Ingeniería Social y Phishing: Simulación de Ataques con SEToolkit y Zphisher

Introducción

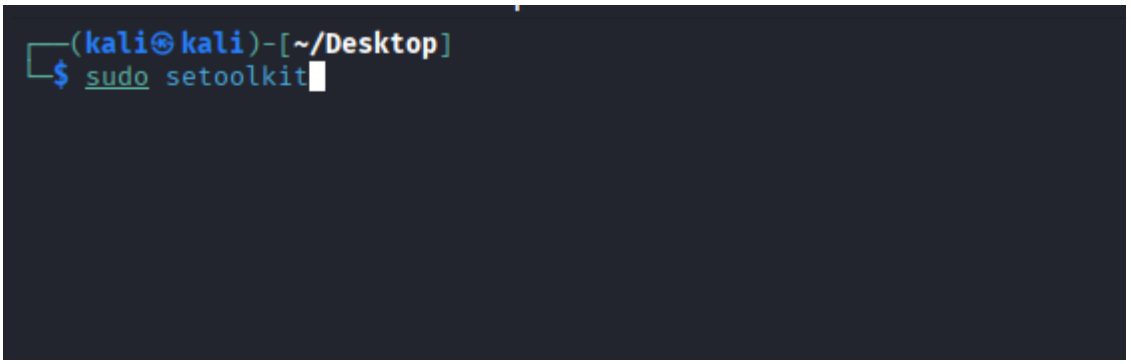
La **Ingeniería Social** es reconocida universalmente como el vector de ataque más eficaz y menos tecnológico, explotando el factor humano para obtener acceso a sistemas e información sensible. El objetivo de esta guía práctica es desmitificar y exponer las técnicas más comunes de este campo, centrándonos específicamente en la simulación de ataques de **Phishing de Recolección de Credenciales**.

Este documento sirve como una herramienta de aprendizaje controlado, detallando el uso de plataformas estándar de la industria como **SEToolkit (The Social-Engineer Toolkit)** y **Zphisher**. Al comprender paso a paso cómo se construyen estos ataques, desde la clonación de páginas de *login* hasta la captura de datos, buscamos proveer a los profesionales de seguridad el conocimiento necesario para **evaluar de manera proactiva** la resistencia de sus organizaciones, medir la **conciencia de sus usuarios** y, lo más importante, diseñar estrategias de mitigación y defensa que sean verdaderamente efectivas contra estas amenazas persistentes.

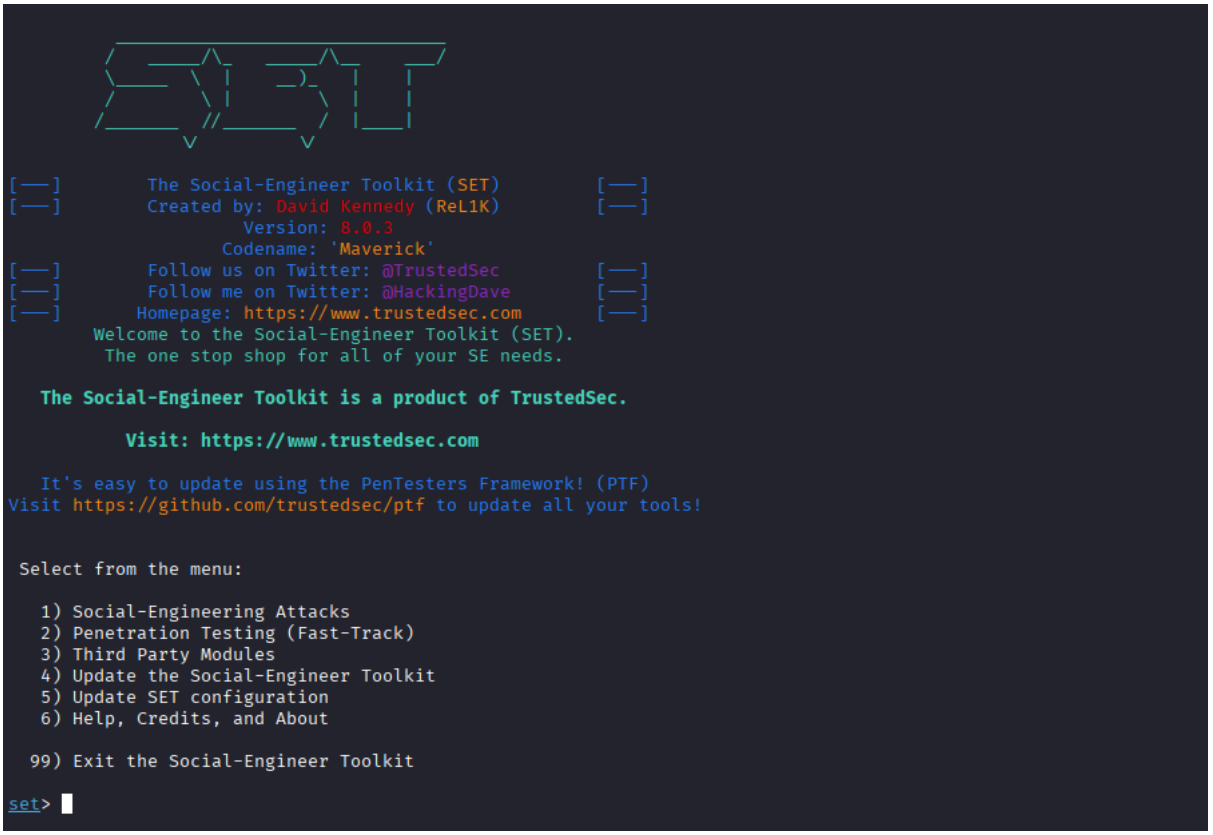
Este documento tiene como objetivo proporcionar una guía comprehensiva sobre dos de las herramientas más utilizadas en pruebas de seguridad ofensiva y concienciación sobre phishing: **The Social-Engineer Toolkit (SET) y Zphishe**r.

