Fortalecimiento del eslabón más débil de la cadena de seguridad informática

Cristo Emmanuel Santos Sierra
cristosantos@gmail.com
Universidad Piloto de Colombia

Resumen- Tal vez una de las mayores vulnerabilidades que siempre ha tenido la seguridad de la información ha sido lo que se denomina Ingeniería Social. Este siempre ha sido un mecanismo bastante ingenioso, que le ha permitido a muchos piratas informáticos, la obtención de información a través de la manipulación de los usuarios que usan algún tipo de información. Por más legítimo que sea el usuario, es una técnica que puede usar cualquier clase de persona. El objetivo de la ingeniería social, es y siempre ha sido, engañar a la gente que revele información que pueda comprometer la seguridad del sistema que puede algún tipo de objetivo.

Abstract- one of the biggest vulnerabilities always had the security of the information has been what is called Social Engineering. This has always been a rather ingenious mechanism, which has enabled many hackers obtaining information through the manipulation of users who use any information system. For more legatine than the user, is a technique that can use any type of people. The purpose of social engineering is and always has been, to trick people into revealing passwords or other information that might compromise the security of any system can be some kind objective.

Palabras claves: — ingeniería social, Seguridad informática, internet, red social, ataque, técnica, código malicioso, rapport, usuario, configuración, acceso, victima, pendrive.

I. INTRODUCCIÓN

La ingeniería social, es una de las más antiguas técnicas que han usado las personas para la obtención de información, acceso e incluso privilegios del sistema de información. Generalmente, este tipo de personas buscan dichos recursos para realizar acciones que puedan perjudicar alguna persona, cosa u organización (llámese empresa, estado, hogar, etc.). Actualmente, las organizaciones que son conscientes de este problema, buscan concientizar a las personas que hacen parte de su personal (directa o indirectamente), para que las personas inescrupulosas las puedan perjudicar. Los expertos afirman, que la mayoría de los ataques en la historia han sido exitosos mediante esta técnica, por lo que además aseguran que "el factor humano es el eslabón más débil de la cadena" ( ). También se dice, que los ingenieros sociales, por lo general son muy buenos en su trabajo estafando personas, que buscan por medio de la manipulación y persuasión, alguien que les puede ayudar a traspasar alguna medida de seguridad que este impuesta en el sistema. Es decir, los ingenieros sociales, buscan que las personas "actúen en contra de su propio sentido común sin darse cuenta" [1]

Quizá el ataque más simple pero efectivo sea engañar a un usuario llevándolo a pensar que el sistema está solicitando una contraseña para varios propósitos legítimos. Los usuarios de sistemas de internet

[1] http://espanol.tdbank.com/exc/html/security_glossary.html

frecuentemente reciben mensajes que solicitan contraseñas o información de tipo personal, con el motivo de "reactivar algún tipo de configuración", u otra operación benéfica para el usuario.

Los usuarios de estos sistemas deberían ser advertidos temprana y frecuentemente para que no divulguen ningún tipo de información sensible al personal que dice ser alguna clase de administrador, En realidad los administradores de sistemas informáticos nunca necesitan saber las contraseñas de los usuarios para poder llevar a cabo sus tareas. Sin embargo incluso este tipo de ataque podría no ser necesario – en una encuesta realizada por Boixnet, el 90% de los empleados de la estación de Waterkii de _Londres revelo sus contraseñas a cambio de un bolígrafo barato.

Otro ejemplo contemporáneo de un ataque de ingeniería social es el uso de archivos adjuntos en e-mails, ofreciendo fotos "intimas" de alguna persona famosa, o algún programa "gratis" (a menudo aparentemente convenientes por personas conocidas), pero ejecutan código malicioso. Luego de que los primeros e-mails maliciosos llevaron a los proveedores de software a deshabilitar la ejecución automática de archivos adjuntos, los usuarios deben activar esos archivos de forma explícita para que ocurra algún tipo de acción maliciosa.

Muchos usuarios, sin embargo abren ciegamente cualquier tipo de archivo adjunto concretando de esta forma algún tipo de posible ataque. Obviamente no se pretende sustentar las técnicas que tengan que ver mucho con sistemas de hardware o software, por el contrario, se pretende es sustentar al lector con las herramientas y técnicas que van más allá de las mismas.

