LABORATORIO DE PHISHING CON GOPHISH

INDICE

DISCLAIMER

Esta guía tiene como único propósito educativo y está diseñada para concienciar sobre la seguridad informática mediante la simulación de ataques de phishing en un entorno controlado. Las técnicas descritas deben utilizarse únicamente con el consentimiento explícito de todas las partes involucradas y en un entorno de prueba o corporativo con la autorización necesaria.

El uso indebido de estas técnicas para llevar a cabo actividades malintencionadas es ilegal y puede acarrear graves consecuencias legales. El autor no se hace responsable del mal uso o interpretación de la información proporcionada.

¿QUE ES EL PHISING Y COMO NOS AFECTA EN NUESTRO DIA A DIA?

El phishing es una técnica de ciberataque que busca engañar a las personas para que revelen información confidencial, como contraseñas, datos bancarios o información personal, haciéndoles creer que están interactuando con una entidad legítima. Estos ataques suelen realizarse a través de correos electrónicos, mensajes de texto o sitios web fraudulentos que imitan a organizaciones conocidas, como bancos, empresas tecnológicas o instituciones gubernamentales.

En nuestro día a día, el phishing es una de las amenazas más comunes y efectivas. Los ciberdelincuentes aprovechan momentos de distracción, mensajes urgentes o simulaciones creíbles para hacernos caer en la trampa. Desde correos que fingen ser alertas de seguridad de nuestra cuenta bancaria, hasta solicitudes para "restablecer contraseñas" en servicios como Microsoft o Google, el phishing es una amenaza constante que afecta tanto a individuos como a empresas.

El impacto puede ser devastador: pérdida de datos personales, robos financieros, accesos no autorizados a sistemas corporativos y, en el peor de los casos, fugas de información crítica que comprometen la seguridad de toda una organización.

Es fundamental que estemos preparados para identificar estos ataques, ya que la formación y concienciación son nuestras mejores defensas frente al phishing.

LABORATORIO DE PHISHING CON GOPHISH

En este laboratorio vamos a simular un ataque de phishing utilizando un servidor Ubuntu y la herramienta Gophish, una plataforma de código abierto diseñada para concienciar sobre la seguridad a través de campañas simuladas de phishing. El objetivo es reproducir un escenario donde los usuarios reciben un correo falso indicando que alguien ha iniciado sesión en su cuenta de Spotify, invitándoles a verificar sus credenciales en un portal de inicio de sesión falso.

El proceso incluirá:

- Configurar un servidor Ubuntu como la plataforma base para ejecutar Gophish.
- Diseñar una campaña de phishing con una plantilla de correo y una página web que imite el portal de login de Spotify.
- Enviar el correo a los usuarios simulados para que accedan a la página fraudulenta y capturar las credenciales de quienes caigan en la trampa.

Este laboratorio permite entender cómo los atacantes lanzan campañas de phishing, y la importancia de estar alerta ante correos sospechosos que piden acciones inmediatas sobre nuestras cuentas personales. Además, nos ayuda a aprender técnicas efectivas para mejorar la concienciación sobre la ciberseguridad en entornos corporativos. Además del escenario que recreamos en este laboratorio, existen una infinidad de ataques de phishing que utilizan diferentes tácticas y plataformas.

REQUISITOS

Para realizar este laboratorio de phishing simulado, necesitaremos los siguientes elementos:

- **Servidor Ubuntu:** Un servidor Ubuntu (local o en la nube) donde se instalará y configurará Gophish para gestionar la campaña de phishing.
- **Gophish:** Instalación de la herramienta Gophish, que permitirá crear y gestionar la campaña de phishing, plantillas de correos y landing pages.
- **Dominio o dirección IP pública:** (Opcional pero recomendado) Para hacer que el ataque sea lo más realista posible, es recomendable utilizar un dominio personalizado que simule una entidad legítima (por ejemplo, un dominio similar al de una empresa). Esto aumenta la credibilidad del ataque y puede engañar más fácilmente a los usuarios.
  Sin embargo, no es estrictamente necesario. También puedes utilizar la dirección IP pública de tu servidor para enlazar las landing pages y enviar los correos de phishing.
- **Servidor SMTP:** Un servidor SMTP configurado para enviar los correos de phishing. Puedes optar por configurar un servidor propio en Ubuntu o utilizar un servicio de terceros (como Gmail o un servicio de correo corporativo).

INSTALACION UBUNTU SERVER

He instalado Ubuntu Desktop 22.04.3 en una máquina virtual utilizando VirtualBox como entorno de virtualización. Este sistema operativo será la base para llevar a cabo todo el laboratorio de phishing. Si deseas replicar este entorno, puedes seguir la guía oficial de instalación de Ubuntu desde el siguiente enlace:

https://ubuntu.com/tutorials/install-ubuntu-desktop#1-overview

Esta guía te llevará paso a paso para instalar Ubuntu Desktop en tu equipo o en una máquina virtual.

Respecto al adaptador de red, lo he configurado en “Red NAT”, pero también se puede realizar en Adaptador Puente.

INSTALACION Y CONFIGURACION GOPHISH

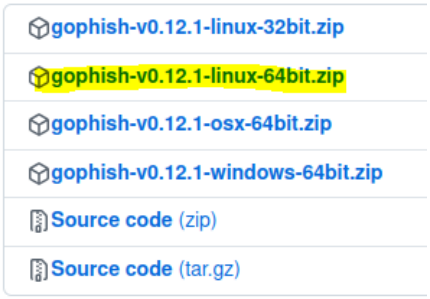
Una vez instalado nuestro Ubuntu, vamos a descargar y configurar la herramienta Gophish

Antes de comenzar con la instalación, es importante actualizar los paquetes del sistema

```
sudo apt update && sudo apt upgrade -y
```

Accedemos al sitio oficial de Gophish y nos descargamos la versión más reciente de nuestro SO, en mi caso Linux-64bit.

https://github.com/gophish/gophish/releases



Descomprimimos el fichero y damos permisos de ejecución al binario gophish

```
unzip gophish-v0.12.1-linux-64bit.zip
chmod +x gophish
```

```
kesh@srv-cibertercios:~/Gophish$ unzip -q gophish-v0.12.1-linux-64bit.zip
kesh@srv-cibertercios:~/Gophish$ ls
config.json  db  gophish  gophish-v0.12.1-linux-64bit.zip  LICENSE  README.md  static  templates  VERSION
kesh@srv-cibertercios:~/Gophish$ chmod +x gophish
kesh@srv-cibertercios:~/Gophish$ ls -la gophish
-rwxr-xr-x 1 kesh kesh 21525728 sep 14  2022 gophish
kesh@srv-cibertercios:~/Gophish$
```

Abrimos y editamos el fichero config.json para configurarle una ip y puerto de gestión de la herramienta, que por defecto es la IP localhost y el puerto 3333, y la IP del servidor web.

```
ip a
```

```
kesh@srv-cibertercios:~/Gophish$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9e:37:a2 brd ff:ff:ff:ff:ff:ff
    inet 14.14.1.140/24 brd 14.14.1.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::77cf:3a63:c0a:5295/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

En mi caso la IP del servidor es: 14.14.1.140

nano config.json

