GUÍAS PRÁCTICAS PARA USO DE TÉCNICAS DE INGENIERÍA SOCIAL CON LA HERRAMIENTA SET INCLUIDA EN LA DISTRIBUCIÓN BACKTRACK 4 R2

AUTORES:
CARMEN LUCIA PEDRAZA GARZÓN
VIVIANA ANDREA CAVIEDES FIGUEROA

CORPORACION UNIVERSITARIA MINUTO DE DIOS
FACULTAD DE INGENIERÍA
TECNOLOGÍA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMÁTICA

BOGOTA, COLOMBIA 2011

Guías prácticas para uso de técnicas de ingeniería social con la herramienta SET incluida en la distribución BackTrack 4 R2

CARMEN LUCIA PEDRAZA GARZÓN
VIVIANA ANDREA CAVIEDES FIGUEROA

Tesis De Grado Para Obtener El Titulo De
TECNOLOGO EN REDES Y SEGURIDAD INFORMATICA

Director:
ING. FEDERICO GACHARNA

Área
SEGURIDAD DE LA INFORMACIÓN

CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS
FACULTAD DE INGENIERÍA
TECNOLOGÍA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMÁTICA

BOGOTÁ DC.
2011

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Jurado

_____

Jurado

_____

Jurado

A los __ días del mes _____ del año ____. Bogotá DC.

"El tiempo es el mejor autor: siempre encuentra un final perfecto"

Charles Chaplin (1889 – 1977). Actor inglés.

"Cuando más buena es el alma de un hombre, menos sospecha la maldad en los otros".

Seneca

DEDICATORIA

A mis padres, por creer y confiar en mis decisiones, a mi hermano por la energía y fuerza que me da para nunca rendirme y en general a todo mi núcleo familiar y amigos por que con su amor y apoyo me llenan de motivación.

Andrea Caviedes.

A toda mi familia, especialmente a mis padres y a mi abuelita materna por darme una carrera para mi futuro, por creer en mí, brindarme toda su ayuda y sabios consejos, a mis amigos por apoyarme en cuanto proyecto emprendo. A todos mil gracias han sido una bendición en mi vida.

Lucia Pedraza.

AGRADECIMIENTOS

En primera medida queremos agradecerle a Dios por permitirnos llegar a este momento tan importante en nuestras vidas. Igualmente le queremos agradecer a todas las personas que se vieron involucradas de alguna manera en este proyecto y especialmente a nuestro director Ing. Federico Gacharna, por su a apoyo, sus apreciados y relevantes aporte, criticas, comentarios y sugerencias durante el proceso de desarrollo del proyecto, también al Ing. Fabián Valero que aunque no pudo culminar con el proceso del proyecto nos colaboro en su momento.

CONTENIDO

RESUMEN

En la actualidad la seguridad informática se ha convertido en un tema importante del ámbito tecnológico. Por ello, se busca cuidar en un mayor nivel, la información personal y empresarial, se han identificado distintos tipos de ataques, para conseguir información sensible. La ingeniería social es sin duda la técnica más poderosa para lograr este cometido, ya que a través de manipulación y engaños se logra que un usuario autorizado revele información que, compromete al sistema. Para realizar este tipo de ataques existe SET, que es un kit de herramientas diseñado específicamente para realizar ataques de ingeniería social, su objetivo principal es hacer que el usuario sea tentado a realizar una acción necesaria para dañar el sistema, como por ejemplo abrir un archivo adjunto o abrir una página web aparentemente legitima, pero en realidad falsa.

En el presente documento se analiza la importancia de la seguridad de la información, basada en el factor humano como mayor vulnerabilidad, y proponiendo acciones para contrarrestar la ingeniería social.

ABSTRACT

Today computer security has become an important issue of the technology. Therefore, it seeks a higher level care, personal and business information, we have identified different types of attacks, to obtain sensitive information. Social engineering is arguably the most powerful technique to achieve this goal, as through manipulation and deception is accomplished by an authorized user to disclose information that compromises the system. To perform this type of attack exists SET, which is a toolkit designed specifically for social engineering attacks, its main goal is to make the user is tempted to perform an action necessary to damage the system, such as opening a file enclosed or open a web page appears legitimate, but actually false.

This paper discusses the importance of information security based on human factors such as increased vulnerability, and propose actions to counter social engineering.

INTRODUCCIÓN

“Aunque se dice que el único ordenador seguro es el que está desenchufado, un ingeniero social siempre se encargara de convencer a alguien para que lo enchufe”**.** Conferencista congreso "Access All Areas" de 1997.

La seguridad informática tiene por objetivo principal asegurar que los datos que se almacenan magnéticamente, se mantengan confidenciales, íntegros y disponibles, pero ¿Qué hacer cuando la vulnerabilidad más inminente y peligrosa de este activo es el mismo usuario? Existen varias técnicas y métodos usados para obtener datos, accesos o privilegios de un sistema informático con el fin de manipular o exponer información sensible de una organización o persona, la mayoría de veces quienes las ejecutan requieren grandes conocimientos técnicos y amplia experiencia para que los ataques sean efectivos, sin embargo, la técnica más usada para este fin, es la ingeniería social ya que omite cualquier cuestión técnica y se basa en el aprovechamiento de errores y omisiones del usuario, para conseguir por medio de engaños, la información deseada.

Sucumbir ante la ingeniería social es difícil de evitar pero no imposible. Aunque es una vulnerabilidad universal debido a que cualquier equipo depende del factor humano, se debe tener en cuenta que lo más importante, es educar y capacitar a los usuarios, tomando en consideración las políticas de seguridad suministradas por la dirección de la organización.

I. DESCRIPCIÓN DEL PROBLEMA

Actualmente es evidente la importancia de software que incluya aplicaciones para realizar test de seguridad y análisis forense informático, por esta razón existe BackTrack[1], (distribución libre de Linux), que fue diseñada para ser utilizada en auditorías de seguridad y ajustada específicamente para no dejar registros de sus actividades. Incluye múltiples herramientas para realizar test de penetración, entre las que se destaca SET. Social engineering toolkit, se programo para ser liberado con el lanzamiento del sitio web http://www.social-engineer.org, y se ha convertido rápidamente en una herramienta estándar, un arsenal de test de penetración que incorpora múltiples ataques. Fue liberado en Septiembre de 2009 y se ha actualizado hasta la versión 1.3.5.

A pesar de ser una herramienta potente, carece de documentación adecuada que explique detalladamente los ataques. Comúnmente, los tutoriales se encuentran alojados en foros, manejan conceptos técnicos complejos, no están redactados para principiantes y se encuentran en diferentes idiomas, creando así una problemática de uso.

Por tanto, se propone elaborar guías prácticas con el fin de solucionar la escasa documentación, se pretende ayudar a personas interesadas en la herramienta de ingeniería social SET[2] ofreciendo una solución útil a principiantes, estudiantes, profesionales e investigadores, teniendo presente que el mundo de la seguridad informática y la información avanza constantemente.

---

[1] Web oficial: http://www.backtrack-linux.org/?lang=es

[2] Kit de herramientas de la ingeniería social, que sirve para realizar ataques automatizados y cuenta con algunos métodos como la clonación de sitios web.

I.1 Formulación de pregunta

¿Cómo construir una serie de guías prácticas en español, que ilustre la forma correcta en que, se instala, configura, implementa y usa la herramienta de ingeniería social SET contenida en BackTrack 4 R2, y que sea comprensible para la mayoría de usuarios?

II. ANTECEDENTES

Como es evidente, la mayoría de desarrolladores de herramientas y live cd de auditoría de seguridad informática, se encargan de generar las aplicaciones y no manuales de usuario. Los escasos manuales están hechos por comunidades, y no redactados para principiantes y están disponibles en idiomas diferentes al del interesado.

