Hackear al hacker

Aprende de los expertos que derrotan a los hackers

Roger A. Grimes

Marcombo

Edición original publicada en inglés por John Wiley & Sons, Inc., Indianapolis, Indiana, con el título: *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*, ISBN 978-1-119-39621-5 © Roger A. Grimes 2017

Título de la edición en español:

Hackear al hacker. Aprende de los expertos que derrotan a los hackers

Primera edición en español, 2018

www.marcombo.com

Diseño de la cubierta: Wiley
Imagen de la cubierta: © CTRd/Getty Images

Traductora: Sònia Llena
Revisor técnico: Pablo Martínez
Correctora: Meritxell Peleato
Directora de producción: Mª Rosa Castillo

ISBN: 978-84-267-2679-7

D.L.: B-25492-2018

Impreso en Printek

Printed in Spain

Sumario

1 ¿Qué tipo de *hacker* eres tú?

Hace unos años, me mudé a una casa que tenía un maravilloso garaje adosado. Era perfecto para aparcar y proteger mi bote y mi pequeña autocaravana. Era de construcción sólida, sin nudos en las maderas. La instalación eléctrica era profesional y las ventanas, de alta calidad y preparadas para vientos de 150 mph (241,39 km/h). Gran parte del interior estaba revestido con una aromática madera de cedro rojo, el mismo tipo que usaría un carpintero para revestir un baúl o un ropero para que oliera bien. Aunque yo no sé ni clavar un clavo, fue fácil para mí ver que el constructor sabía bien lo que hacía, cuidaba la calidad y se preocupaba por los detalles.

Unas semanas después de mudarme, vino un agente de policía y me contó que el garaje había sido construido de forma ilegal unos años atrás sin licencia y que tenía que derribarlo o hacer frente a una serie de multas por cada día de incumplimiento. Fuí a la policía para solicitar una dispensa, ya que el garaje estaba construido desde hacía muchos años y me lo habían vendido como parte de la compra de la vivienda. Nada que hacer. Tenía que ser derribado de inmediato. Las multas de un solo día eran más de lo que podía conseguir vendiendo los componentes para chatarra si lo derribaba con cuidado. Financieramente hablando, cuanto antes lo derribara y lo hiciera desaparecer, mejor.

Saqué un mazo de martillo (básicamente, una hacha de hierro gruesa para trabajos de demolición) y en unas horas ya había convertido toda la estructura en un montón de madera y otros residuos de construcción. No me costó comprender que el trabajo que a un artesano cualificado le había costado probablemente semanas, o meses, en construir, yo lo había destruído con mis manos no cualificadas en mucho menos tiempo.

Contrariamente a lo que muchos piensan, el hackeo malicioso tiene más de mazo que de artesano.

Si eres lo suficientemente afortunado para dedicarte al hackeo informático, tendrás que decidir si lo que quieres es proteger los bienes comunes o bien

conformarte con objetivos más pequeños. ¿Quieres ser un *hacker* malo o un defensor justo y poderoso? Este libro es la prueba de que los *hackers* más inteligentes y mejores trabajan para el lado bueno. Ellos deben ejercitar sus mentes, crecer intelectualmente, y no han de preocuparse por si los arrestan. Trabajan a la vanguardia de la seguridad informática, se ganan la admiración de sus compañeros, promueven el avance humano en nombre de lo bueno y son recompensados económicamente por ello. Este libro trata sobre héroes a veces desconocidos que hacen posible nuestras increíbles vidas digitales.

NOTA Aunque los términos *hacker* o *hackeo* pueden hacer referencia a una persona o actividad con buenas o malas intenciones, el uso popular tiene casi siempre una connotación negativa. Yo he podido descubrir que los *hackers* pueden ser buenos y malos, pero en este libro utilizo los términos sin calificaciones que impliquen connotaciones negativas o positivas simplemente para ahorrar espacio. Toma el significado completo de las frases para juzgar la intención de los términos.

