

# Delivery walkthrough

## Index

Index .....	1
List of pictures .....	1
Disclaimer .....	2
Reconnaissance .....	2
Initial foothold .....	2
User flag.....	6
Privilege escalation .....	6

## List of pictures

Picture 1 - nMap scan results .....	2
Picture 2 - Web Application running on port 80.....	2
Picture 3 - Web application running on port 8065 .....	3
Picture 4 - Ticket opened .....	3
Picture 5 - Signed in Mattermost platform .....	4
Picture 6 - Confirmation email.....	4
Picture 7 - Logged in Mattermost platform .....	5
Picture 8 - Mattermost platform.....	5
Picture 9 - Useful information on Mattermost platform .....	5
Picture 10 - Chat with useful information on Mattermost platform .....	6
Picture 11 - SSH connection and user flag.....	6
Picture 12 - Database credentials in config.json file.....	7
Picture 13 - Connection to the database .....	7
Picture 14 - User credentials .....	7
Picture 15 - Hash cracked .....	8

## Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

## Reconnaissance

The results of an initial nMap scan are the following:

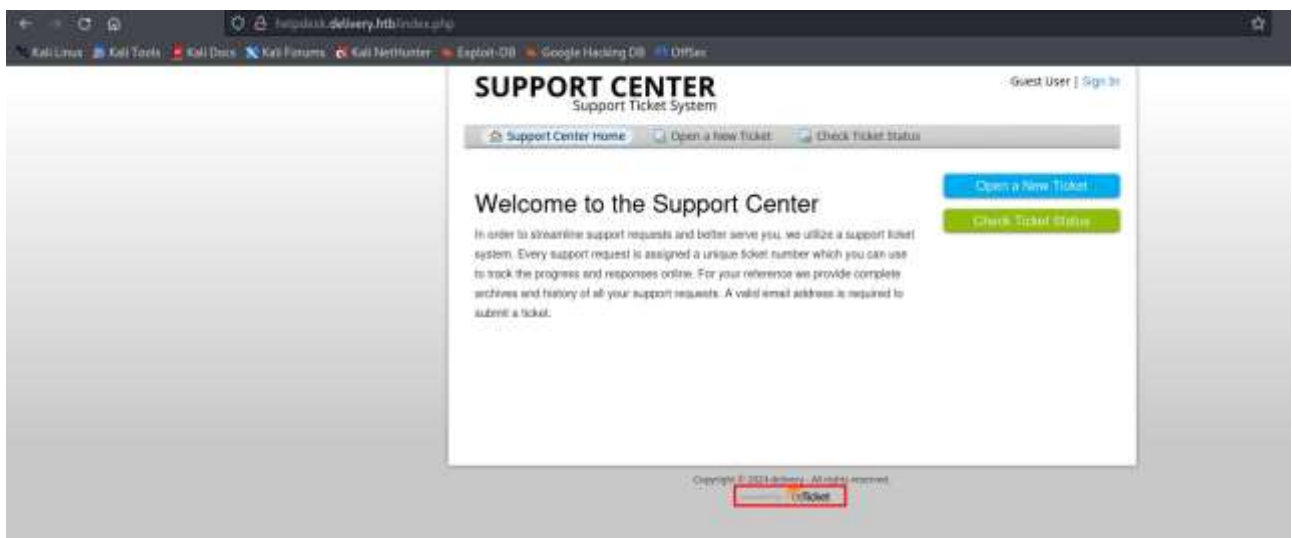


Picture 1 - nMap scan results

Open ports are 22, 80 and 8065. So, the machine has SSH enabled and an application running on port 80. NMap didn't recognize the service running on port 8065. Also, nMap recognized Linux operative system, but not a specific version.