En el caso de la documentación de SET y BackTrack, se encuentran manuales y video-tutoriales de la configuración inicial:

- Descargar Backtrack 4 R2 (2 Ago. 2010), Consultado el 3 de Septiembre de 2010, de http://www.dragonjar.org/descargar-backtrack-4-r1.xhtml

- Video Tutorial BackTrack: Booteo, Interfaz Gráfica y Directorios (23 Jul. 2009) Consultado el 3 de Septiembre de 2010, de http://labs.dragonjar.org/video-tutorial-backtrack-booteo-interfaz-grafica-y-directorios

- BackTrack 4 – Instalación en disco duro, (n. d.), Consultado el 3 de Septiembre de 2010, de http://www.backtrack-linux.org/tutorials/backtrack-hard-drive-install/?lang=es

- Instalar BackTrack 4 Live USB, (n. d.), Consultado el 3 de Septiembre de 2010, de http://www.backtrack-linux.org/tutorials/usb-live-install/?lang=es

- SET Tutorials: Intro, (n. d.), Consultado el 3 de Septiembre de 2010, de http://www.social-engineer.org/resources/settuts/01.html

- LoganWHD, (n. d.), Social Engineering Tools, Videos and Resources: Malicious PDF Email Attack, Consultado el 3 de Septiembre de 2010, de http://www.social-engineer.org/resources/Social-Engineering-Email-Attack-using-SET/Social-Engineering-Email-Attack-using-SET.html

- LoganWHD, (n. d.), Social Engineering Tools, Videos and Resources: Phishing using SET, Consultado el 3 de Septiembre de 2010, de http://www.social-engineer.org/resources/Phishing-Social-Engineer-Toolkit/Phishing-Social-Engineer-Toolkit.html

III. OBJETIVOS

III.1 Objetivo General

Realizar guías prácticas que faciliten la instalación, configuración implementación y uso de la herramienta de ingeniería social SET contenida en BackTrack 4 R2 documentando los ataques SPEAR-PHISHING y WEBSITE ATTACK VECTORS con el fin de contribuir con la poca documentación disponible en Español e igualmente para que sirva de documento preventivo, teniendo en cuenta que al momento de consultarlas se identificara las posibles formas de ser víctima de estos ataques.

III.2 Objetivo Específicos

- Determinar cuáles opciones de las herramientas del kit serán documentadas.
- Explicar detalladamente el proceso de las técnicas de spear-phishing y website attack vectors, para lograr: suplantar una página web y conseguir información sensible.
- Realizar las pruebas en ambientes controlados sin infringir la ley.
- Publicar las guías para que estén a disposición de personas sin conocimiento avanzado en el área de seguridad informática y de la información, logrando prevenir a cualquier usuario para que no sea víctima de la ingeniería social.

IV.3 ALCANCE Y LIMITACIONES.

Debe advertirse que en el desarrollo del proyecto, no se incurrió en conductas delictivas y se tuvo siempre en cuenta la legislación vigente en Colombia como las conductas e infracciones contempladas en el Código Penal, la Ley 1273 de 2009 (de la protección de la información y de los datos), la ley 842 de 2003 (Ley de Ética del Ingeniero).

Asimismo un documento habilitante[3] en donde se especifica que está permitida la realización de dichas pruebas. El documento habilitante fue establecido por medio de una carta de autorización concedida por la empresa SADEXIM S.A.S.

En el proceso del desarrollo de las pruebas técnicas, se crearon cuentas de correo electrónico de prueba, y en ningún caso se atacaron sitios diferentes a los permitidos. No se causaron daños ni perjuicios en infraestructuras o bienes ajenos ya que fueron realizados en ambientes controlados.

La finalidad de las guías, es describir el vector de ataque de spear-phishing y website attack vectors, más no como tomar control del sistema informático del objetivo. Entre sus funciones esta:

- Demostrar la metodología y los vectores de ataque, para prevenir ser víctima de ellos.
- Permitir la comprensión, evitando tecnicismos en la elaboración de las guías.

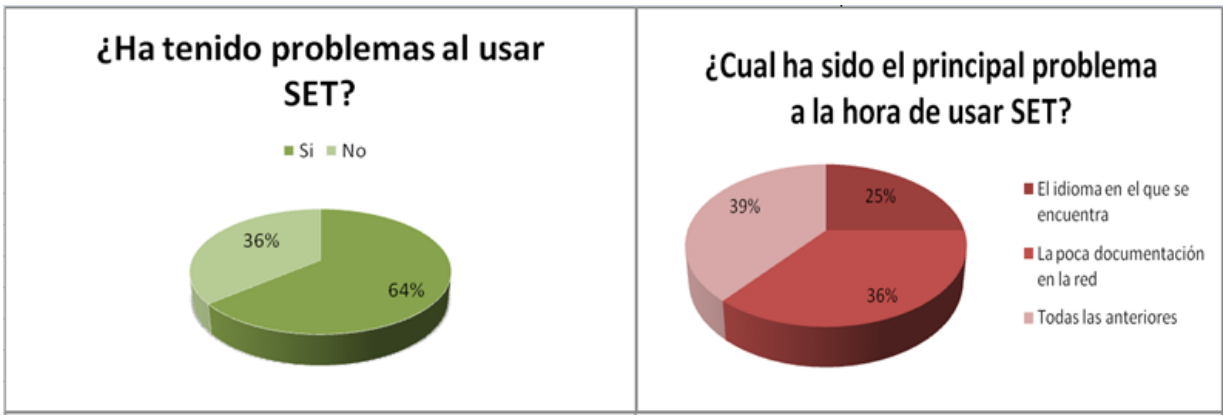
[3] Ver Anexo 2

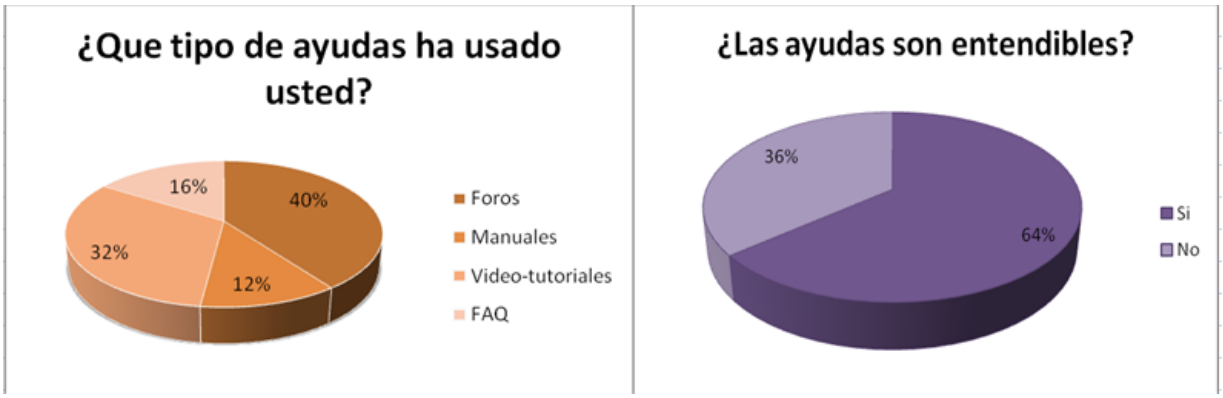
Estas guías están dirigidas a informáticos, técnicos y auditores de seguridad, administradores de red y de sistemas, responsables de TI y al público en general, para que puedan conocer los factores que alteran la seguridad, privacidad de los datos y puedan tomar medidas para evitar ataques de ingeniería social y los perjuicios que implican

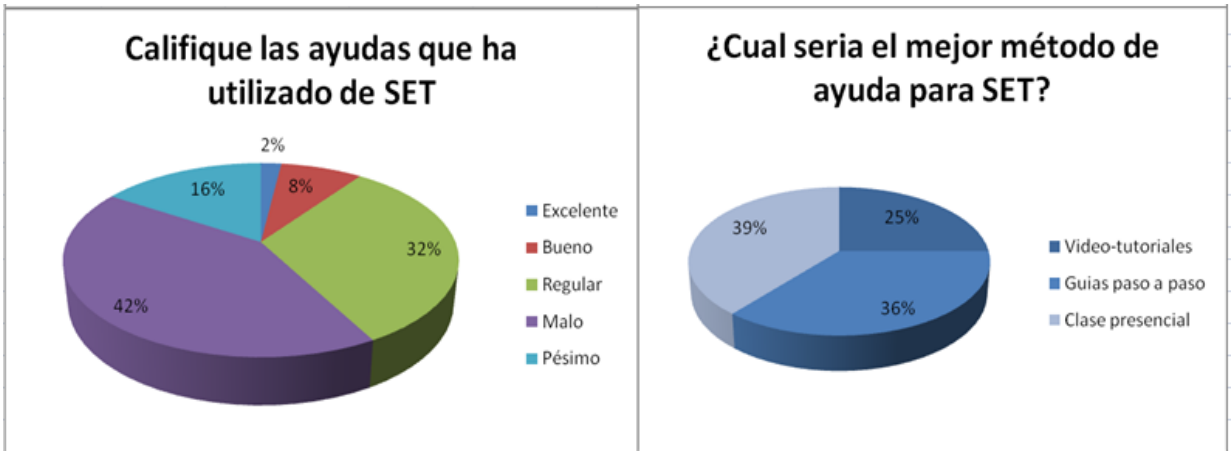
V.3 JUSTIFICACIÓN

Con datos recabados en investigaciones previas, se identificó que la mayoría de información se encuentra en otros idiomas y la poca documentación disponible en español está incompleta o redactada para personas con conocimientos previos en el tema. Además, se realizó una encuesta[4] a 250 personas conocedoras e interesadas en SET, de forma presencial y mediante un formulario web* en 3 universidades: Corporación universitaria Minuto de Dios, Universidad Católica, Universidad Pedagógica, con el fin de verificar la problemática real del uso de la herramienta. Los resultados obtenidos son los siguientes:

[4] Ver anexo







A partir de los resultados adquiridos, se propuso elaborar guías prácticas para darle solución a la problemática de no tener documentación adecuada y unificada acerca de las herramientas de ingeniería social contenidas en la última versión de BackTrack 4 R2.

