La amenaza hacker

Deepak Daswani

Prólogo de **Mikko Hypponen**

Todo lo que empresarios, directivos, profesionales y particulares deberíamos saber para protegernos adecuadamente

Un hacker experto en ciberseguridad nos explica cómo evitar ataques, robos, estafas y otros peligros en la era de la revolución digital

DEUSTO

La amenaza hacker

Todo lo que empresarios, directivos, profesionales y particulares deberíamos saber para protegernos adecuadamente

DEEPAK DASWANI

EDICIONES DEUSTO

© de esta edición: Centro de Libros PAPF, SLU., 2018
Deusto es un sello editorial de Centro de Libros PAPF, SLU.
Av. Diagonal, 662-664
08034 Barcelona

www.planetadelibros.com

ISBN: 978-84-234-2931-8
Depósito legal: B. 21.306-2018
Primera edición: octubre de 2018
Preimpresión: Medium Preimpressió
Impreso por Romanyà Valls, S. A.

Impreso en España - *Printed in Spain*

Contenido

1

Hackers, *Script Kiddies* y el vecino que te roba el wifi

Los ríos de información que nos llegan a través de diferentes canales respecto a la figura del hacker generan una imagen pública que no siempre se corresponde con la realidad. Sobre la idea del hacker giran todo tipo de especulaciones, falsos mitos, debates e incluso dilemas morales. Es inevitable comenzar definiendo este polémico concepto con el objetivo de transmitir su significado real, que para nosotros tiene, de hecho, una connotación positiva.

Sin embargo, esta visión no ha sido compartida tradicionalmente por medios de comunicación u organismos oficiales. Como muestra, el diccionario de la RAE define al hacker en su primera acepción como «pirata informático». Fue gracias a la insistencia de nuestro gremio que desde principios de 2018 se incorporó una segunda acepción mucho más próxima a lo que para nosotros es un hacker: «Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora».

¿Qué es un hacker?

El término hacker fue acuñado por primera vez en los años sesenta entre los informáticos del Instituto Tecnológico de Massa-

chusetts (MIT). De ahí que siempre haya estado ligado al ámbito tecnológico. Su traducción literal no es otra que la de «curioso».

Un hacker es una persona inquieta, que no se conforma con utilizar la tecnología a nivel de usuario, sino que ansía profundizar en cada detalle. Es una persona apasionada por ahondar en el conocimiento de los sistemas, por superar los límites que la tecnología nos impone, llevándola más allá y logrando hacer cosas para las que, en principio, no fue concebida. Desde incorporar nuevas funcionalidades que *a priori* eran impensables, hasta romper las barreras de seguridad que tratan de impedir su control. ¿Cómo? Descubriendo vulnerabilidades. Encontrarlas es fruto de horas y horas de aprendizaje, lectura, experimentación e investigación. Eso es realmente un hacker, y para todo lo demás existen otras denominaciones.

> Un hacker no es un pirata informático como dice el diccionario de la RAE, sino todo lo contrario.
>
> Erróneamente asociado a la ciberdelincuencia, un hacker es en realidad alguien curioso, inquieto, apasionado por conocer cada detalle de lo que estudia, sea tecnología u otra cosa.

Esta definición implica diferentes conceptos y aspectos que iremos desgranando, pero difiere radicalmente de la de pirata informático. Los piratas, los que utilizan todo este conocimiento y estas técnicas para hacer el mal, son los llamados ciberdelincuentes, que trataremos en el próximo capítulo. Quizá en el desconocimiento de este último concepto radica la confusión de la gran masa social. Debido a la tradicional estigmatización del término hacker, muchos lo utilizan incorrectamente para referirse a piratas o ciberdelincuentes. Afortunadamente, esta tendencia está comenzando a cambiar, como ilustra la decisión de la RAE para incluir una segunda definición del término.

Para quien aún no lo tenga claro, los hackers son los buenos, los inconformistas que intentan siempre llegar un paso más allá,

motivados por la pasión que les mueve, para alcanzar un objetivo que han trazado en su cabeza y que muchas veces parece imposible.

