Phising

Un enfoque práctico

Fase I: Preparación

Obtención del consentimiento

- Debemos asegurarnos de obtener el **consentimiento por escrito** de la dirección de la empresa y/o departamento de recursos humanos, así como de los empleados que serán incluidos en la campaña.

Instalación de Gophish

- Es necesario descargar e instalar Gophish en un sistema públicamente accesible (p. ej. un VPS).
- Una vez instalado, accedemos al panel de control mediante el enlace http://servidor:3333/

Descargas:

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

Documentación oficial de Gophish:

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

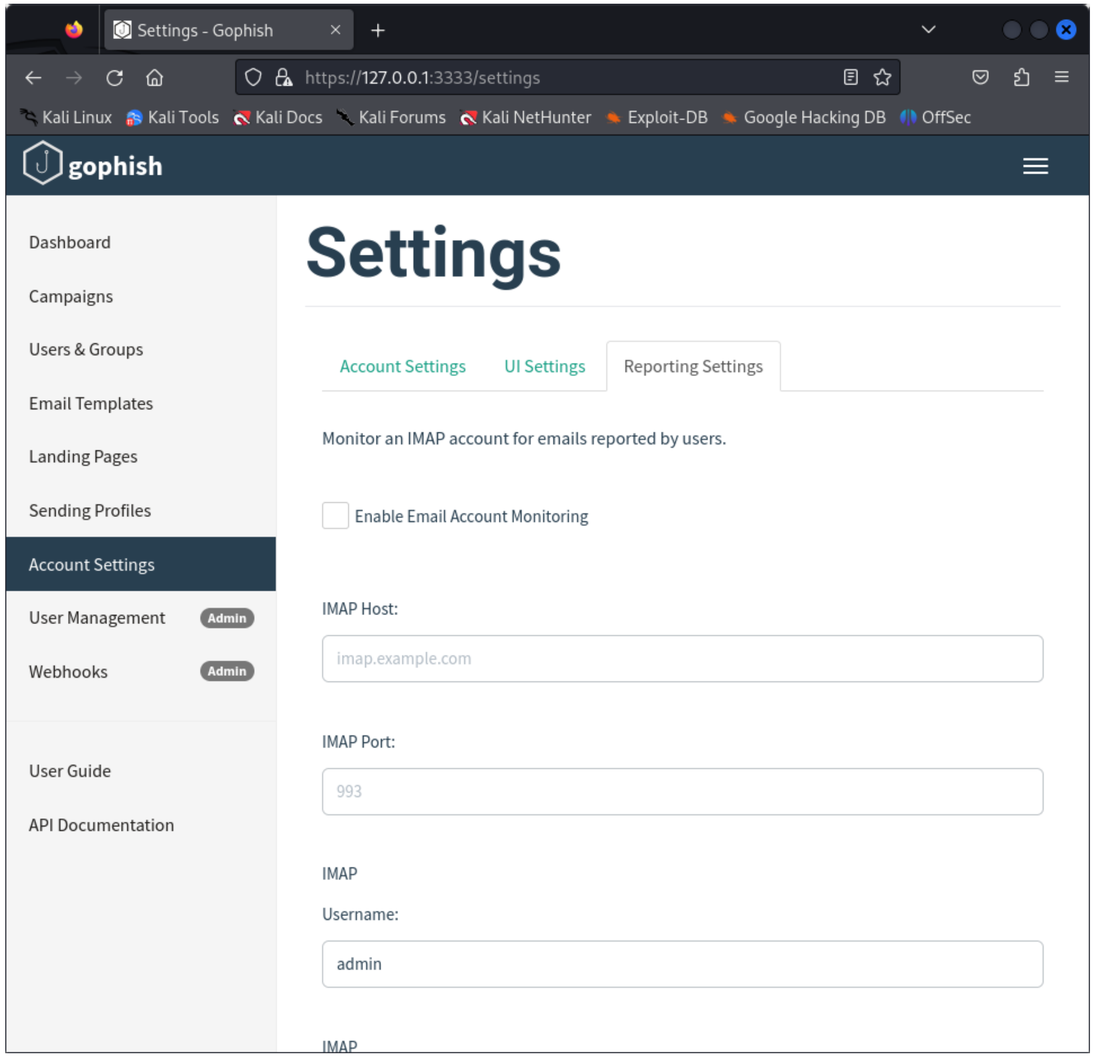
Requerimientos:

- Servidor donde instalar y ejecutar Gophish
- Servidor SMTP para envío de correo
- Proxy inverso HTTPS con certificado SSL válido (opcional)

Configuración de Gophish

Información relevante

- Datos de acceso al servidor SMTP
  - Nombre de dominio o IP del servidor
  - Puerto del servicio SMTP
  - Usuario de SMTP
  - Contraseña de dicho usuario
- Información de dominios a utilizar



Fase II: Creación de la Campaña

Definición del objetivo

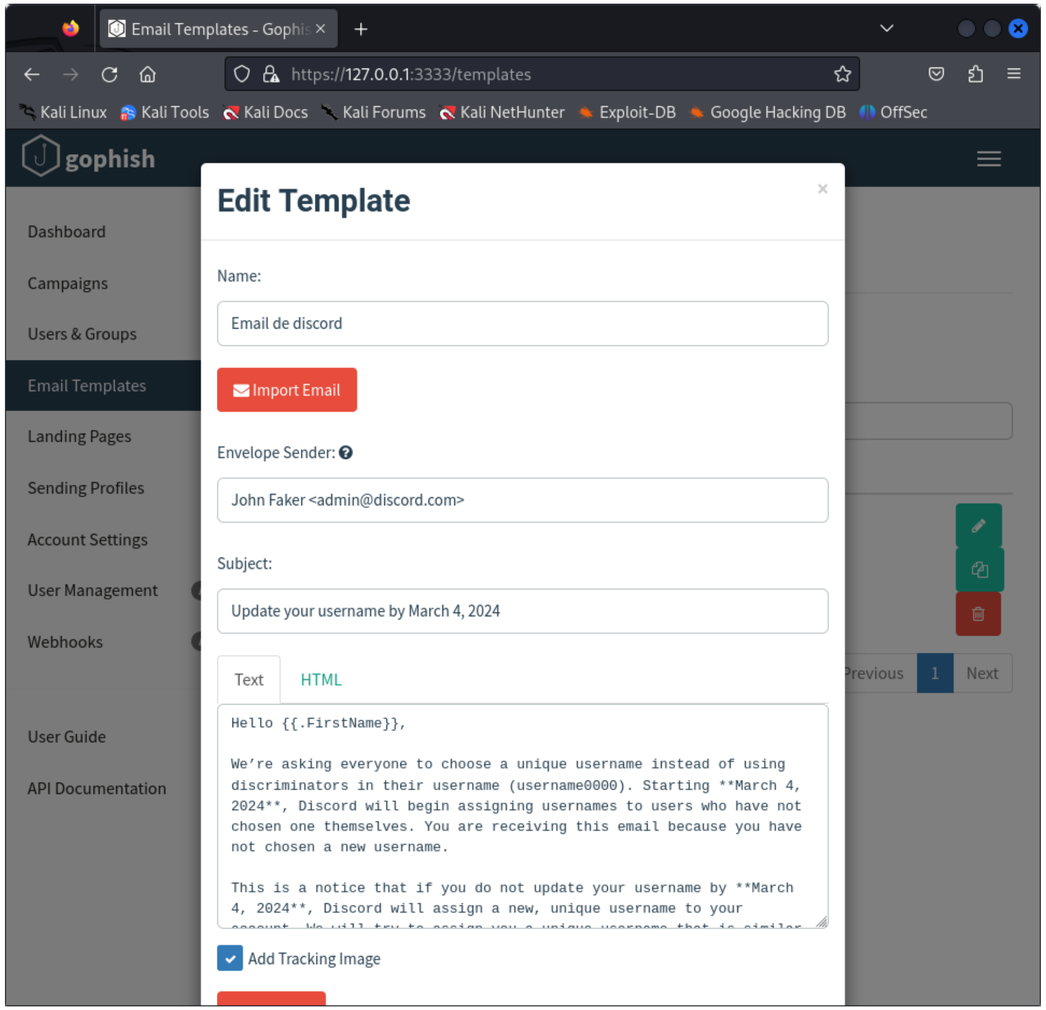
Planificación

- Decidir la finalidad de la campaña:
  - Obtener información de los usuarios (credenciales de inicio de sesión, información confidencial, …)
  - Llevar a cabo alguna acción potencialmente maliciosa

Plantilla de correo electrónico

