Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Tema

Ingeniería social y sus herramientas informáticas

Título

“Ingeniería social y las herramientas informáticas involucradas en un ataque”

Autor: Martín Colli

Tutor: Dr. Pedro Hecht

Año 2020

Cohorte 2018

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Martín Colli

Licencia

Aviso

Resumen

El trabajo consiste en reflejar la información referente a los conceptos necesarios para comprender lo relacionado a la ingeniería social en cuanto a los datos y técnicas utilizadas para llevar a cabo los ataques.

En adición a lo anterior, se realiza la recopilación de la información de las herramientas informáticas más utilizadas hoy en día en el campo de la ingeniería social para las diferentes etapas involucradas a la hora de llevar a cabo un ataque de este tipo.

En base a lo recopilado se realizan recomendaciones para lograr una prevención y mitigación contra este tipo de ataques en cuanto el objetivo de los mismos sea una organización.

Palabras claves: ingeniería social, phishing, OSINT, seguridad.

Índice

Introducción

Hoy en día la ingeniería social ocupa un lugar relevante en lo que se refiere a la seguridad informática dada la efectividad de sus métodos y los resultados consistentes en su aplicación. En el siguiente trabajo se realiza una abordaje de los diferentes puntos concernientes a la ingeniería social y las herramientas informáticas involucradas en el desarrollo de esta área.

Inicialmente, se lleva a cabo la definición de múltiples conceptos básicos relevantes de la ingeniería social que permiten mejorar la comprensión de las metodologías involucradas en las diferentes etapas de un ataque en esta área.

A continuación, se definen las etapas que conforman los pasos seguidos para llevar a cabo un ataque exitoso de ingeniería social. Además de esto, se procede a la descripción y enumeración de las herramientas informáticas involucradas en las etapas de recopilación de información y en la de concreción del ataque de ingeniería social.

Finalmente, se realiza un recorrido por las medidas que corresponden tomar para lograr una prevención y mitigación efectiva de un ataque de ingeniería social en donde una organización es el objetivo del mismo.

1. Definición de la ingeniería social y sus aspectos más generales

En este capítulo se van a relatar y analizar los aspectos más fundamentales de la ingeniería social.

1.1. Definición de la ingeniería social

La ingeniería social es definida por Christopher Hadnagy como "...cualquier acto que influencia a una persona a tomar una acción que puede o no estar en su mejor interés"[1] [1].

1.2. Categorías de personas que utilizan ingeniería social

Las personas que utilizan ingeniería social en su día a día pueden agruparse en las diferentes categorías que se describen a continuación.

Sin contar necesariamente con la intención directa, muchas personas comunes utilizan en forma regular métodos de la ingeniería social para alcanzar objetivos en forma rápida y efectiva.

En referencia a los niños, estos se dan cuenta en forma temprana del deseo de los padres de que ellos sean felices y emplean métodos de la ingeniería social enfocados en este punto en particular. Esto se da sobre las acciones que toman los padres que no son deseadas por los niños, a lo que responden realizando malas caras o expresando un estado de tristeza con respecto a lo realizado.

Los padres por su lado utilizan métodos de ingeniería social que se manifiestan en la provocación de sentimientos de vergüenza o culpa por parte de sus hijos para lograr que ellos realicen lo deseado por sus

1 Traducción propia del inglés: "…*social engineering is defined as any act that influences a person to take an action that may or may not be in their best interest.*"

progenitores. Estas acciones explotan el deseo de aprobación que los hijos quieren obtener por parte de sus padres.

La mayoría de las empresas buscan que cuando el cliente se comunique por primera vez con las áreas de atención se tenga una interacción fácil con el mismo. Para esto se utilizan métodos de ingeniería social por parte del empleado utilizando una forma de trato amigable y alegre con la intención que el cliente se manifieste de forma recíproca a este comportamiento.

Los programas televisivos de noticias utilizan habitualmente métodos de ingeniería social en la forma de avances y promesas de una noticia muy interesante pero evitando decir exactamente cuándo la misma va a ser transmitida, logrando así mantener cautivos la mayor cantidad de televidentes posible.

Los negocios a la hora de retener sus clientes utilizan a menudo ingeniería social enfocándose en el método de aceptación social haciendo que la migración de una solución de una compañía a otra sea más costosa que continuar utilizándola [2].

Los vendedores utilizan varios de los métodos de los ingenieros sociales para entender las necesidades que presentan los clientes y determinar si ellos la pueden satisfacer con sus productos. Entre los métodos empleados se tiene la recolección de información sobre los clientes, obtención de información a través de la interacción con el objetivo, influencia y principios psicológicos [3].

Los médicos, psicólogos y abogados deben utilizar a menudo las tácticas necesarias de la ingeniería social para obtener información y realizar entrevistas adecuadas para influenciar a sus clientes en la dirección que ellos necesitan tomar [3].

Un reclutador ejecutivo debe tener en su arsenal de habilidades el manejo experto de las técnicas para obtener información de las personas como así también dominar los muchos principios psicológicos de la

ingeniería social. Con estas competencias el reclutador lograr leer a las personas y sobre todo entender qué es lo que las motiva, tanto por parte del empleado como del empleador [3].

Los gobiernos, para obtener los resultados deseados, buscan transmitir los mensajes a la sociedad que gobiernan de la forma que consideren más efectiva. Para esto muchos gobiernos recurren a diferentes metodologías como pueden ser la evidencia social, la autoridad y la escasez para asegurar la gobernabilidad [3].

Para los espías la ingeniería social es una forma de vida que aprenden para engañar a sus víctimas y hacerles creer que son alguien o algo que realmente no son. La credibilidad que desarrollan en estos engaños va a en base al conocimiento sobre el objetivo del ataque y el negocio o gobierno del mismo [3].

Los estafadores dominan la habilidad de leer muy bien a las personas, esto les da la posibilidad de identificar ciertas características en las personas que la vuelven víctimas fáciles para sus ataques. Estas son lo suficientemente susceptibles a grandes oportunidades de ganar dinero de forma fácil y así el atacante explota su codicia para realizar la estafa [3].

Los criminales que realizan robo de identidad se enfocan en utilizar información personal de personas reales sin su autorización como ser sus nombres, fechas de nacimiento, números de identificación y cuentas bancarias entre otros. Luego los criminales utilizan esto en conjunto con varias técnicas de la ingeniería social para cometer suplantación de identidad o fraudes entre otros delitos [3].

Un empleado descontento muchas veces termina desarrollando una relación antagonista con su empleador. Cuando el descontento supera cierto umbral el empleado encuentra más fácil justificar actos criminales en donde la ingeniería social se vuelve parte del arsenal que estos utilizan para sus ataques internos en la organización [3].

Los hackers están encontrando hoy en día que lograr acceder a ciertos sistemas se está volviendo más y más difícil debido a una mejor seguridad en el desarrollo de software y mayor dificultad para realizar hacking remoto. Esto conlleva a adicionar métodos de ingeniería social para poder lograr el objetivo y se está viendo reflejado tanto en grandes ataques como en pequeños que se dan alrededor del mundo [3].

Los penetration testers buscan acceder a los sistemas utilizando la mayoría de las veces los mismos métodos que usan los criminales. En este caso la ingeniería social es una de las herramientas claves que se ve reflejada en el uso de phishing, vishing y suplantación de identidad para así utilizar el mismo vector de ataque que un ingeniero social malicioso utilizaría [4].

