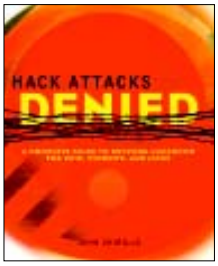
HACK ATTACKS DENIED

A complete guide to network lockdown for Unix, Windows and Linux

Second Edition
Autor: John Chirillo
Editorial: John Wiley & Sons
Año 2002- 689 páginas - ISBN: 0-471-23283-1
www.wiley.com / www.diazdesantos.es



El libro escrito por **John Chirillo** pertenece al género de volúmenes enfocados a compilar información y procedimientos, en su mayoría de carácter técnico, con el objetivo de diseccionar problemas de seguridad comunes, aparecidos en sistemas operativos y dispositivos como *routers*, cortafuegos y variantes, para a continuación ofrecer la solución a cada uno de ellos. Como si de un camino de iniciación se tratara, el autor propone una serie de fases, más concretamente cuatro, que conducen gradualmente –desde lo más sencillo a lo más complejo–, a la consecución del fin propuesto: la protección de los sistemas de información frente a posibles amenazas.

Sucintamente, *Hack Attacks Denied*, en esta su segunda edición, se encuentra dividido en cuatro partes, siete capítulos y tres anexos que responden a la siguiente estructura: **Fase 1: Protección de puertos y servicios** [Temas: 1) Puertos comunes y servicios, 2) Ocultación de puertos y servicios, 3) Implantando las contramedidas]; **Fase 2: Mecanismos de defensa contra intrusos** [Temas: 4) Protección contra intrusiones]; **Fase 3: Secretos del equipo Tigre** [Temas: 5) Cerrando el perímetro: demonios de servicio y hardware, 6) Compendio de los 75 ataques más críticos]; **Fase 4: Ponerlo todo junto** [Temas: 7) Políticas de seguridad]. También se incluye un glosario de términos generales y tres anexos, A) Autoprotección, B) Preparación de un plan de seguridad, C) Contenidos del CD-Rom.

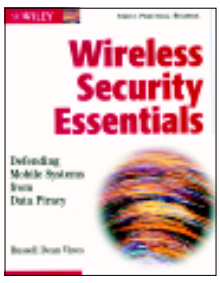
Del conjunto de fases propuestas, las más representativas son la tercera, donde se examinan las vulnerabilidades más críticas (seleccionadas de las listas publicadas por organismos como el SANS y el CERT, entre otros), así como sus contramedidas –clasificadas por sistemas operativos y por dispositivos de distintos fabricantes–, y la cuarta, donde se analiza la parte organizativa de la seguridad TI, es decir, las políticas, los criterios y los controles necesarios en la gestión de riesgos de un sistema de información.

Por último, cabe destacar que el libro está plagado de notas, recomendaciones técnicas y referencias a sitios web que ayudan, en gran medida, a su correcta lectura. Eso sí, teniendo en cuenta la fecha de publicación –el año 2002– resulta chocante comprobar que tanto en el texto como en numerosas capturas de pantalla se sitúa al producto BlackIce Defender como perteneciente a la empresa Network ICE, cuando es conocido que el fabricante de soluciones de detección de intrusiones ISS adquirió esta compañía en junio de 2001.

WIRELESS SECURITY ESSENTIALS

Defending Mobile Systems from Data Piracy

Autor: Russel Dean Vines
Editorial: John Wiley & Sons
Año 2002- 345 páginas - ISBN: 0-471-20936-8
www.wiley.com



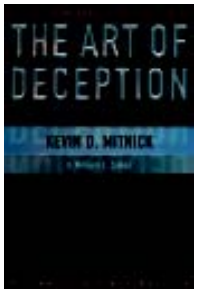
En la actualidad, uno de los temas que se encuentra en el candelero de la seguridad TIC es el relacionado con el despliegue de infraestructuras inalámbricas, y por ende, la aparición de problemas relacionados con la novedad de esta tecnología. Por esta razón, el libro escrito por **Russel Dean Vines** viene a compilar diverso material e información de fuentes varias con el objetivo de elaborar un marco de contextualización que pueda aplicarse, con relativa exactitud, al conocimiento de la evolución de la tecnología *wireless* y sus mecanismos de seguridad inherentes.

Concretamente, el índice de esta obra se ha vertebrado en dos partes y cuatro anexos con la siguiente distribución: **Parte I: Nociones de tecnología básicas** [Temas: 1) Introducción a la informática, 2) Teorías sobre redes inalámbricas, 3) Contexto actual]; **Parte II: Seguridad imprescindible** [Temas: 4) Metodología y conceptos, 5) Tecnología en seguridad, 6) Soluciones y amenazas]; **Anexos:** A) Glosario de términos, B) Guía de explotación WLAN, C) Usando los ataques Fluhrer, Mantin y Shamir para romper el protocolo WEP, D) Documentos de la NASA sobre cortafuegos en la pasarela de Internet inalámbrica.