Diseño del correo electrónico a enviar

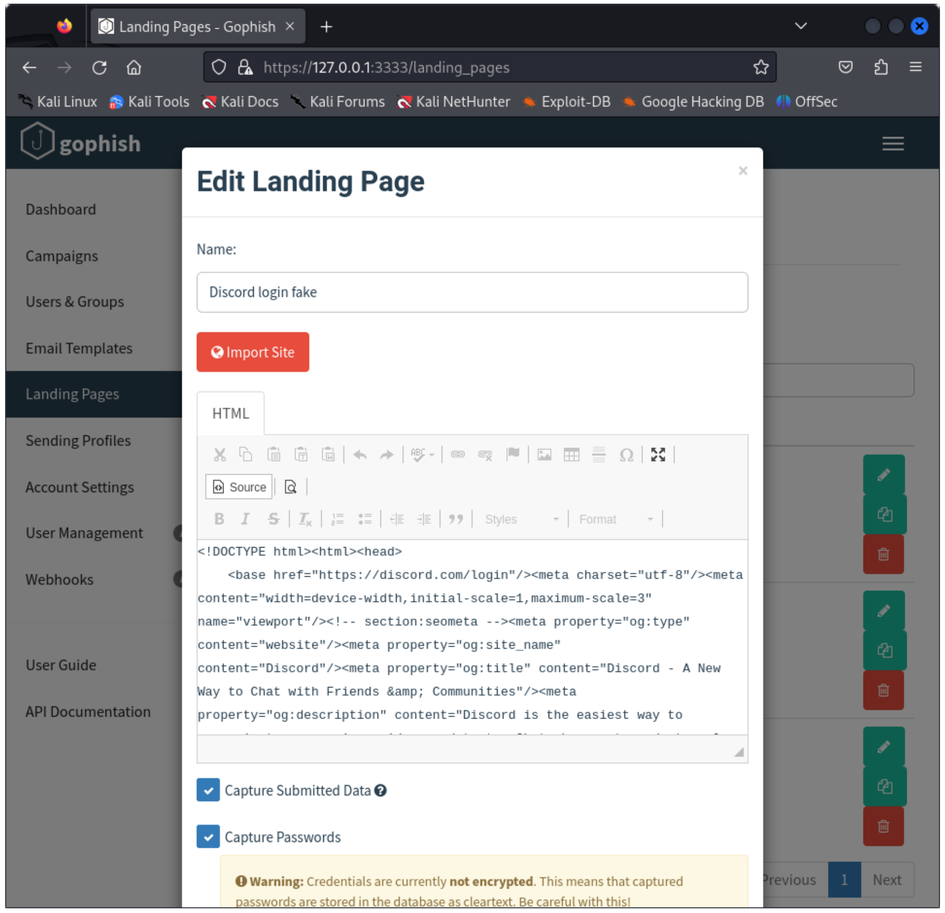
- Diseñar un mensaje de correo electrónico **creíble** y **persuasivo**
- Para obtener la plantilla se puede:
  - Crear manualmente mediante el editor
  - Importar de un mensaje de correo electrónico existente



Página de phising

Confeccionar la página a la que dirigirá el email

- Diseñar la página web engañosa lo más parecida a la del sitio web legítimo.
- Para obtener el código se puede:
  - Crear manualmente mediante el editor
  - Importar de un sitio web a partir de su URL
- Para la captura de credenciales o información confidencial la página ha de contar con algún tipo de formulario que envíe los datos al servidor de Gophish.

