SEGURIDAD EN WINDOWS 2000
Guía avanzada

Autor: Jeff Schmidt
Editorial: Prentice Hall/Pearson Educación
Año 2001 - 802 páginas - ISBN: 84-205-2973-7
Sitio: www.pearsoned.es

El libro de Jeff Schmidt, traducido de Microsoft Windows 2000 Security Hadbook (2000), trata de proporcionar los conocimientos necesarios para la correcta configuración de la familia Windows 2000 desde la óptica de la seguridad en sus distintas modalidades.

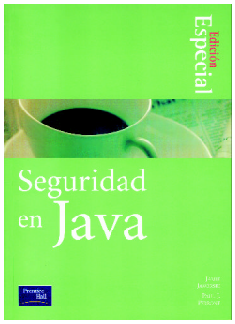
En sus 29 capítulos se analizan aspectos como la arquitectura, los modelos de seguridad, protocolos y redes de comunicaciones, criptografía (crytoAPI), Kerberos y su aplicación práctica a programación (código seguro), redes privadas virtuales y pruebas de penetración, tan necesarias en este tipo de sistemas operativos.

Es de destacar especialmente el capítulo 9, correspondiente a la introducción a IPSec. En esta parte se explican elementos básicos como los tipos de protocolos y el concepto de tunelado, entre otros.

En conclusión, esta obra se erige en una útil guía de ayuda y puesta al día para administradores y desarrolladores en lo que se refiere a componentes del sistema y pros-contras del uso de esta tecnología, que servirán para paliar y predecir, en la medida de lo posible, las amenazas presentes y futuras. Solo resta hacer una salvedad: la falta de ejemplos prácticos agudiza considerablemente la dificultad en la lectura y comprensión de los conceptos que analiza.

SEGURIDAD EN JAVA

Autores: Jamie Jaworski, Paul J. Perrone
Editorial: Prentice Hall/Pearson Educación
Año 2001 - 575 páginas - ISBN: 84-205-3134-0
Sitio: www.pearsoned.es



El título del presente volumen, traducido de *Java Security Hadbook*, publicado por Sams Publishing en el año 2000, tiene como público objetivo aquellos programadores Java que deseen diseñar y construir aplicaciones o *applets* seguros.

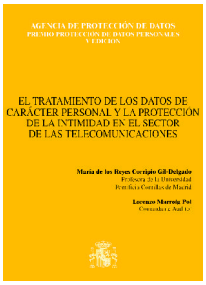
La obra está estructurada en tres partes y siete apéndices. En la primera de ellas, **los fundamentos de la seguridad en Java**, se estudia en cuatro capítulos los modelos básicos para construir aplicaciones seguras y los conceptos que subyacen a la seguridad.

La segunda parte, **seguridad criptográfica**, es una introducción –por lo demás innecesaria a estas alturas– a la criptografía desde sus inicios, pasando por las opciones de la API Java 2, la extensión criptografíca JCE y la gestión de claves y certificados digitales, entre otros. Es una pena que a tenor de su fecha de publicación no haya sido posible incluir la pertinente referencia al AES, algoritmo sustituto del venerable DES, tras resultar ganador de la convocatoria realizada por el NIST con el acrónimo «RIJNDAEL».

Finalmente, la tercera y última parte analiza la **seguridad en los sistemas distribuidos,** y se centra, fundamentalmente, en aspectos como la seguridad de redes, bases de datos o el servicio de autenticación y autorización de Java. En resumen, es un libro que viene a enriquecer el escasísimo número de referencias en español pertenecientes a esta temática.

EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL Y LA PROTECCIÓN DE LA INTIMIDAD EN EL SECTOR DE LAS TELECOMUNICACIONES

Autor: María de los Reyes Corripio y Lorenzo Marroig
Editorial: Agencia de Protección de Datos
Año 2001 - 279 páginas - NIPO: 052-01-002-9
Sitio: www.agenciaprotecciondatos.org



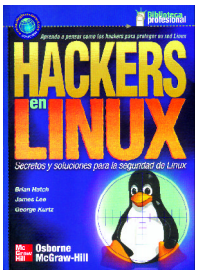
El libro escrito por **Lorenzo Marroig Pol** y **María de los Reyes Corripio Gil Delgado** ha sido el ganador del V Premio Protección de Datos Personales, a instancias de la Agencia de Protección de Datos,dotado con un millón de pesetas. En el prólogo, el director de la APD, **Juan Manuel Fernández López**, afirma que la obra premiada se caracteriza por realizar un diagnóstico completo e interdisciplinar del sector de las telecomunicaciones y de su régimen jurídico no sólo presente, sino también de futuro, al ser constantes las referencias a los trabajos en curso sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre el tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas.

El libro comprende un preámbulo y cuatro partes, estructuradas por capítulos: Preámbulo (Derecho y tecnología), Primera parte (Las telecomunicaciones y los derechos fundamentales a la protección de datos y al secreto de las comunicaciones), Segunda parte (Elementos de la protección de datos personales en el sector de las telecomunicaciones), Tercera parte (El contenido de la protección de los datos de carácter personal en el sector de las telecomunicaciones), y Conclusiones.

Es de destacar, especialmente la primera parte, dedicada a analizar la Directiva 95/46/CE, la Directiva sectorial 97/66/CE, y la Ley Orgánica 15/1999, de 13 de diciembre, y la Ley 11/1998, de 24 de Abril, General de Telecomunicaciones y sus normas de desarrollo.

HACKERS EN LINUX
Secretos y soluciones para la seguridad en Linux

Autores: Brian Hatch, James Lee, Georges Kurtz
Editorial: Osborne McGraw-Hill
Año 2001 - 624 páginas - ISBN: 84-481-3175-4
Sitio: www.mcgraw-hill.es



El libro escrito por Brian Hatch, James Lee y George Kurtz mantiene aún intacto el objetivo inicial marcado para esta serie, que comenzó con el título 'Hackers' ya glosado en esta sección (véase SIC 47, noviembre 2001). En esta ocasión se centra en el estudio de las herramientas y técnicas utilizadas por los intrusos cibernéticos en la vulneración del sistema operativo Linux.

Es de destacar, especialmente la concentración de los procedimientos más habituales de protección al principio del manual. De igual manera, cada ataque y medida de defensa que forman los distintos capítulos de la obra son independientes en su forma y contenido, lo que supone una ventaja para aquellos lectores que prefieran leer y corregir según sus necesidades.

Básicamente, el índice de esta obra se ha vertebrado en cinco partes: Parte I – **Protegiendo Linux** [Temas: 1) breve introducción, 2) cómo protegerse, 3) exploración de sistemas]; Parte II – **Accesos desde el exterior** [Temas: 4) ingeniería social, 5) ataques físicos, 6) accesos desde Internet, 7) intrusiones basadas en fallos de red o de sus protocolos]; Parte III – **Ataque de usuarios locales** [Temas: 8) acceso como super-usuario, 9) vulnerabilidades en las contraseñas, 10) defensa del intruso]; Parte IV – **Problemas relacionados con los servidores** [Temas: 11) correo y FTP, 12) seguridad web, 13) control de recursos accesibles desde la Red]; Parte V – **Apéndices** A) actualización de paquetes, B) desactivar servicios innecesarios, C) recursos de información en la red y D) estudio de casos reales.