Ingeniería social

PID_00178969

Sergi Robles Martínez
Sergio Castillo Pérez

Universitat Oberta de Catalunya

Índice

Introducción

Existe un gran número de vulnerabilidades de naturaleza muy variada que permiten una gran diversidad de ataques. Esto hace difícil el diseño de una política de prevención completa y da lugar a la necesidad de tener expertos en seguridad de la información con un amplio conocimiento sobre el tema. Las vulnerabilidades, los ataques y los mecanismos de prevención vistos hasta ahora son de naturaleza tecnológica, lo que permite realizar un análisis completo, con las puntualizaciones remarcadas en los módulos anteriores.

Sin embargo, se ha obviado hasta ahora un elemento común a todos los sistemas de información y que precisamente es el más vulnerable y fácil de atacar, y que dificulta en gran manera el análisis de seguridad de los sistemas. Nos referimos a los humanos. Tras un sistema de información siempre hay personas, como los usuarios, los administradores, o el personal de desarrollo y mantenimiento.

Si incluimos a las personas como parte integrante de estos sistemas de información, aspecto que desgraciadamente aparece muchas veces descuidado en los análisis de seguridad, resulta que suele ser, con diferencia, el eslabón más débil de toda la cadena de seguridad. Aunque la consideración de este factor humano en el estudio de las vulnerabilidades de un sistema parece obvio, hay circunstancias que favorecen su exclusión. El primer impedimento está en la propia naturaleza del problema, ya que puede pensarse que está fuera del dominio de las tecnologías de la información y de las comunicaciones y descartarlo en vez de buscar su integración. Sin lugar a dudas, considerar a las personas como parte del sistema dificulta enormemente su análisis. Puede pensarse que en muchos aspectos este análisis de la actividad humana alrededor de los sistemas de información pertenece más al dominio de la psicología social.

En este módulo veremos que es posible analizar lo que denominaremos ingeniería social desde un punto de vista metodológico. Identificaremos las estrategias, las técnicas y los medios utilizados por la ingeniería social, y de qué manera se relacionan para conseguir atacar vulnerabilidades del sistema. Aprenderemos también a detectar los elementos más vulnerables a partir de los diagramas de ataque de ingeniería social y por medio de casos prácticos, así como a incluir estrategias para su prevención en las soluciones de seguridad. De esta manera, se conseguirá una visión más holística de las vulnerabilidades de seguridad de los sistemas de información que permitirá no solo ampliar y complementar los mecanismos de prevención vistos hasta ahora, sino además enfocar de manera diferente el propio diseño de los sistemas. Se estudiarán también otras instancias de ingeniería social que tienen especial relevancia por su cotidianidad, como los ataques de *phishing*, *scareware* y *hoaxes*.

Objetivos

Los objetivos que el estudiante debe haber conseguido después de estudiar los contenidos de este módulo son los siguientes:

1. Saber identificar las estrategias, las técnicas y los medios más comunes utilizados por la ingeniería social.
2. Aprender a realizar diagramas de ataques de ingeniería social (DAIS).
3. Identificar los elementos más vulnerables de un sistema a partir del DAIS.
4. Diseñar estrategias para la prevención de los ataques de ingeniería social.
5. Tener una visión más completa de las vulnerabilidades de un sistema de información.

1. El proceso de la ingeniería social

Una de las claves para afrontar con éxito el problema de la inclusión del factor humano en el análisis de seguridad de un sistema de información es la identificación de manera precisa de todos los elementos que intervienen en él, y el seguimiento de una metodología concreta. Si no se realiza de esta manera, es fácil adentrarse demasiado en el ámbito de la psicología social, en particular en el análisis de la confianza humana, o el de la persuasión, que aumenta la complejidad y hace más difícil el diseño de soluciones prácticas para la detección y prevención de ataques. Una parte importante del trabajo de investigación realizado sobre este tema no se encuentra en el dominio de informática, sino en el de las ciencias sociales.

En este apartado se presenta un enfoque práctico y simple para el análisis de la intervención humana en la seguridad de un sistema, permitiendo la detección y prevención de ataques que utilizan a las personas. El primer paso será definir los conceptos básicos que usaremos.

Análisis de casos concretos

Muchos de los trabajos realizados sobre el tema de la ingeniería social hasta ahora se basan en el análisis de casos concretos, como el de Mitnick y Simon (2002).

En el contexto de la seguridad informática, llamaremos **ingeniería social** a la secuencia de acciones que tienen como finalidad la obtención de información, el fraude o el acceso no autorizado a sistemas informáticos, y que ha implicado en algún momento la manipulación psicológica de personas.

Un sistema **vulnerable a ataques de ingeniería social** será, por tanto, aquel susceptible a ser atacado mediante estas técnicas. El punto que hace diferentes a los ataques de ingeniería social de otros ataques es la manipulación psicológica de las personas que se realiza en algún momento.

Otros colectivos

Fuera del dominio de la informática, la policía, los detectives privados y los periodistas, entre otros colectivos, utilizan también a veces la ingeniería social para conseguir información.

Así pues, un aspecto básico en la ingeniería social será la manipulación psicológica de personas. En el siguiente subapartado se verá de qué maneras se puede realizar esta manipulación.

1.1. Aspectos explotables

La base de la ingeniería social es la aplicación de técnicas de psicología para conseguir, por medio de la manipulación, que las personas realicen ciertas

acciones o desvelen la información deseada. Encontramos la base teórica de estas técnicas en la psicología social.

Hay tres aspectos de la psicología social que serán importantes para los propósitos de la ingeniería social: las técnicas para la persuasión y la influencia, las actitudes y creencias que afectan a la interacción social, y la falsa confianza.

Lectura complementaria

La psicología social engloba el estudio de cómo las personas piensan, influyen y se relacionan entre ellas. Se puede encontrar más información sobre la psicología social en la obra de Myers (1994).

1.1.1. Técnicas de persuasión e influencia

En la psicología social se identifican dos modos que se pueden utilizar para persuadir. Por un lado, utilizando argumentos sistémicos y lógicos para estimular una respuesta favorable, induciendo a la persona a pensar detenidamente y dar un consentimiento. Por otro, de una manera más lateral, basada en indicaciones periféricas y atajos mentales para eludir el argumento lógico y la contraargumentación para intentar provocar la aceptación, sin pensar en profundidad sobre el tema. Un modo como se puede hacer a una persona más susceptible a esta persuasión periférica es a través de mensajes o acciones en el inicio de la interacción que provoquen reacciones emocionales, como excitación o miedo. Estas reacciones, así como otras formas de distracción, sirven para interferir en la capacidad de pensamiento lógico de la víctima y permitir explotar esta persuasión periférica para realizar ataques de ingeniería social.

Una gran parte de la bibliografía de la psicología social reconoce al menos siete factores que se basan en la persuasión periférica que son efectivas en la persuasión e influencia de personas (Cialdini, 2008):

1) Autoridad. La mayoría de las personas son muy receptivas a la autoridad. En las condiciones adecuadas, la autoridad se cuestiona poco, y la tendencia a obedecer instrucciones de alguien que dice tenerla es muy alta, incluso cuando se reciben de manera indirecta (por ejemplo, a través del teléfono).

Ejemplo de autoridad

Un ejemplo de recurso a la autoridad es pedir que abran una puerta haciéndose pasar por un agente de policía.

2) Parquedad. Cuando hay escasez de un bien o servicio en el que se podría estar interesado, o su disponibilidad es solo por un período de tiempo limitado, las personas tienden a quererlo más. Saber que esta disponibilidad limitada puede crear competencia entre otras personas para su adquisición incrementa más aún el deseo de adquirirlo.

Ejemplo de parquedad

Un ejemplo de recurso a la parquedad es anunciar que solo quedan tres unidades de *pendrive* para las primeras personas que contesten una encuesta.

3) Similitud. Existe una innegable tendencia humana a que nos guste aquello que es similar a nosotros mismos. Tener elementos en común, como por ejemplo aficiones, gustos musicales o artísticos, o incluso compartir los mismos problemas, crean un fuerte incentivo para tratar a alguien de una manera especial, más favorable.

Ejemplo de similitud

Un ejemplo de recurso a la similitud es comentar casualmente que hemos nacido en la misma ciudad para pedir posteriormente una información no pública.

4) Reciprocidad. Cuando alguien da algo, o promete que lo hará, las personas sentimos una fuerte tendencia a devolver algo a cambio, incluso si lo que se ha recibido nunca fue solicitado. Esta regla básica de la interacción humana es

innata a las personas y funciona aun cuando el coste de lo dado y recibido es muy diferente.

Ejemplo de reciprocidad

Un ejemplo de recurso a la reciprocidad es desconectar inadvertidamente a alguien el cable de acceso a la red de un ordenador simulando una avería para solucionar el problema después y pedir un favor a cambio.

5) Compromiso. Si se incumplen las promesas, las personas tienen la certeza de que serán consideradas de poca confianza por otras personas. Esto provoca que las personas realicen un gran esfuerzo para cumplir con los compromisos adquiridos.

Ejemplo de compromiso

Si se convence a una persona de que hizo una promesa, cuando en realidad no la hizo, esta se esforzará por cumplirla.

6) Consistencia. Las personas tienen tendencia a actuar de manera consistente con sus acciones pasadas, aunque en la situación actual mantener esta coherencia ya no tenga sentido, ya que creen que al no hacerlo serán consideradas de poca confianza (Cacioppo y otros, 1986).

Ejemplo de consistencia

Se puede predecir la reacción de una persona a partir de sus acciones pasadas.

7) Prueba social. Ante la duda sobre si realizar o no una acción, o cuál es la más apropiada, las personas deciden según el comportamiento de otras personas cercanas. Esto puede llevar a realizar acciones que van contra los intereses de las personas sin que se lleguen a pensar detenidamente.

Ejemplo de prueba social

Si tres personas compinchadas muestran el DNI a un falso portero, la siguiente persona también lo mostrará.

1.1.2. Actitud y creencias

Otro aspecto de la psicología social importante en la ingeniería social son las creencias y actitudes. Las personas generalmente piensan que los otros comparten sus mismos sentimientos e ideas, lo que se denomina el efecto del falso consenso. El ingeniero social puede utilizar estas creencias para manipular a la víctima y conseguir que realice alguna acción.

Experimentos de psicología social muestran que incluso algunas de las personas que analizan detenidamente los mensajes persuasivos dejan de hacerlo cuando perciben que el origen es más honesto. Así, algunas víctimas de ingeniería social tienden a confiar más en sus creencias o impresiones personales sobre la honestidad que les ofrece alguien, que en el análisis objetivo del contenido del propio mensaje. Un ataque, por ejemplo, podría venir precedido de una estrategia de mejorar la percepción de la honestidad del atacante por parte de la víctima.

1.1.3. Falsa confianza

Por defecto, las personas tienen una tendencia natural a confiar en sus congéneres, aunque no haya un histórico de interacciones que avale dicha confianza. Es más, ser desconfiado de entrada suele ser mal visto socialmente y supone una percepción negativa de las personas. Cuando no existe una per-

cepción elevada de riesgo, se concede de entrada el beneficio de la duda en contra de lo que aconsejaría un pensamiento racional detenido, hasta ciertos límites (no se suelen dejar la llaves de casa al primer desconocido que nos las pide, por ejemplo). Incluso si de entrada una persona decide no confiar, suele ser sencillo hacerle cambiar de idea simplemente haciéndole ver que está desconfiando.

Además de la confianza natural directa, resulta fácil realizar acciones que se perciben como indicadores que aumentarán la confianza que se deposita en alguien. Estaríamos hablando de, por ejemplo, las técnicas de persuasión periféricas vistas anteriormente con el objetivo de incrementar la confianza que se tiene en el atacante o de su credibilidad. Sin llegar a la persuasión, el simple contacto continuado en el tiempo aumenta automáticamente la percepción de confianza. Por ejemplo, confiaremos más en alguien que hemos visto cada mañana en el metro durante el último mes que en alguien que acabamos de conocer, aunque racionalmente no haya ninguna razón para ello.

El pretexto es una de las técnicas más conocidas para ganar confianza. Establecer contacto con una persona a través de una historia falsa suele ser suficiente para que esa persona deposite confianza sobre el atacante y reduzca su reluctancia a ofrecer información privada. Esta percepción de confianza es uno de los puntos explotables de las personas más utilizados en la ingeniería social y que suele ser más efectivo.

1.1.4. Otros aspectos explotables

A parte de los aspectos ya vistos, hay otras cualidades humanas que son explotables desde el punto de vista de la ingeniería social. A continuación encontramos algunos ejemplos:

Curiosidad	Ignorancia	Cortesía	Avaricia	Apatía
Paranoia	Lujuria	Inseguridad	Amabilidad	Caridad
Recelo	Orgullo	Envidia	Empatía	Compasión
Consuelo	Solidaridad	Ira	Indulgencia	Amor

Estas cualidades humanas, no siempre presentes en todas las personas, representan puntos débiles que facilitan el engaño y la manipulación. La curiosidad, por poner un caso, es una cualidad humana muy común. ¿Quién puede resistirse, por ejemplo, a ver el contenido de un *pendrive* encontrado accidentalmente en la calle? Muchos ataques de ingeniería social utilizan este rasgo humano de una manera u otra.

Otras se perciben como cualidades deseables en una buena persona, y son incluso inculcadas en algunas religiones, como la caridad, la compasión o la

amabilidad. Muchas personas deberían hacer un gran esfuerzo para resistir el impulso de ofrecer ayuda al necesitado o de aliviar el sufrimiento del que padece. ¿No se saltaría alguna norma de la política de seguridad de la empresa para cubrir el error de alguien con una familia a cargo, parar sus lloros, y quitarle el miedo del despido?

