

Delivery – 10.10.10.222

USER Walkthrough

This is my first ever writeup/walkthrough and we will be doing Delivery on hackthebox.eu.

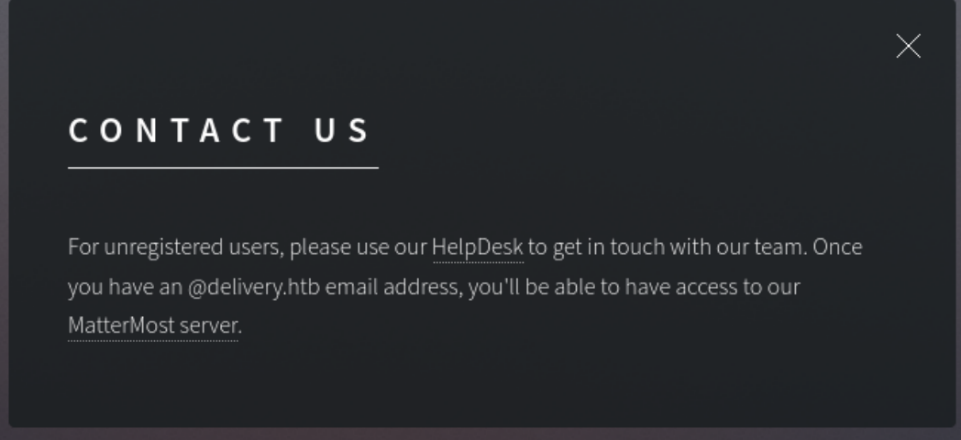
Generally, my first play is to always start with a nmap scan, and I check if there is a website running and use gobuster to search for directories.

Start by scanning the site with **nmap -sV -sC -O -p- 10.10.10.222**

In the meantime, I will also use gobuster to search for the directories on the website.

**gobuster dir -e -u 10.10.10.222 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt**

While those are running, let’s not waste any time and take a look around on the website   
A few things to take note of:

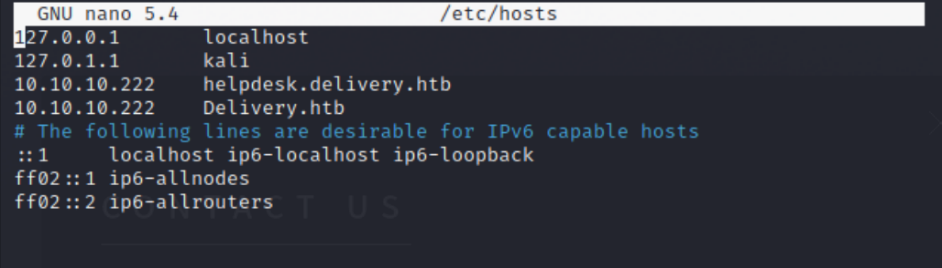
* When you click on the helpdesk link it does not seem to work.
* When looking through the contact us link it gives you specific instruction

These two links don’t work however they lead you to two sites called:

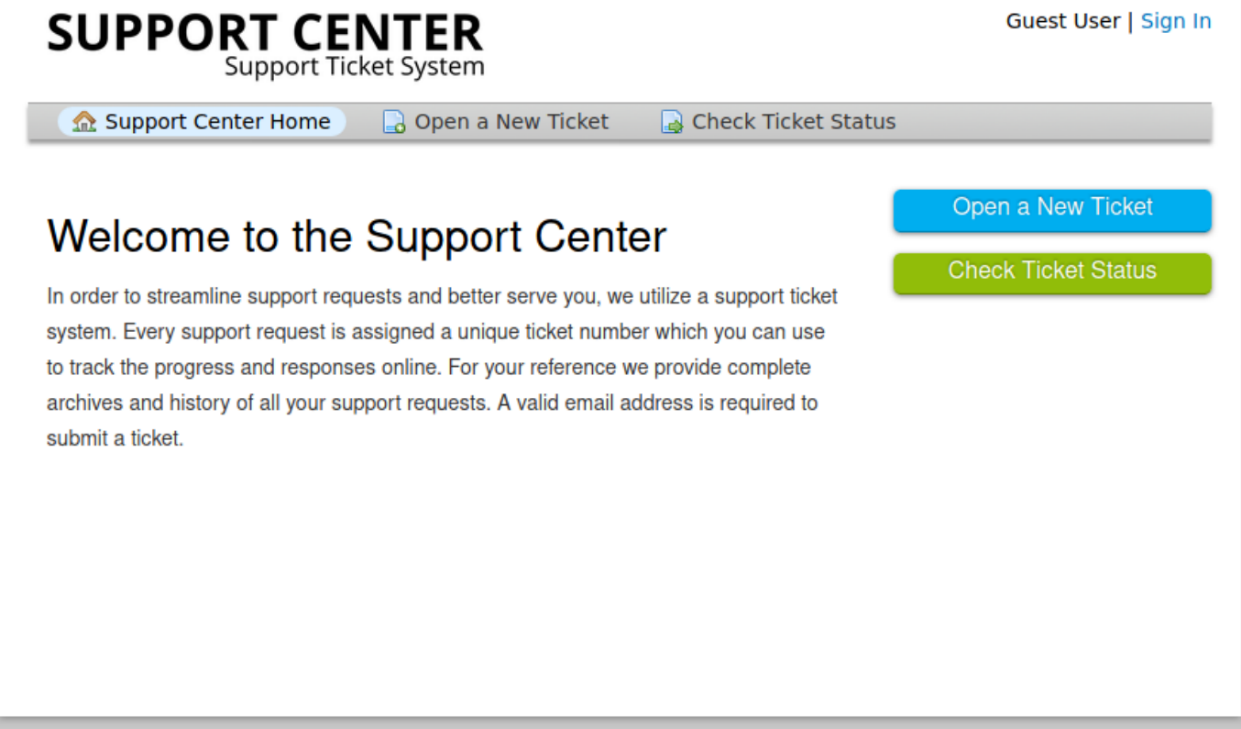
Delivery.htb:8065

Helpdesk.delivery.htb

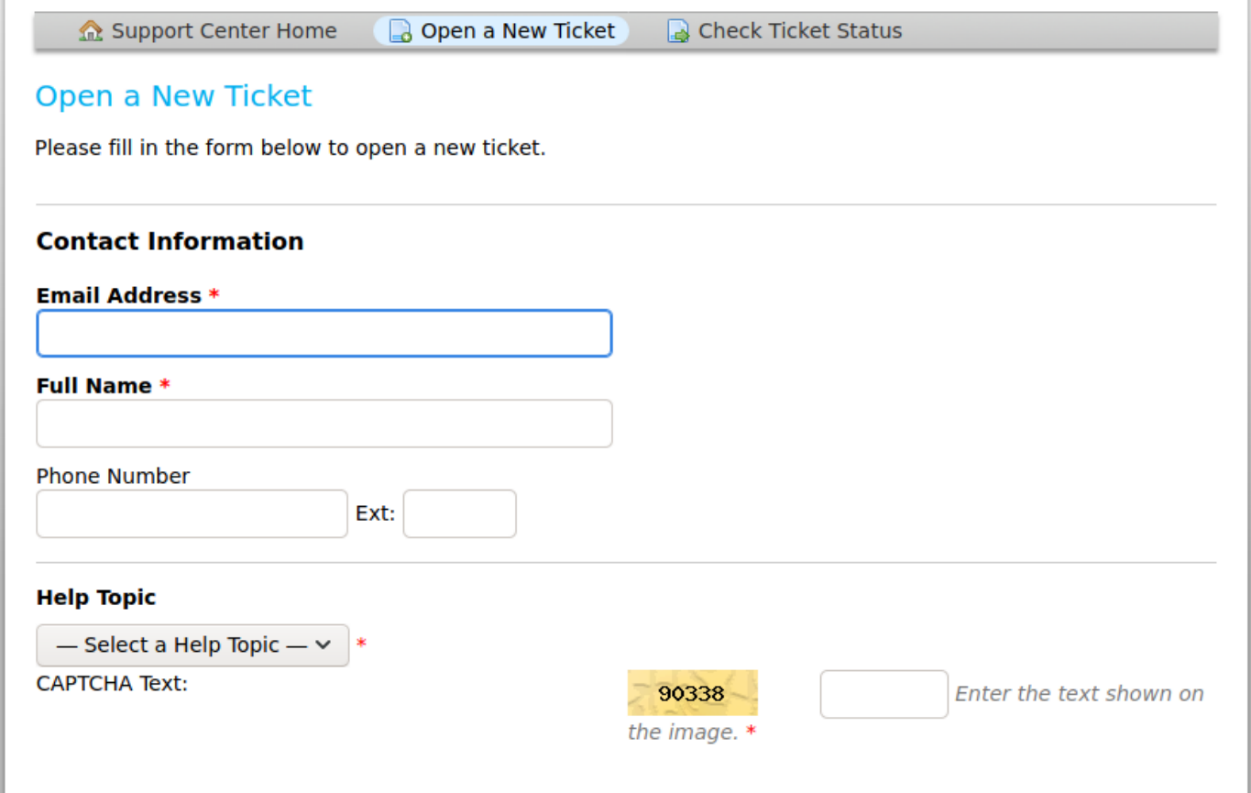
What we must do is add these to /etc/hosts file, so it knows that those domains are associated with that particular IP address.



