**HACK THE BOX MACHINE NAME: DELIVERY**

**IP of the machine: 10.10.10.222**

**Reconnaissance**

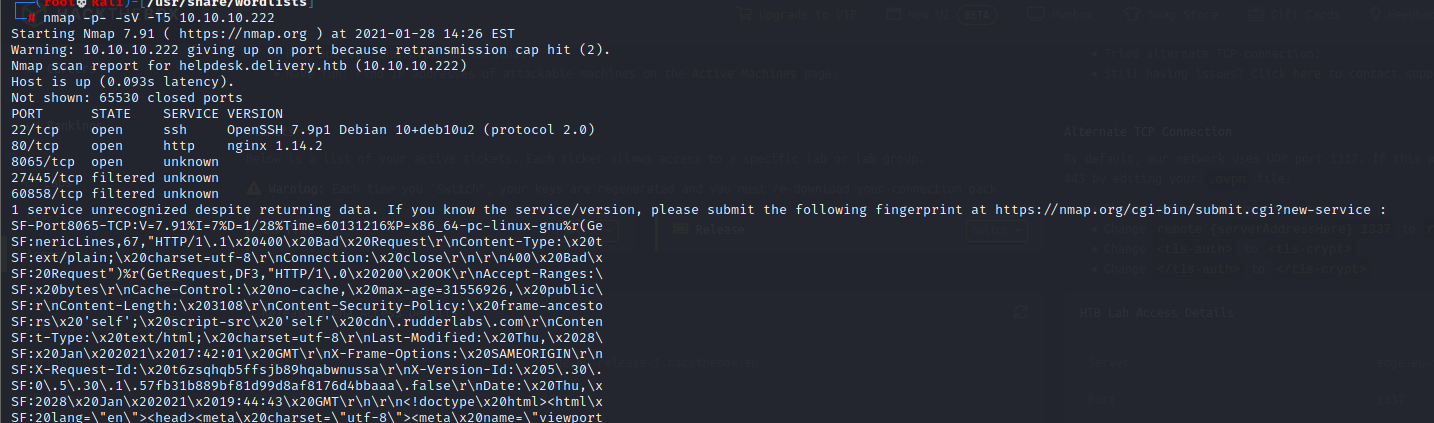
1) Connect to the VPN using HTB lab access details

2) Activate the VPN using the command like eg <<openvpn bnm.ovpn>>

3) ifconfig to check whether there are VPN interfaces like tun0/tun1 is added

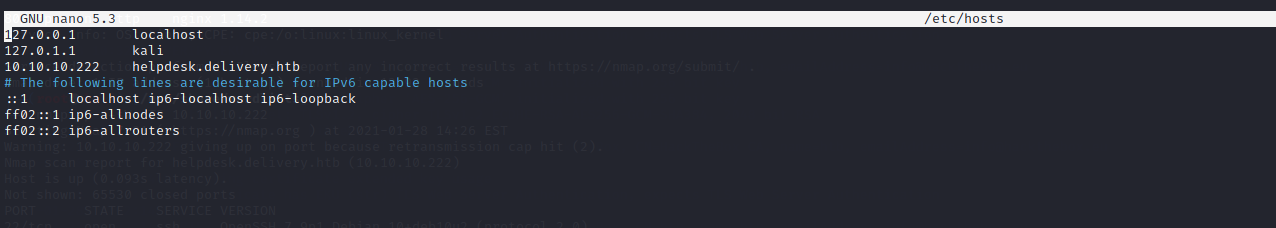
4) Ping the respective system to hack and ensure that it is working