Quizá en estos momentos usted está diciendo que no le pasaría algo así. Un ejemplo claro es el acontecimiento de hace un par de años, en el que estuvo de moda los exploits más conocidos como falsas postales que se enviaban de un email y que a la hora de hacer clic lo reenviaban a otra página de Hotmail en la que nuevamente se le solicitaba al usuario algún tipo de autenticación y así poder mirar la postal que le enviaron. Este tipo de sucesos solo lleva a preguntarse a sí mismo, caíste en la trampa? Cuantos picaron el anzuelo?

Kevin Mitnick es una leyenda viva de la ingeniería social, escribió un libro llamado "The art of deception". Como gran parte de admiradores de este personaje de la ingeniería social, puede ser indignante con todo lo relacionado con el tema, pero a su vez puede ser muy útil dependiendo de los objetivos propios del lector.

II. UN POCO DE HISTORIA

Kevin Mitnick es uno de los hackers y phreackers más famoso de los Estados unidos. Su Nick o apodo fue el Cóndor. Su último arresto se produjo el 15 de febrero de 1995, tras ser acusado de entrar en algunos de los ordenadores más seguros de éste país. Ya había sido procesado en 1981, 1983, 1987 por diversos delitos informáticos.

El caso de Mitnick (su ultimo encarcelamiento) alcanzo una gran popularidad entre los medios estadounidenses por su lentitud del proceso (hasta la celebración del juicio pasaron más de dos años), y las estrictas condiciones de encarcelamiento a las que estaba sometido (se le aisló del resto de los presos y se le prohibió realizar llamadas telefónicas por su supuesta peligrosidad).

Tras su libertad en 2002, Kevin Mitnick se dedica a la consultoría y el asesoramiento en materia de seguridad, a través de su compañía Mitnick Security (anteriormente llamada Defensive thinking).

Kevin Mitnick se dedica a la consultoría desde la óptica particular de la ingeniería

social, considera que más allá de las técnicas de hardware y software que se pueden implementar, el factor determinante de la seguridad es la capacidad del usuario de interpretar correctamente las políticas de seguridad.

La vida de Kevin Mitnick y, en especial, la persecución que condujo a su captura en 1995 han dado lugar a multitud de libros y otros materiales de ficción. De entre todos, destaca la novela takedown, que relata su ultimo arresto.

El 27 de mayo del 2005 relato en Buenos Aires, en una de sus conferencias, el modo a través del cual pudo acceder fácilmente al código de un teléfono móvil en desarrollo, incluso antes de su anuncio en el mercado y con tan solo 6 llamadas telefónicas y en escasos minutos.

III. HERRAMIENTAS

A. Teléfono

En la práctica, un ingeniero social suele usar el teléfono para engañar a la gente. Esto lo hacen para que sus rostros no puedan ser identificados, y además les facilita fingir ante la víctima, haciéndose pasar por otro tipo de persona (clientes, empleados de la misma entidad, etc.).

B. Internet

Por medio del internet, al igual que el teléfono pueden hacer cualquier tipo de suplantación. Esto lo logran generalmente por medio de renovación de permisos, correos resteo o recuperación de contraseñas.

Incluso por medio de las nuevas redes sociales, proveen tanta información a este tipo de personas, que para ellos ahora le es más fácil recolectar información de alguna víctima.

A su vez utilizan correos electrónicos dicientes con el fin de persuadir la atención de la víctima y comenzar una relación de confianza que se ve más estrecha en el momento en el que el atacante solicita realizar comunicación a través de los chats en donde la comunicación se puede realizar de manera más ágil, por lo cual el atacante tiene más posibilidades de adquirir información valiosa.

C. La basura.

Muchas veces la gente arroja a la basura datos que son vitales para la integridad del sistema de información. Por ejemplo, muchas veces sin darse cuenta pueden haber tirado a la basura listados telefónicos, organigramas, manuales de sistemas, contraseñas, cuentas bancarias e incluso medios magnéticos, que les permitan a los delincuentes obtener información ultra sensible del sistema y de la compañía. El modus operandy de esta técnica radica en buscar directamente sobre los archivos de la víctima desechados que se ocultan en la papelera de reciclaje o incluso realizan recuperación de datos para obtener los archivos borrados en los últimos días.

