Índice

Introducción

Como se ha visto en clase, la Ingeniería Social es una técnica utilizada para obtener información confidencial, acceso no autorizado a sistemas informáticos, o persuadir a individuos para que tomen ciertas acciones que podrían no ser en su propio interés. Esta técnica se basa en el engaño, la manipulación y la explotación de la confianza para obtener acceso no autorizado a información o recursos.

Me gustaría profundizar algo más sobre el modo que se logra llevar a cabo una operación de Ingeniería social.

Tal como se menciona en el contenido de la unidad, la base de la ingeniería Social se basa en la confianza, ya que es el primer pilar para lograr cualquier acción que se quiera llevar a cabo.

En las relaciones sociales, el engaño pasa por el conocimiento de ciertos aspectos sobre el entorno, su estilo de vida, sus pertenencias, sus problemas o sus creencias.

Para realizar el engaño se debe usar la manipulación, y una de las técnicas de manipulación es el uso de la verdad como fuente potencial, tergiversando esa verdad a fin de obtener un beneficio propio. Se debe usar la verdad, porque la verdad es lo que otorga confianza.

Pongamos un ejemplo: En la vida real llega alguien y te dice que le has dado un golpe a su coche, te enseña unos golpes en su parachoques y argumenta que aparcando le diste, pero tú no tienes vehículo ni conduces. Obviamente el engaño se cae por sus propios argumentos, no hay nada de verdad.

Pero si en vez de eso llega un amigo tuyo, ‘Alex’ y te dice que tu novia te está poniendo los cuernos con ‘Pedro’.

Aquí disponemos de una información real y otra dudosa. Por un lado, sí que existe una persona de la cual soy pareja, además la relación no está en su mejor momento. Por otra ¿Quién es Pedro y cómo ha recibido esa información?

Alex me cuenta que es el mismo Pedro quien se lo ha contado, que es un amigo con el que llevaba años sin hablar y cuando se vieron ayer Pedro le comentó que había estado con un pibón y le mostró fotos de su Instagram.

Vas a hablar con Pedro acompañado de Alex, ya que es en quien confías y Pedro corrobora la historia argumentando que no sabía que tenía novio y menos que era novia de un amigo de Alex.

Pedro y Alex lo planearon todo a sabiendas de que eso sería la gota que colmaría el vaso en la relación, ya que Alex conocía de la situación. Yo iba a reaccionar yendo a pedirle explicaciones a mi novia, la cual lo negaría todo, pero Pedro me ha presentado con quien me había sido infiel por lo que me enfadaría aún más y la dejaría.

Ahora Pedro, que es amigo de mi novia también tiene vía libre para pasar tiempo con ella, que le cuente su experiencia, realizar una manipulación a una persona susceptible dada su situación emocional y los problemas que haya podido haber en la relación, utilizar los argumentos de ella para distanciarse de mí y por último suplantar mi papel de novio con ella.

Esta misma historia que podría darse en la vida real se puede extrapolar a una operación de Ingeniería social:

1. Se realiza un seguimiento y recopilación de información de la víctima.
2. Se determina el vector de ataque según la información obtenida.
3. Se realiza una estrategia para ese vector orientado en la confianza. Ejemplo: Santander.
4. Se manda una notificación suplantando la identidad de Santander.

a. Clonación de la web.
b. Identificador de correro / SMS.
c. Plantilla original del mensaje.
d. Argumento.
e. Etc.

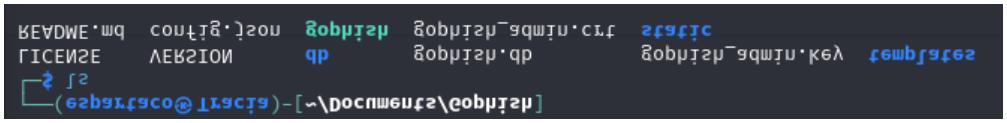
5. El usuario realiza las acciones que han sido diseñadas para el ataque.
6. Se consigue el objetivo.

La confianza para el ataque diseñado la confianza de la víctima reside en el banco Santander y las notificaciones que normalmente suele recibir por un canal en concreto.

