UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ABRIL 2022 – SEPTIEMBRE 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUBA PRÁCTICA

PREVIO A LA OBTENCION DEL TITULO DE INGENIERO(A)

TEMA:

INGENIERÍA SOCIAL: TÉCNICAS UTILIZADAS POR LOS CIBERDELINCUENTES Y CÓMO PROTEGERSE.

EGRESADA(O):

TOBAR ALVAREZ JUANA DEL ROCIO

TUTOR:

ING. RAÚL RAMOS MOROCHO

AÑO 2022

RESUMEN

En la presente investigación se desea explicar por medio de un extenso análisis de la Ingeniería Social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse; por lo que, se analiza de manera óptima la información con el fin de prevenir a los usuarios de lo que figura al día de hoy como práctica ilegal de obtener información a través de la manipulación de usuarios legítimos, se pueden definir como un conjunto de técnicas que pueden usar ciertas personas para obtener accesos o permisos en sistemas de información con el fin de realizar daños a determinadas empresas y usuarios, para luego ser utilizado en diversas formas de estafas y suplantación de identidad. Al momento de realizar un ataque de Ingeniería Social lo que más se utiliza es el correo electrónico debido al uso masivo por empresas, como por personas particulares; ya que esto permite hacer uso de medios de comunicación como mensajería instantánea u otros canales de comunicación como llamadas telefónicas y redes sociales para concretar un ataque.

El presente estudio investigativo da a conocer sobre los ciberdelincuentes que se centran cada vez más en atacar no solo a grandes empresas, sino también a medianas y pequeñas en busca de información, datos confidenciales y valiosos; sin embargo, hay que tener en cuenta que el uso fraudulento de dicha información puede tener graves consecuencias para una empresa. De acuerdo con lo discutido en esta investigación, se profundiza porque es importante tomar las medidas adecuadas para evitar ser víctimas de cualquier tipo de Ingeniería Social, que bien puede suceder en la actualidad.

Palabras Clave: Ciberdelincuentes, Ingeniería Social, Información, Correo electrónico.

SUMMARY

In the present investigation it is desired to explain through an extensive analysis of Social Engineering: techniques used by cybercriminals and how to protect themselves; Therefore, the information is optimally analyzed in order to prevent users from what appears today as an illegal practice of obtaining information through the manipulation of legitimate users, they can be defined as a set of techniques that certain people can use to obtain access or permissions in information systems in order to harm certain companies and users, and then be used in various forms of fraud and identity theft. When carrying out a Social Engineering attack, what is most used is email due to the massive use by companies, as well as by individuals; since this allows the use of means of communication such as instant messaging or other communication channels such as telephone calls and social networks to carry out an attack.

The present investigative study reveals about cybercriminals who increasingly focus on attacking not only large companies, but also medium and small ones in search of information, confidential and valuable data; however, it must be taken into account that the fraudulent use of such information can have serious consequences for a company. According to what was discussed in this investigation, it is deepened because it is important to take the appropriate measures to avoid being victims of any type of Social Engineering, which may well happen today.

Keywords: Cybercriminals, Social Engineering, Information, Email.

INTRODUCCIÓN

En el presente documento se detalla al análisis de la Ingeniería Social como técnica utilizada por los ciberdelincuentes y como saber protegerse, sabiendo que en la actualidad somos testigos de cómo la tecnología evoluciona cada día más, al igual que nosotros utilizando internet, constantemente hacemos uso de redes sociales como Facebook, Instagram, WhatsApp en las que publicamos prácticamente toda nuestra vida. También se encuentran las empresas que se han acogido a estas tecnologías con la incorporación de nuevos sistemas volviéndolas así más exitosas.

Por lo tanto, los ciberdelincuentes hacen uso de una gran variedad de herramientas informáticas, las cuales aprovechan debido al descuido de las empresas y usuarios físicos haciendo uso de una de las técnicas como la Ingeniería Social con diversos métodos engañosos para así cometer algunos tipos de delitos; sin embargo, esta ingeniería es la habilidad ilegitima de conseguir información por medio de la manipulación de los usuarios legítimos.

Por tal efecto, la tecnología evoluciona y los hackers o delincuentes informáticos aprovechan las técnicas debido a la importancia de los datos o información que puede resultarles beneficioso, estos ciberdelincuentes informáticos filtran información a través de un conjunto de métodos y técnicas conocidas como Ingeniería Social, que se centran en los ataques contra los empleados de una entidad o usuario.

La característica principal de esta presente investigación es analizar todo lo que se necesite para protegerse de ataques de los ciberdelincuentes por medio del objetivo planteado de tratar que un usuario sepa identificar cuando este siendo atacado por Ingeniería Social, de forma inconsciente.

El objetivo de esta presente investigación es determinar los mejores métodos de defensa ante los diversos ataques informáticos en los ambientes empresariales de desarrollo. Se indicará que canales utilizan para los ataques, sus métodos, técnicas más difundidas, y herramientas de seguridad, ya que todos podemos llegar a ser víctimas potenciales de la Ingeniería Social.

En este proyecto se empleó el método cualitativo - descriptivo que me permitió reunir, simplificar, organizar y mostrar información de diferentes sitios web con fuentes bibliográficas. Al ir seleccionando información existente sobre que es la Ingeniería Social, que ataques usualmente puede recibir una empresa, cuáles son los riesgos a los que se enfrentan, y como evitarlos; la técnica de investigación que se opto es la entrevista y la metodología de investigación a utilizar es la deductiva.

La línea de investigación a utilizarse en el presente estudio investigativo es la de Sistema de Información y Comunicación, Emprendimiento e Innovación, y la Sublínea es redes y tecnología de software y hardware.

DESARROLLO

En la actualidad hay muchas técnicas de Ingeniería Social que comúnmente emplean los ciberdelincuentes, desde cebos, que es brindar al usuario algo tentador con el fin de que descargue algún archivo malicioso; también se tiene al phishing que es la más común, en este caso el usuario recibe un correo electrónico con la intención de robar su información personal o algún dato valioso; el scareware también es una técnica utilizada para engañar a los usuarios, haciéndoles pensar que su computadora se encuentra infectada con malware, ofreciéndoles soluciones que a la final terminan infectándola.

Otra de las técnicas conocidas es el vishing, que se lleva a cabo por medio de una llamada telefónica donde suplantan la identidad de una persona, trabajador o empresa conocida con la intención de obtener datos personales o acceso a algún dispositivo; sin embargo, las redes sociales también son frecuentemente utilizadas por los ciberdelincuentes para obtener cualquier tipo de información extorsionando a los usuarios y el smishing también es una técnica usada mediante el cual intentan obtener información confidencial a través de mensajes de textos (Gonella, s.f.).

