INSTITUTO NACIONAL DE CIBERSEGURIDAD

RETOS DESCARGABLES

DIFICULTAD: INTERMEDIA

RETO: APRENDIENDO FORENSE DE MEMORIA

CATEGORÍA: FORENSE

Contenido

ENUNCIADO

El objetivo es adquirir un documento PDF que se encontraba abierto en el momento de adquisición de memoria RAM. Para ello, se tendrá que analizar la memoria RAM mediante herramienta de volcado de memoria, en nuestro caso utilizaremos la herramienta Volatility3, y posteriormente adquirir dicho fichero.

PREPARACIÓN DEL ENTORNO

El primer paso es asegurarse de que todos los paquetes necesarios estén instalados y que el sistema esté actualizado.

Comando: Actualizar los paquetes

Para asegurarnos de que el sistema esté completamente actualizado y que tengamos las dependencias necesarias, podemos ejecutar el siguiente comando:

$ sudo apt update

Actualizar el sistema garantiza que tienes las versiones más recientes de las herramientas y las bibliotecas necesarias para ejecutar Volatility3 y otros componentes del sistema. Aunque este paso es opcional, es altamente recomendado para evitar errores durante el análisis.

Instalación de herramientas necesarias

Como hemos comentado, utilizaremos la herramienta volatility3 que podemos descargar desde su repositorio GitHub.

También utilizaremos *foremost*, por lo que deberemos de asegurarnos de tenerlo instalado en nuestro sistema operativo Linux.

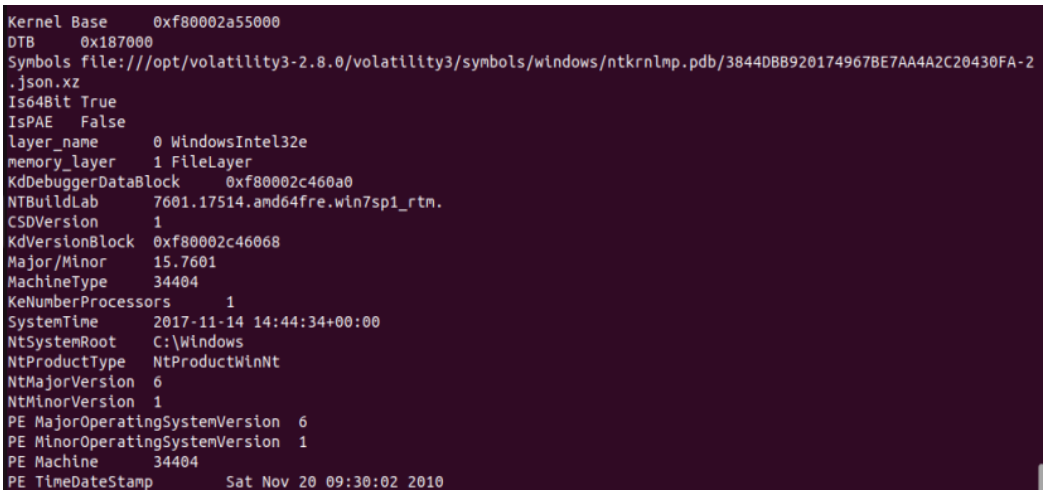
Resolución del reto

Comando: Obtener información del sistema

El siguiente paso consiste en obtener información básica sobre el sistema operativo que está presente en el volcado de memoria. Esto es crucial para entender el contexto del volcado de memoria y garantizar que los siguientes comandos se ejecuten en el contexto adecuado.

$ vol.py -f dump.mem windows.info.Info

- **Explicación del comando:**
    - *-f dump.mem:* Especifica el archivo de volcado de memoria que estamos analizando (en este caso, dump.mem).
    - *windows.info.Info:* Es un plugin de Volatility3 que extrae detalles sobre el sistema operativo desde la memoria volcada. Esta información incluye detalles como la versión del sistema operativo, la arquitectura, las fechas relevantes, etc.



Obtener esta información es vital para contextualizar el análisis. Nos permite saber detalles como la versión de Windows y la arquitectura (32-bit o 64-bit), lo cual puede afectar cómo se analizan otros aspectos de la memoria. También garantiza que estemos analizando la memoria de acuerdo con el sistema adecuado.

