

CURSO **SEGURIDAD EN REDES CORPORATIVAS**

CÓDIGO **SAT - SEGURIDAD**

DURACIÓN 3 Días

OBJETIVOS DEL CURSO

Se cubren aspectos de TCP/IP, servicios Internet en general, herramientas específicas de seguridad, criptografía, sistemas operativos (Unix y Windows NT) y legislación. En principio no se cubren otros sistemas de red (Novell, IBM) ni se hace énfasis en aspectos de desarrollo (programación segura, bases de datos). El curso va acompañado de unas prácticas de ejemplo que complementan lo explicado.

AUDIENCIA

Se trata de una introducción a todos los aspectos de la seguridad de redes, y por su carácter muy general es válido para varios perfiles diferentes: técnicos de sistemas, técnicos de comunicaciones, planificación de proyectos de red, etc.

CURSO

- **Temario:**

El curso está dividido en tres módulos, cada uno de ellos con una duración de un día. Las prácticas se intercalan con la teoría para afianzar los conceptos explicados.

- **Módulo I - Introducción a la seguridad en redes**

Ejercicio práctico: puesta en marcha de un ataque de fuerza bruta contra el fichero de contraseñas del sistema.

1. Introducción

- Motivación de la seguridad

2. Terminología

- Riesgos y amenazas
- Servicios de seguridad

3. Criptografía

- Conceptos criptográficos
- Algoritmos simétricos
- Algoritmos asimétricos
- Firma digital
- Certificados digitales

Ejercicio práctico: ejemplos prácticos de criptografía simétrica y asimétrica con PGP (Pretty Good Privacy) o GNUPG.

4. Criptografía aplicada

- SSL
- HTTPS
- Correo electrónico seguro
- Comercio electrónico y SET
- GSM

Ejercicio práctico: uso de SSH con autenticación con cifrado asimétrico. Redirección de puertos.

5. Técnicas de autenticación

• Módulo II - Seguridad en redes TCP/IP

6. Seguridad en Internet

- Introducción a los protocolos de Internet
- Implicaciones de seguridad en TCP/IP
- IPsec

Ejercicio práctico: utilización de sniffers en redes con switches y posibilidades de sniffers especializados.

7. Servicios de Internet

- Tipos de servicios
- DNS
- DNSSEC

8. El proceso de intrusión

- Obtención de información
- Compromiso del sistema
- Eliminación de rastros
- Comienzo de actividades hostiles

Ejercicio práctico: descubrimiento e investigación de los servicios en red IP: herramientas básicas de TCP/IP y escaneadores automáticos.

Ejercicio práctico: utilización de una puerta trasera sobre ICMP.

- **Módulo III - Gestión de la seguridad**

- **9. Dispositivos de protección**

- Cortafuegos
- Sistemas de detección de intrusos
- Sistemas de prevención de intrusos
- Gestión y monitorización

- **10. Diseño de redes seguras**

- **11. Bastionado de los sistemas**

- Fundamentos
- Routers
- SS.OO.
- Servicios

Ejemplo práctico: recuperación de información de un servidor X mal configurado.

- **12. Seguridad en los puestos de trabajo**

- Correo electrónico
- WWW
- Mensajería instantánea
- Cortafuegos personales

- **13. Desarrollo de aplicaciones**

- **14. Aspectos administrativos**

- Participantes
- Análisis de riesgos
- Política de seguridad

- **15. Aspectos legales**

- Criptografía
- Delitos informáticos
- LOPD

- **Entorno de prácticas**

Cada puesto de trabajo consta de un PC con Windows 2000 y Linux, que se arrancan en distintos momentos dependiendo del ejercicio que a desarrollar. Se dispone también de switches, routers y servidores con varios sistemas operativos para demostrar los problemas presentes en todos ellos, y de cortafuegos e IDS para demostrar el funcionamiento de las medidas de protección frente a ciertos ataques. Durante uno de los ejercicios los asistentes deben descubrir y estudiar los sistemas presentes en la maqueta.

REQUISITOS

Se parte de conceptos básicos y se llega a un nivel bastante avanzado en poco tiempo. Una cierta base de conocimientos sobre TCP/IP y sistemas operativos es altamente recomendable, si bien no resulta imprescindible. No se requieren conocimientos previos sobre temas de seguridad, ni experiencia práctica más allá del nivel de usuario.