Seguridad práctica en redes.
Cód. B15

DIRECTOR:

Dr. D. Luis Javier García Villalba.

ESCUELA EN LA QUE SE INSCRIBE EL CURSO:

Escuela de Ciencia Experimentales.

HORARIO DEL CURSO:

Mañanas de 9:00 a 14:00 horas, de lunes a viernes.

NÚMERO DE ALUMNOS:

20.

PERFIL DEL ALUMNO:

Este curso está dirigido a las personas que tengan la responsabilidad de implementar, diseñar, administrar o gestionar entornos y sistemas informáticos y redes de comunicaciones (administradores de sistemas y redes, personal encargado de sistemas de seguridad, responsables de sistemas de gestión de información y administradores y personal encargado de la edición de páginas Web). También está dirigido a estudiantes de últimos cursos que deseen profundizar sus conocimientos en el Área de la Seguridad Informática. No es necesario poseer conocimientos avanzados sobre tecnologías de seguridad. Basta con estar familiarizado con los servicios de Internet: correo electrónico, WWW, etc., y tener ciertos conocimientos (no excesivamente avanzados) sobre sistemas operativos y programación (C++ o Java preferentemente). El resto de materias serán tratadas de forma autocontenida a lo largo del curso. Consecuentemente, el curso está especialmente dirigido a estudiantes de últimos cursos de ciertas Ingenierías (Informática, Telecomunicaciones, Electrónica, Industrial, Aeronáutica, Naval), de Arquitectura y de ciertas Licenciaturas en Ciencias tales como Matemáticas, Físicas, Estadística, etc.

OBJETIVOS:

El objetivo fundamental de este curso es el de formar especialistas en los métodos de protección de la información y seguridad de las comunicaciones, con especial atención en la configuración y administración de sistemas y redes informáticas seguras y en la gestión segura de la información.

PROGRAMA:

- **Introducción y motivación.**
  - Introducción y motivación.
  - Confidencialidad, integridad, disponibilidad, no-repudio.
  - Hipótesis y modelos de confianza: Fortaleza, Aeropuerto, Peer-to-Peer.
  - Políticas, normas y mecanismos de seguridad.
  - Análisis de riesgo y relación coste/beneficio.
- **Fundamentos.**
  - Filosofías de control de acceso: CL, ACL, ACM.
  - Modelos de confidencialidad: Bell-La Padula.
  - Modelos de integridad: Biba, Lipner.

- Modelos híbridos: Muralla China.
- Principios básicos.

- **Criptografía.**
  - Criptografía Clásica o Simétrica.
    - Cifrador en bloque.
    - Cifrador de flujo.
  - Criptografía de Clave Pública o Asimétrica.
  - Firma digital.
  - Mecanismos de autenticación de mensajes.
    - Funciones Hash.
  - Certificados digitales (X.509, PKCS).

- **Modelos de ataques.**
  - DoS, DDoS.
  - Intrusiones.
  - MITM.
  - Malware (virus, gusanos, troyanos).
  - Hoaxes.
  - Phishing.
  - SQL Injection.
  - Spoofing.
  - Spam.
  - Ingeniería Social.

- **Infraestructura de defensa.**
  - Cortafuegos.
  - Sistemas de detección de intrusos.
  - Sistemas de prevención de intrusos.
  - Antivirus.
  - Filtros antispam.
  - Honeypots.
  - VPNs.
  - CERTs.

- **Programación robusta.**
  - Prevención de desbordamientos de memoria.
  - Prevención de condiciones de carrera.
  - Prevención de DoS.
  - Prevención de SQL Injections.
  - Prevención de XSS, XST.

- **Seguridad en aplicaciones.**
  - Servidores de correo.
  - Servidores WWW.
  - Servidores de nombres.
  - Bases de datos.

- **Seguridad en redes de datos.**
  - Modelo de Capas.
  - Seguridad en Capa de Enlace.
  - Seguridad en Capa de Red.
  - Seguridad en Capa de Transporte.
  - Seguridad en Capa de Aplicación.

ACTIVIDADES PRÁCTICAS:

Se realizarán ejercicios de ataque y defensa de servidor WWW + BD. Habrá prácticas de firma digital y cifrado, certificación con OpenSSL, Sniffers de red, configuración de IPTables, ataques DoS, Tripwire, Túneles IPSec, Plataforma Metasploit, etc.

PROFESORADO:

- Dª. Lorena Isabel Barona López, GASS/UCM.
- D. Luis Javier García Villalba, GASS/UCM.
- D. Jorge Maestre Vidal, GASS/UCM.
- Dª Ana Lucila Sandoval Orozco, GASS/UCM.
- D. Ángel Leonardo Valdivieso Caraguay, GASS/UCM.