Nombre: Alejandro Asenjo

Módulo 4: sistemas seguros de acceso y transmisión de datos

Fecha: 25 de junio de 2014

Reto Forense basado en Linux

1) Preparar el entorno forense a utilizar, físico y lógico (ejemplo clonar el disco duro y llevarlo a nuestro ordenador preparado para realizar el análisis forense)
2) Análisis Forense
3) Estudio de análisis de herramientas que utilizó el intruso.
4) Conclusión final.

Lo primero que debemos hacer es la recogida de datos (tiempos de modificación, accesos y creación)

Ej: Recuperar archivos borrados

Segundo estudiar las evidencias halladas (buscar los agentes causales)

Terceros determinar y realizar el borrador de conclusión.

Utilizamos de guía:

RETO FORENSE

http://www.seguridad.unam.mx/eventos/reto/retov2.dsc

INFORME

http://www.seguridad.unam.mx/eventos/reto/uno_tecnico.pdf

Herramientas:

- Kali Linux
- Sleuthkit
- Tripwire
- Rkhunter
- Autopsy