

CURSO *ONLINE* DE CIBERSEGURIDAD__

Taller 5

Unidad 3. Aspectos avanzados de ciberseguridad






VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

 **incibe**
INSTITUTO NACIONAL DE CIBERSEGURIDAD



Contenidos

	EL ATAQUE <i>PHISHING</i>	3
	ENUNCIADO EJERCICIO PRÁCTICO 5: ATAQUE DE <i>PHISHING</i>	58
	SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE <i>PHISHING</i>	60

Duración total del taller: 50 minutos.

1000 JOURNAL OF POST KEYNESIAN ECONOMICS

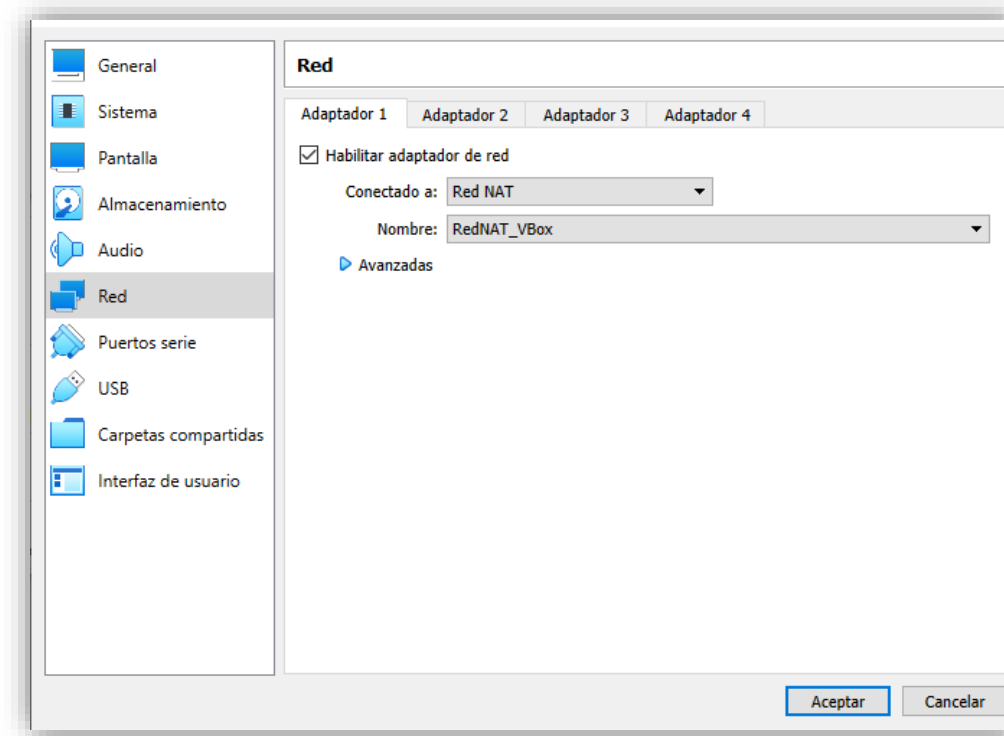
1

1 EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

Para realizar un ataque *phishing*, primero aprenderás a utilizar la herramienta Gophish.

- En la configuración previa de GoPhish, es necesario colocar el adaptador de red de la máquina virtual Kali en modo «*Bridge*» o «Punto».

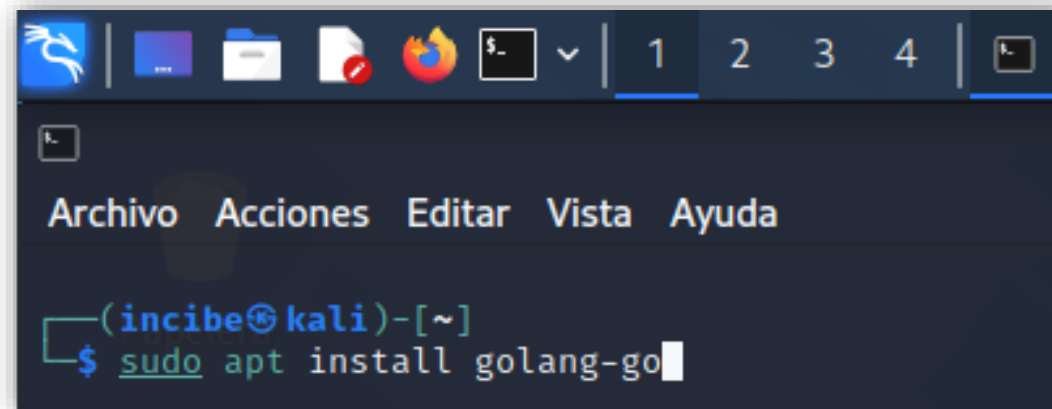


Selecciona la opción
«*Bridge*» o
«Punto» y pulsa
Aceptar».

1 EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- A continuación, deberás instalar Golang. Golang es un lenguaje de programación concurrente inspirado en «C» y sobre el que está desarrollado GoPhish.
 - Para ello, en la máquina Kali Linux abrirás una nueva terminal. Ejecuta el comando «**sudo apt install golang-go**» y haz clic en «Aceptar» en el aviso de espacio de disco necesario.



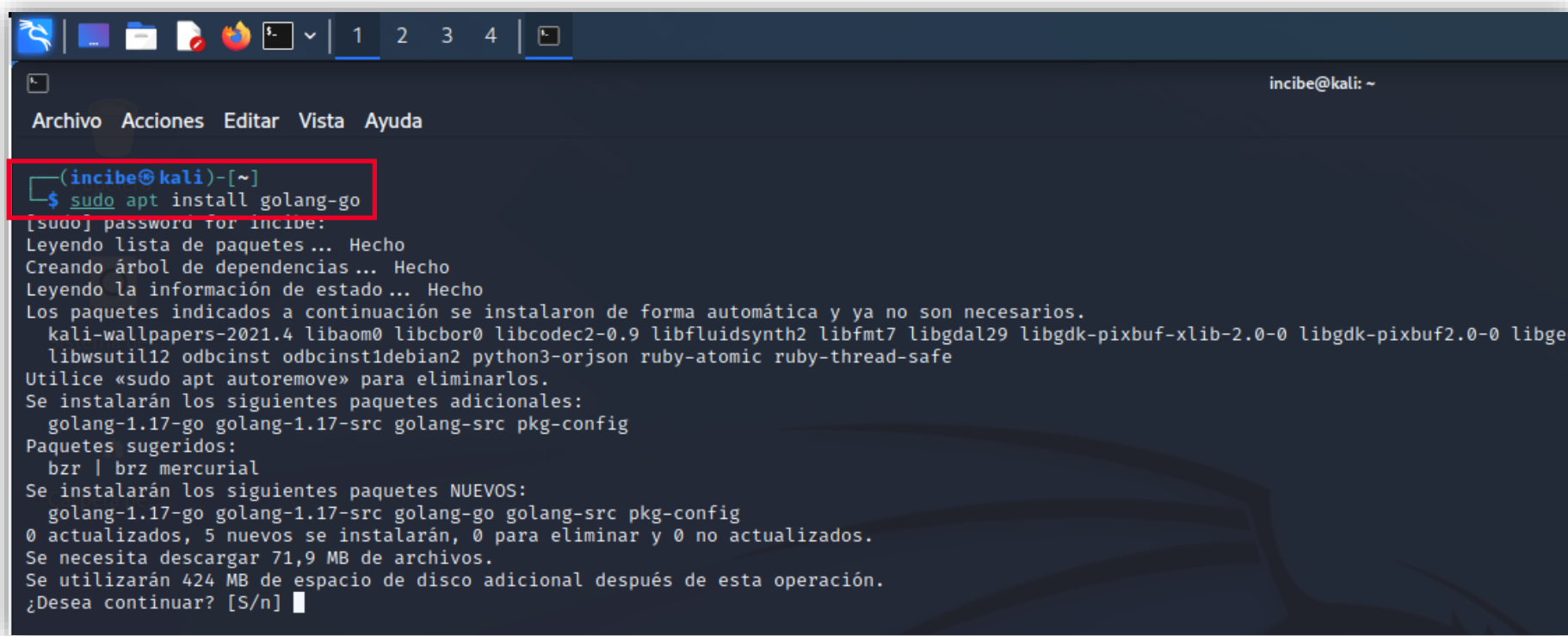
The image shows a terminal window on a Kali Linux desktop. The window has a dark theme and a menu bar with options: Archivo, Acciones, Editar, Vista, Ayuda. The prompt is (incibe@kali)-[~]. The command being typed is `$ sudo apt install golang-go`.

Ilustración 2: Ejecución del comando «sudo apt install golang-go».

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Pulsa «Enter» o teclea la letra «S» + «Enter».



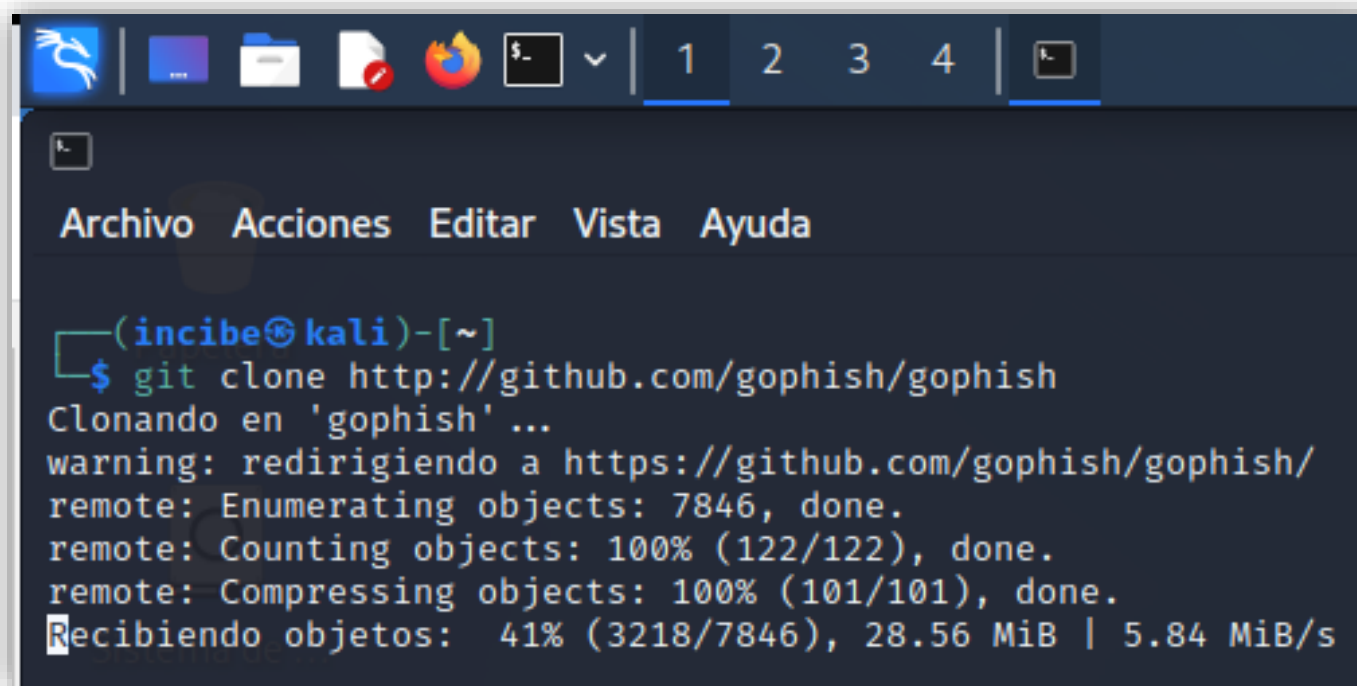
```
(incibe@kali)-[~]  
$ sudo apt install golang-go  
[sudo] password for incibe:  
Leyendo lista de paquetes ... Hecho  
Creando árbol de dependencias ... Hecho  
Leyendo la información de estado ... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.  
kali-wallpapers-2021.4 libaom0 libcbor0 libcodec2-0.9 libfluidsynth2 libfmt7 libgdal29 libgdk-pixbuf-xlib-2.0-0 libgdk-pixbuf2.0-0 libgeoclue-2.0-0  
libgsf-1.14-0 libgsf-1.14-dev libgsf-1.14-doc libgsf-1.14-glib libgsf-1.14-gtk libgsf-1.14-qt5 libgsf-1.14-webkit libgsf-1.14-xml libgsf-1.14-xml-glib libgsf-1.14-xml-qt5  
libgsf-1.14-xml-webkit libgsf-1.14-xml-webkit-glib libgsf-1.14-xml-webkit-qt5 libgsf-1.14-xml-webkit-xml-glib libgsf-1.14-xml-webkit-xml-qt5  
libgsf-1.14-xml-webkit-xml-qt5-xml-glib libgsf-1.14-xml-webkit-xml-qt5-xml-qt5  
Utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes adicionales:  
golang-1.17-go golang-1.17-src golang-src pkg-config  
Paquetes sugeridos:  
bzip2 libbz2-1.0 libbz2-dev libbz2-doc  
Se instalarán los siguientes paquetes NUEVOS:  
golang-1.17-go golang-1.17-src golang-go golang-src pkg-config  
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
Se necesita descargar 71,9 MB de archivos.  
Se utilizarán 424 MB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n]
```

Ilustración 3: «Enter» o letra «S» + «Enter».

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Después, clona el [código fuente de GoPhish](https://github.com/gophish/gophish) con el comando: «**git clone**» de forma que la instrucción quede «**git clone http://github.com/gophish/gophish**»



```
(incibe@kali)-[~]
$ git clone http://github.com/gophish/gophish
Clonando en 'gophish' ...
warning: redirigiendo a https://github.com/gophish/gophish/
remote: Enumerating objects: 7846, done.
remote: Counting objects: 100% (122/122), done.
remote: Compressing objects: 100% (101/101), done.
Recibiendo objetos: 41% (3218/7846), 28.56 MiB | 5.84 MiB/s
```

Ilustración 4: Código fuente de GoPhish a través de la ejecución del comando: «git clone».

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Entra en el nuevo directorio «**gophish**» con el comando «**cd /gophish**» y compila los códigos con el comando «**go build**», esto es, compilar el proceso de traducción del código fuente que se ha clonado previamente.

Ilustración 5: Directorio «gophish» a través del comando «cd /gophish» y compilación de los códigos «cd /gophish» y «go build».

```
(incibe@kali)~[/gophish]
$ go build
go: downloading gopkg.in/alecthomas/kingpin.v2 v2.2.6
go: downloading github.com/emersion/go-imap v1.0.4
go: downloading github.com/emersion/go-message v0.12.0
go: downloading github.com/jordan-wright/email v4.0.1-0.20200824153738-3f5bafa1cd84+incompatible
go: downloading github.com/sirupsen/logrus v1.4.2
go: downloading github.com/gorilla/csrf v1.6.2
go: downloading github.com/gorilla/securecookie v1.1.1
go: downloading github.com/gorilla/sessions v1.2.0
go: downloading github.com/NYTimes/gziphandler v1.1.1
go: downloading github.com/gorilla/handlers v1.4.2
go: downloading github.com/gorilla/mux v1.7.3
go: downloading github.com/jordan-wright/unindexed v0.0.0-20181209214434-78fa79113c0f
go: downloading bitbucket.org/liamstask/goose v0.0.0-20150115234039-8488cc47d90c
go: downloading github.com/PuerkitoBio/goquery v1.5.0
go: downloading github.com/go-sql-driver/mysql v1.5.0
go: downloading github.com/gophish/gomail v0.0.0-20200818021916-1f6d0dfd512e
go: downloading github.com/jinzhu/gorm v1.9.12
go: downloading github.com/mattn/go-sqlite3 v2.0.3+incompatible
go: downloading github.com/oschwald/maxminddb-golang v1.6.0
go: downloading github.com/alecthomas/template v0.0.0-20190718012654-fb15b899a751
go: downloading github.com/alecthomas/units v0.0.0-20190924025748-f65c72e2690d
go: downloading golang.org/x/text v0.3.2
go: downloading github.com/emersion/go-sasl v0.0.0-20191210011802-430746ea8b9b
go: downloading golang.org/x/sys v0.0.0-20191224085550-c709ea063b76
go: downloading github.com/pkg/errors v0.8.0
go: downloading golang.org/x/crypto v0.0.0-20200128174031-69ecbb4d6d5d
go: downloading golang.org/x/time v0.0.0-20200416051211-89c76fbc5d1
go: downloading github.com/kylelemons/go-gypsy v0.0.0-20160905020020-08cad365cd28
go: downloading github.com/lib/pq v1.1.1
go: downloading github.com/ziutek/mymysql v1.5.4
go: downloading github.com/andybalholm/cascadia v1.0.0
go: downloading golang.org/x/net v0.0.0-20190404232315-eb5bcb51f2a3
go: downloading github.com/jinzhu/inflection v1.0.0
go: downloading github.com/emersion/go-textwrapper v0.0.0-20160606182133-d0e65e56babe
```


1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Ahora, ejecuta GoPhish con el comando «./gophish». A continuación, aparecerán tres líneas en la pantalla:
 - El *login* provisional para acceder a la consola de GoPhish.
 - El puerto donde se está ejecutando el servidor *phishing* de GoPhish.
 - La dirección donde se está ejecutando el servidor de administración.

```
(incibe@kali)~/gophish
$ ./gophish
time="2022-02-19T20:27:51+01:00" level=warning msg="No contact address has been configured."
time="2022-02-19T20:27:51+01:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: migrating db environment 'production', current version: 0, target: 20201201000000
OK      20160118194630_init.sql
OK      20160131153104_0.1.2_add_event_details.sql
OK      20160211211220_0.1.2_add_ignore_cert_errors.sql
OK      20160217211342_0.1.2_create_from_col_results.sql
OK      20160225173824_0.1.2_capture_credentials.sql
OK      20160227180335_0.1.2_store-smtp-settings.sql
OK      20160317214457_0.2_redirect_url.sql
OK      20160605210903_0.2_campaign_scheduling.sql
OK      20170104220731_0.2_result_statuses.sql
OK      20170219122503_0.2.1_email_headers.sql
OK      20170827141312_0.4_utc_dates.sql
OK      20171027213457_0.4.1_maillogs.sql
OK      20171208201932_0.4.1_next_send_date.sql
OK      20180223101813_0.5.1_user_reporting.sql
OK      20180524203752_0.7.0_result_last_modified.sql
OK      20180527213648_0.7.0_store_email_request.sql
OK      20180830215615_0.7.0_send_by_date.sql
OK      20190105192341_0.8.0_rbac.sql
OK      20191104103306_0.9.0_create_webhooks.sql
OK      20200116000000_0.9.0_imap.sql
OK      20200619000000_0.11.0_password_policy.sql
OK      20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK      20200914000000_0.11.0_last_login.sql
OK      20201201000000_0.11.0_account_locked.sql
time="2022-02-19T20:27:51+01:00" level=info msg="Please login with the username admin and the password 3a96d1499f3fe3d7"
time="2022-02-19T20:27:51+01:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2022-02-19T20:27:51+01:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2022-02-19T20:27:51+01:00" level=info msg="Starting IMAP monitor manager"
time="2022-02-19T20:27:51+01:00" level=info msg="Starting new IMAP monitor for user admin"
time="2022-02-19T20:27:51+01:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2022-02-19T20:27:51+01:00" level=info msg="TLS Certificate Generation complete"
time="2022-02-19T20:27:51+01:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
```

Ilustración 6: Ejecución de GoPhish a través del comando «./gophish».

1 EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- En el navegador web, accede a la dirección del servidor de administración de GoPhish que, por defecto, es `http://127.0.0.1:3333`.
 - Una vez dentro, introduce el usuario y la contraseña que se te asignaron durante la instalación.

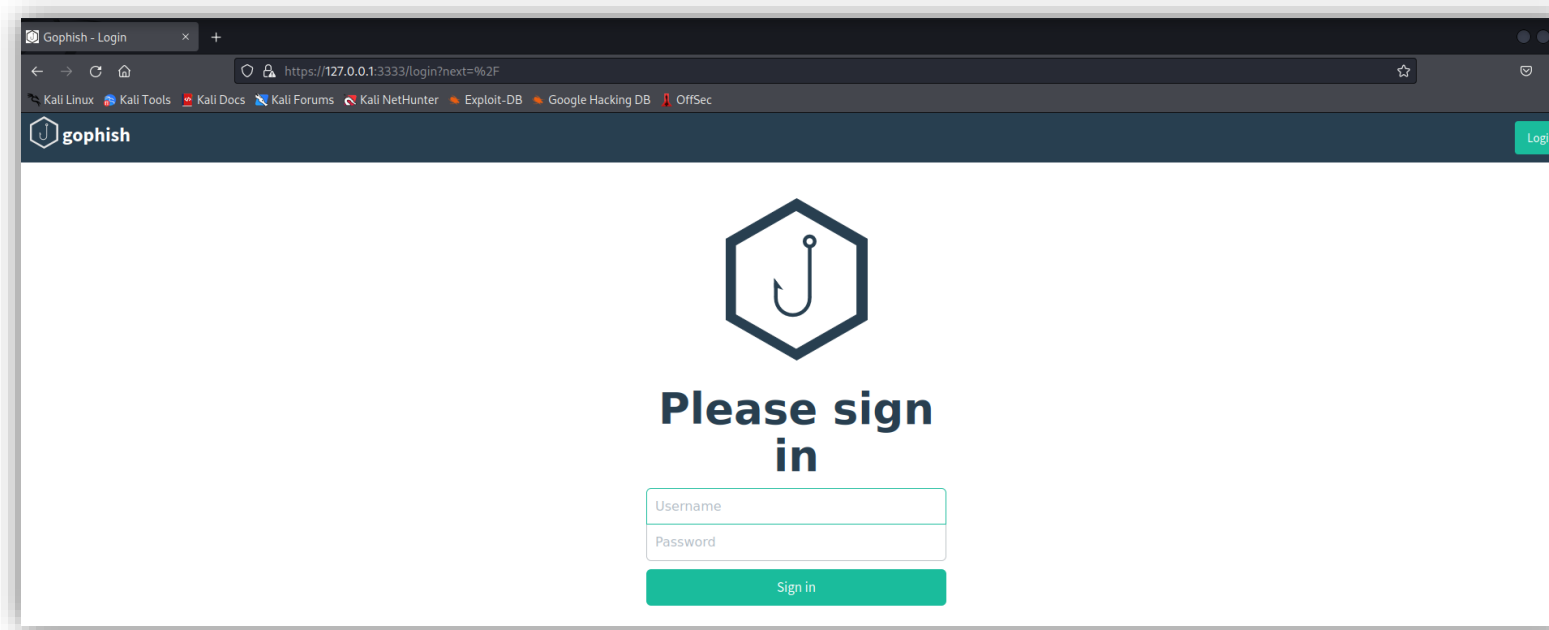


Ilustración 7:
Ejecución de GoPhish
a través del comando
«./gophish».

