

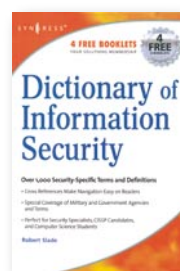
## EL ARTE DE LA INTRUSIÓN

**Autor:** Kevin D. Mitnick y William L. Simon  
**Editorial:** Ra-Ma  
**Año 2006** – 349 páginas (edición española)  
**ISBN:** 84-7897-748-1  
**www.ra-ma.es**

Ra-Ma ofrece en su catálogo la edición española de *The Art of Intrusión*, segundo libro escrito por el conocido *ex-hacker* **Kevin D. Mitnick** y cuya versión original se lanzó en marzo de 2005. La obra debe entenderse como una continuación de *The Art of Deception* (2002), volumen donde se describió un repertorio genérico, y no siempre creíble, de técnicas de ingeniería social utilizadas por intrusos en la realidad (y cuya reseña salió publicada en el número 53 de SIC). En ambos libros, **William L. Simon**, escritor especializado en *best-sellers* para cine y televisión, ha sido coautor, por lo que el resultado final se asemeja más a una novela de misterio para un público generalista que a un libro para profesionales.

Este segundo –y seguro que no último– volumen del polémico personaje, recoge una selección de historias aparentemente reales de ataques de *hackers* a

organizaciones y personas, obtenido a través de entrevistas con sus autores, que sólo las han aportado por la “confianza” hacia Mitnick. De forma sarcástica, los autores señalan que su propósito ha sido “escribir un manual que abra los ojos a las empresas y les ayude a proteger su información confidencial y sus recursos informáticos”. Es decir, un tanto cínico porque en lugar de denunciar los hechos y a sus autores, ciertos datos se han disfrazado para proteger a sus autores, la mayoría ya gente “de bien” reconvertidos en profesionales de la seguridad. El *Arte de la Intrusión* está desarrollado en diez capítulos donde se cuenta el proceso y trama de estas historias, que han pasado “la prueba de olfato” del autor para garantizar su veracidad. También se incluye un anexo de anécdotas breves que intentan sintetizar de forma más gráfica los hechos, y a la vez asombrar, a los lectores. ■



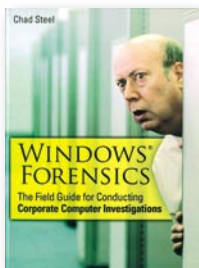
## DICTIONARY OF INFORMATION SECURITY

**Autor:** Robert Slade  
**Editorial:** Syngress Publishing, Inc.  
**Año 2006** – 222 páginas  
**ISBN:** 1-59749-115-2  
**www.syngress.com**

Dado el desarrollo experimentado por el sector de la seguridad TIC, se ha ido formando una opinión generalizada por parte de un nutrido número de profesionales sobre lo beneficioso que resultaría un glosario común que recopilase las acepciones más aceptadas de cada término utilizado en el ámbito mundial. La revista SIC ya evidenció esta necesidad hace justo ahora diez años, para lo cual editó en 1997 su *Glosario de Términos de Seguridad de las T.I.*, bajo la autoría de Arturo Ribagorda. Ahora, muchos otros –tanto en España como en el extranjero– están haciendo lo propio, emprendiendo la tarea, sin duda necesaria, de recopilar y actualizar los términos y definiciones más comúnmente aceptados, para que los profesionales de la seguridad informática y estudiantes de TI se sirvan de ellos en tanto útil herramienta de trabajo. La obra aquí reseñada, de **Robert Slade**, es una más en esta línea.