```
kesh@srv-cibertercios:~/Gophish$ nano config.json
kesh@srv-cibertercios:~/Gophish$ cat config.json
{
        "admin_server": {
                "listen_url": '14.14.1.140:8888',
                "use_tls": true,
                "cert_path": "gophish_admin.crt",
                "key_path": "gophish_admin.key",
                "trusted_origins": []
        },
        "phish_server": {
                "listen_url": '14.14.1.140:80',
                "use_tls": false,
                "cert_path": "example.crt",
                "key_path": "example.key"
        },
        "db_name": "sqlite3",
        "db_path": "gophish.db",
        "migrations_prefix": "db/db_",
        "contact_address": "",
        "logging": {
                "filename": "",
                "level": ""
        }
}

kesh@srv-cibertercios:~/Gophish$
```

Cambiamos ambas listen_url, y en mi caso el puerto de administración de la herramienta se lo he cambiado al 8888, y el del servidor web en el 80, en caso de querer realizar un servidor https y tener un certificado y su llave, solo lo tendríamos que cambiar en las variables cert_path y key_path

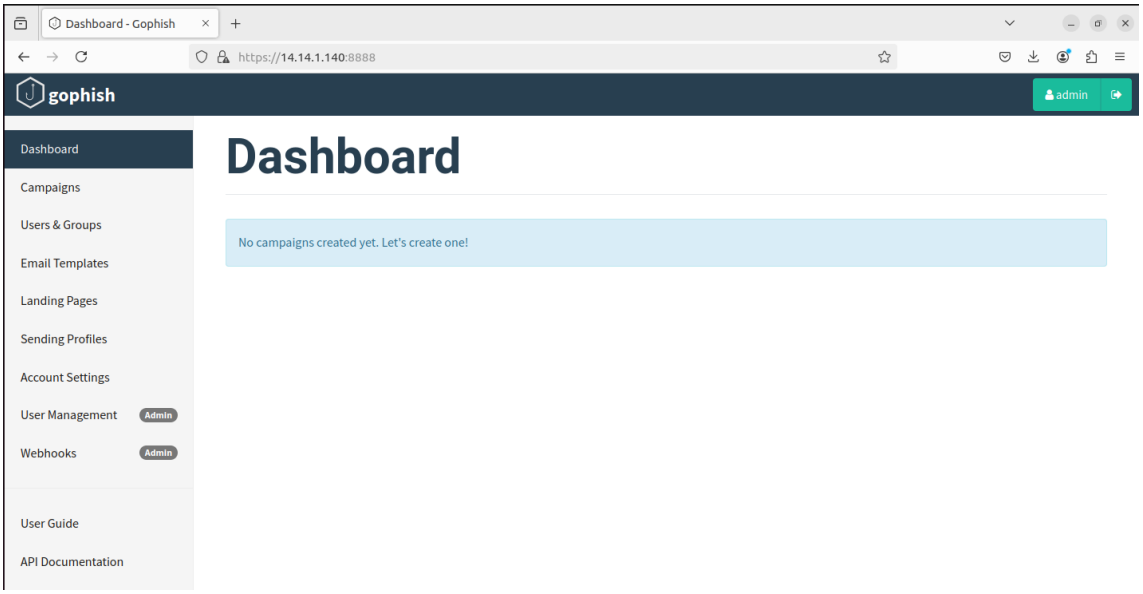
Una vez realizados estos cambios, iniciamos la herramienta e iniciamos sesión con el usuario admin y la pass la tenemos que copiar desde la terminal, en el arranque de la herramienta nos la indica.

sudo ./gophish

