

INTERNET SECURITY DICTIONARY

Autor: Vir V. Phoha
Editorial: Springer-Verlag
Año 2002 - 259 páginas
ISBN: 0-387-95261-6
www.springer.de

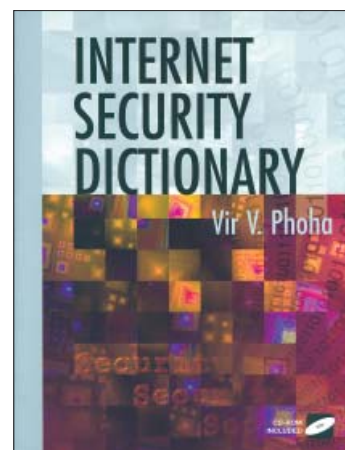
Como el título indica, el presente volumen, escrito por **Vir V. Phoha** es un glosario de términos y definiciones de seguridad focalizado en el área de Internet, diseñado a modo de repositorio de información clasificada en orden alfabético, que cumple con el objetivo de servir a todos aquellos profesionales que necesiten un libro de consulta (en inglés) al alcance de la mano para la revisión de la terminología característica generada por cualquier disciplina científica. Sin duda, para los lectores españoles la llegada de esta obra hace inevitable añorar una pronta actualización del histórico y pionero Glosario de Términos de Seguridad en TI que ya en 1997 el insigne **Arturo Ribagorda** tuvo a bien alumbrar bajo los auspicios de la revista SIC/Ediciones Coda.

Este diccionario específico de seguridad en Internet incluye términos comunes de las siguientes ocho áreas: 1) Autenticación [Temas: Biometría, infraestructuras de clave pública, firma digital, sellado de tiempo y gestión de certificados]; 2)

Cifrado, 3) Niveles de seguridad en red [Temas: IP, IPSec, SHYYP, SSL]; 4) Cortafuegos y gestión centralizada de dispositivos, 5) Políticas de seguridad en Internet [Temas: Análisis de riesgos, integración entre plataformas, administración y auditoría]; 6) Seguridad en código móvil [Temas: Java, Active-X, scripts y agentes de código móvil]; 7) Protección antivirus y detección de intrusiones y 8) Seguridad en el comercio-e.

Además, el volumen incluye varios apéndices que abarcan los siguientes aspectos: A) Abreviaturas y acrónimos, B) Listado de RFCs clasificadas por números, C) Listado de estándares de seguridad, D) Anotaciones y recursos web, E) Bibliografía y, por último, un Índice Alfabético de Términos.

Como conclusión, cabe destacar que uno de los elementos que más ayudan a la comprensión de las definiciones y términos, en algunos casos complicados, son las figuras, gráficos y anotaciones al margen que pueblan el volumen para beneficio de los lectores. Además, el libro viene acompañado de un CD-Rom, que incluye una versión completa del mismo en formato PDF. Eso sí, teniendo en cuenta la fecha de publicación —el año 2002— resulta chocante encontrar acrónimos de certificaciones del tipo ISSO, y sin embargo que no se haga referencia a las más prestigiosas, esto es, las expedidas por el Instituto Sans (GIAC) e ISC² (CISSP), además de obviar el ampliamente reconocido CISA, emitido por ISACA.



802.11 SECURITY

Autores: Bruce Potter y Bob Fleck
Editorial: O'Reilly
Año 2002 - 176 páginas
ISBN: 0-596-00290-4
www.oreilly.com /
www.cocodrilolibros.com

El libro escrito por **Bruce Potter** y **Bob Fleck** tiene como público objetivo a todos aquellos profesionales que quieran conocer de una forma sencilla, clara y concisa todo lo relacionado con los distintos elementos de seguridad implicados en las comunicaciones inalámbricas (despliegue, riesgos, mecanismos de seguridad, plataformas, etc.) y más en concreto, lo que tiene que ver con el estándar IEEE 802.11b, también conocido como *Wireless LAN* o *WiFi*.