D. Ingeniería social reversa.

Ocurre cuando el delincuente crea un rol de autoridad, en el que se encuentra, de tal modo que le pedirán información a él y no al revés. Para ser más claro. Se sustentara un ejemplo con el que se ha visto muchas veces en las novelas o películas que ven las personas todos los días. Primero el hacker SABOTEA un sistema. Entonces el mismo aprovecha la situación para auto promoverse y hacerse parecer que él es el más apropiado para dar solución al problema. Esto le permite, hacer parecer que da asistencia a un problema, y lo cual hace que requiera pedazos de información de algunas personas. Y así, de esta manera, substrae

tanta información como le es posible. Si nos damos cuenta, nadie sabe que el delincuente obtuvo lo que quiso, haciéndolo de una manera bastante sutil.

E. Carisma.

Este también es uno de los factores que se usan los atacantes para su beneficio. Para esto, suelen usar modales amistosos que les haga parecer como una persona correcta. En otros casos suelen adular a la víctima para ganar de alguna manera información, por medio de conversaciones que generan interés.

IV. CLASIFICACIÓN DE INGENIERO SOCIALES

A. Políticos

Utilizan las palabras, el entorno y el cuerpo para transmitir información a la sociedad. Pero previo a esto, tienden en apoyarse de textos previamente supervisados, escenarios bien diseñados y eslóganes claros y concisos.

B. Phreakers

Usan palabras e información privilegiada que les ayuda a engañar y a extraer más información de aquellas personas inocentes, creando vínculos de confianza y explotando elementos rutinarios que son considerados como un problema.

C. Scammers, crackers, phishers

Estos tienden a ser los ciberdelincuentes que utilizan ingeniería social como herramienta para ataques cibernéticos y lograr algún tipo específico.

V. CICLO DE LA INGENIERÍA SOCIAL

ACCIÓN	CANTIDAD
Investigación	Se extrae toda la información posible contenida en cualquier medio que esté disponible en su momento tales como formularios, revistas, informes, entradas de prensa, contenido en internet, la basura, etc.
Desarrolló de rapport y credibilidad	Se usa la información interna. Se reemplazan identidades, se reclama la víctima, se solicita ayuda o se usa la autoridad
Explotar confianza	Se pregunta o se consigue que te pregunten, hasta conseguir el objetivo del mercado
Utilización de información	Se compila la información. Si no es suficiente se vuelve a empezar el ciclo

Tabla 1. Ciclo de vida de la ingeniería social según [a]Kevin Mitnick
Fuente: "Ingenieria social: psicología aplicada a la seguridad informática"

Como se puede observar la tabla anterior es bastante simple, pero eso no implica poca eficacia. Generalmente es lo que hace un atacante, buscar información, crear confianza y utilizarla. Esto hace que los elementos principales de un escenario de ingeniería social sean los siguientes:

A. Atacante

Persona con algún objetivo en particular que tiene la tendencia de ejecutar la acción.

B. Medio

Es la vía de comunicación. Suele ser personal, telefónico o por chat, o en los más raros casos por correo

C. Victima

Es la persona que ejecuta las acciones que

el atacante desea sin conocimiento de la situación

D. Pretexto

Generalmente es algún tipo de historia que pretende convencer a la víctima. Esto ayuda a ganar credibilidad en la forma de lo que se dice y como se dice. Acá influye demasiado la información recopilada, su análisis y el momento justo en cómo se usar

VI. UN VIRUS FAMOSO: "I LOVE YOU"

Con el fin de dar a conocer uno de los casos más populares que no solo implica a personas, si no también máquinas, fue un virus que infecto millones de ordenadores enviándose a sí mismo a través de correos y chat. Este es un ejemplo sencillo, pero muy completo dado que este se alimenta de diferentes factores sociales para propagarse. De igual manera su complejidad no es muy avanzada.

El viernes 4 de mayo de 2000, el virus se libera infectando máquinas y propagándose entre los usuarios que usan un sistema operativos Windows. El día 5 de mayo se reportan otras variantes que muestran diferentes usos. En pocos meses se reportaron más de 30 casos, en la que algunos, el código tenia alteración para su optimización. El día 8 de Mayo, el N.B.I. (National Bureau of investigation), colaborando con la Interpol arresto a Reonel Ramones de 27 años, como sospechoso principal. El día 11 de Mayo, Ine de Guzmán, de 24 años, reporto que él había desarrollado un proyecto de tesis muy similar. Finalmente, cuando se intentó arrestar a Reonel por delitos relacionados con robo de contraseñas, no se pudo llevar a cabo, gracias a las leyes Filipinas, la cual indica que la pena por descubrir malware no es un delito. Tres meses después nace la conocida ley de comercio electrónico para tal fin.

