ctf赛题MISC二维码

原创

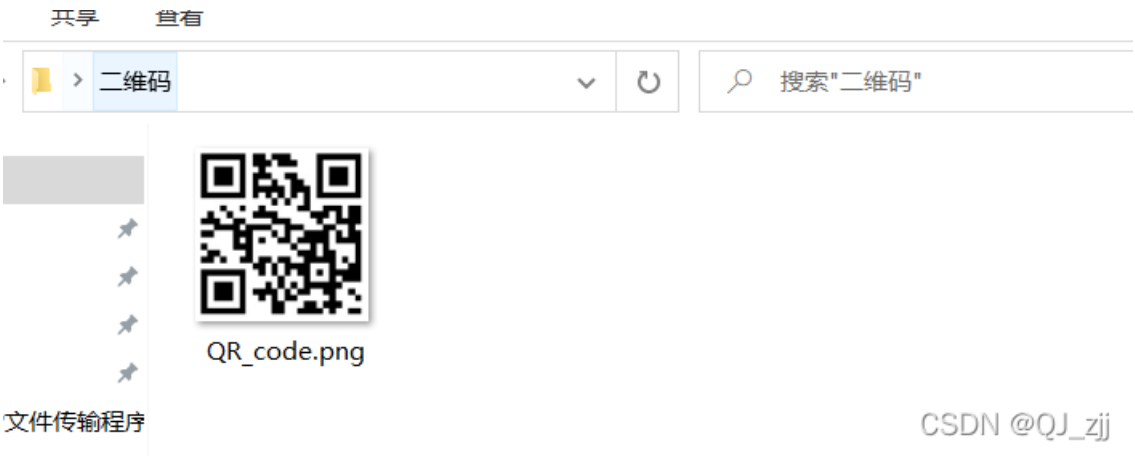
QJ_zjj 于 2022-02-17 14:58:37 发布 2613 收藏
文章标签： 安全

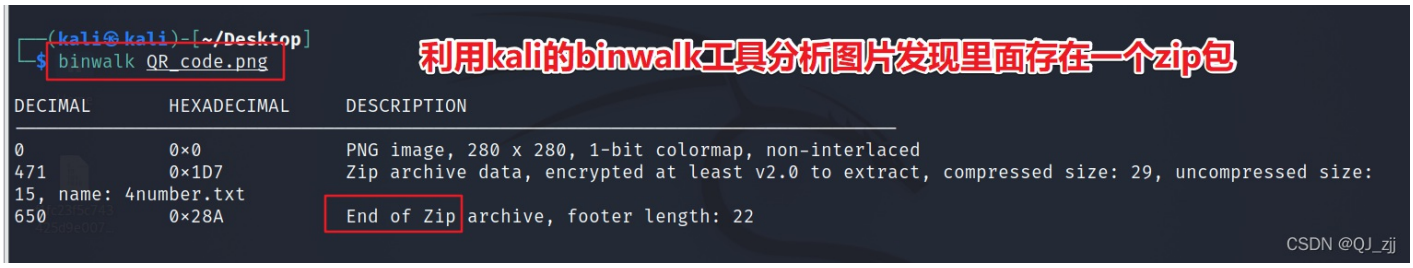
本文链接：https://blog.csdn.net/m0_60319766/article/details/122982767

