



DETECCION DE INTRUSOS (IDS) Y PREVENCION DE INTRUSIONES (IPS) CON GNU/LINUX (15 H.)

🕒 Descripción del Curso

Este Curso de 15 horas permitirá al participante conocer desde un principio hasta la optimización y creación de reglas avanzadas, todas las bases necesarias para la instalación, configuración y la administración de las herramientas empleadas para la detección de intrusos y prevención de intrusiones en redes empleando GNU/Linux y herramientas de software libre.

🕒 Objetivos

Después de completar el curso, el participante será capaz de:

- Conocer la arquitectura de un IDS/IPS
- Diseñar un sistema IDS/IPS
- Configurar las herramientas de acuerdo a la Política de Seguridad de la empresa
- Configurar las herramientas de informe
- Interpretar los informes de intrusión
- Crear reglas propias para el IDS/IPS

🕒 Perfil

Este curso esta orientado a profesionales que necesiten desempeñar labores de auditoría de seguridad en infraestructura de Internet o de red, en particular a técnicos de seguridad, administradores de redes, arquitectos de infraestructura y profesionales relacionados con el área.

🕒 Prerrequisitos

- Conocimiento básico de los dispositivos de red
- Conocimientos de TCP/IP
- Conocimientos de GNU/Linux
- Alto nivel de comprensión de lectura en inglés

🕒 Materiales entregados

- Presentaciones, documentos y herramientas relevantes con acceso online
- Certificado de Asistencia (para aquellos que asistan a un mínimo del 80%)



⊙ Programación

MODULO	CONTENIDO
Modulo I Arquitectura de SNORT	Módulos Preprocesadores Firmas
Modulo II Modos de Operación	Sniffer Packet logger NIDS Inline
Modulo III Implementación de la solución	Modo IDS Modo IPS Inline Offline
Modulo IV Instalación	Instalación de GNU/Linux Instalación en Microsoft® Windows SNEZ/Snorby
Modulo V Gestión de Eventos	Registro en ficheros Registro en bases de datos
Modulo VI Pruebas de Detección	Ataques con herramientas “manuales” Prácticas de ataques basados en exploits
Modulo VII Informes	Instalación de ACID/BASE Configuración Monitorización
Modulo VIII Firmas	Cabecera de reglas Opciones de reglas Opciones generales
Modulo IX Suricata	Instalación Configuración Snorby

⊙ Modalidad

- Modalidad presencial de Lunes a Jueves.

⊙ Precio

- **Importe total del Curso: 100 Euros** (exento de IVA según Artículo 20, apartado uno, número 9º, de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido)

⊙ Fechas programadas

- Octubre, Noviembre y Diciembre de 2012 en horario de mañanas o tardes. Consultar con el Centro de Formación para más información.