Curso de DFIR y Análisis Forense en Redes

Área: General
Modalidad: Presencial
Duración: 20 h
Precio: Consultar

Curso Bonificable
Contactar
Recomendar
Matricularme

OBJETIVOS

Que el alumno aprenda a identificar elementos de una red, así como puntos estratégicos de esta que permitan extraer artefactos, elementos y eventos que sirvan para ser analizados ante un incidente de seguridad.

CONTENIDOS

Introducción
Análisis forense de red
Fuentes de evidencia
Metodología OSCAR
Repaso a conceptos de redes
Topologías típicas de red
Conceptos de switching y routing
Ataques de red
Despliegue de infraestructura necesaria
Herramientas de captura de red: Suite Wireshark
TCPFlows: ntop-ng y argus
Despliegue de infraestructura de IDS: snort, suricata, Zeek y Wazuh
Herramientas de monitorización de tráfico
Security Onion
Intercepción, Captura y Análisis de protocolos
Exfiltración de información
Otras fuentes de evidencia: Firewalls, proxies, WAFs
Casos prácticos e instalaciones