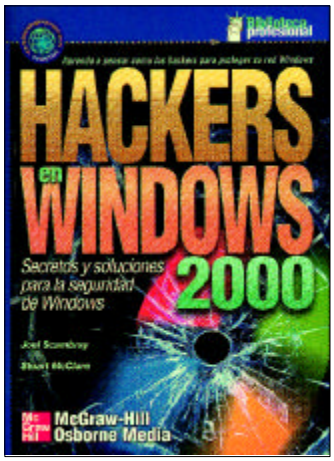
# HACKERS EN WINDOWS 2000 Secretos y Soluciones para la seguridad de Windows

**Autores: Joel Scambray y Stuart McClure**
**Editorial: Osborne McGraw Hill**
**Año 2002- 536 páginas - ISBN: 84-481-3398-6**
**www.mcgraw-hill.es**

El libro escrito por **Joel Scambray** y **Stuart McClure** conserva el estilo marcado en toda la serie, que tuvo como primer título el volumen 'Hackers', ya glosado en esta sección (véase SIC 47). La idea principal que subyace en la obra reseñada alude al análisis del desfase existente entre las configuraciones de fábrica de productos como IIS o Windows 2000, y lo que se necesita en realidad para su ejecución de forma segura. Los autores clasifican los riesgos que una instalación de Windows 2000 puede afrontar y estudian con detalle su funcionamiento para, seguidamente, ofrecer la solución de todos y cada uno de los ataques analizados.

A distintos niveles de organización, el libro se divide fundamentalmente en cinco partes: **Parte I. Fundamentos** [Temas: 1) fundamentos de seguridad en redes y sistemas, 2) la arquitectura de seguridad de Windows 2000 desde la perspectiva de los *hackers*]; **Parte II. Obtención del perfil** [Temas: 3) obtención de huellas y escaneo, 4) enumeración]; **Parte III. Divide y vencerás** [Temas: 5) *hacking* de CIFS/SMB, 6) escalada de privilegios, 7) obtención de interactividad, 8) extensión de la influencia, 9) limpieza]; **Parte IV. Explotación de servicios y clientes vulnerables,** [Temas: 10) *hacking* de IIS 5 y aplicaciones web, 11) *hacking* de SQL Server 12) *hacking* de Terminal Server, 13) *hacking* de clientes de Internet de Microsoft, 14) ataques físicos, 15) denegación de servicio]; **Parte V. La práctica de la defensa** [Temas: 16) características y herramientas de seguridad de Windows 2000, 17) el futuro de Windows 2000]. También se incluye un **Apéndice A. Lista de tareas de fortalecimiento de Windows 2000**, en el que se recogen, de forma resumida y ordenada, todas las contramedidas analizadas en la obra con el objetivo de poder construir un sistema desde cero.

Por último, cabe destacar que se han incluido dos nuevas características al final de cada capítulo: una sección **'Resumen'** y otra de **'Referencias y lecturas complemementarias'**. n



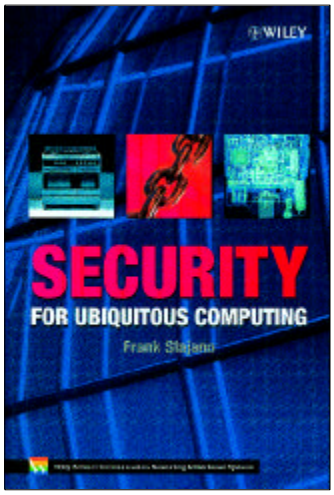

# SECURITY FOR UBIQUITOUS COMPUTING

**Autor: Frank Stajano**
**Editorial: John Wiley & Sons**
**Año 2002- 247 páginas - ISBN: 0-470-84493-0**
**www.wiley.com/ www.diazdesantos.es**

El libro escrito por **Frank Stajano** –miembro del Departamento de Ingeniería de la Universidad de Cambridge– sobre la seguridad de la 'informática ubicua' es una reflexión acerca del fenómeno que supone que las máquinas estén presentes en todos y cada una de los sitios y esferas de nuestra sociedad. Según el autor, la evolución en la historia de las comunicaciones digitales -desde el ordenador multimedia, pasando por Internet, la miniaturización, las comunicaciones inalámbricas y los sistemas de software distribuidos- va a hacer posible un cambio de paradigma, y por lo tanto, la necesidad de una visión más generalista.