1 EL ATAQUE PHISHING

Instalación y configuración de GoPhish

- En el primer acceso o *login*, te pedirá resetear la contraseña por seguridad.

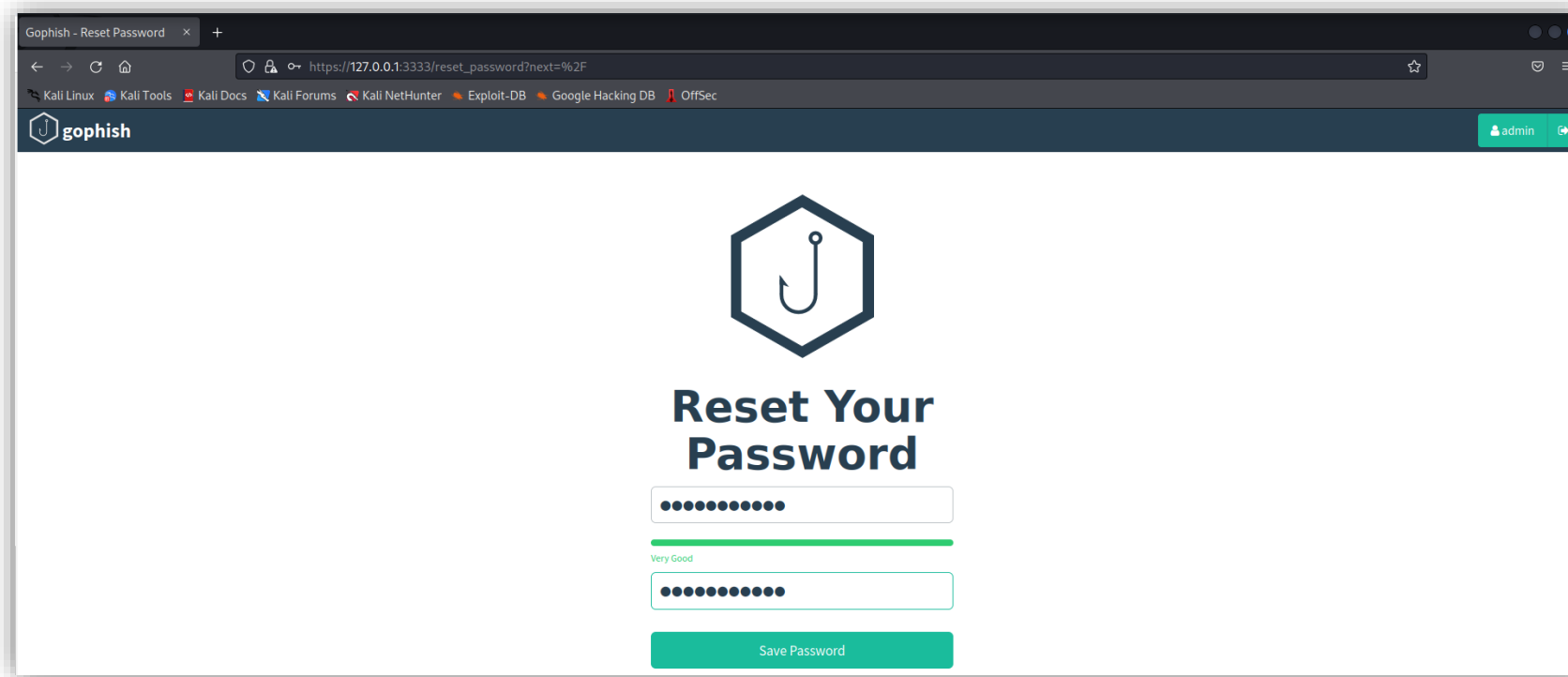


Ilustración 8: Pantalla de acceso o *login*. Reseteo de la contraseña por seguridad.

1 EL ATAQUE *PHISHING*

Instalación y configuración de GoPhish

- Una vez que has accedido, verás los siguientes menús principales de la herramienta, que debes conocer antes de a crear tu primer ataque de *phishing*.
 - **Dashboard:** en esta pantalla verás el resumen de todas tus campañas o ataques de *phishing*.

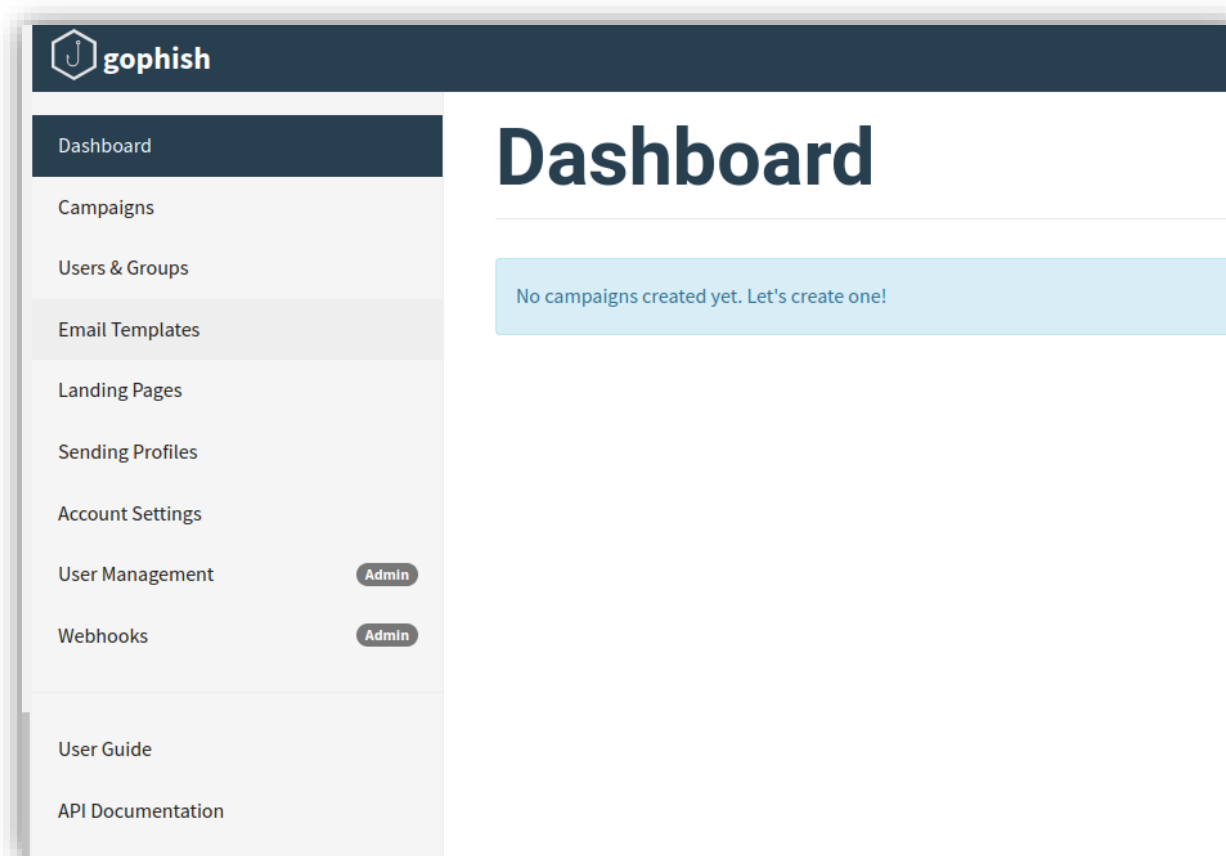


Ilustración 9: Pantalla de inicio *Dashboard*.

1 EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- **Campaigns:** Este es el menú desde el que crearemos las campañas y las distribuiremos a los diferentes objetivos.

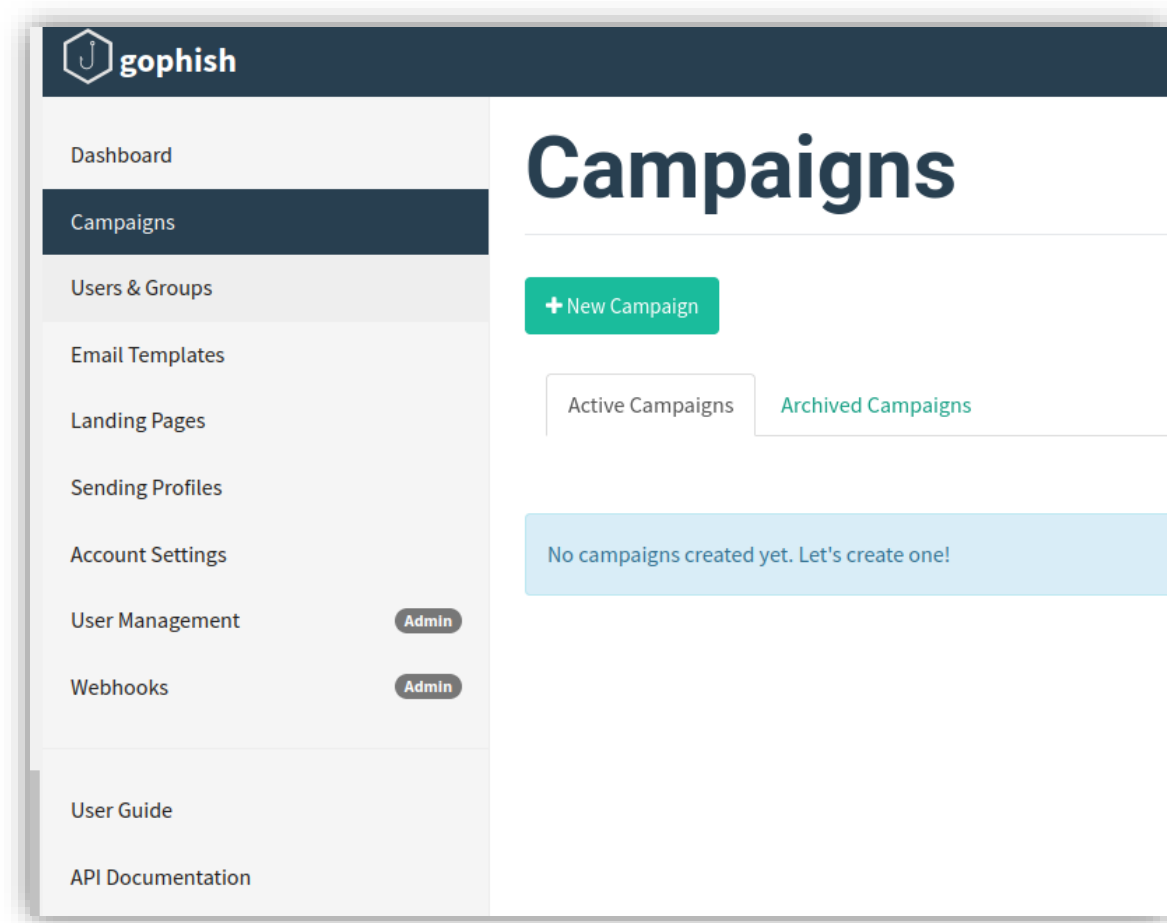


Ilustración 10: Pantalla de inicio *Campaigns*.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- **Users and Groups:** en una campaña de *phishing* se suelen diferenciar diferentes grupos de usuarios según, por ejemplo, del departamento, función, área, etc., lo que permite ver los resultados de manera más segregada y evita que se levanten sospechas entre compañeros. En este menú se configuran los diferentes grupos de usuarios objetivo.

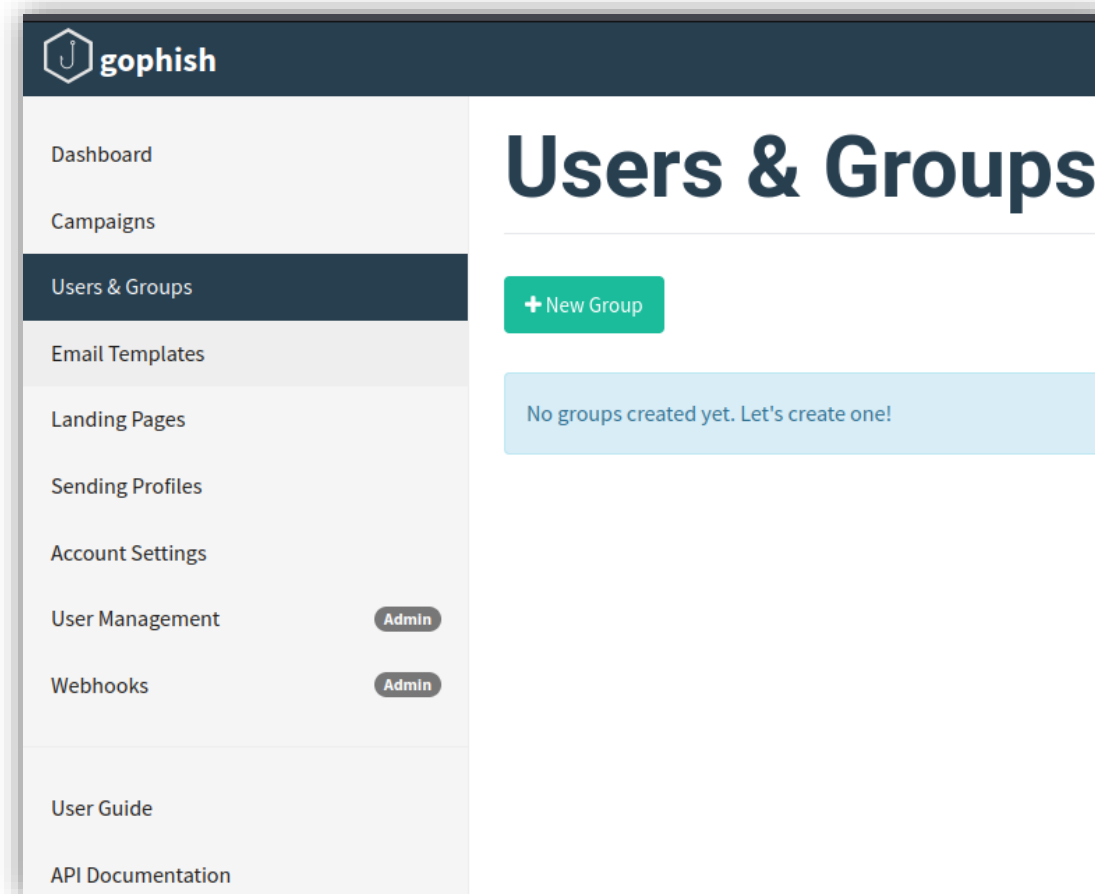


Ilustración 11: Pantalla de inicio *Users & Groups*.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- **Email Templates:** desde aquí se configura el correo electrónico que recibirá la víctima con diferentes encabezados, imágenes, enlaces, etc. Normalmente, este texto o estilo se acuerda con el cliente o se utiliza un correo electrónico legítimo de la persona o entidad que se suplanta para tomarlo como modelo y que sean muy similares para no levantar sospecha.

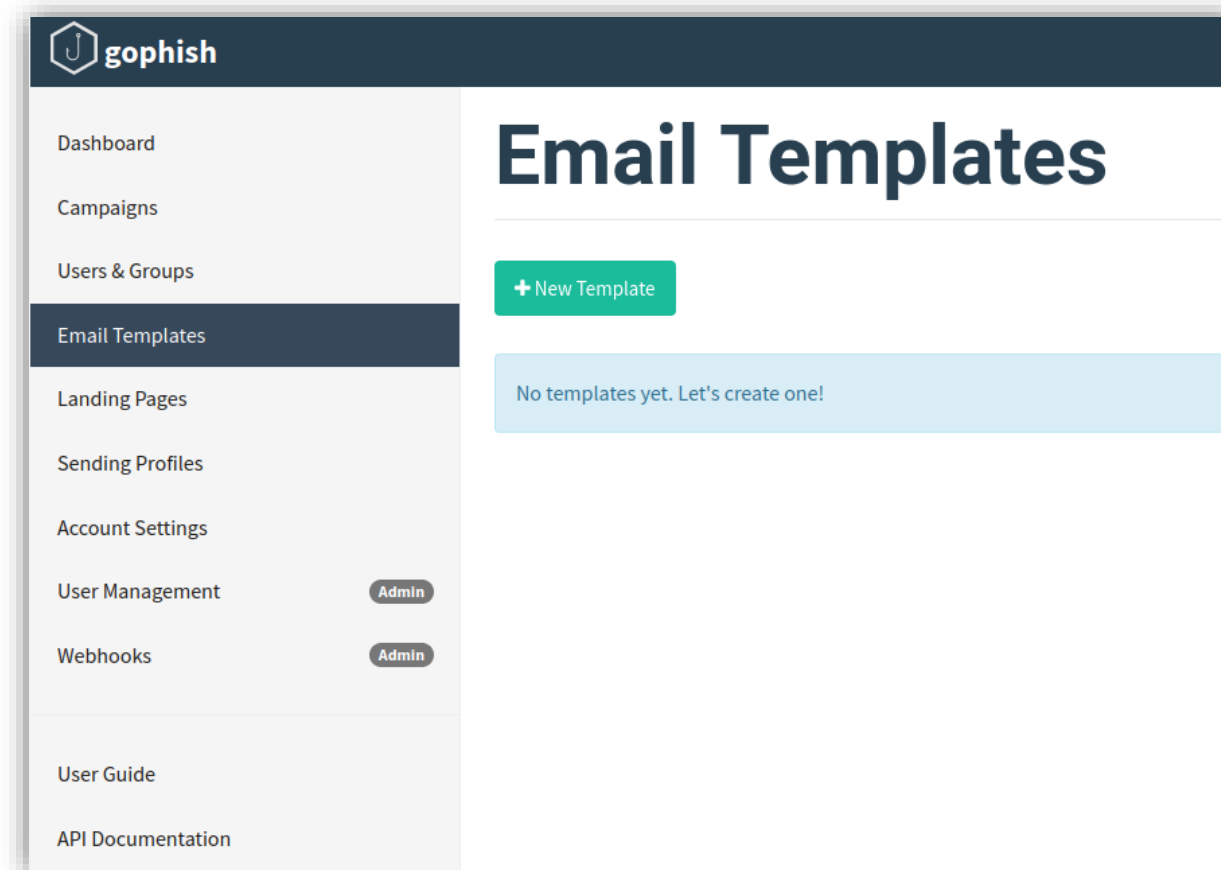


Ilustración 12: Pantalla de inicio *Email Templates*.

1 EL ATAQUE *PHISHING*

Instalación y configuración de GoPhish

- **Landing Pages:** para tu campaña de *phishing*, deberás tener una *landing page*, es decir, una página fraudulenta a la que redirige el enlace del correo electrónico que se envíe a las víctimas. Puede ser una página en la que se tengan que descargar un archivo malicioso o donde se soliciten datos confidenciales que acabarán bajo nuestro control. GoPhish permite diseñar una *landing page* desde cero o importar una página del sitio que se quiera suplantar.

