SAD - U1.3 Análisis Forense

Descargar estos apuntes

Índice

1. Análisis forense de sistemas informáticos
   - 1.1 Objetivos de la informática forense
   - 1.2. Proceso de análisis forense
   - 1.3. Herramientas de análisis forense
   - C.A.I.N.E.
   - Perito informático
   - Resumen

1. Análisis forense de sistemas informáticos

¿Qué ocurre cuando todas las medidas de seguridad que hemos puesto en nuestros sistemas no han sido suficientes y se ha producido un incidente de seguridad? En ese caso, es necesario llevar a cabo un análisis forense de los sistemas informáticos para determinar qué ha ocurrido y cómo se ha producido el incidente.

La informática forense es una disciplina que se encarga de la recuperación, preservación, análisis y presentación de datos almacenados en dispositivos electrónicos con el fin de ser utilizados como pruebas en un proceso judicial. La informática forense se aplica en casos de fraude, espionaje, robo de información, sabotaje, etc.

1.1 Objetivos de la informática forense

Los objetivos de la informática forense son los siguientes:

- **Recuperación de datos**: recuperar datos almacenados en dispositivos electrónicos.
- **Preservación de la evidencia**: preservar la evidencia digital para que pueda ser utilizada en un proceso judicial.
- **Análisis de la evidencia**: analizar la evidencia digital para identificar a los responsables de un delito informático.
- **Presentación de la evidencia**: presentar la evidencia digital en un proceso judicial.

1.2. Proceso de análisis forense

El proceso de análisis forense consta de las siguientes fases:

1. **Identificación del incidente**: en esta fase se identifica el incidente de seguridad que ha ocurrido. Por ejemplo, un ataque de denegación de servicio, un robo de información, etc. Se realiza una entrevista con los afectados para recabar información sobre el incidente.
2. **Recopilación de evidencias**: en esta fase se recopilan las evidencias digitales que permitirán determinar qué ha ocurrido. Las evidencias digitales pueden ser correos electrónicos, logs de sistemas, registros de acceso, historial del navegador, listados de vulnerabilidades, etc.
   En este paso **se duplican o clonan los dispositivos** para trabajar con las copias y no con los originales. Además se establece una **cadena de custodia para garantizar la integridad** de las evidencias digitales.

3. **Análisis de las evidencias**: en esta fase se analizan las evidencias digitales recopiladas para determinar qué ha ocurrido. Por ejemplo, se analizan los logs de sistemas para determinar si ha habido un acceso no autorizado a un sistema.
4. **Presentación de las evidencias**: en esta fase se presentan las evidencias digitales recopiladas y analizadas en un informe forense que será utilizado en un proceso judicial. El informe debe ser redactado de forma clara y concisa para que pueda ser entendido por un juez o un jurado. Debe usar un lenguaje técnico pero comprensible para un no técnico, añadiendo un glossary con los términos técnicos utilizados.

> ⚠ **Vulnerabilidades**
>
> Las vulnerabilidades usadas por los atacantes, si están identificadas, aparecen en listados de vulnerabilidades que se actualizan periódicamente. Estos listados son públicos y se pueden consultar en Internet.
>
> - CVE
> - INCIBE

1.3. Herramientas de análisis forense

Las herramientas utilizadas en análisis forense de sistemas informáticos abarcan desde herramientas de recuperación de datos hasta herramientas de análisis de logs de sistemas. Algunas de las herramientas más utilizadas son:

- Computer Aided Investigative Environment (CAINE): es una distribución de Linux que incluye herramientas de análisis forense.
- The Sleuth Kit es una colección de herramientas de análisis forense que permite recuperar y analizar datos almacenados en dispositivos electrónicos.
- Kali Linux es una distribución de Linux que incluye herramientas de análisis forenses y de seguridad informática.
- Forensics Wiki: es una wiki que contiene información sobre herramientas de análisis forense y técnicas de análisis forense.

> ⚠ **Pentesting vs Forensics**
>
> No confundir el análisis forense con el pentesting. El pentesting es una técnica de seguridad informática que consiste en simular un ataque informático para identificar vulnerabilidades en un sistema. El análisis forense, en cambio, consiste en analizar un sistema después de que ha ocurrido un incidente de seguridad para determinar qué ha ocurrido.
> Algunas herramientas de pentesting también pueden ser utilizadas en análisis forense, pero no todas las herramientas de pentesting son adecuadas para análisis forense. Este es el caso de Kali Linux, que es una distribución de Linux que incluye herramientas de pentesting y de análisis forense.