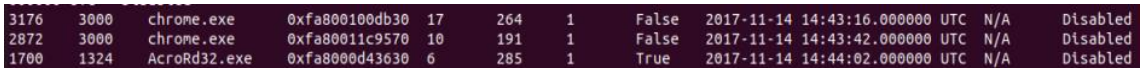
Comando: Listado de procesos

Ahora que tenemos una visión general del sistema, el siguiente paso es identificar qué procesos estaban activos en la memoria en el momento en que se tomó el volcado. Esto nos ayudará a identificar el proceso que probablemente estaba utilizando el archivo PDF que queremos recuperar.

$ vol.py -f dump.mem windows.pslist.PsList

- **Explicación del comando:**
  - *-f dump.mem:* Especifica el archivo de volcado de memoria.
  - *windows.pslist.PsList:* Este plugin de Volatility3 lista todos los procesos activos en el sistema al momento de la captura de la memoria.

Este comando es esencial para identificar el proceso o los procesos que estaban en ejecución en el sistema en el momento del volcado. En nuestro caso, buscaremos un proceso relacionado con un visor de PDF (por ejemplo, Acrobat Reader, SumatraPDF, o un navegador que estaba visualizando el PDF).



3176	3000	chrome.exe	0xfa800100db30	17	264	1	False	2017-11-14 14:43:16.000000 UTC	N/A	Disabled
2872	3000	chrome.exe	0xfa80011c9570	10	191	1	False	2017-11-14 14:43:42.000000 UTC	N/A	Disabled
1700	1324	AcroRd32.exe	0xfa8000d43630	6	285	1	True	2017-11-14 14:44:02.000000 UTC	N/A	Disabled

La salida de este comando incluye detalles como el **PID** (Identificador del Proceso), el nombre del proceso, y el estado del proceso, lo que nos permitirá encontrar el proceso que estaba utilizando el archivo PDF.

- **Identificar el PID:** Una vez que tengamos la lista de procesos, identificamos el PID correspondiente al proceso que estaba abriendo el PDF. Este es el PID que utilizaremos en el siguiente paso.

Comando: Volcar la memoria del proceso

Una vez que hemos identificado el proceso que estaba utilizando el archivo PDF (usando el PID del proceso que encontramos con windows.pslist.PsList), el siguiente paso es volcar la memoria de ese proceso específico.

$ vol.py -f dump.mem -o /opt/ windows.memmap.Memmap --dump -pid 1700

- **Explicación del comando:**
  - *-f dump.mem:* Especifica el archivo de volcado de memoria.
  - *-o /opt/:* La opción -o se utiliza para especificar dónde guardar el volcado de memoria del proceso.
  - *windows.memmap.Memmap:* Este plugin aún se está utilizando para analizar y mapear la memoria.

- *--dump:* Indica que se realizará un volcado de la memoria del proceso.
- *-pid 1700:* El -pid se usa para especificar el PID del proceso a volcar. El PID de interés es el que identificamos en el paso 3.

Volcar la memoria de un proceso específico permite recuperar los datos que se encuentran en la memoria asociada a ese proceso. Si el archivo PDF estaba abierto en ese proceso, es muy probable que esté almacenado en la memoria volcada y, por lo tanto, pueda ser recuperado.

Recuperación del Archivo PDF del Volcado de Memoria

Una vez que has volcado la memoria del proceso utilizando el comando anterior, necesitarás herramientas adicionales para examinar el volcado y extraer el archivo PDF.

Pasos para extraer el archivo PDF:

1. **Utiliza herramientas forenses como Foremost** para buscar archivos en el volcado de memoria. Estas herramientas permiten escanear los volcados en busca de firmas de archivos conocidos.

$ foremost pid.1700.dmp -o /opt/output

```
root@usuario-VirtualBox:/opt/volatility3-2.8.0/output# cd /opt/output/
root@usuario-VirtualBox:/opt/output# ls
audit.txt  bmp  dll  exe  gif  htm  jpg  ole  pdf  png
```

2. **Verifica el archivo extraído**: Después de ejecutar el volcado, verifica los archivos recuperados. Visualizamos que disponemos de un directorio PDF, lo analizamos teniendo en cuenta los permisos.