****Ingeniería Social, El arte del Hacking Personal****

----------Por Christoper Hadnagy ----------

Dedicatoria especial, a todo el grupo de Hacking Red Hat.

Mención especial para colaboradores: ……..

John Arias Cardoso,(Adm) Christian Santos,(Adm) Black Tiger (Grupo Telegram), Steven.Arrencis(profesor telegram) . Johel RmR, (Grupo Telegram) , Mr robot (Victor Vertel Profesor ,,Grupo Telegram) , Enrique Security(Telegram) Merlyn Mago fis, cal Facebook , Mylord Rayito moderador, Milton Vega, Yader Rey, Matriux Leandrex,, FacundoEzequiel moderador ,Panda , Ernesto(grupo telegram), pedro Hack (administrador escuela virtual), Alfonzo Osorio moderador. Estos son los principales aportadores,.. Este libro fue traducido por Mistral Hernández, en el mes de octubre de 2018. Del original en inglés

SOCIAL ENGINEERING THE ART OF HUMAN HACKING

Nota:

Prefacio

La seguridad es un rompecabezas con dos lados. Desde el interior, buscamos una sensación de confort y seguridad. Desde el exterior, los ladrones, los hackers y los vándalos están buscando vacíos. La mayoría de nosotros creemos que nuestras casas están seguras hasta que un día nos encontramos bloqueados. De repente, nuestra perspectiva cambia y las debilidades se encuentran fácilmente.

Para comprender completamente cualquier tipo de seguridad, es esencial salir de la cerca, en esencia, bloquearnos, y comenzar a buscar otras formas de entrar. El problema es que la mayoría de nosotros estamos cegados a los problemas potenciales por nuestra propia confianza o nuestra creencia de que las cerraduras fuertes, las puertas gruesas, un sistema de seguridad de alta gama y un perro guardián son más que suficientes para mantener a la mayoría de las personas a raya.

No soy la mayoría de la gente. En los últimos diez años he logrado más contras y estafas que nadie en la historia. He vencido a los casinos, falsificado eventos deportivos, he arreglado subastas, he convencido a la gente de sus posesiones más preciadas y he superado niveles de seguridad aparentemente incomparables.

Me he ganado la vida exponiendo los métodos de ladrones, mentirosos, estafadores en un exitoso programa de televisión llamado The Real Hustle. Si hubiera sido un verdadero criminal, Probablemente sería rico, famoso o muerto, probablemente los tres. He utilizado toda una vida de investigación sobre todas las formas de engaño para enseñar al público cuán vulnerables son en realidad.

Cada semana, junto con Alexis Conran, hago estafas reales en personas reales que no tienen idea de que están siendo estafadas. Usando cámaras ocultas, le mostramos al público en casa lo que es posible para que puedan reconocer lo mismo estafa.

Esta carrera inusual ha resultado en una comprensión única de cómo piensan los criminales. Me he convertido en una oveja vestida de lobo. He aprendido que, no importa lo imposible que pueda parecer algo, casi siempre hay una forma inteligente e inesperada de resolver el problema.

Un ejemplo de esto es cuando ofrecí mostrar lo fácil que sería no solo robar el bolso de una mujer, sino también hacer que me diga el PIN de sus cajeros automáticos o tarjetas de crédito. La BBC no creía que fuera posible lograr esto.

Cuando presentamos esto como un artículo para The Real Hustle, el comisionado de la BBC escribió “nunca sucederá” junto a él y lo envió de vuelta. Sabíamos que era completamente posible porque se habían informado diferentes versiones de la misma estafa, donde se invitó a las víctimas de robo a revelar sus PIN en varias estafas inteligentes en el Reino Unido. Tomamos elementos de diferentes de estafas para ilustrar exactamente cómo una persona puede ser engañada para que otra persona tenga acceso completo a su cuenta bancaria.

Para probar nuestro punto, establecimos la estafa en un café local. El café estaba en el último piso de un centro comercial en Oxford Street en Londres. Estaba relativamente tranquilo cuando me senté en una mesa vacía con un traje de negocios. Puse mi maletín sobre la mesa y esperé a una víctima adecuada. En unos momentos, una víctima así llegó con un amigo y se sentó en la mesa junto a la mía, colocando su bolso en el asiento a su lado. Como probablemente era su hábito, acercó el asiento y mantuvo la mano en la bolsa en todo momento.

Necesitaba robar la bolsa entera, pero, con la mano apoyada en ella y su amiga sentada enfrente, empezaba a parecer una mala noticia. Pero, después de unos minutos, su amiga se fue a buscar un baño. La marca estaba sola, así que le di la señal a Alexand Jess.

Haciendo el papel de una pareja, Alex y Jess le preguntaron si ella les tomaría una foto a ambos. Ella estaba feliz de hacerlo. Sacó la mano de su bolsa para tomar la cámara y tomar una foto de la “pareja feliz” y, mientras estaba distraída, me acerqué casualmente, tomé su bolsa y la guardé con calma dentro de mi maletín. Mi víctima aún no había notado la silla vacía cuando Alex y Jess salieron del café. Una vez fuera de la vista, Alex se dirigió rápidamente hacia el estacionamiento.

No le tomó mucho tiempo darse cuenta de que su bolso se había ido. Al instante, ella comenzó a entrar en pánico. Se puso de pie y miró a su alrededor, frenéticamente. Esto era exactamente lo que esperábamos, así que le pregunté si necesitaba ayuda.

Ella comenzó a preguntarme si había visto algo. Le dije que no. la convencí de que se sentara y pensara en lo que había en la bolsa. Un teléfono. Maquillaje. Un poco en efectivo. Y sus tarjetas de crédito. ¡Bingo!

Le pregunté a qué banco depositaba y luego le dije que trabajaba para ese banco. Que golpe de suerte! Le aseguré que todo estaría bien, pero que tendría que cancelar su tarjeta de crédito de inmediato. Llamé a la mesa de ayuda

Número, que en realidad era Alex, y le di mi teléfono. Ella estaba Enganchada y ahora le tocaba a Alexto atraerla.

Alex estaba abajo en la furgoneta. En el tablero de instrumentos, un reproductor de CD reproducía ruidos de oficina que habíamos descargado de Internet. Mantuvo la marca tranquila, la acompañó y luego le aseguró que su tarjeta podía cancelarse fácilmente pero, para verificar su identidad, tenía que ingresar su PIN en el teclado del teléfono que estaba usando

Puedes adivinar el resto. Una vez que tuvimos su PIN, la dejé con su amiga y me dirigí a la puerta. Si fuéramos ladrones reales, hubiéramos tenido acceso a su cuenta a través de retiros en cajeros automáticos y compras de chips y PIN. Afortunadamente para ella, era solo un programa de televisión y estaba muy feliz cuando regresé para devolverle el bolso y decirle que todo era una falsa alarma. Incluso me agradeció por devolverle el bolso al que respondí: “No me lo agradezcas. Soy yo quien lo robó.”

No importa qué tan seguro sea un sistema, siempre hay una manera de abrirse paso. A menudo, los elementos humanos del sistema son los más fáciles de manipular y engañar. Crear un estado de pánico, usar influencia, tácticas de manipulación o causar sentimientos de confianza son todos los métodos utilizados para tranquilizar a una víctima.

El escenario descrito aquí es un ejemplo extremo, pero muestra que, con un poco de creatividad, se pueden realizar estafas aparentemente imposibles.

No importa qué tan seguro sea un sistema, siempre hay una manera de abrirse paso. A menudo, los elementos humanos del sistema son los más fáciles de manipular y engañar. Crear un estado de pánico, usar influencia, tácticas de manipulación o causar sentimientos de confianza son todos los métodos utilizados para tranquilizar a una víctima.

El escenario descrito aquí es un ejemplo extremo, pero muestra que, con un poco de creatividad, se pueden realizar estafas aparentemente imposibles.

Recuerde: los que construyen muros piensan de manera diferente a los que buscan pasar por encima, debajo, alrededor o a través de ellos. Como a menudo le digo a mi público, si piensa que no puedes ser estafado, solo eres la persona que me gustaría conocer.

Prefacio y Agradecimientos

Hace apenas unos años estaba sentado con mi amigo y mentor, Mati Aharoni, decidiendo lanzar www.social-engineer.org. La idea creció y creció hasta que se convirtió en un sitio web increíble con el apoyo de algunas personas realmente brillantes. No tardó mucho en llegar a la idea de poner esos años de investigación y experiencia en las páginas de un libro. Cuando tuve la idea, me recibieron con un apoyo abrumador. Dicho esto, algunos reconocimientos específicos son muy importantes para cómo este libro se convirtió en lo que es hoy.

Desde muy joven siempre me interesó manipular a las personas. No de una mala manera, pero me pareció interesante cuántas veces pude obtener cosas o estar en situaciones que serían irreales. Una vez estuve con un buen amigo y socio de negocios en una conferencia tecnológica en el Javits Center en la ciudad de Nueva York. La corporación Alarge había alquilado a FAO Schwarz para una fiesta privada. Por supuesto, la fiesta fue solo por invitación, y mi amigo y yo éramos dos peces pequeños en un estanque grande: la fiesta era para los directores ejecutivos y la alta gerencia de compañías como HP, Microsoft y similares. Mi amigo me dijo: “Sería realmente genial entrar en esa fiesta.”

Simplemente respondí: “¿Por qué no podemos?” En ese momento pensé: “Sé que podemos llegar allí si solo preguntamos de la manera correcta”. Así que me acerqué a las mujeres a cargo de la taquilla y al Lista de invitados y les hablé por unos minutos. Mientras les hablaba, Linus Torvalds, el creador de la Kernel de Linux, andaba por alli. Había recogido un juguete de peluche de Microsoft en una de las cabinas y, mientras bromeaba, me dirigí a Linus y le dije: “Oye, ¿quieres autografiar mi juguete de Microsoft?””

Se echó a reír y, mientras tomaba sus boletos, dijo: “Buen trabajo, joven. Te veré en la fiesta.

Regresé a las mujeres a cargo de la taquilla y me entregaron dos boletos para una fiesta exclusiva en el interior de FAOSchwartz.

No fue hasta más tarde en mi vida que comencé a analizar historias como esta, después de que algunos comenzaron a llamarlo “el Efecto de Hadnagy”.”Como gracioso que suena, comencé a ver que gran parte de lo que se me ocurrió no fue la suerte ni el destino, sino mas bien Sabiendo cómo estar donde necesitaba estar en el momento adecuado.

Eso no significa que no requirió mucho trabajo y mucha ayuda en el camino. Mi ilusión en mi vida es mi maravillosa esposa. Durante casi dos décadas, me has apoyado en todas mis ideas y esfuerzos y eres mi mejor amiga, mi confidente y mi pilar de apoyo. Sin ti no estaría donde estoy hoy. Además, has producido a dos de los niños más hermosos de este planeta. Mi hijo y mi hija son la motivación para seguir haciendo todo esto. Si algo de lo que hago puede hacer que este lugar sea un poco más seguro para ellos, o enseñarles cómo mantenerse seguros, vale la pena.

Para mi hijo e hija, no puedo expresar suficiente gratitud por su apoyo, amor y motivación. Mi esperanza es que mi hijo y mi pequeña princesa no tengan que lidiar con las personas malintencionadas y malas de este mundo, pero sé lo poco probable que es eso. Que esta información les mantenga a ambos un poco más seguro.

Paul, también conocido como rAWjAW, gracias por todo su apoyo en el sitio web. Las miles de horas que pasó como el "wiki-master" dieron sus frutos y ahora tenemos un hermoso recurso para que lo use el mundo. Sé que no lo digo lo suficiente, pero "estás despedido". Combinado con la bella creación de Tom, también conocido como DigPP, el sitio web es una obra de arte.

Carol, mi editora en Wiley, trabajó sin descanso para organizar esto y seguir una especie de línea de tiempo. Ella hizo un trabajo increíble al juntar un gran equipo de personas y hacer de esta idea una realidad. Gracias.

Brian, quise decir lo que dije. Te voy a extrañar cuando esto termine. A medida que trabajé con usted durante los últimos meses, empecé a esperar mis sesiones de edición y el conocimiento que me brindaría. Su consejo y consejo honestos y francos hicieron que este libro fuera mejor de lo que era.

Mi gratitud se dirige a Jim, también conocido como Elwood, también. Sin ti mucho de lo que ha sucedido en social-engineer.org, así como dentro de este libro, diablos en mi vida en los últimos dos años, no sería una realidad. Gracias por mantenerme humilde y bajo control. Sus constantes comprobaciones de la realidad me ayudaron a mantenerme enfocado y equilibrar los diferentes roles que tenía que desempeñar. Gracias.

Liz, hace unos doce años me dijiste que debería escribir un libro. Estoy seguro de que tenías algo diferente en mente, pero aquí está. Me has ayudado a través de algunos tiempos bastante oscuros. Gracias y te amo.

Mati, mi mentor y mi achoti, ¿dónde estaría sin ti? Mati, realmente eres mi mentor y mi hermano. Gracias desde el fondo de mi corazón por tener la fe en mí de que podría escribir este libro y lanzar www.social engineer.org y que ambos serían buenos. Más que eso, tu constante. El consejo y la dirección se han traducido en las páginas de este libro para hacerme más de lo que pensé que podría ser.

Su apoyo con el equipo de BackTrack junto con el apoyo del equipo en www.offensive-security.com han trascendido todo lo que podría haber esperado. Gracias por ayudarme a equilibrar y priorizar. Myachoti, un agradecimiento especial a ti por ser la voz de la razón y la luz al final de algunos días frustrantes. Con todo mi amor te lo agradezco.

Cada persona que mencioné aquí contribuyó a este libro de alguna manera. Con su ayuda, apoyo y amor, este libro se ha convertido en una obra de la que estoy orgulloso de tener mi nombre. Para el resto de ustedes que han apoyado el sitio, el canal y nuestra investigación, gracias.

Mientras lees este libro, espero que te afecte la forma en que yo lo eh escrito.

Albert Einstein dijo una vez: "La información no es conocimiento". Ese es un pensamiento poderoso. El solo hecho de leer este libro no implantará de alguna manera este conocimiento en tu ser. Aplique los principios, practique lo que se enseña en estas páginas y haga que la información sea parte de su vida cotidiana. Cuando haces eso es cuando verás que este conocimiento tiene efecto.

Christopher Hadnagy Octubre 201

Capítulo 1

Una mirada al mundo de la ingeniería social Si conoces al enemigo y te conoces a ti mismo no debes temer los resultados. de cien batallas.

- Sun Tzu La ingeniería social (SE) ha sido en gran parte mal entendida, lo que lleva a muchas opiniones diferentes sobre qué es la ingeniería social y cómo funciona. Esto ha llevado a una situación en la que algunos pueden ver a la SE como simplemente mentir para estafar artículos triviales, como pizza u obtener gratificación sexual; otros piensan que SE simplemente se refiere a las herramientas utilizadas por criminales o estafadores, o tal vez es una ciencia cuyas teorías se pueden desglosar en partes o ecuaciones y estudiarse. O tal vez es un arte místico perdido hace mucho tiempo que les brinda a los practicantes la capacidad de usar trucos mentales poderosos como un mago o un ilusionista.

En cualquier campamento que vuele tu bandera, este libro es para ti. La ingeniería social se usa todos los días por personas de todo el día en situaciones cotidianas. Un niño que intenta abrirse camino en el candyaisle o un empleado que busca un aumento de sueldo está utilizando la ingeniería social. La ingeniería social ocurre en el gobierno o en la comercialización de pequeñas empresas. Desafortunadamente, también está presente cuando los delincuentes, estafadores y personas similares engañan a las personas para que revelen información que los hace vulnerables a los delitos. Como cualquier herramienta, la ingeniería social no es buena o mala, sino simplemente una herramienta que tiene muchos usos diferentes.

Considere algunas de estas preguntas para llevar ese punto a casa:

¿Se le ha asignado la tarea de asegurarse de que su empresa sea tan segura como
¿posible?
¿Eres un entusiasta de la seguridad que lee cada uno de los últimos
información por ahí?

¿Es usted un probador de penetración profesional que es contratado para probar la seguridad de sus clientes?

¿Eres un estudiante universitario que está tomando algún tipo de especialización en TI como

¿su especialidad?

¿Eres actualmente un ingeniero social en busca de nuevos y mejorados?

¿Ideas para utilizar en tu práctica?

¿Es usted un consumidor que teme los peligros del fraude y el robo de identidad?

Independientemente de cuál de estas situaciones se adapte a usted, la información contenida en este libro le abrirá los ojos a cómo puede usar las habilidades de ingeniería social. También se asomará al oscuro mundo de la ingeniería social y aprenderá cómo los “malos” usan estas habilidades para obtener una ventaja. A partir de ahí, aprendes a ser menos vulnerable a los ataques de ingeniería social.

Una advertencia al frente: este libro no es para los débiles. Te lleva a esos rincones oscuros de la sociedad donde viven los “sombreros negros”, los hackers maliciosos. Se descubre y se adentra en áreas de ingeniería social que son empleadas por

Tartas y estafadores. Revisa tácticas y herramientas que parecen haber sido robadas de una película de James Bond. Además, cubre comunes, cotidianos.

Situaciones y luego muestra cómo son complejas la ingeniería social.

escenarios Al final, el libro descubre los consejos y trucos “de información privilegiada” de los ingenieros sociales profesionales y, sí, incluso los delincuentes profesionales.

Algunos han preguntado por qué estaría dispuesto a revelar esta información. La respuesta es simple: los “malos” no se detienen por una multa contractual o por su propia moral. No cesan después de un intento fallido. Los piratas informáticos malintencionados no desaparecen porque las empresas no desean que sus servidores se infiltren. En cambio, la ingeniería social, el engaño de los empleados y el fraude por Internet se utilizan cada día más. Mientras las compañías de software están aprendiendo cómo fortalecer sus programas, los piratas informáticos y los ingenieros sociales malintencionados están recurriendo a la parte más débil de la infraestructura: la gente. Su motivación tiene que ver con el retorno de la inversión (ROI); ningún hacker que se precie va a gastar 100 horas para obtener los mismos resultados que obtendría en una hora o menos con un simple ataque.

El triste resultado al final es que no hay forma de estar 100% seguro:

A menos que desenchufes todos los dispositivos electrónicos y te muevas a las montañas. Porque eso no es demasiado práctico, tampoco es muy divertido, este libro discute

Maneras de estar más conscientes y educados sobre los ataques y luego describe los métodos que puedes usar para protegerte de ellos. Mi lema es “seguridad a través de la educación”. Ser educado es una de las únicas maneras seguras de mantenerse a salvo de las crecientes amenazas de la ingeniería social y el robo de identidad. Kaspersky Labs, un proveedor líder de software antivirus y de protección, estimó que más de 100,000 muestras de malware se propagaron a través de las redes sociales en 2009. En un informe reciente, Kaspersky estimó que “los ataques contra las redes sociales son 10 veces más exitosos” que otros tipos de ataques. .

El viejo adagio del hacker, “el conocimiento es poder” se aplica aquí. Cuanto más conocimiento y comprensión tenga uno de los peligros y amenazas de la ingeniería social que pueden tener cada consumidor y empresa, y cuanto más se analice cada escenario de ataque, más fácil será protegerlo, mitigarlo y detenerlo. Ahí es donde entrará el poder de todo este conocimiento.

Por qué este libro es tan valioso

Hay muchos libros disponibles en el mercado sobre seguridad, piratería, pruebas de penetración e incluso ingeniería social. Muchos de estos libros tienen información muy valiosa y consejos para ayudar a sus lectores. Incluso con toda la información disponible, se necesitaba un libro que lleve la información de ingeniería social al siguiente nivel y describa estos ataques en detalle, explicándolos desde el lado malicioso de la cerca. Este libro no es simplemente una colección de historias geniales, hacks pulcros o ideas descabelladas. Este libro cubre los primeros

Marco para la ingeniería social. Analiza y analiza la base misma de lo que hace un buen ingeniero social y brinda consejos prácticos sobre cómo usar estas habilidades para mejorar las habilidades de los lectores para probar el

Mayor debilidad: la infraestructura humana.

El diseño Este libro ofrece un enfoque único a la ingeniería social. Está estructurado estrechamente al marco de ingeniería social en profundidad que se encuentra en

www.social-engineer.org/framework. Este marco describe las habilidades y las herramientas (físicas, mentales y de personalidad) que una persona debe esforzarse por poseer para ser un excelente ingeniero social.

Este libro adopta un enfoque de “decir y mostrar” al presentar primero un principio detrás de un tema, luego definir, explicar y diseccionar, y luego mostrar su aplicación utilizando colecciones de historias reales o estudios de casos. Esto no es simplemente un libro sobre historias o trucos, sino un manual, una guía a través del oscuro mundo de la ingeniería social.

A lo largo del libro, puede encontrar muchos enlaces de Internet a historias o cuentas, así como enlaces a herramientas y otros aspectos de los temas tratados. A lo largo del libro, aparecen ejercicios prácticos que están diseñados para ayudarlo a dominar no solo el marco de la ingeniería social, sino también las habilidades para mejorar sus comunicaciones diarias.

Estas declaraciones son especialmente ciertas si usted es un especialista en seguridad. Al leer este libro, espero poder advertirle que la seguridad no es un trabajo de “tiempo parcial” y no es algo que deba tomarse a la ligera. A medida que los delincuentes y los ingenieros sociales maliciosos parecen ir de mal en peor en este mundo, los ataques a las empresas y las vidas personales parecen intensificarse. Naturalmente, todos quieren estar protegidos, como lo demuestra el aumento en las ventas de software y dispositivos de protección personal. Aunque estos elementos son importantes, la mejor protección es el conocimiento: la seguridad a través de la educación. La única manera verdadera de reducir el efecto de estos ataques es saber que existen, saber cómo se realizan y entender el proceso de pensamiento y la mentalidad de las personas que harían esas cosas.

Cuando posee este conocimiento y comprende cómo piensan los piratas informáticos malintencionados, se apaga una bombilla. Esa luz proverbial brillará en las esquinas una vez oscurecidas y te permitirá ver claramente a los “chicos malos” que acechan allí. Cuando pueda ver la forma en que se usan estos ataques con anticipación, puede preparar los asuntos personales y de su compañía para protegerlos

Esa luz proverbial brillará en las esquinas una vez oscurecidas y te permitirá ver claramente a los “chicos malos” que acechan allí. Cuando pueda ver la forma en que se usan estos ataques con anticipación, puede preparar los asuntos personales y de su compañía para evitarlos.

Por supuesto, no estoy contradiciendo lo que dije antes; Creo que no hay manera de estar 100% seguro. Incluso los secretos de alto secreto y altamente guardado pueden ser y han sido hacheados de la manera más simple.

Mire la historia archivada en www.social engineer.org/resources/book/TopSecretStolen.htm de un periódico en Ottawa, Canadá. Esta historia es muy interesante, porque algunos documentos terminaron en las manos equivocadas. Estos no eran solo documentos, sino documentos de alto secreto de la defensa que describían cosas como ubicaciones de cercas de seguridad en la Base de las Fuerzas Canadienses (CFB) en Trenton, el plano de planta de la Unidad de Respuesta de Incidentes Conjuntos de Canadá y más. ¿Cómo ocurrió la brecha? Los planes se desecharon en el basurero y alguien los encontró en el contenedor de basura. Una simple inmersión en un contenedor de basura podría haber llevado a uno de los mayores ataques de seguridad de ese país.

Todos los días se lanzan ataques simples pero mortíferos que apuntan al hecho de que las personas necesitan educación; debe cambiar la forma en que se adhieren a las políticas de contraseña y la forma en que manejan el acceso remoto a los servidores; y debe cambiar la forma en que manejan las entrevistas, entregas y empleados que son contratados o despedidos. Sin embargo, sin educación, la motivación para el cambio simplemente no existe.

En 2003, el Instituto de Seguridad Informática realizó una encuesta junto con el FBI y descubrió que el 77% de las empresas entrevistadas declararon que un empleado descontento era la fuente de una violación de seguridad importante. Vontu, la sección de prevención de pérdida de datos de Symantec (http://go.symantec.com / vontu /), dice que 1 de cada 500 correos electrónicos contiene datos confidenciales. Algunos de los puntos destacados de ese informe, citados de http://financialservices.house.gov/media/pdf/062403ja.pdf, son los siguientes:

El 62% informó incidentes en el trabajo que podrían poner en riesgo los datos de los clientes.

para el robo de identidad.

El 66% dice que sus compañeros de trabajo, no los hackers, representan el mayor riesgo para

privacidad del consumidor. Solo el 10% dijo que los hackers eran la mayor amenaza.

El 46% dice que sería “fácil” a “extremadamente fácil” para que los trabajadores lo retiren

Datos sensibles de la base de datos corporativa.

El 32%, aproximadamente uno de cada tres, desconoce las políticas internas de la compañía para proteger los datos del cliente.

Estas son estadísticas asombrosas y desgarradoras.
Los capítulos posteriores discuten estos números en más detalle.

mostrar un defecto grave en la forma en que se maneja la seguridad. Educación, con suerte antes de una brecha, entonces la gente puede hacer

Puede prevenir pérdidas no deseadas, dolor y daños monetarios.

Sun Tzu dijo: “Si conoces al enemigo y te conoces a ti mismo, no debes temer los resultados de cien batallas”. Cuan cierto son esas palabras, pero saber es solo la mitad de la batalla. La acción sobre el conocimiento es lo que define la sabiduría, no solo el conocimiento solo.

Este libro es el más eficaz utilizado como manual o guía en el mundo de los ataques sociales, la manipulación social y la ingeniería social.

Lo que viene

Este libro está diseñado para cubrir todos los aspectos, herramientas y habilidades utilizadas por ingenieros sociales profesionales y maliciosos. Cada capítulo profundiza en la ciencia y el arte de una habilidad específica de ingeniería social para mostrarle cómo se puede utilizar, mejorar y perfeccionar.

La siguiente sección de este capítulo, “Descripción general de la ingeniería social”, define la ingeniería social y los roles que desempeña en la sociedad actual, así como los diferentes tipos de ataques de ingeniería social, incluidas otras áreas de la vida en las que se utiliza la ingeniería social de forma no convencional. De manera maliciosa. También discutiré cómo un ingeniero social puede usar el marco de ingeniería social para planificar una auditoría o mejorar sus propias habilidades.

El capítulo 2 es donde comienza la verdadera carne de las lecciones. La recopilación de información es la base de toda auditoría de ingeniería social. El mantra del ingeniero social es: “Soy tan bueno como la información que recopilo. “Un ingeniero social puede poseer todas las habilidades en el mundo, pero si él o ella no conoce el objetivo, si el ingeniero social no ha descrito todos los detalles íntimos, es más probable que ocurra una falla. La recopilación de información es el quid de cada compromiso de ingeniería social, aunque las habilidades de las personas y la capacidad de pensar en tus pies pueden ayudarte a salir de una situación difícil. La mayoría de las veces, cuanto más información reúna, mayores serán sus posibilidades de éxito.

Las preguntas que responderé en ese capítulo incluyen lo siguiente:

¿Qué fuentes puede usar un ingeniero social?
¿Qué información es útil?
¿Cómo puede un ingeniero social recolectar, recopilar y organizar esta información?
¿Cuánta información es suficiente?

Después de analizar la recopilación de información, el siguiente tema tratado en el Capítulo 2 es el modelo de comunicación. Este tema está estrechamente relacionado con la recopilación de información. Primero discutiré qué es el modelo de comunicación y cómo comenzó como una práctica. Luego, el capítulo explica los pasos necesarios para desarrollar y luego usar un modelo de comunicación adecuado. Describe cómo un ingeniero social usa este modelo contra un objetivo y los beneficios al describirlo para todos los compromisos.

El capítulo 3 cubre la obtención, el siguiente paso lógico en el marco. Ofrece una visión muy profunda de cómo se utilizan las preguntas para obtener información, contraseñas, un conocimiento profundo del objetivo y su compañía. Aprenderá qué es lo que es bueno y adecuado, y aprenderá lo importante que es tener planeados sus felicitaciones.

El Capítulo 3 también cubre el importante tema de precargar la mente del objetivo con información para que sus preguntas sean más fácilmente aceptadas. A medida que desenrede esta sección, verá claramente lo importante que es convertirse en un excelente indicador. También verás claramente cómo puedes usar esa habilidad no solo en tus prácticas de seguridad sino en Dailylife.

El capítulo 4, que cubre los pretextos, es poderoso. Este heavytopic es uno de los puntos críticos para muchos ingenieros sociales. Pretexting implica desarrollar el papel que el ingeniero social desempeñará para el ataque a la compañía. ¿Será el ingeniero social un cliente, proveedor, soporte técnico, nuevo empleado o algo igualmente realista y creíble? La expresión previa implica no solo crear una historia, sino también desarrollar la forma en que su persona se vería, actuaría, hablaría, caminaría; decidir qué herramientas y conocimientos tendrían; y luego dominar todo el paquete, de modo que cuando te acercas al objetivo, eres esa persona y no simplemente un personaje. Las preguntas cubiertas incluyen lo siguiente:

¿Qué es pretexting?
¿Cómo se desarrolla un pretexto?

¿Cuáles son los principios de un pretexto exitoso? ¿Cómo puede un ingeniero social planear y luego ejecutar un pretexto perfecto?

El siguiente paso en el marco es uno que puede llenar volúmenes. Sin embargo, debe ser discutido desde el punto de vista de un ingeniero social. El Capítulo 5 es una discusión sin restricciones sobre algunos temas muy conflictivos,

incluido el de las claves oculares. Por ejemplo, ¿cuáles son las opiniones variables de algunos profesionales sobre las señales de los ojos y cómo puede un ingeniero social usarlas? El capítulo también profundiza en la fascinante ciencia de las microexpresiones y sus implicaciones en la ingeniería social.

El capítulo 5 continúa analizando la investigación, dando respuestas a estas preguntas:

¿Es posible utilizar microexpresiones en el campo de la seguridad?
¿Cómo lo harías?
¿Qué beneficio tienen las microexpresiones?
¿Pueden las personas entrenarse para aprender cómo aprender?
¿Microexpresiones automáticamente?
Después de hacer la capacitación, qué información se obtiene a través de microexpresiones?

Probablemente uno de los temas más debatidos en el Capítulo 5 es la programación neurolingüística (PNL). El debate tiene muchas personas indecisas sobre qué es y cómo puede usarse. El Capítulo 5 presenta una breve historia de la PNL y lo que hace que la PNL sea una controversia. Puede decidir por sí mismo si la PNL es utilizable en ingeniería social.

El Capítulo 5 también trata uno de los aspectos más importantes de la ingeniería social en persona o por teléfono: saber cómo hacer buenas preguntas, escuchar las respuestas y luego hacer más preguntas. La interrogación y la entrevista son dos métodos que la policía ha utilizado durante años para manipular a los delincuentes para que confiesen y resuelvan los casos más difíciles. Esta parte del Capítulo 5 pone en práctica el conocimiento que adquirió en el Capítulo 3.

Además, el Capítulo 5 explica cómo crear una relación instantánea, una habilidad que puede utilizar en la vida cotidiana. El capítulo finaliza cubriendo mi propia investigación personal sobre “el desbordamiento de búfer humano”: la noción de que la mente humana es al igual que el software que los hackers explotan todos los días. Aplicando ciertos principios, Un ingeniero social experto puede desbordar la mente humana e inyectar

Cualquier orden que ellos quieran.

Al igual que los piratas informáticos escriben desbordamientos para manipular el software para ejecutar código, a la mente humana se le pueden dar ciertas instrucciones para, en esencia, “desbordar” el objetivo e insertar instrucciones personalizadas. El Capítulo 5 es una lección alucinante sobre cómo usar algunas técnicas simples para dominar cómo piensa la gente.

Muchas personas han pasado sus vidas investigando y probando lo que puede e influye en las personas. La influencia es una herramienta poderosa con muchas facetas. Con este fin, el capítulo 6 discute los fundamentos de la persuasión. Los principios comprometidos en el Capítulo 6 lo iniciarán en el camino hacia convertirse en un maestro de la persuasión.

El capítulo presenta una breve discusión de los diferentes tipos de persuasión que existen y proporciona ejemplos para ayudar a consolidar cómo puede usar estas facetas en la ingeniería social.