```
kesh@srv-cibertercios:~/Gophish$ sudo ./gophish
time="2024-10-24T23:02:25+02:00" level=warning msg="No contact address has been configured."
time="2024-10-24T23:02:25+02:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2024-10-24T23:02:25+02:00" level=info msg="Please login with the username admin and the password 3605f4d2ee0dee94"
time="2024-10-24T23:02:25+02:00" level=info msg="Starting IMAP monitor manager"
time="2024-10-24T23:02:25+02:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2024-10-24T23:02:25+02:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2024-10-24T23:02:25+02:00" level=info msg="Starting phishing server at http://14.14.1.140:80"
time="2024-10-24T23:02:25+02:00" level=info msg="Starting new IMAP monitor for user admin"
time="2024-10-24T23:02:25+02:00" level=info msg="TLS Certificate Generation complete"
time="2024-10-24T23:02:25+02:00" level=info msg="Starting admin server at https://14.14.1.140:8888"
```

Iniciamos nuestro navegador y nos conectamos a nuestra IP y al puerto de administración que le hayamos configurado.

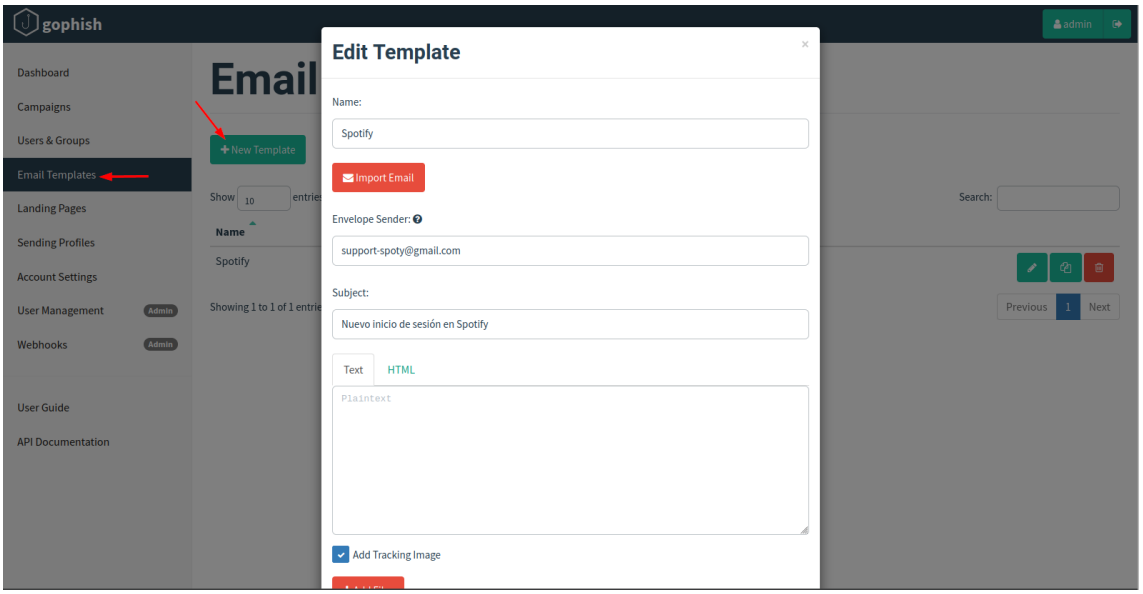
Una vez nos logamos nos pide cambiar la contraseña y ya podemos comenzar a utilizar la herramienta.



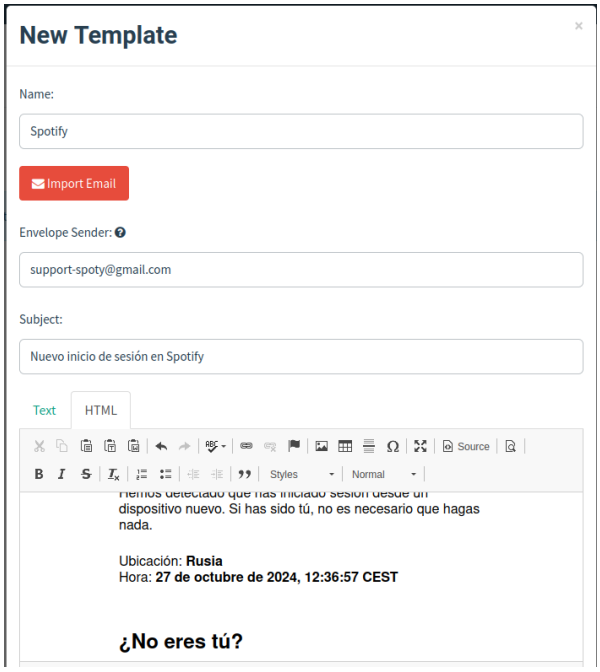
EMAIL TEMPLATE

Un Email Template en Gophish es una plantilla de correo electrónico que simula ser un mensaje legítimo para engañar a los destinatarios, con el objetivo de recolectar datos en un entorno controlado. Estas plantillas se personalizan para replicar correos electrónicos de entidades confiables (como servicios de streaming, bancos, etc.) y suelen incluir enlaces que llevan a páginas falsas (landing pages) que configuraremos más adelante.

Email Templates > New Template



Y ya podemos configurar nuestro correo para engañar a nuestras víctimas.



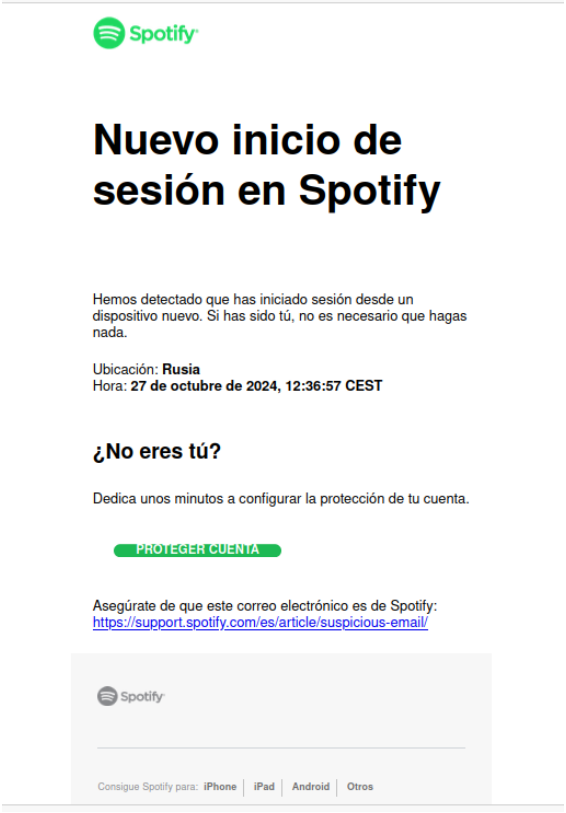
- **Name:** Se refiere al nombre que le vamos a dar a la template.
- **Envelope Sender:** Se refiere a la dirección de correo desde la que vamos a enviar esta template de correo.
- **Subject:** Se refiere al asunto del correo

A continuación, debemos configurar nuestro código HTML para que el correo tenga un aspecto lo más realista posible. Es crucial que, al insertar los enlaces y botones en el correo, estos redirijan a la dirección de nuestro servidor de phishing, donde la víctima será conducida a una página diseñada para capturar credenciales u otra información sensible.

Aquí es donde entra en juego la opción de utilizar un dominio personalizado o, en su defecto, una IP pública. Utilizar un dominio permite hacer que el ataque parezca más legítimo, ya que los usuarios suelen confiar más en un dominio que en una IP. Sin embargo, no siempre es necesario un dominio; si la campaña está dirigida a una red interna, se puede utilizar una IP local.

En este ejemplo, hemos configurado el servidor en una red local, pero si quisiéramos que usuarios fuera de esta red puedan acceder, es posible exponer el servidor a Internet mediante port forwarding. Este método redirige el tráfico de una IP pública (como la de tu router) hacia la IP privada del servidor en la red local, permitiendo que usuarios externos accedan al servidor de phishing desde cualquier lugar. Explicaremos cómo hacerlo en detalle más adelante.

