Práctica de laboratorio: Ingeniería social
Enmanuel Sanchez Rodriguez 2021-0618

Objetivo

En esta práctica de laboratorio, se investigarán ejemplos de ingeniería social y se identificarán maneras de reconocerla y evitarla.

Recursos

- Computadora con acceso a Internet

Instrucciones

Paso 1: Ejemplos de investigación en ingeniería social

La ingeniería social, en lo que se refiere a la seguridad de la información, se utiliza para describir las técnicas utilizadas por una persona (o personas) que manipulan a otros con el fin de acceder o comprometer la información sobre una organización o sus sistemas informáticos. Un ingeniero social suele ser difícil de identificar y puede afirmar ser un nuevo empleado, una persona de reparación o un investigador. El ingeniero social podría incluso ofrecer credenciales para apoyar esa identidad. Al ganar confianza y hacer preguntas, él o ella puede ser capaz de reunir suficiente información para infiltrarse en la red de una organización.

Utilice cualquier navegador de Internet para investigar incidentes de ingeniería social. Resuma tres ejemplos encontrados en su investigación.

- **El Ataque de Phishing a Google y Facebook (2013-2015):** Un estafador lituano, Evaldas Rimasauskas, engañó a empleados de Google y Facebook para que le transfirieran más de 100 millones de dólares entre 2013 y 2015. Rimasauskas se hizo pasar por un proveedor de hardware taiwanés llamado Quanta Computer, utilizando correos electrónicos de phishing y facturas falsas para convencer a los empleados de estas grandes empresas de que le debían dinero. La combinación de correos electrónicos falsos y documentos fraudulentos fue lo suficientemente convincente para que las transferencias se realizaran sin sospecha hasta que fue demasiado tarde .

- **El Ataque de Spear Phishing a RSA Security (2011):** En 2011, RSA Security, una empresa de seguridad cibernética, fue víctima de un sofisticado ataque de spear phishing. Los atacantes enviaron correos electrónicos a un grupo selecto de empleados de RSA con un archivo adjunto titulado "2011 Recruitment Plan". Cuando los empleados abrieron el archivo, un exploit en Adobe Flash permitió a los atacantes instalar una puerta trasera en los sistemas de RSA, lo que les permitió robar datos sensibles relacionados con sus productos de autenticación de dos factores SecurID. Esto comprometió gravemente la seguridad de muchos de sus clientes a nivel mundial .

- **El Ataque de Pretexting a la Compañía de Teléfonos de Kevin Mitnick (1979-1995):** Kevin Mitnick, uno de los hackers más famosos del mundo, utilizó la técnica de pretexting para obtener información de la compañía telefónica Pacific Bell y otras empresas durante su carrera como hacker. Mitnick se hacía pasar por un empleado legítimo de la compañía y utilizaba su conocimiento de la jerga técnica y los procedimientos internos para engañar a los verdaderos empleados y así obtener acceso a sistemas y datos sensibles. Este tipo de ataque subraya la importancia de la capacitación en seguridad para todos los empleados para prevenir la divulgación accidental de información sensible .

Paso 2: Reconocer los signos de la ingeniería social

Los ingenieros sociales no son más que ladrones y espías. En lugar de piratear (hackear) su camino en su red a través de Internet, intentan obtener acceso confiando en el deseo de una persona de ser complaciente. Aunque no es específico para la seguridad de la red, el escenario siguiente, descrito en el libro de Christopher Hadnagy, *The Art of Human Hacking*, ilustra cómo una persona desprevenida puede regalar involuntariamente información confidencial.

> *"El café era relativamente tranquilo, ya que yo, vestido con un traje, me senté en una mesa vacía. Puse mi maletín sobre la mesa y esperé a una víctima adecuada. Pronto, una víctima llegó con un amigo y se sentó a la mesa junto a la mía. Colocó su bolso en el asiento a su lado, tirando del asiento cerca y manteniendo su mano sobre la bolsa en todo momento.*
>
> *Después de unos minutos, su amiga se fue a buscar un baño. La marca [objetivo] estaba sola, así que le di la señal a Alex y Jess. Jugando como una pareja, Alex y Jess le preguntaron a la marca si ella le tomaría una fotografía. Ella estaba feliz de hacerlo. Sacó su mano de su bolso para tomar la cámara y tomar una fotografía de la "feliz pareja" y, mientras estaba distraída, me acerqué, tomé su bolso y la guardé dentro de mi maletín. Mi víctima aún no se había dado cuenta de que su bolso había desaparecido cuando Alex y Jess salieron del café. Alex luego fue a un estacionamiento cercano.*

No pasó mucho tiempo para que se diera cuenta que su bolso se había ido. Entró en pánico, mirando a su alrededor frenéticamente. Esto era exactamente lo que esperábamos, así que le pregunté si necesitaba ayuda.