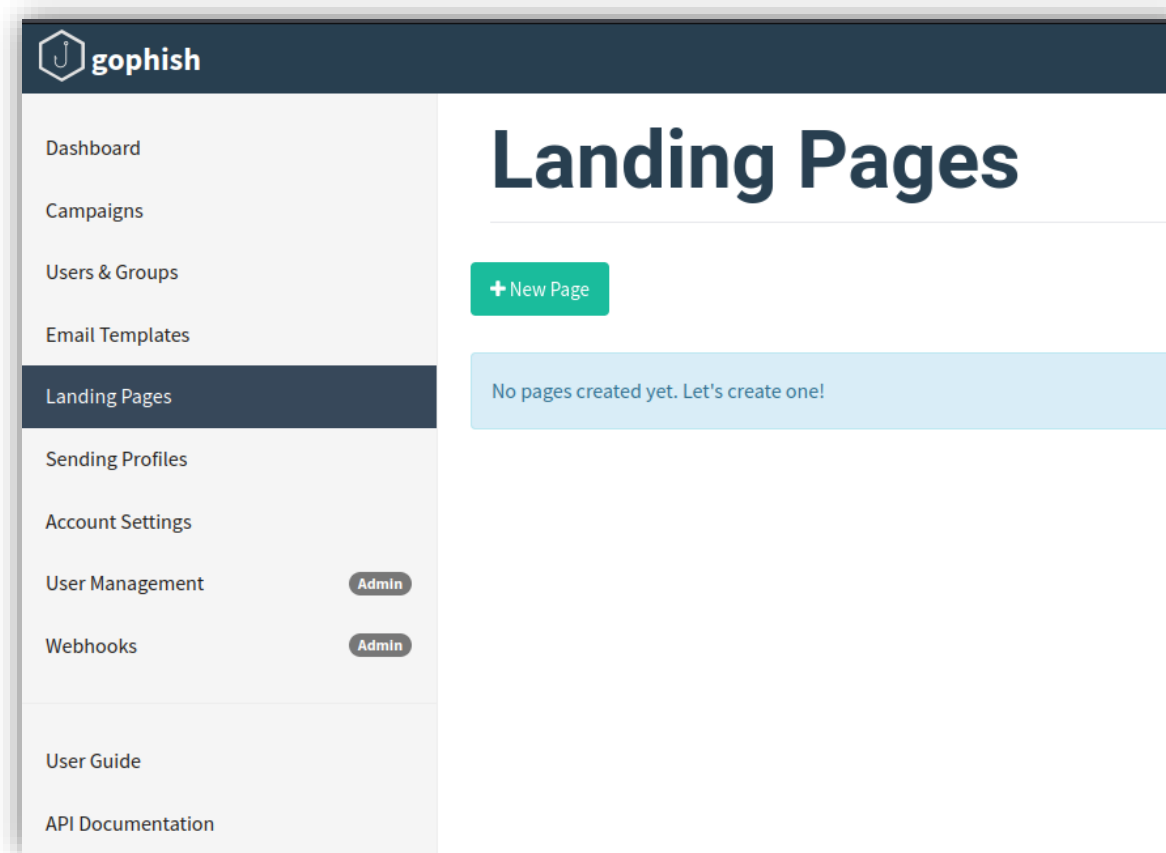


Ilustración 13: Pantalla de inicio *Landing Pages*.

1 EL ATAQUE *PHISHING*

Instalación y configuración de GoPhish

- ***Sending Profiles***: para cualquier campaña de *phishing* se necesita un servidor SMTP, que es el que se encargará de hacer de pasarela para distribuir los correos electrónicos. Los atacantes experimentados y minuciosos o las empresas de ciberseguridad implementan sus propios servidores SMTP con soluciones como PostFix. Esto les permite poder enviar los correos electrónicos con dominios personalizados y tener más probabilidades de éxito. Por ejemplo, en caso de querer suplantar la dirección de una compañía «AlertasCiber», posibles páginas falsas similares podrían ser: a1ertasCiber.es, AlertasC1ber.es, AlertasCiber.co, etc.

Sin embargo, los usuarios menos experimentados o que no están dispuestos a desplegar su propio servidor tienen la opción de usar los servidores SMTP de plataformas gratuitas.

EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

Cabe destacar que, usando una plataforma gratuita como SMTP, en la mayoría de los casos, se debe tener una cuenta propia en dicha plataforma. Los atacantes que usan este método crean cuentas específicas para estas campañas, por ejemplo, si se quisiese emplear Gmail como plataforma de SMTP gratuita, algunas de las posibles cuentas falsas podrían ser: empresa@gmail.com, alertas_empresa@gmail.com, etc. Otra opción es jugar con las cabeceras del correo añadiendo un correo electrónico personalizado en el texto del remitente que pretende engañar a la víctima, por ejemplo, «Alerta *empresa* < alertas@empresa.es > Enviado desde: alertas_empresa@gmail.com».

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

En este caso, usarás el SMTP de una cuenta de Gmail creada expresamente para este ejercicio práctico.

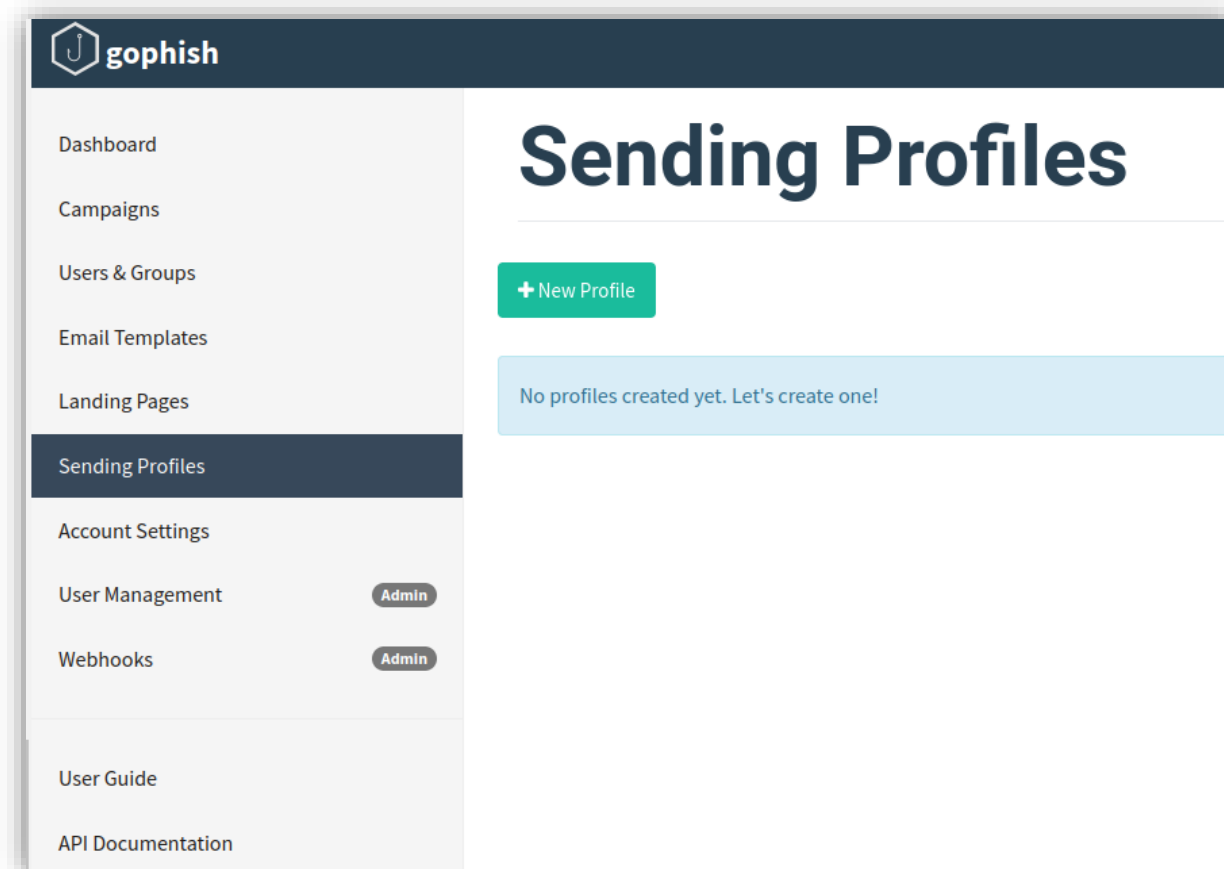


Ilustración 14: Pantalla de inicio *Sending Profiles*.

1 EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- **Account Settings:** puedes cambiar tu contraseña de usuario, configurar la interfaz y el sistema de envío de reporting si fuese necesario.

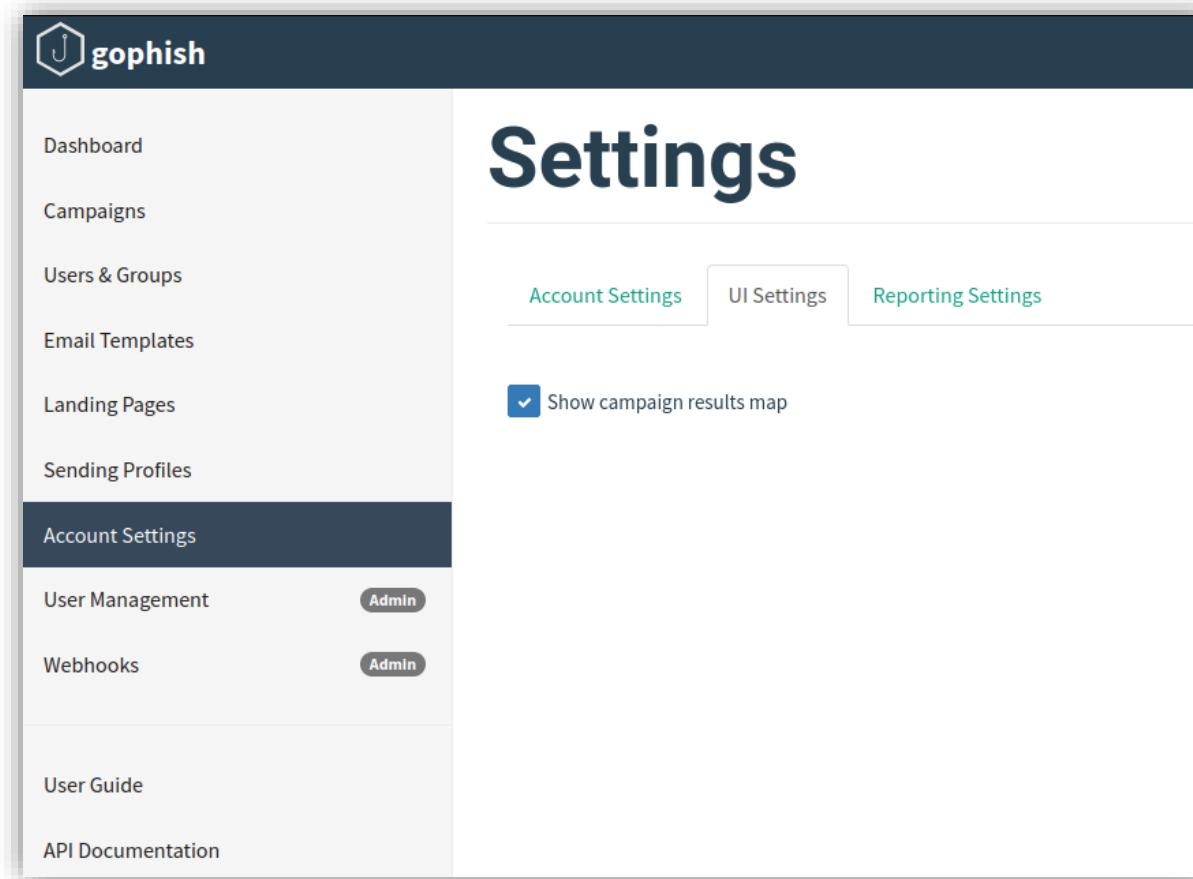


Ilustración 15: Pantalla de inicio *Settings*.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- **User Management:** se utiliza para gestionar los diferentes usuarios que usarán la plataforma de GoPhish.

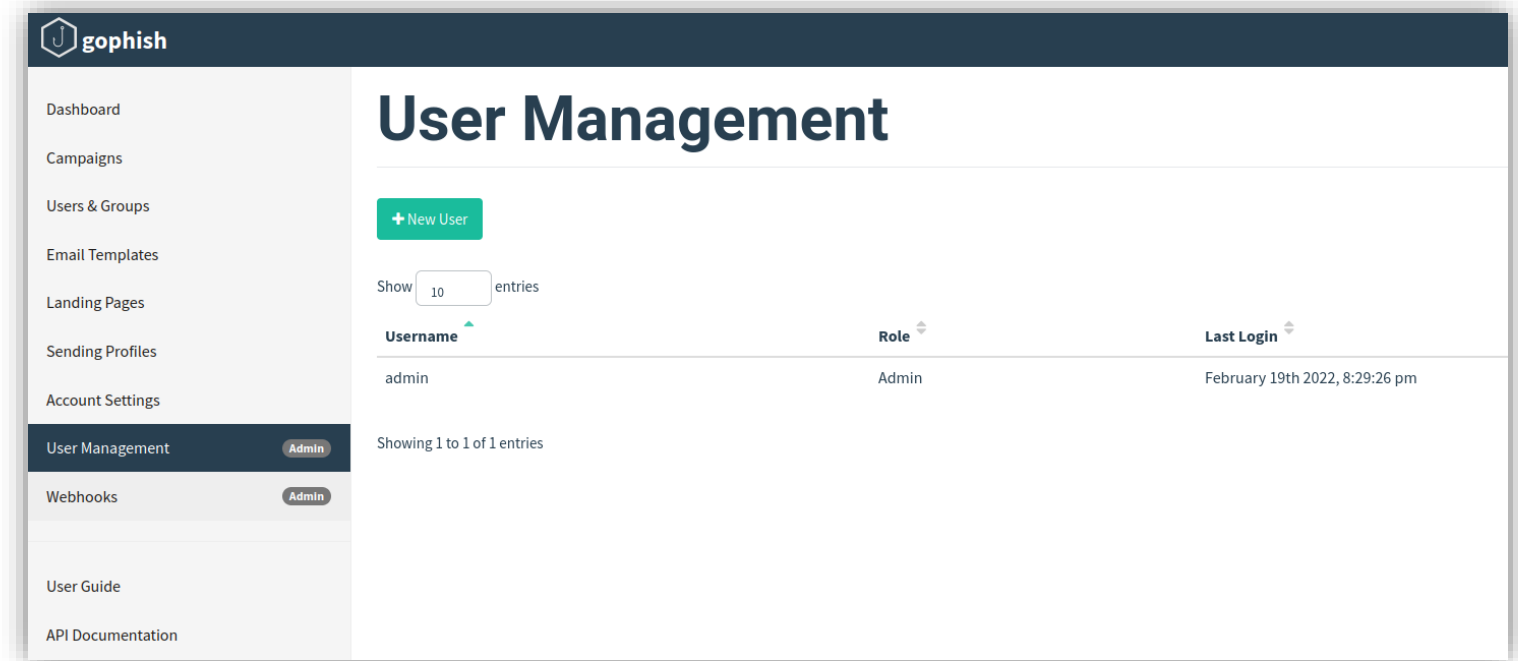


Ilustración 16: Pantalla de inicio *User Management*.

1 EL ATAQUE PHISHING

Instalación y configuración de GoPhish

- **Webhooks:** son sistemas de llamada entre aplicaciones para intercambiar información.

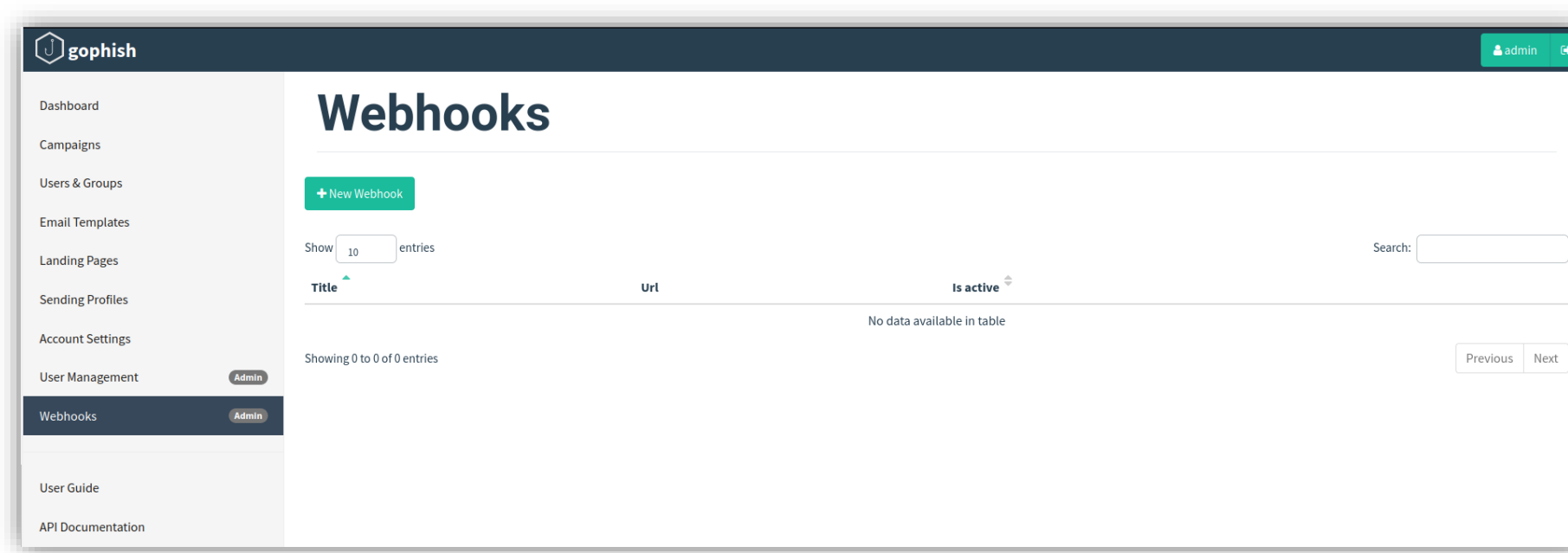


Ilustración 17: Pantalla de inicio *Webhooks*.

1 EL ATAQUE PHISHING

Instalación y configuración de GoPhish

- Para crear un perfil, deberás hacer clic en el menú lateral de «*Sending Profiles*».



Ilustración 18: Pantalla de inicio *Sending Profiles*: *New Sending Profile*.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- A continuación, cumplimenta los campos del formulario. Para poder enviar correos es necesario usar un servidor SMTP de una cuenta de correo existente. Esta puede ser nuestra cuenta corporativa, Gmail, Yahoo, etc. Por ejemplo, para usar un SMTP externo de una cuenta de Gmail, como *host* escribe **smtp.gmail.com:587** especificando, además, el usuario y contraseña de la cuenta. El campo «*From*», sin embargo, es personalizable.

New Sending Profile

Name:

Interface Type:

From:

Host:

Username:

Password:

☒ Ignore Certificate Errors ⓘ

Email Headers:

Header	Value
X-Custom-Header	{{.URL}}-gophish

[+ Add Custom Header](#)

Show entries Search:

No data available in table

Showing 0 to 0 of 0 entries

[Send Test Email](#) [Previous](#) [Next](#)

[Cancel](#) [Save Profile](#)

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

Ilustración 20: Campos cumplimentados del formulario *New Sending Profile*.

New Sending Profile

Name: Campaña Phishing

Interface Type: SMTP

SMTP From: Correo@correo.com

Host: 192.168.99.19:587

Username: admin

Password:

☒ Ignore Certificate Errors

Email Headers:

Header	Value
X-Custom-Header	{{URL}}-gophish

Show 10 entries Search:

No data available in table

Showing 0 to 0 of 0 entries

[Previous](#) [Next](#)

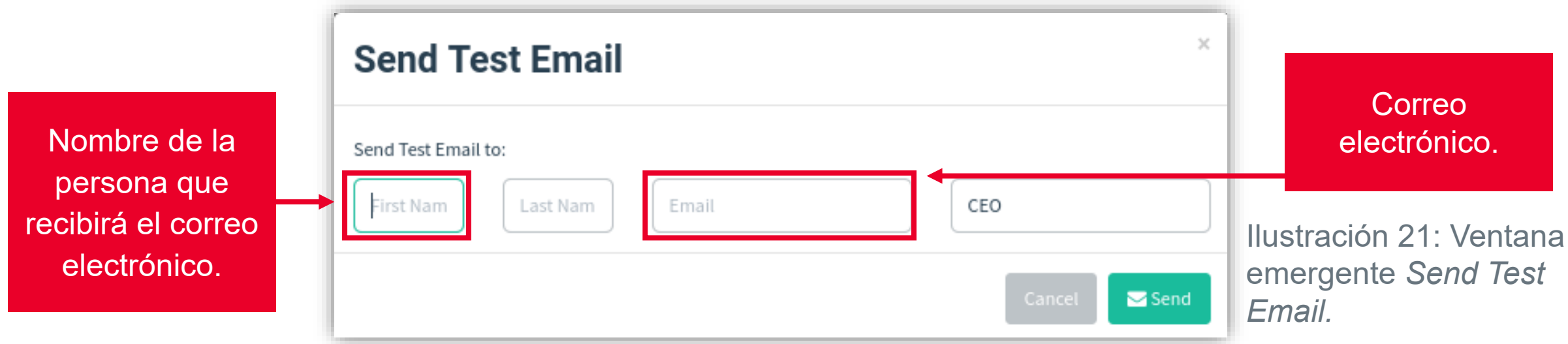
[Send Test Email](#)

[Cancel](#) [Save Profile](#)

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Una vez que todos los campos estén completos, puedes enviar un correo electrónico de prueba para verificar el funcionamiento del SMTP con el botón «*Send Test Email*».



[Nota] Si se opta por usar un SMTP de una cuenta de externa como, por ejemplo, Gmail, puede dar un error al intentar utilizarlo con Gophish.

1 EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- Si todo está correcto, recibirás en tu correo electrónico un correo por defecto de GoPhish confirmando este punto.