Concretamente, el libro está dividido en cuatro partes, estructuradas del siguiente modo: **Parte 1: Seguridad básica en el estándar 802.11** [Temas: 1) Un mundo inalámbrico, 2)

Ataques y Riesgos]; **Parte II: Seguridad en las estaciones** [Temas: 3) Seguridad en las estaciones, 4) FreeBSD, 5) OpenBSD, 6) Mac OS X, 7) Windows]; **Parte III: Seguridad en los puntos de acceso** [Temas: 6) Configurando un punto de acceso]; **Parte IV: Seguridad en la pasarela de Internet** [Temas: 10) Seguridad en los gateways, 11) Pasarelas sobre Linux, 12) Pasarelas sobre FreeBSD, 13) Pasarelas sobre OpenBSD, 14) Autenticación y cifrado, 15) Poniéndolo todo junto].

Así, uno de los capítulos más interesantes incluidos en el volumen es el segundo, dedicado a los ataques y riesgos a los que se enfrenta una compañía que decida ampliar su infraestructura de red utilizando para ello las comunicaciones inalámbricas. Entre los ataques analizados, detallados incluso a nivel físico de OSI, se encuentran los clasificados en el grupo de la denegación de servicio (*Denial of Service Attacks*), los ataques de interceptación e inserción (*man in the middle*), los ataques de escucha y monitorización pasiva (*eavesdropping*) y los ataques físicos, entre otros.

Como conclusión, cabe destacar que la aridez tecnológica de los distintos temas analizados en el libro se encuentra rebajada y amenizada con numerosos ejemplos y gráficos incluidos en el mismo, que ayudan, en gran medida, a su lectura y comprensión.



HACKERS DE SITIOS WEB

Secretos y soluciones para la seguridad de los sitios web

Autores: Joel Scambray y Mike Shema
Editorial: Osborne McGraw-Hill
Año 2002 - 421 páginas
ISBN: 84-481-3378-1
www.mcgrawhill.es

En síntesis, la obra aquí referenciada, escrita por dos de los autores ya clásicos en la serie, **Joel Scambray** y **Mike Shema**, mantiene aún intacto el objetivo inicial marcado para toda la saga, que comenzó con el título 'Hackers', ya glosado en esta sección (véase SIC 47, noviembre 2001) y sucesivos, y que no es otro que el análisis exhaustivo de las técnicas, herramientas y metodologías utilizadas por los intrusos cibernéticos en sus incursiones a través de Internet.

En esta ocasión, el volumen se centra en el estudio de las herramientas y técnicas empleadas en la vulneración y modificación de sitios web. Más en concreto, los autores han clasificado, en un primer bloque, las amenazas más importantes con las que los diseñadores se tienen que enfrentar, para posteriormente, y como cabe esperar, ofrecer las soluciones y los remedios destinados a impedirlos o minimizarlos.

Así, el volumen ofrece en sus 421 páginas, capítulos dedicados al análisis e impacto de las vulnerabilidades en servidores web, las herramientas para el análisis automático de aplicaciones, los ataques a la validación de entradas y a los servicios web, entre otros. El índice programático se ha vertebrado en tres secciones: **Parte I: Identificar el problema** [Temas: 1) Introducción a las aplicaciones web y a la seguridad, 2) Generación de un perfil, 3) Hacking de servidores web, 4) Análisis de aplicaciones]; **Parte II: El ataque** [Temas: 5) Autenticación, 6) Autorización, 7) Ataque a la administración del estado de la sesión, 8) Ataques por validación de entradas, 9) Ataques a los almacenes de datos web, 10) Ataques a los servicios web, 11) Hacking de la administración de la aplicación web, 12) Hacking del cliente web, 13) Estudio de casos]; **Parte III: Apéndices** [A) Listas de comprobación de la seguridad en un sitio web, B) Chuleta de herramientas y técnicas de hacking web, C) Cómo utilizar libwhisker y D) Instalación y configuración de UrlScan].

Por último, cabe destacar que se continua manteniendo el sitio web asociado a la dirección <http://www.hackingexposed.com>, que contiene noticias actualizadas y enlaces a todas las herramientas y recursos de Internet a los que se hace referencia en este volumen.