Realizaremos primero la exploración de la herramienta **Setoolkit** para el uso de táctica de phishing para la recolección de credenciales

para poder empezar a usar la herramienta abriremos una terminal y usaremos el siguiente comando
(‘ **sudo setoolkit** ’)

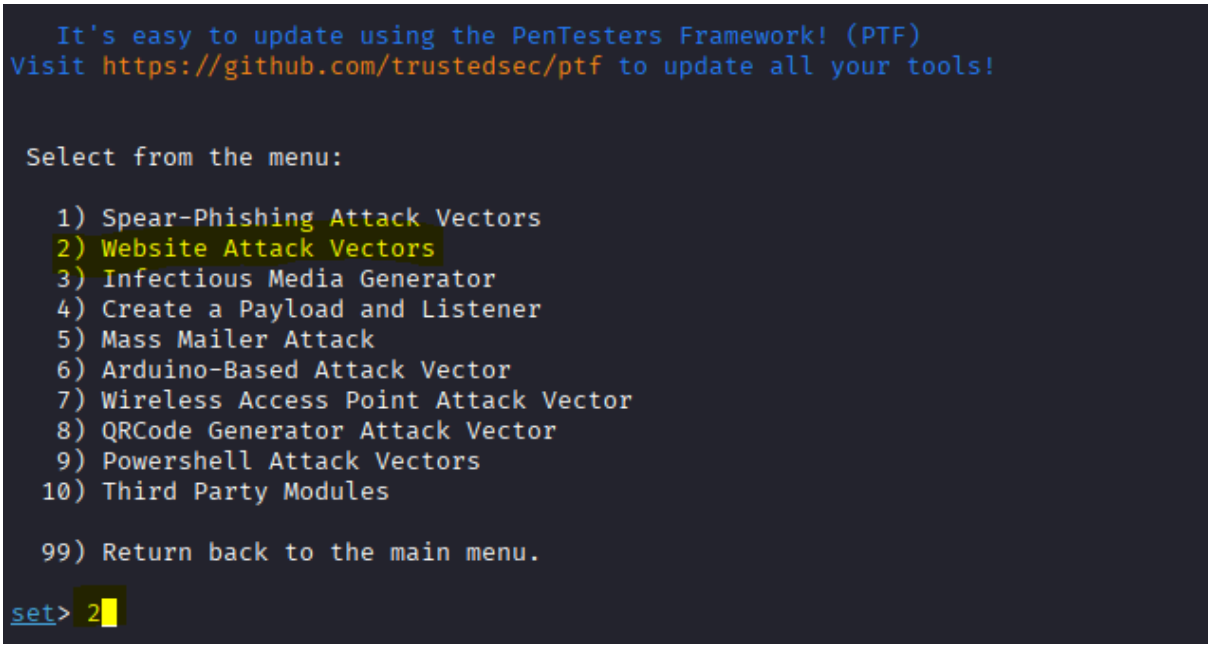


cuando se haya dado enter se creará un menú como el siguiente:

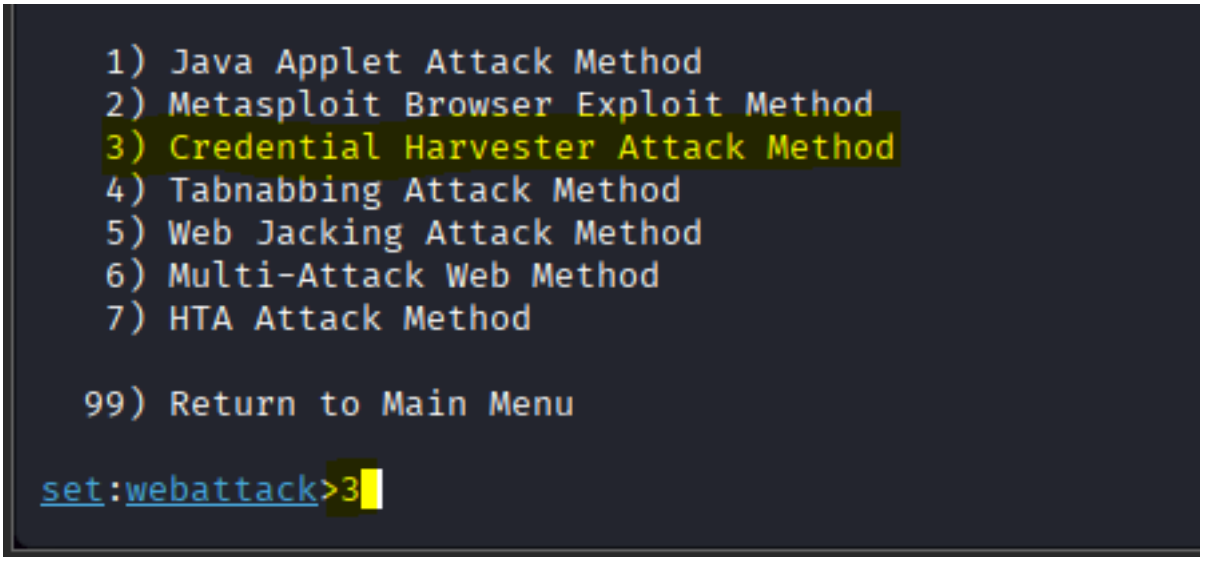


En esta práctica nos enfocaremos en el módulo **1) Social-Engineering Attacks** el cual nos ayudará para realizar el ataque se phishing y recolectar las contraseñas de nuestro objetivo

