

CTF-Misc-二维码（一）

原创

归子莫 于 2020-05-14 17:10:43 发布 3366 收藏 15

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_45163122/article/details/106124143

版权

CTF-Misc-二维码（一）

博客说明

文章所涉及的资料来自互联网整理和个人总结，意在于个人学习和经验汇总，如有什么地方侵权，请联系本人删除，谢谢！本文仅用于学习与交流，不得用于非法用途！

CTP平台

网址

<https://buuoj.cn/challenges>

题目

Misc类，二维码（一）

思路

这类题目首先把文件下载下来，是一个二维码，扫描没得，只是这个"secet is here"

使用 binwalk

```
binwalk QR_code.png
```

```
tanglei@ubuntu:~/Desktop/ctf/misc$ binwalk QR_code.png
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          PNG image, 280 x 280, 1-bit colormap, non-interlac
ed
471          0x1D7        Zip archive data, encrypted at least v2.0 to extra
ct, compressed size: 29, uncompressed size: 15, name: 4number.txt
650          0x28A        End of Zip archive, footer length: 22
```

里面有一个zip压缩包

使用 foremost

```
foremost QR_code.png
```

```
tanglel@ubuntu:~/Desktop/ctf/misc$ foremost QR_code.png
Processing: QR_code.png
♦foundat=4number.txtn
Qjxu♦J♦♦♦♦[♦♦♦♦0PF4L♦
*|
```

在output文件夹里面找到



打开txt文件时需要密码，提示为4位的数字

使用fcrackzip

下载安装

```
sudo apt-get install fcrackzip
```

使用

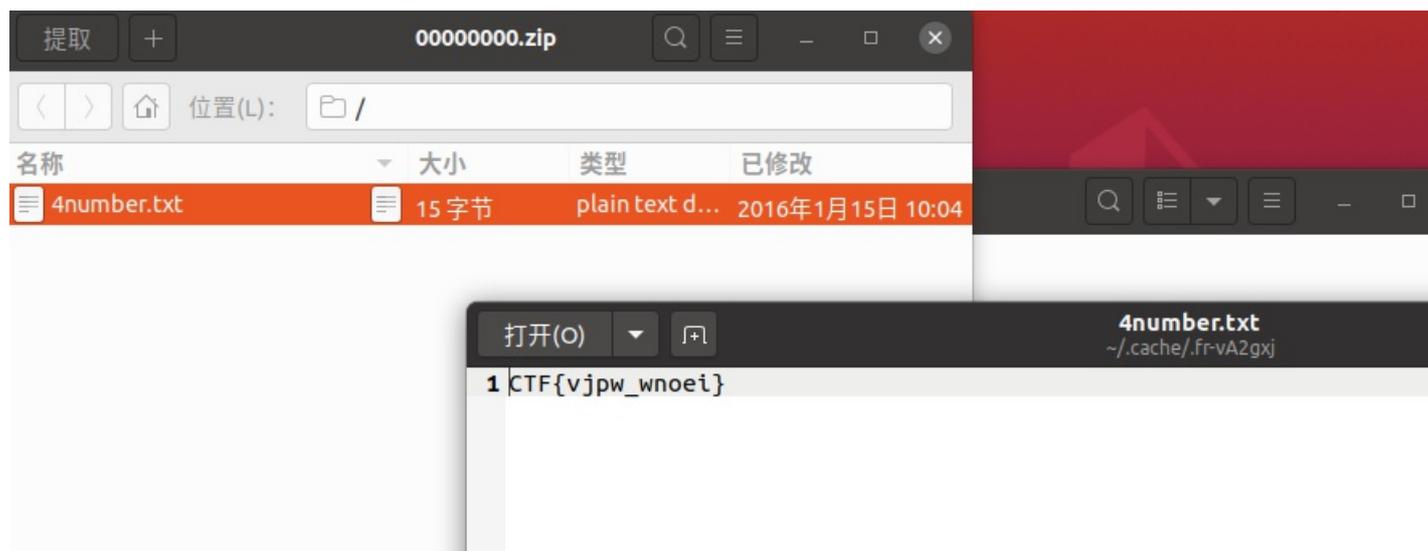
```
fcrackzip -b -ca -l 1-4 -u 压缩文件
```

-b 暴力破解模式 -c 指定掩码类型 (a=a-z;1=0-9;! =特殊字符) -l 密码长度 -u 压缩文件名

```
fcrackzip -b -c1 -l 4 -u 00000000.zip
```

```
tanglel@ubuntu:~/Desktop/ctf/misc/output/zip$ fcrackzip -b -c1 -l 4 -u 00000000.zip
PASSWORD FOUND!!!!: pw == 7639
```

输入密码，打开得到flag



感谢

BUUCTF
以及勤劳的自己