició el caso).

Es importante que todas las evidencias recogidas en el informe pericial se encuentren adecuadamente descritas: nombre del archivo, localización, mactime del archivo, bytes que ocupa, valor hash, así como cualquier otro atributo característico que el analista pueda considerar de interés. Si las evidencias localizadas se encuentran en el espacio no asignado del disco duro (o en el file slack de un fichero, por ejemplo), tienen que ser cuidadosamente descritas (a criterio del analista), y extraídas en un formato visible para su traslado al informe pericial. Asimismo, es interesante que el informe pericial refleje la cronología de los sucesos y ordene y relacione, en caso que sea posible, todas las evidencias digitales que se hayan podido localizar.

Finalmente, también debes reflejar aquellas pruebas que has realizado, el resultado de las cuales haya sido negativo.

Si fuera técnicamente posible, y dada la naturaleza delictiva del hecho que se investiga en este ejemplo, es muy relevante que se pueda determinar el origen de las evidencias localizadas, es decir, que se identifique el medio por el cual las evidencias han sido introducidas en el ordenador analizado: un dispositivo USB, un programa de intercambio de archivos, un correo electrónico, etc.

Procedimiento general de análisis

A pesar de que no existe un método general de análisis, una de las posibles metodologías a tener en cuenta es la siguiente:

Recuperación de los archivos borrados

Consiste en realizar una recuperación parcial o total de la información borrada existente en los dispositivos susceptibles de ser analizados. Esta operación incluye los datos localizados en las áreas del disco duro sin asignar, así como una recuperación de los datos de archivos y carpetas "huérfanos", la vinculación de los cuales se ha perdido. Este método de recuperación puede incluir procedimientos de recuperación de archivos basados en *carving*.

Estudio del sistema operativo

En cuanto al estudio del sistema operativo, a nivel muy básico, se podrían efectuar las comprobaciones siguientes:

- Identificación del sistema operativo del equipo y localización de la partición que lo aloja.
- Identificación de la fecha de instalación del sistema.
- Identificación de los distintos usuarios.
- Última fecha de acceso al equipo (para cada usuario).
- Identificación de los dispositivos hardware y software reconocidos por el sistema.
- …

Cada analista deberá decidir, según el caso, aquellas pruebas que debe practicar necesariamente y aquellas que, quizás, no sean relevantes.

Estudio de la seguridad

En esta etapa, el objetivo consistirá en estudiar si las evidencias analizadas han sido comprometidas (o incluso añadidas deliberadamente con el fin de

perjudicar una persona). En definitiva, se deberá identificar cualquier aplicación vulnerable (versiones antiguas), software malicioso (virus, troyano, etc.), evaluar el daño sufrido, identificar los archivos que han sido comprometidos (eliminados, modificados, etc.), así como determinar la vía de acceso al sistema.

Análisis detallado de las evidencias digitales

Sin ánimo de ser demasiado exhaustivos, el análisis detallado de las evidencias podría incluir los apartados siguientes, algunos de los cuales ya han sido tratados en los apartados anteriores:

- Información relativa al sistema analizado: hardware instalado y reconocido por el sistema operativo, fecha, hora y usuario que utilizó el sistema por última vez.
- Estudio de los dispositivos físicos que en algún momento fueron conectados al sistema estudiado: móviles, USBs, impresoras, escáneres, cámaras, tarjetas de memoria, etc.
- Estudio del escritorio y de la papelera de reciclaje.
- Conexiones de red, identificación de la MAC y direcciones IP.
- Estudio del registro del sistema y *logs* de auditoría del sistema operativo y de las aplicaciones instaladas (en caso de que dichas aplicaciones dispongan de *logs*).
- Estudio de la información contenida en los *unallocated cluster* o en el *file slack*.
- Información contenida en los archivos de hibernación, paginación, particiones y archivos de intercambio (*swap*).
- Análisis de la cola de impresión.
- Visualización de los *links* de los archivos y de los archivos accedidos recientemente.
- Estudio de los directorios de usuario.

- Estudio de las aplicaciones instaladas relacionadas con actividades de programación, grabación y tratamiento de imágenes, procesamiento de audio y video, programas de contabilidad, ofimática, etc.
- Estudio de los metadatos de los archivos, si se considera que pueden ser relevantes para el caso.
- Estudio de las aplicaciones de virtualización.
- Estudio de las bases de datos instaladas y las aplicaciones que permiten su gestión.
- Estudio de los programas de cifrado, particiones cifradas, etc.
- Estudio de la navegación por Internet y de sus históricos y *cookies*.
- Análisis de los clientes de correo electrónico y del *webmail* (suponiendo que el analista disponga de la autorización necesaria).
- Análisis de los registros de mensajería instantánea, chats y contactos.

Algunas de estas operaciones pueden ser difíciles de llevar a cabo si no se dispone del hardware original o de las aplicaciones gestoras de los datos (por ejemplo, programas de grabación de vídeo, de contabilidad, etc.).

Memoria RAM

Además de las evidencias localizadas en el disco duro, necesitas realizar el análisis de la memoria RAM, el cual puedes llevar a cabo con la herramienta *Volatility*.

Estructura de los informes periciales

No existe ningún estándar que determine de forma obligatoria cómo debe de ser un informe pericial. Sin embargo, a modo de ejemplo, puedes consultar la siguiente referencia bibliográfica para definir la estructura de un informe pericial:

La peritación informática. Un enfoque práctico (Xabiel García Pañeda y David Melendi Palacio), Colegio Oficial de Ingenieros en Informática del Principado de Asturias, ISBN: 978-84-612-4594-9.

