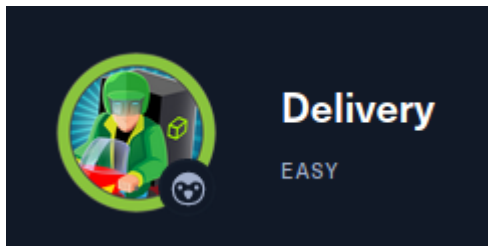


# DELIVERY



## enumeracion

```
-p-      todos los puertos
--open   solo los abiertos
-T5      forma rápida de escanear
-v       verbose (avisa ni bien encuentra un puerto)
-n       no realiza la resolución DNS
-oG      exportar en formato grepeable
allPorts nombre del archivo
```

filtramos los puertos con extractPorts

```
extractPorts allPorts
```

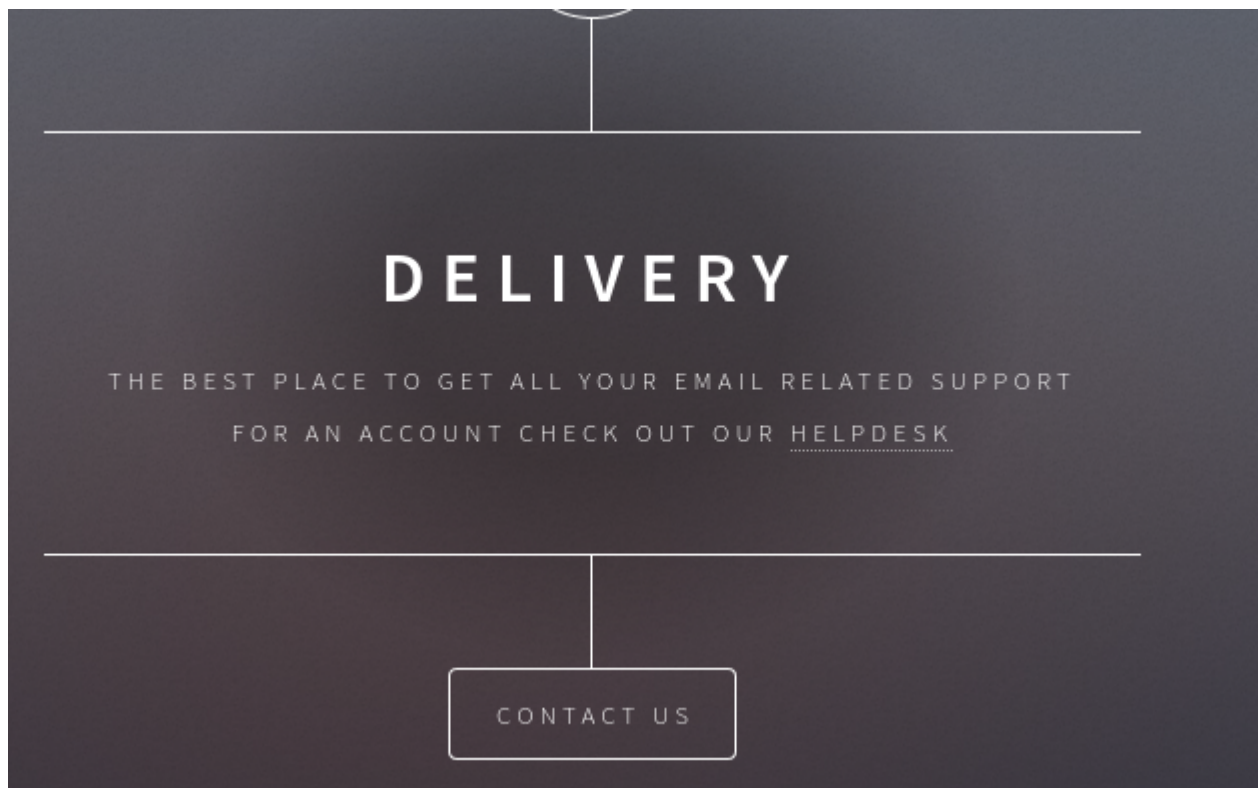
```
nmap -p22,80,8065 -sS -sC -sV 10.10.10.222 -oN targeted
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 21:02 -04
Nmap scan report for spectra.htb (10.10.10.222)
Host is up (0.14s latency).

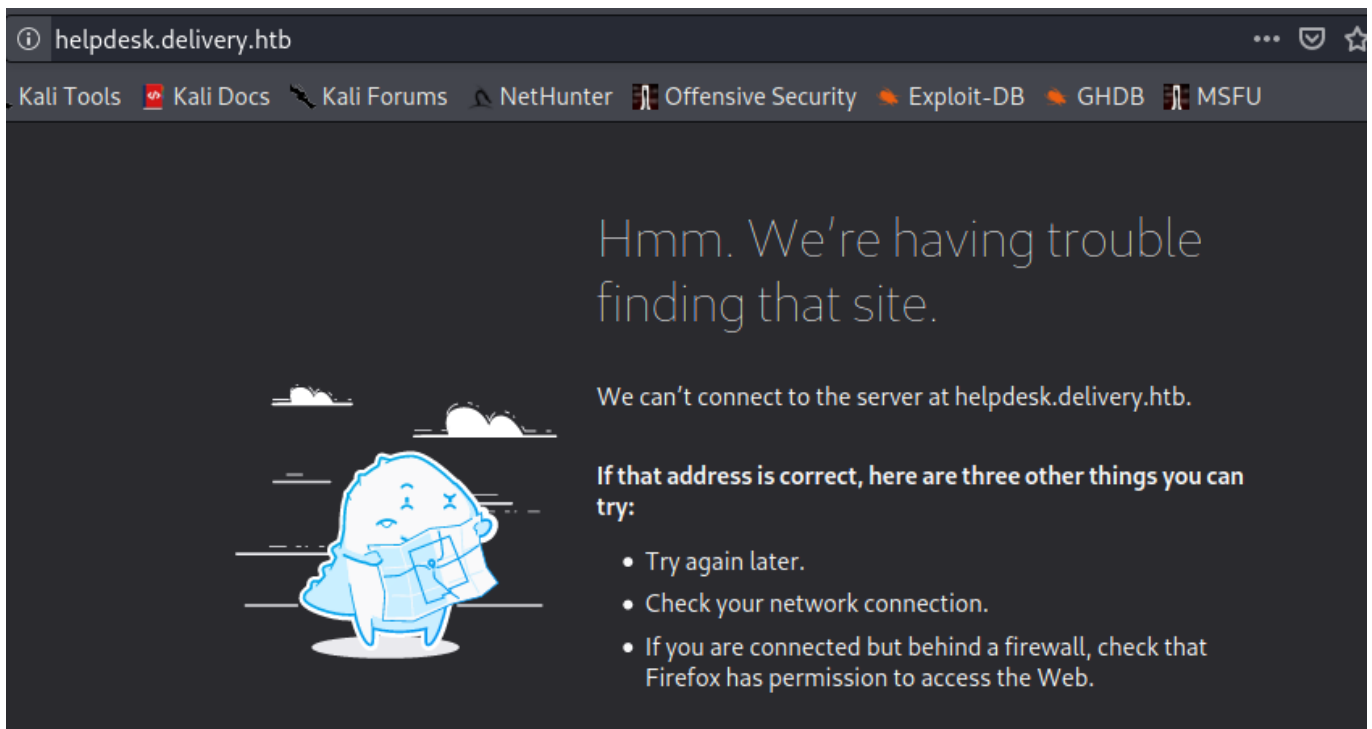
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:40:fa:85:9b:01:ac:ac:0e:bc:0c:19:51:8a:ee:27 (RSA)
|   256 5a:0c:c0:3b:9b:76:55:2e:6e:c4:f4:b9:5d:76:17:09 (ECDSA)
|_  256 b7:9d:f7:48:9d:a2:f2:76:30:fd:42:d3:35:3a:80:8c (ED25519)
80/tcp    open  http     nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Welcome
```

```
8065/tcp open  unknown
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest, SSLSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Accept-Ranges: bytes
|     Cache-Control: no-cache, max-age=31556926, public
|     Content-Length: 3108
|     Content-Security-Policy: frame-ancestors 'self'; script-src 'self'
cdn.rudderlabs.com
|     Content-Type: text/html; charset=utf-8
|     Last-Modified: Fri, 14 May 2021 20:18:52 GMT
|     X-Frame-Options: SAMEORIGIN
```