Ilustración 1 Ataques por Ingeniería Social
Fuente: https://tecalsa.net/ataques-por-ingenieria-social/

En este contexto, las víctimas de estos ciberdelincuentes tienden a caer de manera muy fácil por medio de las técnicas de Ingeniería Social, ya que estos ataques se pueden perpetrar directamente a las personas por sus redes sociales y existe la posibilidad del robo de documentos o falsificación de cheques, entre otros. Por lo tanto, las personas se encuentran expuestas a ser víctimas de ataques a través de técnicas bien elaboradas, conocidas como Ingeniería Social, las cuales consisten en saber convencer a una o varias personas para que brinden información confidencial con el fin de realizar un ataque, robo o cualquier actividad maliciosa contra una determinada empresa o persona.

La metodología de investigación a utilizar es la deductiva, con el método cualitativo – descriptivo que me permitió reunir, simplificar, organizar y mostrar información de diferentes sitios web con fuentes bibliográficas. Al ir seleccionando información existente sobre que es la Ingeniería Social, que ataque usualmente puede recibir una empresa, cuáles son los riesgos a los que se enfrentan, y como evitarlos; la técnica de investigación que se opto es la entrevista.

Las empresas en la actualidad usan internet de manera constante, por lo que pueden ser víctimas de ataques que las ponen en riesgo, enfrentar amenazas a su privacidad y a la de sus clientes, el continuo uso de las computadoras y sistemas de información las hacen vulnerables a técnicas de ataques de los ciberdelincuentes siendo persuadidos por sus habilidades, para así obtener alguna información confidencial de alto valor. Por ello, la Ingeniería Social es una herramienta muy poderosa que los ciberdelincuentes utilizan, por lo que una empresa haría bien en tomar medidas necesarias para la prevención de este tipo de ataques.

Algunas veces las víctimas no se dan cuenta que están siendo atacadas, ya que estos ataques se presentan por medio de un correo electrónico, mensaje de texto, mensajes de voz o por medio de fuentes que aparentemente parecen confiables; por ende, se ha propuesto realizar un cuadro en el que se definirá cada una de las técnicas de la Ingeniería Social, de la que se trata en la presente investigación. Por esta razón es de suma importancia que conozcamos sobre la Ingeniería Social y sus técnicas para poder prevenir y minimizar el daño.

Pero quienes son estos ciberdelincuentes, hoy en día se los conoce como Cracker a diferencia de un hacker, el cracker no merece ningún reconocimiento ya que no ayuda a mejorar aplicaciones ni aporta ningún progreso en ese sentido. La palabra cracker o hacker de sombrero negro es utilizada para describir a una persona que irrumpe en un sistema de información y vulnera contraseñas o licencias de programas informáticos intencionalmente, son capaces de robar información de tarjetas de créditos o datos confidenciales con el objetivo de venderlos y obtener beneficios personales.

Personas sin conocimiento del tema, como auxiliares administrativos, miembros de seguridad, recepcionistas etc.
Personas con privilegios, como los de apoyo técnico, dirección de sistemas etc.
Secciones especificas como las de contabilidad, y las de recursos humanos o las que cuenten con información potenciaalmente valiosas.
Elaborador/Suministrador de empresas que producen hardware, software etc. Que son de interés para los ciberdelincuentes.

Tabla 1 Posibles víctimas de un ataque de Ingeniería Social
Elaborado por: Juana Tobar

TIPOS DE ATACANTES DE INGENIERIA SOCIAL

Por lo general, cuando uno piensa en la ingeniería social y quien está detrás de ella, lo primero que se nos viene a la mente es la imagen de una persona con altos conocimientos en programación o informática, pero resulta ser que hay diferentes tipos de atacantes, pueden dividirse en varias categorías. Estas personas van desde espías, piratas informáticos, comerciantes, y gente en común. A continuación, se muestra algunos tipos de atacantes:

Cracker

La diferencia entre un hacker y un cracker es que podemos catalogar a este como un tercero que intenta hackear el sistema de seguridad creado por el hacker para realizar acciones ilegales. Utiliza programas que están diseñados para detectar debilidades en los programas de seguridad informática, por lo que conoce sus debilidades y estudia la mejor manera de acceder a ellas. Comúnmente el cracker sin las habilidades de crear software, para su propio beneficio utiliza programas diseñados por otros (Ruiz Martinez, 2021). Ellos andan en busca de cualquier alternativa para lograr su propósito, y les ha sido de utilidad implementar la ingeniería social en conjunto con todos sus conocimientos.

Probadores de seguridad

Es una persona que prueba un sistema en busca de vulnerabilidades o acceso no autorizado, las pruebas de penetración implican inspeccionar un sistema informático, una red, una aplicación web o los alrededores de un sitio web en busca de vulnerabilidades

que puedan ser explotadas por atacantes maliciosos, la ingeniería social es el aspecto humano de las pruebas de vulnerabilidad en una red empresarial (Testers, 2021).

Espías

Es la actividad oculta de recopilar información sobre una industria competitiva, con el fin de colocarla en una ventaja estratégica o financiera. En el pasado, el espionaje a menudo se centraba en recopilar información política y militar, pero con el auge de la tecnología, el énfasis se ha ampliado a elementos como las TI. Actualmente la ingeniería social es uno de los métodos más utilizados por estos espías para intentar obtener la información que desean.

Ladrones de identidad

Los ladrones de identidad son un grupo de personas que recopilan varios tipos de información de identidad personal, robada para sus propios fines. Es fundamental saber que el robo de identidad le puede ocurrir a cualquiera, ya que no existe un límite de edad para convertirse en una víctima.

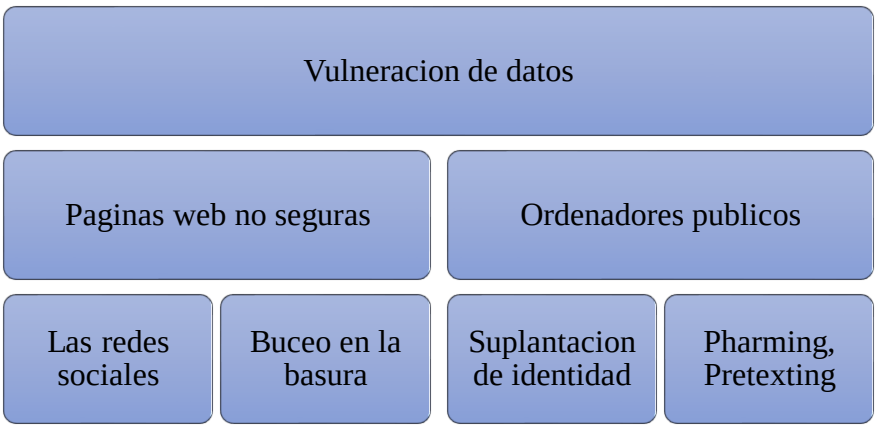


Tabla 2 Maneras en la que los ladrones de identidad roban información

Elaborado por: Juana Tobar

Empleados descontentos

Generalmente en este ámbito existen tres tipos de amenazas internas las cuales son: empleados comprometidos, son aquellos a quienes les roban las credenciales, también se encuentra la negligencia de los empleados, por ejemplo, si un empleado pierde una computadora portátil o envía un correo electrónico incorrecto y los empleados malintencionados, incluidos los empleados descontentos, que participan en actos como robo, fraude, sabotaje, espionaje y extorsión (Beaver, 2019).