Muchas de estas cualidades son parte de la educación que se recibe. Carecer de ellas, en algunos casos, puede hacer tildar las personas de "maleducadas". En general, cualquier aspecto que haga que las personas estén por encima de cualquier regla es explotable por la ingeniería social para saltar mecanismos de seguridad.

1.2. El proceso de la ingeniería social

En el subapartado anterior hemos visto maneras de manipular a las personas a través de técnicas estudiadas en la psicología social. Los ataques de ingeniería social tienen en común la utilización de alguna técnica de este tipo, en un momento u otro, para cumplir sus objetivos. Por lo general, estos ataques no usan exclusivamente estas técnicas, sino que las combinan con otros ataques de índole más tecnológica y con otros tipos de acciones.

Generalmente, los ataques de ingeniería social se basan en la realización de acciones de este tipo para conseguir resultados parciales, que podrán combinarse para poder realizar nuevas acciones, y así reiteradamente hasta conseguir el objetivo final. Es lo que denominamos el proceso de la ingeniería social. La representación gráfica de este proceso para casos concretos nos permitirá estudiar sus características y realizar un análisis para determinar cuáles son los puntos críticos del sistema o diseñar estrategias de prevención.

Cada una de las acciones particulares que se realizan en estos ataques vendrá caracterizada a tres niveles:

1) Estrategia. Determina el tipo de la acción y los objetivos que persigue. Existen tres posibles estrategias: recogida de información, forzar una acción y ataque directo. Todas las acciones pertenecerán a una u otra de estas categorías.

2) Técnica. Para cada estrategia existen varias técnicas concretas para conseguir sus objetivos. Estas técnicas pueden ser muy variadas y pueden ir apareciendo nuevas a medida que se desarrollen nuevas tecnologías.

3) Vía. La vía identifica exactamente el medio por el cual se utiliza una cierta técnica en una acción. Una misma técnica puede aplicarse a través de vías diferentes.

En la representación gráfica de los ataques de ingeniería social, cada acción se identifica mediante la estrategia a la que pertenece, la técnica utilizada y la vía de aplicación, y está representada en un nodo.

Dentro del proceso de la ingeniería social, las acciones se realizarán secuencialmente hasta conseguir la finalidad del ataque. En algunos casos serán necesarias varias acciones previas para realizar otras, o existirán acciones alternativas para conseguir un mismo resultado parcial. Los diagramas DAIS (diagramas de ataques de ingeniería social) nos permitirán representar gráficamente estas relaciones de secuencialidad entre las acciones.

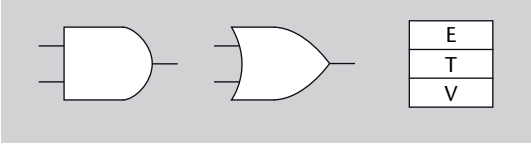
1.2.1. Diagramas DAIS

Una vez vistos los componentes básicos de la ingeniería social, presentamos ahora los diagramas de ataques de ingeniería social (DAIS), que nos permitirán ver de manera gráfica las acciones que intervienen en un determinado ataque de ingeniería social, cuál es su secuencialidad y poder realizar un análisis del ataque. Aunque existen en la bibliografía algunas maneras similares de representar ataques, ninguna considera especialmente el caso de la ingeniería social. Los diagramas DAIS están especialmente indicados para la representación y el análisis de este tipo de ataques.

Un **diagrama de ataques de ingeniería social (DAIS)** es una representación gráfica de las acciones, y sus relaciones, que pueden intervenir en un ataque de ingeniería social.

En los diagramas DAIS los principales nodos son las acciones del ataque, y están representadas por una caja con la identificación de la estrategia, de la técnica que utiliza, así como de la vía por la que se aplica. Las acciones están relacionadas entre ellas o bien a través de una relación directa, o bien a través de nodos conjunto o alternativa. Finalmente, el objetivo final del ataque se especifica con un nodo objetivo. La figura 1 muestra los principales componentes de los diagramas DAIS. Las relaciones se representan como flechas, donde el sentido indica la secuencia.

Figura 1. Elementos clásicos del DAIS



1.2.2. Acciones

Las acciones se representan con una caja de tres secciones: estrategia, técnica y vía. La estrategia puede ser o recoger información o forzar una acción o ataque directo, que en la representación gráfica se representan con las siglas RI, FA o AD, respectivamente, en la sección superior de la caja. La sección central indica la técnica utilizada, y la sección inferior, la vía. En el apartado 2 se detallaran varias técnicas y vías utilizadas en cada estrategia. En este subapartado utilizaremos únicamente el identificador de la estrategia en la representación de las acciones para introducir los diagramas DAIS.

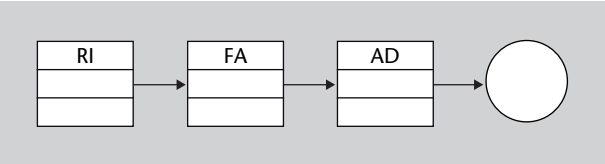
1.2.3. Relaciones secuenciales

Las acciones están conectadas a través de relaciones directas, expresadas como flechas en el diagrama, que representan su secuencialidad, es decir, qué acción debe realizarse antes que otra.

Ejemplo

En el ejemplo de la figura 2 vemos cómo tres acciones deben realizarse una antes que la otra. El resultado de la última acción es necesario para el objetivo final del ataque de ingeniería social, que aparece representado con un círculo en el diagrama DAIS. Para realizar una acción es imprescindible haber realizado antes las acciones que la preceden.

Figura 2. Ejemplo de diagrama DAIS con tres acciones



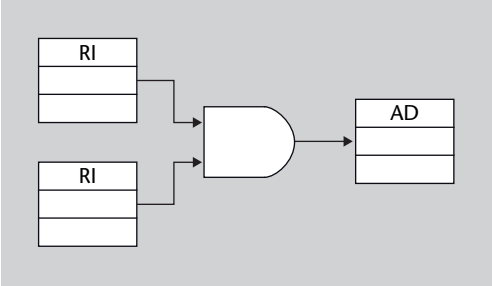
En este caso, hay una acción de recogida de información. Esta información ha sido utilizada para forzar una acción. Finalmente, esta acción ha permitido realizar un ataque directo completando el objetivo inicial del ataque de ingeniería social.

Una acción puede requerir que se haya realizado no solo una acción previa, sino más de una. En este caso, el diagrama DAIS permite especificar a través de un nodo Conjunto que varias acciones deben realizarse para poder llevar a cabo otra. El nodo Conjunto actúa aquí como una "y" lógica. Para poder realizar la acción siguiente a un nodo Conjunto, todas y cada una de las acciones conectadas a este deben haberse completado con éxito.

Ejemplo

En el ejemplo de la figura 3 se puede observar cómo para la realización de una acción de ataque directo es necesaria la obtención de información por medio de dos acciones de recogida de información.

Figura 3. Ejemplo de nodo Conjunto

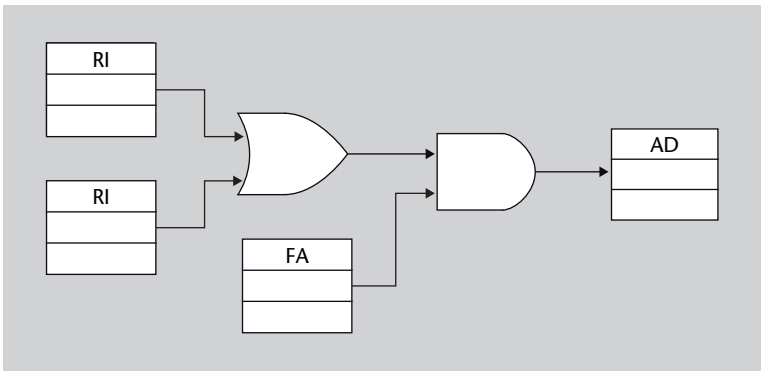


De manera similar, los diagramas pueden expresar alternativas de acciones, es decir, distintas opciones que permiten una cierta acción. En este caso, se utilizarán los nodos Alternativa, que actuarán como la "o" lógica. Si al menos una de las acciones conectadas a un nodo Alternativa se ha conseguido realizar con éxito, aunque ninguna otra lo haya hecho, es suficiente para realizar la acción siguiente en la secuencia.

Ejemplo

La figura 4 muestra un ejemplo donde consiguiendo una información a través de una acción o de otra, y forzando otra acción, se puede llevar a cabo un ataque directo.

Figura 4. Ejemplo con nodo Conjunto y Alternativa



No es necesario ningún otro tipo de nodo para representar las posibles dependencias entre las acciones, ya que cualquier combinación puede ser representada utilizando únicamente las secuencias, las alternativas y los conjuntos.

1.2.4. Normalización

Un mismo ataque de ingeniería social, con exactamente las mismas acciones y relaciones secuenciales entre ellas, puede expresarse de multitud de maneras usando diagramas DAIS. Esto se debe a que hay muchas maneras equivalentes de combinar los nodos Alternativa y Conjunto sin variar la relación final entre las acciones que conectan. Esta flexibilidad se convierte en un inconveniente cuando, por ejemplo, queremos comparar los DAIS de dos ataques. A pesar de ser dos instancias del mismo ataque, la representación en DAIS diferentes, aunque equivalentes, puede obstaculizar su análisis comparativo.

Para solucionar este problema se utiliza el DAIS normalizado, en el que las combinaciones de diferentes nodos Conjunto y Alternativa se fijan en una única posibilidad. En concreto, las relaciones complejas se mostrarán en esta normalización solo como Alternativa de Conjuntos.

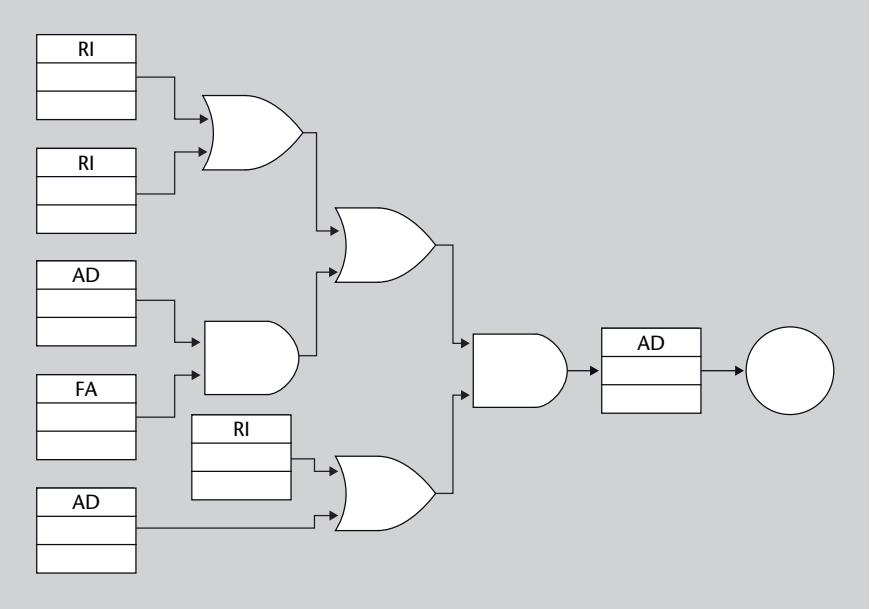
Un **diagrama de ataques de ingeniería social (DAIS) normalizado** es un DAIS en el que los nodos Alternativa y Conjuntos solo se utilizan de manera combinada como Alternativa de Conjuntos.

Esto no limita la expresividad de los diagramas DAIS, ya que cualquier combinación de estos nodos tiene un equivalente en la forma normalizada. Podemos verlo más claramente si consideramos que cada acción tiene un resultado positivo o negativo dependiendo de si se ha realizado con éxito o no. De esta manera, podemos considerar que tenemos una estructura algebraica con dos operaciones internas, "+" y "*", las dos sin inverso pero con elemento neutro, con las propiedades asociativa, distributiva y conmutativa. Así pues, podemos realizar operaciones sobre esta estructura para conseguir la forma normalizada.

Ejemplo

En el ejemplo de la figura 5 se muestra el DAIS correspondiente a un ataque donde hay una sola combinación de nodos Alternativa y Conjunto.