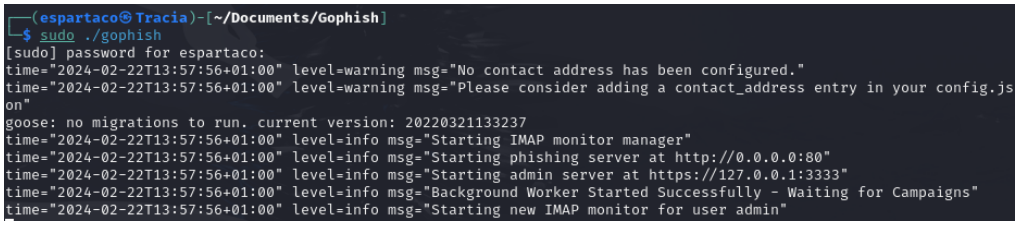
Requerimientos

Gophish

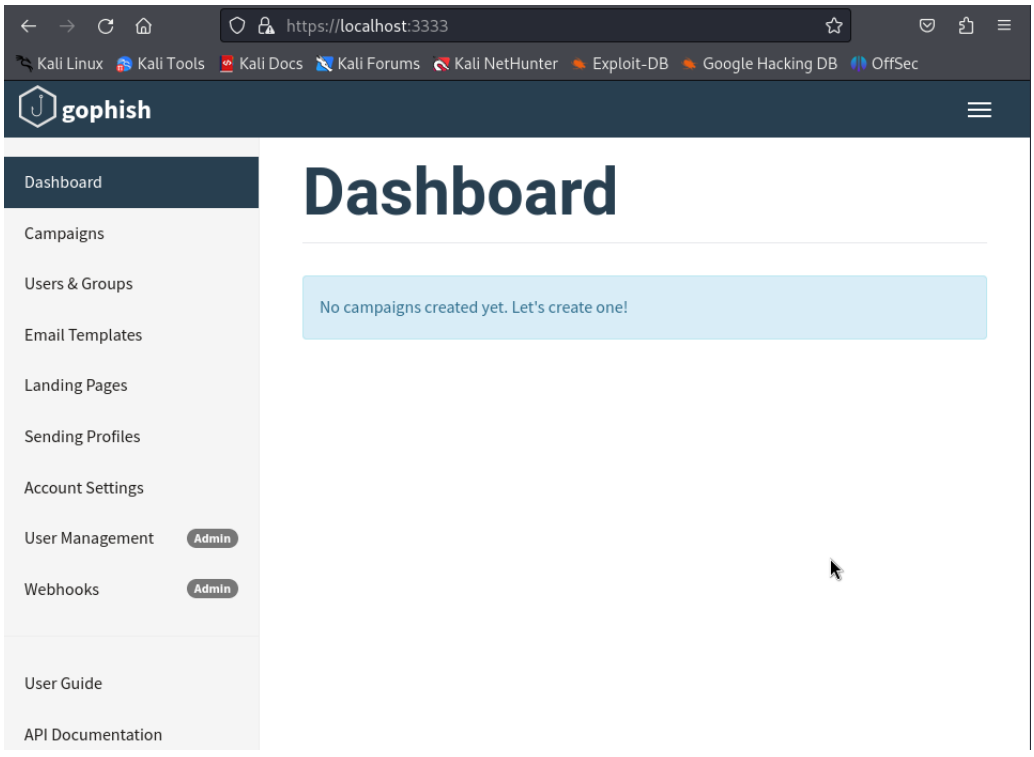
Para obtener Gophish solamente hay que acudir a la web oficial, descargarlo y descomprimirlo en la ruta deseada.



Para iniciarlo se le otorga permisos de ejecución al archivo “gophish” y simplemente se ejecuta.



Una vez iniciado Gophish ya se puede acceder a la interfaz web y comenzar la configuración de los diferentes aspectos para realizar la campaña de phishing.



Servicio de correo

Para esta campaña el objetivo es utilizarme a mí mismo para realizar una simulación de un ataque phishing por vía mail.

Una campaña real, o más sofisticada, requeriría del uso de un dominio con un servicio SMTP para realizar los envíos, pero como la simulación no la requiere voy a realizar toda la configuración con servicios en mi propio equipo Kali.

Personalmente me gustó la opción que usa Jaime de utilizar MailHog para levantar el servicio solamente cuando lo requiera.

Para poder instalar esta herramienta es necesario tener instalado Golang, por lo que compruebo si está instalado en mi máquina, si no es así lo instalo.

```
┌──(espartaco㉿Tracia)-[~/Documents/Gophish]
└─$ which go
go not found

┌──(espartaco㉿Tracia)-[~/Documents/Gophish]
└─$ sudo apt install golang-go
```

El siguiente paso sería instalar MailHog.

```
┌──(espartaco㉿Tracia)-[~/Documents/Gophish]
└─$ go install github.com/mailhog/MailHog@latest
```

Una vez instalado se puede encontrar el ejecutable en el path ~/go/bin/

```
┌──(espartaco㉿Tracia)-[~/Documents/Gophish]
└─$ cd ~/go/bin

┌──(espartaco㉿Tracia)-[~/go/bin]
└─$ ls
MailHog
```

Para iniciarlo simplemente lo ejecuto y levanta un servidor SMTP en el puerto 1025 y el IMAP en el puerto 8025.

```
┌──(espartaco㉿Tracia)-[~/go/bin]
└─$ ./MailHog
2024/02/22 13:44:21 Using in-memory storage
2024/02/22 13:44:21 [SMTP] Binding to address: 0.0.0.0:1025
[HTTP] Binding to address: 0.0.0.0:8025
2024/02/22 13:44:21 Serving under http://0.0.0.0:8025/
Creating API v1 with WebPath:
Creating API v2 with WebPath:
```

Para el funcionamiento de MailHob no hace falta configurar más, ni dominio ni cuentas, ya que por cada petición recibida al servicio SMTP levanta una sesión, realiza todo lo necesario para enviar el correo y luego cierra la sesión:

```
2024/02/22 15:43:38 [SMTP 127.0.0.1:54228] Starting session
```

[…]

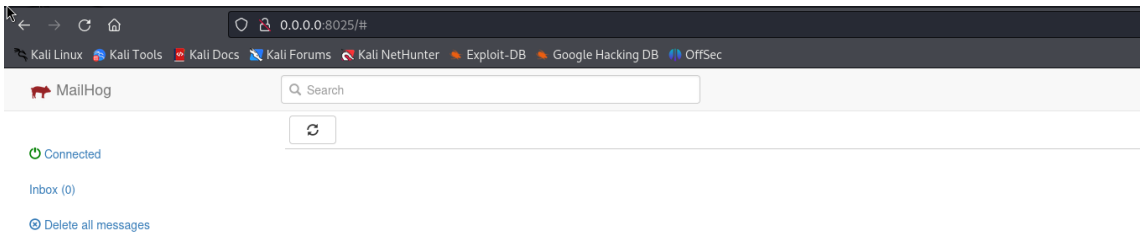
```
2024/02/22 15:43:38 [SMTP 127.0.0.1:54228] Received 34 bytes: 'MAIL FROM:<prueba@midominio.com>\r\n'
```

[…]

```
Date: Thu, 22 Feb 2024 15:43:38 +0100
From: prueba@midominio.com
X-Mailer: gophish
Subject: Default Email from Gophish
To: "prueba prueba" <prueba2@midominio.com>
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

It works!

This is an email letting you know that your gophish
configuration was successful.
Here are the details:

Who you sent from: prueba@midominio.com

Who you sent to:=20
 First Name: prueba
 Last Name: prueba
 Position: prueba

Now go send some phish!'
```

[…]

```
2024/02/22 15:43:38 [SMTP 127.0.0.1:54228] Session ended
```



Gophish

Gophish es una aplicación de código abierto diseñada para facilitar pruebas de phishing y programas de concientización en seguridad dentro de organizaciones y entornos de redes. Derivado de la combinación de las palabras "go" (lenguaje de programación) y "phish" (phishing en inglés), este software proporciona a los administradores de seguridad una plataforma versátil y accesible para evaluar la vulnerabilidad de sus sistemas y empleados frente a ataques de ingeniería social.

