Ingeniería Social

BY ZERO

Prólogo

Nota del Autor:

Yo, Darwin Alexander Silva Pérez, no me hago responsable del mal uso que se dé a la información aqui expuesta ya que su publicación tan solo es para fines informativos y didácticos.

Este es un documento de divulgación, así de simple. Me desligo totalmente de las acciones perpetradas por cualquier persona que utilice la información contenida en este documento con fines ilícitos.

Este documento es gratis y su distribución es libre. Una gran parte de la información fue elaborada apollandome en libros encontrados en internet, foros, website y conocimientos previos.

Mi facebook asi como twitter, canal de youtube y blog.

https://www.facebook.com/dawin.silva.3

@security_zero

http://www.youtube.com/user/zerndate

blog http://0byt3s.org/

Hecho con Software Libre:

- Ubuntu Gnu/Linux 13.04
- LibreOffice 1:4.0.2

Contenido

Introducción

Bueno este mini-manual esta orientado a las personas que les guste aprender cada dia mas sobre temas muy variados asi mismo surgio como iniciativa de un amigo que le gusta mucho el mundo de la informatica y en general el hacking.

El primer problema que surgio fue si era etico o no escribir este manual por lo que encontre en internet hay algunos ya escritos basados en este tema pero de pago por ello decidi escribirlo y distribuirlo de manera gratuita en este formato para su libre distribución.

Otro punto fue que algunas personas lo podran usar para fines delictivos y esa no es la intención su verdadero fin es brindar y proporcionar un medio para aprender.

Espero les guste y se diviertan leyendolo como me diverti escribiendolo un saludos y que tengan un muy buen día.

By Zero

1-Que es la ingenieria social

Bueno el concepto no estan amplio como digamos según wikipedia:

ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

Concepto según mis conocimientos:

Es el arte o tecnica de poder manipular a las personas de tal forma que podamos tener acceso a algun lugar concreto o acceso a cierta información confidencial ya sea de una empresa o una persona en concreto.

Desde el punto de vista psicologico:

Existen determinados procesos que son automáticos tanto en el ser humano como en los animales en virtud de las relaciones con los demás. Así que depende de quién lo analice y los convierta en una ventaja o una desventaja para obtener información. Estos procesos son comúnmente utilizados en campañas de mercadeo y negocios para influenciar sobre la gente.

Otras estrategias o principios de la ingeniería social se basan en rutas periféricas de persuasión en donde se utiliza la emoción como una forma de distracción.

2-Técnicas de Ingeniería Social

a)Técnicas Pasivas:

- Observación

b)Técnicas no presenciales:

- Recuperar la contraseña
- Ingeniería Social y Mail
- IRC u otros chats
- Teléfono
- Carta y fax

c)Técnicas presenciales no agresivas:

- Buscando en La basura
- Mirando por encima del hombro
- Seguimiento de personas y vehículos
- Vigilancia de Edificios
- Entrada en Hospitales
- Acreditaciones
- Ingeniería social en situaciones de crisis
- Ingeniería social en aviones y trenes de alta velocidad
- Agendas y teléfonos móviles
- Desinformación

d)Métodos agresivos

- Suplantación de personalidad
- Chantaje o extorsión
- Despersonalización
- Presión psicológica

3-Como usarla

Kevin Mitnick fundamenta las estrategias de Ingeniería Social en los siguientes **postulados**:

- Todos los seres humanos quieren ayudar
- El primer movimiento es siempre de confianza hacia el otro
- No nos gusta decir NO
- A todos nos gusta que nos alaben
- Todos tenemos algo de ingenuos

a)La primera parte es la observación no concidero que deba explicarse por obvias razones

b)Técnicas no presenciales:

Esta tecnica es de las mas basicas y sencillas de empliar ya que como no requerimos estar en presencia de la victima podemos tomarnos el tiempo necesario para realizar dicho ataque por lo tanto es mas facil estos ataques de hacen via meil,telefono,recuperación de password(famoso en facebook"fuerza bruta") y los phishing entre otros casos como usarlo pues facil por ejemplo le mandamos un link a alguien en especifico diciendo que se reporto una vulnerabilidad en tu sistema o en tu empresa y que dando click en el link puedes cerrar el bug con un parche o cosas asi,algo sencillo de hacer por ejemplo seria llamar a una oficina y pedir el numero de celular de x persona adjudcandote que eres de una de esas empresas de articulos al credito de tu pais y que te urge ese dato para brindar un articulo que cotizo la x persona que deceamos el numero ojo siempre precaber que la persona x no este en la oficina a esa hora.

c)Técnicas presenciales no agresivas:

Bueno esta tecnica es mas usada para investigar o sacar información de una empresa que a una persona se basa en buscar en la basura documentos importantes ya que siempre hay un descuidado que bota algun papel con user y password de alguien de la empresa en la basura o algun documento importante con numeros de telefono de la empresa o numeros de cuenta de ella y datos relevantes,tambien conlleva a seguir a personas o vigilar el edificio para ver hora de entrada de oficinas de salida las rondas y horas exactas de las rondas de los guardas de seguridad o incluso entrar a tu casa y robar tu agenda o algo con datos sobre ti o la entidad para la que laboras; esta medida es mas compleja ya que se requiere de mucho o poco tiempo para entrar y salir de algun lugar con la información que queremos obtener.

d)Métodos agresivos

Este es el metodo mas peligroso y debe ser usado como ultimo recurso para obtener la información que necesitamos o queremos obtener.

