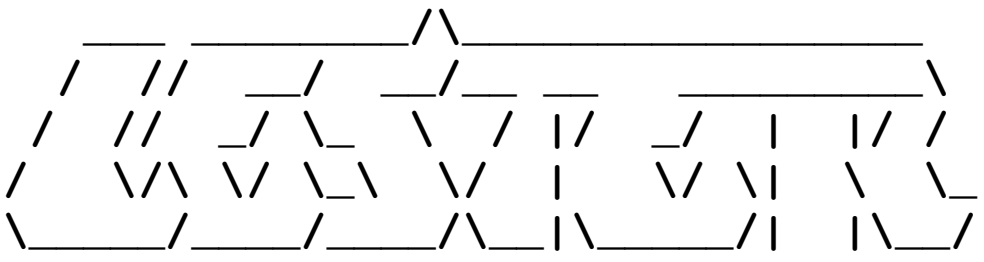
INGENIERIA SOCIAL

1.0
Hasta Cap IV-VII

POR



lester_the_teacher@hotmail.com

A Beatriz, por darle sentido a cada palabra.

Nota del autor (Disclaimer que dicen los americanos)

El autor se hace responsable de todos lo aquí escrito, no así de las acciones que utilizando las técnicas aquí descritas puedan realizar terceros.

Algunas de las cosas que se citan en este documento pueden ser constitutivas de uno o varios delitos. No pretendo con esto hacer ninguna clase de apología, ni tampoco incitar de forma alguna a la comisión de los mismos. Simplemente expongo algunas técnicas utilizadas tanto por consumados delincuentes como por los servicios de inteligencia del mundo con ánimo de estar protegido ante ellas.

CAPITULO I

Qué es la Ingeniería Social

Con el término “ingeniería social” se define el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros.

No existe una limitación en cuanto al tipo de información y tampoco en la utilización posterior de la información obtenida.

Puede ser ingeniería social el obtener de un profesor las preguntas de un examen del colegio o la clave de acceso de la caja fuerte del Banco de España. Sin embargo el origen del término tiene que ver con las actividades de obtención de información de tipo técnico utilizadas por hackers.

Un hecho importante es que el acto de ingeniería social acaba en el momento en que se ha conseguido la información buscada. Las acciones que esa información pueda facilitar o favorecer no se enmarcan bajo este termino. En muchos casos los ingenieros sociales no tocan un ordenador ni acceden a sistemas, pero sin su colaboración otros no tendrían la posibilidad de hacerlo.

¿ Por qué “el caballo de Troya” no es ingeniería social?

Existe una tendencia que trata la ingeniería social como una forma de engaño, equiparable al caballo de Troya o a cualquier forma de timo, como el de la estampita, En este sentido podemos ver lo que dice la Página de Derecho de Internet :

”En nuestro idioma, Social Engineering tiene ya un término muy tradicional y cuyo contenido coincide vulgar y jurídicamente, el engaño, término que usaremos de ahora en adelante.”

Podéis leer el documento completo visitando la siguiente dirección:

http://derecho-internet.org/teoria.php?teoria_id=38

Tendremos en cuenta 2 factores al respecto: en primer lugar, en el caso de la IS puede no haber engaño de ningún tipo. Una persona le pide a otra su contraseña o cualquier otra información en un entorno de confianza y la otra se la da sin presión ni engaño alguno. Luego el mito de que la IS se basa en un engaño, no es correcto en todos los casos.

Y segundo: suele existir un componente técnico o tecnológico. Como ya dije en otra ocasión, el timo de la estampita y la ingeniería social no tienen mucho que ver porque ésta se basa en amplios conocimientos de psicología aplicada y de las tecnologías sobre las que se quiere obtener información.

Os pondré un ejemplo que seguro entendéis. En el mundo del underground, de los hackers, las relaciones se basan en el respeto. Son mundos bastante cerrados de gente que en algunos casos pueden realizar actividades ilegales. Para poder acceder a él hay que tener tantos conocimientos como ellos y así ser considerado como un "igual". Además deberán aportarse conocimientos a compartir que de forma clara permitan ganarse el respeto de estos grupos. Solo de esta forma se tendrá acceso a determinadas informaciones.

Esto mismo ocurre en el mundo de las empresas de alta tecnología en las que se desarrollan proyectos reservados, donde la calificación técnica necesaria para entender la información que se quiere obtener es muy alta. Las operaciones de ingeniería social de este nivel pueden llevar meses de cuidada planificación y de evaluación de muchos parámetros, van más allá de una actuación puntual basada en una llamada con más o menos gracia o picardía.

Muchas veces, el Ingeniero Social simplemente observa el entorno y aprovecha datos que están a la vista cuando el sentido común indica que deberían guardarse en un lugar seguro. Conozco el caso de un servidor de una delegación de la Agencia Tributaria española cuya contraseña está puesta en un “post-it” en su pantalla. Solo hay que tener capacidad de observación de este tipo de detalles.

¿Qué tiene que ver la Ingeniería Social con la seguridad informática?

La seguridad informática tiene por objetivo el asegurar que los datos que almacenan nuestros ordenadores se mantengan libres de cualquier problema, y que el servicio que nuestros sistemas prestan se realice con la mayor efectividad y sin caídas.

En este sentido, la seguridad informática abarca cosas tan dispares como :

Los aparatos de aire acondicionado que mantienen los sistemas en las temperaturas adecuadas para trabajar sin caídas.

La calificación del equipo de administradores que deberá conocer su sistema lo suficiente como para mantenerlo funcionando correctamente.

La definición de entornos en los que las copias de seguridad han de guardarse para ser seguros y como hacer esas copias.

El control del acceso físico a los sistemas.
La elección de un hardware y de un software que no de problemas.
La correcta formación de los usuarios del sistema.
El desarrollo de planes de contingencia.

Debemos tener en cuenta que una gran parte de las intrusiones en sistemas se realizan utilizando datos que se obtienen de sus usuarios mediante diferentes métodos y con la intervención de personas especialmente entrenadas, los ingenieros sociales.

CAPITULO II

Cuando Nace la Ingeniería Social en España

Corre el año 1986/87 se empiezan a instalar algunos sistemas BBS en Madrid, Barcelona, Zaragoza, había acceso a Internet mas allá de las universidades (En estas solo el profesorado tenia acceso, es el nacimiento de Rediris) y de las conexiones UUCP (http://www.learnthenet.com/spanish/glossary/uucp.htm) que, mas tarde, montaría la compañía Goya Servicios Telemáticos y que eran carísimos para la mayoría de los usuarios. Recordemos que no existía Web, únicamente News, Mail y los protocolos de búsqueda de información tipo gopher o archie.

Los servidores estaban instalados sobre todo en USA. Para los amantes de la historia de la informática comentaré que es en 1983 cuando la red ARPANET se desconecta de los servidores militares que hacia 1971 comenzaron a trabajar enlazados. Este año de 1983 se considera realmente el del nacimiento de Internet (si alguno está interesado y lo pide puedo dedicar un capitulo a contar la historia de UNIX y de Internet ya que la red no existiría sin él y ambos sin en nacimiento del lenguaje "C")

Lo que uno podía encontrar en una BBS de aquella época eran ficheros agrupados por temas y mensajes que corrían de unos usuarios a otros utilizando la base de lo que después seria la red Fidonet (http://perso.wanadoo.es/cnb/r34.htm) u otras basadas en la misma tecnología. En estas redes las llamadas entre los nodos las realizaban usuarios "mecenas" que corrían con el precio de esas llamadas. En esta etapa los módems eran muy lentos, 1200 o 2400 bps. los mas rápidos y las llamadas eran muy muy caras. Esto tenía como consecuencia que un usuario no pudiera bajarse toda la información que quería ni conectarse a demasiadas BBS so pena de arruinarse con la factura del teléfono..... o arruinar a sus padres.

Así las cosas, era difícil compartir información propia con otros usuarios y mas aun conseguir información técnica interesante que si se podía encontrar en otros lugares de Europa y Estados Unidos.

Los grupos de hackers (en general personas con un buen nivel técnico y muchísima sed de conocimientos) buscaban formas de abaratar las llamadas de teléfono y conectarse a otros lugares. En su mayoría menores con edades entre los 11 y los 20 años no disponían de mas ingresos que la paga del domingo. El Phreaking era casi una necesidad y así había en nuestro país verdaderos magos del sistema telefónico que proveían de "soluciones" para que los demás pudieran pasar el mayor tiempo posible conectados con el menor coste. Es importante entender que si un usuario español deseaba una información de una BBS finlandesa, debía llamar a Finlandia y conectarse a dicha BBS ya que no había redes que compartieran la información de las BBS del Underground.

Se utilizaban muchas técnicas para no pagar las llamadas, desde el uso de "blue box" que eran útiles cuando el sistema de tarificación emitía para su control tonos en la "banda vocal" esto es, en la que se transmitía la voz. Hasta accesos a través de sistemas PAD (Packet Assembler Dissasembler http://www.codner.com.ar/glosariohtml.htm#GlossP). Sistemas casi siempre de

grandes compañías, que permitían desde una conexión de teléfono normal conectarse a redes de paquetes como la española X.25 y a los que se accedía desde números 900 (Cuantos hackers de la época utilizaron el famoso PAD de la shell oil?) y también números de tarjetas de teléfono americanas, las llamadas "callings cards" de MCI o de At&t que se conseguían de forma mas o menos ilegal.... Algunos recordaran el nombre de "Virgin Boy" un Danés que con sus 15 años había descifrado el algoritmo de creación de los códigos de 14 dígitos de las tarjetas de AT&T y se dedico durante años a vender dichos números al módico precio de 100 $ USA hasta que desapareció de las redes hacia el año 1.995.

En muchos casos para conseguir informaciones de cómo utilizar ciertas funcionalidades de una central de telefónica, o el acceso a una red era necesario el uso de ingeniería social. Así, algunos hackers comenzaron a especializarse en esas tareas. El abanico de posibilidades se multiplico, no solo el propio sistema telefónico sino las configuraciones de servidores, contraseñas de sistemas, datos de compañías empezaron a ser objetivo de los ingenieros sociales, que al facilitárselos a otros hackers les facilitaban en mucho sus tareas ya que se podían dedicar a lo que realmente les interesaba, aprender sistemas.

Son los tiempos en los que nacen Hispahack, Apostols, AFL, KhK Conspiradores y muchos otros grupos ya extinguidos. En cada uno de ellos hay por lo menos un experto en ingeniería social o bien buscan a especialistas en esta materia para temas concretos.

Esto supone un importante cambio sociológico pues los hackers son, en su mayoría, autodidactas que han aprendido muchísimo en la soledad de su habitación, leyendo manuales, conectándose a lugares de los que aprendían ; sin embargo, es cuando comienzan a trabajar en equipo cuando sus logros se hacen mas importantes y aunque existe el "Celo" por la información, aunque dentro de la "célula" del grupo esta se comparte de una manera fluida.

Se produce un fenómeno interesante a este respecto: la practica de técnicas de ingeniería social para conseguir información de otros grupos de Hackers.

