

HACKERS BEWARE Defending your network from the wiley hacker

Autor: Eric Cole
Editorial: New Riders Publishing
Año 2001 - 778 páginas - ISBN: 0-7357-1009-0
www.newriders.com / www.pearsoned.es

En los últimos tiempos, una de las temáticas que más fuerza está cobrando dentro del panorama editorial es la dedicada a la seguridad en las TIC. La traducción al español de algunos títulos publicados a nivel internacional en áreas como la detección de intrusiones, confirma a todas luces la buena salud que está experimentando el sector.



Hackers Beware: defending your network from the wiley hacker tiene como objetivo principal analizar las técnicas, métodos y herramientas utilizadas por los intrusos en sus incursiones ilegales por los sistemas de información. La obra se estructura en 20 'asépticos' capítulos en donde su autor, Eric Cole, instructor de la CIA y reconocido orador del Sans Institute, estudia las más conocidas formas de ataque (denegación de servicio, desbordamiento de *buffer*, secuestro y forzamiento de contraseñas), y

los diferentes *exploits* utilizados en sistemas NT o Unix, entre otros.

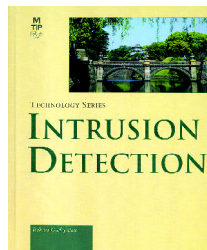
Los tres primeros están configurados como introducción a conceptos y procesos utilizados por los autodenominados *hackers*. Los siguientes segmentos, del número 4 al 7, estudian pormenorizadamente algunos de los caminos empleados en la vulneración de la seguridad de los sistemas 'víctima', y para terminar, la última de las partes está consagrada a la exposición de los agujeros de seguridad y el forzamiento de las contraseñas que presentan los sistemas operativos Windows NT y Unix, dedicando un capítulo a cada uno de ellos.

Todos los casos analizados en este libro están amenizados con ejemplos prácticos y un sumario al final de cada uno de ellos, que ayuda, en gran medida, a su lectura y comprensión.

INTRUSION DETECTION Technology series

Autora: Rebecca Gurley
Editorial: Macmillan Technical Publishing
Año 2000 - 339 páginas - ISBN: 1-57870-185-6
www.pearsoned.es

El libro escrito por Rebecca Gurley trata de transmitir de una forma completa, clara y concisa los conocimientos necesarios para conocer holísticamente uno de los temas que se encuentra actualmente en el candelero de la seguridad TIC: la detección de intrusos.



Concretamente este volumen está formado por 13 capítulos y cuatro apéndices, y una de sus principales características -que le diferencia de otros de su género-, es el enfoque y la estructuración de sus contenidos en tres áreas esenciales: usuarios, organizaciones y fabricantes. Entre otros temas, se analizan aspectos como la escalabilidad de los productos y el código de buenas prácticas (usuario), la estrategia y sus limitaciones (organizaciones), además de las políticas y las etapas recomendadas en el diseño de soluciones de detección de intrusos (fabri-

cantes).

Cabe destacar el análisis de los aspectos más prácticos de la detección de intrusos, comenzando por una revisión histórica, conceptos y definiciones, protocolos y un caso práctico que desglosa paso a paso los aspectos más sensibles a tener en cuenta en un análisis de vulnerabilidades.

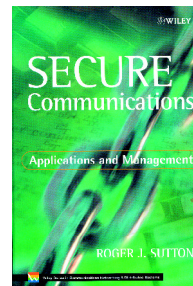
La única salvedad del presente libro es, que en su origen, está publicado en el año 2000, con lo cual, la bibliografía incluida (apéndice B) o los recursos de Internet (apéndice C) acusan cierta obsolescencia debido al incremento de nuevos registros en esta área de actividad. De todas formas, incluye direcciones y títulos esenciales y obligatorios en su consulta para todos aquellos que quieran ampliar conocimientos, bien por vía telemática o a través del medio tradicional: el libro.

SECURE COMMUNICATIONS Applications and Management

Autor: Roger J. Sutton
Editorial: John Wiley & Sons
Año 2002- 322 páginas - ISBN: 0-471-49904-8
www.wiley.com/ www.diazdesantos.es

El título del presente volumen, **Secure Communications**, por sí solo, refleja de forma clara y precisa la temática a tratar en sus numerosas páginas: la seguridad en las comunicaciones. Abordando desde la criptografía básica (incluido lo fundamental del algoritmo AES), aplicaciones de voz militares o la seguridad en las comunicaciones telefónicas y vía radio (VHF/UHF), el libro de Roger J. Sutton proporciona en sus más de trescientas páginas, una completa y actualizada información en todo lo relacionado con el desarrollo e implementación de estas tecnologías.

El contenido del volumen está dividido en dos partes: por un lado, los capítulos dedicados a los aspectos técnico-filosóficos de la seguridad en las comunicaciones (1,2,14), y por otro, los dedicados a las distintas aplicaciones tecnológicas. Los primeros están diseñados para aportar la información básica necesaria para su com-



prensión, y los capítulos dedicados a las aplicaciones proporcionan conocimientos técnicos orientados a todos aquellos lectores que ya posean una base sobre el tema.

El índice de esta obra se ha vertebrado de la siguiente manera: 1) Amenazas y soluciones, 2) Una introducción a la criptografía y a la gestión de la seguridad, 3) Seguridad en aplicaciones de voz militares, 4) Seguridad en las comunicaciones telefónicas, 5) Sistemas GSM seguros, 6) Seguridad en redes privadas de radio VHF/UHF, 7) Medidas para la protección electrónica, 8) Criptografía robusta, 9) Redes seguras de FAX, 10) Seguridad en el PC, 11) Correo electrónico seguro, 12) Redes privadas virtuales, 13) Comunicaciones de datos militares, y 14) Gestión, soporte y mantenimiento.

Por último, cabe destacar la inclusión de un glosario de términos y un apéndice con abreviaturas y acrónimos para facilitar la comprensión de los conceptos más complejos.

INFORMATION HIDING Steganography and Watermarking-attacks and Countermeasures

Autores: Neil F. Johnson, Zoran Duric, Sushil Japodia
Editorial: Kluwer Academic Publishers
Año 2001- 137 páginas - ISBN: 0-7923-7204-2
www.wkap.nl / www.diazdesantos.es

El título del presente volumen, publicado por Kluwer Academic Publishers en 2001, forma parte de una colección dedicada a la seguridad que tiene como principal objetivo conocer el estado del arte de los pilares considerados fundamentales en esta disciplina. El libro escrito por Johnson, Duric y Japodia, primero de esta colección, trata de analizar lo concerniente a la 'información oculta' (*hiding information*) en dos áreas concretas: la privacidad de la información (esteganografía) y la protección de la propiedad intelectual (marcas de agua digitales).

Básicamente, el índice de esta obra se ha vertebrado en cuatro partes: Parte I- Introducción; Parte II - Explorando la esteganografía; Parte III - Esteganoanálisis:



ataques contra la información oculta; Parte IV - Contramedidas para los ataques; Apéndices A) Información oculta en el tráfico de red, B) Glosario de métodos para distorsionar las imágenes esteganográficas.

Es de resaltar especialmente la gradación de contenidos, así como la inclusión de un ejemplo en cada tema analizado para ilustrar de forma precisa las

ideas aportadas. De igual manera, cada ataque, cada medida de defensa y cada herramienta para la ocultación de información en imágenes digitales, están analizados de forma independiente, lo que supone una ventaja considerable para aquellos lectores que prefieran leer este manual con independencia del orden establecido.