Práctica 6. Análisis forense de sistemas Linux.

Acceso a imágenes con sistemas de archivos Linux y recuperación de información.

Objetivo:

- Aprender a acceder a las posibles evidencias contenidas en imágenes de disco generadas en sistemas informáticos que ejecutan sistemas operativos Linux.

- Utilización de herramientas de recuperación de archivos borrados: foremost, photorec y scalpel

Materiales

- Distribución Linux Kali Linux.
- Herramientas propias del sistema operativo: mount, losetup, fdisk, etc.
- Herramientas forenses: Sleuthkit, foremost, scalpel y photorec.
- Información de Internet

Una de las tareas más habituales quehacer diario de un profesional forense informático es realizar imágenes forenses de discos duros (teniendo en cuenta todos los requisitos relativos a la cadena de custodia) para posteriormente realizar un análisis de los contenidos del mismo.

En esta situación, se hace imprescindible disponer de destrezas y habilidades para conocer las peculiaridades de los distintos sistemas de archivos que utilizan los SO Linux, para ser capaces de acceder a la información contenida en estas imágenes. Se nos pueden presentar situaciones donde aparezcan configuraciones más sofisticadas, tipo LVM, ZFS o LUKS encrypted, que hagan más difícil el acceso a la información almacenada.

Para la realización de la práctica se requiere que se descarguen las siguientes imágenes:

- Datos, se trata de un dispositivo de disco normal (ext4) donde sería necesario montar las particiones que se identifiquen y aplicar en ellas herramientas para la recuperación de datos borrados (photorec, foremost y scalpel).

- LVM, se trata de un disco que hace uso de volúmenes lógicos. Habrá que dar los pasos necesarios para “desenmascarar” los grupos de volúmenes, y volúmenes lógicos definidos para acceder a su información.

- Cifrado, se trata de un disco cifrado (contraseña “usuario”) con la tecnología propia de Linux (LUKS). Sería necesario acceder a la información que contenga.