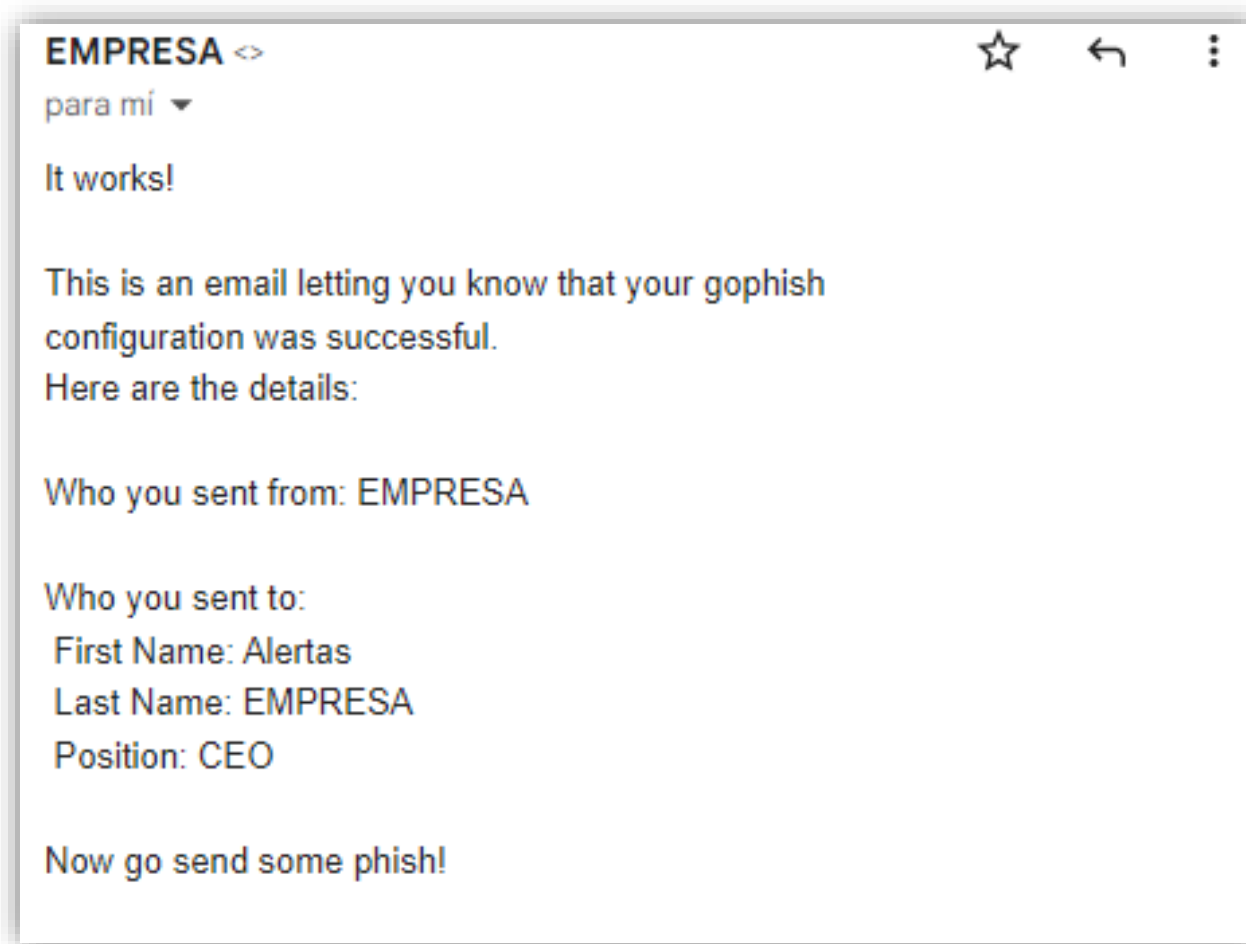
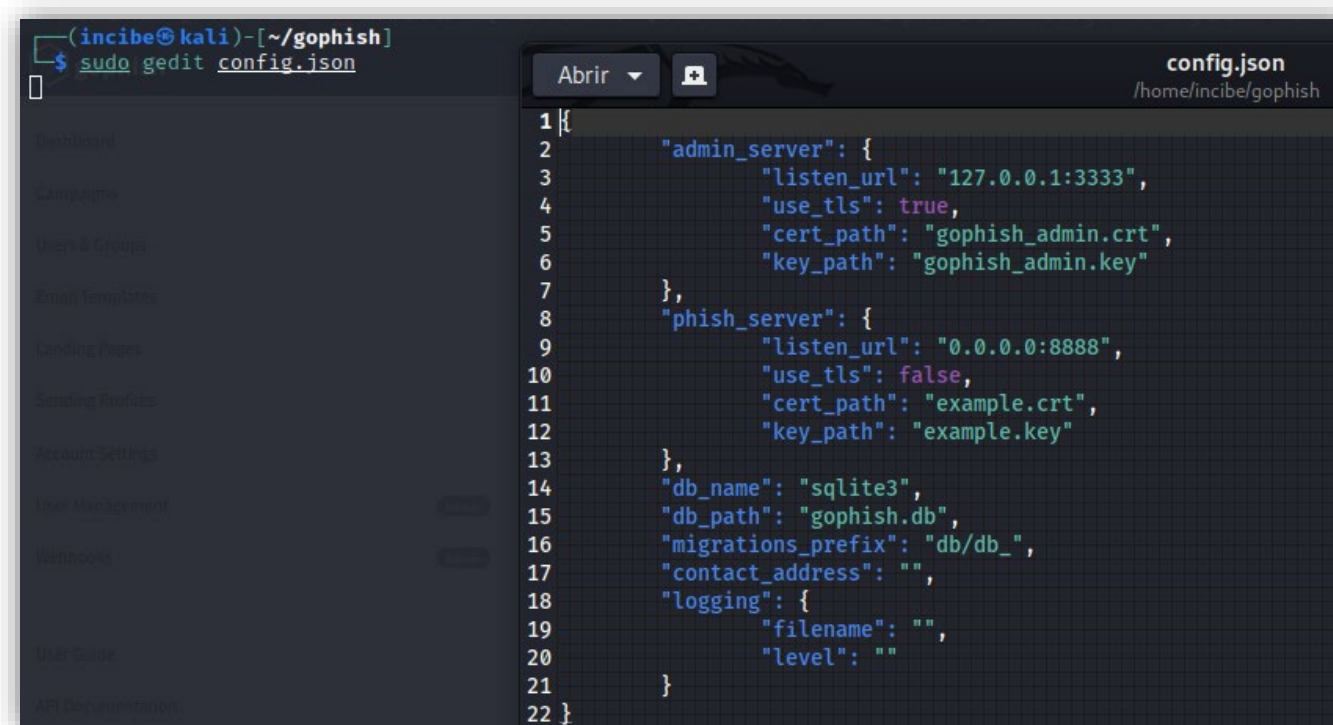


Ilustración 22: Plantilla de correo electrónico para la campaña de *phishing*.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Antes de seguir avanzando, deberás comprobar en el directorio de descarga de GoPhish la configuración descrita en el archivo «config.json».
 - Para ello, abre el archivo con el editor de texto. Es recomendable cambiar el puerto 80 de la dirección IP asignada al «*phish_server*» en la línea «*listen_url*». En el siguiente ejemplo se ha cambiado por el puerto 8888, ya que el puerto 80 es utilizado por múltiples servicios y las probabilidades de conflicto son altas.



```
(incibe@kali)-[~/gophish]
$ sudo gedit config.json

config.json
/home/incibe/gophish

1 {
2   "admin_server": {
3     "listen_url": "127.0.0.1:3333",
4     "use_tls": true,
5     "cert_path": "gophish_admin.crt",
6     "key_path": "gophish_admin.key"
7   },
8   "phish_server": {
9     "listen_url": "0.0.0.0:8888",
10    "use_tls": false,
11    "cert_path": "example.crt",
12    "key_path": "example.key"
13  },
14  "db_name": "sqlite3",
15  "db_path": "gophish.db",
16  "migrations_prefix": "db/db_",
17  "contact_address": "",
18  "logging": {
19    "filename": "",
20    "level": ""
21  }
22 }
```

Ilustración 23: Cambio del puerto 80 de la dirección IP asignada al «*phish_server*» en la línea «*listen_url*» por el puerto 8888.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Guarda los cambios en el archivo y dirígete de nuevo a la consola de GoPhish.
- A continuación, accede al menú «*Landing Page*» para crear la página web a la que redirigirá el correo electrónico malicioso. Esta página web que requerirá el correo electrónico y la contraseña a la víctima y será enviada a nuestro equipo. Para crear la página, haz clic en «*New Page*».

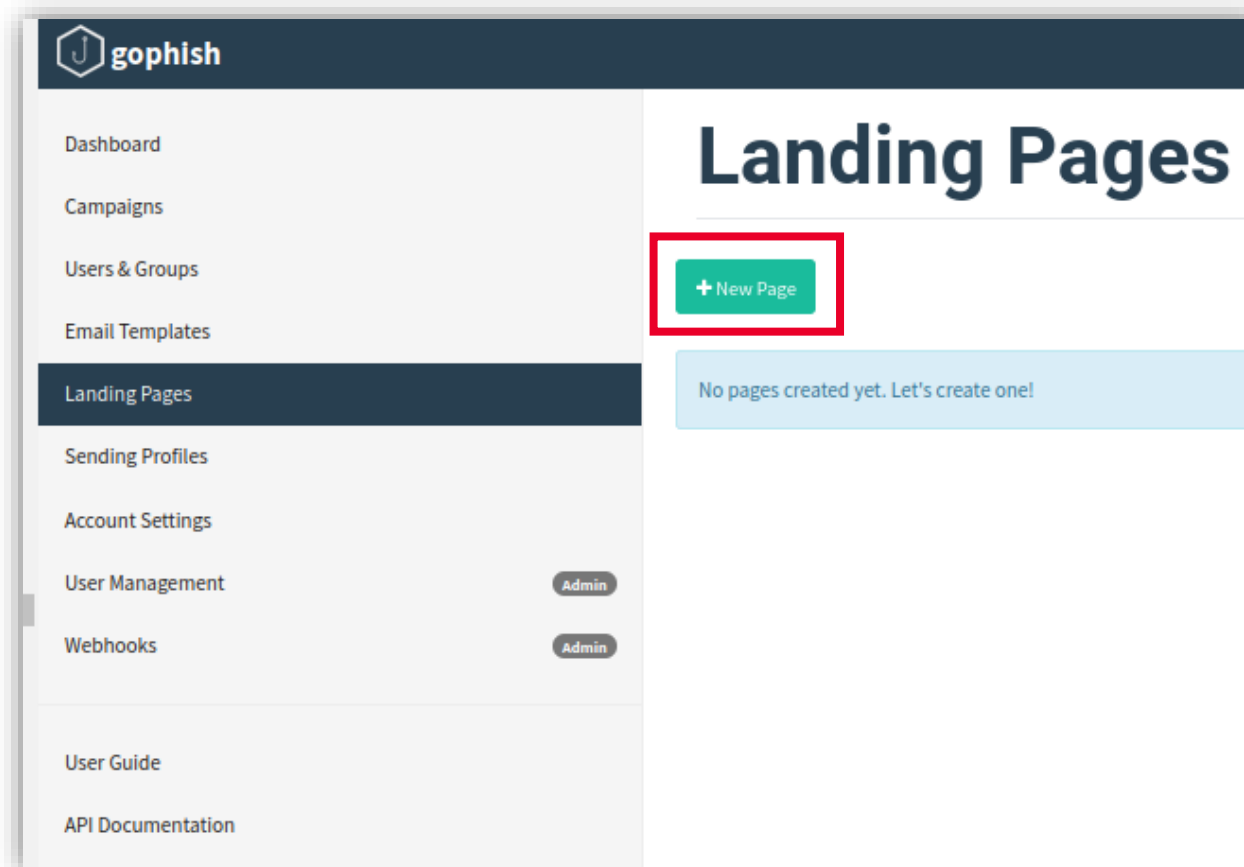


Ilustración 24: Pantalla de inicio *Landing Pages*: *New Landing Pages*.

EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- A continuación, aparecerá la siguiente ventana con el botón «*Import site*». GoPhish requiere introducir a mano el código HTML de la página web maliciosa, en las últimas versiones de la herramienta se ha incorporado la posibilidad de «clonar» una página web indicando solamente la URL legítima.
 - Para ello, vamos a proporcionaros un código HTML que copiaremos y pegaremos el cuál contiene un formulario de *log in*.

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width,
initial-scale=1.0">
  <title>Untitled</title>
```

EL ATAQUE *PHISHING*

Instalación y configuración de GoPhish

```
<link rel="stylesheet"
href="https://cdnjs.cloudflare.com/ajax/libs/twitter-
bootstrap/4.1.3/css/bootstrap.min.css">
<link rel="stylesheet"
href="https://cdnjs.cloudflare.com/ajax/libs/ionicons/2.0.1/cs
s/ionicons.min.css">
<style>
.login-dark {
  height:1000px;
  background:#475d62
  url("https://c1.wallpaperflare.com/preview/262/463/743/night
-sky-stars-silhouette.jpg");
  background-size:cover;
  position:relative;
```

EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

```
}  
.login-dark form {  
  max-width:320px;  
  width:90%;  
  background-color:#1e2833;  
  padding:40px;  
  border-radius:4px;  
  transform:translate(-50%, -50%);  
  position:absolute;  
  top:50%;  
  left:50%;  
  color:#fff;  
  box-shadow:3px 3px 4px rgba(0,0,0,0.2);  
}
```


EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

```
.login-dark .illustration {  
  text-align:center;  
  padding:15px 0 20px;  
  font-size:100px;  
  color:#2980ef;  
}  
.login-dark form .form-control {  
  background:none;  
  border:none;  
  border-bottom:1px solid #434a52;  
  border-radius:0;  
  box-shadow:none;  
  outline:none;  
  color:inherit;  
}
```

EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

```
}  
.login-dark form .btn-primary {  
  background:#214a80;  
  border:none;  
  border-radius:4px;  
  padding:11px;  
  box-shadow:none;  
  margin-top:26px;  
  text-shadow:none;  
  outline:none;  
}  
.login-dark form .btn-primary:hover, .login-dark form .btn-  
primary:active {  
  background:#214a80;  
  outline:none;
```

EL ATAQUE *PHISHING*

Instalación y configuración de GoPhish

```
}  
.login-dark form .forgot {  
  display:block;  
  text-align:center;  
  font-size:12px;  
  color:#6f7a85;  
  opacity:0.9;  
  text-decoration:none;  
}  
.login-dark form .forgot:hover, .login-dark form .forgot:active  
{  
  opacity:1;  
  text-decoration:none;  
}  
.login-dark form .btn-primary:active {  
  transform:translateY(1px);
```

1 EL ATAQUE *PHISHING*

Instalación y configuración de GoPhish

```
}  
</style>  
</head>  
<body>  
  <div class="login-dark">  
    <form method="post">  
      <h2 class="sr-only">Login Form</h2>  
      <div class="illustration"><i class="icon ion-ios-locked-outline"></i></div>  
      <div class="form-group"><input class="form-control" type="email"  
name="email" placeholder="Email"></div>  
      <div class="form-group"><input class="form-control" type="password"  
name="password" placeholder="Password"></div>  
      <div class="form-group"><button onclick="myFunction()" class="btn btn-  
primary btn-block" type="submit">Log In</button></div><a href="#"  
class="forgot">Forgot your email or password?</a></form>  
    </div>
```

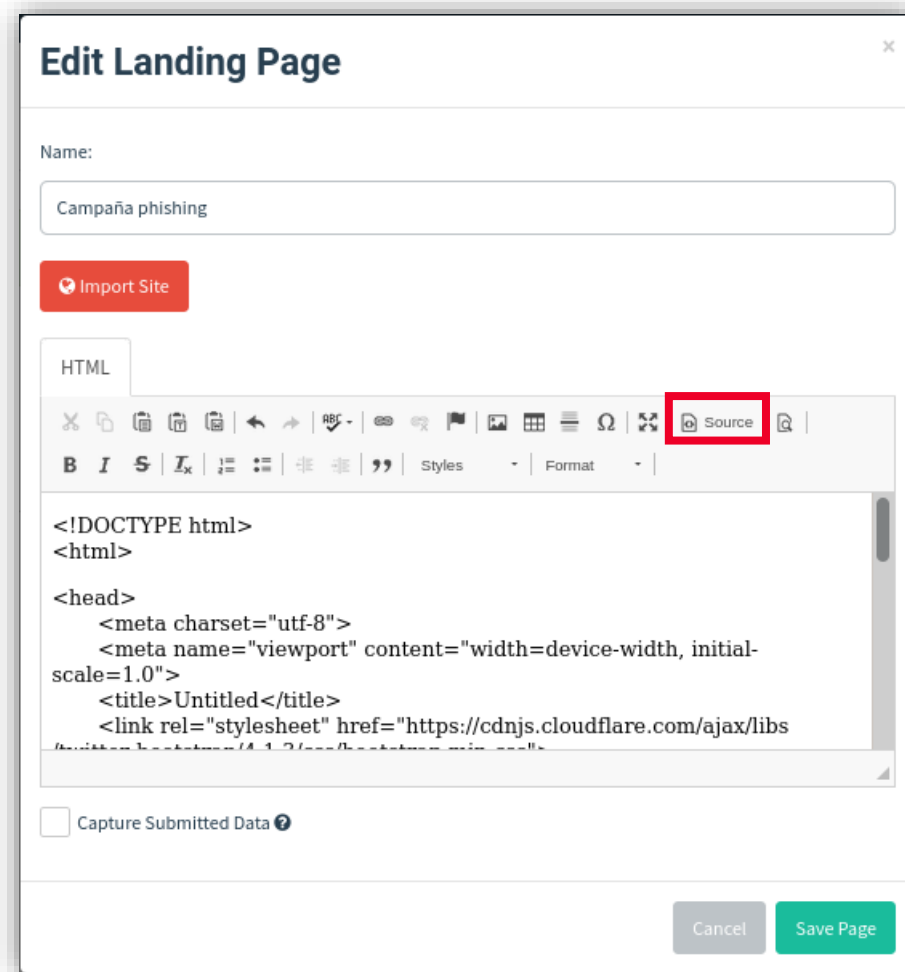
EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

