

bugku caidao writeup

原创

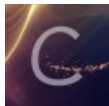
Daniel-0 于 2017-03-30 10:24:17 发布 1509 收藏

分类专栏: [writeup](#)

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/D_pokemon/article/details/68483892

版权



[writeup](#) 专栏收录该内容

17 篇文章 0 订阅

订阅专栏

CTF 中国菜刀不在web里???

作为一个接触CTF不过半个多月的小菜鸟, 刚拿到这题的时候走了弯路, 首先打开题目链接会下载一个zip格式的压缩文件



打开下载的zip文件, 看到这个

名称	大小	类型	已修改
caidao.pcapng	8.0 KB	Packet Cap...	2016年6月27日 16:48

http://blog.csdn.net/D_pokemon

首先看到这个.pcapng文件我以为是要抓包的, 作为菜鸟当然不会抓包了, 所以抱在尝试的态度, 用cat命令查看了一下, 然后发现了几串编码, 然后解码, 发现是与flag无关的东西, 感觉是自己思路错了, 然后换个想法, 用binwalk查看了一下。

```
0-15ISK:~$ cd 文档
0-15ISK:~/文档$ binwalk caidao.pcapng
DECIMAL      DESCRIPTION
-----
43           gzip compressed data, from Unix, last modified:
```

发现一个gzip格式，是在unix下的文件格式，然后改成gzip格式发现打开后什么都没有，就感觉应该不是直接查看的，所以我尝试用dd命令来分离文件

```
14:39
root@kali:~/binwalk# binwalk caidao.pcapng --dd=gzip:zip
HEXADECIMAL DESCRIPTION
1E43
```

发现真的可以，分离出一个文件夹，打开发现一个压缩文件，而且可以打开



我就用cat命令查看，发现不行，然后用notepad++打开，发现flag



新手感觉做CTF题真的需要脑洞要大。