Universitat Oberta de Catalunya

uoc.edu

Estudio de metodologías de Ingeniería Social

Alumno: **Joan Enric Garcia Romero**

Plan de Estudios: **Máster Interuniversitario en Seguridad en las TIC**

Área del trabajo final: **Ad-hoc**

Consultora: **Angela María García Valdés**

Profesor: **Victor Garcia Font**

Fecha Entrega: **Enero 2019**

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Estudio de metodologías de Ingeniería Social*
Nombre del autor:	*Joan Enric Garcia Romero*
Nombre del consultor/a:	*Ángela María García Valdés*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	01/2019
Titulación:	*Máster Interuniversitario en Seguridad en las TIC*
Área del Trabajo Final:	*TFM – Ad hoc*
Idioma del trabajo:	*Castellano*
Palabras clave	*Ingeniería Social, Ciberseguridad*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

Este trabajo consiste en un estudio sobre las metodologías de la ingeniería social, así como los diferentes ataques existentes y técnicas utilizadas.

Con este objetivo se definirá el concepto de ingeniería social, se estudiarán sus diferentes roles y su relación con la ley. A continuación, se repasarán los ataques más conocidos y se explicarán alguno de los más famosos de la historia. Seguidamente se profundizará en las diferentes técnicas que se utilizan para llevar a cabo estos ataques, como de las herramientas existentes que pueden facilitar los mismos. Finalmente se realizará un simulacro de ataque para acabar explicando algunos consejos sobre cómo prevenirlos.

Abstract (in English, 250 words or less):

This work is a study on the social engineering methodologies, as well as the different existing attacks and techniques used.

This objective will define the concept of social engineering, their different roles and the state of the art of law about this topic. Then we will review the best known attacks and explain some of the most famous in history. After that, It will go deeply studying the different techniques used to carry out these attacks, as well as the existing tools that can facilitate them. Finally, there will be a mock attack to finish explaining some advice on how to prevent them.

Índice

Contenido

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

En una sociedad cada vez más tecnológica, la ciberseguridad tiene un peso más importante en el día a día. A día de hoy se conocen y se dispone de miles de programas y/o componentes con la intención de evitar poner en riesgo nuestra información.

Pero entre todas las técnicas y amenazas que se utilizan, hay una antigua técnica que han sabido adaptar perfectamente a este mundo tecnológico, la ingeniería social.

La ingeniería social *es la ciencia y arte de hackear a seres humanos* [1]. Esos ataques que son dirigidos hacia el usuario, no hacia la tecnología.

Actualmente, esos ataques son una de las tres mayores amenazas con las que debe hacer frente la ciberseguridad, hay estudios que sitúan el error humano en el 17%[2] de los ataques, mientras otros elevan está cifra hasta el 27%[3], en este último caso se remarca que el precio asociado a esta cifra es de 128 US$ per cápita.

En este trabajo se realizará un estudio en profundidad sobre las metodologías de la Ingeniería Social, las técnicas actuales, los métodos y programas utilizados, las actuales soluciones y se aprovechará esta

[1] https://www.kaspersky.es/blog/ingenieria-social-hackeando-a-personas/2066/

[2] 2018 Data Breach Investigations Report, Verizon, 2018

[3] 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute and IBM, July 2018

información para desarrollar un ataque mediante todo lo anteriormente comentado y finalmente se buscará la mejor forma de evitarlo.

Se trata de conseguir ayudar a concienciar, conocer y proteger a los usuarios sobre estos métodos.

1.2 Objetivos del Trabajo

El objetivo principal de este trabajo es dar a conocer, concienciar y proteger a los usuarios todo aquello relacionado con la Ingeniería Social con la intención de ayudar a estos mismos a evitar en la mayor medida de los posible todos aquellos métodos y técnicas que se describirán a lo largo de este trabajo. Todo ello se realizará mediante los siguientes objetivos:

1. Descripción Ingeniera social. Roles.
2. Ataques conocidos de ingeniería social.
3. Métodos y estrategias utilizados.
4. Diseño de ataque de ingeniería social.
5. Métodos de prevención.

1.3 Enfoque y método seguido

El enfoque elegido para realizar este trabajo se basa en la búsqueda en los elementos disponibles sean artículos de Internet, libros, vídeos y apuntes.

Una vez obtenida la información se centrará en la recogida y selección de esta, a partir de ese momento se empezarán a usar los conocimientos en diferentes recursos on-line con el objetivo de ampliar ese conocimiento mediante interacción con otros expertos en la materia sea de forma presencial o telemática.

Una vez adquirido ese conocimiento se realizará su redacción y se llevará acabo el diseño del ataque, para finalmente acabar encontrando las diferentes medidas preventivas.

Cabe destacar que este ciclo de:

Búsqueda – Selección – Redacción – Implementación

Es iterativo y puede ser repetido tantas veces como sea necesario durante la duración del proyecto.

En un estudio potencialmente teórico en gran parte, es muy importante tener toda la información correspondiente a las preguntas que se quieran responder, para poder sintetizar y profundizar en aquellos puntos interesantes con el objetivo de obtener ese conocimiento y seguidamente tratar de ponerlos en prácticas dentro del ámbito de la legalidad.

1.4 Planificación del Trabajo

Objetivo 1:	Descripción Ingeniera social. Roles.
	1. Historia 2. Conceptos básicos 3. Roles 4. Ley y la Ingeniería Social
Objetivo 2:	Ataques conocidos de ingeniería social.
	1. Estudio tipos de ataques y victimas 2. Resumen de historia
Objetivo 3:	Métodos y estrategias utilizados.
	1. Métodos de obtención de información

	2. Técnicas de suplantación 3. Psicología en Ingeniería Social 4. PSYOPS 5. La influencia 6. Herramientas Ingeniería Social
Objetivo 4:	Diseño de ataque de ingeniería social.
	1. Selección objetivo 2. Estudio vulnerabilidades. 3. Diseño 4. Realización/Simulación 5. Análisis resultados
Objetivo 5:	Métodos de prevención.
	1. Evaluación de los ataques. 2. Puntos críticos y como prevenirlos.

ID	Outline	WBS Code	Type	Name	Predecessor	Start	Finish	Duration	% Complete	Resources
0	**0**		**Summary**	**TFM**		**01/10/18 08:00**	**31/12/18 08:00**	65d	**7,4**	
1	**1**	**1**	**Summary**	**Recopilación de Información básica y d...**		**01/10/18 08:00**	**16/10/18 12:00**	12d	**66,7**	
2	2	1.1	Normal	Búsqueda de información en Internet y me...		01/10/18 08:00	09/10/18 12:00	7d	100,0	
3	2	1.2	Normal	Búsqueda y lectura de material en libros s...		05/10/18 08:00	15/10/18 12:00	7d	100,0	[Joan Enric Garcia]
4	2	1.3	Normal	Redacción PAC1	2;3	16/10/18 08:00	16/10/18 12:00	1d	0,0	[Joan Enric Garcia]
5	**1**	**2**	**Summary**	**Descripción Ingenieria Social. Roles**		**17/10/18 08:00**	**24/10/18 12:00**	6d	**0,0**	
6	2	2.1	Normal	Historia Ingenieria Social		17/10/18 08:00	17/10/18 12:00	1d	0,0	[Joan Enric Garcia]
7	2	2.2	Normal	Conceptos básicos Ingenieria Social	6	18/10/18 08:00	19/10/18 12:00	2d	0,0	[Joan Enric Garcia]
8	2	2.3	Normal	Roles de la Ingenieria Social	6	18/10/18 08:00	22/10/18 12:00	3d	0,0	[Joan Enric Garcia]
9	2	2.4	Normal	Ley y Ingenieria Social		23/10/18 08:00	24/10/18 12:00	2d	0,0	[Joan Enric Garcia]
10	**1**	**3**	**Summary**	**Ataques conocidos Ingenieria Social**		**25/10/18 08:00**	**29/10/18 12:00**	3d	**0,0**	
11	2	3.1	Normal	Estudio tipos de ataques y victimas	5	25/10/18 08:00	26/10/18 12:00	2d	0,0	[Joan Enric Garcia]
12	2	3.2	Normal	Resumen historia	11	29/10/18 08:00	29/10/18 12:00	1d	0,0	[Joan Enric Garcia]
13	**1**	**4**	**Summary**	**Métodos y estrategias utilizados**		**30/10/18 08:00**	**26/11/18 12:00**	20d	**0,0**	
14	2	4.1	Normal	Métodos básicos	10	30/10/18 08:00	01/11/18 12:00	3d	0,0	[Joan Enric Garcia]
15	2	4.2	Normal	Métofos de recopilación de información	14	02/11/18 08:00	07/11/18 12:00	4d	0,0	[Joan Enric Garcia]
16	2	4.3	Normal	Técnicas de suplantación	15	08/11/18 08:00	09/11/18 12:00	2d	0,0	[Joan Enric Garcia]
17	2	4.4	Normal	Psicología en Ingeniería Social	16	12/11/18 08:00	15/11/18 12:00	4d	0,0	[Joan Enric Garcia]
18	2	4.5	Normal	PSYOPS	17	16/11/18 08:00	20/11/18 12:00	3d	0,0	
19	2	4.6	Normal	Herramientas Ingenieria Social	18	21/11/18 08:00	26/11/18 12:00	4d	0,0	[Joan Enric Garcia]
20	1	5	Normal	PAC 2		03/12/18 08:00	03/12/18 08:00	0h	0,0	[Joan Enric Garcia]
21	**1**	**6**	**Summary**	**Diseño de ataque de ingeniería social**		**27/11/18 08:00**	**20/12/18 12:00**	18d	**0,0**	
22	2	6.1	Normal	Selección objetivo	13	27/11/18 08:00	28/11/18 12:00	2d	0,0	[Joan Enric Garcia]
23	2	6.2	Normal	Estudio vulnerabilidades	22	29/11/18 08:00	30/11/18 12:00	2d	0,0	[Joan Enric Garcia]
24	2	6.3	Normal	Diseño	23	03/12/18 08:00	07/12/18 12:00	5d	0,0	[Joan Enric Garcia]
25	2	6.4	Normal	Realización/ Simulación		10/12/18 08:00	18/12/18 12:00	7d	0,0	[Joan Enric Garcia]
26	2	6.5	Normal	Análisis resultados	25	19/12/18 08:00	20/12/18 12:00	2d	0,0	[Joan Enric Garcia]
27	**1**	**7**	**Summary**	**Métodos prevención**		**21/12/18 08:00**	**26/12/18 12:00**	4d	**0,0**	
28	2	7.1	Normal	Evaluación ataques	21	21/12/18 08:00	21/12/18 12:00	1d	0,0	[Joan Enric Garcia]
29	2	7.2	Normal	Puntos críticos y como prevenirlos	28	24/12/18 08:00	26/12/18 12:00	3d	0,0	[Joan Enric Garcia]
30	1	8	Normal	Redacción conclusiones	27	27/12/18 08:00	28/12/18 12:00	2d	0,0	[Joan Enric Garcia]
31	1	9	Normal	Revisión y entrega		31/12/18 08:00	31/12/18 08:00	0h	0,0	[Joan Enric Garcia]

