UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Departamento Ingeniería en Sistemas de Información

ASIGNATURA:	SEGURIDAD EN REDES
DEPARTAMENTO:	ING. EN SIST. DE INFORMACION
AREA:	ELECTIVA
BLOQUE	TECNOLOGÍAS APLICADAS

MODALIDAD:	Cuatrimestral
HORAS SEM.:	8 horas
HORAS/AÑO:	128 horas
HORAS RELOJ	96
NIVEL:	4°
AÑO DE DICTADO:	Plan 95

Objetivos

- Desarrollar una actitud crítica y reflexiva con referencia a la Seguridad de las Redes de Datos y de Comunicaciones.
- Dar al alumno las herramientas necesarias para desarrollar las políticas, planificar los procedimientos de Seguridad e implementar los planes de mitigación y contingencia.
- Facilitar al alumno los elementos necesarios para aplicar los criptosistemas.
- Proporcionar al alumno las metodologías y estándares de seguridad informática.

Contenidos Mínimos (Programa Sintético).

Introducción a la criptografía. Introducción a la seguridad en redes. Sistemas operativos de red, vulnerabilidades y ataques. Autenticación y distribución de claves. Kerberos. Certificados. Seguridad para la Capa de Transporte. Seguridad para la Capa de Red. Infraestructura de Firma Digital. Metodologías y Estándares: ISO 17799. Vulnerabilidades y Diseño seguro de redes. Auditoria y Análisis Forense. Redes inalámbricas. Aspectos legales.

Contenido Analítico:

Unidad I: Introducción a la Criptografía

Introducción a la Matemática Discreta. Mecanismos criptográficos: cifrado de clave simétrica y asimétrica, cifrado de bloques y de flujo. Hashing. Código de autenticación de mensaje o MAC. Mecanismos híbridos: firma digital. Cifrado a nivel de enlace y a nivel de aplicación.

Unidad II: Introducción a la Seguridad en Redes.
Modelo de seguridad en la comunicación mediante redes de datos. Ataques a la seguridad: pasivos y activos. Servicios de seguridad: confidencialidad, autenticación de entidad y de origen de datos, integridad, no repudio de emisión y de recepción, disponibilidad.

Unidad III: Sistemas operativos de red, vulnerabilidades y ataques.
Sistemas operativos abiertos. Seguridad en Linux. Sistemas operativos comerciales. Seguridad en Windows 2000. Framework de instalación de un Servidor Seguro. Vulnerabilidades. Ataques: Virus, Troyanos, Hoaxes, Spyware, Hijackers, Spam.

Unidad IV: Autenticación y distribución de claves.
Características de los protocolos de seguridad. Ataques. Distribución centralizada de claves simétricas: servidor de claves. Clave de sesión y jerarquía de claves. Protocolo de Needham-Schroeder. Análisis de los mensajes. Justificación de cada elemento. Ataques. Otros protocolos para clave simétrica y asimétrica, interactivos o no.

Unidad V: Kerberos. Certificados.
El sistema Kerberos de autenticación de red. Concepto de ticket y autenticador. Servidor de autenticación y servidor de tickets. Análisis de los mensajes. Justificación de cada elemento. Ataques.

Unidad VI: Seguridad para la Capa de Transporte.
SSL/TLS. Arquitectura y conceptos. Record Protocol. Change Cipher Spec Protocol. Alert Protocol. Handshake Protocol. Análisis de los mensajes. Justificación de cada elemento. Ataques. HTTPS. Certificados de servidor y de cliente.

Unidad VII: Seguridad para la Capa de Red.
IPsec. Arquitectura y conceptos. AH: Authentication Header. ESP: Encapsulating Security Payload. Análisis de los mensajes. Justificación de cada elemento. Ataques. Modo transporte y modo túnel. VPN: Red privada virtual. IKE: Internet Key Exchange. ACL: Access Control Lists.

Unidad VIII: Infraestructura de Firma Digital.
Intercambio de Diffie-Hellman. Obtención segura de la clave pública: el problema y sus soluciones. Certificados X.509: obtención, estructura, revocación. CA: Autoridades de certificación y registro. Jerarquía de las CA´s. PKI: Infraestructura de clave pública.

Unidad IX: Metodologías y Estándares: ISO 17799.
Presentación de la norma ISO 17799. Políticas y Procedimientos. Gestión de Comunicaciones y Operaciones. Administración de la Red. Control de Acceso a la Red. Control de Acceso al Sistema Operativo de Red. Monitoreo. Plan de Continuidad del negocio.

Unidad X: Vulnerabilidades y Diseño seguro de redes.
Vulnerabilidades de las Redes. Desarrollo de Estrategias de Seguridad y Administración de Redes. Firewalls: distintos tipos. IDS: Intrusion Detection Systems. IPS: Intrusion Prevention Systems. Firewalls personales. V-LAN´s: redes viruales.

Unidad XI: Auditoria y Análisis Forense.
Auditoria Informática. Análisis de logs. Uso de sniffers: SNORT. Objetivos de Control del COBIT. Análisis forense informático. Honeypots. Ethical hacking. El estándar: OSSTMM.

Unidad XII: Redes inalámbricas.
Introducción a las Wireless LAN. Ataques y vulnerabilidades. Seguridad en las redes Wireless: 802.11x.

Unidad XIII: Aspectos normativos y legales.
Ley de Delitos Informáticos. Ley de Propiedad Intelectual. Ley de Confidencialidad. Ley de Firma Digital. Ley de Habeas Data.

Bibliografía.

- William Stallings, 2010, Network Security Essentials: Applications and Standards, 5º edición, Ed. Prentice Hall.
- William Stallings, 2010, Cryptography and Network Security. Principles and Practice, 5th edition, Editorial Prentice Hall.
- Julia H Allen, 2001, The CERT Guide to System and Network Security Practices, Ed. Addison-Wesley.
- Raúl Siles Peláez, 2002, Análisis de Seguridad de la Familia de Protocolos TCP/IP y sus Servicios Asociados, GNU Free Documentation Licence.
- Antoon Rufi, 2006, Network Security 1 and 2 Companion Guide, Editorial Cisco Systems, Academia de Networking.
- Shon Harris, Allen Harper, Chris Eagle and Jonathan Ness, 2007, Gray Hat Hacking: The Ethical Hacker's Handbook, 2º edición, Editorial McGraw Hill.
- Sitio Web del NIST: www.nist.gov
- Sitio Web del CERT: www.cert.org

Correlativas

Para Cursar:

Cursadas:

- Diseño de Sistemas
- 3 (tres) materias del 3º nivel (además de la anterior)
- 1 (una) materia de 4º nivel

Aprobadas:

- Sistemas Operativos

Para rendir:

Aprobadas:

- Diseño de Sistemas
- 3 (tres) materias del 3º nivel (además de la anterior)
- 1 (una) materia de 4º nivel