La discusión no se detiene allí, el encuadre también es un tema candente en la actualidad. Existen muchas opiniones diferentes sobre cómo se puede usar el encuadre, y este libro muestra algunos ejemplos reales de ello. Luego, diseccionando cada uno, lo guío a través de las lecciones aprendidas y las cosas que puede hacer para practicar el replanteamiento y el uso de marcos en la vida cotidiana como ingeniero social.

Otro tema abrumador en la ingeniería social es la manipulación:

¿Cual es su propósito?
¿Qué tipo de incentivos manejan los manipuladores?
¿Cómo puede una persona usarlo en ingeniería social?

El Capítulo 6 presenta todo lo que un ingeniero social necesita saber sobre el tema de la manipulación y cómo aplicar con éxito tales habilidades.

El Capítulo 7 cubre las herramientas que pueden hacer que una auditoría de ingeniería social sea más exitosa. Desde las herramientas físicas, como las cámaras ocultas hasta las herramientas de recopilación de información controladas por software, cada sección cubre herramientas probadas y comprobadas para ingenieros sociales.

Una vez que entienda el marco de la ingeniería social, el Capítulo 8 analiza algunos estudios de casos de la vida real. He elegido dos excelentes

Cuentas del ingeniero social de renombre mundial Kevin Mitnick. Analizo, analizo y luego propongo lo que puede aprender de estos ejemplos e identifico los métodos que utilizó en el marco de la ingeniería social.

Además, analizo qué se puede aprender de sus vectores de ataque y cómo se pueden usar hoy. Discuto algunas cuentas personales y las diseccionо, también.

¿Qué guía de ingeniería social estaría completa sin analizar algunas de las formas en que puede mitigar estos ataques? El apéndice proporciona esta información. Respondo algunas preguntas comunes sobre mitigación y ofrezco algunos consejos excelentes para ayudarlo a usted ya su organización a protegerse contra estos ataques malintencionados.

La descripción anterior es solo una muestra de lo que está por venir. Espero sinceramente que disfruten leyendo este libro tanto como yo disfruté escribiéndolo. La ingeniería social es una pasión para mí. Creo que hay ciertos rasgos, ya sean aprendidos o inherentes, que pueden hacer que alguien sea un gran ingeniero social. También me suscribo a la creencia de que con el tiempo y la energía suficientes, cualquiera puede aprender los diferentes aspectos de la ingeniería social y luego practicar estas habilidades para convertirse en un ingeniero social competente.

Los principios en este libro no son nuevos; No hay una tecnología alucinante que verás que cambiará la cara de la seguridad para siempre. No hay pastillas mágicas. De hecho, los principios han existido durante tanto tiempo como lo ha hecho la gente. Lo que hace este libro es combinar todas estas habilidades en un solo lugar. Le da una dirección clara sobre cómo practicar estas habilidades, así como ejemplos de situaciones de la vida real en las que se utilizan. Toda esta información puede ayudarlo a obtener un verdadero sentido de comprensión de los temas tratados.

El mejor lugar para comenzar es con lo básico, respondiendo a una pregunta fundamental: “¿Qué es la ingeniería social?”

Descripción general de la ingeniería social
¿Qué es la ingeniería social?

Una vez le hice esta pregunta a un grupo de entusiastas de la seguridad y me sorprendí por las respuestas que recibí:

“La ingeniería social está mintiendo a la gente para obtener información”.
“La ingeniería social es ser un buen actor.”
“La ingeniería social es saber cómo obtener cosas gratis”.

Wikipedia lo define como “el acto de manipular a las personas para que realicen acciones o divulguen información confidencial. Si bien es similar a un truco de confianza o un fraude simple, el término generalmente se aplica a trucos o engaños con el propósito de recopilar información, fraude o acceso a sistemas informáticos; en la mayoría de los casos, el atacante nunca se encuentra cara a cara con la víctima.”

Aunque se le ha dado un mal nombre por la gran cantidad de sitios de “pizza gratis”, “café gratis” y “cómo recoger polluelos”, algunos aspectos de la ingeniería social en realidad se relacionan con muchas personas de vida diaria.

El Diccionario Webster define lo social como “relacionado con la vida, el bienestar y las relaciones de los seres humanos en una comunidad. “También define ingeniería como” el arte o la ciencia de hacer una aplicación práctica del conocimiento de las ciencias puras, como física o química, como en la construcción de motores, puentes, edificios, minas, barcos y plantas químicas o artilugios hábiles o ingeniosos. ; maniobra.”

Combinando estas dos definiciones puede ver fácilmente que la ingeniería social es el arte o, mejor aún, la ciencia, de maniobrar hábilmente a los seres humanos para que actúen en algún aspecto de sus vidas.

Esta definición amplía los horizontes de los ingenieros sociales en todas partes. La ingeniería social se usa en la vida cotidiana en la forma en que los niños hacen que sus padres se rindan a sus demandas. Se utiliza en la forma en que los maestros interactúan con sus estudiantes, en la forma en que los médicos, abogados o psicólogos obtienen información de sus pacientes o clientes. Definitivamente se usa en la aplicación de la ley y en las citas; se usa verdaderamente en cada interacción humana, desde bebés hasta políticos y todos los demás.

Me gusta llevar esa definición un paso más allá y decir que una verdadera definición de ingeniería social es el acto de manipular a una persona para que tome una acción que puede o no estar en el mejor interés del "objetivo". Esto puede incluir obtener información, obtener acceso o lograr que el objetivo tome ciertas medidas.

Por ejemplo, los médicos, psicólogos y terapeutas a menudo usan elementos que yo considero que la ingeniería social "manipula" para que sus pacientes tomen acciones que son buenas para ellos, mientras que un estafador usa elementos de ingeniería social para convencer a su objetivo

el psicólogo puede usar una serie de preguntas bien concebidas para ayudar al paciente a llegar a la conclusión de que se necesita un cambio. De manera similar, un estafador usará preguntas bien elaboradas para mover su objetivo a una posición vulnerable.

Ambos ejemplos son la ingeniería social en su forma más verdadera, pero tienen objetivos y resultados muy diferentes. La ingeniería social no se trata solo de engañar a las personas, de mentir o de actuar. En una conversación que tuve con Chris Nickerson, un conocido ingeniero social del equipo Tiger de TVseries, dijo: "La verdadera ingeniería social no es solo creer que estás desempeñando un papel, sino que en ese momento eres esa persona, eres ese Rol, es lo que es tu vida."

La ingeniería social no es una acción cualquiera, sino una recopilación de las habilidades mencionadas en el marco que cuando se integran conforman la acción, la habilidad y la ciencia que llamo ingeniería social. De la misma manera, una comida maravillosa no es solo un ingrediente, sino que está compuesta por la cuidadosa combinación, mezcla y adición de muchos ingredientes. Así es como me imagino que sería la ingeniería social, y un buen ingeniero social es como un maestro de cocina. Ponga un poco de e licitación, agregue una sacudida de manipulación, y unos cuantos puñados de pretextos, y ¡bam! - viene una gran comida del ingeniero social perfecto.

Por supuesto, este libro analiza algunas de estas facetas, pero el enfoque principal

es lo que puede aprender de las autoridades policiales, los políticos, los psicólogos e incluso los niños para mejorar sus habilidades para auditar y luego asegurarse. Analizar cómo un niño puede manipular a un padre tan fácilmente.

le da al ingeniero social una visión de cómo funciona la mente humana. Notar cómo un psicólogo formula las preguntas puede ayudar a ver qué es lo que tranquiliza a las personas. Al darse cuenta de cómo un agente de la ley realiza un éxito

La interrogación proporciona un camino claro sobre cómo obtener información de un objetivo. Viendo cómo los gobiernos y los políticos enmarcan sus mensajes para la

El mayor impacto puede mostrar qué funciona y qué no. Analizando como un

El actor se mete en un papel que puede abrir tus ojos al asombroso mundo de los pretextos. Al diseccionar la investigación y el trabajo de algunas de las mentes líderes en

Las microexpresiones y la persuasión pueden ver cómo usarlas.

Técnicas en ingeniería social. Al revisar algunos de los motivadores de algunos de los mejores vendedores y expertos en persuasión del mundo, puede aprenda cómo establecer una buena relación, tranquilizar a la gente y cerrar tratos.

Luego, al investigar y analizar la otra cara de esta moneda (los estafadores y los ladrones), puede aprender cómo todas estas habilidades se unen para influir en las personas y hacer que las personas se dirijan a direcciones que pensaron que nunca irían.

Combine este conocimiento con las habilidades de selección de cerraduras, espías que usan cámaras ocultas y recolectores de información profesionales, y usted tiene un ingeniero social talentoso.

No usas todas estas habilidades en cada compromiso, ni puedes dominar todas estas habilidades. En cambio, al comprender cómo funcionan estas habilidades y cuándo usarlas, cualquiera puede dominar la ciencia de la ingeniería social. Es cierto que algunas personas tienen un talento natural, como Kevin Mitnick, quien podría convencer a cualquiera de cualquier cosa, al parecer. Frank Abagnale, Jr., parecía tener los talentos naturales para engañar a la gente para que creyera que él era quien él quería que creyeran que era. Victor Lustig hizo lo increíble, en realidad convenció a algunas personas de que tenía los derechos para vender la Torre Eiffel, superada solo por su estafa en Al Capone.

Estos ingenieros sociales y muchos más como ellos parecen tener talento natural o una falta de miedo que les permite probar cosas que la mayoría de nosotros nunca consideraríamos intentar. Desafortunadamente en el mundo actual, los hackers maliciosos están mejorando continuamente sus habilidades para manipular personas y los ataques maliciosos de ingeniería social están aumentando. Dark Reading ha publicado un artículo.

(www.darkreading.com/database_security/security/attacks/showArticle.jhtml? articleID = 226200272) que menciona que las violaciones de datos han alcanzado entre $ 1 y $ 53 millones por violación. Al citar la investigación realizada por el Instituto Ponemon, DarkReading afirma que “Ponemon descubrió que los ataques por Internet, los códigos maliciosos y los iniciados maliciosos son los tipos de ataques más costosos, que constituyen

más del 90 por ciento de todos los costos de delitos informáticos por organización por año: un ataque basado en la Web cuesta $ 143,209; código malicioso, $ 124,083; y información privilegiada maliciosa, $ 100,300 “. Personas internas malintencionadas se enumeran en la parte superior tres sugieren que las empresas deben ser más conscientes de las amenazas planteadas por una ingeniería social malintencionada, incluso por parte de los empleados.

Muchos de estos ataques podrían haberse evitado si las personas hubieran sido educadas, porque podrían actuar en base a esa educación. A veces simplemente descubriendo cómo

Las personas malintencionadas piensan y actúan pueden ser una revelación.

Como ejemplo, en una escala mucho más pequeña y más personal, recientemente estuve hablando con un amigo cercano sobre sus cuentas financieras y sobre cómo le preocupaba que la piratearan o la estafaran. En el curso de la conversación, comenzamos a discutir qué tan fácil es “adivinar” las contraseñas de las personas. Le dije que muchas personas usan las mismas contraseñas para cada cuenta; Vi su cara blanca cuando se dio cuenta de que era ella. Le dije que la mayoría de las personas usan contraseñas simplistas que combinan cosas como el nombre de su cónyuge, su cumpleaños o fecha de aniversario. La vi ir un tono cada vez más brillante de pálido. Continué diciendo que la mayoría de las veces las personas eligen la “pregunta de seguridad” más simple, como “su apellido de soltera (o el de su madre)” y lo fácil que es encontrar esa información a través de Internet o algunas llamadas telefónicas falsas.

Mucha gente incluirá esta información en las cuentas de Blippy, Twitter o Facebook. Esta amiga en particular no usaba demasiado los sitios de redes sociales, así que le pregunté que si pensaba con algunas llamadas telefónicas podría imaginarse a sí misma entregando esta información. Por supuesto que ella dijo que no. Para ilustrar con qué facilidad las personas entregan información personal, le dije que una vez vi un mantel en un restaurante que tenía un cupón de $ 50 para un campo de golf local, una oferta muy atractiva. Para aprovechar esta oferta, solo tenía que proporcionar su nombre, fecha de nacimiento y dirección, y proporcionar una contraseña para una cuenta que se configuraría y enviaría a su dirección de correo electrónico. (Solo noté esto en primer lugar porque alguien había comenzado a llenar el cupón y lo dejó sobre la mesa.) Todos los días se crean sitios web para recopilar dicha información confidencial. Una llamada telefónica con una encuesta o una investigación rápida en Internet puede producir una fecha de nacimiento o fecha de aniversario, y armado con esta información, tengo suficiente para construir una lista de ataque de contraseña. Además, una docena de sitios ofrecen registros detallados de todo tipo de información personal de una persona por solo $ 9 a $ 30 USD.

Al darse cuenta de cómo piensan los ingenieros sociales malintencionados, cómo reaccionan los estafadores a la información y cómo los estafadores intentarán cualquier cosa, puede ayudar a las personas a estar más conscientes de lo que sucede a su alrededor.

Un equipo de entusiastas de la seguridad y yo hemos rastreado Internet recolectando historias que muestran muchos aspectos diferentes de la ingeniería social. Estas Las historias pueden ayudar a responder una pregunta vital: "¿Cómo se usa la ingeniería social en la sociedad en el tiempo?", y ver dónde está el lugar de la ingeniería social y cómo se usa de manera maliciosa.

La ingeniería social y su lugar en la sociedad

Como ya se ha comentado, la ingeniería social se puede utilizar en muchas áreas de la vida, pero no todos estos usos son maliciosos o malos. Muchas veces, la ingeniería social puede usarse para motivar a una persona a tomar una acción que sea buena para ella. ¿Cómo?

Piensa en esto: John necesita perder peso. Él sabe que no es saludable y necesita hacer algo al respecto. Todos los amigos de John también tienen sobrepeso. Incluso hacen bromas sobre las alegrías de tener sobrepeso y dicen cosas como: "Me encanta no preocuparme por mi figura". Por un lado, este es un aspecto de la ingeniería social. Es una prueba o consenso social, donde lo que encuentre o considere aceptable será determinado por quienes lo rodean. Debido a que las asociaciones cercanas de John consideran que el sobrepeso es aceptable, es más fácil para John aceptarlo. Sin embargo, si uno de esos amigos perdió peso y no se convirtió en crítico, pero estaba motivado para ayudar, existe la posibilidad de que el marco mental de John sobre su peso pueda cambiar y pueda comenzar a sentir que perder peso es posible y bueno.

Esto es, en esencia, la ingeniería social. Para que pueda ver claramente cómo la ingeniería social se adapta a la sociedad y la vida cotidiana, las siguientes secciones presentan algunos ejemplos de ingeniería social, estafas y manipulación, y una revisión de cómo funcionaron.

La estafa 419

La estafa 419, más conocida como la estafa nigeriana, se ha convertido en una epidemia. Puede encontrar una historia archivada y un artículo sobre esta estafa en www.social-engineer.org/wiki/archives/ConMen/ConMen-Scam NigerianFee.html.

Básicamente, un correo electrónico (o en los últimos tiempos, una carta) llega al objetivo diciéndole que ha sido seleccionado para un trato muy lucrativo y que todo lo queLa suma de dinero de los bancos extranjeros puede tener un porcentaje. Después de que el objetivo es seguro y "se apunta", surge un problema que hace que el objetivo pague una cuota. Después de que se paga la tarifa, surge otro problema, junto con otra tarifa.

Cada problema es "el último" con "una tarifa final" y esto puede prolongarse durante muchos meses. La víctima nunca ve dinero y pierde entre $ 10,000 y $ 50,000 USD en el proceso. Lo que hace esta estafa tan increíble es que en el pasado, se han informado documentos oficiales, documentos, membretes e incluso reuniones personales.

Recientemente, apareció una variación de esta estafa en la que literalmente se envía un cheque real a las víctimas. Los estafadores prometen una enorme suma de dinero y quieren. a cambio solo una pequeña porción por sus esfuerzos. Si el objetivo transfiere una suma pequeña (en comparación) de $ 10,000, cuando reciba el cheque prometido, puede depositar el cheque y mantener la diferencia. El problema es que el cheque que viene es un fraude y cuando la víctima va a cobrarlo ella es abofeteado con cargos y multas por fraude de cheques, en algunos casos después de que la víctima ya haya transferido dinero al estafador.

Esta estafa es exitosa porque juega con la codicia de la víctima. ¿Quién no daría $ 10,000 para ganar $ 1,000,000 o incluso $ 100,000? Más inteligente la gente lo haría Cuando estas personas se presentan con documentos oficiales,

Pasaportes, recibos e incluso oficinas oficiales con "personal del gobierno", entonces su creencia está establecida y harán todo lo posible para completar el trato.

Compromiso y consisten en que son parte de esta estafa así como también de obligación. Discutiré estos atributos con mayor detalle en capítulos posteriores, y cuando lo haga, verán por qué esta estafa es tan poderosa.

El poder de la escasez

El artículo archivado en www.social engineer.org/wiki/archives/Governments/Governments FoodElectionWeapon.html habla sobre un principio llamado escasez.

La escasez es cuando a las personas se les dice algo que necesitan o desean, tienen una disponibilidad limitada y para obtenerlas deben cumplir con cierta actitud o acción. Muchas veces el comportamiento deseado ni siquiera se habla, pero la forma en que se transmite es mostrando a las personas que están actuando "adecuadamente" obteniendo recompensas.

El artículo habla sobre el uso de alimentos para ganar las elecciones en Sudáfrica.

Cuando un grupo o persona no apoya al líder "correcto", los productos alimenticios se vuelven escasos y los empleos que una vez tuvieron se otorgan a otros que lo apoyan más. Cuando la gente ve esto en acción, no se tarda mucho en hacer que se pongan en línea. Esta es una forma de ingeniería social muy maliciosa e hiriente, pero no obstante, una de la cual aprender. A menudo ocurre que las personas quieren lo que escasean y harán cualquier cosa si llevan a creer que ciertas acciones harán que pierdan esos artículos. Lo que hace que ciertos casos incluso

Peor, como en el ejemplo anterior, es que un gobierno tomó algo necesario para la vida y lo hizo "escaso" y disponible solo para los partidarios, una táctica de manipulación maliciosa, pero muy efectiva.

El Dalai Lama y la ingeniería social.

El interesante artículo archivado en www.social engineer.org/wiki/archives/Spies/Spies-DalaiLama.html detalla un ataque realizado contra el Dalai Lama en 2009.

El grupo de piratas informáticos de chinos, quería acceder a los servidores y archivos de la red propiedad del Dalai Lama. ¿Qué métodos se utilizaron en este ataque exitoso?

Los atacantes convencieron al personal de la oficina de Dalai Lama para que descargar y abrir software malicioso en sus servidores. Este ataque es interesante porque combina tanto la tecnología hacking como la ingeniería social.

El artículo dice: "El software se adjuntó a los correos electrónicos que pretendían provenir de colegas o contactos en el movimiento tibetano, según el investigador Ross Anderson, profesor de ingeniería de seguridad del Laboratorio de Computación de la Universidad de Cambridge, citado por el Washington Times el lunes. . El software robó contraseñas y otra información, que a su vez les dio acceso a los piratas informáticos al sistema de correo electrónico de la oficina y a los documentos almacenados en las computadoras allí."

Se utilizó la manipulación, así como los vectores de ataque comunes, como el phishing (la práctica de enviar correos electrónicos con mensajes atractivos y enlaces o archivos que deben abrirse para recibir más información; a menudo esos enlaces o archivos conducen a cargas maliciosas) y explotación. Este ataque Trabajó y ha trabajado contra grandes corporaciones, así como contra gobiernos. Este ejemplo es solo uno en una gran cantidad de ejemplos donde estos vectores pueden causar daño masivo.

Robo de empleados

El tema del robo de empleados podría llenar volúmenes, especialmente a la luz de la estadística asombrosa que se encuentra en www.social engineer.org/wiki/archives/DisgruntledEmployees/DisgruntledEmployees EmployeeTheft.html que más del 60 por ciento de los empleados entrevistados admitieron que tomaron datos de un tipo u otro de sus empleadores.

Muchas veces estos datos se venden a competidores (como sucedió en esta historia de un empleado de Morgan Stanley: www.social engineer.org/wiki/archives/DisgruntledEmployees/DisgruntledEmployees MorganStanley.html). Otras veces el robo de empleados es a tiempo u otros recursos; en algunos casos, un empleado descontento puede causar un daño mayor.

Una vez hablé con un cliente sobre políticas de despido de empleados, cosas como deshabilitar tarjetas de acceso, desconectar cuentas de red y escoltar a empleados despedidos fuera del edificio. La compañía sintió que todos eran parte de la "familia" y que esas políticas no se aplicarían.

Desafortunadamente, llegó el momento de dejar ir a "Jim", una de las personas de mayor rango en la compañía. El "despido" salió bien; Fue amistoso y Jim dijo que entendía. Lo único que hizo bien la compañía fue manejar los despidos alrededor del horario de cierre para evitar la vergüenza y la distracción. Le estrecharon las manos y luego Jim hizo la fatídica pregunta: "¿Puedo tomarme una hora para limpiar mi escritorio y sacar algunas fotos personales de mi computadora? Convertiré mi tarjeta de acceso en la guardia de seguridad antes de irme."

Sintiéndose bien con la reunión, todos estuvieron de acuerdo rápidamente y se fueron con sonrisas y algunas risas. Luego, Jim fue a su oficina, empacó una caja de todos sus artículos personales, sacó las fotos y otros datos de su computadora, se conectó a la red y borró el valor de los 11 servidores: registros contables, nómina, facturas, pedidos, historial gráfico y mucho más

Suprimido en cuestión de minutos. Jim entregó su tarjeta de acceso tal como lo había prometido y abandonó con calma el edificio sin pruebas de que él fue el que inició estos ataques.

A la mañana siguiente recibí una llamada del propietario que describía la carnicería a raíz del ex empleado. Con la esperanza de obtener una bala de plata, el cliente no tuvo más remedio que intentar recuperar lo que podía recuperarse de forma forense y volver a empezar desde las copias de seguridad, que tenían más de dos meses.

Los empleados contrariedades que quedan sin control pueden ser más devastadores que un equipo de piratas informáticos capacitados y determinados. Por una suma de $ 15 mil millones de dólares, eso es lo que se calcula que la pérdida es para las empresas en los Estados Unidos solo debido al robo de empleados.

Estas historias pueden dejar una pregunta sobre las diferentes categorías de ingenieros sociales que existen y si se pueden clasificar.

DarkMarket y Master Splynter

En 2009 se publicó una historia sobre un grupo clandestino llamado DarkMarket, el llamado eBay para criminales, un grupo muy estricto que intercambiaba números de tarjetas de crédito robadas y herramientas de robo de identidad, así como los elementos necesarios para hacer credenciales falsas y más.

Un agente del FBI llamado J. Keith Mularski se ocultó y se infiltró en el sitio de DarkMarket. Después de un tiempo, el agente Mularski se convirtió en administrador del sitio. A pesar de que muchos intentaron desacreditarlo, se mantuvo durante más de tres años como administrador del sitio.

Durante este tiempo, Mularski tuvo que vivir como un hacker malicioso, hablar y actuar como uno, y pensar como uno solo. Su pretexto fue uno de un spammer malicioso y tenía el conocimiento suficiente para lograrlo. Su pretexto y sus habilidades de ingeniería social dieron sus frutos porque el Agente Mularski se infiltró en DarkMarket como el infame Maestro Splynter, y después de tres años fue esencial para cerrar una red de robo de identidad masiva.

La operación de tres años de la ingeniería social provocó 59 arrestos e impidió más de $ 70 millones en fraude bancario. Este es solo un ejemplo de cómo las habilidades de ingeniería social pueden usarse para bien.

Los diferentes tipos de ingenieros sociales

Como se discutió anteriormente, la ingeniería social puede tomar muchas formas. Puede ser malicioso y amigable, puede acumularse y derribar. Antes de pasar al núcleo de este libro, observe brevemente las diferentes formas de ingenieros sociales y una breve descripción de cada uno:

Hackers: los proveedores de software se están volviendo más hábiles para crear. Software que está endurecido, o más difícil de penetrar. Como hackers están golpeando más software endurecido y como software y red Los vectores de ataque, como la piratería remota, son cada vez más difíciles, Los hackers están recurriendo a las habilidades de ingeniería social. A menudo utilizando una mezcla de hardware y habilidades personales, los hackers están usando redes sociales Ingeniería en ataques mayores así como en infracciones menores. alrededor del mundo.

Pruebas de penetración: desde un probador de penetración en el mundo real (también conocido como pentester) es de naturaleza muy ofensiva, esta categoría debe Sigue a los hackers. Los verdaderos probadores de penetración aprenden y usan las habilidades. que los hackers maliciosos utilizan para ayudar verdaderamente a garantizar la seguridad de un cliente. Los probadores de penetración son personas que pueden tener las habilidades de un Sombrero negro malicioso pero que nunca usa la información para uso personal. Ganar o dañar al objetivo.

Espias: Los espías usan la ingeniería social como una forma de vida. A menudo empleando todos los aspectos del marco de la ingeniería social (discutido más adelante en En este capítulo), los espías son expertos en esta ciencia. Espias de todo En el mundo se enseñan diferentes métodos para "engañar" a las víctimas creyendo que son alguien o algo que no son. Además de enseñando el arte de la ingeniería social, muchas veces los espías también construir sobre la credibilidad al saber un poco o incluso mucho sobre el negocio o el gobierno están tratando de ingeniero social.

Ladrones de identidad: el robo de identidad es el uso de información como el nombre de una persona, los números de cuenta bancaria, la dirección, la fecha de nacimiento y Número de seguro social sin el conocimiento del propietario. Este crimen puede ir desde ponerse un uniforme hasta hacerse pasar por alguien para Estafas mucho más elaboradas. Los ladrones de identidad emplean muchos aspectos. De la ingeniería social y con el tiempo se envalentonan e indiferentes al sufrimiento que causan.

Empleados descontentos: Después de que un empleado se ha descontento, a menudo entran en una relación adversa con su empleador. A menudo, esto puede ser una situación unilateral, porque el empleado Por lo general, tratan de ocultar su nivel de disgusto para no poner su Empleo en riesgo. Sin embargo, cuanto más descontentos se vuelvan, más fácil se vuelve justificar los actos de robo, vandalismo u otros delitos.

Artista de la estafa: las estafas o los contras apelan a la codicia u otros principios que atraen las creencias y los deseos de las personas de "ganar dinero". los estafadores dominan la capacidad de leer a las personas y captar pequeñas señales que Haz que una persona sea una buena "marca". También son hábiles para crear situaciones que se presentan como oportunidades imbatibles para una marca.

Reclutadores ejecutivos: los reclutadores también deben dominar muchos aspectos de la ingeniería social. Al tener que dominar la elicitación, así como muchos de los principios psicológicos de la ingeniería social, se vuelven muy expertos no solo en leer a las personas sino también en comprender lo que motiva a las personas. Muchas veces, un reclutador debe tener en cuenta y agradar no solo al solicitante de empleo sino también al póster del trabajo.

Vendedores: similares a los reclutadores, los vendedores deben dominar muchos los talentos de la gente. Muchos gurús de las ventas dicen que un buen vendedor no manipula a las personas sino que utiliza sus habilidades para averiguar cuáles son las necesidades de las personas y luego ve si pueden satisfacerlas. El arte de las ventas.

toma muchas habilidades como la recopilación de información, elicitación, influencia, principios psicológicos, así como muchas otras personas habilidades.

Gobiernos: no son vistos a menudo como ingenieros sociales, los gobiernos utilizan la ingeniería social para controlar los mensajes que emiten, así como las personas que gobiernan. Muchos gobiernos utilizan pruebas sociales, autoridad y escasez para asegurarse de que sus sujetos estén en control. Este tipo de ingeniería social no siempre es negativo, porque algunos de los mensajes que transmiten los gobiernos son para el bien de las personas y el uso de ciertos elementos de la ingeniería social puede hacer que el mensaje sea más atractivo y más ampliamente aceptado

Médicos, psicólogos y abogados: aunque las personas en estos Puede parecer que las carreras profesionales no encajan en la misma categoría que muchos De estos otros ingenieros sociales, este grupo emplea el mismo. Métodos utilizados por los otros grupos en esta lista. Deben usar elicitación y las tácticas de entrevista e interrogación adecuadas, así como muchos si no todos los principios psicológicos de la ingeniería social para manipular sus "objetivos" (clientes) en la dirección que ellos desean que tomar.

Independientemente del campo, parece que puedes encontrar ingeniería social o un aspecto de ella. Por eso sostengo firmemente que la ingeniería social es una ciencia. Existen ecuaciones de conjunto que permiten a una

persona “sumar” elementos de ingeniería social para lograr el objetivo. En el ejemplo de un estafador, piense en la ecuación como esta: pretexto + manipulación + apego a la codicia = el objetivo es una ingeniería social.

En cada situación, saber qué elementos funcionarán es la parte difícil, pero luego aprender a utilizar esos elementos es donde entra en juego la habilidad. Esta fue la base para el pensamiento detrás del desarrollo del marco de ingeniería social. Este marco ha revolucionado la forma en que se disecciona la ingeniería social, como se analiza en la siguiente sección.

El marco de la ingeniería social y cómo usarlo

A través de la experiencia y la investigación, he tratado de delinear los elementos que conforman un ingeniero social. Cada uno de estos elementos define una parte de la ecuación que equivale a un ingeniero social completo. Estos aspectos no están escritos en piedra; De hecho, desde su estado original hasta ahora, el marco ha sido crecido.

El propósito del marco es proporcionar suficiente información para que cualquiera pueda desarrollar estas habilidades. El marco no está diseñado para ser un recurso integral para toda la información en cada capítulo. Por ejemplo, la parte del Capítulo 5 que cubre las micro expresiones se basa en la investigación de algunas de las mejores mentes en este campo y mi experiencia en el uso de esa información. De ninguna manera tiene la intención de reemplazar los 50 años de investigación por mentes tan grandes como el Dr. Paul Ekman.

A medida que lea el marco, verá que al utilizar las muchas habilidades que contiene, no solo puede mejorar su práctica de seguridad, sino también su forma de pensar acerca de cómo mantenerse seguro, cómo comunicarse más plenamente y cómo entender cómo piensa la gente. .

Consulte la tabla de contenido para obtener una imagen clara del marco o véalo en línea en www.social-engineer.org/framework. A primera vista, el marco puede parecer desalentador, pero dentro de este libro encontrará un análisis de cada tema que le permitirá aplicar, mejorar y desarrollar estas habilidades.

El conocimiento es poder, es verdad. En este sentido, la educación es la mejor defensa contra la mayoría de los ataques de ingeniería social. Incluso aquellos contra los que el conocimiento no puede proteger al 100 por ciento, tener detalles de estos ataques lo mantiene alerta. La educación puede ayudarlo a mejorar sus propias habilidades, así como a estar alerta.

Sin embargo, junto con la educación, necesitas práctica. Este libro no fue diseñado para ser un manual de una sola lectura; En su lugar, fue diseñado para ser una guía de estudio. Puedes practicar y personalizar cada sección según tus necesidades. El marco es progresivo en el sentido de que es la forma en que se presenta un ataque de ingeniería social. Cada sección del marco analiza el siguiente tema en el orden en que un ingeniero social podría utilizar esa habilidad en sus fases de compromiso o planificación.

El marco muestra cómo se puede describir un ataque. Después de planear el ataque, las habilidades que se necesitan se pueden estudiar, mejorar y practicar antes de la entrega.

Supongamos, por ejemplo, que está planeando una auditoría de ingeniería social contra una empresa que quería ver si podría obtener acceso a su sala de servidores y robar datos.

Tal vez su plan de ataque sea pretender ser una persona de soporte técnico que necesita acceso a la sala de servidores. Usted querría recopilar información, tal vez incluso realizar una inmersión en un contenedor de basura.

Luego, bajo el pretexto de ser el chico de la tecnología, podrías utilizar algunas herramientas de cámara secretas, así como practicar el lenguaje adecuado y las señales faciales / vocales para saber cómo actuar, sonar y lucir como un chico de la tecnología. Si localiza qué compañía utiliza su cliente para el soporte técnico, tal vez necesite

para hacer información reuniendo en él. ¿A quién suele atenderle su cliente? ¿Cuáles son los nombres de los empleados con los que interactúan? El ataque necesita ser planeado adecuadamente.