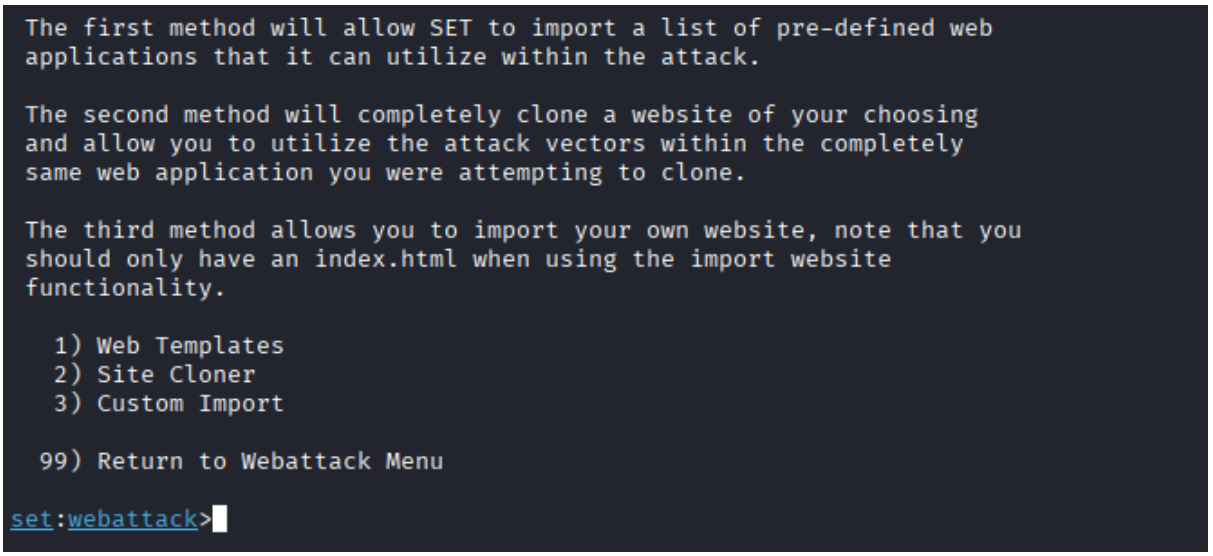
cuando hayamos seleccionado la opción 1 se nos desplegara el siguiente menú y usaremos la opción **2) Website Attack Vectors**



una vez mas se nos desplegara un menus de opciones y nos enfocaremos en la siguiente opción **3) Credential Harvester Attack Method**



después de realizar la selección de **Credential Harvester Attack Method** se despliega un menú donde nos preguntara si daemon realizar las siguientes opciones

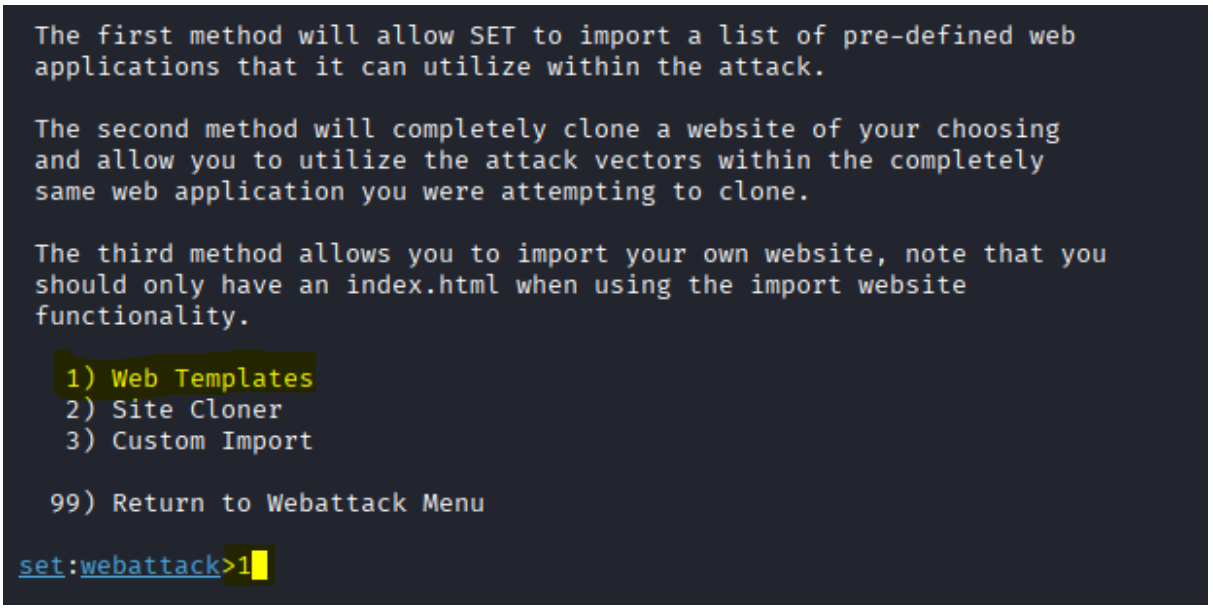


1) Web Templates
Plantillas predefinidas de sitios web legítimos (Facebook, Gmail, Twitter, etc.) listas para usar en pruebas de phishing controladas. SEToolkit genera automáticamente páginas de inicio de sesión falsas que simulan servicios reales.

