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

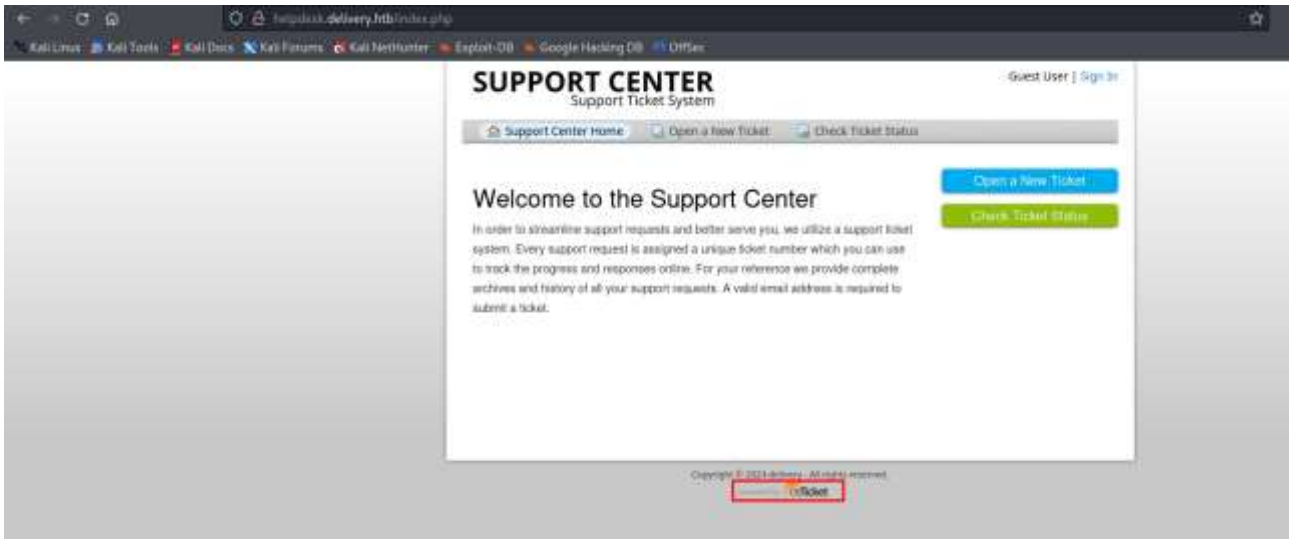
The results of an initial nMap scan are the following:

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.