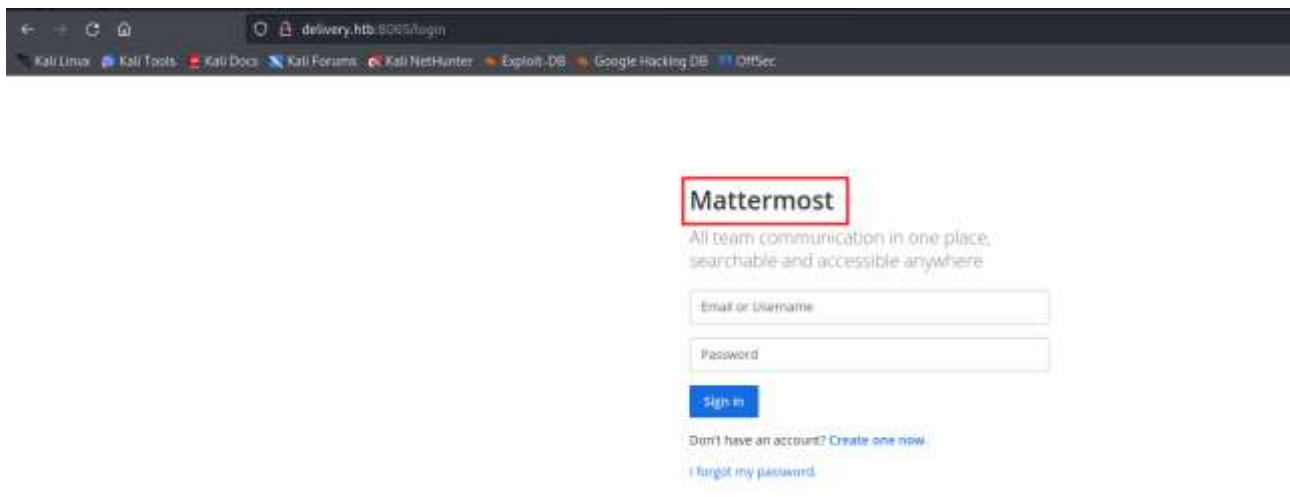
## Initial foothold

Web application running on port 80 is **OSTicket** and its index page is:



Picture 2 - Web Application running on port 80

Also, web application running on port 8065 is **Mattermost** and its index page is:



Picture 3 - Web application running on port 8065

On OSTicket application, I opened a new ticket using the following information:

A screenshot of the OSTicket 'Open a New Ticket' form. The page has a navigation bar with 'Support Center Home', 'Open a New Ticket', and 'Check Ticket Status'. The main heading is 'Open a New Ticket' with a subtext 'Please fill in the form below to open a new ticket.' The form is divided into three sections: 'Contact Information' with fields for 'Email Address \*' (prova@prova.it), 'Full Name \*' (provolone), and 'Phone Number' (1111111) with an 'Ext: 61' field; 'Help Topic' with a dropdown menu set to 'Contact Us'; and 'Ticket Details' with a subtext 'Please Describe Your Issue' and an 'Issue Summary \*' field containing the text 'new'. At the bottom is a rich text editor with a toolbar and the text 'neeeeeeeeeew'.

Picture 4 - Ticket opened

When the ticket is opened, I obtained a **ticket ID** and an email to use to add information to the ticket (based on the pattern <ticketID>@delivery.htb). These information are very useful, so I needed to noted them. At this point, I browsed on **Mattermost** platform and I signed in using the following information:

# 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?

Valid email required for sign-up

Choose your username

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

Choose your password

Create Account

Picture 5 - Signed in Mattermost platform

So, I used as email the mail useful to add information to the ticket I previously opened on **OSTicket** platform. In this way I can receive the confirmation email and completed the registration process on **Mattermost** platform:

Basic Ticket Information		User Information	
Ticket Status:	Open	Name:	Provolone
Department:	Support	Email:	prova@prova.it
Create Date:	1/26/24 5:12 AM	Phone:	111-1111 x61

Avatar

provolone posted 1/26/24 5:12 AM

---- Registration Successful ---- Please activate your email by going to: [http://delivery.htb:8065/do\\_verify\\_email?token=ec6ancmndjimisy98174e4otrufpwebwbikys6gkq7q7x81rcr8t78jbnbp5f4eb&email=5030451%40delivery.htb](http://delivery.htb:8065/do_verify_email?token=ec6ancmndjimisy98174e4otrufpwebwbikys6gkq7q7x81rcr8t78jbnbp5f4eb&email=5030451%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>

