Seguridad en sistemas de información

Objetivo

Presentar políticas generales de autenticación, controles de acceso, protección a sistemas de archivos, respaldos y algunas otras nociones.

Descripción

Es un curso compartido por varios profesores y tiene componentes teóricos y prácticos, propios de ingeniería computacional y de protocolos ad-hoc en cuanto a aplicaciones.

Contenido

1. Seguridad en comunicaciones y redes de computadoras
    a. Introducción a TCP/IP
    b. Conceptos de seguridad en redes
    c. Configuración de red en el sistema GNU/Linux
    d. Configuración de una puerta (gateway)
    e. Uso de IPTables
    f. Configuración de cortafuegos
    g. Zonas militarizadas y redireccionamiento de servicios
    h. Configuración y compilación del núcleo de GNU/Linux
    i. Cómo crear un cortafuegos sin un disco duro. Arranque desde CDROM.
    j. LDAP
    k. Seguridad en redes inalámbricas:
    l. autenticación de usuarios y un cortafuego dinámico: NoCAT y WifiDog
    m. Redes virtuales

2. Aplicaciones en áreas profesionales
    a. Servicios de Seguridad en Sistemas de Información: Introducción.
    b. Servicios de Seguridad en Sistemas de Información: Aplicaciones.
    c. Casos de Estudio: Notaría Digital, Elecciones electrónicas, dinero digital
    d. Protocolo IKE de IPSec: Sigma.
    e. Certificados e Infraestructura de clave Pública (PKI)
    f. Caso de estudio 1: Certificados con información biométrica.
    g. Caso de estudio 2: Facturas electrónicas del SAT
    h. Protocolo SSL/TLS.
    a. Open SSL
    i. PGP
    j. Seguridad en el cómputo nube
    k. Seguridad en Ambientes Computacionales Altamente Restringidos.
    l. Seguridad en Redes Inalámbricas de Sensores.

3. Redes de computadoras
    a. Análisis de Tráfico en Redes Locales
    b. SNMP
    c. Control de Acceso

d. Autentificación mediante Kerberos y otros protocolos
e. Instalación y configuración de un servidor de correo electrónico con políticas de seguridad
f. Mecanismos Anti-SPAM para el Correo Electrónico
g. Servicios de seguridad en SMS
h. Sistemas de Detección de Intrusos

Bibliografía

a. Alexander Clemm. Network Management Fundamentals. Cisco Press. 2006.
b. De la Fraga, L. G. Seguridad en Redes de Computadoras Usando GNU/Linux. Notas del curso impartido el 9 de septiembre 2004 en el 1st International Conference on Electrical and Electronics Engineering. Acapulco, Guerrero. September 8-10, 2004.
c. Brian Hayes, "Cloud Computing", Communications of the ACM July 2008 Vol. 51 No 7.
d. Gerhard Mourani, Securing & Optimizing Linux: The Ultimate Solution gmourani@openna.com, version 2.0, July 2002 http://www.tldp.org
e. Thomas Wadlow and Vlad Gorelik, "Security in the Browser", Communications of the ACM, Vol. 52 No. 5, May 2009.
f. Ryan West, "The Psychology of Security", Communications of the ACM, Vol. 51 No. 4, April 2008.
g. William Stallings. Cryptography and Network Security: Principles and Practice, 5th Edition. Prentice Hall. 2011.
h. Stallings, Cryptography and Network Security. Principles and Practice, Third Edition.W. Prentice-Hall, 2003.
i. Securing & Optimizing Linux: The Ultimate Solution Gerhard Mourani, gmourani@openna.com, version 2.0, July 2002 http://www.tldp.org
j. Sitio de OpenSSL (www.openssl.org)

Referencias adicionales

1. Christian Cachin, Protocols for Secure Cloud Computing, IBM, April 2011
2. Estrategia Nacional de Ciberseguridad, Gobierno de México, 2017
3. Open Web Application Security Project (OWASP), Top 10 - 2017, The TenMost Critical Web Application Security Risks
4. Open Web Application Security Project (OWASP), Software Assurance Maturity Model (SAMM) ver. 2.0 (Local copy)
5. RedHat Developer, Secure Coding. Includes videos for Getting Started with Secure Coding, but the most interesting part is The Fedora Project's Defensive Coding Guide
6. Serie de plantillas para definir políticas de seguridad informática, recomendadas por el Instituto SANS (SysAdmin, Audit, Network and Security).
7. William Stallings and Lawrie Brown. Computer Security: Principles and Practice. Prentice Hall Press, USA, 3rd edition, 2014.
8. Avi Kak, TCP/IP Vulnerabilities and DoS Attacks: IP Spoofing, SYN Flooding, and The Shrew DoS Attack, Lecture Slides, 2020