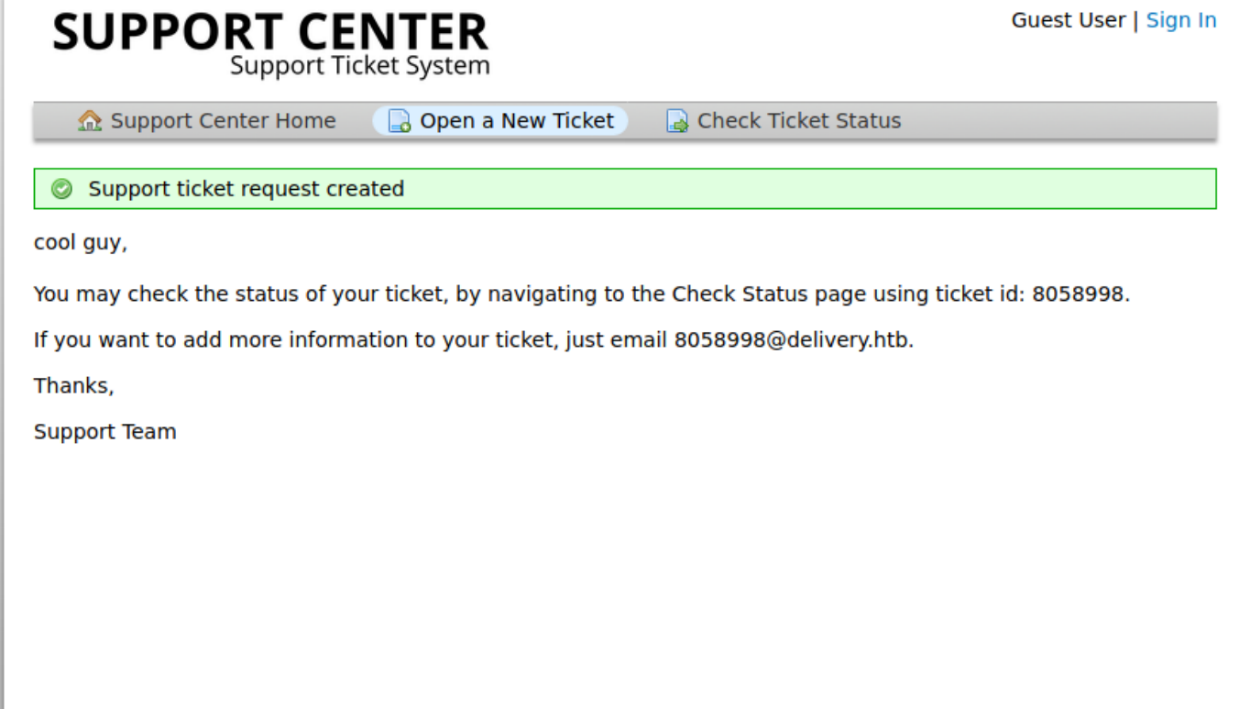
From the “CONTACT US” page earlier we learned that we need to get in touch with the helpdesk team to get a @deliver.htb email. Then we can use the Mattermost server.  
So with that information we are going to see what we can do on the helpdesk site.



We only two options, so we are going to start by opening a new ticket.



You are going to fill out this form and It’s important to keep note of the email for this account we may need to use it later. After you fill out the information and submit it you should get a “Support ticket request created” page.