Figura 5. DAIS correspondiente a un ataque



Si expresamos el diagrama DAIS de esta figura representando el nodo Alternativa como el operador "+", el nodo Conjunto como el operador "$*$", y las acciones como los operandos A_i, tenemos una expresión:

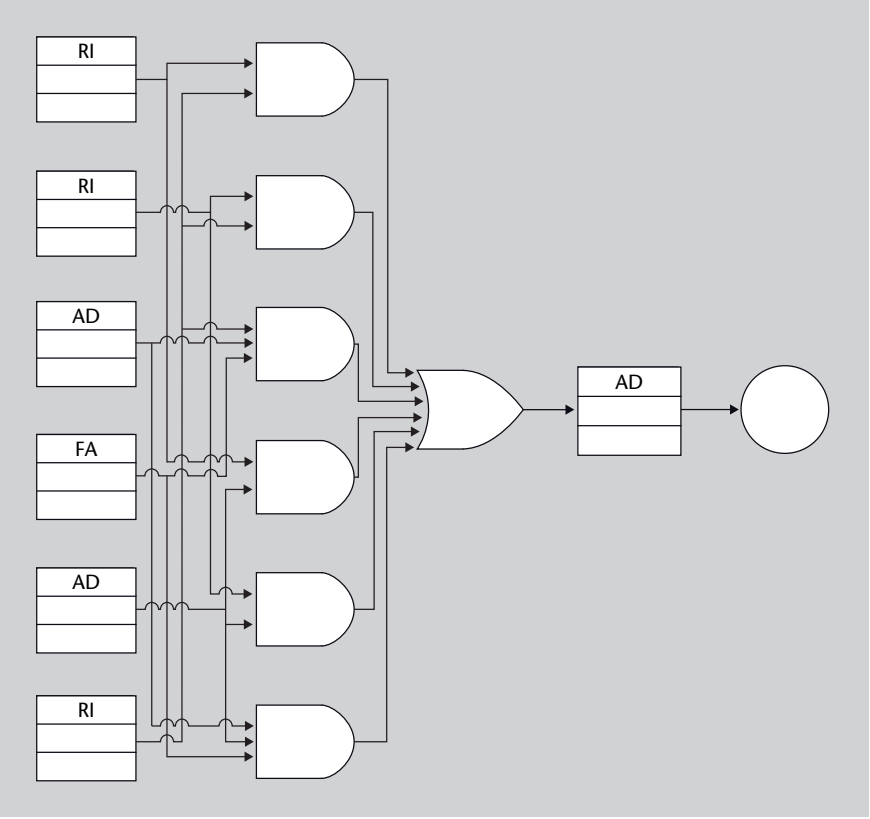
$$[(A_1 + A_2) + (A_3 * A_4)] * (A_5 + A_6)$$

Para convertir esta expresión en su forma normalizada la expandiríamos hasta conseguir esta otra:

$$(A_1 * A_5) + (A_2 * A_5) + (A_3 * A_4 * A_5) + (A_1 * A_6) + (A_2 * A_6) + (A_3 * A_4 * A_6)$$

Después del proceso de normalización (figura 6), se observa cómo sin cambiar la secuencia de acciones del ataque, éste se representa de manera equivalente como una alternativa de conjuntos. Esta manera normalizada permitirá la comparación directa con otros diagramas DAIS.

Figura 6. DAIS equivalente normalizado



Este ejemplo de normalización corresponde a una relación muy compleja de acciones. En los ataques más habituales, tal como se verá en el apartado 3 de casos prácticos, las relaciones suelen ser más sencillas.

2. Estrategias y técnicas

Como hemos visto, el proceso de la ingeniería social comprende un conjunto de estrategias, técnicas y vías para alcanzar un objetivo final. De acuerdo con ello, en este apartado presentamos una taxonomía de dichas estrategias según tres categorías principales:

1) recogida de información,

2) forzar una acción y

3) ataque directo.

A continuación se describirán cada una de ellas de manera más detallada, mostrando también algunos ejemplos de técnicas y vías asociadas. Es importante remarcar que, a diferencia de la categorización que se hace para las estrategias, que es cerrada, tanto las técnicas como las vías asociadas que se exponen aquí no son únicas. Es decir, las técnicas y vías aquí presentadas deben ser consideradas como ejemplos particulares. De hecho, tanto las técnicas como las vías son suficientemente abiertas como para que no sea posible realizar una clasificación e incluso, en un futuro, es posible que aparezcan nuevas que desconocemos. Por tanto, es posible que podáis encontrar otras técnicas asociadas a cada una de las estrategias diferentes a las aquí expuestas.

2.1. Recogida de información

La estrategia de **recogida de información** tiene como finalidad captar información útil para el atacante, y para la cual no debería hipotéticamente tener acceso.

Se trata de la estrategia más sencilla que un atacante puede emplear. La razón de esto estriba en el hecho de que en la mayoría de los contextos en los que el ingeniero social puede actuar, siempre suele existir una cierta fuga de información.

Esta fuga de información puede obedecer a dos patrones posibles. En primer lugar, la información puede ser obtenida al ser expuesta de manera inconsciente por los usuarios. Aquí, el concepto de inconsciencia lo expresamos en

relación con las consecuencias que puede tener desde un punto de vista de la ingeniería social. Cabe destacar el hecho de que este primer patrón siempre implica la existencia de algún componente social o humano. Por tanto, la utilización de, por ejemplo, un *sniffer* de red de manera aislada no es considerado como parte de la estrategia de recogida de información. En segundo lugar, el siguiente patrón se sustenta en obtener la información mediante la interacción del ingeniero social con otras personas. Cada uno de estos patrones los denominaremos como *fuga de información sin interacción humana* y *fuga de información por interacción humana*, respectivamente.

2.1.1. Patrón de fuga de información sin interacción humana

Dentro de la fuga de información sin interacción humana encontramos varias técnicas. En concreto, existen tres posibles:

1) búsqueda en Internet,

2) el agenciamiento físico de información y

3) la observación.

En relación con la técnica de **búsqueda en Internet**, un usuario malintencionado puede encontrar una gran cantidad de información que le puede ser de utilidad simplemente explorando por la Red de redes. Para esto, el atacante puede utilizar algún buscador web empleando filtros diseñados específicamente, o explorando directamente webs conocidas. Algunos tipos de vías para esta estrategia pueden ser las redes sociales, los foros o las páginas web corporativas. En estos entornos la cantidad de información que puede conseguirse es considerable y muy dispar. Algunos ejemplos de tal información pueden ser: relaciones entre personas, información sobre la red o los sistemas de una empresa, personas asociadas a cargos, o números de teléfono, entre otros.

La técnica de **agenciamiento físico de información** se basa en la apropiación no autorizada de elementos físicos que contienen información, y de los cuales el ingeniero social extraerá los datos de su interés posteriormente. Algunos ejemplos de este tipo de información pueden ser nombres, direcciones, números de teléfono, cuentas bancarias, cuentas de correo, etc. Esta categoría podemos subdividirla en dos subcategorías según si el tipo de elemento físico es desechable o no. En el primer caso, la apropiación se realizará en sistemas destinados al almacenamiento de desechos para su posterior recogida y tratamiento (figura 7). Así, algunas de sus posibles vías asociadas son papeleras, contenedores de basura, contenedores de papel para su reciclado, máquinas destructoras de documentos, etc.

Figura 7. Recogida de información

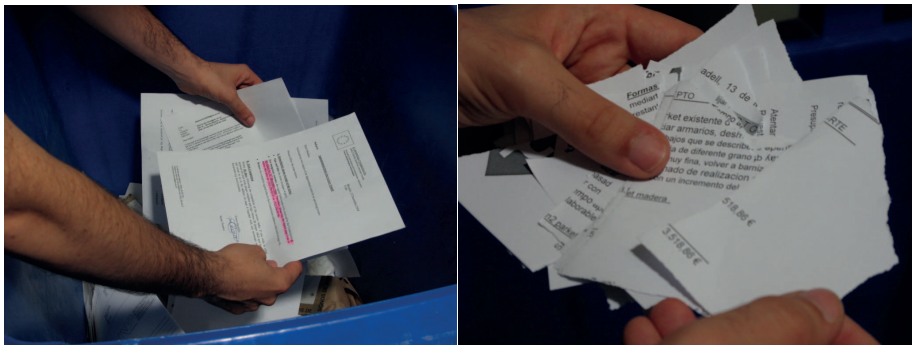


Figura 7

Ejemplo real de búsqueda de información en un contenedor de papel reciclado. Se puede observar a la izquierda documentos sin destruir, y a la derecha un documento en fragmentos que puede ser reconstruido manualmente.

Aunque esto pueda parecer inverosímil, la realidad muestra que existe una cierta despreocupación por parte de organizaciones y empresas por la destrucción efectiva de elementos que contienen información. Ya no solo de información en papel, sino también en dispositivos tales como discos duros o *pendrives*. En este contexto, existen incluso empresas especializadas en la destrucción de componentes que contienen información. En cuanto a la segunda subcategoría, los elementos físicos no serán desechables, y la apropiación puede realizarse en cualquier lugar frecuentado por usuarios. Esta subcategoría incluye vías como pueden ser agendas, documentos, cartas, teléfonos móviles, portátiles, *pendrives*, etc.

Figura 8. Trituradora de documentos

Figura 8

Ejemplo de trituradora. Se puede observar arriba a la izquierda el aspecto de esta abierta, y a su izquierda el detalle del patrón de corte del papel. Abajo a la izquierda, una imagen de la misma destructora triturando un disco compacto junto al detalle de las cuchillas encargadas del corte.

Por último, la técnica de **observación** se centra en la obtención de información basándose exclusivamente en examinar el comportamiento de personas, hechos u objetos. Asimismo, sobre esta observación se pueden aplicar razonamientos lógicos basados en relaciones entre elementos visualizados para extraer conclusiones. Alguna de las vías posibles que puede utilizar un ingeniero

social son las cámaras ocultas, las relaciones o los comportamientos sociales, el seguimiento de personas, etc. A esta categoría también pertenece la vía que denominados como *shoulder surfing* (figura 9). Esta se basa en observar detenidamente la pulsación de las teclas realizadas por un usuario en el proceso de entrada a un sistema. Durante este proceso, el usuario malicioso captará visualmente las pulsaciones tanto para el nombre de usuario como para su contraseña.

Figura 9. *Shoulder surfing*

Figura 9

Simulación de un ataque de *shoulder surfing*. En la foto de la izquierda se puede ver cómo la víctima introduce, sin percatarse del peligro, sus credenciales por teclado. Mientras, el atacante, desde una posición privilegiada observa la contraseña introducida. En la foto de la izquierda, el atacante, con unas gafas de sol que incorporan una cámara oculta, graba las pulsaciones para el posterior análisis del vídeo con detenimiento.

2.1.2. Patrón de fuga de información por interacción humana

Este patrón incluye dos tipos de técnicas. La primera la denominamos *interacción directa* y la segunda, *interacción mediante un medio de comunicación*.

La **interacción directa** es aquella técnica en la que la acción recíproca de comunicación entre el ingeniero social y la víctima se realiza de manera personal y directa, es decir, sin el uso de ningún medio de comunicación entre ambas personas.

Esta técnica puede afectar a tantas personas como puedan existir en una corporación u organismo. Algunos ejemplos pueden ser vigilantes, repartidores, recepcionistas, etc. En este caso, la vía utilizada es la misma conversación que se establece entre el ingeniero social y las personas implicadas.

La técnica de **interacción mediante un medio de comunicación** es la homóloga a la interacción directa, con la diferencia de que existe un medio de comunicación entre el ingeniero social y la víctima.

En este caso, la vía vinculada tiene multitud de formas, tales como teléfono, carta, correo electrónico, fax, aplicaciones de mensajería instantánea, software de VoIP, etc.

2.2. Forzar una acción

La estrategia de forzar una acción es aquella que emplea alguno de los aspectos explotables presentados en el subapartado 1.1, y cuya finalidad es la de conseguir –de manera directa o indirecta– que alguien realice una acción en beneficio del ingeniero social.

Así, una técnica que explotase la autoridad podría ser la impersonación de alguien que ocupase un cargo superior a la víctima, y a la que persuadiría para que modificase la regla de un cortafuegos amenazándole con un posible despido en el caso de no cooperar. En este caso, la vía empleada podría ser, por ejemplo, el teléfono.

Figura 10. Estrategia de forzar una acción

Figura 10

Ejemplo de la estrategia de forzar una acción. Un *pendrive* con un *keylogger* especialmente preparado es dejado en un sitio común como puede ser una fotocopiadora. Si alguna persona tiene la curiosidad de conocer el contenido del *pendrive*, puede ser infectada al introducirlo en su máquina. A partir de este momento sus contraseñas pueden ser comprometidas.

Keylogger

Un ejemplo diferente de técnica podría ser la captura de la contraseña de un usuario utilizando un *keylogger*. Asociada a esta técnica se podría emplear un *pendrive* preparado como vía que contendría el *keylogger* camuflado y que sería puesto en un lugar cercano a la víctima. La víctima, al ver el *pendrive* y desconocer su propietario, podría tomarlo e introducirlo en su máquina influenciada por la curiosidad de conocer su contenido. A partir de aquí, el software malicioso podría instalarse de manera automática empleando algún tipo de vulnerabilidad (Larimer, 2011) para, posteriormente, enviar las pulsaciones de teclas a través de la red.

Explotar la empatía

Otro ejemplo de técnica estaría basado en explotar la empatía. En particular, el atacante podría "dar pena" a una víctima para que esta proporcionase ayuda al ingeniero social y le facilitase, por ejemplo, información sobre la arquitectura de una red con la excusa de que le han amenazado en despedirlo si no soluciona un problema. Aquí la vía empleada sería la misma conversación que mantendrían el atacante y la víctima.

2.3. Ataque directo

La estrategia de ataque directo comprende aquellos ataques de carácter técnico que forman parte de un proceso de ingeniería social. Como ya hemos visto, estos tipos de ataque pueden ser finales o intermedios respecto al proceso de ingeniería social. Estos ataques explotan alguna de las vulnerabilidades que hemos ido viendo a lo largo de esta asignatura. Algunos ejemplos particulares de técnica empleada en este tipo de estrategia podrían ser un ataque de denegación de servicio vía un SYN *flooding* o una escalada de privilegios vía un desbordamiento de un *buffer*.