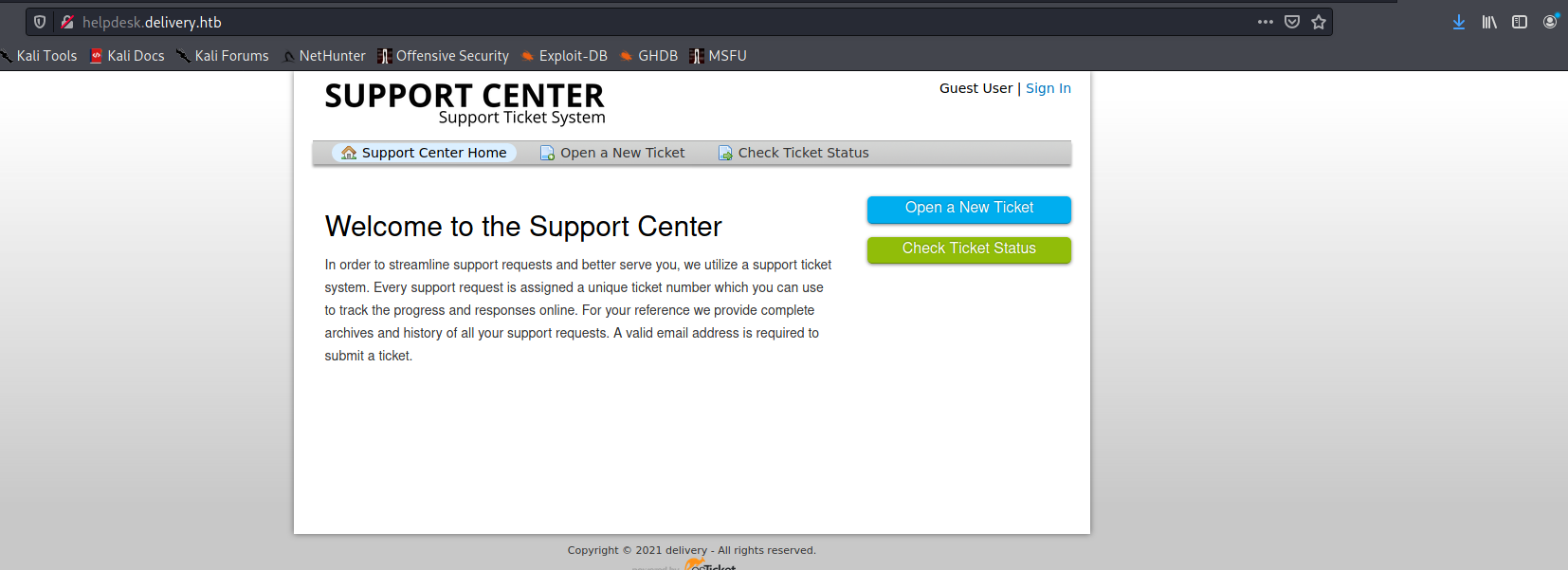
**Scanning**

5) Give nmap to check what are all the open ports like shown belowGot to see the port 22, 80 and 8065 are open and there are services like ssh and http running

6) In the site <http://10.10.10.222:80> there was nothing interesting to be seen from the page or the source code

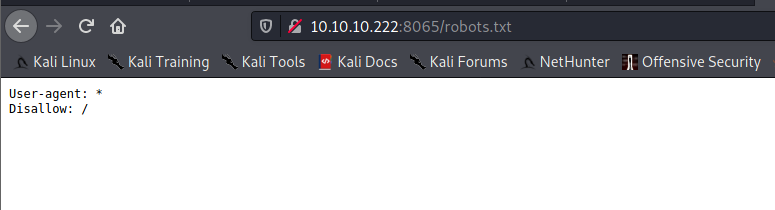
7) There was a link in the source code (<http://helpdesk.delivery.htb>) which when tried to open, I was not able to access it and I got an error loading page. Hence tried it add to the /etc/hosts to check whether it is able to load the page. Successfully the page loaded after that.





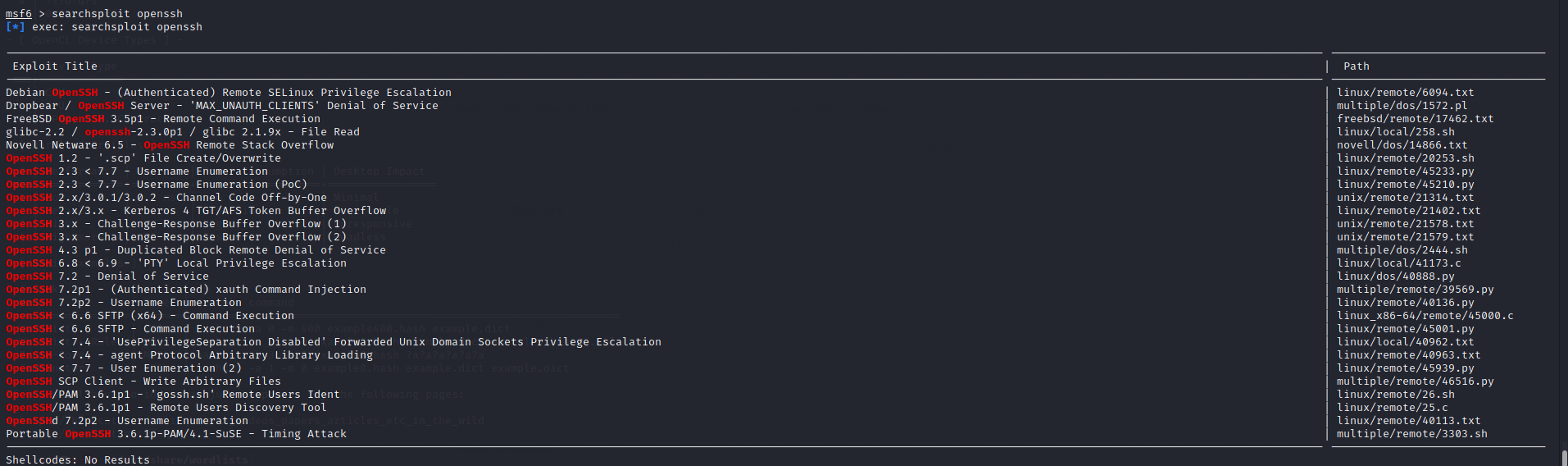
8) Not helpful here yet useful:

Checked for the robots.txt



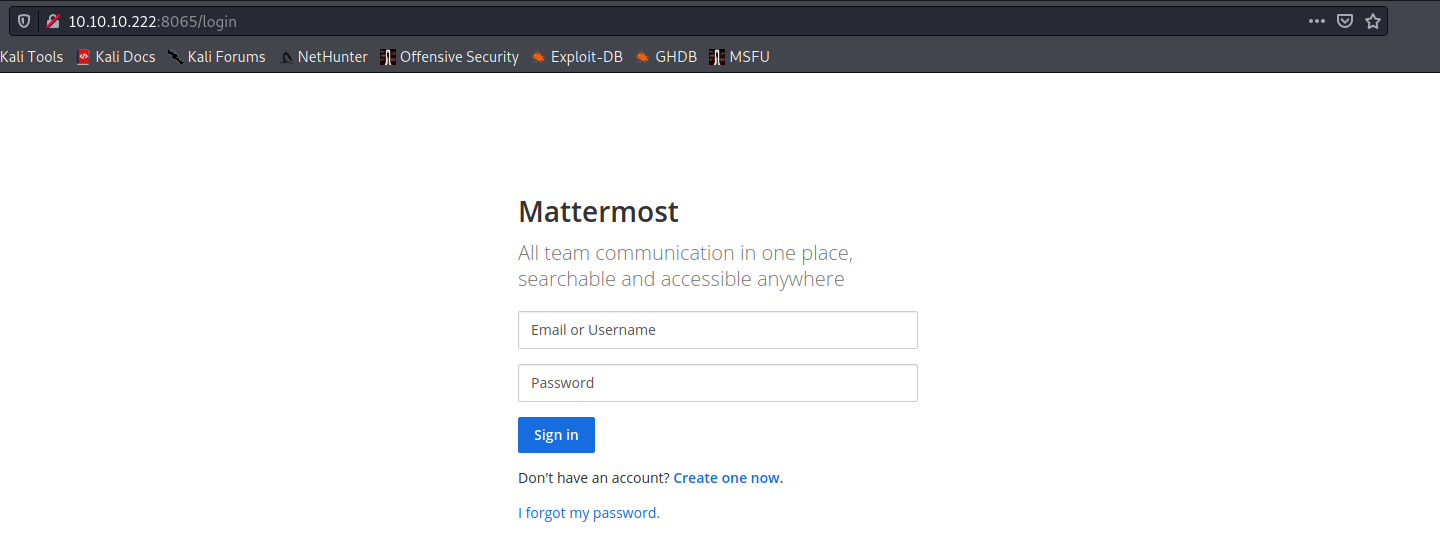
Found nothing interesting here in this robots.txt file

Using ssh version tried to check for the vulnerability in msfconsole

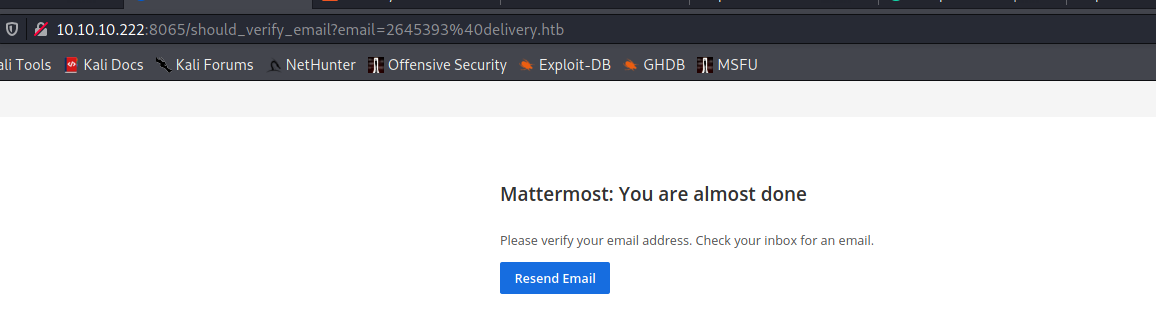


Couldn’t find any exploit for the open ssh version present

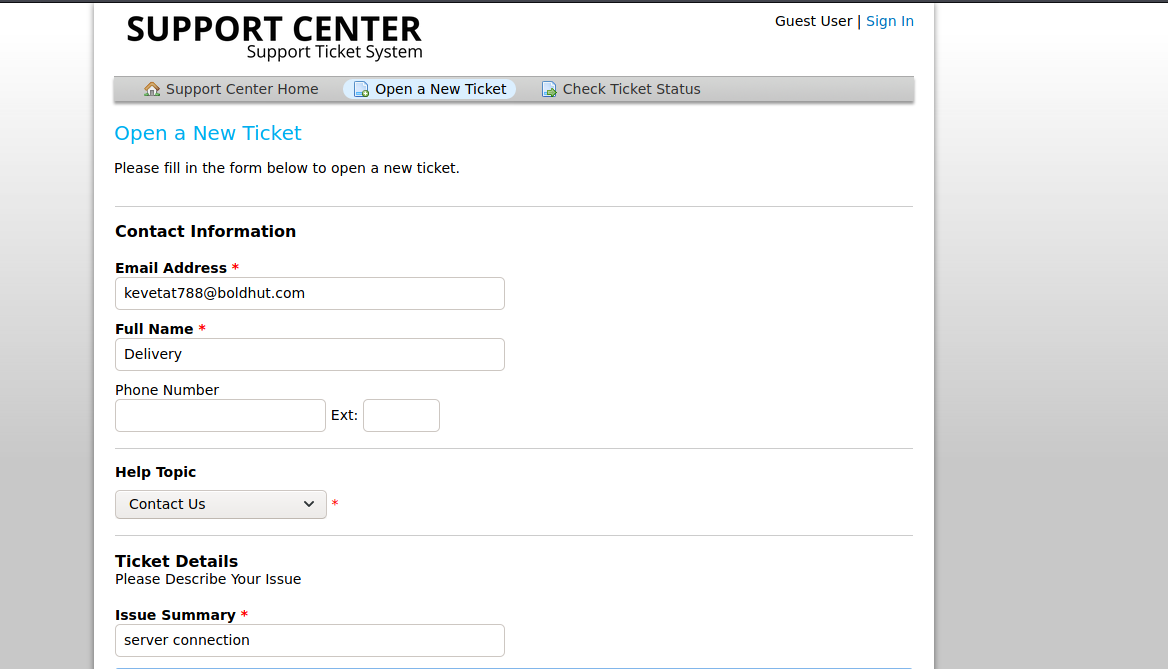
9) In one of the open ports 8065 got to see that the mattermost is running