Gracias a que existen hackers tenemos internet y disfrutamos de todas esas maravillas que la tecnología nos ofrece. Cada año podemos comprar dispositivos que los fabricantes tecnológicos nos presentan con nuevas funcionalidades, así como disponer de sistemas más robustos, más seguros, algo fundamental en estos tiempos donde la privacidad es un bien tan codiciado, pese a que muchos usuarios renuncian voluntariamente a ella sin tan siquiera ser conscientes de las implicaciones que tiene. De ello también hablaremos en un capítulo de este libro.

Todas las vulnerabilidades que los hackers descubren permiten que nuestros dispositivos, los sistemas con los que se comunican y la tecnología que los conecta sean corregidos y fortificados. Esto es lo que nos permite a la larga vivir en una sociedad digital más segura para todos.

Cualidades de un hacker:

— Pasión.
— Inquietud.
— Perseverancia.
— Sacrificio.
— Ansia de conocimiento.
— Pensamiento lateral.
— Inconformismo.

Cualidades de un hacker

Lograr este tipo de mejoras, a veces auténticas hazañas, implica no sólo disponer de un alto nivel de conocimiento técnico en la materia, sino de una serie de cualidades innatas que forman parte del ADN de cualquier hacker.

Además de cualidades como la inquietud, la curiosidad o la pasión, insuficientes por sí solas, hay otras más. A lo largo del ca-

mino, podemos encontrarnos con muchos obstáculos, con horas y horas de trabajo invertidas en una determinada línea de investigación que finalmente desemboca en un intento frustrado más. Con escollos insalvables por falta de recursos, de conocimiento o de tiempo. En estos momentos, la constancia y la perseverancia son también fundamentales.

Si has programado alguna vez, probablemente sabrás que cualquier código que escribimos, por muy simple que sea, casi nunca funciona a la primera. Siempre hay un error a la hora de compilar o hay algo que no está bien. Forma parte del rito. Por otro lado, también es posible que, en alguna ocasión, tras una serie de intentos fallidos por lograr que un programa haga lo que queremos, milagrosamente conseguimos arreglarlo sin saber muy bien cómo lo hemos hecho. Por explicarlo de una manera simple, es «como si lo tuviésemos cogido con pinzas», nunca llegamos a controlarlo del todo.

Para no perdernos...
«Compilar» es traducir un programa escrito por humanos en lenguaje de alto nivel a un código interpretado por una máquina.

Los errores o fallos de programación se conocen como *bugs*.

Esto era muy común a la hora de entregar prácticas de programación en la facultad. Muchas veces, en función del nivel de complejidad y de lo tarde que uno las empezara, podían requerir auténticas gestas, y escribir líneas de código toda la noche antes de la entrega. El resultado eran programas que funcionaban de manera un tanto inestable, a lo mejor ejecutándose correctamente tres de cada cuatro veces. Era habitual cruzar los dedos, mirar hacia arriba e implorar ayuda divina a la hora de presentar la práctica al profesor. En las entregas, muchos alumnos acababan recitando una expresión recurrente y casi mítica: «¡No puede ser, en mi casa funcionaba y aquí no!».

Este ejemplo es válido para exponer dos ideas:

— La primera es que evitar este tipo de situaciones es lo que sin duda alguna diferencia a un hacker. No dejar jamás cosas al azar, sin entender del todo cuándo, cómo y por qué se ha solucionado el problema de manera casual o casi accidental. Debemos huir del pragmatismo, aunque se haya logrado el objetivo.
— La segunda es que este tipo de actitudes por parte de los programadores cuando desarrollan cualquier programa son las que abren la puerta a que un hacker habilidoso, con ansia de conocimientos y con la constancia necesaria, pueda encontrar la razón de un comportamiento erróneo. Generalmente, gracias a un error (*bug*), el hacker identificará una vulnerabilidad para explotarla y alterar así el comportamiento original del programa. Así es como se comprometen los sistemas, pero son cuestiones que explicaremos con más detalle a lo largo de este libro.

