PRÁCTICA 2: Shadow Copy

Shadow Copy (también conocido como Volume Snapshot Service, Volume Shadow Copy Service o VSS) es una tecnología incluida en Microsoft Windows que permite realizar copias de seguridad manuales o automáticas o instantáneas de archivos o volúmenes de computadora, incluso cuando están en uso.

Se implementa como un servicio de Windows llamado servicio Volume Shadow Copy y requiere que el sistema de archivos sea NTFS para poder crear y almacenar instantáneas: las instantáneas se pueden crear en volúmenes locales y externos mediante cualquier componente de Windows que utilice esta tecnología.

Windows Shadow Volumes puede proporcionar datos adicionales que de otro modo no estarían disponibles. Pueden permitir que un investigador forense recupere archivos eliminados y sepa qué estaba sucediendo en un sistema antes de comenzar la investigación. Son una excelente herramienta para descubrir datos que fueron eliminados previamente por un usuario del sistema.

Aunque las instantáneas pueden proporcionar a los investigadores forenses archivos que han sido eliminados entre el momento en que se realizó la instantánea y el momento en que comenzó la investigación, sólo proporcionan una versión anterior de los archivos.
Si se realizaron cambios previos a los archivos antes de que se creara la instantánea, esos cambios no se conocerán.

Debido a que las instantáneas se clonan a nivel de bloque en lugar de a nivel de archivo, es posible que los cambios en archivos individuales no sean suficientes para hacer que Windows realice los cambios en una instantánea correspondiente.

Además, es posible que el usuario desactive el servicio de instantáneas, por lo que no se almacenarán instantáneas. Otras veces, la configuración del espacio en disco puede estar configurada demasiado baja para que se guarden varias instantáneas, o incluso para que se guarde una instantánea si es más grande de lo que permite la configuración.

Además, Windows sobrescribe automáticamente las instantáneas cuando se alcanza el límite de espacio en disco, por lo que las instantáneas deberían ser una ayuda en una investigación forense, pero no están garantizadas como un medio para descubrir información útil.

Al incorporar VSCs en análisis forenses, hay que considerar las siguientes posibilidades:

- Al usar herramientas como libvshadow, que pueden brindar una representación de Volume Shadow Copy como un volumen lógico, se pueden aplicar herramientas de análisis secundario como log2timeline / Plaso y crear líneas de tiempo masivas que se remontan aún más atrás en la historia. Hay que tener en cuenta que puede tener un exceso de los mismos datos.

- Si se disponen de indicadores para ayudar en el análisis, como malware o períodos de interés, hay observar cómo interactúan sus instantáneas de volumen con estos períodos de tiempo. Es posible que se encuentre en una situación en la que se pueda echar un vistazo al sistema antes de la infección. Además, si hay sospechas de alteración del tiempo, estudiar si sus instantáneas de volumen respaldan esa teoría.

- El hecho de que los datos estén dentro de una instantánea de volumen no significa que las técnicas de análisis tengan que cambiar. Todavía se pueden ejecutar scripts automatizados, archivos hash, realizar búsquedas de palabras clave, etc. Las VSCs son solo otra fuente de datos.

Objetivos principales de la práctica:

- **Activar la tecnología VSC y estudiar cómo acceder a la información tanto en caliente como en post mortem.**

Software a utilizar:

A. Windows 7,8,10 (32 o 64 bits)
B. ShadowCopyView
C. OSFMount, Arsenal Image Mounter o FTK Imager.

Se pide:

1. Instala o re-utiliza una máquina virtual con Windows (A)
2. Agrega un segundo disco duro de igual o mayor tamaño que el utilizado en 1.
3. Activa los puntos de restauración.
4. Crea contenidos en el disco, instala algún programa y ve creando al menos un par de puntos de restauración.
5. Comprueba de que existen varias versiones de las carpetas/ficheros que vayas creando (Equipo -> Menú Contextual en el volumen -> Propiedades -> Versiones anteriores)
6. Realiza una imagen del disco duro (1) en el otro disco que creaste en el punto 2
7. Monta la imagen con alguna de las herramientas (C).
8. Utiliza las herramienta (B), o alguna otra que investigues por la Web, para acceder a la información almacenada en en las shadow copies.