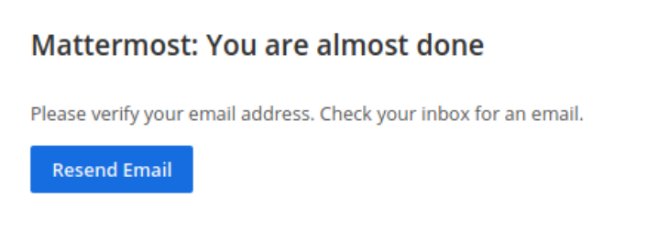
There are a few things we must take note of. First, we must take note of our ticket id. Also, if you recall back to the contact us page earlier you notice how it says we need @delivery.htb email to access Mattermost. Well because the helpdesk support ticket system provides us one, we can now try to sign up for matter most and see where it takes us. Also, this request created page gives us a hint on what we need to do. As you can the last line says "If you want to add more information to your ticket, just email 8058998@delivery.htb"

Once we get back to Mattermost we can first start off by doing the standard admin/admin username and password and looking up the default credentials but ultimately, we are going to end up creating a new account.   
  
Since we now have a @delivery.htb email we can use it fill out the information to make an account.

The account credentials I used to make an account were:

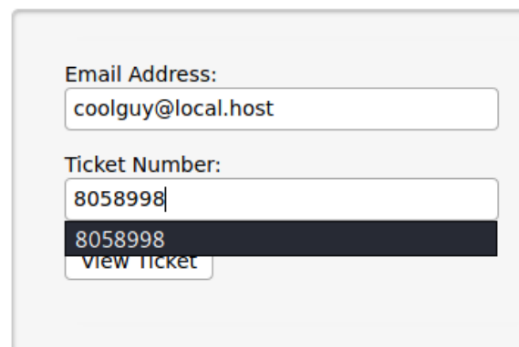
2496731@delivery.htb.  
Coolguy123:Delivery123!

This is the response we get once we complete out account creation on Mattermost

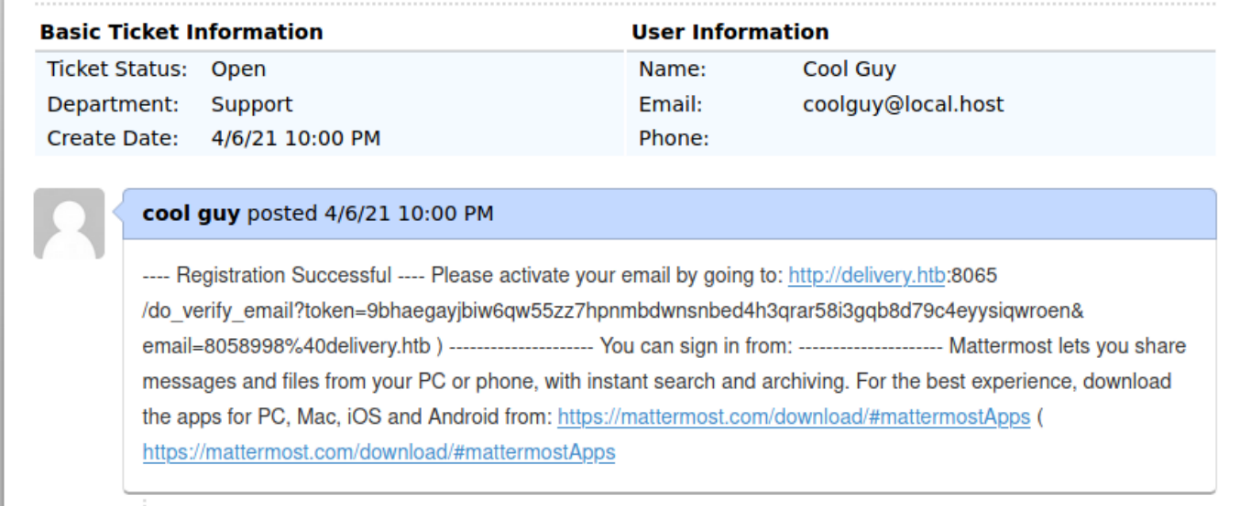


If you recall from earlier, we know that if we **Wanted to add more to our support ticket we just email 2496731@delivery.htb**. Since we used 2496731@delivery.htb. as the email address for the Mattermost that means the verification would technically be sent to the helpdesk ticket we created earlier. Using this we will be able to get access to Mattermost.