Características Principales:

- **Creación de Campañas de Phishing:** Gophish permite a los usuarios diseñar y ejecutar campañas de phishing simuladas de manera sencilla. Esta funcionalidad posibilita el envío de correos electrónicos falsos que emulan comunicaciones legítimas, con el propósito de evaluar la susceptibilidad de los destinatarios a caer en trampas de phishing.
- **Plantillas Personalizadas:** Los usuarios tienen la capacidad de personalizar plantillas de correo electrónico para adaptarse a las necesidades específicas de sus pruebas. Estas plantillas pueden contener elementos como enlaces maliciosos, archivos adjuntos infectados o solicitudes de información confidencial, con el fin de imitar con precisión las tácticas utilizadas por los ciberdelincuentes.

- **Seguimiento y Reportes:** Gophish ofrece herramientas integrales para rastrear y analizar la interacción de los destinatarios con los correos electrónicos de phishing. Los administradores pueden supervisar quién ha abierto los mensajes, quién ha hecho clic en enlaces maliciosos y quién ha proporcionado datos confidenciales, permitiendo una evaluación detallada del impacto de la campaña.
- **Interfaz Gráfica de Usuario (GUI) Intuitiva:** Con una interfaz de usuario amigable y fácil de usar, Gophish simplifica el proceso de configuración y ejecución de campañas de phishing. Esta característica hace que la herramienta sea accesible incluso para usuarios con poca experiencia en seguridad informática, fomentando su adopción y uso efectivo.
- **Personalización y Escalabilidad:** Gophish es altamente personalizable y escalable, lo que lo hace adaptable a una variedad de entornos y requisitos específicos. Además, puede integrarse con otras soluciones de seguridad y herramientas de gestión de redes para ofrecer una solución integral de concientización y pruebas de seguridad.

Objetivo de la campaña

La empresa de nutrición deportiva española HSN quiere realizar una campaña controlada de concienciación sobre ingeniería social a sus empleados. Para ello quiere utilizar el mail phishing con tal de generar un informe para su posterior concienciación.

El proceso por parte del empleado será el siguiente:

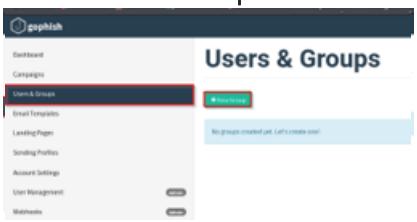
1. El empleado recibe un mail procedente de un dominio parecido al de la empresa. En este correo urgente se pide a los empleados que revisen los proyectos activos, descarguen y cumplimenten un archivo Excel como respuesta al correo.
2. Para acceder a la web se facilita un enlace en el correo al que los empleados pueden “picar” o no.
    a. El usuario puede (o no) enviar sus datos de usuario.
3. El correo contiene un archivo Excel adjunto que contiene los datos a cumplimentar, el cual, si caen en la trampa descargarán, ejecutarán, rellenarán y reenviarán como adjunto al correo recibido.
    a. El archivo adjunto no es malicioso, ya que va dirigido a una campaña de concienciación, pero precisamente por eso es un plus para tener en cuenta para la campaña.

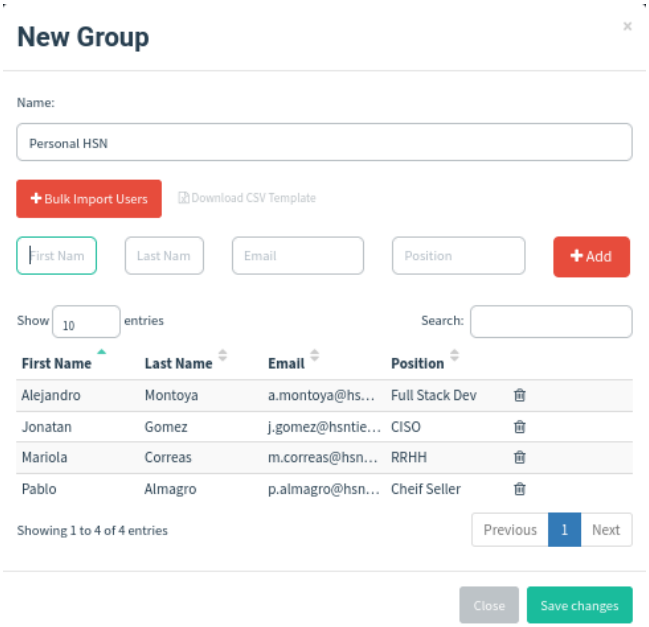
Preparación de la campaña

Los diferentes aspectos a configurar en Gophish para la campaña son los siguientes:

- **Users & Groups:** Usuarios a los que va destinada la campaña.
- **Email Templates:** Plantilla de correo utilizada para el envío de los correos phishing.
- **Landing Pages:** Web utilizada para suplantar el formulario login de la web HSN original.
- **Sending Profiles:** “Perfi de la empresa” y servicio desde donde se van a mandar los mails.
- **Campaigns:** Con todos los datos preparados se crea la campaña y se programa su lanzamiento.