1.3. Elección de la ingeniería social como vector de ataque

Un atacante a la hora de elegir el método de ataque se inclina por la ingeniería social por el simple hecho que da resultados en forma consistente. Esto es en gran medida debido al hecho que no existe una solución rápida, fácil y efectiva de subsanar las vulnerabilidades que explota la ingeniería social. Incluso aquellas personas que han sido entrenadas para evitar ser víctimas de estos ataques pueden llegar a olvidarse de seguir los pasos establecidos por la presión vivida durante un ataque de este tipo [5].

Las ventajas que traen acarreadas los ataques de ingeniería social son variadas. Se tiene que en el caso particular de robar credenciales informáticas a través de diferentes métodos, como pueden ser ataques de fuerza bruta, pueden llevar mucho tiempo en comparación con un ataque de ingeniería social efectivo que puede llevar solo minutos. Además de esto, se tiene que la información relevante para llevar a cabo ataques puede ser recopilada con gran efectividad utilizando las técnicas de la ingeniería social. En adición a lo anterior, si mediante la información recopilada y la utilización de la misma con la ingeniería social se logra tener acceso físico al lugar en

donde se encuentran los recursos informáticos, un hacker malicioso tiene la posibilidad de ejercer ataques informáticos de manera más fácil, simple y efectiva generando consecuencias devastadoras para la organización que es víctima [5].

1.4. Relevancia

A la hora de entender la relevancia de la ingeniería social y sus ataques en el panorama actual de la seguridad informática, se seleccionó para este trabajo el Reporte de Investigaciones de Violación de Datos[2] de 2019 de la empresa líder de la industria Verizon. En el mismo se lleva a cabo el análisis de 41.686 incidentes de seguridad de los cuales 2.013 son violaciones de datos confirmadas. Las fuentes de recopilación de estos incidentes son de diferentes puntos entre los que se encuentran la información pública disponible de incidentes de seguridad, casos provistos por el Centro Consultivo de Investigación de Amenazas[3] de Verizon en conjunto con otros colaboradores externos.

En el reporte se observa que el 33% del total de las tácticas utilizadas por agentes maliciosos incluían ataques sociales. Además, del total de violaciones de datos llevadas a cabo un 32% involucraba el uso del ataque de ingeniería social de phishing.

A la hora de analizar la evolución de la ingeniería social desde el 2013 al 2018 se observa un claro aumento con respecto a las acciones de amenaza en violaciones de seguridad yendo de un 17% a un 35%. En adición a lo anterior, los activos que fueron objetivos en la violaciones de datos sucedidas reflejan la misma tendencia ya que en la categoría de personas se tiene un 19% en 2013 que crece a un 39% en 2018.

Dentro de las acciones de amenaza utilizadas en violaciones de datos, se reporta que en el primer puesto se encuentra el phishing. Luego

2 Traducción propia del inglés: "*Data Breach Investigations Report*"

3 Traducción propia del inglés: "*Threat Research Advisory Center*"

cuando se analizan los vectores de acción de malware se encuentra en el primer lugar los archivos adjuntos en los correos electrónicos como medio de instalación.

En lo que respecta a la categoría social definida en el reporte se encuentran varios puntos de interés. En la categoría de variedades de acciones sociales involucradas en violaciones de datos se encuentra en el primer puesto el phishing, seguido de pretexto, soborno, extorsión, falsificación, influencia y otros. Otra información interesante que brinda el reporte se puede observar en la Ilustración 1.1 que refleja cómo la tasa de clicks ha decrecido del 2012 al 2018 en los ejercicios de phishing autorizados en las organizaciones[6].

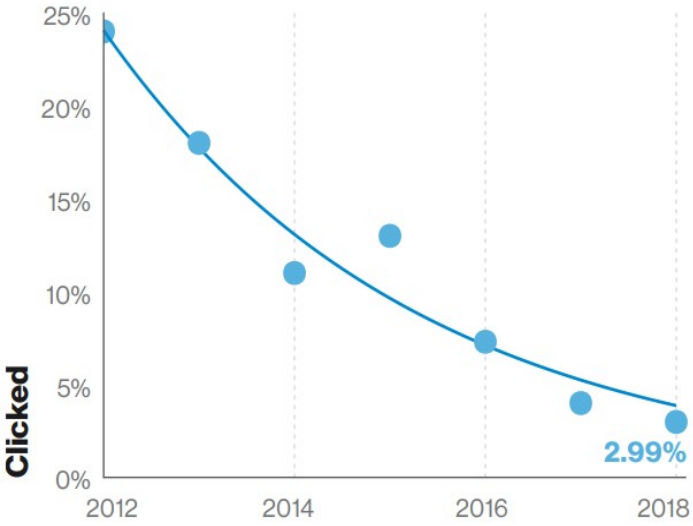

Ilustración 1.1: Tasa de clicks en el tiempo en ejercicios de phishing autorizados.

1.5. Técnicas utilizadas para influenciar y persuadir

El proceso utilizado para hacer que alguien quiera hacer algo, reaccione, piense o crea en la forma que uno quiera se da a través de la influencia y la persuasión [3].

En la ingeniería social existen varias técnicas para influenciar y persuadir al objetivo que van a ser brevemente descriptas a continuación.

1.5.1. Encuadre

Para entender el mundo, las personas utilizan una serie de filtros mentales que crean a través de influencias biológicas y culturales. A estas interpretaciones de la realidad se las llama encuadre y los individuos se ven influenciados por sus propios encuadres a la hora de realizar decisiones. En más detalle, el encuadre es la conjunción de las experiencias nuestras y de las experiencias de otras personas que nos permitimos en forma consciente alterar la forma en la que tomamos las decisiones.

Desde el punto de vista de la ingeniería social, el encuadre es clave ya que si es posible alterar la información que el objetivo toma en cuenta entonces es posible modificar la toma de decisiones del mismo para que sean las que el ingeniero social desee. Esto puede llevar a toma de decisiones que terminen en una violación de seguridad exitosa por parte de un ingeniero social malicioso [7].

1.5.2. Elicitación

Para poder recolectar información del objetivo de manera discreta y sin levantar sospechas se utiliza la técnica denominada elicitación. Esta técnica tiene la particularidad que usualmente no se presenta de una manera amenazante sino que pasa de forma desapercibida, es fácilmente negable su utilización y es bastante efectiva. La elecitación consiste en establecer una conversación con el individuo, ya sea en persona, en forma telefónica o por escrito, apelando a diferentes técnicas para explotar ciertas predisposiciones humanas para que así el objetivo revele la información buscada sin darse cuenta de que lo ha hecho [8].

Las tendencias naturales humanas que un ingeniero social entrenado busca explotar son bastantes. Primeramente, se tiene la aspiración de ser cortés y servicial con las personas, incluso cuando las mismas son completos extraños. Luego se tiene el deseo de cada individuo de mostrarse como alguien bien informado sobre un tema particular, como puede ser la profesión que desempeña, y de convertir al otro a nuestra opinión. En adición a lo anterior, se posee la tendencia de subestimar el valor de la información dada especialmente cuando no se está familiarizado con las maneras malintencionadas en la que puede ser utilizada. Además, se tiene el interés de cada uno de ser tenido en cuenta y creer que se está contribuyendo a algo importante. Otra preferencia es la de expandirse sobre un tema particular cuando se brindan elogios o estímulos para así poder presumir. Una tendencia a mencionar es la relacionada a creer que los demás son honestos teniéndose así una aversión a ser desconfiados de los otros. También se tiene la inclinación a responder honradamente cuando se le realiza a alguien una pregunta explicitando que se quiere una respuesta honesta. Por último, están presente las tendencias de convencer a alguien de nuestra opinión, corregir a los demás y generar rumores [8].