Ilustración 1. Tabla de planificación de tareas

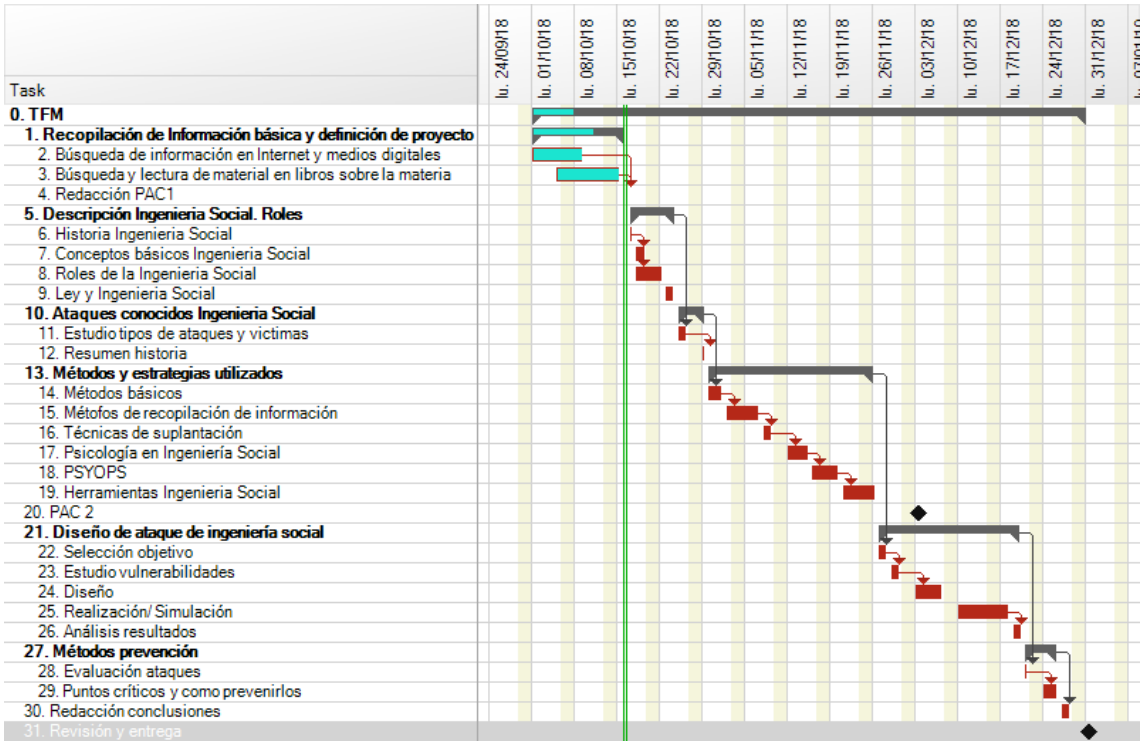


Ilustración 2. Diagrama de Gantt

1.5 Análisis de riesgos

- El autor de este proyecto se encuentra actualmente en busca de trabajo, cosa que podría provocar una variación en el calendario del proyecto.
- El desconocimiento del autor en el momento de iniciar el proyecto también puede ser un riesgo para cumplir las fechas previstas.
- Actualmente solo existen la consultora del proyecto y el profesor responsable como dependencias externas que podrían hacer variar el mismo.
- No es necesaria una aportación económica para realizar el proyecto, motivo por el cual el dinero no es un riesgo.
- Se deberá comprobar que todo material utilizado respeta los pertinentes derechos de autor para su uso.

1.6 Presupuesto del proyecto

Este proyecto está exento de la necesidad de encontrar recursos económicos para la realización de este. Se tratará de sacar el máximo rendimiento posible a las fuentes públicas de información como son las bibliotecas y a todos aquellos recursos que pueden ser obtenidos gratuitamente en la red. En el momento de que por un motivo imprevisto el proyecto necesitara financiación, esta se debería de cubrir mediante el aporte de capital del principal interesado.

1.7 Breve descripción de los otros capítulos de la memoria

- **¿Qué es la Ingeniería Social?**
  Capítulo introductorio a diferentes conceptos donde se verá de forma superficial la historia del término “Ingeniería Social”, las diferentes definiciones actuales de este, los roles que pueden realizar esta acción y finalmente su relación con la ley.

- **Ataques conocidos de ingeniería social**
  En este capítulo se describen algunas de los principales métodos de ataque de la Ingeniería Social, en la segunda parte del capítulo se describen algunos famosos ataques realizados con éxito.

- **Métodos y estrategias utilizados**
  En este capítulo se profundiza en algunas de las técnicas más interesantes en el ámbito de la ingeniería social, basándose en técnicas de recopilación de información, suplantación de identidad y técnicas de psicología como podrían ser las PSYOPS o la PNL.

- **Herramientas Ingeniería Social**
  Capítulo en el cual se van a describir una serie de herramientas que facilitan la realización de los ataques comentados anteriormente. Se

exponen y clasifican herramientas de diferentes tipos como son las herramientas físicas, herramientas de software o herramientas de Internet

- **Diseño de un ataque de Ingeniera Social**
  Capítulo dedicado a dar un ejemplo de un posible ataque de ingeniería social contra una empresa ficticia, mediante la realización de una auditoria solicitada por la misma.

- **Métodos de prevención**
  En este capítulo se ofrecen una serie de consejos para todas aquellas personas que estén interesadas, que pueden resultar muy útiles en una gran cantidad de ataques.

2. ¿Qué es la Ingeniería Social?

En este capítulo se buscará abordar una de las partes esenciales de este proyecto, se tratará el concepto de Ingeniería Social, su historia, sus diferentes definiciones y los roles que intervienen, juntamente con sus características. Finalmente, se explicará la relación actual entre la ley y la IS.

2.1. Historia

Según Joseph M. Hatfield[4] el termino *Social Engineer* aparece por primera vez en 1842 en un libro titulado *An Efficient Remedy for the Distress of Nations* escrito por el economista británico John Gray. En él se habla de los Ingenieros Sociales como aquellas personas encargadas

[4] Joseph M. Hatfield, Social engineering in cybersecurity: the evolution of a concept, *Computers & Security* (2017)

de solucionar los problemas de la sociedad, de igual forma que unos ingenieros mecánicos tratarían de arreglar un motor.

Con el tiempo el termino iría adquiriendo diferentes significados, uno de los más destacados es el hecho de describir las relaciones de poder entre los colonizadores y las tribus colonizadas en África. En 1938, Margaret Read usaba *social engineering* para describir el método usado para conquistar la gente Ngoni de Nyasaland (actualmente Malawi). Read había observado que esa ingeniería social involucraba planificación, modificaciones de las instituciones y estructuras sociales y la construcción de una nueva identidad nacional.

En ese momento el término ingeniería social ya contenía tres ideas básicas fundamentales que prevalecen en la actualidad:

- **Asimetría epistémica**.
  Este concepto se aplica en el momento que una persona o grupo disfruta de una ventaja significativa de conocimiento sobre otra persona o grupo. Dentro de un dominio específico para el que se aplica este conocimiento.

- **Dominio tecnocrático.**
  Este hecho ocurre cuando una persona o grupo posee un alto nivel de conocimiento técnico y utiliza ese conocimiento para promulgar cambios en el comportamiento de los demás. Donde estos comportamientos colocan a los afectados en una posición de disminución del poder o autoridad en relación al primero, dentro del dominio afectado.

- **Reemplazo teológico**.
  El reemplazo teleológico sucede cuando una persona o grupo logra sustituir, en otro individuo o grupo, el propósito original u objetivo de su comportamiento con el del ingeniero social, a

> menudo a través de la alteración del comportamiento del objetivo en sí mismo.

Pero el cambio realmente importante en el término se produce con la entrada de la tecnología en el día a día, en 1984 el termino *social engineering* aparece en un artículo anónimo en una de las primeras revistas *hacker*, *2600: The Hacker Quarterly*. En ella su significado está relacionado con persuadir a alguien para que revele información. A partir de ese momento aparece en diversas publicaciones y post, pero el detalle fundamental es que el concepto de ingeniería social ya forma parte de la comunidad hacker.

2.2 Concepto básico

El concepto básico clave es la definición del propio termino de **Ingeniería Social**. Según el diccionario Oxford[5] el significado relacionado con la seguridad de la información es:

> El *uso del engaño para manipular a las personas para que divulguen información confidencial o personal que pueda usarse con fines fraudulentos.*

Otra posible definición, según la web especializada social-engineer.com[6] es:

> *Cualquier acto que influya en una persona para que realice una acción que puede o no ser lo mejor para sus intereses.*

Para esta segunda definición es importante destacar que la Ingeniería Social (IS) no siempre se usa de forma maliciosa, hay diversos usos como pueden ser comerciales y sociales sin una intención peyorativa para quien la recibe.

---

[5] https://en.oxforddictionaries.com/definition/social_engineering

[6] https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

Finalmente, se añade la definición del módulo 5 de la asignatura de *Vulnerabilidades de la seguridad*[7], el cual trata sobre la Ingeniería Social y la define de la forma siguiente:

> *En el contexto de la seguridad informática, nombraremos la ingeniería social 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.*

Las diferentes definiciones aquí presentadas aportan la necesidad de que la persona realice una acción de manipulación con tal de conseguir un interés, cuando esto se enfoca en la seguridad informática, se entiende que esa acción permitirá al ingeniero social obtener un resultado que, sin el previo trato con el individuo, sea presencial o telemáticamente, no hubiera podido obtener. En otras palabras, tal y como indica su nombre, uno de los pilares principales de la ingeniería social es la interacción con una persona.

2.3. Roles

Cuando se habla de ingenieros sociales, se suele asociar a hackers, pero la realidad es más compleja. Actualmente existen ingenieros sociales con roles muy diversos, a continuación, se comparten una representación de ellos según social-engineering.com[8]:

- **Hackers:** La ciberseguridad ayuda a crear cada día *software* más robusto y seguro, eso unido a que los programadores son más conscientes y proveen un *software* más seguro, ha provocado que

[7] Robles, Sergi y Castillo, Sergio. Ingenieria Social. Asignatura “Vulnerabilitats de la Seguretat” módulo 5(2011)

[8] https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/

los *hackers* busquen nuevas técnicas para lograr sus objetivos, a pequeña y gran escala, sin duda, una de las técnicas estrellas empleadas por estos, es la ingeniería social, combinada con sus conocimientos de *hacking.*

- **Probadores de seguridad:** Los probadores de seguridad utilizan las técnicas de los *hackers* para auditar los diferentes sistemas. Aún con los mismos conocimientos de los anteriores, siempre los usarán con fines positivos, esto hace que, en la actualidad, deban usar también métodos de ingeniería social, por el bien de sus clientes.