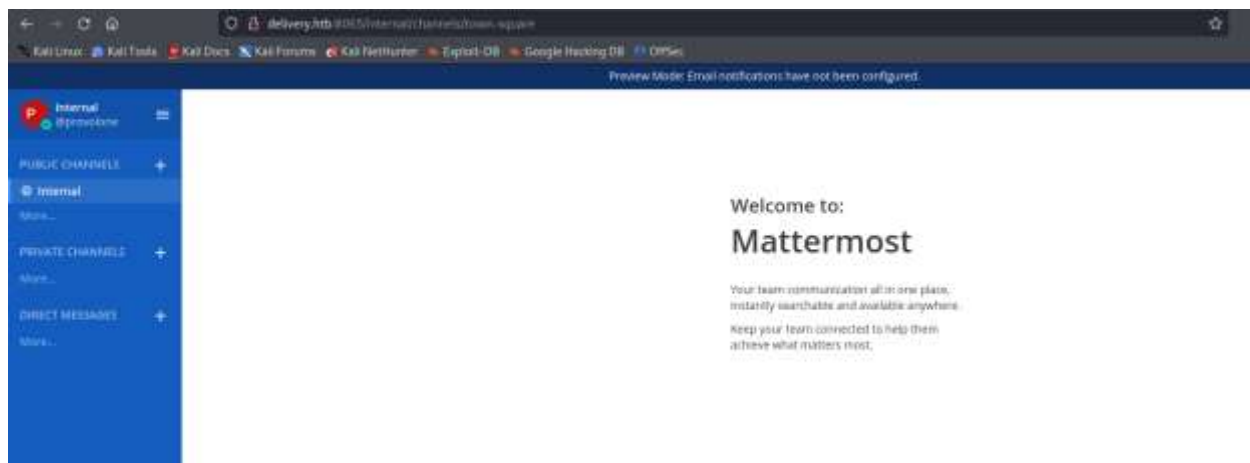
Picture 6 - Confirmation email

I accessed to the **Mattermost** platform with credentials chosen during the sign in process. The first page I met after login on **Mattermost** platform is the following:



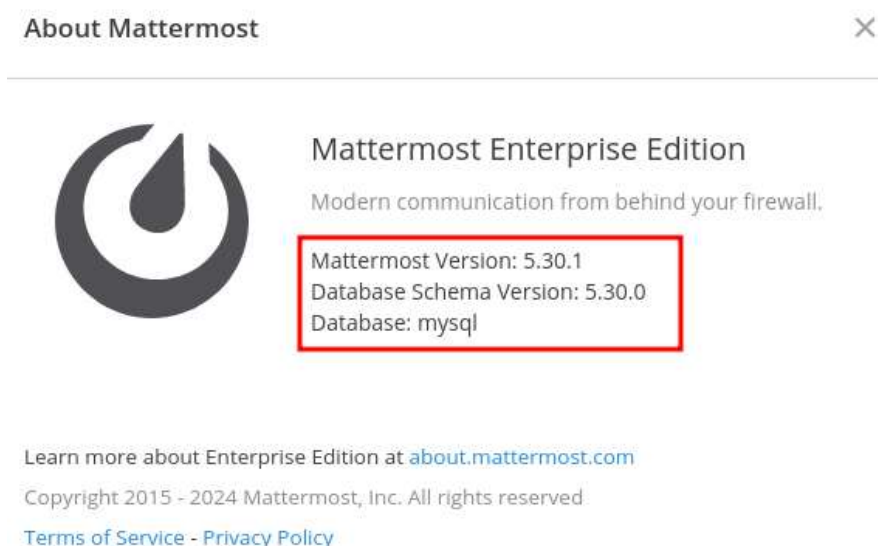
Picture 7 - Logged in Mattermost platform

Here, the only thing I was able to do was to choose the internal team to join in it. After this operation, I saw the following web page:



Picture 8 - Mattermost platform

I was able to find other interesting details on this platform as:



Picture 9 - Useful information on Mattermost platform

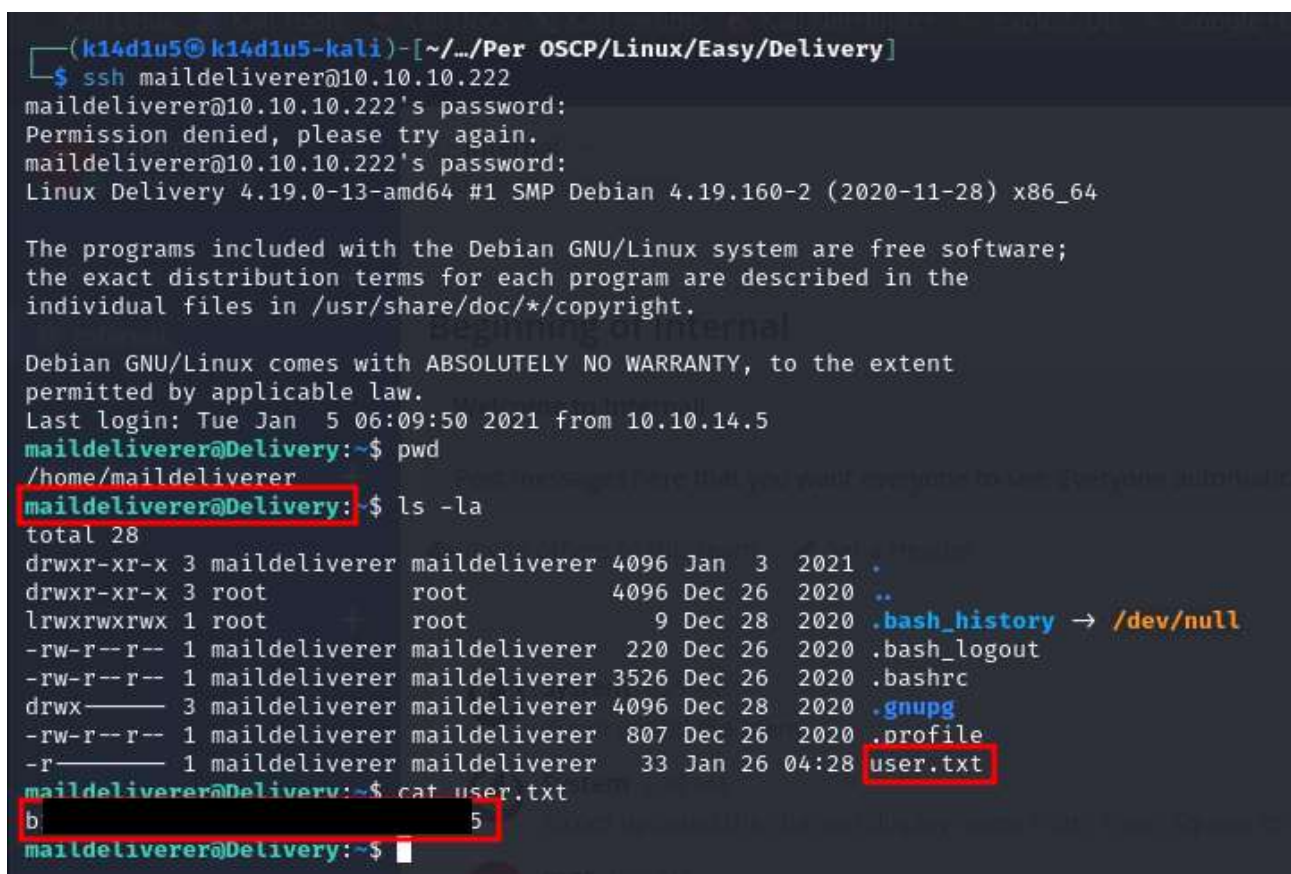
## User flag

I gave a fast glance to the tutorial and completed it I found this very interesting page:



Picture 10 - Chat with useful information on Mattermost platform

In this chat there are two possible passwords and one possible username. I tried these credentials to log in the machine via SSH and I got a user shell. In this shell, I was able to retrieve the user flag, as shown in the following picture:



Picture 11 - SSH connection and user flag

## Privilege escalation

To escalate my privileges, I uploaded linpeas.sh script on the target machine and I run it. In this way, I found a very interesting path: **/opt/mattermost/config**. Searching on the Internet the Mattermost documentation



