Referencias

Bibliografía

Capítulo I

1) **Bryan Burns, SECURITY POWER TOOLS, O Reilly 2007**
2) **Cliff Riggs, Network Perimeter Security: Building Defense In-Depth, Auerbach Publications 2004**
3) **Craig Hunt, TCP/IP Network Administration, 3rd Edition, O'Reilly 2002**
4) **Dr. Eric Cole, Network Security Bible, Wiley Publishing 2005**
5) **Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001**
6) **Libor Dostálek, Undestanding TCP/IP, Packt publishing, 2006**
7) **Programa de la academia Cisco Networking, material multimedia, 2006**
8) **Steven T. Karris, NETWORKS Design and Management, Orchard Publications 2002**

Capítulo II

1) **Charles P. Pfleeger, Security in Computing, Fourth Edition, Prentice Hall 2006**
2) **Daltabuit, La seguridad de la información, Limusa Noriega Editores 2007**
3) **Dr. Eric Cole, Network Security Bible, Wiley Publishing 2005**
4) **Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001**
5) **Jordi Herrera Joancomartí, Aspectos avanzados de seguridad en redes, UOC Formación de Posgrado 2004**
6) **Kimberly Graves, CEH ™ Official Certified Ethical Hacker Review Guide, Wiley Publishing 2007**
7) **Matthew Strebe, Network Security Jumpstart, Sybex, 2002**
8) **Mike Horton, Clinton Mugge, Hacknotes™ Network Security Portable Reference, McGraw-Hill/Osborne 2003**
9) **Risk Management Guide for Information technology System, NIST SP800-30**
10) **Robert Richardson, CSI Computer Crime & Security Survey, 2008**
11) **William Stallings, Fundamentos de seguridad en redes aplicaciones y estándares, segunda edición, Pearson Educación 2005.**

Capítulo III

1) **Antonio Villalón Huerta, seguridad en unix y redes, GNU Free Documentation 2002**
2) **Cliff Riggs, Network Perimeter Security: Building Defense In-Depth, Auerbach Publications 2004**
3) **Dr. Eric Cole, Network Security Bible, Wiley Publishing 2005, p346-348**
4) **James Joshi, Network Security: Know It All, Morgan Kaufmann 2008**
5) **Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001**
6) **John E. Canavan, Fundamentals of Network Security, Artech House 2000**

6) Mike Horton, Clinton Mugge, Hacknotes™ Network Security Portable Reference, McGraw-Hill/Osborne 2003
7) James Joshi, Network Security: Know It All, Morgan Kaufmann 2008
8) Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001
9) John E. Canavan, Fundamentals of Network Security, Artech House 2000
10) Dr. Eric Cole, Network Security Bible, Wiley Publishing 2005, p346-348
11) Melissa M, Syngress, Designing a Windows server 2003 active Directory Infrastructure.
12) Módulo 3 fundamentos de seguridad en redes, aplicaciones y estándares, Diplomado Seguridad de la Información, CEM Polanco DGTIC 2008
13) William Stallings, Fundamentos de seguridad en redes aplicaciones y estándares, segunda edición, Pearson Educación 2005.

Capítulo IV

1) Matthew Strebe, Network Security Jumpstart, Sybex, 2002
2) ISO 27001 ed 2005
3) Daltabuit, La seguridad de la información, Limusa Noriega Editores 2007
4) Dr. Eric Cole, Network Security Bible, Wiley Publishing 2005, p346-348
5) Kimberly Graves, CEH ™ Official Certified Ethical Hacker Review Guide, Wiley Publishing 2007
6) Cliff Riggs, Network Perimeter Security: Building Defense In-Depth, Auerbach Publications 2004
7) MIKE HORTON, CLINTON MUGGE, HACKNOTES™ Network Security Portable Reference, McGraw-Hill/Osborne 2003
8) Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001
9) John E. Canavan, Fundamentals of Network Security, Artech House 2000
10) Bryan Burns, SECURITY POWER TOOLS, O Reilly 2007

Capítulo V

1) NIST 800-30.
2) Peter N.M. Hansteen, The Book of PF 2nd Edition, William Pollock 2011
3) Joel Scambray & Stuart McClure, Hacking exposed windows: windows Security Secrets & Solutions third edition, McGrawHill 2008
4) Andrew Williams, Nessus, Snort & Ethereal Power Tools, Syngress Publishing 2005
5) John R.Vacca, Firewalls Jumpstart for Network and Systems Administrators, Elsevier 2005
6) KerryJ. Cox, Christopher Gerg Managing Security with Snort and IDS Tools, O'Reilly 2004
7) Steve Andrés, Security Sage's guide to hardening the network infrastructure, Syngress Publishing 2004