- **Espías:** Estos profesionales se dedican a obtener información confidencial de forma ilegítima con el uso de engaños, una de las descripciones de ingeniero social.

- **Ladrones de identidad:** En este grupo individuos que roban la información de identificación personal de otra persona y la utilizan para obtener ganancias financieras. Dentro de la información robada se puede encontrar el nombre, dirección, número seguridad social, número de identificación personal, etc.

- **Empleados descontentos:** Empleados enfadados o disgustados con su situación laboral, puede tener un problema con unos de sus superiores o bien con la misma empresa. Estos usuarios no acostumbran a compartir su enfado por miedo a perder su trabajo, pero al mismo tiempo su situación les facilita el realizar actos vandálicos o ilegales, sacando provecho de sus permisos dentro la empresa.

- **Corredores de datos:** Según la Comisión Federal de Comercio de Estados Unidos de América(FTC, por sus siglas en inglés) define a los corredores de datos como "*compañías que recopilan*

información personal sobre los consumidores y revenden o comparten esa información con otros", a parte añade que "*los corredores de datos usan estos datos reales y derivados para tres tipos de productos, principalmente, productos de marketing, productos de mitigación de riesgos y productos de búsqueda de personas".*[9]

- **Artistas del timo:** Los estafadores y timadores apelan a la avaricia de la gente, son capaces de crear situaciones que parecen "oportunidades" para sus víctimas, las cuales, han identificado como objetivos fáciles previamente.

- **Agentes de recursos humanos:** Estos profesionales cuentan con muchos recursos con tal de satisfacer las necesidades de la empresa obteniendo la mayor información posible de sus entrevistados, deben de ir más allá de obtener información, también deben ser capaces de comprobar si las motivaciones de la persona encajaran con su lugar de trabajo y el potencial de esta.

- **Vendedores:** El arte de vender requiere muchas técnicas diferentes como: recopilar datos, maniobras de obtención de información, la influencia, los principios psicológicos, etc. Para ello los vendedores deben usar todas estas habilidades para conseguir que aquello que venden cubra las necesidades del futuro cliente.

- **Gobiernos:** En algunos lugares se cita a los gobiernos como usuarios de técnicas de ingeniería social, sobre todo en el caso del uso de las PSYOPS.

[9] Federal Trade Commission, Data Brokers A Call for Transparency and Accountability, May 2014

- **La gente de cada día:** Las técnicas de ingeniería social son usadas por todo tipo de gente, desde profesionales con empleos respetables como médicos, abogados o psicólogos. Con el objetivo de obtener información con buenas intenciones, así como las usan los niños, familiares, amigos, etc. Cabe especificar que algunas de las técnicas que se usan no las conocen como tal, sino como conductas que con su uso obtienen el resultado esperado.

2.4. Ley y la Ingeniería Social

Cuando se habla de leyes e ingeniería social, uno de los debates más importantes es la dificultad de legislar a nivel territorial un hecho que con las facilidades de la comunicación actualmente se realiza a nivel internacional.

Una de las prácticas más conocidas a nivel de IS se trata del *phishing,* del cual se hablará en los siguientes capítulos, sobre el phishing ha habido diversos intentos de legislación en diversas partes del mundo, pero uno de los principales problemas es la dificultad la comentada anteriormente: ¿cómo legislar a nivel local un hecho en el que el ataque generalmente tiene origen internacional?

Si se focaliza dentro del ámbito español, si nos focalizamos en el artículo de Maria Victoria Rodriguez Caro[10] se dice que en el artículo 248 del Código Penal, tras la reforma introducida por la LO 5/2010:

> *"1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.*

[10] http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro."

En el art. 248.2 del CP, trata de proteger el patrimonio de los ataques que propician las nuevas tecnologías, en este caso el legislador las ha descrito como "manipulación informática o artificio semejante". Este segundo punto también evita que el engaño sea imprescindible, ya que según la STS 533/2007, de 12 de junio dice que "no es precisa la concurrencia de engaño alguno por el estafador, porque el acecho a patrimonios ajenos realizados mediante manipulaciones informáticas actúa con automatismo en perjuicio de tercero, precisamente porque existe la manipulación informática y por ello no se exige el engaño personal."

El problema reside en que el ataque consta del *phisher* (él atacante) que puede contar con la ayuda de una *cyber-mula*, en estos casos, cuenta el mismo artículo que se deberá observar los conocimientos del sujeto que actúa como tal para comprobar su punibilidad en el caso. Dentro de la ley, cuando hablamos de la víctima y de su obligación a la autoprotección, el artículo menciona que la *"STS nº 845 de 2-12-2014 rechaza que pueda culpabilizarse a la víctima ni oponerse un deber de autoprotección frente a un ataque fraudulento como el que representa la dinámica delictiva de este delito, pues fuera de los casos de engaño burdo, no existe ni está en el tipo de la estafa un elemento tal, ni ha de merecer este delito de estafa un inferior grado de protección que el resto de los delitos patrimoniales, estando presente en este caso la buena fe negocial que impregna y fundamenta el ordenamiento jurídico."*

Finalmente, para acabar este apartado hay que mencionar que en la actualidad se está trabajando sobre una nueva directiva europea sobre la lucha contra el fraude con medios de pago distintos del efectivo[11]. En la cual, uno de sus puntos es: *"Armonización de las definiciones de algunas infracciones penales en línea, como el pirateo informático del ordenador de la víctima o el phishing."*

3. Ataques conocidos de ingeniería social

En este capítulo se hará una introducción algunos de los ataques de ingeniería social más conocidos y frecuentes, así como se hará una breve revisión histórica sobre algunos de los ataques más famosos.

3.1. Estudio tipos de ataques

En este capítulo se van a describir algunos de los ataques más conocidos en la IS, como son los siguientes:

3.1.1. Recolección urbana

La recolección urbana, *trashing* o *dumpster diving* en inglés, consiste en buscar dentro de la basura información de cualquier tipo, la cual pueda ser valiosa para un futuro ataque.

Según, el ya desaparecido *LAN Times*[12] existen hasta 19 tipos de información valiosa que se puede recolectar usando esta técnica, aquí citamos unos cuantos:

- Guías telefónicas de la empresa
- Organigramas
- Manuales de políticas de la empresa

[11] https://www.consilium.europa.eu/es/press/press-releases/2018/03/09/fighting-fraud-with-non-cash-means-of-payment-council-agrees-its-position/

[12] https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

- Calendarios de reuniones
- Calendarios de eventos
- Calendarios de vacaciones
- Manuales del sistema
- Impresiones de datos confidenciales
- Impresiones de nombres y contraseñas de inicio de sesión
- Impresiones de código fuente
- CDs
- Dispositivos de almacenamiento
- Membrete de la empresa
- Formularios de notas
- *Hardware* obsoleto
- Facturas de servicios contratados

Esta información puede ser usada para suplantar una identidad, espionaje industrial o algunos servicios de seguridad e investigación privadas los usan para recopilar información de su objetivo.

3.1.2. Eavesdropping

Este ataque consiste en escuchar sin consentimiento una conversación para recopilar información. Existen diversos tipos desde escuchar una conversación de forma presencial, por teléfono (*wiretapping)* o datos a través de internet (*network sniffing).*

3.1.3. Piggybacking y tailgating

El *tailgating* consiste en obtener acceso no autorizado a un área restringida. Este ataque puede explotar costumbres sociales de “buena educación” como el hecho de “aguantar la puerta” o aprovechar la desinformación, por ejemplo, de un empleado que desconozca que un compañero ha sido despedido durante los días anteriores y por costumbre lo deje entrar con él.

3.1.4. Shoulder surfing

Esta técnica de observación directa se realiza en el momento que la víctima está tratando con una información privada y el atacante la intenta obtener de forma discreta aprovechando el descuido de la víctima o la facilidad de la situación. Algunos casos pueden ser la introducción del PIN en un cajero electrónico, leer conversaciones de teléfono móvil aprovechando la cercanía de los transportes públicos o la introducción de una contraseña en un ordenador.

El avance de la tecnología ha permitido que esta técnica sea cada día más fácil de realizar, a los ya existentes prismáticos, telescopios o cámaras fotográficas se han sumado aparatos como las minicámaras, los dispositivos móviles con un gran zum o los drones que permiten obtener la información de una forma aún más discreta.

3.1.5. Office Snooping

El *office snooping* es aprovechar el momento en que la víctima se ausenta de su lugar habitual para poder revisar toda aquella información que se pueda obtener.

El atacante puede aprovechar toda aquella información que la víctima ha dejado accesible por un exceso de confianza o por descuido, como puede ser una sesión de ordenador sin bloquear, información confidencial encima de la mesa, etc.

3.1.6. Baiting

El *baiting* utiliza la avaricia o curiosidad de la víctima para realizar el ataque. Desde un correo electrónico con un mensaje de “afortunado ganador” como el uso de un medio físico como puede ser un USB.
En el caso del USB o dispositivo físico, la víctima puede encontrar un dispositivo cerca de su sitio de trabajo y al abrirlo para conocer su origen o procedencia, activar algún tipo del *malware.*

3.1.7. Phishing

El *phishing* es un método utilizado mediante el uso de un correo electrónico, el cual, usando el engaño provoca que la víctima comparta su información privada con él atacante.

Este es uno de los ataques de ingeniería social más conocidos, usa las emociones o preocupaciones de la víctima, juntamente con un diseño cada vez mejor de un correo electrónico falso para conseguir su objetivo.

3.1.8. Vishing

El *vishing* se realiza de la misma forma que el *phishing*, pero en este caso el medio utilizado es la voz, habitualmente usando un sistema de telefonía tradicional, aunque en algunos casos se pueden usar servicios de VoIP.

3.1.9. SMiShing

El *SMiShing* es una variante del *phishing*, mediante el uso de mensajes de telefonía móvil, también conocidos como SMS (*short message service).*

3.1.10. Scareware

El *scareware* es un *software* de tipo malicioso, el cual se instala el ordenador y muestra una interfaz de antivirus que ha detectado algunas amenazas para el ordenador, ofreciendo una solución con su versión de pago.

En otras palabras, utiliza el miedo y el desconocimiento de los usuarios con tal de obtener un beneficio sin hacer nada a cambio.

3.1.11. Hoaxes

Un *hoax* es un tipo de correo electrónico que propaga una información o rumor completamente falso, con la intención de obligar al destinatario a compartirlo y reenviarlo por el bien de la comunidad.

3.1.12. Quid Pro Quo

En el caso del *quid pro quo* se ofrece un beneficio a cambio de información. En el caso más común de este ataque el atacante se hace pasar por personal de IT, solicitando ciertos datos confidenciales al usuario con motivo de solucionar un problema o facilitando cierto *malware* como si fuera una actualización de seguridad.

