BUUCTF之二维码

原创

陆小路-1 于 2021-10-27 19:55:28 发布 1167 收藏 6

分类专栏： CTF 文章标签： unctf

本文链接：https://blog.csdn.net/weixin_45728231/article/details/120988424

文章目录

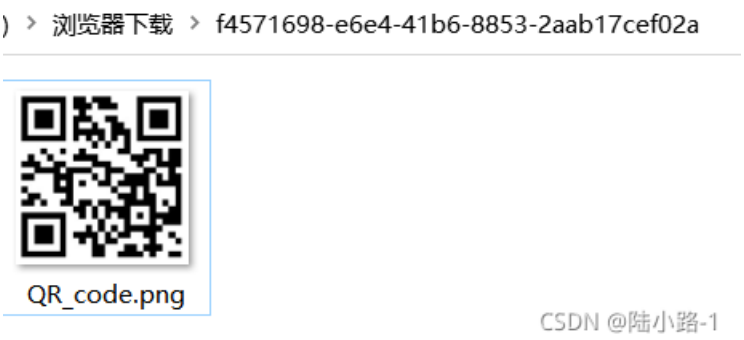
二维码

题目

- 附件链接

解题过程

- 下载附件发现是一个压缩包。
- 解压，发现里面存在一张二维码。



- 毫不犹豫打开二维码扫描工具QR research进行扫描

- ~~天真认为这就是flag点击提交（不放过任何一次机会），结果当然没过啦！~~
- ~~没死心以为是空格的原因，删去空格再次提交，当然还是没过啦！~~
- ~~于是菜鸡开始看教程，向菜狗求救！！！~~
- 由于附件中只有一张二维码，而且刚才的提示信息secret is here 表明flag确实在这里，于是想到可能在图片中可能隐藏了其他文件。隐藏原理如下：

```
一个完整的 JPG 文件由 FF D8 开头，FF D9结尾
图片浏览器会忽略 FF D9 以后的内容，因此可以在 JPG 文件中加入其他文件。
其余同理：
png
十进制数137 80 78 71 13 10 26 10
十六进制数 89 50 4e 47 0d 0a 1a 0a
gif
图像开始标志：47 49 46 38 39 61
结束标志：01 01 00 3B
```

- 首先使用kali查看该二维码图片信息，发现了4number.txt，还有一些PK值，敏感想到可能隐藏了一个zip压缩包(zip的创始人名字简写为PK)和4number.txt文件。

```
┌──(root㉿kali)-[~/CTF/BUUCTF/二维码]
└─# cat QR_code.png
PNG

IHDR½@{ PLTEÿÿÿUÓ~IDATh㉾ 0D膾Ƒ|GpB
m·ş²5«₰¼I<□6ᵑᵡ ₥ł駙W2uľoeB↗盃 iÆ`0#,0ᵣ 3W+2ㄱ□¾"X¼          9ɔbKʃ㿲 sqx㌃ ⸭®g ᵐ7畔g顯 E隅£ᴍ·□
^-SO¦-£«ʅ8[ S    b´)蚩³X±02□¥¹□ᵓ L
                                  Ě¯Uz□§¼ s±y><d)/ǔ`¤□ X¬ɬd¤þXřsĸkZ?½{ ’誠3.öȼKZ¦;»\PL-¦酸
鮓d*2獚p□w L®?¹□cr'3<蝶<&²      £┐ÿ=ꜿyiþ~²gIEND®B`PK    P/HF4L®
                                                          4number.txtn
QjxuǎJ©·¥OPF4L®PK      P/HF4L®
                                  $ 4number.txt
 e'9Opezhd□ezhd□PK|V                                    CSDN @陆小路-1
```

- 当然，既然身在kali环境下，当然要使用Kali下的专业工具binwalk进行检测，结果如下，检测出图片中存在压缩包。

```
┌──(root㉿kali)-[~/CTF/BUUCTF/二维码]
└─# binwalk QR_code.png                                                    127 ×

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 280 x 280, 1-bit colormap, non-interlaced
471           0x1D7           Zip archive data, encrypted at least v2.0 to extract, co
mpressed size: 29, uncompressed size: 15, name: 4number.txt
650           0x28A           End of Zip archive, footer length: 22
                                                                    CSDN @陆小路-1
```