Las guías pretenden describir el manejo de las herramientas de SET, con el fin de beneficiar a la sociedad compartiéndolas para que puedan ser estudiadas, consultadas y así mismo usadas como mecanismo de precaución frente a estas técnicas. De igual forma a la Corporación Universitaria Minuto de Dios, porque fortalecerá la línea de investigación de seguridad informática, y así, podrá ser utilizado de antecedente para los futuros trabajos de grado orientados a esta temática.

Igualmente, buscan proporcionar los elementos que puedan alterar la seguridad y privacidad de los datos. Se espera el mejor uso de estas, ya que fueron realizadas con fines educativos y pretenden generar la documentación faltante.

VI.3 MARCO DE REFERENCIA

VI.1 MARCO TEÓRICO

VI.1.1 SEGURIDAD INFORMÁTICA

Es un conjunto de actividades destinadas a identificar, proteger, y prevenir, aquello considerado como susceptible[5] de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

Para que un sistema pueda ser definido como seguro debe cumplir con los siguientes componentes:

- **Integridad:** Se debe garantizar que los datos no son modificados por personal no autorizado, y son consistentes y verídicos.

[5] Información sensible, aquella cuya difusión puede comprometer la seguridad y convertirse en un punto de exposición innecesario.

- **Confidencialidad:** A través de métodos como el cifrado se debe garantizar que la información pueda ser accesada únicamente por usuarios autorizados.
- **Disponibilidad:** Los datos deben estar disponibles siempre, de tal modo que quienes tengan acceso legítimo a la información puedan consultarla en el momento en que así se requiera.
- **No repudiación:** No se puede negar la autoría, el remitente debe ser quien dice ser. Es decir, un emisor de un mensaje no puede negar que lo generó y viceversa.
- **Observancia:** Cuando la información relacionada con las acciones y actividades de los usuarios (personas o procesos) se encuentra debidamente registrada y monitoreada. Adicionalmente, la administración de la seguridad y accesos privilegiados también son monitoreados. La observancia promueve el adecuado funcionamiento de todo el modelo de seguridad informática.
- **Control de acceso:** Es la habilidad de permitir o denegar el acceso a sistemas informáticos específicos y recursos, pueden ser usados para cuidar recursos físicos y recursos lógicos.

Dependiendo de la naturaleza de la amenaza existen dos tipos de seguridad:

- **Seguridad física:** consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"***. Se refiere a los controles y mecanismos de seguridad de equipos y los medios de acceso remoto hacia y desde el mismo (cámaras de seguridad, mantenimiento eléctrico, anti-incendio, humedad), implementados para proteger los equipos. Este tipo de seguridad está enfocado a

cubrir amenazas ocasionadas por el hombre y la naturaleza, del ambiente físico en que se encuentran los equipos.

- **Seguridad lógica:** consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo"**.

VI.1.2 POLÍTICAS DE SEGURIDAD

Conjunto de requisitos definidos por responsables de un sistema, que indican lo que está o no permitido para mantener segura la información. Igualmente se convierten en medio para concienciar al personal sobre la importancia de la información y servicios críticos que pueden verse afectados por uso inadecuado de los sistemas.

Básicamente, una política de seguridad hace la descripción de lo que se desea proteger y el por qué de ello, cada política es una invitación a reconocer la información como activo principal. Por tal razón, estas deben tener una posición consciente y vigilante del personal en cuanto al uso, limitaciones de los recursos y servicios informáticos, para asegurar los cuatro aspectos fundamentales de la seguridad información que son: disponibilidad, integridad y confidencialidad.

Es importante que al momento de redactar políticas de seguridad se tenga en cuenta, emplear derechos de acceso a datos y recursos con herramientas de control y mecanismos de identificación, ya que permiten verificar que sólo se tengan los permisos asignados. Algunas Técnicas para asegurar el sistema, pueden ser: Codificar la información (Criptografía, contraseñas difíciles), Vigilancia de red, Zona desmilitarizada, Tecnologías repelentes o protectoras (cortafuegos, sistema de detección de intrusos - antispyware, Antivirus), Mantener los sistemas de información con las últimas actualizaciones, Sistema de Respaldo Remoto, Servicio de BackUp remoto.

Otro punto importante que abarca las políticas de seguridad es la capacitación a usuarios de vulnerabilidades de servicios informáticos, ya que las políticas son una forma de comunicarse con los usuarios con recomendaciones como:

- No ejecutar un programa de procedencia desconocida.
- No informar telefónicamente de las características técnicas de la red.
- Nunca tirar documentación técnica a la basura, sino destruirla.
- Verificar previamente la veracidad de la fuente que solicite cualquier información sobre la red.
- No proporcionar cuentas de correo electrónico y otros datos personales a personas u entidades que puedan utilizar estos con otros fines.
- Utilizar claves de acceso complejas.

Claramente las decisiones en cuanto a políticas de seguridad, determinan que tan segura estará la información, y el nivel de funcionalidad que ofrecerá.

VI.1.3 INGENIERÍA SOCIAL

Es un conjunto de técnicas psicológicas y habilidades sociales que permiten que las personas realicen voluntariamente acciones que normalmente no harían. Se vale de errores y fallas en la seguridad informática. Tiene tres tipos. El primero, técnicas pasivas como lo es la observación; el segundo, técnicas no presenciales como el uso del teléfono, carta, fax o mail; y el tercero, técnicas presenciales que a su vez tiene dos tipos: las agresivas y las no agresivas. Las agresivas son el uso de suplantación de identidad, extorsión o presión psicológica. Y las no agresivas como la búsqueda en la basura (Dumpster Diving), mirar por encima del hombro (Shoulder Sourfing), el seguimiento de personas, entre otras.

Existen herramientas y técnicas creadas con el fin de atraer usuarios a determinadas páginas donde se les ofrece algún producto ilícitamente, otros con el fin de llevarlos engañados a una página web idéntica a la de algún banco, o entidad que permita hacer pagos por Internet, donde se solicita al usuario ingresar sus datos personales para utilizarlos de manera ilegal.

Estas herramientas pueden ser usadas para recopilación de información de sospechosos o delincuentes.

VI.1.4 TÉCNICAS DE ATAQUE

DENEGACIÓN DE SERVICIOS: tiene como objetivo imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. Por lo general,

este tipo de ataques está dirigido a los servidores de una compañía, para que no puedan utilizarse ni consultarse, puede afectar a cualquier servidor conectado a Internet. Su objetivo no reside en recuperar ni alterar datos, sino en dañar la reputación de las compañías con presencia en Internet y potencialmente impedir el desarrollo normal de sus actividades en caso de que éstas se basen en un sistema informático.

La mayoría de los ataques de denegación de servicio aprovechan las vulnerabilidades relacionadas con la implementación de un protocolo TCP/IP modelo.

Generalmente, estos ataques se dividen en dos clases:

- Las denegaciones de servicio por saturación, que saturan un equipo con solicitudes para que no pueda responder a las solicitudes reales.
- Las denegaciones de servicio por explotación de vulnerabilidades, que aprovechan una vulnerabilidad en el sistema para volverlo inestable. Los ataques por denegación de servicio envían paquetes IP o datos de tamaños o formatos atípicos que saturan los equipos de destino o los vuelven inestables y, por lo tanto, impiden el funcionamiento normal de los servicios de red que brindan.

Cuando varios equipos activan una denegación de servicio, el proceso se conoce como "sistema distribuido de denegación de servicio" (DDOS, Distributed Denial of Service).

FUERZA BRUTA: se caracteriza por una tentativa continuada de obtener acceso a un servicio del sistema (ssh, smtp, http, etc.), intentando diversas combinaciones de nombre del usuario y su contraseña. Para llevar a cabo este ataque, el atacante puede usar un

software que gestiona diversas combinaciones de caracteres o basarse en una lista de palabras (diccionario).

En ambos casos, un ataque de este género es un ávido consumidor de recursos y potencialmente bastante peligroso, especialmente si los usuarios del sistema no tienen un mínimo de cuidado al elegir sus contraseñas.