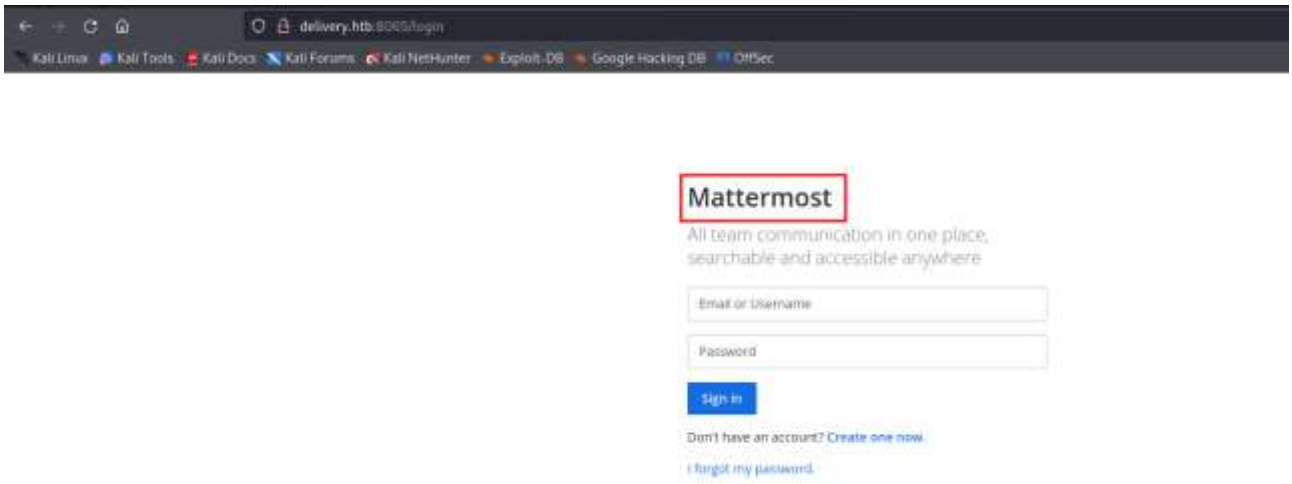
Initial foothold

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



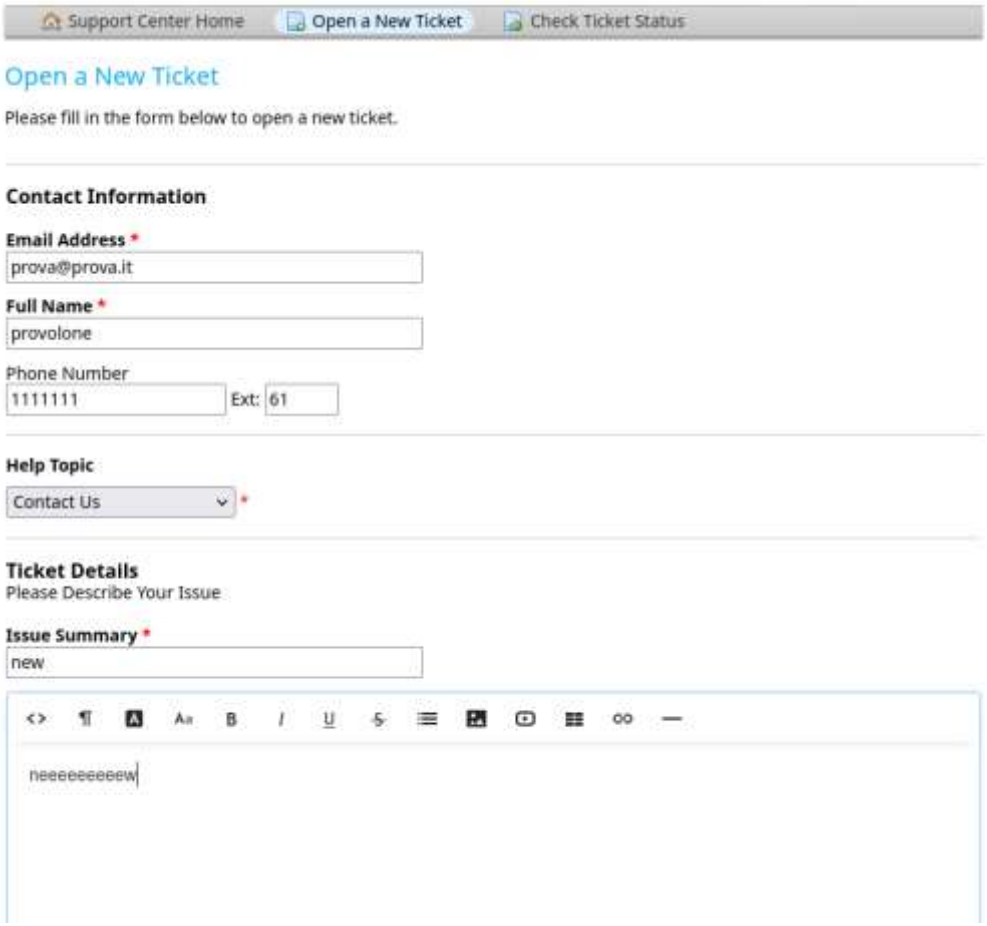
Picture 2 - Web Application running on port 80

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



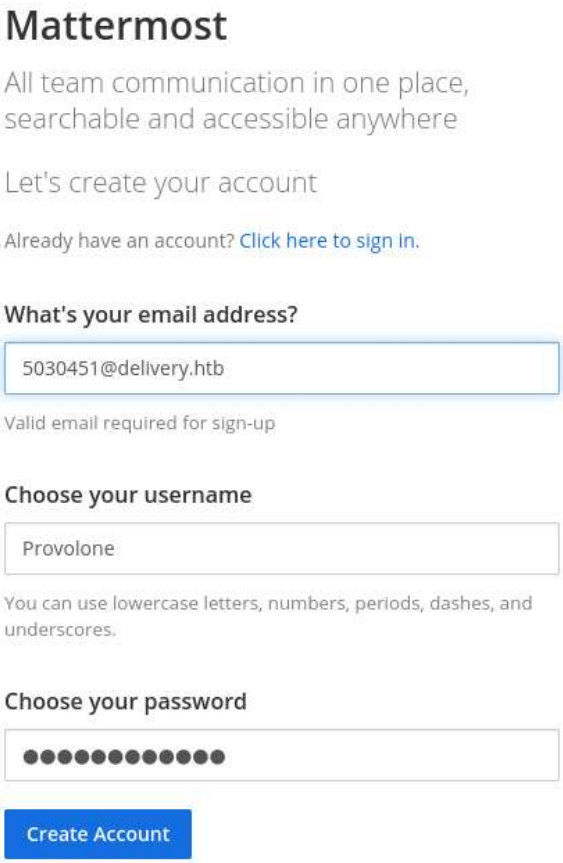
Picture 3 - Web application running on port 8065