Sin embargo, este libro no es solo para aquellos que realizan auditorías. Muchos lectores sienten curiosidad por saber qué son los ataques, no porque estén protegiendo a una empresa, sino porque necesitan protegerse a sí mismos. No ser consciente de la forma en que un ingeniero social malintencionado cree que puede llevar a alguien

por el camino hacia ser hackeado. Los estudiantes universitarios en el campo de la seguridad también han utilizado el marco. La información en el marco describe una ruta realista para estos vectores, o métodos de ataque, y permite al lector estudiarlos en profundidad.

En general, esta información también puede ayudar a mejorar su capacidad para comunicarse en la vida cotidiana. Saber leer expresiones faciales o usar preguntas para tranquilizar a las personas y obtener respuestas positivas puede mejorar su capacidad para comunicarse con su familia y amigos. Puede ayudarlo a convertirse en un buen oyente y ser más consciente de los sentimientos de las personas.

Ser capaz de leer el lenguaje corporal, las expresiones faciales y los tonos vocales de las personas también puede mejorar su capacidad para ser un comunicador eficaz. Comprender cómo protegerse y proteger a sus seres queridos solo lo hará más valioso y más consciente del mundo que lo rodea.

Resumen

Como cualquier libro, el conocimiento aquí contenido solo es útil si lo pones en práctica. Cuanto más practiques, más dominarás estas habilidades.

Anteriormente, hablé de cómo la ingeniería social es como dominar el arte de cocinar. Al mezclar los ingredientes correctos en la cantidad correcta, puede tener una comida llena de sabor y emoción. Es posible que la primera vez que intentes cocinar una comida tenga demasiada sal o que no tenga mucho sabor, pero no tiras la toalla de inmediato; sigues intentando hasta que lo hagas bien. Lo mismo ocurre con la ingeniería social. Algunas de las habilidades necesarias pueden venir más naturalmente para usted y otros tal vez más difíciles.

Si un tema en particular es difícil de entender o de entender, no se dé por vencido y no asuma que no puede aprenderlo. Cualquiera puede aprender y usar estas habilidades con la cantidad adecuada de esfuerzo y trabajo. También tenga en cuenta que, al igual que una receta real, muchos “ingredientes” entran en un buen trabajo de ingeniería social. El primer ingrediente podría tener más sentido después de bajar un poco más la línea. Ciertas habilidades, como el “desbordamiento de búfer humano” que se cubre en el Capítulo 5, solo tendrán sentido después de que domine algunas de las otras habilidades que se analizan en este libro.

En cualquier caso, siga practicando y asegúrese de hacer una investigación adicional sobre temas para los que necesita claridad. Ahora comencemos a cocinar. Su “receta” comienza en el siguiente capítulo con el primer ingrediente, la recopilación de información.

Capitulo 2

Recopilación de información
La guerra es información del noventa por ciento.

- Napoleón Bonaparte Se ha dicho que ninguna información es irrelevante. Esas palabras suenan verdaderas cuando se trata de este capítulo sobre la recopilación de información. Incluso el más mínimo detalle puede llevar a una ruptura exitosa de ingeniería social.

Mi buen amigo y mentor, Mati Aharoni, quien ha sido un pentester profesional durante más de una década, cuenta una historia que realmente lleva este punto a casa. Se le asignó la tarea de obtener acceso a una empresa que tenía una huella casi inexistente en la Web. Debido a que la compañía ofreció muy pocas vías para hackear, obtener este acceso resultaría ser muy desafiante.

Mati comenzó a buscar en Internet cualquier detalle que pudiera conducir a un camino. En una de sus búsquedas encontró a un funcionario de la empresa de alto rango que utilizó su correo electrónico corporativo en un foro sobre coleccionismo de sellos y que expresó interés en los sellos de la década de 1950. . Mati rápidamente registró una URL, algo como www.stampcollection.com, y luego encontró un montón de viejas fotos de sellos de 1950 en Google. Creando un sitio web rápido para mostrar su “colección de sellos”, luego redactó un correo electrónico para la empresa oficial:

Estimado señor,

Vi en www.forum.com que te interesan los sellos de los años cincuenta. Recientemente mi abuelo falleció y me dejó una colección de sellos que me gustaría vender. Tengo un sitio web creado; Si desea verlo, visite www.stampcollection.com.

Gracias, Mati

Antes de enviar el correo electrónico al objetivo, quería asegurarse de que tendría el máximo impacto. Tomó el número de la oficina del foro y llamó por teléfono al hombre. “Buenos días, señor, este es Bob. Vi su publicación en www.forum.com. Mi Abuelo pasó recientemente y me dejó un montón de sellos de los años cincuenta y sesenta. Tomé fotos e hice un sitio web. Si te interesa puedo enviarte el enlace y puedes echar un vistazo “. El objetivo estaba muy ansioso por ver esta colección y aceptó fácilmente el correo electrónico. Mati le envió el correo electrónico al hombre y lo esperó para hacer clic en el enlace. Qué Mati lo hizo fue incrustar un marco malicioso en el sitio web. Este cuadro tenia código en él, que explotaría una vulnerabilidad conocida en el popular navegador Internet Explorer y le daría el control sobre la computadora del objetivo a Mati. La espera no fue larga: tan pronto como el hombre recibió el correo electrónico, hizo clic en el enlace y el perímetro de la empresa se vio comprometido.

Una pieza de información, el correo electrónico corporativo que este hombre solía buscar en los sellos, es lo que llevó a este compromiso. Ninguna información es irrelevante. Con ese conocimiento en mente, Aquí hay preguntas que surgen con respecto a la recopilación de información:

¿Cómo puedes reunir información?

¿Qué fuentes existen para que los ingenieros sociales recaben información?

¿Qué puedes extraer de esta información para perfilar tus objetivos

¿Cómo puede ubicar, almacenar y catalogar toda esta información para el nivel de uso más fácil?

Estas son solo algunas de las preguntas para las que tendrá que encontrar respuestas para lograr una recopilación de información adecuada y efectiva. Con la gran cantidad de sitios de redes sociales que existen, las personas pueden compartir fácilmente cada aspecto de sus vidas con cualquier persona que elijan, haciendo que la información potencialmente dañina esté más disponible que nunca. Este capítulo se centra en los principios de la recopilación de información mediante la presentación de ejemplos de cómo se puede utilizar en ingeniería social y los efectos devastadores que algunas de las informaciones que la gente publica en la Web pueden tener sobre su seguridad personal y empresarial.

Muchas de las habilidades o métodos que un ingeniero social puede usar provienen de otros campos. Un campo que es excelente para recopilar información es ventas.

Los vendedores tienden a ser muy habladores, tranquilos y muy buenos en la recopilación de datos sobre aquellos con quienes interactúan.

Una vez leí un libro sobre ventas en el que el autor alentó a los vendedores a reunir referencias del comprador, algo así como: “¿Puede decirme una persona que crea que podría beneficiarse de este producto tanto como usted?”

El uso de una redacción simple puede hacer que una persona se abra y refiera a familiares, amigos y tal vez incluso a compañeros de trabajo. La recolección, o la recopilación de esta información y luego su almacenamiento, permite que el personal de ventas tenga lo que llaman “clientes potenciales” para llamar. El líder de Awarm es donde tienen a una persona con un “adentro”, una forma de entrar por la puerta sin tener que llamar por teléfono.

El vendedor ahora puede llamar a esas referencias y dice algo como: “Estaba en la casa de Jane dos puertas más abajo, y ella compró nuestra póliza de primas. Después de revisar los beneficios y pagar el año por adelantado, dijo que podría beneficiarse de la misma cobertura. ¿Tienes un minuto para que te muestre lo que compró Jane?”

Estas habilidades utilizadas por los vendedores a menudo son reflejadas por ingenieros sociales.

Por supuesto, un ingeniero social no está pidiendo referencias, sino que piensa en el flujo de información dentro y fuera de esta conversación. El vendedor recopila información de su cliente actual, luego transmite esa información de una manera

eso hará que el nuevo "objetivo" sea más susceptible de escucharlo y dejarlo entrar. Además, al dar pistas sobre lo que compró el primer cliente y al usar palabras como "premium" y "de antemano", el vendedor está precargando el

Nuevo objetivo con las palabras clave que quiere usar en él en poco tiempo. Esta técnica es efectiva porque genera confianza, usa la familiaridad y permite el objetivo de sentirse cómodo con el vendedor o el ingeniero social, dando a su mente un puente sobre la brecha que normalmente existiría allí. Este capítulo, así como el siguiente capítulo, profundizarán en estos temas.

Como ingeniero social, ambos ángulos son de vital importancia para comprenderlos y utilizarlos con eficacia. Para volver a la ilustración utilizada en el Capítulo 1 de siendo un chef, un buen chef sabe todo sobre cómo detectar productos de buena calidad, Verduras frescas, y carnes de calidad. Están bien informados sobre lo que se incluye en la receta, pero a menos que se usen las cantidades correctas, quizás la comida demasiado blando o demasiado fuerte o no lo suficientemente bueno para comer en absoluto. Simplemente sabiendo que Una receta requiere que la sal no te haga un chef, pero saber cómo mezclar la cantidad y los tipos de ingredientes adecuados puede ayudarte a dominar el arte de cocinar. Un ingeniero social necesita dominar el tipo y la cantidad de habilidades que se utilizarán (la "receta"). Cuando se hace eso, pueden convertirse en un maestro ingeniero social.

Este capítulo ayuda a identificar este equilibrio. El primer ingrediente en cualquier receta para un ingeniero social es la información (detallada en la siguiente sección). Cuanto mayor sea la calidad de la información, mayor será la probabilidad de lograr el éxito. Este capítulo comienza discutiendo cómo recopilar información. Luego pasa a discutir qué fuentes se pueden usar para recopilar información. Este capítulo no estaría completo sin discutir cómo vincularlo todo y utilizar estos recursos como ingeniero social.

Reuniendo información

Recopilar información es como construir una casa. Si intentas comenzar con el techo, tu casa seguramente será un fracaso. Una buena casa se construirá con una base sólida y desde allí se construirá literalmente desde cero. A medida que recopila información, puede sentirse abrumado con la forma de organizar y luego usar estos datos, por lo que es una buena idea comenzar un archivo o un servicio de recopilación de información para recopilar estos datos.

Existen muchas herramientas para ayudar a recopilar y luego usar estos datos. Para las pruebas de penetración y las auditorías de ingeniería social, uso una distribución de Linux llamada BackTrack que está diseñada específicamente para este propósito. BackTrack es como la mayoría de las distribuciones de Linux en que es libre y de código abierto. Quizás su mayor ventaja es que contiene más de 300 herramientas diseñadas para ayudar a auditar la seguridad.

Todas las herramientas de BackTrack también son de código abierto y gratuitas. Especialmente atractiva es la alta calidad de las herramientas de BackTrack, muchas de las cuales rivalizan e incluso superan las herramientas por las que pagaría un brazo y una pierna. Dos herramientas de BackTrack que son particularmente útiles para recopilar y almacenar información se llaman Dradis y BasKet. Las siguientes secciones echen un vistazo rápido a cada una.

Usando BasKet

BasKet es similar en funcionalidad a Notepad, pero más como Notepad en esteroides. Actualmente, Kelvie Wong lo mantiene y se puede encontrar de forma gratuita en BackTrack o en http://basket.kde.org/. El sitio web tiene instrucciones completas sobre cómo instalar BasKet. Una vez instalado, BasKet es fácil de usar y la interfaz no es difícil de entender. Como se ve en la Figura 2-1, la interfaz es fácil de entender. Agregar una nueva "Cesta" para almacenar datos es tan simple como hacer clic derecho en el lado izquierdo de la pantalla y seleccionar Nueva cesta.

Una vez que se agregan cestas nuevas, el cielo es el límite. Puede copiar y pegar datos, colocar capturas de pantalla en la Cesta o incluso atar en OpenOffice u otros tipos de tablas, gráficos y otras utilidades.

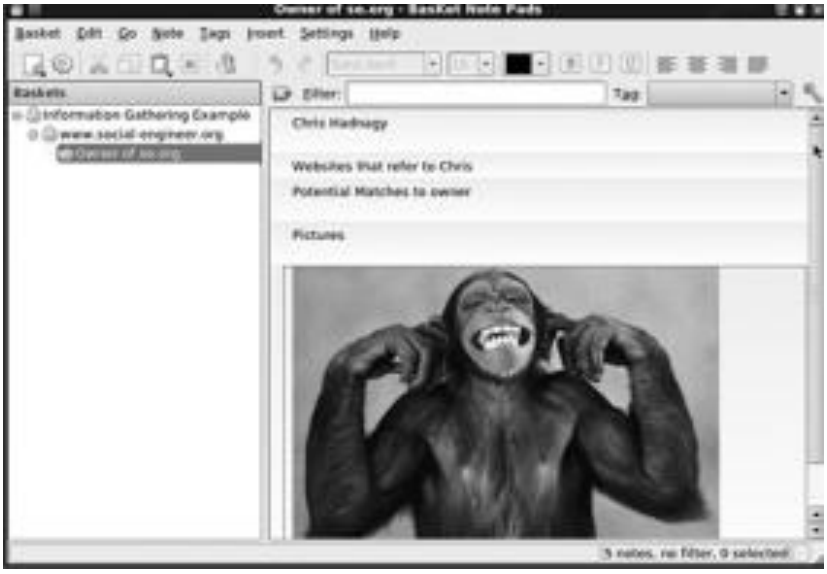


Figura 2-1: BasKet permite una fácil organización de los datos encontrados durante la recopilación de información.

Agregar una captura de pantalla se puede hacer de varias maneras. Lo más fácil es copiar la imagen y luego hacer clic con el botón derecho en la nueva Cesta y hacer clic en Pegar. Como se muestra en la Figura 2-1, agregar imágenes es simple pero también muestra la imagen de inmediato. Las notas se pueden escribir o pegar alrededor de las imágenes simplemente haciendo clic en la Cesta y comenzando a escribir.

En una auditoría de seguridad normal, lo que hace atractivo a BasKet es la forma en que cataloga los datos y los muestra en la pantalla. Por lo general, agregué una Cesta diferente para cada tipo de datos, como Whois, redes sociales, etc.Después de eso, haré un poco de reconocimiento utilizando Google Maps o Google Earth para capturar algunas imágenes del edificio o las instalaciones del cliente, que también puedo almacenar en BasKet. Cuando se completa la auditoría, es muy fácil poder extraer y utilizar esta información rápidamente. La Figura 2-2 ilustra un BasKet casi completo que contiene mucha información y pestañas útiles.

Como se muestra en la Figura 2-2, BasKet es fácil de almacenar la información en un formato fácil de leer. Intento incluir la mayor cantidad de información posible porque ninguna información es demasiado pequeña para almacenar. La información que incluyo es Los artículos del sitio web del cliente, la información de WhoIs, los sitios de redes sociales, las imágenes, la información de contacto de los empleados, los currículos encontrados, los foros, los pasatiempos y cualquier otra cosa que encuentre vinculada a la compañía.

Figura 2-2: BasKet completamente completado con mucha información útil.

Cuando termine, simplemente hago clic en el menú llamado Cesta, luego Exportar y exportar todo el BasKet como una página HTML. Esto es genial para informar o compartir esta información.

Para un ingeniero social, recopilar datos, como se explicará en detalle más adelante, es el punto crucial de cada concierto, pero si no puede recordar y utilizar los datos rápidamente, se vuelve inútil. Una herramienta como BasKet facilita la retención y el uso de datos. Si le das una oportunidad a BasKet y la usas una vez, estarás enganchado.

Usando dradis

Si bien BasKet es una gran herramienta, si realiza mucha recopilación de información o si trabaja en un equipo que necesita recopilar, almacenar y utilizar datos, entonces es importante contar con una herramienta que permita el uso compartido por múltiples usuarios de estos datos. Entra en Dradis. Según los creadores de la fuente abierta Dradis, el programa es un "aplicación web autónoma que proporciona un repositorio centralizado de información "que ha recopilado, y un medio por el cual planificar lo que se debe ven.

Al igual que BasKet, Dradis es una herramienta gratuita de código abierto que se puede encontrar en http://dradisframework.org/. Ya sea que esté utilizando Linux, Windows o una Mac, Dradis tiene instrucciones de configuración e instalación fáciles de usar que se encuentran en http://dradisframework.org/install.html.

Una vez que Dradis está instalado y configurado, simplemente navega hasta el host local y el puerto que asignó, o usa el estándar 3004. Puede hacerlo abriendo un navegador y escribiendo https: // localhost: 3004 /.

Una vez que haya iniciado sesión, será recibido con la pantalla que se muestra en la Figura 2-3. Observe el botón Añadir rama en la parte superior izquierda. Agregar una rama le permite agregar detalles similares a BasKet: notas, imágenes y más, e incluso puede importar notas.

Figura 2-3: Dradis tiene una interfaz agradable y fácil de usar.

Dradis y BasKet son solo dos herramientas que he utilizado para recopilar y almacenar

datos. Los sitios web de Dradis y BasKet tienen muy buenos tutoriales sobre la configuración y el uso de estas potentes herramientas.

Sea cual sea el sistema operativo que use, Mac, Windows o Linux, hay opciones disponibles para usted. Lo importante es usar una herramienta con la que se sienta cómodo y que pueda manejar grandes cantidades de datos.

Por esa razón, sugiero que se mantenga alejado de cosas como el Bloc de notas en Windows o Smultron o TextEdit en Mac. Quieres poder formatear y Resalta ciertas áreas para resaltarlas. En el servidor myDradis, que se muestra en la Figura 2-3, tengo una sección para los scripts del teléfono. Esta funcionalidad es útil para transcribir ideas que podrían funcionar según la información que reuní. Estas herramientas sugieren cómo un ingeniero social comienza a utilizar la información que recopila. La primera etapa en la utilización de la información que recopila es pensar como un ingeniero social.

Pensando como un ingeniero social

Tener unos cientos de megabytes de datos e imágenes es genial, pero cuando empiezas a revisarlos, ¿cómo te entrenas para revisar y luego pensar en los datos de una manera que tenga el máximo impacto?

Por supuesto, puede abrir un navegador y escribir búsquedas aleatorias que puedan llevar a algún tipo de información, algunas de las cuales pueden ser útiles. Si tienes hambre, probablemente no solo corres a la cocina y comiences a tirar los ingredientes que veas en un tazón y comiences a cavar. La planificación, la preparación y el

pensamiento hacen que la comida sea buena. Al igual que en una comida real, un ingeniero social necesita planificar, preparar y pensar qué información intentará obtener y cómo la obtendrá.

Cuando se trata de este paso vital de la recopilación de información, muchas personas tendrán que cambiar su forma de pensar. Tienes que acercarte al mundo de la información que tienes delante con una opinión y una mentalidad diferentes a las que tienes normalmente. Tienes que aprender a cuestionarlo todo y, cuando veas una parte de la información, aprendes a pensar en ello como lo haría un ingeniero social. La forma en que hace preguntas a la web u otras fuentes debe cambiar. La forma en que ve las respuestas que regresan también debe cambiar. Escuchar una conversación, leer lo que parece un mensaje de foro sin sentido, ver una bolsa de basura, debe asimilar esta información de una manera diferente a como lo hacía antes. Mi mentor, Mati, se emociona cuando ve que un programa falla.

¿Por qué? Porque es un probador de penetración y escritor de exploits. Acrash es el primer paso para encontrar una vulnerabilidad en el software, por lo que, en lugar de sentirse irritado por la pérdida de datos, se emociona con el accidente. El ingeniero social debe abordar la información de la misma manera. Cuando encuentre un objetivo que utilice muchos sitios de redes sociales diferentes, busque los enlaces entre ellos y la información que puede crear un perfil completo.

Como ejemplo, una vez alquilé un auto para conducir a unos pocos estados por negocios. Mi compañero y yo cargamos todo nuestro equipaje en el maletero; Cuando entramos al auto, notamos una pequeña bolsa de basura en el asiento trasero. La otra persona dijo algo como: “El servicio de hoy simplemente apesta. Calculas por lo que pagas, al menos limpiarían el auto.”

Es cierto que uno esperaría eso, Pero dejé esa bolsa de ser solo Me tiré a la lata más cercana y dije: “Déjame ver eso muy rápido”. Cuando abrí la bolsa y aparté las envolturas de Taco Bell, lo que estaba a la vista fue una sorpresa para mí, la mitad de un rasgado chequeo Rápidamente tiré la bolsa y encontré un recibo bancario y la otra mitad del cheque. El cheque se emitió por un par de miles de dólares, luego se rompió, no en pedazos pequeños, sino en cuatro trozos grandes, y luego se arrojó en una pequeña bolsa con un envoltorio de Taco Bell. Al volver a grabarlo, se reveló el nombre de esta persona, el nombre de la empresa, la dirección, el número de teléfono, el número de cuenta bancaria y el número de ruta del banco. Junto con el recibo bancario ahora tenía el saldo de su cuenta. Afortunadamente para él no soy una persona maliciosa porque solo se necesitan un par de pasos más para cometer el robo de identidad.

Esta historia personifica cómo las personas ven su valiosa información. Este arrastró el auto frente a mí y luego, como arrojó el cheque, sintió que se había ido, se deshizo de él de manera segura. O eso creía él; Pero este no es un caso aislado. En esta URL puede encontrar una historia reciente sobre cosas muy valiosas que la gente simplemente tiró o vendió por casi nada en una venta de garaje: www.social-engineer.org/wiki/archives/BlogPosts/LookWhatIFound.html.

Cosas como:

Descubriendo que un museo compró por $ 1.2 millones

1937 Bugatti Type 57Stalante con apenas 24,000 millas vendidas por $ 3 millónes ,Una copia de la declaración de independencia.

Si la gente tira un cuadro con una copia oculta de la Declaración de Independencia, entonces tirar las facturas, los registros médicos, las facturas antiguas o los estados de cuenta de las tarjetas de crédito probablemente no sea tan importante.

Cómo interactuar con la gente en público puede tener efectos devastadores. En el siguiente escenario, me pidieron que auditara una empresa y antes de poder continuar necesitaba reunir algunos datos. Eche un vistazo a cómo una información simple, aparentemente sin sentido, puede llevar a una violación.

Simplemente seguir a uno de los miembros más altos de la compañía objetivo durante un día o dos me mostró que se detenía a tomar un café todas las mañanas a la misma hora. Como era consciente de su parada de café a las 7:30

a.m. en la cafetería local, podía planear una “reunión”. Se sentaba durante 30 a 35 minutos, leía el periódico y tomaba un café latte mediano. Entro en la tienda alrededor de 3 a 5 minutos después de que se sienta. Pido la misma bebida que él y me siento a su lado en la tienda. Miro hacia arriba mientras coloca una sección del papel y pregunto si puedo leer el documento con el que ha terminado. Después de haber recogido un documento sobre la forma en que sabía que la página tres contenía un artículo sobre un reciente asesinato en el área. Después de actuar como si acabara de leerlo, digo en voz alta: “Incluso en estos pueblos pequeños las cosas dan miedo hoy en día. ¿Vives por aquí? Ahora, en este punto, el objetivo puede volarme, o si jugaba bien mis cartas, mi lenguaje corporal, mi tono vocal y mi apariencia lo tranquilizarán. Él dice: “Sí, me mudé hace unos años por un trabajo. Me gustan las ciudades pequeñas, pero escuchas esto cada vez más.”

Continúo, “Estoy viajando por la zona. Vendo servicios de consultoría de negocios de alta gama a grandes empresas y siempre disfruto viajar por ciudades más pequeñas, pero parece que escucho cada vez más estas historias incluso en las zonas rurales “. Luego, en tono muy burlón, digo:” No resulta que seas un gran pez gordo en una gran empresa que necesita una consulta, ¿verdad?”

Se ríe y luego, como si lo hubiera desafiado a demostrar su valía, dice: “Bueno, soy vicepresidente de finanzas en XYZ Corp. aquí localmente, pero no manejo ese departamento”.

“Oye, mira, no estoy tratando de venderte algo, solo disfruto del café, pero ¿si crees que puedo pasar y dejarte algo de información mañana o el miércoles?”

Aquí es donde la historia es interesante, como él dice: “Bueno, lo haría, pero voy a tomar unas muy necesarias vacaciones el miércoles. Pero, ¿por qué no me lo envías por correo y te llamo? “Luego me entrega una tarjeta.

“¿Iré a un lugar cálido y soleado, espero?” Le pregunto, sabiendo que probablemente me esté acercando al punto en el que necesito cortarlo.

“Llevar a la esposa en un crucero hacia el sur”. Puedo decir que no quiere decirme dónde, lo que está bien, por lo que nos damos la mano y nos separamos.

Ahora, ¿podría haberme estado espantando? Probablemente, pero tengo alguna información valiosa:

Su numero directo
Cuando se va de vacaciones
Que tipo de vacaciones

Que es local
El nombre de su compañia
Su título en su compañía
Que recientemente se reubicó

Por supuesto, parte de esta información que ya tenía de la recopilación de información anterior, pero pude agregar una cantidad sustancial después de esta reunión. Ahora, para lanzar la siguiente parte del ataque, llamo a su línea directa el día después de que se supone que se ha ido y pregunto por él, solo para que su recepcionista le diga: “Lo siento, Sr. Smith está de vacaciones, ¿puedo tomar un mensaje?

Excelente. La información está verificada y ahora todo lo que necesito hacer es lanzar el fase final, que significa vestirse con un traje y llevar mis tarjetas de visita de $ 9 a su oficina. Entro, me registro y le digo a la recepcionista que tengo una cita con el Sr. Smith a las 10:00 a.m. A lo que ella responde: “Está de vacaciones, ¿está seguro de que es hoy?” Usando mis sesiones de práctica en microexpresiones, un tema tratado en el Capítulo 5, muestro una verdadera sorpresa: “Espera, ¿su crucero fue esta semana? Pensé que se iba a ir la próxima semana “.

Ahora esta afirmación es vital, ¿por qué?

Quiero que la cita sea creíble y quiero que la recepcionista me confíe por poder. Al decir que conozco su crucero, esto debe significar el Sr. Smith

y he tenido una conversación íntima, lo suficiente como para conocer su itinerario. Pero mi impotencia provoca lástima y de inmediato la secretaria viene en mi ayuda. “Oh, cariño, lo siento, ¿quiero que llame a su asistente?”

“Ah, no.” Respondo. “Tenía muchas ganas de dejar algo de información con él. ¿Qué tal esto? Lo dejaré contigo y podrás dárselo cuando regrese. Estoy terriblemente avergonzado; ¿Tal vez puedas evitar incluso diciéndole que hice esto?

“Mis labios están sellados.”

“Gracias. Mira, me voy a fuera de aquí, pero antes de hacerlo, ¿puedo simplemente usar tu baño? “Sé que normalmente no me llamaría la atención, pero espero que la combinación de mi relación, mi impotencia y su compasión conduzcan a éxito, y lo hace.

Mientras estoy en el baño, coloco un sobre en un puesto. En la tapa del sobre pongo una pegatina que dice PRIVADO. Dentro del sobre “privado” hay una memoria USB con una carga maliciosa. Hago esto en un puesto y también en el pasillo junto a una sala de descanso para aumentar mis posibilidades y espero que la persona que encuentre a uno de ellos tenga la curiosidad de insertarlo en su computadora.

Efectivamente, este método parece funcionar siempre. Lo que da miedo es que este ataque probablemente no funcionaría si no fuera por una pequeña conversación inútil en una cafetería.

El punto no es solo sobre cómo los datos pequeños pueden llevar a una violación, pero También cómo recopila estos datos. Es importante comprender y probar las fuentes que puede utilizar para recopilar datos hasta que sea competente con cada método y cada fuente de recopilación. Hay muchos tipos diferentes de fuentes para recopilar datos. Un buen ingeniero social debe estar preparado para pasar un tiempo aprendiendo las fortalezas y debilidades de cada uno, así como la mejor manera de utilizar cada fuente. De ahí el tema de la siguiente sección.

Fuentes para la recopilación de información

Existen muchas fuentes diferentes para la recopilación de información. La siguiente lista no puede abarcar todas las fuentes, pero sí describe las principales opciones que tiene.

Recopilación de información de sitios web

Los sitios web corporativos y / o personales pueden proporcionar una gran cantidad de información. Lo primero que hará un buen ingeniero social es reunir la mayor cantidad de datos que pueda del sitio web de la empresa o de la persona. Pasar un poco de tiempo de calidad con el sitio puede llevar a una clara comprensión:

Lo que hacen
Los productos y servicios que brindan.
Ubicaciones fisicas
Ofertas de trabajo
Números de contacto
Biografías de los ejecutivos o junta directiva.
Foro de soporte
Convenciones de nombres de correo electrónico
Palabras o frases especiales que pueden ayudar en la creación de perfiles de contraseñas.

Ver los sitios web personales de las personas también es asombroso porque se vincularán con casi todos los detalles íntimos de sus vidas: niños, casas, trabajos y más. Esta información debe catalogarse en secciones porque a menudo será algo de esta lista que se usa en el ataque.

Muchas veces los empleados de la compañía serán parte de los mismos foros, listas de pasatiempos o sitios de redes sociales. Si encuentras un empleado en LinkedIn o Facebook, es probable que haya muchos más también. Tratar de recopilar toda esa información puede ayudar realmente a un ingeniero social a definir el perfil de la empresa y de los

empleados. Muchos empleados hablarán sobre su título de trabajo en sus redes sociales. Esto puede ayudar a un ingeniero social a determinar cuántas personas pueden estar en un departamento y cómo están estructurados los departamentos.

Los motores de búsqueda

Johnny Long escribió un famoso libro llamado Google Hacking for Penetration Testers y realmente abrió los ojos de muchas personas a la increíble cantidad de información que tiene Google.

Google perdona pero nunca olvida, y ha sido comparado con el Oráculo. Mientras sepa cómo preguntar, puede decirle casi todo lo que quiera saber. Johnny desarrolló una lista de lo que él llama "Google Dorks", o una cadena que se puede utilizar para buscar en Google para encontrar información sobre una compañía. Por ejemplo, si tuviera que escribir: site: microsoft.com filetype: pdf se le dará una lista de todos los archivos con la extensión de PDF que se encuentra en el dominio microsoft.com.

Estar familiarizado con los términos de búsqueda que pueden ayudarlo a localizar archivos en su objetivo es una parte muy importante de la recopilación de información. Hago el hábito de buscar filetype: pdf, filetype: doc, filetype: xls, y filetype: txt. También es una buena idea ver si los empleados realmente dejan archivos como DAT, CFG u otra base de datos o archivos de configuración abiertos en sus servidores para ser cosechados.

Libros completos están dedicados al tema de usar Google para encontrar datos, pero lo más importante que debe recordar es aprender sobre los operandos de Google que lo ayudarán a desarrollar los suyos.

Un sitio web como www.googleguide.com/advanced_operators.html tiene una lista muy buena de los operandos y cómo usarlos.

Google no es el único motor de búsqueda que revela información sorprendente. Un investigador llamado John Matherly creó un motor de búsqueda al que llamó Shodan (www.shodanhq.com).

Shodan es único porque busca servidores, enrutadores, software específico y mucho más en la red. Por ejemplo, una búsqueda de microsoft-iis os: "windows 2003" revela la siguiente cantidad de servidores que ejecutan Windows 2003 con Microsoft IIS:

Estados Unidos 59,140
China 5,361
Canada 4,424
Reino Unido 3,406
Taiwan 3,027

Esta búsqueda no es específica de un objetivo, pero demuestra una lección vital: la web contiene una increíble cantidad de información que necesita un ingeniero social que busca ser competente en la recopilación de información.

Reconocimiento Whois

Whois es un nombre para un servicio y una base de datos. Las bases de datos de Whois contienen una Gran cantidad de información que, en algunos casos, incluso puede contener información de contacto completa de los administradores del sitio web.

El uso de un indicador de comando de Linux o el uso de un sitio web como www.whois.net pueden llevarle a resultados sorprendentemente específicos, como la dirección de correo electrónico de una persona, el número de teléfono o incluso la dirección IP del servidor DNS.

La información de Whois puede ser muy útil para perfilar una empresa y conocer detalles sobre sus servidores. Toda esta información puede ser utilizada para más información.

Recopilación de información o para lanzar ataques de ingeniería social.

Servidores publicos

Los servidores de acceso público de una empresa también son excelentes fuentes de información para lo que no dicen sus sitios web. La toma de huellas dactilares de un servidor para su sistema operativo, aplicaciones instaladas e información de IP puede decir mucho sobre la infraestructura de una empresa. Después de determinar la plataforma y las aplicaciones en uso, puede combinar estos datos con una búsqueda en el nombre de dominio corporativo para encontrar entradas en los foros de soporte público.