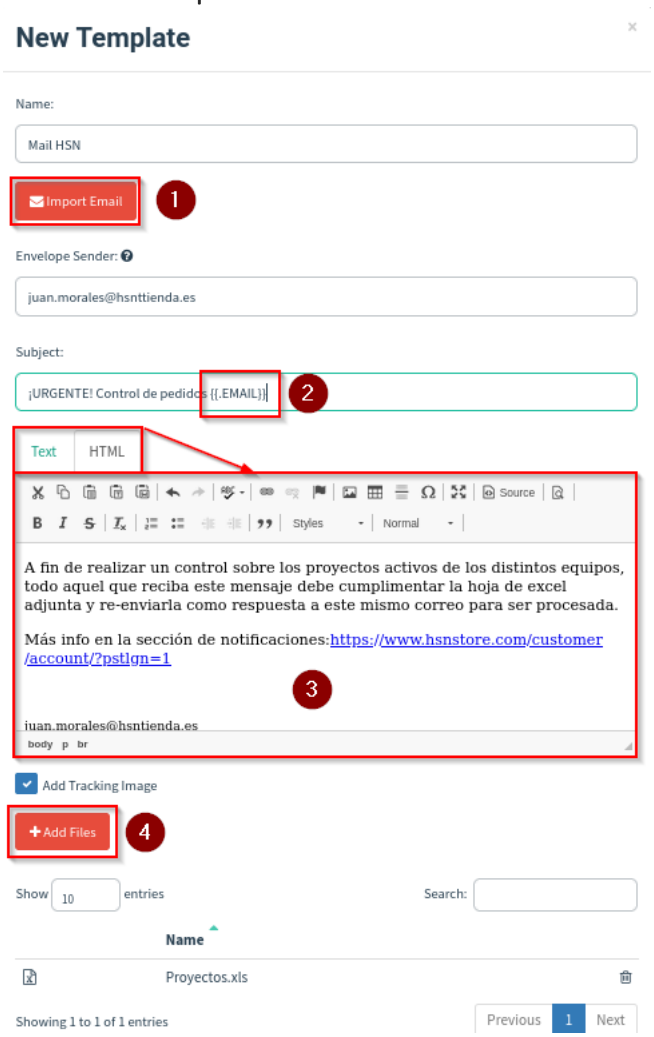
Users & Groups





Los usuarios pueden añadirse de forma manual o pueden ser importados a través de un CSV para agilizar el proceso.

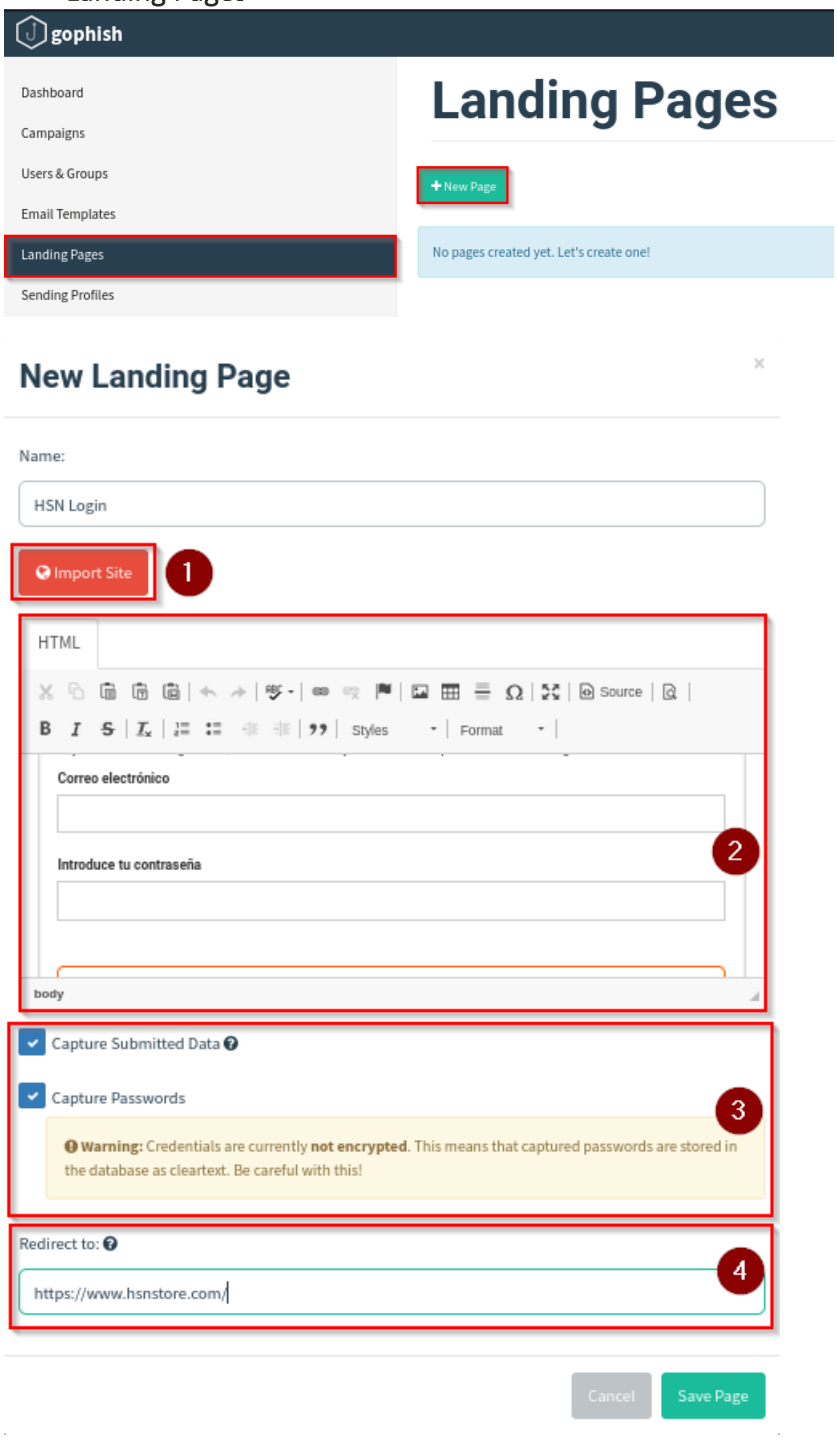
Email Templates



He señalado distintos puntos a destacar para la configuración de la plantilla del correo:

1. Se puede importar desde un correo real.
2. Hay modificadores que se pueden utilizar para personalizar la plantilla
    a. En este caso el modificador no envía un correo genérico con la lista de todos los destinos, sino que solo aparece como destino quien lo recibe.
3. El cuerpo del mensaje se puede editar a nivel de texto plano o por código HTML.
4. Se pueden añadir ficheros al correo. Para este ejemplo se adjunta un archivo llamado Proyectos.xls.