Vendedores

La habilidad de vender es un tipo de ocupación dentro del mercado laboral, en la que se hace uso de varias técnicas que utilizan la ingeniería social. Algunas de ellas pueden ser reunir datos, tácticas para la obtención de información, influencia, etc. Estos vendedores las usan para asegurarse de que la venta satisfaga las necesidades de su futuro cliente.

Timo del CEO

También conocida como el fraude del CEO, en donde los ciberdelincuentes se hacen pasar por ejecutivos de turno, para lograr que los empleados hagan lo que desean, este tipo de atacantes ha causado problemas a las empresas durante años por sus ataques altamente personalizado y de gran impacto. Esta estafa se aprovecha del hecho de que cada vez más empresas confían en el uso de correo electrónico para realizar negocios, siendo este uno de los delitos más perjudiciales financieramente (Alonso, 2020).

CICLO DE VIDA DE UN ATAQUE DE INGENIERIA SOCIAL

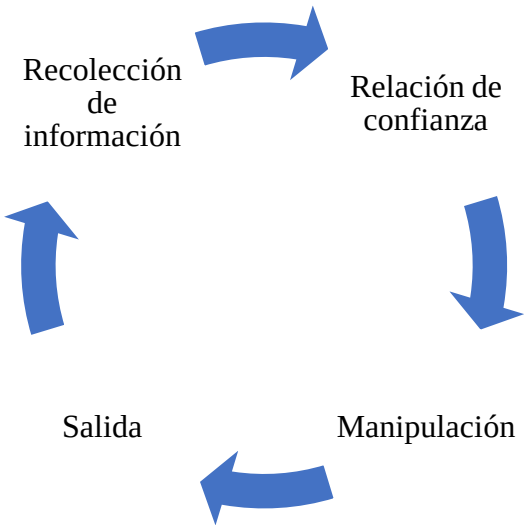


Ilustración 2 Ciclo de vida
Elaborado por: Juana Tobar

Recopilación de información: También conocido como Footprinting (también denominado espionaje), es una de las etapas del pre-hackeo, que es el proceso de recopilar la mayor cantidad de información posible sobre lo que queremos "hackear" para localizar la vulnerabilidad y cómo acceder a ella. Para obtener esta información, los "hackers" pueden usar una variedad de herramientas y procesos. Por lo general, la información que recopilan es la siguiente:

- Nombre de dominio
- Direcciones de protocolo de internet
- Sistema operativo utilizado
- Información del empleado
- Número de teléfono
- Dirección de correo electrónico

El Footprinting es básicamente un paso previo a un ciberataque, en el que los "hackers" recopilan toda la información posible sobre su víctima para encontrar la manera de acceder al sistema o decidir sobre un ciberataque, que será más eficaz para cumplir sus metas (Peña, 2021).

Establecer una relación de confianza: Una vez recopilada la información, el atacador establecerá una relación más estrecha con la víctima.

Manipulación: En este paso, el ingeniero social utiliza la confianza ganada en la etapa anterior para explotar la máxima información confidencial u obtener operaciones secretas relacionadas con el sistema de destino realizadas por el propio empleado para acceder al sistema con mucha facilidad. Una vez que se haya recopilado toda la información confidencial solicitada, el ingeniero social puede pasar al siguiente objetivo o concentrarse en explotar el sistema actual que se está considerando (Ramiro, 2018).

Salida: Una vez extraída la información, el atacante hará todo lo que esté a su alcance para evitar que cualquier tipo de sospecha caiga sobre él. Para ello, tendrá cuidado de no dejar ningún indicio que pueda vincularle. De esta manera, en el futuro, puede realizar un seguimiento de las entradas del sistema para mantener su fuente de información en funcionamiento (Seguridad, 2020).

TIPOS DE ATAQUE DE INGENIERIA SOCIAL

Un atacante puede engañar a los usuarios de varias formas, ya que en una sociedad "bien percibida", la gente tiende a devolver algo después de haber recibido inicialmente

otra cosa, por reciprocidad, según el caso y la situación (Prado Díaz, 2021). Siendo esta una de las formas en las que un ciberdelincuente aprovecha para que dicho usuario comparta información confidencial.

Se distingue de la piratería convencional en la que los ingenieros sociales acceden a información confidencial con el permiso del propietario de la información. Podemos decir que son timadores, lo suficientemente buenos como para convencerlo de que les dé una información o manipular directamente a los usuarios para que crean que su acceso es legítimo, a continuación, se puntualizan los tipos de ataques.

ATAQUE/HACK	DESCRIPCIÓN
CARNADA O CEBO	Como cebo, los atacantes cibernéticos utilizan un objeto físico, como una unidad flash USB, para atraer a las personas y aumentar su curiosidad, y cuando lo inserten en un dispositivo, el software malicioso se instalará y ejecutará, recopilando información confidencial.
PHISHING	Los ciberdelincuentes envían correos electrónicos falsos a usuarios aparentemente legítimos, sugiriendo que los destinatarios del correo electrónico actúen lo antes posible. Cuando se hace clic en el enlace del correo electrónico o

	se descarga el archivo adjunto, el malware se instala en el dispositivo y se ejecuta.
VARIAS FORMAS DE PHISHING	Phishing: Usar de llamadas telefónica. Smishing: Uso de SMS. Whaling: Envió de un correo electrónico falsificado a una persona específica, generalmente un miembro del equipo de administración, que parece ser de alguien dentro de la organización. Suplantación: Falsificación de correos electrónicos personalizados.
SCAREWARE	Este tipo de ataque incita a las personas a tomar medidas sugiriendo que, si toman la acción solicitada, evitarán el daño.
PRETEXTING	Esto sucede cuando un atacante investiga, crea una historia y luego se hace pasar por alguien que puede considerarse legítimo (como un empleado de TI).
FARMING/CACERÍA	Los piratas informáticos se vinculan con las víctimas y desarrollan relaciones con el tiempo (Gotthart, 2022).