C.A.I.N.E.

CAINE (Computer Aided Investigative Environment) es una distribución de Linux que incluye herramientas de análisis forense. CAINE es una distribución de Linux basada en Ubuntu que incluye herramientas de análisis forense, como The Sleuth Kit, Autopsy, etc.

Dentro de las herramientas que proporciona CAINE, se encuentran las herramientas de adquisición de datos, como dd, dcfldd, etc., que permiten realizar una copia de un dispositivo de almacenamiento. Estas herramientas permiten realizar una

copia exacta de un dispositivo de almacenamiento para trabajar con la copia y no con el original.

Para hacer la copia el dispositivo de almacenamiento se monta en modo de solo lectura para evitar que se modifiquen los datos originales. La copia se realiza con una herramienta de adquisición de datos. Tenemos herramientas de consola como dd, dcfldd aunque también tenemos herramientas gráficas como Guymager o FTK-Imager.

Aquí tenemos un tutorial de cómo realizar una adquisición de imagen con CAINE

Autopsy

Autopsy es una herramienta de análisis forense que permite recuperar y analizar datos almacenados en dispositivos electrónicos. Autopsy es una interfaz gráfica para The Sleuth Kit que facilita la recuperación y el análisis de datos almacenados en dispositivos.

Autopsy permite recuperar y analizar datos almacenados en dispositivos electrónicos, como discos duros, memorias USB, tarjetas de memoria, etc. Autopsy permite recuperar y analizar datos eliminados, buscar archivos por palabras clave, analizar logs de sistemas, etc.

Dentro de las fases de análisis forense, Autopsy se utiliza en la fase de análisis (fase 3) de las evidencias digitales. Autopsy permite analizar los datos recuperados para determinar qué ha ocurrido y quién es el responsable de un delito informático. Además, nos permite generar un informe forense que será utilizado en un proceso judicial.

Puedes ver un breve tutorial de Autopsy

Perito informático

El perito informático es un profesional especializado en informática forense que se encarga de realizar análisis forenses de sistemas informáticos. El perito informático es un profesional con conocimientos técnicos y legales que se encarga de recuperar, preservar, analizar y presentar evidencias digitales en un proceso judicial.

El perito informático debe ser imparcial y objetivo en su análisis forense. El perito informático debe seguir un protocolo de actuación para garantizar la integridad de las evidencias digitales y la validez del informe forense.

El perito informático puede ser contratado por una empresa, un particular o un organismo público para realizar un análisis forense de sistemas informáticos. El perito informático puede ser llamado a declarar como testigo en un proceso judicial para explicar su informe forense y responder a las preguntas de las partes.

Perito informático

Resumen

INCIBE: Forense en Windows

Descubriendo evidencias

Caso práctico 1. Encontrar imágenes ocultas en un disco duro.

En la imagen de disco 8-jpeg-search se pueden descubrir evidencias ocultas en las imágenes digitales.

Por ejemplo, se pueden descubrir metadatos en las imágenes digitales que indiquen la fecha y la hora en que se tomó la foto, la ubicación geográfica en la que se tomó la foto, etc.

Pero no solo es eso, vemos como con ayuda de una herramienta de análisis forense como Autopsy se pueden descubrir imágenes ocultas en un archivo comprimido, imágenes que fueron eliminadas del sistema, o incluso imágenes dentro de documentos.

La búsqueda de evidencias digitales en un sistema informático puede ser una tarea compleja y laboriosa, pero con las herramientas adecuadas se pueden descubrir evidencias ocultas que permitan determinar qué ha ocurrido y quién es el responsable de un delito informático.

Hay muchos indicadores, como los `magic numbers` que nos pueden dar pistas de la existencia de archivos ocultos o de la existencia de archivos que han sido modificados.

Magic numbers

Para esa imagen de disco, completa la siguiente tabla indicando donde se ha encontrado cada tipo de archivo y qué modificación u ocultación se ha realizado sobre el mismo.

#	Archivo (Ubicación)	Modificación
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		