Figura 11. Ataque directo

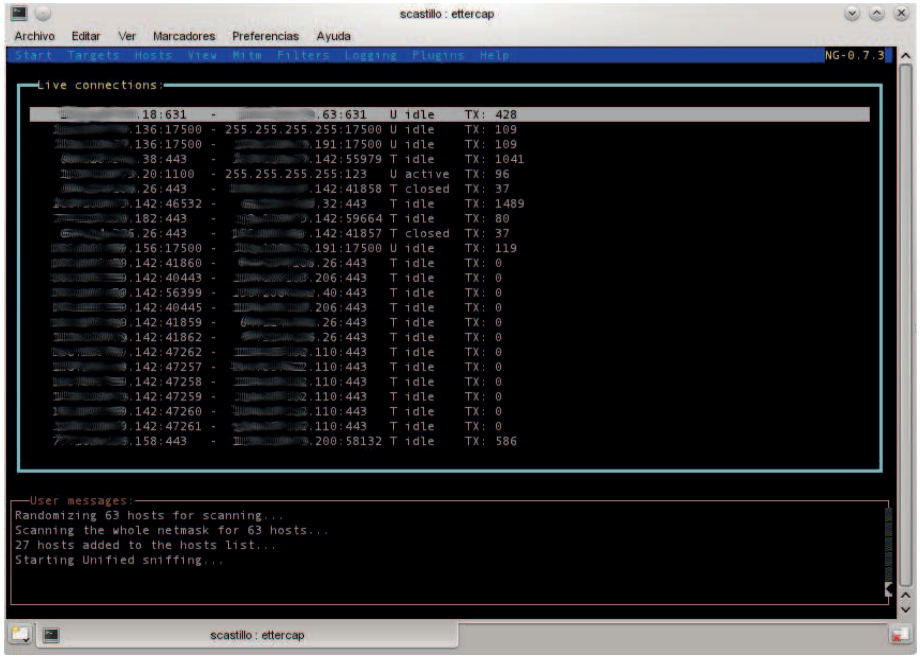


Figura 11

Uso de la aplicación *ettercap* para realizar un ataque directo de tipo ARP *poisoning*.

3. Casos prácticos

En este apartado incluimos una serie de ejemplos prácticos de ataques de ingeniería social. El objetivo es consolidar los conocimientos vistos en los apartados anteriores. Cada uno de los casos que se exponen han sido estructurados de la misma manera. En primer lugar, se expondrá cuál es el objetivo final que persigue el usuario malicioso. Seguidamente, se relatará cuál es el proceso del ataque enumerando los distintos pasos que se realizan hasta que se alcanza el objetivo final. Para concluir, para cada ejemplo se dibujará su diagrama DAIS y se comentará brevemente cada uno de estos.

Lectura recomendada

Os animamos también a consultar la referencia *The Art of Deception: Controlling the Human Element of Security* (2000) de Kevin Mitnick, donde podréis encontrar otros ejemplos que os permitirán complementar los expuestos aquí.

Observación

Estos casos son totalmente ficticios y cualquier parecido con la realidad es pura coincidencia.

3.1. Caso 1: Robo a un banco electrónico

3.1.1. Objetivo

Realizar un robo en un banco que opera por Internet. Es decir, realizar una transferencia monetaria a una cuenta remota.

3.1.2. Escenario

En la sala de juntas de e-Calers, S. A., un conocido banco que opera por Internet, se respira un aire tenso. La directora general está explicando que durante la ausencia del jefe de seguridad ha habido un robo importante (de hecho, una transferencia irrevocable no autorizada de muchos euros a una cuenta de las Islas Caimán). Las fuertes medidas de seguridad informática no parecen haber sido efectivas, pero todavía no saben qué ha fallado. De repente, Carlos, que escuchaba con atención los hechos, abre mucho los ojos y empieza a sonrojarse.

Hace unos días, Carlos recibía una llamada. Era de un técnico de los servicios de informática de la propia empresa que lo llamaba en relación con un cambio de software que se había de producir en breve. Carlos ya sabía de este cambio por una circular interna (recordaba haberla tirado a la papelera). El técnico le explicó que había hablado con el jefe de seguridad, Roque Sierra, antes de que marchara y habían acordado que le pasarían el código de seguridad para la administración de cuentas. Eso era, le explicó, para comprobar que todo funcionara correctamente en la nueva versión antes de ponerla en producción. La clave era diferente cada día, y por ello no se la había dado el propio Roque antes de irse. A Carlos no le hacía mucha gracia dar aque-

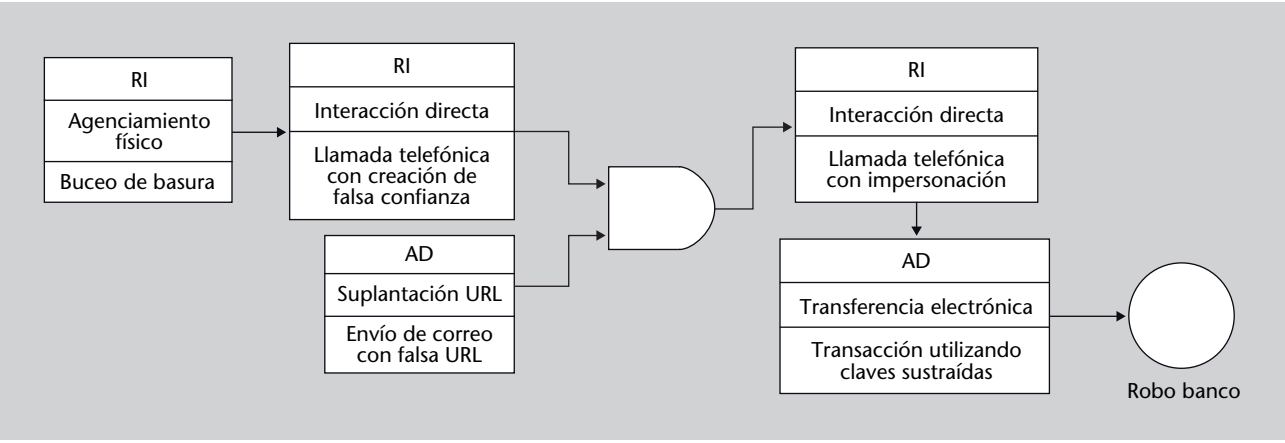
lla clave, pero lo hizo finalmente considerando racionalmente la situación: el técnico sabía dónde estaba el jefe, sabía que él estaba a cargo ahora, y, como le hizo ver, no dársela supondría retrasar el cambio del software por culpa suya y, muy probablemente, una reprimenda de Roque. Además, al conectarse desde su navegador a la URL que le dio el técnico pudo validar la veracidad de lo que le decía: bajo el logotipo corporativo estaba la hoja de seguimiento del proceso de cambio, y en la tarea 16 decía que él mismo debía proporcionar el código al recibir esta llamada.

Unas semanas antes, alguien "buceaba" la basura en los contenedores de papel de e-Calers. Algunos empleados que lo vieron pensaron que era algún indigente buscando cartón para venderlo. Nada más lejos de la realidad. Este personaje estaba muy contento porque había encontrado una circular donde se avisaba de un cambio de software, un resguardo de una reserva de un billete de avión a nombre de Roque Sierra Arán, y algunas copias de facturas de proveedores de servicios. No le costó mucho establecer cierta confianza con la recepcionista de mañanas de la empresa: después de muchas llamadas haciendo ver que era de una de las empresas proveedoras, ¡ya eran casi amigos! Sin mucho esfuerzo le sustrajo qué posición ocupaba en la empresa Roque ("por cierto, ¿no conocerás a un tal Roque Sierra que trabaja allí, que es primo lejano de mi cuñada?"), y quién lo sustituía.

3.1.3. Diagrama DAIS

En la figura 12 se muestra el diagrama DAIS de este escenario.

Figura 12. Diagrama DAIS Caso 1



En este caso tenemos un único nodo de relación de Conjunto, que define dos conjuntos de acciones que realizar: por un lado, la obtención de la información sobre quién es el sustituto del responsable de seguridad; y, por otro, la preparación de un sitio web que será necesario en la siguiente parte del ataque. A partir de aquí vendrá el punto más difícil, conseguir las claves de acceso a través de la persuasión y el engaño, para finalmente culminar el ataque con la sustracción económica a través del desvío a una cuenta extranjera.

3.2. Caso 2: modificación de la página web de un portal

3.2.1. Objetivo

Modificar la página web principal de un portal de venta de libros como medida para desacreditarlo.

3.2.2. Escenario

La tienda online e-Books, una tienda que vende libros a través de Internet, sabe lo importante que es tener una buena imagen desde el punto de vista de la seguridad. Esta es consciente de que noticias acerca de ataques en los que se compromete la seguridad de portales que ofrecen venta de productos perjudica seriamente a las ventas, ya que este tipo de situaciones genera desconfianza hacia los usuarios compradores.

Desde hace unos meses, las ventas de e-Books ha descendido considerablemente tras la aparición del portal CheapBooks, que realiza ofertas muy competitivas y contra las que e-Books no puede competir. Tras este período de tiempo de crisis para e-Books, y en vista de la inminente quiebra de la empresa, el directivo de la empresa decide poner en práctica una campaña de desacreditación de CheapBooks. Para ello, decide contratar a BlackMan —un experimentado individuo en comprometer la seguridad de sistemas— con la finalidad de modificar la web principal del portal de la competencia.

Tras realizar BlackMan un análisis de la seguridad del portal de CheapBooks, concluye que aparentemente no existe ninguna brecha remota que explotar de manera sencilla y que le permita comprometer el sistema. Asimismo, determina que la máquina remota es un sistema GNU/Linux corriendo un servidor web Apache. También descubre que el mismo portal contiene un *frontend* de administración para el que se requiere un nombre de usuario y contraseña.

En esta situación, y dado que BlackMan sabe que en muchas ocasiones el eslabón más débil en seguridad es el propio hombre, decide emplear técnicas de ingeniería social. Después de buscar por la web de CheapBooks, encuentra el nombre y el teléfono tanto del responsable IT, como del administrador de la red, así como el correo electrónico de este último, al que dirigirse en el caso de haber algún problema con la página web.

En primer lugar, BlackMan decide intentar llamar por teléfono al administrador de la red para conseguir la contraseña del *frontend* que le dé acceso a la parte restringida del portal. Para conseguir esto, se intenta hacer pasar por el responsable de IT y le exige que le proporcione la contraseña para modificar una configuración urgentemente. A pesar de ello, el administrador de la red, con una dilatada experiencia en seguridad, reconoce rápidamente el intento

de ataque al no coincidir el timbre de voz con la de su inmediato superior. Seguidamente el administrador de la red informa a su jefe del intento de ingeniería social.

Tras este fracaso, BlackMan decide dejar pasar un tiempo como medida preventiva para no levantar sospechas de que alguien está intentando comprometer la seguridad de CheapBooks. Transcurrido un mes, decide emplear una estrategia de ingeniería social más elaborada. En esta ocasión llama por teléfono al responsable de IT haciéndose pasar por un proveedor de hardware. En esta conversación, BlackMan convence al responsable de IT para mantener una reunión y poder presentarle así supuestas ofertas de interés para la empresa. Antes de mantener la reunión, BlackMan prepara un *pendrive* con un *keylogger* programado por él mismo, y que no es detectable por ningún software antivirus actual al implementar distintos mecanismos de ofuscación. Este software malicioso es almacenado en el *pendrive* con apariencia de ser un documento de nóminas, cuando en realidad se trata de un ejecutable. En concreto, se denomina "Nominas.doc_____.exe". Durante la reunión, realizada en el despacho del responsable de IT, BlackMan deja caer el *pendrive* sin que nadie se percate. Durante el tiempo que dura la presentación de productos, BlackMan intenta ser lo más convincente posible presentando datos reales que ha conseguido previamente. Al despedirse, le pide el correo electrónico al responsable de IT con el pretexto de que le enviará más información.

Al cabo de unos días, el servicio de limpieza encuentra el *pendrive* en el despacho del responsable de IT y, pensando que pertenecería a él, se lo dejan encima de la mesa. Al llegar ese día al despacho el responsable de IT y ver el *pendrive* tiene la curiosidad de saber qué contiene y lo conecta a su portátil. Al inspeccionar el contenido ve un supuesto documento con el nombre "Nominas", sin darse cuenta de que en realidad es un ejecutable. Tras esto, decide abrirlo sin ser consciente del peligro que supone. Procede entonces a hacer un "doble clic" en el archivo y, seguidamente, el mismo ejecutable malicioso muestra una ventana diciendo que el documento está corrupto. Tras esto, el responsable de IT piensa que por algún motivo aquel documento está incompleto o es erróneo y no presta mayor atención a lo ocurrido. Después de esto, el portátil del responsable queda infectado por el *keylogger* que preparó BlackMan y, a partir de entonces, todas las pulsaciones de teclas son enviadas por la red a BlackMan. Gracias a esto, no lleva más de una hora a BlackMan tener en su poder las credenciales de acceso como administrador a una máquina de la red interna denominada `neptuno`.