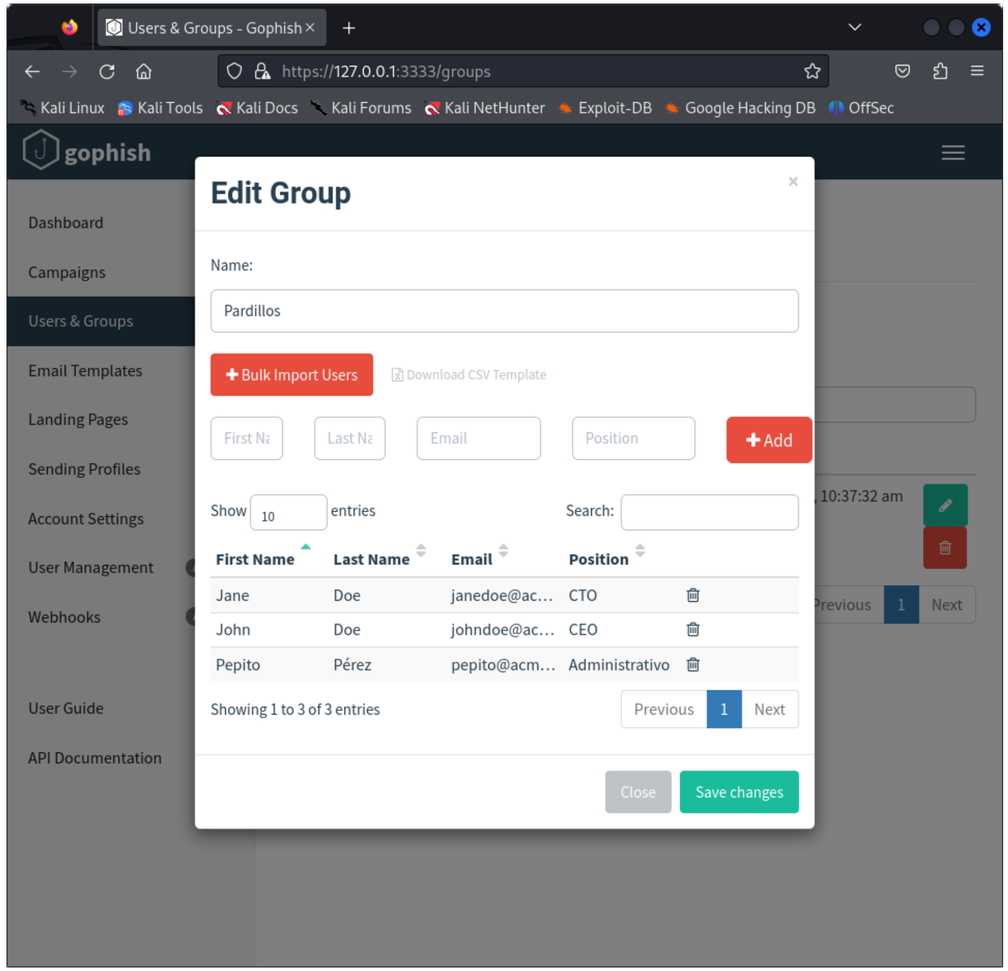


Fase III: Ejecución de la Campaña

Audiencia objetivo

Creación de un grupo de contactos

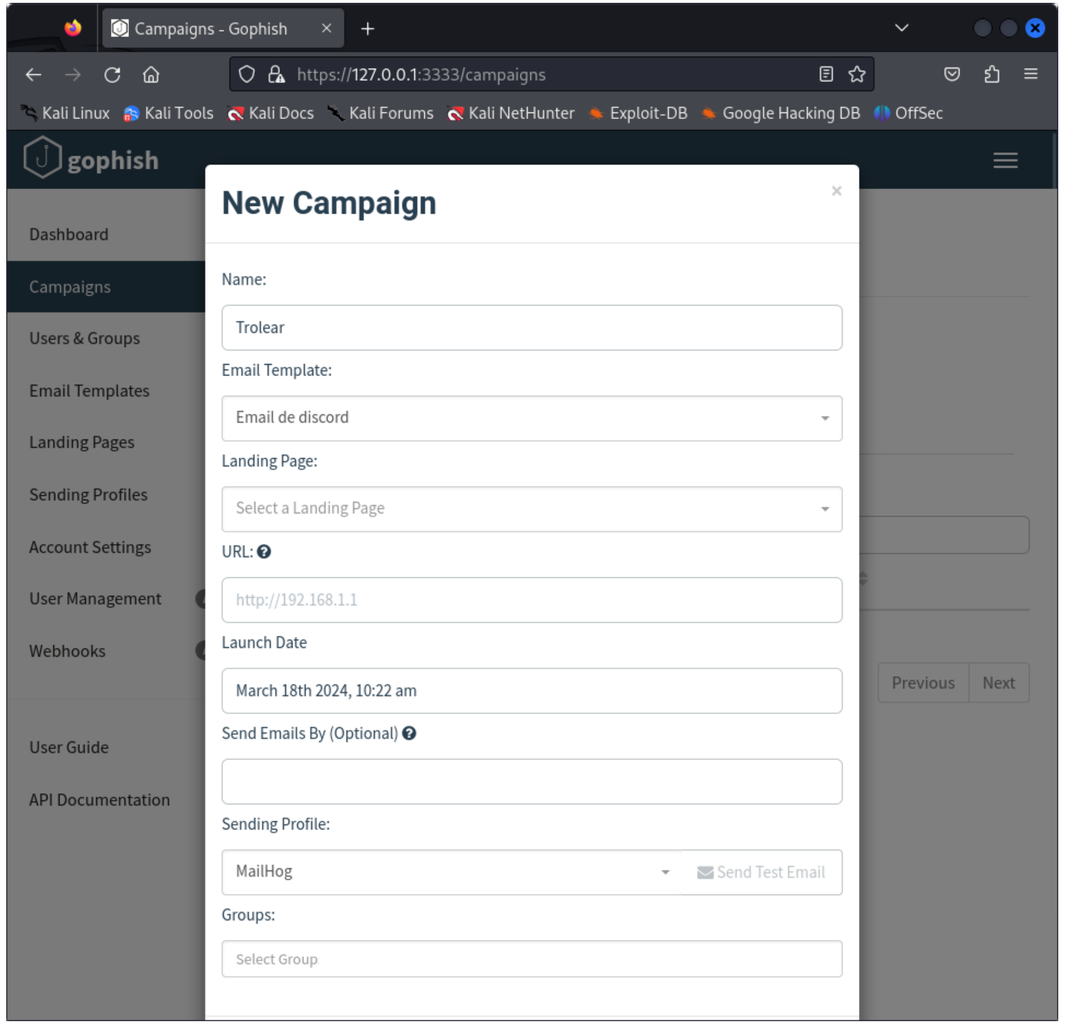
- Es necesario crear una lista de contactos con la siguiente información:
  - -Nombre
  - -Apellidos
  - -Dirección de correo electrónico (fundamental)
  - -Puesto en la organización (opcional)
- Se puede importar la lista desde un fichero CSV