VII. ANÁLISIS DEL VIRUS

A continuación se demostrara un poco los factores psico-sociales, y un poco de explicación técnica que intentan aclarar algunas de las características más relevantes del virus.

A. Código Fuente

El lenguaje del virus es Visual Basic de Microsoft Windows, un lenguaje interpretado. Todos los usuarios infectados disponían del código. Igualmente se puede descargar de http://www.therockgarden.ca/security/love_letter.txt [16/11/2010].

El sistema de interpretación de texto, el cual es ejecutado por Visual Basic, estaba activado por defecto en todas las ediciones del sistema operativo Windows. Dicha característica era desconocida por la sociedad, a esto se le agrega la falta de políticas de seguridad en la separación de permisos.

B. Ocultamiento de la extensión

El virus aprovechaba que el sistema ocultaba la última extensión de los archivos. Esto es debido a que el sistema leía de derecha a izquierda hasta el primer punto y lo ocultaba a la vista del usuario. Esto da la sensación que el nombre del archivo es el texto. Igualmente en el icono de los archivos con extensión ".vbs" era similar al del tipo ".txt".

C. Propagación a través del correo

El medio principal de propagación del virus fue el correo electrónico hacia uso de

una función encargada de leer la libreta de contactos de Microsoft Outlook enviando un correo masivo a todos los contactos de la víctima. Esta acción solo se ejecutaba una vez.

```
set male=out.CreateItem(0)
male.Recipients.Add(malead)
male.Subject = "ILOVEYOU"
male.Body = vbcrlf&"kindly check the attached LOVELETTER coming from me."
male.Attachments.Add(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
male.Send
```

Fig. 1: código de creación para el nuevo correo
Fuente: "Ingenieria social: psicología aplicada a la seguridad informática"

D. Ocultamiento de la extensión

Por último, el virus hacia un recorrido de todo el contenido del disco duro y modificaba ciertos archivos con una extensión especifica (VBS, JS, JSE, CSS, WSH, SCT, HTA, JPG, JPEG, MP3 y MP2). Un caso especial era el ejecutable del cliente de chat. Esta acción la realizaba a través de la modificación del archivo "script.ini"el cual contiene las acciones predeterminadas del cliente, y añadía la función de enviarse a sí mismo en versión HTM como si fuera un archivo web.

```
scriptini.WriteLine "n0=on 1:JOIN:#:{"
scriptini.WriteLine "n1=  /if ( $nick == $me ) { halt }"
scriptini.WriteLine "n2=  /.dcc send $nick "&dirsystem&"\LOVE-LETTER-FOR-
YOU.HTM"
scriptini.WriteLine "n3=}"
```

Fig. 2: Código de programación
Fuente: "Ingenieria social: psicología aplicada a la seguridad informática"

E. Psicología: procedencia y contenido

Si un usuario recibe un correo y este a su vez contiene un adjunto, el usuario común tiende a revisar su contenido para ver de qué trata. Esto hace que el sistema operativo actué interpretando su contenido. La falta de advertencia del peligro que podía significar la ejecución de código malicioso no percataba al usuario de los riesgos que conlleva mirar el contenido adjunto del correo, por lo que llevaba al inevitable peligro del estado del sistema. Actualmente los sistemas operativos Microsoft (como es el caso de Windows 7) arroja la ventana solicitando permisos del administrador del sistema. Esto no elimina virus o troyanos, pero si dificulta un poco más su propagación. Como el medio era el chat o el correo, tiende a aparentar para el usuario que un contacto conocido solamente quiere compartir algo. Normalmente se cree que ninguno de los contactos tiene tendencias a enviar algo perjudicial, por lo que tendía a saltarse la duda de su comprobación. Esta falsa sensación también se puede dar por la popularidad en el uso de alguna aplicación. Generalmente se piensa que es segura ya que alguien la abra revisado y evaluado en su momento, en búsqueda de la verificación de malware.