THE ART OF DECEPTION

Controlling the human element of security

Autores: Kevin D. Mitnick y William L.Simon
Editorial: John Wiley & Sons
Año 2002- 352 páginas - ISBN: 0-471-23712-4
www.wiley.com / www.diazdesantos.es



La temática que han abordado en conjunto **Kevin D. Mitnick** y **William L. Simon** en este su primer libro, como era de esperar, no se sale de la norma general y utiliza el mismo modelo que han seguido otros "compañeros de profesión", como Kevin Poulsen, para encumbrarse en el mundo del pseudo-periodismo tecnológico barato. ¿De qué pueden hablar un exconvicto y un escritor de *bestsellers* para cine y televisión?. Obviamente, de algo que les resulta familiar, en este caso, teorizar sobre una de las técnicas utilizadas por Mitnick en sus intrusiones a los sistemas de información de compañías como Sun, Motorola y Nokia: la ingeniería social.

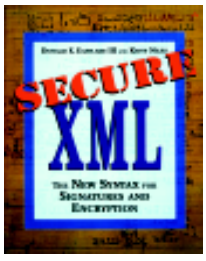
En *Art of Deception*, Mitnick hace gala de sus conocimientos en la materia glosada, y para demostrarlo tiene la osadía de mezclar su experiencia personal –dudosa y aún sin esclarecer–, con otros elementos del mundo de la seguridad TI, léase técnico-organizativos, todos incluidos en el mismo recipiente con el siguiente pretexto: "qué mejor que un ladrón para controlar y conocer a otro ladrón". Dejando a un lado la parte lucrativa de este negocio (no hay que olvidar que estas dos personas han montado una empresa de consultoría, denominada *Defense Thinking*), Mitnick resume en este volumen –seguramente el primero de una larga serie–, un repertorio genérico y poco creíble de técnicas de ingeniería social utilizadas por intrusos en la realidad. Para darle un mayor realismo, reproduce textualmente las conversaciones telefónicas con un alto grado de imaginación, para posteriormente y como era de esperar, analizar cada caso y dar consejos al respecto.

Como conclusión, cabe destacar que no es de recibo que los intrusos más conocidos en la pléyade del submundo informático terminen arengando a las masas con sus teorías viciadas y sus conocimientos adquiridos a base de realizar intrusiones en los sistemas de información de compañías respetables, que realmente son las que conocen e invierten en seguridad. Para muestra, un botón: Mitnick fue condenado a un total de 80 meses de prisión por 25 delitos relacionados con el robo de información vital a multinacionales y organismos gubernamentales, que le ha supuesto, además, tres años de libertad vigilada y una multa de 4.100 euros de indemnización a las víctimas. La verdad, todo un curriculum para comenzar a abrirse camino en el oficio de escritor.

SECURE XML

The New Syntax for Signatures and Encryption

Autores: Donald E. Eastlake III y Kitty Niles
Editorial: Addison-Wesley
Año 2002- 532 páginas - ISBN: 0-201-75605-6
www.awprofessional.com/ www.pearsoned.es



El título del presente volumen, escrito por **Donald E. Eastlake III** y **Kitty Niles**, tiene como público objetivo todos aquellos profesionales que quieran conocer de una forma sencilla, clara y concisa todo lo relacionado con los distintos elementos de seguridad que confluyen en el metalenguaje XML (*Extensible Markup Language*). En sus distintos capítulos se analizan aspectos como los requerimientos especificados en el protocolo SOAP, las implementaciones de seguridad en XML (la autenticación y el cifrado) y los distintos documentos aportados al respecto por organismos como el W3C, el IETF o el NIST, entre otros.

Concretamente, el libro está dividido en seis partes y 19 capítulos estructurados del siguiente modo: **Parte I: Introducción** [Temas: 1) XML y la seguridad, 2) Criptografía digital básica]; **Parte II: XML básico** [Temas: 3) Aspectos Genéricos, 4) Documentos de definición tipo, 5) Definiciones en XML, 6) Xpath: pilares de construcción básicos, 7) URIs, xml:base y XPointer, 8) SOAP]; **Parte III: Autenticación y descarte de información no esencial** [Temas: 9) Eliminación de información no vital: la clave de la robustez, 10) Autenticación y Firma en XML, 11) Perfilando el estándar XMLDSIG para las aplicaciones, 12) Extensiones de firma electrónica del ETSI]; **Parte IV: Introduciendo datos** [Temas: 13) Elementos KeyInfo, 14) XKMS]; **Parte V: Cifrado** [Temas: 15) Cifrado XML, 16) Combinación de firma digital y cifrado]; **Parte VI: Algoritmos** [Temas: 17) Resumen de Algoritmos, 18) Algoritmos criptográficos, 19) Algoritmos no criptográficos]. También se incluyen en el libro seis anexos [A) Implementaciones de seguridad en XML, B) W3C, C) IETF, D) NIST, E) "Documento" frente a "protocolo" y, por último, F) Especificaciones de cifrado en SOAP].