



Universidad Nacional de Salta
FACULTAD DE CIENCIAS EXACTAS
Avda. Bolivia 5150 – 4400 SALTA
REPUBLICA ARGENTINA

SALTA, 18 de Setiembre de 2009

EXP-EXA: 8.343/2009

RESCD-EXA: 425/2009

VISTO:

La presentación efectuada por el Mgr. Daniel Arias Figueroa en el sentido de solicitar la autorización para dictar el curso de posgrado "*Seguridad en Redes de Datos*" (3^{ra} Cohorte), organizado por el CIDIA en conjunto con el Proyecto del CIUNSa N° 1690;

CONSIDERANDO:

Que se cuenta con el aval del Departamento de Informática (fs. 21 vta.);

Los despachos favorables de las Comisiones de Posgrado (fs. 29), de Hacienda (fs. 29 vta.) y de Docencia e Investigación (fs. 30);

Que el curso en cuestión se encuentra enmarcado en la Res. CS. N° 640/08;

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

EL CONSEJO DIRECTIVO DE LA FACULTAD DE CIENCIAS EXACTAS
(en su sesión ordinaria del día 09/09/09)

R E S U E L V E:

ARTICULO 1°: Autorizar, en el marco de la Res. CS - 640/08, el dictado del Curso de Posgrado "*Seguridad en Redes de Datos*", organizado por el CIDIA en conjunto con los Proyectos del CIUNSa N° 1690, bajo la dirección del Mgr. Daniel Arias Figueroa, con las características y requisitos que se explicita en el Anexo I de la presente.

ARTICULO 2°: Disponer que una vez finalizado el curso, el docente responsable elevará el listado de los participantes promovidos para la confección de los certificados respectivos, los que serán emitidos por esta Unidad Académica.

ARTÍCULO 3°: Hágase saber al Director responsable del curso, a los Departamentos Docentes que integran esta Facultad, a la Dirección de Mesa de Entradas, a la Dirección Adm. Económica, al Departamento Adm. de Posgrado y publíquese en la página web de la Facultad y de la Universidad. Cumplido, RESÉRVESE.

mxs
az

Prof. MARIA ELENA HIGA
SECRETARIA ACADEMICA
FACULTAD DE CIENCIAS EXACTAS



Ing. NORBERTO ALEJANDRO BONINI
DECANO
FACULTAD DE CIENCIAS EXACTAS



Universidad Nacional de Salta
FACULTAD DE CIENCIAS EXACTAS
Avda. Bolivia 5150 - 4400 SALTA
REPUBLICA ARGENTINA

ANEXO I de la RESCD-EXA: 425/2009 - EXP-EXA: 8.343/2009

Curso de Posgrado: "SEGURIDAD EN REDES DE DATOS"

Organizado por: CIDIA en conjunto con el Proyecto de Investigación CIUNSa. N° 1690

Director del Curso: Mgr. Daniel Arias Figueroa

Instructor a Cargo: C.U. Sergio Rocabado Moreno

Cuerpo docente: Mag. Gustavo Daniel Gil, C.U. Ernesto Sánchez, Lic. Jorge Silvera.

Objetivos generales:

- Este curso le proporcionará al estudiante un conocimiento suficiente para poder acceder a otros cursos de posgrado y extensión más específicos en el tema seguridad en redes de datos.
- Favorecer la puesta al día de los conocimientos científicos y técnicos (teóricos y prácticos) de los egresados, docentes universitarios y administradores de red.
- Ampliar el marco referencial del egresado en informática con el aporte de la tecnología de redes de comunicaciones de datos.
- Especializar al egresado en el área de los sistemas de redes y seguridad en redes de datos.

Objetivos específicos:

- Mostrar los diferentes tipos de ataques informáticos a una organización.
- Describir los diferentes aspectos relacionados con la confianza digital.
- Especificar la implementación de los conceptos anteriores en redes LAN/WAN.
- Proporcionar diferentes soluciones para la gestión de seguridad en una Organización.
- Presentar una posible planificación para el desarrollo e implementación de una Política de Seguridad para una Organización, cubriendo aspectos generales y utilizando normativas.