Landing Pages

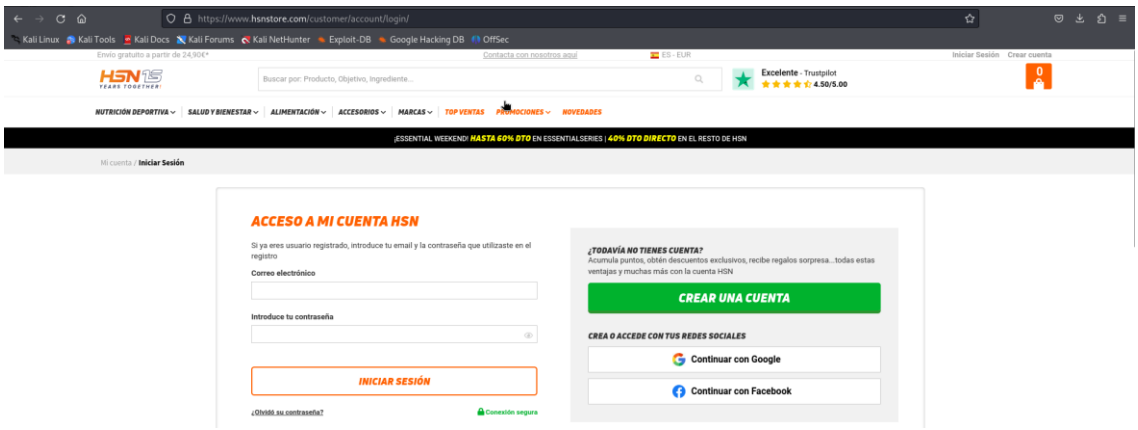


He señalado distintos puntos a destacar para la configuración de la plantilla de la web:

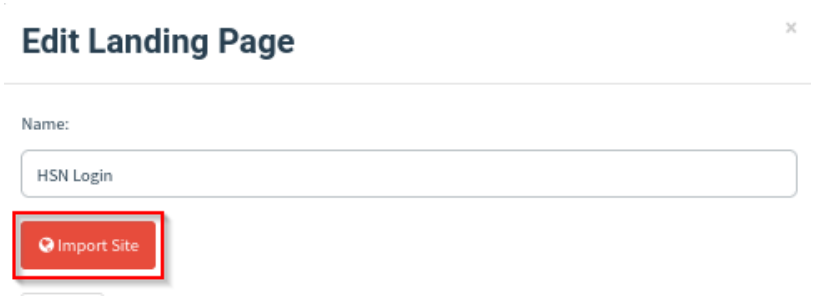
1. Se puede importar una web automáticamente introduciendo una url.
    a. Para este caso https://www.hsnstore.com/customer/account/login/
    b. Esta funcionalidad no funciona de forma correcta en todas las webs, debiendo hacer un trabajo manual para la clonación de la web.
2. Edición del código HTML y resultado renderizado del mismo.
3. Al interactuar con la web opcionalmente se puede capturar los datos introducidos por el usuario, incluyendo la contraseña en texto plano.
4. Una redirección opcional a un sitio web.

Proceso de clonación web

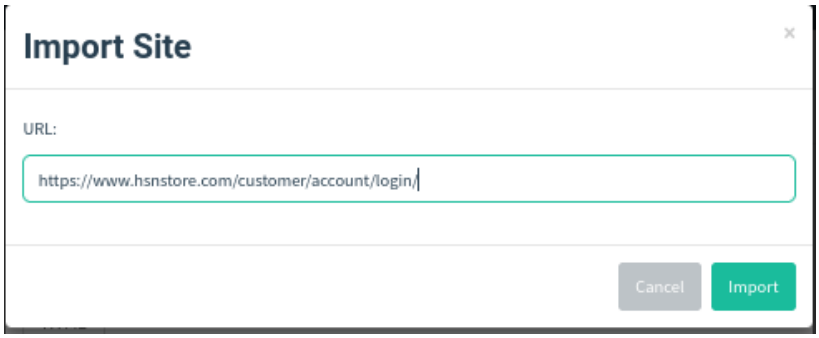
Lo primero es acceder al apartado de la web que se desea clonar, para este caso es la web de login de hsnstore.com.



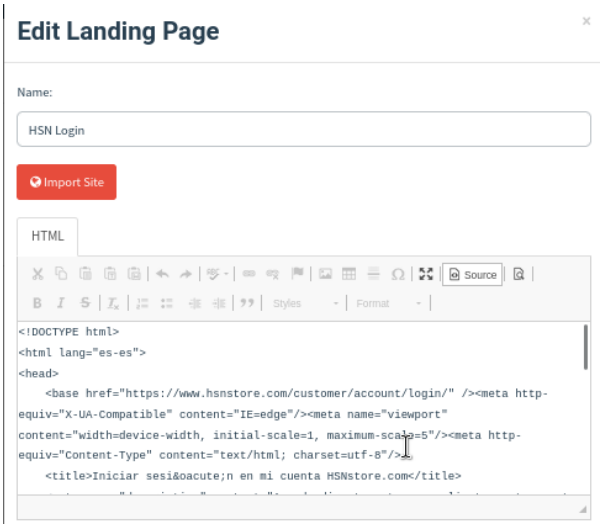
Una vez dentro de la web se copia la URL y se clica sobre Import Site en el apartado de edición de Landing Page mostrado en el apartado anterior.



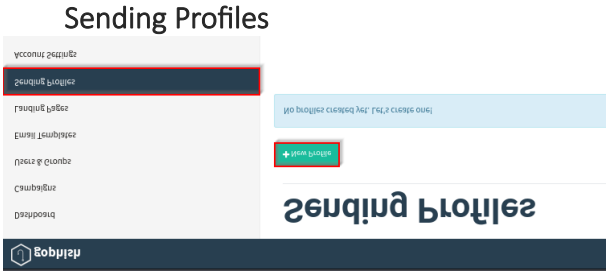
Se coloca la URL de la web a clonar y se clica en Import.