La mayoría de los *hackers* no son genios

Desgraciadamente, casi todos los que escriben sobre *hackers* informáticos criminales sin una experiencia real los idealizan como si fueran seres superinteligentes y míticos, como dioses. Ellos pueden adivinar cualquier contraseña en menos de un minuto (especialmente bajo la amenaza de una pistola, si os creéis todo lo que viene de Hollywood), entrar en cualquier sistema y crackear cualquier secreto encriptado. Trabajan sobre todo por la noche y beben grandes cantidades de bebidas energéticas mientras ensucian sus puestos de trabajo con restos de patatas fritas y *cupcakes*. Un alumno utiliza la contraseña robada de su profesor para cambiar sus notas y los medios de comunicación lo adulan como si fuera el nuevo Bill Gates o Mark Zuckerberg.

Los *hackers* no tienen por qué ser brillantes. Yo soy la prueba viviente. A pesar de que he podido entrar en todos los lugares en los que me han contratado para hacerlo, nunca he entendido por completo la física cuántica o la teoría de la relatividad. Suspendí dos veces inglés en el instituto, no he sacado nunca más de un Bien en matemáticas y mi promedio de notas del primer semestre en la universidad fue un 0,62: 5 Insuficientes y 1 Sobresaliente. El único Sobresaliente fue en

natación, porque había sido vigilante de playa durante 5 años. Mis malas notas no eran solo porque no me esforzara. Simplemente no era tan inteligente y no me esforzaba. Más tarde aprendí que estudiar y trabajar duro suele ser más valioso que haber nacido inteligente. Terminé acabando mi carrera universitaria y sobresaliendo en el mundo de la seguridad informática.

Aun así, incluso cuando a los *hackers* malos los escritores no los llaman superinteligentes, los lectores suelen asumir que lo son porque siempre se muestran practicando algún tipo de magia negra avanzada que el resto del mundo no conocemos. En la psique colectiva mundial, es como si «*hacker* malicioso» y «superinteligencia» deban ir siempre juntos. Y esto no es así. Unos cuantos son inteligentes, la mayoría son normales y algunos no son demasiado brillantes, como el resto del mundo. Los *hackers* simplemente conocen datos y procesos que el resto de la gente ignora, como un carpintero, un fontanero o un electricista.

Los defensores son más que *hackers*

Si hacemos una comparación intelectual, como promedio, los defensores son más inteligentes que los atacantes. Un defensor debe saber todo lo que sabe un *hacker* malicioso y, además, cómo detener el ataque. Y esa defensa no funcionará a menos que casi no requiera participación del usuario final, trabaje de forma silenciosa entre bambalinas y lo haga siempre a la perfección (o casi). Muéstrame un *hacker* malicioso con una técnica particular y yo te mostraré múltiples defensores que son mejores y más inteligentes. Lo que ocurre es que el atacante normalmente recibe más portadas. Este libro contiene argumentos para un tratamiento más equilibrado.

Los *hackers* son especiales

Aunque yo no clasifico a todos los *hackers* como superinteligentes, buenos o malos, todos ellos comparten una serie de características. Una de estas características que tienen en común es una gran curiosidad intelectual y el deseo de probar cosas fuera de la interfaz y los límites proporcionados. No tienen miedo a hacerlo a su manera. Los *hackers* informáticos suelen ser *hackers* de la vida, que hackean todo tipo de cosas más allá de los ordenadores. Hay gente que, cuando llega al control de seguridad de un aeropuerto, ya está pensando

en cómo podría colar un arma por los detectores, aunque no tenga ninguna intención de hacerlo. Gente que piensa si las entradas tan caras de un concierto se podrían falsificar fácilmente, aunque no tenga ninguna intención de entrar gratis. Gente que cuando compra un televisor, se pregunta si podrá acceder a su sistema operativo para conseguir alguna ventaja. Muéstrame un *hacker* y yo te mostraré a alguien que siempre está cuestionando el *status quo* e investigando.

NOTA Mi hipotético esquema para colar armas por el control de seguridad del aeropuerto pasa por utilizar sillas de ruedas y esconder las armas y los explosivos dentro de las partes de metal. Las sillas de ruedas normalmente pasan por los controles de seguridad de los aeropuertos sin ser sometidas a fuertes registros.

