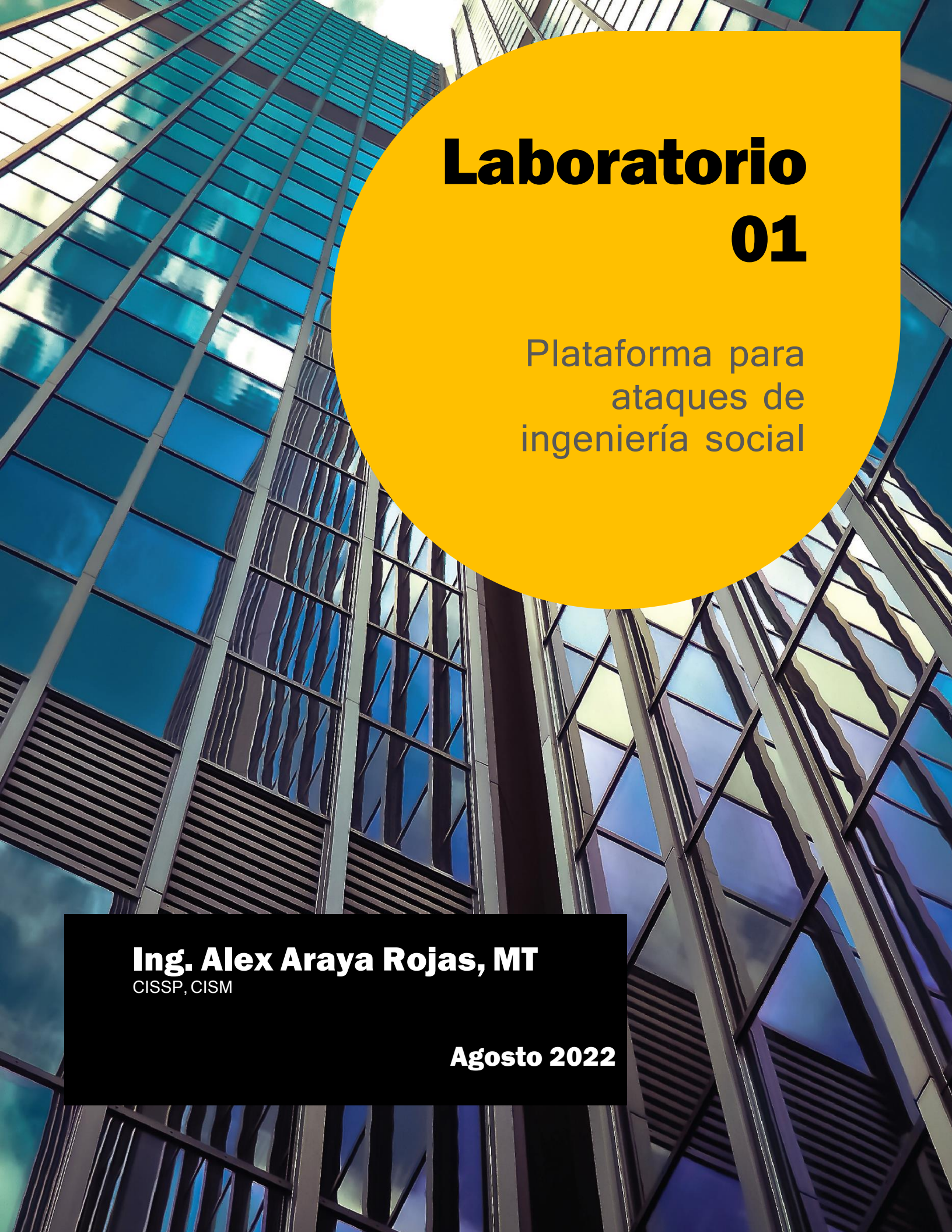


Laboratorio 01

Plataforma para ataques de ingeniería social

Ing. Alex Araya Rojas, MT
CISSP, CISM

Agosto 2022

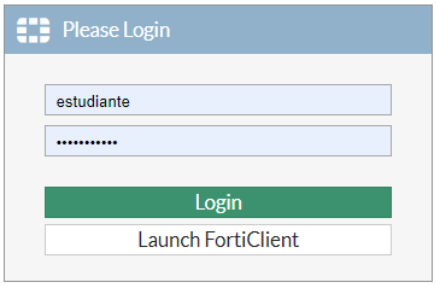
Lab 01

Plataforma para ataques de ingeniería social

Procedimiento

Preparación

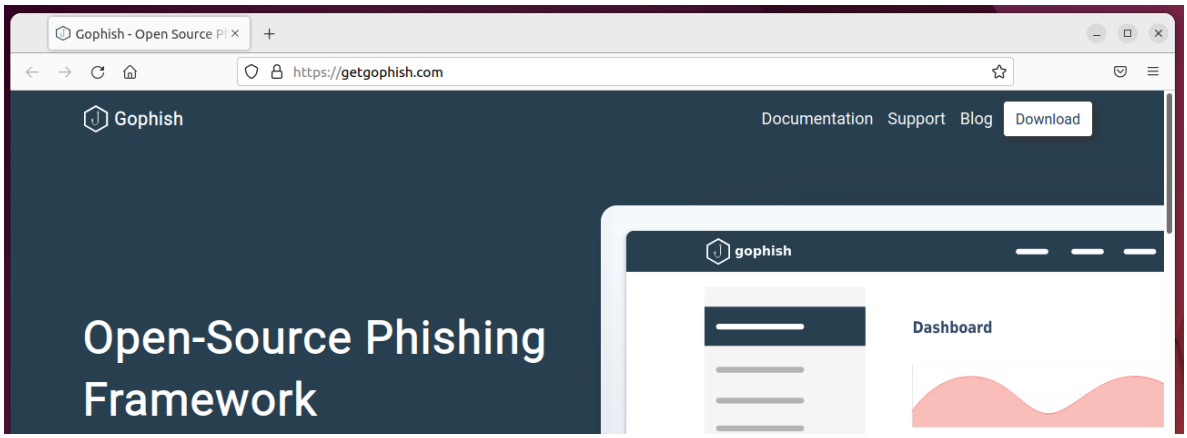
01. Esta herramienta es compatible tanto para Windows, Linux como MacOS, puede ejecutar el laboratorio en cualquiera de esas plataformas.
02. Se ha preparado una máquina en el laboratorio para cada estudiante, para el ejercicio, utilizaremos una virtual con Ubuntu instalado, a la cual usted accederá vía RDP.
03. Ingrese al sitio web https://vpn.araya.vip:10443 las credenciales para su acceso son "estudiante" con la contraseña " CIFTen2022! " Esta es una VPN vía SSL por lo que **no** debe instalar ningún cliente en su equipo ya que el acceso será vía un navegador de internet a los equipos asignados, solo ingrese las credenciales y presione el botón Login.



04. Una vez que haya ingresado, verá varios íconos con un número de estudiante, ingrese al que le fue proporcionado para el laboratorio.