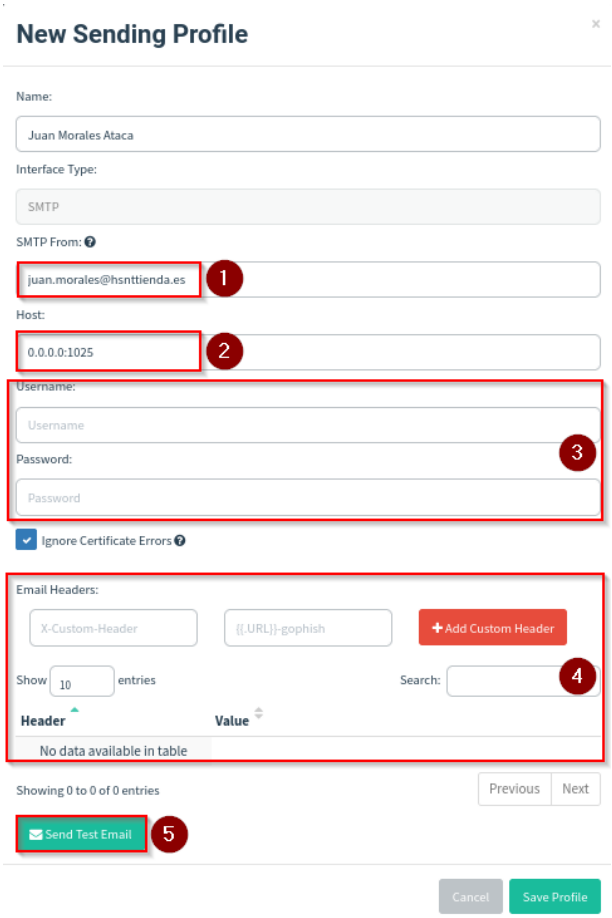


Una vez hecho se puede probar y modificar en caso de que sea necesario.



También se puede optar por realizar una clonación totalmente manual.

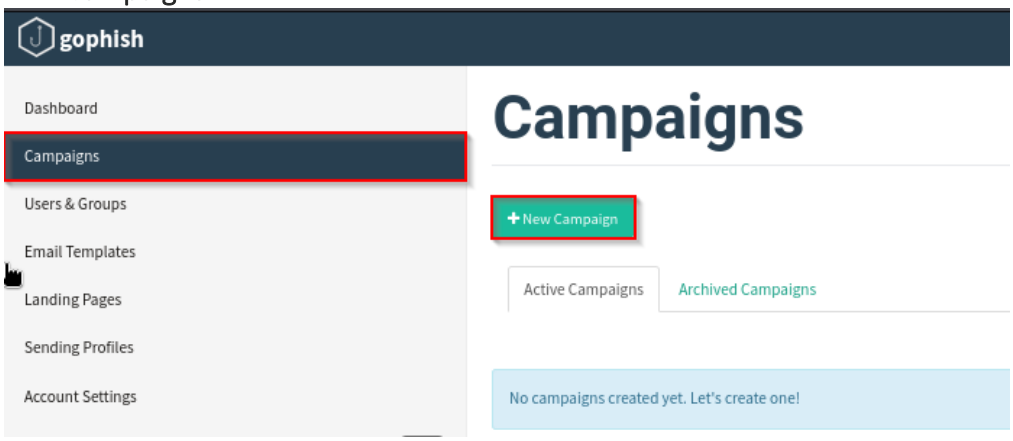


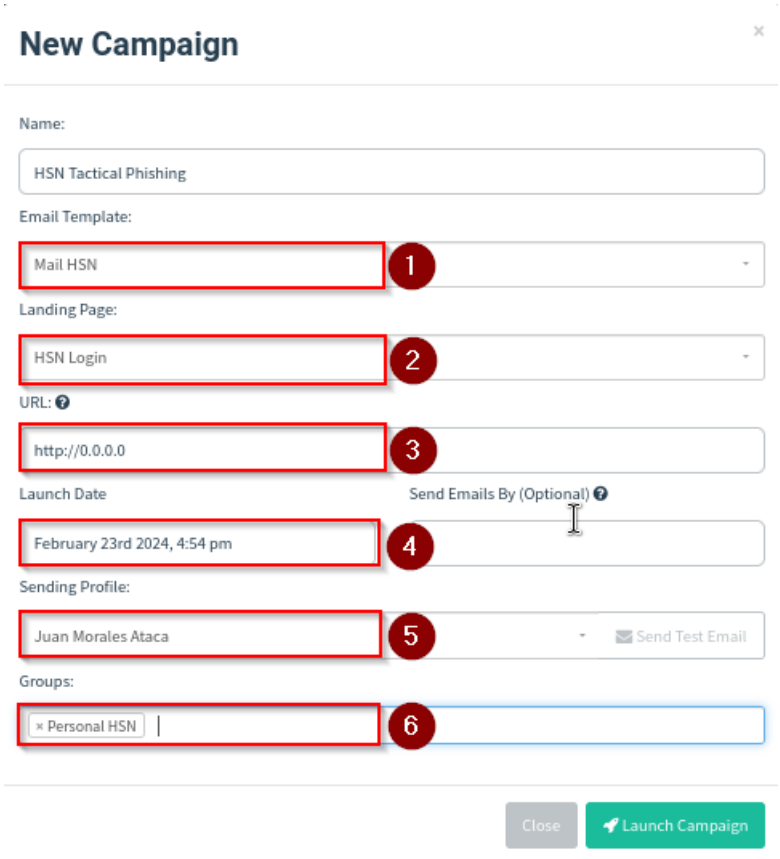


He señalado distintos puntos a destacar para la configuración del sender prifile:

1. Quien será el sender del correo electrónico.
    a. Se puede apreciar que el nombre del dominio del correo no es el mismo que el de la empresa, ya que una campaña real de phishing no haría esto a no ser que ya esté dentro y tenga el acceso y control de una cuenta de correo.
    b. Hsnttienda.es con dos t.
2. El servidor SMTP desde donde se realizará el envío de los correos electrónicos.
    a. Para un escenario real se utilizarían los datos del servicio SMTP del dominio que se haya contratado.
3. Si hiciera falta una autenticación se especifica.
4. Se pueden personalizar las cabeceras de los correos, esta parte es opcional para hacer más o menos agresivo el ataque
5. Send Test Email envía un correo de prueba para comprobar la conexión.