MAN IN THE MIDDLE: es un ataque en donde se intercepta los mensajes en un intercambio de claves públicas y luego se retransmite, sustituyendo su propia clave pública para el atacante, por lo que las dos partes iniciales aún parecen estar comunicándose entre sí.

El ataque debe su nombre al juego de pelota donde dos personas tratan de lanzar un balón directamente el uno al otro, mientras que una persona de entre ellos lo intenta capturar. En un MAN IN THE MIDDLE, el intruso utiliza un programa que parece ser el servidor al cliente y parece ser que el cliente al servidor. El ataque puede ser usado simplemente para tener acceso al mensaje, o permitir al atacante modificar el mensaje antes de retransmitirlo.

PHARMING: consiste en manipular las direcciones DNS (Domain Name Server) que utiliza el usuario. Los servidores DNS son los encargados de conducir a los usuarios a la página que desean ver. Pero a través de esta acción, los ladrones de datos consiguen que las páginas visitadas no se correspondan con las auténticas, sino con otras creadas para recabar datos confidenciales, sobre todo relacionadas con la banca online.

A través del “pharming”, cuando el usuario teclea en su navegador la dirección de la página a la que quiere acceder, en realidad puede ser enviado a otra creada por el

hacker, que tiene el mismo aspecto que la original. Así, el internauta introducirá sus datos confidenciales sin ningún temor, sin saber que los está remitiendo a un delincuente.

El pharming puede tener algunas similitudes con las estafas de phishing que se llevan a cabo a través del correo electrónico, aunque las primeras resultan más insidiosas, dado que pueden desviar al usuario a un sitio falso sin que aquél participe o tenga conocimiento de ello.

SPOOFING: se conoce como la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque es: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado.

BOMBAS LÓGICAS: ataque con fines maliciosos que se ejecuta un día especifico, en una hora específica, etc, y que puede ejecutar modificaciones como borrado de un disco duro, entre otras acciones.

WARDRIVING: ataque usado para crackear contraseñas de redes inalámbricas. Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como un ordenador portátil o un PDA. El método es realmente simple: el atacante simplemente pasea con el dispositivo móvil y en el momento en que detecta la existencia de la red, se realiza un análisis de la misma.

Para realizar el Wardriving se necesitan realmente pocos recursos. Los más habituales son un ordenador portátil con una tarjeta inalámbrica, un dispositivo GPS para ubicar el

PDA en un mapa y el software apropiado (AirSnort para Linux, BSD- AriTools para BSD o NetStumbler para Windows).

WARCHALKING: Se trata de un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que 'pasen por allí'.

PHISHING: es una forma de engañar a los usuarios para que revelen información personal o financiera mediante un mensaje de correo electrónico o sitio web fraudulento. Normalmente, una estafa por suplantación de identidad empieza con un mensaje de correo electrónico que parece un comunicado oficial de una fuente de confianza, como un banco, una compañía de tarjeta de crédito o un comerciante en línea reconocido. En el mensaje de correo electrónico, se dirige a los destinatarios a un sitio web fraudulento, donde se les pide que proporcionen sus datos personales, como un número de cuenta o una contraseña. Después, esta información se usa para el robo de identidad.

TROYANOS: código malicioso que se ejecuta sin que la víctima se dé cuenta, permite el acceso remoto del atacante al computador víctima, denegaciones de servicio, robo de contraseñas y usuarios, entre otras.

BUFFER OVERFLOW: Es un error de sistema causado por un defecto de programación, de tal forma que el programa que lo sufre pretende escribir más información en el buffer (unidad de memoria) de la que este puede alojar.

Este desbordamiento es posible porque el autor del programa no incluyó el código necesario para comprobar el tamaño y capacidad del buffer en relación con el volumen de datos que tiene que alojar.

Los problemas comienzan cuando el exceso de datos se escribe en otras posiciones de memoria, con la perdida de los datos anteriores.

Si entre los datos perdidos por la sobre escritura se encuentran rutinas o procedimientos necesarios para el funcionamiento del programa que se está ejecutando, el programa dará error.

Cuando la memoria de un programa llega a sobrescribir en forma aleatoria, el programa generalmente se colgará.

SQL INJECTION: consiste en la inserción directa de código en variables especificadas por el usuario que se concatenan con comandos SQL y se ejecutan. Existe un ataque menos directo que inyecta código dañino en cadenas que están destinadas a almacenarse en una tabla o como metadatos. Cuando las cadenas almacenadas se concatenan posteriormente en un comando SQL dinámico, se ejecuta el código dañino.

El proceso de inyección consiste en finalizar prematuramente una cadena de texto y anexar un nuevo comando. Como el comando insertado puede contener cadenas adicionales que se hayan anexado al mismo antes de su ejecución, el atacante pone fin a la cadena inyectada con una marca de comentario "--". El texto situado a continuación se omite en tiempo de ejecución.

BLIND SQL INJECTION: ataque a ciegas de inyección de sentencias SQL, usado para explotar las vulnerabilidades de una base de datos que después de ser inyectadas se espera que retorne un error (proceso de adivinación).

SMURF: ataque de denegación de servicios, que junto a spoofing busca dejar fuera de servicio un sistema con el uso de grandes paquetes icmp.

VI.1.5 BACKTRACK

Es un software que usa un arsenal de pruebas de intrusión basado en Linux que ayuda a profesionales de la seguridad en la capacidad de realizar evaluaciones en un entorno nativo exclusivamente dedicado al Hacking. Sin importar si se está utilizando como sistema operativo principal, arranque de un Live Cd, o en una maquina virtual, BackTrack se ha personalizado hasta el último paquete de configuración del kernel, la escritura, entre otros, con el propósito de realizar pruebas de intrusión. Se ha ampliado desde su creación 4 veces haciendo que cada versión sea mejor que la anterior para de esta forma lograr que sea un marco de pruebas de penetración confiable.

BackTrack 4 R2 es la segunda actualización para la rama 4 en donde se incluye el kernel 2.6.34 y a la cual se le hicieron varias mejoras tales como el soporte de hardware, la capacidad de respuesta del escritorio, entre muchas otras. Este software de seguridad, es considerado por el equipo que lo desarrollo la mejor versión que se ha publicado a la fecha.

Fue diseñado para la auditoría de seguridad y relacionado con la seguridad informática en general, su enfoque es la realización de test de penetración y proporciona acceso a más de 300 herramientas de todo tipo (sniffers, Exploits, auditoría wireless, análisis forense, etc) entre las que se destaca el kit de herramientas de ingeniería social SET.

IV.1.6 SOCIAL ENGINEERING TOOLKIT (SET)

Es un kit de herramientas que ayuda en la tarea de realizar ataques de ingeniería social, permite suplantar fácilmente la identidad de un sitio determinado, o enviar ataques por mail a las cuentas de correo de alguna compañía o persona, infectar memorias USB, etc, fue diseñado por David Kennedy (ReL1K).

Estas herramientas se usan para verificar el nivel de vulnerabilidad de una empresa ante ataques de ingeniería social y para tomar las medidas correspondientes. La versión actual es la 1.3 y fue liberada en abril de 2011.

VI.1.7 METASPLOIT FRAMEWORK

Es una solución de pruebas de penetración de código abierto desarrollado por la comunidad de Open Source y Rapid7. Estándar para pruebas de penetración, con la base de datos publica más grande y de calidad para explotar.

Es la herramienta líder en pruebas de penetración del mundo. Se trata de un proyecto de código abierto que proporciona el software de pruebas de penetración, la información sobre vulnerabilidades de seguridad, y permite el código de explotación y el desarrollo de firma DS.

El Metasploit Framework, está desarrollado en Ruby con algunos componentes C y assembler, es la plataforma de desarrollo real utilizada para crear herramientas de seguridad de prueba y módulos de explotación, también se puede utilizar como un sistema de pruebas de penetración. Es una herramienta de línea de comandos muy poderosa que ha publicado algunas de las hazañas más sofisticadas a las vulnerabilidades de seguridad pública. También es conocida por sus herramientas anti-forense y de evasión, que se construyen en el marco de Metasploit.

VI.2 MARCO CONCEPTUAL

Ambiente controlado: Es el entorno o lugar donde se cuida hasta el mínimo detalle de control y seguridad para el desarrollo de actividades de experimentación, investigación y enseñanza de ataques informáticos.

Ataque informático: Método organizado por el cual se intenta tomar el control, desestabilizar o dañar un sistema informático o red.

Auditoria: Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida.

BT4R2: Backtrack 4 release 2, última versión lanzada de este software, distribución en live cd diseñada para la auditoria de seguridad.

Confidencialidad: Calidad de secreto, que no puede ser revelado a terceros o personas no autorizadas.

