SAD - U1.3 Análisis Forense

Descargar estos apuntes

Índice

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.

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.

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.