Mi plantilla quedaría tal que así:



En estas plantillas recomiendo mirar la documentación oficial para configurar todo correctamente y entender como funcionan las templates y las referencias para redirigir a las víctimas a las landing pages.

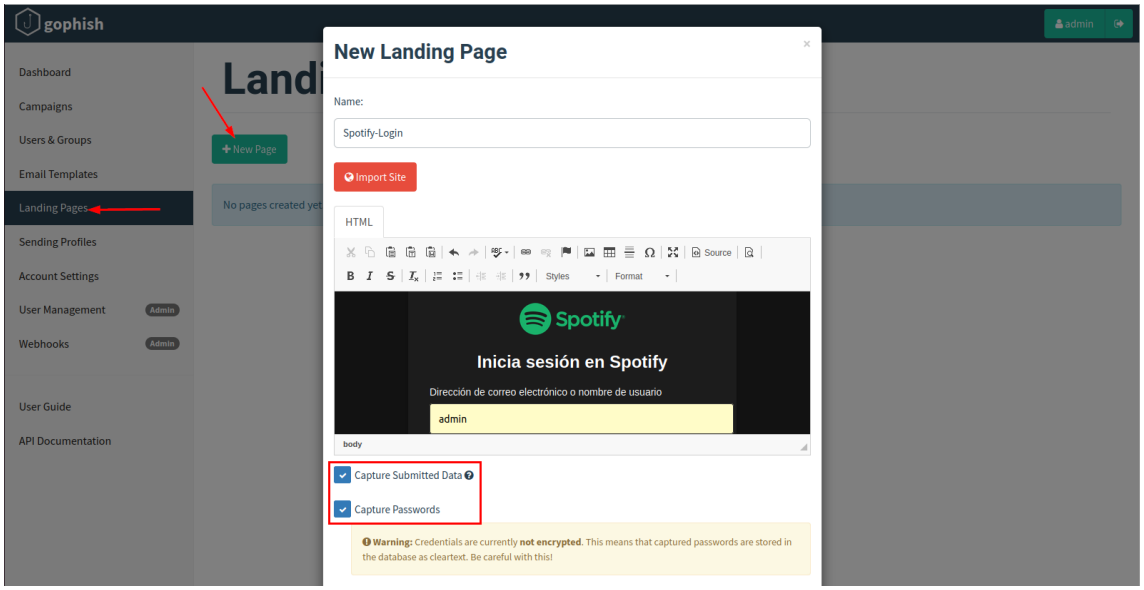
https://docs.getgophish.com/user-guide/documentation/templates

https://docs.getgophish.com/user-guide/template-reference

LANDING PAGES

Las landing pages en el contexto de una campaña de phishing son páginas web a las que los usuarios son dirigidos tras hacer clic en un enlace en un correo electrónico o mensaje malicioso. Estas páginas suelen estar diseñadas para imitar sitios legítimos, como servicios populares (bancos, redes sociales, plataformas de streaming, etc.), con el objetivo de engañar a los usuarios y hacer que ingresen información sensible, como credenciales de inicio de sesión, números de tarjetas de crédito, entre otros.

Landing Pages > New Page



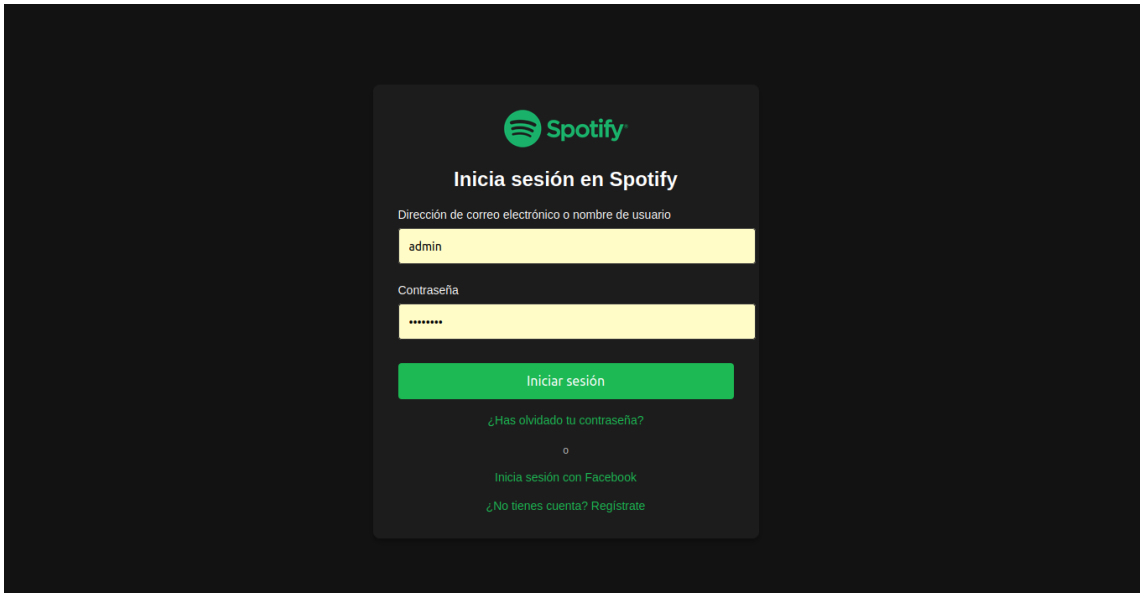
En este apartado, lo único que tenemos que hacer es agregar un nombre de landing page, junto con el código html que simula el panel de login, en este caso de Spotify para capturar las credenciales de nuestras víctimas.

¡IMPORTANTE!

Habilitar la captura de los datos introducidos, tanto usuarios/correos como sus contraseñas.

¡IMPORTANTE!

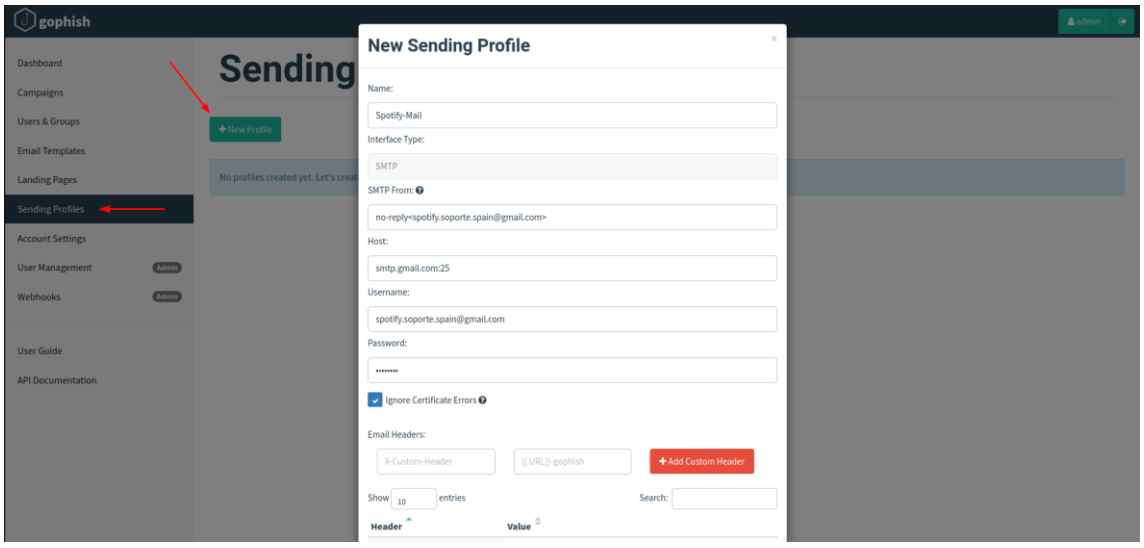
La página que he configurado se vería tal que así;



SENDING PROFILES

Los sending profiles en herramientas de phishing como Gophish son configuraciones que definen el perfil de envío de correos electrónicos en una campaña de phishing. Básicamente, especifican detalles clave sobre el remitente, como la dirección de correo desde la que se enviarán los mensajes y el servidor SMTP que utilizará para realizar el envío. Estos perfiles permiten personalizar el remitente para que el correo se vea más auténtico y realista, aumentando la probabilidad de que el usuario objetivo abra el mensaje y haga clic en los enlaces proporcionados.

Sending profiles > New profile

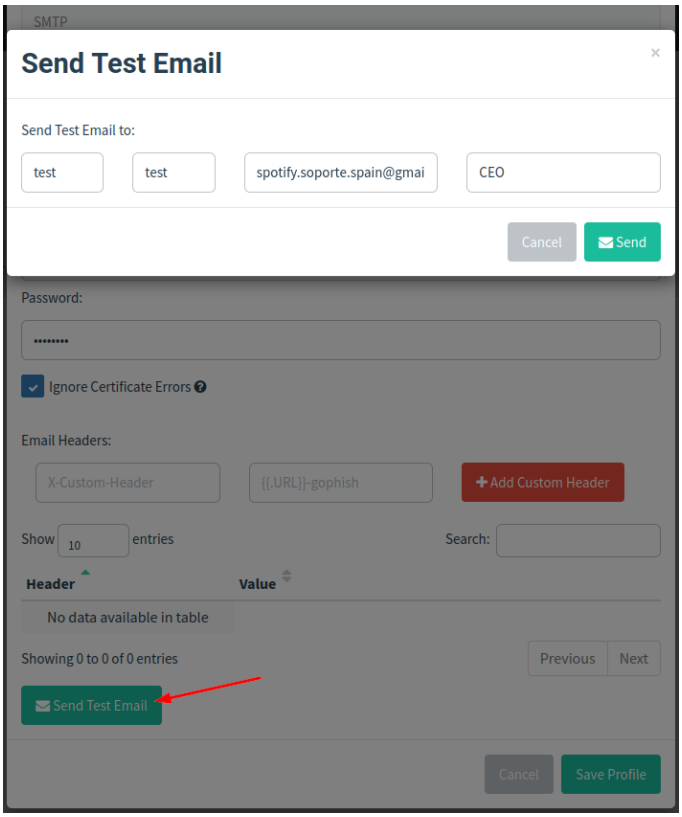


Las opciones que se pueden configurar son:

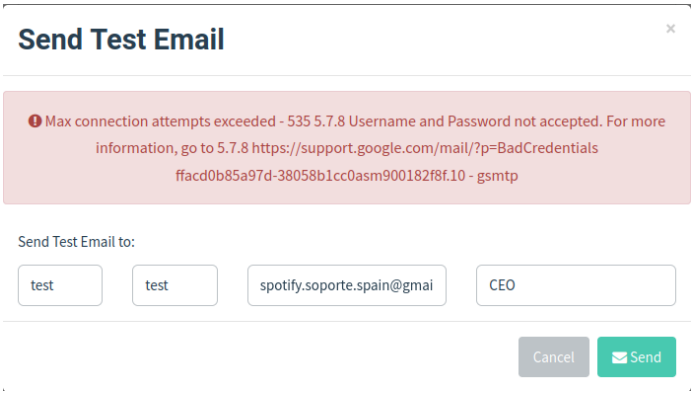
- **Name:** Se refiere al nombre que le vamos a dar a nuestro sending profile.
- **SMTP Form:** representa la dirección de correo electrónico que se mostrará como remitente en los correos electrónicos de la campaña de phishing. Es la dirección que los usuarios verán en su bandeja de entrada como "De:" o "From:", lo cual ayuda a simular que el mensaje proviene de una fuente confiable.
- **Host:** se refiere a la dirección del servidor SMTP que se utilizará para enviar los correos de la campaña de phishing.
- **Username y password:** Se refiere a las credenciales de una dirección de correo electrónico válida

En mi caso he utilizado el servidor SMTP de Gmail, ya que me he creado una nueva cuenta de correo electrónico para este laboratorio.

Podemos probar si el SMTP funciona correctamente, para ello podemos utilizar la opción de 'Send Test Email'



En este caso vamos a probar si se pueden enviar correos desde este servidor smtp.