3.1.13. Pretexting

El *pretexting* se basa en una suplantación de identidad, que se puede realizar a nivel local o remoto. A través de este mecanismo se puede conseguir información confidencial de la víctima o de su empresa.

3.1.14. Ingeniería social inversa

La ingeniería social inversa consiste en el caso que el atacante utiliza una técnica pasiva para conseguir su objetivo.

El atacante estudia a su víctima, para seguidamente crear una trampa por el cual la victima sea quien activamente busca la ayuda o contactar con el atacante, a partir de esa situación el atacante usará todos aquellos métodos y técnicas que precise para llevar su ataque con el mayor éxito posible.

3.2. Resumen de historia de los ataques

En la historia se encuentran diversos tipos de ataques en diferentes épocas y usando diferentes técnicas, en este apartado se va a realizar un breve repaso de alguno de los más famosos.

3.2.1. El caballo de Troya

En la mitología griega Ulises conseguía vencer una guerra contra los troyanos la cual había durado diez años, mediante la utilización de un caballo enorme de madera, el cual repleto de soldados reposaba enfrente las puertas de Troya. Los troyanos introdujeron el caballo al interior de sus murallas por motivos supersticiosos, superando así aquellas barreras que habían conseguido evitar la entrada de los griegos y metiendo ellos mismos al enemigo sin ser conscientes de ellos. En otras palabras, es la descripción de un ataque de *baiting.*

3.2.2. Frank Abagnale, el falso piloto comercial

Frank Abagnale consiguió mediante el *pretexting* de ser un periodista de un periódico escolar, recolectar toda la información que necesitaba de la compañía *Pan Am*. Con ese conocimiento se hizo pasar por un piloto de *Pan Am*, de forma que obtuvo cheques de la compañía y vuelos gratis. Su historia se llevó al cine en la película “Atrápame, si puedes”.

3.2.3. Kevin Mitnick y el quid pro quo

Kevin Mitnick es uno de los más famosos ingenieros sociales de este siglo. A través del estudio previo conocía a sus víctimas y posteriormente, junto a sus conocimientos del ciberespacio, obtenía la información que necesitaba para realizar su siguiente paso. Explotaba las vulnerabilidades sociales de sus víctimas obteniendo máximo rendimiento. Entre sus crímenes se puede encontrar:

- Haber entrado ilegalmente a través de una línea telefónica al ordenador de la Fuerza Aérea de Colorado.
- Falsificar el balance general del *Securty Pacific Bank*
- Apoderarse de la *Digital Equipment Corporation*

3.2.4. El día que un tweet puso en riesgo la economía mundial

El 23 de abril de 2013, un grupo conocido como *The Syrian Electronic Army*, quien posteriormente reclamó la autoría del ataque, se hizo con el control de la cuenta oficial de *Twitter* de *Associated Press* mediante un correo electrónico de *phishing*.


Hello,

Please read the following article, it's very important :

http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/

[A different AP staffer]
Associated Press
San Diego
mobile [removed]

Ilustración 3. El email de phishing enviado

Con el control de esa cuenta público un *tweet* donde se afirmaba que había habido dos explosiones en la casa blanca y que Barack Obama se encontraba herido.

Ilustración 4. Tweet hackeado de AP

El mercado bursátil americano se desplomo temporalmente, seguidamente la Casa Blanca desmintió la noticia y la cuenta fue suspendida, hasta que la empresa original recuperó el control y el mercado se restableció.

Ilustración 5. El comportamiento del mercado económico el día del ataque

(Las imágenes han sido obtenidas del siguiente artículo[13])

4. Métodos y estrategias utilizados

En este capítulo se profundizará sobre las metodologías y estrategias más utilizadas, así como, en su funcionamiento, como se usan y que herramientas existen.

[13] https://opendatasecurity.io/the-most-famous-cases-of-social-engineering/

4.1. Métodos de recopilación de información

En el punto anterior se han explicado diversos tipos de ataques donde su función principal no es otra que obtener información para sacar un beneficio de esta. Estos ataques son descritos en punto 3.1. Estudio tipos de ataques, para ser precisos estamos hablando de:

- Recolección urbana
- *Eavesdropping*
- *Piggybacking y tailgating*
- *Shoulder surfing*
- *Office snooping*
- *Baiting*
- *Quid Pro Quo*

Es por ello por lo que en este punto se va a centrar en otras formas de obtener información, en concreto, en aquellas que intervienen las relaciones sociales.

El primer paso es entender que las estrategias que se van a comentar se basan en unas características que comparten la mayoría de los seres humanos en el mundo laboral:

- La cordialidad, especialmente con extraños.
- Parecer inteligente y bien formado.
- La gente no miente por mentir.
- Preocuparte por alguien genera amabilidad habitualmente como respuesta.
- Si elogias a la gente, acostumbra a hablar más.

Para ello el atacante debe tener una serie de cualidades:

- Debe ser natural. Cualquier incomodidad o nerviosismo le haría perder credibilidad.
- Estar formado en el campo en el que debe actuar.
    - No ser avaricioso, a veces el querer exprimir mucho una oportunidad puede conllevar el perder la oportunidad.

Una vez clarificados estos puntos, se pasan a describir diferentes formas de obtener información:

4.1.1. Apelar al ego de una persona

Está técnica muy utilizada en el mundo del marketing es un gran método para obtener información siempre y cuando, se realice con el tacto necesario, des de la sinceridad y sin exageración.

Consiste en realizar un halago a la persona de la cuál quieres obtener una información relevante y aprovechando tanto su modestia (o falsa modestia) como la aceptación de este, esperar que esta amplié la información y matice en aquellos aspectos que interesan al atacante.

4.1.2. Expresar interés mutuo

Esta otra estrategia consiste en compartir un interés con la victima ofreciéndole ayuda e información sobre un interés que ambas partes comparten, la victima muy probablemente exponga su estado actual en la materia, para orientar a la persona que, supuestamente, le quiere ayudar y facilitar su labor. Seguidamente el atacante compartirá aquella información que le interese obteniendo así un control total de la situación.

4.1.3. Hacer una afirmación falsa intencionadamente

El compartir un dato falso durante una charla en un lugar con expertos o trabajadores de la empresa que se quiere atacar, puede provocar la corrección por parte de una de las víctimas que de forma inconsciente expondrá datos reales que el atacante podrá obtener de forma sencilla.

4.1.4. Ofrecer información voluntariamente

Esta estrategia aprovecha el sentido de la obligación que sienten un gran número de personas, cuando en un evento social o situación de conversación, una persona empieza una conversación con una frase que comparte una información importante. Este hecho suele provocar que los participantes de la conversación se sientan obligados a compartir información de un nivel o trascendencia parecidos.

4.1.5. El conocimiento asumido

Esta estrategia se acostumbra a observar en conversaciones donde varios expertos de un tema están debatiendo e intercambiando datos de interés, entre ellos está el atacante, que durante la conversación se ve con la obligación de intervenir en algún momento para demostrar un nivel de conocimiento apto para poder seguir en la misma. En ese momento aprovechando la situación, si el atacante es capaz de compartir una opinión sólida e interesante, aunque esté basado en un conocimiento reducido, los demás integrantes le otorgaran un conocimiento mayor y seguirán compartiendo información importante como si el propio atacante ya la conociera.

4.1.6. Utilizar los efectos del alcohol

El alcohol tiene un efecto desinhibidor en las personas que los consumen, la estrategia de compartir una bebida alcohólica con cualquier excusa mientras que se trata una conversación puede producir que la víctima comparta información que, sin haber consumido ese alcohol, posiblemente no compartiría.

4.1.7. El arte de hacer preguntas

Finalmente, no podía faltar dentro de estas estrategias, el arte de hacer preguntas. Las preguntas oportunas en el momento indicado son posiblemente una de las mejores armas para obtener información. Los ingenieros sociales deben dominar esa capacidad, así como conocer los diferentes tipos de preguntas que existen y cuando usarlas.

4.2. Técnicas de suplantación

La suplantación o el *pretexting,* mencionado en el apartado 3.1.13. Pretexting, es una de las metodologías más importantes cuando se debe emplear la Ingeniería Social, para ello es muy importante seguir una serie de fases al momento de aplicarlo.

En primer lugar, existe una fase de investigación para conocer el máximo de detalles posibles de la víctima a suplantar. A continuación, otro detalle de suma importancia es que el atacante involucre sus intereses personales, eso dará más realidad a la suplantación y facilitara la parte de credibilidad. También se debe tener en cuenta la importancia de practicar dialectos o expresiones típicas de la víctima y de su forma de ser. Es muy importante que el pretexto parezca que surge de forma espontánea y que la simplicidad de este sea máxima, cuanto más simple mayor probabilidad de éxito.

De suplantaciones encontramos de tres tipos que se comentan a continuación:

4.2.1. Suplantación lógica

En este apartado podríamos destacar diferentes ataques del apartado 3, como podrían ser:

- 3.1.7. Phishing

- 3.1.8. Vishing
- 3.1.9. SMiShing

Estos tres ataques, de metodologías parecidas y medios diferentes, tratan de engañar a las víctimas a través de formas telemáticas, como pueden ser correo electrónico, teléfono o mensaje de texto (SMS).

4.2.2. Suplantación física

La suplantación física, concretamente, la personificación es el arte de hacerse pasar por otra persona. Se basa en el estudio previo de la persona, de sus rutinas, su modo de hablar y su forma de interactuar con los demás para poder sustituirlo en una situación cualquiera explotando al máximo la situación.

Esta técnica según una infografía de Social Engineering[14] del año 2014 era una de las más usadas, las personas suplantadas tenían una edad media de 41.7 años y la cantidad de dinero perdida se estimaba en 4.187 $ por ataque.

4.2.3. Suplantación digital

La identidad digital cada vez tiene un peso más importante en el día a día. Esta permite realizar trámites legales e interacciones sociales a través de la pantalla de los diferentes dispositivos. Es por ello, por lo que las redes sociales permiten a los atacantes tener la opción de suplantar la persona real de una forma relativamente sencilla, pues los diferentes usuarios creen en las medidas de seguridad que protegen esas cuentas. Mediante esta suplantación el usuario puede recopilar información de sus víctimas, de todas aquellas personas que han interactuado o interactúan con ellas y hasta puede cambiar su imagen digital y sus

[14] https://www.social-engineer.org/social-engineering/social-engineering-infographic/

relaciones con los otros a través de esas interacciones. Definitivamente un riesgo muy alto que a veces protegen contraseñas poco seguras.

