CTF writeup: rbash 逃脱方法

原创

samohyes 于 2017-08-03 15:17:28 发布
分类专栏： CTF writeup 文章标签： bash 信息安全 vim 谷歌 百度

今天做了一个rbash逃脱的题目。百度了好久没找到，后来翻墙用了google才找到思路，大致的思路是这位外国友人贡献的。

https://eddy3oy.com/2017/02/28/breaking-out-of-rbash/

好了，我来说下我的解题过程。

首先，我开始尝试出来可以用echo命令，但是不知道有什么用，其实采用compgen -c就可以知道能用什么命令。

那么输入 echo /*,发现了一个文件。

```
ctfuser@jail:~$ echo /*
/bin /boot /dev /etc /flag_thisfilename1ss0longt0guess_HAHAHA /home /lib /lib64
/media /mnt /opt /proc /root /run /sbin /srv /sys /tmp /usr /var
```


用ls -l知道那不是一个文件夹，那么就采用参考文献中的方法，设置环境变量BASH_CMDS吧，轻松搞定,得到一个flag.

其他常用的像是bash,vim的方法就不列举了。