EL FRAMEWORK

🎣 ¿Qué es GoPhish y por qué usarlo?

GoPhish es un toolkit de código abierto diseñado para que empresas y pentesters puedan crear, ejecutar y medir campañas de phishing de forma controlada y ética [citation:1].

🧠 ¿Para qué sirve en el Hacking Ético?

En el Módulo 3, el objetivo no es robar contraseñas reales, sino **medir el nivel de concienciación** de una organización. GoPhish te permite:

- Crear correos electrónicos falsos pero realistas (simulando un aviso de TI, un banco, etc.).
- Alojar páginas de inicio de sesión clonadas (Landing Pages) para capturar credenciales (solo con permiso).
- Rastrear quién abrió el correo, quién hizo clic en el enlace y quién introdujo datos.
- Generar reportes automáticos para la empresa.

> 💡 **Dato Clave**
>
> GoPhish viene preinstalado en Kali Linux. El comando `gophish` está deprecado; ahora se usa `gophish-start` [citation:1]. Las credenciales por defecto son `admin` / `kali-gophish`, pero debes cambiarlas al primer inicio de sesión.

PASO 01

💻 Instalación y Primer Arranque

Si usas Kali Linux, GoPhish ya está en los repositorios. Si no, puedes descargarlo manualmente desde GitHub [citation:1][citation:2].

📦 Instalación en Kali

```
Terminal

kali@root:~$ sudo apt update && sudo apt install gophish
Leyendo lista de paquetes ... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  gophish
...
Configurando gophish ...
```

🚀 Iniciar el Servidor

Una vez instalado, inicia GoPhish con el comando `gophish-start`. Verás en la terminal la URL de administración y la contraseña generada [citation:1].

```
Terminal

kali@root:~$ gophish-start
[*] Web UI: https://127.0.0.1:3333
[*] You might need to refresh your browser once it opens

Default credentials:
  user: admin
  password: kali-gophish
```

Abre Firefox y ve a `https://127.0.0.1:3333`. Acepta la advertencia de certificado (es normal, GoPhish usa un certificado autofirmado). Inicia sesión con `admin` / `kali-gophish`.

🔐 Cambiar la Contraseña

Lo primero que debes hacer es cambiar la contraseña por defecto. Ve al menú de usuario (arriba a la derecha) y selecciona **"Settings"** o **"Account Settings"**. Ingresa una contraseña segura y guarda.

PASO 02

📧 Configurar Sending Profile (SMTP)

El Sending Profile le dice a GoPhish desde qué servidor de correo enviará los emails. Necesitas una cuenta SMTP (Gmail, Brevo, Mailtrap, etc.) [citation:2][citation:5].

📮 Crear el Perfil

En el menú lateral, haz clic en **Sending Profiles** y luego en **New Profile**. Rellena los campos:

- **Name:** "SMTP de Pruebas" (o el nombre que prefieras).
- `it-support@tu-dominio.com`
- `smtp-relay.brevo.com:587`
- **Username:** Tu correo o usuario SMTP.
- **Password:** La contraseña o **API Key** del servicio (en Gmail es la "contraseña de aplicación").
- **Ignore Certificate Errors:** Déjalo desmarcado si usas un servicio confiable.

> 💡 **Prueba de Envío**
>
> Antes de guardar, haz clic en **"Send Test Email"**. Introduce tu propio correo y verifica que el mensaje llega a tu bandeja de entrada (no a spam). Si no llega, revisa las credenciales SMTP.

⚠️ Sobre el Header "X-Mailer"

Por defecto, GoPhish añade un header `X-Mailer: GoPhish` en los correos. Esto es una **bandera roja** para los filtros antispam [citation:2]. Para simular un correo legítimo, puedes añadir un header personalizado en la configuración del Sending Profile (ej. `X-Mailer: Microsoft Outlook 16.0`) [citation:3].

PASO 03

📝 Crear Plantillas de Correo

La plantilla es el cuerpo del correo que recibirá la víctima. Debe ser convincente y contener el enlace a tu Landing Page [citation:2].

✉️ Nueva Plantilla

Ve a **Email Templates** → **New Template**. Puedes escribir el HTML desde cero o importar un correo existente (guardado como `.eml`) [citation:2].