4.3. Psicología en Ingeniería Social

Hasta el momento los diferentes casos y situaciones que se han expuesto en capítulos anteriores incluyen en gran parte metodologías que utilizan conocimientos de psicología que explotan características que tienen la mayoría de las personas como pueden ser la curiosidad o el miedo. Pero en este capítulo se van a tratar algunos aspectos en concreto que permiten conseguir ventajas a los ingenieros sociales

4.3.1. PNL

La programación Neurolingüística se basa en una serie de estrategias que tratan de identificar y aprovechar modelos de pensamiento que actúan directamente sobre el comportamiento de una persona al momento de tomar decisiones.

La PNL fue creada por el matemático Richard Badler y el lingüista John Grinder en los años 70, que buscaban crear un modelo formal y coherente del funcionamiento de la mente humana, a partir de una recopilación de estudios, investigaciones y técnicas.

Para ello se basaron en 3 aspectos relacionados con la forma que tienen las personas de interactuar con su entorno. Una vez se detecta cuál es el aspecto dominante de la persona, esto permite interactuar con ella de una forma más fácil, pues si el atacante es capaz de detectar cuál de los 3 aspectos es más dominante en la víctima, podrá encontrar la forma de que su mensaje sea mejor interpretado por la misma. Entonces se puede clasificar a las personas en 3 tipos según su aspecto dominante:

- **Visuales:** Son aquellas personas que experimentan el mundo principalmente a través del sentido de la vista. Dan un peso mayor a la parte visual de la comunicación, acostumbran a ser

locuaces y pensamiento rápido. Prefieren las imágenes y usan expresiones como “lo veo” o “punto de vista”.

- **Auditivas:** En este caso, son las personas que experimentan lo que acontece en el mundo exterior a través del sentido de la oída. Por ese motivo procesan la información de forma secuencial, de forma más ordenada y pausada. Utilizan expresiones como “Escúchame” o “poner el acento”.

- **Kinestésicas:** Las personas kinestésicas dan una mayor importancia a la interacción física, es decir al contacto. Gestos como dar una palmada en la espalda o un abrazo son muy comunes. Es por ello por lo que utilizan expresiones como “tener la piel de gallina” o los “poner los pelos de punta”.

Pero la PNL incluye otras estrategias que pueden resultar sumamente interesantes como puede ser el efecto espejo. El efecto espejo se basa en las “neuronas espejo”, que tienden a imitar a la persona que se está observando, repitiendo la acción del otro, estás neuronas también están presentes en los animales. Aprovechando este fenómeno y aunque es un tema de debate en la comunidad científica, parece ser que estás neuronas también afectan en la empatía de las personas, siendo así que el imitar de forma no exagerada comportamientos de la otra persona, como pueden ser expresiones, la forma de expresarse o el lenguaje corporal permiten empatizar de forma más fácil con el interlocutor.

Aunque la PNL sigue siendo discutida por grandes expertos, se usa cada vez más de forma habitual por psicólogos, coach o vendedores entre otras profesiones. Para un buen ingeniero social podrían resultar de gran utilidad los conocimientos en esta materia.

4.3.2. Principios básicos de la ingeniería social

Estos principios básicos son sumamente parecidos a los usados en las ventas y son usados para ganar la confianza y así poder engañar a una posible víctima. Fueron escritos por el psicólogo y escritor estadounidense Robert Cialdini, quien escribió en *1984 Influence: The Psychology of Persuasion* ("Influencia: la psicología de la persuasión"). Se pueden resumir en seis:

- **Aprobación social:** Los seres humanos son seres sociales que por lo tanto buscan la aprobación del colectivo, también denominado "seguir el rebaño" establece que se tiende a acomodar una opinión a lo que opine la mayoría. Es por ello por lo que algunas campañas de marketing utilizan expresiones como "el más vendido del mundo". Si un atacante vendiera un *software* malicioso basándose en que es básico y que las grandes empresas ya lo usan, podría ser que la víctima lo instalase más fácilmente.

- **Autoridad:** Según Cialdini los seres humanos están más predispuestos a dejarnos influenciar cuando somos interpelados por una autoridad. Ya que una persona con autoridad tiende a tener más conocimiento y/o experiencia, por tanto, mayor derecho a opinar. Es por ello por lo que las técnicas con el *phishing* tienden a tener más éxito cuando se hacen pasar por un entidad o persona con cierta ascendencia sobre la víctima.

- **Consistencia:** Las personas tienden a tener la necesidad de mantener su palabra o cumplir sus compromisos. Si el atacante consigue que la víctima crea que ha adquirido un compromiso, será más sencillo que pueda conseguir su objetivo.

- **Escasez:** Esta técnica se observa fácilmente en momentos de rebajas o descuentos cuando se adhieren contadores a las ofertas.

Los seres humanos tienden a estar más receptivos o cercanos a un objetivo si este es escaso o difícil de conseguir.

- **Reciprocidad:** Las personas acostumbran a tratar a sus semejantes de la misma forma en que son tratadas. Esto permite a los atacantes crear perfiles, normalmente falsos, para atraer a las víctimas y obtener una información privilegiada aprovechando el principio de reciprocidad.

- **Simpatía:** Robert Cialdini, psicólogo y escritor estadounidense, explicaba que "El principio de simpatía, también traducido como de afición, gusto o atracción, nos señala algo que a primera vista puede parecer simple: estamos más predispuestos a dejarnos influir por personas que nos agradan, y menos por personas que nos producen rechazo." Es por ello por lo que los ingenieros sociales realizan perfiles de sus víctimas y tratan de compartir gustos para conseguir de forma inconsciente de la víctima, una situación de ventaja.

4.3.3. PSYOPS

Las operaciones psicológicas, popularmente conocidas como PSYOPs, son las operaciones planificadas para transmitir información e indicios a ciertas audiencias selectas para influir sobre sus emociones, motivos, el razonamiento objetivo, y finalmente sobre el comportamiento de gobiernos, organizaciones, grupos e individuos.[15]

Estas operaciones han sido usadas por diversas entidades militares durante conflictos bélicos con diferentes materiales como podrían ser folletos, mensajes de audio o similares. En los últimos años han visto un gran incremento de potencial en el momento que estás se han unido a la potencia de comunicación que ofrece la sociedad actual.

[15] http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2001/2trimes01/goldstein.htm

La conectividad presente hoy en día, mediante redes sociales y sistemas de comunicación ha permitido alcanzar a este tipo de operaciones una facilidad y potencia enorme, de tal forma, que un ataque orquestado multipunto puede obtener resultados sorprendentes.

Es por ese motivo, que estás operaciones son una metodología o estrategia muy útil de aplicar en ingeniería social, no posiblemente para un ataque contra una persona en concreta, pero si para una macroperación con algún objetivo muy concreto.

5. Herramientas Ingeniería Social

En la ingeniería social a parte de las diferentes metodologías y técnicas, hay una serie de complementos, programas y diferentes objetos que facilitan la realización de estas, estas son conocidas como herramientas y como se observara a continuación, tenemos de diferentes tipos y funciones.

5.1. Herramientas físicas

5.1.1. Herramientas para abrir cerrojos

Una de las claves de la ingeniería social es acceder a información confidencial, habitualmente protegida de manera digital y en otras ocasiones con dispositivos físicos como pueden ser candados o cerraduras. Es por ese hecho que se presentan una serie de herramientas que juntamente con su técnica correspondiente permiten superar estos obstáculos.

- **Ganzúas**

  Según la RAE una ganzúa es *un alambre fuerte y doblado por una punta, a modo de garfio, con que, a falta de llave, pueden correrse los pestillos de las cerraduras*.[16] Estos

[16] http://dle.rae.es/srv/search?m=30&w=ganz%C3%BAa

utensilios que se usan para abrir cerraduras y permitir acceso aquello que estás protegen. Existen muchos tutoriales[17] y cursos para aprender a utilizar las ganzúas, así como, cerraduras de vidrio para facilitar el uso y práctica.

Ilustración 6. Juego de ganzúas y 2 cerraduras transparentes para practicar.[18]

- **Cuchillo *shove***

  El cuchillo *shove* es uno de los medios más rápidos para abrir puertas de casas y/o oficinas que utilizan una cerradura de pestillo en el pomo. Está herramienta se usa principalmente por los bomberos para abrir puertas en situaciones de emergencia, su forma permite introducir el cuchillo por cualquiera de los dos lados de la puerta, se introduce a la altura del pestillo y tirando hacia al lado oportuno hace ceder el pestillo y permite abrir la puerta.

[17] https://www.ganzuas24.com/manual-de-uso-de-las-ganzuas/

[18]https://amzn.to/2SleFWc1

Ilustración 7. Cuchillo shove[19]

- **Llaves *bumping***

  Las llaves *bumping* son unas llaves diseñadas para abrir cerraduras sin la necesidad de la llave de la cerradura. La llave *bumping* se introduce en la cerradura y mediante un golpe esta se adapta al diseño de la cerradura permitiéndole abrir la puerta sin forzarla. Está técnica es comúnmente usada por los cerrajeros, aunque recientemente han aumentado los robos de viviendas usando estás llaves.

5.1.2. Dispositivos de grabación

En la actualidad, los dispositivos de grabación están por todas partes, desde todas las áreas videovigiladas, así como las cámaras o micrófonos de los móviles, las webcams de las *tablets,* pantallas o portátiles. Punto y aparte son las cámaras y micrófonos de espionaje, las cuales normalmente restan camufladas dentro de algún objeto que a simple vista parece inofensivo. En este punto vamos a profundizar en cada uno de ellos.

- **Webcams de videovigilancia**

  Estos aparatos cuya función principal es proteger aquello que están grabando para evitar que los delincuentes

[19] https://bit.ly/2E3TCEw

actúen de forma no deseada, mal configurados pueden ser usados en nuestra contra. Actualmente existen páginas web[20], las cuales permiten acceder aquellas webcams IP que no tienen contraseña propia, mostrando toda la información que estas pueden revelar. Desde el funcionamiento de un lugar de trabajo, hasta los clientes de un establecimiento.

- **Webcams portátiles y *tablets***

  Estos aparatos tan habituales en el día a día que forman parte de los dispositivos con los que interactúan diariamente millones de usuarios y cuya utilidad en muchos casos parece que es escasa. Son uno de los puntos que hacen más vulnerables a los usuarios, pues con diversos *malwares* o negligencias de los usuarios se puede acceder de forma remota a ellas y ese hecho permite que un atacante acceda a una visión privilegiada de un usuario en cualquier momento si este no ha tomado las medidas necesarias.

- **Smartphones**

  Estos dispositivos cada día tienen características más potentes, des de mejores cámaras como mejor grabación de voz, esto los vuelve unos dispositivos muy útiles al momento de obtener información privilegiada de las víctimas. Se puede grabar una conversación mientras se finge que se está usando el teléfono o, por ejemplo, se puede grabar a distancia una persona introduciendo una

[20] Un ejemplo de esas webs seria www.insecam.org, durante la realización de este proyecto se localizó a uno de los negocios afectados, comunicándose previamente con él por teléfono y posteriormente por correo electrónico (ver anexos) para que pudiera poner solución a la situación y así lo hizo.

contraseña en cualquier dispositivo, para utilizarla luego con la intención deseada.