Metodología: El curso se desarrollará con una clase semanal presencial apoyado por plataformas y herramientas de e-learning para discusión, distribución de material, distribución de videos con los laboratorios y talleres realizados por el instructor, evaluaciones parciales y seguimiento de los trabajos. Cada tema esta acompañado por un laboratorio y/o taller práctico que será desarrollado por los participantes de forma obligatoria, esto les permite aplicar fundamentos teóricos en situaciones prácticas reales. El instructor presentará durante el desarrollo de la clase presencial guías de ejemplo para el desarrollo de los laboratorios.

Horas totales del curso: 60 horas (distribuidas en 30 horas presenciales y 30 horas no presenciales para el desarrollo de laboratorios y talleres (con apoyo e-learning).

Lugar y Fecha de realización: a definir

Requisitos: Tener sólidos conocimientos de networking (Modelo OSI, Dispositivos de networking, Protocolos TCP/IP, etc.).

Destinado a: Gerentes de sistemas, responsables de seguridad informática, administradores de redes, y administradores de servidores, que intervengan en el proceso de prevención, monitoreo, detección, análisis y corrección de incidentes de seguridad informática dentro de una organización.

Cupo máximo: 100 personas.

Certificado: se entregará constancia de asistencia y certificado de aprobación.

Condiciones de Aprobación: Para obtener certificado de asistencia deberá tener como mínimo el 80% de asistencia al curso.

Para obtener certificado de aprobación se deberá:

- Aprobar con al menos un 60% una evaluación final o su recuperatorio.
- Presentar la implementación de cada laboratorio y taller en forma individual o en grupos de hasta 4 integrantes.

///...



ANEXO I de la RESCD-EXA: 425/2009 - EXP-EXA: 8.343/2009

Arancel: \$ 200 por participante.

Destino de los Fondos: no más del 50% de lo recaudado para honorarios de instructores dependiendo de la cantidad de inscriptos y cantidad de docentes necesarios, el remanente para compra de insumos y equipamiento para el CIDIA.

Informes: Box N° 17 – Departamento de Informática – Facultad de Ciencias Exactas – UNSa. teléfono 4255446 y desde el Campus *6097.

Inscripciones: Mesa de Entrada de la Facultad de Ciencias Exactas, en el horario de atención al público (Lunes a Viernes de 10:00 a 13:00 y de 15:00 a 17:00).

Contenidos:

1. Introducción

- 1.1 Definición de seguridad. Conceptos preliminares. Marco legislativo..
- 1.2 Hacking. Hackers vs crackers. Motivaciones. Tipos de hackers. Tipos de amenazas. Metodología de ataque.
- 1.3 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.

Laboratorio:

- Taller de herramientas de sniffing y scanning.
- Ataque Man in the Middle (MITM) utilizando ARP cache Poisoning, DNS spoofing y web site phishing

2. Confidencialidad

- 2.1 Criptografía y criptoanálisis. Cifrado y descifrado. Principios criptográficos fundamentales
- 2.2 Criptoanálisis. Texto cifrado. Texto cifrado conocido. Texto cifrado seleccionado
- 2.3 Criptografía clásica. XOR, sustitución, transposición.
- 2.4 Criptografía moderna.
 - Clave privada. DES, 3DES, Métodos basados en flujo.
 - Clave publica RSA modo encriptación. EL GAMMAL modo encriptación

Laboratorio:

- Implementación de discos virtuales con encriptación en tiempo real. Uso de archivos de claves.

3. Autenticación

- 3.1 Modelo general de validación e intrusos. Métodos de autenticación. Modelos de validación basados en métodos distribuidos
- 3.2. 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
- 3.3 Autenticación con clave pública y privada. Ataque MITM. Protocolo de interbloqueo.



ANEXO I de la RESCD-EXA: 425/2009 - EXP-EXA: 8.343/2009

Laboratorio:

- Análisis del protocolo de autenticación NTLM.
- Implementación y prueba de un servidor de autenticación RADIUS.