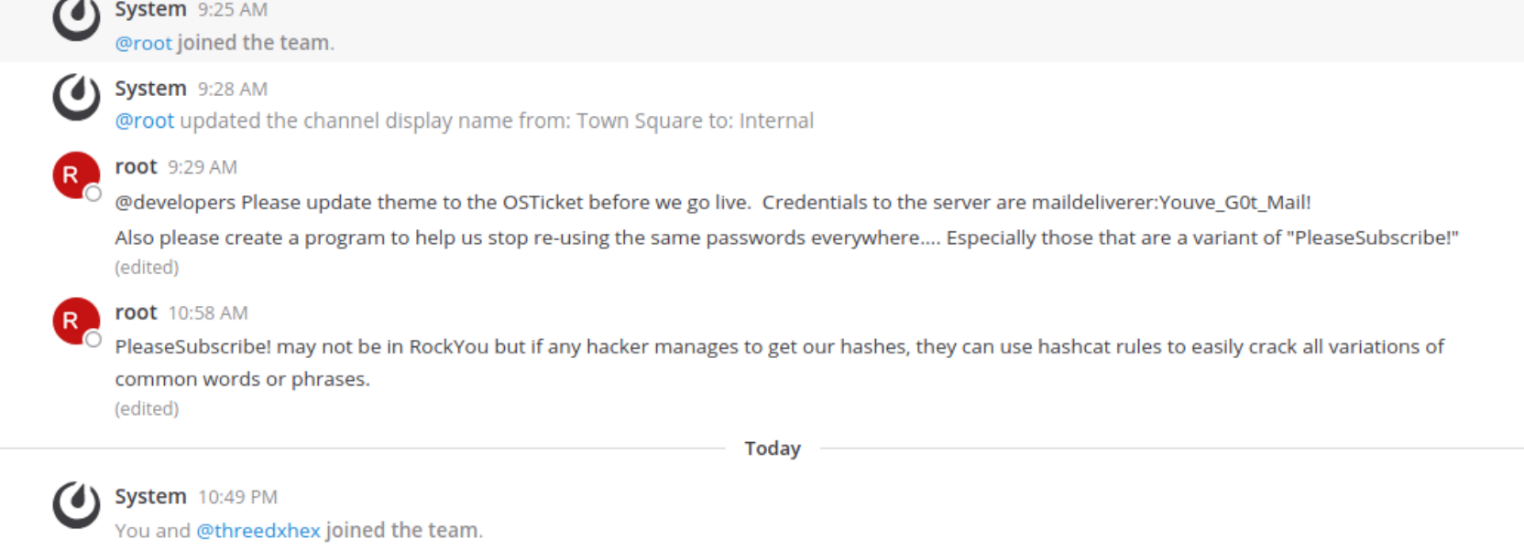
We now go back to the helpdesk site and we go to view the status of our ticker. We then want to **Use the email you created associated with the helpdesk site used to create the ticket and the ticket number to view our ticket. Just for clarification think of the email we created earlier as an account for only helpdesk and the 2496731@delivery.htb email used to create a Mattermost account only used to login to Mattermost.**



After signing in you should see this.

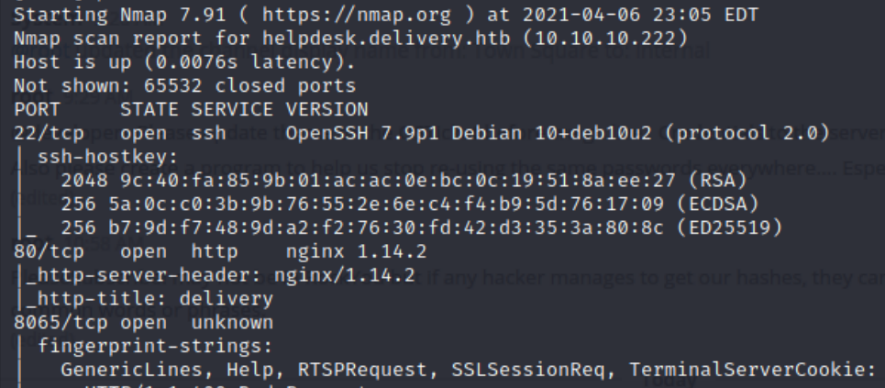


All we want to do from here is copy and paste the link in-order to verify our account with Mattermost and then we would use the credentials from earlier to login.

