Aplicación de metodologías de análisis forenses (Análisis forense informático)

El análisis forense también se denomina ciencia forense informática. Cuando se trata de la seguridad de la información, se refiere a la aplicación de herramientas de investigación y técnicas de análisis para recolectar evidencia a partir de recursos informáticos a fin de determinar la causa del riesgo de los datos.

Identificación de los dispositivos a analizar

Todos los dispositivos que puedan aportar información sobre lo ocurrido deben ser analizados, los routers, proxys, firewalls, móviles, ordenadores, etc.

Recolección de evidencias (trabajar un escenario)

Las pruebas necesarias para esclarecer lo que ha ocurrido serán recabadas con sumo cuidado y realizando operaciones de integridad para cada prueba.

Ejemplos

Comprobar integridad

- https://www.jesusninoc.com/02/04/integridad/

Analizar DLL

- https://www.jesusninoc.com/11/29/mostrar-los-procesos-que-estan-ejecutando-una-dll-de-un-listado-de-dlls-con-powershell/
- https://www.jesusninoc.com/02/01/explicacion-sobre-el-uso-de-funciones-que-estan-en-dll-del-sistema-operativo-en-powershell/

Volcado de memoria

- https://www.jesusninoc.com/10/14/crear-un-fichero-de-volcado-de-memoria-de-un-proceso-de-forma-grafica/
- https://www.jesusninoc.com/03/04/crear-un-fichero-de-volcado-de-memoria-de-un-proceso/
- https://www.jesusninoc.com/03/13/buscar-una-cadena-dentro-de-un-fichero-de-volcado-de-memoria/
- https://www.jesusninoc.com/09/12/crear-un-fichero-de-volcado-de-memoria-de-un-proceso-y-buscar-una-cadena/
- https://www.jesusninoc.com/09/14/realizar-un-volcado-de-memoria-de-un-proceso-cuando-se-empieza-a-ejecutar/
- https://www.jesusninoc.com/10/22/crear-un-fichero-de-volcado-de-memoria-de-un-proceso-y-detectar-dll/

Extraer imágenes de volcado de memoria

- https://www.jesusninoc.com/10/01/jpegextractor/
- https://www.jesusninoc.com/10/15/extract-all-the-jpgs-found-in-chrome-dmp-dump-file/

Coordenadas GPS en imágenes

- https://www.jesusninoc.com/01/01/extraer-coordenadas-gps-de-imagenes-con-powershell/

Más información

- https://www.jesusninoc.com/03/24/ver-informacion-en-el-registro-de-windows-sobre-los-fabricantes-de-software-

instalado/
- https://www.jesusninoc.com/11/10/searching-teamviewer-system/
- https://www.jesusninoc.com/03/23/ver-informacion-en-el-registro-de-windows-sobre-las-variables-de-entorno/

Análisis de la línea de tiempo (TimeStamp)

A medida que se va realizando el análisis de los elementos que han intervenido en el caso se van colocando en una línea temporal.

Análisis de volatilidad – Extracción de información (Volatility)

La información que desaparece en poco tiempo hay que almacenarla inmediatamente, por ejemplo la situación actual de ejecución de los procesos en el sistema o la información que reside en la memoria RAM.

Más información

- https://www.jesusninoc.com/03/13/buscar-una-cadena-dentro-de-un-fichero-de-volcado-de-memoria/
- https://www.jesusninoc.com/05/16/the-volatility-framework/

Análisis de Logs, herramientas más usadas

Los registro, logs o historial de log para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular. De esta forma constituye una evidencia del comportamiento del sistema.

Más información

- https://www.jesusninoc.com/04/30/acceso-al-cmd-exe-mediante-vulnerabilidad-lfi/
- https://www.jesusninoc.com/logs/
