

buuctf misc 二维码

原创

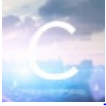
珞珞雨雨 于 2021-02-01 21:06:05 发布 436 收藏 4

分类专栏: [ctf题记](#) 文章标签: [linux](#) [信息安全](#)

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_51462441/article/details/113529214

版权



[ctf题记 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

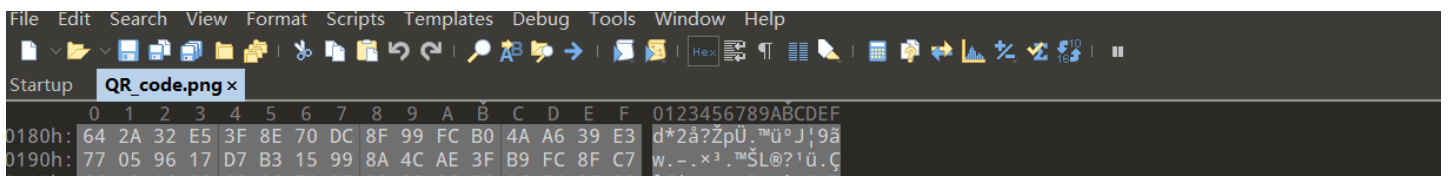
buuctf misc 二维码

下载下题目, 得到了一张二维码图片



扫了一下, 发现啥有用的都没有。。。。。

用010看了一下, 发现这张图片里藏了一点东西



```

01A0h: 6C 43 A6 02 63 96 72 27 33 85 3C E8 9C F6 3C 99  LC;C-F 3...<ew0<
01B0h: 26 8C D7 9A 13 A3 09 B2 FF 3D DB 90 79 93 A1 FE &E×$.£.²ÿ=Û.y"jb
01C0h: 8B 7E 01 B2 1B 8D D5 E6 69 67 86 00 00 00 00 49 <~.².Ûeight....I
01D0h: 45 4E 44 AE 42 60 82 50 4B 03 04 14 00 09 00 08 END@B',PK.....I
01E0h: 00 8B 50 2F 48 46 34 4C AE 1D 00 00 00 0F 00 00 .<P/HF4L@.....
01F0h: 00 0B 00 00 00 34 6E 75 6D 62 65 72 2E 74 78 74 ....4number.txt
0200h: 6E 0D DA 0B 3F 5A 17 7A 31 0D 51 6A 78 75 C6 03 n.Û.?Z.z1.Qjxu£.
0210h: 4A 9D 97 A9 B7 5B FC EA 01 CB 7F A5 4F 50 4B 07 J.-@-[üê.Ë.¥OPK.
0220h: 08 46 34 4C AE 1D 00 00 00 0F 00 00 00 50 4B 01 .F4L@.....PK.
0230h: 02 1F 00 14 00 09 00 08 00 8B 50 2F 48 46 34 4C .....<P/HF4L
0240h: AE 1D 00 00 00 0F 00 00 00 0B 00 24 00 00 00 00 @.....$.
0250h: 00 00 00 20 00 00 00 00 00 00 00 34 6E 75 6D 62 ...4numb
0260h: 65 72 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 er.txt.....
0270h: 18 00 80 65 27 0E 39 4F D1 01 65 7A 68 64 F3 4C ..€e'.90Ñ.ezhdóL

```

Template Results - PNG.bt ↗

Name	Value	Start	Size	Color	Comment
struct PNG_SIGNATURE ...		0h	8h	Fg: Bg:	
struct PNG_CHUNK chu...	IHDR (Critical,...	8h	19h	Fg: Bg:	
struct PNG_CHUNK chu...	PLTE (Critical,...	21h	12h	Fg: Bg:	
struct PNG_CHUNK chu...	IDAT (Critical,...	33h	198h	Fg: Bg:	
struct PNG_CHUNK chu...	IEND (Critical,...	1CBh	Ch	Fg: Bg:	
struct PNG_CHUNK chu...	␣ (Critical, Pu...	1D7h	0h	Fg: Bg:	

Output

https://blog.csdn.net/qq_51462441

看到了zip文件格式的文件头：504B0304

当然，如果只觉得藏了东西却看不出是什么，可以用kali上的binwalk命令尝试分离

```

(root@kali)~[~/桌面]
# binwalk QR_code.png

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, compressed size: 29, uncompressed
size: 15, name: 4number.txt
650          0x28A          End of Zip archive, footer length: 22