VIII.ERRORES DEL ATACANTE

Se podría decir que el atacante cometió dos errores. El primero, utilizar código de otra persona. El autor salió a relucir en defensa propia, lo cual redujo el número de culpables por origen de publicación. El vínculo principal fue que ambos habían compartido la misma facultad. El segundo error (y sin duda uno de los más comunes), fue el afán de popularidad o protagonismo. El culpable añadió datos personales que se podían identificar.

```
REM  barok -loveletter(vbe) <i hate go to school>
REM by: spyder / ispyder@mail.com / @GRAMMERSoft Group /
Manila,Philippines
```

```
<META NAME="Generator" CONTENT="BAROK VBS - LOVELETTER">
<META NAME="Author" CONTENT="spyder / ispyder@mail.com / @GRAMMERSoft
Group / Manila, Philippines / March 2000">
<META NAME="Description" CONTENT="simple but i think this is good...">
```

Fig. 3: Código de programación
Fuente: "Ingenieria social: psicología aplicada a la seguridad informática"

Para terminar hay que resaltar a la

sociedad que nunca se está exento de ataques mientras el equipo tenga algún contacto con el entorno de la red. Siempre es recomendable seguir los consejos de los expertos que se encargan de estudiar cada una de las técnicas y sus posibles adaptaciones que pueden llegar a afectar nuestros entornos.

La evolución de las técnicas de ataques y defensa, siempre viven en un constante cambio a la vanguardia de la tecnología.

A pesar de ser un hecho histórico bastante relevante, han existido diferentes virus con el mismo comportamiento, pero igualmente la gente sigue cayendo en la trampa de estos individuos.

IX.SOCIAL ENGINEERING TOLLKIT

Es una herramienta desarrollada para agilizar patrones de ataques relacionados en la Ingeniería Social. Esta herramienta ya ha logrado un reconocimiento por los profesionales de la seguridad informática. Generalmente se complementa con Metasploit, la cual es una herramienta bastante completa, que permite enviar payloads, es decir ciertas acciones específicas por el programador.

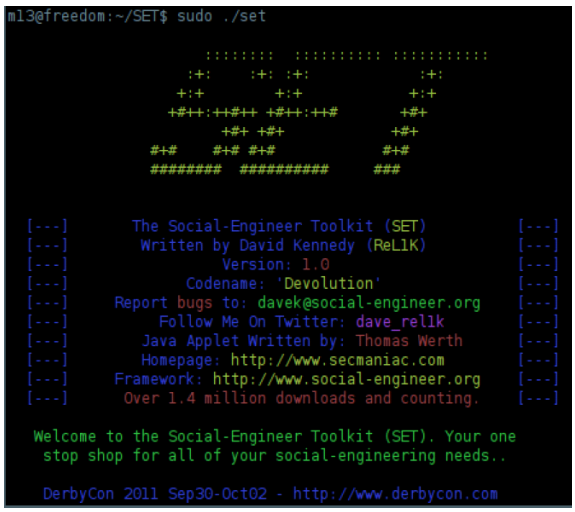

Fig. 4: Ilustración de la herramienta
Fuente: El autor

A. Phishing

La herramienta proporciona un sistema avanzado con capacidad de ser personalizado a partir de plantillas, incrustar ficheros adjuntos, etc. Permite hasta manipular la dirección del remitente en caso de contar con un servidor de correo.

B. Website Attack Vector

Es un conjunto de técnicas que atacan el navegador desde una web vulnerable. Las cosas que permite la herramienta son las siguientes:

- Infección a través de un applet Java
- Explota y payloads
- Recolección de credenciales por BeEF
- Tabnapping
- Man Left in the Middle
- Webbugs
- Clonación de paginas

C. Infectous Media Generator

Permite crear los archivos necesarios para hacer CDs, USBs, y DVDs auto infectables. Esta opción es un poco obsoleta, ya que los sistemas operativos de la actualidad (Windows 7 en adelante) tienen desactivada ciertas opciones por defecto.

D. Creador de Payloads y listeners

Cuando se usa Metasploit, se es capaz de crear ejecutables con cierto tipo de opciones. Normalmente se usa el ejecutable para enviarse a través del correo o subirlo a una página web para que sea descargado.

E. Teensy USB HID

Este permite la programación de la placa Teensy, un circuito programable con forma

visual similar a la de un pendrive. Este permite transformarse en un teclado, un mouse y/o una memoria interna, escribiendo código malicioso y su ejecución simulándolo como si fuera el usuario quien lo escribiera. Ofrece una suite de plantillas programables en lenguajes como PowerShell y WScript. También permite la posibilidad de BeEF. Afecta a cualquier sistema que permita la conexión de USB sin confirmación.