Al percatarse BlackMan de que la máquina `neptuno` forma parte de la red interna de CheapBooks y de que, por tanto, tiene una IP de un rango privado, decide proceder de la siguiente manera. Al haber obtenido el correo electrónico del responsable de IT durante la reunión, y conocer el del administrador de la red, envía a este último un correo falseando el remitente y haciéndose pasar

por su superior. Esto es posible, ya que el sistema de correo de electrónico de CheapBooks no implementa ninguna tecnología como podría ser OpenSPF o DKIM. El contenido de dicho correo es el siguiente:

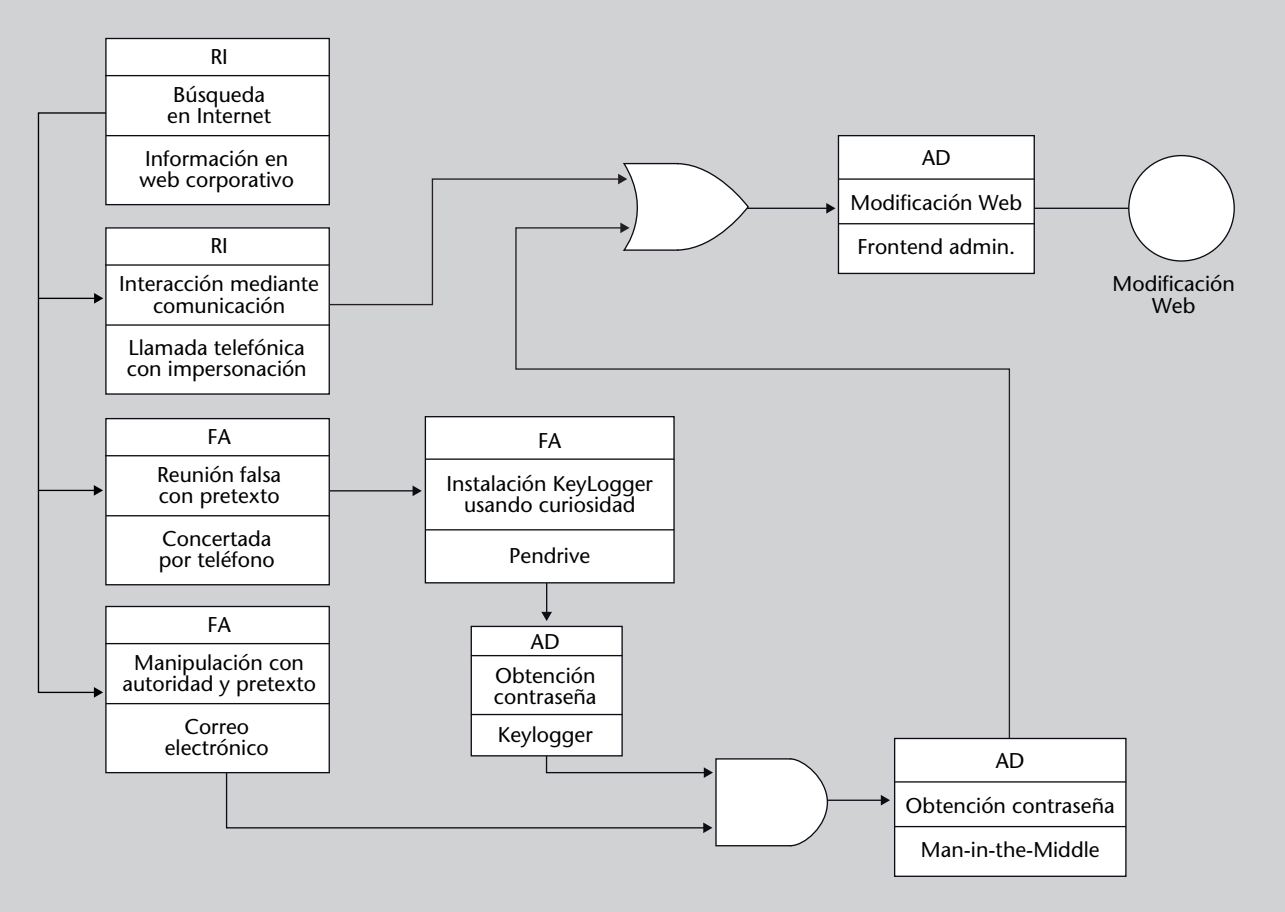
```
Subject: Habilitar NAT hacia neptuno!
From: Juan Sánchez Hipólito <JSanchez@cheapbooks.com>
To: webadmin@cheapbooks.com
Date: 01-06-11 13:50

Hola Toni!
Este próximo fin de semana necesitaría poder acceder a
la máquina neptuno desde casa. Por favor, añade una regla
en el firewall para hacer NAT redirigiendo el puerto 2222
hacia el 22 de la máquina neptuno.
Buen fin de semana!
```

Al recibir el responsable de la red el correo procede a realizar la petición que le ordenan. Durante ese fin de semana BlackMan se conecta a la máquina `neptuno` desde el exterior, y se da cuenta que desde ella no puede acceder directamente al servidor web para modificar su contenido. Sin embargo, en el archivo `/etc/hosts` de `neptuno` descubre que la IP del servidor web es 10.0.0.10. Después de un rápido análisis del servidor web desde la red interna, concluye que la única manera de acceso a este es físicamente o a través del *frontend* que ya conocía de hacía tiempo. Entonces, decide esperar al lunes, momento en el que lanza un ataque de tipo *Man-in-the-Middle* empleando *ARP-Spoofing* que le permite capturar las credenciales del administrador de la red que le autentican hacia el *frontend*. En ese momento, BlackMan, con pleno acceso al servidor web, modifica la página web principal. En esta deja un mensaje donde se proclama que la seguridad de CheapBooks es deficiente y que los clientes no deberían fiarse de las compras que realizan.

3.2.3. Diagrama DAIS

El diagrama DAIS de la figura 13 corresponde a este caso de estudio. A partir de información obtenida del web corporativo, se inician una serie de acciones que pueden realizarse en paralelo. En este punto no hay ninguna relación de alternativa ni de conjunto. A partir de aquí, deberán completarse la acciones de instalación del *keylogger* y la obtención de la contraseña para poder continuar (secuencia de conjunto) y obtener la contraseña con un ataque de *Man-in-the-Middle*. Una vez se dispone de esta contraseña, o si ha resultado con éxito una recogida de información a través de llamada telefónica (secuencia alternativa), ya se podrá realizar el ataque final: la modificación de la web a través del *frontend* de administración.

Figura 13. Diagrama DAIS Caso 2



3.3. Caso 3: Modificación de notas en una universidad

3.3.1. Objetivo

Alterar la nota de una asignatura en el expediente electrónico de un alumno en una universidad.

3.3.2. Escenario

No podía ser que a ella, que se consideraba buena en seguridad computacional, le suspendieran *Criptografía* sólo por haber tenido un mal día cuando hicieron el examen final. Tenía que actuar para poner los puntos sobre las íes: se modificaría ella misma el 4 que le había puesto el profesor, por un 9, una nota más acorde a su nivel, según ella.

Después de averiguar más o menos cómo funcionaba el proceso de introducción de calificaciones finales en el expediente electrónico y cierre de actas, por medio de los manuales de ayuda para profesores publicados en la página web de la universidad, ya podía empezar a urdir su plan de ataque basado, cómo

no, en la ingeniería social. Después de todo, estudiar el criptosistema utilizado para encontrar vulnerabilidades tampoco acababa de ser lo suyo.

Intentar conseguir directamente las contraseña del profesor estaba descartado. Era un profesor de seguridad, así que el riesgo era grande. El primer objetivo, por tanto, sería saber la máquina donde estaba el servidor central de LDAP. Si comprometía esa máquina, podría conocer, probablemente, la contraseña de su profesor para entonces entrar utilizando su identidad y realizar el cambio de nota.

Después de algunas llamadas para intentar averiguar qué ordenador albergaba el servidor, decidió cambiar de estrategia. El personal de la universidad se mostraba muy recelosa a revelar detalles tan técnicos. Pensó en una alternativa ingeniosa, y en unas pocas llamadas telefónicas averiguó pronto dónde enviaban los equipos obsoletos cuando eran sustituidos por otros más nuevos. No le fue difícil agenciarse, en la planta de reciclaje donde enviaban los ordenadores viejos, de algunos discos duros que venían de la universidad. Aunque el contenido de los discos había sido borrado, con la ayuda de software especializado consiguió recuperar mucha de la información que contenían. En el segundo disco encontró lo que buscaba: un fichero de configuración con la dirección IP del servidor de LDAP y su contraseña de autenticación.

No sería sencillo entrar en el servidor de LDAP desde fuera, así que debería arreglárselas para realizar una intrusión en uno de los ordenadores internos. Después de preparar un programa troyano, lo envió por correo electrónico a varias personas de la administración de la universidad. El correo parecía un mensaje típico que se envían entre amigos, con una multitud de destinatarios, y haciendo referencia a un vídeo que se incluía y parecía ser muy gracioso. Una de las víctimas seleccionó el vídeo para visualizarlo, lo que, además, instaló un pequeño programa que daría acceso remoto al ordenador. Una vez dentro, consiguió entrar en el servidor de LDAP y tener acceso al *hash* SHA1 de la contraseña del profesor. Utilizando un programa de romper contraseñas basado en palabras de diccionario encontró después de unas horas la palabra de paso que buscaba. ¡Bingo!

Con la contraseña de acceso ya podía entrar en el portal web de introducción de calificaciones impersonando a su profesor, pero aún necesitaba otra contraseña, la de traspaso de calificaciones al acta de la asignatura. Teniendo ya el *password* de acceso y los datos básicos del profesor (número de identificación en la universidad, nombre completo, DNI, etc.) consiguió cambiar esta segunda contraseña por teléfono alegando que la había olvidado.

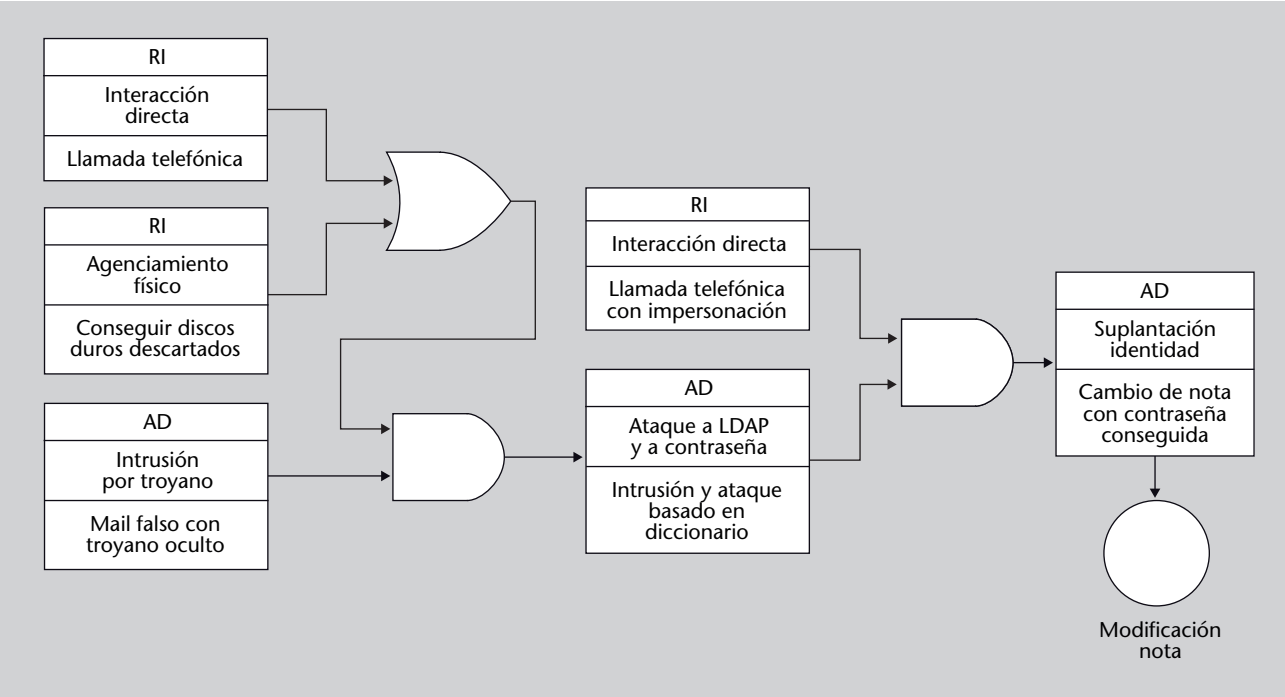
Ahora ya tenía todo, solo faltaba la estocada final. Desde un navegador de la biblioteca, accedió al portal de notas, se cambió el 4 a un 9, y transfirió las notas al acta. Ya lo había conseguido; ¡se había hecho justicia! La alegría, sin embargo, le duró poco. Después de unos días, el profesor detectó el cambio

cuando estaba repasando los sobresalientes para decidir quién recibiría matrículas de honor. Aunque durante todo el ataque no dejó ninguna traza que la inculpara, estaba claro quién era la única interesada en modificar esa nota en concreto.

3.3.3. Diagrama DAIS

El diagrama DAIS correspondiente a este caso se muestra en la figura 14.

Figura 14. Diagrama DAIS Caso 3



En este caso vemos las seis acciones más importantes en este ataque de ingeniería social organizadas a través de dos relaciones de conjunto y una de alternativa. En las acciones de la alternativa, comenzando cronológicamente, se intenta primero obtener información por medio de una llamada y al no conseguirlo, se opta por buscar esta información en un disco duro desinventariado. Con la información de la localización del servidor de LDAP, juntamente (relación conjunto) con el control de una máquina interna conseguido mediante un troyano, ya se puede realizar el ataque a LDAP y al *hash* de la contraseña del profesor que está en él. Con otra llamada telefónica se consigue la otra contraseña necesaria para realizar el último ataque, que es el cambio de la nota.

4. Casos especiales de ingeniería social

En el contexto de la ingeniería social podemos encontrar multitud de ataques con características diferentes. Esta afirmación cobra sentido si recordamos que estos ataques vienen definidos como un proceso compuesto por un conjunto de acciones relacionadas secuencialmente. Entre todo el abanico de diferentes posibilidades, existen una serie de ataques de ingeniería social que tienen una especial relevancia por su cotidianidad. En este apartado trataremos brevemente cinco casos de ingeniería social que son familiares para la mayoría de los usuarios, y cuyo denominador común es que, a excepción del *SMiShing*, se producen en el contexto de Internet. Estos casos especiales de ingeniería social son el *phishing*, el *vishing*, el *SMiShing*, el *scareware* y los *hoaxes*.

4.1. *Phishing*

El *phishing* es un ataque de ingeniería social cuyo objetivo final es el de obtener datos bancarios de una víctima con una finalidad fraudulenta. Para conseguirlo, el ingeniero social suplanta la identidad de una entidad financiera y convence a un usuario para realizar una acción que le permite captar dichos datos.