Las direcciones IP pueden indicarle si los servidores están alojados localmente o con un proveedor; Con los registros DNS puede determinar los nombres y las funciones del servidor, así como las direcciones IP.

En una auditoría después de buscar en la web usando la herramienta llamada Matelgo (que se analiza en el Capítulo 7), pude descubrir un servidor público que alojaba literalmente cientos de documentos con piezas clave de información sobre proyectos, clientes y los creadores de esos documentos. Esta información fue devastadora para la empresa.

Una nota importante a tener en cuenta es que al realizar una exploración de puertos (el uso de una herramienta como NMAP u otro escáner para ubicar puertos abiertos, software y sistemas operativos utilizados en un servidor público) puede ocasionar problemas con la ley en algunas áreas.

Por ejemplo, en junio de 2003, un israelí, Avi Mizrahi, fue acusado por la policía israelí del delito de intentar el acceso no autorizado de material informatico Había escaneado el puerto del sitio web del Mossad. Unos ocho meses después, fue absuelto de todos los cargos. El juez incluso dictaminó que este tipo de acciones no deben desalentarse cuando se realizan de manera positiva (www.law.co.il/media/computer-law/mizrachi_en.pdf).

En diciembre de 1999, Scott Moulton fue arrestado por el FBI y acusado de intento de intrusión informática por la Ley de Protección de Sistemas Informáticos de Georgia y la Ley de América contra el Fraude y el Abuso informático. En ese momento, su compañía de servicios de TI tenía un contrato en curso con el condado de Cherokee de Georgia para mantener y mejorar la seguridad del centro 911 (www.securityfocus.com / noticias / 126).

Como parte de su trabajo, Moulton realizó varios escaneos de puertos en servidores del condado de Cherokee para verificar su seguridad y eventualmente escaneó un servidor web monitoreado por otra compañía de TI. Esto provocó una demanda, aunque fue absuelto en 2000. El juez dictaminó que no se produjo ningún daño que pudiera afectar la integridad y la disponibilidad de la red.

En 2007 y 2008, Inglaterra, Francia y Alemania aprobaron leyes que hacen ilegal la creación, distribución y posesión de materiales que permiten que alguien infrinja cualquier ley informática. Escáneres de puerto caen bajo esta descripción.

Por supuesto, si está involucrado en una auditoría pagada de una empresa, la mayor parte de esto estará en el contrato, pero es importante afirmar que depende del auditor de ingeniería social conocer las leyes locales y asegurarse de que no está infringiendo

Medios de comunicación social

Muchas empresas han llegado recientemente a las redes sociales. El marketing barato afecta a un gran número de clientes potenciales. También es otro flujo de información de una compañía que puede proporcionar una gran cantidad de información viable. Las compañías publican noticias sobre eventos, nuevos productos, comunicados de prensa e historias que pueden relacionarlos con los eventos actuales.

Últimamente, las redes sociales han tomado una opinión propia. Cuando uno se vuelve exitoso, parece que aparecen algunos más que utilizan tecnología similar. Con sitios como Twitter, Blippy, PleaseRobMe, ICanStalkU

En Facebook, LinkedIn, MySpace y otros, puede encontrar información sobre las vidas de las personas y su paradero en el sitio abierto. Más adelante, este libro tratará este tema con mucha más profundidad y verás que las redes sociales son increíbles fuentes de información.

Sitios de usuario, blogs, etc.

Los sitios de usuarios como blogs, wikis y videos en línea pueden proporcionar no solo información sobre la compañía objetivo, sino que también ofrecen una conexión más personal a través de los usuarios que publican el contenido. Los empleados contrariedades que escriben en su blog sobre los problemas de su compañía pueden ser susceptibles de ser escuchados por alguien con opiniones o problemas similares. De cualquier manera, los usuarios siempre están publicando grandes cantidades de datos en la web para que cualquiera pueda verlos y leerlos.

Caso en cuestión: eche un vistazo a un nuevo sitio que ha aparecido: www.icanstalku.com (consulte la Figura 2-4). Contrariamente a su nombre, no alienta a las personas a acechar a los demás. Este sitio apunta a la completa desconsideración de muchos usuarios de Twitter. Raspa el sitio de Twitter y busca usuarios que sean lo suficientemente tontos como para publicar fotos con sus teléfonos inteligentes. Muchas personas no se dan cuenta de que la mayoría de los teléfonos inteligentes incorporan datos de ubicación GPS en sus fotos. Cuando un usuario publica una imagen en la web con estos datos incrustados, puede llevar a una persona directamente a su ubicación.

Mostrar información basada en la ubicación es un aspecto aterrador de los sitios web de redes sociales. No solo le permiten publicar fotos suyas, sino que también revelan implícitamente su ubicación, posiblemente sin su conocimiento.

Sitios como ICanStalkU subrayan el peligro de esta información. Echa un vistazo a una historia (una de muchas) que muestra cómo se usan estos datos para robos en casa, robos y, a veces, más en www.social engineer.org/wiki/archives/BlogPosts/TwitterHomeRobbery.html.

Este tipo de información le puede dar un perfil muy detallado de su objetivo. A la gente le encanta twittear sobre dónde están, qué están haciendo y con quién están. Blippy permite que una persona conecte sus cuentas bancarias y, en esencia, “twittea” con cada compra, de dónde era y cuánto cuesta. Con imágenes que incluyen datos de ubicación incrustados y luego sitios como

Facebook, que muchos utilizan para poner fotos personales, historias y otra información relacionada, es el sueño de un ingeniero social. En poco tiempo, se puede desarrollar un perfil completo con la dirección, trabajo, fotos, pasatiempos y más de una persona.

Otro aspecto de los sitios de redes sociales que los convierte en excelentes fuentes de recopilación de información es la capacidad de ser anónimos. Si el objetivo es un hombre de mediana edad recientemente divorciado que ama su página de Facebook, puede ser una mujer joven que está buscando un nuevo amigo. Muchas veces, mientras coquetean, las personas divulgan información valiosa. Combine la capacidad de ser cualquier persona o cualquier cosa que desee en la web con el hecho de que la mayoría de las personas creen que todo lo que leen como hechos evangélicos y lo que tiene es uno de los mayores riesgos para la seguridad.

Figura 2-4: Escena atípica en la página de inicio de ICanStalkU.com.

Informes públicos

Los datos públicos pueden ser generados por entidades dentro y fuera de la empresa objetivo. Estos datos pueden consistir en informes trimestrales, informes gubernamentales, informes de analistas, ganancias publicadas para empresas que cotizan en bolsa, etc. Un ejemplo de esto son los informes de Dunn y Bradstreet u otros informes de ventas que se venden por muy poco dinero y contienen muchos detalles sobre el objetivo empresa.

Otra vía discutida con más detalle más adelante es usar verificadores de antecedentes como los que se encuentran en www.USSearch.com y www.intelius.com. Estos sitios, junto con muchos otros, pueden ofrecer servicios de verificación de antecedentes por tan solo $ 1 por un informe limitado a una tarifa de $ 49 por mes que le permite ejecutar tantos cheques como desee. Puede obtener gran parte de esta información de forma gratuita mediante los motores de búsqueda, pero algunos de los datos financieros detallados y la información personal solo pueden obtenerse de manera fácil y legal a través de un servicio pagado. Quizás lo más sorprendente es que muchas de estas compañías incluso pueden proporcionar datos como el Número de Seguro Social de una persona a algunos clientes.

Usando el poder de la observación

Aunque no se usa lo suficiente como herramienta de ingeniería social, la simple observación puede decirle mucho sobre su objetivo. ¿Los empleados del objetivo usan llaves, tarjetas RFID u otros métodos para ingresar al edificio? ¿Hay un área designada para fumar? ¿Los contenedores de basura están cerrados y el edificio tiene cámaras externas? Los dispositivos externos, como las fuentes de alimentación o las unidades de aire acondicionado, generalmente revelan quién es la empresa de servicios, y eso puede permitir que el ingeniero social acceda a otro vector.

Estas son solo algunas de las preguntas para las que puede obtener respuestas a través de la observación. Tomarse un tiempo para ver el objetivo, filmar usando una cámara oculta y luego estudiar y analizar la información más adelante puede enseñarle mucho y darle un gran impulso a su archivo de información.

Pasando por la basura

Sí, por más difícil que sea imaginar disfrutar saltando a través de la basura, puede generar uno de los beneficios más lucrativos para la recopilación de información. Las personas a menudo desechan facturas, avisos, cartas, CD, computadoras, llaves USB y una gran cantidad de otros dispositivos e informes que pueden proporcionar una cantidad asombrosa de información. Como se mencionó anteriormente, si las personas están dispuestas a

deshacerse del arte que vale millones, las cosas que ven como basura a menudo se quedan sin pensarlo dos veces, directamente en la basura.

A veces, las empresas destruyen documentos que consideran demasiado importantes para tirar, pero usan una trituradora ineficiente que hace que el papel sea demasiado fácil de armar, como se muestra en la Figura 2-5.

Figura 2-5: Las palabras de una sola vía grandes dejan algunas palabras aún legibles.

Esta imagen muestra algunos documentos después de la destrucción, pero aún se pueden distinguir algunas palabras completas.

poco tiempo y paciencia y algo de cinta, como se ve en la Figura 2-6. Los documentos que pueden ser incluso parcialmente grabados juntos pueden revelar información muy devastadora.

Figura 2-6: volver a armar los documentos solo requiere tiempo y paciencia. Sin embargo, el uso de una trituradora que destruye ambas direcciones en un lío fino y picado hace que volver a pegar los documentos sea casi imposible, como se muestra en la Figura 2-7.

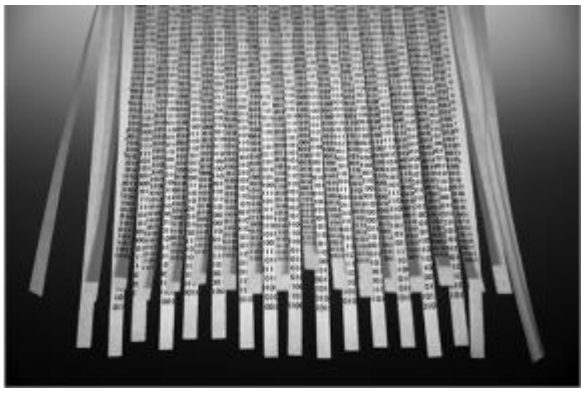


Figura 2-7: Casi no se puede decir que alguna vez fue dinero. Muchas compañías usan servicios comerciales que quitan sus documentos triturados para la incineración. Algunas compañías incluso dejan la trituración a un tercero, lo que, como probablemente haya adivinado, los

deja abiertos a otro vector de ataque. Un ingeniero social que averigua el nombre de su proveedor para esto puede imitar fácilmente a la persona que lo recoge y entregarle todos sus documentos. Sin embargo, Dumpster Diving puede ofrecer una forma rápida de encontrar toda la información que desee. Recuerde algunos puntos clave al realizar una inmersión en un contenedor de basura:

Use buenos zapatos o botas: nada arruinará su día más rápido que Saltar en un basurero y tener un clavo atravesado a tu pie. Asegúrese de que sus zapatos se ajusten bien y ajustados, además de ofrecer protección contra objetos afilados. Use ropa oscura: esto no necesita mucha explicación. Usted Probablemente desee usar ropa que no le importe tener que deshacerse de, Ropa oscura para evitar ser detectado.

Traer una linterna

Agarra y corre: a menos que estés en un área tan aislada que tengas no hay posibilidad de ser atrapado, agarrar algunas bolsas e ir En otro lugar, para hurgar en ellos podría ser mejor. Bucear en el basurero casi siempre conduce a información muy útil. En ocasiones, un ingeniero social ni siquiera tiene que sumergirse en un basurero para los bienes. Ya mencionado en el Capítulo 1 es el artículo que se encuentra en ww.social-engineer.org/resources/book/TopSecretStolen.htm, pero difiere este pensamiento. La CTU canadiense (Unidad de lucha contra el terrorismo) tenía ans de un nuevo edificio que describía sus cámaras de seguridad, cercas y otros

- Artículos secretos. Estos planos simplemente se tiraron, sí, solo tiraron la basura, ni siquiera fueron triturados, y afortunadamente fueron encontrados por una persona amigable.

Esta historia es solo una de las muchas que muestran “la altura de la estupidez”, como lo dijo la clave, pero desde el punto de vista de un ingeniero social, el buceo con basura es uno de mejores herramientas de recopilación de información que hay.

Uso de software de perfiles

El Capítulo 7 analiza las herramientas que conforman algunos de los conjuntos de herramientas profesionales de ingenieros sociales, pero esta sección ofrece una descripción general rápida.

Los perfiladores de contraseñas, como Common User Passwords Profiler (CUPP) y Who's Your Daddy (WYD), pueden ayudar a un ingeniero social a perfilar las posibles contraseñas que una empresa o persona puede usar.

El uso de estas herramientas se explica en el Capítulo 7, pero una herramienta como WYD raspará el sitio web de una persona o compañía y creará una lista de contraseñas de las palabras mencionadas en ese sitio. No es raro que las personas usen palabras, nombres o fechas como contraseñas. Estos tipos de software facilitan la creación de listas para probar.

Herramientas asombrosas como Maltego (ver Capítulo 7 para más detalles), hechas por Paterva, son el sueño de un recolector de información. Maltego le permite a un ingeniero social realizar muchas búsquedas de información pasiva y basada en la web sin tener que usar ninguna utilidad, sino Maltego en sí.

Luego almacenará y graficará estos datos en la pantalla para usarlos en informes, exportaciones u otros fines. Esto realmente puede ayudar en el desarrollo de un perfil en una empresa.

Recuerde, su objetivo al recopilar datos es conocer la empresa objetivo y las personas dentro de la empresa. Una vez que un ingeniero social recopila datos suficientes, se formará una imagen clara en sus mentes sobre la mejor manera de manipular los datos de los objetivos. Desea hacer un perfil de la compañía como un todo y descubrir de forma aproximada cómo muchos empleados forman parte de algún club, un pasatiempo o grupo. ¿Están comprometidos con una determinada organización o sus hijos van a la misma escuela? Toda esta información es muy útil para desarrollar un perfil.

Un perfil claro puede ayudar al ingeniero social no solo a desarrollar un buen pretexto, sino también a delinear qué preguntas usar, qué días buenos o malos llamar o cómo llegar, así como muchas otras pistas que pueden hacer el trabajo mucho más fácil.

Todos los métodos discutidos hasta ahora son en su mayoría métodos físicos y muy personales de recopilación de información. No toqué el lado muy técnico de la recopilación de información, como servicios como SMTP, DNS, Netbios y el todopoderoso SNMP. Cubro algunos de los aspectos más técnicos con los que Maltego puede ayudar en el Capítulo 7 con más detalle. Vale la pena estudiar estos métodos, pero son de naturaleza muy técnica, en lugar de ser más "humanos".

Cualquiera que sea el método que utilice para recopilar información de manera lógica, la pregunta que puede surgir ahora es que usted sabe dónde recopilar, cómo recopilar, e incluso cómo catalogar, almacenar y mostrar esta información. ¿Qué hace con eso?

Como ingeniero social, después de tener información, debe comenzar a planificar sus ataques. Para hacer eso necesitas comenzar a modelar un esquema que usará esta información. Una de las mejores maneras de comenzar a utilizar estos datos es desarrollar lo que se llama un modelo de comunicación.

Modelado de la comunicación

Cuanto más elaborados sean nuestros medios de comunicación, cuanto menos nosotros nos comunicamos.

comunicar.

- Joseph Priestley

La comunicación es un proceso de transferencia de información de una entidad a otra. La comunicación implica interacciones entre al menos dos agentes, y puede percibirse como un proceso de dos vías en el que hay un intercambio de información y una progresión de pensamientos, sentimientos o ideas hacia una meta o dirección mutuamente aceptada.

Este concepto es muy similar a la definición de ingeniería social, excepto que se supone que los involucrados en la comunicación ya tienen un objetivo común, mientras que el objetivo del ingeniero social es utilizar la comunicación para crear un objetivo común. La comunicación es un proceso por el cual la información se adjunta en un paquete y es canalizada e impartida por un remitente a un receptor a través de algún medio. El receptor luego decodifica el mensaje y le da retroalimentación al remitente. Todas las formas de comunicación requieren un remitente, un mensaje y un receptor. Comprender cómo funciona la comunicación es esencial para desarrollar un modelo de comunicación adecuado como ingeniero social. Modelar su comunicación como un ingeniero social nos ayudará a decidir el mejor método de entrega, el mejor método de retroalimentación y el mejor mensaje para incluir.

La comunicación puede tomar muchas formas diferentes. Existen medios auditivos, como el habla, la canción y el tono de voz, y existen medios no verbales, como el lenguaje corporal, el lenguaje de señas, el lenguaje, el lenguaje, el tacto y el contacto visual.

Independientemente del tipo de comunicación utilizada, el mensaje y la forma en que se entrega tendrán un efecto definido en el receptor.

Comprender las reglas básicas es esencial para construir un modelo para un objetivo. Algunas reglas no se pueden romper, como la comunicación siempre tiene un remitente y un receptor. Además, cada uno tiene diferentes realidades personales que están construidas y afectadas por sus experiencias pasadas y sus percepciones.

Todos perciben, experimentan e interpretan las cosas de manera diferente según estas realidades personales. Cualquier evento dado siempre será percibido de manera diferente por diferentes personas debido a este hecho. Si tienes hermanos, Un buen ejercicio para probar esto es pedirles su interpretación o memoria de un Evento, especialmente si es un evento emocional. Verás que su interpretación de este evento es muy diferente de lo que recuerdas.

Cada persona tiene un espacio personal tanto físico como mental. Usted permite o no permite que las personas ingresen a ese espacio o se acerquen a usted dependiendo de muchos factores. Cuando se comunica con una persona de cualquier manera, está intentando ingresar a su espacio personal.Cuando un ingeniero social se comunica, están tratando de traer a otra persona a su espacio y compartir esa realidad personal. La comunicación efectiva intenta llevar a todos los participantes a la ubicación mental de cada uno. Esto sucede con todas las interacciones, pero debido a que es muy común, la gente lo hace sin pensar en ello.

En las comunicaciones interpersonales se envían dos capas de mensajes: verbales y no verbales.

La comunicación generalmente contiene una parte verbal o de lenguaje, ya sea en palabras habladas, escritas o expresadas. Por lo general, también tiene una parte no verbal: expresiones faciales, lenguaje corporal o algún mensaje que no esté en el idioma, como emoticonos o fuentes.

Independientemente de la cantidad de cada tipo de señal (verbal o no verbal), este paquete de comunicación se envía al receptor y luego se filtra a través de su realidad personal. Ella formará un concepto basado en su realidad, luego, basándose en eso, comenzará a interpretar este paquete.A medida que el receptor descifra este mensaje, ella comienza a descifrar su significado, incluso si ese significado no es lo que pretendía el remitente. El remitente sabrá si su paquete se recibe de la forma que pretendía si el receptor entrega un paquete de comunicación a cambio de indicar su aceptación o rechazo del paquete original.

Aquí el paquete es la forma de comunicación: las palabras o letras o correos electrónicos enviados. Cuando el receptor recibe el mensaje, tiene que descifrarlo. Muchos factores dependen de cómo se interpreta. ¿Está de buen humor, mal humor, feliz, triste, enojada, compasiva? Todas estas cosas, así como las otras señales que alteran su percepción, la ayudarán a descifrar ese mensaje.

El objetivo del ingeniero social debe ser dar a las señales verbales y no verbales la ventaja de alterar la percepción del objetivo para que tenga el impacto que desea el ingeniero social.

Algunas reglas más básicas para la comunicación incluyen las siguientes:

Nunca des por sentado que el receptor tiene la misma realidad que usted.

Nunca des por sentado que el receptor interpretará el mensaje que Wayit estaba destinado.

La comunicación no es una cosa absoluta, finita.

Siempre asuma que existen tantas realidades diferentes como existen diferentes

Personas involucradas en la comunicación.

Conocer estas reglas puede mejorar enormemente la capacidad de comunicaciones buenas y útiles. Todo esto es bueno y excelente, pero ¿qué tiene que ver la comunicación con el desarrollo de un modelo? Más aún, ¿qué tiene que ver con la ingeniería social?

El modelo de comunicación y sus raíces.

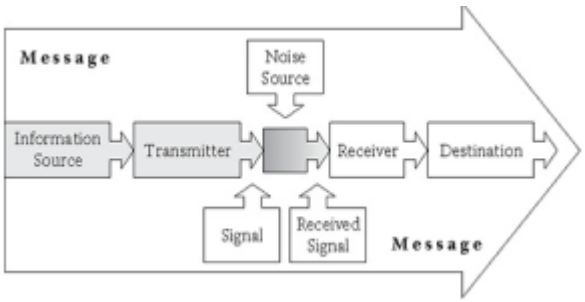
Como ya se ha establecido, la comunicación básicamente significa enviar un paquete de información a un receptor previsto. El mensaje puede provenir de muchas fuentes como la vista, el sonido, el tacto, el olfato y las palabras. Este paquete es procesado por el objetivo y se usa para dibujar una imagen general de "Lo que se dice."Este método de evaluación se denomina proceso de comunicación. Este proceso fue descrito originalmente por los científicos sociales Claude Shannon y Warren Weaver en 1947, cuando desarrollaron el modelo de Shannon-Weaver, también conocido como "la madre de todos los modelos"."

El modelo de Shannon-Weaver, según Wikipedia, "incorpora los conceptos de fuente de información, mensaje, transmisor, señal, canal, ruido, receptor, destino de la información, probabilidad de error, codificación, decodificación, velocidad de la información, [y] capacidad del canal, " entre otras cosas.

Shannon y Weaver definieron este modelo con un gráfico, como se muestra en la Figura 2-8.

En un modelo simple, también conocido como modelo de transmisión, la información o el contenido se envían de alguna forma desde un remitente a un destino o receptor. Este concepto común de comunicación simplemente considera la comunicación como un medio para enviar y recibir información. Las fortalezas de este modelo son su simplicidad, generalidad y cuantificabilidad.

Figura 2-8: La madre de todos los modelos de Shannon-Weaver." Shannon y Weaver estructuraron este modelo basándose en: Una fuente de información, que produce un mensaje. Transmisor, que codifica el mensaje en señales.



Achannel, al que se adaptan las señales para su transmisión. Un receptor, que "decodifica" (reconstruye) el mensaje de la Señal Un destino, donde llega el mensaje

Argumentaron que tres niveles de problemas para la comunicación existían dentro de esta teoría:

El problema técnico: ¿con qué precisión puede ser el mensaje? transmitido?

El problema semántico: ¿de qué manera precisamente se transmite el significado?

El problema de la efectividad: la eficacia con la que se recibe

¿El significado afecta el comportamiento? (Este último punto es importante recordar

para la ingeniería social. Todo el objetivo del ingeniero social es Crea un comportamiento que el ingeniero social quiera.)

Casi 15 años después, David Berlo amplió el modelo lineal de comunicación de Shannon y Weaver y creó el Canal de mensajes de remitente.Modelo de comunicación del receptor (SMCR). SMCR separó el modelo en partes claras, como se muestra en la Figura 2-9.

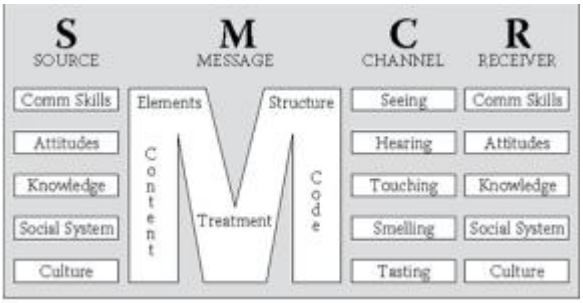


Figura 2-9: El modelo Berlo.Puede pensar en la comunicación como procesos de transmisión de información regidos por tres niveles de reglas:

Propiedades formales de los signos y símbolos.
Las relaciones entre signos / expresiones y sus usuarios.
Las relaciones entre signos y símbolos y lo que hacen. representar

Por lo tanto, puede refinar aún más la definición de comunicación como interacción social donde al menos dos agentes que interactúan comparten un conjunto común de signos y un conjunto común de reglas.

En 2008, otro investigador, D. C. Balmund, combinó la investigación de muchas de sus cohortes anteriores con la suya y desarrolló el modelo transaccional de comunicación, como se muestra en la Figura 2-10.

En este modelo, puede ver que el canal y el mensaje pueden tomar muchas formas, no solo habladas, como lo representa la imagen. El mensaje puede ser escrito, video, o forma de audio y el receptor puede ser una persona o

muchas personas. La retroalimentación también puede tomar muchas formas.

Combinar y analizar esta investigación puede ayudar a un ingeniero social a desarrollar un modelo de comunicación sólido. No solo los ingenieros sociales pueden beneficiarse de esto, todos pueden hacerlo. Aprender a desarrollar un plan de comunicación puede mejorar la forma en que trata con su cónyuge, sus hijos, su empleador o sus empleados, cualquier persona con la que se comunique.

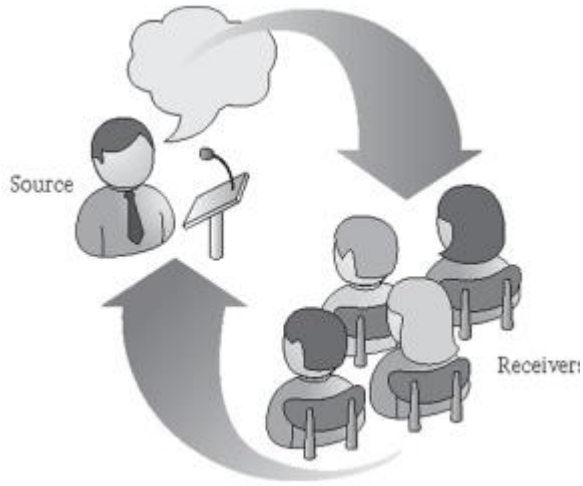


Figura 2-10: El nuevo y mejorado modelo de comunicación.

Debido a que el enfoque de este libro son los ingenieros sociales, es necesario analizar lo que un ingeniero social puede quitar de todo esto. Despues de leer todo esto

Teóricamente, puedes comenzar a preguntarte cómo se puede usar esto. Recuerda, un social El ingeniero debe ser un maestro en comunicación. Deben poder entrar y permanecer efectivamente en el espacio personal y mental de una persona y no ofender o apagar el objetivo. Desarrollar, implementar y practicar modelos de comunicación efectivos es la clave para lograr este objetivo. El siguiente paso entonces es desarrollar un modelo de comunicación.

Desarrollando un modelo de comunicación

Ahora que conoces los elementos clave de un modelo de comunicación, échales un vistazo desde los ojos de un ingeniero social:

La Fuente: El ingeniero social es la fuente de la información o Comunicación que va a ser retransmitida.
El Canal: Este es el método de entrega.
El Mensaje: Probablemente la mayor parte del mensaje es saber
Lo que vas a decir al (los) receptor (es).

El (los) receptor (es): este es el objetivo.

La retroalimentación: ¿Qué quieres que hagan después de dar efectivamente?

¿Cómo puedes usar estos elementos de manera efectiva? El primer paso en el mundo del modelado de la comunicación comienza con su objetivo. Intente trabajar con un par de escenarios que podrían ser parte de un concierto típico de ingeniería social:

Desarrolle un correo electrónico de phishing dirigido contra 25–50 empleados y tratar de que vayan durante las horas de trabajo a una empresa no comercial sitio web que se incrustará con código malicioso para piratear en su

redes Haga una visita al sitio para retratar a un entrevistado potencial que acaba de arruinó su currículum derramando café sobre él y necesita convencer al Persona de recepción para permitir que se inserte una llave USB en una computadora para imprimir una copia del currículum.

Al desarrollar una estrategia de comunicación, puede ser beneficioso trabajar en el modelo en orden inverso.

Feedback: ¿Cuál es tu respuesta deseada? La respuesta deseada es Para tener la mayoría de los empleados que envíe este correo electrónico haga clic en eso. Eso es ideal; por supuesto, puede estar contento con solo un puñado o incluso uno, pero el objetivo, la retroalimentación deseada, es hacer que la mayoría de los objetivos haga clic en el enlace de phishing.

Receptores: Aquí es donde sus habilidades de recopilación de información son útiles. Necesitas saber todo sobre los objetivos. ¿Les gustan los deportes? ¿Son predominantemente hombres o mujeres? ¿Son miembros de clubes locales? ¿Qué hacen en su tiempo libre? ¿Tienen familias? ¿Son mayores o menores? Las respuestas a estas preguntas pueden ayudar al ingeniero social a decidir qué tipo de mensaje enviar.

Mensaje: Si el objetivo es predominantemente de hombres de entre 25 y 40 años, y algunos son parte de una liga de fútbol o baloncesto de fantasía, sus objetivos pueden hacer clic en un enlace sobre deportes, mujeres o un evento deportivo. Desarrollar el contenido del correo electrónico es esencial, pero también es muy importante tener en cuenta la gramática, la ortografía y la puntuación. Una de las mayores sugerencias de correos electrónicos de phishing en el pasado ha sido la mala ortografía.

Recibiendo un correo electrónico que dice así: “Haga clic aquí e ingrese su contraseña para configuración de la cuenta del verificador “, es un regalo para que no sea legítimo correo electrónico. Su correo electrónico debe ser legítimo con una buena ortografía y una oferta atractiva que se ajusta al objetivo. Incluso con el mismo objetivo el mensaje cambiará.

Dependiendo del género, la edad y muchos otros factores. El mismo email probablemente fallaría si los objetivos fueran predominantemente femeninos.

Canal: esta respuesta a este elemento es fácil, porque ya Sé que va a ser un correo electrónico.

Fuente: Nuevamente, este elemento es una obviedad, porque usted, el social ingeniero, son la fuente. Qué tan creíble eres depende de tu Nivel de habilidad como ingeniero social.

Escenario uno: correo electrónico de phishing

Los objetivos son 45 varones que van desde la edad de 25 a 45. De los 45 objetivos, 24 están en la misma liga de baloncesto de fantasía. Todos van diariamente a un sitio (www.myfantasybasketballleague.com) para registrar sus selecciones. Esto es verificado por postposts en los foros.

El objetivo es llevarlos a un sitio que esté disponible y que usted ahora posee, www.myfantasybasketballeague.com, que es un pequeño error ortográfico. Este sitio es un clon del sitio que visitan con un solo cambio: tiene un iframe incrustado. Habrá un botón de inicio de sesión en el centro de la página que, al hacer clic, los devolverá al sitio real. La demora en cargar y hacer clic dará al código el tiempo que necesita para hackear sus sistemas.

¿Cómo escribirías el correo electrónico? Aquí hay una muestra que escribí:

Hola, Tenemos algunas noticias emocionantes en My Fantasy Basket Ball League. Nosotros Se han agregado algunas características adicionales que le permitirán un mayor control. sobre sus selecciones, así como algunas características especiales. Estamos trabajando duro en ofrecer esto a todos nuestros miembros, pero algunas tarifas de servicio adicionales puede solicitar.

Nos complace decir que las primeras 100 personas que inicien sesión obtendrán esta nueva Servicio gratuito. Haga clic en este enlace para ir a la página especial, haga clic en botón gris INICIAR SESIÓN en la página e iniciar sesión para que se agreguen estas funciones a tu cuenta. www.myfantasybasketballeague.com

Gracias,

El equipo de MFBB

Lo más probable es que este correo electrónico reciba al menos a los 24 que ya están en el interés lo suficientemente interesados como para hacer clic en el enlace, visitar el sitio y probar estas nuevas funciones de forma gratuita.

Analizar ese correo electrónico. Primero, contiene una oferta que atraería a los miembros actuales de esa liga de fantasía. Muchos de ellos se dan cuenta de que la oferta está limitada solo a los primeros 100, por lo que la harían clic en el momento en que reciban el correo electrónico, lo que probablemente está en el trabajo. El sitio al que los llevan los correos electrónicos tiene un código malicioso y, aunque la mayoría será víctima, todas las necesidades del ingeniero social malicioso son una sola víctima.

También tenga en cuenta que el correo electrónico contiene buena gramática y ortografía, un gancho atractivo y suficiente motivación para hacer clic rápidamente. Es un correo electrónico perfecto basado en un modelo de comunicación sólido.

