Universidad Nacional de Salta
FACULTAD DE CIENCIAS EXACTAS
Av. Bolivia 5150 - 4400 - Salta
Tel. (0387)425-5408 - Fax (0387)425-5449
Republica Argentina

SALTA, 11 de abril de 2011.

EXP-EXA Nº 8168/2011

RESCD-EXA: Nº 206/2011

VISTO: las presentes actuaciones por las cuales se tramita la aprobación del programa y Régimen de Regularidad de la asignatura Optativa I: Seguridad en Redes de Datos, para la carrera de la Licenciatura en Análisis de Sistemas (Plan 2010); y

CONSIDERANDO:

Que la Comisión de Carrera de la Licenciatura en Análisis de Sistemas, aconseja la aprobación del Programa de la asignatura antes mencionada, el cual cumple con los contenidos mínimos contemplados en el Plan de Estudio.

Que el Departamento de Informática, analizó el Reglamento y Régimen de Regularidad de la asignatura Optativa I: Seguridad en Redes de Datos, aconsejando la aprobación del mismo.

Que la Comisión de Docencia e Investigación aconseja favorablemente.

POR ELLO y en uso de las atribuciones que le son propias;

EL CONSEJO DIRECTIVO DE LA FACULTAD DE CIENCIAS EXACTAS
(en su cuarta sesión ordinaria del 30/03/11)

R E S U E L V E

ARTICULO 1.- Aprobar, a partir del presente período lectivo, el Programa Analítico y Régimen de Regularidad de la asignatura Optativa I: Seguridad en Redes de Datos, para la carrera de la Licenciatura en Análisis de Sistemas (Plan 2010), que como Anexo I forma parte de la presente Resolución.

ARTICULO 2º.- Hágase saber a Prof. Sergio Rocabado, Msc. Daniel Arias Figueroa, Departamento de Informática, Comisión de Carrera de Licenciatura en Análisis de Sistemas, Departamento Archivo y Digesto y siga a la Dirección de Alumnos para su toma de razón, registro y demás efectos. Cumplido, archívese.-

RGG

Mag. MARIA TERESA MONTERO LAROCCA
SECRETARIA ACADEMICA
FACULTAD DE CS. EXACTAS - UNSa

UNIVERSIDAD NACIONAL DE SALTA
Facultad Cs. Exactas

Ing. CARLOS EUGENIO PUGA
DECANO
FACULTAD DE CS. EXACTAS - UNSa

Universidad Nacional de Salta
FACULTAD DE CIENCIAS EXACTAS
Av. Bolivia 5150 - 4400 - Salta
Tel. (0387)425-5408 - Fax (0387)425-5449
Republica Argentina

Anexo I – RESCD-EXA: N° 206/2011- EXP EXA N° 8168/2011

Asignatura: Optativa I: Seguridad en Redes de Datos
Carrera: Licenciatura en Análisis de Sistemas (Plan 2010)
Fecha de presentación: 14/03/2011
Departamento o Dependencia: Departamento de Informática
Profesores responsables: Prof. Sergio Rocabado, Msc. Daniel Arias Figueroa.
Modalidad de dictado: Cuatrimestral

Objetivos de la asignatura:

Presentar al alumno los conceptos fundamentales de seguridad en redes.

Capacitar al alumno en el uso de mecanismos, herramientas y procedimientos adecuados para la recolección y el análisis de información relacionada con incidentes de seguridad informática.
Al finalizar el curso, el alumno será capaz de:

- *Comprender y manejar los diferentes aspectos relacionados con la confianza digital.*
- *Definir políticas de seguridad a nivel de Organización, utilizando normativas.*
- Resolver tratamiento de los incidentes de seguridad de la información y los procesos asociados.

Desarrollo del programa analítico:

TEMA 1: Introducción.
Definición de seguridad. Conceptos preliminares. Marco legislativo.
Hacking. Hackers vs crackers. Motivaciones. Tipos de hackers. Tipos de amenazas. Metodología de ataque.
Modos de ataque. Sniffing pasivo. Sniffing activo. Port scanning. Bugs de software. Buffer overflow. Troyanos. Backdoors. Denegación de servicios. SYN Flooding. mail bombing. Smurf, Fraggle. Saturación de ancho de banda. DDOS. Ingeniería social. Acceso físico. Password cracking. Spoofing. ARP Spoofing. IP Spoofing. DNS Spoofing. Phishing. Hijacking. Spoofed SYN RQST. TCP idle scanning. Source routing. ICMP Redirect.
TEMA 2: Confidencialidad.
Criptografía y criptoanálisis. Cifrado y descifrado. Principios criptográficos fundamentales.
Criptoanálisis. texto cifrado. texto cifrado conocido. texto cifrado seleccionado.
Criptografía clásica. XOR, sustitución, transposición.
Criptografía moderna. Clave privada. DES, 3DES, Métodos basados en flujo. Clave publica RSA modo encripción. EL GAMMAL modo encripción
TEMA 3: Autenticación
Modelo general de validación e intrusos. Métodos de autenticación. Modelos de validación basados en métodos distribuidos. Autenticación con clave privada compartida. Establecimiento de una clave compartida. Diffie Hellman 2 y N participantes. Método de clave secreta compartida. Ataque por reflexión. KDC Key distribution center. Protocolo Rana de boca amplia. Ataque por repetición. Protocolo de Needham-Schroeder. Ataque al protocolo de Needham-Schroeder. Protocolo de Otway y Rees. Kerberos. Autenticación con clave pública y privada. Ataque MITM. Protocolo de interbloqueo.

///...