```
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
  <script src="https://cdnjs.cloudflare.com/ajax/libs/twitter-
bootstrap/4.1.3/js/bootstrap.bundle.min.js"></script>
  <script>
    function myFunction() {
      alert("Log in realizado correctamente.");
    }
  </script>
</body>
</html>
```

1 EL ATAQUE *PHISING*

Instalación y configuración de GoPhish



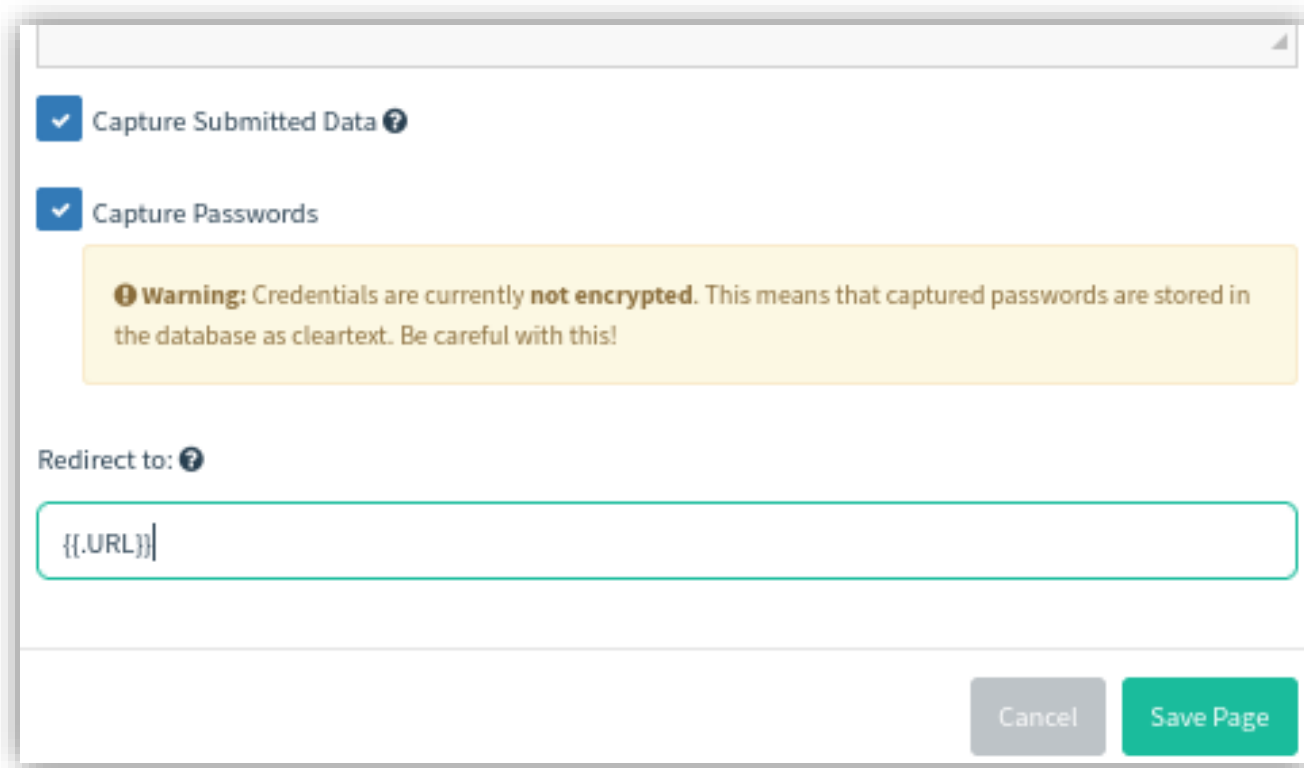
EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- Este diseño se puede cambiar añadiendo en el código lo que consideremos haciendo clic en el botón «*Source*» en las opciones de edición de texto que nos ofrece la herramienta, destacado en rojo en la imagen anterior.
 - En la siguiente pantalla, asegúrate de que las casillas «*Capture Submitted Data*» y «*Capture Passwords*» **están seleccionadas**. Aparecerá una advertencia de que las contraseñas serán capturadas y almacenadas sin cifrado, por lo que se debe tener especial cuidado con almacenar esta información cuando se trate de una campaña masiva para un cliente.

1 EL ATAQUE *PHISING*

Instalación y configuración de GoPhish



The screenshot shows a web form for configuring a new landing page in GoPhish. It includes two checked checkboxes: 'Capture Submitted Data' and 'Capture Passwords'. A yellow warning box states: 'Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!'. Below this is a 'Redirect to:' label and a text input field containing '{{.URL}}'. At the bottom right are 'Cancel' and 'Save Page' buttons.

☒ Capture Submitted Data ?

☒ Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: ?

{{.URL}}

Cancel Save Page

Ilustración 26: Formulario de campos *New Landing Page*.

EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- En la vista diseño o en la vista de código puedes editar los textos y los nombres de los campos del formulario para adaptarlos al mensaje que quieras transmitir. En cuanto a los enlaces del código a los que originalmente se enviaba esta información, GoPhish se encarga de adaptarlos al potencial objetivo.
- Si en el código se quiere hacer mención al nombre, apellidos, correo electrónico del destinatario o a la URL maliciosa, deberás incluir los parámetros `{{.FirstName}}` `{{.LastName}}` `{{.Email}}` o `{{.URL}}`, respectivamente.
- A continuación, haz clic en «*Save Page*».

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Después, vas a configurar la plantilla del correo electrónico. Aquí personalizarás el texto que recibirá la víctima y que incluirá un enlace a la *Landing Page* maliciosa diseñada en el paso anterior. Para ello, haz clic en «*Email Templates*» y, después, en el botón «*New Template*».

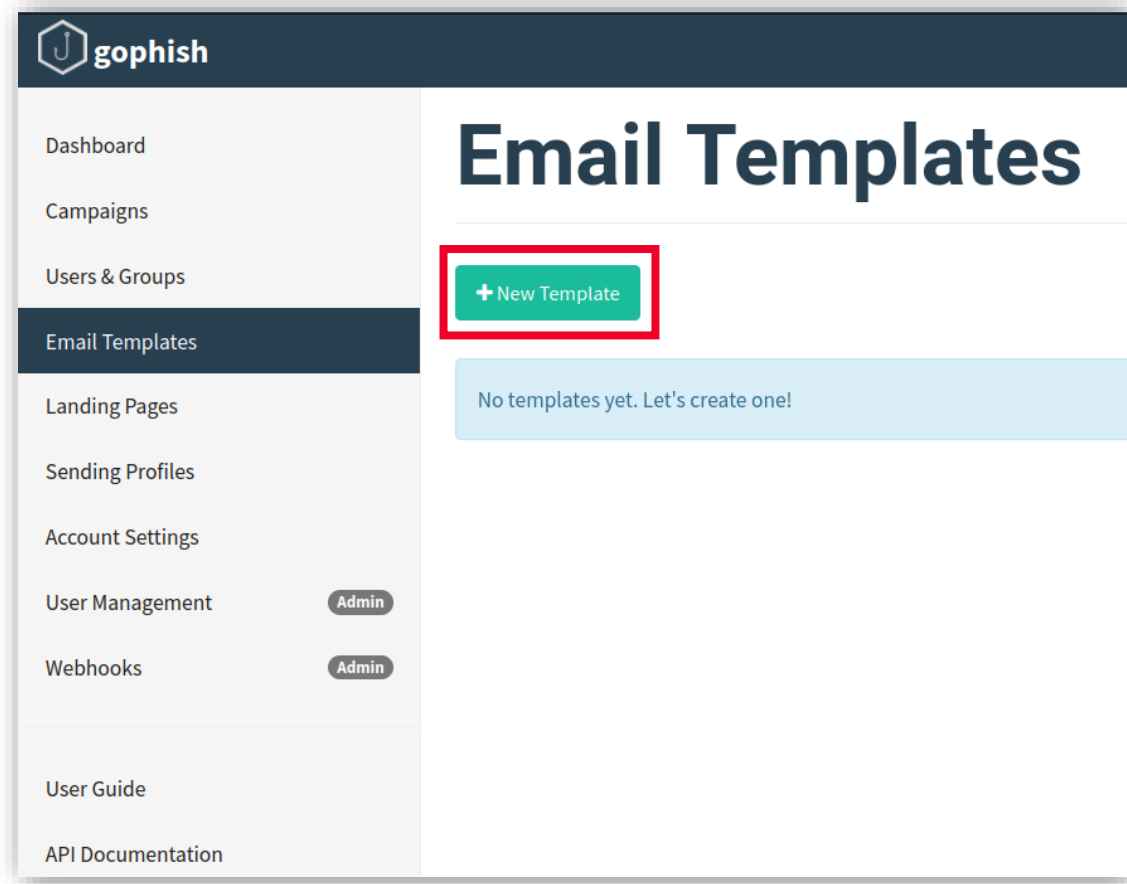


Ilustración 27: Pantalla de inicio *Email Templates*:
New Template.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- En la ventana emergente, deberás especificar un nombre para la plantilla. Además, al igual que en el diseño de la *Landing Page*, tendrás un botón para importar el diseño de un correo electrónico predefinido.

New Template

Name:

Envelope Sender:

Subject:

☒ Add Tracking Image

Show entries Search:

Name

No data available in table

Showing 0 to 0 of 0 entries

EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

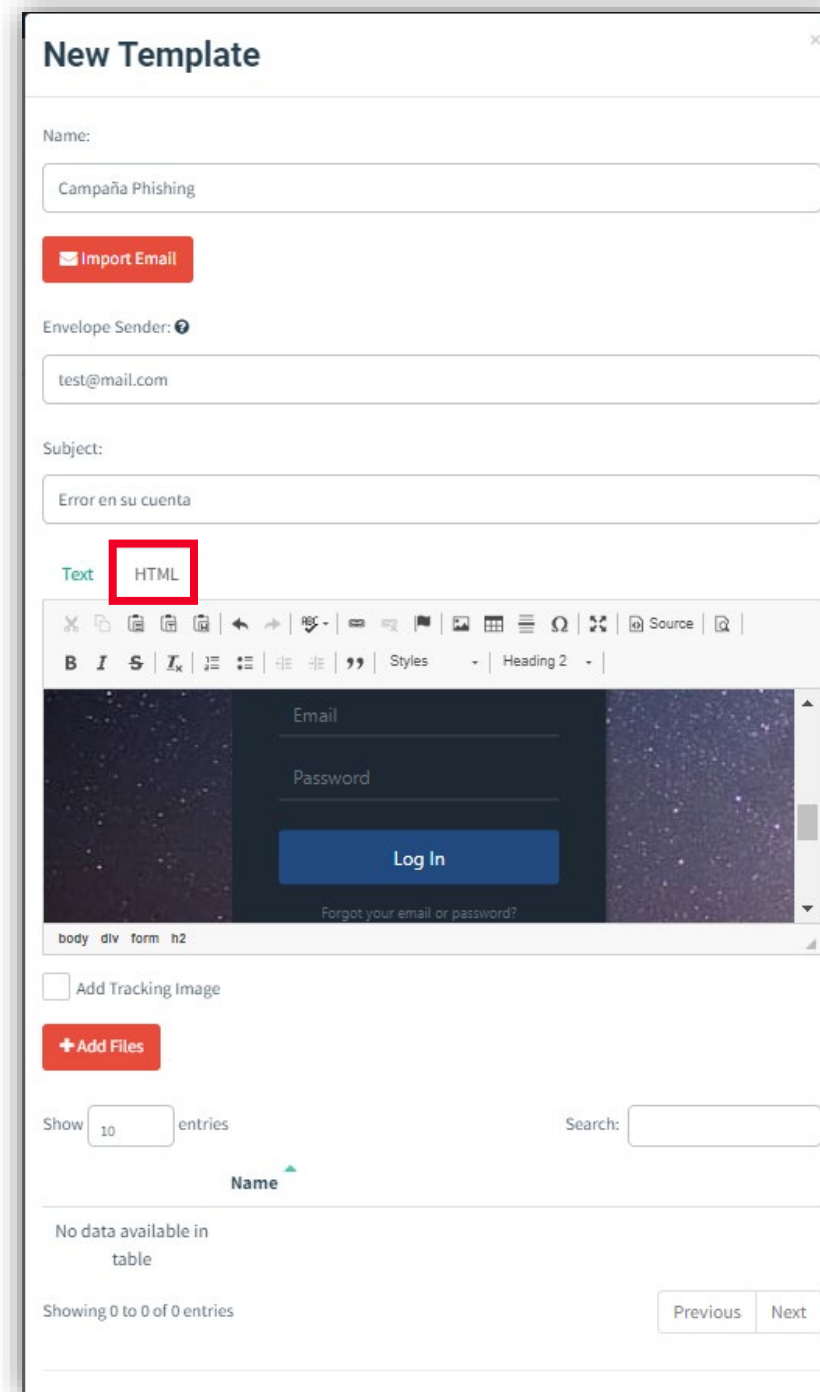
- Cualquiera de las dos opciones anteriores es válida aunque, importando un correo electrónico se consiguen mejores resultados. En cualquier caso, un paso obligatorio es añadir un enlace que redirija a la *Landing Page*. Para ello, haz clic en la vista «HTML» y añade un enlace pulsando en el símbolo de la cadena.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Aquí configurarás el texto con el que se verá el enlace y, debajo de él, el enlace en sí mismo. Se recomienda usar el parámetro {{.URL}} en este campo para que coincida con la configuración de GoPhish. Por defecto, GoPhish analiza los enlaces del correo electrónico fraudulento y los sustituye por la URL maliciosa.

Ilustración 29: Campos cumplimentados del formulario *New Email Template*.



The screenshot shows the 'New Template' form in GoPhish. The 'Name' field is filled with 'Campaña Phishing'. The 'Envelope Sender' field is filled with 'test@mail.com'. The 'Subject' field is filled with 'Error en su cuenta'. The 'Text' tab is selected, and the 'HTML' sub-tab is highlighted with a red box. The HTML content area shows a login form with fields for 'Email' and 'Password', a 'Log In' button, and a 'Forgot your email or password?' link. Below the HTML content, there is a checkbox for 'Add Tracking Image' and a red button for '+ Add Files'. At the bottom, there is a search bar and a table with the header 'Name' and a message 'No data available in table'.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Al finalizar, haz clic en «*Save Template*».
- Dirígete al menú «*Users & Groups*» para indicar los destinatarios, por grupos, a los que irá dirigida la campaña de *phishing*. Para ello, puedes importarlos de manera masiva a través de un archivo «.csv». Después, haz clic en «*Save Changes*».

New Group

Name:

Campaña Phishing

+ Bulk Import Users Download CSV Template

First Nam Last Nam Email Position + Add

Show 10 entries Search:

First Name Last Name Email Position

No data available in table

Showing 0 to 0 of 0 entries Previous Next

Close Save changes

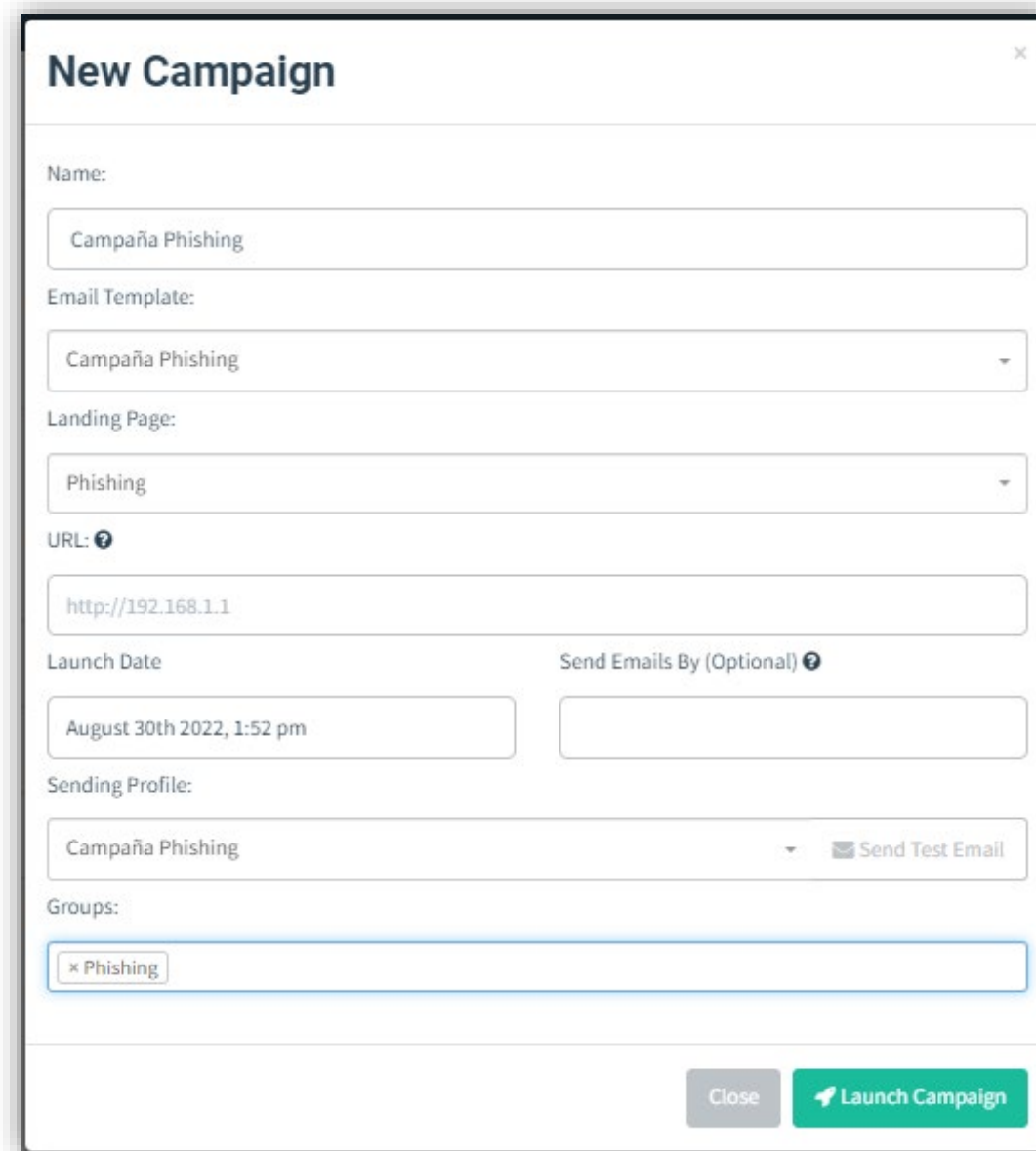
Ilustración 30: Formulario *New Group*.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

- Después de completar toda la configuración, crearás tu campaña de *phishing*. Para ello, accede al menú «*Campaigns*» y selecciona los respectivos desplegados, cada una de las plantillas que has configurado anteriormente: *Email, Landing Page, Profile y Groups*.

Ilustración 31: Creación de la campaña de phishing mediante el menú «*Campaigns*» y los respectivos desplegados, *Email, Landing Page, Profile y Groups*.



New Campaign

Name:

Email Template:

Landing Page:

URL:

Launch Date:

Send Emails By (Optional):

Sending Profile:

Groups:

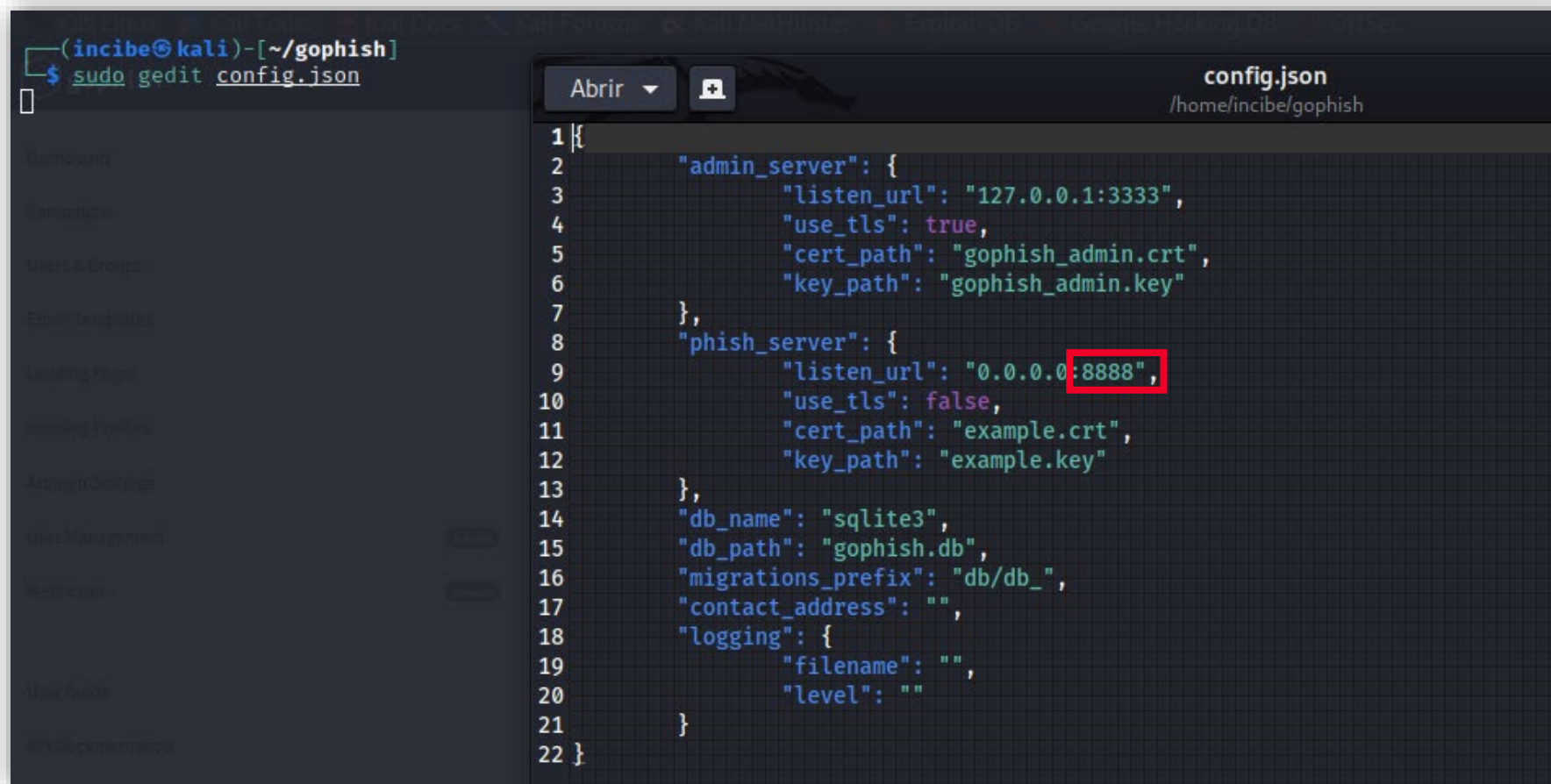
EL ATAQUE *PHISHING*

Instalación y configuración de GoPhish

- Define una fecha de ejecución de la campaña de *phishing*. Un paso muy importante es comprobar de nuevo que la máquina virtual está en modo «*Bridge*» o «Punto» y añadir en el campo «URL» la dirección IP pública (esta se puede consultar en cualquier página como, <https://www.cual-es-mi-ip.net/>) seguida del puerto configurado como «*listener*» en el archivo «*config.json*» de GoPhish visto anteriormente.

1 EL ATAQUE PHISHING

Instalación y configuración de GoPhish



