

Asignatura: Seguridad en Aplicaciones

Carrera:Ingeniería en Informática

Ciclo Lectivo: 2016

Docente/s:Ing. Carlos Alberto Schenone.

Carga horaria semanal: 4 horas.

Tipo de Asignatura: Teórico-práctica.

Fundamentación: Seguridad en aplicaciones es una materia obligatoria correspondiente al cuarto año de la carrera Ingeniería en Informática. En la materia se abordan temáticas relacionadas con las vulnerabilidades y protección de las aplicaciones informáticas.

Las unidades teóricas y actividades practicas vinculan lo académico con lo profesional de forma que los estudiantes integren las temáticas de la cursada con los conocimientos adquiridos en las asignaturas Redes de Computadoras I, Redes de Computadoras II y Seguridad de la Información. Durante el cuatrimestre se desarrolla un trabajo práctico integrador aplicando los nuevos conceptos, herramientas y recursos presentados en la asignatura en un entorno similar al ámbito laboral.

Objetivos:

Que los alumnos

- sean capaces de identificar las amenazas a las que están expuestas las aplicaciones.
- detecten e identifiquen las vulnerabilidades de las aplicaciones
- sean capaces de seleccionar y aplicar mecanismos de protección contra las amenazas a las que están expuestas las aplicaciones
- puedan evaluar el nivel de riesgos a los cuales están expuestos los activos de una organización

Contenidos mínimos: Conceptos básicos de seguridad en el desarrollo de aplicaciones. Problemas relacionados con la seguridad en aplicaciones tradicionales. Problemas de seguridad en aplicaciones web. Modelo OWASP. Aspectos de seguridad en aplicaciones de Base de datos. Firewall, IDS y Honeypots. Test de penetración.

Contenidos Temáticos o Unidades:

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 Overflow. 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 Obligatoria:

- Graves, Kimberly. CEH – Certified Ethical Hacking. Study Guide. Wiley Publishing, Inc. (ISBN 978-0-470-52520-3). Año 2010.
- Harris, Shon. CISSP – Certification Exam Guide, Sixth Edition. Editorial McGraw Hill (ISBN 978-0-07-178173-2). Año 2011.

Bibliografía de consulta:

- 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.
- ISO 27000. Family of information security standards. ISO 27001: 2005.

Modalidad de dictado: Las clases se desarrollaran en el Laboratorio de informática. Se organizaran en las modalidades teórico-practicas 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.

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

Régimen de aprobación: La evaluación integradora de las instancias teóricas se realiza a través de dos parciales teóricos. Además, los estudiantes deberán desarrollar un trabajo

práctico para cada unidad temática y 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.

La asignatura puede aprobarse mediante el régimen de promoción directa, o por exámenes finales regulares o libres.

Al finalizar la cursada, cada estudiante tendrá una calificación correspondiente a la parte teórica (NT) obtenida del promedio de los dos parciales, una calificación de la parte teórica (NP) obtenida del promedio de los trabajos prácticos y una calificación de la defensa del Trabajo Integrador (NTI), así la nota final de la asignatura se obtiene de la siguiente manera:

$$\text{NOTA CURSADA} = 0.3 * \text{NT} + 0.3 * \text{NP} + 0.4 * \text{NTI}$$

Todas las instancias evaluativas tienen una posibilidad de examen recuperatorio para quienes hayan obtenido entre 0 (cero) y 6 (seis) puntos y para quienes hayan estado ausentes con justificación en la evaluación parcial.

Para acceder a la promoción directa los alumnos deberán obtener como NOTA CURSADA un mínimo de 7 (siete) y con una nota mínima de 6 (seis) en cada instancia de evaluación. Para acceder a la promoción, en caso de haber obtenido 6 (seis) en alguno de los parciales, deberá obtener un mínimo de 8 (ocho) en el parcial restante.

Si se obtuviera una NOTA CURSADA inferior a 6 (seis) y superior o igual a 4 (cuatro), en cualquiera de las instancias puede acceder al recuperatorio para intentar mejorar la nota y acceder a la promoción directa; en caso que o logre alcanzar una NOTA CURSADA de 7 (siete) implica que no logra la promoción de la materia y deberá rendir un examen final que se aprobara con una nota no inferior a 4 (cuatro) puntos.

La asignatura se regulariza obteniendo una NOTA CURSADA de 4 (cuatro) o más puntos y cumpliendo el régimen de asistencia al 75% de las clases presenciales como mínimo.