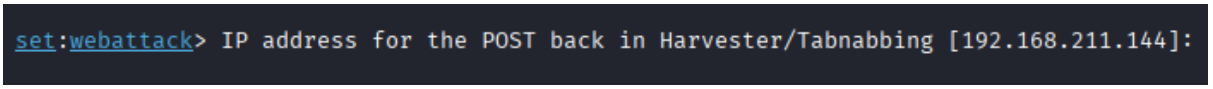
2) Site Cloner
Herramienta que permite clonar cualquier sitio web en tiempo real. Captura la estructura y apariencia de un sitio legítimo ingresando su URL, replicando incluso formularios de login para análisis de seguridad.

3) Custom Import
Opción avanzada que permite importar plantillas personalizadas o páginas web desarrolladas externamente. Ideal cuando se requieren diseños específicos no incluidos en las plantillas predeterminadas.

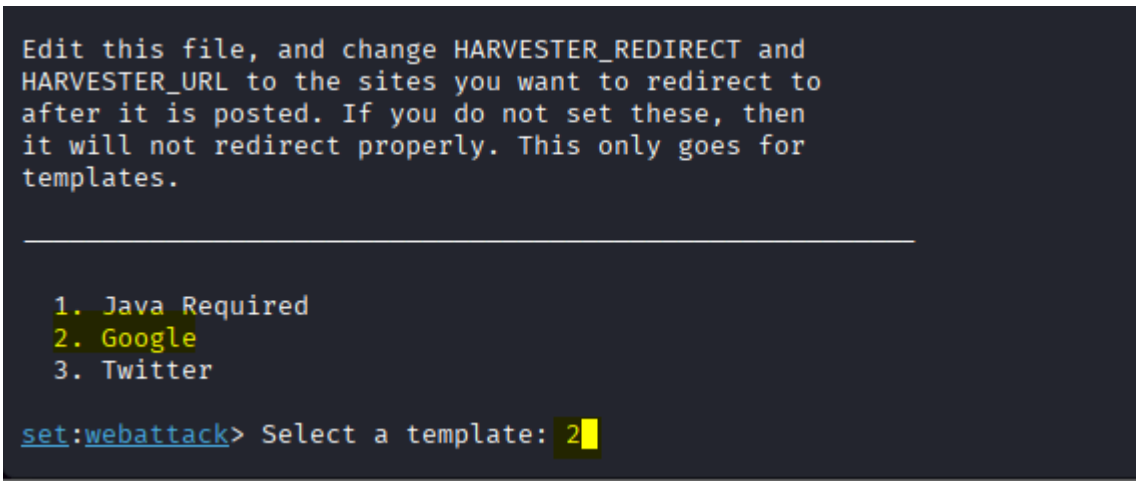
Para fines de la práctica usaremos la opciones número **1) Web Templates**



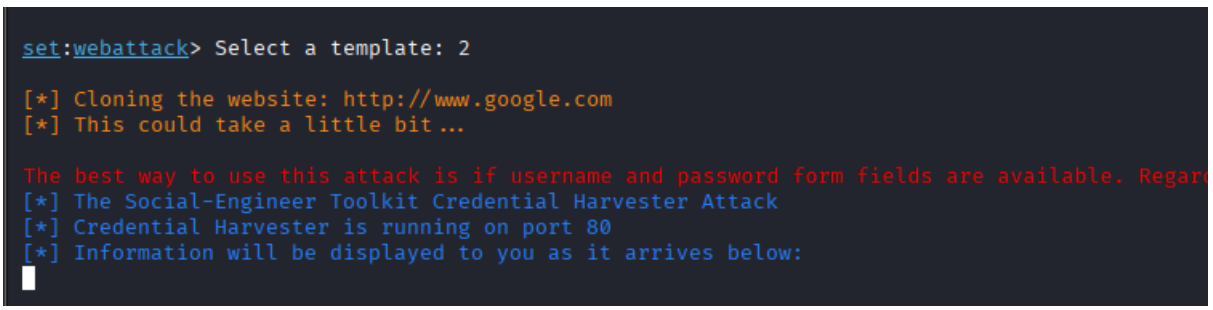
una vez selecciones la opción 1 se desplegará una serie de preguntas como las siguientes: nos dices si todos los metodos POST que se realicen cuando captura la credenciales en enviaran a la ip **192.168.211.144** que la ip de la maquina kali host para ello solo daremos **ENTER**