Control de accesos: Se utiliza para restringir el acceso a determinadas áreas del PC, de la red, mainframes, Internet, ftp, web, etc... El permiso o la denegación de acceso puede realizarse en función de la dirección IP, el nombre de dominio, nombre de usuario y password, certificados del clientes, protocolos de seguridad de redes, etc...

Delito informático: Delito cometido utilizando un PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.

Información sensible: Información personal privada, aquella que podría dañar los intereses de una organización o terceros, ocasionando daños o perdidas por su revelación no autorizada.

SET: Kit de herramientas que ayuda en la tarea de realizar ataques de ingeniería social, permite suplantar fácilmente la identidad de un sitio determinado.

Vector de ataque: Básicamente son los pasos y estrategias q se deben realizar para lograr el éxito de un ataque informático.

Vulnerabilidad: Debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

VI.3 MARCO LEGAL

VI.3.1 Derechos De Autor

Ley 23 De 1982 sobre Derechos de Autor

El Derecho de Autor es el conjunto de normas que protegen los derechos subjetivos de los creadores de las obras. Comprende dos aspectos: los derechos morales y los derechos patrimoniales. Los primeros hacen referencia al conjunto de prerrogativas en virtud de las cuales el autor podrá reivindicar en todo tiempo la paternidad de la obra, oponerse a cualquier deformación que demerite la obra o su reputación, publicarla, o conservarla inédita, modificarla y a retirarla de circulación. Los derechos morales son intransferibles, irrenunciables e imprescriptibles.

Por su parte, los derechos patrimoniales son todas las facultades que le permiten al autor explotar económicamente la obra. El titular de tales derechos podrá realizar, autorizar o prohibir cualquier forma de utilización que se quiera hacer de la obra, tales como reproducirla, comunicarla al público, distribuirla, transformarla, ponerla a disposición, entre muchas otras. Su término de duración está limitado a la vida del autor más 80 años después de su muerte.

De esta forma, Las estudiantes ceden voluntariamente y gratuitamente los derechos patrimoniales de autor a la **Corporación Universitaria Minuto de Dios** diligenciando un formato con firma reconocida ante notario público de acuerdo con la normatividad vigente. De esta forma la Universidad podrá hacer uso patrimonial de este trabajo de grado.

En cuanto a la publicación de las guías, los derechos reservados son:

RECONOCIMIENTO-NOCOMERCIAL-COMPARTIRIGUAL 2.5 COLOMBIA

Usted es libre de:


Copiar, distribuir y comunicar públicamente la obra


Hacer obras derivadas

Bajo las condiciones siguientes:


Reconocimiento — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador (pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra).


No comercial — No puede utilizar esta obra para fines comerciales.


Compartir bajo la misma licencia — Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

Entendiendo que:

Renuncia — Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

Dominio Público — Cuando la obra o alguno de sus elementos se halle en el dominio público según la ley vigente aplicable, esta situación no quedará afectada por la licencia.

Otros derechos — Los derechos siguientes no quedan afectados por la licencia de ninguna manera:

- Los derechos derivados de usos legítimos u otras limitaciones reconocidas por ley no se ven afectados por lo anterior.
- Los derechos morales del autor
- Derechos que pueden ostentar otras personas sobre la propia obra o su uso, como por ejemplo derechos de imagen o de privacidad.

Aviso — Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

VI.3.2 RENUNCIA DE RESPONSABILIDAD

Considerando la existencia de leyes vigentes en Colombia se especifica que LAS AUTORAS, EL DIRECTOR DEL PROYECTO Y LA CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS, NO se responsabilizan por el uso indebido o mal intencionado que se haga de todo lo aquí expuesto ya que el contenido e intención de las guías es netamente de carácter educativo. Asimismo, se advierte que se tomara en cuenta el principio de la territorialidad de la ley que ejercen los Estados. Los usuarios de las guías aceptan y se hacen responsables de cualquier daño o perjuicio que se presente como consecuencia de del uso de las guías, siendo consientes de que si infringe la ley, esta conducta será castigada

VII. DISEÑO METODOLÓGICO

VII.1 TIPO DE INVESTIGACIÓN

La propuesta metodológica del presente proyecto se basa en la investigación exploratoria ya que no existen investigaciones previas sobre el objeto de estudio, y por lo tanto se requiere explorar e indagar, con el fin de alcanzar el objetivo planteado.

"Los estudios exploratorios se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado o que no ha sido abordado antes. Es decir, cuando la revisión de la literatura revela que únicamente hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio.

La investigación exploratoria terminará cuando, a partir de los datos recolectados, se adquiera el suficiente conocimiento como para saber qué factores son relevantes al problema y cuáles no. Hasta ese momento, se está ya en condiciones de encarar un análisis de los datos obtenidos de donde surgen las conclusiones y recomendaciones sobre la investigación"[6].

[6] HERNÁNDEZ SAMPIERI y otros (1994). Metodología de la investigación, México, Mc Graw Hill, Cap. 4

VII.2 MÉTODOS

VII.2.1 TESIS ANTÍTESIS Y SÍNTESIS

VII.2.1.1 TESIS

La ingeniería social es la técnica más usada para obtener acceso a información usando métodos de convencimiento y persuasión contra el elemento humano, los cuales explotan las debilidades propias y la falta de mantenimiento de un sistema de información. Ya sea por ingenuidad, inocencia, ignorancia, los humanos cometen errores muy seguidamente que pueden poner en peligro la seguridad de un sistema y la mayoría de veces la víctima no se percata de lo que está haciendo. Algunos ejemplos: una llamada telefónica en donde un cierto personaje se hace pasar por agente de soporte técnico de alguna aplicación o empresa, que pregunta ciertos datos para corroborar el estado de dicha aplicación; la información transmitida a través de un correo electrónico en donde se suplanta la identidad de un sitio oficial para que el usuario descargue o acceda a sitios en donde puede ser estafado; hacerse pasar por las autoridades policiales afirmando estar en un proceso que requiere la mayor colaboración y sobre todo discreción con la información que se está solicitando para un determinado caso; espiar la pantalla y el teclado de alguna persona mientras esta está ingresando a un sitio que requiera información confidencial o autenticación; o pedir prestado el computador de la victima ya sea para ser usado directamente o para que la victima permita conectar un dispositivo de almacenamiento a él; entre otras.

La seguridad de la información no solo se basa en los controles de accesos físicos y lógicos o en las políticas de seguridad, sino también debe enfocarse al elemento humano ya que este es el encargado de interactuar con estos elementos que por sí solos

no se equivocan, como lo son el hardware y el software. El ingeniero social está entrenado en técnicas que permitan la detección de vulnerabilidades de la persona, desde verificar si la información que está brindando es verídica de forma presencial (expresiones faciales, tono de voz, expresión corporal, uso de los sentidos y las emociones) hasta lograr tender la trampa bien estructurada para que la víctima no se percate del ataque (via web).

VII.2.1.2 ANTÍTESIS

Con los avances tecnológicos de hoy en día, los sistemas de información crecen de forma más rápida y con estos los problemas de seguridad de la información. Una de las amenazas más importantes es la ingeniería social ya que por medio de la psicología logra manipular al elemento humano para obtener la información necesaria y conseguir penetrar un sistema. Esta es una problemática que afecta directamente a las grandes compañías ya que los crackers y delincuentes informáticos se centran en conseguir un beneficio propio, algo de dinero o simplemente el desprestigio de dicha compañía, su objetivo principal son las personas más influyentes, las que poseen la mayor información para que el ataque sea exitoso, la ingeniería social se aplica a las personas que tienen contacto con la tecnología y por esto en las políticas de seguridad se encuentran implementados los antivirus y los firewalls que están en la capacidad de prevenir en gran parte ser víctima de los ataques. La mejor estrategia para prevenir ser víctima es la inversión en equipos de cómputo y la implementación de software.

VII.2.1.3 SÍNTESIS

La falta de creación y cumplimiento de políticas de seguridad, fallas en la programación, poca actualización de software, falta de educación y prevención para los usuarios, son algunos de los motivos que hacen vulnerable un sistema de información, pero en gran medida el elemento humano es el más importante y al cual se le debe prestar más atención ya que este constituye uno de los problemas más importantes porque tienen la capacidad de decidir voluntaria o involuntariamente, romper las reglas y normas impartidas en las políticas de seguridad, permitiéndole a un atacante obtener información y acceder a un sistema informático eludiendo los mecanismos y las tecnologías de seguridad.

La ingeniería social va mas allá de los conocimientos técnicos, por esta razón es una grave amenaza que puede ocasionar enormes pérdidas sin precedentes[7], ya sea a grandes o pequeñas empresas e igualmente a cualquier persona.