05. Valide el acceso a su equipo, no debe continuar hasta que tenga visión acceso a su equipo.

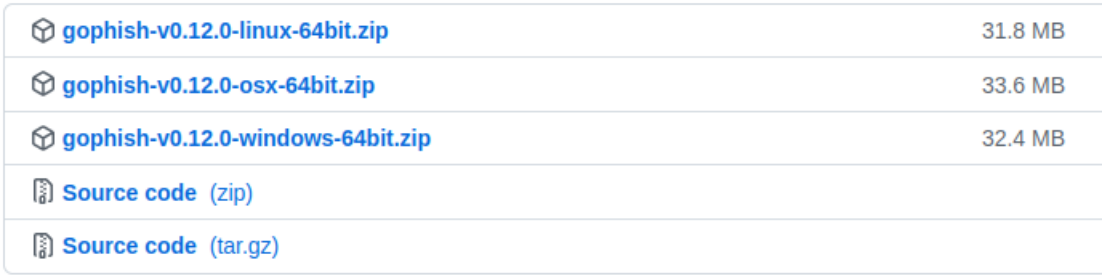
06. Es necesario que este equipo sea visible desde la Internet, por ejemplo, puede utilizar una máquina virtual en Azure o en su red empresarial y publicar el servicio en una DMZ. Nosotros lo instalaremos en una máquina virtual local y utilizaremos direcciones de la LAN para efectos del laboratorio.
07. Ahora es el turno de la herramienta GoPhish, que habilitará el framework para poder hacer nuestros ataques de phishing, puede descargarlo de este url: https://getgophish.com/ la última versión liberada al realizar esta guía era la v0.12.0, nosotros utilizaremos la versión para Linux que más adelante instalaremos. Si abre el Firefox en su equipo Ubuntu deberá llevarlo directo a ese sitio web.



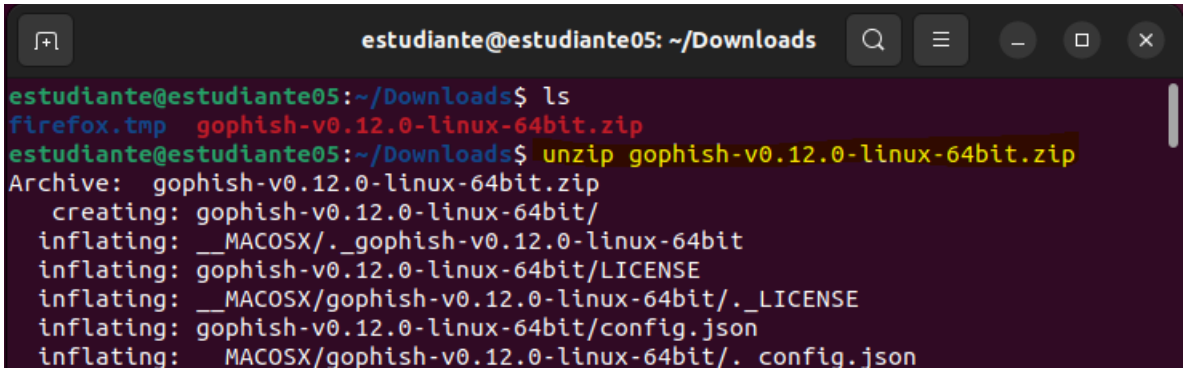
08. Es necesario utilizar una cuenta de correos para el envío del ataque de phishing, para efectos de practicidad, se le está compartiendo una cuenta de correo estudiante@araya.vip con las credenciales " CIFTen2022! " más adelante veremos el proceso de configuración.