Estos grupos de hackers crecían de 2 formas: la primera porque los componentes estaban en la misma ciudad o eran usuarios de la misma BBS, y en reuniones de usuarios de las BBS se conocían hablando de sus temas favoritos y se ponían a trabajar juntos. La otra era cuando en alguno de esos grupos se te invitaba a entrar porque habían leído un documento escrito por ti en alguna BBS, o algún mensaje dejado en las áreas de hackers que estaban abiertas a todo el mundo. (En casi todas las BBS se abrían áreas "ocultas" solo para un grupo determinado de usuarios y otras abiertas que servían un poco como "cantera" o filtro) y dichos documentos parecían interesantes para el grupo.

CAPITULO III - I

Algunos Ingenieros sociales del panorama español mas antiguo

No pretendo realizar con este capítulo una historia exhaustiva de la Ingeniería Social en nuestro país sino ofrecer algo más que información sobre técnicas relacionadas con la IS. En contra de lo que se cree, en nuestro país hay excelentes Ingenieros Sociales y he querido ofrecer una pequeña muestra explicando actuaciones concretas de algunos hackers prácticamente olvidados.

Los pequeños casos que aquí cuento de forma un poco novelada para así hacer mas amena su lectura, son todos ellos reales y están protagonizadas por hackers muy activos en las listas de correo y BBS´s españolas hace ya mas de 8 años. Todos ellos eran muy buenos técnicamente en sus disciplinas pero además utilizaban la ingeniería social como parte de sus habilidades.

Prácticamente ninguno de ellos esta ya en activo, algunos dejaron de "jugar con ordenadores" para dedicarse a otras cosas y la mayoría se encuentran actualmente en lo que se solía llamar "El otro lado", esto es, administrando servidores, dirigiendo proyectos, trabajando en compañías de seguridad, etc. Seguro que algún oldtimer recuerda sus nicks.

Obviamente se omiten, en las narraciones, algunos datos concretos para mantener su anonimato.

Omega

Había estado estudiando diversos edificios del centro de la ciudad durante muchos meses. Revisaba periódicamente los cajetines de telefónica de varios de ellos para testar si había nuevas incorporaciones de números (pares conectados). Verificaba utilizando un software de "wardialing" (aplicación que realiza automáticamente llamadas a series de números de teléfonos y guarda los resultados en una base de datos) las series de números que encontraba en aquellos edificios . Hablamos de un momento en el que las centrales no tenían la función de "caller ID" y las líneas eran analógicas por lo que no era sencillo tracear una llamada de teléfono.

Seleccionó de entre estos números los que sistemáticamente no contestaban y comenzó una aproximación a los domicilios por diversos caminos. Algunas veces como repartidor de propaganda, una vez haciéndose pasar por un agente del municipio y en otras como personal de telefónica que revisaba instalaciones domesticas. Supo así que en varios de esos pisos en los que no contestaban al teléfono vivían personas que solo pasaban determinadas temporadas en aquellos pisos y cuales eran las temporadas concretas. Por fin tenía todos los datos necesarios para comenzar la siguiente fase de la operación.

Hacia algo de frio aquella noche y no paraba de llover, esa lluvia finita que aunque no lo parece te cala hasta los huesos. El mono que vestía lo había conseguido en un mercadillo de fin de semana: lo vio y en seguida supo que le sería de utilidad cualquier día. Estaba algo sucio pero lo prefería así. Era mejor dar la sensación de que lo usaba cada día para trabajar. Caminaba despacio con aquella caja de

herramientas metálica de color azul óxido en la mano y una bufanda al cuello que le protegía algo el rostro. Tenía 17 años aunque por su tamaño aparentaba mas.

Llegó a la puerta de aquel edificio gris sin apenas ventanas, como un bunker en medio de la ciudad, mas allá de la media noche. No llevaba encima documentación alguna. Llamó al timbre y le habló la voz del vigilante.

.- ¿ quien es?

.- Alberto de Sintel, al parecer alguien de tercer canal se ha quejado por una caída en las líneas de no se qué hotel y me han sacado de la cama para que venga a mirarlo. Hace una noche de perros podían dejar de tocarme los cojones y venir directamente alguno de esos comerciales encorbatados.

.- Pasa, te abro que te estás empapando.

El vigilante no le pidió ni un dato, ninguna identificación, ningún parte de avería. La cara de mala leche, las ropas de Omega y su conocimiento de los departamentos de telefónica fueron suficientes.

Había mas gente en las salas de monitorización del edificio aunque jugaban a las cartas y nadie le preguntó nada mientras subía a la sala donde estaba la propia centralita. Una "*Pentaconta"*. Había conseguido los manuales de aquellas salas llenas de cables y relés en una librería alemana de Madrid donde se especializaban en información sobre sistemas eléctricos y electrónicos de la industria. Si no lo tenían lo traían de donde fuera. Solo le bastó una llamada a la librería comentando que preparaba oposiciones para telefónica para que se lo enviaran sin problemas.

Sabía que el número que le interesaba, uno de esos cuyos abonados solo los usaban en navidad, pertenecía a la central en la que él se encontraba. A través de una charla "casual" con un técnico de telefónica que fue a su casa a reparar su línea de teléfono supo cómo se organizaban las numeraciones en aquellos armarios de la central.

Tardó menos de 15 minutos en encontrar lo que buscaba y otros 5 en instalar el "*Diverter"*. En total no estuvo mas allá de 20 minutos en la central. Una vez ganada la confianza del vigilante, nadie le pregunto absolutamente nada.

Utilizando aquel *Diverter* se realizaron llamadas durante un año entero por diversos hackers que tenían acceso al famoso numero desviado.... Quizá debería contaros un poco que es un "*Diverter"*

¿Qué es un *Diverter* y para que sirve?

El termino *Diverter* quiere decir en ingles "desviador". En centralitas telefónicas "divert" se utiliza para designar el "desvío de llamada" . P. Ej, cuando llamamos a un número de teléfono y por cualquier razón (no esta disponible , comunica, etc.) esta llamada se "desvía" a otro número. Con la utilización de teléfonos móviles esto se entiende ahora mejor que hace unos años.

Un ejemplo: llamamos a un teléfono que tiene un desvío a una línea de salida (lo que en una central telefónica llamamos “trunk” [Enlace]). Nos daría un tono de llamada que corresponde a la otra línea, por lo que si hiciéramos una llamada en ese momento , sería desde la línea de salida y los cargos serian para ella así como suya sería la identificación de llamada si existiera la funcionalidad de CallerID. Tendríamos que pagar una llamada local para acceder al “*Diverter”* y desde allí realizar cualquier llamada con cargo a la otra línea, por ejemplo una llamada internacional.

Tiene su sentido, ¿no?

En la época en la que esto sucede, hace más de 8 años, al utilizar este *Diverter* el delito que se cometía era el de “robo de fluido eléctrico” ya que no existía legislación sobre delitos informáticos.

CAPITULO III - II

Agnus Young

Con tan solo 14 años, Agnus era probablemente la persona que mas sabia de Phreaking en nuestro país a principios de los 90. Desde el teclado cubierto de tipex blanco y teñido con tinta fluorescente de rotulador y escuchando música de Kortatu o La Polla Records recorría las líneas del mundo utilizando para ello un ordenador "Amiga 500" y un altavoz roto pegado con cinta aislante al micrófono de carbón de un teléfono antiguo. Cada noche se conectaba a las líneas internacionales de diferentes carriers y escribía documentos que los demás hackers utilizaban para poder llamar gratis a cualquier lugar.

Pero, para todo esto, necesitaba documentación acerca de los métodos de codificación y los sistemas de tarificación de llamadas que no estaban al alcance de todo el mundo. No le costo mucho conseguir un manual del departamento de ingeniería de telefónica en el que se detallaban todas las centrales de telefónica así como el tipo de enlaces que estas tenían hacia el exterior. En aquella época telefónica tenia salida al exterior a través de una serie de puntos concretos.

Lo intentó 2 veces sin resultados claros pero a la tercera y utilizando para ello la terminología de algunos libros sobre el tema, llamo a una de las centrales catalanas en las que había una línea internacional importante y se hizo amigo de uno de los técnicos de noche.

Para ello, se hizo pasar por un compañero nuevo de la casa y así consiguió que aquel técnico "mucho mas experimentado" le contara un montón de cosas que luego el utilizaba para sus pruebas, la soledad de la noche hizo el resto. Pero no solo consiguió información, su amigo técnico, cuando estaba de turno, le dejaba una conexión abierta al exterior por la que luego Agnus llenaba el disco duro de una de las BBS del underground informático mas importantes de la época "God´s House" equipada con un modem US Robotics que era capaz de soportar a 9.600 Baudios los microcortes y el ruido de las líneas analógicas cuando para hacer una llamada a USA había que pasar por varios países.

Había conseguido aquella conexión tras convencer a su "compañero de trabajo" que su familia residía fuera de España y así sus llamadas le salían mas baratas.

Lo mas interesante desde el punto de vista de la IS es que Agnus consiguió que este técnico nunca se interesara en llamarle por teléfono y dio siempre por validos todos los datos que se le ofrecieron. Agnus Young tenia una marcada voz de niño y sin embargo fue capaz de entablar varias conversaciones de muy alto nivel técnico con su "compañero" de aquella central catalana que lo convencieron completamente... Lastima que actualmente esta alejado de los ordenadores y dedicado a otros menesteres.

CAPITULO III - III

D-Orb/Telephonika

Era un sábado cualquiera de verano, cerca ya del atardecer, en una ciudad del norte de España y las tiendas de una conocida calle peatonal de la ciudad estaban llenas de turistas haciendo sus compras en plenas rebajas.

No era demasiado habitual ver a compradores españoles pagando con tarjetas en aquella época pero si a los extranjeros que venían en cruceros de placer y pasaban solo unas horas en la ciudad.

Una señora de mediana edad se acerca a la caja de una tienda de modas con varias prendas en la mano, le acompaña su hija pequeña, una niña de unos 12 o 13 años.

La chica de la caja suma el total de las compras y entrega el ticket de compra a la clienta que saca una tarjeta VISA para pagar.

La cajera hace pasar la tarjeta por una maquina manual que imprime por presión el nombre y el numero de la tarjeta sobre un formulario pequeño con varias copias en papel carbón.

A continuación realiza una llamada al centro de autorizaciones de la compañía de tarjetas para verificar que dicha tarjeta tiene crédito suficiente para realizar el pago de la compra. La llamada dura apenas un par de minutos y al final de la misma la cajera ofrece a la clienta el formulario y un bolígrafo para que firme la compra.

Desde el escaparate, como si estuviera entretenido viendo la ropa de mujer de la tienda, observa D-Orb toda la operación.