Tanto el puerto 80 como el 8065 son paginas web, veamos primero el 80:



Vamos a helpdesk:

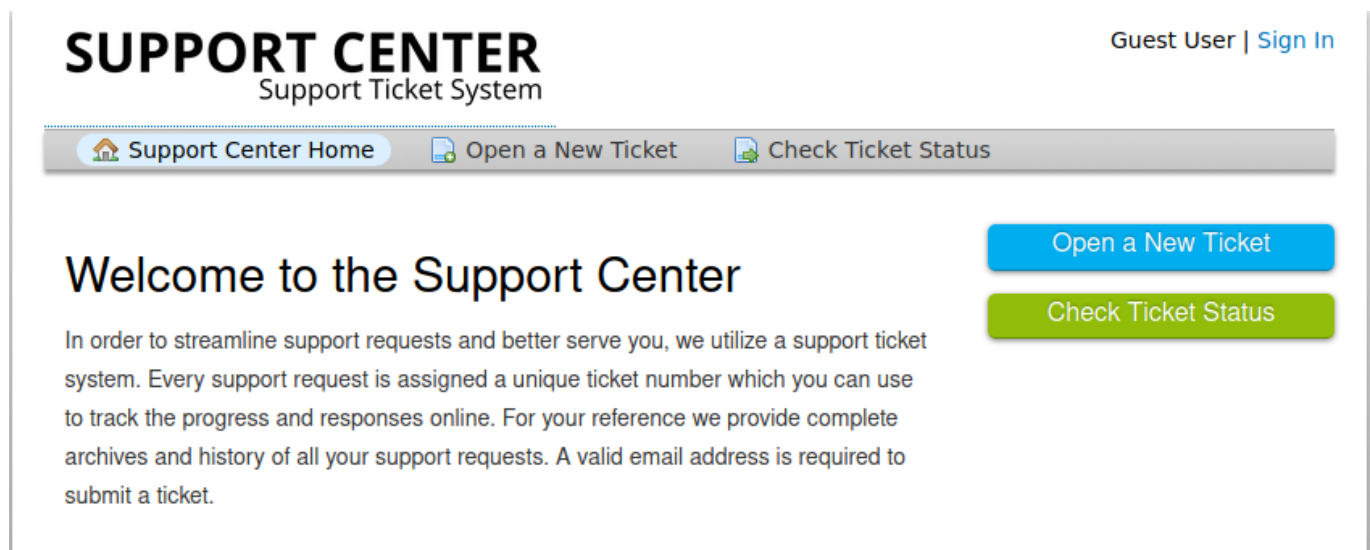


No se nos interpreta porque tiene un subdominio helpdesk, vamos a agregarlo a /etc/hosts:

```
nano /etc/hosts

10.10.10.222    delivery.htb
10.10.10.222    helpdesk.delivery.htb
```

ahora veremos la pagina de helpdesk:



El wappalyzer indica que usa osTicket, un sistema de tickets:

vamos a crear uno con el boton "Open a New Ticket":

## Open a New Ticket

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

---

### Contact Information

**Email Address \***

**Full Name \***

Phone Number

 Ext: 

---

### Help Topic

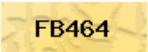
Contact Us  \*

**Issue Summary \***

<> ¶ A Aa B / U ↺ ☰ 🖼️ 📺 ☰ 🔗 —

Details on the reason(s) for opening the ticket.