Proceso de instalación

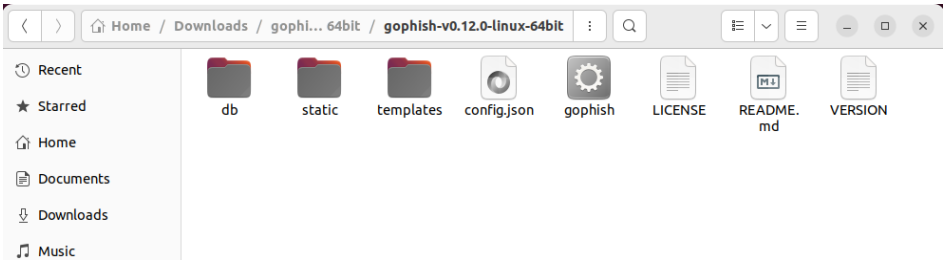
01. Descargue el archivo para su plataforma de software que funcione para el que será su servidor de Phishing. https://github.com/gophish/gophish/releases, para efectos de este lab, los vamos a instalar en un equipo con Ubuntu, por lo que debe descargar la primera opción.



02. Una vez descargado el archivo zip, toca el turno de descomprimirlo, la forma fácil sería ubicar el archivo en la carpeta DOWNLOADS, clic derecho y EXTRACT HERE. Si lo quiere hacer vía comando, a continuación, se muestra una captura de pantalla que lo logra.



03. Una vez que se haya ejecutado el proceso para su descomprensión, ubique la carpeta y dentro de la estructura, abra con su editor de texto favorito el archivo config.json



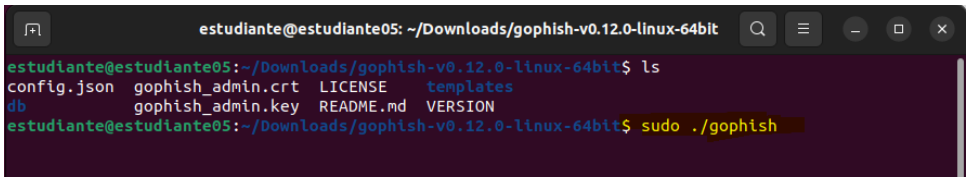
04. En la siguiente imagen, se aprecia el config.json abierto con el editor de texto de Ubuntu.


```
{
        "admin_server": {
                "listen_url": "127.0.0.1:3333",
                "use_tls": true,
                "cert_path": "gophish_admin.crt",
                "key_path": "gophish_admin.key"
        },
        "phish_server": {
                "listen_url": "0.0.0.0:80",
                "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": ""
        }
}
```

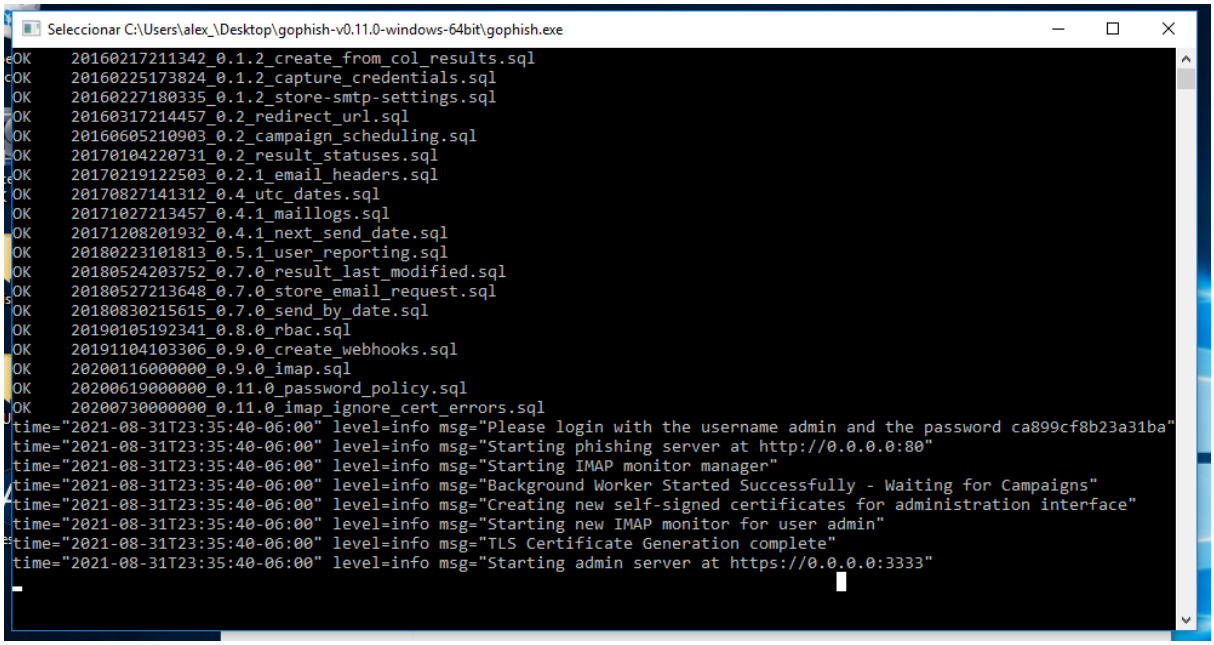
05. El apartado de admin_server le permite configurar la forma en que se gestiona el servidor de gophish.
06. El apartado de phish_server, le permite definir los parámetros del servidor que almancenará las páginas web de phising.
07. Se pueden agregar más secciones, por ejemplo, la configuración smtp, pero para efectos de este lab no serán necesarios.
08. Reemplace el listen_url del admin_server, con este cambio, ya podrá conectarse al servidor por ese puerto desde otros equipos vía la IP que tenga asignado físicamente el servidor. Si el certificado le da problemas, cambie a false la opción "use_tls"

