



WINDOWS INTERNET SECURITY

Protecting your Critical Data

Autores: Seth Fogie y Cyrus Peikari

Editorial: Prentice Hall

Año 2002 - 370 páginas - ISBN: 0-13-042831-0

www.personed.es

En los últimos años se han publicado numerosos libros enfocados a proteger los ordenadores de ataques realizados desde Internet. Por lo general, son obras que más parecen escritas para los atacantes —por la exhaustividad con que desmenuzan las herramientas de ataque y defensa— que para el común de los administradores, que no disponen del tiempo necesario para interesarse por las primeras, ni para penetrar en los múltiples entresijos de las segundas. Ello dejando al margen que tales entresijos son a menudo superfluos para los fines perseguidos: proteger la red y los sistemas a ella conectados.

Por otra parte, este detallismo hace de tales obras —con independencia de las dotes divulgativas de sus autores— de farragosa prosa y más penosa lectura. Todo lo cual conlleva un imposible estudio integral —es decir, de principio a fin—, sirviendo sólo como obras de consulta de temas puntuales, lo cual, sin ser despreciable, no es siempre lo idóneo.

En contraste, el manual que en esta ocasión nos ocupa: **WINDOWS INTERNET SECURITY: Protecting your critical data**, de Seth Fogie y Cyrus Peikari, editado por Prentice Hall el pasado año, trata de la seguridad frente a Internet con un estilo fluido y fresco, lo que hace de su lectura una tarea interesante y amena, seguro que incluso para los relativamente legos en seguridad. De este modo, y ello es lo más difícil para el autor y valioso para el lector, el equilibrio entre profundidad de tratamiento y facilidad de lectura, alcanza su punto álgido.

El texto se centra exclusivamente en sistemas Windows (distinguiendo en los ejemplos entre sus dos grandes familias: 95/98/Millennium y 2000/XP), lo que sin duda desilusionará a los —cada vez más numerosos— liberados del yugo de Microsoft y su altanera conducta. Empero, y en descargo de los autores, es obvio que el tratamiento conjunto de ambos mundos haría a la obra de difícil manejo, además de requerir de sus redactores unas dotes enciclopédicas inalcanzables hoy en día.

El libro está estructurado en cinco partes o secciones en las que se introducen los ordenadores e Internet (el campo de batalla, en cita literal de sus autores), se presentan los métodos de ataque y la psicología de los delincuentes, se exponen los sistemas de defensa, se esbozan varias formas de comprometer la intimidad de los usuario, se aventuran las tendencias de futuro y se ofrecen dos muestras de temas avanzados: el registro y la recuperación de desastres. En todas, son de reconocer su claridad y concisión, lo que consigue —al margen de la cuidadosa redacción y didáctico planteamiento—, merced al auxilio de frecuentes

metáforas del mundo real, y al recurso a ilustraciones obtenidas mediante la captura de abundantes pantallas de ordenador.

Pasando a desbrozar someramente la obra, la primera parte, *Studying the battleground*, la conforman tres capítulos, en los que se exponen las bases mínimas imprescindibles, acerca de sistemas y redes, para abordar la seguridad. Aunque sea una hipérbola afirmar —como hacen sus autores— que la lectura de su obra no presupone conocimientos previos de ordenadores, bien es verdad que esta primera sección contribuye a que usuarios relativamente legos en informática adquieran unos conocimientos muy valiosos para el seguimiento del texto. Aún más, dado que aquí se avanzan temas después extensamente desplegados, su lectura no debiera considerarse superflua por ningún interesado.

La segunda división, *Knowing the enemy*, se detiene en sus cuatro capítulos en la forma de actuación de los *hackers* (adviento, para evitar el rasgado de vestiduras de algunos, que es el término usado por los autores). Para ello, el capítulo cuatro: *Know your enemy*, categoriza a los atacantes, destacando la distinción entre *hackers* y *script kiddies* en cuanto a motivación, objetivos y métodos. Mientras, en los dos siguientes: *Hacking Techniques for unauthorized access* y *Hacking Techniques for attacks*, se exponen, junto con todas las técnicas archiconocidas de exploración y ataque: analizadores de red, secuestro de sesión, inundación, desbordamiento de memoria, etc., otras también sabidas, aunque escasamente estudiadas en la bibliografía, como la ingeniería y el espionaje social. Para concluir, el capítulo siete: *Walk-Through of a hacker attack*, sigue a un atacante-tipo en los pasos que sucesivamente acomete para ejecutar sus fechorías: búsqueda de un objetivo, recopilación de información, planificación, ejecución y borrado de huellas.