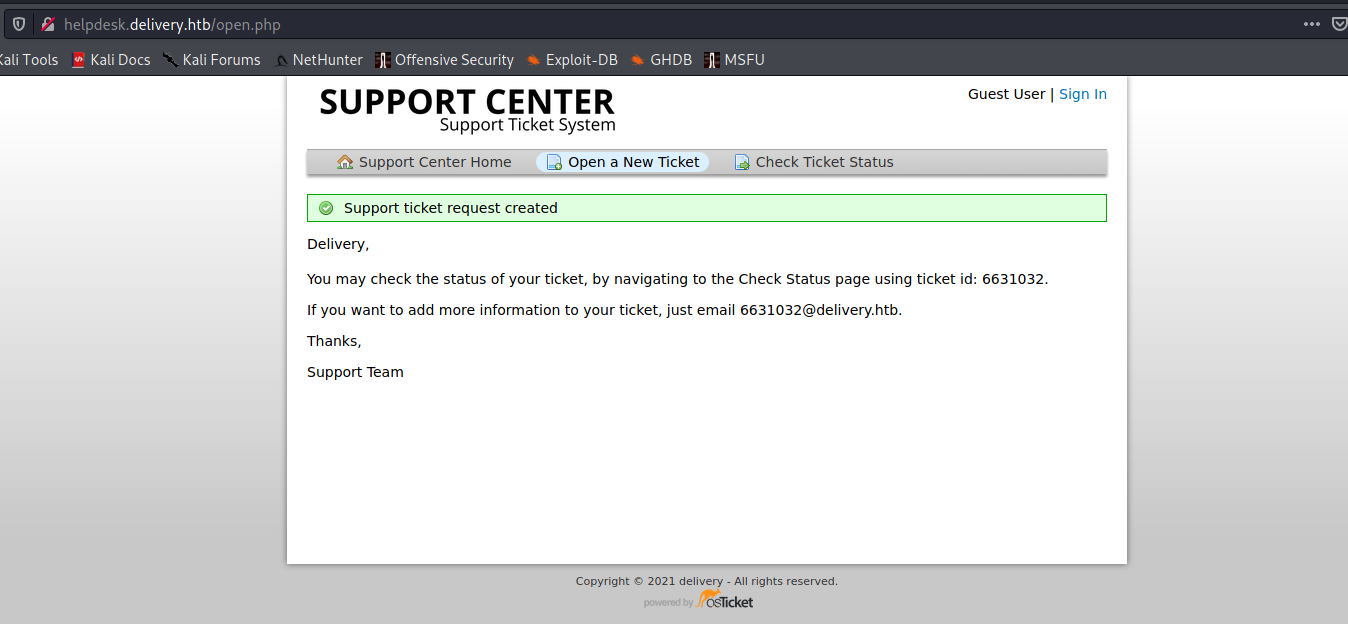


10)Tried to create an account using temp-mail.org just to see how it is working. But was not receiving the verification mail to validate even though user got created.



11) Hence tried to open a new ticket in support center





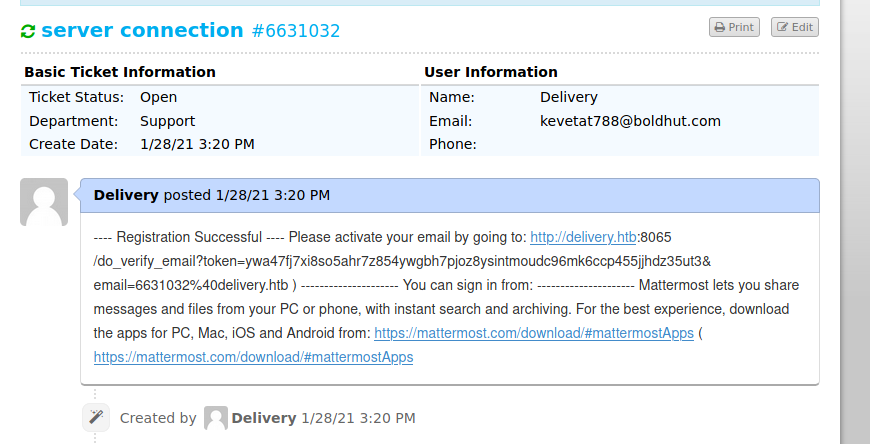
12)Got the information like I need to email [6631032@delivery.htb](mailto:6631032@delivery.htb)

Tried to create a user holding this email account in the mattermost with the name d6631032

