Práctica 3. Análisis forense de sistemas Linux.

Compilación de herramientas memory dump.

Cuando en nuestra práctica forense nos enfrentemos a un sistema operativo “vivo”, procederemos a extraer todas las evidencias posibles (artefactos) por medio de un script como el que se realizó en la práctica número 1.

Los siguientes pasos a tener en cuenta serían realizar un volcado de memoria y obtener una imagen del disco duro. La imagen del disco duro no presenta mayor dificultad, realizaremos un procedimiento de clonado haciendo uso del comando “dd” similar al que hicimos en las prácticas del tema 2.

En cuanto al volcado de memoria, utilizar la herramientas avml, fmem o LiME no presentan dificultad una vez que disponemos de las herramientas compiladas para la versión del kernel de Linux donde se van a ejecutar.

Objetivo:

- Aprender a compilar las herramientas de volcado de memoria en Linux.

Materiales

- Distribución Debian 10.9.0 de 64 bits con kernel version 4.9.0-16-amd
- Código fuente de las herramientas: fmem, LiME y avml.

Enlaces de interés:

- https://www.dwarmstrong.org/kernel
- https://www.kernel.org/doc/html/v4.10/process/applying-patches.html
- https://stackoverflow.com/questions/34379013/insmod-error-inserting-hello-ko-1-invalid-module-format

Se pide crear una máquina virtual dónde se instalará la distribución mencionada anteriormente (se puede reutilizar la de la práctica 2) y documentar el proceso compilación, a partir del código fuente, de las herramientas de volcado de memoria mencionadas anteriormente.