1.5.3. Pretexto

Para poder obtener información privada muchas veces un atacante se presenta como alguien más esgrimiendo documentación, precedentes e historias elaboradas para respaldar esta falsa identidad, siendo esto enmarcado dentro del concepto de pretexto.

El pretexto que se desarrolla para un ataque es más efectivo cuando logra que la víctima desarrolle confianza hacia el atacante. Para esto el pretexto debe ser lo suficientemente sólido como para ser creíble y no levantar sospechas [9].

Debido a la efectividad y rapidez de este método, el mismo es muy popular entre periodistas, interrogadores, detectives privados y fuerzas armadas entre otros.

La complejidad del pretexto a desarrollar en una operación va a depender del objetivo a conseguir. El desarrollo del pretexto en cuanto a la creación del personaje puede partir de algo simple como ser amigable con la víctima hasta el punto de poseer diferentes elementos para soportar la identidad falsa como pueden ser páginas en redes sociales, publicaciones, registros públicos y documento de identidad.

Dentro del contexto de un ataque, más allá de la información que se posee del ambiente en que se maneja la víctima, el éxito del mismo depende en gran medida de la forma en que se implemente y esto es esencial con respecto al pretexto. Para esto es necesario tomar en cuenta cómo el atacante comunica esa información a través de su actuación, su tono de voz, estado de ánimo, lenguaje corporal e inclusive la forma de vestir del mismo. Todo esto es usualmente planeado por parte del ingeniero social a la hora de realizar su ataque [10].

1.5.4. Principios psicológicos

Muchos de los conceptos visto hasta ahora poseen su base en ciertos principios psicológicos que serán tratados a continuación.

Microexpresiones:

Cuando una persona se encuentre bajo estrés, los músculos de la cara realizan rápidamente pequeños movimientos involuntarios. Debido a la corta duración de los mismos, alrededor de 1/25 de segundo, los mismos son difíciles de ver y correlacionar con una emoción para aquél que no se encuentra entrenado adecuadamente. A pesar de su corta duración, ha sido demostrado que las microexpresiones muestran las emociones universales

como son la furia, el desprecio, el disgusto, el miedo, la alegría, la tristeza y la sorpresa [11].

Rapport:

Para lograr una rápida evolución de un vínculo positivo con alguien, el ingeniero social desarrolla lo que se denomina “rapport” que consiste en construir una relación con alguien que incluya elementos tales como el mutuo agrado y confort. Con esto el ingeniero social puede hacer que la persona se sienta cómoda compartiendo información con él y que luego de la interacción se sienta de mejor humor haciendo que la misma no cuestione las acciones realizadas evitando así ser descubierto el accionar del ingeniero social [12].

Entrevista e interrogación:

Ciertas situaciones pueden ser enmarcadas dentro de los parámetros de una entrevista o una interrogación. La principal diferencia existente entre las mismas es que en una de ellas, la entrevista, la persona entrevistada se encuentra cómoda tanto en el aspecto físico como en el psicológico. En cambio en la interrogación se busca la incomodidad psicológica a través de las preguntas realizadas, entre otros recursos, y/o se crea incomodidad en el lugar físico.

La interrogación tiene como objetivo crear presión sobre la persona con la meta de obtener algún conocimiento que la misma posea. Las técnicas empleadas para esto, principios de interrogación, son parte del repertorio de los ingenieros sociales para obtener información de una persona de forma fácil [3].

Evidencia social:

A la hora de determinar cuál es el comportamiento correcto en una situación que no es familiar, las personas ven un comportamiento como más correcto cuando ven a otros realizándolo. A este principio se lo denomina evidencia social o influencia social informativa y aplica especialmente a la manera en que una persona decide lo que constituye un comportamiento correcto.

En la mayoría de los casos, la tendencia a ver una acción como más apropiada mientras más personas la realizan funciona bien ya que nos lleva a cometer menos errores. Sin embargo, esta característica del principio hace que sea en forma simultánea su mayor fortaleza como así también su mayor debilidad ya que oportunistas pueden explotarlo para influenciar el comportamiento de una persona en una determinada situación [13].

1.6. Herramientas utilizadas en la ingeniería social

A la hora de analizar las herramientas utilizadas en la ingeniería social se tiene un amplio espectro que puede ser dividido en las herramientas físicas y las herramientas informáticas.

Dentro de las herramientas físicas se tienen aquellas utilizadas para la apertura de candados. Un candado funciona básicamente cuando la llave es insertada, se alinean los pernos internos y esto permite girar el cilindro. Las herramientas físicas utilizadas para simular una llave en los candados son las ganzúas y los tensores. La ganzúa permite alinear los pernos internos y los tensores permiten girar el cilindro.

Aparte de lo mencionado para candados tradicionales existen diferentes herramientas y métodos para vulnerar candados magnéticos y electrónicos. Además de esto, se presentan herramientas más desarrolladas tecnológicamente a la hora de interactuar con cerraduras activadas por RFID (Identificación por Radiofrecuencia) que para ser vulneradas se utilizan herramientas como lectoras y copiadoras de RFID.

Otras herramientas utilizadas son los dispositivos que permiten la grabación de audio y de video. Estos cumplen un rol importante en lo que son las auditorías de ingeniería social ya que permiten por un lado recopilar pruebas de los ataques que fueron exitosos, evitando así la negación de lo sucedido por personas que no quieren reconocer que han cometido un error que llevó a que un ataque fuera exitoso. Por otro lado, se utiliza la grabación de video para resguardo ya que a la hora de analizar los detalles, las expresiones faciales y las microexpresiones no se depende exclusivamente de la memoria del ingeniero social sino que se tiene el material grabado para un análisis posterior más profundo y detallado.

Además de lo mencionado, se tienen los rastreadores de GPS que utilizan los ingenieros sociales para conocer más a sus objetivos. Se puede conocer mucha información sobre una persona sabiendo cuáles son las paradas que realiza en su camino o cuando comienza y termina su día entre otras cosas. Armados con esta información el ingeniero social puede desarrollar pretextos más efectivos o realizar mejores preguntas para elicitar la información correcta del objetivo [3].

Dentro de las herramientas informáticas se encuentran aquellas utilizadas para la recopilación de la información, tema desarrollado en el punto “3 Herramientas informáticas utilizadas en la recopilación de información”, y aquellas utilizadas para realizar ataques, tema desarrollado en el punto “4 Herramientas informáticas utilizadas en ataques”.

2. Análisis de las etapas de un ataque de ingeniería social

A la hora de realizar un ataque se tiene que tanto un ingeniero social malicioso como uno que ayuda a los clientes a través de auditorías de seguridad siguen ciertas etapas en la planificación y ejecución que se encuentran descriptas en la Ilustración 2.1.

Ilustración 2.1: Etapas de planificación y ejecución de un ataque ingeniería social [14].

2.1. Recopilación de información

La primer parte de la pirámide, y la que más tiempo representa de las etapas, es lo relacionado a la recopilación de información que puede ser

extraída de las fuentes abiertas de inteligencia, denominadas OSINT por sus siglas en inglés[4] [14].

Esta primera parte es de suma importancia y Christopher Hadnagy lo manifiesta en el mantra del ingeniero social que es “soy solamente tan bueno como la información que recolecto”[5][3].