Páginas electrónicas

Capítulo I

1) **Carlos Vicente, Servicios de red Universidad de Oregon, Gestión de Traps SNMP (última revisión: 01-febrero-2011).**
http://www.nsrc.org/workshops/2008/walc/presentaciones/gestion_traps.ppt
2) **Dirección física (última revisión: 01-febrero-2011).**
http://standards.ieee.org/regauth/oui/index.shtml
3) **Definición de puerto (última revisión: 01-febrero-2011).**
http://www.iana.org/assignments/port-numbers
4) **Protocolo ARP (última revisión: 01-febrero-2011).**
http://www.rfc-es.org/rfc/rfc0826-es.txt
5) **Three-way handshake (última revisión: 01-febrero-2011).**
http://www.telefonica.net/web2/marco2z/doc/tcp_ip.es.pdf
6) **RFC854 - Telnet Protocol Specification (última revisión: 01-febrero-2011).**
http://www.faqs.org/rfcs/rfc854.html
7) **RFC959 - File Transfer Protocol (última revisión: 01-febrero-2011).**
http://www.faqs.org/rfcs/rfc959.html
8) **Modos de conexión FTP (última revisión: 01-febrero-2011).**
http://www.ignside.net/man/ftp/pasivo.php
9) **RFC 2616 - Hypertext Transfer Protocol (última revisión: 01-febrero-2011).**
http://www.faqs.org/rfcs/rfc2616.html
10) **RFC 1939 - Post Office Protocol - Version 3 (última revisión: 01-febrero-2011).**
http://www.faqs.org/rfcs/rfc1939.html(pop3)
11) **Domain Name Service (DNS) (última revisión: 01-febrero-2011).**
http://technet.microsoft.com/en-us/library/bb726935.aspx
12) **Servidores DNS raíz (última revisión: 01-febrero-2011)**
http://www.root-servers.org/
13) **Miguel Angel Hernández Vallejos, Riesgos en el sistema DNS, ESA Security S.A. (última revisión: 01-febrero-2011).**
http://www.esa-security.com/pdf/SIC_68_Riesgos%20en%20el%20Sistema%20de%20DNS.pdf
14) **BOOTP y DHCP (última revisión: 01-febrero-2011).**
http://technet.microsoft.com/es-es/library/cc781243.aspx
15) **María Gabriela Briseño, Protocolo básico de administración de red (snmp) versión 3. (última revisión: 01-febrero-2011)**
http://neutron.ing.ucv.ve/revista-e/No6/Brice%C3%B1o%20Maria/SNMPv3.html

Capítulo II

1) **Amenazas lógicas, tipos de ataques (última revisión: 01-febrero-2011).**
http://www.segu-info.com.ar/ataques/ataques.htm
2) **Virus (última revisión: 01-febrero-2011).**
http://www.2privacy.com/www/viruses/virus-glossary.html
3) **IP Spoofing (última revisión: 01-febrero-2011).**
http://www.symantec.com/connect/articles/ip-spoofing-introduction
4) **Rule Set Based Access Control, (última revisión: 01-febrero-2011).**
http://www.microsoft.com/latam/seguridad/hogar/spam/phishing.mspx
5) **Envenenamiento ARP (última revisión: 01-febrero-2011).**
http://blackspiral.org/docs/arp_spoofing.html
6) **Ataque Man In the Middle (última revisión: 01-febrero-2011).**
http://casidiablo.net/man-in-the-middle/
7) **Fingerprintings Tools (última revisión: 01-febrero-2011).**
http://www.securityfocus.com/archive/112/323521
8) **Fingerprinting activo (última revisión: 01-febrero-2011).**
http://bpsmind.wordpress.com/2008/07/17/fingerprinting-activo-y-pasivo/
9) **Botnet (última revisión: 01-febrero-2011).**
http://eliax.com/index.php?/archives/4665-El-nuevo-Botnet-Kraken,-amenaza-contra-el-Internet.html
10) **Cuatro pasos para luchar contra los botnets (última revisión: 01-febrero-2011).**
http://www.idg.es/computerworld/articulo.asp?id=183857
11) **El super ordenador más potente del mundo (última revisión: 01-febrero-2011).**
http://www.elmundo.es/navegante/2008/06/10/tecnologia/1213080910.html
12) **Rendimiento de las computadoras (última revisión: 01-febrero-2011).**
http://www.tecnologiahechapalabra.com/datos/soluciones/implementacion/articulo.asp?i=3269
13) **Footprinting, escaneos, enumeración (última revisión: 01-febrero-2011).**
http://www.hacktimes.com/?q=taxonomy/term/24