Ejemplos de hackers en la historia y en la ficción

A la hora de hablar de hackers famosos a lo largo de la historia, probablemente el primer nombre que sale a la palestra es el del mítico Kevin Mitnick, perseguido en la década de los noventa durante tres años por el FBI. Hablaremos de él en el capítulo dedicado a la ingeniería social. Otros referentes del hacking a nivel mundial son Mikko Hypponen, reconocido por su amplia labor de investigación en el campo del malware y de la seguridad con numerosos galardones y distinciones; Fermín Serna, hacker español que trabaja en el equipo de seguridad de Google y en su día lo hizo para Microsoft; o Charlie Miller, famoso por descubrir importantes vulnerabilidades, como las que permitían tomar el control de un vehículo en movimiento. Hay muchos otros hackers que quizá no suelen identificarse como tales. Bill Gates y Steve Jobs, referentes y responsables del éxito de Microsoft y Apple, o el creador del sistema operativo Linux, Linus Torvalds, son también hackers. Lo son en realidad todos los que transgreden los límites y van más allá, siempre con el objetivo de crear algo nuevo.

Otra de las cualidades que sin duda caracterizan a un hacker es su capacidad de resolver problemas complejos a través del pensamiento lateral. Para quien no haya oído jamás este concepto, se trata de la habilidad natural para encontrar soluciones ingeniosas a la hora de abordar un problema aparentemente irresoluble, a través de caminos alternativos. Uno de los mejores ejemplos para entender lo que es el pensamiento lateral se encuentra en el mundo de la ficción. Michael Scofield, protagonista de la serie *Prison Break*, ilustra cómo el hacking puede ir mucho más allá del teclado y la pantalla.

En esta adictiva y espectacular trama conspiratoria con elevadas dosis de intriga, Scofield, un genio con una mente brillante, abandona su exitoso trabajo como ingeniero de estructuras para embarcarse en una trepidante misión: ayudar a su hermano a escapar de la cárcel, ya que éste ha sido condenado injustamente a raíz de una conspiración que se origina en las esferas más altas del Gobierno de Estados Unidos.

Para ello, Scofield planifica con minuciosidad todos los pasos para poder entrar en la cárcel y lograr su cometido, lo que implica acciones tan ingeniosas como la de tatuarse el plano de la prisión en su cuerpo en aras de disponer en todo momento de los mapas de las dependencias del recinto.

Como suele suceder en las series, el plan inicial del protagonista se va torciendo a medida que avanza la trama. A pesar de que cuenta con una hoja de ruta perfectamente trazada en la que ha cuidado todos los detalles, depende de muchos factores y agentes externos que se suceden y actúan en la historia. Es entonces cuando Michael Scofield hace gala del pensamiento lateral para resolver situaciones muy complejas capítulo tras capítulo. Momentos irresolubles para la mayoría de los mortales, pero no para este genio que encuentra siempre un recurso inesperado.

Estas cualidades innatas de Scofield se reflejaban desde la infancia. Su madre cuenta cómo de pequeño se dedicaba a romper todos los juguetes y aparatos que caían en sus manos para volver a repararlos o convertirlos en nuevos. Aunque algunas de sus acciones trasciendan lo tecnológico, Michael Scofield es caracterizado como un hacker en toda regla.

Michael Scofield, protagonista de *Prison Break*, era un hacker.

McGyver, capaz de crear cualquier artilugio a partir de objetos variopintos, era un hacker.

Cualquiera puede ser un hacker en su campo de especialización o en su vida.

Cuando la motivación no es otra que la de aprender, innovar y crear, en contraposición al beneficio económico que suele imperar a menudo, podemos encontrar hackers en muchas disciplinas o campos de la vida. Por eso es más acertado pensar en el concepto de hacker como una actitud, antes que como una persona. Cualquiera puede ser un hacker en su área de conocimiento o en su propia vida si adopta en ella ese talante.

Lammers y *script kiddies*

La sensación de satisfacción que se obtiene al alcanzar cada hito en esa búsqueda de conocimiento constante es muy superior a cualquier otro tipo de remuneración que cualquiera pueda imaginar. Pero sólo se obtiene cuando uno llega a la consecución del objetivo, sea cual fuere, adoptando la vía del conocimiento y del trabajo duro. Sin buscar atajos, sin omitir etapas ni hacer trampas.

De nada sirve arreglar un programa si no sabemos cómo lo hemos hecho, o comprometer la seguridad de un sistema con herramientas automatizadas si no tenemos ni idea de lo que hacen dichas herramientas. No pasa nada por usar herramientas de terceros. Compartir conocimiento forma parte de esta cultura. Es totalmente lícito y todos lo hacemos, siempre y cuando nos hayamos tomado la molestia de documentarnos, de conocer y asimilar los conceptos técnicos que sustentan dichas herramientas, así como de controlar su funcionamiento a un nivel exhaustivo.

