Programa Regular

Seguridad en Aplicaciones

Modalidad de la Asignatura: Teórico-práctica.

Carga horaria: 4 hs.

Objetivos:

Al finalizar el curso, el estudiante será capaz de comprender e identificar las amenazas a las que están expuestas las aplicaciones y conocerá mecanismos de protección para las mismas.

Contenidos:

Conceptos básicos de seguridad en el desarrollo seguro de aplicaciones. Problemas de seguridad en aplicaciones tradicionales. Problemas de seguridad en aplicaciones web. Seguridad en aplicaciones de Base de datos. Seguridad en aplicaciones de Correo Electrónico. Firewall, IDS y Honeypots. Test de penetración.

Unidades temáticas:

Unidad I

Introducción. Conceptos básicos de seguridad en aplicaciones. Marco legal y estándares. Organismos de consulta.

Unidad II

Seguridad en aplicaciones Web: Google, WebServer. Reconocimiento de Servidor Web (IIS y Apache). Vulnerabilidades de las aplicaciones Web, Técnicas de password cracking para aplicaciones Web. Ataques y contramedidas para Servidores Web (IIS y Apache)

Unidad III

Seguridad en aplicaciones de Base de datos: Vulnerabilidades de servidores de base de datos, técnicas SQL Injection y Buffer Overflows. Ataques a los servidores de base de datos y contramedidas.

Unidad IV

Seguridad en aplicaciones de Correo Electrónico. Protocolos de correo electrónico. Implementaciones. Reconocimiento de Servidores de correo electrónico (Exchange y POSFIX). Ataques y contramedidas.

Unidad V

Firewall, IDS y Honeypots. Técnicas de evasión de Firewall, Honeypots y contramedidas. Reconocimiento de Firewall (Hardware y Software), IDS (Hardware y Software) y de Honeypots. Técnicas de evasión de IDS y contramedidas. Ataques a Firewall e IDS y contramedidas.

Unidad VI

Test de penetración. Metodologías. Framework. Caso de estudio. Herramientas para realizar test de penetración.

Bibliografía:

- Graves, Kimberly. CEH - Certified Ethical Hacking. Study Guide. Año 2010
- Faircloth, Jeremy. Penetration Tester's Open Source Toolkit, Third Edition. Año 2011
- Denning, D. Cryptography and Data Security. Addison-Wesley. Año 1982.
- Kaufman, C.; Perlman, R.; Speciner, M. Network Security. Prentice Hall. Año 1995.
- Stallings, W. Network and Internetwork Security. Prentice Hall. Año 1995.
- Chapman, D. ; Zwicky E. Building Internet Firewalls. O'Reilly Media. Año 2000.
- Doraswamy, N.; Harkins, D. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall. Año 1999.
- ISO27000 family of information security standards. ISO 27001: 2005.

Propuesta didáctica: Las clases se desarrollarán en el Laboratorio de Informática. Se organizarán en modalidades teórico-prácticas con soporte de presentaciones digitales y prácticas en función de cada clase.

En las clases se presentan los contenidos teóricos y se van resolviendo en forma conjunta ejemplos que ayuden a comprender los nuevos conceptos introducidos.

La formación práctica está basada en la resolución de problemas tipo y de actividades de proyecto y diseño, cuyas resoluciones se realizan principalmente en las computadoras, utilizando aplicaciones de uso en la industria que permitan un contacto directo con las tecnologías actuales.

En cuanto a las actividades de proyecto y diseño, los estudiantes deberán desarrollar un proyecto relacionado a un caso práctico de campo que vincule lo académico con lo profesional, y que les signifique a los estudiantes una aplicación concreta de los conocimientos adquiridos hasta el momento, integrando los

conceptos de las unidades temáticas desarrolladas durante la cursada y en las asignaturas Redes de Computadoras I, Redes de Computadoras II y Seguridad de la Información. El trabajo debe estar relacionado con el análisis de la vulnerabilidad y seguridad de un sistema que satisfaga una determinada necesidad, optimizando el uso de los nuevos conceptos, herramientas y recursos presentados en la asignatura. El proyecto debe incluir un detalle de los problemas encontrados, las formas de solucionarlos, las condiciones de ejecución, formato de los datos de entrada e ideas o sugerencias para realizar una versión mejorada del mismo. La realización de este proyecto permite consolidar la formación práctica del estudiante así como también se lo sitúa en un entorno de trabajo similar al que encontrará en su ámbito laboral.

El material correspondiente a las clases teóricas, así como los documentos de la práctica se encontrarán disponibles a través de un grupo Web al cual los estudiantes tendrán acceso. Este mecanismo también será utilizado para realizar consultas simples.

Actividades extra-áulicas: Se establecerán guías de actividades prácticas para que el estudiante pueda ejercitar, a fin de consolidar los conceptos aprendidos en clase.

Evaluación: La evaluación integradora de las instancias teórico-prácticas se realiza a través de un parcial teórico-práctico en máquina. Además, los estudiantes deberán desarrollar un trabajo final donde se integren los temas vistos en la materia. Las clases son obligatorias ya que implican participación y debate que forman parte de la evaluación.