No se puede afirmar que el hecho de tener una buena estructura tecnológica garantiza la seguridad informática. Por esta razón se debe disminuir el riesgo de ser víctimas de la ingeniería social, teniendo claro que es fundamental la capacitación del usuario ya que el desconocimiento de este tema es la mayor ventaja que tiene un ingeniero social, y puede ser contrarrestada creando conciencia sobre los riesgos y daños potenciales frente a estos ataques.

[7] Ver anexo 3

VII.2.2 PRUEBA ERROR

Este método se caracteriza por ser cíclico, es decir, se prueba una opción y se observa si funciona. Si funciona, entonces se tiene una solución. Si no, esto es un error y se intenta otra opción, así sucesivamente hasta llegar a una solución.

Según lo anterior, se tendrán en cuenta algunos parámetros para la realización de las guías y la obtención de posibles soluciones en cada una de ellas:

- Las guías tratarán de encontrar sólo una solución, no todas las soluciones, ni tampoco la mejor.
- Requieren de diferentes medios para realizarse y no siempre el resultado obtenido es exitoso.
- Las guías no descubrirán por qué funciona una solución, sino que sólo señala cuál es la solución.

VII.3 UNIVERSO

Todas las empresas privadas ubicadas sector en la ciudad de Bogotá, específicamente concesionarios de carros y motos que distribuyan accesorios y tengan acceso a internet.

VI.4 POBLACIÓN

Concesionarios de motos que presten servicio técnico a sus clientes, tengan acceso a internet y estén ubicadas en el área noroccidente de la ciudad de Bogotá, más exactamente en la Av. Boyacá, entre las calles 53 y 68.

VII.5 MUESTRA

Se tomará como prototipo la empresa SADEXIM S.A.S ubicada en la dirección Av. Boyacá # 67-34 Barrio Normandía - Bogotá.

VII.6 TÉCNICAS O INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Por la complejidad del tema, se implementaron dos técnicas para la obtención de información que permitieron la medición de las variables a fin de obtener los datos necesarios para el estudio del problema o aspecto de la realidad.

Inicialmente se realizo una encuesta para determinar el porcentaje de la problemática del proyecto, esto con el fin de determinar cuáles eran los aspectos más importantes para tener en cuenta al momento de realizar las guías y darle solución al problema.

Asimismo se realizo una entrevista antes y después de lanzar algún ataque, a las "victimas" escogidas y así determinar las posibles causas que hacían vulnerable a la persona al momento de enfrentarse con un ataque de ingeniería social.

VII.6.1 ENCUESTA: Es una Técnica cuantitativa que consiste en una investigación realizada sobre una muestra de sujetos, recogen información de una porción de la población de interés, dependiendo el tamaño de la muestra en el propósito del estudio. Con esta se pueden detectar ideas, necesidades, preferencias, hábitos de uso, etc. La encuesta tiene la ventaja de su amplio alcance, puede ser rápida en su construcción y económica en su aplicación. Básicamente su finalidad es conseguir mediciones cuantitativas sobre una gran cantidad de características objetivas y subjetivas de la población.

VII.6.2 ENTREVISTA Este es un método de investigación social que sigue los mismos pasos de la investigación científica; sólo que en su fase de recolección de datos, éstos se obtienen mediante un conjunto de preguntas, orales o escritos, que se les hace a las personas involucradas en el problema o motivo de estudio.

CONCLUSIONES

Las guías prácticas para uso de técnicas de ingeniería social, Están elaboradas para permitir la comprensión del usuario, en su elaboración se evito el uso de tecnicismos, pero también se omite el paso de toma de control de la víctima, es decir en las guías se ilustran los pasos para realizar el ataque pero nunca como tomar control de la víctima, esto no quiere decir q los ataques no sean exitosos, simplemente q se pretende mostrar cuales son los pasos que hace un “delincuente” para robar nuestra información. Esto se hizo porque nuestras guías están dirigidas al publico general y no sabemos q tan responsable sea la persona al momento de usarlas. Además contienen anexos en donde se explican los Exploits y las cargas maliciosas a usar.

En cuanto a las pruebas, se realizaron en ambientes controlados teniendo siempre presentes las leyes vigentes. Con los resultados de las pruebas se puede comprobar que es importante la actualización del software, ya que si estos no las poseen pueden ser explotadas las vulnerabilidades y el atacante puede tomar el control de la máquina víctima. Además, se deben realizar capacitaciones en donde se informe de los efectos que pueden causar un ataque exitoso de ingeniería social y las formas de identificarlos o contrarrestarlos.

La mayoría de personas de la muestra fueron vulnerables ante la ingeniería social. Desde que el atacante clone o robe una cuenta de correo electrónico autorizada es más alto el porcentaje de victimas.

SET es una herramienta poderosa que junto a Metasploit logra hacer ataques de ingeniería social, para ejecutarla no se necesita el mayor conocimiento sobre seguridad.

El elemento que permite ataques de Ingeniería Social y una serie de problemáticas que se encierran dentro del conocimiento y desconocimiento sobre el tema es sin duda alguna, el factor humano, ya que es parte esencial y primordial de la seguridad. No existe un sistema informático que no dependa de algún dato ingresado por un usuario. Por esta razón se convierte en una debilidad de seguridad universal, independiente de

plataformas, software, red, equipo y la edad de la persona que sea afectada. La falta de conocimiento y capacitación sobre las distintas técnicas y maneras de ser atacados con el uso de la Ingeniería Social es lo que hace vulnerable a cualquier usuario.

También existen otras causas como: Permitir el acceso a alguna parte del sistema, físicamente o electrónicamente, por parte de personas externas o propias de la empresa que no tengan relación con lo que se realice. Desconocimiento de políticas y protocolos de la organización por parte de los empleados, en donde se les explique la manera de trabajo de la misma. Indiferencia del personal para respaldar información y mantenerse alerta a distintos sistemas de seguridad de información. Utilización de herramientas que no proporcionen seguridad a la información ni al personal, y con esto permitan el robo, o algún daño al sistema. Debido a esto la ingeniería social es un asunto de extremado cuidado para cualquier persona y aun más para empresas u organizaciones. Es vital tener en cuenta las siguientes recomendaciones:

- Actualizaciones oportunas del software (parches)
- Capacitación a los usuarios y personal, desde los operarios hasta personal de limpieza.
- Análisis con antivirus de todos los correos recibidos
- No informar telefónicamente de las características técnicas de la red, ni nombre de personal a cargo.
- Control de acceso físico al sitio donde se encuentra los ordenadores.
- Políticas de seguridad a nivel de Sistema Operativo.

Por otra parte también se concluye que son bastantes las personas que caen a causa de estos ataques, la ingeniería social tiene como fin persuadir, por esta razón se muestran los resultados de las pruebas realizadas (Ver anexo 4).

En síntesis se puede decir que **"La mejor manera de estar protegido contra la ingeniería social y sus técnicas, es el conocimiento."**

BIBLIOGRAFÍA Y WEBGRAFIA

- Ataque por denegación de servicio, (16 Oct 2008), Consultado el 28 de Abril de 2011, de http://es.kioskea.net/contents/attaques/dos.php3
- BackTrack 4 R1 Dev Public Release (10 Mayo 2010), Consultado el 3 de Septiembre de 2010, de http://www.offensive-security.com/backtrack/penetration-testing-information-security-distribution/
- Biscione. Carlos A., (n, d), INGENIERÍA SOCIAL PARA NO CREYENTES, Consultado el 12 de Septiembre de 2010, de http://www.acis.org.co/fileadmin/Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_CarlosBiscione.pdf
- Conceptos básicos de Seguridad Informática, (n, d,), Consultado el 12 de Septiembre de 2010, de http://www.eurologic.es/conceptos/conbasics.htm
- Computer Based Social Engineering Tools: Social Engineer Toolkit (SET), (16 Sep 2009), Consultado el 3 de Septiembre de 2010, de http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_(SET)
- Descargar BackTrack 4 R2 (2 Ago. 2010), Consultado el 3 de Septiembre de 2010, de http://www.dragonjar.org/descargar-backtrack-4-r1.xhtml
- HERNÁNDEZ SAMPIERI y otros (1994). Metodología de la investigación, México, Mc Graw Hill, Cap. 4
- Inyección de código SQL, (N, D), Consultado el 28 de Abril de 2011, de http://msdn.microsoft.com/es-es/library/ms161953.aspx
- Man in the middle attack (fire brigade attack), (22 Nov 2000), Consultado el 28 de Abril de 2011, de http://searchsecurity.techtarget.com/definition/man-in-the-middle-attack
- Nueva técnica de fraude informático: el pharming, (30 Mar 2005), Consultado el 28 de Abril de 2011, de http://www.belt.es/noticias/2005/abril/01/pahrming.htm
- Prevención de ataque de fuerza bruta, (N, D), Consultado el 28 de Abril de 2011, de http://servidordebian.wikidot.com/squeeze-es:security-bruteforceattack
- ¿Qué es la suplantación de identidad (phishing)?, (N, D), Consultado el 28 de Abril de 2011, de http://windows.microsoft.com/es-XL/windows-vista/What-is-phishing