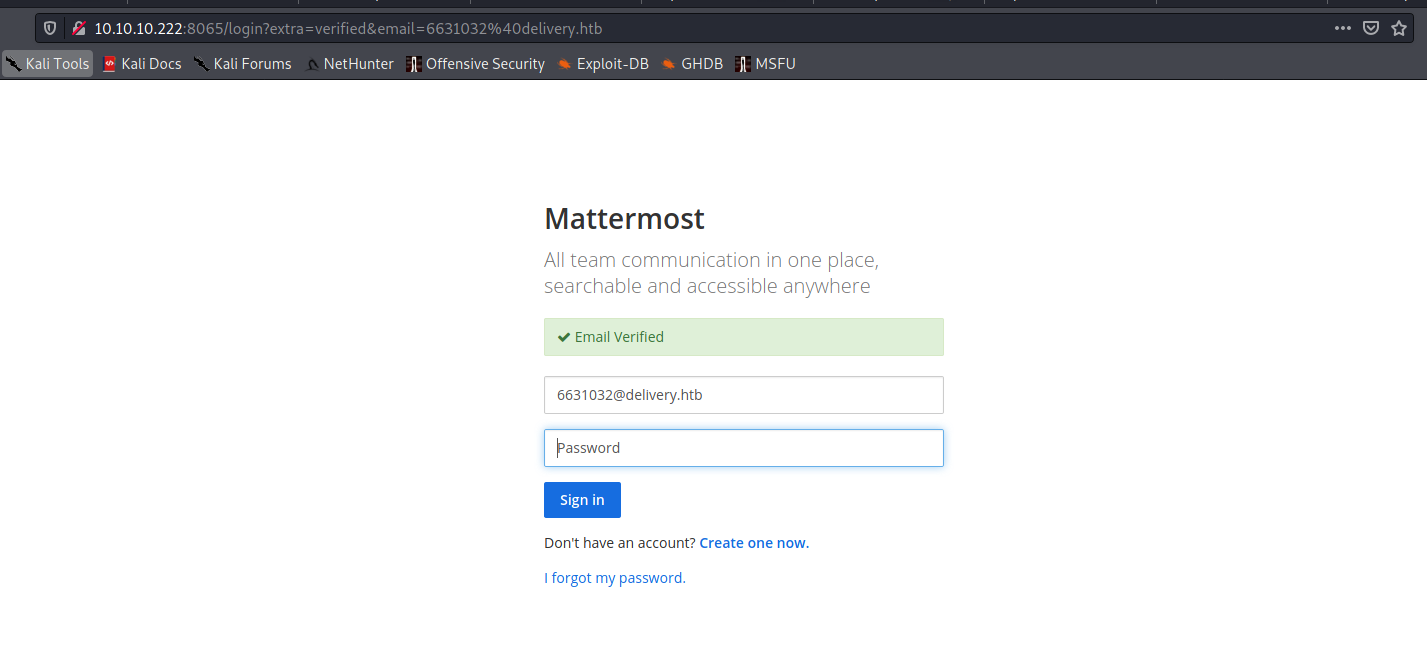
Just enter into the support center like check ticket status by giving the details as

The temp-mail id and the corresponding ticket number

Got to see the information after clicking on check ticket status as below



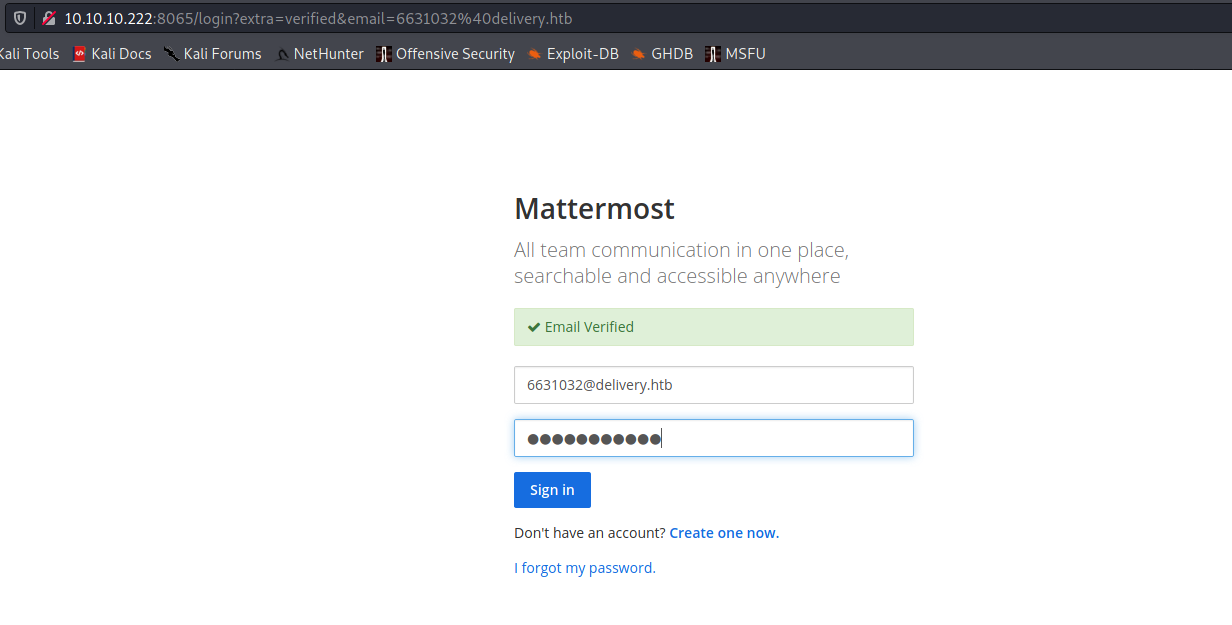
13)Tried to take the id to activate the email by going to the link as mentioned. Changed the delivery.htb in the URL to the ip address as 10.10.10.222 as shown below