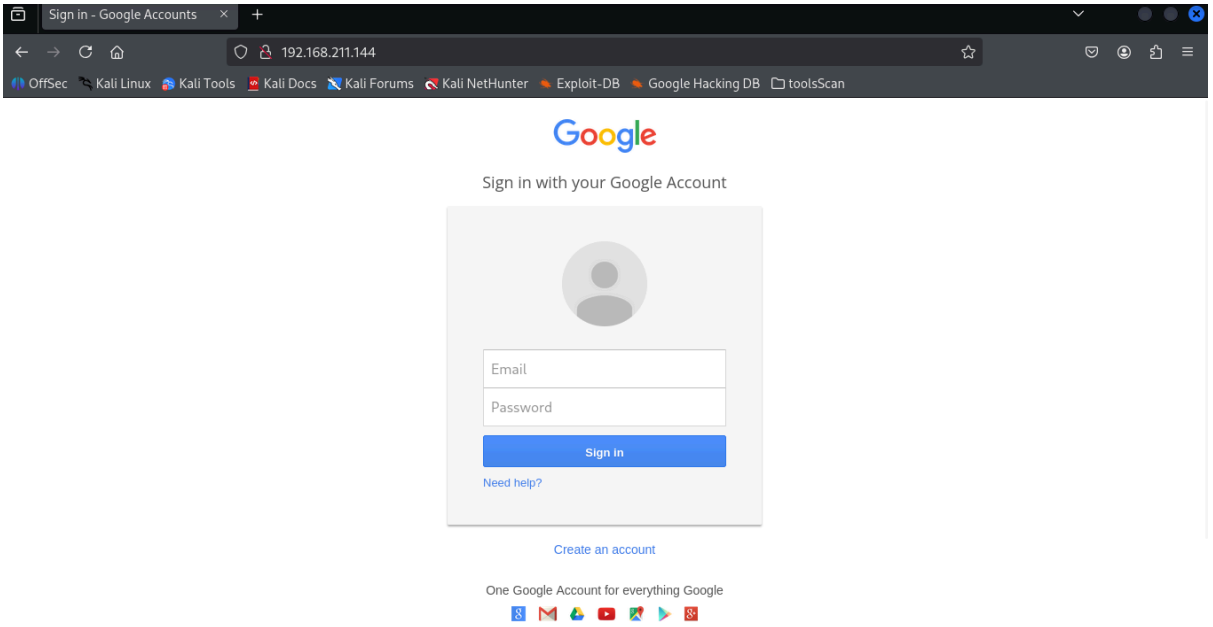
en el siguiente menú configuraremos nuestra plantilla



una vez seleccionada vemos como realiza la configuración de la template del login de google.com y que estara alojado en nuestra maquina host en el puerto 80

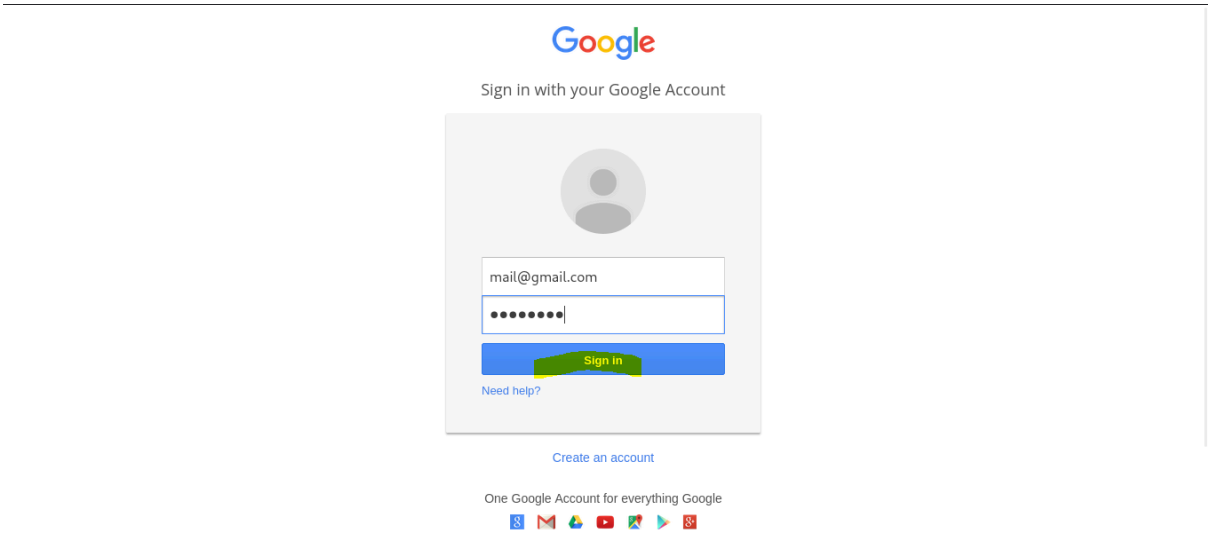


abrimos una ventana en el navegador y tecleamos la ip de nuestra máquina host en mi caso en la ip **192.168.211.144**



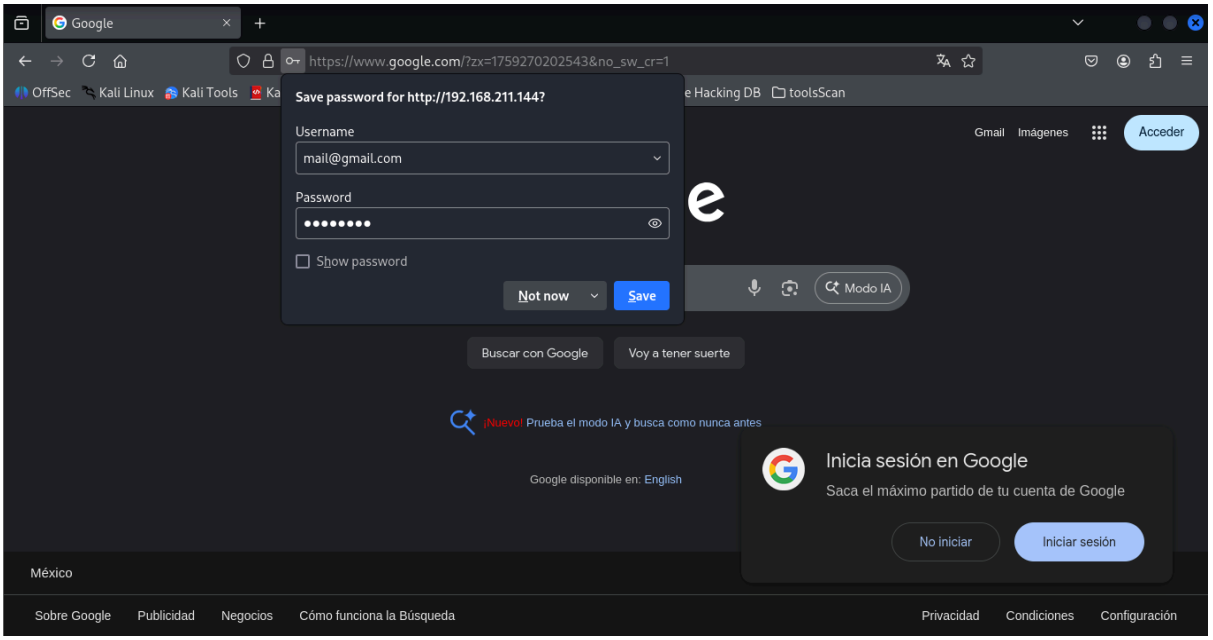
en la imagen anterior podemos ver como se ha realizado el despliegue de nuestra template maliciosa para la captura de credenciales de un objetivo