- ¿Qué es un buffer overflow ?, (14 Ene 2007), Consultado el 28 de Abril de 2011, de http://www.ignside.net/man/seguridad/buffer_o.php
- Seguridad de las redes inalámbricas: Wardriving y Warchalking, (19 Nov 2002), Consultado el 28 de Abril de 2011, de http://www.hispasec.com/unaaldia/1486
- Video Tutorial SET (Social Engineering Toolkit), (24 May 2010), Consultado el 12 de Septiembre de 2010, de http://www.dragonjar.org/video-tutorial-set-social-engineering-toolkit.xhtml
- Visentin. Maximiliano, (13 Dic 2006), La Ingeniería Social "Oportunidades que le brindan las nuevas amenazas", Consultado el 12 de Septiembre de 2010, de http://www.eset-la.com/pub/mvis.pdf

Anexo 1

ENCUESTA

Nombre:_____Edad:____
Ocupación: _____ Correo electrónico:_____

Por favor responda las siguientes preguntas:

1. Ejecuta usted el kit de herramientas de ingeniería social (SET) usando:
   a. BackTrack
   b. Descarga directa a su distribución de Linux preferida

2. ¿Ha tenido problemas al usar SET?
   a. Si
   b. No

3. Si la respuesta anterior fue si, ¿Cuál ha sido el principal problema a la hora de usar SET?
   a. El idioma en el que se encuentra
   b. La poca documentación en la red
   c. Todas las anteriores

4. ¿Qué tipo de ayudas ha usado usted?
   a. Foros
   b. Manuales
   c. Video-tutoriales
   d. FAQ
   e. Ninguna de las anteriores

5. ¿Las ayudas son entendibles?
   a. Si
   b. No

6. Califique las ayudas que ha utilizado de SET:
   1. Excelente
   2. Bueno
   3. Regular
   4. Malo
   5. Pésimo

7. ¿Cuál sería el mejor método de ayuda para SET?
   a. Video-tutoriales
   b. Guías paso a paso
   c. Clase presencial
   d. Otra, ¿cuál?: _____

ANEXO 2

SADEXIM S.A.S
PERSEVERANCIA INTEGRIDAD INNOVACIÓN

Bogotá, 7 de febrero de 2011.

Srta. (s)
Carmen Lucia Pedraza – Viviana Andrea Caviedes.
Administradoras de Red.
Departamento de Sistemas SADEXIM S.A.S

Referencia: Solicitud de Autorización para la evaluación de los niveles de seguridad informática en la plataforma tecnológica de la empresa SADEXIM S.A.S

Cordial saludo.

Autorizamos la realización de pruebas de penetración – Etical Hacking sobre la plataforma tecnológica de la empresa (SADEXIM S.A.S), de acuerdo con lo especificado en el documento entregado por ustedes.

Manifestamos que la responsabilidad total por la ejecución de los procesos realizados, sus consecuencias y la confidencialidad de la información es asumida por el departamento de sistemas.

Cordialmente.

SADEXIM S.A.S.
Nit. 900.341.360-4

JOHANN ANTONIO CRUZ V.
Coordinador de proyectos especiales

ANEXO 3

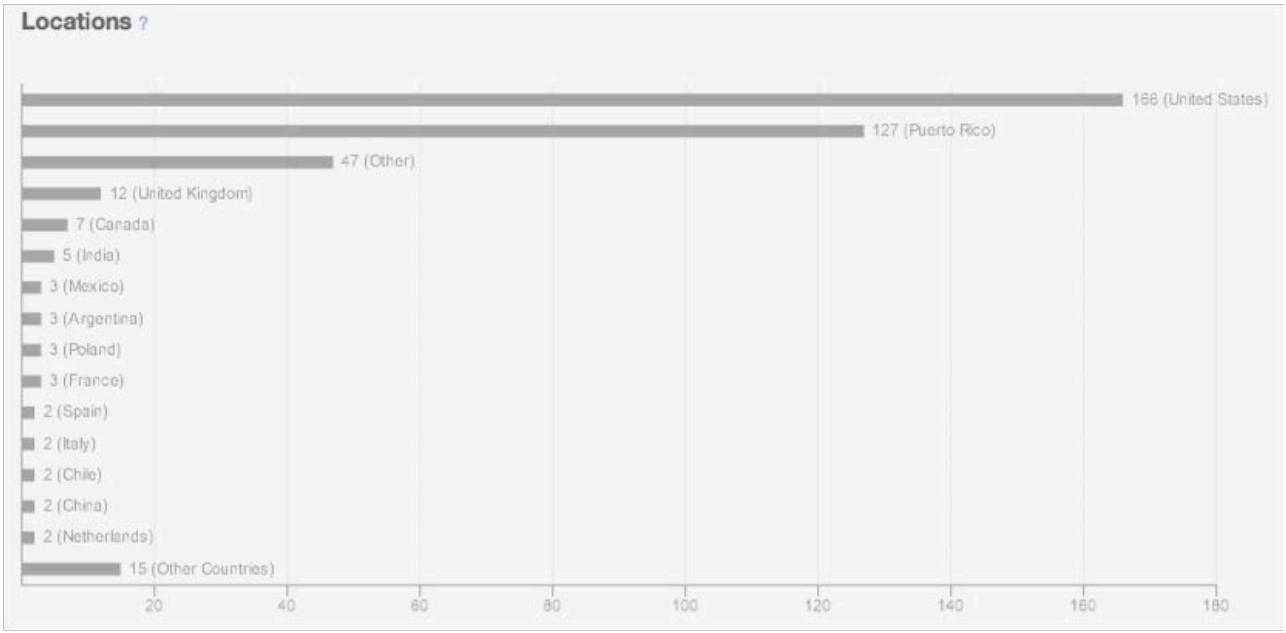
Estudio de pérdidas a causa de ingeniería social.

La ingeniería social es el tema más relevante al momento de hablar de seguridad de la información. Pero no todo el mundo es realmente consciente de ello, por esta razón se realizo un proyecto de investigación sobre la ingeniería social, con el objetivo de demostrar que la mayoría de los usuarios de la red no puede identificar un vínculo o la legitimidad de un correo electrónico. El experimento fue diseñado en base a una encuesta on-line y que incluye tres secciones principales.

La primera sección recoge datos demográficos sobre los encuestados, conocimientos de informática, la educación y su uso de Internet. Esto es seguido por la parte principal de la encuesta, que consistió en una prueba pequeña, compuesta de nueve preguntas, cada presentación de los participantes con un mensaje de correo electrónico o una URL, y un juzgamiento de su legitimidad. En todos los casos, los encuestados pueden elegir una de tres opciones ("ilegítimo", "legítimo" y "No sé"). Si optan por ilegítimo, a continuación, se pregunta ¿por qué creen que el correo electrónico que se presento es ilegítimo?

De acuerdo con los resultados el total de participantes incluyó a 17 nacionalidades diferentes y la mayoría de los participantes fueron de Estados Unidos y Puerto Rico. Esto incluyó una mezcla de género de 70% hombres y 30% mujeres. La mayoría de edad de los participantes fue de 30 a 49 años de edad con un 51%, 39% de la gama de 10-29 y 9% a partir de las edades de 50 a 69. En una nota interesante que la mayoría de los

participantes (45%) tenían un título de licenciatura, y una cantidad significativa tenían educación superior, como una maestría con un 27%.



A los efectos de esta investigación este dato es muy importante, en un grado el nivel de educación de los usuarios significa que son más capaces de comprender un curso de sensibilización de mejor detallado que los que no tienen una educación. Aunque se necesitan más investigaciones para probar este punto, se sugiere que una mejor distribución de los cursos de sensibilización puede beneficiar a la organización.

Las personas con algún tipo de grado de la universidad tienden a tener más comprensión de las computadoras que otros. Podría ser que la gente con educación han estado más expuestos al uso de las computadoras que las personas sin una educación. Adicional a la investigación podría proporcionar una evidencia más de este asunto, pero para el alcance

del proyecto, parece que el tipo de sistema operativo utilizado es importante para ver entender el tipo de usuario de la computadora.