📎 Drop files here or [choose them](#)

CAPTCHA Text:   Enter the text shown on the image. \*

Vamos a llenar los datos:

- email: [soporte@mailinator.com](mailto:soporte@mailinator.com)
- full name: kriko69

- phone: 7777777777
- Ext: 1234
- Help Topic: Contact us
- Issue Summary: local
- Details: hello

(son datos aleatorios)

Al llenar el formulario vamos a ver que se nos crea un ticket:

✔ Support ticket request created

kriko69,

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 7548135.

If you want to add more information to your ticket, just email [7548135@delivery.htb](mailto:7548135@delivery.htb).

Thanks,

Support Team

Estos valores los vamos a guardar porque para algo serviran:

- id: 7548135
- email: [7548135@delivery.htb](mailto:7548135@delivery.htb)

En la parte del inicio, donde existia la opcion para crear un ticket tambien se puede verificar su estado, vamos a perobar eso con nuestro ticket creado:

Nos pide el correo con el que creamos el ticket y su id:

## Check Ticket Status

Please provide your email address and a ticket number. This will sign you in to view your ticket.

Email Address:

Ticket Number:

Have an account with us? [Sign In](#) or [register for an account](#) to access all your tickets.



Y le damos en view ticket:

### Basic Ticket Information

Ticket Status: Open  
Department: Support  
Create Date: 5/17/21 6:20 PM

### User Information

Name: Kriko69  
Email: soporte@mailinator.com  
Phone: (777) 777-7777 x1234



**kriko69** posted 5/17/21 6:20 PM

hello



Created by **kriko69** 5/17/21 6:20 PM

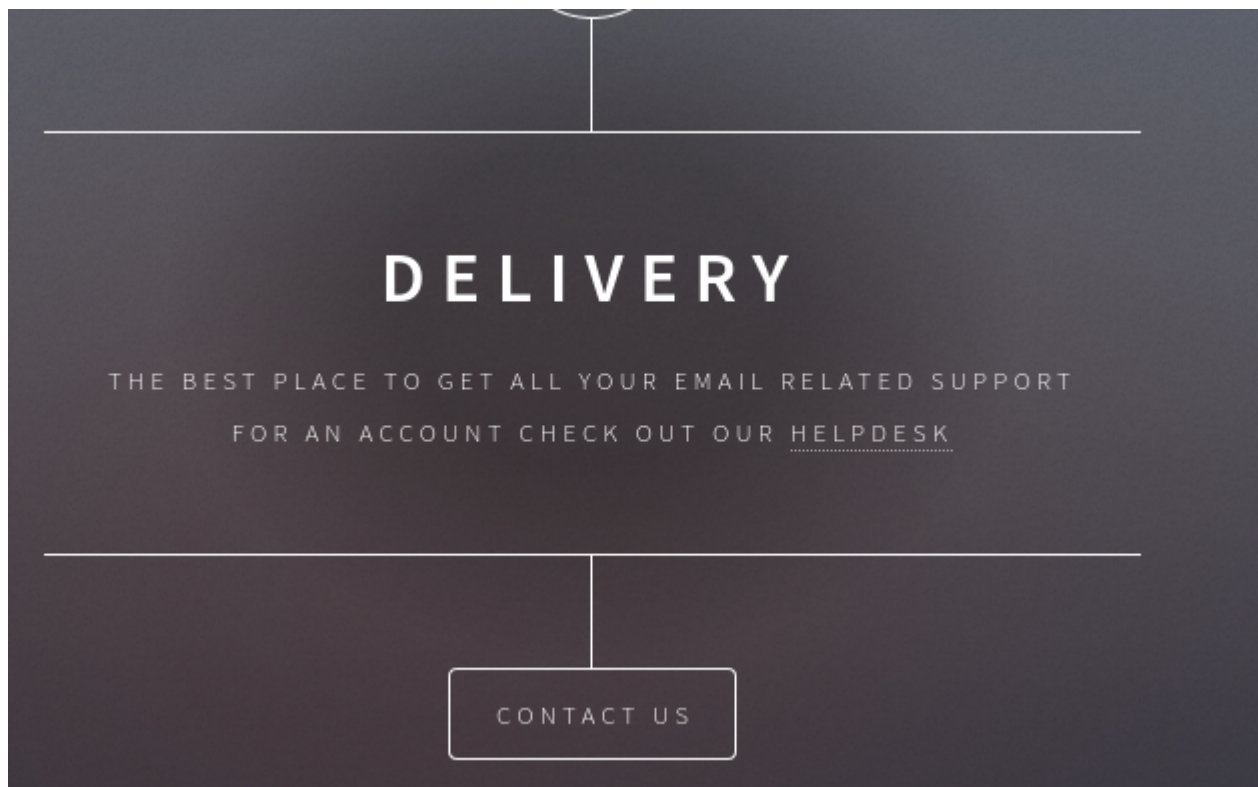
### Post a Reply

To best assist you, we request that you be specific and detailed \*

<> —

Parece algo como una bandeja de entrada.

Veamos la pagina de inicio otra vez:



Veamos que nos da el boton de contact us:



## CONTACT US

---

For unregistered users, please use our [HelpDesk](#) to get in touch with our team. Once you have an [@delivery.htb](#) email address, you'll be able to have access to our [MatterMost server](#).