La parte más extensa de todas las que conforman el compendio es la tercera: *Planning the defense*, donde expone (ciertamente mezclando técnicas, sistemas y procedimientos, lo que no deja de ser estéticamente rechazable) los pilares de cualquier sistema integral de protección: cifrado, cortafuegos, antivirus, planes de recuperación, junto con algún otro material disperso y de menor interés. En los siete capítulos en que se articula, del octavo al decimocuarto, podemos encontrar algunos de los más brillantes de la obra, como son el noveno, décimo, duodécimo y decimocuarto. Se comienza con el séptimo, de título *Building your defense strategy*, en el que se acota el objetivo de esta parte, sirviendo a la vez de presentación de la misma. Aunque satisfactoria como introducción, son obje-

tables algunas de sus definiciones (por ejemplo, la de caballo de Troya) que distan de ser unánimemente aceptadas. El noveno, *Personal firewall and intrusion detection systems*, es una notable exposición del tema que le presta el título, con interesantes digresiones, como aquella en que debate la efectividad de los cortafuegos personales. Además, se estudian las bases comunes a los dispositivos de este tipo, y, muy de reseñar, se comparan cuatro de los más populares de ellos. El décimo, *Stop sharing your computer*, teoriza y conciencia sobre los riesgos de las carpetas compartidas, mostrando cómo deshabilitar las comparticiones allí donde existan. Sin embargo, el interés alcanza su mínimo en el undécimo, *E-commerce security overview*, de escasas ocho páginas, obviamente insuficientes para acomodar las facetas de seguridad de dicha modalidad comercial. Nuevamente se eleva el interés en *Mastering network tools*, con una extensa exposición de las herramientas de rastreo de programas malignos en el ordenador y de seguimiento del rastro del atacante. Seguidamente, *Virus, worms and trojans horses*, es una convencional exposición de los especímenes indicados, y que poco incrementará el conocimiento de los lectores, salvo acaso por su último epígrafe, *Hostile web pages and scripting*. Finalmente, el decimocuarto *Malicious code*, parte de los lenguajes máquina, para elevarse hasta los lenguajes de script y proseguir con el uso de éstos en el desarrollo de programas malignos. El último epígrafe muestra el código del Melissa, explicando sus partes esenciales, lo que facilita la comprensión de los códigos malignos.

La sección cuarta, *Moving with stealth*, ya mucho más breve, comienza con *Privacy and anonymity*, en donde destaca la exposición de las cookies (a partir de varias reales tomadas como ejemplo). También son de interés los apartados que ilustran los peligros para nuestra intimidad de la navegación desprevenida por la red. Este mismo objetivo, proteger nuestra intimidad, es el que anima el último capítulo de esta parte, de ilustrativo título: *Big brothers is watching you*.

Igualmente breve se presenta la parte quinta, *Future trends*, donde el interés de su primer capítulo, *Windows XP*, proviene, más que de su extenso tratamiento, de la aún escasa bibliografía acerca de la seguridad de este sistema. El segundo y último, *Future security threats*, explora las amenazas por venir, algunas ya muy presentes, como las derivadas del creciente uso de las redes inalámbricas o de los dispositivos móviles.

La obra concluye con una última sección, *Advanced topics*, nombre justificado por la materia tratada en su primer capítulo, *Registry editing*, (pues sólo lectores experimentados, o muy osados, deberían atreverse con el registro), aunque no por el segundo, *Disaster recovery*, que además de pobre en su contenido, poco tiene que explique su calificativo de avanzado.

En conclusión, es una obra de amplia visión cuya lectura no defraudará, fundamentalmente a los que precisen de una primera aproximación a la seguridad que conjuga equilibradamente la profundidad de tratamiento con la claridad expositiva. ■

ARTURO RIBAGORDA GARNACHO

Catedrático y Director

del Dpto. de Informática

UNIVERSIDAD CARLOS III DE MADRID

arturo@inf.uc3m.es