ahora procederemos a realizar la simulación de un login con una cuenta



damos al botón de login y veamos que procede

Nos realiza una redirección el buscador de google



revisamos nuestra herramienta se **SetoolKit** podemos ver que a capturado la credenciales que hemos puesto en el login de google también cabe destacar de que es posible que haya hecho la captura de cookies para el bypass de MFA
PARAM:continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX

POSSIBLE USERNAME FIELD FOUND: Email=**mail@gmail.com**
POSSIBLE PASSWORD FIELD FOUND: Passwd=**password**

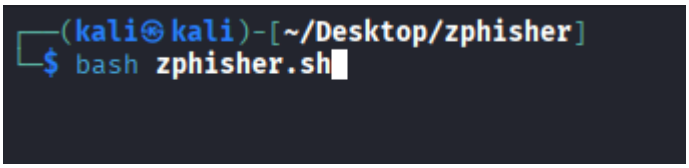
```
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

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:
192.168.211.144 - - [30/Sep/2025 18:06:52] "GET / HTTP/1.1" 200 -
192.168.211.144 - - [30/Sep/2025 18:06:53] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=mail@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=password
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

La práctica realizada con **SEToolkit (The Social-Engineer Toolkit)** ha demostrado la alta eficacia y la relativa simplicidad con la que un atacante puede ejecutar un ataque de **Phishing de Recolección de Credenciales**. La clonación exitosa de una plantilla de login legítima (como la de Google) subraya la importancia de la **concienciación del usuario** como primera línea de defensa.

Avanzando en nuestra comprensión de las técnicas de ingeniería social, a continuación explicaremos la herramienta **Zphisher**.
link del repositorio: https://github.com/htr-tech/zphisher

Mientras que SEToolkit es una suite amplia, Zphisher se enfoca específicamente en la creación de páginas de *phishing* con una interfaz más moderna y plantillas actualizadas, a menudo utilizadas para simular ataques en plataformas de redes sociales.

