Programa Regular

Seguridad de la Información

Modalidad de la Asignatura: Teórico-práctica.

Carga horaria: 4 hs.

Objetivos:

Al finalizar el curso, el estudiante será capaz de comprender conceptos básicos relacionados con la seguridad de la información; conocer los riesgos existentes y las contra medidas que se puede tomar; analizar distintas herramientas para comprender riegos existentes y analizar la seguridad en la organización; estudiar normas, mecanismos y protocolos para proteger las redes y sus aplicaciones.

Contenidos:

Conceptos básicos de seguridad. Terminología relacionada. Legislación nacional relacionada con la seguridad de la información. Criptografía. Firma digital. PKI. PGP. Esteganografía. SSL. Amenazas: Técnicas de descubrimiento, scanning, sniffing, etc Mecanismos de protección: Firewalls, IDS y honeypots. Nociones básicas de gestión de seguridad de la información.

Unidades temáticas:

Unidad I

Introducción: Conceptos generales. Terminología. Confidencialidad. Integridad. Disponibilidad. Autenticidad. No repudio. Autenticación. Mecanismos.Autorización. Auditoría. Buenas Prácticas. Vulnerabilidades. Amenazas. Clasificación de amenazas. Incidentes. Gestión de seguridad – ISO 27000

Unidad II

Criptografía: Fundamentos. Criptografía simétrica. Criptografía asimétrica. Funciones de hash. Firma digital. Modelos de confianza (jerárquico vs distribuidos). PKI: Infraestructura de clave pública. Componentes. Roles y funciones. Procesos. Certificados digitales. Validez. Compromiso de clave. Listas de revocación. OSCP. Legislación relacionada. PGP. Confianza. Operaciones criptográficas con PGP. Validez. Compromiso de clave. Servidores de claves. Esteganografía. Canales de comunicación seguros: VPNs, SSL.

Unidad III

Amenazas de red: Técnicas de descubrimiento. Técnicas intrusivas y no intrusivas. Enumeración. Fingerprinting. Banner Grabbing. Descubrimiento de Hosts. Escaneo de Puertos. Escaneo de vulnerabilidades. Herramientas. Análisis de Vulnerabilidades. Herramientas de propósito general. Herramientas de propósito específico. Análisis de Metadatos. Sniffing. Modo promiscuo. Spoofing. MITM. Técnicas para snifear redes switcheadas. Ataques posibles. Sniffers de propósito general y específico. Ataques a SSL. Keyloggers por software y hardware. Malware.

Unidad IV

Mecanismos de protección y monitoreo. Firewalls. Tipos de firewalls. Políticas. DMZ. Configuraciones. IDS. IDS de sistema de archivos. IDS de host. IDS de red. IPS. Ejemplos. VPNs. Honeypots. Monitoreo de seguridad. Monitoreo de Logs. Netflow.

Bibliografía:

- Foster, James C.; Bayles, Aaron W.; Long, Johnny. Penetration Tester'S Open Source Toolkit. Editorial Syngress (ISBN: 978-1-59749-021-4). Ed. 1°. Año 2005.
- Graves, Kimberly. CEH - Certified Ethical Hacker. Study Guide. Editorial Wiley (ISBN 978-0470525203). Ed. 1°. Año 2010
- Harris, Shon. CISSP Certification Exam Guide. Editorial McGraw-Hill Osborne Media (ISBN 978-0071781749). Ed. 6°. Año 2012.
- Gheorghe, Lucian. Designing And Implementing Linux Firewalls And QoS. Editorial Kindle (ISBN 9781904811657). Año 2006.

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 exponiendo situaciones reales en forma de ejemplos que ayuden a comprender los nuevos conceptos introducidos.

La formación práctica está basada en la resolución de problemas tipo y de problemas abiertos de ingeniería, 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 los problemas abiertos de ingeniería, se realizarán trabajos relacionados a casos prácticos de campo que vinculan lo académico con lo

profesional, integrando los conceptos de las unidades temáticas desarrolladas durante la cursada y en la asignatura Redes de Computadoras I. Se debe realizar el diseño de seguridad de la infraestructura de red y servicios para una aplicación determinada. La realización de los trabajos implica la identificación de un problema dado y la solución del mismo, a partir de la aplicación de los conocimientos adquiridos hasta entonces, lo cual constituye la base formativa para que el estudiante adquiera las habilidades que le permitan encarar proyectos y diseños de ingeniería.

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.