Escenario Dos: USBKey

El escenario en el sitio es un poco más difícil de hacer porque es en persona. Solo puede hacer mucho para "falsificar" su identidad en persona. En este escenario, recuerde que debe tener todos estos detalles en la memoria porque no puede sacar y usar las tarjetas de referencia. También es importante recordar que muchas veces solo tenemos una oportunidad de impresionarnos. Si hacemos un mal trabajo, puede arruinar el resto del concierto.

Comentarios: el objetivo con este escenario es conseguir la atencion del recepcionista para aceptar su unidad USB que tiene un programa malicioso en eso. El programa cargará automáticamente y raspará su sistema para todos.

información, como nombres de usuario, contraseñas, cuentas de correo electrónico, SAM archivos que contienen todas las contraseñas en el sistema, y más, copiando todo a un directorio en la unidad USB. También crea un revés. conexión de la máquina de la recepcionista a sus servidores, dando Usted accede a su máquina y con suerte a la red. soy aficionado de utilizando el marco Metasploit o el kit de herramientas de ingeniería social

(Ver Capítulo 7) que se relaciona con Metasploit. Metasploit ejecuta explotar el código en sus víctimas y tiene un controlador incorporado llamado Meterpreter. El usuario puede escribir muchas cosas como el registro de teclas,

Capturas de pantalla, y reconocimiento desde las máquinas de la víctima.

Receptores: tener un objetivo verdadero puede ser complicado, ya que si su objetivo no es receptivo a la idea, su plan se dispara. Debes ser cálido, amable y convincente. Esto también debe hacerse rápido, porque demasiado tiempo permitirá que surja la duda. Pero si te mueves demasiado rápido, puedes causar dudas y miedo, matando tus posibilidades. Un equilibrio perfecto debe ser logrado.

Mensaje: Debido a que está entregando el mensaje en persona, debe ser claro y conciso. La historia básica es que vio el anuncio en el documento para un administrador de base de datos y llamó y habló con Debbie, la persona de recursos humanos. Ella dijo que estaba reservada hoy, pero debes parar y dejar un currículum para su revisión y luego reunirte con ella al final de la semana. Mientras conducías, una ardilla salió corriendo, lo que provocó que pisaras los frenos y que tu café saliera del soporte y se derramara en tu bolsa. arruinando tu currículum y otras cosas. De todos modos, tienes otra cita pero de verdad necesita este trabajo y pregúntese si ella le imprimirá una copia nueva desde su unidad USB.

Canal: Vas en persona usando verbal, facial y corporal. comunicación lingüística.

Fuente: De nuevo, este es usted como ingeniero social

Sostener una carpeta manchada de café con algunos papeles mojados puede ayudar a la historia. Mirar abatido y no alfa-masculino también puede ayudar a venderlo. Hablar de manera educada con ella y no usar lenguaje grosero la ayudará a sentir una simpatía por ti y tal vez incluso algo de pena. La llave USB debe contener un archivo llamado myresume.doc o myresume.pdf y ser imprimible. Los PDF son los formatos más utilizados, ya que la mayoría de las empresas utilizan una versión anterior de Adobe Reader que es vulnerable a muchas vulnerabilidades diferentes. Asegúrese de que el currículum esté en un formato que permita que la mayoría de las personas puedan abrirlo, no un formato extraño. La mayoría de las veces la gente quiere ayudar. Quieren poder ayudar a un Persona en apuros si la historia es creíble, así como desgarradora. Para un giro especial si realmente carece de corazón como ingeniero social, puede Dale un giro a la historia: de camino, hoy me toca a mí dejar caer mi hija fuera en la escuela Cuando ella se subió al asiento para darme un beso.

Adiós ella tiró mi café en mi bolsa. yo ya estaba llegando tarde y más cerca de aquí que de casa; me podrías imprimir un nuevo.

De cualquier manera, esta historia generalmente funciona y conducirá a que la llave USB se inserte en la computadora y, probablemente, a un compromiso completo de la computadora de la recepcionista, lo que puede llevar a un compromiso total de la compañía.

El poder de los modelos de comunicación

El modelado de la comunicación es una herramienta poderosa que es una habilidad imprescindible para el ingeniero socialista. La parte más difícil del modelado de la comunicación es asegúrese de que sus sesiones de recopilación de información sean sólidas.

En los dos escenarios anteriores, no contar con un plan y un modelo suficientemente buenos dará lugar al fracaso. Una buena manera de practicar el modelado de la comunicación es escribir un modelo para manipular a las personas que usted conoce bien (un esposo, esposa, padre, hijo, jefe o amigo) para hacer lo que quiera, para tomar las medidas que desee.

Establezca una meta, nada malicioso, como hacer que alguien acepte un lugar de vacaciones diferente o ir a un restaurante que ama y que su pareja odia, o que le permita gastar algo de dinero en algo que normalmente no pediría. Sea lo que sea lo que se te ocurra, escribe los cinco componentes de comunicación y luego observa qué tan bien funciona la comunicación cuando tienes un plan escrito. Encontrará que con sus objetivos claramente definidos, puede probar mejor sus métodos de comunicación de ingeniería social y ser capaz de alcanzar sus objetivos más fácilmente. Enumere los siguientes cinco puntos y rellénelos uno por uno, conectando los puntos a medida que avanza.

Fuente.
Mensaje
Canal
Receptores
Comentarios.

El modelado de la comunicación produce información muy valiosa y, sin ella, la mayoría de la comunicación no tendrá éxito para un ingeniero social. Como se mencionó anteriormente, la recopilación de información es el quid de todos los conciertos de ingeniería social, pero si se vuelve competente en la recopilación de información y puede recopilar grandes cantidades de datos pero no sabe cómo usarla, es un desperdicio.

Aprenda a convertirse en un maestro en la recopilación de información y luego practique poner eso en acción con un modelo de comunicación. Esto es solo el comienzo, pero puede cambiar literalmente la forma en que trata a las personas como ingeniero social y en los contextos cotidianos. Sin embargo, se necesita mucho más para desarrollar un mensaje sólido en el modelo de comunicación.

Un aspecto clave de aprender cómo comunicarse, cómo manipular y cómo ser un ingeniero social es aprender a usar preguntas. como se discutira en el proximo capitulo

Capítulo 3

Sonsacamiento

El arte supremo de la guerra es someter al enemigo sin luchar.

- Sun Tzu Ser capaz de atraer personas de manera efectiva es una habilidad que puede hacer o deshacer a un ingeniero social. Cuando las personas te ven y te hablan, deberían sentirse cómodos y querer abrirse.

¿Alguna vez has conocido a alguien y al instante sentiste, "Wow, me gusta esa persona"? ¿Por qué? ¿Qué fue lo que te hizo sentir de esa manera? ¿Fue su sonrisa? La forma en que miró? La forma en que te trató? ¿Su lenguaje corporal? Tal vez incluso parecía estar "en sintonía" con tus pensamientos y deseos. La forma en que te miraba no juzgaba y de inmediato te sentías cómodo con él. Ahora imagina que puedes aprovechar eso y dominar esa habilidad. No te desanimes

¿Qué es la elicitación?

Elicitación significa sacar o sacar, o llegar a una conclusión (la verdad, por ejemplo) mediante lógica. Alternativamente, se define como una estimulación que llama (o saca) una clase particular de conductas, como en "la provocación de Su testimonio no fue fácil."

Lea esa definición otra vez y si no le da la piel de gallina puede tener un problema. Piensa en lo que esto significa. Ser capaz de utilizar efectivamente la elicitación significa que puede formular preguntas que atraigan a las personas y las estimulen a tomar el camino que desee. Como ingeniero social, ¿qué significa esto? Ser eficaz en la obtención de información significa que puede modelar sus palabras y sus preguntas de manera que mejorará su nivel de habilidad a un nivel completamente nuevo. En términos de recopilación de información, la obtención de expertos puede traducirse en su objetivo de querer responder a todas sus preguntas.

Quiero llevar esta discusión un paso más allá porque muchos gobiernos educan y advierten a sus empleados contra elicitación porque se utilizan por todo el mundo.

En los materiales de capacitación, la Agencia de Seguridad Nacional del gobierno de los Estados Unidos define la obtención como "la extracción sutil de información durante una conversación aparentemente normal e inocente."

Estas conversaciones pueden ocurrir en cualquier lugar que sea el objetivo: un restaurante, el gimnasio, una guardería, en cualquier lugar. La elicitación funciona bien porque es de bajo riesgo y, a menudo, muy difícil de detectar. La mayoría de las veces, los objetivos nunca saben de dónde proviene la filtración de información. Incluso si existe la sospecha de que hay alguna mala intención, uno puede fácilmente pasarlo como un extraño enojado acusado de hacer el mal por solo hacer una pregunta.

La elicitación funciona muy bien por varias razones:

La mayoría de las personas tienen el deseo de ser educados, especialmente con los extraños.

Los profesionales quieren aparecer bien informados e inteligentes. Si lo elogian, a menudo hablará más y divulgará más.

La mayoría de la gente no mentiría por mentir.

La mayoría de las personas responden amablemente a las personas que parecen preocupadas por ellos.

Estos factores clave sobre la mayoría de los humanos son la razón por la cual la elicitación funciona tan bien. Lograr que las personas hablen sobre sus logros es demasiado fácil.

En un escenario en el que me encargaron recopilar información sobre una empresa, conocí a mytarget en una función de la cámara de comercio local. Como era un mezclador, me quedé atrás hasta que vi al objetivo acercarse a la barra. Llegamos al mismo tiempo y como el propósito de estas funciones es conocer y saludar a las personas e intercambiar tarjetas de visita, mi primer movimiento no fue extremo.

Yo dije: "¿Escapar de los buitres?"

Respondió con una risita: “Sí, esto es lo que hace que estas cosas valgan la pena: barra libre.”

Le escuché ordenar, y ordené una bebida similar. Me inclino con la mano extendida y dije: “Paul Williams”.

“LarrySmith”.

Saqué una tarjeta de visita que había ordenado en línea. “Trabajo con una pequeña empresa de importación como jefe de compras”.

Dijo mientras me entregaba su tarjeta: “Soy el director financiero de XYZ.”

Con una risita, respondí: “Tú eres el tipo con el dinero; por eso todos te buscan”. ¿Qué es exactamente lo que ustedes hacen?”

Él se refirió a algunos detalles de los productos de su compañía, y cuando mencionó uno que es bien conocido, dije: “Oh, sí, ustedes hacen ese widget; Me encanta esa cosa. Leí en la revista XYZ que llegó a un nuevo récord de ventas para ustedes “. De mi anterior recopilación de información supe que él tenía interés personal en ese dispositivo, por lo que acotacion fue bien recibida.

Suspiro profundo un poco. “¿Sabía que el dispositivo se vendió más en el primer mes que nuestros cinco productos anteriores y siguientes se combinaron?”

“Vaya, bueno, puedo ver por qué, porque yo mismo compré cinco”. Me reí entre dientes a través de los suaves elogios.

Después de otra bebida y un poco más de tiempo, pude descubrir que recientemente compraron un software de contabilidad, el nombre del CSO (y el hecho de que estuvo de vacaciones por unos días), y que mi amigo aquí también se iba de vacaciones pronto para Las Bahamas con su esposa.

Esta información aparentemente inútil no es inútil en absoluto. Tengo una lista de detalles sobre software, personas y vacaciones que me pueden ayudar a planear un ataque. Pero yo no quería parar allí; Fui a matar con una pregunta como esta:

“Sé que esta es una pregunta extraña, pero somos una pequeña empresa y mi jefe me dijo que debo investigar y comprar un sistema de seguridad para las puertas”. Ahora solo usamos las teclas, pero estaba pensando en RFID o algo así. ¿Sabes lo que ustedes usan?”

Esta pregunta que pensé enviaría bengalas rojas y señales de humo. En su lugar, dijo: “No tengo ni idea; Acabo de firmar los cheques para ello. Lo que sí sé es que tengo esta pequeña tarjeta de lujo ... “mientras saca su billetera para mostrarme su tarjeta. “Creo que es RFID, pero lo único que sé es que agito la billetera frente a la pequeña caja y la puerta se abre.”

Intercambiamos risas y me fui con el conocimiento que condujo a algunos vectores de ataque muy exitosos. Como habrá notado, la obtención es similar y está vinculada a la recopilación de información. Esta sesión particular de recopilación de información se hizo mucho más fácil con un pretexto sólido (discutido en el Capítulo 3), así como con buenas habilidades de obtención. Las habilidades de elicitación son las que hacen que las preguntas fluyan sin problemas y lo que hizo que el objetivo se sienta cómodo respondiendo las preguntas.

Sabiendo que estaba de vacaciones y qué tipo de software de contabilidad utilizaban, así como el sistema de seguridad de bloqueo de puertas, pude planificar una visita in situ para reparar una caja RFID y un reloj de tiempo “defectuosos”. Simplemente le dijo al recepcionista de la recepción: “Larry me llamó antes de irse a las Bahamas y dijo que había un reloj del departamento de manufactura que no se está registrando correctamente. Tardaré unos minutos en probarlo y analizarlo ”. Me dieron acceso en cuestión de segundos sin que me cuestionaran.

La obtención me llevó a ese éxito porque, con el conocimiento que me dieron, no había ninguna razón para que la recepcionista dudara de mi pretexto.

Una simple, liviana y aireada conversación es todo lo que se necesita para obtener la mejor información de muchas personas. Como se discutió hasta ahora, definir sus metas para lograr los máximos resultados es vital. La elicitación no es de uso ... Una conversación simple, ligera y espaciosa es todo lo que se necesita para obtener algunos de los mejores información de muchas personas. Como se discutió hasta ahora, definir sus metas para lograr los máximos resultados es vital. La elicitación no se usa meramente para recopilación de información, pero también puede usarse para solidificar su pretexto y obtener Acceso a la información. Todo esto depende de un modelo de elicitación

Los Objetivos de la Elicitación.

Revisar la definición de elicitación puede darle una ruta clara de cuáles son sus objetivos. Sin embargo, realmente puede reducirlo a una sola cosa. El ingeniero social desea que el objetivo realice una acción, ya sea que la acción sea tan simple como responder una pregunta o tan grande como permitir el acceso a un área restringida determinada. Para lograr que el objetivo cumpla, el ingeniero social hará una serie de preguntas o mantendrá una conversación que motivará al objetivo en ese camino.

La información es la clave. Cuanta más información recopile, más exitoso será el ataque. Debido a que la provocación no es amenazante es muy exitoso. Cuenta cuántas veces en una semana tienes pequeñas conversaciones sin sentido con alguien en una tienda, una cafetería o en otro lugar. Toda la metodología de mantener conversaciones está basada en elicitación y se utiliza de forma no maliciosa. Por eso es tan efectivo.

En un episodio del popular programa de televisión británico The Real Hustle, los anfitriones demostraron la facilidad de muchos ataques de ingeniería social. En este episodio, el objetivo era dibujar un objetivo en un juego de suerte que fue amañado. Para hacerlo, alguien tenía un compañero que actuaba como un extraño papel de playa al estar interesado y conversar con el atacante. Esta conversación atrae a las personas que la rodean, lo que hizo que las respuestas adecuadas del objetivo fueran muy fáciles. Este es un método que funciona bien.

Cualquiera que sea el método utilizado, el objetivo es obtener información y luego utilizar esa información para motivar a un objetivo en el camino que el ingeniero social quiere que tome. Comprender este hecho es importante. Los capítulos posteriores cubren el uso de pretextos y otras tácticas de manipulación, pero no debes confundir la provocación con esas. Es importante darse cuenta de que la provocación es una conversación. Claro, puede estar estrechamente relacionado con su pretexto, lenguaje corporal y señales visuales, pero todos ellos palidecen en comparación con su capacidad para entablar conversación con las personas.

Algunos expertos coinciden en que dominar el arte de la conversación tiene tres pasos principales:

1. Ser natural. Nada puede matar una conversación más rápido de lo que parece.

   Ser incómodo o antinatural en la conversación. Para ver esto por tú mismo prueba este ejercicio. Tener una conversación con alguien sobre algo de lo que sabes mucho. Si puede grabarlo de alguna manera o si alguien más lo nota, vea cómo se encuentra, su postura y la forma en que afirma su conocimiento. Todas estas cosas van a gritar confianza y naturalidad. Luego insértese en una conversación de la que no sepa nada y tenga la misma grabación u observación de amigos. Vea cómo todos esos aspectos no verbales cambian para usted cuando intenta inyectar un pensamiento inteligente en una conversación de la que no sabe nada.
   Este ejercicio te muestra la diferencia en ser natural y no ser natural. La (s) persona (s) con la que está conversando podrá verlo fácilmente, lo que eliminará todas las posibilidades de éxito en la obtención. ¿Cómo pareces natural en las conversaciones? Así llegamos al paso 2.

2. Edúcate a ti mismo. Debes tener conocimiento de qué es lo que hablarás con tus objetivos. Esta sección debe incluir una gran advertencia de luz roja de neón, pero como cada libro no puede incluir uno, permítame enfatizar esta parte:

   Es imperativo que no finjas que eres más de lo que razonablemente se puede creer que eres.
   ¿Confuso? Aquí hay un ejemplo para descomponerlo. Si quería obtener la composición química para un producto de alto secreto y su objetivo de obtención es uno de los químicos involucrados en la fabricación del producto, y

decide comenzar a hablar de química, no se haga el papel de químico de clase mundial (a menos que son). Él puede arrojarle algo que le mostrará que no sabe nada y luego su cubierta está perdida y también lo es la provocación. Un enfoque más realista puede ser que usted es un estudiante de investigación que estudia XYZ y se le dijo que tenía un conocimiento increíble en esta área. Debido a su experiencia, solo quería hacerle una pregunta sobre una fórmula química en la que está trabajando y por qué no parece estar funcionando.
El punto es que sea lo que sea que elija para conversar y con quien quiera, investigue, practique y esté preparado. Tenga conocimientos suficientes para hablar de forma inteligente sobre un tema que le interese al objetivo.

3. No seas codicioso. Por supuesto, el objetivo es obtener información, obtener respuestas y recibir la clave del reino. Todavía, no dejes que sea el atención. Que solo estás ahí para ti se hará evidente rápidamente y el objetivo perderá interés. A menudo, darle algo a alguien provocar el sentimiento de reciprocidad (discutido en el Capítulo 6), donde él o ella ahora se siente obligada a darle algo a cambio. Siendo asi En la conversación es importante. Haz que la conversación sea un dar y recibir, a menos que esté conversando con una persona que quiera dominar la

   conversacion. Si él quiere dominar, déjalo. Pero si consigues unos cuantos respuestas, siente la conversación y no seas codicioso tratando de ir Más y más profundo, lo que puede levantar una bandera roja.
   A veces las personas que están etiquetadas como los “mejores conversadores” en El mundo son aquellos que escuchan más que hablando.
   Estos tres pasos para lograr una obtención exitosa pueden, literalmente, cambiar la forma en que conversa con las personas diariamente, y no solo como ingeniero social o auditor de seguridad, sino como una persona común. Personalmente, me gusta agregar uno o dos pasos a los “tres primeros”.”
   Por ejemplo, un aspecto importante de la elicitación son las expresiones faciales durante una conversación. Tener una mirada demasiado intensa o demasiado relajada puede afectar la forma en que las personas reaccionan a sus preguntas. Si sus palabras son tranquilas y ha involucrado al objetivo en una conversación, pero su lenguaje corporal o sus expresiones faciales muestran desinterés, puede afectar el estado de ánimo de la persona, incluso si no se da cuenta.
   Esto puede parecer extraño de mencionar aquí, pero soy fanático de Cesar Milan, también conocido como The Dog Whisperer. Creo que ese tipo es un genio. Toma perros que parecen ingobernables y en cuestión de minutos los perros y sus dueños producen rasgos de personalidad de alta calidad que merecen una relación muy exitosa para ambos. Básicamente, enseña a las personas cómo comunicarse con un perro, cómo pedir y decirle que haga las cosas en un idioma que entienda. Una de las cosas que predica en las que creo plenamente es que el “espíritu” o energía de la persona afecta al “espíritu” o energía del perro. En otras palabras, si la persona se acerca al perro de manera tensa y ansiosa, incluso si las palabras son tranquilas, el perro actuará tenso, ladrará más y estará más nervioso.
   Obviamente, las personas no son lo mismo que los perros, pero realmente creo que esta filosofía se aplica. Cuando un ingeniero social se acerca a un objetivo, su “espíritu” o energía afectará la percepción de la persona. La energía se retrata a través de lenguaje corporal, expresiones faciales, vestimenta y aseo personal, y luego las palabras dichas para respaldar eso. Sin siquiera saberlo, la gente se da cuenta de estas cosas. ¿Alguna vez has pensado o escuchado a alguien decir: “Ese tipo me dio escalofríos” o “Ella se veía como una buena persona”?
   ¿Cómo funciona? El espíritu o la energía de la persona se transmite a sus “sensores”, esos datos se correlacionan con experiencias pasadas y luego se forma un juicio. La gente lo hace instantáneamente, muchas veces sin siquiera saberlo. Por lo tanto, su energía cuando vaya a obtener debe coincidir con el papel que desempeñará. Si tu personalidad o tu mentalidad no te permiten jugar fácilmente como manager, no lo intentes. Trabaja con lo que tienes. Personalmente, siempre he sido una persona de personas y mi fuerte no es temas como química o matemáticas avanzadas. Si estuviera en la situación mencionada anteriormente, no trataría de desempeñar el papel de una persona que conoce esas cosas. En cambio, mi provocación podría ser tan simple como un extraño interesado en iniciar una conversación sobre el clima.

Independientemente de los métodos que elija utilizar, puede seguir ciertos pasos para tener el borde superior. Uno de estos pasos se llama precarga.

Precarga

Usted está en la fila para comprar su boleto de $ 10 y está sobrecargado con una sobrecarga sensorial de carteles de las próximas películas. Te haces cola para comprar palomitas y bebidas por un valor de $ 40, ves más carteles y luego te abres camino para conseguir un asiento. Finalmente, cuando comienza la película, se le presenta una serie de clips sobre las próximas películas. A veces, estas películas aún no están en producción, pero el locutor se acerca y dice: "La película más divertida desde ..." o la música comienza con un tono ominoso, una niebla densa llena la pantalla y la voz en off suena ", pensaste. se acabó en la parte 45 de Teenage Killer ..."

Cualquiera que sea la película, los profesionales de marketing le están diciendo cómo sentirse (en otras palabras, cargando lo que debería estar pensando acerca de esta película) antes de que comience la vista previa. Luego, los cortos 1–3 minutos que tienen para mostrarte de qué se trata la película se gastan en mostrarte clips para atraer tu deseo de ver la película y atraer a la multitud que quiere la comedia, el horror o la historia de amor.

No se ha escrito mucho sobre la precarga, pero es un tema muy complejo. La precarga indica que puede hacer exactamente lo que dice: precargar los objetivos con información o ideas sobre cómo desea que reaccionen ante cierta información. La precarga se utiliza a menudo en los mensajes de marketing; por ejemplo, en los anuncios de la cadena nacional de restaurantes que muestran a personas hermosas riendo y disfrutando la comida que se ve tan hermosa y perfecta. Como dicen "yummm!" Y "ohhh!" Casi se puede probar la comida.

Por supuesto, como ingeniero social, no puede ejecutar un comercial para sus objetivos, ¿cómo puede usar la precarga?

Al igual que con mucho en el mundo de la ingeniería social, tienes que empezar desde los resultados finales y trabajar hacia atrás. ¿Cuál es tu objetivo? Es posible que tenga el objetivo estándar de obtener información sobre un proyecto en el que está trabajando o en las fechas en las que estará en la oficina o de vacaciones. Sea lo que sea, debe establecer el objetivo primero. A continuación, debe decidir el tipo de preguntas que desea formular y luego decidir qué tipo de información puede precargar a una persona para que quiera responder esas preguntas

Por ejemplo, si sabes que más tarde esta noche quieres ir a un lugar de carne que tu esposa amante de los cupones no disfruta realmente, pero estas de humor para una costilla, puedes precargarla para obtener una respuesta que quizás esté a tu favor. Tal vez al principio del día, puedes decir algo así como: "Cariño, ¿sabes de qué estoy de humor? Abig, jugoso, bistec a la plancha. El otro día iba conduciendo a la La oficina de correos y Fred en el camino tenían su parrilla afuera. Acababa de empezar a cocinar los filetes al carbón y el olor entró en la ventanilla del coche y Me ha estado persiguiendo desde entonces."Si esto provoca una respuesta en este El momento exacto no es importante; Lo que hiciste fue plantar una semilla que tocó todos imaginar a los filetes que chisporroteaban en la parrilla, hablaste acerca de verlos de nuevo, habló sobre oler el sumo y sobre cómo lo mucho que querías uno. Supongamos que luego te llevas el papel a casa y cuando lo estás repasando Verá un anuncio con un cupón para el restaurante al que desea ir. Simplemente dejas esa página doblada sobre la mesa.Una vez más, tal vez su esposa lo vea o tal vez ella no lo hace, pero lo más probable es que lo haya dejado con el correo, porque Usted mencionó el bistec, y como a ella le encantan los cupones, verá el cupón que queda en la mesa.

Ahora, más tarde, ella viene a ti y te dice: "¿Qué quieres para cenar esta noche?" Aquí es donde entra toda tu precarga: mencionaste el olor, la vista y el deseo de comer carne. Dejó un cupón fácil de encontrar en la mesa para el restaurante de carnes de su elección y ahora es el momento de la cena.

Responde con ella: "En lugar de cocinarte y tener un desastre para limpiar esta noche, no hemos estado en XYZ Steaks por un tiempo. ¿Qué pasa si acabamos de llegar a ese lugar esta noche?"

Sabiendo que a ella no le gusta ese lugar, todo lo que puede esperar es que la precarga esté funcionando. Ella responde: "Vi un cupón para ese lugar en el periódico. Tenía una comida buyone obtener una segunda mitad de descuento. Pero sabes que no me gusta ..."

Mientras habla, puedes saltar y alabar: "¡Ja! La reina del cupón ataca de nuevo. Demonios, sé que no te gusta demasiado el bistec, pero escuché de Sally que allí también tienen excelentes comidas con pollo."

Unos minutos más tarde estás en el camino para filmar el cielo. Mientras que un asalto frontal que indica que tu deseo de ir a XYZ probablemente se habría encontrado con un rotundo "¡No!", La precarga ayudó a que su mente aceptara tu opinión y funcionó.

Otro ejemplo realmente simplista antes de seguir adelante: una amiga se acerca y dice: "Tengo que contarte una historia realmente divertida". ¿Qué te sucede? Incluso puedes comenzar a sonreír antes de que comience la historia y tu anticipación es escuchar algo divertido, así que miras y esperas las oportunidades para reír. Te precargó y anticipaste el humor.

¿Cómo funcionan estos principios dentro del mundo de la ingeniería social?

La precarga es una habilidad en sí misma. Ser capaz de plantar ideas o pensamientos de una manera que no sea obvia o dominante a veces requiere más habilidad que la propia provocación. Otras veces, dependiendo del objetivo, la precarga puede ser bastante compleja. El escenario de bistec anterior es un problema complejo. La precarga tomó algo de tiempo y energía, donde una precarga simplista podría ser algo tan simple como descubrir qué tipo de automóvil conducen o alguna otra información inocua. En una conversación muy ocasional en la que "suceden" para estar en la misma tienda de delicatessen al mismo tiempo que su objetivo, se inicia una conversación informal con algo como: "Hombre, amo a myToyota. Este tipo en un Chevy acaba de retroceder hacia mí en el estacionamiento, ni siquiera un rasguño."Con un poco de suerte a medida que entablas el objetivo en la conversación, tu exclamación sobre tu coche podría caliéntelo con las preguntas que luego puede hacer sobre los tipos de automóviles u otros temas sobre los que desea reunir información.

El tema de la precarga tiene más sentido a medida que comienza a analizar cómo puede utilizar la elicitación. Los ingenieros sociales han estado dominando esta habilidad desde que la ingeniería social ha estado presente. Muchas veces el ingeniero social se da cuenta de que tiene esta habilidad antes de pasar a una vida de ingeniería social. Como joven o adulto joven, le resulta fácil interactuar con las personas, y más tarde descubre que gravita hacia el empleo que utiliza estas habilidades. Tal vez sea el centro de su grupo de amigos y la gente parece decirle todos sus problemas y no tiene ningún problema en hablar con él sobre todo. Más tarde, se da cuenta de que estas habilidades son las que lo hacen atravesar puertas que, de lo contrario, podrían cerrarse.

Cuando era joven siempre tuve este talento. Mis padres me contaban historias de cómo yo, a los cinco o seis años, entablaba conversaciones con extraños, a veces incluso entrando a la cocina de restaurantes concurridos para hacer preguntas sobre nuestro pedido o preguntar cómo se estaban haciendo las cosas. De alguna manera me salí con la suya, ¿por qué? Probablemente porque no sabía que este comportamiento no era aceptable y porque lo hice con confianza. A medida que crecí, esa habilidad (o la falta de miedo) entró en vigencia.

También parecía que a la gente, a veces incluso extraños, les encantaba contarme sus problemas y hablarme de cosas. Una historia que creo que ayuda a ver cómo pude utilizar la precarga, pero también las buenas habilidades de obtención fue cuando tenía alrededor de 17 o 18 años. Era un ávido surfista y hacía trabajos ocasionales para apoyar mi afición: básicamente, desde la entrega de pizzas hasta el cortador de fibra de vidrio y el salvavidas. Una vez hice recados para mi padre que era dueño de una empresa de consultoría contable / financiera. Entregaría documentos a sus clientes, obtendría firmas y los devolvería. A menudo, muchos de los clientes se abrían y me contaban todo sobre sus vidas, sus divorcios y sus éxitos y fracasos comerciales. Por lo general, esto comenzó con una pequeña sesión con ellos diciéndome lo maravilloso que mi papá era para ellos. En ese momento, nunca entendí por qué las personas, especialmente los adultos, se abrirían a un niño de 17 a 18 años con las razones por las que su universo se está separando.

Un cliente en particular que visitaría a menudo era dueño de un complejo de apartamentos.

no era nada enorme y elegante; él sólo tenía algunas propiedades que poseía y gestionaba. Este pobre hombre tenía problemas reales, problemas familiares, problemas de salud y problemas personales, todos los cuales me contaba de manera rutinaria mientras yo me sentaba y escuchaba. Aquí es cuando comenzó a golpearme y podría decir o hacer cosas increíbles si pasara un tiempo escuchando a la gente. Los hacía sentir importantes y como si yo fuera una buena persona. No importaba si me sentaba allí pensando en mi próxima gran ola; lo que importaba era que yo escuchara.

Normalmente escucharía durante el tiempo que pudiera soportar la increíble cantidad de humo de tabaco que sacaba (fumaba más que cualquier otra persona que haya visto en mi vida). Pero me sentaba y escuchaba, y

como era joven y no tenía experiencia, no ofrecería consejos, ni soluciones, solo un oído. La cosa era que estaba realmente preocupado; No lo fingí. Deseé tener una solución. Un día me contó cómo quería mudarse de regreso al oeste donde estaba su hija y estar más cerca de la familia.

Quería seguir con mi vida y conseguir un trabajo que pensé que sería genial, divertido y darme algo más de dinero para las tablas de surf y otras cosas que "necesitaba". Durante una de mis sesiones de escucha, una idea loca surgió en mi cabeza, y él me vio como un joven responsable y compasivo con una "buena cabeza" sobre mis hombros. La precarga tuvo lugar durante los meses que pasé sentado con él y escuchando. Ahora era el momento de sacar provecho de eso. Le dije: "¿Por qué no regresas y me dejas dirigir tu complejo de apartamentos por ti?"

La idea era tan absurda, tan ridícula que mirar hacia atrás ahora me hubiera reído en mi cara. Pero durante semanas, incluso meses, había escuchado sus problemas. Conocía al hombre y sus males. Además de eso, nunca me reí ni lo rechacé. Ahora él había compartido un problema conmigo, y aquí había una solución perfecta, una que solucionaba todos sus problemas, así como los míos. Mis necesidades de ingreso eran bajas, y él quería estar cerca de su familia. Habíamos establecido una relación en los últimos meses y, por lo tanto, él "me conocía" y confiaba en mí.