4. Integridad y No Repudio

- 4.1 Funciones hash. Compendio. Propiedades. Proceso de chequeo de integridad. Message Digest 5(MD5). Secure Hash Algorithm(SHA)
- 4.2 Firma digital. Características de una firma digital.
 - Firma digital con clave secreta. HMAC. Arbitraje.
 - Firma digital con clave pública. RSA modo autenticación (reversible) .DSA el Gamal modo autenticación (irreversible)
- 4.3 Infraestructura de clave pública (PKI). Certificados digitales. Autoridades de Certificación (CA). Repositorios. Listas de revocación. Certificados X509. Estructura jerárquica

Laboratorio:

- Publicación de información asegurando la integridad mediante compendios MD5 y SHA
- Implementación de una PKI. Manejo de certificados. Ciclo de vida de un certificado digital: Solicitud, firma digital de la CA. Instalación en el browser. Verificación de la validez. Revocación.
- Correo electrónico seguro (SMIME) utilizando firma digital. Firma y codificación de correo electrónico utilizando SMTP.

5. Gestion de la Seguridad en la Organización

- 5.1 Política de seguridad. Definición de una política de seguridad. La norma ISO 17799.
- 5.2 Protocolos seguros. IPsec. SSL/TLS. PGP. SMIME.
- 5.3 Aplicaciones de seguridad. Redes privadas virtuales (VPN). Sistemas de detección de intrusos (IDS). Honeypots. Wrappers.
- 5.4 Seguridad Perimetral. Proxies. Firewalls. Screened host . Dual homed gateway. DMZ. Tipos de filtrado. Listas de acceso.

Laboratorio:

- Aseguramiento de un servidor DNS utilizando IPsec. Calculo del payload generado por IPsec.
- Implementación de un Sitio Web Seguro (HTTPS) utilizando certificados digitales y el protocolo SSL/TLS.
- Implementación de una VPN en modo túnel.
- Aseguramiento del perímetro utilizando una DMZ.

6. Seguridad en redes wireless

- 6.1 Introducción. Conceptos y funcionamiento de redes Wireless.
- 6.2 Seguridad en 802.11 Ataques típicos a redes Wireless basadas en 802.11
- 6.3 Tecnologías Wireless Seguras: WPA, WPA2, 802.11i

Laboratorio:

- Acceso a una configuración insegura de una infraestructura Wireless
- Acceso a una configuración WEP segura, "Crackeando" la clave WEP
- Cómo montar una red Wireless Segura.



Universidad Nacional de Salta
FACULTAD DE CIENCIAS EXACTAS
Avda. Bolivia 5150 – 4400 SALTA
REPUBLICA ARGENTINA

///... -4-

ANEXO I de la RESCD-EXA: 425/2009 - EXP-EXA: 8.343/2009

Bibliografía:

FUNDAMENTOS DE SEGURIDAD EN REDES - APLICACIONES Y ESTANDARES

Segunda edición

Autor STALLINGS WILLIAM

Editorial PEARSON ALHAMBRA

ISBN 9788420540023

Cryptography and Network Security Principles and Practices

Cuarta edición

Autor: William Stallings

Editorial: Prentice Hall

ISBN: 9780131873162

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

Autor: Aaron E Earle

Editorial: Auerbach Publications

ISBN: 0849333784

Idioma : Inglés

COMUNICACIONES Y REDES DE COMPUTADORES

Septima edición

Autor STALLINGS WILLIAM

Editorial PEARSON ALHAMBRA

ISBN 9788420541105

REDES DE COMPUTADORAS

Cuarta edición

Autor TANENBAUM ANDREW S.

Editorial PEARSON ADDISON-WESLEY

ISBN 9789702601623

SEGURIDAD EN REDES IP


Trabajo de investigación correspondiente a los estudios de doctorado en Informática

Autor: Gabriel Verdejo Alvarez.

Universidad Autonoma de Barcelona


Prof. MARIA ELENA HIGA
SECRETARIA ACADEMICA
FACULTAD DE CIENCIAS EXACTAS




Ing. NORBERTO ALEJANDRO BONINI
DECANO
FACULTAD DE CIENCIAS EXACTAS