```

emmmmmm，藏了一个zip格式的压缩包和一个txt文件

用binwalk命令生成分离的文件

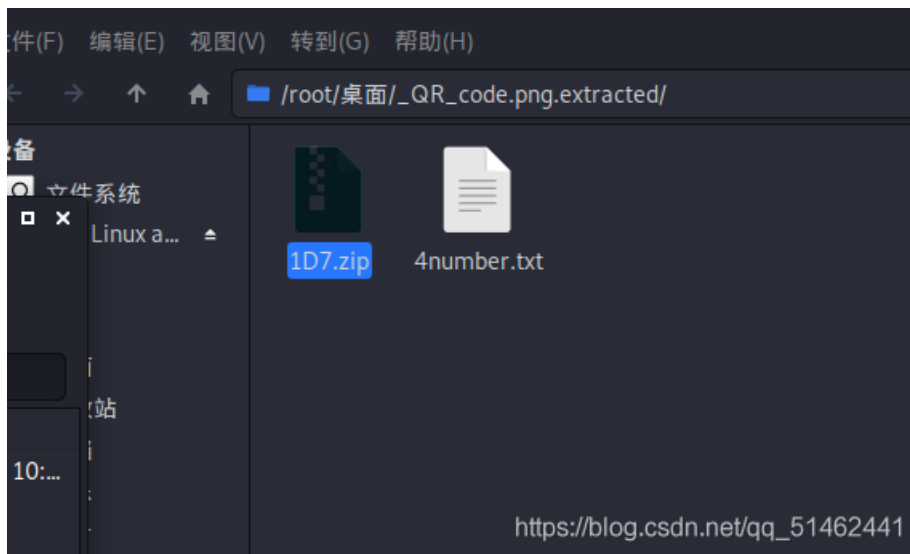
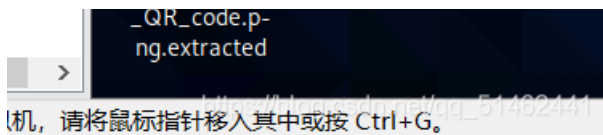
```

(root@kali)~[~/桌面]
# binwalk -e QR_code.png

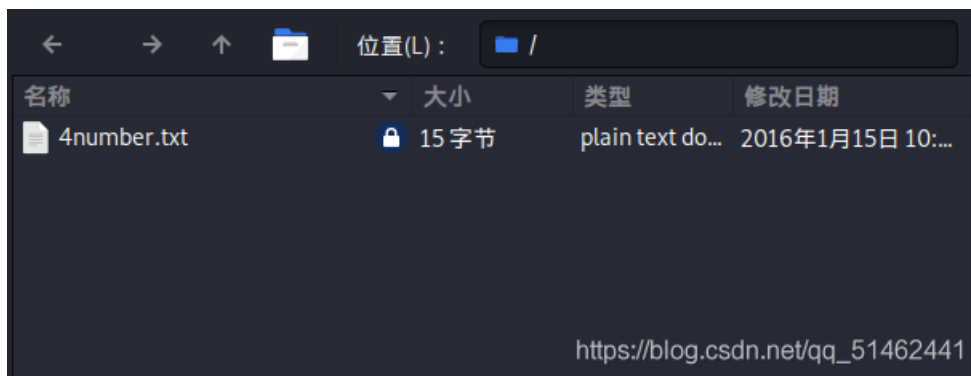
DECIMAL      HEXADECIMAL     DESCRIPTION
-----
0             0x0             PNG image, 280 x 280, 1-bit colormap, non-interlaced
471          0x1D7          Zip archive data, encrypted at least v2.0 to extract, compressed size: 29, uncompressed
size: 15, name: 4number.txt
650          0x28A        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

```

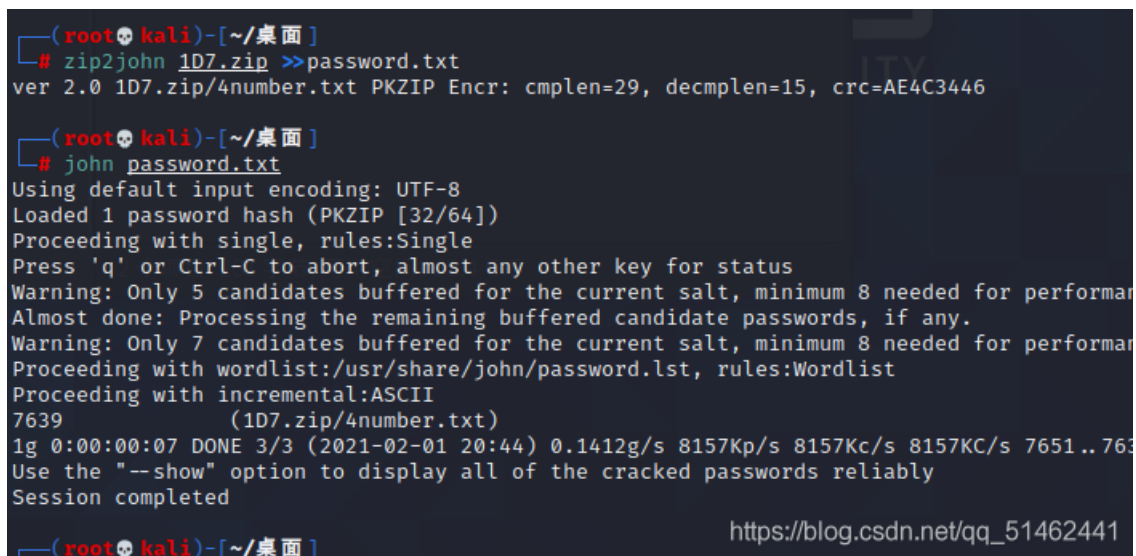




txt文本啥都没有，压缩包里还有个加密的txt文本，看名字应该是四位密码。



这里我就尝试用kali的zip2john来破解。走一波



成功得到四位密码：7639

然后我们就可以优雅地打开文本得到flag