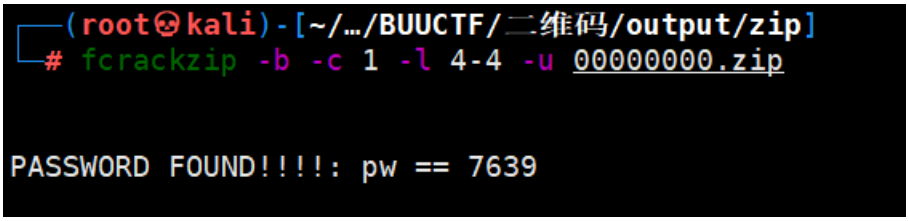
- 那么下一步当然是分离出这个压缩包，利用Linux下的foremost工具，foremost 图片名，结果如下

```
┌──(root㉿kali)-[~/CTF/BUUCTF/二维码]
└─# foremost QR_code.png
Processing: QR_code.png
|foundat=4number.txtn
QjxuǎJ©·¥OPF4L®
*|

┌──(root㉿kali)-[~/CTF/BUUCTF/二维码]
└─# ls
output  QR_code.png

┌──(root㉿kali)-[~/CTF/BUUCTF/二维码]
└─# cd output/

┌──(root㉿kali)-[~/CTF/BUUCTF/二维码/output]
└─# ls
audit.txt  png  zip                                    CSDN @陆小路-1
```

- 当然直冲zip文件夹，并尝试解压zip文件，却发现需要密码，，随便输了几个密码，失败告终。

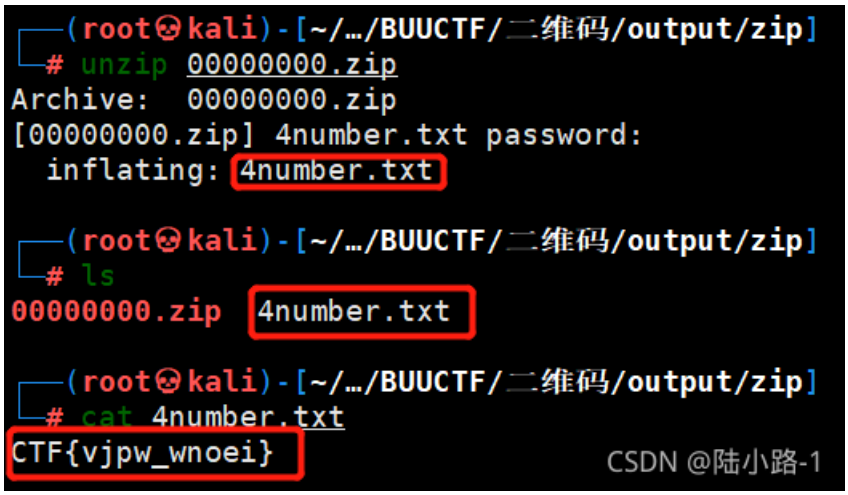
```
┌──(root㉿kali)-[~/CTF/BUUCTF/二维码/output]
└─# cd zip

┌──(root㉿kali)-[~/…/BUUCTF/二维码/output/zip]
└─#
```

- 那还想啥，当然暴力破解啦！，，但回想起看到文件名是4number.txt，似乎是在提示我们密码是一个4位数字。于是破解开始：密码是7639




```
参数解释：
-b:     使用暴力破解
-c 1:     使用字符集，1指数字集合
-l 4-4:    指定密码长度，最小长度-最大长度
-u:     不显示错误密码，仅显示最终正确密码
```

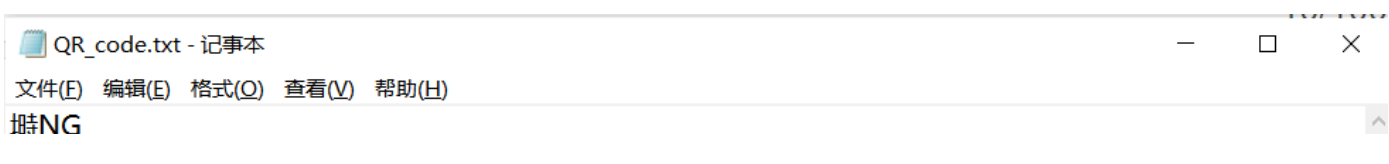
- 下面用密码解压压缩包，得到4number.txt文件，查看该文件后发现flag。

