Metodología básica de análisis forense

Identificación

En esta fase inicial, se realiza una evaluación exhaustiva de los recursos disponibles, el alcance del incidente y los objetivos necesarios para llevar a cabo la investigación interna. Algunas acciones clave incluyen:

- Obtener autorización por escrito para iniciar la investigación forense, junto con acuerdos de confidencialidad.
- Documentar detalladamente todas las acciones, antecedentes y decisiones relevantes que preceden al incidente y su respuesta.
- Organizar y definir un equipo de investigación, estableciendo límites, funciones y responsabilidades claras.
- Realizar una investigación preliminar para comprender completamente la situación actual del incidente, identificando partes afectadas, posibles sospechosos y la gravedad de la situación.
- Identificar el impacto y la sensibilidad de la información comprometida, así como analizar el impacto en los negocios.

El producto final de esta etapa debe ser un documento detallado que sirva como punto de partida para la adquisición de datos y la elaboración del informe final. Además, se inicia la cadena de custodia y se completa la documentación correspondiente.

Adquisición

En esta segunda fase, se ejecutan los pasos necesarios para adquirir la evidencia de forma segura y sin alterarla. Algunas acciones importantes son:

- Definir los equipos y herramientas necesarios para la investigación y establecer un entorno de trabajo adecuado.
- Iniciar una bitácora para documentar con precisión todas las acciones realizadas durante la adquisición de datos.
- Recopilar información de sistemas vivos, como caché del sistema, archivos temporales y registros de eventos.
- Realizar copias bit a bit de los dispositivos comprometidos utilizando herramientas adecuadas, y firmar su contenido con hash MD5 o SHA1 para garantizar la autenticidad de los datos.
- Documentar la evidencia con el embalaje correspondiente y mantenerla protegida física y digitalmente.

Es fundamental seguir buenas prácticas para conservar la integridad de la información y la evidencia, asegurando que sea auténtica, correcta, completa y convincente para su eventual uso legal.

Análisis de datos

En esta fase, se lleva a cabo el análisis detallado de los datos adquiridos, centrándose en tres áreas principales:

- Análisis de datos de la red: Identificación de dispositivos de comunicación y defensa perimetral en la red, recuperación de logs y registros relevantes.
- Análisis de datos del host: Lectura de aplicaciones y sistemas operativos, recuperación de archivos de la evidencia, definición de criterios de búsqueda y

comparación de hashes.

- Análisis de medios de almacenamiento: Definición de criterios de búsqueda, descompresión de archivos, creación de estructura de directorios y recuperación de archivos objetivo.