



Curso de doctorado Seguridad en Redes de Ordenadores

Jose María Sierra
Rafael Palacios
Joaquín Torres

Programa

- TEMA 1 Introducción a la seguridad en las redes e Internet
 - Ataques y vulnerabilidades de los sistemas y redes
 - Mecanismos básicos de protección: Autenticación, control de accesos, criptografía, firma digital, etc.
- TEMA 2 La criptografía para la protección de comunicaciones
 - Introducción a las bases de la criptografía.
 - Técnicas criptográficas para la protección de comunicaciones
 - Firma digital y certificados de clave pública. Infraestructuras de clave pública.
- TEMA 3 Seguridad en Redes Internas
 - Seguridad en topologías de red interna
 - Mecanismos de protección de las redes internas
 - Herramientas de análisis de red y software malicioso
 - Administración de la seguridad
- TEMA 4 Seguridad en Internet y redes corporativas
 - Fundamentos de Internet e implicaciones de seguridad
 - Fundamentos y ubicación de los cortafuegos
 - Establecimiento de redes privadas virtuales e IPv6

Programa

- TEMA 6 Fundamentos de las Redes Privadas Virtuales RPV (IPSEC)
- TEMA 7 Despliegue de una RPV con PGPNET
- TEMA 8 Seguridad en protocolos de Transporte (SSL/TLS)
- TEMA 9 Despliegue de un tunel SSL con Stunnel
- TEMA 10 Protocolos DNS Seguros (DNSSEC)
- TEMA 11 Seguridad en Servidores WEB (HTTPS)
- TEMA 12 Vulnerabilidades de los Servidores WEB
- TEMA 13 Despliegue de un servidor WEB seguro
- TEMA 14 Protocolos de Seguridad en Comercio Electrónico
- TEMA 15 Comercio electrónico basado en Infraestructuras de Clave pública (PKI)

Sistema de evaluación

- Asistencia a clase
- Trabajo desarrollado durante el curso (paper)
- Presentación del trabajo.

Horario

- Clases de teoría
 - Lunes de 15 a 17 Aula 405
- Clases de prácticas
 - Aula 601 (Laboratorio de comunicaciones)