Institución Privada sin Fines de Lucro

VICERRECTORADO ACADÉMICO
FACULTAD DE INGENIERÍA
DEPARTAMENTO:
HARDWARE Y REDES

CÓDIGO: 251G01
HC.: 4 (4 HORAS SEMANALES)
CARÁCTER: OBLIGATORIA
REQUISITO: 252L15
UBICACIÓN: DECIMO SEMESTRE
VALIDEZ: SEPTIEMBRE 2008

PROGRAMA:
SEGURIDAD INFORMATICA

I.- OBJETIVOS GENERALES:

Al culminar el curso el estudiante debe estar en capacidad de: evaluar la seguridad computacional de sistemas así como de las herramientas y técnicas para diseñar, implementar y evaluar soluciones de seguridad.

II.- CONTENIDO PROGRAMATICO:

COMPONENTE TEÓRICO:

Tema 1.- Introducción a la seguridad informática: introducción, propiedades de seguridad, confianza. Ataques, vulnerabilidades. Por que seguridad es más difícil de lo que parece.

Tema 2.- Criptografía: simétrica vs. asimétrica. Encriptación (simétrica), funciones de hash. Encriptación (asimétrica), firmas digitales. Autentificación de mensajes. Confianza: PKI y autoridades certificadoras. Aplicaciones, otros temas

Tema 3.- Seguridad de sistemas: control de acceso: teoría y práctica. Mecanismos vs. políticas. Autentificación: contraseñas, biometría, de una vez, multifactor, mecanismos avanzados. Estudio de casos y aplicaciones

Tema 4.- Amenazas actuales: vulnerabilidades y ataques. Ataques de buffer overflow, Inyección de código. Malware: virus, gusanos, spyware, bots, phishing, Spam. Ataques y defensas. Ingeniería social.

Tema 5.- Seguridad de redes básica: protocolos de autentificación, negociación de claves. Casos (Kerberos, Single-sign-on, autentificación web) y aplicaciones. Infraestructura: TCP, DNS, SMTP, ruteo.

Tema 6.- Introducción al diseño de software seguro: atacar y parchar vs. estrategias de largo plazo: principios. Análisis de riesgos. Programación segura, metodologías y herramientas. Confinamiento.

Tema 7.- Seguridad de redes avanzada: ataques de denegación de servicios (DoS). Cortafuegos (o firewalls). Sistemas de detección/prevención de intrusos (IDS/IPS). Sistemas del mundo real: IPSec, IKE, SSL. Seguridad Web.

Tema 8.- Misceláneos: votación electrónica. Sistemas de anonimato. Sistemas anti-copia (o digital Right Management, DRM). Aspectos éticos, sociales

COMPONENTE PRÁCTICO:

PRACTICA 1.- Introducción a los elementos de seguridad del sistema operativo.
PRACTICA 2.- Elementos de seguridad del sistema de archivos.
PRACTICA 3.- Elementos de seguridad del sistema de red.

III.- MODO DE EVALUACIÓN:

COMPONENTE TEÓRICO: La evaluación se realizará en forma contínua (exámenes, prácticas, exposiciones o trabajos) y tendrán un valor del 50% de la nota definitiva.

COMPONENTE PRÁCTICO: Las prácticas serán evaluadas y tendrán un valor del 50% de la nota definitiva

IV.- BIBLIOGRAFÍA:

- STALLINGS, W., **Fundamentos de seguridad en redes: Aplicaciones y estándares**, Prentice Hall. 2005
- Villalón, **Seguridad en UNIX y redes**, 2a ed, Prentice Hall, 2001
- MCCLURE, SAMBRAY Y KURTZ, **Hacking Exposed: Network Security Secrets and Solutions**, 5ta Edición, Ed. Osborne/McGraw-Hill, 2005

- CHESWICK, William R., BELLOVIN, Steve M. **Firewalls and Internet Security: Repelling the Wily Hacker**, Addison-Wesley, 1994.