Los temas analizados en este volumen se han seleccionado con el fin de confeccionar una panorámica general de todas las variables implicadas en el fenómeno de la informática ubicua, que van desde los términos de seguridad más esenciales hasta la criptografía. Después de realizar un recorrido generalizado de esta materias, el volumen se centra en los elementos tradicionales de un sistema distribuido, ofreciendo como material adicional dos anexos, uno en el que se ofrece un resumen elemental de funciones (A), y otro en el que se recomienda una serie de soluciones de seguridad para redes (B), además de una bibliografía comentada con enlaces a páginas web.

Por último, cabe destacar que el libro está diseñado para un público eminentemente técnico, pero *a priori* no es necesario tener unos conocimientos muy profundos sobre seguridad. Básicamente, el índice de esta obra está vertebrado en nueve capítulos: 1) Introducción, 2) Informática Ubicua, 3) Seguridad Informática, 4) Autenticación, 5) Confidencialidad, 6) Integridad, 7) Disponibilidad, 8) Privacidad, y 9) Conclusiones. n




# REAL WORLD LINUX SECURITY Intrusion Prevention, Detection, and Recovery

**Autor: Bob Toxen**
**Editorial: Prentice Hall**
**Año 2001- 694 páginas - ISBN: 0-13-028187-5**
**www.pearsoned.es**

El título del presente volumen forma parte de la colección de libros editados por Prentice Hall dedicados al sistema operativo Linux. En esta ocasión el volumen escrito por **Bob Toxen** analiza las implementaciones básicas de seguridad destinadas a la protección y recuperación frente a intrusiones de una red diseñada sobre este sistema de código abierto, a modo de guía 'paso a paso'.

Cabe destacar, especialmente, el análisis exhaustivo de cada ataque y forma de defensa, así como la valoración del nivel de daños (escala de 1 al 5), y los cuadros aclaratorios con consejos y direcciones de Internet donde obtener información adicional. Además, incluye un CD-Rom con las herramientas analizadas y desarrolladas por el autor, así como algunos de los ficheros de código abierto encontrados por el FBI, entre otras aportaciones.

Básicamente, el índice está estructurado de la siguiente forma: Capítulo 1) introducción; Parte I- '**Securizando' tu sistema** [Temas: 2) parcheos rápidos para problemas comunes, 3) ataques sencillos y cómo evitarlos, 4) vulnerabilidades comunes en los subsistemas, 5) intrusiones más frecuentes, 6) directrices de seguridad avanzada, 7) estableciendo políticas de seguridad, 8) confiando en otras máquinas, 9) vulnerabilidades difíciles, 10) casos reales, 11) vulnerabilidades más recientes]; Parte II– **Defensa frente a intrusiones** [Temas: 12) protegiendo tu sistema 13) preparando tu hardware, 14) preparando la configuración, 15) escaneando tu propio sistema]; Parte III- **Detectando una intrusión** [Temas: 16) monitorización de actividad, 17) escaneando tu sistema en busca de anomalías, 18) recuperándose de una intrusión, 19) retomando el control de tu sistema, 20) buscando y reparando el daño, 21) en busca de intrusos, 22) casos legales]; **Apéndices** A) recursos de Internet para consultar las últimas vulnerabilidades y sus parcheos, B) libros, CD-roms y vídeos C) servicios de red y puertos, D) listado de puertos.C, E) listado blockip.csh, F) listado Fpromisc.csh, G) listado overwrite.C, H) niveles de daño, I) sobre el Cd-Rom, J) glosario. n