F. Browser Explotation Framework (BEeF)

Es una herramienta web usada por los profesionales de la seguridad informática, para extraer información del navegador que lo carga. Esto es muy interesante si se Es una herramienta web usada por los profesionales de la seguridad informática, para extraer información del navegador que lo carga. Esto es muy interesante si se plantea seleccionar un grupo concreto entre muchas víctimas.

La herramienta dispone de las siguientes opciones:

- Configuración de módulos extra personalizados.
- Registro de las teclas pulsadas por la victima
- Escaneo de puertos de otras redes con varias víctimas.
- Integración con Metasploit por XML-RPC
- Detección de módulos del navegador

X.ÉTICA DE LA INGENIERÍA SOCIAL

Dado que siempre hay peligro, la seguridad informática se refugia mucho sobre el análisis de riesgo. Pero como última instancia, siempre queda la ética personal, la cual puede hacer que se reporte una vulnerabilidad en vez de aprovecharla.

El elemento más importante de la seguridad informática es el personaje que tenga el conocimiento para realizar un determinado ataque. En el caso de un auditor profesional, como la metodología O.S.S.T.M.M, tiene una sección específica que se menciona su uso ético. En algunos casos se presentan buenos samaritanos que reportan las vulnerabilidades a la compañía. Cualquier organización debería agradecer que se le reporten los problemas existentes y no tratar al individuo como delincuente, siempre y cuando no haya utilizado los hallazgos para fines ilegales.

El problema hoy en día, es como realizar una prueba de concepto éticamente correcta. Hay que tener claros los datos que se van a observar, como se recogen y cuales se acaban mostrando. También, hay que valorar hasta qué punto se va a afectar a una persona poniéndola en una situación comprometida, aunque solo sea de prueba. Además es posible que el sujeto amparado por la prueba pueda denunciar al investigador, si éste causa algún perjuicio, aun sin intensión.

A parte del dilema de la ética, también influencia la edad de las personas. Cada uno ve la tecnología con diferentes ojos, y cada uno le da un diferente valor. Lo importante es tener claro lo que se puede y no se puede hacer, pero igualmente saber el porqué.

XI.METODOLOGÍA O.S.S.T.M.M.

El significado de las siglas es “Open Source Security Testing Methodology Manual”. Es una metodología abierta para conocer la seguridad de cualquier organización. El único costo que éste implica es la utilización del sello oficial. Esta metodología se enfoca especialmente en los detalles técnicos de los elementos que requieran ser probados, que hacer antes y después de la prueba de seguridad.

Los fundamentos que persigue la O.S.S.T.M.M. son:

- Qué testear. Localizar los objetivos adecuados.
- Cómo testearlos. Localizar la entrada y salida de información.
- Identificar los diferentes tipos de control existentes.
- Qué se queda sin testear.

XII.DEFENSA.

A parte del dilema de la ética, también influencia la edad de las personas. Cada uno ve la tecnología con diferentes ojos, y cada uno le da un diferente valor. Lo importante es tener claro lo que se puede y no se puede hacer, pero igualmente saber el porqué:

- Hay que recordar que una actitud cautelosa es la mejor defensa que pueda tener frente a delincuentes.

- Tenga cuidado revisando constantemente a qué tipo de personas ayuda y en que la está ayudando. Procure que este escudo, no se vuelva en contra suya volviéndolo paranoico.

- Siempre este pendiente de mirar con quien habla, y no se deje llevar tan fácil por la conversación, en especial cuando le están preguntando por datos relevantes del sistema. Recuerde que los datos relevantes, no son solo factores de hardware y software también pueden ser cosas rutinarias como horas periódicas de backup.

- Al teléfono. Obtenga nombres e identificaciones, que le permitan corroborar autenticidad de la identidad de la persona con la que está hablando.

- No se deje descrestar por el aparente conocimiento de una persona desconocida. Recuerde que muchos pueden aparentar saber mucho para solicitarle información que realmente no necesita.

- Evite responder mensajes de las cadenas de correos electrónicos.

- Evite aceptar a personas que no conoce en redes sociales.

- Evite aceptar a personas que no conoce en redes sociales.

- No revele información privada en entornos web como chats o foros.

XII.COMO IDENTIFICAR UN INGENIERO SOCIAL.