Los *hackers* son persistentes

Después de la curiosidad, la característica más útil de un *hacker* es la persistencia. Todos los *hackers*, sean buenos o malos, conocen la agonía de pasar horas y horas intentando una y otra vez que algo funcione. Los *hackers* maliciosos buscan debilidades en las defensas. Un error del defensor hace toda la defensa más débil. Un defensor debe ser perfecto. Todos los ordenadores y los programas informáticos deben ser parcheados, toda configuración, adecuadamente segura, y todo usuario final debe estar perfectamente capacitado. O, al menos, este es el objetivo. El defensor sabe que las defensas aplicadas no siempre funcionan o que no son aplicadas como deberían, por lo que crea niveles de «defensa en diferentes profundidades». Tanto los *hackers* maliciosos como los defensores buscan las debilidades, aunque desde lados opuestos del sistema. Ambas partes participan en una guerra en curso con distintas batallas, ganadores y vencidos. La parte más persistente será quien gane la guerra.

Los sombreros de los *hackers*

Yo he sido *hacker* toda mi vida. Me han pagado para acceder a sitios (tenía autorización legal para hacerlo). He crackeado contraseñas, me he introducido en redes de trabajo y he desarrollado *malware*. En ningún momento he incumplido la ley ni cruzado los límites éticos. Esto no significa que no haya habido gente que me haya tentado a hacerlo. Durante estos años, he tenido amigos

que me han pedido que entrara en los chats sospechosos del teléfono móvil de su esposa, jefes que me han pedido que accediera al correo electrónico de su superior o gente que me ha pedido que irrumpiera en el servidor de un *hacker* malo (sin autorización judicial) para intentar evitar que continuara hackeando. Cuando empiezas, tienes que decidir quién eres y cuál es tu ética. Yo decidí que sería un *hacker* bueno (un *hacker* «de sombrero blanco»), y los *hackers* de sombrero blanco no hacen cosas ilegales ni no éticas.

Los *hackers* que participan habitualmente en actividades ilegales y no éticas se denominan «de sombrero negro». Los *hackers* que actúan como un sombrero blanco pero que, a escondidas, realizan actividades de sombrero negro se conocen como «de sombrero gris». Mi código moral es binario en este tema. Los *hackers* de sombrero gris son *hackers* de sombrero negro. O haces cosas ilegales o no las haces. Si robas un banco serás un ladrón, hagas lo que hagas con el dinero.

Esto no significa que los *hackers* de sombrero negro no puedan convertirse en *hackers* de sombrero blanco. Esto siempre ocurre. La pregunta para algunos de ellos es si podrán convertirse en *hackers* de sombrero blanco antes de pasar un tiempo sustancial en prisión. Kevin Mitnick (`https://es.wikipedia.org/wiki/Kevin_Mitnick`), uno de los *hackers* detenidos más conocidos de la historia (y presentado en el Capítulo 5), vive actualmente como defensor ayudando al bien común. Robert T. Morris, el primero en programar y lanzar un gusano que tumbó Internet (`https://es.wikipedia.org/wiki/Robert_Tappan_Morris`), finalmente fue galardonado como miembro de la Association for Computing Machinery (`http://awards.acm.org/award_winners/morris_4169967.cfm`) «por sus contribuciones en redes de ordenadores, sistemas distribuidos y sistemas operativos».

Al principio, el límite entre el hackeo legal e ilegal no estaba tan claramente definido como ahora. De hecho, a la mayoría de los primeros *hackers* ilegales se les dio un estado de culto de superhéroe. Incluso no puedo evitar sentirme atraído por alguno de ellos. John Draper (también conocido como Captain Crunch) utilizó un silbato de juguete que se distribuía en las cajas de los cereales Cap'n Crunch para generar un tono (2.600 Hz) que podía servir para realizar llamadas telefónicas de larga distancia gratis. Muchos de los *hackers* que han puesto al descubierto información privada para «una buena causa» han sido aplaudidos. Sin embargo, con pocas excepciones, yo no he adoptado nunca una visión idealizada de los *hackers* maliciosos. Siempre he sido de la opinión que la gente que hace cosas sin autorización en ordenadores e información de otras personas está cometiendo actos criminales.