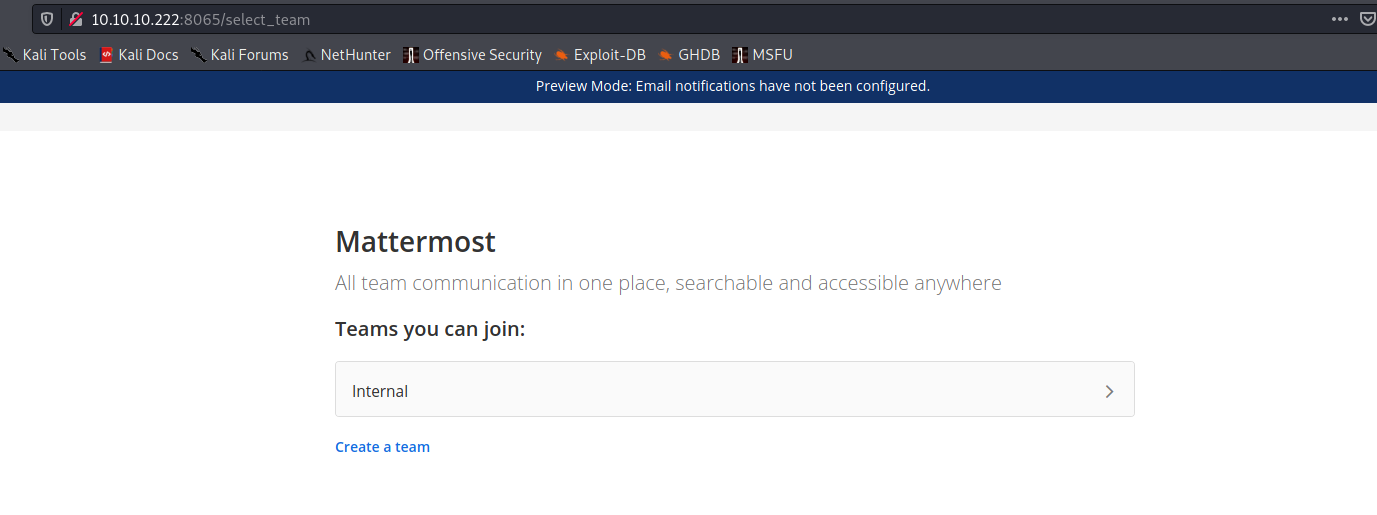
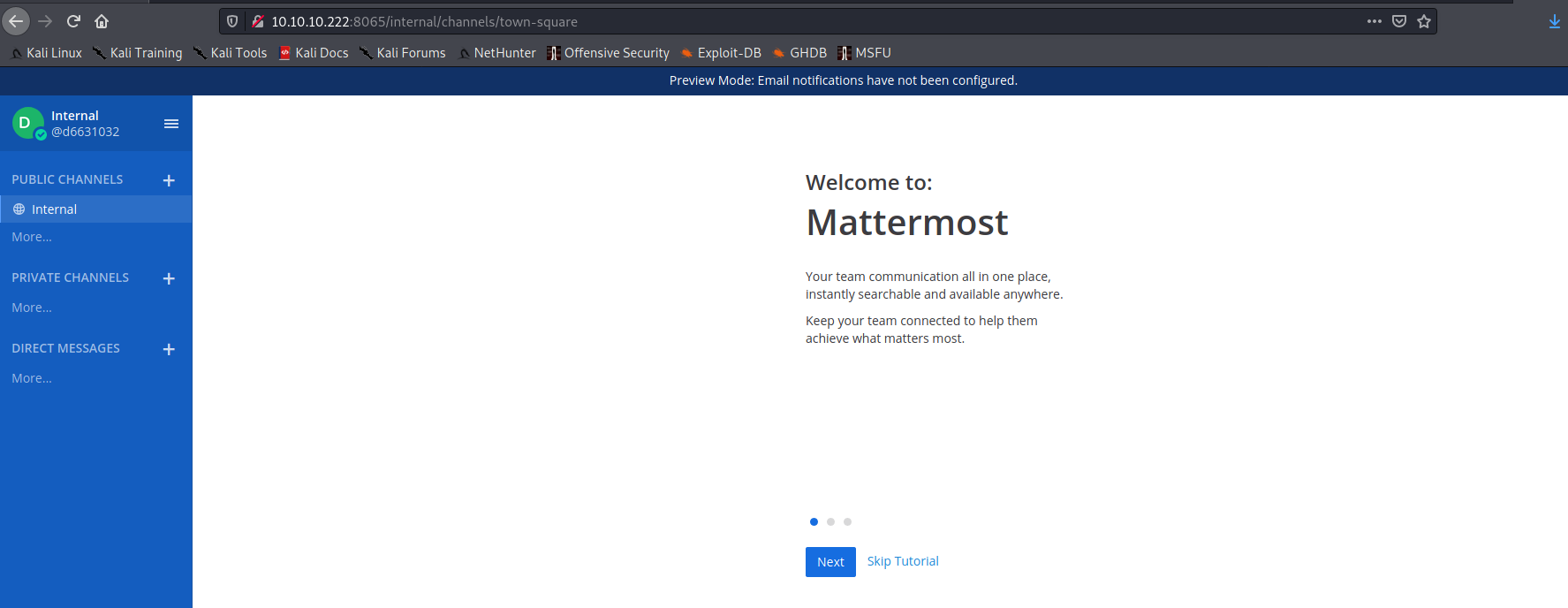
Voila got to see the email verified for the created user