Lo que no procede es descargarse herramientas llamadas «de botón gordo» y ejecutarlas para que hagan todo el trabajo sin tener ni idea de lo que realmente hacen, para posteriormente vanagloriarse de ser un superhacker ante los demás. Esta actitud, totalmente contraria a la de un verdadero hacker, es tan habitual en el mundillo, que tiene su propio apelativo: *lammer*, o *script kiddie* (el chico que ejecuta *scripts*).

Script es un término que hace referencia a un programa, generalmente sencillo, escrito en un archivo de texto.

Un *script kiddie* generalmente es fácil de reconocer si se interactúa con él. Es aquel que en un foro o un chat preguntará directamente por la solución o respuesta a un problema sin pensar en la posibilidad de buscarla por sus propios medios. Es aquel que rehúye la teoría y busca directamente la herramienta que resuelve el problema, hecha por otro. Es quien ejecuta esa herramienta sin haber siquiera leído el manual, y cuando ésta no hace lo esperado, lo primero que hace es preguntar en lugar de ir a la fuente.

Precisamente, el hecho de autoproclamarse como hacker ante los demás es lo que caracteriza a un potencial *lammer* o *lúser* en muchas ocasiones. El apelativo hacker reúne una serie de cualidades que giran en torno al respeto, la devoción y la admiración; bien distintas a las más mediáticas y difundidas. Ganarse este apelativo no es nada fácil. Supone un orgullo y un privilegio dedicarse a ello. Sin embargo, sería algo ambicioso y soberbio definirse a sí mismo como hacker, aunque no lo neguemos cuando una persona ajena nos defina así.

Un verdadero hacker no suele autoproclamarse como tal.

Estos matices pueden parecer menores, pero cobran mucha importancia en un sector donde el ego está más acentuado aún que en otros lugares. El amplísimo campo de investigación disponible, y los potenciales descubrimientos lo convierten en una práctica muy competitiva donde por desgracia la búsqueda del reconocimiento de los demás se prodiga demasiado. Al final, nadie te da o te quita el título de hacker, es una cuestión de actitud.

Hackear al vecino que me robaba el wifi

Un ejemplo real e ilustrativo de lo que es un *script kiddie* está en esta historia que publiqué en su día en el blog de mi amigo Chema Alonso, *El lado del mal*. En aquella ocasión, la expliqué con pelos y señales desde un punto de vista técnico. Para lo que nos interesa aquí, la he desprovisto de datos técnicos innecesarios.

Corría el año 2013, y yo tenía configurada la red wifi de mi casa a propósito con cifrado WEP. Estaba haciendo pruebas de los diferentes ataques posibles en este tipo de redes mientras escribía el libro *Hacking en redes Wifi y Radiofrecuencia* con el equipo de Mundo Hacker, liderado por otro gran hacker amigo, Antonio Ramos. El cifrado WEP es tremendamente inseguro y se identificó como tal desde 2001. Desde entonces, han aparecido multitud de herramientas «de botón gordo» que permiten obtener la contraseña de la red wifi en cuestión de minutos, sin necesidad de conocimiento técnico alguno.

Al tener configurada la red de manera insegura, era consciente de que algo malo podría pasar. Durante aquellos días, revisaba concienzudamente las conexiones a mi red en el panel de administración del *router*, por si de repente alguien se unía a la fiesta.

> En las redes abiertas de hoteles, cafeterías o aeropuertos, el tráfico que generamos puede ser monitorizado por cualquiera.

«WEP» es un estándar de cifrado antiguo, declarado inseguro desde hace más de una década.

Como regalo traído del cielo por los Reyes Magos, la tarde del seis de enero apareció un dispositivo más, con nombre «Rober1», que se unía al registro de conexiones, junto con mi ordenador, el móvil, y la PlayStation (que en aquellos maravillosos días aún tenía tiempo para encender).

Enseguida supe que tenía un intruso en mi red, posiblemente un vecino del edificio. Si así era, la seguridad de mis dispositivos estaba comprometida. ¿Sería un hacker haciendo pruebas o un ciberdelincuente, un verdadero pirata? Todo dependía de sus intenciones. La tercera posibilidad era que se tratara de un *script kiddie* con la única intención de obtener acceso gratuito a internet.