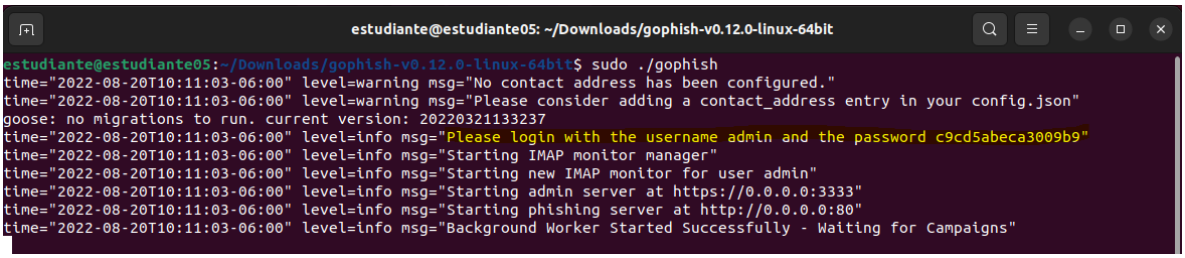
```
"admin_server": {
    "listen_url": "0.0.0.0:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key"
}
```

09. Si está corriendo esta máquina en su proveedor de nube, deberá habilitar los permisos en su firewall correspondiente.
10. Ejecute el archivo gophish.exe (Windows) o en nuestro caso, abra una terminal en la carpeta donde están los archivos de gophish y ejecute el comando:



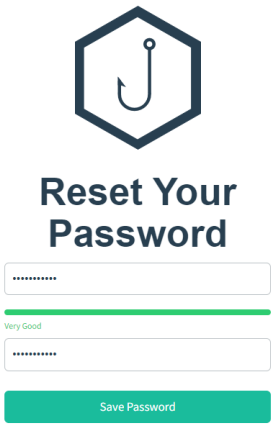
11. En la consola, al tratarse de la primera vez que se ejecuta el GoPhish, debe estar atento ya que aparece la contraseña aleatoria asignada.



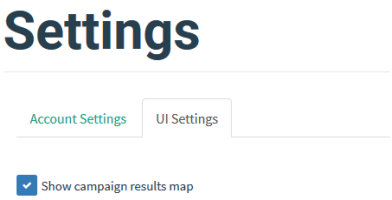


12. Ingrese a la consola de administración del GoPhish y deberá ver la página de inicio de sesión.

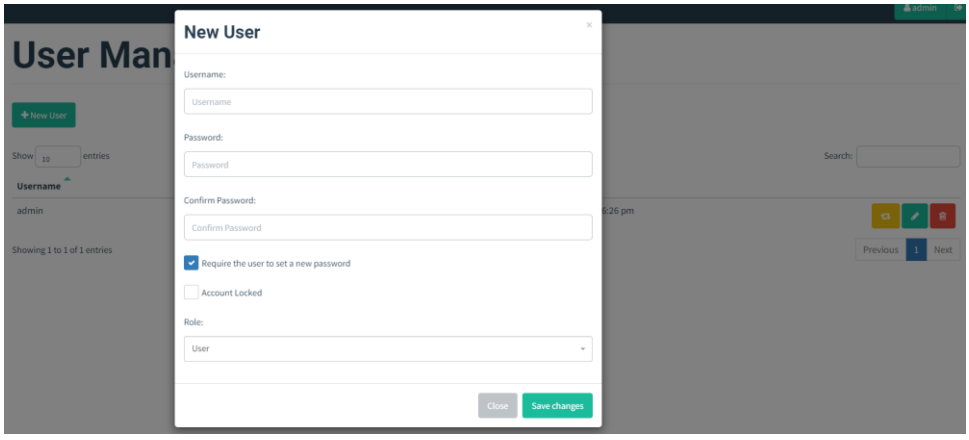
13. La primera vez que ingrese deberá cambiar el password de la consola de administración, como recomendación, utilice CIFTen2022!



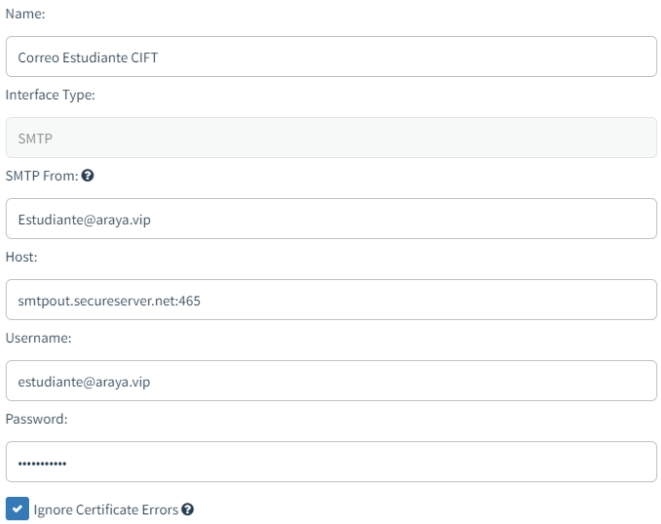
14. Marque la opción del mapa en Account Settings, esto le permitirá tener una visualización gráfica de la apertura de nuestros correos.



