

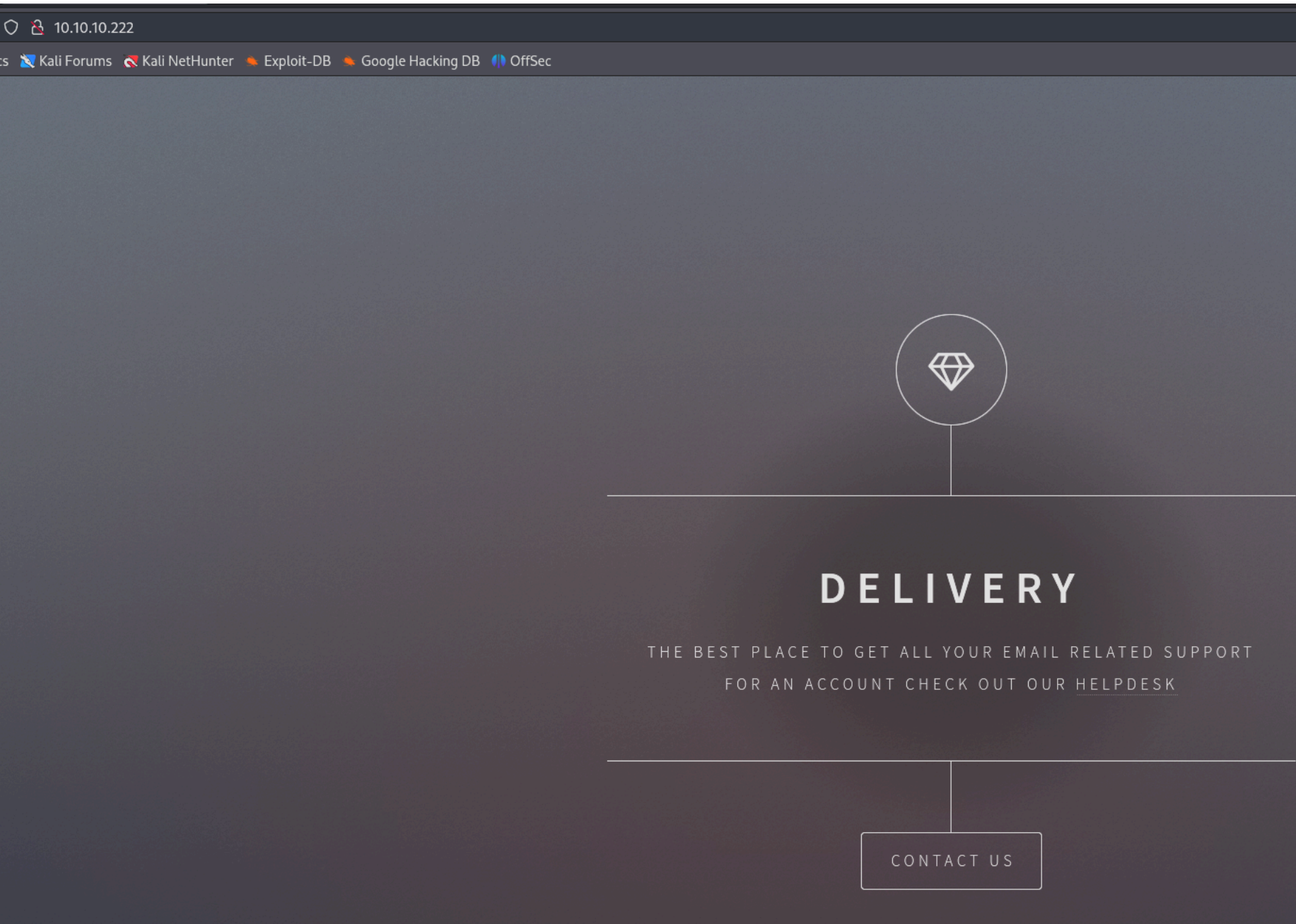
Delivery - Writeup

RECONOCIMIENTO - EXPLOTACION

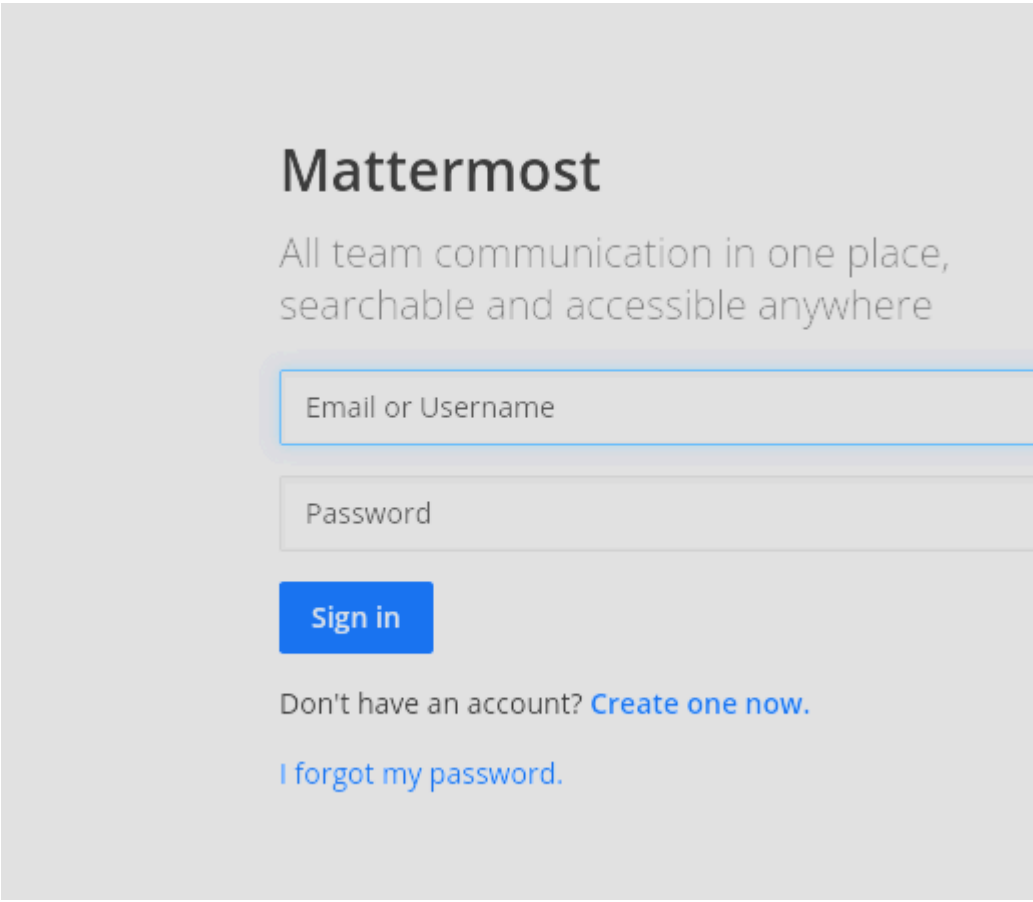
Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:40:fa:85:9b:01:ac:ac:0e:bc:0c:19:51:8a:ee:27 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACq549E025Q9FR27LDR6WZRQ52ikKjKUQLmE9ndEKjB0i1q0oL
VPDdWfmEiagBlG3H7IZ7yA08gcg0RRrIQjE7XTMV09GmxEUTjojoLoqudUvbUi8COHC06baVmyjZRlXRcQ6qTKIxR
IEhHNL8DBAUfQWzQjvVjYNOLqGp/WdLKA1RLA0klpIdJQ9iehSH0q6nqjeTUv47mIHUiqaM+vLkCEAN3AAQH5mB/1
|   256 5a:0c:c0:3b:9b:76:55:2e:6e:c4:f4:b9:5d:76:17:09 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBAiAKnk2lw0Gxzz
nR9tHvjdN7R3hY=
|   256 b7:9d:f7:48:9d:a2:f2:76:30:fd:42:d3:35:3a:80:8c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEV5D6eYjySqfhW4l4IF1SZkZHxIRihnY6Mn6D8mLEW7
80/tcp    open  http      syn-ack ttl 63  nginx 1.14.2
|_http-server-header: nginx/1.14.2
| http-methods:
|_ Supported Methods: GET HEAD
|_http-title: Welcome
8065/tcp  open  unknown  syn-ack ttl 63
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest, SSLSessionReq, TerminalServerCookie:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain; charset=utf-8
|   Connection: close
|   Request
|   GetRequest:
```

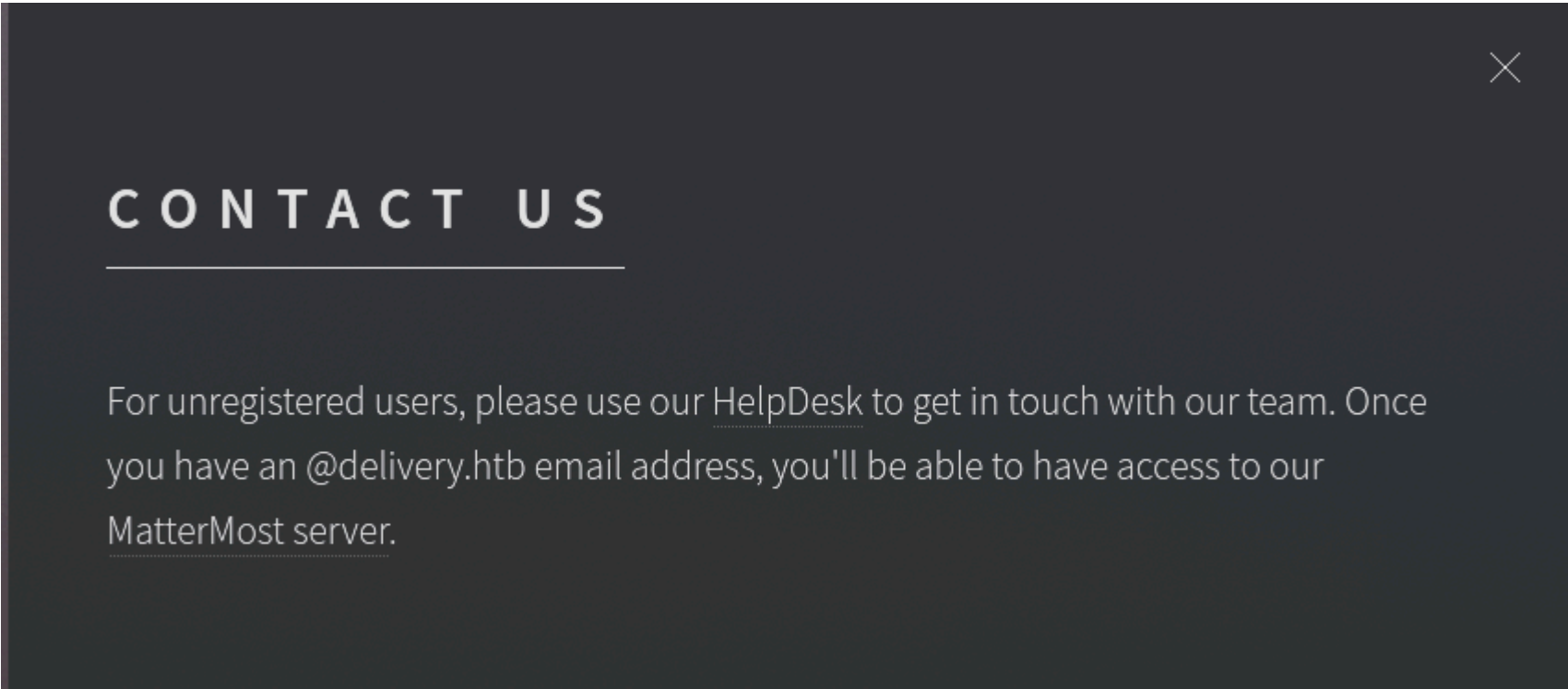