En el momento en el que la mujer abandona la tienda este se dirige al bar que hay justo enfrente y llama desde allí al número que lee en cada una de las bolsas que las clientes llevan en la mano al salir de la tienda. (he cambiado los datos reales, obviamente)

- ¿ buenas tardes señorita hablo con “Virginia Moda”? Suena una voz seca en el auricular.
- Si, dígame usted.
- Mi nombre es Alberto Pérez y le llamo de la central de autorizaciones de VISA ¿ Señorita, puede usted confirmarme su número de tienda?
- Si claro Don Alberto es el JH453
- Perfecto esta todo bien, vera usted, hemos tenido un problema con la autorización que usted acaba de solicitar hace solo un par de minutos. Podría repetirme los datos que le voy a pedir del comprobante?
- Espere un momento, Don Alberto que coja el comprobante, dígame,
- Numero de la tarjeta?
- Si, es el 1234 5678 9012 3456
- Nombre del titular tal como esta escrito?
- Mary High Albany

- Y la fecha de caducidad?
- Es el 11/90
- Muchas gracias, vamos a procesar la operación de inmediato, gracias por su ayuda buenos días.

No hubo en ningún momento duda alguna en la interlocutora, que, no solo había proporcionado a nuestro Hacker todos los datos de aquella tarjeta, con lo que podría ser utilizada en cualquier lugar del mundo a partir de ese momento, sino algo mucho más importante aun, el número de identificación de la tienda en la central de tarjetas.

Con aquel dato podía llamar a Visa y verificar el crédito de cualquier tarjeta generada con una de las muchas aplicaciones que en aquel entonces generaban números validos de VISA. D-Orb con una voz completamente formada ya, tenía en ese momento solamente 15 años y hablaba a la perfección 4 idiomas.

Algunas consideraciones al robo de datos de tarjetas de crédito

Mucho más importante que el robo físico de una tarjeta, es el robo de sus datos, ya que el titular de la misma no se da cuenta hasta que llega el extracto de la tarjeta a casa (a veces hasta 2 meses después) o hasta el momento en el que se sobrepasan el crédito asignado. Esto se sabe generalmente de una forma bastante embarazosa pues en el momento en el que se quiere realizar cierto pago no se dispone de crédito para realizarlo.Algo similar ocurre con las tarjetas telefónicas (calling cards). En la sección de técnicas explicaré algunas formas típicas utilizadas para la obtención de estos datos.

CAPITULO III - IV

LeSteR ThE TeAcHeR (Perdónenme la inmodestia)

Caso 1

Durante aquella época me encontraba desarrollando proyectos para un operador de telefonía cuyo nombre omito.

Por razones del corto tiempo para el desarrollo total del proyecto y la escasez de personal (dos males endémicos de los proyectos tecnológicos en nuestro país), no era raro que saliéramos del edificio a altas horas de la madrugada.

El trabajo se desarrollaba en un lugar de aquel edificio situado en los sótanos, muy cerca de la cafetería donde las chicas de atención al cliente tomaban sus cafés nocturnos, y también muy cerca de la maquina fotocopiadora descomunal que servia a todo el edificio. Así las cosas no era difícil entablar conversación en algún momento de descanso con aquellas chicas tan simpáticas que un poco cansadas de sus condiciones de trabajo contaban con tranquilidad casi cualquier cosa que se les preguntara abiertamente. El simple hecho de encontrarse en aquel edificio a las 3 de la mañana, como ellas, era razón suficiente para que te incluyeran en la lista de "profesionales maltratados que comparten sus penas".

Días después de que el azar me hiciera conocer a aquella chica menudita de ojos despiertos aunque un poco tristes la vi aparecer por el pasillo un poco despistada con un montón de papel en la mano, por fin asomo la cabeza por nuestro despacho un poco vacilante.

.- Hola, me puedes decir donde esta la maquina de fotocopias? Llevo poco aquí y tengo que fotocopiar esto.

"esto" era el manual completo de operador del sistema de facturación de aquella operadora de telefonía. Mas o menos unas 150 paginas a 2 caras cuya importancia no radicaba en que explicara como debían hacerse los procesos operativos sino, y esto es a veces mas normal de lo que se puede uno imaginar, porque explicaba con pelos y señales las cosas que "nunca" debían hacerse. Se detallaban cosas como la manera de conectarse desde un PC de aquella compañía a diferentes direcciones IP donde se encontraban las maquinas que almacenaban todo el sistema de cobros y facturación a los usuarios y los programas que debían ejecutarse. Como modificar la facturación de un cliente o eliminar sus llamadas, como darlo de baja o de alta, como modificar los parámetros de facturación, precio por paso, etc.

Para "facilitarle las cosas" a mi nueva amiga la acompañe al cuarto de las copias y tras pedirle el manual yo mismo me encargue de hacer las copias. Mientras ella charlaba tranquilamente conmigo y tomábamos un café haciendo tiempo, la maquina realizo las 2 copias que aquella chica necesitaba y solo me quedo entregárselas al terminar.

¿ Se hicieron solo 2 copias de aquel manual? ... Permitidme que me guarde el secreto que, al fin y al cabo es ya menos importante pues el hecho es que “pudieron haberse hecho mas” y eso es lo verdaderamente grave de la historia.

¿porque un documento confidencial tan importante estaba tan mal custodiado?

¿porque nadie le dijo a aquella jovencita tan simpática la importancia de aquellos papeles?

¿porque las copias de algo así no estaban controladas y numeradas por un departamento de seguridad física o lógica?

La respuesta es la de casi siempre en estos casos y es que “a nadie se la habría ocurrido” o peor aun “como nunca pasa nada no nos imaginamos que fuera importante”. Juzgar vosotros.

Caso 2

Se trataba esta vez de verificar uno de los sistemas de correo mas importante del mundo (www.hotmail.com de Microsoft) era verdaderamente seguro y me marque el objetivo de conseguir la contraseña de una cuenta concreta de la que tenia algunos datos (esta cuenta se creo hace unos años pero se uso muy poco y era un nicho perfecto para experimentos). Se han encontrado diversos problemas de seguridad en los servidores de Hotmail, todos han sido reportados por listas de seguridad como “bugtraq” o incluso el CERT y en la mayoría de los casos se han subsanado los mismos por la compañía propietaria del servicio, sin embargo no había documentados ataques de ingeniería social que pudieran demostrar una vulnerabilidad de sus servicio de atención al cliente.

Lo primero que se hace es enviar un mail utilizando el servicio de recuperación de la contraseña. Se supone que la hemos perdido y por lo tanto rellenamos un formulario en la web y cubrimos mas o menos los datos que sabemos de la cuenta que nos interesa (esta cuenta puede ser o no nuestra), los mails que incluyo son reales pero se han modificado los nombres de personas y cuentas de correo.

La primera respuesta tarda solo unas horas :

From: "MSN Hotmail Customer Support" <service_x_es@css.one.microsoft.com>
To: <pepito@mimail.com >
Sent: Sunday, February 15, 2002 8:30 PM
Subject: RE: CST50216034ID - Passport

> Gracias por escribir a MSN Hotmail. Apreciamos su interés en nuestros servicios.
>
> Hemos revisado la información que usted nos ha enviado sobre la cuenta
>objetivo@hotmail.com con la que se encuentra en nuestra base de datos. Verifique los datos
>que envió, ya que tenemos algunas diferencias; por consiguiente y hasta no poder verificar
>su autenticidad no le podremos dar acceso a su cuenta.
>
> No dude en contactarnos de nuevo con cualquier duda, pregunta o sugerencia.

> Antony
> --- Original Message ---
> From: < pepito@mimail.com >
> To: "MSN Hotmail Customer Support" <service_x_es@css.one.microsoft.com>
> Sent: Sun Feb 15 08:43:46 PST 2002
> Subject: Passport
>
>
> SignInDate : 11 o 12 de Febrero 2001
> ContactEmailAddress : objetivo@hotmail.com
> CustomerName : Perico de los palotes
> UpdateCountry : false, false
> CUBirthdate : 28-09-1957
> CreateDate : en el ao 1999
> Submit : Enviar
> Country : ES
> FirstName : Ingrid
> LastName : fernandez
> Region : 10111302

Como veis no conozco los datos de país, y el mensaje que me envía Microsoft me aclara que debería conocer todo lo concerniente a la cuenta para recuperar la contraseña.

Segundo intento : Para afianzar mi postura de usuario real creo un fichero ".iaf" (fichero de exportación de cuenta de correo de Outlook Express que les envió para que verifiquen que aunque con otra contraseña yo accedía a mi cuenta que "ya no funciona" y lo que ocurre es que me indican también por mail que mejor me abra otra cuenta de correo ya que no pueden darme datos para recuperar mi contraseña hablan de confidencialidad y seguridad, esta es la respuesta :

----- Original Message -----
From: "MSN Hotmail Customer Support" <service_x_es@css.one.microsoft.com>
To: <pepito@mimail.com >
Sent: Thursday, February 24, 2002 5:51 AM
Subject: RE: Re: CST50216034ID - Passport

> Gracias por escribir a MSN Hotmail. Apreciamos su interés en nuestros servicios.
>
> Debido a la privacidad que hotmail brinda a sus clientes los datos deben ser lo más exactos
>posible. Si recuerda la pregunta y respuesta secreta,algunos de sus contactos,y también
>algunas de sus carpetas por favor envíelas.
> Le agradecemos el envío de su información, sin embargo, los datos no coinciden con lo
>registrado al iniciar su cuenta. Le recordamos que Passport & Hotmail requieren que usted
>registre correctamente su información personal, así, en caso de olvidar su contraseña
>podemos verificar los datos correspondientes. Esta información la necesitamos por la
>seguridad de la cuenta y por su propio beneficio. Por favor verifique que la información
>suministrada sea correcta.
>
> Le invitamos a abrir una nueva cuenta. Por favor llene adecuadamente los espacios

pertinentes a información personal.
>
> No dude en contactarnos de nuevo con cualquier duda, pregunta o sugerencia.
>
> Roger B.

Parece que la cosa esta cerrada pero este mail nos brinda una información muy importante y es que cada vez que enviamos un mail, la persona que responde es diferente y por lo tanto querrá quitarse en problema de encima lo antes posible pues no "tiene el caso asignado" sino que seguramente su rendimiento se mida en numero de respuestas correctas dadas o en soluciones positivas conseguidas, etc.

Así que envió un tercer mail con un tono completamente enfadado con la compañía :

----- Original Message -----
From: "Perico de los palotes " <pepito@mimail.com>
To: "MSN Hotmail Customer Support" <service_x_es@css.one.microsoft.com>
Sent: Saturday, February 23, 2002 7:21 PM
Subject: Re: Re: Re: CST50216034ID - Passport

> Estoy muy enfadado con su servicio, son ustedes unos ineptos ya que mientras
> alguien esta utilizando mi cuenta de forma fraudulenta habiendome robado la
> contraseña en un ciber-cafe no con capaces simplemente de cerrarla y
> enviarme una contraseña nueva. ¿ ustedes creen de veras que si la cuenta no
> fuera mia estaria enviando mensajes y mensajes tratando de que ustedes me
> hagan caso ?
>
> Por segunda vez les envió el fichero .IAF con el que yo configuro mis
> ordenadores para leer mi mail.
>
> Dejen ya de dar vueltas y envienme una contraseña de nueva para mi cuenta
> objetivo@hotmail.com ya que esto me esta causando graves perjuicios.
>
> Me pregunto si tendre que publicar toda esta historia en alguna revista para
> que la gente se de cuenta de lo malo que es su servicio.