```
(incibe@kali)~[/gophish]
$ sudo gedit config.json

config.json
/home/incibe/gophish

1 {
2     "admin_server": {
3         "listen_url": "127.0.0.1:3333",
4         "use_tls": true,
5         "cert_path": "gophish_admin.crt",
6         "key_path": "gophish_admin.key"
7     },
8     "phish_server": {
9         "listen_url": "0.0.0.0:8888",
10        "use_tls": false,
11        "cert_path": "example.crt",
12        "key_path": "example.key"
13    },
14    "db_name": "sqlite3",
15    "db_path": "gophish.db",
16    "migrations_prefix": "db/db_",
17    "contact_address": "",
18    "logging": {
19        "filename": "",
20        "level": ""
21    }
22 }
```

Ilustración 32: Puerto 8888 configurado anteriormente en el archivo «config.json» de GoPhish.

1 EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- Haz clic en «*Launch Campaign*» para programar la campaña de *phishing* y prepararla.

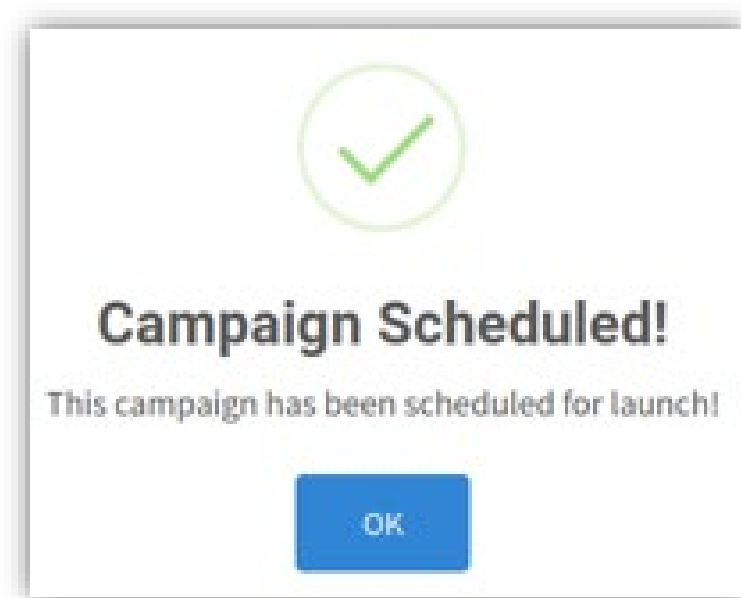


Ilustración 33: Campaña de *phishing* preparada.

EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- En este punto, aunque la víctima recibiría el correo electrónico, no podría acceder a la *Landing Page*. Un usuario externo a la red que quiera acceder a un *host* concreto, como el que está desplegado en GoPhish, necesitará que se implemente la redirección de puertos del *router*. De lo contrario, solo podrían acceder usuarios de la misma red. Por lo tanto, deberás entrar en el *router* y buscar el apartado «*Port Forwarding*» para configurarlo de la siguiente manera y que todas las peticiones entrantes al puerto 8888 sean redirigidas a la dirección IP de la máquina virtual Kali Linux y al puerto 8888.

1 EL ATAQUE PHISING

Instalación y configuración de GoPhish

Ilustración 34: Configuración de peticiones entrantes al puerto 8888 para ser redirigidas a la dirección IP de la máquina virtual Kali Linux y al puerto 8888.

Add New Rule

Active ☒

Service Name Phishing INCIBE

WAN Interface Default

Start Port 8888

End Port 8888

Translation Start Port 8888

Translation End Port 8888

Server IP Address 192 . 168 . 1 . 104

Configure Originating IP ☐ Enable

Protocol TCP

Note

1.To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

Here's an example to configure port translation. Configure **Start Port** to 100, **End Port** to 120, **Translation Start Port** to 200, and **Translation End Port** to 220.

2.TCP port 30005 is reserved for system use.

Cancel OK

1 EL ATAQUE *PHISHING*

Instalación y configuración de GoPhish

- La víctima recibirá un correo electrónico similar al siguiente, en función del diseño.

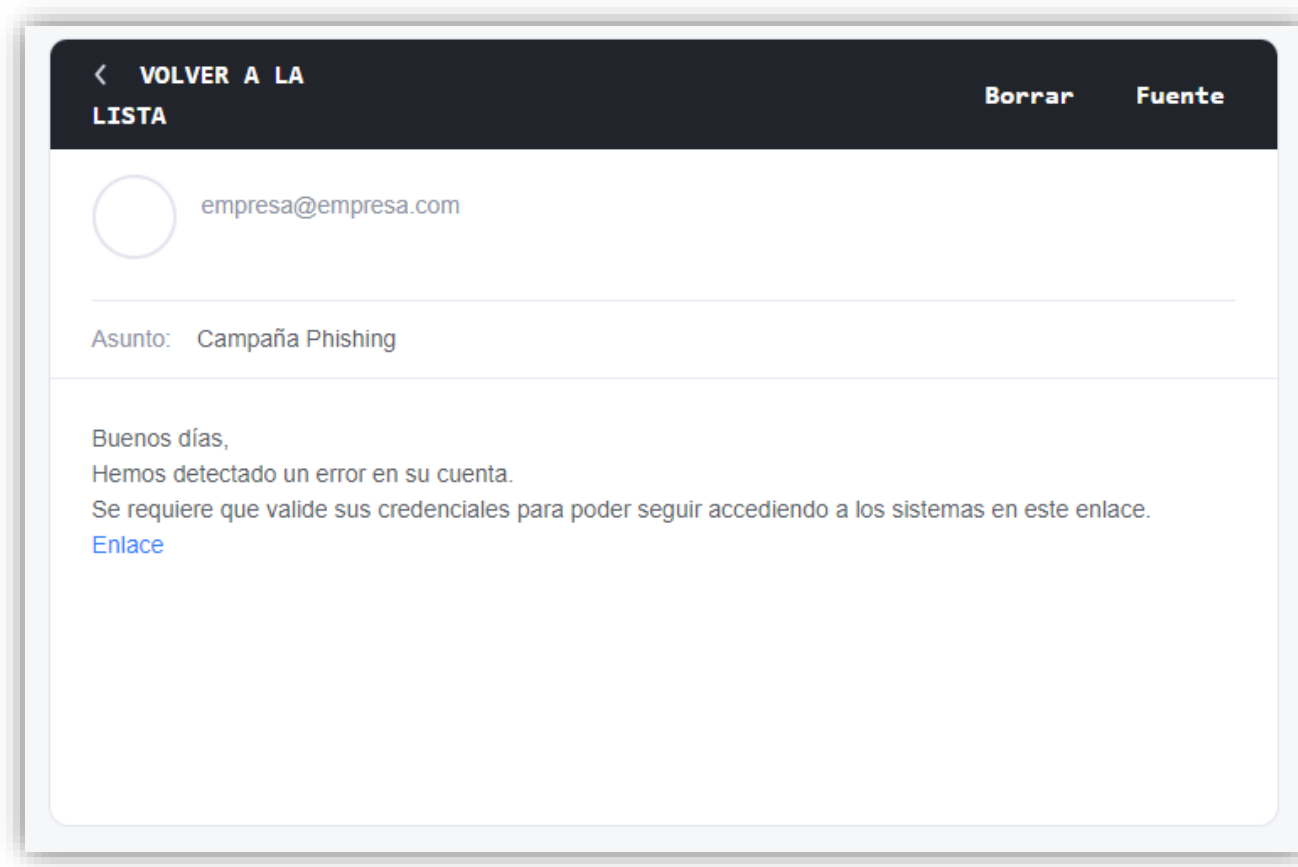


Ilustración 35: Correo electrónico que recibirá la víctima.

EL ATAQUE *PHISING*

Instalación y configuración de GoPhish

- Al hacer clic en el enlace, llevará a la víctima a tu *Landing Page*.
- Desde este mismo punto, ya puedes ver los resultados de la campaña de *phishing* en el menú «*Dashboard*» de GoPhish. Puedes visualizar, de manera global, cuántos correos electrónicos han sido enviados, cuántos abiertos, cuántos usuarios han hecho clic y cuántos han llegado a enviar sus credenciales.

1 EL ATAQUE PHISHING

Instalación y configuración de GoPhish

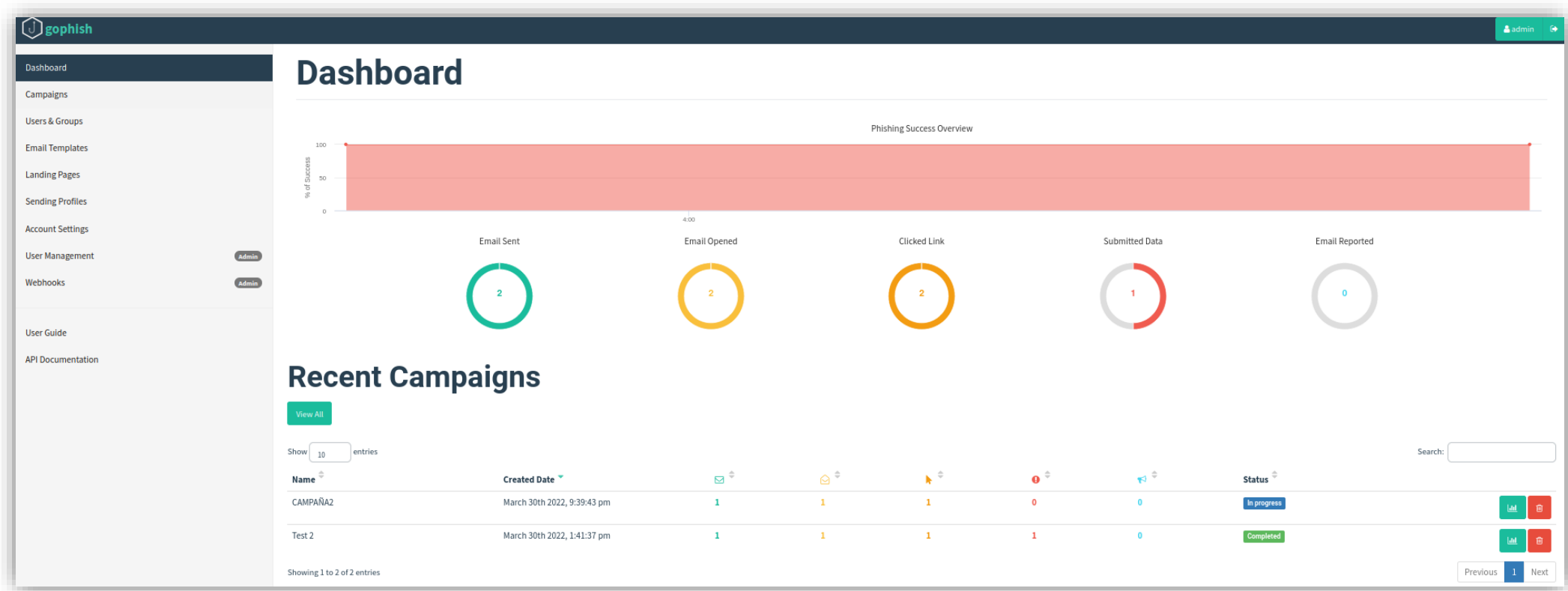


Ilustración 36: Resultados de la campaña de phishing en el menú «Dashboard» de GoPhish.

1 EL ATAQUE *PHISHING*

Instalación y configuración de GoPhish

- Además, haciendo clic en cada campaña de *phishing*, podrás ver con más detalle los resultados de cada usuario e incluso qué correo electrónico y contraseña han introducido.



The screenshot displays the GoPhish web interface. At the top, there is a world map with Brazil highlighted in green. Below the map, there is a table with the following columns: Last Name, Email, Position, and Status. The table contains one row of data for a user named Alonso, whose email is redacted with a black box, and whose position is CEO. The status column shows a green button labeled 'Email Sent'.

Last Name	Email	Position	Status
Alonso		CEO	Email Sent

Ilustración 37: Resultados que muestran de cada usuario su correo electrónico y contraseña.

1 EL ATAQUE *PHISHING*

Instalación y configuración de GoPhish

- Para finalizar la campaña de *phishing*, accede al menú «*Campaigns*» y haz clic en el botón rojo con el símbolo de la papelera. Esto eliminará la *Landing Page*, los datos recogidos y los envíos programados de nuestra campaña.

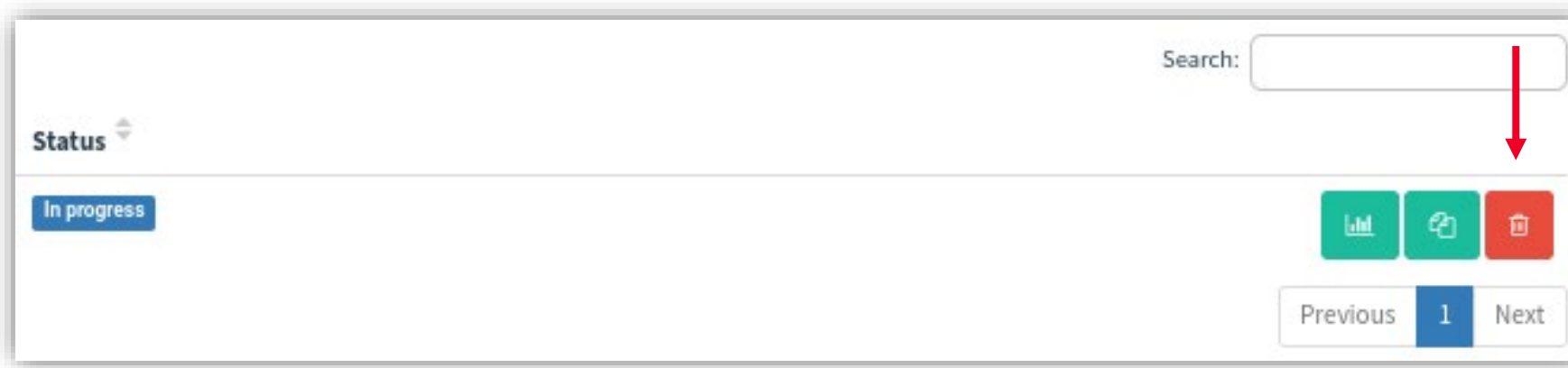
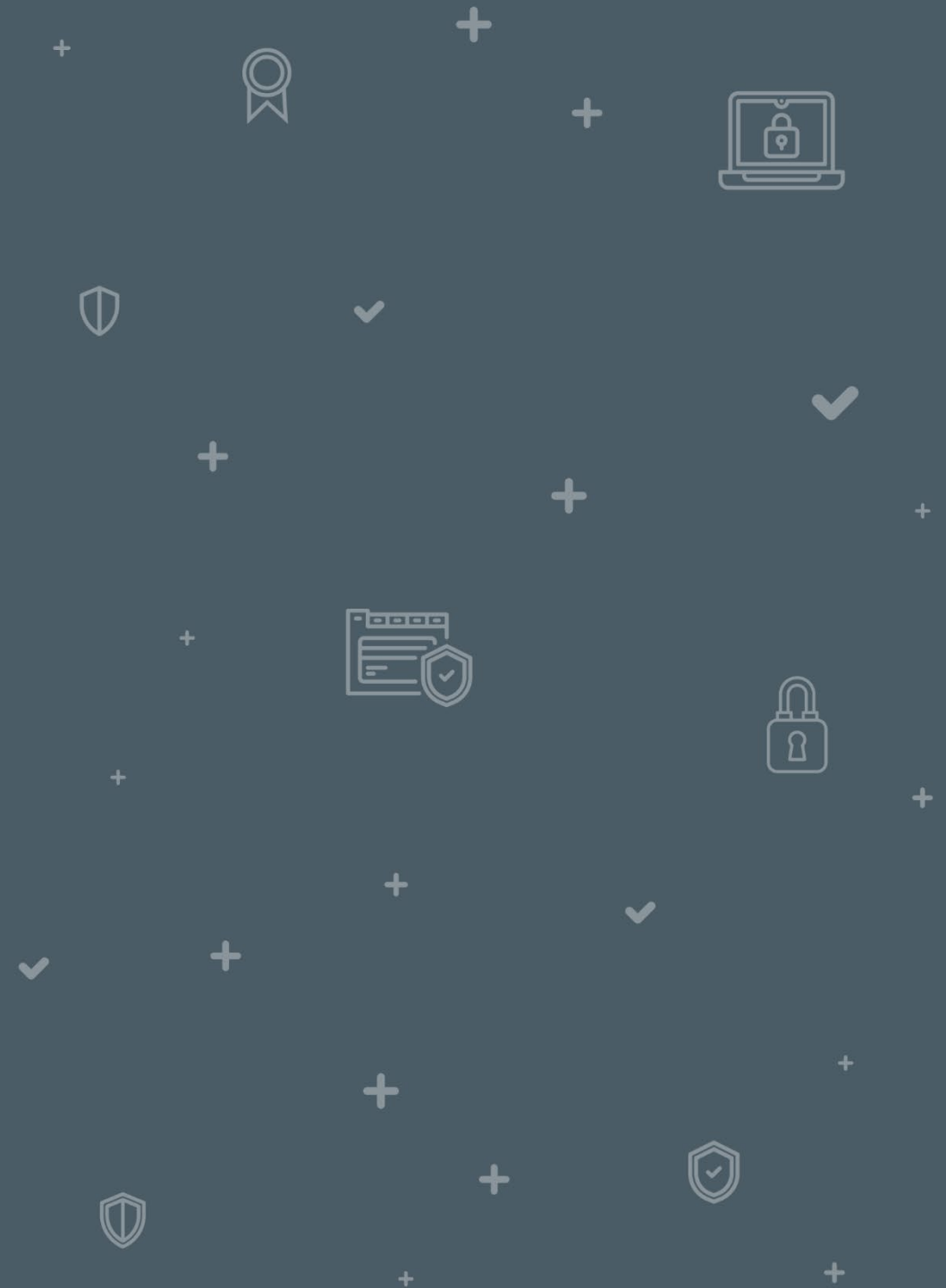


Ilustración 38: Eliminación de la campaña de *phishing*.

ENUNCIADO
EJERCICIO
PRÁCTICO 5:
ATAQUE DE
PHISHING

2



2 ENUNCIADO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*



Una empresa quiere llevar a cabo una campaña de concienciación en ciberataques. Para ello, utilizaremos GoPhish y realizaremos una campaña de *phishing* en la que suplantaremos una página web de la propia empresa y solicitaremos las credenciales de acceso de los usuarios para que nos devuelva los resultados a nuestro correo electrónico.