Generalmente, este tipo de personas buscan pasar desapercibidos y aparentar que son gente buena por medio de una presentación.

Estas personas siempre actúan con calma para transmitir seguridad de lo que se esté sucediendo.

Tiene una clara perspectiva de los protocolos sociales, y buscan usarlos para manipulación de las personas.

Ordinariamente demuestran un perfil que emita confianza para su propio beneficio.

También tratan de manipular personas

menos agradecidas y en general a todos aquellos que se consideran a sí mismos con poca validación social.

Son personas que hablan y confunden o son persuasivos con mucha facilidad.

Y lo más importante, siempre le dirán lo que usted espera oír de ellos.

XII.CONCLUSIONES

El secreto de cómo obtener la información, está en cómo se obtiene la información. Si nos damos cuenta, los ingenieros sociales nunca obligan a las víctimas de revelar la información, solamente se encargan de generarles algún sentimiento que puede proporcionarles alguna especie de satisfacción.

De todas maneras también pueden intimar a sus víctimas de alguna manera, suplantando alguna identidad que les permita hacer uso del abuso. Recordemos que en nuestro país, somos ajenos a este problema, y además se han visto casos donde roban a personas por medio del dialogo.

Las victimas tienden a caer por la falta de conocimiento de la ingeniería social. Generalmente este tipo de personas, tienden a tener un perfil de inocencia y cooperación hacia las otras personas.

La seguridad informática debe tender a mirar más allá del sentido común con respecto a la parte técnica. La ingeniería social es y será una técnica que puede ser utilizada por cualquier tipo de persona, y que además, tiende a mejorar con la práctica. Esta es la técnica con mayor adaptabilidad orientada hacia su objetivo. Y aun que es importante identificar aquellos elementos que contribuyeron con el ataque, los casos nunca se repetirán.

La gente aún sigue con falta de conciencia por el uso de las herramientas que se encuentran en la web. No son conscientes que al navegar por el internet están expuestos a cualquier tipo de ataque.

REFERENCIAS

[1] Kevin D. Mitnick & William L. Simon. The Art of Deception: Controlling the Human Element of Security 1st. John Wiley & Sons, Inc., New York, NY, USA

[2] Joe Chappele. Hackers 2: Takedown. (Película) Wilmington, North Carolina, USA, 2000

[3] http://www.subliminalhacking.net/ social [Visto 2013-04-09].

[4] Peter Bright. Anonymous speaks: the inside story of the HBGary hack. Ars Technica, Feb 2011. URL http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-storyof- the-hbgary-hack.ars/3 [Visto 2013-04-13]

[5] Diccionario de la lengua española. Definición. Real Academia Española, 2011. URL http://rae.es/social [Visto 2013-04-09].

[6] BBC News. Love Bug suspect held. News, (Monday) 8 May, 2000. URL http://news.bbc.co.uk/2/hi/science/nature/740623.stm [Visto 2013-04-30]

[7] TheRegister News. No 'sorry' from Love Bug author. News, 11 May, 2005. URL http://www.theregister.co.uk/2005/05/11/love_bug_author/ [Visto 2013-04-30]

[8] BBC News. Police close in on Love Bug culprit. News, (Saturday) 6 May, 2000. URL http://news.bbc.co.uk/2/hi/science/nature/738537.stm [Visto 2013-04-29]

[9] HeadQuarters United States Army Forces Command. FORSCOM "ILOVEYOU" Virus Lessons Learned Report. Department of the army, July 2000. URL http://www.iwar.org.uk/iwar/resources/call/love.pdf [Visto 2013-04-28]

[10] Anónimo. Vulnerabilidades en ListaRobinson.es. SecurityByDefault, octubre de 2010. URL http://www.securitybydefault.com/2010/10/vulnerabilidades-en-listarobinsones.html [Visto 2013-04-30]

[11] Johnny Long. No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Syngress (February 21, 2008). ISBN 978-1597492157.

Universidad Piloto de Colombia. Cristo Emmanuel Santos Sierra. Fortalecimiento del eslabón más débil de la cadena de seguridad informática

Autores

Cristo Emmanuel Santos Sierra
Ingeniero de sistemas de La Escuela Colombiana de Ingeniería "Julio Garavito" tarjeta profesional numero: 25255194030CND, Estudiante de la universidad Piloto de Colombia en el programa de especialización de seguridad informática.