Bingo, la receta a funcionado y el mensaje que recibo de la compañía es entonces el siguiente :

----- Original Message -----
From: "MSN Hotmail Customer Support" <service_x_es@css.one.microsoft.com>
To: <perpito@mimail.com>
Sent: Saturday, February 25, 2002 11:50 PM
Subject: RE: Re: Re: Re: CST50216034ID - Passport

> Gracias por escribir a MSN Hotmail. Apreciamos su interés en nuestros servicios.
>
>
> Hemos restablecido la contraseña de su cuenta
> como: ganaste2001

>
> Cuando tenga de nuevo acceso a su cuenta, cambie la contraseña. Haga clic en el botón
>"Opciones" en la barra de exploración horizontal. En "Su información", haga clic en el
>vínculo "Passport". Cree una pregunta para recuperar la contraseña y una respuesta a esa
>pregunta para poder utilizar el sistema automático de recuperación de contraseñas.
> Hotmail garantiza la privacidad de su correo electrónico al pedirle una contraseña para
>entrar en su cuenta de Hotmail. NO comparta su contraseña con nadie, incluso si afirma
>trabajar en Hotmail. Ningún empleado de Hotmail le pedirá su contraseña, ni por teléfono ni
>correo electrónico.<p>
> MSN Hotmail dispone de una completa ayuda en línea para el usuario. Para obtener más
>información acerca de las características, funciones y problemas de Hotmail, haga clic en el
>botón "Ayuda" en la barra de exploración horizontal.
>
> Si los pasos anteriores no han solucionado su problema, responda a este mensaje y hágame
>saber qué pasos del proceso fallaron o si el problema persiste. Quiero ayudarle a obtener el
>mayor provecho de MSN Hotmail.
>
> Ann R.
> Su satisfacción con mi servicio al cliente es muy importante para mí. Si usted considera que
>el problema fue resuelto, ingrese al hipervínculo incluido para hacerme conocer mi
>desempeño. En sus comentarios incluya mi nombre y el número de caso, los cuales se
>encuentran en la línea de tema o asunto del correo. De esta forma podré llevar un control de
>mi servicio.

Como vemos la cosa no ha sido tan complicada, las técnicas utilizadas en estos mails son las que se denominan “ingeniería social inversa” que ya explicare mas adelante.

¿ porque dieron una contraseña nueva si no podían verificar la propiedad de la cuenta ?

En muchas compañías siguiendo la norma “El cliente siempre tiene razón” zanjan problemas simplemente cediendo ante la insistencia de un usuario que “como hemos demostrado” no siempre tiene razón. Esto ocurre porque el numero de casos en los que el cliente no cuenta la verdad es muy bajo y el coste de un problema no resuelto por ajustarse a la normativa puede ser peor para una compañía que la metedura de pata en caso de que el cliente este mintiendo

El truco desde el punto de vista del IS es que sea conocedor de este hecho y lo pueda aprovechar.

The Saint

Como otros muchos, utilizaba un acceso intermedio en un sistema local para poder conectarse a Internet, ya que cuando esto sucede no había proveedores en nuestro país. Durante mucho tiempo utilizo el mismo acceso, pero ahora sabia que los datos para el acceso al sistema local se cambiaban a primeros de mes. Sabia también que las claves llegaban por carta al apartado de correos que el CPD de aquella caja de ahorros tenia en una ciudad de Aragón. Lo había sabido porque al lado de su instituto tomaban todos los días café algunos directivos de la compañía y a el le

gustaba ir allí a “estudiar”. Tardo mas o menos un par de meses en enterarse de ello ya que estos directivos siempre se sentaban en la misma mesa y era sencillo escuchar lo que decían.

Conocía varios datos mas acerca de la compañía porque cuando las limpiadoras sacaban las bolsas de basura el buscaba entre los papeles listados de las aplicaciones en cobol o trabajos del Host IBM que tenían allí, un 3090 Sierra. Se acercaba final de mes y necesitaba conseguir la llave de aquel apartado de correos y así poder conseguir las claves de acceso por X.28 .

Busco en la guía el teléfono de la oficina de correos cercana a aquellos edificios y pregunto por el responsable de los apartados. Utilizo un micrófono preamplificado y un altavoz que realzaba los graves para hablar, curiosamente de un órgano electrónico muy barato que hacia sampling .

- Buenos días Emiliano Pérez al habla dígame que desea?

-Hola, me llamo Federico Tomas de la “caja grande y azul” tenemos ahí un apartado de correos al que va a llegarnos una carta urgente y la llave la tengo en mi poder aquí en Paris. He tenido que venir en viaje de trabajo y no vuelvo hasta dentro una semana. Si le parece bien mandare a un mensajero para retirar la copia y así poder revisar el correo que es muy urgente.

- No se preocupe, que venga que yo le espero hasta las 2, dígale que venga de su parte para que no haya confusión.

No pasaron mas allá de 30 minutos cuando The Saint con un casco de moto y una cazadora de cuero (ambas cosas prestadas) entraba en aquella pequeña oficina de correos y preguntaba por don Emiliano de parte de Don Federico.

- Hola, venia porque mi jefe se ha marchado con la llave del apartado de correos de la empresa y me han dicho que tenia que darme una copia o no se que.

- Si, precisamente aquí la tengo preparada.

- Pues muchas gracias por todo, vuelvo corriendo a la oficina.

- De nada chaval, hasta otra.

Cada vez que llegaba una nueva contraseña The Saint la obtenía y la depositaba de nuevo en aquel apartado de correos solo unas horas después.

A partir de ese momento y durante varios meses The Saint estuvo entrando por una conexión X.28 a aquel banco y desde el y gracias a las contraseñas que recibía cada mes saltaba a otros servidores de la red X.25 que le permitían la salida fuera del país. No hubo denuncia alguna, nadie se entero nunca y solo dejo aquellas entradas cuando cambio de ciudad. The Saint trabaja ahora en una importante compañía de seguridad fuera de nuestro país.

CAPITULO IV - I

Técnicas de Ingeniería Social

He dudado bastante a la hora de hacer una clasificación de las técnicas de IS. Hay quien se centra en practicas concretas o formas de actuación. Sin embargo y tras su análisis creo establecer con cierto rigor una clasificación de compromiso que divide estas practicas en tres tipos según el nivel de interacción del Ingeniero social :

Técnicas Pasivas :
* Observación

Técnicas no presenciales :
* Recuperar la contraseña
* Ingeniería Social y Mail
* IRC u otros chats
* Teléfono

Por desarrollar en siguientes ediciones :

Carta y fax

Técnicas presenciales no agresivas :
Buscando en La basura
Mirando por encima del hombro
Seguimiento de personas y vehículos
Vigilancia de Edificios
Inducción
Entrada en Hospitales
Acreditaciones
Ingeniería social en situaciones de crisis
Ingeniería social en aviones y trenes de alta velocidad
Agendas y teléfonos móviles
Desinformación

Métodos agresivos
Suplantación de personalidad
Chantaje o extorsión
Despersonalización
Presión psicológica

Formas de actuación

Además de esta primera clasificación, una acción de IS puede ser asimismo “casual” o “planificada” .

Acciones “casuales” requieren en el Ingeniero Social capacidad para la improvisación, un buen nivel de autocontrol y buenas dotes de observación o memoria visual y la capacidad de mantener siempre una vía de salida.

En las acciones planificadas, casi siempre las mas peligrosas pero las que persiguen objetivos mas importantes, no se deben dejar cabos sueltos. Estas son indispensables si hablamos de acciones desarrolladas por mas de 1 persona. Veamos un ejemplo sencillo de análisis para una acción planificada :

Sabemos que para obtener el código de acceso de un cajero automático o una puerta con contraseña podemos simplemente leer como lo teclean en el tecladillo numérico, pero las personas que suelen abrir dicha puerta van juntas y una de ellas suele tapar la vista de terceros observadores. Si conseguimos despistar a el acompañante el tiempo suficiente para que el compañero teclee el código ya tendríamos la solución a nuestros problemas. ¿ que hacemos ?

1 .- Pedirle fuego : y si no fuma o no lleva tabaco ? la respuesta seria rápida y no daría tiempo.

2.- Preguntarle la hora : si no lleva reloj se acabo el tema.

3.- Preguntar por una calle mas o menos lejana : deberá ser una calle en la dirección opuesta a donde queremos mirar e intentar que el compañero nos acompañe o se de la vuelta ¿ y sino se sabe la calle ?

4 .- Simular una caída : y esperar que nos ayuden mientras nuestros compañero toma nota del numero ¿ y sin nos ayudan los 2 ? ¿ y si al ver la caída alguien mas se acerca ?

Entendemos entonces que se trata de conseguir desviar la atención de una sola de las dos personas sin que la otra deje de hacer su trabajo y durante el tiempo necesario para lograr el objetivo. también podríamos utilizar un cierto equipamiento electrónico.

En fin, como veis, son problemas sencillos pero aportan variables que debemos analizar antes de llevar nuestra acción a cabo.

La planificación se utiliza en "operaciones" complejas en las que un equipo de personas busca un objetivo común, no tiene demasiado interés si lo que buscamos es el numero de abonado a C+ de nuestro vecino del 5º.

Una vez mas es muy importante entender que cuando hablamos de ingeniería social, no nos referimos solamente a grupos de chicos mas o menos jóvenes que quieren conseguir la contraseña de nuestro e-mail para jugar un rato.

Trataremos grupos de técnicas que utilizan grandes compañías para obtener información de proyectos de la competencia y que para ello invierten muchísimo dinero en medios. También son utilizadas estas técnicas por diversos servicios de información como La CIA, MI5 o MI6, Mossad, Cesid y en contra de lo que se pueda pensar estas practicas son verdaderamente comunes si bién muchas de ellas son también claramente ilegales.

Durante las próximas secciones realizaremos un pequeño estudio de cada una de estas técnicas . En la sección dedicada a los medios técnicos hablaremos de cómo utilizar la tecnología para la obtención de información, como veremos hay en el mercado equipos con los que se muchos agentes secretos de película palidecerían.

Capitulo IV – II

Técnicas Pasivas

Si se plantea la pregunta ¿ Que información interesa a un ingeniero social? obtendremos la respuesta : "Toda la información". El aprendizaje de una persona en el campo de la IS es constante y hay muchos ámbitos de conocimiento que le serán de utilidad, desde conocimientos de historia, ingenierías, arquitectura, electrónica, etc.

Cuanta mayor sea su cultura mas posibilidades tendrá de ofrecer diferentes perfiles a terceros cometiendo el menor numero de errores. Existe un proceso conocido como realimentación que consiste en la utilización de unos pocos conocimientos de un tema determinado para obtener otros muchos que no se tienen, un ejemplo practico.

Imaginemos una conversación con un arquitecto en la que el ingeniero social se hace pasar por un igual. Este último apenas sabe de arquitectura pero conoce algunos temas concretos, por ejemplo la nueva legislación sobre el seguro decenal de la construcción y la normativa EH de composición del hormigón. Bien usados estos conocimientos someros de temas tan dispares, que en teoría debería conocer cualquier arquitecto, ayudan a crear un perfil personal ajustado a lo que se supone que se es. Luego y conforme avanza la conversación aprenderá de su interlocutor sobre la marcha y se "realimentará" de estos nuevos conocimientos que podráutilizar cuando séa necesario.