Capítulo III

1) **DRP (última revisión: 01-febrero-2011)**
http://132.248.173.15/labsec/3semsi/filminas/Administracionderiesgos.pdf
2) **Active Directory (última revisión: 01-febrero-2011)**
http://ditec.um.es/aso/teoria/tema13.pdf
3) **Seguridad del terminal, HP (última revisión: 01-febrero-2011)**
http://docs.hp.com/es/5187-2217/ch07s02.html?btnPrev=%AB%A0anterior
4) **Beneficios, políticas de seguridad (última revisión: 01-febrero-2011)**
http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node333.html
5) **Mecanismos de protección, servicios seguros (última revisión: 01-febrero-2011)**
http://sistemas.itlp.edu.mx/tutoriales/sistemasoperativos2/unidad3.htm
6) **Métodos de autenticación, algo que se es, (última revisión: 01-febrero-2011)**
http://www.biometriaaplicada.com/nosotros.html
7) **Planeación de la seguridad, (última revisión: 01-febrero-2011)**

http://www.cujae.edu.cu/eventos/convencion/cittel/Trabajos/CIT052.pdf
8) **Matriz de acceso, (última revisión: 01-febrero-2011)**
http://www.esdebian.org/articulos/23887/rule-set-based-access-control
9) **Gunnar Wolf, Herramienta "Logcheck", (última revisión: 01-febrero-2011)**
http://www.gwolf.org/files/logcheck/index.html
10) **Gunnar Wolf, Herramienta "PortSentry", (última revisión: 01-febrero-2011)**
http://www.gwolf.org/files/portsentry/index.html
11) **C. Allen, The TLS Protocol, Network Working Group (última revisión: 01-febrero-2011)**
http://www.ietf.org/rfc/rfc2246.txt
12) **CyberLocator and The van Dillen GroupAutenticación basada en localización física, (última revisión: 01-febrero-2011)**
http://www.lbszone.com/index2.php?option=com_content&do_pdf=1&id=1144
13) **Elena Pérez Gómez, La gestión de la seguridad de la información, Socia de la firma de abogados Sánchez-Crespo (última revisión: 01-febrero-2011)**
http://www.microsoft.com/business/smb/es-es/legal/gestion-seguridad.mspx
14) **Carlos Alberto Vicente, Seguridad perimetral, DGSCA 2005(última revisión: 01-febrero-2011)**
http://www.seguridad.unam.mx/eventos/admin-unam/Monitoreo.pdf
15) **Mecanismos básicos de seguridad para redes de cómputo, (última revisión: 01-febrero-2011)**
http://www.seguridad.unam.mx/eventos/admin-unam/politicas_seguridad.pdf
16) **Estrategias Básicas de Seguridad Informática: Defensa en Profundidad, (última revisión: 01-febrero-2011)**
http://www.sentineldr.com/post/estrategias-basicas-de-seguridad-informatica-defensa-en-profundidad
17) **Estrategias de seguridad, (última revisión: 01-febrero-2011)**
http://www.textoscientificos.com/redes/firewalls-distribuidos/estrategias-seguridad
18) NSA Suite B Cryptography, NSA, nov. 8 2010
http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml
19) Steven M. Bellovin, Access Control Matrix, Columbia University, sep 12 2005.
http://www1.cs.columbia.edu/~smb/classes/f05/l03.pdf
20) **Rule Set Based Access Control, Controles de acceso** (última revisión: 01-febrero-2011)
http://www.esdebian.org/articulos/23887/rule-set-based-access-control