Para realizar el *phishing*, el ingeniero social utiliza el correo electrónico como vía. En ocasiones este tipo de envío se realiza de manera masiva a cuentas de correo que han podido ser obtenidas a través de distintos medios. El envío indiscriminado de correos se realiza con el objetivo de maximizar las probabilidades de éxito del ataque. En este correo se solicita a la víctima que visite la web de la entidad, donde posteriormente se le pide que introduzca sus datos personales junto a sus credenciales. El engaño en este proceso reside en el mismo correo, donde se suele incluir un enlace a la supuesta web legítima; sin embargo, dicho enlace apunta en realidad a un servidor especialmente preparado por el atacante, donde es capaz de recoger los datos de su interés. Dependiendo de la habilidad del ingeniero social en preparar un correo electrónico convincente, y de lo creíble que le resulte a la víctima, el ataque tendrá éxito o no.

4.2. *SMiShing*

El *SMiShing* es una variante del *phishing*, con la diferencia de que este se realiza utilizando mensajes de telefonía móvil de tipo SMS (*short message service*).

Aquí, el usuario recibe un SMS procedente de una supuesta entidad bancaria y en el que se le fuerza, mediante ingeniería social, a realizar una llamada a un número particular, o a enviar una respuesta al mensaje con datos solicitados.

Figura 15. Ejemplo de *phishing*

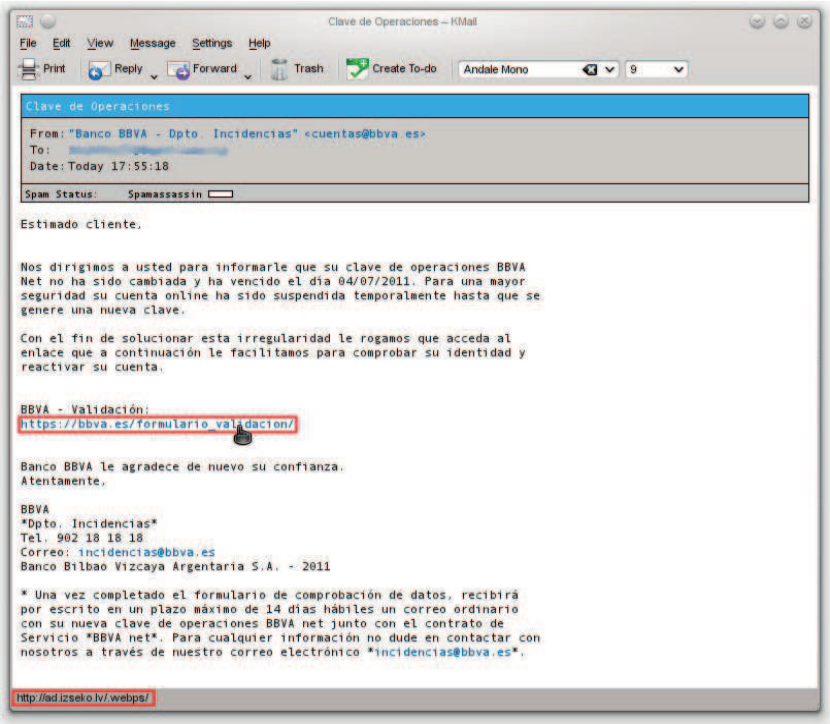


Figura 15

Ejemplo de *phishing* por correo electrónico. Nótese que la URL mostrada en el cuerpo del correo no coincide con la apuntada por el enlace en la parte inferior izquierda de la imagen.

4.3. *Vishing*

El *vishing* es también una variante del *phishing*. En este caso, la diferencia radica en que es realizado por voz utilizando el sistema de telefonía tradicional, o en algunas ocasiones el ingeniero social suele usar los servicios ofrecidos por la telefonía sobre IP (VoIP).

El ataque se basa en utilizar un sistema automático que realiza llamadas a números de teléfono. Cuando detecta que en el otro extremo hay una persona, se le comunica que hay algún tipo de problema con su tarjeta de crédito y se le convence para que proporcione ciertos datos, entre los que figura el número de su tarjeta, la fecha de caducidad y el código de seguridad.

4.4. *Scareware*

El *scareware* es una forma de software malicioso para obtener beneficios empleando ingeniería social. En concreto, explota el engaño, la persuasión, la coacción o el miedo mediante mensajes de alarma o de amenaza para forzar a la víctima a realizar un pago. El ejemplo más común es el de supuestas soluciones de seguridad que se instalan y nos advierten de que el sistema está infectado por algún tipo de código malicioso. A partir de aquí, el *scareware* brinda la posibilidad al usuario de eliminar el hipotético *malware* realizando un pago, ya sea mediante una tarjeta de crédito o incluso vía SMS.

Una alternativa en cuanto al método utilizado es el *malware* identificado por algunos antivirus como *W32/CardPay.A*, *Win32/DotTorrent.A* o *FraudTool.W32 /Fakecopyright*, entre otros. Se basa en explotar el sentimiento de culpa y el miedo que pueden sentir usuarios al descargar software ilegal. En particular, una vez instalado muestra mensajes de advertencia indicando que se están violando las leyes del *copyright* y que se tiene identificada la IP del usuario. Seguidamente, propone evitar un juicio realizando un pago como modo de solventar la situación.

Figura 16. Ejemplo de *scareware*

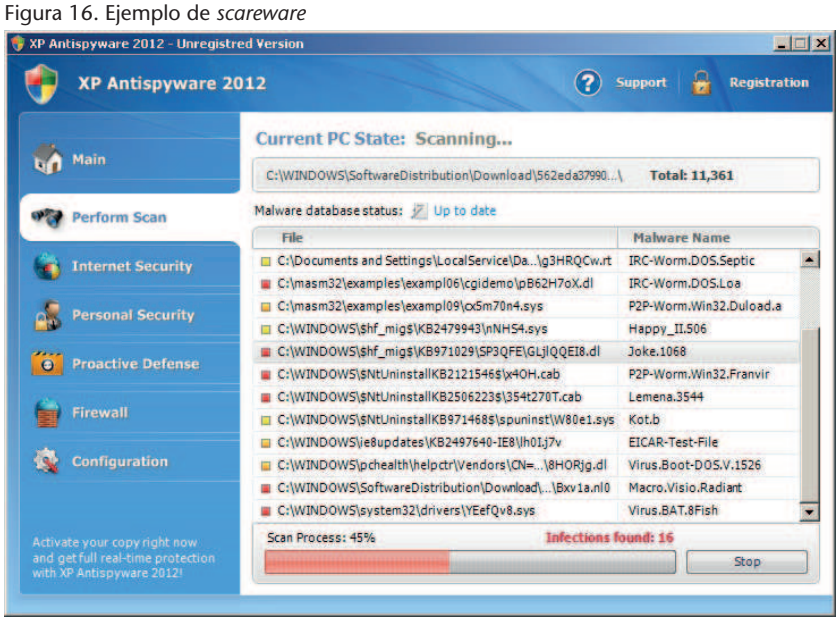


Figura 16

Ejemplo de *scareware*. La supuesta aplicación antivirus muestra que el sistema está infectado por una gran cantidad de software malicioso, cuando en realidad no es así. Posteriormente ofrece la posible compra del producto para desinfectar el sistema.

4.5. *Hoaxes*

Un *hoax* es un tipo de ataque de ingeniería social que se da en el ámbito del correo electrónico. Se basa en crear una noticia o un rumor totalmente falso en forma de correo electrónico, en el que se fuerza al destinatario, utilizando algunos aspectos explotables mezclados vistos en el subapartado 1.1, al reenvío de este para que se propague y distribuya en cadena.

Detrás de los *hoaxes* pueden existir distintos intereses, tales como causar alarma social, confundir o modificar la opinión pública, desprestigiar una empresa o recogida de correos electrónicos para posteriormente utilizarlos como destinatarios de *spam*. De ahí la necesidad de explotar aspectos como son el engaño, la parquedad, la prueba social, la amabilidad o la empatía entre otros. Asimismo, la temática de estos suele ser muy variada, como por ejemplo: virus informáticos, leyendas urbanas, cadenas de solidaridad, etc. Sirva de ejemplo el siguiente correo considerado como un *hoax*:

```
¡ATENCIÓN ESTE MENSAJE ES VERÍDICO!

¿Sabes que la leche en cartón que no se vende dentro
del plazo de caducidad regresa a la fábrica para ser
repasteurizada y vuelve al supermercado de nuevo?.
Increíble ¿verdad?. Pues la ley permite a las centrales
lecheras repetir este ciclo hasta 5 veces, lo que termina
dejando la leche casi sin sabor y con una significativa
reducción de su calidad y valor nutricional.

Cuando la leche llega al supermercado para la venta al
consumidor final, el cartón debe exhibir un pequeño número
que está marcado en su parte inferior. Ese número varía del
1 al 5. Lo más que se debe tolerar es comprar leche hasta
el número 3, es decir, leche que ha sido repasteurizada 2
veces, recomendándose no comprar cartones de leche cuyo
número sea 4 o 5, ya que ello significa que la calidad de
la lecha estará degradada. Si compras una caja cerrada,
basta verificar el número de la caja, ya que todos los
cartones en su interior tendrán la misma numeración.
Por ejemplo, si un cartón tiene el número 1, significa
que es la primera vez que sale de la fábrica y llega al
supermercado para su venta, pero si tiene el número 4,
significa que caducó 3 veces y que fue repasteurizada 3
veces volviendo al supermercado para tratar de ser vendida
y así sucesivamente...

Así es que, ya sabes, cuando compres leche, mira el fondo
del cartón y no compres cajas que tengan los números 4 o 5,
y para los más escrupulosos, ni siquiera el 3.

En el archivo adjunto podrán ver el número en cuestión. Id
al super, tomad una caja de leche y comprobad el número,
dudo que encuentréis el 1 o el 2.

SI TIENES CONCIENCIA CIUDADANA, ¡DIVULGA ESTE MENSAJE!!
```

5. Análisis

Tradicionalmente, las recomendaciones que se han sugerido para la lucha contra la ingeniería social han estado enfocadas a la formación del personal y las auditorías. Este tipo de formación tiene una fuerte dependencia en función de cada persona, su cargo dentro de una organización y el nivel de acceso que tiene a información crítica. Así, la formación que se debe dar a una persona de mantenimiento no debería ser la misma que a otra que trabaja como administrador de sistemas. En ocasiones, esta formación es nula o tan genérica que no tiene en cuenta las características de cada individuo. A pesar de ello, incluso personas con formación adecuada recibida no se escapan de los factores humanos tan explotado por la ingeniería social. Existe, por tanto, la necesidad de una metodología que permita determinar las personas críticas, así como los requisitos de formación de cada una de ellas. De esta manera, se podrá hacer un especial énfasis en la concienciación que deben tomar determinadas personas dentro de una organización.

Tal y como se ha podido comprobar en el apartado anterior por medio de distintos casos, la utilización del diagrama DAIS permite obtener una visión global de un ataque de ingeniería social. También se ha podido verificar cómo el diagrama puede construirse desde la perspectiva del ingeniero social antes de realizar el ataque, o desde el punto de vista de una auditoría de seguridad tras haberse perpetrado el ataque. Como se verá en este apartado, el uso de este tipo de diagramas va más allá de la simple comprensión de cuál ha sido la planificación o la evolución de un ataque de este tipo. Concretamente, se presenta aquí una metodología que, partiendo de un diagrama DAIS, permite analizar la seguridad de los sistemas de información desde la perspectiva de la ingeniería social. En particular, la estrategia que se muestra permite analizar y detectar de una manera evolutiva los factores de riesgo que pueden intervenir en un posible ataque de ingeniería social. De este modo, no sólo es posible ser consciente de qué medidas técnicas podrían ser incorporadas para mejorar la seguridad, sino también de cómo determinar las personas críticas que requieren una formación específica dada su criticidad ante ataques de este tipo.

Esta metodología se denomina *retro-ampliación inversa del diagrama DAIS*. A continuación describiremos esta estrategia, enumerando los pasos que se deben seguir y haciendo especial hincapié en los elementos críticos que nos permite identificar.

5.1. Retro-ampliación inversa del diagrama DAIS

La retro-ampliación inversa del diagrama DAIS es una metodología iterativa y evolutiva que permite determinar elementos críticos en una organización desde la visión de la ingeniería social. Como su propio nombre sugiere, está basada en los diagramas DAIS ya presentados anteriormente. Como se ha podido comprobar, el diagrama DAIS puede ser construido desde diferentes puntos de vista. Hasta ahora solo se han mostrado dos tipos: el diagrama DAIS construido por un ingeniero social antes de un ataque y el diagrama DAIS construido por un especialista de seguridad tras perpetrarse un ataque.

La retro-ampliación inversa del diagrama DAIS parte del ataque final del diagrama DAIS. A partir de aquí, el experto en seguridad deberá analizar e identificar todas los posibles acciones de la ingeniería social predecesoras que han conducido a dicho ataque final. Cada una de estas acciones es considerada entonces como un factor de riesgo. A partir de esto, por cada acción predecesora se aplica de manera recursiva la misma idea. Es decir, se buscarán las acciones predecesoras de estas ultimas y así sucesivamente.

Estrategia preventiva

La retro-ampliación inversa trabaja con los diagramas DAIS tras perpetrarse un ataque como método correctivo. Sin embargo, también puede ser aplicado como una estrategia preventiva partiendo de potenciales ataques finales que se podrían llevar a cabo en una empresa o entidad, y cuyo denominador común es el uso de la ingeniería social.