(<https://docs.mattermost.com/configure/configuration-settings.html>), I found out that, in this path, **config.json** file contains database credentials, among other configurations:

```
{
  "SqlSettings": {
    "DriverName": "mysql",
    "DataSource": "tcp(127.0.0.1:3306)/mattermost?charset=utf8mb4,utf8\u0026readTimeout=30s\u0026writeTimeout=30s",
    "DataSourceReplicas": [],
    "DataSourceSearchReplicas": [],
    "MaxIdleConns": 10,
    "ConnMaxLifetimeMilliseconds": 3600000,
    "MaxOpenConns": 100,
    "Trace": false,
    "AtRestEncryptKey": "n5uax3d4f9100btsp1w1k5xtq1a0er",
    "QueryTimeout": 10,
    "DisableDatabaseSearch": false
  }
}
```

Picture 12 - Database credentials in config.json file

At this point, I connected to the database, as showed in the following picture:

```
}maildeliverer@Delivery:/opt/mattermost/config$ mysql -u mmuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 225
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)]> 
```

Picture 13 - Connection to the database

I was able to retrieve user credentials from the database:

```
10 rows in set (0.001 sec)

MariaDB [mattermost]> SELECT Username,Password FROM Users;
+-----+-----+
| Username | Password |
+-----+-----+
| surveybot | $2a$10$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvpiLaS7ImuiItEiK |
| c3ecacacc7b94f909d04dbfd308a9b93 | $2a$10$3m0quguvCF87/R1qEcCOWQ6tEi6EtgtRn8fRAYQYmaKmg_HDGnS/G |
| 5b785171bf34762a933e127630c4860 | $2a$10$3m0quguvCF87/R1qEcCOWQ6tEi6EtgtRn8fRAYQYmaKmg_HDGnS/G |
| root | $2a$10$RnJ5I5TLc9W3i0cUgg1iK0G9vqABED24CQcQ8zvUm1Ir9px5.Pduq |
| ff0a21fc6fc2408195e16ea054c963ee | $2a$10$RnJ5I5TLc9W3i0cUgg1iK0G9vqABED24CQcQ8zvUm1Ir9px5.Pduq |
| provolone | $2a$10$14EvxKiD72qMxudwxWygme1j5hVFS.sU2yDokEWC1hm5m4R2Detyu |
| channelexport | $2a$10$14EvxKiD72qMxudwxWygme1j5hVFS.sU2yDokEWC1hm5m4R2Detyu |
| 9ecfb4be145d47fda0724f697f35ffaf | $2a$10$s.cLPSjAVgawG0JwB7vrqenPg2lrDt0ECRTjwWah0zHfq1CoFyFqm |
| claudio | $2a$10$5spQcU.UD61v.UQ27woiMOXAlpGU9qYkMuF1D5rjMHrsiHaRxXopm |
| claudio90 | $2a$10$bW3soducj.y0yu5wKfzT0.JfLxYMB4q0Ut96djIGu08b0k.bbisJC |
+-----+-----+

10 rows in set (0.001 sec)
```

Picture 14 - User credentials

Now, I tried to crack this hash. I remembered that in the **Mattermost** chat there were two possible passwords and about the one I didn't use yet the message said to not use similar password to that one. So, I created a mangles password list based on that one with the following command and used **JohnTheRipper** to crack the has:

```

(k14d1u5@k14d1u5-kali)~[~/Per_OSCP/Linux/Easy/Delivery]
$ cat pass.txt | rsmangler -m 16 -x 20 --file - > mangled.txt

(k14d1u5@k14d1u5-kali)~[~/Per_OSCP/Linux/Easy/Delivery]
$ mousepad mangled.txt

(k14d1u5@k14d1u5-kali)~[~/Per_OSCP/Linux/Easy/Delivery]
$ john --wordlist=mangled.txt --format=bcrypt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
p 1 (?)
lg 0:00:00:03 DONE (2024-01-26 23:23) 0.2724g/s 48.22p/s 48.22c/s 48.22C/s PleaseSubscribe!20..PleaseSubscribe!21
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Picture 15 - Hash cracked

So, I used this credential to login in the machine via SSH and retrieved the root flag (sorry, I forgot to take this screenshot).