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



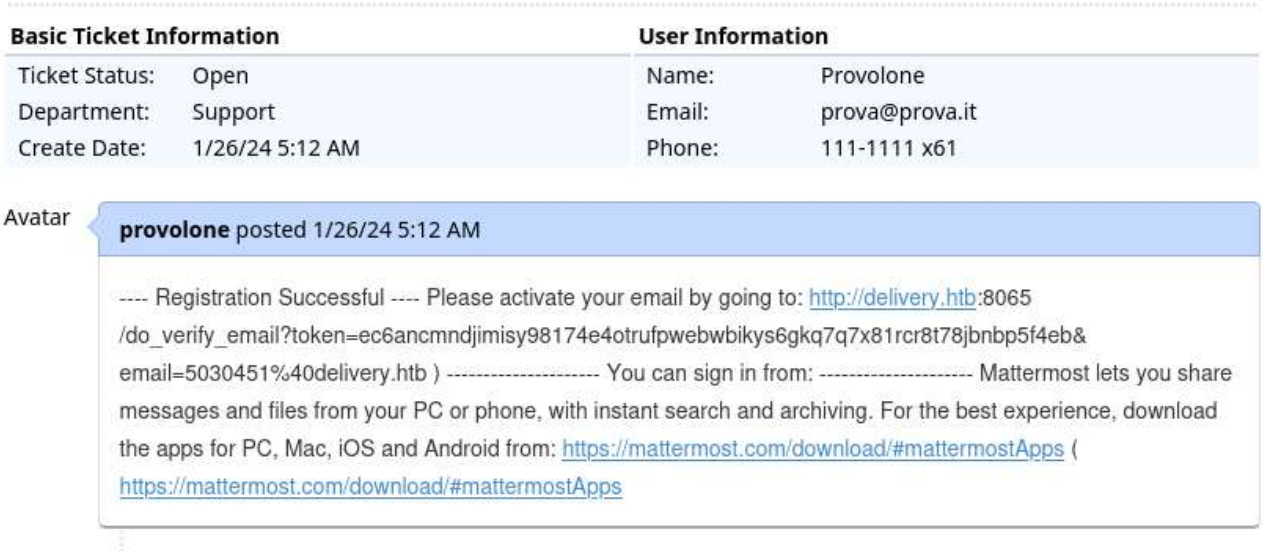
Picture 4 - Ticket opened

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:



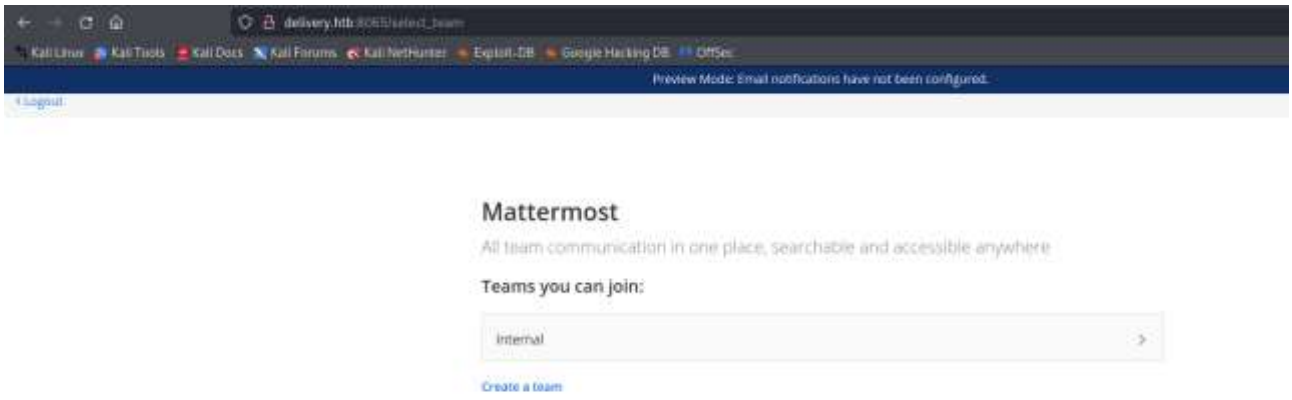
Picture 5 - Signed in Mattermost platform