Tabla 3 Tipos de ataques de Ingeniería Social
Elaborado por: Juana Tobar

TECNICAS UTILIZADAS POR LOS CIBERDELINCUENTES

Los ciberdelincuentes a menudo usan técnicas de ingeniería social porque los humanos son mucho más fáciles de piratear que las vulnerabilidades de la red. En un ataque social, los delincuentes apuntan a emociones como el miedo, la urgencia o la obediencia para influir en la toma de decisiones. El compromiso del individuo no es el objetivo final, sino que sirve como plataforma de lanzamiento.

Después de obtener información personal, contraseñas, cuentas de usuarios remotos y más, el ciberdelincuente utilizará esta información para lanzar un ataque contra el objetivo, es decir, una empresa u organización. Los resultados pueden literalmente devastar a dicha empresa u organización en cuestión de minutos (Hackers, 2021). A continuación, se muestran las técnicas más utilizadas, también se hablará sobre las distintas herramientas de las que disponen estos ingenieros sociales para perpetrar sus ataques.

Técnicas de generación de ataques de Ingeniería Social

Métodos para la obtención de información	Google hacking: Es un operador de búsqueda avanzado que nos permite un mejor filtrado de resultados al buscar información de Google. Redes sociales: Nos ofrecen grandes cantidades de información.
Técnicas para generación de ataques de manera más personal.	
Relaciones sociales	La amabilidad de las personas con extraños.

	La adulación es una forma de apertura y da la posibilidad de divulgar más información. La mayoría de las personas responden amablemente a aquellos que se preocupan por ellos.
Cualidades del atacante para la obtención de una mayor tasa de éxito.	
Cualidades	La naturalidad, ya que si llega a existir una pequeña incomodidad se puede llegar a perder una conversión. Formación, para establecer una conversación con el objetivo y saber responder en cualquier momento. Ser avaricioso, no debe presionarse para obtener más información de la obtenida, dado que se puede perder una oportunidad.
Vías de ataques utilizada por los ciberdelincuentes	
Ingeniería social por teléfono	Es la más habitual, el atacante hace la llamada haciéndose pasar por alguien importante para la empresa.
Ingeniería social por internet	Adopta diferentes formas, el atacante envía un correo electrónico o archivo adjunto infectado con un malware.
Ingeniería social por Dumpster Diving	El atacante adquiere información sobre el cliente o empresa, buscando en la basura que estos ya han desechado.
Ingeniería social por persuasión psicológica	En este caso el atacante recurre a la persuasión, y así ganarse la confianza del cliente.

Tabla 4 Técnicas de generación de ataques utilizadas por los ciberdelincuentes
Elaborado por: Juana Tobar

HERRAMIENTAS UTILIZADAS POR LOS CIBERDELINCUENTES

Los ingenieros sociales utilizan diferentes herramientas y software para lograr acceder de una forma más sencilla a la información de una persona. De hecho, Kali Linux es la herramienta perfecta para los ciberdelincuentes que buscan (y encuentran) limitaciones y fallas en la seguridad de las redes y los sistemas informáticos. Linux es un sistema operativo de código abierto similar a Unix desarrollado por la comunidad para computadoras, servidores, mainframes, dispositivos móviles y dispositivos integrados.

Kali Linux cuenta con muchas herramientas en modo grafico como en comando lo que lo convierte en un sistema muy completo, que puede ser utilizado tanto por usuarios que buscan un sistema más seguro, como por ciberdelincuentes que buscan esos datos valiosos como cuentas, contraseñas y otros datos personales, dado que si bien se puede decir hay una serie de imprescindibles herramientas que los ayudan, las cuales algunas se detallan a continuación.

Herramientas físicas	***Herramientas software***
Abrir cerraduras. *En el mundo de la ingeniería social, el atacante puede tener diferentes herramientas para abrir candados que le permitan acceder a lugares restringidos o confidenciales. Algunas de estas herramientas pueden ser;*	*Programas para descifrar contraseñas.* *El uso de estos softwares es de mucha utilidad para los ingenieros sociales ya que les ayuda a descifrar contraseñas y extraer información confidencial.* *John the Ripper: Es probablemente el software de pirateo de contraseñas (hackeo) más popular, por lo que siempre*

Ganzúas: Esta herramienta es similar a la llave del sitio donde se pretende entrar.	*estará en la categoría de las "Diez mejores herramientas cortas de pirateo".*
Cerraduras magnéticas y electrónicas: Esta herramienta es frecuentemente usada considerando su precio y facilidad de uso, ofrece cierto nivel de seguridad, aunque el corte de corriente es su punto débil.	*Nmap: Es un programa de código abierto que es utilizado para escanear una red y sus puestos en busca de información importante para así controlar y administrar su seguridad.*
Llaves bumping: Diseñada para abrir cerraduras sin necesidad de l llave de bloqueo.	*Social-Engineer Toolkit (SET): Es un conjunto de herramientas utilizada por el Ingeniero social. Es un marco de prueba de penetración de código abierto, SET tiene muchos vectores de ataque dedicados, lo que le permite realizar rápidamente un ataque confiable.*
Cuña para candado: Pieza delgada de metal que se desliza y libera el mecanismo de cierre.	

Tabla 5 Herramientas utilizadas para la generación de ataques
Elaborado por: Juana Tobar

TECNICAS Y HERRAMIENTAS DE PREVENCION ANTE UN ATAQUE DE INGENIERIA SOCIAL

Como hemos analizado, la ingeniería social engloba una infinidad de métodos y técnicas que la hacen muy complicadas de controlar. Hasta ahora no podemos asegurar que no llegaremos hacer víctimas de ingeniería social, cualquier tipo de persona es susceptibles de ser víctimas de sus ataques, por esa razón es de gran ayuda disponer de conocimientos y medios para contrarrestarlos o tener la capacidad de reaccionar ante ellos. A continuación, se detallará algunas técnicas y herramientas de prevención que nos pueden ayudar a mitigar parte de esos ataques en pequeña o gran medida.