Después de un poco de discusión, llegamos a un acuerdo, él se levantó y se mudó de regreso a West y yo tenía 17 años de edad y manejaba un complejo de apartamentos de 30 unidades como el vice-propietario. Podría seguir y contarle mucho más sobre esta historia, pero el punto ya está leído. (Le diré que el trabajo fue excelente hasta que me pidió que intentara venderle el complejo, lo que hice en un tiempo récord. al mismo tiempo vendiéndome sin trabajo.

El punto es que desarrollé una relación, una confianza, con alguien y sin intentarlo y sin malas intenciones, tuve la oportunidad de precargarlo durante meses con las ideas de que era amable, compasivo e inteligente. Luego, cuando llegó el momento, pude presentar una idea absurda y, debido a los meses de precarga, se aceptó.

No fue hasta más tarde en la vida que me di cuenta de lo que estaba pasando aquí. Había tantos factores en juego que no me di cuenta en ese momento. La precarga desde el punto de vista de la ingeniería social implica conocer su objetivo antes de comenzar. En este caso, no sabía que iba a intentar conseguir un trabajo loco con este tipo. Pero la precarga aún funcionaba.

En la mayoría de los casos de ingeniería social sería mucho más rápido, pero creo que los principios se aplican. Ser tan genuino como sea posible es esencial. Debido a que la precarga involucra las emociones y los sentidos de la persona, no les dé ninguna razón para dudar. La pregunta que hagas debe coincidir con tu pretexto. Para que la precarga funcione, debes pedir algo que coincida con la creencia que creaste en ellos. Por ejemplo, si mi oferta fuera a visitar a la familia de mi cliente y tomar fotografías en lugar de administrar su complejo de apartamentos, no habría coincidido con el sistema de creencias que tenía de mí, a saber, que era una persona inteligente, orientada a los negocios, joven cariñoso Finalmente, la oferta, cuando se hace, debe ser beneficiosa para el objetivo, o al menos percibida como beneficio. En mi caso, hubo muchos beneficios para mi cliente. Pero en ingeniería social, el beneficio puede ser tan poco como "presumir de derechos": darle a la persona una plataforma para presumir un poco. O el beneficio puede ser mucho más e involucra beneficios físicos, monetarios o psicológicos.

Practicar la elicitación y dominarla te hará un ingeniero social maestro. Lógicamente, la siguiente sección es cómo convertirse en un elicitor exitoso.

Convertirse en un exitoso Elicitor

Analizando solo mis propias experiencias, puedo identificar algunos componentes clave que llevaron a mi éxito desde los cinco años hasta ahora:

Falta de miedo para hablar con la gente y estar en situaciones que no son Realmente me preocupo por las personas, incluso si no las conozco.

Quiero y disfruto escuchando a la gente

Ofrezco consejo o ayuda solo cuando tengo una solución real.

Ofrezco un oído que no juzga a las personas para hablar sobre sus problemas.

Estos son elementos clave para la obtención exitosa. El Departamento de Seguridad Nacional de los Estados Unidos (DHS, por sus siglas en inglés) tiene un folleto interno sobre la obtención que entrega a sus agentes que pude obtener y archivar en www.social-engineer.org/wiki/archives/BlogPosts/ocso-elicitation folleto. pdf

Este folleto contiene algunos excelentes punteros. Básicamente, como se indica en él y en este capítulo, se utiliza la elicitación porque funciona, es muy difícil de detectar y no es amenazante. El folleto del DHS aborda la elicitación desde un punto de vista de "cómo evitar", pero las siguientes secciones analizan algunos de los escenarios y muestran lo que se puede aprender.

Apelando al ego de alguien

El escenario pintado en el folleto del DHS es el siguiente:

Atacante: "Debes tener un trabajo importante; tal y como parece pensar muy bien de ti ".

Target: "Gracias, es un placer de tu parte decirlo, pero mi trabajo no es tan importante. Todo lo que hago aquí es ...

El método de apelar al ego de alguien es simplista pero efectivo. Sin embargo, hay que tener en cuenta que: acariciar el ego de alguien es una herramienta poderosa, pero si lo exagera o lo hace sin sinceridad, la gente se vuelve loca. No querrás salir como un acosador loco: "Wow, eres la persona más importante del universo y también tienes un aspecto asombroso". Decir algo así podría hacer que te llamen la seguridad.

El uso de las apelaciones del ego debe hacerse de manera sutil, y si usted está hablando con un verdadero narcisista, evite rodar los ojos, suspirar o argumentar cuando se jacta de sus logros. Las apelaciones sutiles al ego son cosas como: "Esa investigación que hiciste realmente cambió la opinión de muchas personas sobre ..." o "Oí por casualidad al Sr. Smith le dice a ese grupo que eres uno de los datos más entusiastas

analistas que tiene ". No haga el enfoque tan exagerado que sea obvio.

Una persona coaxa sutil de flattery puede participar en una conversación que tal vez nunca haya tenido lugar, como se indica en el folleto del DHS, y eso es exactamente lo que usted quiere como ingeniero social.

Expresando un interés mutuo

Considere este escenario simulado:

Atacante: "Wow, ¿tiene antecedentes en las bases de datos de cumplimiento con la norma ISO 9001? Debería ver el modelo que construimos para que un motor de informes ayude con esa certificación. Puedo conseguirte una copia."

Objetivo: "Me encantaría ver eso. Hemos estado jugando con la idea de agregar un motor de informes a nuestro sistema."

Expresar interés mutuo es un aspecto importante de la provocación. Este escenario particular es incluso más poderoso que apelar al ego de alguien porque extiende la relación más allá de la conversación inicial. El objetivo acordó seguir contactando, aceptar el software del atacante y expresó interés en discutir los planes para el software de la compañía en el futuro. Todo esto puede llevar a una violación masiva en la seguridad.

El peligro en esta situación es que ahora el atacante tiene el control total. Controla los siguientes pasos, qué información se envía, cuánto y cuándo se libera. Este es un movimiento muy poderoso para el ingeniero social. Por supuesto, si el compromiso fuera a largo plazo, entonces tener una pieza literal de software que se pueda compartir sería aún más ventajoso. Compartir software utilizable y no malicioso generaría confianza, establecería una relación y haría que el objetivo tuviera un sentido de obligación.

Hacer una declaración falsa deliberada

La entrega de una declaración falsa parece que sería contraproducente, pero puede ser una fuerza poderosa a tener en cuenta.

Atacante: "Todo el mundo sabe que XYZ Company produjo el software de mayor venta para este widget en la tierra".

Objetivo: “En realidad, eso no es cierto. Nuestra empresa comenzó a vender un similar producto en 1998 y nuestros registros de ventas los han superado de manera rutinaria en más del 23% “.

Estas declaraciones, si se usan de manera efectiva, pueden provocar una respuesta del objetivo con hechos reales. La mayoría de las personas deben corregir las afirmaciones erróneas cuando las escuchan. Es casi como si tuvieran el desafío de probar que están en lo correcto. El deseo de informar a los demás, parece estar informado y ser intolerante con las declaraciones erróneas parece estar integrado en la naturaleza humana. Comprender este rasgo puede hacer que este escenario sea poderoso. Puede usar este método para obtener detalles completos del objetivo sobre hechos reales y también para discernir quién en un grupo puede tener más conocimiento sobre un tema.

Información de voluntariado

El folleto del DHS hace una buena observación sobre un rasgo de personalidad que muchos de nosotros tenemos. Algunas menciones de esto ya han aparecido en el libro y se tratan con mucho más detalle más adelante, pero la obligación es una fuerza fuerte. Como ingeniero social, ofrecer información en una conversación casi obliga al objetivo a responder con información igualmente útil.

¿Quieres probar este? La próxima vez que esté con sus amigos, diga algo como: “¿Escuchaste sobre Ruth? Escuché que ella acaba de ser despedida del trabajo y está teniendo serios problemas para encontrar más trabajo.”

La mayoría de las veces obtendrás “Wow, no escuché eso. Esa es una noticia terrible. Escuché que Joe se está divorciando y que ellos también van a perder la casa.”

Un aspecto de la humanidad es que tendemos a vivir el dicho “la miseria ama a la compañía”, lo cierto que es en este caso. Las personas tienden a querer compartir noticias similares. Los ingenieros sociales pueden utilizar esta tendencia para establecer el tono o el estado de ánimo de una conversación y crear un sentido de obligación.

Asumiendo conocimiento

Otra herramienta de manipulación poderosa es la del conocimiento asumido. Es un lugar común suponer que si alguien tiene conocimiento de una situación particular, es aceptable discutirlo con ellos.Un atacante puede explotar deliberadamente este rasgo presentando información como si estuviera informado y luego utilizando elicitación para entablar una conversación a su alrededor. Entonces él puede regurgitar la información como si fuera la suya y continúe construyendo la ilusión de que él tiene Conocimiento íntimo de este tema. Este escenario podría estar mejor ilustrado con un ejemplo.

Una vez fui a China para negociar un gran acuerdo sobre algunos materiales. Necesitaba tener un conocimiento íntimo de mi compañía objetivo en las negociaciones y tenía que encontrar una manera de obtenerlo antes de reunirme con ellos. Nunca nos habíamos visto cara a cara, pero me dirigía a una conferencia en China antes de que empezaran mis negociaciones. Mientras estaba en la conferencia, escuché por casualidad una conversación que comienza acerca de cómo ubicarse en una posición más alta al tratar con los chinos en las negociaciones.

Sabía que esta era mi oportunidad, y para hacer la situación aún más dulce, una de las personas del pequeño grupo era de la compañía con la que iba a reunirme. Rápidamente me inyecté en la conversación y supe que si no decía algo rápido, perdería la cara. Mi conocimiento era limitado, pero ellos no necesitaban saber eso. Cuando surgió una pequeña pausa, comencé a hablar sobre la teoría de Guanxi. Guanxi es básicamente cómo dos personas que pueden no tener el mismo estatus social pueden conectarse, y luego una es presionada para que se haga un favor a la otra. Hablé sobre cómo se puede usar esta conexión, y luego llegué a la conclusión de lo importante que es para los estadounidenses no solo tomar una tarjeta de negocios y guardarla en mi bolsillo, sino revisarla, comentarla y luego colocarla. En algún lugar respetuoso.

Esta conversación fue suficiente para establecerme como alguien que tenía algún conocimiento y merecía permanecer en el círculo de confianza allí. Ahora que había establecido mi base de conocimientos, me senté y escuché a cada persona expresar su experiencia y conocimiento personal sobre cómo negociar adecuadamente con grandes empresas chinas. Presté mucha atención y especial atención cuando hablaron los caballeros que trabajaban para mi empresa objetivo. Mientras hablaba, podía decir que los “consejos” que estaba dando estaban

estrechamente relacionados con las filosofías empresariales de su empresa. Este conocimiento fue más valioso que cualquier otra cosa por la que podría haber pagado y condujo a un viaje exitoso.

Hay un par de escenarios más que creo que se usan a menudo en elicitaciones.

Usando los efectos del alcohol

Nada afloja más los labios que el jugo. Este es un hecho desafortunado pero cierto. Mezcle una de las cinco situaciones anteriores con alcohol y puede aumentar sus efectos en 10.

Probablemente la mejor manera de describir este escenario es con una historia real.

En 1980, un científico senior del Laboratorio Nacional de Los Álamos viajó a un instituto de investigación en la República Popular China (PRC) para hablar sobre su especialidad, la fusión nuclear. Tenía un amplio conocimiento de la información sobre armas nucleares de los Estados Unidos, pero sabía que la situación en la que estaba ingresando era peligrosa y tenía que estar decidido a atenerse a su tema.

Sin embargo, fue constantemente atacado con investigaciones cada vez más detalladas directamente relacionadas con las armas nucleares. Las tácticas de los atacantes cambiarían y harían muchas preguntas benignas sobre la fusión y la astrofísica, su especialidad.

Una vez incluso hicieron un cóctel en su honor. Se reunieron alrededor y aplaudieron su conocimiento e investigación, cada vez con un brindis y una bebida. Comenzaron a indagar sobre asuntos clasificados como las condiciones de ignición del deuterio y el tritio, los dos componentes de la bomba de neutrones de entonces. Lo hizo bien para defenderse de las preguntas constantes, pero después de muchos brindis y una fiesta en su honor, decidió dar una analogía. Le dijo al grupo que si enrollaba esos dos componentes en una bola y luego los sacaba de la mesa, probablemente se encenderían porque tenían niveles de umbral de temperatura tan bajos.

Esta historia e información aparentemente inútil probablemente causó la Investigadores en China para discernir un camino claro de investigación sobre armas nucleares. Llevarían esta información a otro científico y ahora armado con un poco más de conocimiento, utiliza ese conocimiento para llegar a la siguiente etapa con él o ella. Después de muchos intentos, es muy probable que el científico chino posea una imagen clara de qué camino tomar.

Este es un ejemplo serio de cómo el uso de la obtención puede llevar a obtener una imagen clara de toda la respuesta. En ingeniería social puede ser lo mismo. para ti. Todas las respuestas pueden no provenir de una sola fuente. Puede obtener cierta información de una persona sobre su paradero en una fecha en particular, y luego usar esa información para obtener más información de la próxima

etapa, y así sucesivamente y así sucesivamente. Reunir esas pepitas de información a menudo es la parte difícil de perfeccionar las habilidades de obtención. Eso se discute a continuación.

Uso de preguntas inteligentes

Como ingeniero social, debe darse cuenta de que el objetivo de la obtención no es acercarse y decir: “¿Cuál es la contraseña para sus servidores?”

El objetivo es obtener información pequeña y aparentemente inútil que ayude a construir una imagen clara de las respuestas que está buscando o el camino para obtener esas respuestas. De cualquier manera, este tipo de recopilación de información puede ayudar a dar al ingeniero social un camino muy claro hacia la meta objetivo.

¿Cómo sabes qué tipo de preguntas usar?

Las siguientes secciones analizan los tipos de preguntas que existen y cómo un ingeniero social puede usarlas.

Preguntas de final abierto

Las preguntas abiertas no pueden responderse con sí o no. Preguntar: “Hace bastante frío hoy, ¿eh?” Llevará a un “Sí”, “Uh-uh”, “Sí”, o alguna otra expresión gutural afirmativa similar, mientras que pregunta: “¿Qué piensa usted del clima hoy? ”Provocará una respuesta real: la persona debe responder con más de un sí o un no.

Una forma en que un ingeniero social puede aprender a usar preguntas abiertas es analizando y estudiando a los buenos reporteros. El reportero de Agood debe usar preguntas abiertas para continuar obteniendo respuestas de su entrevistado.

Supongamos que tenía planes de conocer a un amigo y él canceló, y quería saber por qué. Puedo hacer una pregunta como: "Tenía curiosidad por lo que pasó con nuestros planes la otra noche".

"No me sentía muy bien".
"Oh, espero que estés mejor ahora. ¿Que está mal?"

Esta línea de preguntas generalmente obtiene más resultados que hacer un asalto total a la persona y decir algo como: "¿Qué diablos, hombre? ¡Me abandonaste la otra noche!"

Otro aspecto de las preguntas abiertas que agrega poder es el uso de por qué y cómo. Hacer un seguimiento de una pregunta sobre cómo o por qué puede llevar a una explicación mucho más profunda de lo que originalmente estaba preguntando.

De nuevo, esta pregunta no es "sí" o "no", y la persona revelará otros detalles que le puedan parecer interesantes.

A veces, las preguntas abiertas pueden encontrar cierta resistencia, por lo que usar el enfoque piramidal podría ser bueno. El enfoque piramidal es donde comienza con preguntas estrechas y luego hace preguntas más amplias al final de la línea de preguntas. Si realmente quieres mejorar en esta técnica, aprende a usarla con adolescentes.

Por ejemplo, muchas veces las preguntas abiertas como "¿Cómo estuvo la escuela hoy?" Se encontrarán con un "OK" y nada más, por lo que hacer una pregunta estrecha podría abrir mejor el flujo de información.

"¿Qué estás haciendo en matemáticas este año?" Esta pregunta es muy estrecha y solo puede responderse con una respuesta específica: "Álgebra II."

"Ah, siempre he odiado eso. ¿Te gusta eso?"

Desde allí, siempre puede dividirse en preguntas más amplias, y después de obtener el objetivo de hablar, obtener más información generalmente se vuelve más fácil.

Preguntas cerradas

Obviamente, las preguntas cerradas son lo opuesto a las preguntas abiertas, pero son una forma muy efectiva de dirigir un objetivo a donde quieras. Las preguntas cerradas a menudo no pueden responderse con más de una o dos posibilidades.

En una pregunta abierta, uno podría preguntarse: "¿Cuál es su relación con su gerente?", Pero una pregunta cerrada podría estar redactada como "¿Es buena su relación con su gerente?"

La información detallada no suele ser el objetivo con preguntas cerradas; más bien, liderar el objetivo es la meta.

La policía y los abogados utilizan este tipo de razonamiento a menudo. Si quieren guiar a su objetivo por un camino particular, hacen preguntas muy cerradas que no permiten la libertad de respuestas. Algo como esto:

"¿Conoce al acusado, señor Smith?"
"Sí."
"En la noche del 14 de junio, ¿viste al señor Smith en la taberna ABC?"
"Yo si."
"¿Y a qué hora fue eso?"
"11:45 pm."
Todas estas preguntas tienen un final muy cerrado y solo se permiten para uno o dos tipos de respuestas.
Preguntas principales

Combinando los aspectos de las preguntas abiertas y cerradas, las preguntas principales están abiertas con una sugerencia que conduce a la respuesta. Algo así como: "Estabas en la taberna ABC con el Sr. Smith el 14 de junio a las

11:45 pm, ¿verdad?”Este tipo de pregunta conduce al objetivo donde usted quiere, pero también le ofrece la oportunidad de expresar sus opiniones, pero de manera muy limitada. También precarga el objetivo con la idea de que tiene conocimiento de los eventos que se le preguntan.

Las preguntas principales a menudo pueden responderse con un sí o un no, pero son diferentes de las preguntas cerradas porque se siembra más información en la pregunta que, cuando se responde, le da al ingeniero social más información para trabajar. Las preguntas principales indican algunos hechos y luego le piden al objetivo que esté de acuerdo o en desacuerdo con ellos.

En 1932, el psicólogo británico Frederic C. Bartlett concluyó un estudio sobre la memoria reconstructiva. Les contó a los sujetos una historia y luego les pidió que recordaran los hechos inmediatamente, dos semanas después y luego cuatro semanas más tarde. Bartlett descubrió que los sujetos modificaron la historia basándose en su cultura y creencias, así como en su personalidad. Ninguno pudo recordar la historia con precisión y en su totalidad. Se determinó que los recuerdos no son registros precisos de nuestro pasado. Parece que los humanos intentan hacer que la memoria se adapte a nuestras representaciones existentes del mundo. Cuando se hacen preguntas, muchas veces respondemos de memoria en función de nuestras percepciones y lo que es importante para Nosotros. Debido a esto, es posible hacer una pregunta importante a las personas y manipular su memoria. Elizabeth Loftus, una figura destacada en el campo de investigación de testimonios de testigos, ha demostrado a través del uso de preguntas principales cómo distorsionar la memoria de un evento de una persona es fácilmente

posible. Por ejemplo, si le mostró a una persona una imagen de la habitación de un niño que no contenía osos de peluche y luego le preguntó: “¿Viste un osito de peluche?”No estás insinuando que uno estaba en la habitación y que la persona es libre

Para responder sí o no como lo deseen. Sin embargo, preguntar: “¿Viste el osito de peluche?” Implica que uno estaba en la habitación y que la persona tiene más probabilidades de

responde “sí”, porque la presencia de un oso de peluche es consistente con eso esquema de la habitación de un niño.

Herramienta en manos de un ingeniero social capacitado. Aprender a dirigir el objetivo también puede mejorar la capacidad de un ingeniero social para recopilar información.

Preguntas de asunción

Las preguntas asumidas son exactamente como suenan, donde usted asume que cierto conocimiento ya está en posesión del objetivo. La forma en que un ingeniero social puede determinar si un objetivo posee o no la información que está buscando es hacer una pregunta asumida.

Por ejemplo, una habilidad empleada por la policía es asumir que el objetivo ya tiene conocimiento, por ejemplo, de una persona, y preguntar algo como “¿Dónde vive el Sr. Smith?” Dependiendo de la respuesta dada, el oficial puede determinar si el objetivo conoce a la persona y cuánto sabe de él.

Un buen punto a tener en cuenta es que cuando un ingeniero social utiliza supuestas preguntas, la imagen completa nunca debe darse al objetivo. Al hacerlo, le da todo el poder al objetivo y elimina gran parte de la capacidad del ingeniero social para controlar el ambiente. El ingeniero social nunca quiere usar preguntas de asunción para acusar al objetivo de un error. Hacerlo aliena el objetivo y nuevamente le cuesta al ingeniero social.

Un ingeniero social debe usar preguntas de asunción cuando tenga alguna idea de los hechos reales que puede usar en la pregunta. Usar una pregunta asumida con información falsa puede desactivar el objetivo y solo confirmará que el objetivo no sabe algo que no sucedió. Volver a una En un ejemplo anterior, si quisiera obtener información de un químico líder e hice algunas investigaciones y sabía lo suficiente como para formular una oración inteligente, podría formular una pregunta asumida, pero arruinaría el seguimiento futuro si no pudiera respaldar el supuesto. objetivo haría de mi conocimiento.

Por ejemplo, si tuviera que preguntar: “Debido a que el deuterio y el tritio tienen umbrales de temperatura tan bajos, ¿cómo se manejan estos materiales para evitar la ignición?” La información de seguimiento podría ser difícil

de seguir si no soy un físico nuclear. Esto es contraproducente y no demasiado útil. Planea tus preguntas de asunción para tener el máximo efecto.

Un complemento que se le enseña a los oficiales de la ley que resulta muy útil cuando se usan preguntas asumidas es decir: “Ahora piense detenidamente antes de responder la siguiente pregunta ...” Este tipo de afirmación precarga la mente del objetivo con la idea de que debe ser Verdadero con su siguiente declaración.

Puede tomar meses o años para dominar estas habilidades. No se desanime si los primeros intentos no tienen éxito, y siga intentándolo. Sin embargo, no temas, hay algunos consejos para dominar esta habilidad. Voy a revisar estos en el cierre.

Dominar la elicitación

Este capítulo tiene mucha información para que usted la absorba, y si no es una persona de personas, emplear las técnicas cubiertas puede parecer una tarea desalentadora. Como la mayoría de los aspectos de la ingeniería social, la obtención tiene una serie de principios que, cuando se aplican, mejorarán su nivel de habilidad. Para ayudarlo a dominar estos principios, recuerde estos consejos:

Demasiadas preguntas pueden cerrar el objetivo. Salpicando el objetivo con un aluvión de preguntas no hará nada más que apagar el objetivo.

Recuerda, la conversación es un dar y recibir. Quieres preguntar pero tu Hay que dar para que el objetivo se sienta cómodo.

Muy pocas preguntas harán que el objetivo se sienta incómodo. Tienes ¿Alguna vez has estado en una conversación que está llena de “silencios incómodos”? Eso no es bueno es? No asuma que su objetivo es un experto y dispuesto conversador. Debes trabajar en hacer una conversación y experiencia disfrutable.

Haga solo una pregunta a la vez. Capítulo 5 cubre desbordamientos de búfer en la mente humana, pero en este momento su objetivo no es desbordar el objetivo. Es meramente recopilar información y construir un perfil. Para hacer esto No puedes parecer demasiado ansioso o no interesado.

Como probablemente se haya reunido, hacer que la elicitación funcione correctamente es un delicado equilibrio. Demasiado, demasiado poco, demasiado a la vez, no lo suficiente, cualquiera de ellos matará sus posibilidades de éxito.

Sin embargo, estos principios pueden ayudarte a dominar este increíble talento. Ya sea que utilice este método para la ingeniería social o simplemente para aprender a interactuar con las personas, intente esto: piense en la conversación como un embudo, donde en la parte superior está la parte más grande, más “neutral” y en la parte inferior es la parte muy estrecha y directa. finalizando.

Comience por hacer preguntas muy neutrales al objetivo y reúna algo de información usando estas preguntas. Dé y reciba su conversación, y luego pase a algunas preguntas abiertas. Si es necesario, use algunas preguntas cerradas para dirigir el objetivo hacia donde desea ir y luego, si la situación se ajusta, pase a preguntas altamente dirigidas a medida que llega al final del embudo. Lo que saldrá del “pico” de ese embudo es un río de información.

Piénselo en la situación discutida en este capítulo de mi puntero en la reunión de la cámara de comercio. Mi propósito fue reunir información sobre cualquier cosa que pudiera conducir a una brecha de seguridad.

Comencé la conversación con una pregunta muy neutral. “¿Escapar de los buitres?” Esta pregunta rompió el hielo en la conversación y también utilizó un poco de humor para crear un puente que nos permitió existir en el mismo plano de pensamiento. Le hice algunas preguntas más neutrales y le entregué mi tarjeta mientras le preguntaba qué hacía. Esto continúa suavemente en las preguntas abiertas.

Una breve sesión de recopilación de información que se realizó antes, utilizando preguntas cerradas o supuestas cuidadosamente colocadas fue clave. Después de enterarme de la reciente compra de la compañía para un nuevo software de contabilidad y actualizaciones de red, quise ir por el asesinato. Habiendo explorado el edificio, sabía que usaba RFID, pero no estaba seguro de si el objetivo llegaría tan lejos como para describir el Tarjeta y me la enseñas.

Aquí es donde el uso de preguntas directas jugó un papel importante: salir y preguntar qué seguridad usaba la compañía. Cuando utilicé ese tipo de pregunta, nuestra relación y el factor de confianza eran tan altos que probablemente habría respondido a todas las preguntas que hice.

Comprender cómo comunicarse con las personas es una habilidad esencial para un elicitor. El ingeniero social debe ser adaptable y capaz de adaptar la conversación a su entorno y situación. Construir rápidamente incluso la menor cantidad de confianza con el objetivo es crucial. Sin esa relación, la conversación probablemente fracasará. Otros factores clave incluyen asegurarse de que su estilo de comunicación, las preguntas utilizadas y la manera en que habla, coincidan con su pretexto. Saber cómo hacer preguntas que obliguen a una respuesta es clave para lograr una obtención exitosa. Pero si toda esa habilidad y todas esas preguntas no coinciden con su pretexto, entonces el intento de obtención seguramente lo hará fallar.

Resumen

Este capítulo cubrió algunos de los puntos más poderosos de todo este libro: poderoso en el sentido de que aplicarlos puede cambiar no solo sus habilidades de ingeniería social, sino también sus habilidades como comunicador. Saber cómo hacer las preguntas correctas en el tiempo correcto y de la manera correcta puede abrir tantas oportunidades. Como ingeniero social, esto es lo que separa el éxito del fracaso. Las primeras impresiones se basan inicialmente a la vista, pero lo que sale primero de la boca puede hacer o deshacer el trato. Dominar la elicitación casi puede garantizar el éxito como ingeniero social y puede agregar mucho peso a cualquier texto que decida usar. A lo largo de este capítulo mencioné el poder de los pretextos. Este es otro tema que todo ingeniero social, tanto malicioso como profesional, debe dominar. ¿Pero cómo puedes asegurarte de lograr este objetivo? Para responder a esto, debe aprender acerca de los pretextos y comprender exactamente qué es, como se explicó en el Capítulo 4.

Capitulo 4

Pretexto: Cómo convertirse en alguien

La honestidad es la clave de una relación. Si puedes fingir eso, estás dentro.

- Richard Jeni A veces probablemente desearíamos ser otra persona.

Heck, me encantaría ser un poco más delgado y mejor aspecto. A pesar de que la ciencia médica no ha ideado una píldora que pueda hacer eso posible, existe una solución a este dilema: se llama pretexto.

¿Qué es pretexto?

Algunas personas dicen que es solo una historia o mentira de que actuará durante un compromiso de ingeniería social, pero esa definición es muy limitada. Pretexto se define mejor como la historia de fondo, la vestimenta, el aseo, la personalidad y la actitud que conforman el personaje que será para la auditoría de ingeniería social. Pretexto abarca todo lo que imaginas que esa persona sería. Cuanto más sólido sea el pretexto, más creíble será como ingeniero social. A menudo, cuanto más simple sea tu pretexto, mejor estás. Pretexto, especialmente desde la llegada de Internet, ha visto un aumento en los usos maliciosos. Una vez vi una camiseta que decía: “Internet: donde los hombres son hombres, las mujeres son hombres, y los niños son agentes del FBI que están esperando para atraparte”. Aunque este dicho tiene un poco de verdad, tiene mucha verdad. En internet puedes ser quien quieras ser. Los piratas informáticos malintencionados han estado utilizando esta capacidad para su ventaja durante años y no solo con Internet.

En la ingeniería social, desempeñar un papel o ser una persona diferente para lograr el objetivo con éxito es a menudo imperativo. Chris Hadnagy podría no tener tanta atracción como el técnico de soporte técnico o el CEO de una importante organización importadora. Cuando surge una situación de ingeniería social, es importante tener las habilidades necesarias para convertirse en el pretexto. En una discusión estuve Pretexto, especialmente desde la llegada de Internet, ha visto un aumento en los usos maliciosos. Una vez vi una camiseta

que decía: “Internet: donde los hombres son hombres, las mujeres son hombres, y los niños son agentes del FBI que están esperando para atraparte”. Aunque este dicho tiene un poco de verdad, tiene mucha verdad. En internet puedes ser quien quieras ser. Los piratas informáticos malintencionados han estado utilizando esta capacidad para su ventaja durante años y no solo con Internet. Después de hablar con el ingeniero social de renombre mundial, Chris Nickerson, sobre este tema, dijo algo que creo que realmente afecta a su hogar. Nickerson afirmó que pretextar no se trata de representar un papel o de desempeñar un papel. Dijo que no se trata de vivir una mentira, sino de convertirse en esa persona. Usted es, en cada fibra de su ser, la persona que está retratando. La forma en que camina, la forma en que habla, el lenguaje corporal, te conviertes en esa persona. Estoy de acuerdo con esta filosofía en pretexto. A menudo, cuando la gente ve una película, las que creemos que son “lo mejor que hemos visto” es donde los actores nos cautivan tanto con sus partes que no podemos separarlas de sus personajes representados. Esto fue comprobado para mí cuando, hace muchos años, mi esposa y yo vimos una gran película con Brad Pitt, Leyendas de la caída. Fue un imbécil egoísta en esta película, un alma atormentada que tomó muchas malas decisiones. Era tan bueno interpretando esta parte. Mi esposa, literalmente, lo odiaba como actor durante algunos años. Ese es un buen pretexter. El problema con el uso de pretextos para muchos ingenieros sociales es que sienten que se está vistiendo como una parte y eso es todo. Es cierto que el vestido puede ayudar, pero pretexto es una ciencia. En cierto modo, toda tu persona te retratará bajo una luz que es diferente de quién eres. Para hacer esto, usted, como ingeniero social, debe tener una idea clara de lo que realmente es pretexto. Entonces puedes planear y realizar el pretexto perfectamente. Finalmente, puede aplicar los toques finales. Este capítulo cubrirá aquellos aspectos de pretexto. Primero es una discusión de lo que realmente es pretexto. A continuación, se analiza cómo utilizar el pretexto como ingeniero social. Finalmente, para unirlo todo, este capítulo explora algunas historias que muestran cómo usar pretextos de manera efectiva.

¿Qué es pretexto?

El Pretexto se define como el acto de crear un escenario inventado para persuadir a una víctima objetivo para que libere información o realice alguna acción. Es más que crear una mentira; en algunos casos puede crear una identidad completamente nueva y luego usar esa identidad para manipular la recepción de información. Los ingenieros sociales pueden usar el pretexto para hacerse pasar por personas en ciertos trabajos y Roles que ellos mismos nunca han hecho. El Pretexto no es una solución única para todos. Ingeniero social debe desarrollar muchos pretextos diferentes a lo largo de su carrera. Todos ellos tendrán una cosa en común: la investigación. Las buenas técnicas de recopilación de información pueden hacer o deshacer un buen pretexto. Por ejemplo, imitar al representante de soporte técnico perfecto es inútil si su objetivo no usa soporte externo.