Se va a tratar este tema en profundidad en el punto “3 Herramientas informáticas utilizadas en la recopilación de información”.

2.2. Desarrollo del pretexto

Para poder desarrollar un pretexto de forma exitosa es necesario haber realizado una buena búsqueda de información en la etapa previa. En la presente etapa se realiza el desarrollo de lo que va a ser el pretexto en conjunto con la definición de la elección de las herramientas necesarias para soportarlo [14].

2.3. Diagramación del ataque

En esta etapa lo que se busca es primeramente definir qué es lo que se desea alcanzar como resultado final y cómo lograr esto. Las definiciones necesarias pueden ser encontradas en las respuestas a las siguientes preguntas: ¿cuál es el plan?, ¿cuál es el objetivo? y ¿qué es lo que el cliente quiere?

Como segundo paso, es muy importante establecer cuándo es el mejor momento para lanzar el ataque para así alcanzar los mejores resultados. Finalmente, es clave definir de antemano quienes deben estar

4 Open-source Intelligence

5 Traducción propia del inglés: “*The social engineer’s mantra is, “I am only as good as the information I gather.”*”

disponibles para tomar acción inmediatamente en caso de necesitar soporte o asistencia [14].

2.4. Realización del ataque

El siguiente paso es la ejecución del ataque en sí, en donde se pone en práctica lo preparado. En este punto se sigue lo previamente definido pero múltiples variables son impredecibles especialmente cuando se está interactuando con las personas. Por esta razón se tiende a evitar tener un diálogo estrictamente guionado para privilegiar más la definición de un camino a seguir en donde la improvisación ocupa un lugar importante [14].

2.5. Reporte

Básicamente el reporte es lo único que se le entrega al cliente y por ende es necesario que el mismo refleje lo realizado de la mejor manera. Aquí se debe ser lo más expeditivo para que el cliente reciba la información en donde se detallen los problemas que fueron identificados y las posibilidades que existen para solucionar los mismos [14].

3. Herramientas informáticas utilizadas en la recopilación de información

En este capítulo se realiza la descripción de diferentes técnicas y herramientas utilizadas durante la etapa de recopilación de información. Se lleva a cabo principalmente la enumeración de las herramientas disponibles en sus versiones libres y gratuitas utilizadas hoy en día para Ethical hacking.

Esta etapa puede ser tanto pasiva como activa. En el caso de la forma pasiva se evita interactuar con el sistema del objetivo en forma directa o se lo hace de una manera que el sistema no lo interpreta como algo intrusivo. En el caso de la forma activa se entabla una interacción directa e intrusiva con el sistema que puede generar alarmas y precipitar alguna defensa por parte del objetivo. El enfoque utilizado consta en detallar la recopilación de información en la etapa en forma pasiva y semi-pasiva de tal manera que en el sistema objetivo quede el mínimo rastro de la actividad y éste sea difícil de relacionar a un ataque malicioso.

Para llevar a cabo la recopilación existen diferentes técnicas y herramientas que van a ser descriptas a continuación.

3.1. Buscadores web

Una de las formas de recopilar información es mediante buscadores web. Estos pueden ayudar a descubrir contenido indexado que se encuentra público y sin restricción de acceso.

3.1.1. Google hacking

El buscador Google posee una amplia capacidad de realizar web-crawling que consiste en inspeccionar las páginas webs para indexar el contenido que encuentre allí publicado. Es en este punto en donde se

convierte en una herramienta especial para el ingeniero social ya que la información publicada puede incluir información relevante o incluso información sensible del objetivo del ataque en cuestión[15].

Para acceder a esta información se realizan consultas al buscador de internet diseñadas de tal manera que devuelvan como respuesta la información relevante que indexó el buscador sobre el sitio de interés. A este proceso se le llama “Google Hacks” o “Google Dorks” entre otras denominaciones.

Dentro del repositorio público de exploits llamado “Exploit Database” se encuentra una sección denominada GHDB (Google Hacking DataBase) en donde se encuentran diferentes formas de realizar búsquedas en Google que den como resultado información hecha pública por el crawler de Google. Algunas de las categorías que se pueden encontrar en este repositorio son archivos sensibles, servidores vulnerables, mensajes de error e información de redes o vulnerabilidades entre otras[16].

3.1.2. Shodan

Los dispositivos que se encuentran conectados públicamente a la Internet corren servicios entre los cuales se pueden nombrar SSH, FTP, SNMP, Telnet, RTSP, IMAP y HTTP. Ante una consulta a los dispositivos, los mismos responden con información que ofrecen para poder realizar una conexión correcta y en esta respuesta se encuentra un objeto de los servicios llamado banner. En el banner se puede encontrar diferentes tipos de información como puede ser el sistema operativo que está corriendo el dispositivo y su versión. Solo con esta información ya se pueden encontrar versiones de sistemas operativos que tengan vulnerabilidades críticas reportadas permitiendo su ataque efectivo[17].

A la hora de obtener la información del banner se puede realizar en forma directa, realizando una consulta al dispositivo, o en forma directa utilizando una herramienta de un tercero para que realice la consulta. De

esta última forma solo queda registrada la interacción de la herramienta con el sistema de interés y no queda registrada la interacción del usuario final como en el caso de la forma directa[18].

Una de las herramientas que realiza la obtención de información del banner de dispositivos conectados a internet es Shodan. Esta herramienta busca sistemáticamente y constantemente internet con su crawler indexando información sobre los banners de los dispositivos conectados a internet. Un usuario de esta herramienta puede entrar luego al buscador y consultar la base de datos del mismo con respecto a dispositivos con ciertas características que resulten de interés. Una de las principales diferencias que presenta este buscador con respecto a Google es que este último solo indexa resultados de la World Wide Web y en cambio el primero indexa resultado sobre la Internet[17].

Para utilizar la herramienta se tiene la posibilidad de hacerlo de forma gratuita con ciertas limitaciones o se puede contratar algún plan que amplíe diferentes parámetros para realizar búsquedas de mayor amplitud y contar con servicios adicionales por parte de Shodan.

3.2. Información de dominio de internet

A continuación se va a realizar la enumeración de las diferentes herramientas por comando que pueden ser utilizadas principalmente en los sistemas operativos Unix y Linux.

3.2.1. Dig

Con el comando dig (domain information groper) se tiene la posibilidad de consultar la información de DNS (Domain Name Server) que tenga almacenada el servidor público de interés. Con la utilización de esta herramienta no solo se puede estar obteniendo información del servidor de

nombres sino que además se puede obtener información de servidores de correo[19][20].

3.2.2. Ping

A la hora de determinar la disposición de la comunicación con un sistema conectado se utiliza el comando ping. Lo que hace ping es enviar un ICMP echo request a la dirección señalada del dispositivo para así obtener una respuesta del mismo. Como resultado se puede determinar si el objetivo se encuentra conectado, responde los ICMP echo requests, el delay existente en la respuesta, la existencia de pérdidas de paquetes por mala conexión, descubrimiento de información del dominio objetivo y demás datos[19].

3.2.3. Host

El comando host permite realizar consultas de DNS que brindan información sobre los distintos tipos de registros DNS del servidor y la IP del dominio objetivo y viceversa[19].

3.2.4. Whois

El comando whois permite realizar consultas a la base de datos WHOIS en donde se encuentran la información sobre los dueños de los dominios de internet. De esta base de datos se puede estar encontrando datos de los dueños tales como direcciones de email, teléfonos, domicilios, nombres completos y demás[19].