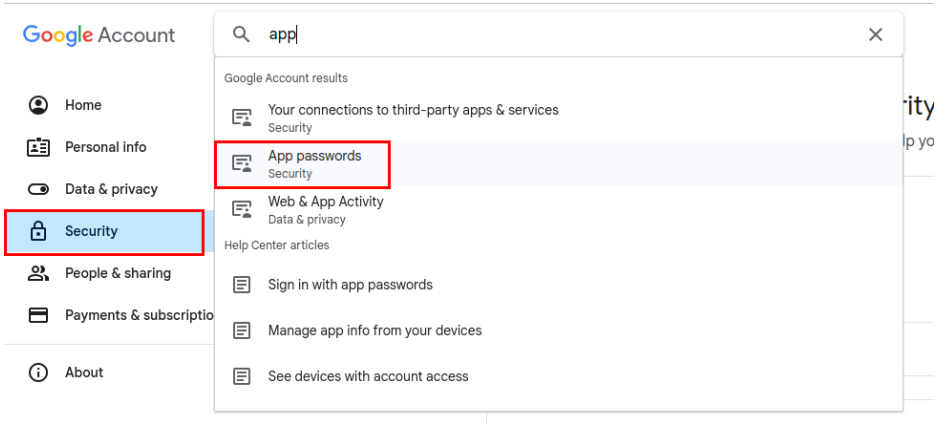


Este error es bastante común al utilizar el servidor SMTP de Gmail para enviar correos a través de herramientas como Gophish. Gmail aplica medidas de seguridad estrictas para proteger las cuentas, y muchas veces bloquea los intentos de conexión desde aplicaciones de terceros que intentan enviar correos mediante el protocolo SMTP, especialmente si no cumplen con los requisitos de autenticación de dos factores.

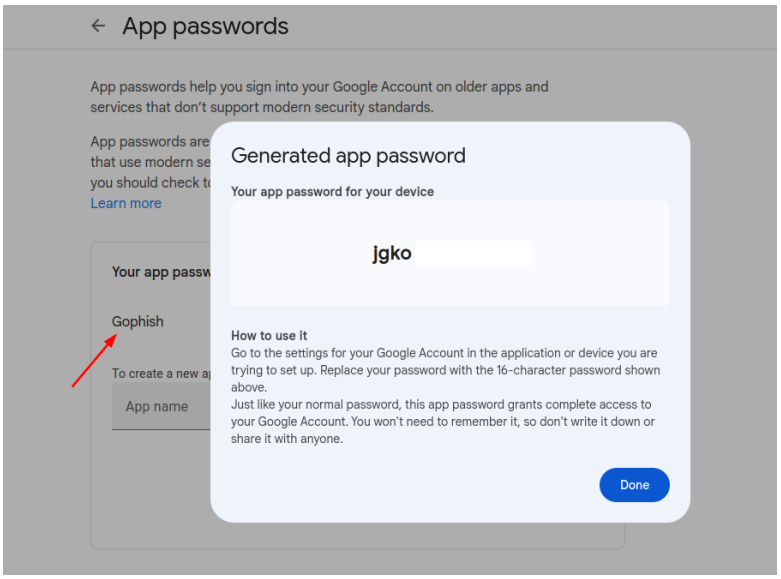
Para resolverlo, es necesario que la cuenta de Gmail que se está utilizando tenga habilitada la autenticación multifactor (MFA). Además, en el caso de Google, se debe crear una contraseña de aplicación específica. Esta contraseña especial permite que aplicaciones externas (como Gophish) puedan conectarse y enviar correos de manera segura sin comprometer la seguridad de la cuenta principal.

Para configurar esta contraseña nos vamos a:

Configuración de cuente > Seguridad > APP Passwords

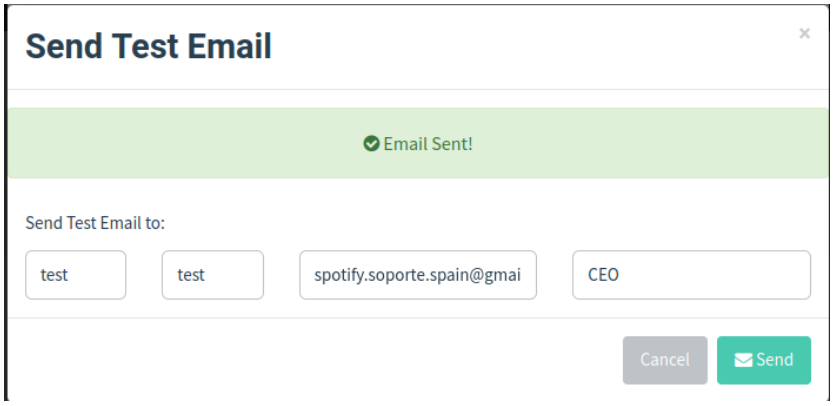


Generamos una nueva contraseña de aplicación específica para Gophish y utilizamos esta contraseña en lugar de la contraseña principal al configurar el perfil de envío en Gophish.

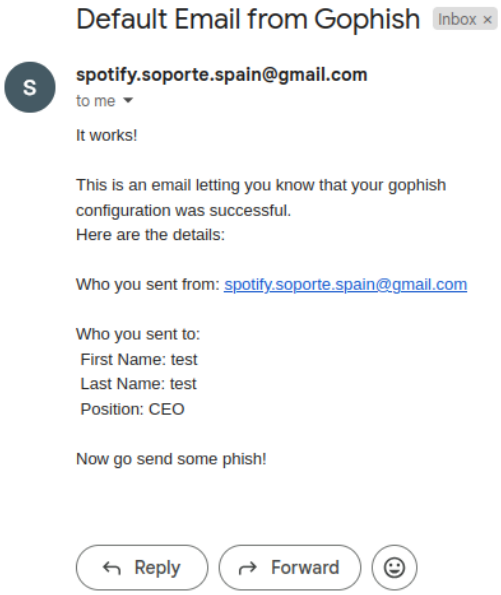


Este proceso garantiza que Gmail permita el acceso y el envío de correos desde la cuenta a través de SMTP, sin que los bloqueos de seguridad interfieran.

Una vez añadimos esta contraseña en el sending profile, volvemos a realizar la prueba y vemos que ya se envía correctamente el correo.



Si nos vamos a nuestro correo, podemos ver en la bandeja de entrada que nos ha llegado este nuevo correo de prueba.



Hasta este punto, ya hemos configurado los elementos clave para nuestra campaña de phishing:

1. **Email Template:** el diseño y contenido del correo que recibirán las víctimas, simulando un mensaje legítimo para aumentar su efectividad.
2. **Landing Page:** la página web que imitará a un sitio legítimo donde se solicitarán las credenciales u otra información sensible.
3. **Sending Profiles:** el perfil de envío de correos, con los detalles de autenticación y el servidor SMTP configurado para el envío de mensajes.

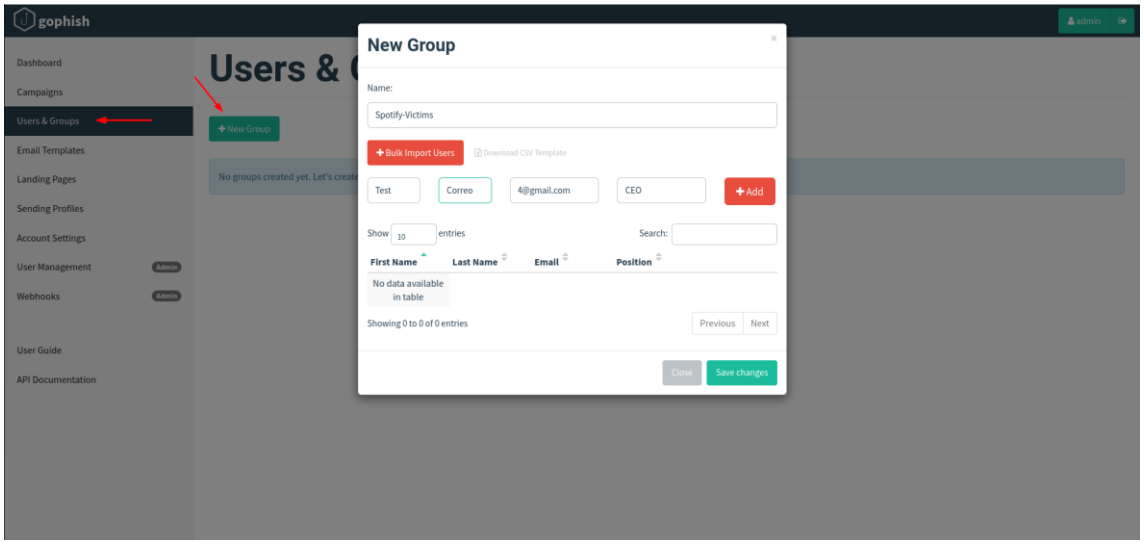
Ahora solo nos queda un paso crucial, añadir a nuestras víctimas o destinatarios, quienes recibirán los correos de la campaña. A continuación, configuraremos los destinatarios y lanzaremos la campaña para evaluar su efectividad y el nivel de concienciación de los usuarios.

USERS & GROUPS

La sección de Users & Groups permite gestionar los destinatarios de la campaña de phishing. Aquí puedes crear grupos de usuarios o listas de contactos que recibirán los correos electrónicos de la campaña, facilitando la organización y segmentación de los objetivos según criterios específicos (departamento, nivel de acceso, etc.).

Cada grupo contiene una lista de destinatarios con información básica como nombre y dirección de correo. Esta estructura también facilita el análisis de resultados una vez lanzada la campaña, ya que puedes evaluar la respuesta de cada grupo por separado y obtener una visión detallada del comportamiento de los usuarios frente al phishing.