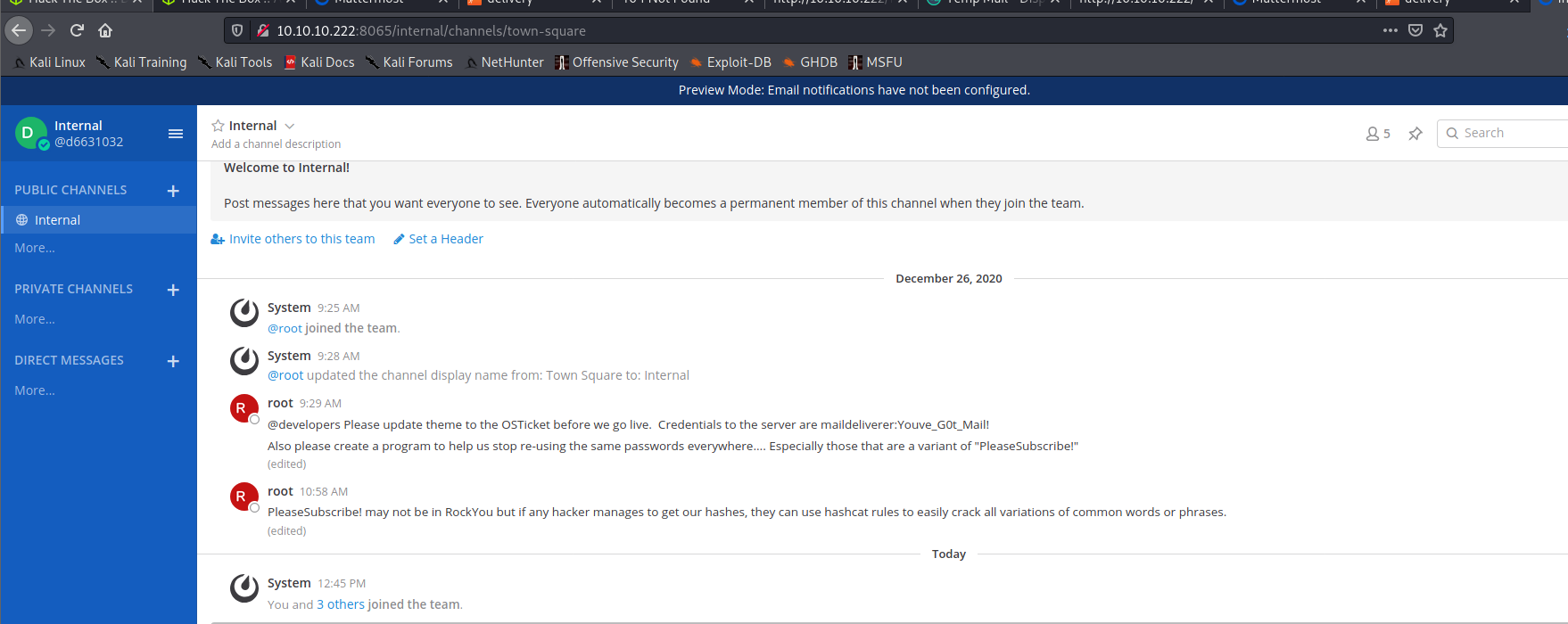
14)Enter into the mattermost with the userid and the password as mentioned earlier

**Gaining access**



Got into the team

Proceeded to the internal team

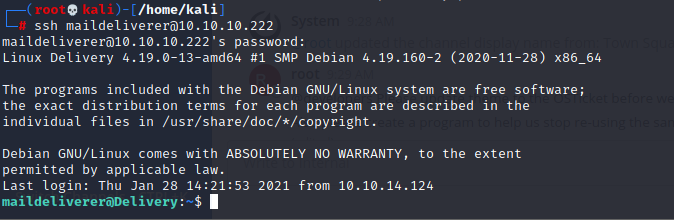


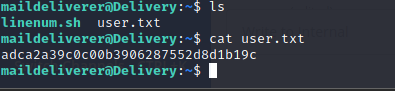
In the discussion while reading got to see there is a user named as maildeliverer and the password is

Youve\_G0t\_Mail!

15) We already knew that the port 22 ssh is open hence I tried to connect the server using the command

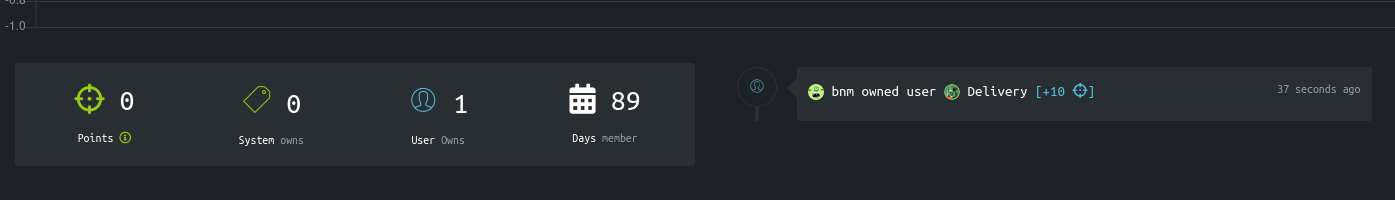
ssh [maildeliverer@10.10.10.222](mailto:maildeliverer@10.10.10.222)



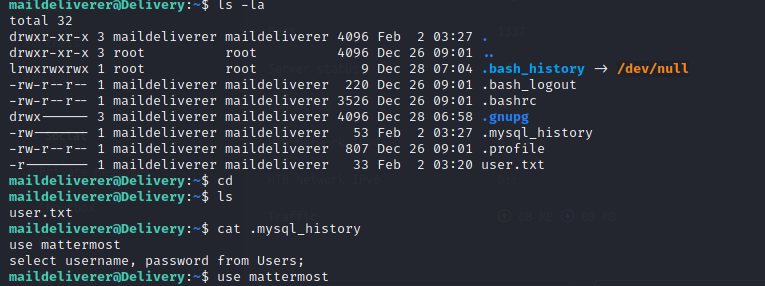


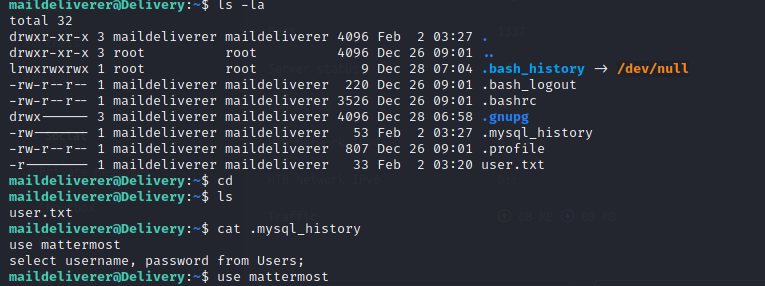
This is the value of the own user in HTB