3.2.5. Nmap

A la hora de realizar el descubrimiento de los dispositivos conectados a una red en diferentes contextos, como puede ser una auditoria de seguridad, una de las herramientas principales a utilizar es Nmap (Network Mapper). Esta herramienta funciona tomando la información que brindan los paquetes IP para determinar los diferentes hosts que se encuentran conectados a la red en cuestión, los sistemas operativos y sus versiones que se encuentran corriendo, el nombre de los servicios en funcionamiento en conjunto con su versión y el tipo de filtrado de paquete que se está realizando entre otras características que se pueden recopilar[21].

Para realizar una recopilación de datos semi-pasiva es necesario correr los comandos con los parámetros acordes para que la actividad no sea clasificada como sospechosa por parte del objetivo.

3.2.6. Traceroute

El comando traceroute es utilizado en diferentes áreas como puede ser la administración de sistemas y redes e investigadores de seguridad por el hecho que puede encontrar la ruta que se establece entre un dispositivo de origen y el destino con el que este se quiere comunicar. Además de esto, permite descubrir las conexiones establecidas entre los hosts [19].

3.2.7. Mtr

Combinando la funcionalidad de traceroute con cierta información que brinda ping, el comando mtr (My Traceroute) brinda datos sobre la ruta entre origen y destino de una conexión con el adicional de contar con información sobre tiempos de respuesta, pérdida de paquetes y saturación de los enlaces entre otros datos[19].

3.3. Información de metadatos

Cuando se genera o modifica un documento se le adiciona al mismo, muchas veces de manera no intencionada, información que se denominada metadatos. Los datos que pueden brindar los metadatos pueden ser por ejemplo el autor del documento, la fecha y hora cuando se realizó la última modificación, la cantidad de revisiones que se han realizado del documento y demás. La metadata puede brindar información sobre diferentes aspectos dependiendo del tipo de archivo como puede ser que en ciertas fotografías se pueden encontrar las coordenadas GPS en donde las mismas fueron tomadas y el tipo de cámaras entre otros datos[14].

A la hora de realizar la extracción de los metadatos, dentro de las herramientas existentes se cuenta con FOCA (Fingerprinting Organizations with Collected Archives) que permite llevar a cabo el análisis de metadatos de diferentes documentos que se encuentren en forma local o como resultado de una búsqueda en dominio web de interés. Luego de extraer los metadatos la herramienta busca identificar diferentes datos como pueden ser los usuarios, software, sistemas operativos, impresoras, carpetas y demás[22].

3.4. Herramientas OSINT

OSINT es Open Source Intelligence que implica todas las fuentes de información públicamente disponibles que pueden ser recolectadas. A continuación se va a realizar la descripción de las herramientas más relevantes que hacen uso de esto.

3.4.1. OSINT Framework

La herramienta OSINT Framework se encuentra en un sitio web en el cual brinda enlaces a diferentes buscadores, recursos y herramientas de OSINT en general que en la mayoría de los casos son gratuitas[23].

3.4.2. Awesome OSINT

La herramienta Awesome OSINT se encuentra en la plataforma GitHub y consiste en un amplio listado de enlaces a páginas web que permiten acceder a recursos de información públicamente disponibles[24].

3.4.3. Discover

La herramienta Discover cuyo repositorio se encuentra en la plataforma GitHub consiste en un grupo de scripts de bash utilizados para la automatización de diferentes acciones entre las que se encuentra la función de recopilación de información. El dominio que realiza a cabo lo anterior se denomina RECON y dentro del mismo se encuentran diferentes opciones como reconocimiento pasivo. Para esto se utilizan las herramientas ARIN, dnsrecon, goofile, goog-mail, goohost, theHarvester, Metasploit, URLCrazy, Whois, multiple websites, y recon-ng[25].

3.4.4. Recon-ng

La herramienta Recon-ng es un marco operativo que permite realizar tareas de reconocimiento sobre fuentes abiertas web. Esta herramienta permite agregarle módulos los cuáles son variados sobre diferentes fuentes de información que pueden explorar[23][26].

3.4.5. TheHarvester

La herramienta TheHarvester cuyo repositorio se encuentra en la plataforma GitHub permite realizar la recolección de información de diferentes fuentes públicas de información sobre un objetivo. Entre los resultados que se obtienen del uso de la herramienta se pueden encontrar subdominios, IPs, URLs, nombre de personas del objetivo y correos electrónicos entre otros[27].

3.4.6. Maltego

El software Maltego es una herramienta que permite recolectar información del objetivo de diferentes OSINTs. A la hora de realizar la recolección utiliza plug-in llamados transformadas que permiten la recolección especifica de datos. Luego la información resultante puede ser observada gráficamente relacionada entre sí por conectores y en tiempo real en algunos casos[23].

4. Herramientas informáticas utilizadas en ataques

En este capítulo se van a analizar los diferentes métodos de ataque que pueden ser llevados a cabo tanto en forma individual como combinados.

4.1. Phishing

Según los autores Christopher Hadnagy y Michele Fincher, phishing se define como la "práctica de enviar correos electrónicos aparantando ser originados de fuentes reputables con el objetivo de influenciar u obtener información personal"[6][28].

Con respecto a los objetivos englobados en la influencia sobre la víctima, se pueden dirigir a que la misma realice una acción concreta. Una de las acciones más comunes que espera el atacante sea realizada es que la víctima acceda a un sitio web fraudulento haciendo click sobre un link que se encuentra en el cuerpo del correo electrónico. Otra acción es que el que recibe el mail abra el material adjunto permitiendo que un malware sea instalado y ejecutado en el terminal del usuario. Todas estas acciones llevan a que el atacante pueda acceder a información sensible y/o pueda ejecutar acciones en el terminal afectado.

Para lograr mayor credibilidad con respecto a los URL maliciosos el atacante usualmente compra dominios que se asemejan mucho a la direcciones de páginas web legítimas difiriendo en el deletreo o cambiando algún campo de la dirección. Otro recurso es la utilización de URL cortos que tienen como destino una página web fraudulenta bajo el dominio del atacantes para robar información o instalar malware entre otros usos.

Otra estrategia que toman los atacantes para ganar mayor credibilidad es utilizar como pretexto representar a instituciones, personas con autoridad o alguien con un rol en un evento actual relevante dentro del

6 Traducción propia del inglés: "*...practice of sending e-mails that appear to be from reputable sources with the goal of influencing or gaining personal information.*"

contexto de la víctima. Dentro de este último ítem, los eventos pueden ser desastres naturales, celebraciones nacionales, grandes incidentes de seguridad, grandes eventos públicos o una pandemia entre otros[29].

Dejando de lado el envío masivo del mismo tipo de mail para la realización de phishing, agentes maliciosos desarrollaron una técnica de ataque más enfocada en ciertas víctimas para hacer envío de mail de phishing. A esta técnica se le llama spear phishing y tiene objetivos específicos de alto perfil que dentro de una organización puede tener acceso a diferentes sistemas, algo muy valioso para un criminal. Para que el ataque realizado sea efectivo el criminal se apoya mucho en buscar información relevante sobre la víctima. Teniendo en cuenta esta información se puede diseñar un mail de phishing que pueda resultar más interesante al objetivo y lo influencie para que cometa la acción deseada.