Nos indica que si no estamos registrado, que en el apartado de helpdesk una vez que obtengamos un email con el "@delivery.htb" podemos acceder al Mattermost server. Ya tenemos ese correo con el ticket ([7548135@delivery.htb](mailto:7548135@delivery.htb)). Entonces vamos a ver a donde nos lleva el MatterMost Server:

## Mattermost

All team communication in one place, searchable and accessible anywhere

Sign in

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

[I forgot my password.](#)

Vemos un inicio de sesion, tenemos el correo pero no una contraseña asi que vamos a crearnos una cuenta en "Create one now":

What's your email address?

Valid email required for sign-up

Choose your username

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

Choose your password

Create Account

Ponemos los datos:

- email: [7548135@delivery.htb](mailto:7548135@delivery.htb)
- username: kriko6969
- password Kriko6969!

**Mattermost: You are almost done**

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

Resend Email

No indica que nos envío un correo para verificar la cuenta, veamos en el apartado de tickets que parecía un buzón:

Después de recargar nos aparece esto:



### Basic Ticket Information

Ticket Status: Open  
Department: Support  
Create Date: 5/17/21 6:20 PM

### User Information

Name: Kriko69  
Email: soporte@mailinator.com  
Phone: (777) 777-7777 x1234



**kriko69** posted 5/17/21 6:20 PM

---- Registration Successful ---- Please activate your email by going to: [http://delivery.htb:8065/do\\_verify\\_email?token=4iaym3cxwpfk3y6a3aahj8b57bihocdmkqo9o67zubrtuzncs6zbcyf/daceprqji&email=7548135%40delivery.htb](http://delivery.htb:8065/do_verify_email?token=4iaym3cxwpfk3y6a3aahj8b57bihocdmkqo9o67zubrtuzncs6zbcyf/daceprqji&email=7548135%40delivery.htb) ) ----- You can sign in from: ----- Mattermost lets you share messages and files from your PC or phone, with instant search and archiving. For the best experience, download the apps for PC, Mac, iOS and Android from: <https://mattermost.com/download/#mattermostApps> (<https://mattermost.com/download/#mattermostApps>)

Así que para activar vamos a la ruta subrayada:

# Mattermost

All team communication in one place, searchable and accessible anywhere

✓ Email Verified

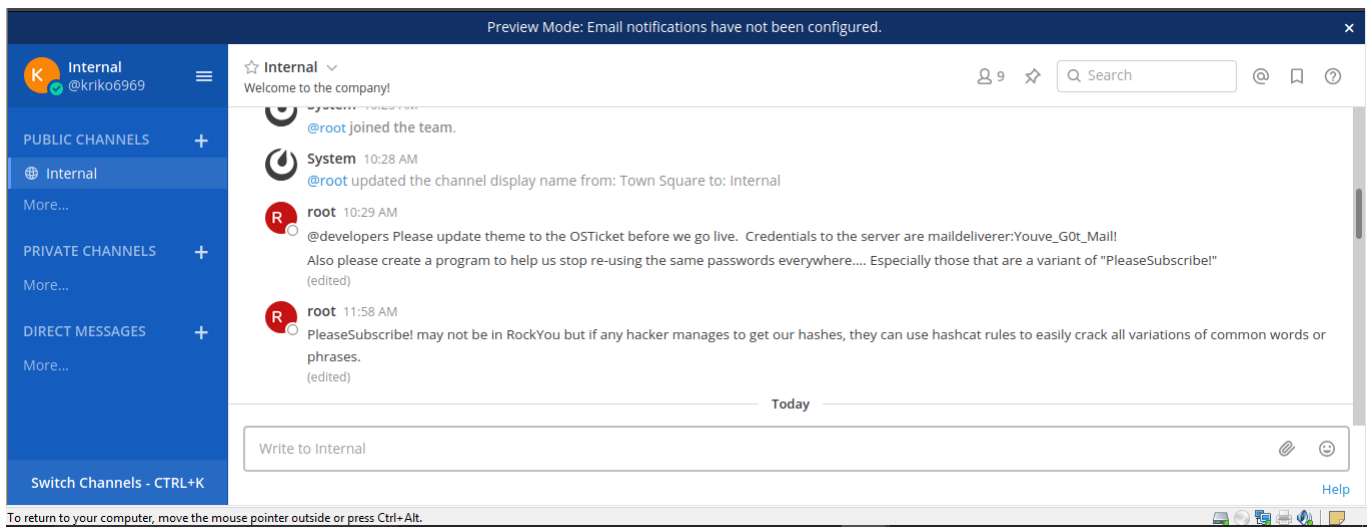
7548135@delivery.htb

Password

Sign in

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

Ahora ponemos la contraseña Kriko6969!:



Y estamos adentro.

## explotacion

Vemos unas credenciales en esa pagina:

- maildeliverer:Youve\_G0t\_Mail!

Y vemos una palabra clave entre comillas **"PleaseSubscribe!"** y nos indica que esa palabra no se encuentra en rockYou (me imagino que en diccionario) y que usan una variante de esa contraseña. Por lo que pienso que vamos a tener que crackear una contraseña mas adelante.

Recordemos que el puerto 22 ssh estaba abierto asi que veamos si podemos conectarnos:

```
(root@kali)-[/home/.../Escritorio/HTB/delivery/nmap]
# ssh maildeliverer@10.10.10.222
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: Mon May 17 18:22:47 2021 from 10.10.14.170
maildeliverer@Delivery:~$
```

Y estamos dentro, podemos ver la user.txt:

```
maildeliverer@Delivery:~$ whoami
maildeliverer
maildeliverer@Delivery:~$ ls
user.txt
maildeliverer@Delivery:~$ cat user.txt | head -c 10
d80c1cfea0maildeliverer@Delivery:~$
```

## elevacion de privilegios

Vamos a la ruta de /opt y ahi veremos que esta el servidor de mattermost y unos archivos de configuracion:

```
maildeliverer@Delivery:~$ cd /opt
maildeliverer@Delivery:/opt$ ls
mattermost
maildeliverer@Delivery:/opt$ cd mattermost/
maildeliverer@Delivery:/opt/mattermost$ ls
bin client config data ENTERPRISE-EDITION-LICENSE.txt fonts i18n logs manifest.txt NOTICE.txt plugins prepackaged_plugins README.md templates
maildeliverer@Delivery:/opt/mattermost$ cd config/
maildeliverer@Delivery:/opt/mattermost/config$ ls
cloud_defaults.json config.json README.md
maildeliverer@Delivery:/opt/mattermost/config$ cat config.json
```

Vamos a ver unas credenciales de base de datos mysql:

```
"SqlSettings": {
  "DriverName": "mysql",
  "DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:3306)/mattermost?charset=utf8mb4,utf8\u0026readTimeout=30s\u0026writeTimeout=30s",
  "DataSourceReplicas": [],
  "DataSourceSearchReplicas": [],
  "MaxIdleConns": 20,
  "ConnMaxLifetimeMilliseconds": 3600000,
  "MaxOpenConns": 300,
  "Trace": false,
  "AtRestEncryptKey": "n5uax3d4f919obtsp1pw1k5xetq1enez",
  "QueryTimeout": 30,
  "DisableDatabaseSearch": false
},
```

Intentemos conectarnos:

```
mysql -u mmuser -D mattermost -p

-D para especificar la database
```

contraseña: Crack\_The\_MM\_Admin\_PW

curiosa contraseña nos inidica de crackear la password del administrador...