El Pretexto también se utiliza en áreas de la vida que no sea la ingeniería social. Ventas; hablar en público; los llamados adivinos; expertos en programación neurolingüística (PNL); e incluso los médicos, abogados, terapeutas, y similares, tienen que usar una forma de pretexto. Todos tienen que crear un escenario en el que las personas se sientan cómodas con la divulgación de información que normalmente no harían. La diferencia en los ingenieros sociales que usan pretexto y otros son los objetivos involucrados. Un ingeniero social, una vez más, debe vivir esa persona por un tiempo, no solo actuar una parte.

Mientras dure la auditoría o el concierto de ingeniería social, debes estar en la persona. Yo mismo me “pongo en el personaje”, al igual que muchos de mis colegas, algunos de los cuales incluso permanecen en el personaje “fuera del reloj”. En cualquier lugar que necesites, debes ser el pretexto que te propongas ser. Además, muchos ingenieros sociales profesionales tienen diferentes cuentas en línea, redes sociales, correo electrónico y otras cuentas para respaldar una gran cantidad de pretextos.

Una vez entrevisté al ícono de la radio Tom Mischke sobre este tema para un podcast de ingeniería social del cual formo parte (alojado en www.social engineer.org/episode-002-pretexting-not-just-just-for-social-engineers/). Los locutores de radio deben ser expertos en pretextos porque constantemente tienen que divulgar solo la información que desean al público. Tom era tan hábil en esto que muchos oyentes sentían como si lo “conocieran” como amigo. Recibía invitaciones a bodas, aniversarios e incluso nacimientos. ¿Cómo pudo Tom lograr este increíble tipo de

pretexto? La respuesta es la práctica. Mucha y mucha práctica es lo que él prescribió. Me dijo que en realidad planearía sus "actos" y luego los practicaría: usaría la voz que tendrían, se sentaría cómo se sentarían, tal vez incluso se vistiera como si se vistieran. La práctica es exactamente lo que hace un buen pretexto.

Un aspecto muy importante a recordar es que la calidad del pretexto está directamente relacionada con la calidad de la información recopilada. Mientras más, mejor, y cuanto más relevante sea la información, más fácil será para que el pretexto se desarrolle y tenga éxito. Por ejemplo, el pretexto clásico de un chico de soporte técnico fallaría por completo si acudieras a una empresa que tuviera soporte interno o fuera a una compañía muy pequeña de una o dos personas. Tan natural como usted es cuando conversa con alguien acerca de quién es realmente, lo fácil que es aplicar su pretexto.

Para que puedas ver cómo puedes utilizar esta habilidad, La siguiente sección cubre los principios de pretexto y luego muestra cómo puede aplicarlos para planificar realmente un plan sólido.

Los Principios y Etapas de Planificación del Pretexto

Al igual que con Everyskill, ciertos principios dictan los pasos para realizar esa tarea. Pretexto no es diferente. La siguiente es una lista de principios de pretexto que puede utilizar. De ninguna manera estos son los únicos principios ahí afuera; tal vez se puedan agregar otros, pero estos principios encarnan la esencia de los pretextos:

Cuanta más investigación hagas, más posibilidades de éxito tendrás.

La participación de sus propios intereses personales aumentará el éxito.

Practicar dialectos o expresiones.

Muchas veces el esfuerzo de ingeniería social puede reducirse si el teléfono es visto como menos importante Pero como ingeniero social, usando el teléfono.

No debe reducirse el esfuerzo puesto en el concierto de ingeniería social.
Cuanto más simple sea el pretexto, mayor será la probabilidad de éxito.
El pretexto debe aparecer espontáneo.
Proporcionar una conclusión lógica o seguir para el objetivo.
Las siguientes secciones discuten cada uno de estos principios en detalle.
Cuanto más investigue, mejor será la probabilidad de éxito

Este principio se explica por sí mismo, pero no se puede decir lo suficiente: el nivel de éxito está directamente relacionado con el nivel y la profundidad de la investigación. Como se discutió en el Capítulo 2, es el quid de la ingeniería social exitosa. Cuanta más información tenga un ingeniero social, más posibilidades tendrá de él o ella.

de desarrollar un pretexto que funcione. ¿Recuerda la historia que conté en el Capítulo 2 sobre mi mentor Mati Aharoni y cómo convenció a un ejecutivo de alto nivel para que visite su sitio de "colección de sellos" en línea? A primera vista, el camino dentro de esa compañía podría haber parecido algo relacionado con las finanzas, la banca, la recaudación de fondos o algo parecido, porque era una institución bancaria. Cuanta más investigación hiciera Mati, más claro resultaba que el pretexto podía ser una persona que vendía una colección de sellos. Averiguar qué intereses del ejecutivo permitió a Mati encontrar una empresa en la empresa, y funcionó.

A veces esos pequeños detalles que son los que marcan la diferencia.

Recuerda, ninguna información es irrelevante. Al recopilar información, buscar historias, artículos o aspectos de carácter personal también es una buena idea. El uso de adjuntos personales o emocionales de un objetivo puede permitirle poner un pie en la puerta. Si el ingeniero social descubre que todos los años el CFO dona una suma considerable al centro de investigación del cáncer infantil, entonces un pretexto que involucra la recaudación de fondos por esta causa podría funcionar, por muy despiadado que parezca.

El problema es que los ingenieros sociales maliciosos usan pretextos que se alimentan de Emociones sin un segundo pensamiento. Después de los ataques a las Torres Gemelas en la ciudad de Nueva York el 11 de septiembre de 2001,

muchos piratas informáticos e ingenieros sociales malintencionados utilizaron las pérdidas de estas personas para recaudar fondos por sí mismos a través de sitios web y correos electrónicos dirigidos a las computadoras de personas y recaudadores de fondos falsos que obtuvieron fondos de Aquellos con un corazón generoso. Después de los terremotos en Chile y Haití en 2010, ocurrieron las mismas situaciones en las que muchos ingenieros sociales malintencionados desarrollaron sitios web que proporcionaban información sobre la actividad sísmica o las personas que se habían perdido. Estos sitios fueron codificados con código malicioso y computadoras pirateadas.

Esto es incluso más evidente directamente después de la muerte de una estrella de cine o música. La optimización de motores de búsqueda (SEO) y los genios del marketing harán que los motores de búsqueda elaboren sus historias en cuestión de horas. Junto con los especialistas en marketing, los ingenieros sociales maliciosos aprovecharán la mayor atención del motor de búsqueda al lanzar sitios maliciosos que se alimentan de ese SEO. Atrayendo personas a estos sitios, recolectan información o los infectan con virus.

Que la gente se aproveche de la desgracia de los demás es un hecho triste sobre este mundo, y uno de esos rincones oscuros que dije que visitarías en este libro. Como auditor de ingeniería social, puedo usar las emociones de un empleado para mostrarle a una empresa que incluso las personas con intenciones aparentemente buenas pueden engañar a los empleados de la empresa para que den acceso a datos valiosos y que arruinan el negocio.

Todos estos ejemplos consolidan el punto de que cuanto mejor sea el proceso de recopilación de información e investigación de un ingeniero social, más posibilidades tendrá de encontrar algún detalle que aumente las posibilidades de un pretexto exitoso.

Involucrar intereses personales para aumentar el éxito

Utilizar sus propios intereses personales para aumentar las posibilidades de un movimiento exitoso de ingeniería social parece muy simple, pero puede llegar a convencer al objetivo de que usted es creíble. Nada puede arruinar la relación y la confianza más rápido que una persona que dice tener conocimiento sobre un tema y luego se queda corta. Como ingeniero social, si nunca antes ha visto una sala de servidores y nunca ha desarmado una computadora, tratar de interpretar la parte de un técnico puede ser un camino rápido hacia el fracaso. Incluir temas y actividades en su pretexto que le interesan le da mucho de qué hablar y le brinda la capacidad de interpretar la inteligencia y la confianza.

La confianza puede hacer mucho para convencer al objetivo de que eres quien dices que eres. Ciertos pretextos requieren más conocimiento que otros (por ejemplo, coleccionista de sellos versus investigador nuclear) para ser convincentes, por lo que, de nuevo, la investigación se convierte en el tema recurrente. A veces, el pretexto es lo suficientemente simple como para obtener el conocimiento al leer algunos sitios web o un libro.

Sin embargo, si adquiere el conocimiento, es importante investigar temas que le interesen personalmente, como ingeniero social. Después de aprender sobre una historia, un aspecto, un servicio o un interés, tiene muchos conocimientos o al menos se siente cómodo para discutir ver si ese ángulo puede trabajar El Dr. Tom G. Stevens, PhD, dice: “Es importante recordar que la confianza en uno mismo es siempre relativa a la tarea y la situación. Tenemos diferentes niveles de confianza en diferentes situaciones ”. Esta declaración es muy importante, porque la confianza se vincula directamente con la forma en que otros lo ven como un ingeniero social. La confianza (siempre que no sea un exceso de confianza) genera confianza y relación y hace que las personas se sientan a gusto. Es muy importante encontrar un camino hacia su objetivo que le ofrezca la oportunidad de hablar sobre temas con los que se sienta cómodo y de los que pueda hablar con confianza.

En 1957, el psicólogo Leon Festinger propuso la teoría de la disonancia cognitiva. Esta teoría establece que las personas tienden a buscar la coherencia entre sus creencias, opiniones y básicamente todas sus cogniciones. Cuando existe una inconsistencia entre actitudes y comportamientos, algo debe cambiar para eliminar la disonancia.
Dr. Festinger afirma que dos factores afectan la fuerza de la disonancia:

El número de creencias disonantes.
La importancia de cada creencia.

Luego afirmó que existen tres formas de eliminar la disonancia (lo que debería hacer que los oídos de un ingeniero social se animen):

Reducir la importancia de las creencias disonantes.
Agregue más creencias consonantes que superan a las disonantes.
Cambia las creencias disonantes para que ya no sean inconsistentes.

¿Cómo utiliza un ingeniero social esta información? Acercarse a un pretexto con falta de confianza cuando su pretexto dice que debe tener confianza, automáticamente crea disonancia. Esta disonancia levanta todo tipo de señales de alerta y pone barreras a la comunicación, la confianza y el movimiento hacia adelante. Estas barreras afectan el comportamiento del objetivo, de quien se espera que equilibre sus sentimientos de disonancia y elimine cualquier posibilidad de que su pretexto funcione.

Uno de los métodos para contrarrestar esto es agregar más creencias consonantes de manera Que superen a los disonantes. ¿Qué esperaría el objetivo de tu pretexto? Saber eso le permitirá alimentar sus mentes y emociones con acciones, palabras y actitudes que construirán el sistema de creencias y superarán cualquier creencia que pueda generar dudas.

Por supuesto, un ingeniero social capacitado también puede cambiar las creencias disonantes para que ya no sean inconsistentes. Aunque esto es más complicado, es una habilidad poderosa para tener. Es posible que tu apariencia no se ajuste a lo que El objetivo podría prever su pretexto. Podrías volver a pensar en el programa Doogie Howser, M.D. El problema de Doogie era que su "pretexto" de ser un médico de primer nivel nunca encajaba desde que era tan joven. Esa era una creencia disonante, pero su conocimiento y sus acciones a menudo lo llevaban a las creencias consonantes de sus "objetivos". "Al igual que en el ejemplo anterior, un ingeniero social puede alinear su pretexto con las creencias del objetivo por sus actitudes, acciones y, especialmente, su conocimiento del pretexto.

Un ejemplo de esto que recientemente vi en la vida real fue en Defcon 18. Formé parte del equipo que llevó el CTF de Ingeniería Social a Defcon. Vimos muchos concursantes que utilizaron el pretexto de un empleado interno. Cuando se le presenta una objeción como, "¿Cuál es el número de identificación de su empleado? "Un ingeniero social no calificado se pondría nervioso y no tendría una respuesta o colgaría, mientras que un ingeniero social capacitado alinearía esas creencias disonantes para el objetivo. Simplemente indicando un número de placa que encontraron en línea o utilizando otro método pudieron convencer al objetivo de que no se necesitaba información, por lo tanto, alinear el objetivo con sus creencias.

Estos puntos son respuestas muy técnicas a un problema muy simple, pero debes entender que uno solo puede hacer tantas falsificaciones. Elige tu camino sabiamente.

Practicar dialectos o expresiones

Aprender a hablar en un dialecto diferente no se puede mirar rápidamente. Dependiendo de dónde vivas, aprender un dialecto diferente o con acento puede llevarte un tiempo. Poner un acento sureño o un acento asiático puede ser muy difícil, si no imposible. Una vez que estaba en una clase de capacitación con una organización de ventas internacional y tenía algunas estadísticas que decían que el 70% de los estadounidenses prefieren escuchar a las personas con acento británico. No estoy seguro de si esa estadística es verdadera o no, pero puedo decir que disfruto del acento. Ahora, después de esa clase, escuché a muchas personas en la clase practicar sus "cheerios" y "Alo Govenors", que eran horribles. Tengo un buen amigo del Reino Unido, Jon, que se enoja mucho cuando oye a los estadounidenses que intentan usar líneas de Mary Poppins con un acento británico de imitación. Si hubiera escuchado a este grupo, él podría haber fundido un fusible.

Lo que me enseñó esa clase fue que, aunque las estadísticas podrían decir que un acento es mejor que otro para las ventas o simplemente porque puedes ser ingeniería social en el sur o en Europa, no significa que puedas poner el acento fácilmente para hacerte parecer local. . En caso de duda, tíralo. Si no puede hacer que el dialecto sea perfecto, si no puede ser natural, y si no puede ser suave, entonces no intente. Los actores usan entrenadores vocales y sesiones de entrenamiento para aprender a hablar claramente con el acento que hablan. Hay que retratar. El actor Christian Bale es de Gales, pero determinar ese hecho al escucharlo es muy difícil. No parece británico en la

mayoría de sus películas. El actor Gwyneth Paltrow adquirió un acento británico muy convincente para la película Shakespeare in Love.

La mayoría de los actores tienen instructores de dialecto que trabajarán con ellos para perfeccionar el acento objetivo. Debido a que la mayoría de los ingenieros sociales no pueden pagar un entrenador de dialectos, existen muchas publicaciones que pueden ayudarlo a aprender al menos los conceptos básicos de cómo poner un acento, como Dialects for the Stage de Evangeline Machlin. Aunque este es un libro más antiguo, Contiene muchos consejos geniales:

Encuentra ejemplos nativos del acento que quieras aprender, escuchar.

Libros como Dialects for the Stage a menudo vienen con cintas de audio llenas de Acentos para escuchar.

Intenta hablar junto con la grabación que tienes, para practicar el sonido. como esa persona

Después de que te sientas algo seguro, graba tu mismo hablando en acento para que pueda escucharlo más tarde y corregir errores.

Crea un escenario y practica tu nuevo acento con un compañero.
Aplique su acento en público para ver si a la gente le resulta creíble.

Hay innumerables dialectos y acentos, y personalmente me resulta útil escribir fonéticamente algunas de las oraciones que hablaré. Esto me permite practicar su lectura y hacer que las ideas se hundan en mi cerebro para hacer que mi acento sea más natural.

Estos consejos pueden ayudar a un ingeniero social a dominar o al menos dominar el uso de otro dialecto.

Incluso si no puede dominar otro dialecto, aprender las expresiones que se usan en el área en la que está trabajando puede marcar la diferencia. Una idea es pasar algún tiempo escuchando a las personas en público hablar entre sí. Un gran lugar para esto es un restaurante o un centro comercial, o en cualquier lugar donde pueda encontrar grupos de personas sentados y charlando. Escuche atentamente frases o palabras clave. Si los escucha en algunas conversaciones, es posible que desee encontrar una manera de Incorpore estos en su pretexto para agregar credibilidad. De nuevo, este ejercicio requiere investigación y práctica.

Usar el teléfono no debería reducir el esfuerzo del ingeniero social

En los últimos años, Internet ha llegado a dominar ciertos aspectos más “impersonales” de la ingeniería social, mientras que en los últimos días el teléfono era una parte integral de la ingeniería social. Debido a este cambio, los ingenieros manisociales no ponen la energía o el esfuerzo en el uso del teléfono que puede hacer que su éxito sea exitoso.

Este tema está aquí para mostrar que el teléfono sigue siendo una de las herramientas más poderosas del ingeniero social y el esfuerzo puesto en su uso no debe disminuir debido a la naturaleza impersonal de Internet.

A veces, cuando un ingeniero social planea un ataque telefónico, su pensamiento puede diferir porque el uso de Internet puede parecer más fácil. Tenga en cuenta que debe planear poner el mismo nivel de esfuerzo, el mismo nivel y profundidad de investigación y recopilación de información, y lo más importante, el mismo nivel de práctica en sus ataques de ingeniería social basados en el teléfono. Una vez estuve con un pequeño grupo que iba a practicar presentaciones por teléfono. Esbozamos los métodos adecuados, el tono, la velocidad, los tonos y las palabras a utilizar. Esbozamos un guión (más sobre esto en un minuto) y luego iniciamos una sesión. La primera persona hizo la llamada, se puso al teléfono con alguien y arruinó las primeras líneas. Por completo vergüenza y miedo, simplemente colgó sobre la persona. Allí hay una muy buena lección: la persona que está en el otro extremo del teléfono no tiene ni idea de lo que va a decir, por lo que realmente no puede “desordenar”.”Las sesiones de práctica pueden ayudarlo a aprender cómo manejar las” incógnitas “causadas por la alteración accidental de algo en su script que lo desorienta. Si no es tan afortunado de tener un grupo para practicar o perfeccionar estas habilidades, tendrá que ser

creativo. Intenta llamar a familiares o amigos para ver qué tan lejos Puedes conseguir manipularlos. Otra forma de practicar es grabarte como si estuvieras en el teléfono y luego reproducirlo más tarde para escuchar cómo suena.

Personalmente, creo que usar un guión delineado es muy importante. Aquí hay una ilustración: suponga que tuvo que llamar a su compañía telefónica u otra utilidad. Tal vez tramaron una factura o usted tuvo otro problema de servicio y se va a quejar. Después de que te expliques al representante, le digas lo molesta y decepcionada que estás y el representante no hace absolutamente nada por ti, ella dice algo como: "XY&Z está comprometida con un servicio excelente; ¿He respondido a todas sus preguntas hoy? "Si el esta detrás del teléfono pensó por un segundo en lo que estaba preguntando, se daría cuenta de lo tonto que es, ¿verdad? Esto es lo que sucede cuando se usa un script escrito en lugar de un esquema. Un esquema le permite a la "libertad artística creativa" moverse en la conversación y no preocuparse por lo que debe venir a continuación.

Usar el teléfono para consolidar su pretexto es uno de los métodos más rápidos dentro de la puerta de su objetivo. El teléfono le permite al ingeniero social "simular" o falsificar casi cualquier cosa. Tenga en cuenta este ejemplo: si quisiera llamarlo y fingir que estaba en una oficina bulliciosa para agregar al pretexto que estaba tratando de usar, simplemente podría capturar la pista de audio de Thriving Office (www.thrivingoffice.com/). Este sitio ofrece una pista llamada "Ocupado" y otra llamada "Muy Ocupado"."De los creadores:" Este valioso CD, que está lleno de los sonidos que la gente espera escuchar de una compañía establecida, proporciona credibilidad instantánea. ¡Es simple, efectivo y garantizado!"

Esa frase sola está llena de bondad de ingeniería social, llena de lo que la gente espera escuchar de una compañía establecida. Ya puede ver que el CD está diseñado para satisfacer las expectativas y brindar credibilidad (al menos, en la mente del objetivo, después de que se cumplan sus expectativas), por lo tanto, se crea confianza.

Además, falsificar la información del identificador de llamadas es relativamente simple. Los servicios como SpoofCard (www.spoofcard.com) o el uso de soluciones locales, permiten que un ingeniero social le diga al destinatario que está llamando desde una sede corporativa, la Casa Blanca o el banco local. Con estos servicios, usted puede falsificar el número que viene de cualquier parte del mundo.

El teléfono es una herramienta mortal para los ingenieros sociales; desarrollando los hábitos para practicar su uso y tratarlo con total respeto mejorará el conjunto de herramientas de cualquier ingeniero social para pretexting. Debido a que el teléfono es una herramienta tan mortal y no ha perdido su efectividad, debes darle el tiempo y el esfuerzo que se merece en cualquier concierto de ingeniería social.

Cuanto más simple sea el pretexto, mayor será la probabilidad de éxito

El principio de "más simple, mejor" simplemente no puede ser exagerado. Si el pretexto tiene tantos detalles intrincados que olvidarse de uno causará un fallo en la ingeniería social, probablemente fracasará. Mantener las líneas de la historia, los hechos y los detalles simples puede ayudar a construir credibilidad.

El Dr. Paul Ekman, un reconocido psicólogo e investigador en el campo del engaño humano, escribió un artículo en 1993 titulado, "Mentiras que fallan." En ese artículo dice

[t] aquí no siempre hay tiempo para preparar la línea que se debe tomar, para ensayar y memorizarla. Incluso cuando ha habido un amplio aviso previo, y se ha ideado cuidadosamente una línea falsa, es posible que el mentiroso no sea lo suficientemente inteligente como para anticipar todas las preguntas que se le pueden hacer, y para haber pensado bien cuáles deben ser sus respuestas. Incluso la inteligencia puede no ser suficiente, ya que los cambios invisibles en las circunstancias pueden traicionar una línea efectiva. E incluso cuando las circunstancias no obligan a un mentiroso a cambiar de línea, algunos mentirosos tienen problemas para recordar la línea con la que se han comprometido previamente, por lo que las nuevas preguntas no pueden responderse constantemente de manera consistente.

Este punto muy importante explica claramente por qué simple es mejor. Tratar de recordar un pretexto puede ser casi imposible si es tan complejo que su La cubierta puede ser volada por un simple error. El pretexto debe ser natural y suave. Debe ser fácil de recordar, y si te parece natural, entonces recordar los hechos o las líneas utilizadas anteriormente con el pretexto no será una tarea.

Para ilustrar lo importante que es recordar los pequeños detalles, quiero compartir una historia con usted. Érase una vez que probé mi mano en las ventas. yo estaba colocado con un gerente de ventas para aprender las cuerdas. Puedo recordar mi primera llamada con él. Condujimos hasta la casa, y antes de dejar el auto, miró la tarjeta de información y me dijo: “Recuerda, Becky Smith envió una tarjeta de solicitud para seguro suplementario. Presentaremos la política de XYZ. Mira y aprende.”

En los primeros tres minutos de la llamada de ventas, la llamó Beth y Betty. Cada vez que usaba el nombre equivocado, veía cambiar su actitud y luego decía en voz baja: “Becky”. Creo que podríamos haber estado regalando lingotes de oro y ella habría dicho que no. Estaba tan apagada que él no podía diga bien que no estaba interesada en escuchar nada.

Este escenario realmente pone de relieve el punto de mantener los hechos simples en orden.

Además de recordar los hechos, es igualmente importante mantener los detalles pequeños. Un simple pretexto permite que la historia crezca y el objetivo use su imaginación para llenar los vacíos. No intente hacer el pretexto elaborado, y sobre todo, recuerde los detalles minúsculos que marcarán la diferencia en cómo las personas ven el pretexto. Por otro lado, aquí hay un dato interesante: la táctica apopular utilizada por los criminales y estafadores famosos es cometer algunos errores a propósito. La idea es que “nadie es perfecto”, y algunos errores hacen que las personas se sientan como en casa. Tenga cuidado con los tipos de errores que decide cometer si emplea esta táctica porque agrega complejidad a su pretexto, pero hace que la conversación parezca más natural. Use este consejo con moderación, sin embargo, si decide continuar, hágalo simple.

Permítame unir todo esto con algunos ejemplos que he usado o que he visto que se usaron en las auditorías. Después de una excelente obtención en el teléfono, un ingeniero social anónimo recibió el nombre de la empresa de eliminación de residuos. Unas pocas búsquedas en Internet y tenía un logotipo utilizable e imprimible. Hay docenas de tiendas locales y en línea que imprimirán camisetas o sombreros con un logotipo.

Luego de unos minutos de alinear las cosas en una plantilla, ordenó una camisa y una gorra con el logotipo de la compañía de residuos. Un par de días más tarde, vistiendo la ropa cargada con el logotipo y cargando un portapapeles, el ingeniero social se acercó a la cabina de seguridad de la empresa objetivo.

Él dijo: “Hola, soy Joe con ABC Waste. Recibimos una llamada de su departamento de compras solicitando enviar a alguien para revisar un contenedor de basura dañado en la parte posterior. La recogida es mañana y si el contenedor no es reparable, haré que traigan uno nuevo. Pero necesito volver corriendo y inspeccionarlo “.

Sin parpadear, el oficial de seguridad dijo: “Está bien, necesitará esta credencial para estar en el sitio. Simplemente pase por aquí y conduzca por la parte de atrás y verá los contenedores allí.”

El ingeniero social tenía un pase libre para realizar una inmersión en un contenedor de basura muy largo y detallado, pero quería maximizar su potencial, por lo que se mató con esta línea. Mientras miraba su portapapeles, dijo: “La nota dice que no son los contenedores de comida, sino uno de los lugares donde va el papel o la basura tecnológica. ¿En qué bloque están los?”

“Oh, simplemente conduzca de la misma manera que le dije y están en la tercera bahía”, respondió el guardia de seguridad.

“Gracias”, dijo Joe.

Un simple pretexto, respaldado por ropa y “herramientas” (como el portapapeles), y las historias fueron fáciles de recordar y no complejas. La simplicidad y la falta de detalles hicieron que este pretexto fuera más creíble, y funcionó.

Otro pretexto muy utilizado es el del técnico de soporte técnico. Este solo requiere un polo, un par de khakis y una pequeña bolsa de herramientas para computadora. Muchos ingenieros sociales emplean esta táctica para entrar por la puerta principal porque el “técnico” generalmente tiene acceso a todo sin supervisión. Se aplican las mismas reglas: mantener la trama simple ayudará a que este pretexto en particular sea muy real y creíble.

El pretexto debe aparecer espontáneo

Hacer que el pretexto parezca espontáneo se remonta a mi punto de usar un esquema en lugar de usar un script. Los esquemas siempre le permitirán al ingeniero social más libertad y un guión hará que el ingeniero social parezca demasiado robótico. También se relaciona con el uso de elementos o historias que interesan personalmente al ingeniero social. Si cada vez que alguien te hace una pregunta o hace una declaración que te obliga a pensar, y dices "Ummmm" y empiezas a pensar profundamente, y no puedes regresar con una respuesta inteligente, arruinará tu credibilidad. Por supuesto, muchas personas piensan antes de hablar, por lo que no se trata de tener la respuesta en un segundo, sino de tener una respuesta o una razón para no tener la respuesta. Por ejemplo, En una llamada telefónica estaba Pedí una información que no tenía. Simplemente le dije: "Déjame ver eso". Luego me incliné y lo hice sonar como si estuviera gritando por un compañero de trabajo: "Jill, ¿puedes pedirle a Bill que me envíe el formulario de pedido de la cuenta XYZ? Gracias."

Luego, cuando "Jill" me estaba entregando el papel, pude obtener los datos que necesitaba y el papel nunca volvió a aparecer.

He recopilado una pequeña lista de formas en las que puedes trabajar para ser más espontáneo:

No pienses en cómo te sientes. Este punto es bueno, porque a menudo en un pretexto si piensa demasiado comenzará a agregar emoción a la mezcla, que puede causar miedo, nerviosismo o ansiedad, todo lo cual lleva al fracaso. Por otro lado, es posible que no experimente nerviosismo. o miedo, pero el exceso de emoción, que también puede hacer que usted haga mucho de errores.

No te tomes demasiado en serio. Por supuesto, este es un gran consejo en La vida, pero se aplica maravillosamente a la ingeniería social. Como seguridad Profesional tienes un trabajo serio; Este es un asunto serio. Pero si no puedes reírte de tus errores, puedes aclamarte o conseguir demasiado Nervioso por manejar una pequeña protuberancia en el camino. No te estoy sugiriendo Tomar la seguridad como una broma. En tu mente, sin embargo, si ves un potencial el fracaso como el pináculo del fracaso en tu vida, la presión que creas puede causar justo lo que más temes. Las fallas menores a menudo pueden conducir a mayor éxito si tienes la habilidad de rodar con él.

Aprende a identificar lo que es relevante. Me gusta expresar este concepto como, "Sal de tu cabeza y adéntrate en el mundo", que es un gran consejo. Un ingeniero social puede estar tratando de planificar tres pasos adelante y en el Mientras tanto, pierda un detalle vital que puede causar que el pretexto se desmorone.

Sea rápido para identificar el material relevante y la información a su alrededor, si es el lenguaje corporal del objetivo, las palabras habladas, o microexpresiones (vea el Capítulo 5 para más información sobre este tema), y asimila la información en el vector de ataque.

También tenga en cuenta que las personas pueden decir cuando alguien no está realmente escuchando lo que están diciendo. Tener la sensación de que incluso las oraciones sin importancia están cayendo en oídos sordos puede ser un desvío masivo para muchos gente. Todo el mundo ha experimentado estar con alguien que simplemente no

Parece que le importa lo que él o ella está diciendo. Tal vez esa persona incluso tuvo una Razón legítima para estar pensando en un camino diferente, pero hacerlo sigue siendo un apagar.

Asegúrate de escuchar lo que dice tu objetivo. Presta mucha atencion y tu recogerá los detalles que son muy importantes para ellos y mientras tanto, Es posible que escuches algo para ayudarte en tu éxito. Busca ganar experiencia. Este concepto se remonta a lo que quieras. Probablemente vea repetido cuatro millones de veces en este libro: la práctica.

Ganar experiencia a través de la práctica puede hacer o deshacer el pretexto. Practica la espontaneidad con familiares y amigos y extraños con Absolutamente ningún objetivo en mente sino ser espontáneo. Entablar conversaciones con personas, pero no de un modo acosador aterrador, Pequeñas conversaciones simples pueden recorrer un largo camino hacia el momento de hacerte sentir Cómodo siendo espontáneo.

Estos puntos definitivamente pueden dar a un ingeniero social la ventaja cuando se trata de pretexting. Tener la habilidad de parecer espontáneo es un regalo. Anteriormente en este capítulo mencioné mi entrevista con Tom

Mischke, quien tuvo una visión interesante de la espontaneidad. Dijo que quiere dar la ilusión de espontaneidad envuelta en la práctica y la preparación. Practicaría tanto que su pretexto saldría como una generación espontánea de humor y talento.

Proporcionar una conclusión lógica o seguimiento para el objetivo

Lo creas o no, la gente quiere que le digan qué hacer. Imagina que si fueras a un médico y él entrara, te revisara, escribiera algunas cosas en su historial y dijera: “De acuerdo; Nos vemos en un mes ”. Eso sería inaceptable. Incluso en el caso de malas noticias, la gente quiere que se les diga el siguiente paso y qué hacer.

Como ingeniero social, cuando abandonas el objetivo, es posible que necesites que actúe o no, o puede que hayas recibido lo que viniste y solo necesitas dejar. Cualquiera sea la circunstancia, al dar una conclusión o seguimiento al objetivo se llenan los vacíos esperados para el objetivo.

Al igual que si un médico lo revisara y lo enviara a casa sin instrucciones, si se abre camino en una instalación como técnico de soporte técnico y simplemente se va sin decir nada a nadie después de clonar la base de datos, deja a todos preguntándose qué sucedió. Alguien puede incluso llamar a la “compañía de soporte técnico” y preguntarle si necesita hacer algo, o en el peor de los casos, simplemente deja a los trabajadores preguntándose. De cualquier manera, dejar a todos colgando no es la manera de irse. Incluso un simple: “Revisé los servidores y reparé el sistema de archivos; debería ver un aumento del 22% en la velocidad en los próximos dos días “, deja a los objetivos con la sensación de que” tienen el valor de su dinero “.”

La parte difícil para un ingeniero social es lograr que el objetivo realice una acción después de que se haya ido. Si la acción es vital para completar la auditoría del ingeniero social, entonces puede que desee asumir ese rol. Por ejemplo, en la cuenta en el Capítulo 3 de la sesión de recopilación de información en el evento de la cámara de comercio, si quisiera que el objetivo me siguiera por correo electrónico, podría haber dicho: “Aquí está mi tarjeta; ¿Me enviará por correo electrónico algunos detalles sobre Mondayabout XYZ?”Es muy posible que se haya dado cuenta, o podría haber ido a la oficina, olvidado de mí por completo, y todo el concierto habría fracasado”. Lo que sería mejor es decir: “Me encantaría obtener más información de usted. El lunes, ¿quizás podría llamarte o enviarte un correo electrónico para obtener más detalles?”