CONSEJOS BÁSICOS PARA LA PREVENCION ANTE UN ATAQUE DE INGENIERIA SOCIAL

- Cuando reciba un correo electrónico, asegúrese de que el remitente sea confiable.
- Hay que prestar atención a los mensajes con solicitudes urgentes, promociones, ofertas demasiado atractivas o errores gramaticales. Si se suscribe a promociones u ofertas, debe utilizar una cuenta de correo electrónico diferente.
- Si nos invitan a hacer clic en un enlace, debemos comprobar que corresponde a la dirección a la que apunta introduciendo la URL en el navegador.
- Antes de descargar algún archivo adjunto, debe verificarse con su antivirus.
- No ceda a la presión de las personas que nos llaman por teléfono con malas intenciones. En tales situaciones, lo mejor es ponerse en contacto con las agencias de seguridad.
- No conecte su dispositivo USB o una memoria externa al dispositivo. Además, deben estar actualizados y contar con soluciones de seguridad.
- Active el filtro de spam en la configuración de su cuenta de correo electrónico.
- Es recomendable el uso de un filtro de pantalla espía evita que otros vean el contenido del dispositivo desde diferentes ángulos.
- En Internet, asegúrese de usar contraseñas seguras, un administrador de contraseñas, un sistema de autenticación de dos factores o superior.
- Finalmente, es importante desechar de forma segura la información que no nos sirve ya sea impresa o digital de forma segura (Valades, 2021).

DISPOSITIVOS DE PROTECCIÓN DE RED

En este ámbito la protección de red se refiere a cualquier tipo de actividades destinadas a proteger el acceso, uso e integridad de una red y datos corporativos, actividades destinadas a prevenir y protegerse contra intrusiones. Ingreso no autorizado a la red corporativa, centrándose en dispositivos individuales. Comenzando con el control de acceso, las políticas y controles que gestionan el acceso a la red por parte de los usuarios autorizados, pero también por dispositivos y datos. Algunos tipos de seguridad de red son (Bernardo, 2021):

- Firewalls, VPN
- Software antivirus y antimalware
- Segmentación de la red
- Control de acceso
- Seguridad de las aplicaciones
- Prevención de pérdida de datos
- Seguridad de dispositivos móviles

SEGURIDAD DE CORREO ELECTRÓNICO

A continuación, se muestran algunas herramientas que nos ayudan a tener nuestros correos electrónicos seguros.

Abnormal: Nos presenta una solución integrada de seguridad de correo electrónico en la nube. Como resultado, nos protegerá de peligros como el phishing, el ransomware, el fraude, la ingeniería social, la suplantación de identidad corporativa y el

spam. Su método de funcionamiento se basa en el análisis de más de 5.000 señales para detectar anomalías y bloquear con precisión todo el spam y los correos electrónicos de ingeniería social, tanto internos como externos. También monitorea a nuestros proveedores en busca de riesgos de seguridad al identificar automáticamente cuando nuestras cuentas están comprometidas y proteger a nuestros usuarios (Lorenzo, s.f.).

Barracuda: Se basa en técnicas como el análisis de virus, el análisis en tiempo real, la puntuación de spam, las comprobaciones de reputación, la prevención de enlaces de URL y más. para proporcionar la mejor protección. Su centro de operaciones de amenazas global las 2 horas, los 7 días de la semana, Barracuda Central monitorea continuamente nuevas vulnerabilidades de seguridad e implementa tecnologías de filtrado (Prasad, 2021).

Mimecast: Es un gestor de correo electrónico que podemos utilizar para tener un buzón seguro. Con esta solución, las comunicaciones de los empleados están protegidas y los riesgos se reducen al protegerse contra amenazas específicas. Además, protege contra ataques de phishing, amenazas de mensajes internos y filtraciones de datos. Teniendo en cuenta que también protege de spam, malware, ataques de ransomware y phishing (Antonio, 2022).

EDUCACIÓN Y CONCIENTIZACIÓN EN LAS EMPRESAS

Una estrategia defensiva regularmente sugerida ante los ataques de ingeniería social, es asegurarse de que todos los empleados estén capacitados para reconocer y manejar estos ataques. Además, se debe prestar particularmente mucha atención a las

redes sociales, ya que normalmente su uso es muy frecuente, además se da el caso en que el usuario comparte infinidad de datos públicamente, en el que probablemente se los identifica como empleados de una organización u empresa, indirectamente aumentando el riesgo de convertirse en víctimas de ingeniería social. Una recomendación seria sugerir a los empleados que no muestren su lugar de trabajo en las redes sociales, para que no lleguen a ser víctimas como tal.

IMPLEMENTAR POLÍTICAS DE SEGURIDAD

A nivel empresarial, una de las medidas para aumentar la seguridad es implementar una fuerte política de seguridad al personal. De esta forma, se pueden mitigar los ataques de ingeniería social. Algunas de estas políticas podrían ser:

- Implemente una política de "Least Privilege" y asegúrese de que los usuarios entiendan las razones detrás de esto y que esté diseñado para protegerlos también. Ya que otorgar permisos a un usuario fuera de los permisos requeridos para una acción puede permitir que el usuario obtenga o cambie información sin darse cuenta.
- Implemente el uso de "scripts" para cada flujo de trabajo cuando los empleados se comuniquen por teléfono o correo electrónico.
- Es indispensable que se tenga un punto de contacto bien establecido y una ruta de denuncia para presuntos ataques de ingeniería social. Esto ayudará a los empleados a ser proactivos en la protección de la empresa contra ataques, si se combina con la cultura y la capacitación de la empresa.

- Crear una cultura organizacional de conciencia compartida de la ingeniería social. Por ejemplo, puede ser muy útil explicar por qué el tailgating/piggybacking es un problema y comunicar claramente que cada empleado tiene la responsabilidad de prevenir tales incidentes (Lluís, 2022).

AUDITORIAS Y PRUEBAS DE PENETRACIÓN

Otro mecanismo de defensa es realizar pruebas externas y de penetración periódicas, estas verificaciones y validaciones de controles de seguridad in sitúes, es un punto positivo en relación con la seguridad de la información general de la empresa. Desde luego todas las pruebas de penetración acreditadas y las auditorías de seguridad más completas incluyen pruebas de vectores de ingeniería social. Los resultados de estas pruebas y auditorías podrían beneficiar en gran medida a la organización al proporcionar información sobre los problemas actuales, lo que a su vez podría permitir a la gerencia implementar un plan de mejora y, en última instancia, lograr un nivel aceptable de seguridad.

CONCLUSION

Una vez finalizada esta investigación a través de un profundo análisis con su respectivo método de investigación y técnicas de recolección de información se buscó profundizar sobre lo que es la Ingeniería social, en la que hemos llegado a concluir que son técnicas que usan comúnmente los ciberdelincuentes, en la que el usuario se convierte en el principal objetivo.

Por medio de la presente investigación se indica que el usuario utiliza tecnologías para comunicarse convirtiéndose así en el elemento más débil y esto pueden generar graves problemas tanto a nivel personal como a empresas. Hoy en día, los atacantes utilizan la Ingeniería Social para así obtener información confidencial de las personas utilizando técnicas para obtener beneficios propios; por ello, se considera que las empresas trabajen arduamente para educar a sus empleados, mitigar y prevenir este tipo de ataques.