Otra técnica de ataque de phishing consiste en realizar phishing sobre un objetivo individual de un valor muy alto dentro de una organización y a esto se lo denomina whaling. Estos individuos suelen ser ejecutivos de mucho poder en organizaciones o funcionarios de alto nivel en un gobierno, solo por nombrar algunos, que pueden tener acceso a información confidencial de mucho valor. Para este tipo de ataque es clave la recolección de información que se realice sobre el individuo ya que va a tener solo a esta persona como víctima[29].

Dentro de las diferentes herramientas para llevar a cabo un ataque de Phishing se encuentra la plataforma Social-Engineer Toolkit (SET). Entre sus muchas funcionalidades por defecto, en la versión 8.0.3, se pueden seleccionar diferentes vectores de ataques de phishing. Uno de ellos es el ataque masivo que se encuentra en la opción “Mass Mailer Attack” en el menú principal de ataques de ingeniería social. Allí la herramienta presenta dos opciones dentro de las cuales se encuentra la posibilidad de enviar mails en forma masiva eligiendo “E-Mail Attack Mass Mailer” o la opción de atacar a una sola dirección de correo electrónico. El siguiente paso es la creación del cuerpo del correo electrónico en donde se incluye el enlace a la dirección

del dominio web donde se implementa el mecanismo para el robo de la información o la descarga de un malware entre otras opciones.

En la categoría de spear phishing en “Spear-Phishing Attack Vectors” se ingresa desde el menú principal en la sección “Social-Engineering Attacks”. Esta opción permite a un pentester la creación de correo electrónico para ser enviado a muchos destinatarios o solo a un grupo pequeño de ellos. Además, brinda la posibilidad de la utilización de payloads creados a medida por parte del usuario seleccionando la opcióno “Create a FileFormat Paylod”. Eligiendo la opción “Perform a Mass Email Attack” se pueden utilizar los payloads por defecto de la plataforma[30].

4.2. Vishing

Cuando se realiza un ataque de ingeniería social para elicitar información valiosa o para influenciar a la víctima así realiza una acción a través de una comunicación telefónica, se está hablando entonces de lo que se denomina vishing. Para darle más credibilidad los atacantes utilizan técnicas de pretexto para hacerle creer a la víctima por ejemplo que son parte de soporte técnico de la organización, una figura de autoridad o un colega de trabajo entre otros perfiles. Para cada una de estas personificaciones se realiza la recopilación de información correspondiente, tanto del rol del pretexto como del perfil de la víctima, para darle validez y efectividad cuando se lleva a cabo un ataque.

En adición a lo anterior, el atacante se sirve de diferentes herramientas para hacer un ataque exitoso. Primeramente utiliza una forma de comunicación que puede ser a través de una línea telefónica fija, una línea de celular o un servidor de VoIP. El número de origen de la llamada puede ser fraudulento, privado o incluso bloqueado. Para lograr lo anterior se utilizan diferentes herramientas. Adicionalmente el atacante puede utilizar

aplicaciones que le permitan realizar cambios de voz para ayudar a una personificación más creíble y/o para ocultar su identidad[31].

4.3. SMiShing

Si a la hora de realizar un ataque de ingeniería social se utilizan SMS (Short Message Service) para hacer que la víctima tome una acción inmediata se está hablando entonces de SMiShing. Las acciones inmediatas que se implican pueden ser la visita a sitios web maliciosos, la descarga de malware para móviles o un llamado a un número de teléfono fraudulento. Con estas acciones lo que buscan los criminales es que el objetivo entregue información personal que ellos luego pueden utilizar para cometer crímenes.

Las herramientas utilizadas para este tipo de ataques permiten realizar la emisión de SMS a diferentes clientes de telefónica celular y la emisión puede llegar a ser limitada a ciertas regiones geográficas. Para llevar a cabo esto existen servicios en EEUU y Canadá entre los que se destacan BurnerApp y SpoofCard que permiten enviar SMS utilizando números de teléfono suplantados[32].

4.4. Baiting

Los ataques de baiting se aprovechan de la ambición y/o curiosidad de las personas para poder ganar acceso a información sensible o tomar control de sistemas. Un ejemplo de un ataque de baiting consiste en dejar una o varias memorias USB tiradas en diferentes lugares que llamen la atención de los empleados de la organización objetivo. Estas memorias puede que además se encuentren con alguna identificación relacionada a la organización como ser algún rótulo relevante que le de más legitimidad. El atacante espera que el empleado que encuentre esta memoria USB, motivado por la curiosidad, realice la conexión de la misma a un terminal de

la organización y así poder introducir malware que permita al criminal tomar control o robar información sensible de la organización[33].

Para ataques básicos se pueden utilizar memorias USB estándar infectadas con malware para ser instalado automáticamente. Para ataques más avanzados, una de las posibilidades es contar con el hardware USB Rubber Ducky que se hace pasar como un USB HID (Human Interface Device) que el sistema reconoce como un teclado USB. Esto da la posibilidad de instalar backdoors, robar contraseñas y sustraer documentos electrónicos entre otras acciones[34].

5. Prevención y mitigación de ataques de ingeniería social

En el siguiente capítulo se realizará una recolección de las diferentes medidas que una organización puede tomar para poder prevenir y mitigar efectivamente los ataques de ingeniería social.

A la hora de tomar acciones para reforzar la seguridad de una organización con respecto a la ingeniería social hay dos aspectos principales que deben ser fortalecidos paralelamente. Uno de estos aspectos son los miembros de la organización que deben ser educados, entrenados y puestos a prueba para identificar y responder adecuadamente ante ataques de ingeniería social. El otro aspecto que contar con las solución técnicas de seguridad informática actualizadas para así lograr una protección integral de los sistemas en conjunto con la correcta preparación de sus usuarios.

Las etapas detalladas y su orden de aplicación se basan en las descriptas por el ingeniero social Christopher Hadnagy en sus diferentes libros.

5.1. Identificación de ataques de ingeniería social

El primer paso a realizar para poder protegerse frente a un ataque de ingeniería social es poder reconocerlos. Para esto los individuos de una organización necesitan entender cómo se desarrollan los mismos, cuáles son los objetivos que busca un atacante y cómo un ataque afecta en la vida real a la persona en su puesto de trabajo particular.

Una de los principales puntos que una persona debe saber sobre un ataque de ingeniería social es el valor de la información que poseen y cuáles pueden ser las consecuencias de compartir la misma con un atacante. Muchas veces los atacantes juegan con la percepción de la víctima sobre la importancia de cierta información para así obtener la misma sin ningún esfuerzo por parte del objetivo para protegerla. Si el empleado es educado

para saber el valor de la información se tiene una posibilidad de que el mismo pueda solicitar los requisitos pertinentes antes de compartirla.

En adición a lo anterior, la persona debe ser atenta a la hora de observar diferentes aspectos de un atacante. En este sentido se hace referencia a la expresión corporal, las expresiones faciales, las frases utilizadas y el tono de voz entre otros muchos factores que componen un ataque de ingeniería social.

La educación de los empleados sobre los diferentes ataques debe ser realizada en forma periódica para así mantener los conocimientos adquiridos y aprender nuevos. Con esto, mientras un empleado conozca más sobre los ataques de ingeniería social que puedan suceder, más fácil le va a resultar identificarlos y mejor va a ser el nivel de seguridad que la organización va a poder contar[3][14].