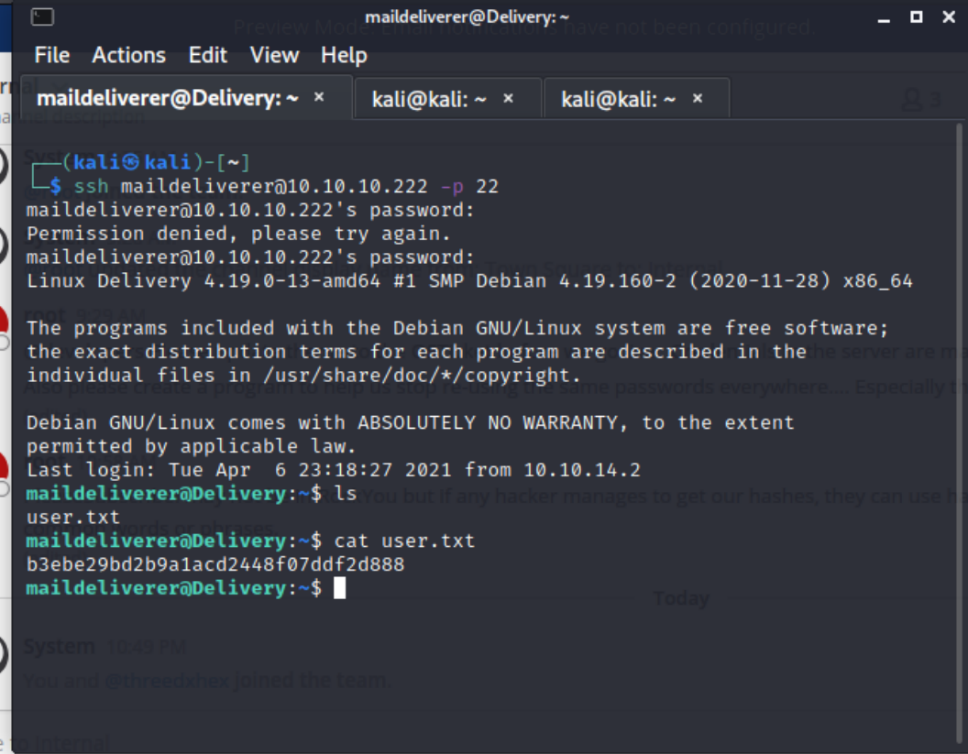


This is what should be displayed when you login. We want to take note of some of the messages and save them for later.   
  
We first find credentials for the server using **maildeliverer:Youve\_G0t\_Mail!**  
We also where able to find that they reuse the same passwords using a variant of "PleaseSubscribe!". There is also a hint displaying say that this password can be cracked using rules.

If we check the results from our scan earlier, we can see that ssh is open on port 22 so let’s try to login with the credentials we found.

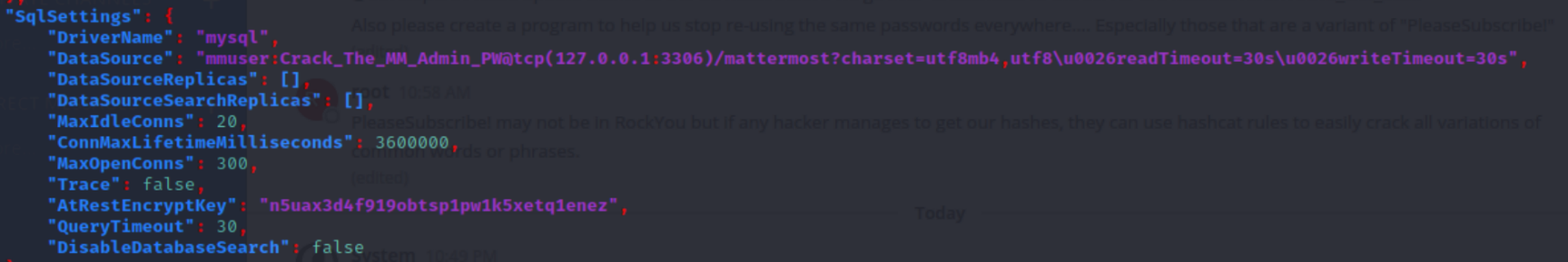


Once we are signed in, we can do a simple ls command and we can see the user flag right when we log in.



