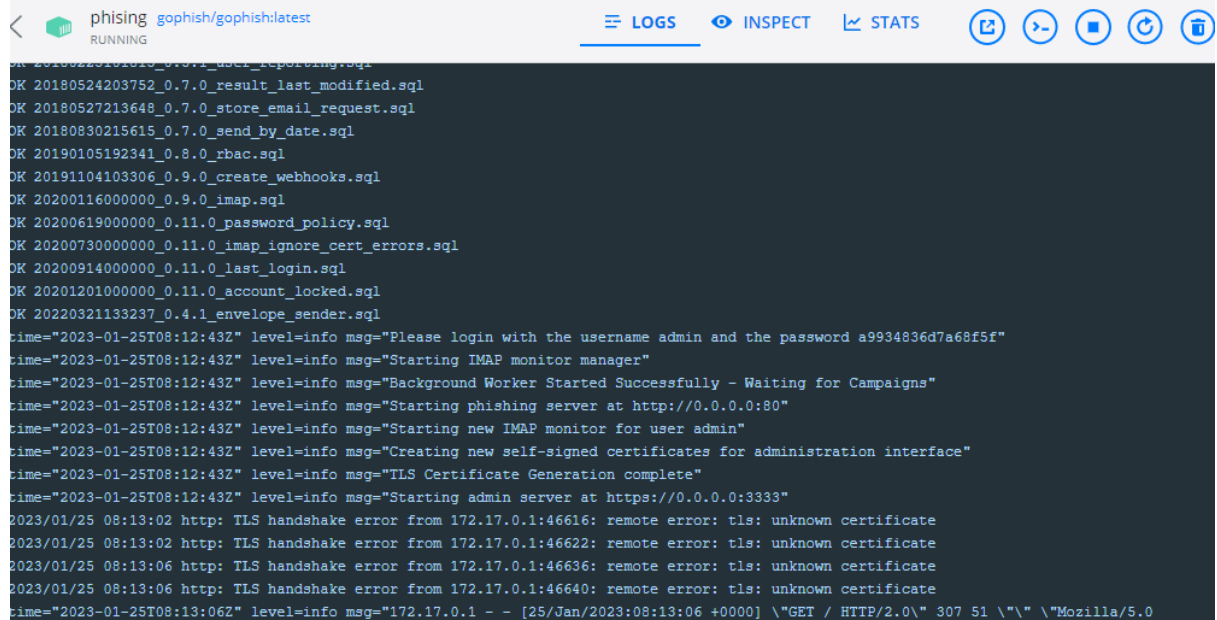


Phishing a uno mismo

Instalamos Gophish y miramos los logs para ver la contraseña inicial. Iniciamos sesion y cambiamos la contraseña.



```
< phishing gophish/gophish:latest
RUNNING

LOGS INSPECT STATS

OK 20180524203752_0.7.0_result_last_modified.sql
OK 20180527213648_0.7.0_store_email_request.sql
OK 20180830215615_0.7.0_send_by_date.sql
OK 20190105192341_0.8.0_rbac.sql
OK 20191104103306_0.9.0_create_webhooks.sql
OK 20200116000000_0.9.0_imap.sql
OK 20200619000000_0.11.0_password_policy.sql
OK 20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK 20200914000000_0.11.0_last_login.sql
OK 20201201000000_0.11.0_account_locked.sql
OK 20220321133237_0.4.1_envelope_sender.sql
time="2023-01-25T08:12:43Z" level=info msg="Please login with the username admin and the password a9934836d7a68f5f"
time="2023-01-25T08:12:43Z" level=info msg="Starting IMAP monitor manager"
time="2023-01-25T08:12:43Z" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2023-01-25T08:12:43Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2023-01-25T08:12:43Z" level=info msg="Starting new IMAP monitor for user admin"
time="2023-01-25T08:12:43Z" level=info msg="Creating new self-signed certificates for administration interface"
time="2023-01-25T08:12:43Z" level=info msg="TLS Certificate Generation complete"
time="2023-01-25T08:12:43Z" level=info msg="Starting admin server at https://0.0.0.0:3333"
2023/01/25 08:13:02 http: TLS handshake error from 172.17.0.1:46616: remote error: tls: unknown certificate
2023/01/25 08:13:02 http: TLS handshake error from 172.17.0.1:46622: remote error: tls: unknown certificate
2023/01/25 08:13:06 http: TLS handshake error from 172.17.0.1:46636: remote error: tls: unknown certificate
2023/01/25 08:13:06 http: TLS handshake error from 172.17.0.1:46640: remote error: tls: unknown certificate
time="2023-01-25T08:13:06Z" level=info msg="172.17.0.1 - - [25/Jan/2023:08:13:06 +0000] \"GET / HTTP/2.0\" 307 51 \"\" \"Mozilla/5.0"
```

Añadimos las credenciales de quien va a enviar los correos, así como el servidor que utiliza y el puerto.

