



HACKERS

SECRETOS Y SOLUCIONES PARA LA SEGURIDAD DE LAS REDES

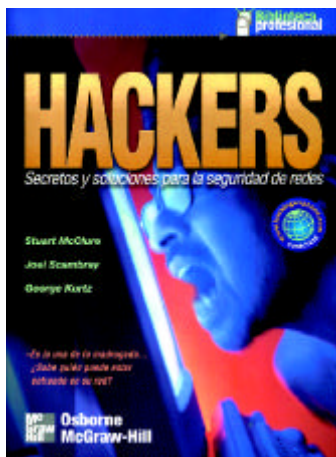
Autores: Stuart McClure, Joel Scambray, George Kurtz
Editorial: Osborne McGraw-Hill
Año 2000 - 514 páginas - ISBN: 84-481-2786-2
Sitio: www.mcgraw.hill.es

Un debate recurrente en este mundo de la seguridad versa sobre la oportunidad de divulgar –urbi et orbi– las vulnerabilidades de los programas que corren en nuestras máquinas, y ello aunque tal revelación pública se acompañe –como hace el CERT o, para sus productos, el Boletín de Seguridad de Microsoft– del oportuno «parche» corrector. Pero en realidad esta polémica trasciende los errores del software y su difusión, y en su enunciado más general –ocultismo frente a transparencia– se engloban debates de gran solera, como el que largo tiempo enfrentó a los defensores del público conocimiento de los algoritmos criptográficos de uso en el mundo civil, con los valedores a ultranza de su mantenimiento en secreto. Como es sabido por los aficionados a la materia, la pugna quedó zanjada el siglo XIX por el criptógrafo holandés, aunque afinado en Francia, Kerckhoffs¹: «La seguridad del cifrado debe de residir, exclusivamente, en el secreto de la clave», aunque existan nostálgicos que aún hoy sigan pregonando las excelencias del secretismo.

A este respecto, son muy instructivos dos estudios de muy reciente publicación. El primero, por orden de aparición, es el artículo *Windows of vulnerability: A case study analysis*, aparecido en el pasado diciembre en la prestigiosa revista *Computer* órgano de la *Computer Society*, que como es comúnmente sabido es una de las sociedades del no menos prestigioso IEEE. En dicho trabajo se muestra cómo las vulnerabilidades ya corregidas (mediante los pertinentes «parches») constituyen el objetivo principal de los intentos de intrusión, la mayoría de los cuales concluyen, sorprendentemente, con éxito. Es más, el mayor número de ataques se produce meses después de dadas a conocer vulnerabilidades y sus correcciones.

El segundo estudio, más cercano en el tiempo, ha sido objeto de atención días atrás por parte de diversos servicios de información de seguridad, que se hacían eco del aviso² del FBI's *National Infrastructure Protection Center* (NIPC) acerca de recientes ataques contra equipos de comercio electrónico y banca por Internet. En particular, el Boletín de Seguridad de Microsoft, de ocho de marzo de 2001, lo hacía en los siguientes términos: «Uno de los aspectos más inquietantes de estos ataques es que virtualmente todos ellos se realizan mediante vulnerabilidades conocidas, para las que están disponibles parches desde hace meses o, en ocasiones, años».

Así pues, parece cierto que el conocimiento de una vulnerabilidad (aunque acompañada de su parche) origina un importante incremento de ataques a la misma, pero no existe duda alguna de que la



comunidad mundial de *kackers*, *crackers* y atacantes de todo pelaje tienen sus propios canales y cualquier vulnerabilidad, más pronto que tarde, termina siendo conocida por todos ellos. De modo que, puestas así las cosas, lo mejor es el desarrollo rápido de soluciones a las debilidades del software, su presta difusión e inmediata instalación por los responsables de las redes. Naturalmente, siempre existirán algunos de éstos que, sea por negligencia o por exceso de trabajo, no atenderán a los avisos y pertinentes actualizaciones, manteniendo a sus sistemas en permanente riesgo, hasta la instalación

de una nueva versión del producto ya con la corrección incorporada.

En conclusión, se puede aseverar que en esta incipiente sociedad de la información, la mejor arma contra la variopinta caterva de delincuentes informáticos es la información, y ello es lo que pretende el libro que nos ocupa, de turbador título: **HACKERS**, pero ilustrativo y ajustado subtítulo: **Secretos y soluciones para la seguridad de redes** (traducción de *Hacking Exposed: Network Security Secrets and Solutions*, McGraw-Hill, 1999), traducido y publicado en 2000. Escrito por tres profesionales de la seguridad, empleados en una multinacional de la consultoría, el manual tiene como público objetivo los administradores de redes, aunque el nivel expositivo del mismo, y su pormenorizada explicación, permite su lectura a cualquier usuario avanzado.