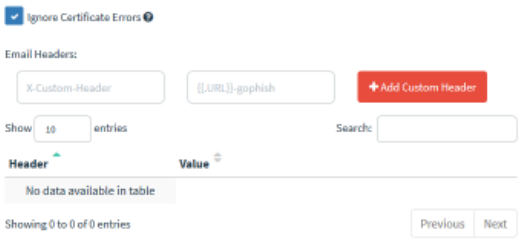
15. En la opción de User Management, podrá crear otros administradores y usuarios son privilegio, esto en caso de ser necesario brindar acceso a terceros para seguimiento.



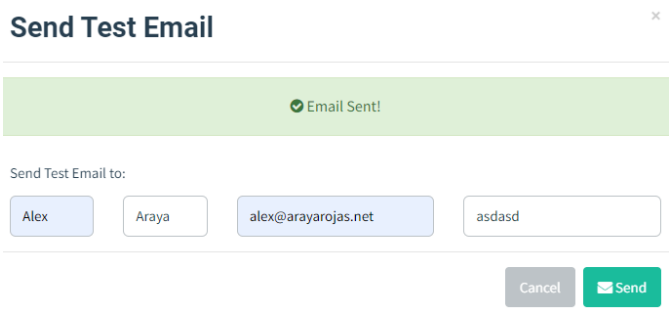
16. Debe ahora crear un sending profile para enviar los correos utilizando su cuenta de correo creamos para este ejercicio. Complete los campos para utilizar según los valores suministrados.



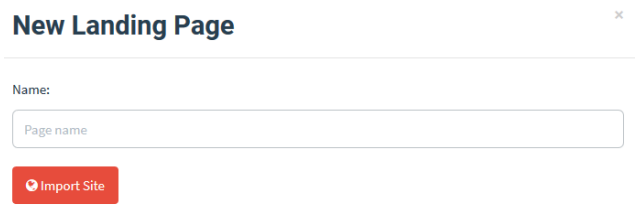
17. Si desea agregar encabezados al correo para que alguna aplicación los pueda marcar, esta es la sección para hacerlo.



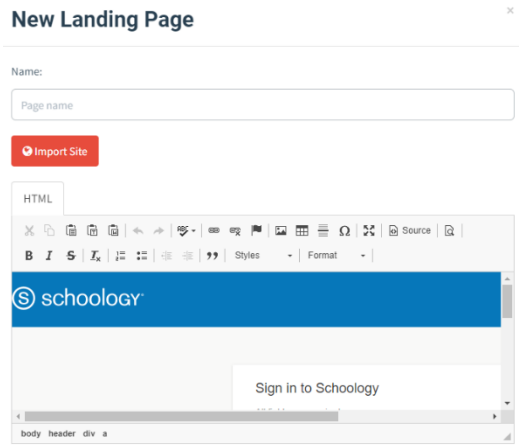
18. Puede probar la configuración del envío de correos con el botón correspondiente, no avance si esto no funciona. No olvide guardar el profile!!



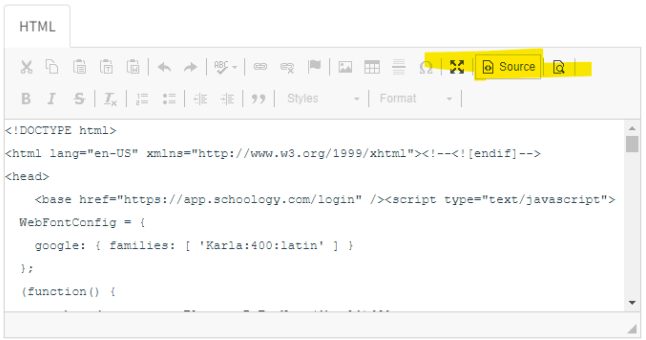
19. El landing page es donde irán nuestras víctimas cuando hagan click en nuestro link malicioso. Puede importarla y la herramienta clonará el sitio por usted.
20. Elija bien el sitio, debe contener el campo de username y password para que el ejercicio funcione. Sino tiene una página, puede utilizar https://app.schoology.com/login



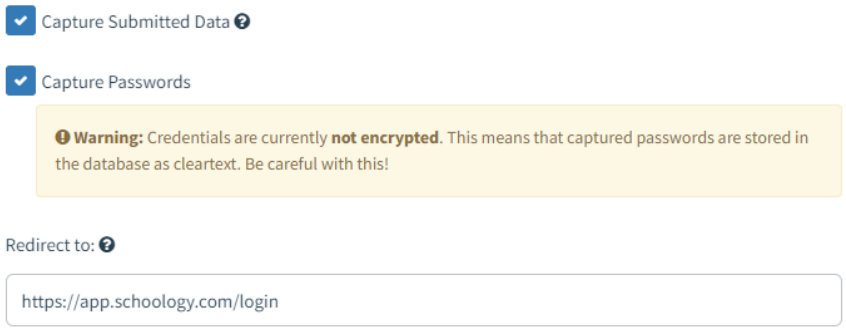
21. Ahora puede ver el contenido de la página y hacer modificaciones, le recomiendo que elimine todo el código tipo script del sitio clonado y haga pruebas hasta que la captura de la contraseña funcione y la apariencia de la página sea la apropiada.