- **Dispositivos de espionaje**

  Actualmente se pueden comprar en Internet una gran diversidad de objetos cotidianos que permiten obtener grabaciones de audio y video *on-line* de forma completamente discreta. Estos dispositivos pueden guardar la información o compartirla mediante Wi-Fi siendo usados para obtener información de forma secreta. Existen toda clase de objetos que permiten estas prácticas: relojes de pared, peluches, bolígrafos, marcos de fotos etc.

Ilustración 8. Reloj espía vendido online[21]

5.1.3. GPS

Durante la recopilación de información de una posible víctima, sus movimientos pueden ser determinantes para poder usar diferentes ataques con ella, des de un ataque de pretexto o realizar un *tailgating*. Para ello se puede utilizar un dispositivo GPS, tanto sobre la misma persona, una de sus pertinencias o su

vehículo. El dispositivo emite una señal continua la cual permite en tiempo real conocer la posición de la víctima, así como ir monitorizando todos sus movimientos para tener un estudio y así poder sacar ventaja.

5.2. Herramientas software

5.2.1. Métodos para descifrar contraseñas

Una de las partes claves de los ingenieros sociales es obtener información confidencial de sus víctimas, esta información suele estar protegida de diversas formas, una de las más comunes son las contraseñas.

Existen diferentes herramientas para descifrar contraseñas, a continuación, se nombran unas cuantas:

- ***John the Ripper***[22]

  John the Ripper es una aplicación de *software* libre y código abierto para desencriptar contraseñas por fuerza bruta, para ello utiliza un diccionario de contraseñas, el cual se puede descargar por Internet o aprovechar el que incluye la propia aplicación.

  Para poder desencriptar la contraseña necesita que las diferentes partes de la contraseña pertenezcan al diccionario y para ello explota que gran parte de las contraseñas comparten una serie de palabras y características similares.

- ***OphCrack***[23]

---

[21] https://spyassociates.com/wall-clock-hidden-camera-w-dvr-wifi-remote-view/

[22] https://www.openwall.com/john/

[23] http://ophcrack.sourceforge.net/

Orphcrack es una herramienta gratuita utilizada para crackear contraseñas de *Windows* usando *Rainbow tables*. Es una gran implementación del método *Rainbow tables* ya que está hecho por los inventores de este. *Orphcrack* viene con una GUI y funciona en múltiples plataformas.

- ***AirCrack NG***[24]

  AirCrack-ng es un kit completo de herramientas para conseguir acceso a redes WiFi con seguridad. Este se enfoca en cuatro áreas, el monitoreo de la red para capturar paquetes, ataque a base de inyección de paquetes, el testeo de la red y la parte final del crackeo para obtener la contraseña de acceso.

5.2.2. Software para ingenieros sociales

Anteriormente se han descrito muchos ataques, métodos de obtener información y hasta herramientas físicas, pero en el mundo de la ingeniería social actualmente existe una gran cantidad de *software* que permite realizar ataques o facilitar la realización de estos, a continuación, se exponen algunas de las herramientas más destacadas en ese sentido.

- ***Maltego***[25]

  Maltego es una herramienta desarrollada por la compañía Paterva que recopila información y la muestra en forma de grafos, se complementa con diferentes *transforms*, unas aplicaciones externas, que aumentan notablemente su potencial. Permite crear entidades propias, a parte de las que genera, para poder crear y recopilar toda la información en un mismo lugar.

---

[24] https://www.aircrack-ng.org/

[25] https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php

Es una herramienta ideal para recopilar toda aquella información accesible, el cual combina diferentes tipos de búsqueda y la interacción con redes sociales. Existen diferentes versiones del producto desde versiones gratuitas a las versiones más potentes de pago.

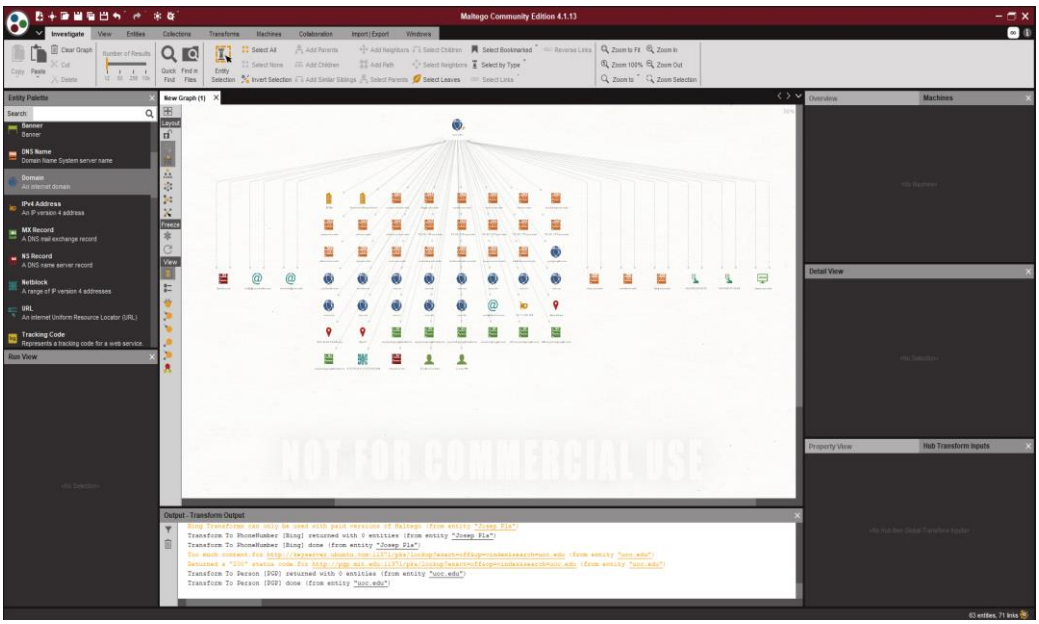


Ilustración 9. Ejemplo de la información obtenida con Maltego de uoc.edu

- ***SET***[26]

  SET también conocido como *Social-Engineer Toolkit* es una *suite* de herramientas para la realización de ingeniería social. SET es un framework de código abierto diseñado para realizar ataques avanzados contra el elemento humano.

  SET es multiplataforma y permite realizar de forma relativamente sencilla los siguientes ataques:

  - Ataques *Phishing*
  - *Website attacks*
  - Generador de medios infectados
  - Generador de *Payload and Listener*

- Ataques masivos de correos electrónicos
- Ataques basados en Arduino
- Ataques SMiShing
- Ataques contra puntos de acceso *Wireless*
- Generador de QR para ataques
- Ataques PoweShell

Estos ataques entre otros módulos hacen de esta herramienta posiblemente una de las más potentes, completas e interesantes al momento de realizar ingeniería social. Esto la convierte en una de las herramientas más utilizadas para realizar auditorías de este tipo.

- ***FOCA***[27]

  Fingerprinting Organizations with Collected Archives es, según la página web referenciada anteriormente, una herramienta utilizada para encontrar metadatos e información oculta en los documentos que examina. Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar.

  Los documentos que es capaz de analizar son muy variados, siendo los más comunes los archivos de Microsoft Office, Open Office, o ficheros PDF, aunque también analiza ficheros de Adobe InDesign, o svg por ejemplo.

  Estos documentos se buscan utilizando tres posibles buscadores que son Google, Bing y DuckDuckGo. La suma de los tres buscadores hace que se consigan un gran número de documentos. También existe la posibilidad de

[26] https://github.com/trustedsec/social-engineer-toolkit

[27] https://www.elevenpaths.com/es/labstools/foca-2/index.html

añadir ficheros locales para extraer la información EXIF de archivos gráficos, y antes incluso de descargar el fichero se ha realizado un análisis completo de la información descubierta a través de la URL.

Con todos los datos extraídos de todos los ficheros, FOCA va a unir la información, tratando de reconocer qué documentos han sido creados desde el mismo equipo, y qué servidores y clientes se pueden inferir de ellos. Permitiendo recopilar una gran cantidad de información, que puede ser usada posteriormente.

5.2.3. Uso herramientas Internet

De igual forma que en el apartado interior, se podrían destacar una serie de herramientas que se pueden encontrar *online*, pero entre todas ellas hay una, que por su cotidianidad y su frecuente uso destaca en este proyecto, estamos hablando de:

- ***Google Dorks***

  Google Dorks son las búsquedas avanzadas que se pueden realizar mediante el famoso buscador *Google* que permiten obtener resultados sorprendentes por malas configuraciones o poco seguras de los diferentes *websites.*

  Estás búsquedas consisten en búsquedas estructuradas que encuentran resultados que en las búsquedas habituales no se encontrarían.

  En la *Google Hacking-Database*[28] podemos encontrar miles de estas combinaciones, para probarlas y poder comprobar así sus resultados.

[28] https://www.exploit-db.com/google-hacking-database

6. Diseño de un ataque de Ingeniera Social

Durante este proyecto se han visto diferentes metodologías y formas de usar la ingeniería social. En este capítulo se va a desarrollar un ataque contra una empresa ficticia, desde la selección de un objetivo el estudio de sus vulnerabilidades hasta la simulación de ataque final. Todo el contenido de este capítulo es pura ficción.

6.1. Selección objetivo

La empresa escogida para este ataque es la empresa ficticia encargada de la recogida y destrucción de material confidencial de otras empresas.

El jefe de seguridad de esta ha solicitado una auditoria frente a un ataque de ingeniería social ya que un error en su seguridad permitiría a los atacantes obtener información privilegiada de sus clientes, entre los cuáles se encuentran algunas empresas tecnológicas de gran potencial, así como sucursales de entidades bancarias. Este hecho sería el fin del negocio de la empresa.

6.2. Recopilación de información

El primer paso es recolectar información de la empresa objetivo. Tienen una página web actualizada en la cual se puede encontrar mucha información sobre la misma, a parte de la dirección de contacto de la empresa, su correo electrónico y su teléfono, también se pueden ver publicados algunos de sus clientes más importantes. Tienen un apartado de personal donde se encuentran los nombres de los responsables de cada departamento, con un pequeño texto debajo con algún mensaje motivacional respecto a los valores de la empresa.

Toda la información se guarda en un proyecto creado en un sistema con un editor de notas que permita el acceso privado y remoto a toda la información recopilada, seguidamente con se usa el *software* Maltego, explicado anteriormente en el punto 5.2.2 Software para ingenieros sociales. Con Maltego y la información recopilada en la página web y en las diferentes redes sociales se obtiene información relevante sobre la empresa, como sería la dirección de su servidor de correo electrónico, los diferentes contactos de los empleados y otras empresas con las que tienen relación.

