

## SEGURIDAD EN SISTEMAS OPERATIVOS WINDOWS Y LINUX

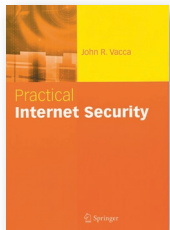
**Autores:** Julio Gómez y Raúl Baños  
**Editorial:** Ra-Ma  
**Año 2006 – 200 páginas**  
**ISBN:** 84-7897-749-X  
**www.ra-ma.es**

El volumen Seguridad en Sistemas Operativos Windows y Linux se presenta como una obra cuyo propósito es el de enseñar a asegurar un sistema informático haciendo uso de las herramientas que se suministran a través del propio sistema operativo que utiliza; herramientas que, además, en la mayoría de las ocasiones son gratuitas.

El manual está dividido en cinco bloques: **Introducción a la Seguridad Informática**, que define qué se entiende por seguridad informática y analiza la metodología que sigue un atacante para obtener información de un sistema; **Prevención de los Sistemas Informáticos**, con recomendaciones a nivel físico y lógico para asegurarlo y, además, muestra cómo instalar y configurar cortafuegos y servidores proxy; **Sistemas de Detección de Intrusos**, que ayuda a configurar un

sistema de detección de intrusos y a diseñar un *honeypot* para engañar a potenciales atacantes; **Copias de seguridad**, para realizar, restaurar y programar copias de seguridad en el sistema y, por último, **Análisis Forense**, que muestra cómo realizar el análisis forense de un equipo atacado para poder determinar el mecanismo que ha seguido el atacante para entrar en el sistema.

Al principio de cada capítulo se abordan los fundamentos teóricos para, posteriormente, aplicarlos a los sistemas operativos Windows y Linux. La dimensión de la obra en sí, y de los capítulos en particular, no permite más que una sucinta referencia a los temas propuestos; no obstante, a través de la página web del libro, el lector puede descargarse software referenciado a lo largo del mismo y otros recursos. ■



## PRACTICAL INTERNET SECURITY

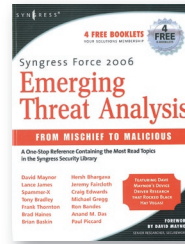
**Autor:** John R. Vacca  
**Editorial:** Springer  
**Año 2007 – 536 páginas**  
**ISBN:** 0-387-40533-X  
**www.springer.com**

Dado que las organizaciones actuales incrementan sus sistemas de conexión a través de redes empresariales y VPNS, y aumentan sus contactos con clientes, competidores, navegantes, e incluso *hackers* a través de Internet, se hace cada vez más necesario que los profesionales web se entrenen en técnicas para proteger eficazmente sus sitios frente a amenazas externas e internas.

En este sentido, esta nueva obra del veterano **John R. Vacca** es un manual profesional que revela cómo preparar el terreno para que las comunicaciones sean seguras dentro de las organizaciones y entre los usuarios en general. Asimismo, pretende proveer del conocimiento fundamental necesario para analizar los riesgos de los sistemas y poner en práctica una política de seguridad que proteja el activo de la información de potenciales intrusiones, daños o

robos. Por ello, el volumen proporciona docenas de escenarios reales y ejemplos, así como la instrucción concreta para asegurar comunicaciones y sitios web.

En concreto, muestra las vulnerabilidades más comunes de los sitios web, así como el modo de realizar comunicaciones seguras a través de redes desprotegidas. Todos los administradores de sistemas y responsables de seguridad TI podrán encontrar en este libro un recurso práctico. La obra está organizada en quince bloques que suman un total de 38 capítulos y siete apéndices, donde se hace una introducción general a la seguridad en Internet para, posteriormente, introducirse en temas como el desarrollo de políticas de seguridad, redes interconectadas, el principal punto de vulnerabilidad, o la configuración de sistemas operativos y redes seguras. ■