Campaigns





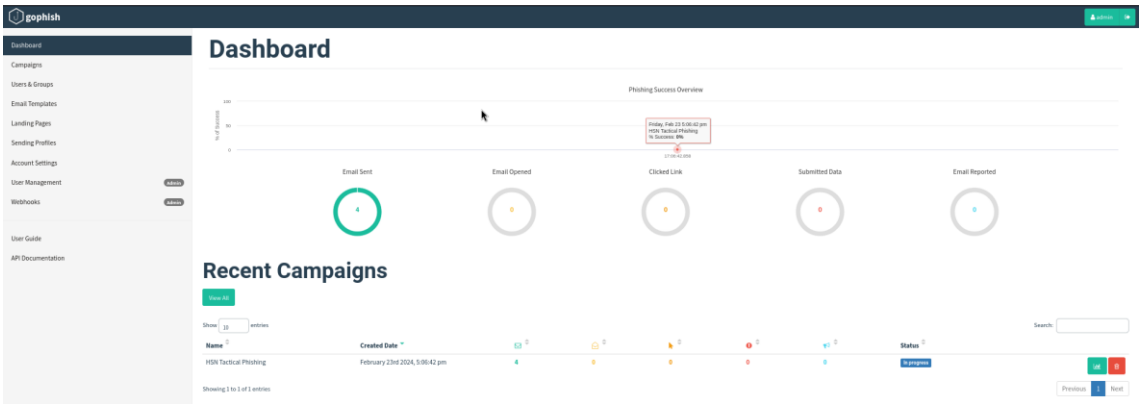
He señalado distintos puntos a destacar para la configuración de la campaña:

1. Se selecciona la plantilla de correo a utilizar.
2. Se selecciona la plantilla de la web a utilizar.
3. Se introduce la URL hacia donde va destinada la plantilla.
    a. En un escenario real podría ser el dominio adquirido.
4. Se configura el momento exacto de lanzamiento de la campaña
    a. Una opción lógica sería momentos antes de comenzar la jornada laboral de un día específico, donde todo el mundo deba iniciar sesión.
5. Se selecciona el sender de los correos.
6. Se seleccionan los grupos a los que va destinada la campaña. Pueden ser varios grupos.

Al clicar en Launch Campaign se lanza la campaña, estando activa una vez llegue al Launch Date.

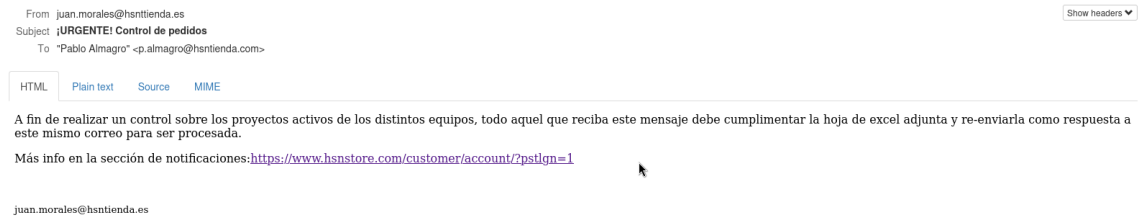
Lanzamiento

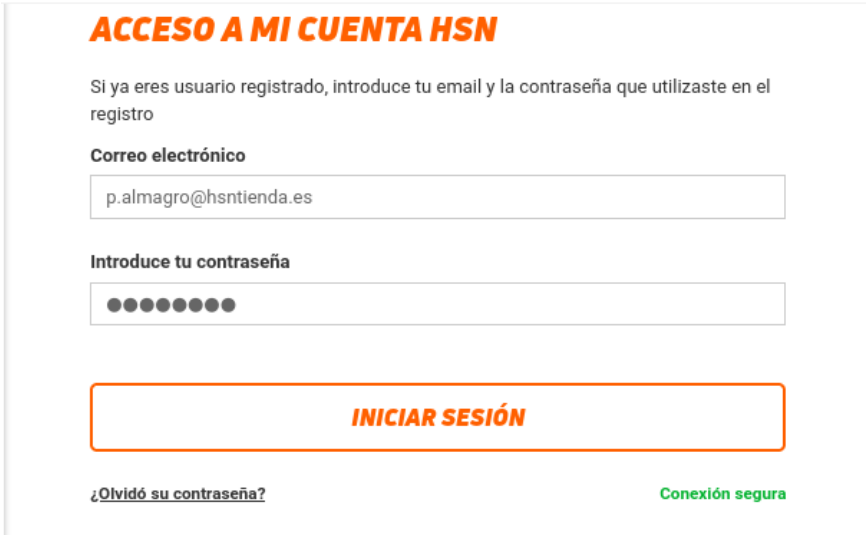
Una vez lanzada la campaña se puede observar los resultados en el Dashboard de Gophish, donde se puede observar que los correos han sido enviados en primera instancia.



Si voy al Inbox del correo puedo ver los mails recibidos a cada usuario. Obviamente esto es un escenario de pruebas, en un escenario real cada un habría recibido el suyo en su bandeja de entrada.