Me preguntó si había visto algo. Le dije que no, y la convencí para que se sentara y pensara en lo que había en la bolsa. Un teléfono. Maquillaje Un poco de dinero. Y sus tarjetas de crédito. ¡Bingo!

Le pregunté con quién vino y luego le dije que trabajaba para ese banco. ¡Que golpe de suerte! Le aseguré que todo estaría bien, pero tendría que cancelar su tarjeta de crédito de inmediato. Llamé al número de "asistencia", que en realidad era Alex, y le entregué mi teléfono.

Alex estaba en una furgoneta en el estacionamiento. En el tablero, un reproductor de CD estaba reproduciendo ruidos de oficina. Le aseguró a la marca que su tarjeta podía ser cancelada fácilmente, pero, para verificar su identidad, necesitaba introducir su PIN en el teclado del teléfono que estaba usando. Mi teléfono y mi teclado.

Cuando teníamos su PIN, me fui. Si hubiésemos sido verdaderos ladrones, habríamos tenido acceso a su cuenta a través de retiros en cajeros automáticos y compras con el PIN. Afortunadamente para ella, era sólo un programa de televisión.

Recuerde: "Los que construyen muros piensan de manera diferente a aquellos que buscan ir por encima, debajo, alrededor o a través de ellos". Paul Wilson - The Real Hustle

Investigue formas para reconocer la ingeniería social. Describa tres ejemplos encontrados en su investigación.

- **Reconocimiento de Phishing a través de Correos Electrónicos Sospechosos:** Los correos electrónicos de phishing suelen contener señales reveladoras que pueden ayudar a identificarlos. Estas señales incluyen errores ortográficos y gramaticales, direcciones de correo electrónico de remitentes que no coinciden con la organización que dicen representar, enlaces sospechosos y solicitudes urgentes de información personal o financiera. Además, estos correos electrónicos a menudo crean una sensación de urgencia o temor para que el destinatario actúe rápidamente sin pensar detenidamente. Una forma de verificar la autenticidad de un correo es examinar cuidadosamente el dominio del remitente y verificar los enlaces sin hacer clic en ellos.

- **Detección de Pretexting mediante la Verificación de Identidades:** El pretexting implica que el atacante se haga pasar por alguien de confianza para obtener información. Para reconocer este tipo de ataque, es fundamental siempre verificar la identidad de la persona que solicita información sensible. Esto puede incluir hacer preguntas de verificación que solo la persona real sabría responder, o utilizar canales de comunicación alternativos para confirmar su identidad. Las empresas también pueden implementar políticas estrictas donde se requiere confirmación por parte de un superior antes de divulgar cualquier información sensible.

- **Identificación de Vishing a través de Llamadas Telefónicas Inusuales:** Vishing, o phishing por voz, es una táctica donde los atacantes llaman a sus víctimas fingiendo ser representantes de instituciones legítimas, como bancos o compañías de seguros. Para reconocer estos intentos, es importante estar alerta a llamadas no solicitadas que soliciten información personal o financiera. Los empleados deben ser capacitados para nunca proporcionar información sensible por teléfono sin verificar la identidad del llamante. Una práctica recomendada es colgar y llamar directamente a la institución utilizando un número oficial, en lugar de los proporcionados por el posible atacante durante la llamada.

En pocas palabra hay que tener cuidado hasta de lo que uno abre

Paso 3: Investigue formas de prevenir la ingeniería social

¿Su empresa o escuela tiene procedimientos para ayudar a prevenir la ingeniería social?
No, que yo sepa :n pero quizás y un día la tenga 😊

Si es así, ¿cuáles son algunos de esos procedimientos?

Utilice Internet para investigar procedimientos que otras organizaciones utilizan para evitar que los ingenieros sociales obtengan acceso a información confidencial. Enumere sus hallazgos.