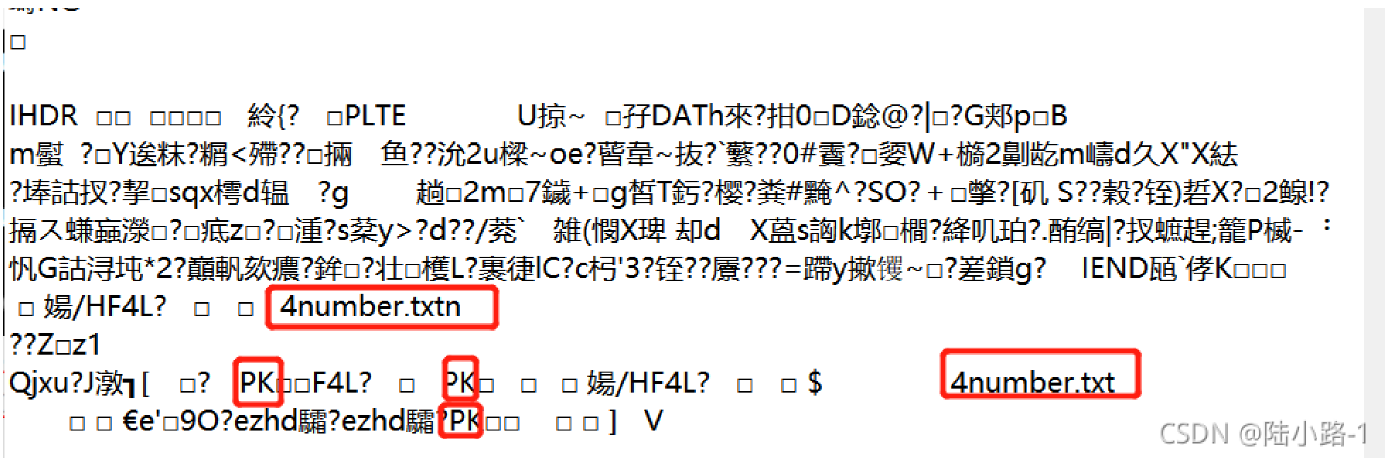


- 提交通过

补充：windows系统下的解题流程

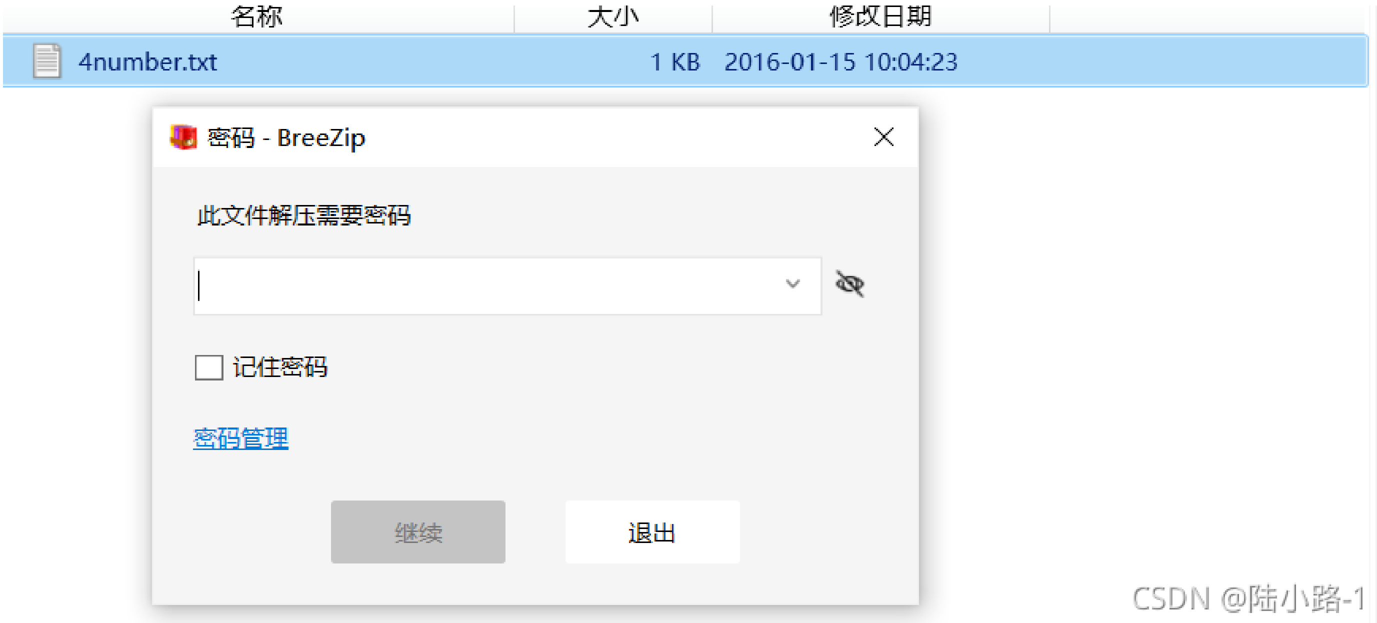
- 扫描二维码无果后，先将png图片更改后缀转为txt文件，同样发现了4number.txt，还有一些PK值，敏感想到可能隐藏了一个zip压缩包(zip的创始人名字简写为PK)和4number.txt文件。





- 再将后缀改为zip格式，用压缩软件能打开，并且发现一个4number.txt文件（猜想正确）。

- 尝试打开，却发现需要解压密码。。



- 然后用zip爆破工具爆破就好了。

- 打开4number.txt文件，得到flag。

总结

挺简单的一道题，做的无比复杂，就当学着用工具了吧！！！
在网上找了好久windows下的压缩包破解工具，或多或少都有缺陷。。。

附录

- 采用010editor工具分析文件头，佐证上述猜测。