FACULTAD DE INGENIERIA
Universidad de Buenos Aires

Planificaciones

6648 - Seminario de Electrónica

Docente responsable: PAGOLA HUGO ALBERTO

OBJETIVOS
Adquirir las competencias necesarias para especificar y desarrollar sistemas y aplicaciones seguras en Internet.
Comprender los problemas de seguridad en aplicaciones de Internet
Enseñar a detectar las debilidades en las distintas aplicaciones de Internet y capacitar en herramientas de diagnóstico.

CONTENIDOS MÍNIMOS
Seguridad en Aplicaciones de Internet

PROGRAMA SINTÉTICO
Conceptos de redes y criptografía. Debilidades en redes. Problemas de implementación y del protocolo TCP/IP. Análisis de seguridad IP y TCP. IDS, IPS, honeypots, pruebas de intrusión. Seguridad en Servicios WEB. Verificación y pruebas de aplicaciones WEB. Seguridad física. Desarrollo seguro. Modelos de seguridad. Alta disponibilidad. Zero knowledge proof. Marcas de agua. Seguridad en mobile agent systems.

PROGRAMA ANALÍTICO
1. Introducción
1.1. Conceptos básicos de Seguridad:
1.2. Repaso de Primitivas Criptográficas
1.2.1. Cifradores Simétricos. Modos de Operación.
1.2.2. Cifradores Asimétricos: RSA
1.2.3. Funciones de Hash y MAC
1.3. Revisión de Redes TCP/IP. Servicios fundamentales.

2. Problemas, amenazas, ataques, defensa y prevención.
2.1.1. Problemas de Implementación y del protocolo TCP/IP.
2.1.2. Análisis de seguridad IP y TCP
2.1.3. Amenazas Pasivas. Ataques y Códigos Maliciosos.
2.1.4. Defensa y Prevención
2.1.4.1. Intrusion Detection Systems: NIDS/NIPS
2.1.4.2. Honeypots
2.1.4.3. Análisis de vulnerabilidades, pruebas de intrusión.

3. Seguridad en Aplicaciones Internet.
3.1. Seguridad en Web Services
3.2. Verificación y pruebas de aplicaciones WEB
3.3. Tópicos de desarrollo seguro
3.4. Seguridad en mobile agent systems.
4. Aplicaciones Avanzadas de Criptografia:
4.1. Zero knowledge proof.
4.2. Marcas de agua

5. Seguridad en Empresas
5.1. Arquitecturas de Redes Corporativas
5.1.1. Modelos de alta disponibilidad y seguridad
5.1.2. Monitoreo de seguridad, puntos de control
5.1.3. Dominios de seguridad. Ubicación de Firewalls, IDS, Honeypots.
5.1.4. Seguridad física.

BIBLIOGRAFÍA
* WEB SERVICES SECURITY AND EBUSINESS. G. RADHA MANI & G:S:V RADHA KRISHNA RAO IDEA GROUP PUBLISHING 2007
* SECURITY ASSESSMENT OF THE INTERNET PROTOCOL. CPNI. FERNANDO GONT. 2008
* SECURITY ASSESSMENT OF THE TRANSMISSION CONTROL PROTOCOL (TCP) CPNI TECHNICAL NOTE 3/2009
* "HACKING EXPOSED: NETWORK SECURITY SECRETS AND SOLUTIONS", FIFTH EDITION, OSBORNE/MCGRAW-HILL, 2005, STUART MCCLURE, JOEL SAMBRAY AND GEORGE KURTZ.

* OWASP TESTING GUIDE V3.0, 2008 OWASP FOUNDATION
* OWASP CODE REVIEW GUIDE, OWASP FOUNDATION, 2008 V1.1
* APPLIED CRYPTOGRAPHY SECOND EDITION BRUCE SCHNEIER JOHN WILEY & SONS, 1996

RÉGIMEN DE CURSADA

Metodología de enseñanza

Clases Teórico Practico. Introducción teórica de los temas, con practicas donde se resuelven y discuten los trabajos prácticos.
Para finalizar la materia el alumno desarrolla el conocimiento adquirido en clase mediante la confección de un trabajo practico final.

Modalidad de Evaluación Parcial

La modalidad de evaluación del aprendizaje se realizara mediante una prueba escrita con dos fechas de recuperación.

La calificación final será el promedio de la evaluación parcial,Trabajo final y los trabajos prácticos.

CALENDARIO DE CLASES

Semana	Temas de teoría	Resolución de problemas	Laboratorio	Otro tipo	Fecha entrega Informe TP	Bibliografía básica
<1> 09/03 al 14/03	redes Conceptos de Criptografia					
<2> 16/03 al 21/03	Analisis de seguridad IP					Hacking exposed Security Assessment of the Internet Protocol. CPNI.
<3> 23/03 al 28/03	Analisis de seguridad TCP					SECURITY ASSESSMENT OF THE TRANSMISSION CONTROL PROTOCOL (TCP) CPNI TECHNICAL NOTE
<4> 30/03 al 04/04	IDS IPS Honeypots pruebas de penetracion					
<5> 06/04 al 11/04	Seguridad en Web Service		Laboratorio de Web Service			
<6> 13/04 al 18/04	Verificacion y Pruebas de aplicaciones WEB		Laboratorio Webgoat			OWASP Testing Guide v3.0
<7> 20/04 al 25/04	Seguridad Fisica		Laboratorio Webgoat	Definicion del Proyecto		
<8> 27/04 al 02/05	Desarrollo Seguro		Verificacion de Codigo			OWASP CODE REVIEW GUIDE
<9> 04/05 al 09/05	"Aplicaciones Avanzadas de Criptografia: Zero Knowledge Proof"			consultas de proyecto		Web Services Security And Ebusiness. Applied Cryptography
<10> 11/05 al 16/05	Arquitecturas corporativa Modelos de Seguridad Alta Disponibilidad			Repaso		
<11> 18/05 al 23/05	EXAMEN					
<12> 25/05 al 30/05	Aplicaciones Avanzadas de Criptografia: Marcas de Agua			consultas de proyecto		Applied Cryptography
<13> 01/06 al 06/06	Seguridad en sistemas de Agentes Mobiles			consultas de proyecto		Web Services Security And Ebusiness.
<14> 08/06 al 13/06	Entrega de Proyecto			Entrega de Proyecto		

Semana	Temas de teoría	Resolución de problemas	Laboratorio	Otro tipo	Fecha entrega Informe TP	Bibliografía básica
<15> 15/06 al 20/06	Monitoreo de la Seguridad			recuperatorio 1		
<16> 22/06 al 27/06	Presentacion del TP					

CALENDARIO DE EVALUACIONES

Evaluación Parcial

Oportunidad	Semana	Fecha	Hora	Aula
1º	11			
2º	15			
3º	16			
4º				