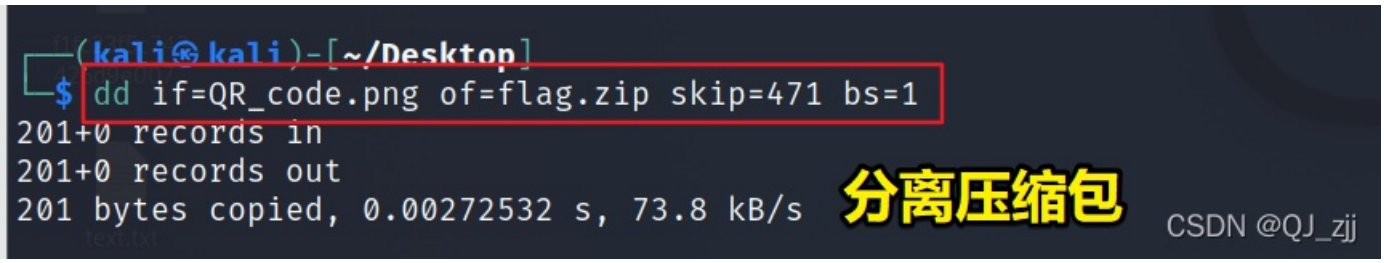
素材：百度网盘 请输入提取码

提取码：7yk2

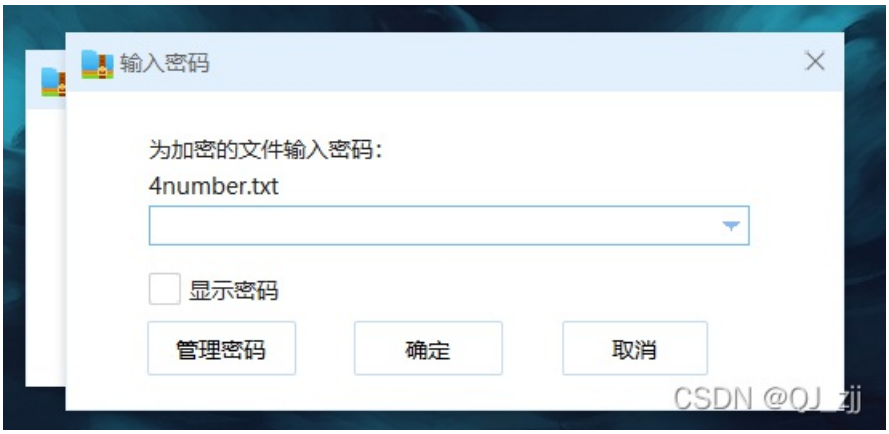
1、解压压缩包得到一个二维码







2、分离出来的压缩包需要密码才能解密




```
┌──(kali㉿kali)-[~/Desktop]
└─$ hexdump -C flag.zip
```

分析压缩包不是伪加密

```
00000000  50 4b 03 04 14 00 09 00  08 00 8b 50 2f 48 46 34  |PK.........P/HF4|
00000010  4c ae 1d 00 00 00 0f 00  00 00 0b 00 00 00 34 6e  |L.............4n|
00000020  75 6d 62 65 72 2e 74 78  74 6e 0d da 0b 3f 5a 17  |umber.txtn ... ?Z.|
00000030  7a 31 0d 51 6a 78 75 c6  03 4a 9d 97 a9 b7 5b fc  |z1.Qjxu..J....[.|
00000040  ea 01 cb 7f a5 4f 50 4b  07 08 46 34 4c ae 1d 00  |.....OPK..F4L ...|
00000050  00 00 0f 00 00 00 50 4b  01 02 1f 00 14 00 09 00  |......PK........|
00000060  08 00 8b 50 2f 48 46 34  4c ae 1d 00 00 00 0f 00  | ... P/HF4L.......|
00000070  00 00 0b 00 24 00 00 00  00 00 00 00 00 20 00 00  |....$.....  ...|
00000080  00 00 00 00 34 6e 75 6d  62 65 72 2e 74 78 74 0a  |....4number.txt.|
00000090  00 20 00 00 00 00 00 01  00 18 00 80 65 27 0e 39  |. ..........e'.9|
000000a0  4f d1 01 65 7a 68 64 f3  4c d1 01 65 7a 68 64 f3  |O..ezhd.L..ezhd.|
000000b0  4c d1 01 50 4b 05 06 00  00 00 00 01 00 01 00 5d  |L..PK..........]|
000000c0  00 00 00 56 00 00 00 00  00                       | ...V.....|
000000c9
```

CSDN @QJ_zjj

3、利用kali中的工具破解压缩包

```
┌──(kali㉿kali)-[~/Desktop]
└─$ zip2john flag.zip > passwd.hash
```

1、zip2john获得中间hash文件

john破解加密的zip包

```
ver 2.0 flag.zip/4number.txt PKZIP Encr: cmplen=29, decmplen=15, crc=AE4C3446

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
```

2、获得hash文件

```
f1fc23f5c743425d9e0073887c846d23  flag.zip  passwd.hash  passwd.txt  QR_code.png  text.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ john passwd.hash
```

3、john破解中间hash文件

```
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
7639             (flag.zip/4number.txt)
1g 0:00:00:06 DONE 3/3 (2022-02-17 01:49) 0.1663g/s 9612Kp/s 9612Kc/s 9612KC/s 08r..7kjr
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

4、破解出密码

CSDN @QJ_zjj

4、利用工具ziperello对压缩包进行解密


Ziperello
ziperello
zip password recovery tool
帮助
关于
退出
加密的 ZIP 压缩包
C:\Users\28290\Desktop\flag.zip
打开
步骤 1
1. 打开 ZIP 压缩包。Ziperello 将读取并显示其中加密的文件。
2. 根据提示选择相应的文件及操作。
3. 点击右侧箭头进入下一步
压缩包中加密的文件列表:
文件名
大小
加密方式
4number.txt
15 b
标准 Zip 2.0
如何复选加密文件?
两点规则:
1. 加密方式相同
2. 密码相同
BACK
步骤 1 / 4: 选择ZIP文件
NEXT
Ziperello ver. 2.1
版权所有 (C) 2008 FDRLab
CSDN @QJ_zjj


Ziperello
ziperello
zip password recovery tool
帮助
关于
退出
当前密码长度
4
当前密码
7639
当前速度
3036294密码/秒
4%
逝去时间: 00:00:00
步骤 4
准备就绪，请点击 [开始] 按钮
注意：搜索进度条 (%) 及剩余时间字段显示的信息与当前的密码效验长度相关。破解 AES 算法加密的密码可能耗时较长。
信息
密码: 7639
确定
14:39:02: 密码: "7639".时间: 1 s
BACK
步骤 4 / 4: 破解密码.Go
NEXT
Ziperello ver. 2.1
版权所有 (C) 2008 FDRLab
CSDN @QJ_zjj

5、解密得到flag