User&Groups > New Group



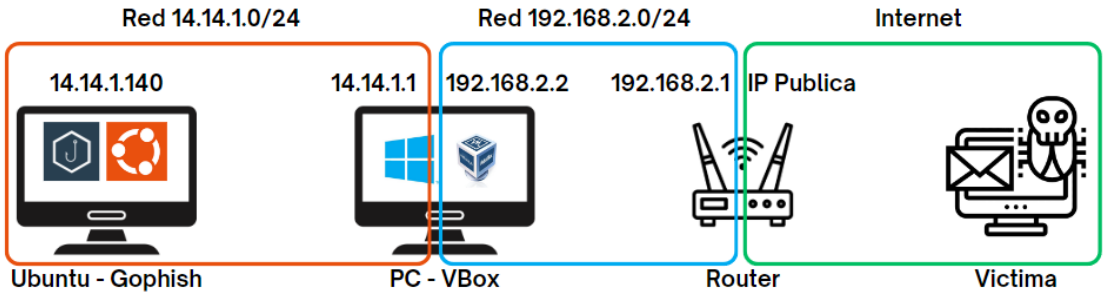
Con los usuarios y grupos ya añadidos como destinatarios de nuestra campaña de phishing, tenemos todo listo para el último paso: crear y lanzar la campaña. Al configurar la campaña, seleccionaremos el email template, la landing page, el perfil de envío (sending profile) y el grupo de usuarios objetivo. Este paso es fundamental, ya que nos permitirá iniciar el envío de correos y comenzar a recopilar datos sobre la interacción de los usuarios, como aperturas, clics en enlaces y, en caso de que intenten iniciar sesión, la captura de credenciales.

PORT FORWARDING

El port forwarding o reenvío de puertos es una técnica que permite que las solicitudes de conexión desde Internet lleguen a un dispositivo específico dentro de una red privada. En este caso, si quieres que tu servidor de phishing esté accesible desde fuera de tu red local, necesitas configurar el port forwarding en tu router para redirigir el tráfico que llega a la IP pública (asignada por tu proveedor de Internet) hacia la IP interna de tu servidor.

Cómo funciona el port forwarding:

- **IP Pública:** Es la dirección que tu ISP (Proveedor de Servicios de Internet) asigna a tu conexión de red. Es única y permite que otros dispositivos en Internet puedan enviarte datos. Todas las conexiones desde Internet apuntan primero a esta IP.
- **Configuración del puerto:** En el router, se configura una regla que asocia un puerto específico (por ejemplo, el puerto 8080 para HTTP) con la IP interna de tu servidor de phishing en la red local. Esto asegura que cualquier tráfico que llegue a la IP pública en ese puerto sea redirigido al dispositivo correspondiente.
- **Acceso desde Internet:** Una vez configurado el port forwarding, los usuarios externos que accedan a tu IP pública y el puerto configurado (por ejemplo, http://tu_ip_publica:8080) serán dirigidos al servidor donde está tu herramienta de phishing.



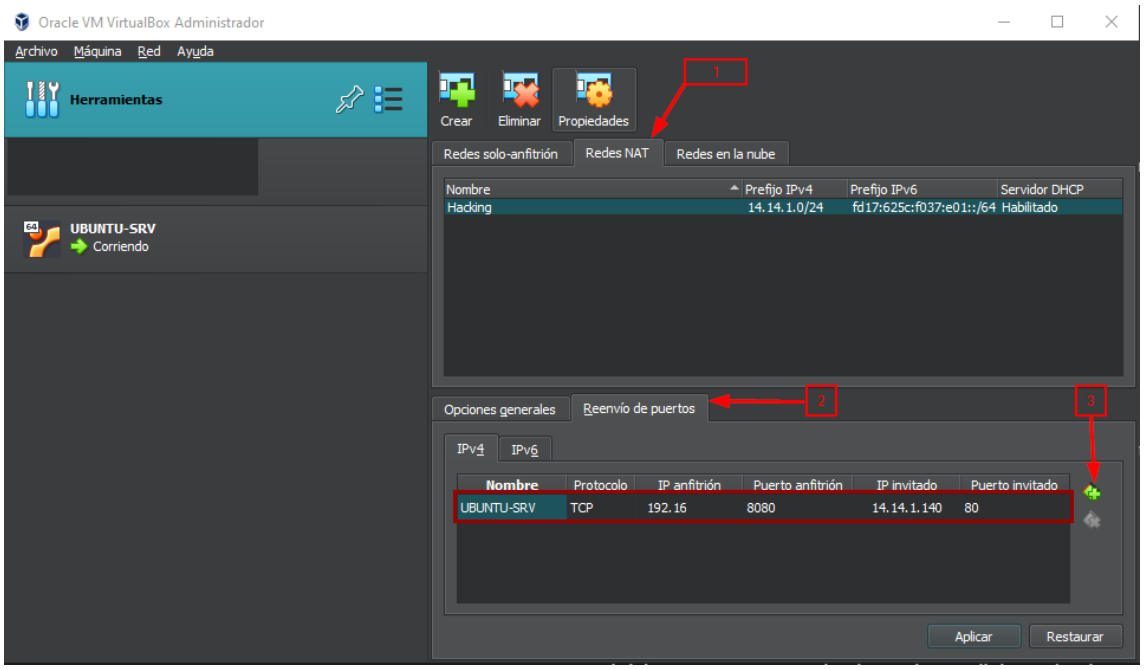
En este caso, vamos a realizar dos configuraciones de port forwarding para que nuestro servidor de phishing, que está en una red NAT interna de VirtualBox, sea accesible tanto desde la red local como desde Internet.

- **Primer Port Forwarding:** VirtualBox a Red Local (NAT a red local). Como el servidor de phishing se aloja en una red NAT dentro de VirtualBox (en la topología, la red naranja), necesitamos un reenvío de puertos dentro de la configuración de VirtualBox. Este primer port forwarding permite que el tráfico de la red local (la red azul) pueda llegar al servidor de phishing, redirigiendo el tráfico del puerto 80 de la IP 14.14.1.140 (configurada para la máquina VirtualBox) hacia la IP local 192.168.2.2 en el puerto 8080. Con esta configuración, el servidor de phishing ya será accesible desde cualquier dispositivo en la red local (red azul).
- **Segundo Port Forwarding:** Red Local a Internet (Red local al router). Para que el servidor de phishing sea accesible desde cualquier lugar de Internet, configuramos un segundo port forwarding en el router de la red local. En este caso, redirigimos las conexiones entrantes de la IP pública del router, asignada por el ISP, en el puerto 8080 hacia la IP interna 192.168.2.2:8080. De esta manera, cuando alguien acceda a la IP pública de tu red en el puerto 8080, el tráfico será dirigido al servidor de phishing, haciéndolo accesible desde cualquier ubicación externa.