Paste the same in own user of HTB to get own the system



**To get the root flag:**

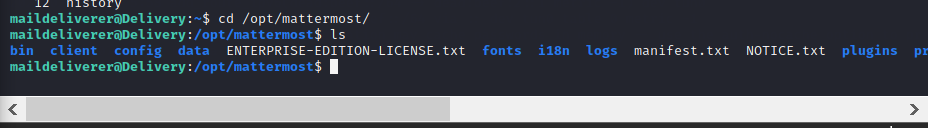




We see that there is mattermost database and there is a table like Users with the columns username,password. So, let’s try to check where it is

Trying with the below commands to get to the mattermost database



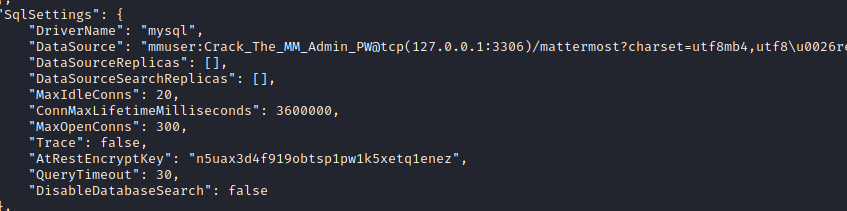


Hence, we could see the config file of the mattermost

Trying to get in to the mattermost config file

Tried to open to see the config.json



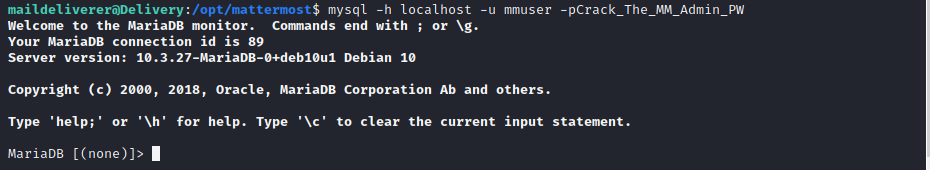


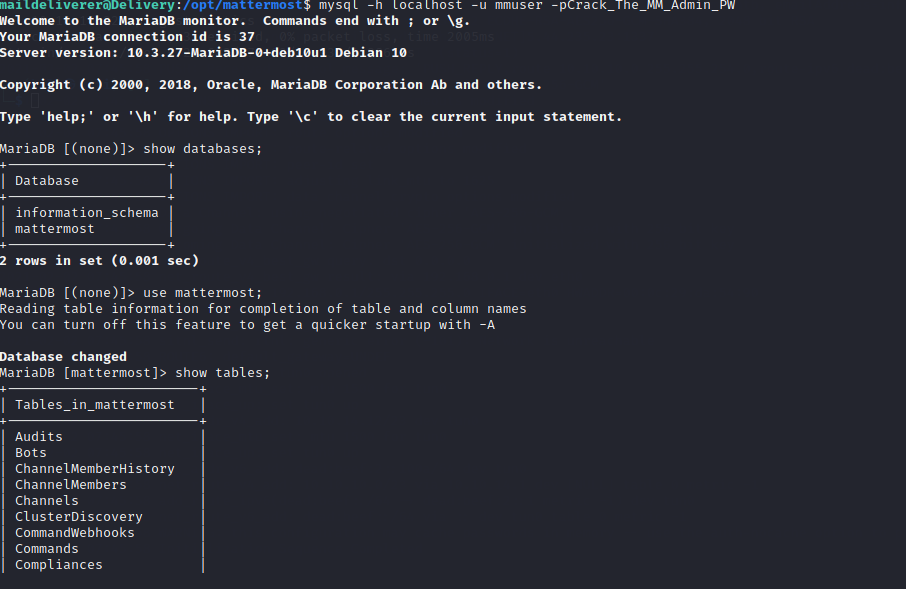
Got to see the username and password of mysql

Username:mmuser

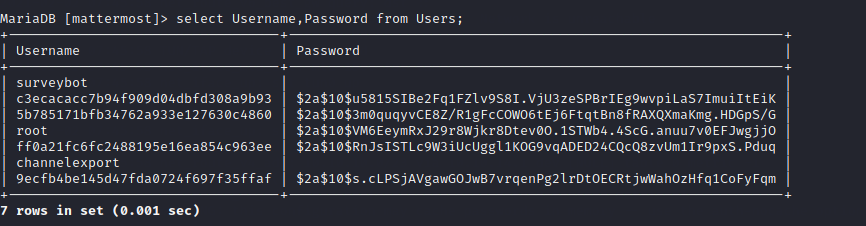
Password:Crack\_The\_MM\_Admin\_PW

Using the above credentials to connect to mysql





From the hint got from mysql.history I am giving the query as below



Got to see the root hash

$2a$10$VM6EeymRxJ29r8Wjkr8Dtev0O.1STWb4.4ScG.anuu7v0EFJwgjjO

Considering the PleaseSubscribe! as entry and giving the command below based on the clue from the mattermost internal team given



Put the root hash in delivery.hash

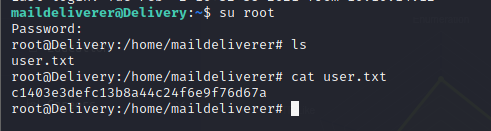
3200 is the value to use bcrypt in hashcat

The bcrypt hashing function allows us to build a password security platform that scales with computation power and always hashes every password with a salt

With the hash and the list of words obtained, we can try to attack







This is the flag for the root