Capítulo IV

1) **The 7 best for network security in 2007 (última revisión: 01-febrero-2011)**
http://www.networkworld.com/columnists/2007/011707miliefsky.html
2) **The 7 best for network security in 2007, (última revisión: 01-febrero-2011)**
http://www.networkworld.com/columnists/2007/011707miliefsky.html?page=3
3) **The Top Cyber Security Risk, SANS**
http://www.sans.org/top20/
4) **Seguridad en sistemas, (última revisión: 01-febrero-2011)**
http://technet.microsoft.com/es-es/library/ms143455(SQL.90).aspx
5) **Seguridad en sistemas, (última revisión: 01-febrero-2011)**

http://technet.microsoft.com/es-es/library/cc782569(WS.10).aspx
6) **Seguridad en sistemas, Windows IIS hardening(última revisión: 01-febrero-2011)**
http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1096044,00.html#general
7) **Hardening en sistemas operativos Windows, (última revisión: 01-febrero-2011)**
http://www.microsoft.com/spain/empresas/seguridad/articulos/plan_seguridad.mspx
8) Robert Comella, Computer Disaster Recovery Plan Policity, SANS
http://www.sans.org/security-resources/policies/disaster_recovery2.pdf
9) **Hardening en sistemas operativos Unix y Linux, (última revisión: 01-febrero-2011)**
http://www.seguridad-informatica.cl/web/content/hardening-de-servidores-linux-y-windows-
10) **Hardening en sistemas operativos Unix y Linux , Lynis (última revisión: 01-febrero-2011)**
http://www.rootkit.nl/projects/lynis.html
11) **Hardening, HowTos(última revisión: 01-febrero-2011)**
http://www.linux-sec.net/Harden/howto.gwif.html
12) **The First Ten Steps to Securing a UNIX Host, (última revisión: 01-febrero-2011)**
http://www.arsc.edu/~lforbes/cug/HHPaper.html
13) **The Bastille Hardening program, increased security for you OS (última revisión: 01-febrero-2011)**
http://bastille-linux.sourceforge.net/running_bastille_on.htm#top
14) **Buenas prácticas para evitar "hackeos" de servidores, (última revisión: 01-febrero-2011)**
http://www.cristalab.com/blog/buenas-practicas-para-evitar-hackeos-de-servidores-c68898l/
15) **Buenas prácticas de seguridad para servidores Windows, (última revisión: 01-febrero-2011)**
http://www.atencion.ula.ve/documentacion/seguridad/recomendaciones_adm_windows.pdf
16) **Buenas prácticas en seguridad, informática (última revisión: 01-febrero-2011)**
http://www.eset-la.com/press/informe/buenas_practicas_seguridad_informatica.pdf
17) **VOIP Security Series , (última revisión: 01-febrero-2011)**
http://blogs.sans.org/security-leadership/
18) **What are the 20 Critical Controls , (última revisión: 01-febrero-2011)**
https://blogs.sans.org/security-leadership/2009/08/01/what-are-the-20-critical-controls/
19) **Los 20 controles críticos según SANS Institute, (última revisión: 01-febrero-2011)**
http://symc.com.mx/index.php/2009/08/07/los-20-controles-criticos-segun-sans-institute/
20) **20 Critical Security Controls, (última revisión: 01-febrero-2011)**
http://www.sans.org/critical-security-controls/print.php

Capítulo V

1) **Filtrado de contenido, OpenDNS(última revisión: 01-febrero-2011)**
http://www.opendns.com/
2) **Sistema operativo OpenBSD, packet filter (última revisión: 01-febrero-2011)**
http://www.openbsd.org/faq/pf/shortcuts.html
3) **Sistema operativo OpenBSD, (última revisión: 01-febrero-2011)**
http://www.openbsd.org/

4) **IDS open source, (última revisión: 01-febrero-2011)**
http://www.snort.org/
5) **NTOP, análisis de tráfico de red (última revisión: 01-febrero-2011)**
http://www.ntop.org/news.php
6) **Portal cautivo ChilliSpot (última revisión: 01-febrero-2011)**
http://www.chillispot.info/
7) **ChilliSpot configuración, (última revisión: 01-febrero-2011)**
http://www.chillispot.info/chilliforum/viewtopic.php?id=18
8) **Task Secure Hardening, Microsoft (última revisión: 01-febrero-2011)**
http://msdn.microsoft.com/en-us/library/ee695875(VS.85).aspx
9) Switch hardening on your network, (última revisión: 01-febrero-2011).
http://isc.sans.edu/diary.html?storyid=6910
10) **White paper, IronShield best practices hardening Foundry router & switch, (última revisión: 01-febrero-2011)**
http://www.genesisglobalinc.com/PDF/foundry-hardening-routers-switches.pdf