La realimentación es, en electrónica, el proceso por el que se consigue que un transistor amplifique una señal (perdonadme los que entendais el concepto de forma mas profunda, lo escribo así para que todos lo comprendan).

El primer paso en Ingeniería Social es muy simple pero a su vez nada sencillo, aprender a observar. La observación de un acontecimiento concreto, de un lugar, de una persona o grupos de personas va mas allá del concepto de "ver lo que pasa". Observar con detenimiento pero a la vez sin despertar sospechas. Fomentar capacidades como la "memoria visual" es muy importante para obtener de una situación la mayor cantidad de datos en el menor tiempo posible.

Si el objetivo es un lugar al cual se quiere acceder, es necesario conocer sus medidas de seguridad, sus accesos, el personal que lo vigila, la situación de los sistemas de alarma, si los despachos usan o no llave, si hay salidas sencillas o complicadas, si hay sistemas de grabación y si realmente se usan o no. Un punto a muy interesante a estudiar en seguridad perimetral son los caminos de una sola dirección en un edificio. Son, casi siempre, una opción muy válida para entrar en un lugar.

¿ que es esto?. Un ejemplo simple son las salidas de emergencia. En general no se pueden abrir desde fuera pero podemos esperar que nos la abran desde dentro, esto vale para las salidas de personal de muchos edificios, por ellas no se puede entrar pero podemos esperar que salgan y casi nunca dirán nada. Pensemos también en las puertas de "llegadas" de un aeropuerto. Casi nadie se fijará si uno entra para saludar a un viejo amigo que llega en avión o si lo que se pretende es llegar a la pista. En general las pistas son accesibles desde estas zonas.

Si el objetivo es una persona, antes de abordarla por otros medios se debe analizar toda la información disponible de esa persona por métodos "no intrusivos"

La observación es el camino para crear la mayoría de las situaciones casuales que ayudan al ingeniero social a obtener una información, unos ejemplos de informaciones obtenidas por simple observación :

- Recordemos la anécdota de la contraseña del PC puesta en un post-it en la pantalla del ordenador.

- Conozco el caso de una entidad bancaria en la cual los mensajeros responsables de llevar las tarjetas de crédito a correos para su envío pasan andando con ellas en cajas por el lugar donde está la impresora que imprime los números secretos. ¿que pasaría si uno de estos vigilantes se llevara una tira de números secretos al pasar llevando las tarjetas?

- En cierta ocasión en la que se desarrollaba un proyecto en una importante empresa española en la que había todo tipo de controles de seguridad en las puertas principales del edificio (vigilantes, cámaras, tornos con tarjetas, detectores de metales) no existía ninguna vigilancia en el ascensor que llevaba al parking del edificio. Era prácticamente imposible meter o sacar un disquete del edificio pero si lo bajabas a tu coche podías vaciar una oficina entera y nadie sabría como fue.

- Cuantas veces habéis visto que un cierto servidor queda abierto con el prompt de root en su pantalla porque su administrador "salió un momento".O si utilizáis cibers, ¿nunca os encontrasteis una sesión de IRC abierta en el PC que os ha tocado, o de un webmail cualquiera, o el messenger?.Un porcentaje alto de las perdidas de contraseñas o de accesos no permitidos a servidores ocurren así.

Este tipo de errores de seguridad son muy normales, no solo ocurre a nivel informático sino en seguridad perimetral y de accesos. Si se observa con

detenimiento se detectan muchos de estos fallos garrafales. Si simplemente miramos sin analizar lo que vemos estaremos perdiendo una valiosa información.

¿ Porqué se cometen estos fallos?

En cualquier situación, la adopción de más medidas de seguridad supone un incremento en costes económicos y en tiempo. Un sistema corriendo bajo seguridad C2 (Véase el texto original del "Libro naranja" http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html) es más complejo de administrar y también más lento y, aunque parezca mentira, cuanto más alto es el nivel de seguridad implementado en un sistema se encuentran puertas mas grandes para entrar, casi siempre por dejadez. Eso es fruto de la tendencia a la "Ley del mínimo esfuerzo" ya que con el tiempo las medidas tienden a relajarse.

Imaginemos que tenemos en la puerta de nuestra casa 12 candados que ponemos cuando cerramos porque al vecino de arriba le robaron 2 veces. Con el paso del tiempo dejaremos de ponerlos todos al salir a hacer cosas de corta duración y un día solo usaremos uno, pues "no han vuelto a robar en la zona". Así un día que bajamos 10 mins a comprar algo entran en nuestra casa y se lo llevan casi todo. Este mismo fenómeno ocurre muchas veces administrando sistemas cuando no se tiene clara conciencia del problema de la seguridad.

CAPITULO IV - III

Técnicas no presenciales

Muchas de las actuaciones de los ingenieros sociales se realizan a distancia, utilizando ya sea el teléfono, el fax, las redes de datos o incluso cartas tradicionales.

A lo largo de los años se han ido perfeccionando las formas de operar y abriendo el abanico de las mismas a otros medios, he aquí algunas de ellas.

La contraseña perdida

Todos hemos leído muchas veces que no es bueno utilizar en las contraseñas palabras que tengan significado, fechas que se relacionen con nosotros, números de DNI, nombres de familiares, etc. Esta recomendación no siempre se sigue, además de ello, existe una tendencia generalizada a utilizar la misma contraseña en múltiples servicios y esto facilita mucho el trabajo a aquellos que pretenden obtenerla de forma ilícita. No olvidare tampoco a aquellos que guardan en sus agendas los números secretos de los cajeros (ATM para los americanos), contraseñas de los PC de casa u oficina, mail, etc.

Para obtener una contraseña, y antes incluso que las de aplicaciones basadas en el uso de diccionarios y la fuerza bruta, están los propios sistemas de recuperación de contraseñas de casi todos los servicios de la red.

A veces creo que los analistas que desarrollan esos sistemas no los han utilizado nunca.

Estudiemos algunos con su nombre y apellidos :

Terra.es

En la sección de usuarios registrados de Terra hay una opción llamada "**¿Ha olvidado su contraseña?** En la cual y una vez que se introduce un usuario valido, presenta la pregunta que dicho usuario selecciono para recuperar la contraseña. Por ejemplo ¿ como se llama mi perro? Y si tecleamos "toby" que es como se llama el perro de nuestro usuario, el sistema muestra la contraseña.

En esta caso el sistema es endeble pues depende únicamente de la calidad de la pregunta que el usuario haya puesto. Si cualquiera conoce la respuesta a esta pregunta tendrá la contraseña del sistema y podrá suplantar a otro usuario y lo peor de todo es que lo hará sin que nadie se de cuenta de ello. Y es que se mantiene la misma configuración que nuestro usuario propietario del buzón tenía.

Elistas.net

En ese sistema la opción de recuperar contraseña esta un poco mas escondida, en la sección :"Mi cuenta" en la cual podemos leer "Sino recuerdas tu clave de acceso averigua como conseguir una nueva" Tras esto y una vez que se introduce un mail valido el sistema envía a dicho mail una nueva contraseña.

Esto es mucho mas seguro pues aun sabiendo el login de un usuario, no recibiré dicha contraseña si no soy el propietario de la cuenta valida. Pero esto tiene un inconveniente importante, veámoslo: si un usuario que esta registrado en el sistema ya no mantiene la cuenta con la que se dio de alta, perderá el acceso a su cuenta ya que nunca recibirá la nueva contraseña. Una curiosa forma de "denegación de servicio" basada en el conocimiento que un tercero tiene de los datos que un cierto usuario utiliza para entrar en E-listas.

Lycos Mail

En este caso se utiliza un sistema mixto en el cual un usuario puede recibir su contraseña en su mail alternativo, que sufre del mismo problema que en Elistas.net o contestar a la pregunta secreta, que como vimos antes es mucho menos seguro. No es mala idea pero es algo así como que nos permitan elegir el método por el que un ladrón entrara en casa (pulse 1 para ventana, 2 para puerta blindada, 3 para escalera de incendio) .

Telepolis.com

Utiliza el esquema de realizar la pregunta que el usuario selecciono al registrarse pero obliga a cambiar la contraseña si se acierta la respuesta. Una vez mas alguien que conozca la respuesta a la pregunta podría no solamente hacerse con la cuenta sino además dejar a otro usuario sin acceso a ella ¿ peor el remedio que la enfermedad? Vosotros juzgáis.

Hotmail.com

Personalmente creo que es un sistema razonablemente equilibrado. Realiza varias preguntas al usuario como filtro antes de presentar la pregunta que se selecciono al registrarse, y solo después de haber respondido a varios datos diferentes permite que se cambie la contraseña. Lo que se consigue es que la información necesaria para realizar el cambio sea mucho mayor y eso eleva el listón de la seguridad.

Tras estos ejemplos concretos lo que sabemos es que no existe un sistema perfecto y que por lo tanto es casi siempre la imaginación del usuario lo que hará que sea verdaderamente seguro dentro de lo que los diferentes sistemas permiten.

Los sistemas mas seguros son aquellos que envían dicha contraseña a una dirección postal ya que esta no suele cambiar. Sin embargo en estas situaciones se pierde la posibilidad de anonimato del posible usuario.

Como recomendación a los usuarios tanto la contraseña como la pregunta de recuperación deberían modificarse cada cierto tiempo y en ambos casos utilizar como respuestas series pseudo aleatorias de letras y números sin significado y con longitudes iguales o mayores a 8 caracteres, se que quizá son mas complejas de recordar pero también será mucho mas complejo su recuperación por personas no autorizadas. Por otro lado recordemos que es importante utilizar una contraseña distinta para cada servicio. Una técnica de "contraingenieria social" es utilizar una respuesta falsa a la pregunta de recuperación de contraseña. Un ejemplo "en que ciudad nací? = 275Hm-.

Ingeniería Social y Mail

El mail es una forma de acercamiento a terceros que permite una cierta protección de la intimidad y el anonimato del Ingeniero Social si este toma unas mínimas precauciones. A través de el y mediante mensajes mas o menos "simpáticos" llegan muchos virus. Lo veremos en la sección correspondiente, pero sin embargo hay mas técnicas basadas en Mail que utilizan muchos Ingenieros sociales.

Se clasifica la información a obtener a través de mail en tres tipos

1.- información sobre la empresa del objetivo, datos de las oficinas, proyectos etc.
2.- información sobre personas
3.- información técnica

Los métodos para la obtención de cada tipo es diferente, sin embargo hay algo que tienen en común los tres y es que casi siempre se necesita información previa suficiente para salvar la barrera de la confianza, aunque hay algunas excepciones.

Debido al Spam y a las malas practicas de muchas compañías que hacen un marketing poco ético, se tiende a eliminar cualquier mail que no transmite esa confianza o cuyo remitente no parece conocido. En este sentido es importante que el mail venga de una dirección "amigable" o conocida. Direcciones confusas como microsoft@soportes.net ,Internick@internets.ru, helpdesk@wanadu.net que se asemejan a direcciones de sistemas existentes tienen probabilidades de éxito si lo

que se busca es algún dato técnico del sistema y este se solicita a personal no técnico.