La solución pragmática consistía en modificar la configuración de la red a un cifrado más seguro (WPA2), asignarle una contraseña robusta y terminar con el problema. Pero la posibilidad de hackear al intruso, identificarlo y realizar una práctica en un escenario real me pareció un reto interesante. Pese a que suponía dedicar tiempo y esfuerzo, merecía la pena.

Sea como fuere, no tenía ninguna información del atacante y además se acercaba la hora de salir de casa para celebrar el día de Reyes con mi familia. Rápidamente, desconecté todos los equipos de mi red y le dejé todo el ancho de banda al vecino. Eso sí, monitorizando el tráfico de mi propia red con una antena conectada a uno de mis equipos. Al tratarse de una red wifi, los paquetes de datos emitidos por cualquier dispositivo conectado a ella viajan en el aire, por lo que pueden ser capturados por cualquiera. Algo que es muy habitual en redes abiertas de hoteles, aeropuertos o centros comerciales.

Al llegar a casa por la noche, comencé a analizar el tráfico capturado durante esas horas. La información disponible en la captura advertía que, efectivamente, había un vecino que estaba utilizando mi red. Su equipo tenía un sistema operati-

vo Windows, con nombre de equipo «Rober1», y en principio había estado utilizando la red para navegar por internet. Los sitios webs más visitados durante esa primera sesión de navegación eran los siguientes:

— http://vanitatis.com: una página de prensa rosa que hasta entonces yo desconocía.
— http://devilwearszara.com: una página de tendencias de moda.
— http://fotoplatino.com: una página de tendencias de moda y peinados.
— http://elpais.com/gente: la sección más rosa de *El País*.

Con una captura de tráfico se puede acceder a toda la información que un usuario genera en una red, por lo que, además de analizar rápidamente los sitios webs más visitados, también reconstruí las imágenes transferidas en esa primera sesión de navegación. Algunas de las imágenes mostraban a Miley Cirus y otros famosos en la gala de los Óscar, así como fotos de peinados y vestidos varios.

El tipo de contenido visualizado por mi vecino me hacía pensar más en una usuaria con conocimientos básicos de internet que en un hacker. Por su historial de navegación supuse que se trataba de una mujer.

Seguí analizando con más detenimiento el tráfico que generaba Rober1. Encontré una petición al sitio web de ASUS para descargar una actualización, donde se podía incluso visualizar el modelo de equipo con el que se conectaba a mi red. Así que, visto que parecía no tener muchos conocimientos en materia de ocultación o anonimato, todo apuntaba a que se trataba de una *script kiddie* que buscaba conexión a internet gratuita.

Con el objetivo de identificarla, empecé a pensar en diferentes vectores de ataque. Una posibilidad era la de interceptar el tráfico entre el equipo de los vecinos y el *router* en tiempo real, una vez conectado a mi red. Este tipo de ataques se conocen como ataques *Man in the Middle*, por aquello de colocarse en medio de la comunicación entre dos dispositivos. Pero esto requería, entre otras cosas, que ambos estuviésemos presentes al mismo tiempo,

lo que ocasionaba tener que estar permanentemente atento al momento en que mi vecina se fuese a conectar.

> Los ataques *Man in the Middle* se llaman así porque el atacante se pone en medio de la comunicación entre dos puntos, generalmente la víctima y el *router* por el que navega en internet.
>
> Este ataque engaña a los dos dispositivos, suplantando en cada uno la identidad del otro mediante el envío de información falseada, para redirigir el tráfico de ambos a la máquina del atacante.
>
> Una vez interceptada la comunicación, es capaz no sólo de acceder al contenido que visualiza, sino también de modificar tanto lo que envía como lo que recibe.

En un par de ocasiones pude coincidir con ella, pero el éxito de estos ataques dependía de muchas circunstancias. Al ver que no podía resolver mi problema de esta manera, comencé a trabajar en una aproximación diferente y algo más compleja.

Mientras tanto, seguía monitorizando continuamente el tráfico que la vecina iba generando en mi red y lo analizaba para poder obtener información que me permitiese identificarla: un nombre, un usuario, una contraseña, una dirección de correo...