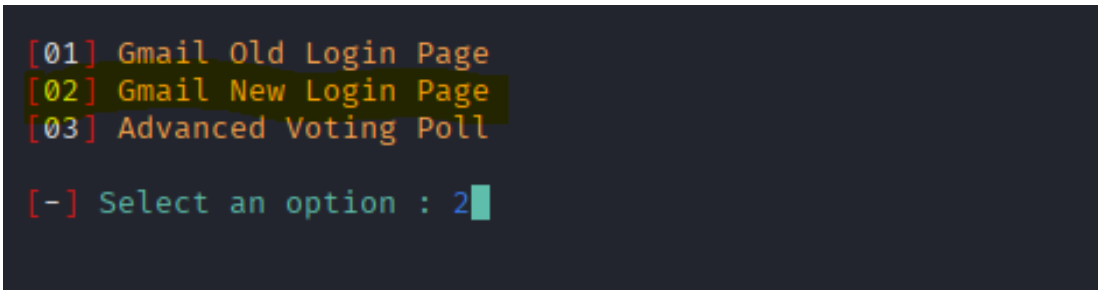
para poder dar inicio a zphisher realizamos el script de bash de la herramienta de la siguiente manera (‘ **bash zphisher.sh** ’)



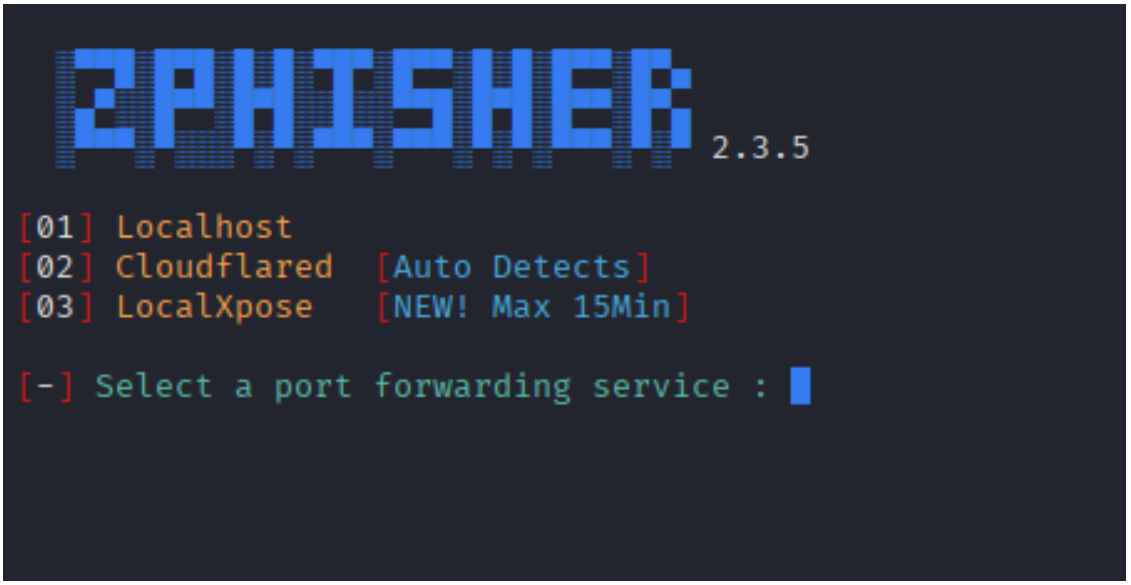
una vez lanzado el script de bash se nos desplegará un menú de la siguiente manera donde tendremos múltiples templates para la recolección de credenciales

para la demostración usaremos la opción de google al igual que la herramienta pasada **setoolkit**

al seleccionar la opción 3 se nos desplegará un menú como el siguiente en el cual usaremos la plantilla más nueva de google osea la opcion 2



una vez seleccionada la plantilla se nos despliega el siguiente menú donde nos dice que servicio desea tener para desplegar la plantilla



[01] Localhost
Hosting local en tu propia máquina (127.0.0.1 o localhost)

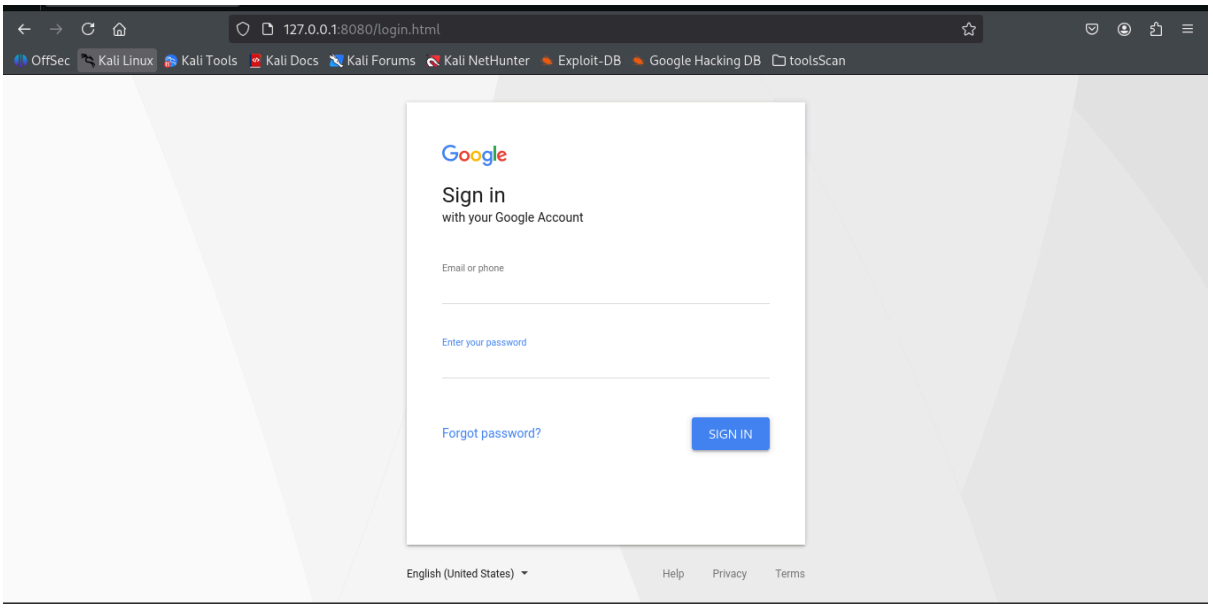
[02] Cloudflared
Túnel seguro mediante Cloudflare Tunnel

[03] LocalXpose
Servicio nuevo con límite de 15 minutos
Exposición temporal perfecta para demostraciones rápidas

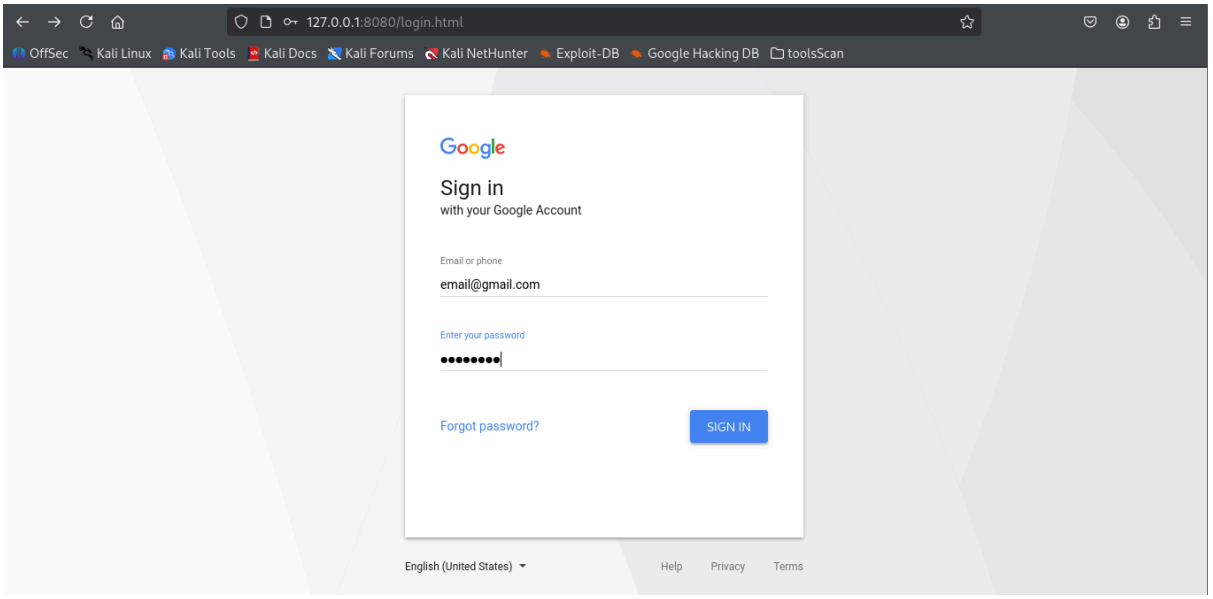
para la demostración usaremos la opción 1 que sería en nuestro localhost

una vez hayamos hecho las configuraciones anteriores podemos ver que la herramienta ha realizado las configuraciones adecuadas para el despliegue de la template

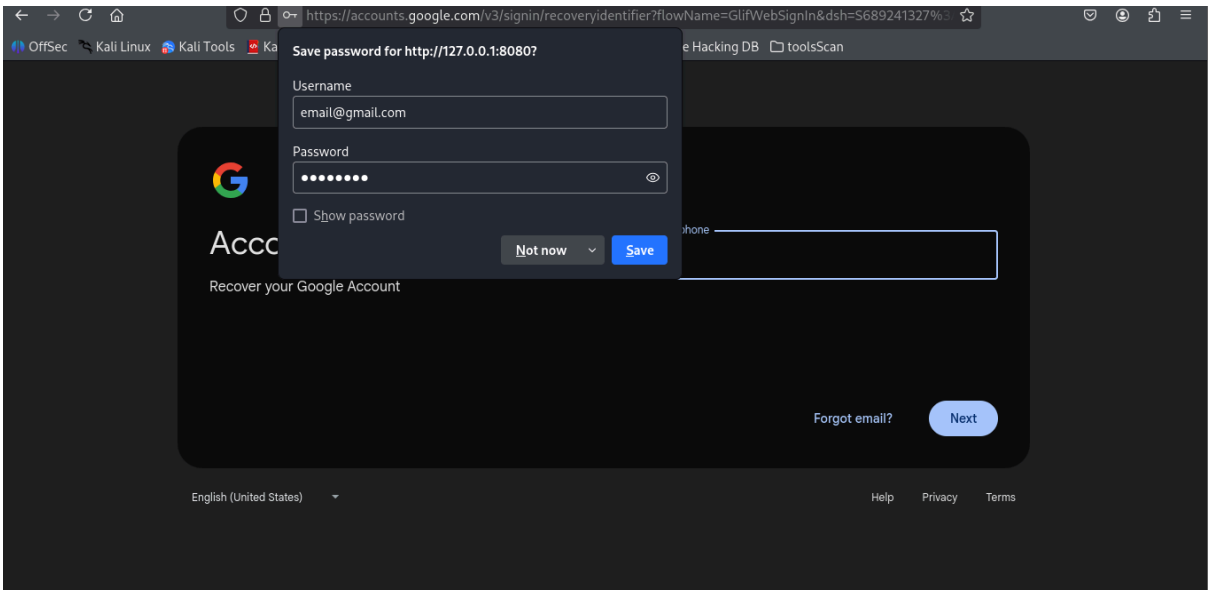
copiaremos y pegaremos la url que nos da en el navegador http://127.0.0.1:8080
para verificar que todo se haya desplegado con éxito



en efecto podemos ver que tenemos una template para poder hacer la prueba realizamos login con datos no válidos