Estas dos configuraciones permiten, por un lado, que cualquier dispositivo de la red local acceda al servidor, y por otro, que este mismo servidor también sea accesible desde fuera de la red local a través de la IP pública.

Para realizar el reenvío de puertos en vbox nos vamos a herramientas de red y seguimos los pasos de la imagen:

1. Seleccionamos redes NAT
2. Nos vamos a la pestaña de reenvío de puertos
3. Hacemos click en el icono de agregar un nuevo reenvío de puertos
4. Configuramos el nombre, protocolo, IP anfitrión, puerto anfitrión, IP invitado y puerto invitado. En este caso lo anfitrión es mi red local y lo invitado es la red NAT.



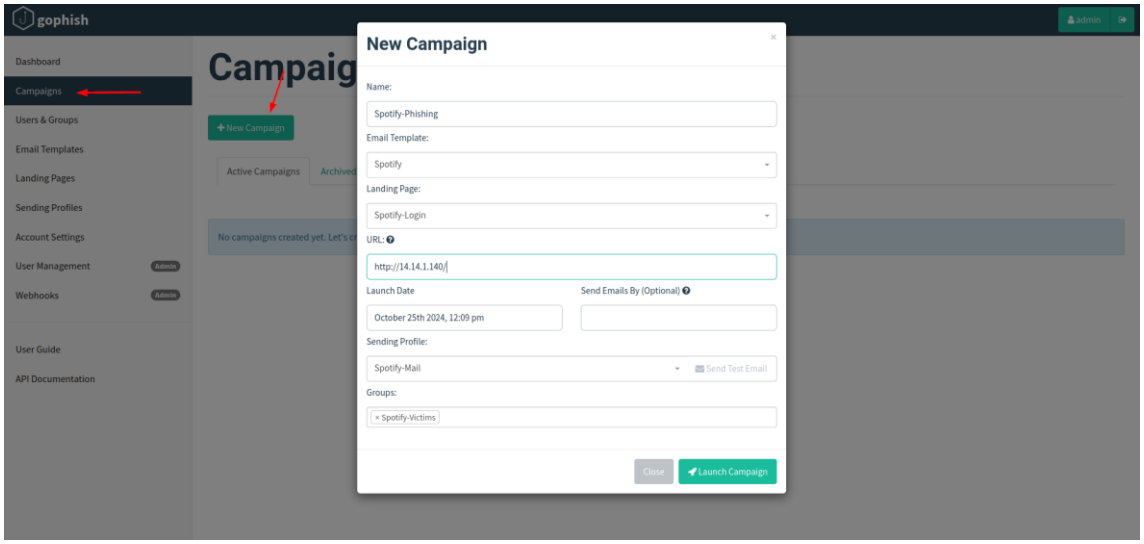
Una vez tenemos este reenvío de puertos realizado, debemos de hacer el segundo en el router, que para este paso os recomiendo buscar información en la pagina oficial de vuestro ISP sobre como realizar un port forwarding.

Una vez tenemos realizados los 2 port forwarding necesitamos saber cual es nuestra IP pública, la cual podemos ver googleando “Cual es mi IP”

CAMPAÑA DE PHISHING

Una vez que se han configurado todos los elementos necesarios como los perfiles de envío (sending profiles), las plantillas de correo (email templates), las páginas de aterrizaje (landing pages) y los usuarios o grupos a los que se enviarán los correos.

Campaigns > New Campaign



Antes de lanzar la campaña, es fundamental revisar todos los componentes configurados, como el email template, la landing page, los perfiles de envío y la lista de usuarios. Asegúrate de que no haya errores y que todos los elementos estén correctamente configurados.

En Gophish, se crea una nueva campaña seleccionando las opciones previamente configuradas. Esto incluye:

- **Email Template:** Selecciona el template que se utilizará para enviar el correo.
- **Landing Page:** Escoge la página de aterrizaje donde los usuarios serán dirigidos.
- **Sending Profile:** Selecciona el perfil de envío para determinar desde qué dirección de correo se enviarán los mensajes.
- **Programación:** Puedes optar por enviar los correos de inmediato o programar el envío para una fecha y hora específicas. Esta opción es útil para crear un sentido de urgencia o para realizar el ataque en un momento en que los usuarios son más propensos a interactuar.

Lanzamos la campaña y en el dashboard podemos ver de forma grafica el estado de esta.

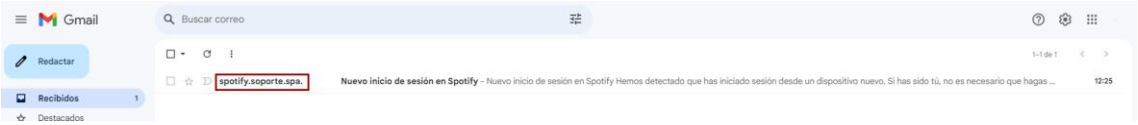
Después del lanzamiento, es importante monitorear el rendimiento de la campaña. Gophish ofrece un panel de control donde puedes ver métricas como:

- **Tasa de apertura:** Cuántos destinatarios han abierto el correo.
- **Clics en el enlace:** Cuántos han hecho clic en el enlace de la landing page.
- **Credenciales capturadas:** Cuántos usuarios han ingresado sus datos en la landing page.