En el puerto 80 nos encontramos lo siguiente:



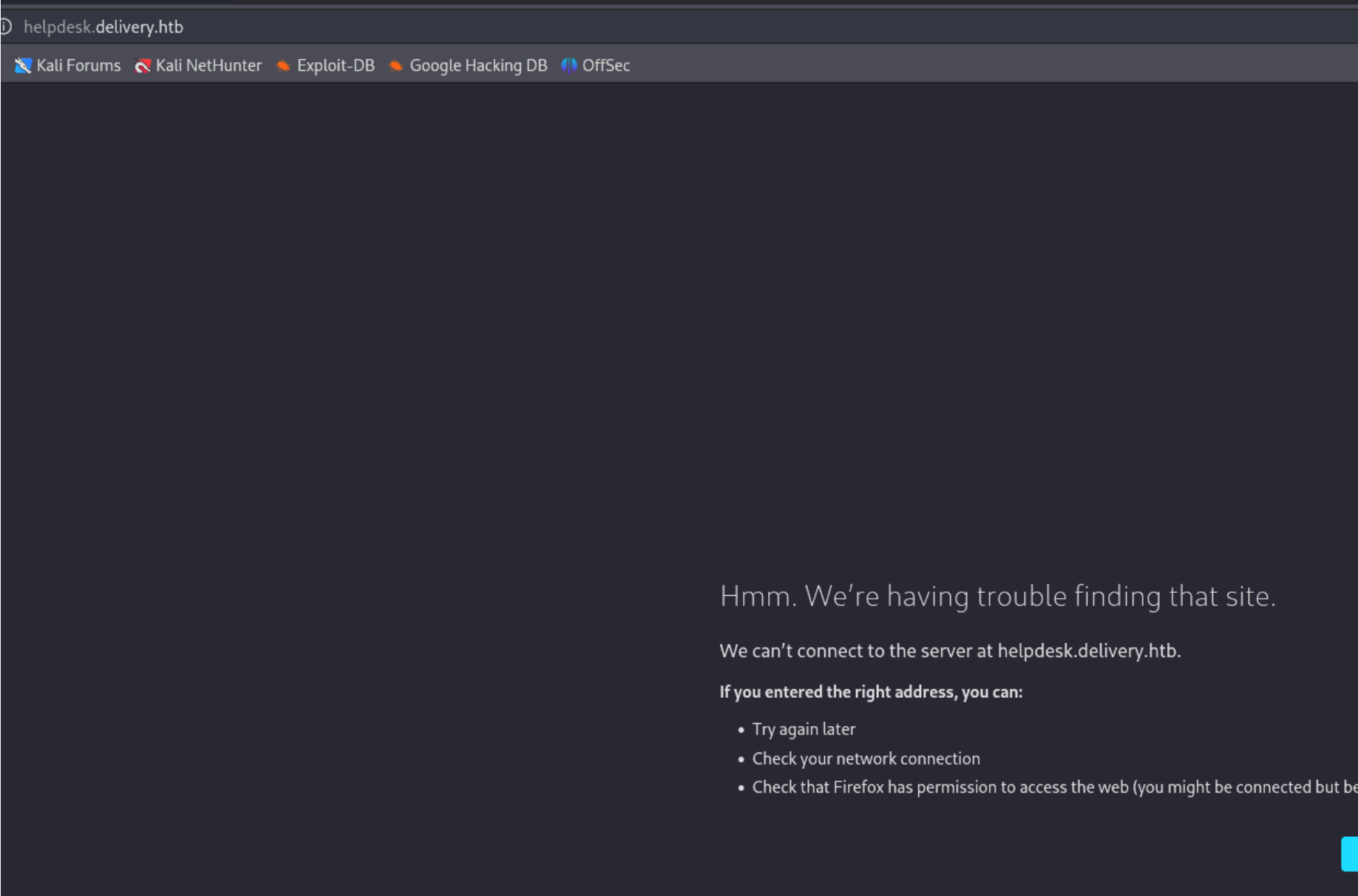
En el puerto 8065:



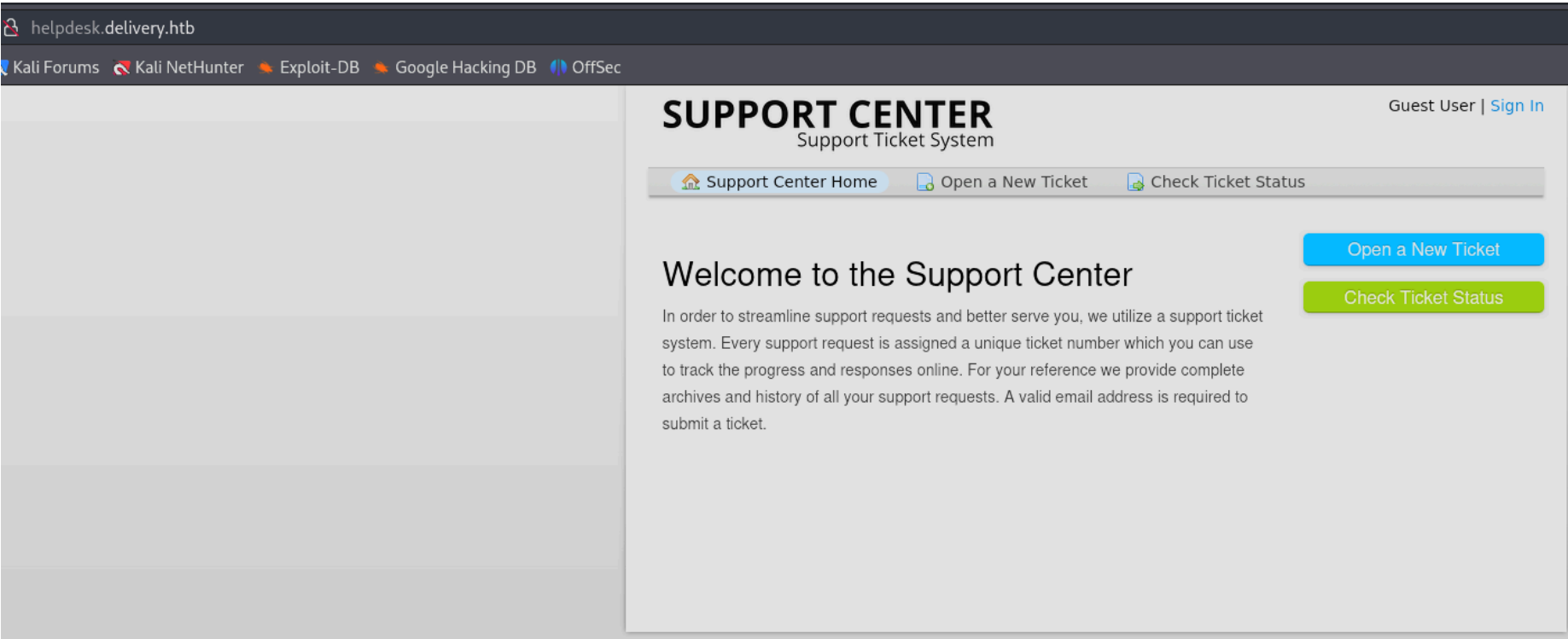
En el puerto 80, si hacemos click en contact us podemos encontrar un dominio:



Si hacemos click en HelpDesk encontramos un subdominio:



Añadimos el subdominio al archivo /etc/hosts y volvemos a acceder:



Podemos abrir un nuevo ticket sin logearnos:

Open a New Ticket

Please fill in the form below to open a new ticket.

Contact Information

Email Address *

hacker@delivery.htb

Full Name *

hacker

Phone Number

123456789

Ext:

11

Help Topic

Contact Us

Ticket Details

Please Describe Your Issue

Issue Summary *

test

<> ¶ A Aa B / U ↻ ☰ 🖼️ 📺 ☰ 🔗 —

test

unsaved

📎 Drop files here or [choose them](#)

CAPTCHA Text:

3C019

3C019

Enter the text shown on the image. *

Create Ticket

Reset

Cancel

Nos dice que podemos ver el estatus del ticket, ademas, podemos añadir mas informacion al ticket si enviamos un email al correo 2871340@delivery.htb :

hacker,

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 2871340.

If you want to add more information to your ticket, just email 2871340@delivery.htb.

Thanks,

Support Team

Entramos en check status:

Cancel

Ahi podemos ver el ticket que hemos tramitado. Ahora volvemos al panel de login de "Mattermost".