A partir de esta información se elaboran perfiles de los diferentes trabajadores de la empresa, se recoge la información de sus perfiles sociales, sus estudios y conocimientos obtenidos de redes como Linkedin, contactos, gustos, etc. Con esos perfiles se puede observar en cada usuario a qué tipo de ataque es más vulnerable, cuáles son sus características predominantes y cuales podrían ser sus puntos débiles.

A continuación, se desarrolla toda la información de la empresa, los correos electrónicos recogidos de los empleados, teléfonos de contacto y diferentes enlaces de la web.

Seguidamente se pasa a una vigilancia directa, se sitúa una webcam camuflada que emita online y se recoge toda la información de entrada y salida de las diferentes furgonetas, así como de los empleados. Con este fin se creará el pretexto de una empresa de mantenimiento de superficies urbanas, aprovechando el discutible estado de las carreteras del polígono, para que fingiendo un trabajo puntual puedan instalar y recoger la webcam sin llamar la atención de los empleados.

Con la intención de conocer cómo se ordenan las diferentes naves de la empresa y el recorrido de los empleados y las furgonetas se utilizará un dron con una cámara de gran alcance y se monitorizará el funcionamiento interno.

Finalmente, se tratará de situar diversos dispositivos de rastreo GPS en diversas furgonetas para conocer su ruta y los clientes con los que trabaja. Para esta fase se aprovechará el estudio previo de información para saber en qué taller y cada cuanto se revisan las furgonetas. Probablemente, estas tengan un tiempo de espera sin vigilancia en el taller pues no contienen nada de valor durante su revisión y puesta a punto, con unos conocimientos básicos se creará un pretexto de relación con el propietario del taller, para en una de esas revisiones, aprovechando un ataque de *office snooping* instalar los GPS en las furgonetas.

Una vez finalizado el estudio, con toda la información anotada se pasa a la fase de diseño del ataque.

6.3. Diseño del ataque

Con toda la fase de estudio realizada y la información recopilada se utiliza la herramienta SET, explicada en el apartado explicado anteriormente en el punto 5.2.2 Software para ingenieros sociales.

Se iniciará con esa herramienta una serie de ataques contra los diferentes trabajadores con tal de obtener sus credenciales. Con la información recogida en los perfiles se decide que ataque tiene más posibilidades para cada trabajador. Por las redes sociales, se observa que el trabajador con más relación con los compañeros a través de estas es el recepcionista. Para él se usará un doble ataque, por un lado, se creará un pretexto de representante de un cliente interesado en sus servicios, para recopilar la máxima información posible sobre la empresa.

Esta parte del ataque es muy importante aprovechar los gustos del recepcionista para crear una relación personal con él e ir recogiendo toda la información necesaria sobre los diferentes departamentos de la empresa. Por ejemplo, si se verifica que el departamento comercial y el

de IT no tienen una relación fluida, como se ha observado en las imágenes recogidas con las diferentes webcams, ya que trabajan en naves diferentes, comen a diferentes horas y no tienen relación en las redes sociales. Se realizará un ataque de phishing a los comerciales.

De la misma forma, si se verifica que cada transportista tiene un teléfono móvil de empresa, se tratará de obtener esta información una vez se acceda al sistema, mediante el ataque de phishing o el ataque de baiting que se realizará en la recepción. Si se consigue realizar con efectividad uno de esos ataques se realizaría uno de SMiShing contra los conductores.

Mientras que estos ataques dan acceso a la parte tecnológica de la empresa, se usará el conocimiento adquirido en la fase de estudio como son las empresas con las que trabajan, gracias a la información recogida por los GPS, los teléfonos internos de los diferentes departamentos y nombres de los trabajadores, se complementara usando un ataque de recolección urbana en los contenedores de la empresa, buscando todos aquellos detalles como pueden ser contraseñas apuntadas en post it, facturas de proveedores o cualquier otro tipo de documento relevante.

Finalmente, para el desarrollo del ataque es muy importante escoger el momento oportuno para llevar a cabo cada uno de los pasos, saber planificar puede ser clave en un proyecto de esta envergadura. Por ejemplo, si por la información recopilada se observa que el recepcionista es un apasionado de la navidad, la época navideña, empezando a finales de noviembre, sería un buen momento para ganarse su confianza.

6.4. Análisis resultados

Se recogerá la información de cada parte del ataque y así se sabrá hasta qué punto es vulnerable la empresa. Con esa información se realizará el resultado del análisis y se facilitará toda la información a la

empresa contratante, así como las imágenes y muestras obtenidas en la auditoria para facilitar un mejor aprendizaje de los errores y una nueva puesta a punto de la seguridad en frente una amenaza de ingeniería social.

En este ataque se aplican las siguientes técnicas:

- *Phishing* contra los comerciales.
- *SMiShing* contra los conductores.
- Recolección urbana.
- *Baiting* en la recepción con un USB infectado.
- GPS en las camionetas.
- Vigilancia con webcam.
- *Pretexting*, para instalar la webcam.
- *Pretexting*, para entrar en las oficinas, mantener una conversación con la recepcionista mientras se realiza la primera fase del ataque de *baiting*.
- *Pretexting* para instalar los dispositivos GPS en las furgonetas, por ejemplo, buscando la información de revisión de estas.
- *Office Snooping* en el taller mecánico.

7. Métodos de prevención

En todas las metodologías explicadas en los capítulos anteriores hay una serie de puntos en común, principalmente el desconocimiento de la víctima o el conocimiento del atacante son los puntos clave. En la actualidad se realizan muchos ataques de ingeniería social, aunque en la mayoría de los casos se realizan de forma masiva y sin el detalle y la especificación necesarios para llevar el ataque al éxito. Un buen ataque perfectamente diseñado, puede ser realmente difícil de detener, pero sí que es muy importante tener una serie de ideas claras que lo pueden dificultar.

7.1. Consejos útiles

Según el artículo publicado en página web de INCIBE[29] hay una serie de consejos que son útiles en la mayoría de los casos, como son:

- No abrir correos de usuarios desconocidos o que no hayas solicitado: elimínalos directamente.
- No contestar en ningún caso a los mensajes sospechosos.
- Tener precaución al seguir enlaces en correos electrónicos, SMS, mensajes en Whatsapp o redes sociales, aunque sean de contactos conocidos.
- Tener precaución al descargar ficheros adjuntos de correos, en SMS, mensajes en Whatsapp o en redes sociales, aunque sean de contactos conocidos.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus comprobar que está activo.
- Verificar la seguridad de las páginas web donde introducimos datos personales. Deben utilizar certificado de seguridad y utilizar el protocolo HTTPS.
- Verificar la seguridad de las redes wifi públicas a las que nos conectamos. En caso de dudas, no compartir información confidencial ni introducir credenciales de usuario o contraseñas que puedan ser robados.
- Escribir las URL manualmente, en vez de usar los enlaces de los mensajes sospechosos.

A estos buenos consejos, es importante añadir:

- No abrir ningún archivo o dispositivo de almacenaje del cual se desconozca su procedencia.

[29] https://www.incibe.es/en/node/4909

- Antes de compartir cualquier información personal ser consciente de quien nos la está pidiendo y comprobar por métodos seguros que es real.
- Conocer la política de privacidad de la empresa y saber que datos está obligado a compartir y con quién.
- Ante la duda, pedir más tiempo o excusarse hasta que pueda estar seguro de la información que va a revelar.
- Si tiene cualquier sospecha o cree que ha cometido algún error, informar a su responsable de seguridad.

Finalmente, hay que añadir que lo más importante es la concienciación y la formación de la plantilla, solo un equipo bien preparado e informado puede hacer frente a amenazas de este tipo, cada vez más comunes y peligrosas.

8. Conclusiones

La ingeniería social convierte al usuario de una tecnología en el objetivo, en la potencial víctima. Es así como el usuario pasa a ser el eslabón más débil de la ciberseguridad en cualquier situación.

Esta antigua técnica no solo ha sabido adaptarse a las nuevas tecnologías y formas de comunicación, sino que ha ido evolucionando de manera continua, aprovechando estos cambios. Los diferentes ataques han sacado ventaja de la introducción del correo electrónico, las páginas web, los SMS o el VoIP entre otros.

La disrupción de los avances tecnológicos también ha facilitado diferentes técnicas y ha creado de nuevas, los dispositivos móviles con cámaras más potentes, buenas grabadoras o los dispositivos GPS son algunos ejemplos de ello.

A todo esto, hay que añadir el conocimiento y mejora de las técnicas de persuasión, de la comunicación no verbal o del estudio de la psicología

entre otras, permiten explotar vulnerabilidades que tienen la mayoría de las personas y que no son conscientes de ello.

Todo ello, unido al rápido crecimiento del uso de la identidad digital y de las redes sociales, hacen de vital importancia el conocimiento y formación en la prevención de esta técnica. Los usuarios deben conocer las metodologías que se pueden usar contra ellos, tener una guía de buenas prácticas y/o conocer las normas sobre la protección de la información en su lugar de trabajo, por ejemplo.

Así como, un buen uso de las herramientas ya existentes, con tal de poder auditar los diferentes lugares de trabajo, para mantener a los usuarios atentos y preparados en un mundo de constante cambio.

Para finalizar, hay que comentar que es probable que una mejor y más actualizada legislación, pueda facilitar esta labor.

A nivel de objetivos, este trabajo tenía la intención de dar a conocer, concienciar y proteger a los usuarios de esta técnica, a través de los objetivos establecidos en los diferentes capítulos. En este punto cabe destacar que en la parte relacionada con proteger a los usuarios no ha sido posible desarrollarla de la forma deseada. Este hecho está fuertemente ligado a la extensión de explicación de las diversas técnicas, los diferentes ataques y herramientas, ya que con la intención de profundizar al máximo posible en aquello que serían amenazas o peligros para los usuarios, la planificación no se pudo cumplir como se había previsto.

Siendo consciente de la situación, se tomó la decisión de profundizar más como se ha comentado anteriormente por un motivo, sólo conociendo el mayor rango de técnicas, ataques y herramientas, se podrían crear unas medidas preventivas lo más efectivas posibles.

Después de repasar detenidamente el trabajo, se puede deducir que en la fase de planificación no se valoró adecuadamente la cantidad de información que existiría en esos puntos, y más, cuando esta sería necesaria para realizar el simulacro de ataque. Posiblemente eso fuera debido a la poca experiencia previa antes de la realización del trabajo sobre la materia.

Finalmente, en una futura línea de trabajo, se profundizaría en las técnicas y se crearía un protocolo estándar para poder realizar una auditoria los más amplia posible en frente los diferentes ataques, así como se estudiarían que medidas preventivas son las más efectivas para cada uno de ellos y que patrones existen en común.

9. Glosario

9.1. Términos

Baiting: Azuzar, cebar, hostigar. Técnica de IS.

