Node,zip(爆破)、mongodb(失敗)

```
└─# nmap -sCV -p22,3000 -A 10.10.10.58
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 00:09 PDT
Nmap scan report for 10.10.10.58
Host is up (0.23s latency).

PORT     STATE SERVICE          VERSION
22/tcp   open  ssh              OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 dc:5e:34:a6:25:db:43:ec:eb:40:f4:96:7b:8e:d1:da (RSA)
|   256 6c:8e:5e:5f:4f:d5:41:7d:18:95:d1:dc:2e:3f:e5:9c (ECDSA)
|_  256 d8:78:b8:5d:85:ff:ad:7b:e6:e2:b5:da:1e:52:62:36 (ED25519)
3000/tcp open  hadoop-tasktracker Apache Hadoop
|_http-title: MyPlace
| hadoop-datanode-info:
|_  Logs: /login
| hadoop-tasktracker-info:
|_  Logs: /login
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose|specialized|phone|storage-misc
Running (JUST GUESSING): Linux 3.X|4.X|5.X (90%), Crestron 2-Series (86%), Google
Android 4.X (86%), HP embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
cpe:/o:crestron:2_series cpe:/o:google:android:4.0 cpe:/o:linux:linux_kernel:5.0
cpe:/h:hp:p2000_g3
Aggressive OS guesses: Linux 3.10 - 4.11 (90%), Linux 3.12 (90%), Linux 3.13 (90%),
Linux 3.13 or 4.2 (90%), Linux 3.16 (90%), Linux 3.16 - 4.6 (90%), Linux 3.18 (90%),
Linux 3.2 - 4.9 (90%), Linux 4.2 (90%), Linux 4.4 (90%)
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 3000/tcp)
HOP RTT       ADDRESS
1   225.16 ms 10.10.14.1
2   226.75 ms 10.10.10.58

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 25.80 seconds
```

3000 port

訊息收集，可能是user
tom
mark
rastating
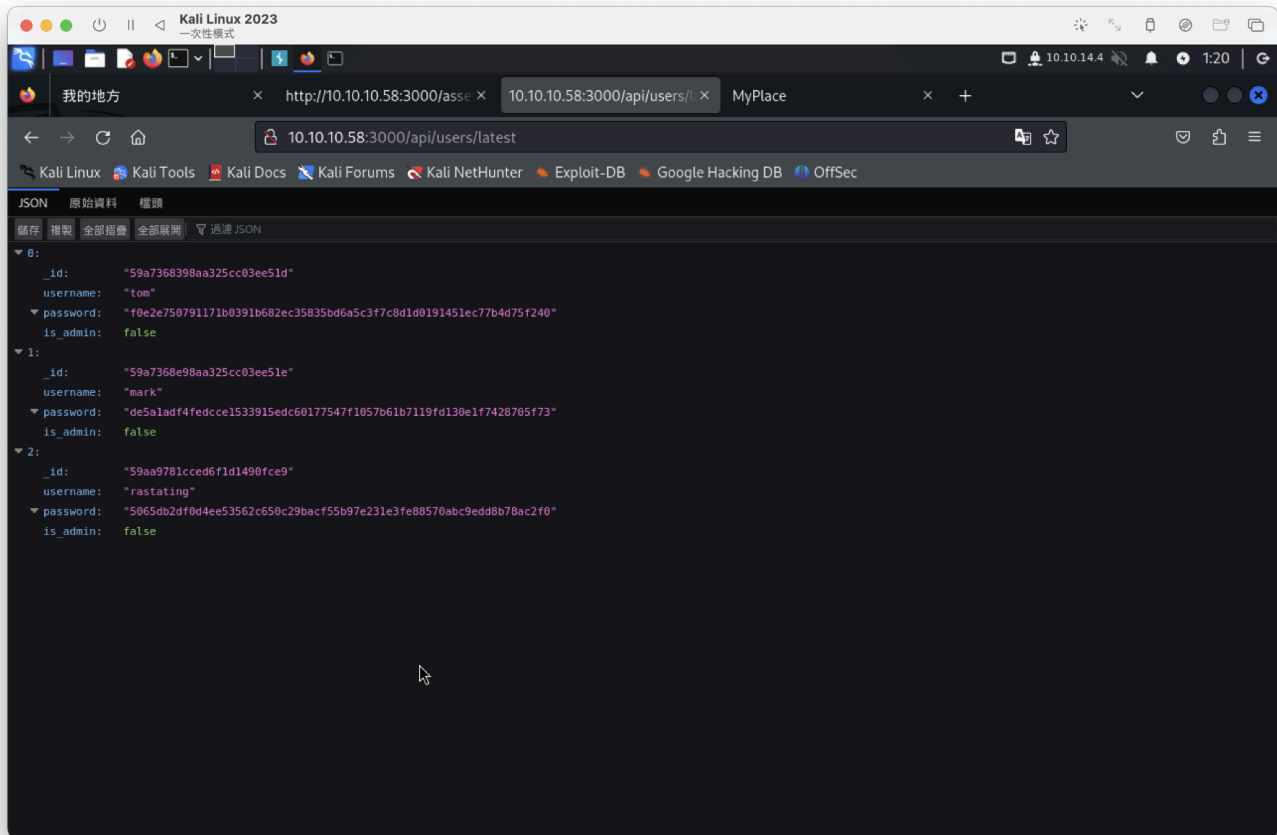
有目錄爆破，但都切回home
只有一筆登入介面，不管用sql..等都失敗，

