EL 65C SEGURIDAD EN TELECOMUNICACIONES

08 U.D.

REQUISITOS: EL 55A Sistemas de Telecomunicaciones DH: (3-2-3)
EL 54B Sistemas para el procesamiento de la Información

CARACTER: Electivo de la carrera de Ingeniería Civil Electricista

OBJETIVOS:

General:

Comprender y aplicar los conceptos de seguridad que se aplican a las redes de telecomunicaciones y a la empresa en general.

Específicos:

- Aplicar protocolos y dispositivos de seguridad para hacer negocios utilizando redes públicas (e-business).
- Conocer metodologías y herramientas de hacking legalmente permitido.
- Conocer como funcionan elementos de red que permiten mejorar la seguridad en una red de datos.
- Entender y manejar arquitecturas de seguridad, basadas en criptografía.
- Realización de actividades reales de aplicación en hacking y aseguramiento de servicios de Internet.
- Aplicar técnicas de control de acceso a los sistemas.
- Entender como se administra la seguridad en la empresa.

CONTENIDOS:

CONTENIDOS:	**Horas de Clases**
1. Introducción a la seguridad	**1,0**
- Motivación - La seguridad en sistemas de información - Evolución de la seguridad informática - Propiedades básicas de un sistema de seguridad informática - Modelos de seguridad - Soluciones de seguridad - Plan general de seguridad - Tipos de ataques - Tecnologías y defensas frente a ataques - Ciclo de seguridad - Metodología de seguridad - Función de seguridad - Certificaciones	
2. Protocolos: vulnerabilidades y seguridad	**3,0**

- - Protocolos de comunicación y vulnerabilidades
    - TCP, Transmission Control Protocol
    - FTP, File Transfer Protocol
    - Telnet
    - SMTP, Simple Mail Transfer Protocol
    - DNS, Domain Name System
    - Web, lado cliente
    - Web, lado servidor
    - SIP, Session Initiation Protocol
    - SNMP, Simple Network Management Protocol
  - Protocolos de seguridad
  - Nivel de aplicación
    - PGP, Pretty Good Privacy
    - SSH, Secure Shell
    - DNSSEC, DNS Security Extensions
  - Nivel de transporte
    - SSL/TLS, Secure Socket Layer
  - Nivel de Red
    - Tunneling
    - IPSec, IP Security
    - VPNs, Virtual Private Networks
  - Nivel de Enlace
    - Protocolos de seguridad para PPP (Point to Point Protocol)
    - STP, Spanning Tree Protocol
  - Seguridad en wireless

3. Ataques en la red **2,0**

- - Spoofing
    - DNS
    - ARP, Address Resolution Protocol
    - Web
  - Sniffing
  - Scaning
    - nmap
  - Código malicioso
  - Virus
  - Denegación de servicio

4. Elementos de red **3,0**

- - Introducción a los firewalls
  - Firewalls
  - NAT, Network Address Translation
  - IDS, Intrusion Detection Systems
  - SBCs, Session Border Controllers
  - Introducción al monitoreo en redes, ejemplos

5. Arquitecturas de seguridad **3,0**

- - Cifrado simétrico (o de clave secreta)
    - Algoritmo DES, Data Encryption Standard
    - Algoritmo 3DES
    - Algoritmo AES, Advanced Encryption Standard
  - Métodos criptográficos
    - Cifrado en bloque
    - Cifrado en flujo

- Cifrado asimétrico
  - Algoritmo RSA,
  - Intercambio de claves Diffie-Hellman
- Cifrado híbrido
- Funciones Hash
- Firmas digitales
- Certificado digital, certificados X.509v3
- Autoridades de certificación
- PKI, Public Key Infraestructure
- Tipos de PKI

6. Administración de la seguridad **2,0**

- Introducción a la administración de la seguridad
- Políticas de seguridad
- Modelos de seguridad
- Control de acceso
- Análisis de riesgos
- Planes de contingencia
- Instituciones de Seguridad

7. OPCIONAL: Seguridad en WiMaX **2,0**

- Introducción a WiMaX, 802.16-2004
  - Capa MAC
  - Tipos de PDUs MAC
- Introducción a la Seguridad en WiMaX, 802.16-2004
  - Necesidad de una arquitectura de seguridad
  - Elementos y funciones en seguridad
  - Fases para establecimiento de conexiones seguras
  - Autentificación
  - Intercambio de llaves
  - Cifrado de los datos
- Conclusiones, mejoras en roadmap, revisión de futuras especificaciones

ACTIVIDADES:

Clases expositivas y actividades practicas (auxiliares)
Controles y tareas

EVALUACION:

La nota final se calcula de la siguiente forma:

$$NF = 0.3\,NT + 0.7\,NC$$

NT : Nota Trabajos de desarrollo de actividades reales de aplicación en hacking y aseguramiento de servicios de Internet
NC : Nota de Control

BIBLIOGRAFIA:

1. Network Security, Private Communication in a public world (2nd Edition), Charlie Kaufman, Radia Perlman, Mike Speciner, Prentice Hall 2002.

2. CISSP Certification, All in One, Shon Harris, McGraw-Hill/Osborne 2002.

3. The CISSP Prep Guide: Gold Edition, Ronald L. Krutz, Russell Dean Vines, John Wiley & Sons 2002.

4. Linux Firewalls (3rd Edition), Steve Suehring, Robert Ziegler, Novell Press 2005.

5. Maximun Linux Security (2nd Edition), John Ray, Anonymous, Sams 2001.

6. Computer Networks, Fourth Edition, Andrew S. Tanenbaum, Prentice Hall PTR 2002.

7. CISSP Examination Textbooks, Volume 2: Practice, S. Rao Vallabhaneni & Devi Vallabhaneni, SRV Professional Publications, 2002

8. Software Libre/ Open Source Security Tools: Herramientas de seguridad, Tony Howlett, Anaya Multimedia 2005

Links:
http://www.cert.org/ CERT
http://www.nsa.gov/ NSA
http://www.sans.org/ Sans
http://computer.org/security/ IEEE
https://www.isc2.org/cgi-bin/index.cgi ISC2
http://packetstorm.linuxsecurity.com/ Packetstorm
http://www.kriptopolis.com/ Kriptopolis
http://www.hispasec.com/ Hispasec
http://www.icsa.com/ ICSA
http://www.nist.gov/ NIST
http://www.cccure.org/ CCCURE
http://www.isaca.org/ ISACA
http://www.coso.org/ COSO
http://www.cisecurity.org/ Cisecurity
http://www.cybercrime.gov/CSI_FBI.htm CSI_FBI
http://www.cioview.com/ Cioview Software free para evaluación de proyectos y seguridad 2005
http://www.sans.org/top20/ Sans TOP 20
http://openvpn.net/ VPN SSL para linux y windows

RESUMEN DE CONTENIDOS:

Introducción. Protocolos de Internet y sus vulnerabilidades, aplicaciones seguras en Internet, redes privadas virtuales (VPNs). Ataques en redes de computadores. Dispositivos de seguridad en red. Arquitecturas de seguridad, criptografía y PKIs. Cómo administrar la seguridad en la empresa. Seguridad en redes Inalámbricas. Actividades reales de aplicación en hacking y aseguramiento de servicios de Internet.