3

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- Accede al menú «*Landing Page*» y haz clic en «*New Page*».

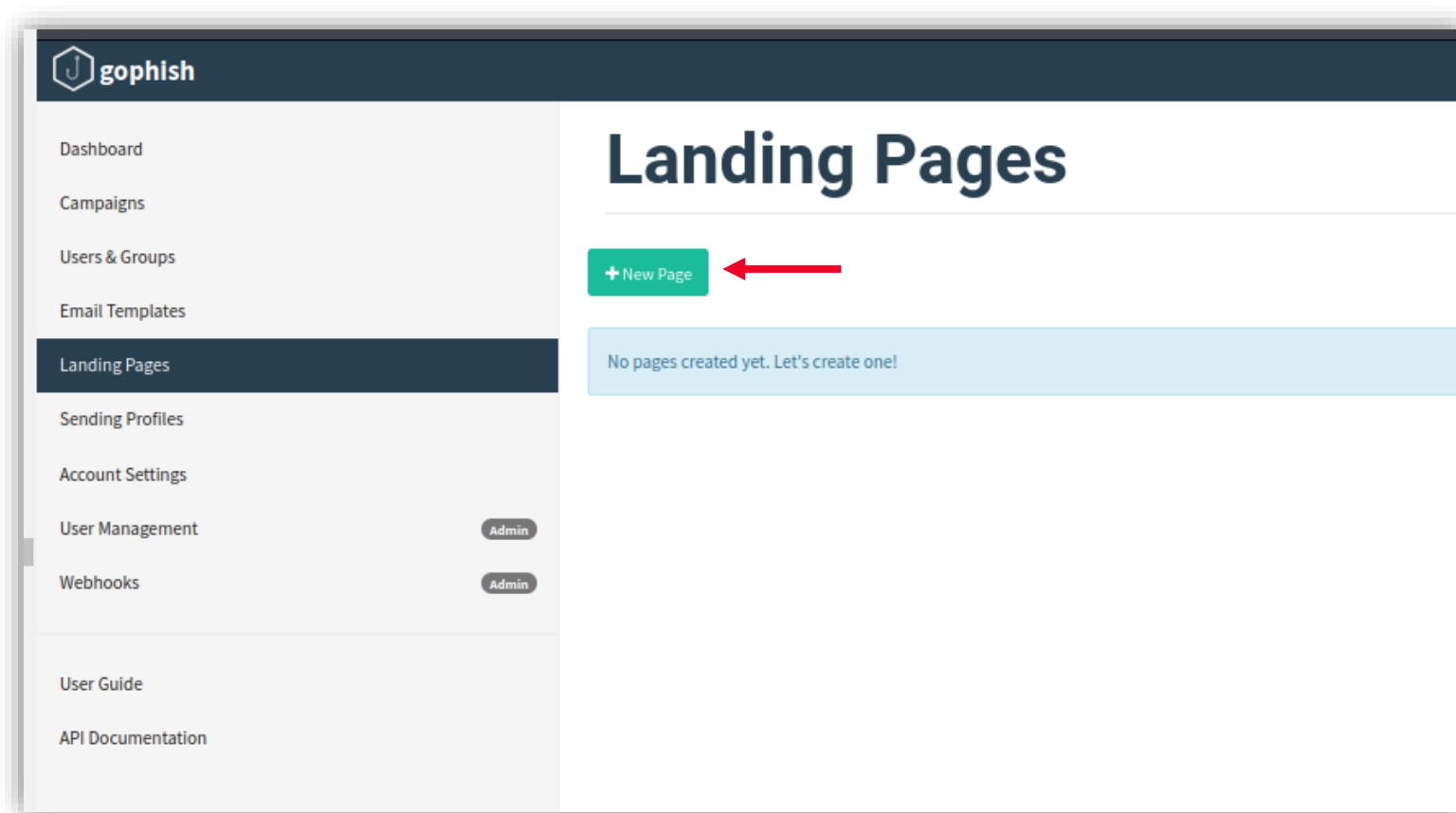
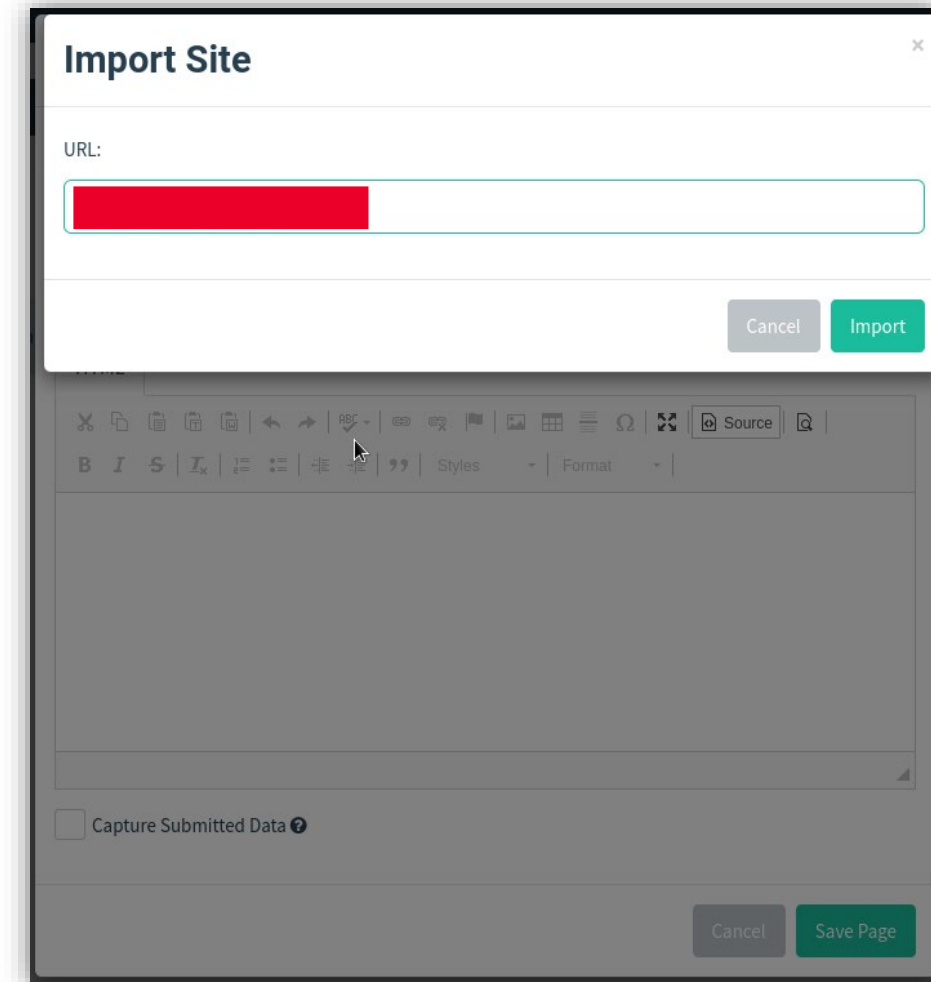


Ilustración 39: Pantalla de inicio de *Landing Pages: New Page*.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- A continuación, haz clic en el botón «*Import Site*» e indica que se quiere utilizar como base la página que hemos seleccionado como ejemplo, ya que contiene un formulario con la estética que necesitamos.

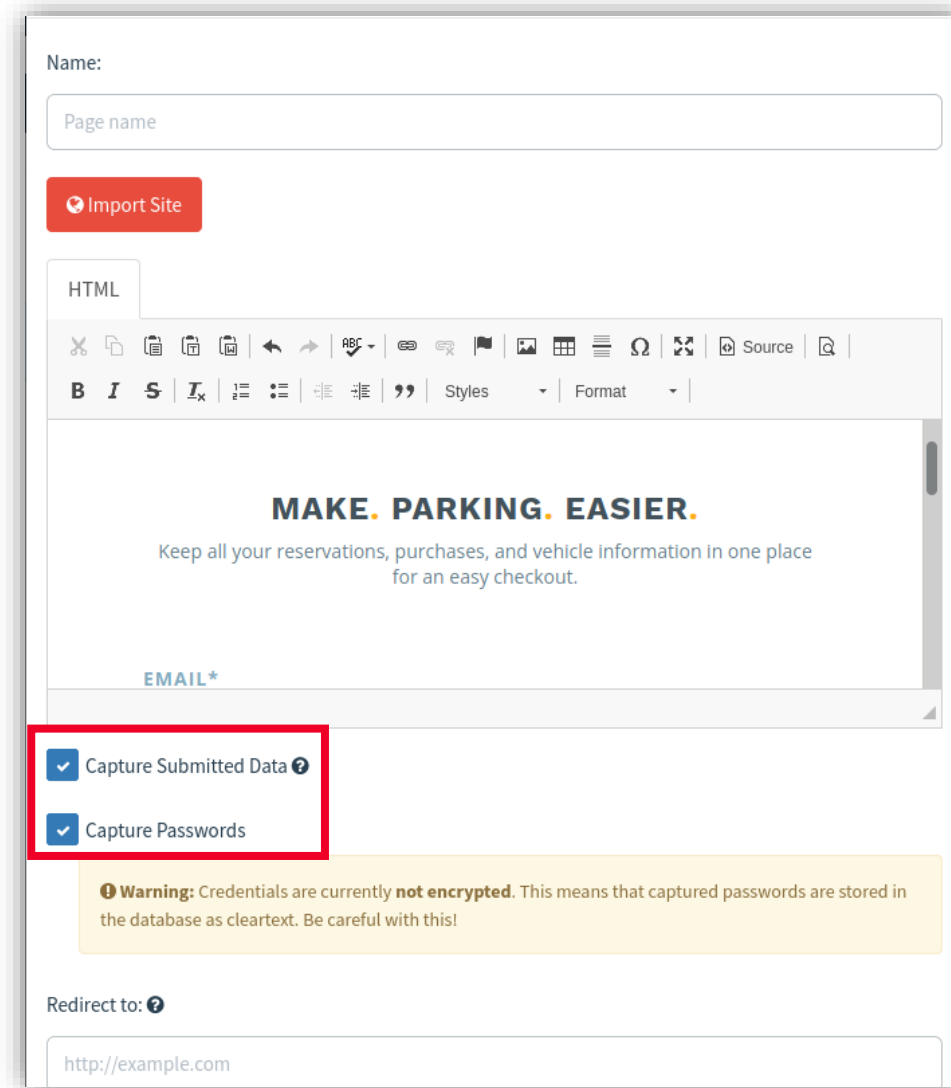
Ilustración 40: Formulario para insertar la página web de base.



The image shows a screenshot of a web browser interface. In the foreground, there is a modal dialog box titled "Import Site". Inside the dialog, there is a label "URL:" followed by a text input field. The input field has a red background. Below the input field, there are two buttons: "Cancel" and "Import". The background of the browser window is blurred, showing a web page editor with a toolbar and a "Capture Submitted Data" checkbox.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- En la siguiente pantalla, deberás asegurarte de que las casillas «*Capture Submitted Data*» y «*Capture Passwords*» están seleccionadas.



The screenshot shows a web-based configuration interface for a phishing kit. At the top, there is a 'Name:' field with a placeholder 'Page name' and an 'Import Site' button. Below this is a rich text editor with a toolbar and a preview area. The preview area displays a phishing page with the heading 'MAKE. PARKING. EASIER.' and a subtext 'Keep all your reservations, purchases, and vehicle information in one place for an easy checkout.' followed by an 'EMAIL*' input field. At the bottom of the configuration panel, two checkboxes are visible: 'Capture Submitted Data' and 'Capture Passwords', both of which are checked. A red rectangular box highlights these two checkboxes. Below the checkboxes is a yellow warning box that reads: 'Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!'. At the very bottom, there is a 'Redirect to:' field with a placeholder 'http://example.com'.

Ilustración 41: Casillas «*Capture Submitted Data*» y «*Capture Passwords*» seleccionadas.

SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- En la vista diseño o en la vista de código, podrás editar los textos y los nombres de los campos del formulario para adaptarlos al mensaje que quieres transmitir. En nuestro caso, alertamos de una brecha de seguridad en el correo electrónico. Por ello, eliminaremos todos los campos del formulario salvo dos, que serán donde indiquen el correo electrónico y la contraseña.
 - GoPhish se encargará de adaptar al objetivo de este ejercicio práctico los enlaces del código a los que originalmente se enviaba esta información.
- Si en algún momento del código se quiere hacer mención al nombre, apellidos, correo electrónico del destinatario o a la URL maliciosa, deberás incluir los parámetros `{{.FirstName}}` `{{.LastName}}` `{{.Email}}` o `{{.URL}}`, respectivamente.

3

SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

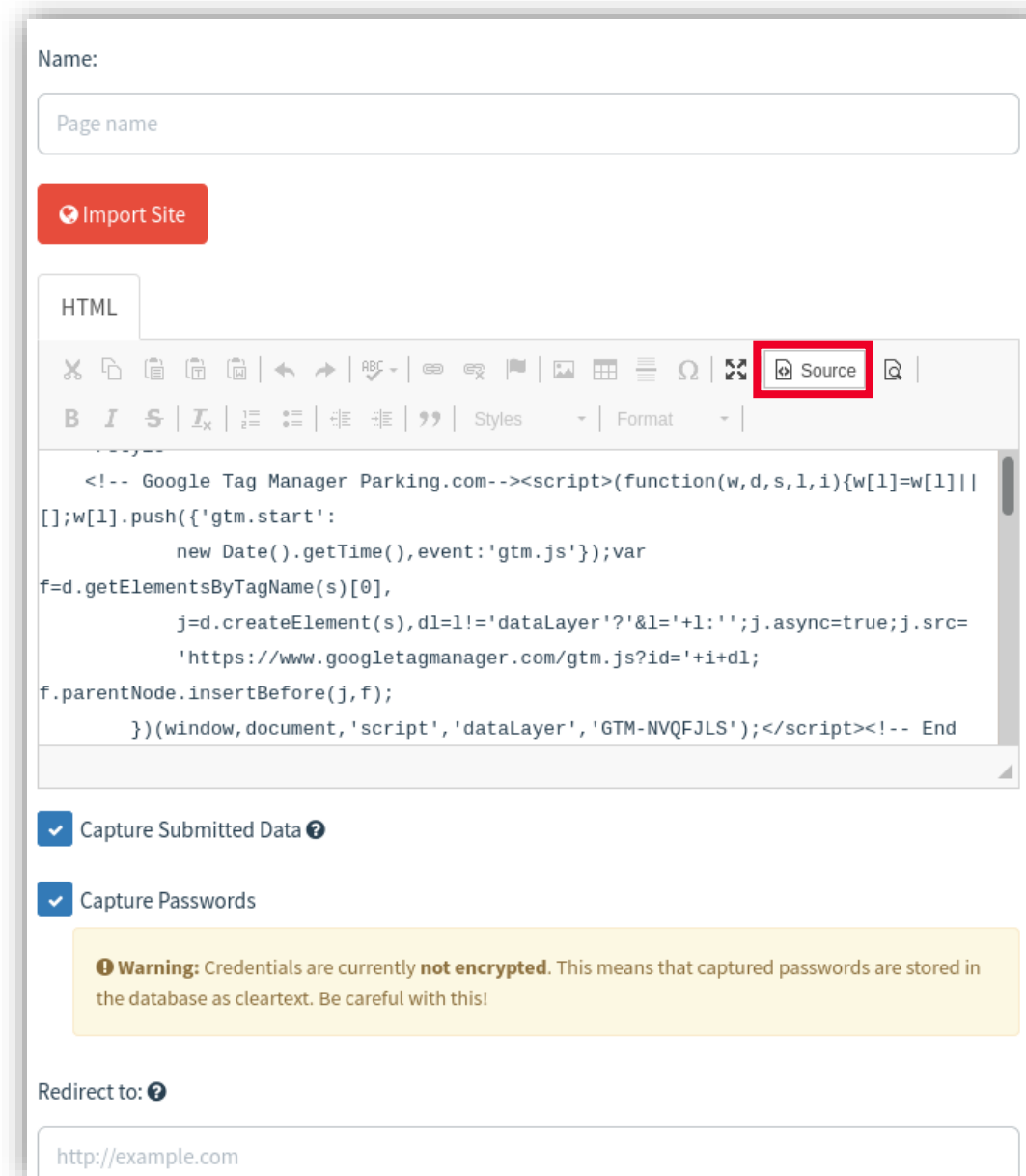


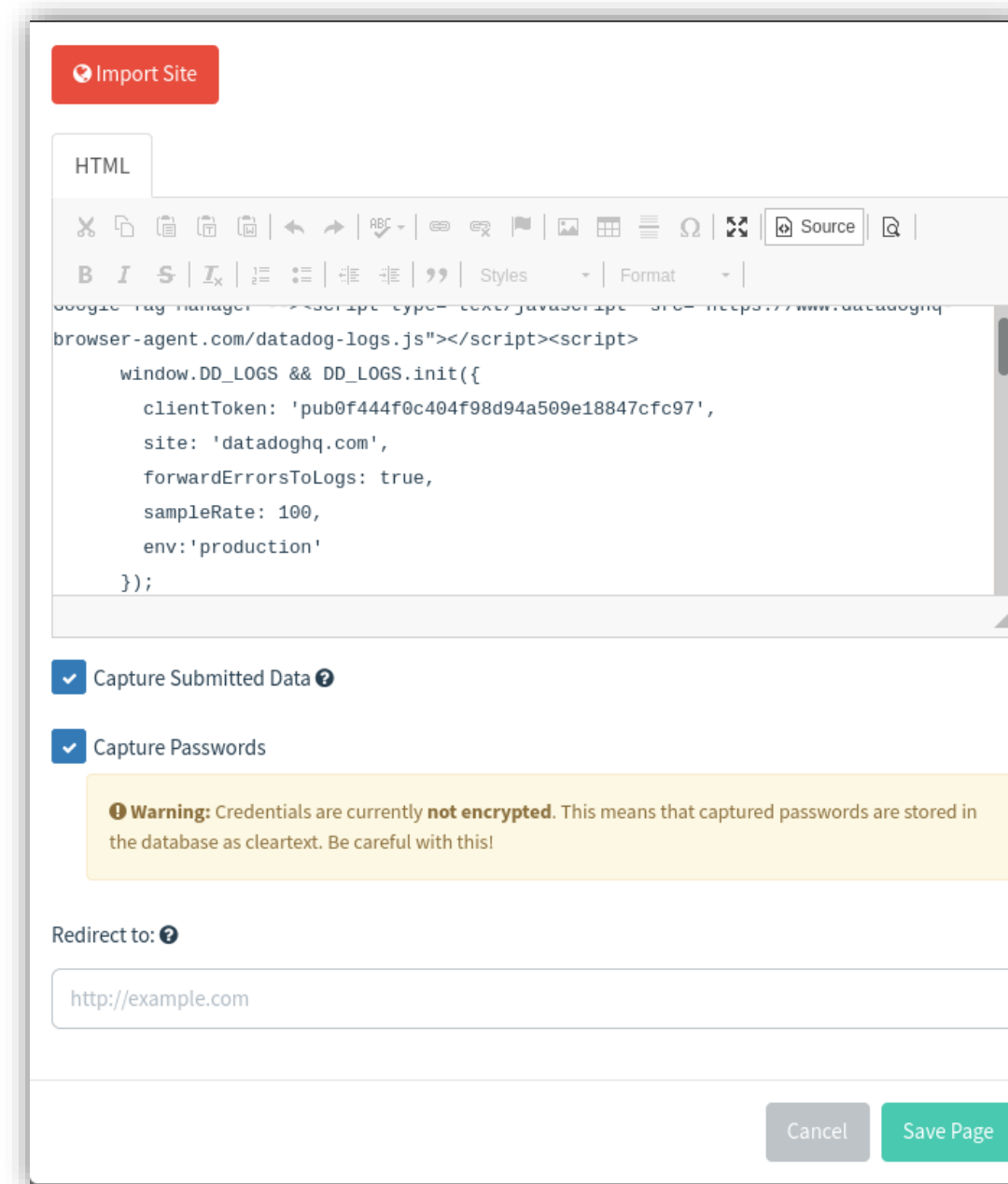
Ilustración 42: Localización del botón *Source*.

3

SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- Para finalizar, haz clic en «*Save Page*».

Ilustración 43: Localización del botón *Save Page*.



3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- A continuación, configura la plantilla del correo electrónico que se va a enviar. Para ello, haz clic dentro de «*Email Templates*», en el botón «*New Template*».

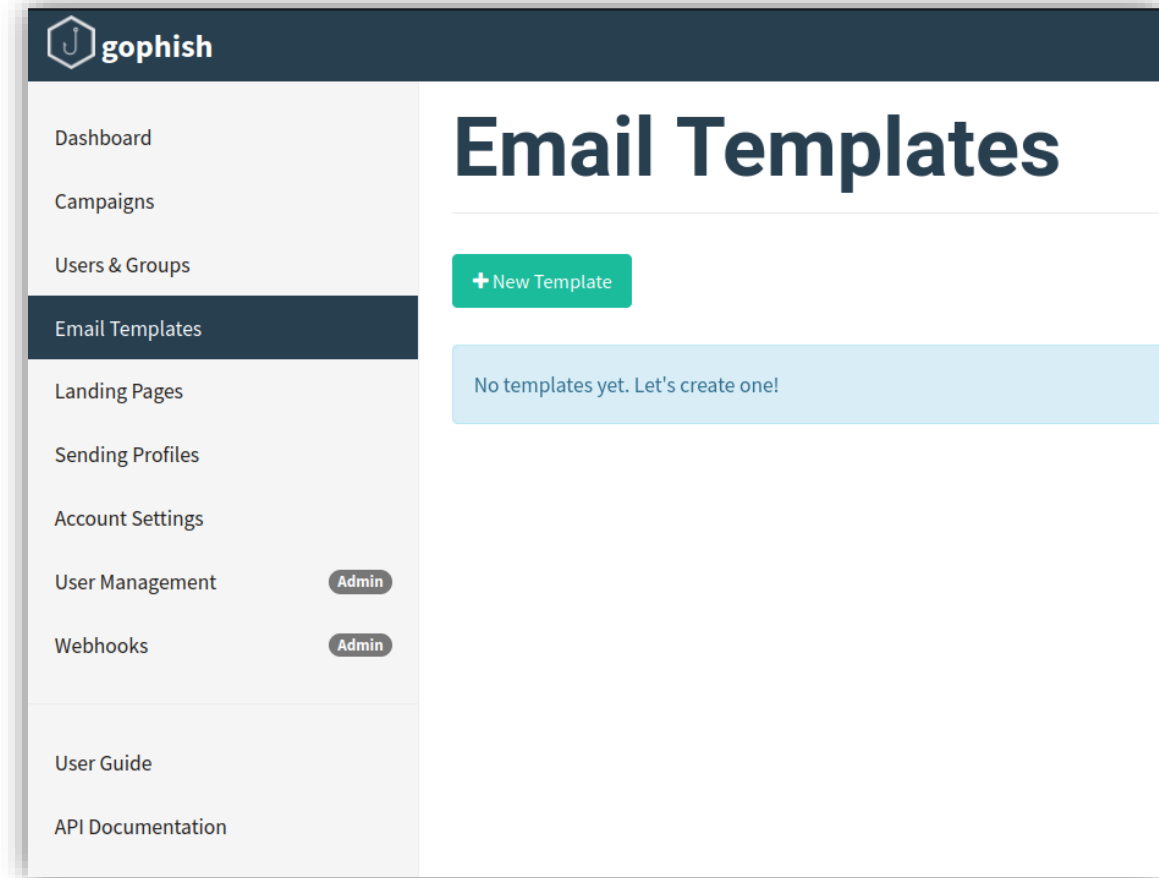


Ilustración 44: Pantalla de inicio *Email Templates*: *New Template*.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- En la ventana emergente, deberás especificar un nombre para la plantilla. Además, al igual que en el diseño de la *Landing Page*, aparecerá un botón para importar el diseño de un correo electrónico predefinido.

Name:

Ejemplo|

Import Email

Envelope Sender: ?

First Last <test@example.com>

Subject:

Email Subject

Text HTML

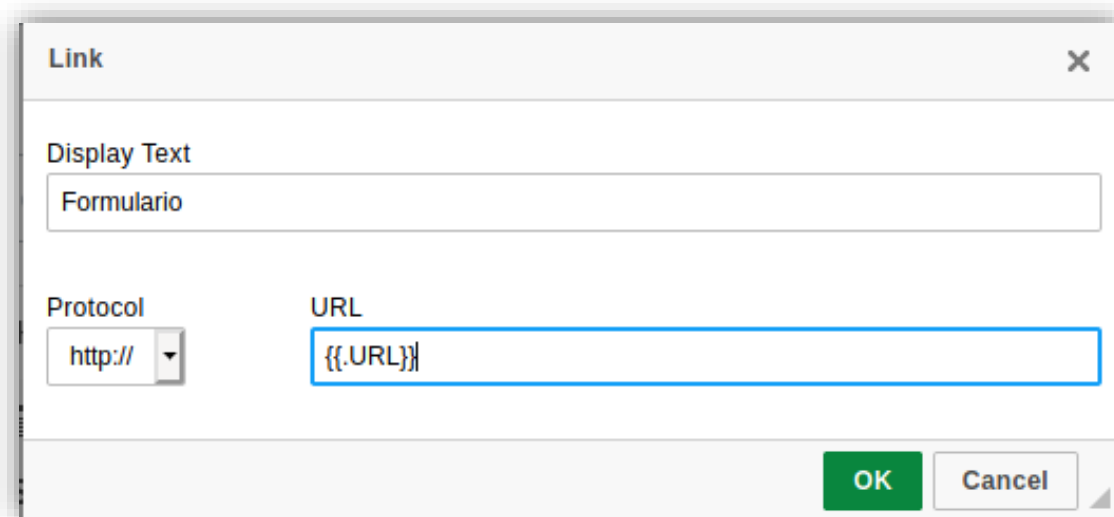
Plaintext

☒ Add Tracking Image

Ilustración 45: Formulario de *New Template*.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- Cualquier de las dos opciones es igual de válida, aunque, importando un correo electrónico se pueden conseguir mejores resultados. No obstante, un paso obligatorio en ambos casos es añadir un enlace que redirija a la *Landing Page*. Para ello, haz clic en la vista «HTML» e incluye un enlace haciendo clic en el símbolo de la cadena.
 - En este paso configurarás el texto con el que se verá el enlace y debajo indicarás el propio enlace. Se recomienda usar el parámetro `{{.URL}}` en este campo para que coincida con la configuración de GoPhish.



