WIRESHARK V.2:
DETECCIÓN DE ATAQUES EN RED

Nivel: AVANZADO - **Duración:** 1 día

Este curso está basado en casos prácticos.

Para ello se analizan diferentes traces con problemas de seguridad. El objetivo es analizar, detectar e identificar el tipo de ataque que se está produciendo, quién lo esta realizando y qué medidas correctivas tomar.
Es imprescindible que el asistente tenga conocimientos medio/avanzados en la utilización de Wireshark o en su caso que haya asistido a nuestro curso "Wireshark: Análisis de Protocolos y Redes".
Si no es así, el alumno tendrá dificultades para seguir adecuadamente el desarrollo de este curso.

1. El Wireshark como herramienta de análisis de Seguridad en Redes y Sistemas TCP/IP

- Herramienta de ayuda
- Configuración de disectores para detectar ataques
- Análisis Experto
- Análisis Gráficos
- Análisis Estadísticos
- Generación de ACLs
- Telefonía y VoIP-SIP
- Perfiles de Seguridad

2. Detección y Análisis de Ataques con WireShark

- Detección de scaneos
- Análisis del ICMP
- Detección de IRDP
- Identificación de spoofing IP
- Detección de paquetes malformados
- Detección de ataques de hombre en medio
- Detección de fragmentación IP
- Detección de ataques DoS
- Detección de OS fingerprinting
- Utilización adecuada de la colorización en cada caso

3. Casos Prácticos basados en Traces

A lo largo del curso se verán diferentes traces con ataques de seguridad, con el objeto de que los alumnos se familiaricen en el uso del WireShark para estas labores.

Entre otros se analizan:

- Ataques DoS
- Ataques de hombre en medio
- Robo de stack
- Ataques en entornos Wi-Fi
- Detección de tráficos anómalos