Llegado a este punto, ya tenía un patrón de comportamiento. Sabía que mi presunta vecina se conectaba dos o tres veces al día y que sus sesiones de navegación eran de aproximadamente quince minutos. En todas esas sesiones, solía consultar las páginas de prensa rosa y tendencias, pero también algunas nuevas que no aparecieron las primeras veces, y que me llamaron la atención:

— elimperiodelaley.blogspot.com.
— quieroserjuez.blogspot.com.
— vidadeunaopositora.blogspot.com.
— sufridoraenejercicio.blogspot.com.
— quenovoyaserlasecretariadeunjuez.blogspot.com.

Sí, has deducido bien: opositora a juez robando wifi. «Marca España».

Además de estas sesiones de navegación, a lo largo del día se sucedían otras muy cortas, de apenas unos pocos minutos de duración. Por el tipo de contenido que generaban, presuponía que ya no correspondían a mi vecina, sino a su pareja. Las páginas visitadas eran las siguientes:

— sport.es (sección *El Balón Rosa*, protagonizada por las novias de los futbolistas).
— marca.com.
— tenerifedeportivo.com.

Dejando a un lado los tópicos sobre el fútbol y los hombres, es interesante tener en cuenta cómo podemos obtener mucha información de una persona anónima por el tráfico que genera en una red.

> «Dime por dónde navegas y te diré quién eres.»
>
> El historial de navegación que generamos en una red dice mucho de nosotros y de nuestra personalidad.

Un domingo, después de consultar fugazmente su lista de diarios deportivos de referencia, Rober1 visitó también la página de unos cines cercanos a nuestro domicilio en Santa Cruz de Tenerife para echar un vistazo a la cartelera. Al cabo de unas horas, pude concluir que en última instancia no acudió a ver la película que estaba barajando o que, si finalmente lo hizo, decidió ir solo o con algún amigo, pero no con su pareja. A la hora que se proyectaba la película, ella estaba conectada a mi red viendo páginas de moda y blogs de oposiciones a juez. Probablemente haciendo su habitual descanso de quince minutos.

El colofón a esta serie de sucesos fue comprobar que en alguna ocasión accedieron a su cuenta de banca en línea desde un wifi ajeno usurpado, lo que evidenciaba la falta de conocimiento técni-

co y el desconocimiento de las consecuencias que pueden acarrear estos actos.

HTTP *versus* HTTPS

Hasta ahora os he contado que disponía de la información de todos los sitios webs visitados por mis vecinos, pero aún no he mencionado otros portales casi esenciales en cualquier sesión de navegación de un usuario estándar, como pueden ser Gmail, Facebook, Twitter o LinkedIn. ¿Por qué no había recopilado información referente a estos servicios?

Afortunadamente, este tipo de servicios y muchos otros que manejan información personal de usuarios son ofrecidos para acceder a ellos desde nuestro navegador mediante el protocolo HTTPS, que se representa con la imagen de un candado en la barra del navegador. Este protocolo cifra la información transmitida por el medio físico utilizando por debajo otros protocolos, como TLS o SSL. Esto quiere decir que, aunque alguien escuche el tráfico en una red como yo lo estaba haciendo, y como alguien podría hacer en cualquier red wifi pública a la que os conectéis, los paquetes que vayan cifrados con estos protocolos son ininteligibles. Es por eso que hasta ahora estaba viendo en claro el tráfico de los sitios web de moda, blogs de oposiciones a juez o diarios deportivos que mis vecinos visitaban regularmente. Puesto que el acceso a estos portales se realizaba mediante HTTP convencional. Sin embargo, hasta el momento no había podido obtener nada relacionado con sus redes sociales y servicios de correo que me permitiera identificarlos.

Lo que tenemos que saber:

— HTTP: protocolo de transferencia de hipertexto.
— HTTPS: protocolo de transferencia de hipertexto **segura**. Asegura la información mediante protocolos de cifrado transparentes al usuario, como SSL y TLS.

