PRÁCTICA 2: Análisis avanzado con Volatility

En esta práctica, aprenderás a utilizar las funcionalidades básicas de Volatility para analizar volcados de memoria. Volatility es una herramienta poderosa para el análisis de memoria que permite identificar procesos, conexiones de red, información del registro de Windows, archivos abiertos, y más**.** Durante esta actividad, trabajarás con un volcado de memoria real y deberás emplear diversos plugins y modificadores de comando para resolver las 16 cuestiones planteadas.

A continuación, se describen los pasos necesarios:

1. Determina el perfil del sistema operativo correspondiente al volcado de memoria.
2. Utiliza los plugins adecuados para extraer la información solicitada.
3. Aplica modificadores de comando para filtrar y organizar los resultados.

Al final de la práctica, deberás ser capaz de identificar procesos activos, claves del registro, conexiones de red, y otros artefactos relevantes.

Requisitos

1. Asegurate de tener instalado Volatility 2.x o Volatility 3.
2. Descarga el volcado de memoria asignado para esta práctica.
3. Documenta los comandos utilizados para resolver cada una de las preguntas.

Entrega un informe detallado con las respuestas a las 16 preguntas, acompañado de capturas de pantalla de los comandos y resultados obtenidos.

Cuestiones

1. Determina el perfil del sistema operativo Utiliza el volcado de memoria para identificar el perfil del sistema operativo compatible con este volcado.

2. Procesos en ejecución ¿Cuántos procesos estaban activos en el sistema en el momento de la captura de memoria?

3. Proceso padre ¿Cuál es el PID del proceso padre del programa 7zFM.exe?

4. Registro de Windows Determina cuántos hives de registro están presentes en el volcado de memoria. Esta información es clave porque hay sospechas de que el sistema está infectado.

5. Claves del registro ¿Cuántas claves de registro existen en la raíz del hive SYSTEM, incluyendo las claves volátiles?

6. Clave ImagePath Identifica el valor de ImagePath en la clave: `ControlSet001\services\Smb`

7. Contraseña de usuario Recupera la contraseña de inicio de sesión del usuario Admin.

8. Conexiones externas Determina cuántas conexiones hacia direcciones IP externas estaban establecidas en el momento de la captura.

9. Estructuras FILE_OBJECT ¿Cuántas estructuras FILE_OBJECT aparecen en la memoria?

10. Fichero comprimido Uno de los ficheros abiertos está comprimido con 7z. ¿Qué nombre por defecto asigna Volatility al exportarlo como .dat?

11. Ruta del fichero ¿Cuál es la ruta en disco del fichero comprimido 7z, tal como la muestra el plugin filescan?

12. Fecha de creación del fichero ¿Cuándo se creó el fichero comprimido? Formato esperado: `DD/MM/YYYY`

13. Website visitada Encuentra la dirección de una web sobre ciencia visitada mediante Firefox. Formato esperado: `https://xxxxxxx.xx`

14. Fecha y hora de la visita ¿Cuándo se visitó la web mencionada en la pregunta anterior? Formato esperado: `DD/MM/AAAA HH:MM:SS` (UTC)

15. Bloc de notas El bloc de notas contenía una contraseña que queremos recuperar. ¿Puedes identificarla? Pista: el usuario reutiliza parte de sus contraseñas.

16. Fichero cifrado Analiza el contenido del fichero comprimido y cifrado en formato 7z. ¿Qué contiene?