CURSO DE DFIR Y ANÁLISIS FORENSE EN REDES

Área: General
Modalidad: Presencial
Duración: 19 h
Precio: Consultar

Curso Bonificable
Contactar
Recomendar
Matricularme

OBJETIVOS

Que el alumno aprenda a identificar, adquirir y analizar evidencias forenses tanto en máquina viva como muerta cuyo sistema operativo sea Windows, con la finalidad de identificar la actividad que ha sucedido en la misma, tanto con fines investigativos como probatorios.

CONTENIDOS

Metodología y peritaje
Herramientas de adquisición (triage, WMI y PS) y clonado de evidencias
Captura de memoria
El Registro de Windows
Herramientas de búsqueda activa
Los eventos en Windows
Artifacts: Papelera, Prefetching, USBs, LNKs, Tareas programadas, VSS, Navegadores, Correo electrónico, aplicaciones, ficheros recientes, jumplists,
Malware: características, ocultación, servicios y procesos de Windows, abuso de Svchost, persistencia
Técnicas típicas de persistencia en sistemas
Análisis de Memoria Ram, Técnicas de análisis remota o local, Volatility, volcado de archivos, Credenciales en memoria
Intrusión: Ficheros recientes, Descubrimiento de ataques laterales
Sistemas de ficheros: Interpretación y análisis de sistemas de ficheros NTFS