Anexo I – RESCD-EXA: Nº 206/2011- EXP EXA Nº 8168/2011

TEMA 4: Integridad y No Repudio.
Funciones hash. Compendio. Propiedades. Proceso de chequeo de integridad. Message Digest 5(MD5). Secure Hash Algoritm(SHA).
Firma digital. Características de una firma digital. Firma digital con clave secreta. HMAC. Arbitraje. Firma digital con clave publica. RSA modo autenticación (reversible) .DSA el Gamal modo autenticación (irreversible)
Infraestructura de clave pública (PKI). Certificados digitales. Autoridades de Certificación (CA). Repositorios. Listas de revocación. Certificados X509. Estructura jerárquica.
TEMA 5: Gestión de la Seguridad en la Organización.
Política de seguridad. Definición de una política de seguridad. La norma ISO 17799.
Protocolos seguros. IPsec. SSL/TLS. PGP. SMIME.
Aplicaciones de seguridad. Redes privadas virtuales (VPN). Sistemas de detección de intrusos (IDS). Honeypots. Wrappers. Seguridad Perimetral. Proxies. Firewalls. Screened host . Dual homed gateway. DMZ. Tipos de filtrado. Listas de acceso.
TEMA 6: Seguridad en redes wireless.
Introducción. Conceptos y funcionamiento de redes Wireless. Seguridad en 802.11 Ataques típicos a redes Wireless basadas en 802.11. Técnologías Wireless Seguras: WPA, WPA2, 802.11i.

Desarrollo del programa de Trabajos Prácticos

TEMA I: Introducción.
Taller de herramientas de sniffing y scanning.
TEMA II: Confidencialidad.
Implementación de protocolo IPSEC en conexiones punto a punto.
TEMA III: Autenticación.
Implementación y prueba de un servidor de autenticación RADIUS.
TEMA IV: Integridad y no repudio.
Implementación de una PKI. Manejo de certificados. Seguimiento del ciclo de vida de un certificado digital.
Implementación electrónico seguro (SMIME) utilizando firma digital. Firma y codificación de correo electrónico utilizando SMTP.
TEMA V: Gestión de la Seguridad en la Organización.
Implementación de una DMZ.
Implementación de una VPN en modo túnel.
TEMA VI: Seguridad en redes wireless.
Diseño de una red Wireless Segura.

TRABAJO FINAL INTEGRADOR
Definición de una política de seguridad para una organización genérica.

Metodología y descripción de las actividades teóricas y prácticas:
El dictado de la asignatura esta organizado en base a exposiciones teóricas y clases prácticas, brindándose en las clases teóricas los conocimientos necesarios para ser aplicados y desarrollados en las clases prácticas en la forma de problemas tipo y problemas abiertos. Se jerarquizará especialmente la comprensión conceptual de los temas y su aplicación a situaciones de la realidad.

Anexo I – RESCD-EXA: Nº 206/2011- EXP EXA Nº 8168/2011

Se prevé la realización de trabajos prácticos individuales y grupales con contenidos de problemas tipo y problemas abiertos que permitan al alumno reforzar los conocimientos.
En los casos que resulten adecuados de acuerdo al contenido de la unidad, se realizarán trabajos de laboratorio, investigación y visitas didácticas.
Se hará uso de un laboratorio de informática, software de virtualización y simulación para el desarrollo de prácticas.
Se establecerá el uso de una plataforma educativa on-line basada en entorno Moodle, la que permite interacción con los alumnos, consultas y publicaciones de material

Bibliografía:

Bibliografía Básica:

FUNDAMENTOS DE SEGURIDAD EN REDES - APLICACIONES Y ESTANDARES
Segunda edición
Autor: STALLINGS WILLIAM
Editorial: PEARSON ALHAMBRA
ISBN 9788420540023

COMUNICACIONES Y REDES DE COMPUTADORES
Septima edición
Autor: STALLINGS WILLIAM
Editorial: PEARSON ALHAMBRA
ISBN 9788420541105

SEGURIDAD EN REDES IP
Trabajo de investigación correspondiente a los estudios de doctorado en Informática
Autor: Gabriel Verdejo Alvarez. - Universidad Autónoma de Barcelona

Bibliografía de Consulta:

Cryptography and Network Security Principles and Practices
Quinta edición
Autor: William Stallings
Editorial: Prentice Hall
ISBN: 9780136097044
Idioma : Inglés

Internet Firewalls & Network Security
Segunda edición
Autores: Chris Hare y Karanjit Siyan
Editorial: New Riders
ISBN: 9781562054373
Idioma : Inglés

Wireless Security Handbook
Segunda Edición

Universidad Nacional de Salta
FACULTAD DE CIENCIAS EXACTAS
Av. Bolivia 5150 - 4400 - Salta
Tel. (0387)425-5408 - Fax (0387)425-5449
Republica Argentina

Anexo I – RESCD-EXA: N° 206/2011- EXP EXA N° 8168/2011

Autor: Aaron E Earle
Editorial: Auerbach Publications
ISBN: 0849333784
Idioma : Inglés

Sistemas de evaluación y promoción:
La asignatura se promociona con examen final.
La asignatura se regulariza con:

- la aprobación de dos exámenes parciales o sus respectivas recuperaciones con más del 60% del puntaje asignado.
- 80% de asistencia a clases.

rgg

Mag. MARIA TERESA MONTERO LAROCCA
SECRETARIA ACADEMICA
FACULTAD DE CS. EXACTAS - UNSa

UNIVERSIDAD NACIONAL DE SALTA
Facultad Cs. Exactas

Ing. CARLOS EUGENIO PUGA
DECANO
FACULTAD DE CS. EXACTAS - UNSa