Es importante que haya la formación pertinente a los usuarios de identificar el valor de la información que manejen y el buen uso que se le debe dar; siendo consciente de los peligros que representan porque los ataques de la Ingeniería Social son especialmente complicados de detectar, ya que están precisamente diseñados para aprovecharse de las personas por su curiosidad, el respeto a la autoridad y el deseo de ayudar a los amigos; por lo que, esta investigación ha ayudado a concientizar y aumentar el conocimiento de los posibles ataques de Ingeniería Social dando a conocer las diferentes técnicas, métodos, aplicaciones y software que pueden ayudar a comprender mejor la seguridad informática y la forma de ataque.

Bibliografía

Alonso, R. (9 de Diciembre de 2020). *abc*. Obtenido de https://www.abc.es/tecnologia/redes/abci-timo-ciberataque-roban-millones-haciendo-sola-llamada-202012090135_noticia.html

Antonio, L. J. (25 de Abril de 2022). *RedesZone*. Obtenido de https://www.redeszone.net/noticias/seguridad/gestores-e-mail-bandeja-entrada-segura/

Beaver, K. (22 de Septiembre de 2019). *ComputerWeekly.es*. Obtenido de https://www.computerweekly.com/es/consejo/Seis-tipos-de-amenazas-internas-y-como-prevenirlas

Bernardo, Q. G. (1 de Julio de 2021). *Servnet.mx*. Obtenido de https://www.servnet.mx/blog/seguridad-de-la-red-en-las-empresas-como-conseguirla

Gonella, S. (s.f.). *politicayeducacion*. Obtenido de https://politicayeducacion.com/la-ingenieria-social-su-status-dentro-de-la-ciberseguridad/#:~:text=En%20la%20actualidad%20existen%20infinitas,nuestro%20pa%C3%ADs%2C%20es%20decir%20un

Gotthart, B. (4 de Febrero de 2022). *ifb blog*. Obtenido de https://www.ifb-group.com/blog/es/riesgos-de-la-ingenieria-social-y-como-prevenirla/

Hackers. (7 de Junio de 2021). *Security Through Education*. Obtenido de https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/hackers/

Lluís, L. A. (NF de Febrero de 2022). *Uned.es.* Obtenido de http://e-spacio.uned.es/fez/eserv/bibliuned:master-ETSInformatica-II-Lagil/Gil_Lluis_Luis_TFM.pdf

Lorenzo, J. (s.f.). *Mc.net.co*. Obtenido de https://mc.net.co/protege-tu-correo-electronico-con-estas-herramientas-y-evita-ataques/

Peña, M. J. (19 de Mayo de 2021). *Másteres Online Nº 1 Empleabilidad*. Obtenido de https://eiposgrados.com/blog-ciberseguridad/que-es-footprinting/

Prado Díaz, J. P. (2021). Ingeniería social, un ejemplo práctico. *REVISTA ODIGOS*, 47-76.

Prasad, D. (25 de Marzo de 2021). *Geekflare*. Obtenido de https://geekflare.com/es/email-security-solution/

Ramiro, R. (9 de Abril de 2018). *CIBERSEGURIDAD .blog*. Obtenido de https://ciberseguridad.blog/anatomia-del-ataque-de-ingenieria-social-y-como-prevenirlo/

Ruiz Martinez, J. C. (30 de Agosto de 2021). *YMANT*. Obtenido de https://www.ymant.com/blog/que-diferencia-hay-entre-un-cracker-y-un-hacker/

Seguridad, R. C. (10 de Febrero de 2020). *Cuadernos de Seguridad*. Obtenido de https://cuadernosdeseguridad.com/2020/02/ingenieria-social-seguridad-incibe/

Testers, P. (16 de Marzo de 2021). *Security Through Education*. Obtenido de https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/penetration-testers/

Valades, B. (10 de Enero de 2021). *Segurilatam*. Obtenido de https://www.segurilatam.com/actualidad/dia-del-internet-seguro-10-consejos-para-prevenir-los-ciberataques-de-ingenieria-social_20210110.html

ANEXOS

ENTREVISTAS

Preguntas dirigidas a Ingenieros

1. **¿Cómo se mantiene usted actualizado en cuanto a la ciberseguridad?**

   Referencia: Anexo Pregunta 1

   El Ing. Harry Saltos Viteri indico que, leyendo novedades de blogs, y grupos en redes sociales, así como también ejerciendo en la práctica varias actividades como testeo.

   El Ing. Alfonso Agama Chico menciono que, se mantiene actualizado mediante seminarios online.

   El Ing. José Herrera Rivas expreso que, en cuanto a la ciberseguridad de manera constante toma cursos de fundamentos de la ciberseguridad donde actualiza sus conocimientos acerca de los peligros del ciberespacio y los retos de la ciberseguridad.

2. **¿Por qué cree que es importante conocer sobre la Ingeniería Social en la actualidad?**

   Referencia: Anexo Pregunta 2

   El Ing. Harry Saltos Viteri indico porque, existe delincuencia que se mueve en el ámbito de las redes y la informática.

   El Ing. Alfonso Agama Chico menciono porque, juega un papel muy importante en la democracia.

   El Ing. José Herrera Rivas expreso porque, es importante conocer acerca de la ingeniería social para no ser víctimas de este tipo de actividades ilegales que obtienen nuestra información confidencial para luego manipularnos.

3. **¿Qué medios considera que son los más utilizados por los ciberdelincuentes para realizar ataques de Ingeniería Social?**

   Referencia: Anexo Pregunta 3

El Ing. Harry Saltos Viteri indico que, son las redes sociales, teléfonos móviles (Internet), llamadas telefónicas.

El Ing. Alfonso Agama Chico menciono que, son los correo electrónico y redes sociales.

El Ing. José Herrera Rivas expreso que, en cuanto a los medios más utilizados actualmente son los correos electrónicos dado que las empresas y las personas particulares le damos un uso masivo.

4. **¿Qué red social considera que es la más vulnerable al ataque de Ingeniería Social? ¿Por qué?**

   Referencia: Anexo Pregunta 4

El Ing. Harry Saltos Viteri indico que, Facebook, ya que es la más difundida y usada.

El Ing. Alfonso Agama Chico menciono que, Facebook, porque da mucha información confidencial.

El Ing. José Herrera Rivas expreso que, la red social más vulnerable es Facebook, por su popularidad y fácil manejo.

5. **¿Qué tipos de Ingeniería Social conoce, explique una de ellas?**

   Referencia: Anexo Pregunta 5

El Ing. Harry Saltos Viteri indico que, el Phishing que usualmente lo usan para engañar a las personas, a través de medios de comunicación digital como el correo electrónico.

