

[illegible]

Cuando en el sistema que pretendemos auditar, no sea preciso salvaguardar la integridad del mismo; por ejemplo máquina vulnerada y arrancada en la que se disponen de procesos cargados en memoria RAM volátil que en caso de apagarse se perderían; recurriremos a herramientas de análisis forense portables desde el sistema arrancado.

En la mitología forense se ha escuchado de todo, desde forenses que en caliente han salvaguardado los registros cargados en memoria RAM en un dispositivo removible, hasta aquellos que rociando la memoria RAM con nitrógeno pretenden salvaguardar los procesos cargados a fines de usarlos en juicio si fuese necesario para salvaguardar las pruebas, es evidente que el primer caso es el normal, el segundo rumurología.

En cualquier caso es evidente que cuando participamos en el uso de la maquina atacada estamos borrando posibles pruebas ya que estamos sobreescribiendo eventos e información, por lo que deberemos ser aún más precisos en el control y transcripción de nuestras acciones a los fines de diferenciar lo que hemos provocado nosotros, de lo que ya existía. Como quiera que sea es evidente que no estamos en el mismo caso que una auditoría en frio, ya que participamos activamente en el sistema auditado.

Para realizar este tipo de auditoría en caliente, es necesario como hemos indicado disponer de otras herramientas que lanzaremos desde la maquina afectada, si bien para documentar nuestro trabajo será necesario que dispongamos de un portatil en el que habremos lanzado nuestra herramienta forense preferiblemente (Autopsy) ya que dispone de una aplicación integrada de catalogación de actividades y acciones emprendidas que nos ayudarán a documentar mejor las tareas forenses emprendidas.

Las herramientas forenses que lanzaremos serán las siguientes:

Dado que pretendemos salvaguardar, aun con nuestra participación activa en la maquina afectada las acciones y actividades previas a nuestro análisis usaremos la herramienta 2TWare Convert de VMWare para virtualizar el disco duro y poderlo emular en nuestro portatil mediante snapshots que permitirán analizar el contenido del mismo, avanzar y retroceder en nuestros cambios según analicemos la copia virtual del disco duro afectado, un proceso lento pero que permite clonar un disco duro y usarlo en una maquina virtual para su analisis independiente.

La FOCA de la empresa ElevenPaths (ex Informatica64 - Chema Alonso) es la herramienta por excelencia usada para revisar metadatos de los ficheros infectados o alterados en el sistema que con frecuencia se ocultan sin participación del usuario, pero que habitualmente si conocen los hackers y crackers que explotan un sistema por lo que salvo que exista poca destreza por parte de los mismos será difícil encontrar metadatos que no hayan sido borrados o modificados a los fines de enmascarar su actividad, aunque como es evidente para alterar, borrar y manipular dichos ficheros algún rastro se quedará, identificarlos es una labor autodidactica de difícil adquisición.



Como indicábamos al principio la memoria RAM que está cargando todos los programas que se ejecutan en el sistema, es lo primero que debemos salvaguardar a la hora de interactuar en un sistema arrancado, programas como FTK Imager, salvaguardarán los datos en un fichero para su posterior análisis, pero como acostumbra a ocurrir existen numerosos programas disponibles para realizar esta labor. De hecho las sysinternals del mismo Sistema Operativo podrían valernos para realizar dicha función, pero como es evidente debemos desconfiar de todas las herramientas instaladas ya que podrían desvirtuar o alterar resultados al pertenecer al sistema comprometido.

Otra herramienta que podemos usar para analizar la RAM es Volatility, precargada en la distribución de seguridad Kali Linux, también puede ser instalada en Windows y Mac

Para recuperar posibles ficheros borrados que ya no observamos a simple vista disponemos igualmente de herramientas como Testdisk y Foremost ambos cumplen su función de recuperación de información en sectores del disco duro alterados o borrados.

Así pues y a modo de pequeño resumen debemos salvaguardar los siguientes datos en un sistema comprometido y que deba ser analizado al estar arrancado.

#### PASOS:

1. Salvaguardar contenido memoria RAM. FTK Imager o Volatility
2. Realizar copia del disco duro, bien virtualizado (2T Ware Convert), bien copia fisica para su montaje (DD en linux).
3. Búsqueda de ficheros borrados mediante herramientas de recuperación Testdisk o Foremost.

4. Análisis de los ficheros instalados y recuperados mediante FOCA y su análisis, verificando propietario, fecha, hora, titulo, alteraciones, etc., respecto a los adyacentes en la misma carpeta (usualmente los ficheros de logs que registran la actividad de los ficheros son alterados para borrar el rastro de intrusión).

Si deseásemos profundizar aún más en el análisis del sistema comprometido podríamos capturar el tráfico entrante y saliente del mismo mediante herramientas como Wireshark que capturan todo el trafico IP o de cualquier otro protocolo para su análisis mediante un procedimiento de volcado.