1(ms)

660/10

Nombre de la Asignatura

Taller de Seguridad Informática

Créditos

7 créditos

Objetivo de la Asignatura

Profundizar en los conceptos de seguridad informática. Introducir al estudiante en la implementación de servicios y funcionalidades orientadas al ámbito de seguridad, por ejemplo, desarrollando funciones de autenticación, plugins para herramientas de seguridad, modificando y configurando funcionalidades complejas de los sistemas operativos, etc.

Adquirir conocimientos de desarrollo de código de programación seguro mediante el estudio de las estructuras y funcionalidades provistas por diferentes frameworks de seguridad disponibles en los sistemas operativos.

Objetivos específicos:

- Que el estudiante comprenda las principales decisiones de diseño que deben ser tomadas para la implementación de diversas herramientas de seguridad.
- Que el estudiante adquiera conocimiento de las estructuras y algoritmos principales que son utilizados para el desarrollo.
- Que el estudiante implemente nuevos servicios.
- Realizar trabajos prácticos que apliquen los conceptos y técnicas vistas a lo largo de este curso y del curso Fundamentos de Seguridad Informática.

Metodología de enseñanza

El curso posee una duración de 12 semanas con 2 horas semanales de teórico-práctico y reuniones periódicas con los docentes supervisores de los laboratorios. El trabajo en esta asignatura será esencialmente práctico. El equipo docente presentará trabajos de laboratorio que deberán ser resueltos por los estudiantes que se organizarán en grupos de a lo máximo 2 (dos) personas. Los grupos de trabajo serán asistidos y supervisados por el equipo docente a lo largo de la realización de cada laboratorio. Se realizarán clases teóricas según lo requieran las tareas a ser desarrolladas.

La realización de trabajos prácticos tiene como objetivo principal formar al estudiante en el desarrollo y utilización de herramientas de seguridad.

CARGA TOTAL DE TRABAJO: 104 horas

Horas de aula semanales: 2
Horas de trabajo del estudiante semanales: 6

Temario

El temario de base para este curso lo constituye los conceptos fundamentales de criptografía aplicada, seguridad de sistemas operativos y de redes, y los principios de desarrollo de código seguro. Los trabajos prácticos o laboratorios podrán varias en diferentes ediciones del curso, pero el objetivo es cubrir aspectos ingenieriles de cada unas de las mencionadas áreas, que son resumidas a continuación:

<u>Criptografía Aplicada</u>

Algoritmo público, clave secreta. Objetivos de un algoritmo. Tipos de ataques a los que debe ser inmune un algoritmo. Cifrado perfecto. "One time pads". Clasificaciones: Cifrados de clave simétrica, de clave pública, en bloque, en flujo.Encadenamiento de algoritmos en bloques. Otras funciones criptográficas. Hashes. Diffie-Hellman. Gestión de claves. Firma electrónica. Infraestructura de clave pública (PKI). Certificados digitales. Protocolos criptográficos.

<u>Seguridad de Sistemas</u>

Identificación, Autenticación: mecanismos tradicionalmente utilizados en los sistemas operativos comunes. Métodos de Autenticación. Algoritmos y protocolos de autenticación.

Políticas de seguridad. Mecanismos de control de acceso: ACL, Control de acceso centralizado (AAA), RADIUS, TACACS, Single Sign-On. Seguridad en Windows. Seguridad en Unix.

Seguridad en Redes TCP/IP

Introducción a la seguridad en redes TCP/IP. Problemas en las distintas capas del modelo OSI simplificado. Seguridad por debajo de la capa 3. Seguridad física. Seguridad en los protocolos de capa 2 y capa MAC. Ataques a estos protocolos. Redes inalámbricas. (IN)Seguridad en capa 3 y 4. Ataques a los protocolos IP, TCP, UDP, ICMP. Qué nos dá IPSec y qué no. Seguridad en los protocolos de aplicación. Servicios de infraestructura críticos: DNS. Ataques a las aplicaciones. Seguridad de la infraestructura. Ataques a la infraestructura. (IN)Seguridad en los protocolos de ruteo. Herramientas para la seguridad en redes TCP/IP: Firewalls, VPNs, IDS, Honeypots. El estado de la seguridad en Internet: DDoS, Ataques "Man in the middle", Ataques a las aplicaciones. Botnets, Canales encubiertos, Ataques "sociales". El factor humano. Phishing, etc.

Seguridad en las Aplicaciones

Errores en los programas y defensas: Ataques al Stack, Bugs en el formato de los strings, Ataques de Timing, Defensas contra estos ataques. Diseño de código seguro: Diseño modular, Herramientas para hacer código seguro, Verificadores de modelos. Manejando código inseguro: Sandboxing, Máquinas virtuales. Seguridad en los browsers: Cookies, Privacidad y multitudes, Java Script, Java Applets y ActiveX. Secure Coding.

Bibliografía

La bibliografía será especificada en cada laboratorio para guíar al estudiante en la temática objetivo cubierta y en el uso de las herramientas necesarias para el desarrollo de los mismos.

Conocimientos previos recomendados

Sólidos conocimientos de redes de computadoras, sistemas operativos y programación.
Esta asignatura asume como ya adquiridos por el estudiante conceptos básicos de Seguridad Informática. En caso de no contar con los mismos, la incorporación de esos conceptos será responsabilidad única del estudiante , lo que redundará en una mayor dedicación horaria. Se recomienda fuertemente haber cursado y exonerado la asignatura Fundamentos de la Seguridad Informática.

Anexo: Ingeniería en Computación

Cronograma tentativo

Semana 1 a 3: laboratorio 1

Semana 4 a 6: laboratorio 2

Semana 7 a 9: laboratorio 3

Semana 10 a 12: laboratorio 4

Modalidad del curso y procedimiento de evaluación

La asignatura se evaluará por medio de una prueba final escrita y por la suficiencia de los trabajos de laboratorio. El nivel mínimo de suficiencia en los trabajos de laboratorio es eliminatorio. El puntaje del laboratorio se integrará al puntaje total del curso, prorrateándose con el de la prueba escrita final.

En todos los casos de los resultados obtenidos surgen dos posibilidades:

- Exoneración del curso
- Insuficiencia en el curso; el estudiante reprueba el curso

Se presenta a continuación el esquema de evaluación del curso

Exoneración. El estudiante debe cumplir los siguientes requisitos:

- llegar al nivel mínimo en cada uno de los trabajos de laboratorio, y
- reunir al menos el 60% del puntaje de la prueba final.

Insuficiencia. El estudiante no cumple los requisitos especificados para exonerar el curso.

Materia Sistemas Operativos y Redes de Computadores.

Previaturas Plan 97: Tener aprobado el examen de las siguientes asignaturas:
Programación 3, Bases de datos
Tener aprobado el curso de Introducción a las Redes de Computadoras.

Plan 87: Tener aprobado tercer año.
Tener aprobado el examen de Comunicación de Datos.

Cupo Máximo: 30, Mínimo: 10

15 estudiantes serán seleccionados por avance en la carrera. Los restantes 15 lugares se seleccionarán mediante sorteo priorizando aquellos estudiantes que tengan aprobadas: Sistemas Operativos, Arquitectura de Sistemas, Redes de Computadoras/Comunicación de datos y Programación 4 / Programación III, según el plan. El cupo se debe a la cantidad de máquinas disponibles para la realización de los trabajos de laboratorio y del seguimiento requerido por parte de los docentes.

Esta asignatura no adhiere a resolución del consejo sobre condición de libre