Logramos ingresar a la DB, en mysql normalmente hay una tabla de "Users" que contiene entre muchas cosas el username y el password:

```
select username,password from Users;
```

Que vemos ahi? el hash del usuario root y de otros usuarios:

- usuario: root
- hash: 2a\$10VM6EeymRxJ29r8Wjkr8Dtev0O.1STWb4.4ScG.anuu7v0EFJwgjJO

Todo los indicios nos dicen que debemos crackear este hash. Primero veamos que tipo de hash es con hash-id herramienta de kali:

```
hashid
```

```
(pegamos hash)
```

```
# hashid
$2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0
Analyzing '$2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0'
[+] Blowfish(OpenBSD)
[+] Woltlab Burning Board 4.x
[+] bcrypt
```

Al parecer es bcrypt, vamos a utilizar hashcat para realizar el crackeo.

Primero vamos a buscar el modulo para realizar el ataque:

```
hashcat | more | grep bcrypt
```

```
more para verlo en formato more
```

```
grep bcrypt para ver que tipo de modulo usa
```

```
(root@kali)-[/home/kali]
# hashcat --help | more | grep bcrypt
3200 | bcrypt $2*$, Blowfish (Unix) | Operating System
```

Como ven si es bcrypt ya que hashcat indica que el formato es 2\*...

El modulo es el 3200. Vamos a hacer un ataque con diccionario pero si recuerdan se daba una pista que que la contraseña era una variacion de **PleaseSubscribe!** que no se halla en rockyou (un diccionario famoso en CTF)

Vamos a crear combinaciones de esta palabra para formar un diccionario. Hashcat tiene la opcion de reglas que a partir de una palabra o conjunto de palabras puede crear como un diccionario en base reglas de formacion de palabras.

Por ejemplo tu le puedes dar la palabra 'hola' y hashcat tiene ya reglas definidas (tambien se puede crear reglas) que realizan la transformacion de esta palabra:

```
Hola
```

```
h0la
```

```
h0l4
```

```
holA
```

...

Eso es lo que haremos, existe una regla en hashcat que se llama best64.rule ubicada en /usr/share/hashcat/rules/best64.rule esa usaremos contra la palabra clave que tenemos.

Primero vamos a crear un archivo con el contenido PleaseSubscribe! llamado pista:

```
echo PleaseSubscribe! > pista
```

Ahora vamos a crear un diccionario con la regla y esa palabra:

```
hashcat -r /usr/share/hashcat/rules/best64.rule --stdout pista > dict
```

Ya con nuestro diccionario creado vamos a intentar crackear nuestro hash:

```
echo $2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0 > hash
```

```
hashcat -a 0 -m 3200 hash dict
```

Vemos que encontró la contraseña, es **PleaseSubscribe!21**

```
(root@kali)-[/home/.../Escritorio/HTB/delivery/exploits] 11420
# hashcat -a 0 -m 3200 hash dict --show
$2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0:PleaseSubscribe!21
```

entonces si nos cambiamos al usuario root y ponemos esa clave ya somos root:

```
su root
```

```
PleaseSubscribe!21
```

```
root@Delivery:/home/maildeliverer# ls
lse.sh user.txt
root@Delivery:/home/maildeliverer# cd /root
root@Delivery:~# ls
mail.sh note.txt py-smtp.py root.txt
root@Delivery:~# cat root.txt
655f6378623fcd0db09c891b6ff0548e
root@Delivery:~#
```