De manera más formal, podemos definir la retro-ampliación inversa del diagrama DAIS de la siguiente manera:

1) Obtener el diagrama DAIS asociado a un proceso de ingeniería social.

2) Normalizar el diagrama DAIS.

3) Considerar como **acción actual** el objetivo del diagrama DAIS normalizado. Notaremos la acción actual mediante la expresión A_C.

4) Para la acción actual A_C, identificar y determinar las acciones predecesoras A_i (i = 1...n) tales que existe una relación secuencial entre cada A_i y A_C.

5) Si algún A_i no forma parte del diagrama DAIS, añadirlo junto a su relación secuencial respecto a A_C en forma normalizada.

6) Considerar cada A_i como un factor de riesgo.

7) Para cada A_i, considerar $A_C := A_i$ y repetir de manera recursiva el paso 4 hasta que no se identifiquen más acciones predecesoras.

Es importante destacar que el concepto de identificación y determinación de acciones predecesoras que aparece en el paso 4 depende exclusivamente del conocimiento que tenga el experto en seguridad sobre la organización que esté realizando el análisis. Este tipo de conocimiento no será exclusivamente social, sino también técnico. El motivo de esto radica en el hecho de que, tal y como hemos visto anteriormente, en un ataque de ingeniería social aparecen acciones tanto de carácter social como técnico. Por tanto, el experto de seguridad deberá conocer aspectos no sólo tecnológicos, sino también organizativos,

personal que forma parte de la empresa, niveles de acceso a información que tiene cada individuo, etc. Como se puede desprender de esto, este tipo de análisis no es exhaustivo y completo, ya que la cantidad de acciones que pueden intervenir en un ataque de ingeniería social son incontables. A pesar de ello, la retro-ampliación inversa del diagrama DAIS debe ser entendida como una herramienta de ayuda para mejorar la seguridad global de una organización.

Tras el proceso de ampliación del DAIS, y mediante la visualización del nuevo diagrama, se pueden identificar gráficamente aspectos relevantes en relación con el ataque sobre el que se está trabajando. Así, como ya hemos visto en el pseudo-código anterior, una vez que ha finalizado la ejecución de algoritmo, tendremos identificados los factores de riesgo tanto humanos como tecnológicos. Sin embargo, el nuevo diagrama nos permite obtener mayor información. En concreto, podemos emplear dicha representación del ataque para obtener los siguientes datos útiles:

- Acciones críticas (tanto de carácter tecnológico como social). Estas acciones serán aquellas que, eliminándolas, el ataque se ve mitigado considerablemente o incluso eliminado.

- Conjunto/s de acciones mínimas para que un ataque tenga éxito.

- Probabilidad de éxito de llevarse a cabo un ataque. Esto se puede obtener si introducimos probabilidad en cada relación secuencial y calculamos la probabilidad de éxito final.

- Nivel de riesgo del ataque respecto a la seguridad global. De modo similar al caso anterior, se puede calcular asignando a cada relación secuencial un valor numérico asociado al riesgo.

Esta forma de análisis incluso nos permitiría establecer un conjunto de diagramas DAIS que podríamos definir como *patrones tipo de la ingeniería social*. Esto posibilita realizar taxonomías y categorizaciones de ataques, de manera que conocido un patrón y la solución que se ha de aplicar, se puede extrapolar a aquel ataque que contenga el mismo patrón.

5.2. Ejemplo de análisis mediante retro-ampliación inversa

Con el objetivo de que os familiaricéis con el procedimiento que se debe seguir en la retro-ampliación inversa del diagrama DAIS, presentamos en este subapartado un caso ficticio de ataque de ingeniería social. En este ejemplo, tras estudiar el caso y obtener el diagrama DAIS correspondiente, procederemos a realizar un análisis según la retro-ampliación del diagrama, lo que nos permitirá deducir los aspectos destacables del ataque, tales como elementos críticos, acciones mínimas para llevar a cabo el ataque, etc.

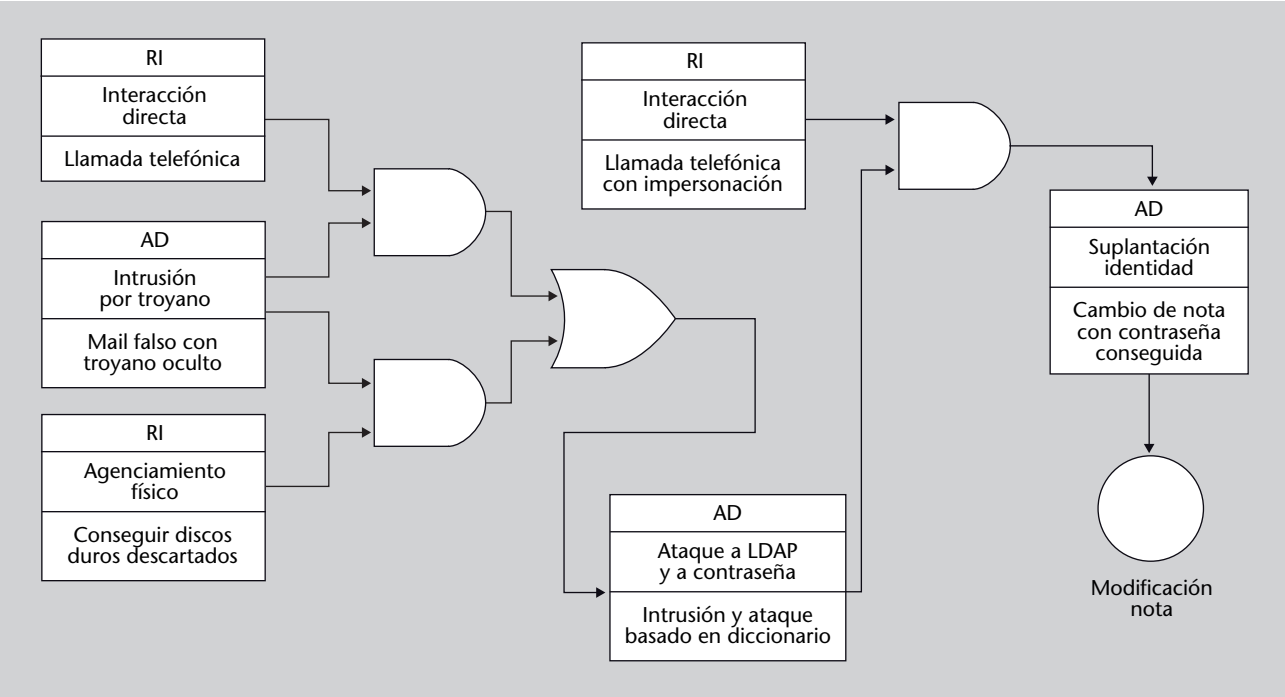
5.2.1. Descripción del escenario

Para realizar este ejemplo de análisis se utilizará el escenario de modificación de notas en una universidad descrito en el subapartado 3.3 de ejemplos prácticos.

5.2.2. Retro-ampliación inversa del diagrama DAIS

Los primeros pasos para realizar el análisis es obtener el diagrama DAIS y normalizarlo. El diagrama DAIS se observa en la figura 14, y su versión normalizada en la figura 17.

Figura 17. Diagrama DAIS normalizado del caso 2



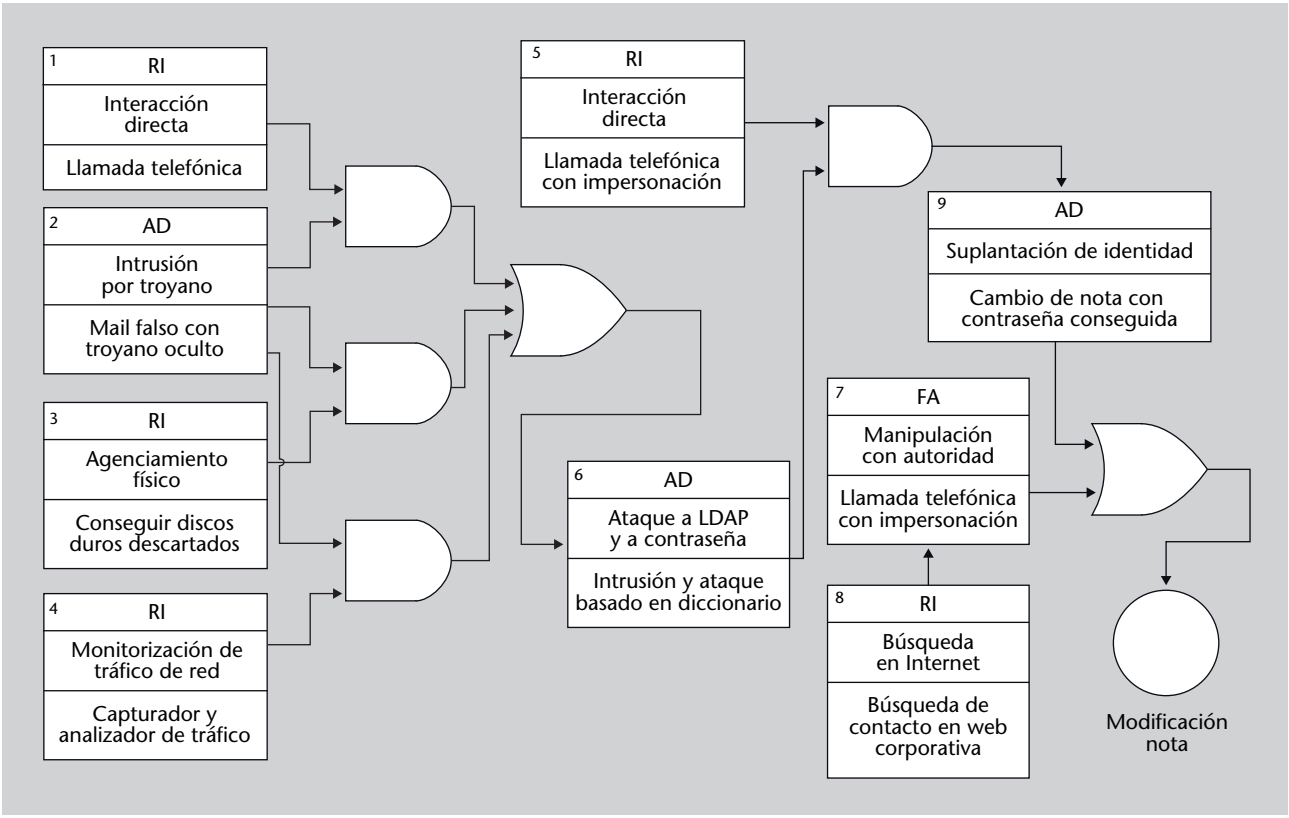
Tras la normalización del diagrama DAIS, el analista de seguridad puede proceder a identificar y determinar acciones predecesoras, así como sus relaciones de secuencialidad, partiendo del objetivo final. En nuestro caso, este proceso no lo haremos de manera exhaustiva, dada la existencia de una estrecha relación entre las acciones que se deben añadir en el diagrama retro-ampliado y el contexto en el que nos encontremos.

En el escenario que nos ocupa, el analista partiría del objetivo final, es decir, del cambio de una nota por suplantación de identidad mediante una contraseña obtenida. Para conseguir esta modificación, una alternativa sería forzar una acción. En concreto, esta consistiría en convencer, vía teléfono, a alguien de gestión académica de que el ingeniero social es el propio profesor responsable de la asignatura y de que la nota de un alumno particular debe ser modificada. Analizando las posibles formas de conseguir el teléfono de contacto de

gestión académica, el analista de seguridad se percata de que en la web de la universidad aparece dicho número (estrategia tipo recogida de información). Por tanto, la relación de secuencia entre ambas acciones (recogida de información primero, y forzar una acción segundo) conducirían al mismo objetivo final.

Prosiguiendo con el análisis, el experto en seguridad, al estimar cuáles son los predecesores del ataque directo a LDAP y a la contraseña del profesor, podría percatarse de que la autenticación contra el servidor de LDAP se realiza con un protocolo en claro. Es decir, en el proceso de autenticación contra el servidor la correspondiente contraseña viaja sin cifrar. La combinación de usar un troyano junto a la captura de tráfico en la red interna le podría permitir a un potencial usuario malintencionado conseguir la contraseña de autenticación hacia dicho servidor. A partir de entonces, conseguir la contraseña almacenada en SHA1 sería un paso trivial. En la figura 18 podemos observar el diagrama ampliado resultante.

Figura 18. Diagrama DAIS normalizado y ampliado del caso 2



Tras la obtención del diagrama DAIS ampliado, podemos deducir directamente que las acciones críticas son la 2, 6, 7 y 9. Por otro lado, los conjuntos mínimos de acciones para alcanzar el objetivo son {1,2,5,6,9}, {2,3,5,6,9}, {2,4,5,6,9} y {7,8}.

6. Prevención y reflexiones

El proceso de la ingeniería social es bien conocido, y sus bases han sido utilizadas durante siglos para realizar acciones fraudulentas de diversa índole. Con la aparición de los sistemas computacionales de información, la ingeniería social ha cobrado una especial relevancia al no aplicarse ya únicamente en el mundo físico, sino en el mundo digital. A lo largo de este módulo hemos visto cómo desde el punto de vista de la seguridad informática las vulnerabilidades que permiten ataques de este tipo están muy ligadas a las tecnologías disponibles.

Sin embargo, las soluciones para evitar ataques de ingeniería social son un tema mucho más complicado y, pese a ser un aspecto fundamental en la seguridad de los sistemas de información, lo encontramos casi marginado en la bibliografía y excluido en muchos tratados de seguridad. El motivo es la complejidad asociada a este problema. Aunque existen algunas medidas para minimizar la probabilidad de éxito de los ataques de ingeniería social, veremos en este apartado que no existe una manera de erradicar completamente estas graves vulnerabilidades.