Edit Sending Profile

Name:

Interface Type:

SMTP

SMTP From: ?

Host:

Username:

Password:

☒ Ignore Certificate Errors ?


Email Headers:

[+ Add Custom Header](#)

Ahora creamos la plantilla que usaremos para enviar los correos.

Name:

phishing propio

 Import Email


Envelope Sender: ?

Pablo Pérez Martínez (vía AulaVirtual) <noreply@educa.madrid.org>

Subject:

Pablo Pérez Martínez ha hecho un comentario en la tarea Práctica 4: HTTP 2

Text HTML



SR -> [Tarea](#) -> [Práctica 4: HTTP 2](#)

Pablo Pérez Martínez ha aportado alguna retroalimentación en su entrega de la tarea 'Práctica 4: HTTP 2'

Puede verla añadida [a su entrega](#).

{{.Tracker}}

body p

Ahora que tenemos la plantilla hecha vamos a crear la landing page donde robaremos las credenciales de la victima.

[illegible]

Por ultimo nos falta añadir un grupo de victimas para el ataque y lanzar la campaña.

New Group

Name:

+ Bulk Import Users

Download CSV Template

cesar

gil

cesgilher@gmail.cc

Position

+ Add

New Campaign

Name:

Email Template:

Landing Page:

URL: ?

Launch Date

Send Emails By (Optional) ?

January 25th 2023, 10:24 am

Sending Profile:

cesar

Send Test Email

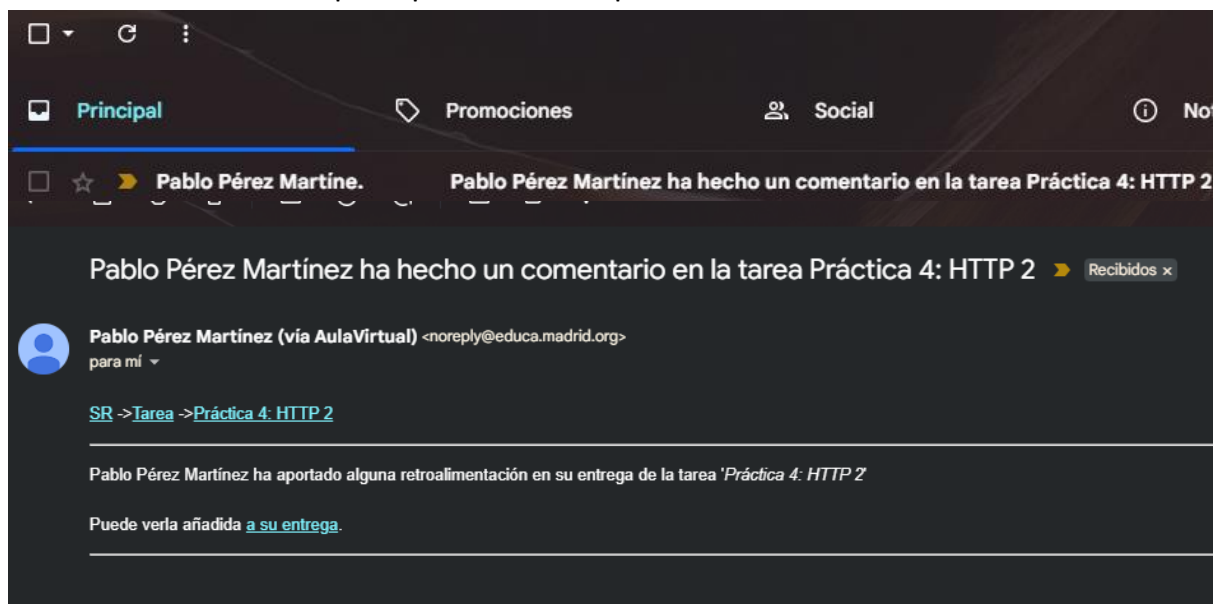
Groups:

× alumnos

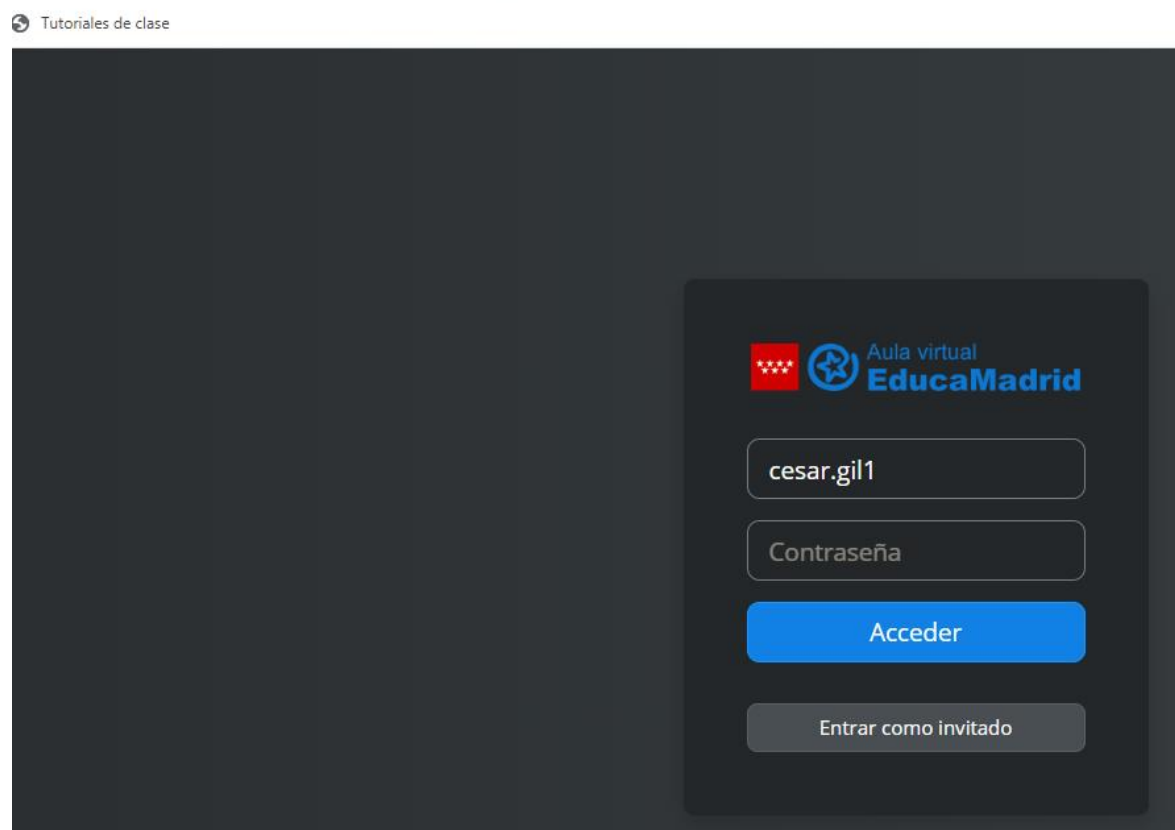
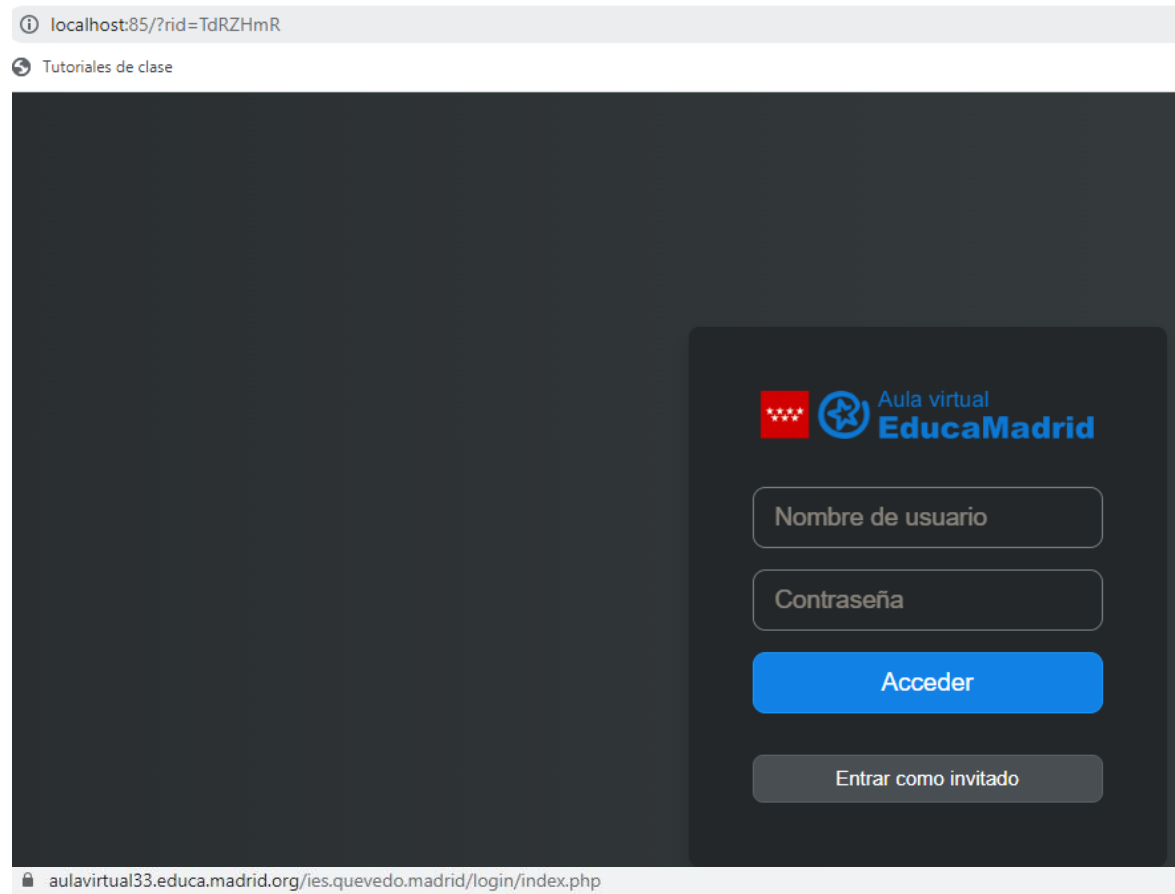
Close

