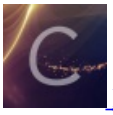
Hack The Box - Help Writeup

原创

ShinJoe 于 2019-01-30 04:41:17 发布 2844 收藏
分类专栏： hackthebox 文章标签： CT

本文链接：https://blog.csdn.net/qq_23026851/article/details/86698333



解题过程：

- nmap + nikto 扫描目标机，开放22，80，3000端口。并且找到80下的support/路径。
- 打开http://[ip]/support，发现一个叫HelpDeskZ的应用，源码：https://github.com/evolutionscript/HelpDeskZ-1.0/。该应用的submit ticket功能可以上传任意文件。虽然有file extension的检查，但是文件依然会被上传，且能被直接访问。不过文件名会用md5加密后存储。
- 找到了一个exploit：https://www.exploit-db.com/exploits/40300。开始时研究了好久的timezone offset，结果发现是浪费时间，这个exploit不用做任何修改，可以直接拿来用，只要找到正确的文件存储路径就行。
- 耐心读一下源码，找到关键信息：
  - $uploaddir = UPLOAD_DIR.'tickets/';
  - define('UPLOAD_DIR', ROOTPATH . 'uploads/');
  - define('ROOTPATH', dirname(dirname(__FILE__)).'/')
  - 文件在http://[ip]/support/uploads/tickets/ 下。
- 上传reverse_shell.php，运行nc监听，运行exploit，得到shell。
- 用户名称为help，可以访问user.txt。接下来考虑如何做priv esc。
- 论坛上提示是Basic enumeration。花了很久，尝试了suid program exploitation, cron jobs exploitation等。后来发现在/tmp下有现成的exploit程序。。。

```
help@help:/$ cd /tmp
cd /tmp
help@help:/tmp$ ls -al
ls -al
total 64
drwxrwxrwt 11 root root  4096 Jan 29 10:51 .
drwxr-xr-x 22 root root  4096 Nov 28 09:18 ..
drwxrwxrwt  2 root root  4096 Jan 29 09:58 .ICE-unix
drwxrwxrwt  2 root root  4096 Jan 29 09:58 .Test-unix
drwxrwxrwt  2 root root  4096 Jan 29 09:58 .X11-unix
drwxrwxrwt  2 root root  4096 Jan 29 09:58 .XIM-unix
drwxrwxrwt  2 root root  4096 Jan 29 09:58 .font-unix
drwxrwxrwt  2 root root  4096 Jan 29 09:58 VMwareDnD
-rwxrwxrwx  1 help help 17880 Jan 22 00:50 exploit
drwxr-xr-x  2 help help  4096 Jan 29 10:35 new
drwx------  3 root root  4096 Jan 29 09:58 systemd-private
pn
drwx------  2 root root  4096 Jan 29 09:58 vmware-root
help@help:/tmp$ ./exploit
./exploit
task_struct = ffff880039d92a00
uidptr = ffff8800055b7804
spawning root shell
root@help:/tmp# cd /root
```

- 几点收获：
  - 耐心读程序的源码，理解对应exploit的原理。
  - 学习了Linux privilege escalation的几种方式。一个不错的guide：https://payatu.com/guide-linux-privilege-escalation/。
  - Don't overthink!!!
  - 3000端口上跑着一个Nodejs Express framework的程序，应该是要做sql injection。这是获取user的另一个途径，后面有空再研究一下。