Aunque en la introducción se puede hallar una frase provocadora: «En este libro se proporcionan instrucciones sencillas y detalladas de cómo introducirse subrepticiamente en redes informáticas», la realidad matiza sustancialmente la categórica afirmación anterior, pues a la par que dichas instrucciones, también se proporcionan contramedidas para fortificar el sistema, de modo que no se puede encontrar en toda la obra una sola vulnerabilidad que no vaya acompañada a renglón seguido de la (o las) contramedida oportuna.

Destacan sobremano en la obra las abundantisimas fuentes de información referenciadas en todos los capítulos (y muy singularmente en los apéndices C y D), que constituyen una delicia para aquellos que deseen profundizar aún más en los aspectos tratados. Igualmente es de justicia destacar las numerosas imágenes de pantallas y tablas que ayudan a sobrelevar la gran cantidad de información proporcionada.

La obra se estructura en torno a cuatro partes y seis apéndices. En la primera de aquellas: **Identificación del problema**, se estudian –en tres capítulos– los caminos, tortuosos e imaginativos a menudo y

siempre tediosos, que sigue el delincuente para tantear las posibles vías de ataque al sistema elegido, así como la exploración de éstas para averiguar las más fructíferas. Naturalmente, acorde con los objetivos de la obra, ya desde esta parte se dan a conocer los instrumentos de detección de estos escarceos y algunos consejos para no dar pistas a los delincuentes, ilustrando esto con diversos casos reales.

La segunda parte, **Hacking del sistema**, se consagra a la exposición de los agujeros de seguridad que presentan los principales sistemas operativos, más concretamente: Windows (9x y NT), Netware de Novell y Unix, dedicándose un capítulo a cada uno de ellos. En estos capítulos se detallan tanto los ataques remotos como los locales, los procedimientos usuales para ir escalando privilegios, las técnicas comunes de ocultación de los rastros de la agresión, los síntomas de ésta y la estela que deja, aspectos estos dos últimos que permiten reaccionar al administrador de la red.

En **Hacking de la red**, tercera parte del manual, se tratan las técnicas, equipos y sistemas propios de las redes: VPN y acceso telefónico, encaminadores, cortafuegos, etc., mostrando sus puntos débiles y cómo se aprovechan de ellos los delincuentes. También se contemplan en el último capítulo los ataques de negación de servicio, DoS, aunque por la fecha de redacción de la edición inglesa, 1999, no se han incorporado los ataques de negación distribuida de servicio, DDoS, popularizados en 2000. Como es norma, tras la habitual presentación de debilidades, se muestran las contramedidas para contrarrestarlas o, al menos, paliarlas.

Para concluir el tratado, en la parte cuarta: **Hacking del software**, aparecen algunos problemas que no son encuadrables en las anteriores partes, según la opinión –muy discutible– de los autores. Estos problemas comprenden el acceso remoto a los sistemas (bendición y al tiempo azote para los administradores, por las facilidades que les ofrece de gestión a distancia y que son una delicia para los delincuentes), los ataques al software: secuestro de sesión, troyanos, puertas traseras, etc. y las vulnerabilidades de los servidores *web*. Las posibles intrusiones aquí tratadas son las más sofisticadas y, al tiempo, las que en el día de hoy más quebraderos de cabeza dan a los administradores.

En resumen, nos hallamos en presencia de un libro actual (aunque con la cadencia de aparición de vulnerabilidades vendrá obsoleto en poco), útil para los usuarios avanzados, e imprescindible para los administradores de red, que carecían hasta su publicación de un compendio de este calibre de vulnerabilidades, ataques y métodos de defensa. A partir de ahora, cualquiera de estos profesionales debería pensárselo mucho antes de achacar a la falta de información –o dificultad de encontrarla– los fallos de seguridad de los sistemas de los que se responsabilizan. ■

¹ Auguste Kerckhoffs von Nieuwenhof, 1835-1903, autor de uno de los libros históricos de la *criptografía*, *La cryptographie militaire*.

² <http://www.nipc.gov/warnings/advisories/2001/01-003.htm>

ARTURO RIBAGORDA
 Catedrático de la Universidad
 Carlos III de Madrid