El lanzamiento de la campaña es el momento culminante del trabajo realizado hasta ahora. Proporciona una oportunidad para evaluar la efectividad de la capacitación en seguridad de los empleados y su capacidad para reconocer intentos de phishing. Al final de la campaña, podrás analizar los resultados y obtener información valiosa para mejorar la concienciación sobre la seguridad en la organización, así como ajustar futuros programas de formación y simulaciones.

VICTIMA

La campaña ya ha sido lanzada, por lo que se han enviado los correos a nuestras víctimas, por lo que vamos a nuestro buzón de correo y....

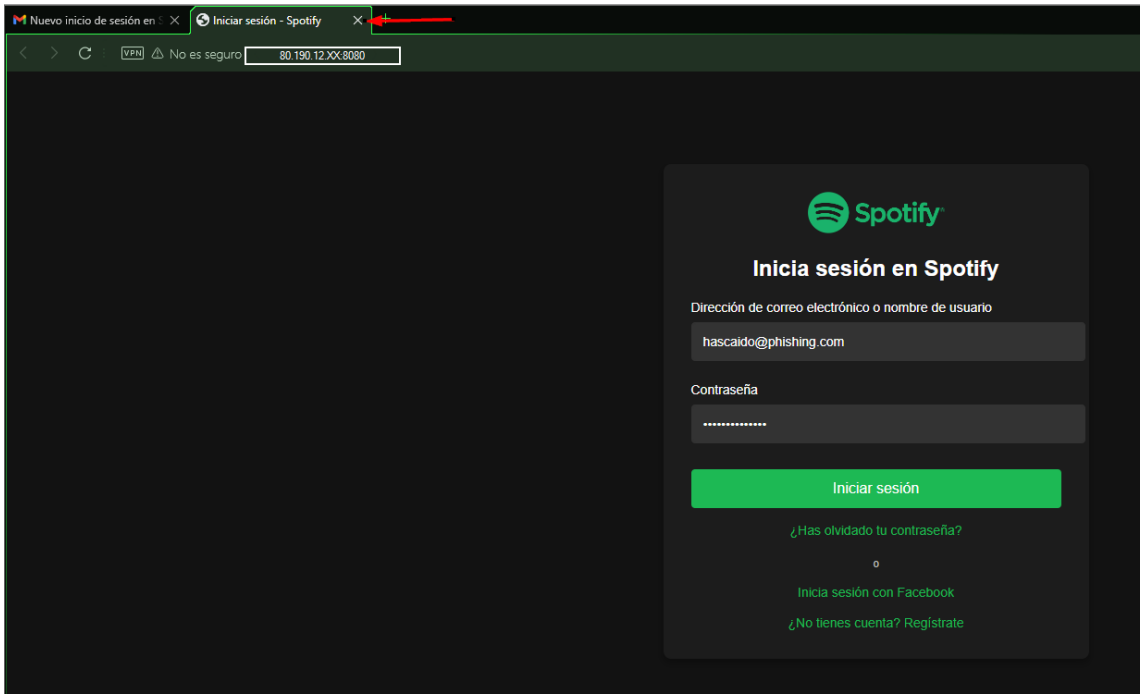


Vemos el correo en la bandeja de entrada, pero en ocasiones estos correos pueden aparecer directamente en la bandeja de SPAM, por lo que recomiendo realizar varias pruebas antes para intentar solucionar ese problema.

Abrimos el correo para ver el contenido de este:

Como podemos observar el correo es idéntico a un correo enviado por la propia empresa, por ello es muy importante saber identificar quien nos envía el correo, y al ver un inicio de sesión, en este caso desde rusia, nos podemos asustar y hacer click en el botón verde para realizar las acciones pertinentes en nuestra cuenta.

En el momento que abre el enlace, ve nuestro servidor, la landing page configurada previamente.



La web también es muy parecida a la original, pero lo que nos falla es la URL, ya que al no tener un dominio aparece nuestra IP publica y puerto configurado (es una IP aleatoria en la imagen).

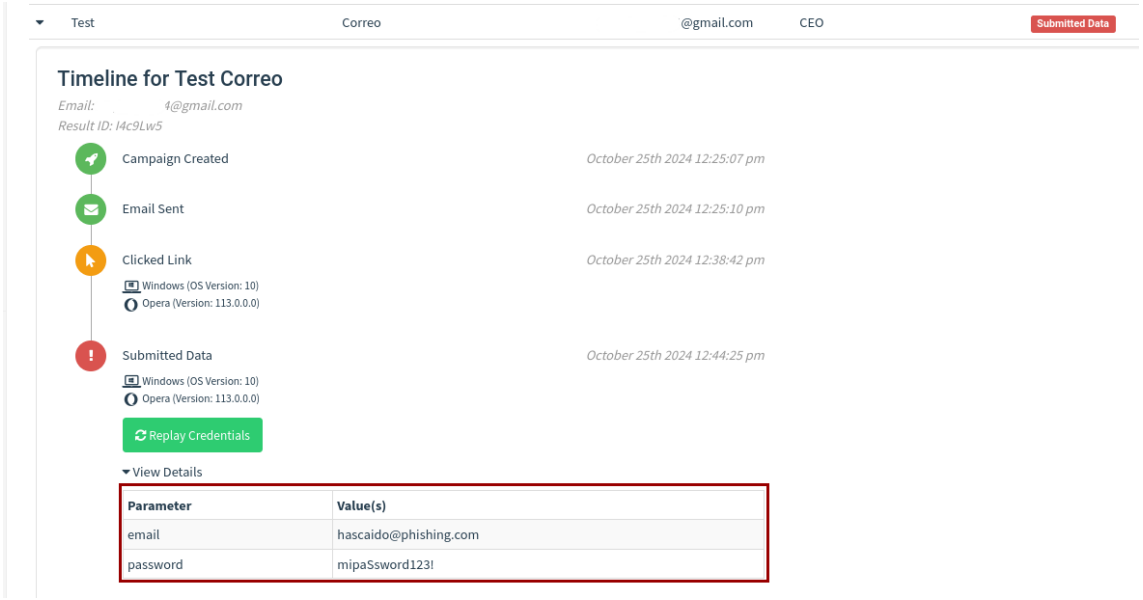
En el momento que introducimos los datos nos redirige a la pagina oficial de login de Spotify, que así lo hemos configurado en la landing page.

CAPTURA DE CREDENCIALES

Una vez la victima a introducido sus credenciales, en el dashboard de la aplicación ya nos aparecen nuevos datos

Podemos ver que aparece como que han abierto el email, han clickado el enlace y, por último, lo han rellenado.

Para ver las credenciales y más información acerca del usuario que ha caído en nuestro phishing, en Details, hacemos click en el nombre del usuario.



Además, nos aparece información extra sobre el navegador que ha utilizado y el SO.

En caso de realizar esta campaña a una organización con cientos de empleados, se pueden exportar los resultados en forma de csv, para ser analizados de forma mas sencilla en Excel, dando tambien información como por ejemplo desde que IP publica se han conectado a nuestro servidor de phishing.

Una vez hemos completado la campaña, se quedará guardada en la pestaña de archived campaigns, donde podremos seguir viendo los resultados de la campaña e incluso copiarla para volver a realizarla.

CONCLUSION

Este laboratorio ha demostrado cómo simular ataques de phishing utilizando Gophish en un servidor Ubuntu. Aprendimos a configurar herramientas, crear páginas de aterrizaje efectivas y personalizar campañas para identificar vulnerabilidades en los usuarios. Además, implementamos técnicas como el port forwarding para alcanzar a usuarios externos y evaluamos sus respuestas para mejorar la conciencia de seguridad. Este ejercicio subraya la importancia de educar a los empleados sobre los riesgos cibernéticos, lo cual es esencial para proteger a la organización de amenazas sofisticadas.