El Ing. Alfonso Agama Chico menciono que, el phishing ya que nos preocupa saber que nuestra información es errónea y nos lleva a caer en ese engaño.

El Ing. José Herrera Rivas expreso que, el phishing – el scareware, a pesar del phishing ser el tipo de ingeniería social más popular el scareware es el tipo de malware que utilizan en la Ingeniería social para que las personas se asusten y empiecen a descargar falsos softwares de seguridad.

6. ¿Cuál método de defensa ante ataques de Ingeniería Social usted conoce?

Referencia: Anexo Pregunta 6

El Ing. Harry Saltos Viteri indico que, primero el sentido común, reducir el trato de los técnicos con personal no autorizado, capacitar a la organización de estas técnicas para que no sean vulnerables a esta Ingeniería Social.

El Ing. Alfonso Agama Chico menciono que, antivirus de alto desempeño como BitDefender Total Security.

El Ing. José Herrera Rivas expreso que, el método más básico y rápido como defensa es analizar de forma periódica nuestros equipos con herramientas de eliminación de virus o herramientas para la protección de nuestros correos electrónicos.

7. **¿Considera que es importante conocer los tipos de ataques y técnicas que utilizan los ciberdelincuentes? ¿Por qué?**

   Referencia: Anexo Pregunta 7

El Ing. Harry Saltos Viteri indico que, si, para reducir riesgos y vulnerabilidades para las empresas y su personal.

El Ing. Alfonso Agama Chico menciono que, si, para poder identificarlos y evitar caer en eso.

El Ing. José Herrera Rivas expreso que, si, es muy importante conocer los tipos y técnicas que utilizan los ciberdelincuentes ya que de esta manera podemos contrarrestar sus ataques y evitamos ser las víctimas vulnerables de estas personas.

8. **¿Qué medidas de seguridad ante ataques de Ingeniería Social considera que deberían de implementar las empresas?**

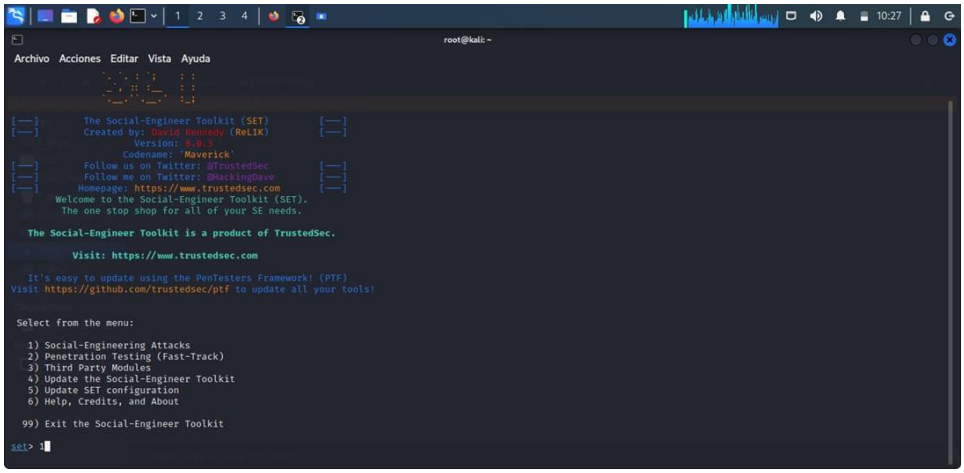
   Referencia: Anexo Pregunta 8

El Ing. Harry Saltos Viteri indico que, aplicación y elaboración de políticas orientadas a la comunicación entre personal de la organización y agentes externos.

El Ing. Alfonso Agama Chico menciono que, antivirus de alto desempeño como BitDefender Total Security, capacitación al personal y uso eficiente de la jornada laboral.

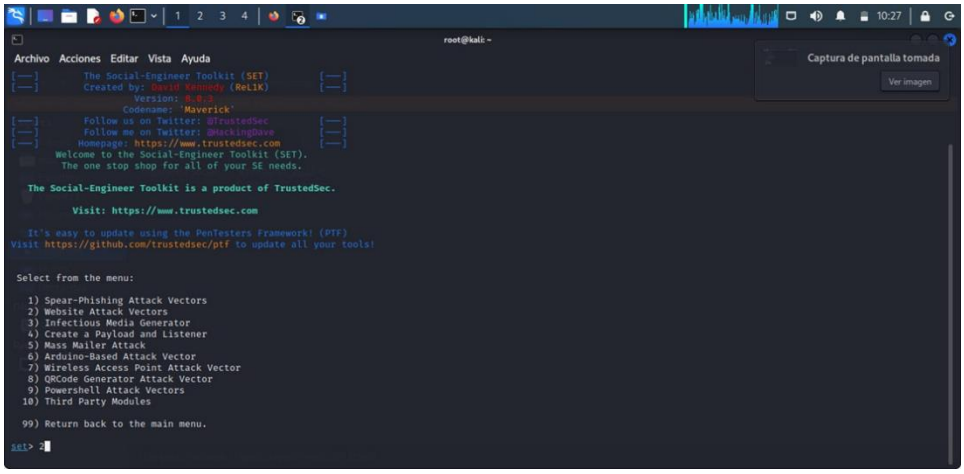
El Ing. José Herrera Rivas expreso que, las empresas como mantienen abundante información la cual es propia de cada una de ellas deberían implementar como método principal es utilizar un aplicativo de análisis inteligente para detectar y bloquear los tipos de ataques que suelen utilizar los ingenieros sociales para infectar los equipos.

Para realizar esta simulación de un ataque de ingeniería social hice uso del sistema operativo Linux y sus herramientas, para así dar a conocer cómo es que estos ciberdelincuentes realizan sus ataques.



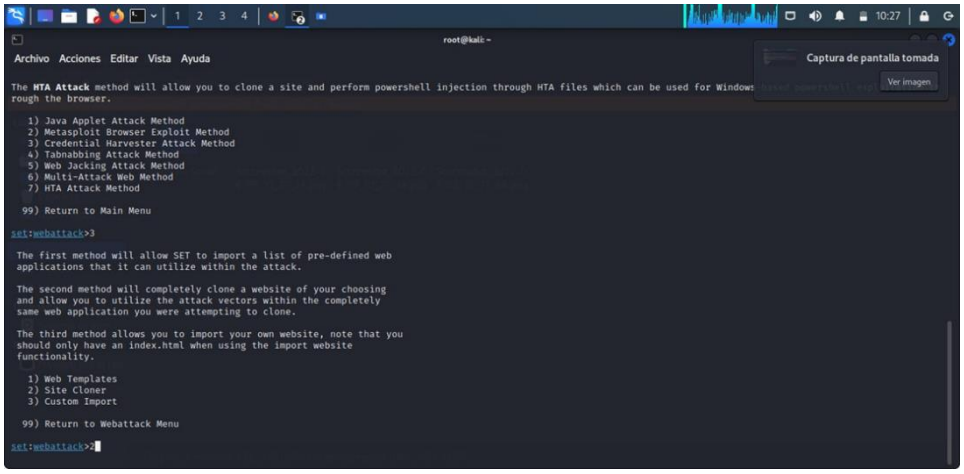
Fuente: Juana Tobar

Análisis: Como primer punto ingresamos a la terminal en modo root, y escribimos el comando setoolkit, que nos permite generar automáticamente un sitio falso con el que pretenderemos engañar a un usuario, siguiendo algunas opciones las cuales, se muestran a continuación.



