

Análisis forense en plataformas Linux/Unix

* OBJETIVOS:

Proporcionar a los asistentes conocimientos básicos de análisis forense en plataformas Unix/Linux tanto en parada como en caliente.

* ORIENTADO A:

Responsables de seguridad, consultores, jefes de proyecto y administradores de redes y sistemas.

* REQUISITOS:

Conocimientos de Windows, Networking y Seguridad.

* TEMARIO:

- Localización de la información en Unix.
- Ficheros de log, Ficheros de configuración.
- Herramientas existentes.
- Acotación en el tiempo del proceso de ataque.
- Búsqueda de signos de exploraciones.
- Búsqueda de signos de ataque y de rastros de una intrusión.
- Análisis "en caliente" de una máquina.
- Análisis de los posibles métodos de ataque utilizados.