5.2. Desarrollo de políticas de seguridad

El siguiente paso luego de que un empleado pueda reconocer un ataque de ingeniería social es realizar un desarrollo de políticas se puedan aplicar y que apliquen al mundo real. La aplicación efectiva de este paso va a permitir el desarrollo de una base sólida a partir de la cuál se pueda progresar en la madurez de la organización en cuanto a la seguridad informática.

A la hora de desarrollar una política de seguridad se deben tener en cuenta diferentes factores para que la misma sea efectiva y aplicable. Uno de los factores es que le permita al empleado entender la política sin dejar lugar a dudas en base a su educación. Es decir, que la política no debería dejar lugar para una mala interpretación que ante un ataque resulte en la toma de decisiones incorrectas con graves consecuencias. La política debe ser simple para lograr un buen entendimiento y lo suficientemente amplia para tener en cuenta los diferentes escenarios y variantes de una ataque.

Un aspecto a tomar en cuenta a la hora del desarrollo de políticas es que en el mundo real las mismas pueden llegar a ser ignoradas si un ingeniero social habilidoso logra explotar la empatía de su víctima. Teniendo en cuenta este escenario las políticas deben establecer claramente la necesidad de autenticar siempre las personas antes de permitirle el acceso a diferentes lugares físicos o sistemas.

Para ayudar a reforzar la aplicación de ciertos aspectos de las políticas definidas es sugerido el desarrollo de guías a seguir cuando un empleado se encuentra bajo un ataque de ingeniería social. Estas guías deben sugerir un camino a seguir con respecto a qué es lo que debe decir y que acciones debe tomar para así darle la posibilidad de tener la situación bajo control y aplicar el pensamiento crítico[3][14].

5.3. Aplicación de auditorias de ingeniería social

Asumiendo la aplicación de los pasos anteriormente descriptos a esta altura se debería tener gente educada en la organización para saber qué es lo que implica un ataque de ingeniería social. Además, ya se debería contar con políticas que permitan a un empleado saber cómo reaccionar correctamente frente a un ataque. El siguiente paso en esta secuencia es poner a prueba con situaciones reales todo lo anteriormente descripto a través de una auditoria de ingeniería social. La auditoría va a permitir saber si realmente se está avanzando bien con respecto a los objetivos previamente planteados, si los dispuesto se adaptada al mundo real y si se posee algún problema que exponga a la organización ante futuros ataques.

A la hora de elegir la compañía con la cual llevar a cabo la auditoria es necesario realizar una evaluación detallada de la misma, los antecedentes, la reputación y las experiencias que han tenido los clientes que la han contratado en los últimos tiempos. Luego, de la elección de la empresa que realizará la auditoría es sumamente importante realizar una puesta en común entre las partes para definir los objetivos que se buscan

alcanzar con la auditoría y por sobre todo establecer claramente cuáles van a ser los límites para llevar a cabo las pruebas. La no realización de este paso en detalle puede generar consecuencias no deseadas tanto para la empresa que lleva a cabo la auditoría como para el cliente.

En base al contexto, se debe realizar la definición de cuáles son los diferentes servicios que se quieren aplicar en la auditoría a llevar a cabo. Otro parámetro a definir es la periodicidad con la que las pruebas definidas se van a llevar a cabo dependiendo de las prioridades de la organización cliente y/o de los resultados obtenidos en las auditorías previas de seguridad[14].

5.4. Desarrollo de cultura de la seguridad

Con todos los pasos previos implementados el último que queda por ver en detalle es la creación y mantenimiento de una cultura de la seguridad en todos y cada unos de los empleados de la organización. Una de la formas de alcanzar a todos los empleados con esto es realizar una formación en seguridad que no sea solo sobre el ámbito laboral sino también en el terreno de lo personal. Para esto es recomendable enseñar a los usuarios sobre los riesgos de seguridad que se pueden tener en el uso del acceso electrónico a cuentas bancarias personales, la utilización de su computadora personal como de su teléfono inteligente. Esto puede llegar a desarrollar un compromiso individual con la seguridad del cuál la organización puede beneficiarse.

Se tienen varios recursos que tienen la posibilidad de ser utilizados dentro del ambiente laboral para poder adoptar una cultura de la seguridad. Uno de ellos es recompensar a los empleados por conductas positivas hacia la seguridad. Otro recurso es distinguir públicamente a quien haya realizado acciones correctas de seguridad. Además de esto, se pueden definir capacitaciones periódicas enmarcadas dentro de diferentes contextos para que sean más atractivas para los empleados. Para lo anterior se pueden

nombrar las modalidades en donde durante la capacitación se ofrece una comida, como un almuerzo, o se realizan juegos centrados en la seguridad dentro de otras modalidades. Por último, algo que es muy importante es contar no solo con el apoyo público por parte de la alta gerencia sino también contar con la participación de la misma tanto en los eventos de capacitación como de las pruebas realizadas dentro del marco de auditorías de seguridad[3][14].

5.5. Aplicación de soluciones técnicas de seguridad avanzada

Hasta ahora todos los pasos nombrados anteriormente necesitan estar acompañados por soluciones técnicas de seguridad avanzada. Es decir, que la organización no solo debe entrenar a sus empleados con respecto a la seguridad sino que todo esto debiera ser llevado a cabo con una sólida base de protección de los activos con los sistemas de seguridad mínimos.

Para la protección de los activos se necesita contar con un presupuesto que permita la adquisición de soluciones tales como firewalls, programas de antivirus, sistemas de prevención y detección de intrusiones y demás recursos. Todo esto permite proteger tanto el perímetro externo de los posibles ataques como de las amenazas que surjan dentro de la red interna.

Además de lo anterior, es necesario contar una política de actualización de software que permita contar lo antes posible con la última versión del mismo. Esto tiene como principal medida evitar que los atacantes puedan explotar vulnerabilidades públicamente conocidas de versiones anteriores del software en cuestión. La acción de mantener constantemente actualizados los software utilizados por la organización tiene un costo mucho menor que ser víctima de un ataque exitoso en la organización[3][14].

Conclusiones

La relevancia actual de la ingeniería social es indiscutible y se puede observar en el día a día en las diferentes noticias alrededor del mundo. Esto queda demostrado en las estadísticas recopiladas por diferentes organizaciones en sus reportes. Por ende es de esperarse que esta área de la seguridad informática continúe su desarrollo en los tiempos que vienen.

La principal característica de la ingeniería social es la explotación de las personas apoyándose en las herramientas información de hoy en día. Esto hace que la resolución de las vulnerabilidades inherentes de las personas sea todo un desafío a resolver. Para esto es necesario tomar conciencia por parte de las organizaciones de la seriedad del asunto y estar a la altura de lo requerido para tener las suficientes defensas para así sobrevivir a los ataques de los ingenieros sociales.

Los temas que abarca el área de la ingeniería social son muy amplios. Analizando un poco la evolución de esta materia se ve un claro avance en la maduración de los temas relacionados a la psicología acompañado del desarrollo de herramientas para hacer la explotación más efectiva de los mismos. En base a esto, solo queda esperar un avance mayor a futuro logrando una mejor comprensión de la naturaleza humana, sus vulnerabilidades y las formas que pueden ser protegidas.

Las diferentes herramientas informáticas que se desarrollan en el presente para ser aplicadas en el campo de la ingeniería social son sumamente diversas y numerosas. Dado que la tendencia en la tecnología de consumo es brindar más formas de conexión para compartir información, es lógico anticipar que una mayor cantidad de herramientas van a ser desarrolladas para poder obtener la información de las personas y sacar provecho de esto a través de los ataques de ingeniería social.