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:



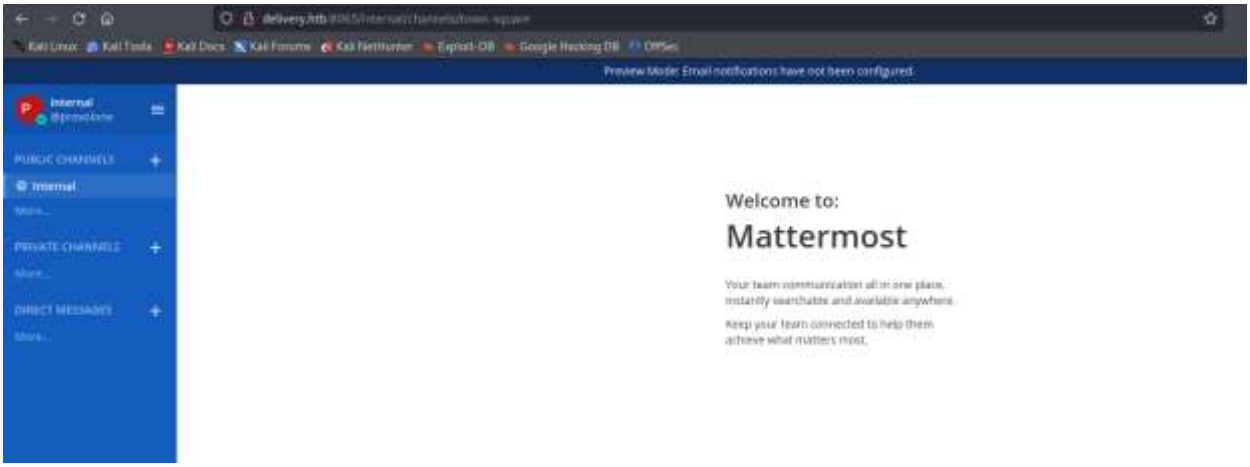
Picture 6 - Confirmation email

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:



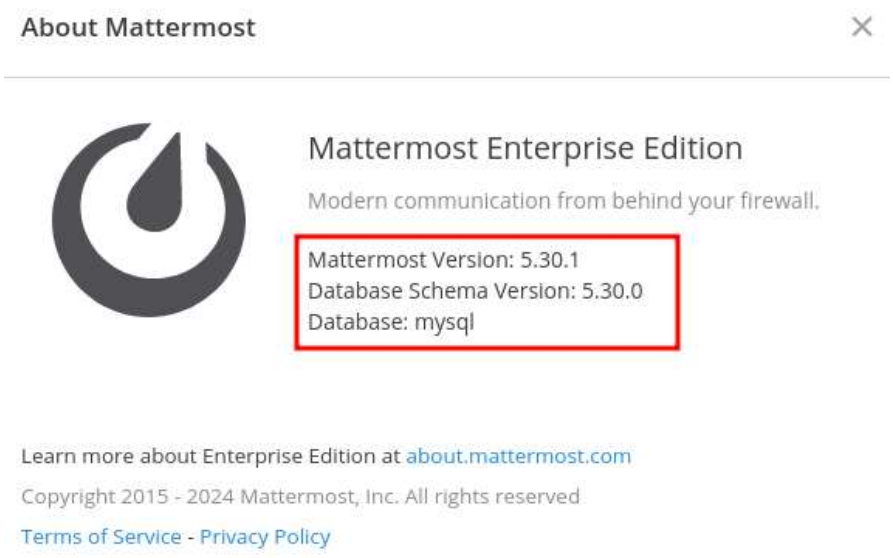
Picture 7 - Logged in Mattermost platform

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:



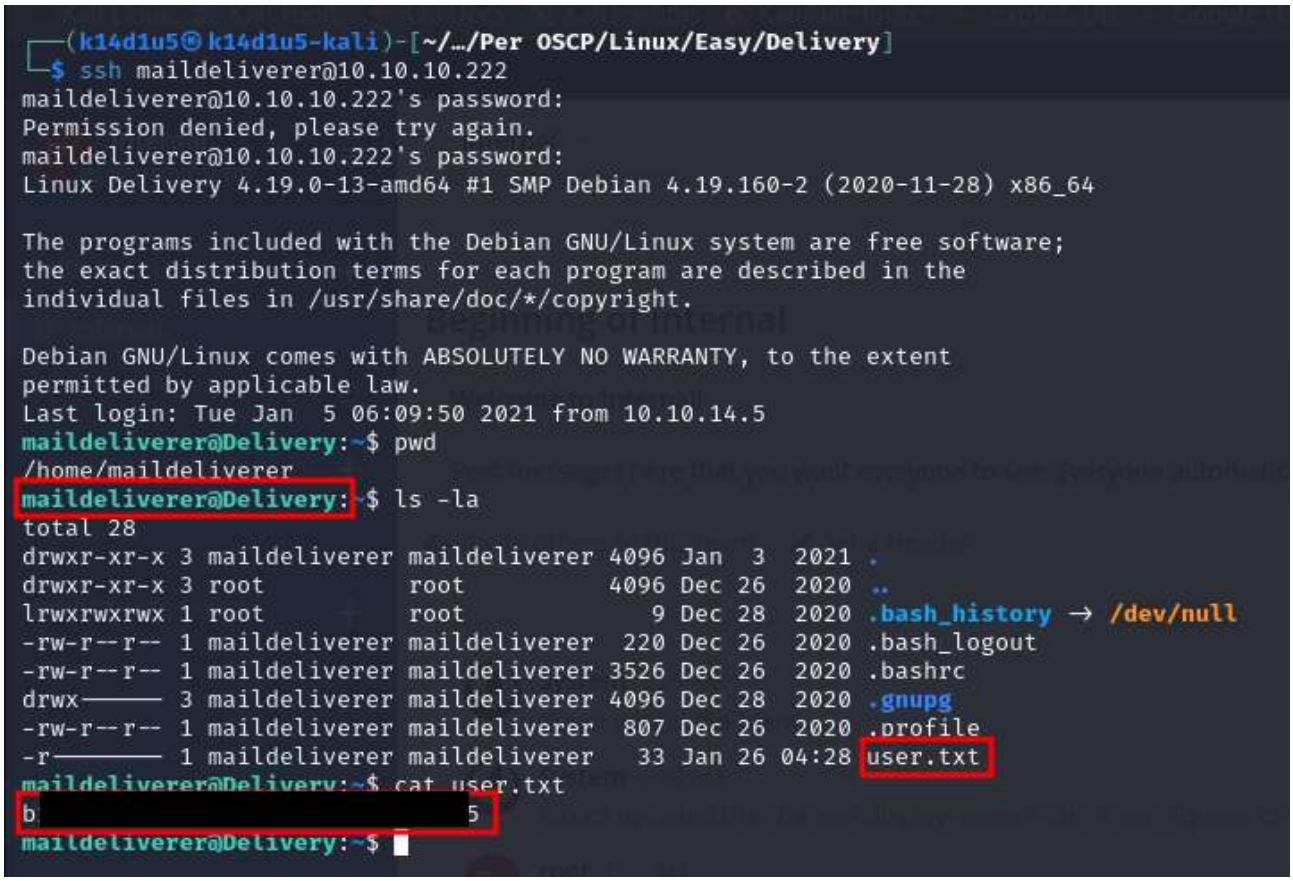
Picture 9 - Useful information on Mattermost platform

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

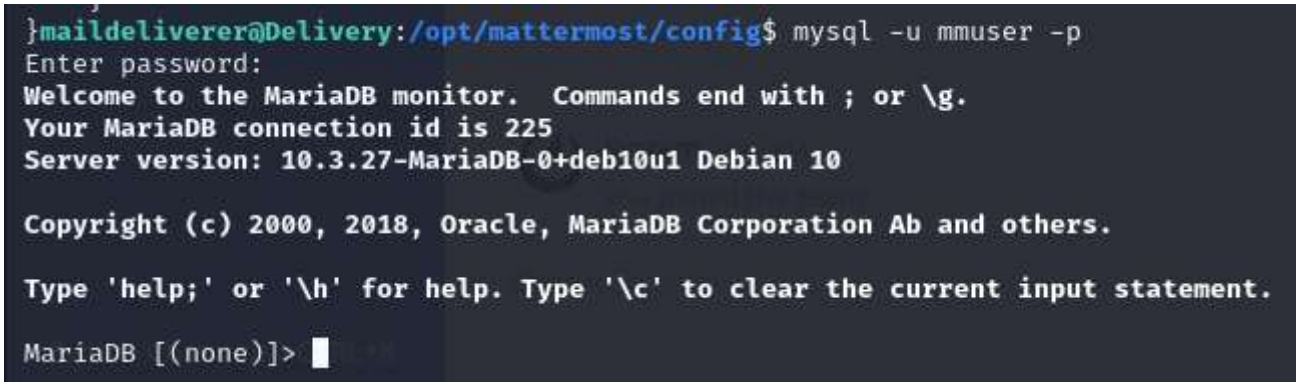
Privilege escalation

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:

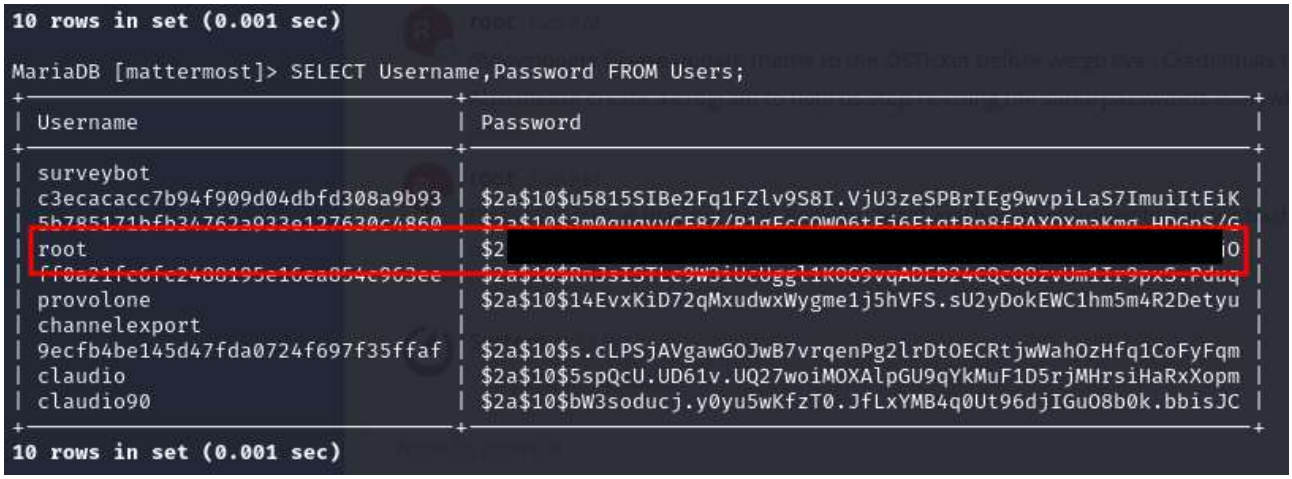
Picture 12 - Database credentials in config.json file

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



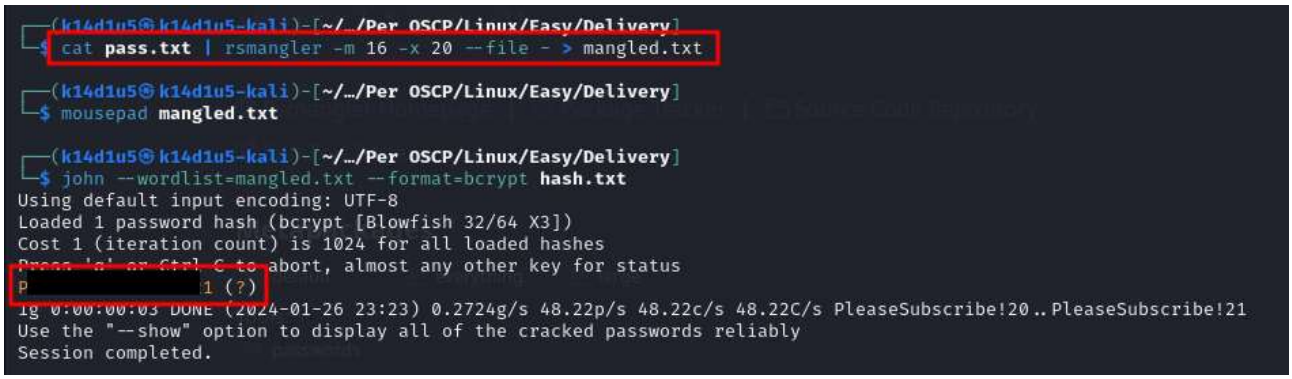
Picture 13 - Connection to the database

I was able to retrieve user credentials from the database:



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:



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).