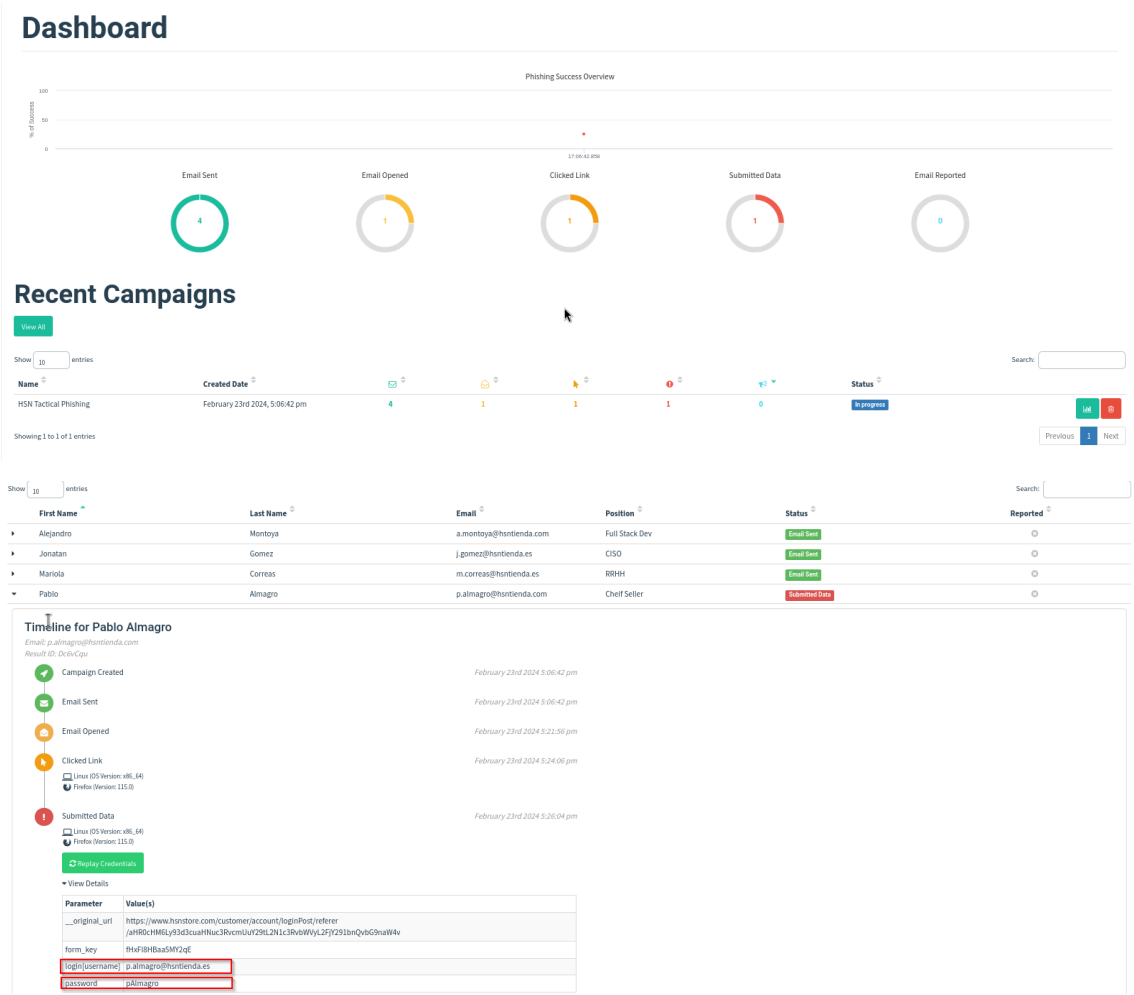
El usuario Pablo Almagro, responsable de ventas abre el correo y se dispone a ver las notificaciones disponibles en la web clicando en el enlace del mail sin fijarse que el correo viene de un dominio que no es el de la empresa.





Realiza el proceso de autenticación y le redirige a la web original, pero Pablo es poco avispado en términos informáticos y vuelve a acceder a su cuenta.

Al no encontrar notificaciones en su perfil con instrucciones descarga el archivo adjunto en el correo, realiza el trabajo y lo reenvía. De esta forma Pablo ha cometido todos los errores posibles.



Los email reported no se pueden visualizar para esta práctica, ya que el servicio SMTP utilizado es MailHog.

Alejandro Montoya ha abierto el correo, pero como es full Stack Developer no ha clicado en el enlace, sino que ha ido desde el navegador, aun así, ha descargado el archivo, lo ha abierto, ha buscado las notificaciones, no las ha encontrado, ha preguntado a sus superiores y ha reportado la situación con ellos.

Mariola ha abierto el correo, ha clicado en el enlace y ha logueado en la página fake, pero como tenía reuniones con candidatos desde primera hora de la mañana no ha descargado el fichero ni ha reenviado el correo. Incluso se le ha olvidado.

Por último el CISO era parte de la operación, por lo que ni si quiera se ha presentado a trabajar el primer día de la campaña como parte de la operación.

Una vez completada la campaña se puede exportar como CSV y darla por concluida.

Conclusión

Lanzar una campaña de phishing la verdad es que es bastante sencillo a nivel técnico. La existencia de herramientas como Gophish hace que el proceso sea muy fácil.

Yo personalmente ya tenía cuidado con este tipo de ataques, ya que se reciben muy a menudo. Ni siquiera abro las notificaciones que se mandan desde la sede del gobierno directamente, entro en la plataforma y accedo a ellas de forma manual.

Conozco mucha gente que no le presta atención o directamente les da igual hacer click en un enlace o exponer sus datos o realizar una acción sin pensarlo, incluso argumentando “¿quién va a venir a hackearme a mi con lo poco que tengo?”.

El phishing es solamente una rama de la ingeniería social. A mi me llama especialmente la atención la ingeniería social física que se ha comentado en clase, utilizando cacharros que permiten hacer cosas y teniendo habilidades sociales directamente. Me imagino una operación de Ingeniería Social llevada a cabo por un Red Team presentándose en la empresa y pinchando cualquier posa por ahí…

En definitiva reflexionar sobre el tiempo que se puede ahorrar usando la ingeniería social para llegar al sistema víctima es interesante. Quizá en una operación sin Ingeniería Social tardes meses y quizá usando la Ingeniería social tardes una semana.

Como siempre acepto feedback acerca de la entrega, cualquier reseña, objetividad o recomendación es bienvenida.