檢查原始碼，逐一測試後，

```
80  <script type="text/javascript" src="vendor/jquery/jquery.min.js"></script>
81  <script type="text/javascript" src="vendor/bootstrap/js/bootstrap.min.js"></script>
82  <script type="text/javascript" src="vendor/angular/angular.min.js"></script>
83  <script type="text/javascript" src="vendor/angular/angular-route.min.js"></script>
84  <script type="text/javascript" src="assets/js/app/app.js"></script>
85  <script type="text/javascript" src="assets/js/app/controllers/home.js"></script>
86  <script type="text/javascript" src="assets/js/app/controllers/login.js"></script>
87  <script type="text/javascript" src="assets/js/app/controllers/admin.js"></script>
88  <script type="text/javascript" src="assets/js/app/controllers/profile.js"></script>
89  <script type="text/javascript" src="assets/js/misc/freelancer.min.js"></script>
```
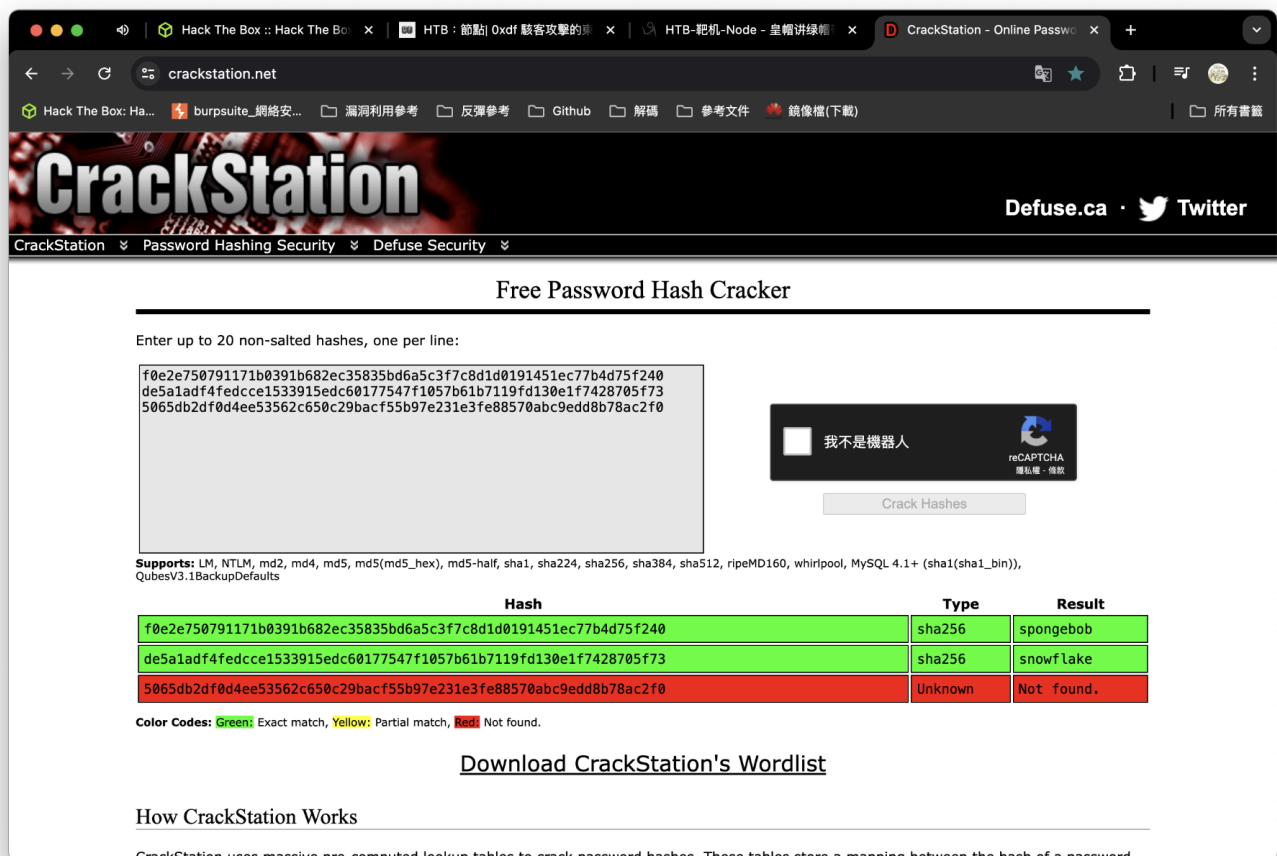
發現這目錄有passwd

```
var controllers = angular.module('controllers');

controllers.controller('HomeCtrl', function ($scope, $http) {
  $http.get('/api/users/latest').then(function (res) {
    $scope.users = res.data;
  });
});
```
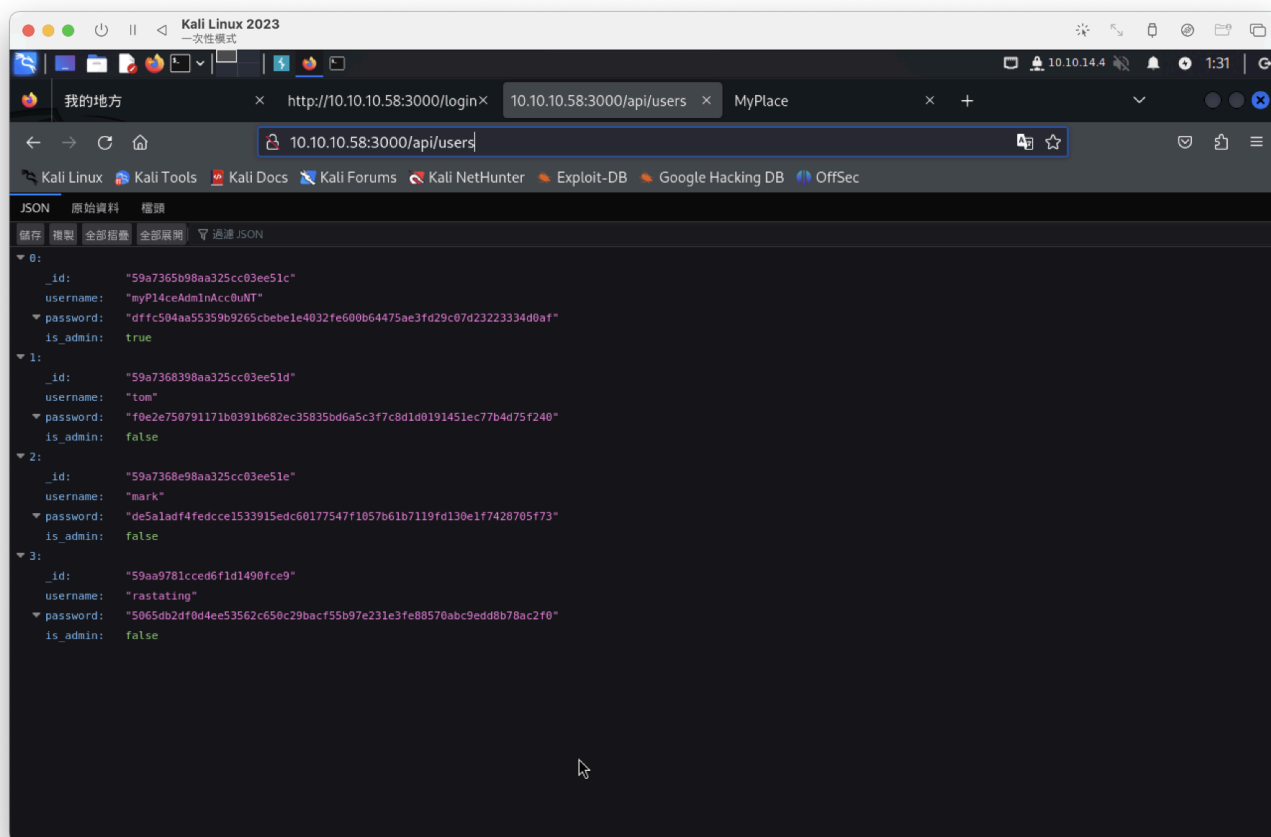
得出