Mattermost

All team communication in one place,
searchable and accessible anywhere

Email or Username

Password

Sign in

Don't have an account? [Create one now.](#)

[I forgot my password.](#)

Creamos una nueva cuenta:

Mattermost

All team communication in one place,
searchable and accessible anywhere

Let's create your account

Already have an account? [Click here to sign in.](#)

What's your email address?

test@test.com

Valid email required for sign-up

Choose your username

test

You can use lowercase letters, numbers, periods, dashes, and underscores.

Choose your password

.GdVxR9frZSX_]8|

Create Account

By proceeding to create your account and use Mattermost,
you agree to our [Terms of Service](#) and [Privacy Policy](#). If you
do not agree, you cannot use Mattermost.

Y tenemos que verificar el correo en `test@test.com` , cosa que no podemos:

Mattermost: You are almost done

Please verify your email address. Check your inbox for an email.

Resend Email

Si hacemos memoria, nos decia que para añadir mas informacion en el ticket podemos usar el correo 2871340@delivery.htb .
Vamos a probar a abrimos una cuenta utilizando ese correo para ver si nos llega la verificación a ticket que he creado:

Mattermost

All team communication in one place,
searchable and accessible anywhere

Let's create your account

Already have an account? [Click here to sign in.](#)

What's your email address?

2871340@delivery.htb

Valid email required for sign-up

Choose your username

hackerx

You can use lowercase letters, numbers, periods, dashes, and underscores.

Choose your password

.GdVxR9frZSX_]8

Create Account

By proceeding to create your account and use Mattermost, you agree to our [Terms of Service](#) and [Privacy Policy](#). If you do not agree, you cannot use Mattermost.

Enviamos la verificación:

Mattermost: You are almost done

Please verify your email address. Check your inbox for an email.

Resend Email


✔ Verification email sent.

Y nos llega la activación de la cuenta donde hemos accedido para ver el ticket:

test #2871340


PrintEdit

Basic Ticket Information	User Information
Ticket Status: Open	Name: Hacker
Department: Support	Email: hacker@delivery.htb
Create Date: 11/5/24 5:11 AM	Phone: 123456789 x11




hacker posted 11/5/24 5:11 AM

---- Registration Successful ---- Please activate your email by going to: http://delivery.htb:8065/do_verify_email?token=wbikbas4h6p87773a6on1pjfo3ck8oe9fbsnxpwdnoxgbga4spcp4jpaumkzbjy5&email=2871340%40delivery.htb



Created by

 hacker 11/5/24 5:11 AM

Nos dice que podemos ir una ruta para activar el correo:

Mattermost

All team communication in one place, searchable and accessible anywhere

✓ Email Verified

2871340@delivery.htb

Password

Sign in

Don't have an account? [Create one now.](#)

[I forgot my password.](#)

Ya esta el email verificado, ahora podemos iniciar sesion:

Preview Mode: Email notifications have not been configured.

Mattermost

All team communication in one place, searchable and accessible anywhere


Teams you can join:

Internal

>

[Create a team](#)


Podemos ver que el usuario root filtra unas credenciales:



System

9:25 AM


@root joined the team.



System

9:28 AM

@root updated the channel display name from: Town Square to: Internal




root

9:29 AM

@developers Please update theme to the OSTicket before we go live. Credentials to the server are maildeliverer:Youve_G0t_Mail!

Also please create a program to help us stop re-using the same passwords everywhere.... Especially those that are a variant of "PleaseSubscribe!"

(edited)



root

10:58 AM

PleaseSubscribe! may not be in RockYou but if any hacker manages to get our hashes, they can use hashcat rules to easily crack all variations of common words or phrases.

(edited)

Vamos a intentar conectarnos por ssh utilizando esas credenciales:

```
(kali@kali)~[~/Downloads]
$ ssh maildeliverer@10.10.10.222
The authenticity of host '10.10.10.222 (10.10.10.222)' can't be established.
ED25519 key fingerprint is SHA256:AGdhHnQ749stJakbrtXVi48e6KTkaMj/+QNYMW+tyj8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.222' (ED25519) to the list of known hosts.
maildeliverer@10.10.10.222's password:
Linux Delivery 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan  5 06:09:50 2021 from 10.10.14.5
maildeliverer@Delivery:~$
```

ESCALADA DE PRIVILEGIOS

Encontramos informacion en la siguiente ruta:

```
maildeliverer@Delivery:/opt/mattermost/config$ ls -la
total 36
drwxrwxr-x  2 mattermost mattermost 4096 Dec 26  2020 .
drwxrwxr-x 12 mattermost mattermost 4096 Jul 14  2021 ..
-rw-rw-r--  1 mattermost mattermost  922 Dec 18  2020 cloud_defaults.json
-rw-rw-r--  1 mattermost mattermost 18774 Nov  5  05:08 config.json
-rw-rw-r--  1 mattermost mattermost  243 Dec 18  2020 README.md
```

El archivo config.json tiene claves para conectarse a mysql:

```
maildeliverer@Delivery:/opt/mattermost/config$ ls -la
total 36
drwxrwxr-x  2 mattermost mattermost 4096 Dec 26  2020 .
drwxrwxr-x 12 mattermost mattermost 4096 Jul 14  2021 ..
-rw-rw-r--  1 mattermost mattermost  922 Dec 18  2020 cloud_defaults.json
-rw-rw-r--  1 mattermost mattermost 18774 Nov  5  05:08 config.json
-rw-rw-r--  1 mattermost mattermost  243 Dec 18  2020 README.md
```

Estamos dentro

```
maildeliverer@Delivery:/opt/mattermost/config$ mysql -h localhost -u mmuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 64
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Dentro de la base de datos "mattermost" en la tabla "users", podemos encontrar unas contraseñas:

Id	Username	Password	MfaSecret
64nq8nue7pyhpgwm99a949mwy	surveybot		
6akd5cxuhfgrbny81nj55au4za	c3ecacacc7b94f909d04dbfd308a9b93	\$2a\$10\$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvpiLaS7ImuiItEiK	
6wxx1gggn63r7f8q1hpzp7t4i	5b785171bfb34762a933e127630c4860	\$2a\$10\$3m0quqyvCE8Z/R1gFcCOW06tEj6FtqtBn8fRAXQXmaKmg.HDGpS/G	
8kej4gajdtbi8p5zpdcpo6ocy	hackerx	\$2a\$10\$jdpGUDx12W0ln6jMmrQKyeavr7YtG.IBhm5g31tW/YkYnAkQQm5Ta	
dijg7mcf4tf3xrgxi5ntqdefma	root	\$2a\$10\$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0	
hatotzdacb8mbe95hm4ei8i7ny	ff0a21fc6fc2488195e16ea854c963ee	\$2a\$10\$RnJsISTLc9W3iUcUggl1KOG9vqADED24CQcQ8zvUm1Ir9pxS.Pduq	
jing8rk6mjdbudcidw6wz94r	channellexport		
n9magehhzincig4mm97xyft9sc	9ecfb4be145d47fda0724f697f35ffaf	\$2a\$10\$s.cLPSjAVgawG0JwB7vrqenPg2lrDtOECrtjwWah0zHfq1CoFyFqm	
xnnxc5nhobfg9qbz1ithmfxkme	test	\$2a\$10\$/XGMDhtLMzDiogSKZ26fQ0zX0dviI7HR/s59CljcphiYD6zY8FLui	

He intentado romper los hashes con rockyou pero no he encontrado la contraseña. Si nos fijamos en la pista que nos da en el chat interno, nos eviten poner variaciones de "PleaseSubscribe!" ya que disponiendo de un hash y añadiendo variaciones a la contraseña de "PleaseSubscribe!" podemos conseguir la contraseña:

Also please create a program to help us stop re-using the same passwords everywhere.... Especially those that are a variant of "PleaseSubscribe!"
(edited)

root 10:58 AM

PleaseSubscribe! may not be in RockYou but if any hacker manages to get our hashes, they can use hashcat rules to easily crack all variations of common words or phrases.
(edited)

Sabiendo que el hash esta en formato bcript:

3200	bcrypt \$2*\$, Blowfish (Unix)	\$2a\$05\$LhayLxezLhK1LhW
------	--------------------------------	---------------------------

Y que queremos utilizar variaciones de "PleaseSubscribe!":

```
(kali@kali)-[~/Downloads]
$ cat custom.txt
PleaseSubscribe!229381927:18271
```

Y chatgpt me recomienda usar la regla de hashcat "best64":

```
(kali@kali)-[~/Downloads]
$ locate best64
/usr/share/hashcat/rules/best64.rule
/usr/share/john/rules/best64.rule
```

Vamos a ejecutar el siguiente comando:

```
hashcat -m 3200 -a 0 pass2.txt custom.txt -r /usr/share/hashcat/rules/best64.rule
```

Nos dice cual es la contraseña en texto plano:

```
$2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0:PleaseSubscribe!21
```

Ese hash es el que corresponde al usuario root:

Id	Username	Password
64nq8nue7pyhpgwm99a949mwy	surveybot	
6akd5cxuhfgrbny81nj55au4za	c3ecacacc7b94f909d04dbfd308a9b93	\$2a\$10\$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvpiLaS7ImuiItEiK
6wqx1ggng63r7f8q1hpzp7t4iiy	5b785171bfb34762a933e127630c4860	\$2a\$10\$3m0quqyvCE8Z/R1gFcCOW06tEj6FtqtBn8fRAXQXmaKmg.HDGpS/G
8kej4gajdtbi8p5zpdcpo6ocy	hackerx	\$2a\$10\$jdpGUDx12W0ln6jMmrQKyeavr7YtG.IBhm5g31tW/YkYnAkQQm5Ta
dijg7mcf4tf3xrgxi5ntqdefma	root	\$2a\$10\$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0

Iniciamos sesion con el usuario root:

```
maildeliverer@Delivery:/opt/mattermost/config$ su root
Password:
root@Delivery:/opt/mattermost/config# whoami
root
```