## EMERGING THREATS ANALYSIS. Syngress Force 2006

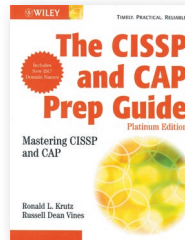
**Autores:** D. Maynor, L. James, Spammer-X, T. Bradley, F. Thornton, B. Haines, B. Baskin, H. Bhargava, J. Faircloth, C. Edwards, M. Gregg, R. Bades, A. M. Das y P. Piccard  
**Editorial:** Syngress Publishing, Inc.  
**Año 2006 – 610 páginas**  
**ISBN:** 1-59749-056-3 **www.syngress.com**

Esta antología de los siete libros sobre seguridad TI más leídos de la editorial Syngress contiene ejemplos de amenazas como VoIP, *phishing*, *malware* y *spyware*, e incluso analiza ataques a través de *wifi/Bluetooth* o RFID. Aunque está recomendado para cualquier responsable de proteger una empresa contra la próxima generación de amenazas, también intenta instruir al usuario informático común sobre qué peligros le acechan y cómo protegerse de ellos sin necesidad de convertirse en un experto.

Las siete obras recopiladas son: **Practical VoIP Security**, de Thomas Porter, que escribe sobre amenazas hacia los sistemas de comunicación VoIP y da recomendaciones al respecto; **Phishing Exposed**, de Lance James, habla sobre lo último en *phishing* y *spam*; **Combating Spyware in the Enterprise**, escrito por Brian Baskin,

trata sobre cómo detectar y eliminar el *spyware*; **Inside de SPAM Cartel**, en el que su autor ("*Spammer X*"), muestra cómo se crea el *spam* y por qué funciona tan bien; **Securing IM and P2P Applications for the Enterprise**, de Paul Piccard y de Craig Edwards, versa sobre la seguridad en Skype e IRC; **RFID Security**, escrito por Frank Thornton y Brad "Renderman" Haines, uno de los miembros más visibles de la comunidad de *wardriving*; y, por último, **Hack the Stack**, del experto en seguridad Michael Gregg.

En definitiva, Emerging Threats Analysis intenta hacer ver que la industria TI y los ordenadores en general, han dividido a la sociedad actual en dos grandes grupos: los informados y los no informados, y que hay gente "malvada" que intenta aprovecharse de la ignorancia tecnológica de los segundos. ■



## THE CIPS AND CAP PREP GUIDE. Platinum Edition

**Autores:** Ronald L. Krutz y Russell Dean Vines  
**Editorial:** Wiley Publishing, Inc.  
**Año 2007 – 1.236 páginas (Incluye CD-Rom)**  
**ISBN:** 0-470-00792-3  
**www.wiley.com**

Continuación de The CISSP Prep Guide, esta nueva y voluminosa obra pone al día cada uno de los diez dominios CISSP para reflejar el pensamiento/tecnología del momento, especialmente en las áreas de prevención del ciberterrorismo y la recuperación de desastres. El volumen incluye mejoras con contenidos extendidos no disponibles en ningún otro texto de estudio, más cuestiones actuales; mayor número de gráficos para la comprensión de los conceptos difíciles y, en general, material actualizado en todas las áreas que reflejan los cambios en los exámenes CISSP. En este sentido, también prepara para la nueva Credencial Profesional de Certificación y Acreditación (CAP), que evalúa el conocimiento, habilidades y capacidades requeridas para el personal involucrado en los procesos

de Certificación y Acreditación, con el mismo nivel que las credenciales CISSP y SSCP.

El volumen se divide en dos partes: **Revisión Centrada en los diez dominios CISSP**, formada por los diez primeros capítulos de la obra; y **Credencial Profesional de Certificación y Acreditación (CAP)**, compuesta por los capítulos del 11 al 15. Además, incluye siete apéndices con información adicional y un CD Rom con preguntas interactivas que utiliza las cuestiones y temas avanzados tratados en el libro. Como es evidente, la obra está destinada a profesionales de la seguridad y estudiantes que sean candidatos a las certificaciones CISSP, CAP, ISSEP, ISSAP o ISSMP o para aquellos que poseyéndola ya quieren actualizar y revisar sus conocimientos. ■