Las peticiones que hagas deben coincidir con el pretexto, también. Si su pretexto es ser un tipo de soporte técnico, no “ordenará” a las personas con lo que deben y no deben hacer; trabajas para ellos Si usted es un repartidor de UPS, no exige acceso a la sala de servidores.

Como se mencionó anteriormente, pueden existir más pasos para perfeccionar un pretexto, pero los que se enumeran en este capítulo pueden dar a un ingeniero social una base sólida para construir un pretexto perfectamente increíble.

Es posible que se pregunte: “De acuerdo, enumeró todos estos principios, pero ¿ahora qué?” ¿Cómo puede un ingeniero social construir un pretexto simple bien investigado, creíble, de sonido espontáneo, que funcione tanto en el teléfono como en persona y obtener los resultados deseados? Sigue leyendo

Pretexto exitoso

Para aprender a construir un pretexto exitoso, eche un vistazo a un par de historias de ingenieros sociales que usaron pretextos que funcionaron y cómo los desarrollaron. Eventualmente, fueron atrapados, razón por la cual estas historias estan ahora disponible.

Ejemplo 1: StanleyMark Rifkin

Stanley Mark Rifkin es acreditado con uno de los más grandes robos a bancos en la historia de los Estados Unidos (vea un gran artículo sobre él en www.social engineer.org/wiki/archives/Hackers/hackers-Mark-Rifkin-Social-Engineer FurtherInfo.htm). Rifkin era un experto en informática que dirigía un negocio de consultoría informática desde su pequeño apartamento. Uno de sus clientes era una compañía que atendía las computadoras en SecurityPacific Bank. Las oficinas centrales de SecurityPacific National Bank en Los Ángeles, de 55 pisos, parecían una

fortaleza de granito y vidrio. Guardias de traje oscuro vagaban por el vestíbulo y las cámaras ocultas fotografiaban a los clientes mientras hacían depósitos y retiros.

Este edificio parecía impenetrable, entonces, ¿cómo es que Rifkin se fue con $ 10.2 millones y nunca sostuvo un arma, nunca tocó un dólar y nunca detuvo a nadie?

Las políticas de transferencia bancaria del banco parecían seguras. Fueron autorizados por un código numérico que cambiaba diariamente y solo se entregaba al personal autorizado. Fue publicado en una pared en una habitación segura a la que solo tenía acceso "personal autorizado".

Del artículo archivado mencionado anteriormente:

En octubre de 1978, visitó Security Pacific, donde los empleados del banco lo reconocieron fácilmente como un trabajador informático. Tomó un ascensor hasta el nivel D, donde se encontraba la sala de transferencia bancaria. Un joven agradable y amigable, logró abrirse paso hasta la habitación donde se colocaba en la pared el código secreto del día del banco. Rifkin memorizó el código y se fue sin levantar sospechas.

Pronto, los empleados del banco en la sala de transferencias recibieron una llamada telefónica de un hombre que se identificó como Mike Hansen, un empleado de la división internacional del banco. El hombre ordenó una transferencia de rutina de fondos en una cuenta en Irving Trust Company en NewYork, y proporcionó los números de código secreto para autorizar la transacción. Nada acerca de la transferencia parecía estar fuera de lo común, y Securi Pacific transfirió el dinero al banco NewYork. Lo que el funcionario del banco no sabía era que el hombre que se hacía llamar Mike Hansen era Stanley Rifkin, y había usado el código de seguridad del banco para robar al banco $ 10.2 millones.

Este escenario ofrece mucho de qué hablar, pero por ahora, enfócate en el pretexto. Piensa en los detalles de lo que tenía que hacer:

Tenía que estar seguro y cómodo para no despertar. Sospecha de estar en esa habitación.

Tenía que tener una historia creíble cuando llamó para hacer la transferencia y tener los detalles para respaldar su historia. Tenía que ser lo suficientemente espontáneo para ir con la corriente con preguntas. Que podrian haber surgido.

También tenía que ser lo suficientemente suave como para no levantar sospechas.

Este pretexto tuvo que ser meticulosamente planeado con el mayor detalle pensado. No fue hasta que visitó a un antiguo asociado que su pretexto falló, y fue capturado. Cuando lo atraparon, la gente que lo conocía se asombró y algunos incluso dijeron cosas como: "No hay forma de que él sea un ladrón; todos aman a mark"

Obviamente su pretexto era sólido. Tenía un plan bien pensado, y uno lo adivinaría, bien ensayado. Sabía para qué estaba allí y desempeñó el papel a la perfección. Cuando estuvo frente a extraños pudo hacer el papel; su caída se produjo cuando estaba con un colega que lo conocía, y ese colega vio una noticia, luego sumo 2 mas 2 y entregó a Mark.

Sorprendentemente, mientras estaba en libertad bajo fianza, Rifkin comenzó a atacar a otro banco usando el mismo esquema, pero un topo del gobierno lo había establecido; Lo atraparon y pasó ocho años en prisión federal. Aunque Mark es un "chico malo", puedes aprender mucho sobre los pretextos al leer su historia. Lo mantuvo muy simple y usó las cosas que le eran familiares para construir una buena historia.

Ejemplo 2: Hewlett-Packard

En 2006, Newsweek publicó un artículo muy interesante (www.social engineer.org/resources/book/HP_pretext.htm). Básicamente, la presidenta de HP, Patricia Dunn, contrató a un equipo de especialistas en seguridad que contrató a un equipo de investigadores privados que utilizaron pretextos para obtener registros telefónicos. Estos profesionales contratados realmente entraron y jugaron los roles de los miembros de la junta de HP y partes de la prensa. Todo esto se hizo para descubrir una supuesta fuga de información dentro de las filas de HP.

La Sra. Dunn quería obtener los registros telefónicos de los miembros de la junta y los reporteros (no los registros de las instalaciones de HP, sino los registros personales del hogar y el teléfono celular de estas personas) para verificar dónde supuso que se encontraba la fuga. El artículo de Newsweek dice:

El 18 de mayo, en las oficinas centrales de HP en Palo Alto, California, Dunn la soltó bomba en el tablero: ella había encontrado el filtrador. Segun tom Perkins, un director de HP que estuvo presente, Dunn expuso la vigilancia esquema y señaló el director infractor, que reconoció siendo la fuga de CNET. Ese director, cuyo identidad aún no ha sido Divulgado públicamente, se disculpó. Pero el director le dijo entonces a su compañero.

Directores, "les habría dicho todo sobre esto. ¿Por qué no lo preguntas?"

A ese director se le pidió que abandonara la sala de juntas, y así lo hizo, Según Perkins.

Lo que es notable sobre esta cuenta es lo que se menciona a continuación sobre el tema de pretexting:

El caso de HP específicamente también arroja otro foco de atención en las tácticas cuestionables utilizadas por los consultores de seguridad para obtener personal información. HP reconoció en un correo electrónico interno enviado desde su exterior.

El abogado de Perkins dijo que consiguió el rastro de papel que necesitaba para vincular al director y filtrar a CNET a través de una práctica controvertida llamada "pretexting"; Newsweek obtuvo una copia de ese correo electrónico. Esa práctica, según la Comisión Federal de Comercio, implica el uso de "falsas pretensiones" para obtener información personal no pública de otro individuo: registros telefónicos, Números de cuenta de banco y tarjeta de crédito, números de Seguro Social y similares.

Por lo general, digamos en el caso de una compañía telefónica, los pretextores llaman y se representan falsamente a sí mismos como el cliente; ya que las empresas rara vez requiere contraseñas, un pretexter no necesita más que una dirección de casa, Número de cuenta y súplica sincera para obtener los detalles de una cuenta.

De acuerdo con el sitio web de la Comisión Federal de Comercio, los detractores venden La información a individuos que pueden ir desde legítimos.

Investigadores privados, prestamistas financieros, litigantes potenciales, y sospechoso cónyuges a quienes podrían intentar robar activos o obtener de manera fraudulenta crédito. Pretexting, dice el sitio de la FTC, "está en contra de la ley."La FTC y Varios fiscales generales del estado han interpuesto acciones de ejecución.

contra los pretextos por supuestamente violar las leyes federales y estatales sobre fraude, Tergiversación y competencia desleal. Uno de los directores de HP es Larry.

Babbio, el presidente de Verizon, que ha presentado varias acciones contra pretexters (Si está interesado en explorarlo, la Ley de protección de privacidad y registros telefónicos de 2006 se puede encontrar en http://frwebgate.access.gpo.gov/cgi bin / getdoc.cgi? Dbname = 109_cong_bills & docid = f: h4709enr. txt.pdf.)

El resultado final fue que se presentaron cargos criminales no solo contra Dunn, sino también contra los asesores que contrató. Usted puede preguntarse, "Como es eso ¿Es posible teniendo en cuenta que fueron contratados y contratados para realizar estas pruebas?

Eche un vistazo a las vías que utilizaron y la información que obtuvieron para ayudar a responder esta pregunta. Los consultores obtuvieron los nombres, direcciones, números de Seguro Social, registros de llamadas telefónicas, registros de facturación telefónica y otra información de los miembros de la junta de HP y los reporteros. Utilizaron efectivamente el número de la Seguridad Social para establecer una cuenta en línea para un reportero y luego obtener registros de sus llamadas personales.

La página 32 de un documento confidencial de Hewlett-Packard a su abogado y personal legal interno (www.social engineer.org/resources/book/20061004hewlett6.pdf) enumera una comunicación de Tom Perkins a los miembros de la junta de HP que ofrece un poco más de información. Sobre qué pretextos se utilizaron. Algunas tácticas utilizadas fueron:

Se representaron a sí mismos como la empresa transportista para obtener el Registros de llamadas ilegales.

Las identidades de los investigados fueron utilizadas y falsificadas. para obtener sus registros de llamadas personales.

Las cuentas en línea con los portadores se generaron utilizando ilegalmente obtenido Nombres, números de Seguro Social y otra información para acceder sus registros de llamadas.

El 11 de septiembre de 2006, el Comité de Energía y Comercio de la Cámara de Representantes de los Estados Unidos le envió una carta a la Sra. Dunn (vea una copia de esta carta en www.social engineer.org/resources/book/20061004hewlett6.pdf) solicitando la información que había obtenido. En su pedido, enumeraron la información obtenida de la siguiente manera:

Facturas de tarjetas de crédito
Nombre del cliente e información de la dirección
Utilidades
Números de buscapersonas
Números de celdas
Números de seguridad social
Todos los números de teléfono publicados y no publicados.
Informes de credito
Información de la cuenta del correo
Información de la cuenta bancaria
Información del activo
Otra información del consumidor

Toda esta información se obtuvo a través de un área muy gris de la ingeniería social profesional: ¿es ético y moral lo que hicieron, aunque fueron contratados para hacerlo? Muchos ingenieros sociales profesionales no harían todo lo posible. La lección que se puede aprender de este caso tan importante es que, como ingeniero social profesional, puede imitar las metodologías y el pensamiento de los ingenieros sociales maliciosos, pero nunca debe inclinarse por completo a sus niveles. El problema con estos consultores fue que estaban autorizados para pretextar, hacer ingeniería social y auditar a Hewlett-Packard. No estaban autorizados para el ingeniero social AT&T, Verizon, empresas de servicios públicos, etc. Cuando emplee el pretexto, debe tenerlo detallado y planeado para que sepa qué líneas legales podría acercarse y qué líneas no debe cruzar.

La historia de HP se presta a una discusión sobre políticas, contratos y una descripción de lo que ofrecerá si es un auditor de ingeniería social, pero estos temas no están dentro del contexto de este capítulo. El uso de los principios descritos hasta ahora en este capítulo puede ayudarlo a tomar decisiones que lo mantendrán fuera de problemas.

El peligro de los pretextos maliciosos es la amenaza de robo de identidad, lo que lo convierte en una parte muy válida de un ingeniero social. Probar, verificar y verificar que los empleados de su cliente no se dejen engañar por los métodos utilizados por ingenieros sociales malintencionados puede hacer mucho para protegerlo de un pretexter exitoso.

Mantenerse legal

En 2005, Private Investigator Magazine recibió una entrevista con Joel Winston, Director Asociado de la Comisión Federal de Comercio (FTC), División de Prácticas Financieras. Su oficina está a cargo de regular y monitorear el uso de pretextos (vea una copia de este valioso artículo en www.social-engineer.org/resources/book/ftc_article.htm).

Estos son algunos de los puntos clave de esta entrevista:

Según la FTC, la expresión previa es la obtención de cualquier información de un banco o consumidor, no solo información financiera, mediante fraude, engaño o preguntas engañosas para obtener dicha información.

El uso de información ya obtenida para verificar que un objetivo es un objetivo, incluso cuando se usan falsos pretextos, es legal según la definición de pretexto de la FTC, a menos que el ingeniero social esté usando esta información para obtener información de una institución financiera.

La adquisición de registros telefónicos o celulares a través de prácticas comerciales engañosas se considera un pretexto ilegal. Adquirir registros telefónicos o celulares a través de negocios engañosos.

Las prácticas se consideran pretextos ilegales. El sitio web de la FTC proporciona cierta claridad e información adicional a esta entrevista:

Es ilegal que cualquiera use declaraciones falsas, ficticias o fraudulentas o documentos para obtener información del cliente de una institución financiera o directamente de un cliente de una institución financiera. Es ilegal que alguien use falsificaciones, o robos documentos para obtener información del cliente de una institución financiera o

directamente de un cliente de una institución financiera. Es ilegal que alguien le pida a otra persona que obtenga el permiso de otra persona.

Información del cliente utilizando declaraciones falsas, ficticias o fraudulentas. o utilizando documentos falsos, ficticios o fraudulentos, o falsificados, perdido, Si bien el enfoque de la FTC está en las instituciones financieras, las pautas descritas son un recordatorio de lo que se considera ilegal en los Estados Unidos. Estudiar sus leyes locales y asegurarse de que no están infringiendo esas leyes es una buena idea para los ingenieros sociales profesionales. En 2006, la Comisión Federal de Comercio decidió ampliar la Sección 5 de la Ley de la FTC para incluir específicamente una ley que prohíba el uso de pretextos para recuperar registros telefónicos.

La situación de pretextos de HP terminó cuando uno de los investigadores privados fue acusado de conspiración y robo de identidad federal, cargos muy serios. Mantener la pretexto legal implicará una investigación por parte del ingeniero social profesional, así como un plan claramente definido y firmado.

De qué pretextos, si los hay, se utilizarán.

A pesar de los asuntos legales mencionados anteriormente, usar un pretexto sólido es una de las formas más rápidas de ingresar en una empresa. Pretexting es un talento en sí mismo y, como puede ver en este capítulo, no es simplemente el uso de una peluca o un par de anteojos falsos y fingir que usted es alguien que no es.

Herramientas adicionales de pretexto

Existen otras herramientas que pueden potenciar un pretexto.

Los apoyos pueden recorrer un largo camino para convencer a un objetivo de la realidad de su pretexto; por ejemplo, señales magnéticas para su vehículo, uniformes o trajes a juego, herramientas u otros accesorios, y lo más importante, una tarjeta de presentación.

El poder de la tarjeta de visita me impactó cuando viajaba recientemente a Las Vegas por negocios. Por lo general, la bolsa de mi computadora portátil se escanea, se vuelve a escanear y luego se limpia con un hisopo en busca de polvo de bomba o lo que sea. Soy uno de esos tipos a quienes realmente no les importan las precauciones de seguridad adicionales porque evitan que explote en el aire, y estoy feliz con eso.

Sin embargo, me doy cuenta de que el 90 por ciento del tiempo voy a recibir atención adicional de la Administración de Seguridad del Transporte (TSA). En este viaje en particular, había olvidado tomar mis selecciones de bloqueo, el escáner RFID, cuatro unidades de disco duro adicionales, llaves de contacto (consulte el Capítulo 7) y una gran cantidad de dispositivos de piratería inalámbrica de mi bolso portátil. A medida que pasa por el escáner, oigo a la señora que trabaja en el x raysay, “¿Qué diablos?”Luego llama a otro caballero que mira la pantalla y dice: “No tengo ni idea de qué diablos son esas cosas”. Luego mira a su alrededor, ve mi cara sonriente y dice: “¿Eres tú?”

Me acerco a la mesa con él cuando está vaciando mi escáner RFID y mi gran caja de cerraduras y me dice: “¿Por qué tienes todos estos artículos y cuáles son?” No tenía nada planeado, pero en el último segundo decidí intentar este movimiento: Saqué una tarjeta de visita y dije: “Soy un profesional de seguridad que se especializa en pruebas de redes, edificios y personas para detectar brechas de seguridad. Estas son las herramientas de mi negocio.”Dije esto cuando le entregué una tarjeta de visita, la miró durante unos cinco segundos y luego dijo:” oh exelente Gracias por la explicación." Él metió cuidadosamente todos mis artículos, cerró la bolsa y me dejó ir. Por lo general, paso por el análisis de bombas, la pequeña máquina de polvo y luego un cacheo, pero esta vez todo lo que obtuve fue un

agradecimiento y un lanzamiento rápido. Comencé a analizar lo que hacía diferente a lo normal. La única diferencia era que le había dado una tarjeta de visita. Por supuesto, mi tarjeta de visita no es el especial de $ 9.99 de una impresora de tarjetas en línea, pero me sorprendió que lo que parecía haber sucedido era que una tarjeta de visita daba un sentido de licencia a mis reclamos.

Mis siguientes cuatro vuelos a propósito empaqué todos los dispositivos de "pirateo" en las bolsas que pude encontrar y luego guardé una tarjeta de presentación en mi bolsillo. Cada vez que examinaban mi bolsa y me preguntaban sobre el contenido, tiré la tarjeta. Cada vez que me disculpaba, tenía mis artículos empacados cuidadosamente y los soltaba.

Imagina que mi experiencia fue un pretexto. Los pequeños detalles pueden agregar tanto peso a lo que estoy diciendo que puedo parecer válido, confiable y sólido con nada más que una tarjeta que le dice a la gente que todo lo que digo es verdad. No subestimes el poder de una tarjeta de presentación. Una palabra de advertencia: obtener una tarjeta de presentación débil y de aspecto patético puede causar el efecto contrario. Una tarjeta de negocios que era "gratuita" con un anuncio en la parte posterior no agregará peso a un pretexto profesional. Sin embargo, no hay razón para gastar $ 300 en una tarjeta de negocios para usar una vez. Muchas impresoras de tarjetas de visita en línea pueden imprimir una pequeña cantidad de tarjetas muy económicas por menos de $ 100.

Otra razón para tomarse muy en serio este capítulo es que muchas veces el pretexto es el primer paso que usan los ladrones de identidad profesionales. Debido a que el robo de identidad se está quedando en primera fila en la industria del crimen en los últimos tiempos, saber qué es y cómo identificarlo es importante para los consumidores, las empresas y los profesionales de la seguridad. Si usted es un auditor de seguridad, debe ayudar a sus clientes a tomar conciencia de estas amenazas y probarlas para detectar posibles debilidades.

Resumen

Además de cubrir ampliamente los pretextos y proporcionar ejemplos reales de pretextos en acción, este capítulo también repasó continuamente Contra los principios psicológicos que afectan diferentes aspectos del pretexting. La siguiente parada lógica en el marco abarca precisamente eso: las habilidades mentales que utilizan los ingenieros sociales profesionales que los hacen parecer maestros de control mental y que le dan a cada ingeniero social una gran ventaja.

CAPITULO 5

Trucos mentales: Principios psicológicos utilizados en ingeniería social

Todo depende de cómo veamos las cosas, y no de cómo son ellas mismas.

—Carl Gustav Jung

En las películas y programas de televisión de Hollywood, estafadores y policías son retratados con talentos casi místicos. Tienen la capacidad de salirse con la suya con cualquier cosa; Parecen poder simplemente mirar a los ojos de una persona y decir si están mintiendo o diciendo la verdad. No es raro ver situaciones como esta: el policía mira a los ojos a su sospechoso y puede decir automáticamente si está mintiendo o diciendo la verdad, o solo con el poder de sugerencia que los objetivos del estafador están entregando los ahorros de su vida. Las películas pueden hacerte creer que las tácticas de manipulación y hacer que la gente haga lo que quieras es plausible o incluso fácil. ¿Son estos escenarios realmente ficticios? ¿Es posible obtener tales habilidades que se guardan para la fantasía en las películas?

Este capítulo podría ser un libro en sí mismo, pero condensaré esta información a principios que realmente cambiarán la forma en que interactúa con las personas. Algunos de los temas de este capítulo se basan en la investigación realizada por las mentes más brillantes en sus respectivos campos. Las técnicas discutidas en estos temas fueron probadas y puestas a prueba en entornos de ingeniería social. Por ejemplo, el tema de las microexpresiones se basa en la investigación del psicólogo e investigador de renombre mundial, el Dr. Paul Ekman,

quien utilizó su genio para desarrollar técnicas para leer expresiones faciales que pueden, literalmente, cambiar la aplicación de la ley, los gobiernos, los médicos y las personas comunes interactúan con los demás.

originadores de la programación neurolingüística, cambiaron la comprensión de las personas sobre los patrones de pensamiento y el poder de las palabras. Estos temas son temas de mucho debate, y este capítulo intenta desmitificar este tema y explicar cómo puede usarlos en ingeniería social.

Algunos de los mejores interrogadores del planeta desarrollaron capacitación y marcos para ayudar a las fuerzas del orden público a aprender cómo interrogar a los sospechosos de manera efectiva. Estos principios tienen raíces psicológicas tan profundas que el aprendizaje de los métodos utilizados puede, literalmente, desbloquear las puertas de las mentes de sus objetivos.

El uso de señales que las personas dan en sus discursos, gestos, ojos y caras puede hacer que parezcas un lector mental. Este capítulo examina estas habilidades y las explica en detalle para que puedan ser utilizadas por un ingeniero social profesional.

Rapport es a menudo una palabra que usan los capacitadores de ventas y los vendedores, pero es un aspecto muy importante para ganar confianza y mostrar confianza. Saber cómo desarrollar una relación con las personas al instante es una habilidad que verdaderamente mejora el conjunto de habilidades de un ingeniero social, y este capítulo le muestra cómo.

Este capítulo termina con mi propia investigación personal sobre cómo puedes usar estas habilidades para hackear la mente humana. Un desbordamiento de búfer es un programa normalmente escrito por un pirata informático para ejecutar código, normalmente con intenciones maliciosas, a través del uso normal de un programa host. Cuando se ejecuta el programa hace lo que quiere el hacker. ¿Qué pasaría si fuera posible ejecutar “comandos” en la mente humana que harían que el objetivo haga lo que pides, entregue la información que busca y, en esencia, demuestre que la mente humana puede ser manipulada?

Esta información poderosa, por supuesto, puede usarse para intenciones muy maliciosas. Mi objetivo al divulgar esta información al público de esta manera es abrir el telón de lo que hacen los "malos" al exponer sus métodos, pensamientos y principios, luego analizar cada uno y mostrar lo que puede aprender de ellos. Exponer estas técnicas hace que identificar, defender y mitigar estos ataques sea más fácil para todos.

Este capítulo es verdaderamente una colección de datos y principios que altera la mente. Siguiendo, estudiando, e investigar los métodos no solo mejorará los esfuerzos de seguridad, sino que estos principios también pueden Alterar la forma en que Comunicarse e interactuar con los demás.

Byno significa, sin embargo, que este capítulo es una colección completa que cubre todos los aspectos de cada una de estas habilidades. Proporciono enlaces y consejos sobre dónde puede encontrar más información y programas para ayudarlo a mejorar estas habilidades. Este capítulo establece una base y actúa como una guía, apuntándole en una dirección para que pueda aprender a mejorar cada habilidad con el tiempo.

Aprender habilidades de ingeniería social no es un proceso rápido, así que no seas impaciente. Los métodos para aprender algunas de estas habilidades pueden tardar años en perfeccionarse y mucha práctica incluso para llegar a ser competentes. Por supuesto, puede poseer una habilidad para cierto aspecto, pero si no lo hace, no se impaciente al tratar de aprenderlo. Sigue esforzándote más y practicando y lo conseguirás.

Antes de entrar en el tema de este capítulo, la siguiente sección establece el escenario de por qué y cómo funcionarán estos principios. Debes entender los modos de pensar que existen. Una vez que entienda más claramente cómo las personas captan y procesan la información, puede comenzar a comprender las representaciones emocionales, psicológicas y físicas de ese proceso.

Modos de pensar

Para alterar la forma de pensar de alguien, debe comprender cómo piensan las personas y en qué modos piensan. Esto parece un primer paso lógico para incluso intentar este aspecto de la ingeniería social.

Podría pensar que necesita ser un psicólogo o un neurólogo para comprender los muchos aspectos de cómo una persona puede pensar. Aunque eso puede ayudar, no es necesario. Con un poco de investigación y alguna aplicación práctica, puede profundizar en el funcionamiento interno de la mente humana.

En agosto de 2001, el FBI publicó un boletín de aplicación de la ley (www.social Engineer.org/wiki/archives/ModesOfThinking/MOT_FBI_3of5).htm) que hizo algunas declaraciones muy detalladas sobre los modos en que las personas piensan:

Simplemente confirmando su comportamiento no verbal al cliente, usando el lenguaje desde el sistema de representación preferido del cliente y el discurso correspondiente el volumen, el tono y el área del habla a menudo superan la renuencia del cliente a comunicar.

Esta simple declaración tiene mucha profundidad. Básicamente, está diciendo que primero puedes descubrir el modo de pensar dominante del objetivo y luego confirmarlo de manera sutil, puedes desbloquear las puertas de la mente del objetivo y ayudarlo a sentirse realmente cómodo cuando te cuenta incluso detalles íntimos. “¿Cómo puedo averiguar el modo de pensar dominante de un objetivo?”

Incluso preguntarle a la gente cuál es su modo de pensar no ofrecerá una respuesta clara, porque muchas personas no saben en qué modo de pensar residen. Debido a eso, como ingeniero social, debe tener algunas herramientas para ayudarlo a determinar este modo y luego Cambia rápidamente los engranajes para que coincida con ese modo. Existe un camino claro y fácil para esta respuesta, pero primero debe conocer los conceptos básicos.

Los sentidos

Durante siglos los filósofos han argumentado el valor de la percepción. Algunos van tan lejos como para decir que la realidad no es "real", sino simplemente lo que nuestros sentidos construyen en nuestras percepciones. Personalmente, no me suscribo a esa idea, pero creo que el mundo es traído a nuestro cerebro por nuestros sentidos. La gente interpreta esos sentidos por su percepción de la realidad. En la clasificación tradicional tenemos cinco sentidos: vista, oído, tacto, olfato y gusto.

Las personas tienden a favorecer uno de estos sentidos y ese es el que es dominante. También es la forma en que las personas tienden a recordar las cosas. Como un ejercicio para determinar su sentido dominante, cierre los ojos e imagine que se despierta esta mañana. ¿Cuál es la primera cosa que recuerda?

¿Era la sensación del cálido sol en tu cara? ¿O quizás recuerdas el sonido de la voz de tu cónyuge o hijos que te llama? ¿Recuerdas claramente el olor a café de abajo? ¿O posiblemente el mal sabor de boca, recordándote que debes lavarte los dientes?

Por supuesto, esta ciencia no es exacta y darse cuenta de lo que es su sentido dominante puede tomar algunos intentos para resolverlo. Una vez hablé con una pareja sobre este concepto y fue interesante observar sus expresiones. La esposa primero recordó despertarse y ver el reloj y luego preocuparse de que llegaba tarde, mientras que el marido primero recordó rodar y No sintiendo a su esposa junto a él. Después de algunas preguntas más, se hizo evidente que el marido era un kinestésico, o su sentido dominante era su sentimiento, mientras que su esposa era muy visual.

Por supuesto, acercarse a su objetivo y decir: "Cierra los ojos y dime lo primero que recuerdes esta mañana", no parece razonable. A menos que, por supuesto, su pretexto sea la reducción de la familia, podría encontrarse con alguna oposición en esta ruta.

¿Cómo puede determinar sin pasar por un interrogatorio vergonzoso acerca de sus rituales matutinos cuál es el sentido dominante de un objetivo?

Los tres modos principales de pensar

Aunque tenemos cinco sentidos, los modos de pensar están asociados con solo tres de ellos:

La vista, o un pensador visual.

Audición, o un pensador auditivo

Sensación, o un pensador kinestésico

Cada sentido tiene un rango dentro del cual funciona, o una submodalidad. ¿Es algo demasiado fuerte o demasiado suave? ¿Demasiado brillante o demasiado oscuro? ¿Demasiado calor o demasiado frío? Ejemplos de esto son los siguientes: mirar al sol es demasiado brillante, los motores a reacción son demasiado fuertes y –30 grados Fahrenheit es demasiado frío. Ivan Pavlov realizó un experimento en el que hizo sonar una campana cada vez que alimentaba a un perro. Al final, el perro oiría el sonido de la campana y luego salivaría. Lo que la mayoría de la gente no sabe es que él estaba más interesado en los aspectos físicos y emocionales de las submodalidades. El punto interesante es que cuanto más fuerte sonaba la campana, más salivaba el perro. El cambio de rango de la submodalidad produjo un cambio físico directo. La investigación de Pavlov y todas sus conferencias se discuten con mucho detalle en www.ivanpavlov.com.

Aunque las personas son muy diferentes de los perros, la investigación de Pavlov es muy importante para entender cómo piensa una persona. Muchos de nosotros podemos pensar en los tres modos, pero dominamos en uno: uno “suena” el más alto. Incluso dentro de nuestro modo dominante, podríamos tener diferentes grados de profundidad para ese sentido dominante.

A continuación discutiré algunos de los detalles de cada uno de estos modos en Más profundidad.

Visual

La mayoría de las personas suelen ser pensadores visuales, ya que normalmente recuerdan cómo se veía algo. Recuerdan claramente la escena: los colores, las texturas, el brillo o la oscuridad. Pueden visualizar claramente un evento pasado e incluso crear una imagen para un evento futuro. Cuando se les presenta material para decidir, a menudo necesitan algo que ver porque la información visual está directamente relacionada con la toma de decisiones. Muchas veces, un pensador visual tomará una decisión basándose en lo que sea visualmente atractivo para él, independientemente de lo que realmente sea "mejor" para él.

Aunque los hombres tienden a ser visuales, esto no significa que todos los hombres sean siempre visuales. El marketing visual o los aspectos visuales que normalmente atraen a los hombres son ciertos, pero no asuma que todos los hombres son visuales.

La persona avisual a menudo usa ciertas palabras en su discurso, tales como:

"Veo a que te refieres."

"Eso me parece bien".

"Me sale la imagen ahora.”

Y el rango en el que funciona el sentido dominante para un pensador visual puede tener ciertas características, o sub-modalidades, como:

Luz (brillante o tenue)

Tamaño (grande o pequeño)

Color (blanco y negro o color)

Movimiento (rápido o lento)

Enfoque (claro o brumoso)

Tratar de debatir, vender, negociar, manipular o influenciar a un pensador visual sin aportes visuales es muy difícil, si no imposible. Los pensadores visuales necesitan aportaciones visuales para tomar decisiones.

Auditivo

Los pensadores auditivos recuerdan los sonidos de un evento. Recuerdan que el La alarma fue demasiado fuerte o la mujer susurró demasiado bajo. Recuerdan la dulzura de la voz del niño o la aterradora corteza del perro. Las personas auditivas aprenden mejor de lo que oyen y pueden evitar que se les digan más cosas que se les muestren cosas.

Debido a que un pensador auditivo recuerda la forma en que sonaba algo, o porque los sonidos mismos ayudan a recordar los recuerdos, puede usar frases como:

"Alto y claro…"

"Algo me dice ..."

"Eso me suena bien."

Y el alcance de este sentido dominante puede estar dentro de estas sub-modalidades:

Volumen (alto o bajo)

Tono (base o agudo)

Pitch (alto o bajo)

Tempo (rápido o lento)

Distancia (cerca o lejos)

Es imperativo elegir sus palabras cuidadosamente con pensadores auditivos. Las palabras que escuchen harán o romperán el trato. He visto encuentros enteros que van de lo mejor a un desastre con una palabra equivocada que se habla a un pensador auditivo.

Auditivo

Los pensadores auditivos recuerdan los sonidos de un evento.