Las maneras de afrontar el problema se basan en la formación y sensibilización, así como en la definición y aplicación de políticas de seguridad.

6.1. Formación y sensibilización

La formación del personal en una organización sobre la ingeniería social es un elemento básico para la lucha contra esta. Sin embargo, no está claro quiénes han de ser los receptores de dicha formación, ya que todo el personal relacionado con la organización de un modo u otro es susceptible de ser víctima de la ingeniería social. Esto incluye desde el personal de limpieza y mantenimiento, hasta los altos cargos de gerencia.

Para ser efectiva, el aprovechamiento de la formación debe validarse frecuentemente, normalmente mediante auditorías especializadas. Asimismo, una medida que suele ayudar a mejorar los resultados de este proceso de formación es la utilización de esquemas de incentivo/penalización, que recompense al personal que utilice de manera adecuada los conocimientos adquiridos y que penalice, económicamente o de otro modo, al que demuestre no haber aprovechado esta formación. De esta manera se incentiva al personal a considerar seriamente los problemas de seguridad asociados a la ingeniería social.

El problema más grave del proceso de formación es su elevado coste, ya que debe estar dirigido a un colectivo muy numeroso, se trata de una docencia muy especializada y requiere su constante validación generalmente por medio de auditorías. Una alternativa mucho más económica son las campañas de sensibilización. El objetivo de estas campañas es concienciar a los miembros de una organización sobre los métodos utilizados por la ingeniería social para poder identificarlos cuando se presentan y poder así evitarlos. La sensibilización puede ser complementaria a la formación, reservando esta última para los colectivos más sensibles.

Figura 19. Ejemplo campaña de sensibilización

Figura 19

Izquierda: ejemplo de póster de una campaña de concienciación sobre el problema de la ingeniería social. Contiene consejos básicos para evitar los ataques más frecuentes. Derecha: camiseta de sensibilización de la ingeniería social.

6.2. Políticas de seguridad y auditorías

Además de la formación, es muy importante incluir puntos específicos sobre la ingeniería social en las políticas de seguridad de la organización. La figura 20 muestra algunos ejemplos de puntos que deberían tenerse en cuenta en las políticas de seguridad de una organización.

Figura 20. Ejemplo campaña de sensibilización

- El alcance de la información sensible no debe de ir más allá del círculo de personas estrictamente necesario.
- Los documentos con información sensible estarán siempre guardados bajo llave cuando nadie los custodie.
- Bajo ningún concepto se facilitaran claves de acceso por teléfono o correo electrónico, aunque quien las solicite proclame ser un administrador.
- La presencia de personas desconocidas debe reportarse siempre al responsable de seguridad.
- Todos los documentos serán destruidos cuando acabe su vida útil, sin importar si contienen información sensible o no.
- Desconfiar sistemáticamente de los mensajes recibidos por correo electrónico y de las llamadas telefónicas.
- Siempre que sea posible, devolver las llamadas o correos electrónicos para asegurar que no existe una impersonación.
- Utilizar criptografía para garantizar la autenticidad y el secreto del correo electrónico.
- Nunca seguir enlaces proporcionados por correo electrónico o teléfono; en su lugar, buscar el enlace de otras fuentes.
- No utilizar dispositivos de almacenamiento (como *pendrives* o discos duros, por ejemplo) que han tenido contacto con el exterior de la organización.

Para validar la correcta aplicación de las políticas de seguridad, es conveniente realizar auditorías especializadas en ingeniería social de manera periódica. La auditorías permiten detectar también nuevas vulnerabilidades, permitiendo la actualización de las políticas. El ciclo de definir políticas de seguridad y auditar debería repetirse de manera continua.

6.3. Ingeniería social, psicología y humanidad

La mayoría de las vulnerabilidades explotadas por la ingeniería social, tal como se ha visto en el primer apartado de este módulo, vienen derivadas de cualidades humanas como la facilidad de establecer cierta confianza entre individuos tras un período de interacción. Algunas de estas cualidades, como la caridad o la cortesía, son generalmente considerados aspectos positivos en nuestra sociedad. Otras, como la empatía o el deseo de ayudar, responden a reacciones más instintivas. Incluso los aspectos más racionalmente controlables, como la reacción ante la autoridad o la avaricia, pueden usarse para manipular psicológicamente al individuo y ejercer una influencia para la realización de acciones inducidas.

Si consideramos a un ordenador inmune a los ataques de ingeniería social es precisamente porque carece de todas estas cualidades que nos acaban haciendo, precisamente, humanos. Si una persona se comporta de tal manera que no sea posible manipularla de algún modo utilizando las técnicas descritas, será muy difícil que esté integrada en la sociedad, ya que la percepción que se tendrá de ella es muy negativa. Lo podemos ver claramente con un ejemplo. Si al tercer intento de introducir una contraseña en un ordenador que utilizamos habitualmente, este nos bloquea el acceso hasta que un supervisor lo vuelva a habilitar, nos conformaremos resignadamente. Si en cambio una persona nos pide la identificación para entrar al trabajo y un día la hemos olvidado, no entenderemos por qué nos bloquea el acceso, y le exigiremos flexibilidad apelando, precisamente, a su humanidad. Es difícil comprender en el momento que esa misma flexibilidad podría permitir el acceso a un atacante.

Evitar el problema, por lo tanto, es muy difícil, si no imposible. Las estrategias de formación y concienciación son claramente útiles y necesarias, pero no eluden totalmente los ataques de ingeniería social. Para evitar el ataque hay que focalizar en la parte final del diagrama DAIS extendido, es decir, en las amenazas directas, para bloquear los ataques asumiendo que el ingeniero social tiene a su disposición toda la información.

Resumen

Sin duda alguna, la seguridad computacional es una disciplina compleja debido a la gran cantidad de áreas interrelacionadas que abarca. En muchas ocasiones se incurre en el error de considerar estas áreas desde una perspectiva exclusivamente tecnológica, cuando la realidad va mucho más allá. Un claro ejemplo de esto es la ingeniería social, uno de los componentes de la seguridad que muchas veces pasa desapercibido o al que no se le da la importancia que merece. La realidad ha demostrado, en más de una ocasión, que en seguridad el eslabón más débil de la cadena sigue siendo el componente humano y, por ende, la ingeniería social no debe ser menospreciada como fuente de posibles ataques.

A lo largo de este módulo hemos diseccionado la ingeniería social hasta concebirla como un proceso, compuesto por un conjunto de acciones y relaciones secuenciales entre ellas. En todo ataque de ingeniería social, el denominador común siempre será la existencia de alguna acción basada en la manipulación psicológica de las personas. Detrás de esta manipulación se esconden múltiples aspectos explotables, y que el atacante puede usar en su favor para alcanzar su objetivo final.

La existencia de estos aspectos humanos explotables, más propios de la psicología social, no deben hacernos caer en el error de pensar que no forman parte del dominio de la seguridad computacional. Debemos, por tanto, integrarlos en todo proceso de análisis y de mejora de la seguridad de los sistemas de información. En este sentido, hemos visto cómo los diagramas DAIS son una herramienta que permite establecer una metodología analítica de gran utilidad. Así, los diagramas DAIS nos permiten representar ataques de ingeniería social de una manera gráfica, al mismo tiempo que son la base para detectar elementos críticos en una organización por medio de la retro-ampliación inversa.

Por último, no debemos olvidar qué estrategias preventivas deben ser utilizadas para evitar ataques de ingeniería social. Estas estrategias pasan por una formación adecuada del personal, considerando su posición dentro de la organización jerárquica, así como el nivel de privilegios de acceso que tenga a sistemas e información. Asimismo, la definición de políticas claras de seguridad para evitar ataques de ingeniería social deben ser impuestas. Como medida para garantizar que estas políticas de seguridad son conocidas y puestas en práctica por todo el personal, las auditorías de seguridad deben ser utilizadas como modo de validar su cumplimiento.

Actividades

1. Buscad en vuestra papelera física información que podría ser utilizada para realizar un ataque de ingeniería social. A partir de los datos individuales que obtengáis, intentad pensar en cómo los relacionarías y sacarías posibles conclusiones.

2. Buscad en vuestro correo electrónico un caso de *phishing* y de *hoax*.

3. Encontrad en Internet ejemplos de *hoaxes* y razonad qué acciones se deberían tomar si recibimos alguno.

4. Buscad ejemplos de *hoax* en Internet y redactad uno nuevo teniendo en cuenta los aspectos explotables vistos en este módulo. No lleguéis a enviarlo.

5. Simulemos que, como ingeniero social, habéis conseguido un *pendrive* del cual queréis extraer información. Para ello, pedid a alguien que copie en él cinco archivos cualesquiera. Tras esto, indicadle a esa persona que elimine dos de estos archivos. A continuación, simulad que os habéis hecho con el *pendrive* sin su consentimiento. Seguidamente, descargad la herramienta TestDisk* e intentad recuperar los archivos eliminados. ¿Creéis que los usuarios son conscientes de la posibilidad de recuperación de datos? ¿Cómo relacionáis esto con la ingeniería social?

6. Pensad un posible ataque de ingeniería social que se podría dar en vuestro lugar de trabajo o estudio habitual. Dibujad su correspondiente diagrama de DAIS y normalizadlo. Intentad aplicarle la retro-ampliación inversa para que sea más completo.

7. Buscad alguna noticia real en la que el uso de la ingeniería social haya estado presente de algún modo.

8. Realizad una pequeña encuesta en vuestro lugar de estudio o trabajo sobre el conocimiento y la concienciación de las personas ante los ataques de ingeniería social. ¿Qué proporción de encuestados creéis que saben qué es la ingeniería social? Comparad vuestra previsión con los resultados que habéis obtenido.

¡Atención!

Este ejercicio podría causar la pérdida de información! Realizad esta actividad con la máxima cautela posible. Leed con detenimiento la documentación de TestDisk antes de realizarla. Aseguraos de que la recuperación la aplicáis sobre el *pendrive* con el que trabajáis.

***http://www.cgsecurity.org/wiki/TestDisk**

Ejercicios de autoevaluación

1. ¿Qué afirmación es cierta sobre los diagramas DAIS?
a) Son una representación exhaustiva de un ataque de ingeniería social que contempla todas las acciones posibles.
b) Su versión normalizada no permite la comparación con otros diagramas.
c) Pueden ser expresados a partir de una estructura algebraica con dos operaciones internas.
d) Ninguna de las anteriores.

2. ¿Cuál de los siguientes aspectos no se explota directamente en la ingeniería social?
a) Receptividad a la autoridad
b) Fácil establecimiento de confianza
c) Inundación por amplificación de peticiones DNS
d) Recuperación de datos de un disco duro

3. El uso de un *pendrive* con un *keylogger* puede ser empleado en un ataque de ingeniería social mediante una estrategia de tipo...
a) recogida de información.
b) forzar una acción.
c) ataque directo.
d) Ninguna de las anteriores.

4. Un ataque de ingeniería social...
a) emplea los aspectos explotables humanos.
b) es la acción con la que finaliza todo proceso de ingeniería social.
c) puede ser contrarrestado con medidas tecnológicas.
d) a) y c)

5. Un programa instalado en un sistema que identifica una gran cantidad de virus y que nos sugiere la compra de éste para desinfectar la máquina es un tipo de...
a) phishing.
b) hoax.
c) scareware.
d) Todas las anteriores.

6. El *phishing* explota...
a) la falsa confianza.
b) la reciprocidad.
c) la similitud.
d) Todas las anteriores.

7. La retro-ampliación inversa...
a) no requiere de un diagrama DAIS normalizado.
b) no es útil si no se ha producido un ataque de ingeniería social.
c) conduce a un DAIS que contiene acciones del ataque aunque éstas no hayan sido identificadas por el analista de seguridad.
d) Ninguna de las anteriores.

8. En la retro-ampliación inversa el analista de seguridad...
a) debe tener un conocimiento social y jerárquico respecto a las personas de la empresa implicada.
b) no es necesario que conozca los mecanismos de seguridad tecnológicos implantados en la empresa.
c) es capaz de identificar todos los elementos críticos.
d) Ninguna de las anteriores.

9. ¿Qué afirmación es cierta sobre la ingeniería social?
a) No es necesario concienciar a los usuarios sobre medidas para evitar ser víctimas de estos ataques.
b) No se puede evitar solamente con medidas tecnológicas.
c) No afecta a los sistemas de tipo Unix.
d) Todas las anteriores.

10. Para minimizar la probabilidad de éxito de los ataques de ingeniería social, una organización puede...
a) ampliar la política de seguridad.
b) ofrecer un plan de formación específica.
c) iniciar una campaña de concienciación.
d) Todas las anteriores.

Solucionario

1. c; **2.** c; **3.** b; **4.** a; **5.** c; **6.** a; **7.** d; **8.** a; **9.** b; **10.** d.

Bibliografía

Cacioppo, J. T.; Petty, R. E.; Kao, C. F.; Rodriquez, R. (1986). «Central and peripheral routes to persuasion: An individual difference perspective». *Journal of Personality and Social Psychology*, (n.º 51, págs. 1032–1043).

Cialdini, R. B. (2008). *Influence: Science and Practice*. (5.ª ed.). Pearson Education.

Larimer, J. (2011). «Beyond Autorun: Exploiting vulnerabilities with removable storage». BlackHat, Washington (USA): IBM X-Force Advanced Research.

Mitnick, K. D.; Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. (1.ª ed.). Nueva York: John Wiley & Sons, Inc.

Myers, D. G. (1994). *Exploring social psychology*. Nueva York: McGraw-Hill.