Un ejemplo de plantilla convincente (simulando un aviso de TI):

Plantilla HTML

```
<html>
<body>
<p>Hola {{.FirstName}},</p>
<p>Tu contraseña corporativa expira en 24 horas. Por favor,
actualízala usando el siguiente enlace:</p>
<p><a href="{{.URL}}">Actualizar Contraseña</a></p>
<p>Atentamente,<br>Equipo de TI</p>
{{.Tracker}}
</body>
</html>
```

Variables importantes: `{{.FirstName}}` se reemplaza con el nombre del objetivo. `{{.URL}}` se reemplaza con la URL de tu Landing Page. `{{.Tracker}}` es un píxel invisible que rastrea si el correo fue abierto [citation:4].

> 💡 **Personalización**
>
> Usa `{{.FirstName}}` y `{{.LastName}}` para que el correo se sienta personal. Los correos personalizados tienen una tasa de clics mucho mayor.

PASO 04

🖥️ Crear la Landing Page (Página Falsa)

La Landing Page es la página de inicio de sesión falsa que verá la víctima. GoPhish puede clonar una página real automáticamente [citation:2][citation:11].

📥 Clonar una Página Real

Ve a **Landing Pages** → **New Page**. En la opción **"Import Site"**, introduce la URL de la página que quieres clonar (ej. `https://login.microsoftonline.com`) y haz clic en "Import". GoPhish descargará el HTML y los estilos [citation:3].

⚙️ Configuración Crítica

- **Capture Submitted Data:** Marca esta casilla. Sin esto, GoPhish no guardará las credenciales que introduzca la víctima [citation:11].
- **Capture Passwords:** Marca esta casilla si quieres ver la contraseña en texto claro (solo en laboratorios controlados).
- **Redirect To:** La URL a la que será redirigido el usuario después de "iniciar `https://www.staysafeonline.org/` 4].

⚠️ Advertencia de Seguridad

GoPhish almacena las contraseñas capturadas en **texto claro** en el archivo `gophish.db` [citation:4]. Después de tu práctica, **elimina ese archivo** o cambia las contraseñas de las cuentas de prueba. Nunca uses contraseñas reales en un laboratorio.

PASO 05

🎯 Crear Grupo de Usuarios y Lanzar la Campaña

Finalmente, agrupamos a los objetivos y lanzamos la simulación. En un laboratorio, usa correos ficticios o tu propio correo [citation:2].

👥 Crear el Grupo

Ve a **Users & Groups** → **New Group**. Puedes añadir usuarios manualmente o importar un CSV con las columnas: `First Name, Last Name, Email, Position` [citation:3].

Ejemplo de CSV

```
First Name,Last Name,Email,Position
Juan,Perez,juan.perez@ejemplo.com,Gerente
Maria,Lopez,maria.lopez@ejemplo.com,Contadora
```

🚀 Lanzar la Campaña

Ve a **Campaigns** → **New Campaign**. Rellena los campos:

- **Name:** "Simulación Interna - Prueba 1".
- **Email Template:** Selecciona la plantilla que creaste.
- **Landing Page:** Selecciona la página clonada.
- **Sending Profile:** Selecciona tu perfil SMTP.
- **URL:** La URL de tu servidor GoPhish (en laboratorio local, usa `http://127.0.0.1`).
- **Groups:** Selecciona el grupo de prueba.

Haz clic en **Launch Campaign**. GoPhish comenzará a enviar los correos.

PASO 06

PASO 06

📊 Análisis de Resultados (Dashboard)

Una vez lanzada la campaña, el Dashboard de GoPhish te muestra en tiempo real las métricas de la simulación [citation:2][citation:5].

📈 Métricas Clave

- **Emails Sent:** Correos enviados correctamente.
- **Emails Opened:** Correos abiertos (gracias al píxel `{{.Tracker}}`).
- **Link Clicked:** Usuarios que hicieron clic en el enlace falso.
- **Data Submitted:** Usuarios que introdujeron datos en la Landing Page.

En un laboratorio con 5 correos de prueba, un resultado típico podría ser: 5 enviados, 3 abiertos, 2 clics, 1 credencial capturada [citation:9].

🎓 ¡Fin de la Clase 3.2!

Ya tienes GoPhish configurado y listo para simular campañas de phishing. En la próxima clase (3.3), crearemos una campaña completa desde cero y analizaremos los resultados en detalle.