username ： tom
passwd ： spongebob

```
username : mark
passwd : snowflake
```

可以登入web但都沒權限。

我把後面的/latest拿掉，多獲取一個帳密


```
username : myP14ceAdm1nAcc0uNT
passwd : manchester
```

登入後，可下載備份檔

檔案不管用web、指令都下載不下來。。。尷尬誒...

直接看答案 + 處理紀錄

參考：https://blog.csdn.net/XavierDarkness/article/details/130642338

下載完之後，是一個base64位元檔案，
└─$ file myplace.backup
myplace.backup: ASCII text, with very long lines (65536), with no line terminators

需解碼，解碼後是一個zip檔，

解zip需要密碼，

可以使用john2zip轉hash，

在john爆破，

爆破完後密碼：magicword。

看他們解壓縮完後，是web所有資訊

裡面有一個app.js檔案有

```
const url = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/myplace?
authMechanism=DEFAULT&authSource=myplace';
```

---

username : mark
passwd : 5AYRft73VtFpc84k

mongodb登入失敗，

參考：

1. https://book.hacktricks.xyz/v/cn/network-services-pentesting/27017-27018-mongodb

2. https://pjchender.dev/database/mongo-cli/

疑似可以ssh連線(成功)

```
Last login: Wed Sep 27 02:33:14 2017 from 10.10.14.3
mark@node:~$ id
uid=1001(mark) gid=1001(mark) groups=1001(mark)
mark@node:~$ whoami
mark
mark@node:~$ █
```

前面的資料庫有開port

```
mark@node:/home/tom$ netstat -tlnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address       Foreign Address     State      PID/Program name
tcp        0      0 127.0.0.1:27017     0.0.0.0:*           LISTEN     -
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN     -
tcp6       0      0 :::3000             :::*                LISTEN     -
mark@node:/home/tom$ █
```

任務裡面沒物件

```
mongo 127.0.0.1:27017/scheduler -u mark -p 5AYRft73VtFpc84k
```

```
> show collections
tasks
> db.tasks.find()
> █
```