En otro ámbito, si lo que se busca es información sobre la compañía, habrá de conocerse algunos datos de proveedores o clientes y utilizar mensajes escritos desde direcciones que utilicen esos nombres de clientes o proveedores pero desde dominios distintos.

Un caso que requiere una especial atención es la simulación de mails que provienen de servicios de banca por Internet. Como todo, con algunos conocimientos técnicos, también son sencillamente suplantables. Basta con crear un mail en HTML utilizando las imágenes y los formatos que alguna de estas entidades utilizan pero enviándolo desde cualquier otra cuenta. Conozco casos en los que un usuario recibe un mail que parece provenir de un banco conocido y que luego lo redirige a un formulario falso en el que se le hace escribir su contraseña de acceso para operar y esta es guardada en una tabla o enviada por mail a una dirección donde luego se utilizan de forma fraudulenta. A continuación dicho usuario es enviado a la pagina real del banco tras haber recibido una pantalla de error. A través de este tipo de operaciones se producen importantes fraudes.

En el caso de que lo que se busque sea información personal, si la persona de la compañía cuya información se busca tiene una secretaria que lleva su correo será mas sencillo obtenerla que si es la persona destinataria del mail quien lo lee, pues en muchos casos dan por hecho que la persona que escribe es realmente un conocido del “jefe” sin confirmarlo con el.

Cuando lo que se pretende conseguir son datos de personas, el envió de mails a las cuentas de la compañía en la que estas trabajan no suele dar buenos resultados. En ese caso es el mail personal el que ofrece mas garantías de éxito. Sin embargo es necesaria mas información para que una persona responda a un mail privado. En los casos en los que no se dispone de demasiada información estos casos hay una opción interesante y que consigue excelentes resultados :

El mail perdido.

Es un sistema que, sobre todo, funciona cuando la persona a la cual queremos aproximarnos es un hombre.

Para ello debemos crear una personalidad femenina y enviar un mail “equivocado” a la persona cuyos datos nos interesan. Probablemente la persona en cuestión nos lo devolverá con algún comentario. En ese momento ha picado el cebo. Al recibir su mail responderemos al mismo y nos desharemos en halagos. Normalmente no será complicado acabar entablando una “amistad” a través de mail que puede llevarnos a donde deseamos. Una vez mas es el sentido común quien debería mandar, cuidado con los desconocidos.

Hay, además de todo esto, métodos para la extorsión a través de mail, de las que hablaremos, o de obtención de las contraseñas a través de envió de mails del servicio técnico del proveedor, veamos un ejemplo real :

El falso mail “Como hackear una cuenta de Hotmail”

He visto varias veces un e-mail con instrucciones que en teoría sirve para hackear la cuenta de Hotmail de cualquier usuario. Este sistema lo que hace es enviar los datos de nuestra cuenta al desaprensivo que nos envió dicho mail. Tengamos cuidado con ello. también podréis encontrar algo similar en alguna página web.

Este es el contenido de uno de estos mails :
---------- INICIO DEL MAIL ----------

PRIMERO TIENES QUE TENER UNA CUENTA EN HOTMAIL PARA COMPONER EL SIGUIENTE MAIL.
LO TIENES QUE MANDAR A : hotmail_support@hotmail.com
EN EL TEMA DEL MAIL TIENES QUE PONER: FORGOT PASSWORD LUEGO TIENES QUE ESCRIBIR EL SIGUIENTE CÓDIGO:(en el lugar para escribir el mensaje)
HTPOST/ <aqui pones tu e-mail>DIF%99USER_LIST<aqui pones tu clave> TO.LOP<aqui pones el nombre de la victima> //%89"%90,//*mail///lostpassword///

Y FINALMENTE PON ENVIAR... ... Y LISTO EN UNAS HORAS RECIBIRÁS LA CLAVE.
ASÍ ENGAÑARAS A LA COMPUTADORA CENTRAL DE HOTMAIL. NO TE PREOCUPES QUE ESTO VA A FUNCIONAR Y NADIE SE DARÁ CUENTA YA QUE ESTA OPERACIÓN LA HACE UNA COMPUTADORA COMPLETAMENTE AUOMATIZADA.

EJEMPLO:

Si quieres hackear a Carlos@hotmail.com y tu eres Jordi@hotmail.com y tu clave es 12345, lo que tienes que poner en en código seria lo siguiente: HTPOST/<Jordi> DIF%99USER_LIST1<12345>TO.LOP<Carlos> //%89"%90,//*mail///lostpassword///

Y RECIBIRÁS UN MAIL COMO ESTE (LA CUENTA QUE APARECE YA HA SIDO MODIFICADA) :

Hotmail_support@hotmail.com

Gracias por confiar en nuestros servicios carlosmaster60, la clave de acceso a la cuenta

bryan5000@hotmail.com es: BLOQUEADA

Si la clave es BLOQUEADA, usted ha de volver a cambiar la clave de acceso y no restringirla, ya que

restringida no podrá iniciar sesión desde otra cuenta Hotmail

Si desea modificar la clave de acceso comuníquenoslo o entre aquí

http://lc3.law13.hotmail.passport.com/cgi-

bin/loginerr?curmbox=F000000001&a=cd723379d7e74e15387dafbc0c825b3f&error=3&sec=no&reaut

h=&id=2&fs=1&cb=_lang%253dES&ct=1003946096&_lang=ES&domain=hotmail%2ecom&utf8=0

Un cordial saludo

El equipo Hotmail

---------- FIN DEL MAIL ----------

CAPITULO IV-V

IRC y otros chats

Los chats son los lugares de la red donde mas información se puede obtener utilizando técnicas de ingeniería social. Los chats en los que grupos de usuarios conversan de forma más o menos anónima, favorecen el acercamiento y la charla intima y sobre todo, es en ellos donde las personas bajan más la guardia. A veces los ratos de charla son largos y es difícil estar siempre alerta. Además de todo ello es verdaderamente sencillo crearse una o varias personalidades falsas que pueden utilizarse según la persona o personas a las que se quiere investigar.

El sistema mas utilizado en estos entornos es crear una personalidad de sexo opuesto al de la persona que pretendemos conocer con la cual se aborda al objetivo. Sin embargo debemos tener en cuenta un dato fundamental. Las mujeres, mucho más sensibles a toda la mala publicidad acerca de los peligros de la red, son casi siempre mucho más precavidas y mucho más discretas en cuanto a lo personal. Sin embargo una vez traspasada la barrera inicial ofrecen una información más minuciosa. En el caso de los hombres la situación se invierte, “pican” de manera mas sencilla a la hora del acercamiento pero se dan cuenta antes de que están siendo investigados. Me refiero en este caso a procesos de acercamiento sin mucha preparación, cuando se planifican las acciones, las probabilidades de éxito son buenas en ambos casos.

Cuando se realizan acercamientos a una persona de forma un poco brusca o con demasiada celeridad es relativamente sencillo que se percate de nuestras intenciones. Es bueno tomarnos las cosas con calma.

En sistemas de Chat donde se registran los nicks (Alias utilizados para identificarnos) es importante que se utilice uno que este registrado hace tiempo. Es sencillo mantener una lista de nicks registrados sin mucho trabajo, podemos incluso realizar un pequeño programa “BOT” que se autentifique ante la red con una lista de nicks que nos interese tener “guardados” para cuando sea necesario.

La gente confía mas cuando siente que el interlocutor conoce bien el medio y lleva tiempo en el. Por algún extraño mecanismo psicológico un nick antiguo transmite siempre mas tranquilidad que un nick sin registro o nuevo. Además, en la mayoría de los chats el registro permite mantener el mismo nivel de anonimato al usuario ya que es posible el uso de bouncers o proxies para realizar la conexión y ocultar así nuestra IP real. Además también es posible el acceso a través de páginas Web.

Cuando uno se crea una personalidad falsa en un Chat de una forma planificada es bueno que además del nick se utilice siempre una dirección de mail creada para los mismos fines y, si es posible, una pagina personal asociada a ese nick que cuente algunas cosas sobre “nuestra persona ficticia”. Si pretendemos llegar a conocer personalmente al objetivo a investigar deberíamos añadir una foto, lo creamos o no cuanta mas información, aunque sea falsa, demos de “nuestra personalidad” mas fácil será conseguir información de nuestros objetivos. En estos casos es importante también utilizar un numero de móvil (celular para nuestros amigos del otro lado del Atlántico) de tarjeta prepago solo asociado a nuestra personalidad falsa.

En el caso de que no deseemos que se nos pueda localizar es fundamentar como ya he citado utilizar algún tipo de bouncer o Proxy.

El momento de ir ofreciendo estos datos depende siempre de cómo evolucionen las cosas.

La forma de escribir es el caballo de batalla de estas técnicas. Cada uno solemos utilizar una serie de coletillas o una forma de escribir determinada. Es importante poner cuidado en estos temas y respetar unas normas de escritura que se asocien a un "personaje" concreto. Unos escribirán con acentos puntos y comas, otros deberán usar un lenguaje mas "joven" con modismos y expresiones modernas. Otros se reirán o saludarán de una forma concreta por donde pasen. Lo importante es que una vez creada una "estructura semántica-lingüística" de tapadera, asociada a un nick, la respetemos siempre.

Casi siempre que en un Chat alguien es descubierto usando diversas personalidades aunque, sin embargo, tuvo cuidado de utilizar scripts o aplicaciones de Chat diferentes, conectándose por bouncer, etc, es porque no cambia su forma de escribir.

Hay algunas situaciones en las que es difícil legar a conocer el origen de una conversación. Esta es la que se tiene con una persona que no se identifica y que utiliza una forma de escritura diferente solo para esa conversación y en el transcurso de la cual esa persona siembra el desasosiego o incluso el miedo al darnos datos sobre nosotros mismos que solo conoce un circulo cerrado de personas. Algunas veces esto empieza como una broma de un amigo que luego se identifica. Pero cuando no es así es, verdaderamente sencillo crear un estado de ansiedad en la persona a la que se aborda que dure varios días.

Los robots publicitarios en IRC y Chat, IS ya la publicidad en el Chat

Han ido evolucionando estos sistemas que utilizan el irc para enviar mensajes publicitarios a los usuarios de los canales de Chat y que lo hacen utilizando muchas veces técnicas de Ingeniería Social.

Inicialmente estas aplicaciones se conectaban a un canal y allí lanzaban sus mensajes publicitarios cada cierto tiempo.

Actualmente analizan las listas de canales o salas de una cierta red y se conectan a aquellos en los que hay más tráfico utilizando nicks llamativos y casi siempre femeninos. Cuando un usuario comienza una charla con estos robots, son capaces de dar un par de respuestas antes de mandar su mensaje publicitario. Transcribo aquí una conversación del usuario "pepito" con uno de estos robots:

<pepito> hola buenos días
<marina2> hola, como estas?
<pepito> muy bien
<pepito> y tú ?