22. Utilice la opción de ver el código para ayudarse en la depuración de la página.

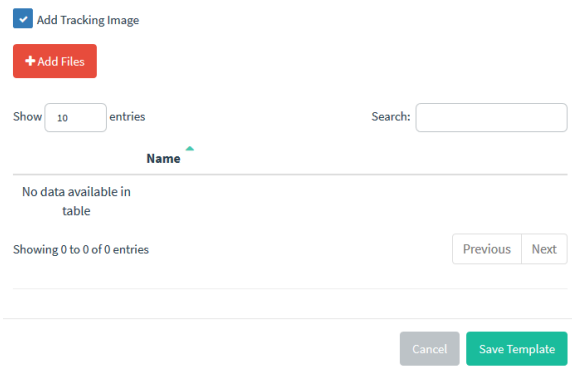


23. Si desea guardar las credenciales de las víctimas, deberá marcar estas casillas, así como la opción de redirigir a la víctima al sitio real.



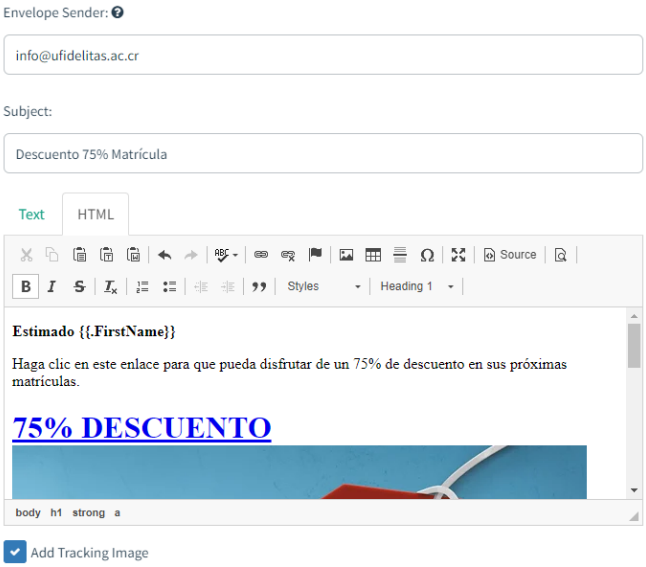
24. El template de email es la estructura de correo que será enviada a las víctimas.
25. Puede obtener un correo real y clonarlo o podrá armarlo usted mismo, tal y como verá en las siguientes filminas.

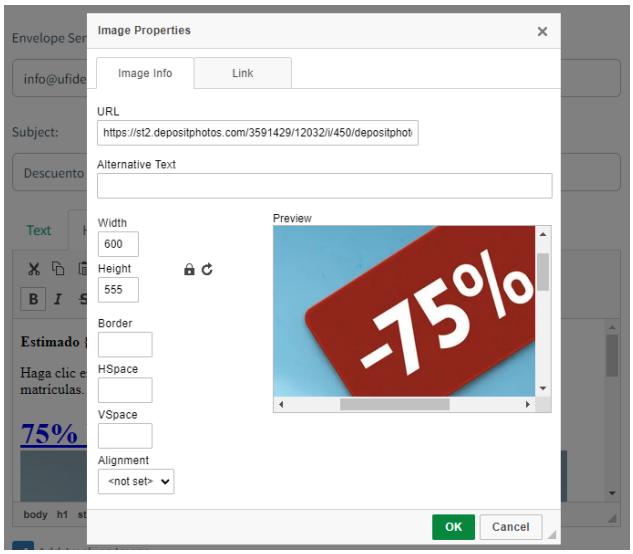
26. Debe agregar imágenes al correo que le hagan pensar a la víctima que es un correo real, una firma, una invitación, etc.
27. Sea creativo, el correo es la pieza clave para el engaño!!!!



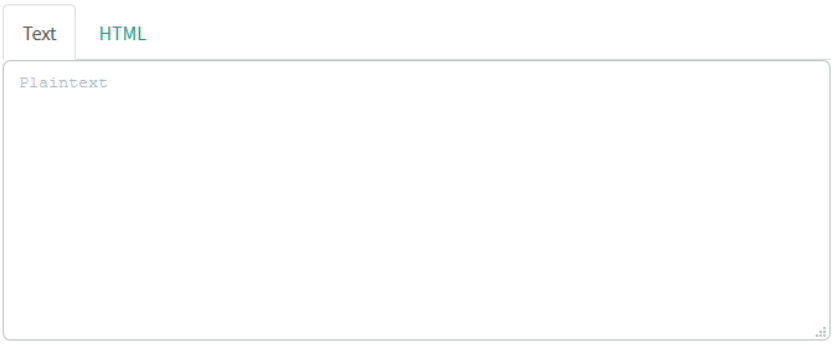
28. Utilice imágenes representativas para la empresa.

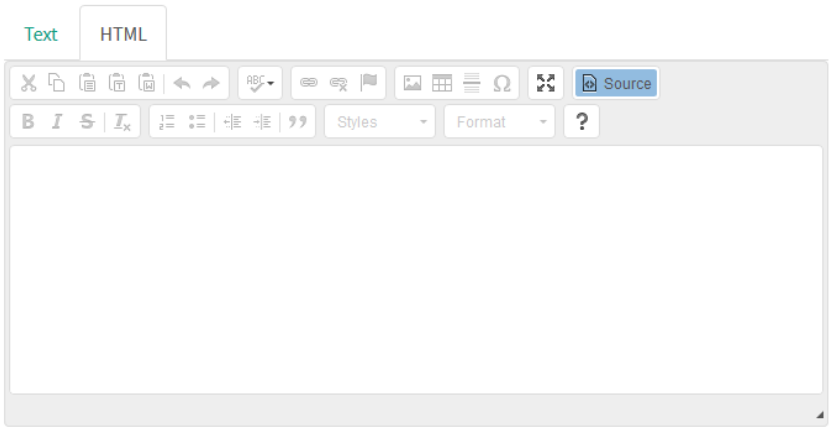
29. Aquí podrá modificar el cuerpo del correo electrónico, puede incluir las variables {{.XXX}} para que sea más personalizado. Para incluir el link, la variable que debe utilizar es {{.URL}} que hará referencia al url de la campaña.
30. Se adjunta una configuración de referencia:



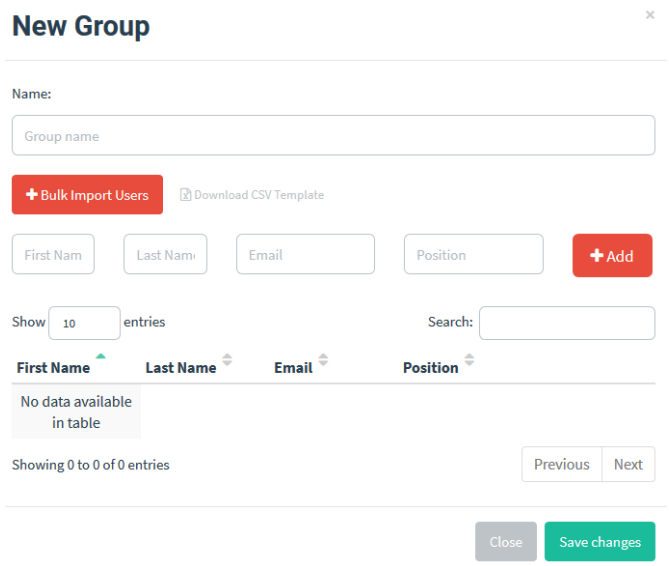


31. Haga pruebas hasta que sea convincente.

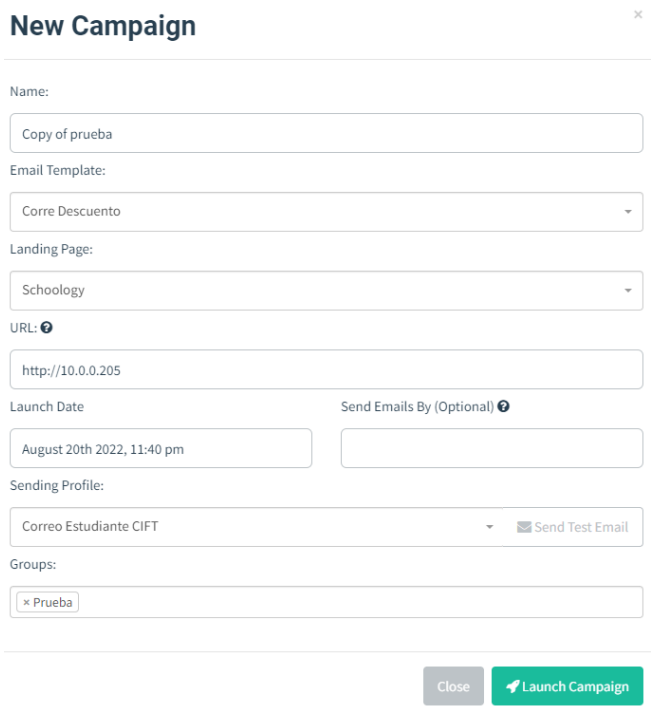


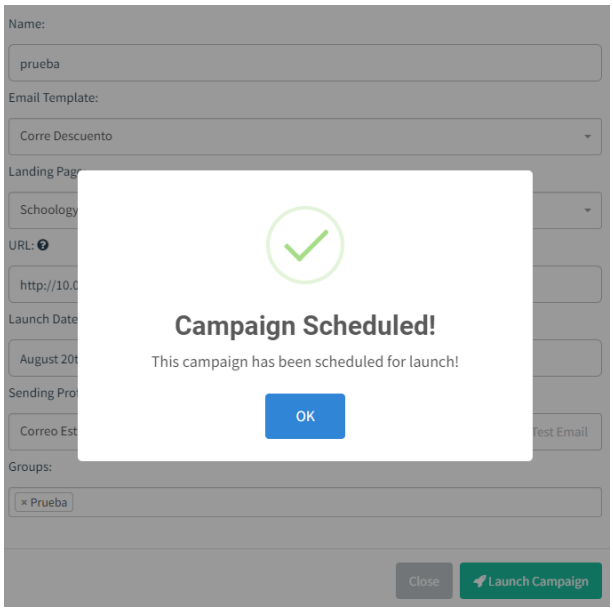


32. Definamos ahora en Users y Groups, la lista de correos a los cuales enviaremos nuestra campaña. Puede importarlos o incluirlos uno a uno.