Hacker: Pirata informático y/o persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora.

Hardware: Voz inglesa que se usa, en informática, para designar el conjunto de los componentes que integran la parte material de una computadora u ordenador.

Malware: Programa informático o virus específicamente diseñado para perturbar o dañar un sistema.

Payload: Es la carga dañina de un virus o ataque, es decir, la parte que realiza la acción maliciosa**.**

Pretexting: El acto de la creación y utilización de un escenario inventado (el pretexto) para acoplarse a una víctima específica de

manera que aumenta la posibilidad de que la víctima divulgar información o realizar acciones que serían poco probables en circunstancias normales.

Software: Voz inglesa que se usa, en informática, con el sentido de 'conjunto de programas, instrucciones y reglas para ejecutar ciertas tareas en una computadora u ordenador'.

USB: Dispositivo de almacenamiento con conexión USB.

Zum: Adaptación gráfica de la voz inglesa zoom, 'teleobjetivo especial, cuyo avance o retroceso permite acercar o alejar la imagen'.

9.2. Siglas

CD: *Compact Disc*
GPS: *Global Positioning System*
IS: Ingeniería Social
IT: *Information Technology*
PIN: *Personal Identification Number*
PNL: Programación Neuro-Lingüística
SMS: *Short Message Service*
STS: Sentencia Tribunal Supremo

10. Bibliografía

1. https://www.kaspersky.es/blog/ingenieria-social-hackeando-a-personas/2066/ [Visitada el 30/12/18]
2. 2018 Data Breach Investigations Report, Verizon, 2018
3. 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute and IBM, July 2018
4. Joseph M. Hatfield, Social engineering in cybersecurity: the evolution of a concept, Computers & Security (2017)
5. https://en.oxforddictionaries.com/definition/social_engineering [Visitada el 30/12/18]

6. https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/ [Visitada el 30/12/18]
7. Robles, Sergi y Castillo, Sergio. Ingenieria Social. Asignatura “Vulnerabilitats de la Seguretat” módulo 5(2011)
8. https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/ [Visitada el 30/12/18]
9. Federal Trade Commission, Data Brokers A Call for Transparency and Accountability, May 2014
10. http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/ [Visitada el 30/12/18]
11. https://www.consilium.europa.eu/es/press/press-releases/2018/03/09/fighting-fraud-with-non-cash-means-of-payment-council-agrees-its-position/ [Visitada el 30/12/18]
12. https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics [Visitada el 30/12/18]
13. https://opendatasecurity.io/the-most-famous-cases-of-social-engineering/ [Visitada el 30/12/18]
14. https://www.social-engineer.org/social-engineering/social-engineering-infographic/ [Visitada el 30/12/18]
15. http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2001/2trimes01/goldstein.htm [Visitada el 30/12/18]
16. http://dle.rae.es/srv/search?m=30&w=ganz%C3%BAa [Visitada el 30/12/18]
17. https://www.ganzuas24.com/manual-de-uso-de-las-ganzuas/ [Visitada el 30/12/18]
18. https://amzn.to/2SleFWc1 [Visitada el 27/11/18]
19. https://bit.ly/2E3TCEw [Visitada el 30/12/18]
20. http://www.insecam.org/ [Visitada el 30/12/18]
21. https://spyassociates.com/wall-clock-hidden-camera-w-dvr-wifi-remote-view/ [Visitada el 30/12/18]
22. https://www.openwall.com/john/ [Visitada el 30/12/18]
23. http://ophcrack.sourceforge.net/ [Visitada el 30/12/18]
24. https://www.aircrack-ng.org/ [Visitada el 30/12/18]
25. https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php [Visitada el 30/12/18]
26. https://github.com/trustedsec/social-engineer-toolkit [Visitada el 30/12/18]
27. https://www.elevenpaths.com/es/labstools/foca-2/index.html [Visitada el 30/12/18]
28. https://www.exploit-db.com/google-hacking-database [Visitada el 30/12/18]
29. https://www.incibe.es/en/node/4909 [Visitada el 30/12/18]

11. Anexos

11.1. Anexo 1: Los Tweets de Ingeniería Social

Durante el proyecto se busca una forma de poder compartir toda aquella información interesante que se va recolectando en las diferentes fuentes y compartir el conocimiento con todas aquellas personas que les pueda ser útil, para ello se crea una cuenta de Twitter donde se comparten conocimientos con todos aquellos usuarios interesados.

Tweet fijado

IngSocialInfo @social_ing · 8 nov.

Social engineering bypasses all technologies, including firewalls. - Kevin Mitnick

Traducir Tweet

1

IngSocialInfo @social_ing · 28 nov.

Las webcams de vídeo vigilancia buscan proteger nuestros lugares importantes, pero su seguridad es fundamental, si no podríamos estar enseñando al mundo aquello que queríamos proteger. Hay webs que las enseñan. #protegewebcam #protegelaintimidad #Ciberseguridad

1

IngSocialInfo @social_ing · 17 nov.

¿Has buscado nunca tu nombre en Google? ¿Sabes que es tu identidad digital?
1. Abre una ventana de navegación privada.
2. Busca tú nombre en Google.
3. Empieza a conocer tu identidad digital.

Ser consciente de lo que enseñamos o de lo que se dice, es el primer paso!

1

IngSocialInfo @social_ing · 17 nov.

"A mi no me va a pasar" "Yo no tengo nada de valor" "Lo de las contraseñas lo dicen siempre, pero quien va a pensar que es mi cumpleaños..." ¿Tienes dudas? Pregunta, infórmate! Aunque sean escépticas, primero conocimiento para tener CONSCIENCIA! #ciberescepticos #ciberseguridad

1

IngSocialInfo @social_ing · 12 nov.

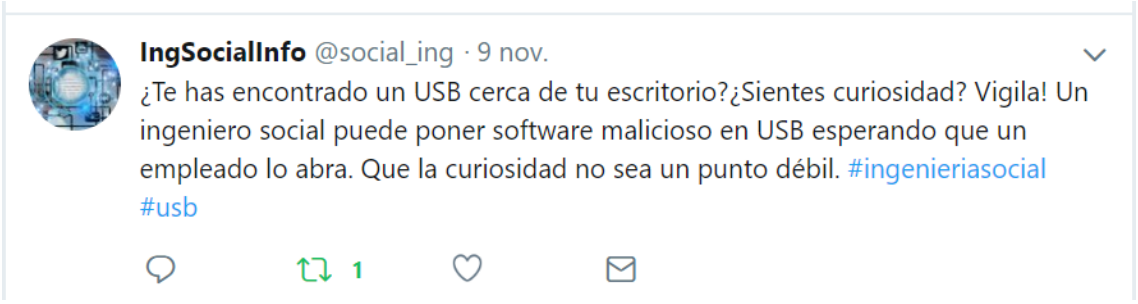
¿Eres consciente de la información que Google tiene sobre ti? Descúbrelo en takeout.google.com/settings/takeo...

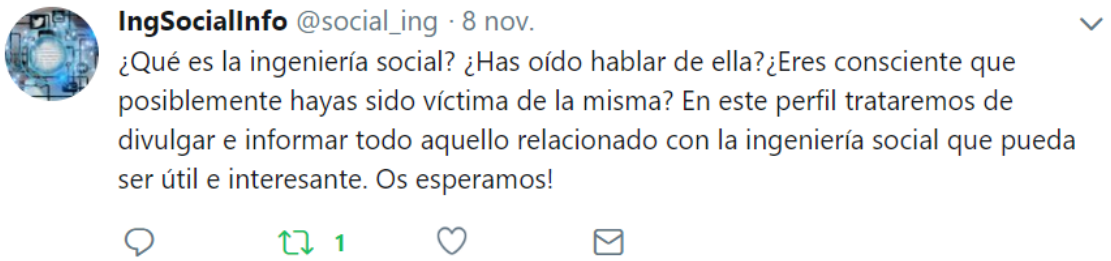
1

IngSocialInfo @social_ing · 12 nov.

¿Conoces el dumpster diving o trashing? La basura puede no ser el final. Elimina cuidadosamente toda aquella información confidencial! Hasta en la basura puede caer en malas manos. Sé consciente. #trashing #ingenieriasocial

1





11.2. Anexo 2: Correo electrónico de ayuda

Durante el proceso de investigación sobre las herramientas, se encuentra una página web www.inescam.org que comparte en la red todas aquellas cámaras web que no tienen seguridad o su seguridad es muy simple. En el transcurso de observación se reconoció un negocio que probablemente no era consciente de la situación. Seguidamente se procedió a realizar una llamada a ese negocio, después de las presentaciones oportunas, se informa a la persona que respondió al teléfono de la situación y se les ofrece la opción de enviar toda esta información por correo electrónico. Opción que ellos aceptan. Al cabo de unos minutos la cámara web dejo de emitir.

Webcam

Joan Enric Garcia Romero <joanenricgarciaromero@uoc.edu>
to [redacted]

Buenas tardes,

Esta es la dirección donde se puede ver vuestra webcam:

[redacted]

Y esta es la página web donde se puede encontrar:

https://www.insecam.org/

Articulos relacionados:

https://www.xataka.com/seguridad/hola-te-llamo-porque-estoy-viendo-tu-restaurante-directo-internet-no-eres-consciente-ello

https://es.gizmodo.com/esta-web-piratea-la-senal-de-73-000-camaras-sin-la-cont-1655747398

Espero que lo podais solucionar.

Atentamente,

--
Joan Enric Garcia

11.3. Anexo 3: Solicitudes y autorizaciones de material con derechos

Chris SEORG <logan@social-engineer.org>
to me

Thank you Joan,

Yes you have permissions to use any of our resources as long as cite where they came from.

Good luck on your program!

Chris "l0gan"
http://twitter.com/humanhacker/
http://www.social-engineer.org

From: "joanenricgarciaromero@uoc.edu" <noreply@social-engineer.org>
Reply-To: <joanenricgarciaromero@uoc.edu>

Date: Thursday, November 8, 2018 at 2:13 PM

To: <logan@social-engineer.org>

Subject: Contact

Name
Joan Enric Garcia
Email
joanenricgarciaromero@uoc.edu
Message
Good morning My name is Joan Enric Garcia, I am a student of Universitat Oberta de Catalunya (UOC) (Spain). Currently I am doing an interuniversity Master in Information and Communication Technologies Security (MISTIC). Nowadays, I am doing my final master's degree project (TFM), which the title is "Studdy on social engineering methodologies". In my research I discover the existence of the website https://www.social-engineer.org and browsing it I have discovered a lot of interesting information to use in my project. Overall in your framework part. Since this website is fully protected by copyright, I have taken the liberty of writing to you, with the intention of requesting the relevant authorisation. My TFM does not pursue any financial gain on my part and the source of the information will obviously be duly mentioned. Thanks. Yours faithfully. Joan Enric Garcia