Para concluir, desde mi punto de vista la ingeniería social va a seguir ganando relevancia en la seguridad informática y mayor va a ser la demanda

de conocimientos y estudios en esta área. El futuro va a representar un verdadero desafío para las personas y por sobre todo para las organizaciones ya que las que estén mejor preparadas para enfrentar un ataque van a poder ganarse la confianza y lealtad de sus clientes.

Bibliografía

Bibliografía específica

[1] Social-Engineer, Inc., "Social Engineering Defined". [En línea]. Disponible en: https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/. [Consultado: 21-mar-2019]

[2] Social-Engineer, Inc., "Everyday People - Categories of Social Engineers". [En línea]. Disponible en: https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/everyday-people/. [Consultado: 25-mar-2019]

[3] C. Hadnagy, *Social Engineering: The Art of Human Hacking*, First edition. Indianapolis, Indiana: Wiley Publishing, 2011.

[4] Social-Engineer, Inc., "Penetration testers - Categories of Social Engineers". [En línea]. Disponible en: https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/penetration-testers/. [Consultado: 03-abr-2019]

[5] Social-Engineer, Inc., "Why Attackers Might Use Social Engineering". [En línea]. Disponible en: https://www.social-engineer.org/framework/general-discussion/attackers-might-use-social-engineering/. [Consultado: 26-mar-2019]

[6] Verizon, "2019 Data Breach Investigations Report". [En línea]. Disponible en: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf. [Consultado: 01-mar-2020]

[7] Social-Engineer, Inc., "Framing". [En línea]. Disponible en: https://www.social-engineer.org/framework/influencing-others/framing/. [Consultado: 31-mar-2019]

[8] Federal Bureau of Investigation, "Elicitation Techniques". [En línea]. Disponible en: https://www.fbi.gov/file-repository/elicitation-brochure.pdf/view. [Consultado: 27-mar-2019]

[9] Social-Engineer, Inc., "Pretexting". [En línea]. Disponible en: https://www.social-engineer.org/framework/influencing-others/pretexting/. [Consultado: 27-mar-2019]

[10] Social-Engineer, Inc., "Principles and Planning - Pretexting". [En línea]. Disponible en: https://www.social-engineer.org/framework/influencing-others/pretexting/principles-planning/. [Consultado: 27-mar-2019]

[11] Social-Engineer, Inc., "Microexpressions - Psychological Principles". [En línea]. Disponible en: https://www.social-engineer.org/framework/psychological-principles/microexpressions/. [Consultado: 28-mar-2019]

[12] Social-Engineer, Inc., "Instant rapport - Psychological principles". [En línea]. Disponible en: https://www.social-engineer.org/framework/psychological-principles/instant-rapport/. [Consultado: 28-mar-2019]

[13] , *Influence: The Psychology of Persuasion*, Revised edition. New York: Harper Business, 2006.

[14] C. Hadnagy, *Social Engineering: The Science of Human Hacking*, Second Edition. Indianapolis, Indiana: John Wiley & Sons, Inc., 2018.

[15] SecurityTrails Blog, "Exploring Google Hacking Techniques". [En línea]. Disponible en: https://securitytrails.com/blog/google-hacking-techniques. [Consultado: 01-mar-2020]

[16] OffSec Services Limited, "About The Exploit Database". [En línea]. Disponible en: https://www.exploit-db.com/. [Consultado: 02-may-2020]

[17] Shodan, "What is Shodan?". [En línea]. Disponible en: https://help.shodan.io/the-basics/what-is-shodan. [Consultado: 03-may-2020]

[18] SecurityTrails, "Banner Grabbing: Top Tools and Techniques Explained". [En línea]. Disponible en: https://securitytrails.com/blog/banner-grabbing. [Consultado: 03-may-2020]

[19] SecurityTrails Blog, "Domain Tools: top DNS, IP and Domain utilities to investigate any website". [En línea]. Disponible en: https://securitytrails.com/blog/domain-tools. [Consultado: 04-may-2020]

[20] IBM, "dig Command". [En línea]. Disponible en: https://www.ibm.com/support/knowledgecenter/en/ssw_aix_71/d_commands/dig.html. [Consultado: 04-may-2020]

[21] Nmap.org, "Nmap: the Network Mapper - Free Security Scanner". [En línea]. Disponible en: https://nmap.org/. [Consultado: 04-may-2020]

[22] Telefónica Digital España, S.L.U., "FOCA". [En línea]. Disponible en: https://www.elevenpaths.com/es/labstools/foca-2/index.html. [Consultado: 06-may-202]

[23] Security Trails, "Top 20 OSINT Tools". [En línea]. Disponible en: https://securitytrails.com/blog/top-20-intel-tools. [Consultado: 09-may-2020]

[24] jivoi, "Awesome OSINT". [En línea]. Disponible en: https://github.com/jivoi/awesome-osint. [Consultado: 09-05-2020]

[25] Lee Baird, "Discover". [En línea]. Disponible en: https://github.com/leebaird/discover. [Consultado: 09-05-2020]

[26] lanmaster53, "The Recon-ng Framework". [En línea]. Disponible en: https://github.com/lanmaster53/recon-ng. [Consultado: 10-05-2020]

[27] Christian Martorella, "theHarvester". [En línea]. Disponible en: https://github.com/laramies/theHarvester. [Consultado: 10-05-2020]

[28] C. Hadnagy y M. Fincher, *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*, First Edition. Indianapolis, Indiana: Wiley, 2015.

[29] Social-Engineer, Inc., "Phishing". [En línea]. Disponible en: https://www.social-engineer.org/framework/attack-vectors/phishing-attacks-2/. [Consultado: 21-05-2020]

[30] David Kennedy (ReL1K) @HackingDave, "The Social-Engineer Toolkit (SET)". [En línea]. Disponible en: https://github.com/trustedsec/social-engineer-toolkit. [Consultado: 24-may-2020]

[31] Social-Engineer, Inc., "Vishing". [En línea]. Disponible en: https://www.social-engineer.org/framework/attack-vectors/vishing/. [Consultado: 19-05-2020]

[32] Social-Engineer, Inc., "SMiShing". [En línea]. Disponible en: https://www.social-engineer.org/framework/attack-vectors/smishing/. [Consultado: 17-05-2020]

[33] Imperva, "Social Engineering". [En línea]. Disponible en: https://www.imperva.com/learn/application-security/social-engineering-attack/. [Consultado: 23-may-2020]

[34] Darren Kitchen, "USB Rubber Ducky Project Wiki". [En línea]. Disponible en: https://github.com/hak5darren/USB-Rubber-Ducky/wiki. [Consultado: 22-may-2020]

General

- Social-Engineer, Inc., "The Social Engineering Framework". [En línea]. Disponible en: https://www.social-engineer.org/framework/general-discussion/. [Consultado: 21-mar-2019]
- C. Hadnagy, *Social Engineering: The Art of Human Hacking*, First edition. Indianapolis, Indiana: Wiley Publishing, 2011.
- *Influence: The Psychology of Persuasion*, Revised edition. New York: Harper Business, 2006.
- C. Hadnagy, *Social Engineering: The Science of Human Hacking*, Second Edition. Indianapolis, Indiana: John Wiley & Sons, Inc., 2018.
- C. Hadnagy y M. Fincher, *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*, First Edition. Indianapolis, Indiana: Wiley, 2015.

Índice de ilustraciones