Con el objetivo de romper de alguna manera esta barrera del cifrado, estaba trabajando en una aproximación distinta al *Man in the Middle*. Los vecinos se conectaban a mi red mediante la conexión wifi habilitada por mi *router* ADSL, por lo que en lugar de intentar atacarlos cuando estuviesen, pensé en cambiar la estructura de mi red, ya que al fin y al cabo yo tenía el control sobre la misma. Ellos se seguirían conectando a través de la conexión wifi que ofrecía mi *router*. Pero quien de verdad haría las funciones de *router* sería mi equipo. Es decir, todo el tráfico que ellos generaran pasaría por mi equipo. Este lo transferiría al *router* y luego lo llevaría de vuelta al equipo de los vecinos. En lugar de un esquema de *Man in the Middle*, estaba implementando un *Machine in the Middle*. Seguiría accediendo al tráfico de mis vecinos como hasta ahora, pero podría hacer algo más. Para evitar dejar indisponible la red cuando ellos fueran a utilizarla, tenía que ser sumamente cuidadoso a la hora de «cacharrear», como se dice vulgarmente, desplegando mi nueva topología de red durante las horas que no estuviesen conectados. Si por algún error en el proceso dejaba mi red inoperativa cuando ellos la fuesen a utilizar, podrían pensar que se había caído y dejar de conectarse, y todo mi trabajo habría resultado en vano.

La diferencia con respecto a la escucha pasiva de tráfico radicaba en que, si ahora dicho tráfico pasaba por mi equipo, además de interceptarlo podría modificarlo en tiempo real, exactamente lo que pretendía hacer. Mediante el uso de una determinada herramienta muy conocida para ataques en redes, interferiría el tráfico de mis vecinos para alterar el código fuente de las páginas web que recibían. En realidad, son unos y ceros. Cuando esos unos y ceros se traducían en enlaces a sitios web con HTTPS, la herramienta suprimía la S de «seguro», dejando los enlaces a los mismos sitios, pero utilizando el estándar HTTP, por lo que el tráfico se transmitiría sin cifrar, igual que el de las páginas de moda o los diarios deportivos.

Acceder a su cuenta de Facebook

Sólo un día después de haber habilitado este esquema de funcionamiento, sucedió lo que esperaba. En el primer descanso que mi vecina se tomó en su sesión de estudio, además de acceder a sus habituales páginas de moda y a los blogs de oposiciones, entró en su cuenta de Facebook, como seguramente habría hecho anteriormente. La diferencia era que esta vez había conseguido que enviara sus credenciales de inicio de sesión mediante HTTP. En términos sencillos, ya tenía en mi poder su usuario y contraseña de Facebook.

En ese momento a uno se le pasan muchas cosas por la cabeza: entrar en su cuenta, echar un vistazo a sus mensajes privados, publicar alguna aberración en su muro... Más allá de lo que habría sido puro vandalismo informático, lo importante, y que sí hice, fue identificarla a ella y a su pareja. ¿Cómo? Buscando la parte pública de su perfil mediante su dirección de correo, que es el usuario de Facebook. Pude confirmar que, en efecto, se trataba de una pareja de abogados, y, además, que no los conocía personalmente. No me había cruzado nunca con ellos en el portal o en el ascensor, por lo que seguramente se habrían mudado hacía poco. Supongo que por eso decidieron conectarse a mi red mientras no tuvieran la suya.

Una vez identificados, les envié un correo electrónico desde una cuenta anónima de Gmail. En él les informaba de que estaba al corriente de su actividad delictiva desde el primer momento y les exponía toda la información que había ido recopilando acerca de su tráfico. Tampoco quise cebarme mucho con ellos, ya que era normal pensar que detrás de una red wifi insegura como la que ellos habían vulnerado seguramente habría un usuario sin ningún tipo de conocimientos, y no un hacker que pudiese invertir los papeles.

No obstante, en ocasiones podemos encontrarnos con redes o sistemas configurados a propósito como inseguros a modo de señuelo para que sean comprometidos por los malos y acabar cazando así a estos ciberdelincuentes. Este tipo de trampas se conocen como *Honeypots*.

El amigo informático

Mi mensaje debió de calarles hondo, ya que a las pocas horas obtuve una respuesta muy educada a mi correo en el que reconocían su error y se disculpaban por su actitud. Admitían que eran conscientes de la ilegalidad de sus actos (aunque no hacía falta ser abogado para ello), pero no de las implicaciones que su actividad podría tener a nivel técnico. Como explicaban en su correo, fue «un amigo informático el que nos dijo que así podíamos tener conexión a internet gratis».

