# HACKERS 2
# Secretos y soluciones para la seguridad de redes

**Autores: Joel Scambray, Stuart McClure y George Kurtz**
**Editorial: Osborne McGraw-Hill**
**Año 2001 - 770 páginas - ISBN: 84-481-3187-8**
**Sitio: www.mcgraw-hill.es**

En la economía actual –como quien dice abierta las veinticuatro horas, completamente digital e hiperconectada–, la seguridad informática es un problema que afecta a todos. En este contexto, **«Hackers 2. Secretos y soluciones para la seguridad de redes»** realiza un profundo análisis de la forma en que los denominados *hackers* se infiltran en el negocio electrónico y cómo se les puede detener.

En síntesis, la obra aquí referenciada es la continuación –actualizada y ampliada–, del *best-seller* del mundillo de la seguridad '**Hackers**', editado de origen en 2000 y ya glosado en esta sección (véase SIC 44, abril 2001).

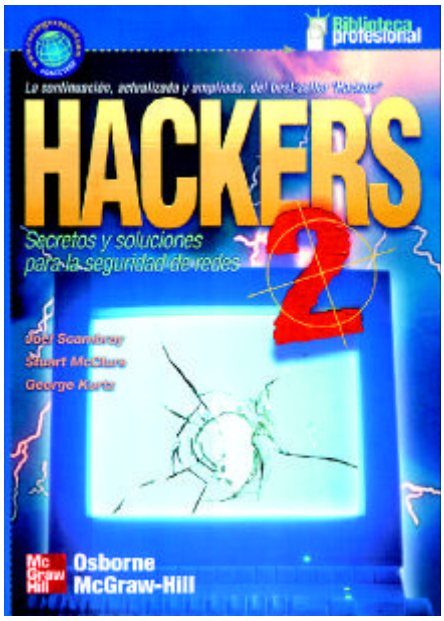
Efectivamente, el mundo de la seguridad en Internet y las redes se mueve incluso más rápido que la economía digital; por ello, en esta segunda edición se analizan todas las nuevas herramientas y técnicas que han surgido desde la publicación de la primera edición de este *best-seller*.

Como no podía ser de otra manera, dados los vertiginosos tiempos actuales en los que los desarrollos TIC –seguridad incluida– no sueltan el acelerador, sus autores, Scambray, Kurtz y McClure, han escrito un libro sobre seguridad todavía mejor y más actualizado que su predecesor, con muchos temas radicalmente nuevos y otros totalmente puestos al día, repleto de detalles técnicos y casos de estudio en un estilo que resulta sencillo de seguir.

### Novedades en la segunda edición

El mundo de la seguridad en Internet se mueve incluso más deprisa que la economía digital y muchas nuevas herramientas y técnicas han aparecido desde la publicación de la primera edición; por esta razón, los autores han realizado un enorme esfuerzo para seguir la pista a lo que realmente es importante en esta nueva edición, a la vez que han realizado todas las mejoras que los lectores les sugirieron a lo largo de este año.

Básicamente, sobre el total de la obra, unas 770 páginas, las correspondientes al nuevo contenido son unas 220, y de ellas, un par se han destinado al nuevo prefacio, escrito para la ocasión por el hoy directivo de Counterpane Internet Security y respetado 'titán' de la seguridad informática, Bruce Schneier. Un breve resumen de los grandes cambios realizados aborda las siguientes áreas:




Un nuevo capítulo entero, titulado «*Hacking del usuario de Internet*», que cubre las amenazas que se ciernen sobre los exploradores web, programas de correo electrónico, contenidos activos y todas las posibles formas de ataque de los programas cliente de Internet, incluyendo los nuevos desbordamientos del búfer del campo fecha del correo electrónico de Outllook y los gusanos del tipo ILOVEYOU.

También incluye un nuevo y extenso capítulo sobre los ataques y contramedidas en Windows 2000, nuevas metodologías actualizadas de pirateo utilizadas en el comercio electrónico en el Capítulo 15 y el análisis de todas las nuevas herramientas de Negación distribuida de servicio (DDoS) y los trucos que casi echan abajo a Internet en el mes de febrero de 2000 (Trinoo, TFN2K, Stacheldraht).

Asimismo, se aborda la cobertura de nuevas puertas traseras y técnicas forenses, incluyendo defensas contra las puertas traseras de Win9x, tal como sub7, se comentan en pormenorizado detalle nuevas técnicas y herramientas de descubrimiento de red, incluyendo un apartado actualizado de herramienta de exploración basadas en Windows, una explicación de cómo escuchar a escondidas en redes conmutadas utilizando la redirección ARP, y un análisis en profundidad de los ataques con trampas RIP.

Además, al principio de cada sección, se reseñan nuevos y actualizados análisis de casos que cubren ataques recientes sobre la seguridad de sistemas reales. Se da cobertura actualizada de ataques de seguridad contra Windows 9x, Millennium Edition (ME), Windows NT, Unix, Linux, NetWare y otras tantas plataformas informáticas, con sus contramedidas apropiadas.

Es de destacar especialmente un capítulo actualizado y revisado de *hacking* a través de conexiones telefónicas, el cual incluye información adicional sobre pirateo de los sistemas PBX y de correo de voz, así como un apartado actualizado sobre VPN.

El apartado visual también concede un valor suplementario a la obra. *Hacker 2* incluye nuevos gráficos que resaltan todos los ataques y las contramedidas, para que resulte sencillo acceder directamente a la información más importante.

Un nuevo sitio web asociado a la dirección *http://www.hackingexposed.com* que contiene noticias actualizadas y vínculos a todas las herramientas y recursos de Internet a los que se haga referencia en el presente libro.

En conclusión, todo este nuevo material se ha combinado para formar la Segunda Edición con un cien por cien más de contenido. El índice se ha vertebrado en cinco partes, las siguientes: **Parte I - Identificar el problema** (Análisis del caso: adquisición del objetivo. Temas: 1) Seguir el rastro, 2) Exploración, 3) Enumeración); **Parte II - Hacking del sistema** (Análisis del caso: conozca a su enemigo. Temas: 4) Hacking de Windows 95/98 y ME, 5) Hacking de Windows NT, 6) Hacking de Windows 2000, 7) Hacking de Novell NetWare, 8) Hacking de Unix); **Parte III - Hacking de la red** (Análisis del caso: ¡Sudar todas las pequeñas cosas! Temas: 9) Hacking de las llamadas de acceso telefónico, PBX, Voicemail y VPN; 10) Dispositivos de red; 11) Cortafuegos, 12) Ataques de negación de servicio (DoS); **Parte IV** (Análisis del caso: empleo de todos los trucos a su alcance para poder entrar. Temas: 13) Inseguridades de control remoto; 14) Técnicas avanzadas; 15) Hacking en la web; 16) Hacking del usuario de Internet); **Parte V - Apéndices** A) Puertos, B) Las catorce principales vulnerabilidades de seguridad, y C) Nuestro sitio Web. n