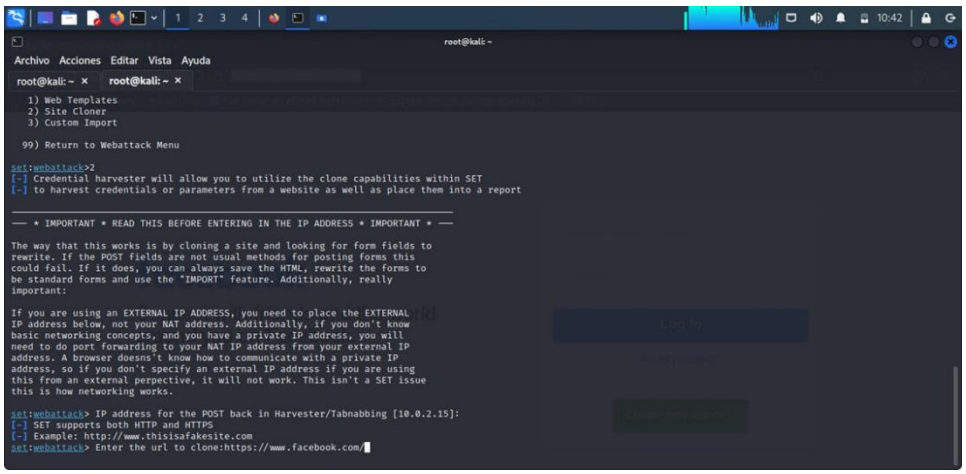
Fuente: Juana Tobar

Análisis: Al elegir la opción uno, ataque de Ingeniería Social, se despliegan 10 opciones la cual elegimos la numero 2 que es vectores de ataque a sitio web, que nos permite realizar ataques a usuarios que ingresen a una dirección que nosotros le vamos a especificar.



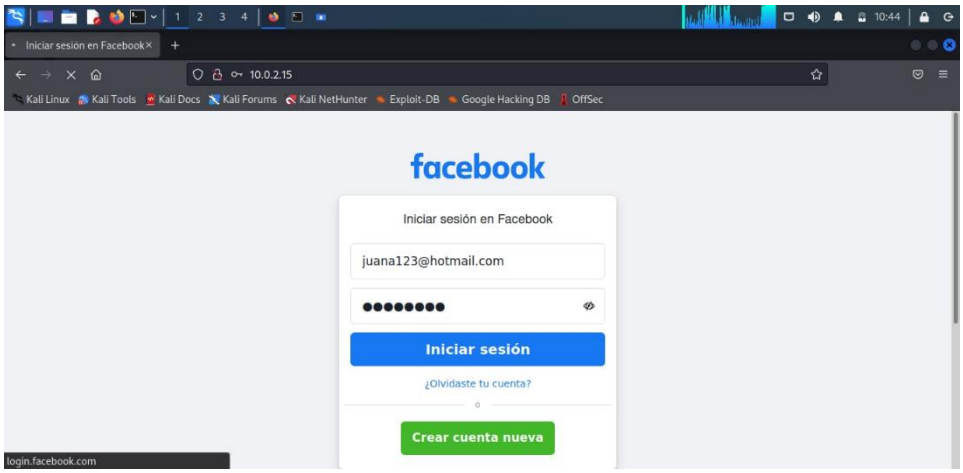
Fuente: Juana Tobar

Análisis: Entre las diversas opciones disponibles elegí la numero 3 Método de ataque para cosechar credenciales, esta se utiliza específicamente para clonar un sitio web que nos ayuda a capturar los campos como usuario y contraseña, y cualquier información enviada hacia el sitio web.



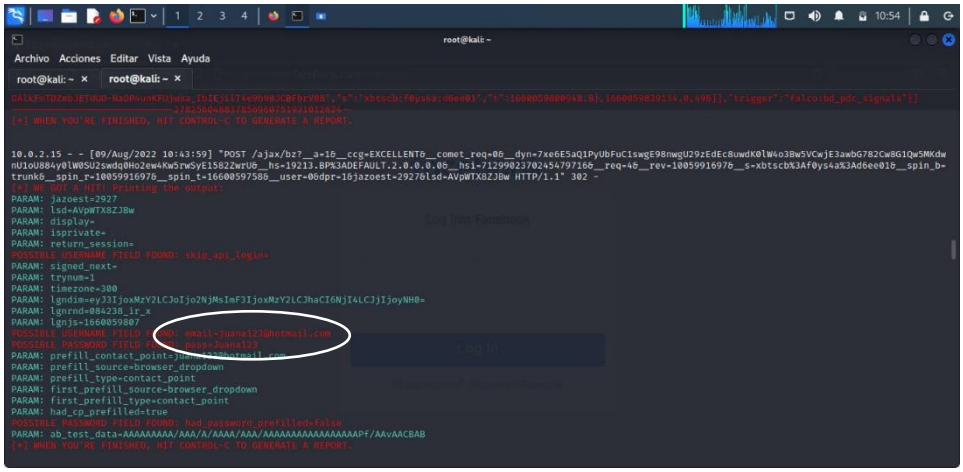
Fuente: Juana Tobar

Análisis: Seleccioné la opción 2 Clonador de sitio, que me permitió clonar completamente el sitio web, ingresando la URL a clonar que este caso fue Facebook, después de finalizar la clonación del sitio se debe utilizar diversas técnicas o métodos para inducir a la víctima a que visité el sitio web.



Fuente: Juana Tobar

Análisis: La victima al ingresar al sitio web clonado y colocar el usuario y contraseña automáticamente sus credenciales serán capturadas por el ciberdelincuente, luego de haber realizado dicho acto será redireccionado hacia el sitio web oficial de Facebook.



Fuente: Juana Tobar

Análisis: Como vemos se capturaron las credenciales de la víctima, esta herramienta en la Ingeniería social suele ser utilizada por los ciberdelincuentes para generar cualquier ataque y así obtener beneficios.