A continuación, te resumimos algunos ejemplos que aparecen en el capítulo 13 de la obra anterior:

1. **Estructura:** A pesar de que no existe, como ya se ha mencionado, ningún formato estándar, los apartados siguientes suelen aparecer en muchos informes periciales (aunque pueden tener distintos nombres): objeto del peritaje, extensión, antecedentes, fuentes de información y datos de partida, estándares y normas, resolución, conclusión y anexos.

   De todos ellos, los que prácticamente aparecen en cualquier peritaje son los siguientes: antecedentes, objeto del peritaje, resolución y conclusiones.

2. **Objeto del peritaje:** En este apartado aparecen los **extremos** que el informe debe responder. Normalmente, este apartado estará formado por una lista de preguntas claramente definidas, proporcionadas por el tribunal. Los extremos pueden ser muy variables y dependen del tipo de informe. El autor del libro propone algunos ejemplos que os pueden ayudar a entender el contenido de este apartado:

   - “Determinar si la empresa Xuan y Cia. recibe de forma continuada un servicio de conexión a Internet mediante línea ADSL por parte de la empresa TeleCo”.
   - “Comprobar la existencia de un conjunto de páginas Web e indicar el servidor donde se alojan”.
   - “Determinar si la aplicación e-Tienda permite la venda de productos a través de Internet”, etc.

3. **Antecedentes:** En este apartado el perito incluirá una lista con los hechos destacados que se han producido hasta llegar a la realización de la pericial. La lista debe ser descriptiva y en ningún caso debe entrar en valoraciones o interpretaciones (la redacción de la resolución y la conclusión también debe ajustarse a esta regla). En este apartado podemos, por ejemplo, reseñar si la clonación se ha efectuado en presencia de secretario judicial, introducir el contexto del caso, la cronología, etc. El autor del libro expone, en este apartado, los ejemplos siguientes:

   - "La empresa Fonticiella contrata una línea ADSL con la empresa TeleCo el 10/11/2002, tal y como se desprende del contrato fotocopiado y presentado como Anexo III del presente informe".
   - "La empresa Fonticiella considera que TeleCo no proporciona correctamente el servicio de acceso a Internet mediante línea ADSL y contacta con el Colegio Oficial de Ingenieros en Informática de Extremadura para solicitar la asistencia de un Perito".
   - "Dicho colegio designa a Antón García para la realización del siguiente informe pericial".

4. **Fuentes de información y datos de partida:** En este apartado se indican las fuentes de información que serán utilizadas para realizar el informe pericial.

   Es decir, se especificará de dónde se ha extraído la información que se ha de utilizar para generar las conclusiones. Este apartado es muy importante porque si el informe se realiza a partir de unas fuentes manipuladas u obtenidas sin ningún tipo de garantía procesal, la prueba puede quedar invalidada, aunque el trabajo realizado en el informe sega técnicamente perfecto.

   Ejemplos:

   - "Información contenida en el disco duro marca SEAGATE de 80 MB con número de serie XXX, del ordenador denominado TA21, en fecha del 15 de Marzo de 2005".

- "Aplicación Tele-pollo extraída del servidor xx el día 15 de Marzo de 2005. Compuesta por los siguientes ficheros: d.php, dr.php, etc.".

5. **Estándares y normas:** En este apartado se indican todos los estándares o normas que se utilizarán para realizar el informe. Ejemplo:

   - **"**Para la extracción de la información de la tarjeta SIM se ha seguido la guía definida a tal efecto por el NIST (ref. XXX)".

6. **Limitaciones:** En este apartado se definen las limitaciones del dictamen pericial: qué elementos no han sido analizados, por qué no se han llevado a cabo determinadas actuaciones (por ejemplo, por no disponer de autorización judicial).

7. **Resolución o informe pericial:** En este apartado se indicará el proceso a seguir para responder las preguntas (o extremos) planteados como objeto de la pericial. Para facilitar la comprensión del informe, es interesante añadir glosarios o notas técnicas a pie de página, fotografías y capturas de pantalla (sólo aquellas que sean estrictamente necesarias).

8. **Conclusiones:** Es el apartado principal del informe. No deberían ser demasiado extensas y deben redactarse de forma no excesivamente técnica, aunque rigurosa a la vez. Deben extraerse a partir del apartado anterior y no deben contener opiniones ni valoraciones. Tampoco deben ser una copia literal de los apartados anteriores.

9. **Anexos:** Ya descritos en el apartado relativo al análisis forense (en este mismo documento).

Nota: **Propiedad intelectual**

A menudo es inevitable, al producir una obra multimedia, hacer uso de recursos creados por terceras personas. Es por tanto comprensible hacerlo en el marco de un trabajo final de máster, siempre y esto se documente claramente y no suponga plagio en dicho trabajo.

or lo tanto, al presentar un trabajo que haga uso de recursos ajenos, se presentará junto con él un documento en el que se detallen todos ellos, especificando el nombre de cada recurso, su autor, el lugar donde se obtuvo y el su estatus legal: si la obra está protegida por copyright o se acoge a alguna otra licencia de uso (reative ommons, , ...). El estudiante deberá asegurarse de que la licencia que sea no impide específicamente su uso en el marco del trabajo. En caso de no encontrar la información correspondiente deberá asumir que la obra está protegida por copyright.

Deberán, además, adjuntar los archivos originales cuando las obras utilizadas sean digitales, y su código fuente si corresponde.