



¿Por qué debemos crear un dispositivo removible para ejecutar nuestra herramienta de análisis forense?

Los dispositivos removibles son una herramienta de seguridad creados principalmente para poder lanzar distribuciones de análisis forense que se ejecuten en un nivel superior al Sistema Operativo instalado que ha sufrido el incidente de seguridad detectado. Para poder realizar la carga de dicho sistema operativo, debemos poder acceder al ordenador desde la BIOS del mismo. El motivo de dicha acción es esencialmente poder analizar el contenido del mismo sin alterarlo, como base fundamental de nuestro análisis.

Para la realización del dispositivo removible se pueden usar muchos tipos de elementos (pendrive, memorias MMC, memorias SD, discos duros extraíbles, etc.) que dependen en gran medida del dispositivo a analizar, ya que basándonos en el nivel de acceso que nos permita, podremos determinar si es necesario disponer de un pendrive o una simple tarjeta microSD con el Sistema Operativo forense cargado.

Dentro del apartado de distribuciones forenses (Deft, Autopsy, Helix, etc.) podemos encontrar varias que realizan la función de catalogación, salvaguarda y análisis de los elementos detectados. Para realizar nuestro primer pendrive con una distribución de análisis forense debemos contar con una serie de herramientas que nos faciliten la creación del mismo, entre ellos debemos destacar los siguientes:

Hardware:

- Pendrive (tamaño a determinar por el auditor. Cuanto mayor sea su capacidad mejor pues nos permitirá la salvaguarda de la información in-situ sin necesidad de otros dispositivos externos complementarios (discos duros portátiles)).

Software:

- Herramienta de creación de distribuciones integradas RUFUS/Unebootin. Permiten instalar un único Sistema Operativo en el pendrive.
- Herramienta de creación de multiples distribuciones integradas YUMI. Permite crear en único pendrive la instalación de varias distribuciones UNIX / Windows con un cargador de arranque propio (GRUB).
- Descargar una distribución de análisis forense de las detalladas anteriormente. Deft, Autopsy, etc., en formato ISO (imagen)

PROCEDIMIENTO DE CREACION DE PENDRIVE/MEMORIA:

Procedimiento de creación del pendrive:

1. En primer lugar y como ya se ha detallado se debera disponer de un medio removible (pendrive, memoriaSD, etc.) que permita la instalación de un S.O. (Sistema Operativo).
1. Deberemos desde un sistema Windows / Unix / Mac formatear la unidad USB/memoria bajo el sistema de ficheros FAT (YUMI acepta NTFS), aunque si lo deseamos las herramientas de instalación YUMI, Unebootin o Rufus lo harán igualmente al disponer de dicha opción.
2. Elegiremos un nombre para dicho dispositivo por ejemplo "*FORENSE*".
3. Dependiendo de la herramienta que deseemos usar habrá que seleccionar que deseamos crear un pendrive/memoria arrancable para hacerlo accesible desde el arranque de la BIOS.
4. A continuación seleccionaremos la imagen ISO que descargamos anteriormente.
5. Y finalmente pulsaremos Iniciar o Start para comenzar el proceso de instalación de la distribución en el pendrive.

Transcurridos al menos 10 minutos dispondremos ya de una herramienta forense con la que poder trabajar. Es vital verificar que la herramienta forense ha sido correctamente creada por lo que procederemos a reiniciar nuestro PC con el pendrive/memoria introducido en alguno de los puertos USB del mismo. Al reiniciarse el PC (pantalla inicial en negro) pulsaremos alguna de las teclas habituales de acceso a la BIOS (ESC, F1,F12, etc. dependiendo de nuestra BIOS) y accedemos al submenu *boot* allí al detectar la presencia del pendrive nos permitirá seleccionarlo. En caso de tener una memoria UEFI, deberemos desactivarla y seleccionar la opción *CSM Boot* que permite un arranque tradicional sin arranque interactivo. Salvada la configuracion reiniciaremos el cliente y

al detectar el pendrive/memoria arrancará desde el mismo. Iniciandose nuestra herramienta "*FORENSE*".