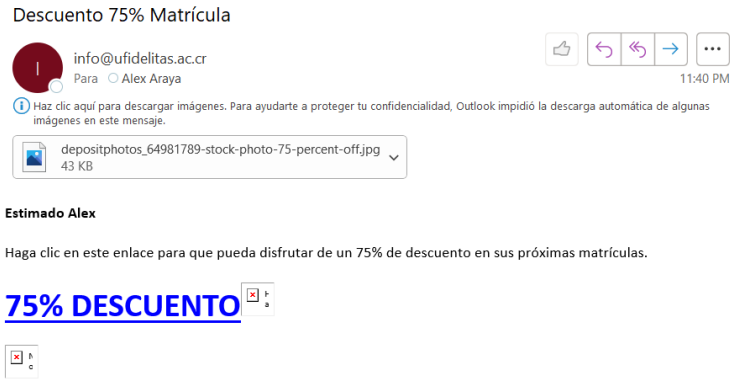


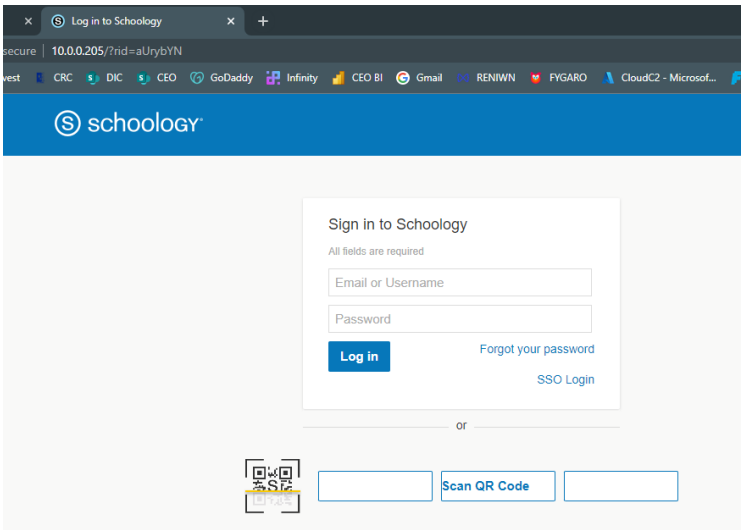
33. Puede definir todos los grupos que desee y seleccionarlos según sea la necesidad o temática del engaño.
34. Vaya ahora a Campaigns, al crear la campaña, deberá seleccionar de las listas desplegables los elementos creados en los pasos anteriores.
35. En el url, debe ser cuidadoso, y poner la ip pública del sitio o el dominio adquirido.



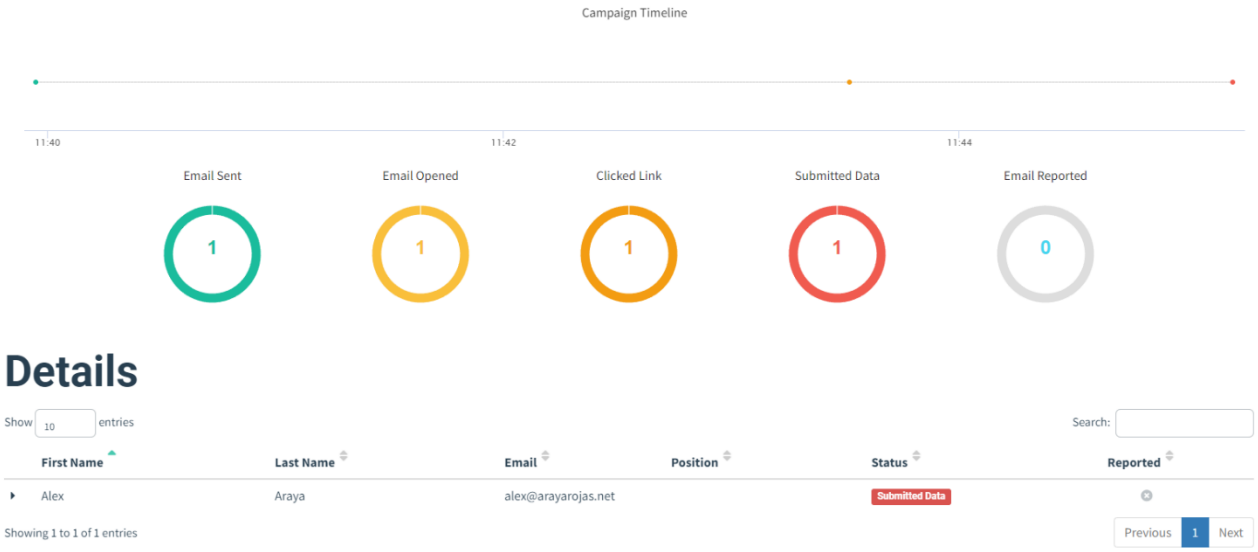


36. Haga pruebas internas hasta que el resultado sea el deseado. Algunos ejemplos:





37. Evalúe los resultados en el dashboard.



Details

Show 10 entries

Search:

First Name	Last Name	Email	Position	Status	Reported
Alex	Araya	alex@arayarojas.net		Submitted Data	

Showing 1 to 1 of 1 entries

Previous 1 Next

Timeline for Alex Araya

Email: alex@arayarojas.net
Result ID: aUrybYN

Campaign Created — *August 20th 2022 11:39:55 pm*

Email Sent — *August 20th 2022 11:39:57 pm*

Clicked Link — *August 20th 2022 11:43:31 pm*

Windows (OS Version: 10)
Chrome (Version: 104.0.0.0)

Submitted Data — *August 20th 2022 11:45:11 pm*

Windows (OS Version: 10)
Chrome (Version: 104.0.0.0)

Replay Credentials

View Details

Parameter	Value(s)
__original_url	https://app.schoology.com/login/login
form_build_id	81e7fc6-_XeW3g6GBmxgLYLZPItll9BU5qWiW1ku3_wacRFc3zQ
form_id	s_user_login_form
mail	pedro
password	password1
school	
school_nid	