UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
COORDINACIÓN DE FORMACIÓN BÁSICA
COORDINACIÓN DE FORMACIÓN PROFESIONAL Y VINCULACIÓN UNIVERSITARIA
DEPARTAMENTO DE ACTUALIZACIÓN CURRICULAR Y FORMACIÓN DOCENTE

DESCRIPCIÓN GENÉRICA DE UNIDADES DE APRENDIZAJE

Descripción Genérica

Nombre: Seguridad en Cómputo

Etapa: Optativa Terminal (Redes y Telecomuncaciones)
Área de conocimiento: Redes
Vigencia del Plan: 2008-1

Competencia:

Aplicar los diversos métodos para garantizar la seguridad y confiabilidad de los datos que circulan en las redes, asegurando el libre transito de información y manteniendo las condiciones de privacidad definidas por los usuarios y los administradores de los sistemas con ética y responsabilidad.

Evidencias de desempeño:

Exámenes teóricos, tareas extraclase, exposición oral y escrita, reportes, prácticas de laboratorio y proyecto final.

Distribución	HC	HL	HT	HPC	HCL	HE	CR	Requisito
	2	2	2	0	0	0	8	Ninguno

Contenidos Temáticos

1. La necesidad de protección
- 1.1. Motivación
- 1.2. ¿Cuál puede ser el valor de los datos?
- 1.3. Definiciones
- 1.4. Seguridad global
- 1.5. Impacto en la organización
- 1.6. Repaso de interconexión de redes (internetworking)

2. Conceptos Generales de seguridad
- 2.1. Principios fundamentales
- 2.2. Ataques, servicios y mecanismos
- 2.3. Ataques de seguridad (activos, pasivos)
- 2.4. Virus, gusanos y caballos de troya
- 2.5. Modelo multiniveles de seguridad
- 2.6. Análisis de riesgos
- 2.7. Estándares de Internet y RFCs
- 2.8. Niveles de trabajo

3. El lado humano de la seguridad
- 3.1. Políticas, normas y procedimientos
- 3.2. Programas de educación
- 3.3. Aspectos jurídicos y éticos

4. Confidencialidad e integridad de la información
- 4.1. Criptografía
- 4.2. Cifrado y autentificación
- 4.3. Firmas digitales
- 4.4. Certificados
- 4.5. Autoridades de certificación
- 4.6. Aplicaciones criptográficas
- 4.7. Secure Socket Layer (SSL)

5. Fortalecimiento de sistemas
- 5.1. Seguridad perimetral
- 5.2. Seguridad en sistemas operativos
- 5.3. Seguridad en aplicaciones
- 5.4. Detectores de intrusos
- 5.5. Respuesta a incidentes
- 5.6. Análisis de estándares y guías

6. Tipos de ataques y vulnerabilidades
- 6.1. Contraseñas
- 6.2. Email bombing & spamming
- 6.3. Problemas de seguridad en FTP
- 6.4. Problemas de seguridad en WWW
- 6.5. TFTP
- 6.6. Telnet
- 6.7. Los commandos “r”
- 6.8. Seguridad en NetBios
- 6.9. Negación de servicio (DOS)

7. Herramientas de seguridad
- 7.1. Herramientas de control y seguimiento de accesos:
- 7.2. Integridad del sistema

Referencias bibliográficas actualizadas

Hacking Exposed Linux, 2nd edition
Brian Hatch, James Lee
McGrawHill Osborne Media
ISBN 0072225645

Practical Unix & Internet Security
Simson Garfinkel, Gene Spafford
O'Reilly & Associates
ISBN 1565921488

Maximum Linux security, 2nd. Edition
John Ray, A Anonymous
Sams
ISBN 0672321343

Network security: private communication in public world
Charlie Kaufman, Radia Perlman, Mike Specimer
Prentice Hall
ISBN 0130460192

Network security Essentials
William Stallings
Prentice Hall
ISBN 0130351288

Hack proofing Linux
James Stanger, Patrick T. Lane, Edgar Danielyan
Singress
ISBN 1928994342

Security Complete
Sybex, Mark Lierley
Sybex, Inc.
ISBN 0782129684

Guide to Linux Networking and Security
Nicholas Wells
Course Technology
ISBN 0619000945

Computer Security: Art and science
Matt Bishop
Addison-Wesley
ISBN 0201440997