Launch Campaign

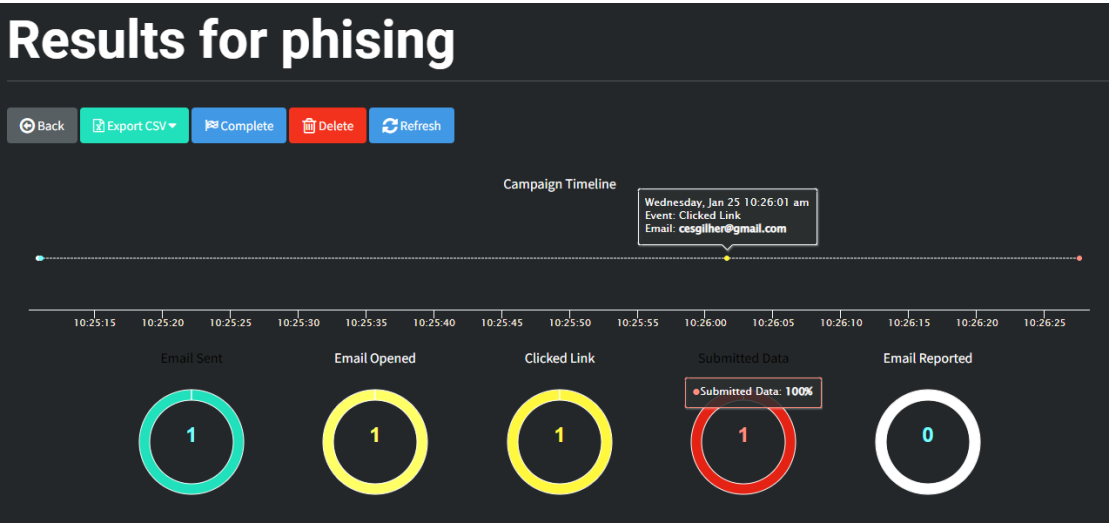
Una vez lanzada la campaña podemos ver que el correo se ha enviado.



Podemos ver que la landing page es idéntica a la original salvo por la url, pero si por ejemplo lo abres desde el móvil, el enlace no es tan obvio.



Podemos controlar cada paso del ataque para así tener control de que efectividad tiene , o donde pudiera estar el fallo.



Credenciales ingresadas.

Timeline for cesar gil

Email: cesgilher@gmail.com
Result ID: TdRZHmR

Campaign Created

January 25th 2023 10:25:10 am

Email Sent

January 25th 2023 10:25:11 am

Clicked Link

January 25th 2023 10:26:01 am

Windows (OS Version: 10)

Chrome (Version: 109.0.0.0)

Submitted Data

January 25th 2023 10:26:27 am

Windows (OS Version: 10)

Chrome (Version: 109.0.0.0)

Replay Credentials

View Details

Parameter	Value(s)
__original_url	https://aulavirtual33.educa.madrid.org/ies.quevedo.madrid/login/index.php
logintoken	ohTe26TRGigDZiog1l8IHhBEDtypCVOF
password	oscar espabila maquina
username	cesar.gil1