Este metodo consiste en falsificar documentos(es un delito) pretender ser una persona que no se es; llamar o acercarse a una persona y pedirle dicha información amenazandola con algo ya sea hacerle daño a ella o su familia o divulgar algun secreto de ella o su familia o cosas asi para obligarla a darnos información requerida.

Tips

1-Nunca dar nuestro verdadero nombre

2-Nunca llamar o mandar un correo desde nuestro numero privado o correo privado siempre hacerlo desde telefonos publicos o correos falsos.

3-Planear alguna historia con anticipación por si somos descubiertos en el acto.

4-Alejate de bancos y gobierno(gastaran millones solo para atraparte)

5-Crearnos toda una vida falsa siempre diferente para cada ataque(puedes investigar a alguna persona de la compañía o victima saber sus gustos y cosas asi finje ser todo lo que ella o el desea y dara mas facil la información).

6-Siempre ten un plan b y c por si falla tu primer plan

7-Nunca te confies al 100% de las personas que atacaras

8-Empieza practicando con personas que encuentres en las calles(no conocidas).

4-pasos

1. **Identificar a la Victima**- En esta área se comprende la psicología de la víctima, y de ser necesario, el ingeniero social se convierte en una persona totalmente distinta a fin de agradarle y obtener la información que desea.

2. **Reconocimiento**-No es otra cosa que obtener información de la víctima.

    1. Ahora bien, ¿dónde obtenemos información de la víctima? La obtención de información se puede realizar mediante sitios Web, bases de datos, grupos de noticias, socios de negocios, “dumpster diving” búsqueda en la basura.

    2. Existe una herramienta que para mí es una de las más poderosas y se llama: **Facebook**. Al visitar los perfiles de Facebook, uno puede darse cuenta que la mayoría de las personas no se toman la molestia de manejar su perfil como privado, sino que al contrario, lo dejan como público. Gracias a estos “muros” de datos personales encontramos información como nombre, fecha de nacimiento, lugar de nacimiento, escuelas donde estudió, empresas en las que ha laborado, amistades e incluso fotografías.

    3. Telefónicamente, el atacante se hace pasar por otra persona o sorprende en su buena fe al usuario aprovechándose de su ignorancia o inocencia, y así consigue información importante.

    4. **3-Crear el escenario**-Una vez estudiado cuidadosamente quién es la víctima, se procede a crear un escenario creíble en el cual participarán la víctima y el ingeniero social. La parte más importante de un ataque es la creación del escenario que dará pie al ataque en sí.Este escenario puede ser una situación por teléfono, puede ser una aparición física al área de trabajo, puede ser a través de Internet en fin existen diversos medios para crear el escenario del ataque.

    5. **Realizar el taque**- Por supuesto la realización del ataque supone que se conocen de ante mano toda la información necesaria para llevarlo a cabo sin dejar rastros.

    6. **Obtener la información**- Una vez se obtiene la información deseada solo procede a salir.

    7. **Salir** –Finalmente el salir implica el borrado de huellas, de modo que no queden evidencias de que se estuvo allí.

5-Practicas

1-Encontrarte alguien po la calle con un reloj preguntar la hora y despues que te la den decir a ese reloj es de tal marca y ellos diran la marca que es(las personas tienden a corregir a los demas)

2-Buscar guia telefonica de tu pais y encontrar una empresa o negocio pequeño llamar y preguntar por x persona inventada si asiertas en el nombre pues cuando te la pasen haste pasar por alguna compañía o banco que te gustaria tener su numero de celualar y sus datos por si surge algun cargo ya que la recomendaron o tu inventas otra historia si no haciertas con el nombre preguntar quienes trabajan alli ya que posiblemente te dieron el segundo nombre no el primero(Si fallas en todo no hay problema es practica para mejorar capacidad de inventar y convencer a la gente)

3-Alguna persona x acercartele y decirle que si por casualidad no trabaja en lugar x ya que su rostro se te hace conocido posiblemente te diga que no o puede que te diga donde trabaja si le sigues metiendo platica.

4-Disfrazate o ponte ropa muy vieja y viaja a un lugar x lejos de tu casa y personas y busca alguien en las paradas diciendole que te acaban de asaltar si no puede darte algo para el bus (haste notar agotado o cansado o a punto de llorar) te daran el money (las personas tienden a ayudar a los desanparados si no le das tiempo de pensar solo habla tu con mucha angustia)te lo daran te lo aseguro no pidas mucho.

5-Trata de ir algun barrio investiga algun nombre de alguien de ese barrio; ve a una venta y di que necesitas yo que se un jugo,leche o medicamento y di que te manda esa persona que esta enferma que te lo de fiado que en un rato vuelves a pagarselo.

6-Prestale a alguien un cel diciendo que te han robado o no tienes forma de volver a tu casa puede que tengas unas llamadas gratis xd no abuses del time o sospecharan(muestrate super agobiado).

7-hablale a lguien en un restaurante o comideria asumiendo que ella o el es alguien aquien esperas cuando ella o el diga que no es finje tristesa y diciendo que te han dejado plantado otra ves hay personas que tienen a escucharte si sufres y asi le sacas el numero de cel a ella o a el si te gusta.

Bueno puedes inventarte mas situaciones y poco a poco escala en nivel de riesgo con el time podras crear mil y un historias en un segundo y así obtener lo que deceas.

Eso es todo espero les guste y sirva saludos by zero.