Envío de los correos electrónicos

Lanzamiento de la campaña

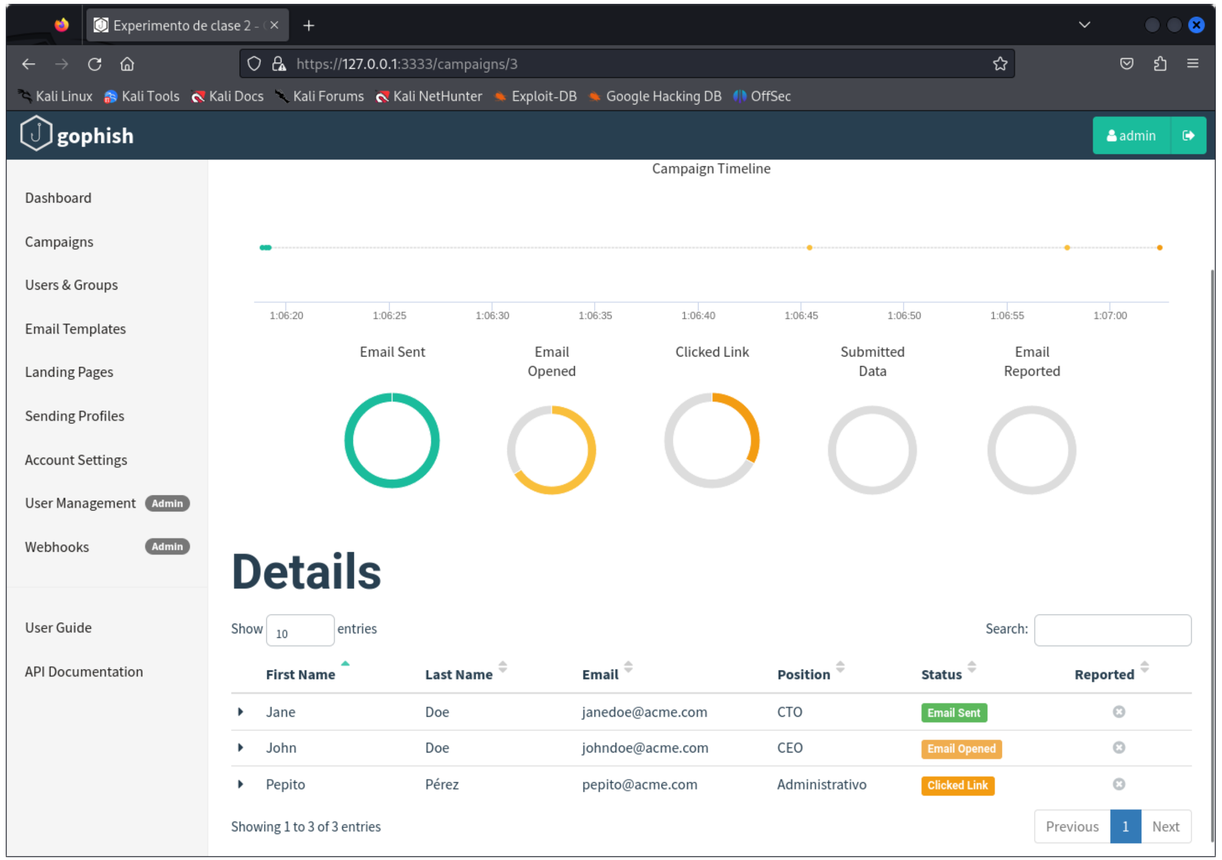
- Crear nueva campaña, relacionando:
  - Plantilla de email
  - Página de phising
  - URL de phising, apuntando al servidor de Gophish (p. ej. http://servidor/ruta)
  - Grupo de contactos
- Elegir el momento adecuado para el envío de los correos
- Lanzar la campaña desde el panel de control



Fase IV: Seguimiento y evaluación

Supervisión de respuestas

- Desde el dashboard de Gophish se pueden obtener estadísticas de:
  - Mensajes enviados
  - Mensajes abiertos por los destinatarios
  - Acciones de apertura de enlaces
  - Datos enviados
- También se puede acceder a los detalles de cada envío (fechas y horas, datos enviados en el formulario, …)



Análisis de resultados

- Transcurrido un tiempo, finalizaremos la campaña, deteniendo el proceso de recopilación de datos.
- Gophish puede generar un informe en formato CSV con resultados.
- Con los resultados obtenidos, procederemos a dar retroalimentación a la corporación o a los usuarios que han participado:
  - Explicación de los riesgos del phising
  - Consejos para identificar correos maliciosos o fraudulentos