En este caso no llegó la sangre al río, pero si en lugar de conmigo se hubiesen topado con alguien que tuviese intenciones maliciosas, además de comprometer su cuenta de Facebook y quizá revocarles el acceso, las consecuencias podrían haber sido mucho más graves. Con un poco de paciencia, podría haber accedido, por ejemplo, a sus cuentas bancarias sin que tuvieran la más mínima idea. A lo largo de este libro iremos viendo algunas de las técnicas que pueden aplicarse con relativa facilidad y que los ciberdelincuentes utilizan para vulnerar la seguridad de los usuarios.

Lecciones aprendidas de esta historia y recomendaciones

El relato de los vecinos y el wifi es una historia real y habitual que ilustra los peligros a los que nos exponemos a la hora de conectarnos a redes wifi públicas o ajenas, así como las recomendaciones que debemos tener en cuenta en estos casos.

En primer lugar, conviene dejar claro los siguientes aspectos:

— En las redes wifi públicas de hoteles, cafeterías, aeropuertos o centros comerciales, todo el tráfico que generamos puede ser monitorizado por cualquiera.
— Esto se aplica tanto si la red es abierta como si dispone de cifrado WEP, WPA o WPA2 y tiene contraseña, pues todos los que se conectan a ella conocen la contraseña.
— Monitorizar el tráfico HTTP que generamos en estas redes es trivial, no ocurre así con el tráfico HTTPS que está cifrado.

— Aun así, existen formas de romper la barrera de cifrado HTTPS, como la que utilicé para comprometer la cuenta de Facebook de mi vecina.
— A día de hoy, esta técnica es más difícil de implementar que en el momento en que esta historia tuvo lugar, hace ya cinco años.
— No obstante, sigue siendo posible encontrar la manera de aprovechar la inseguridad inherente a este tipo de redes y comprometer la seguridad de los usuarios.

Así pues, debemos tener claro qué medidas adoptar a la hora de conectarnos a redes wifi tanto públicas como ajenas:

— Podemos utilizar sin problemas estas redes para consultar información, leer noticias, acceder a sitios web... pero debemos extremar la precaución a la hora de utilizar servicios personales.
— A pesar de que tanto Facebook como Twitter, LinkedIn o nuestro banco nos proporcionan una interfaz segura mediante HTTPS, y que, a día de hoy, estos ataques son más difíciles de llevar a cabo, es recomendable evitar usar estos servicios desde redes wifi públicas.

Una VPN es una red privada virtual. Se trata de una tecnología que nos permite conectarnos remotamente a una red local doméstica o corporativa desde cualquier punto de internet.

Esto hace que las comunicaciones desde dicho punto hasta esa red vayan cifradas y no puedan ser monitorizadas por cualquiera, lo que permite obtener seguridad en cualquier red wifi donde nos conectemos.

— Si utilizamos un dispositivo corporativo y nuestra empresa dispone de conexión VPN, es imperativo utilizarla siempre que nos conectemos a una red wifi pública. En ese caso, podremos utilizar todos los servicios que queramos sin problema.

— Si somos responsables de la seguridad de una empresa y, debido a su tamaño o modelo de negocio, no dispone de VPN, es recomendable implantar una para garantizar la seguridad de las comunicaciones de aquellos trabajadores con movilidad, que viajan y se conectan a redes wifi públicas.
— A nivel personal también es posible utilizar una solución VPN para poder garantizar nuestras comunicaciones. En ese caso, podremos utilizar todos los servicios que queramos sin problema.
— Si como usuarios no tenemos a nuestro alcance configurar una conexión VPN por falta de conocimiento o recursos, es posible contratar este servicio a un proveedor. Existen multitud de alternativas en el mercado que, a precios asequibles, nos permiten contratar servicios de VPN para poder navegar seguros en cualquier red a la que nos conectemos.

Por supuesto, sobra decir que no debemos conectarnos jamás de manera ilícita y sin permiso a redes wifi ajenas, aunque alguien nos proporcione las herramientas para lograrlo. Además de ser inmoral e ilegal, como hemos podido comprobar, puede poner en grave riesgo nuestra seguridad.