En concreto, *Dictionary Of Information Security* se centra en encontrar

e identificar la definición más exacta de aproximadamente 1.000 vocablos usados de forma habitual en publicaciones, artículos o sitios web relacionados con la seguridad TIC. El volumen ofrece una cobertura digna aunque no exhaustiva de términos de seguridad y de las tecnologías TIC de plena actualidad, además de incorporar bastantes voces de la más reciente jerga aceptada entre los profesionales. Sin duda, los lectores candidatos a certificarse en seguridad, como CISSP, CISM, Seguridad + y similares, encontrarán útil este volumen para su formación. Cabe destacar que el diccionario se ocupa con especial énfasis de los términos usados en el sector militar y en las agencias gubernamentales. Según indica el autor, la obra se entiende abierta para seguir engrosándola con términos que aparezcan en función de la evolución del sector de la seguridad informática. Con todo, sorprende que el libro no venga acompañado del correspondiente CD-Rom. ■



## WINDOWS FORENSICS. The Field Guide for Conducting Corporate Computer Investigations

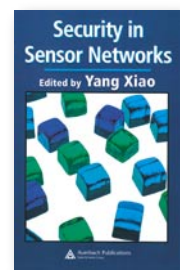
**Autor:** Chat Steel  
**Editorial:** Wiley Publishing, Inc.  
**Año 2006** – 382 páginas  
**ISBN:** 0-470-03862-4  
**www.wiley.com**

*Windows Forensics* se presenta como un manual-guía con el propósito de dirigir las investigaciones forenses de un ordenador en un entorno corporativo, con una atención especial a los equipos con el sistema operativo predominante, Windows. La obra, obviamente, está pensada para lectores interesados en introducirse en esta área de investigación que está experimentando un crecimiento importante, puesto que su objetivo es preparar para combatir el delito en el entorno Windows.

Los 13 capítulos del volumen se dividen en tres bloques: **Análisis forense básico del ordenador**, con un informe de los campos básicos que toda corporación debe observar en el análisis forense de sus equipos; **Examen básico para el análisis forense de Windows**, que se centra en el desarrollo de Windows desde una perspectiva forense y, por último, **Análisis forense de Windows**, donde

se recopilan las técnicas investigadoras de la sección 1 y los datos concretos de Windows de la sección 2 y los aplica a las verdaderas acciones de análisis en cuestión. En conjunto, se ofrecen los instrumentos para ayudar a recuperar archivos sabotados, detectar las fuentes de amenazas en los correos-e, investigar el espionaje industrial y descubrir a los delincuentes informáticos.

También resulta de utilidad para identificar la evidencia del fraude y el abuso de Internet por parte de los empleados; investigación del delito relacionado con la mensajería instantánea, Lotus Notes y los navegadores cada vez más populares como Firefox; proteger la integridad de la evidencia; evaluar y analizar el daño del delito en el PC y procesar la escena del mismo; desarrollar la estructura para conducir efectivamente las investigaciones y descubrir cómo localizar la evidencia en el registro de Windows. ■



## SECURITY IN SENSOR NETWORKS

**Autor:** Yang Xiao  
**Editorial:** Auerbach Publications  
**Año 2007** – 341 páginas  
**ISBN:** 0-8493-7058-2  
**www.auerbach-publications.com**

Las redes de sensores están formadas por un conjunto de ordenadores pequeñísimos (“nodos”), equipados con sensores que colaboran en una tarea común. Se diferencian de las redes tradicionales en muchos aspectos, especialmente en su energía limitada, espacio de memoria y capacidad de computación. Por ello, en *Security in Sensor Networks* se señala que estas redes están afectadas por vulnerabilidades que se podrían calificar de “únicas”. Por ello, el objetivo nuclear de la obra es cubrir todos los aspectos de interés de este tipo de redes de sensores.

El volumen se desarrolla en trece capítulos, en los que también participan un nutrido grupo de expertos internacionales, a través de los cuales se cubren todas las áreas de interés.

A su vez, estos capítulos se dividen en cinco bloques diferenciados: I. **Ataques**; II. **Cifrado, Autenticación y Marca de Agua**; III. **Gestión de claves**; IV. **Routing Seguro** y V. **Localización y Agregación segura y Cross-Layer**. Por supuesto, los temas abordados no son una representación exhaustiva del mundo de la seguridad en redes de sensores, pero sí tienen el mérito de mostrar unas estrategias y contenidos muy válidos por los que el lector profesional puede encaminar sus pasos e investigaciones al respecto. Su autor, **Nang Sayo** trabaja en la actualidad con el Departamento de Ciencia de Computación en la Universidad de Alabama y trabajó hasta 2004 en Micro Linear como arquitecto MAC involucrado en el desarrollo del estándar IEEE 802.11o Wi-Fi. ■