al dar login nos redirecciona a lo siguiente



pero en nuestra herramienta podemos ver que hemos realizado la recolección de las credenciales correctamente

Hasta este punto damos por terminado la sección de Zphisher, una herramienta que nos ha permitido observar de cerca la **eficiencia y el enfoque** de las técnicas de *phishing* más recientes. A través de su interfaz sencilla y sus plantillas actualizadas, comprendimos la facilidad con la que un atacante puede crear campañas convincentes, especialmente utilizando métodos avanzados de **suplantación de URL**

Conclusión

Tras haber analizado y puesto en práctica las metodologías ofensivas detrás de herramientas como SEToolkit y Zphisher, la conclusión fundamental es ineludible: la **vulnerabilidad humana** sigue siendo la puerta de entrada más explotada en la ciberseguridad. La facilidad y rapidez con la que se pueden desplegar *scripts* de *phishing* altamente convincentes subraya que la dependencia exclusiva de la seguridad tecnológica es insuficiente.

El conocimiento adquirido debe ser el cimiento para un enfoque de seguridad proactivo y centrado en el ser humano. Esto implica:

1. **Priorizar la Autenticación Multifactor (MFA)** para invalidar el simple robo de credenciales.
2. **Invertir continuamente en la capacitación del personal**, enfocándose en la identificación de la **URL real** y los indicadores de compromiso de un enlace.
3. **Realizar ejercicios de *phishing* periódicos** y éticos para medir la madurez defensiva de la organización.

La **Ingeniería Social** es una amenaza constante que exige una respuesta adaptable e integral. Al entender al adversario, aseguramos un perímetro de defensa que es tanto tecnológico como humano.