The screenshot shows a 'Link' dialog box with the following fields:

- Display Text:** A text input field containing 'Formulario'.
- Protocol:** A dropdown menu currently showing 'http://'.
- URL:** A text input field containing the placeholder '{{.URL}}'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Ilustración 46: Enlace que se mostrará en el correo electrónico de la víctima.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- Para finalizar, haz clic en «*Save Template*».

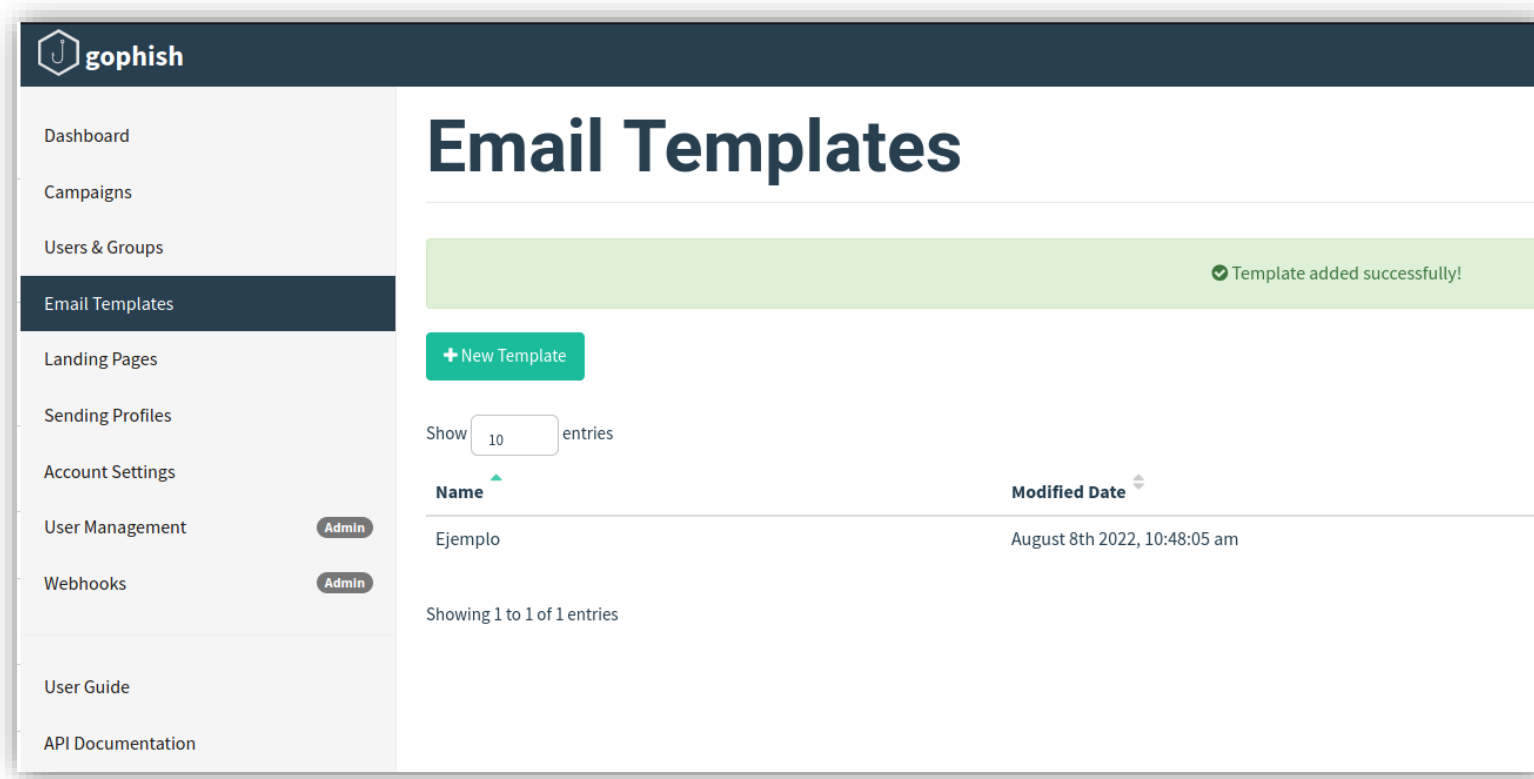
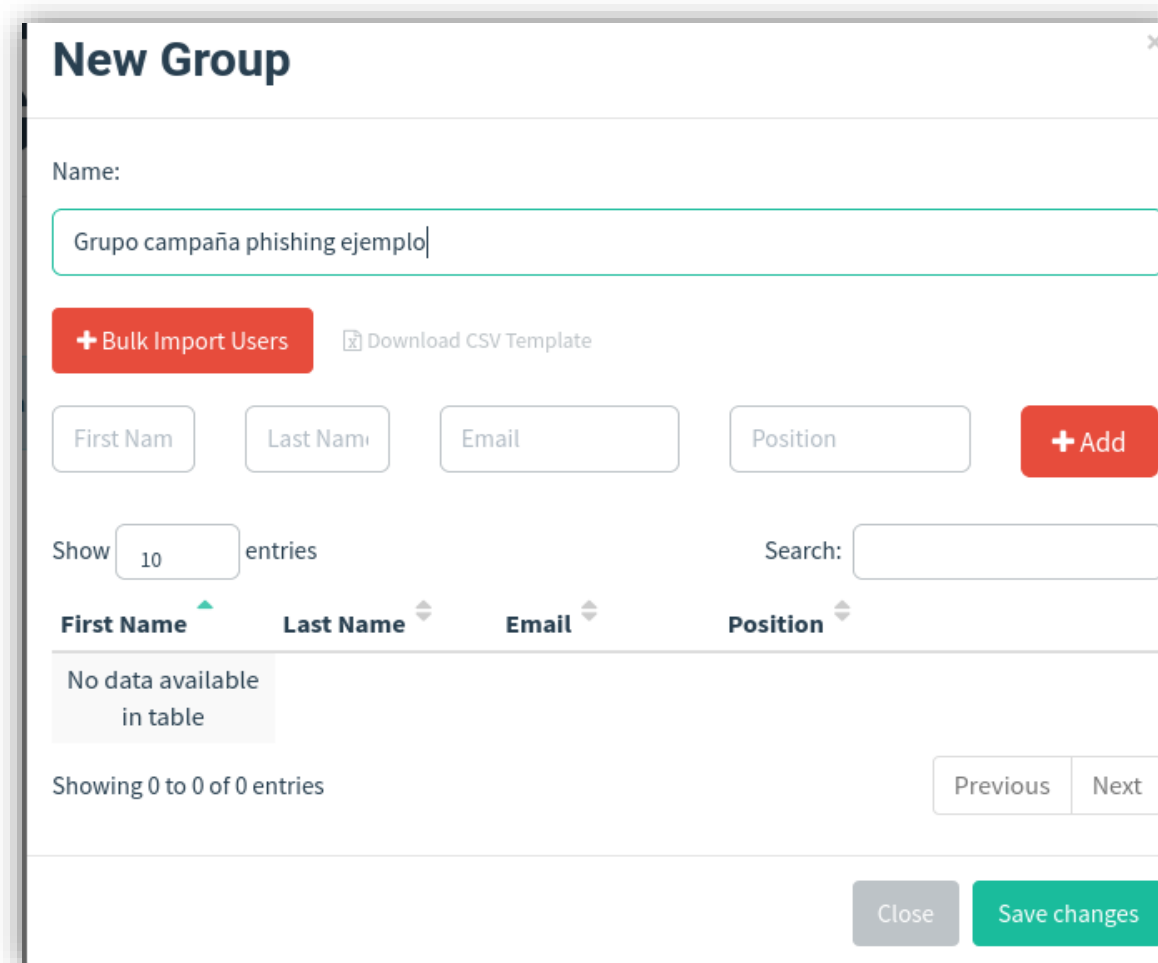


Ilustración 47: Histórico de plantillas guardadas.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- Ahora, haz clic dentro del menú en «*Users & Groups*». En este paso, indicarás los destinatarios por grupos a los que irá dirigida la campaña de *phishing*. Podrás hacerlo uno a uno o podrás importándolos de manera masiva en un archivo CSV. Para finalizar, haz clic en «*Save Changes*».

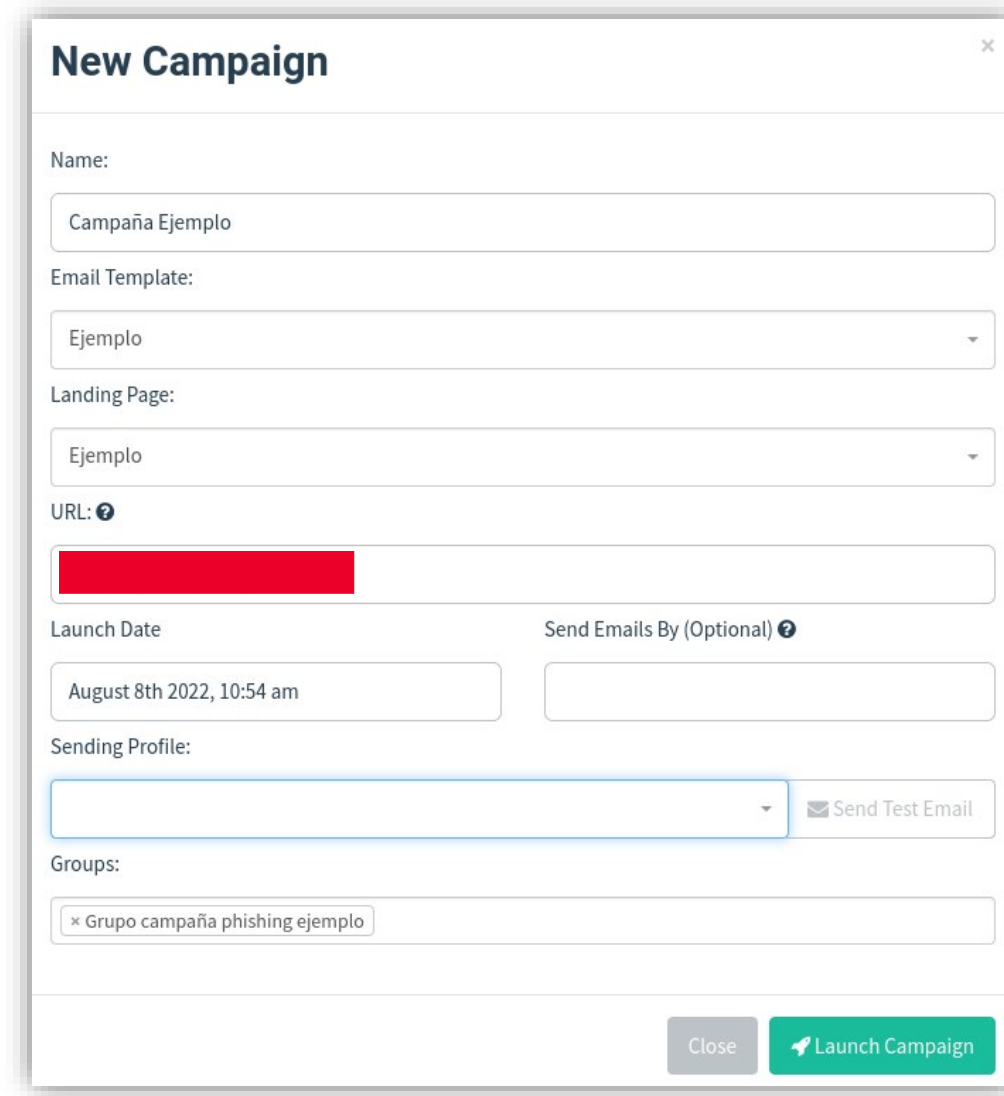


The screenshot shows a 'New Group' modal window. At the top, there's a title bar with a close button. Below it, a 'Name:' label is followed by a text input field containing 'Grupo campaña phishing ejemplo'. Underneath, there are two buttons: a red '+ Bulk Import Users' and a grey 'Download CSV Template'. Below these are four input fields: 'First Name', 'Last Name', 'Email', and 'Position', followed by a red '+ Add' button. Further down, there's a 'Show' dropdown set to '10' and a 'Search:' input field. Below this is a table header with columns: 'First Name', 'Last Name', 'Email', and 'Position'. The table body is empty, showing 'No data available in table'. At the bottom of the table area, it says 'Showing 0 to 0 of 0 entries' and has 'Previous' and 'Next' buttons. At the very bottom of the modal, there are 'Close' and 'Save changes' buttons.

Ilustración 48: Formulario de configuración del público víctima objetivo.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- Tras esta configuración, vamos a crear la campaña. Para ello, accede al menú «*Campaigns*». Dentro de la ventana, selecciona en los respectivos desplegables cada una de las plantillas configuradas anteriormente: *Email*, *Landing Page*, Perfil de envío y Grupos objetivo. Además, también tendrás que definir una fecha de ejecución de la campaña.
 - Un paso muy importante es comprobar de nuevo que nuestra máquina virtual está en modo puente y añadir en el campo «URL» nuestra IP pública seguida del puerto configurado como *listener* en el archivo config.json de GoPhish visto anteriormente.



New Campaign

Name:

Email Template:

Landing Page:

URL:

Launch Date:

Send Emails By (Optional):

Sending Profile:

Groups:

Ilustración 49: Configuración de la campaña de *phishing*.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- A continuación, haz clic en «*Launch Campaign*» para programarla y dejarla lista.

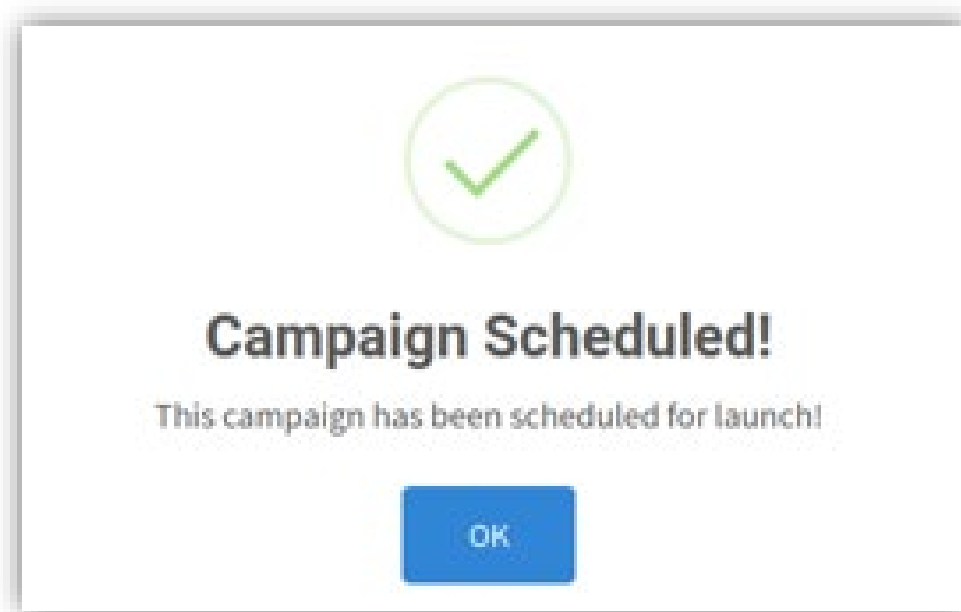


Ilustración 50: Programación de la campaña de *phishing*.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- En este momento, las víctimas objetivo recibirán un correo electrónico según lo que hayamos diseñado.
 - Al hacer clic en el enlace, les redirigirá a la *Landing Page* que hemos configurado.
 - Desde este mismo punto, se podrán ver los resultados de la campaña en el menú «*Dashboard*» de Gophish.
Se podrán visualizar de manera global cuántos correos electrónicos han sido enviados, cuántos de ellos han sido abiertos, cuántos usuarios han hecho clic en el enlace y cuántos de ellos han enviado sus credenciales.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

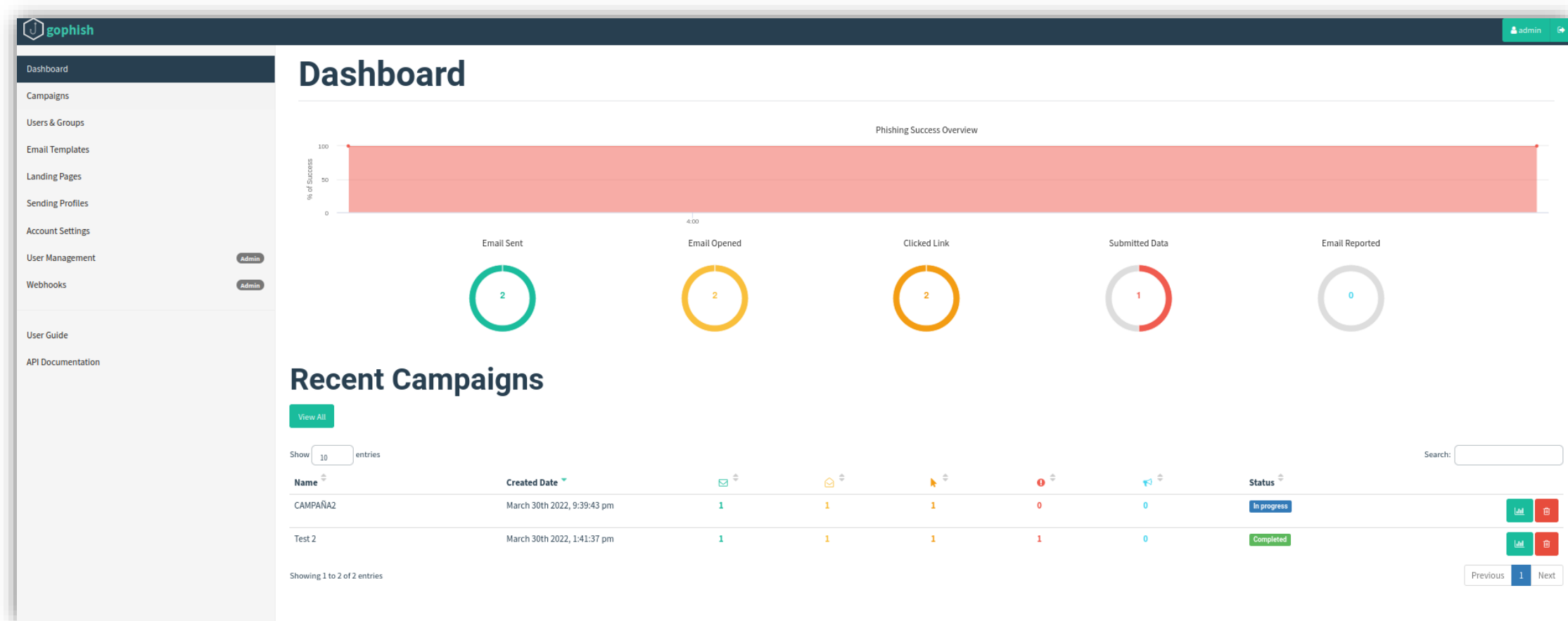


Ilustración 51: Resultados de la campaña en el menú «*Dashboard*» de Gophish.

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- Además, haciendo clic en cada campaña, se podrán ver con más detalle los resultados de cada usuario e incluso qué correo electrónico y qué contraseña han introducido.

Ilustración 52: Resultados por usuario de su correo electrónico y contraseña.

The screenshot displays a 'Timeline for' interface for a phishing campaign. It lists several events with timestamps and user agent information (Windows 10, Chrome 100.0.4896.60). The events include 'Campaign Created', 'Email Sent', 'Email Opened', 'Clicked Link', and 'Submitted Data'. The 'Submitted Data' event is expanded to show a table of parameters and values.

Parameter	Value(s)
__original_url	[REDACTED]
op	Enviar
submitted[nombre]	sfsdfsdfsdf@gmail.com
submitted[pass]	sdfsdfsdf

3 SOLUCIONARIO EJERCICIO PRÁCTICO 5: ATAQUE DE *PHISHING*

- Un paso muy importante es terminar la campaña. Para ello, accede al menú «*Campaigns*» y haz clic en el botón rojo con el símbolo de la papelera.

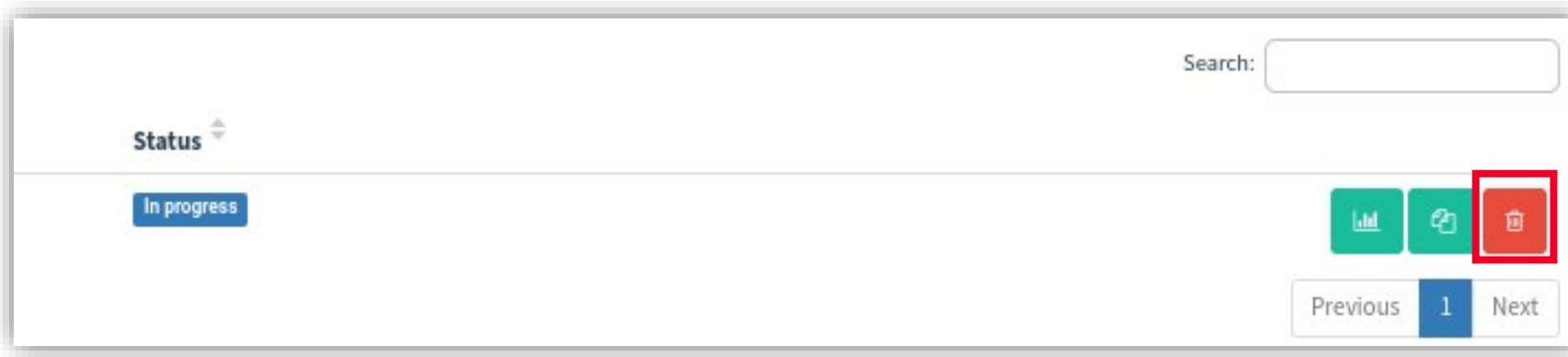


Ilustración 53: Eliminación de la campaña de *phishing*.

¡GRACIAS!



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