<marina2> de donde eres?
<marina2> yo, no muy lejos...tu edad? yo 27 años.
<pepito> hjhjk hj
<marina2> que buscas hache? un encuentro simpático?
<pepito > sss
<marina2> como estas fisicamente? yo rubia, 1m60,48kg,85b
<pepito > lljklsjklfjksdl
<marina2> me gustas mucho! oye,estoy harta de recibir mensajes aqui!
<pepito > uiouio wquiouio
<marina2> bueno, corto, voy en otro chateo
<pepito > yuiyuiyui
<marina2> es http://sarahcam.free.fr mismo pseudo si te gusta alli
<pepito > jkl jkljkuio
<marina2> si tu vienes te daré mi teléfono será mas sencillo un beso

En este caso la acción de la IS es simplemente el engaño para hacer que un usuario visite una cierta web, casi siempre de sexo. Este tipo de trucos funcionan únicamente con recién llegados a los chats, pero dado que son muchos, la efectividad es apreciable. Obsérvese que el usuario se da cuenta de que habla con un BOT y que este escribe lo que tiene programado aunque se le responda con un "churro" de caracteres. Además el lenguaje del Bot. parece una mala traducción de otro idioma al castellano.

Troyanos en IRC , ICQ o Messengers de todo tipo

Los troyanos se utilizan como una forma más de obtención de información. Con algunos de ellos una persona puede tomar el control de nuestra máquina, copiar ficheros, ver lo que tecleamos y en muchos casos realizar hasta una copia remota de un disco duro completo sin que su dueño se percate.

Un troyano, como muchos sabéis, es algún tipo de programa que una vez alojado en el PC de la victima realiza acciones que van desde la simple destrucción de información, el envío de esta a terceros o el permitir que otros pueden disponer de un acceso al ordenador donde se alojan. No se consideran troyanos las aplicaciones comerciales dedicadas al espionaje ya que estas suelen requerir el ser instaladas directamente en el PC en el que se ejecutan. Esto no ocurre así con aplicaciones como Back Orifice, Subleven o similares que no requieren mas que la ejecución de un pequeño programa que se puede enviar por mail o a través de alguna aplicación de Chat.

En el IRC o similares es normal el envío de documentos de todo tipo entre los usuarios utilizando el protocolo DCC o protocolos específicos de cada aplicación que se utiliza para este tipo de cosas (Messenger, Icq, Yahoo Messenger, etc.).

Muchas veces, lo que un usuario envía por DCC cuando, en teoría nos esta mandando sus fotos o cualquier otra cosa que esperamos, no es mas que un troyano que una vez ejecutado permitirá a dicho usuario acceder a nuestra maquina. De entre estos los más conocidos son el "Netbus" el "Back Orifice" y el "SubSeven" pero hay más. Por eso es fundamental no ejecutar nada que otros usuarios nos envíen a través de estos sistemas sin haber utilizado antes un antivirus

para verificarlo. Contra este tipo de troyanos también funcionan aplicaciones cortafuegos que solo permiten que ciertos puertos de nuestras máquinas permanezcan abiertas y así una aplicación de este tipo aun cuando se llegue a ejecutar no podrá pasar a través del firewall y no será peligroso.

Hay, sin embargo aplicaciones más peligrosas, que una vez instaladas envían la información que desean obtener por correo electrónico o usando un cliente FTP embebido que casi nunca son frenadas por un cortafuegos. Entre estas están muchas aplicaciones tipo keyloger (que guardan la información de las teclas que son pulsadas en un PC para enviarlas a una dirección de mail cada pocas horas) o ciertos Sniffers, que revisan el tráfico de red buscando ciertas tramas y luego las envían como si de un mail normal se tratase.

MS Messenger

Es otro sistema de Chat que tiene, en teoría, mejoras de seguridad de forma que solo los usuarios que nosotros autorizamos puedan hablarnos o enviarnos ficheros. Además permite que como usuarios regulemos aquellas personas que pueden vernos on-line.

Sin embargo esto no es del todo cierto. Hay aplicaciones que funcionando como clientes de Messenger permiten sin mas, ponerse a charlar con otra persona y verla on-line aunque estemos bloqueados por ella. Se basan para hacerlo en un parámetro de los contactos que figuran como ocultos y que por lo tanto no pueden ser eliminados de la lista de contactos ni tampoco modificados y que sin embargo están en ella.

Una vez mas el sentido común dicta la norma, no admitamos envíos de información de usuarios desconocidos. Esto nos evitara problemas.

CAPITULO IV-VI

IS y Videoconferencia

Entendemos ya todos el hecho de que la razón de la IS es la obtención de la información. En muchos casos, esta se consigue sin conocimiento de la persona cuya información se esta aprovechando. Sin embargo, no siempre es así. Hay una forma de actuación asociada a este tipo de de aplicaciones que permiten no solo escribirnos sino también ver y oír a nuestro interlocutor, esta forma de actuación es el chantaje.

Una de las aficiones de muchos de los usuarios de estas aplicaciones es el practicar cibersexo. Así 2 personas se ven mientras “hacen sus cosas”. En esta situación es muy sencillo grabar imágenes fijas o incluso la sesión completa. Una vez guardadas en el disco se utilizan como forma de extorsión a personas casadas o con responsabilidades para las que asumir que realizan estas prácticas puede ser un verdadero problema.

He conocido personalmente varios casos de mujeres u hombres que han sufrido extorsiones por terceros que utilizaban estas técnicas. En todos los casos la persona

que realizaba la extorsión se había hecho con una buena colección de fotos de sus victimas en actitudes sexualmente explicitas.

Personalmente yo recomiendo la denuncia a la policía, pero cada uno conoce sus propios problemas personales y puede que no siempre sea posible.

El problema con el que nos encontramos es que es difícil demostrar que estas cosas están ocurriendo sin la intervención de personal técnicamente cualificado.

Analicemos un caso real tal como suele ocurrir la secuencia de hechos:

El usuario A se conecta con el usuario B en una sesión de NetMeeting (podría ser cualquier sistema de videoconferencia).

El usuario B graba la conversación con A , o varias fotos fijas de este sin que A lo sepa

El usuario B envía por mail alguna prueba de que efectivamente tiene una grabación y en ese momento le plantea el chantaje y le pide algo a cambio.

A veces, ese algo es información para la comisión de delitos. Otras, cuando la acción esta planificada puede llegar a ser incluso una forma de captación de informadores para los servicios secretos (Hay bastante bibliografía que documenta esta afirmación)

El problema es que si aceptamos una comunicación por videoconferencia estamos permitiendo a otra persona ver nuestra imagen con nuestro consentimiento. Quizá no le estemos permitiendo que la grabe pero es complejo que en un juicio esto quede verdaderamente claro.

Por otro lado no queda constancia técnica de que la persona que tiene las imágenes de A es realmente el que las grabara, salvo que A disponga de herramientas de análisis de trafico que permitan logear cada conexión a su máquina y este log pueda ser guardado sin que pueda luego ser modificado. Y aun cuando las tuviera, solo se llegaría a demostrar que es la máquina del usuario B quien grabo las imágenes pero ¿como sabemos que era B realmente el que estaba en el teclado en ese momento?

Para demostrar esto es necesaria una investigación policial tradicional.

Sin embargo, lo que si queda meridianamente claro ante un juez es el concepto de chantaje, por lo que el mail en el que se chantajea al usuario A se convierte en la prueba fundamental. Si, es verdad que solo nos llevara, como comentamos antes, al PC de B sin embargo es muy posible que este mail enviado este aun en su bandeja de “enviados” y por otro lado y mediante análisis policial (huellas, restos de partículas, etc.) puede llegar a demostrarse que personas usaron esa máquina. A veces se realizan amenazas cruzadas utilizando Mail y también mensajes SMS a móviles lo cual permite cercar todavía más al acosador.

Como vemos, el último paso es siempre una investigación tradicional y algunas situaciones concretas ayudan mucho a solucionar un problema de este tipo. Por

ejemplo, que el PC este en un domicilio en el que solo viva B, que este en su despacho de la oficina, que utilice la dirección de alguna institución oficial, etc.

Puede parecer curioso pero muchos acosadores lo hacen desde su propio trabajo y sin tomar ninguna precaución. Lo hacen pensando que no serán investigados ya que esperan que el amenazado actúe con miedo y cumpla lo que se espera de el sin cuestionarlo, lo que facilita mucho la localización de las máquinas desde las cuales se realiza el chantaje.

Capitulo IV –VII

Ingeniería Social y teléfono

El teléfono es el medio predilecto de los ingenieros sociales. Seguramente donde se origino el termino y donde mas ataques de este tipo hay documentados. Su uso ofrece ventajas con respecto a otros :

- La ocultación de numero permite , en un primer momento, mantener el anonimato de una manera simple.
- Permite además actuar a distancia, incluso desde otro país, lo que hace difícil la captura del Ingeniero Social.
- La voz ofrece muchísima información a quienes practican ingeniería social. Datos acerca del estado de animo del interlocutor, o si es un profesional del medio(teleoperadores, etc.).

Esto lo convierte en el elemento mas utilizado para obtención de información de forma no presencial.

Pero analicémoslo poco a poco.

El anonimato en las líneas telefónicas

Profundizaremos en este tema mas adelante, en los apartados dedicados a tecnología utilizada para la Ingeniería Social, tomemos esto como una pequeña introducción.

Cuando se realiza una llamada de teléfono es posible no enviar el “caller-ID” (identificador de numero llamante) de forma que el número no se muestre en el terminal o la centralita receptora. Para hacerlo y hablando de España, hay varios caminos. Podemos , si realizamos la llamada desde una línea telefónica básica (rtc), marcar antes del numero al que se llama el prefijo “067”. Existe en las líneas RDSI (ISDN) una funcionalidad similar e incluso en las redes móviles existe una secuencia que realiza esta misma función (#31# Número de teléfono <Enviar>) .Otra forma de realizar esto es efectuando una llamada internacional ya que el caller ID, en muchos casos, no se mantiene entre operadores de diferentes países.

En la mayoría de los casos esto servirá para que un usuario no vea el numero de teléfono desde el que se realiza la llamada que esta atendiendo, sin embargo, en el operador que envía la llamada y en el que la recibe si queda rastro de la misma. Por

lo tanto, ante una denuncia, el seguimiento de las llamadas será bastante sencillo y el anonimato quedará burlado.

Hay casos, cuando se trata de países con redes antiguas, en las que por disponer de centrales analógicas la información de numero llamante ni siquiera se guarda.

Con la aparición de los teléfonos móviles de prepago, se complican un poco las cosas, ya que no existe una correspondencia directa entre una persona o una dirección y un cierto número de teléfono. Pero en caso de llamadas repetitivas desde un mismo número hay otros métodos de seguimiento que también permiten la localización del terminal desde el que se efectúa la llamada.

En este sentido, un doble mensaje, para los que gustan de utilizar estas técnicas, cuidado, una aplicación del viejo refrán “tanto va el cántaro a la fuente...”. Para aquellos sufridores de llamadas poco “agradables” denunciemos, en muchos casos se soluciona el problema.

Caller ID Spoof

Seguro que muchos ya saben que , en el mundo de las redes IP, es posible suplantar la dirección de una máquina desde otra a esto se le llama “IP Spoofing”. En el caso de las redes telefónicas esto también es posible. El proceso para ello no es sencillo pero si posible.

