i春秋 - Exploit-Exercises: Nebula（1）

原创

R1ght0us 于 2018-04-29 22:02:44 发布 1269 收藏 1
分类专栏： linux提权 文章标签： nebula

还是老哥的锅，兴冲冲的给我说这个比赛很有意思，一脸懵逼的进来，但是绝对不会一脸懵逼的出去。

这个对于我这个才是WEB方面的小白的我来说有点懵逼，最后百度了百度还是懂了一点。那就写下我做这个题的想法。

nebula其实就是专门针对linux提权训练的一个靶机，就这个我需要理解很多知识顺便补充了一个find命令（这个find命令补充还是在我的博客里）

```
find / -user flag00 -perm -4000 2>/dev/null
```

我有必要解释一下 **2>/dev/null**

- 0 —— stdin（标准输入）
- 1 —— stdout （标准输出）
- 2 —— stderr （标准错误）

这几个数字代表着这些含义，如果不懂请度娘，毕竟我也是百度的！

> 这个代表着重定向符

/dev/null是一个特殊设备就像一个垃圾桶，往里面扔你不需要的东西就OK。

还有这个4000是什么意思

八进制数	权限
4000	SUID
2000	SGID
1000	粘附位
0400	所有者可读
0200	所有者可写
0100	所有者可执行
0040	组成员可读
0020	组成员可写
0010	组成员可执行
0004	其它用户可读
0002	其它用户可写
001	其它用户可执行

在此吐槽cmcc的网速，网速奇慢体验极差！上图就是一个八进制的权限表达形式，因为我们需要找到这个suid（super ID）来提升权限。

继续开始我们的正题，我们执行上述命令后会得到一个可执行的文件。

```
/bin/.../flag00
```

直接执行就好了，系统会提示你有了flag00的权限，于是就可以查看呢个flag00地下flag了嗷，这个操作再不会就求求你别秀了，好好看看linux的基础命令。