**ROOT walkthrough**  
  
Now that we have access to the system we want to do some looking around and see if we can find anything that may be useful.   
  
When running systemctl status I was able to notice -mariadb which means that there is a SQL database running on this machine. When trying to run it we get a permission denied so let’s take a look around and see if we can find anything in the Mattermost directory assuming its using SQL to store data.

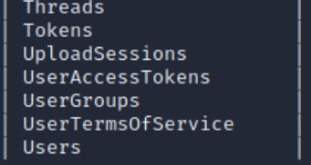
If we go to /opt/Mattermost/ we can find a config directory and in there we find config.json. The full path would be /opt/mettermost/config/config.json and let’s use nano to take a look at it.   
As we keep scrolling, we can see there is a "SQLSettings" section of code that has the username and password in plaintext in Data Source section.



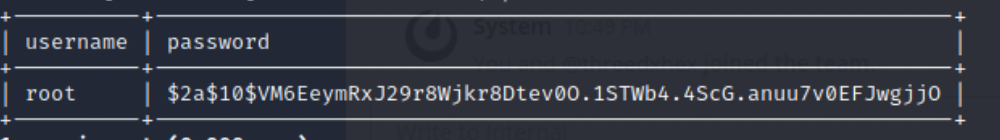
Now we can try to login to SQL specifying the username and password.  
the credentials are mmuser:Crack\_The\_MM\_Admin\_PW

mysql -u mmuser -D mattermost -p   
----------------------------------------------------------  
password: Crack\_The\_MM\_Admin\_PW  
  
Once we are logged into the SQL database the first thing we can do is show all the tables so we can get the names of them.   
  
**show tables;**

When we look at all the tables we can see there is a “Users” table. That is something we should investigate.



From here you can do a SELECT \* from USERS; statement and this will show everything from the USERS table (It's about to get messy). If we look at the table, the first things we should look at are Username and Password fields. When glancing through the table we can see there is a user called 'root'. So, this means we want to create a statement to only show the user root and its password.   
  
The statement I used was **SELECT username, password FROM Users WHERE username ='root';**



This is the hash of the password for root. If we recall we know that from the Mattermost chat, we learned that "PleaseSubscribe!" variant is used for a lot of passwords. It was also implied that rule-based password crack might be able to crack the hash. Moving forward we will try to use a rule-based hashcat to crack the hash.

I went on google and searched best rule based hashcat lists. I ended up using the d3adhob0.rule. Next, we want to take the time to figure out what type of hash this so we can specify what kind of hash this is.

<https://www.tunnelsup.com/hash-analyzer/>

This website worked the best for me. Since the results came by as bcrypt we now must craft out hashcat command to try and break the hash.

Hashcat has a lot of arguments and options so for reference it’s always good to look at the documentation to guide you.

<https://hashcat.net/wiki/doku.php?id=hashcat>

The syntax of the command I used is:

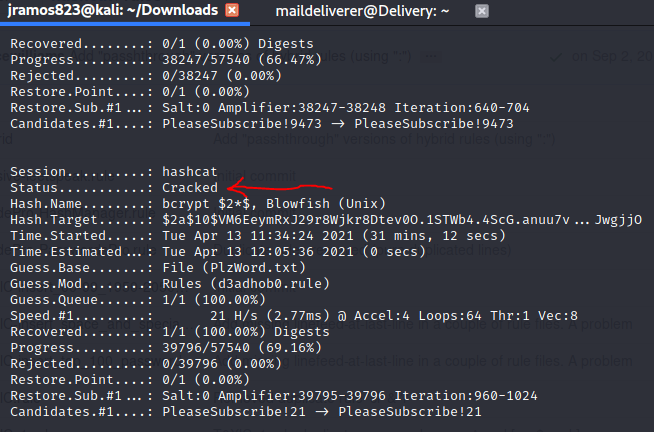


^ ^ ^ ^

Type of Attack Hash Wordlist   
encryption Mode To crack in this case

its only

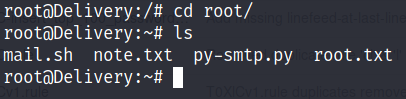
"PleaseSubscribe!”

As for the other two arguments -r stands for the rule list we will be using.

Along with our wordlist and -o outputs the results to a file to a file called "bam.txt"

Once we get back the result, we can try to login to root and….



Bingo!