El primer paso es realizar una llamada a una centralita de una empresa que disponga de varias líneas y que conozcamos en profundidad. Una vez conectado a dicha centralita marcaremos el código para realizar una llamada saliente. En ese momento dispondremos de tono de llamada en nuestro terminal telefónico y podremos realizar una llamada cuyo número de origen es del de la centralita que hemos atacado, y no el nuestro real. Será difícil asociar las llamadas entrantes con las salientes, y en general las sospechas acerca de quien realiza las llamadas irán dirigidas al personal de la empresa donde esta la centralita.

Como siempre las posibilidades de ser localizado aumentan al crecer el numero de llamadas realizadas por este método.

La confianza a través de la línea

Obviamente, lo mas importante para un ingeniero social es precisamente que no se produzca denuncia, por lo menos, que no se produzca en el tiempo en el que se mantiene el contacto telefónico.

Es raro que el contacto a través del teléfono se mantenga mucho tiempo . En la mayoría de los casos se trata de obtención de informaciones puntuales sobre un tema concreto. En otros se trata de saltarse la barrera de secretarias que una persona con cierta responsabilidad puede tener en una empresa de manera que sea mas fácil llegar a ella.

Aunque no siempre es así, un ejemplo de relación larga a través del teléfono puede ser la siguiente historia real en la que omito los datos del protagonista por petición suya.

Nuestro protagonista descubrió en las páginas de un periódico local, lo que parecía ser un anuncio de una agencia de contactos, anuncio que en principio ofrecía unos servicios claramente legales. Ofrecía contactos entre los socios, teniendo estos que pagar una cuota al asociarse. El ingeniero Social realizo una llamada a aquel lugar :

.- Hola Buenos días, con quien hablo?

.- Soy Antonio del centro de contactos.

.- Bien soy el Subinspector Romero del grupo X de la policía Judicial, quería hablar con el dueño.

.- Soy yo mismo, usted dirá.

.- Mi llamada tiene que ver con una denuncia que tenemos de un socio suyo que nos ha indicado que alguna de las personas con las que ha contactado a través de su empresa le han pedido dinero para verse. Esto, claro, supone una violación de la ley.

.- Si bueno, la verdad es que nosotros no cobramos mas que por ser socios, lo que ellos hablen entre ellos no nos importa.

.- Comprendo pero al ser usted quien les pone en contacto hay una responsabilidad subsidiaria y podríamos tomar medidas contra usted. Nos gustaría saber si esta dispuesto a colaborar. O si tengo que pedir una orden de registro para revisar todos sus archivos.

.- No bueno, seguro que podemos arreglarlo.

.- Claro, mire a mi me parece un poco tonta la denuncia pero se me ocurre que podíamos hacer algo que nos beneficie a los dos.

.- Dígame.

.- A mi personalmente me puede interesar conocer a algunas personas de su base de datos así que si esta dispuesto a darme los datos de las personas que se den de alta, yo podría “solucionarle” cualquier denuncia o avisarle cuando se prevén investigaciones de negocios como el suyo para que durante unos días no ponga su anuncio en el periódico. ¿Qué le parece?

.- Si eso me va a ayudar a estar mas tranquilo por mi correcto.

Aunque no lo parezca, esta es una historia cierta que ocurrió en La Coruña entre 1995 y 96 y nuestro amigo, el Ingeniero Social estuvo llamando cada cierto tiempo a aquella agencia y obteniendo datos de personas como si de un socio mas se tratase. A cambio, consiguió convencer al dueño de la misma que estaba protegido de cualquier problema con la policía gracias a el.

En ningún momento se vieron y la relación termino cuando el centro cerro sus puertas.

Mantener la confianza

Es especialmente difícil conseguir mantener la confianza de alguien sin que este pase al siguiente nivel que es el de verse físicamente tras algunas conversaciones.

En muchos casos la confianza desaparece con el tiempo si no se produce un acercamiento. Obviamente si ambos están en distintas ciudades la cosa es mas sencilla. En este caso el planteamiento es similar al de una “simbiosis” en el mundo animal. Cada uno aporta, o cree aportar, su parte en una relación que mas que de amistad es de conveniencia. Es una de las claves de esta forma de actuación.

El control del tiempo de respuesta

Otra de las claves básicas al abordar a alguien por teléfono es el factor sorpresa. Esto no es nuevo , se aplica en tácticas bélicas desde “El arte de la guerra”. A veces, cuando el alubión de información que se ofrece a alguien es mayor del que es capaz de entender se produce un fenómeno que consiste en que sus mecanismos de protección se rebajan y en ese momento es capaz de ofrecernos la respuesta a cualquier pregunta que hagamos. Muchas veces la información que ofrecemos no tiene que ser cierta, solo ha de parecerlo. Si además de un alubión de datos se apremia con una excusa a la persona a la que llamamos, no se le da tiempo de reaccionar y evaluar en su justa medida lo que se le ofrece. En ese momento se quebró la barrera de la prudencia.

Ilustrare esto con una historia, como siempre real, de alguien que estaba interesado en obtener la información de contratación de un apartado de correos. Como sabemos, esta es una información que solo se suministra por la vía de una petición judicial y que por lo tanto es, en teoría, segura.

Nuestro “investigador” realiza una llamada a una oficina de correos y pregunta por la persona encargada de los apartados de correos.

.- Hola con quien hablo ¿

.- Soy Eduardo Eduardez

.- Mi nombre es Elisendo Elisez y le llamo desde la oficina de la fiscalía antidroga de la audiencia nacional. Antes de continuar quiero indicarle que según la ley 127/4 del 9 Nov. 87 esta conversación esta siendo grabada y su contenido que será clasificado como secreto no podrá ser revelado a terceros. Si acepta la llamada usted quedara obligado a mantener dicho secreto. De lo contrario, el estado, a través de esta fiscalía antidroga podrá tomar medidas contra usted en virtud de violación de secretos de estado, lo que supondría no solo un expediente sancionador sino acciones penales contra su persona. ¿ Acepta los términos de la conversación o damos por terminada la llamada?

.- Si, por supuesto dígame que ocurre.

.- Vera, estamos en medio de una importante operación y no es posible seguir el procedimiento reglamentario de solicitud por vía de petición judicial. Necesito de forma inmediata los datos de contratación del apartado de correos 243 de sus oficinas.

.- Le puedo llamar en 5 minutos a su teléfono con los datos.

.- Mire usted, tenemos gente en la calle ahora mismo y no puedo esperar , mire el dato en su archivo y me lo comenta, yo espero al teléfono. Es fundamental para nosotros.

Bien, el funcionario le dio al ingeniero social todos los datos de contratación de aquel apartado de correos sin que fuera necesario procedimiento legal alguno. Bastó la explicación inventada en terminología "pseudolegal", el miedo, la falta de tiempo para el análisis de lo que ocurría y la voz ronca del protagonista que de manera firme daba credibilidad al contenido de la conversación. Aun así hubo un punto critico, el momento en que el funcionario ofreció llamar el. Esto podría haber supuesto un desenmascaramiento del llamante, sin embargo consiguió capear el temporal siendo rápido en la respuesta que dio sin dudar. Como siempre, la credibilidad se gana con pequeños detalles, una simple duda o titubeo habría dado al traste con la operación.

"Hints and tips" sobre la ingeniería social y teléfono

- Llamar siempre con numero oculto.

- Cuando hagamos una llamada no debemos dudar , hablemos siempre claro y de forma fluida, la duda genera desconfianza.

- Preparemos la llamada, una lista de posibles preguntas o respuestas, e incluso la preparación de un guión con las frases largas que vamos a utilizar nos ayudara . Es importante que no se note que leemos, si es que lo hacemos así.

- No colguemos el teléfono de forma brusca, eso genera desconfianza y si vamos a realizar una segunda llamada será mejor siempre despedirse de una forma cordial.

- No es bueno extenderse demasiado en la información aportada en una llamada cuando pretendemos hacer creer que formamos parte de la organización a la que estamos llamando. Debe parecer que conocemos la compañía, y entre compañeros la información vaga será suficiente. Por otro lado es muy importante que la conversación no sea demasiado larga pues la probabilidad de cometer errores es mucho mayor.

- La llamada encadenada es una técnica que se utiliza mucho cuando se quiere penetrar en el entramado de una compañía. Se realiza una primera llamada en la que se recaba cierta información sobre nombres de personas o datos técnicos. Basta en muchos casos hacerse pasar por un cliente o proveedor posible de la compañía a la que llamamos. Luego, en una segunda llamada utilizamos esa información que ya sabemos para que otra persona distinta apoyándose en ella obtenga la que verdaderamente le interesa. Para no levantar sospechas, entre ambas llamadas transcurre un cierto tiempo que evita que alguien puede establecer una conexión de ambas llamadas. Se pueden ir encadenando llamadas hasta llegar al objetivo.

- Técnica del candado de voz. Se llama así cuando lo que se desea es llegar a entrar en un edificio de oficinas en el que se realiza un control informático de visitas. En estos edificios los equipos de seguridad requerirán la documentación de las visitas y algunos datos para controlar su acceso al edificio. Sin embargo, existe en muchos casos la posibilidad de saltarse el control de accesos con un poco de ayuda desde el interior. Lo primero que se necesita es el nombre completo de un directivo importante de alguna de las firmas en dicho edificio. Algo que es fácil de conseguir con una llamada. Luego es necesario el teléfono de la recepción del edificio. Lo que se hace a continuación es llamar a la recepción suplantando al directivo cuyos datos tenemos. Se advierte a recepción de la visita de una persona muy importante que llegara a una cierta hora y que es importante que se le permita el paso al edificio. Vale un directivo de una gran compañía, o un político. Eso es menos importante, lo que suele pasar es que es el propio vigilante el que acompaña al Ingeniero social al interior del edificio, mas allá de los controles de entrada.

- La falsa interferencia es otro sistema curioso que lo creamos o no tiene éxito. Se trata de realizar una llamada desde un teléfono que se modifica para que la calidad de la señal emitida sea muy pobre. Basta con usar un par de cables en contacto con el auricular para que nuestra voz se entrecorte y se escuche con ruido. Se efectúa la llamada al objetivo que escuchara gritar entre ruidos. La idea es que el esfuerzo del interlocutor para mantener la conversación es alto y por lo tanto, cuanto antes nos de lo que pedimos mas rápido acabara su tormento. Es bueno en estos casos hacer que la llamada se corte deliberadamente varias veces, hasta casi hartar a la persona que la recibe. En ese momento se pide la información que deseamos “hola, soy Matías de informática, es que estoy tratando de solucionar un problema y desde aquí no se que pasa que no tengo cobertura. ¿ Me puedes decir como era la contraseña de acceso a la aplicación de facturación?. En un alto porcentaje de los casos, las personas que reciben la llamada trataran de ayudarnos y nos darán la información que buscamos sin preguntar mas cosas solo porque así zanjan esa desagradable situación de incomodidad que tienen al hablar entre tanto ruido.

En fin, como vemos hay multitud de pequeños trucos que se aplican cuando se practica Ingeniería Social a través del teléfono. Seguro que Mitnick tiene constancia de alguno mas.