La mayoría de los participantes mencionaron que el uso de ordenadores cada día tanto en casa como en el trabajo. El propósito de uso varía, pero el sistema de correo electrónico era la mayoría. La figura 11 representa los números:

#	Answer	Response	%
1	News	159	83%
2	Work research	121	63%
3	Personal research	147	77%
4	Investments	26	14%
5	Shopping	116	61%
6	Auctions	49	26%
7	Email	177	93%
8	Chat/communities	94	49%
9	Banking	113	59%
10	Social Media	124	65%
11	Job Hunt	72	38%
12	Entertainment	131	69%
13	Other	12	6%

La segunda parte de la encuesta fue la prueba con la dirección URL y correos electrónicos. Como se mencionó anteriormente esta parte se compone de nueve preguntas, donde cuatro mensajes de correo electrónico y direcciones URL para identificar cinco. Todos los correos electrónicos en la encuesta donde fuera ilegítima y de la dirección URL cinco expuestos sólo dos eran legítimos. Si el participante identificar el correo electrónico o la dirección URL como ilegítimo, él / ella fue impugnada con un

cuadro de texto para explicar su razonamiento. Una observación rápida de los más de todos los resultados: de los nueve preguntas expuestas en cuatro de ellos (13, 15,21, y 29) la mayoría de los participantes en el correcto sobre el correo electrónico o una URL y sostenida la respuesta de por qué. Esto significa que el 56% de la prueba global causado algún tipo de problemas para que el participante identifique correctamente. En la pregunta 17, la mayoría de los participantes (57%) indicaron que la dirección era ilegítimo, sino porque la mayoría sólo el 52% de ellos pudo mantener su configuración de nuevo esta respuesta mayoritaria a un 28%. En el resto de la prueba a menos que la mitad de los participantes indicaron que la respuesta correcta, e incluso menor que la mitad no podría sostener su respuesta

Question #	Type	Identification	Total Responses	%
13	Can you recognize this email?	Illegitimate	96	52.00%
		I don't know	36	20.00%
		Legitimate	52	28.00%
15	----------...----------	Illegitimate	127	73.00%
		I don't know	31	18.00%
		Legitimate	15	9.00%
17	Can you identify a URL? http://paypalsecurity.co.uk/security/protectyourdata.asp	Illegitimate	98	58.00%
		I don't know	48	28.00%
		Legitimate	24	14.00%
19	Can you identify a URL? http://203.144.234.138/us/safedata/index.html	Illegitimate	82	49.00%
		I don't know	76	45.00%
		Legitimate	10	6.00%
21	Can you identify a URL? https://paypal.com	Illegitimate	27	16.00%
		I don't know	20	12.00%
		Legitimate	120	72.00%
23	Can you recognize this email?	Illegitimate	65	40.00%
		I don't know	59	36.00%
		Legitimate	40	24.00%
25	Can you identify a URL? https://security.ebay.passwordreset.com/	Illegitimate	76	47.00%
		I don't know	52	32.00%
		Legitimate	33	20.00%
27	Can you recognize an email?	I don't read Spanish	35	22.00%
		Illegitimate	78	49.00%
		I don't know	14	9.00%
		Legitimate	32	20.00%
29	Can you identify a URL? http://cars.com	Illegitimate	14	9.00%
		I don't know	50	31.00%
		Legitimate	95	60.00%
		Total	225	

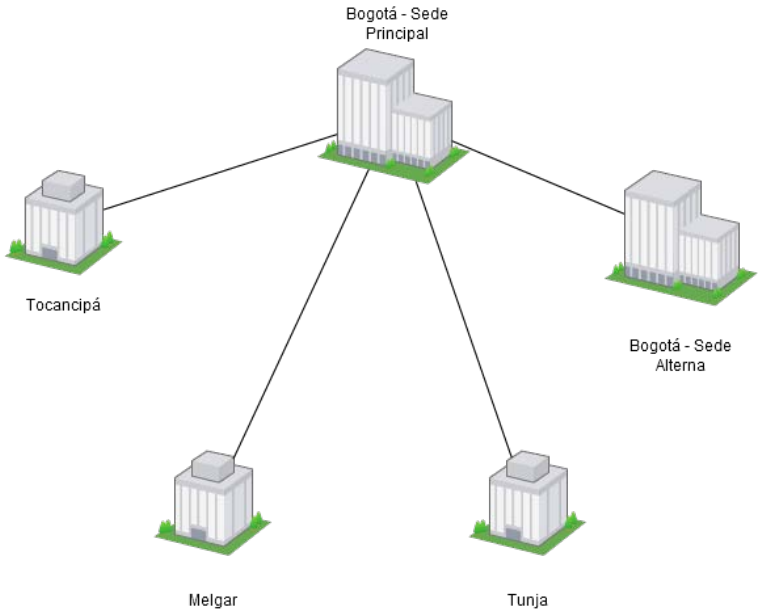
El principal objetivo de esta investigación se basó en el hecho de que muchas personas, incluso los que tienen un curso de conocimiento de la información carecen de los conocimientos necesarios para identificar una estafa. La encuesta identifica que los cursos de conocimiento de la información deben ser dirigidas a un público específico y que la información recurrente La sensibilización debe incluir ejemplos de ingeniería social y las pruebas para medir realmente la eficacia de la formación.

ANEXO 4

INFORMACIÓN DE LA MUESTRA

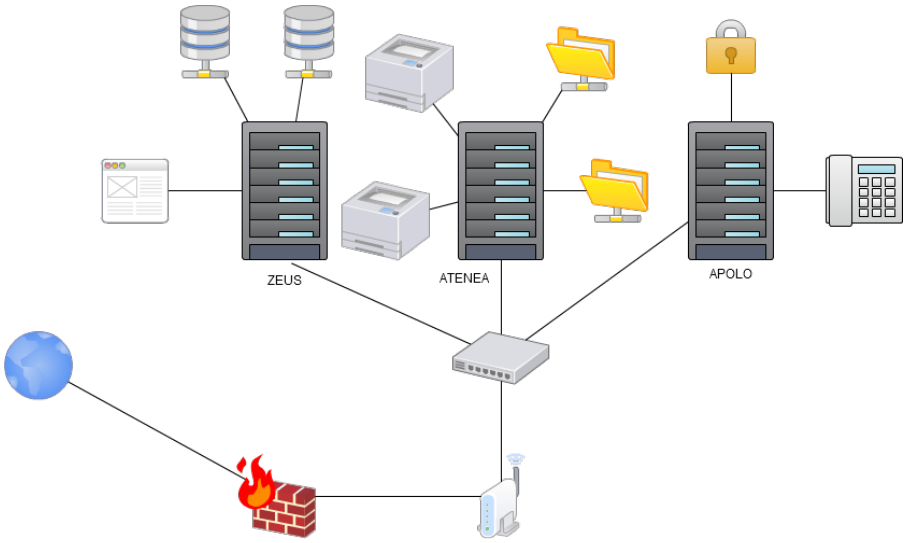
SADEXIM S.A.S

Es una empresa dedicada a la importación y comercialización de motocicletas, la cual tiene como casa matriz al grupo **MAHINDRA 2 WHEELERS**, una empresa de la India dedicada a la fabricación y comercialización en toda la industria automovilística y en otras industrias, cuenta con tres seccionales a nivel nacional y una auxiliar en Bogotá. La totalidad de empleados es de 150 a los cuales serán aplicadas las pruebas de penetración. Estas pruebas se realizarán con el fin de identificar cuan vulnerable son los empleados frente a la ingeniería social usando el kit de herramientas SET. Se tomaran en cuenta los empleados de todas las áreas y no de un departamento específico.



En la sede principal se encuentra centralizado todo el sistema, La red empresarial implementa una topología estrella, siguiendo algunos de los estándares de instalación de cableado estructurado.

Los PCs y dispositivos están conectados a un switch que se encarga de distribuir los recursos y aplicaciones necesarios que provee los servidores para el funcionamiento de la empresa, además facilita la comunicación entre clientes y otros dispositivos de la red.



Consta de 3 servidores: Apolo, servidor Linux Centos 5.5 que provee la telefonía VoIP y la seguridad de la infraestructura a nivel nacional; Atenea, servidor Windows server 2008R2 que provee los servicios de carpetas compartidas, servidor de transferencia de archivos (FTP) y servicios de impresión; Zeus, servidor WEB, Windows server 2008R2 que maneja las bases de datos y el sistema contable. Sus seccionales se conectan a la sede principal a través de enlaces VPN.

Visión

Superar con excelencia las expectativas de nuestros clientes y nuestra casa matriz compitiendo nacional internacionalmente en el mercado; ubicarnos en el pódium de los importados y comercializadores más importantes de motocicletas logrando así forjar un nuevo estilo de vida

Misión

Forjar un estilo de vida ofreciendo cuidado calidad e innovación

Valores

Perseverancia, integridad e innovación

ANEXO 5

Estadísticas de las pruebas