

BuuCTF 九连环

原创

Kevin_xiao~ 于 2021-08-13 18:49:22 发布 66 收藏

分类专栏: [CTF题目\(misc\)](#) 文章标签: [安全](#) [压缩包](#) [隐写](#)

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_52907838/article/details/119681981

版权



[CTF题目\(misc\)](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

下载附件, 是一个加密压缩包, 放进010editor, 发现是伪加密:

```
起始页 00000038 - Copy.zip* X
编辑方式: 十六进制(H) 运行脚本 运行模板: ZIP.bt
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
7060h: A3 C1 BA 4D A1 2A 54 6D 76 5C 01 39 EE AA 42 ED fÃ°Mj*Tmv\.9i*Bï
7070h: 41 F5 81 DC 15 0B 05 70 76 5D 86 9B 61 F2 E1 E5 Aõ.Ü...pv]†>aóáá
7080h: F6 5D 48 C6 1B 95 84 0F E5 87 EF A1 3F AF 70 74 ö]HE.°.ã+i;?~pt
7090h: E2 88 97 D3 27 F8 ED C7 9D C9 B6 80 33 E5 8C 7E á^-Ó'øiÇ.Éq€3ã€~
70A0h: 8A 34 16 4D AC AC CB 7C D7 98 28 D5 51 57 D5 F0 Š4.M-→E|x~(ÖQWÖš
70B0h: A5 D7 CB FD 6C FC 37 81 67 23 D1 32 59 0F 33 B0 ¥*Ëýlú7.g#Ñ2Y.3°
70C0h: A7 78 22 71 B5 D1 FD 60 24 03 34 56 7F 5C C5 F0 Sx"quñý`$.4V.\Áš
70D0h: DB 4A 0A B2 5E FD BF 5D BB 40 31 26 FE 5F 50 4B ŪJ.^`ý¿]»@l&p_PK
70E0h: 03 04 0A 00 00 08 00 00 F1 52 53 4B D3 13 C6 E0 .....ñRSKÓ.Èà
70F0h: B8 00 00 00 B8 00 00 00 0B 00 00 00 61 73 64 2F .....asd/
7100h: 71 77 65 2E 7A 69 70 50 4B 03 04 0A 00 01 08 00 gwe.zipPK.....
7110h: 00 8E 4E 53 4B 8A C4 35 B6 22 00 00 00 16 00 00 .ŽNSKŠÅ5q".....
7120h: 00 08 00 00 00 66 6C 61 67 2E 74 78 74 A7 A0 9B .....flag.txt$ >
7130h: A6 BC 37 21 E7 B0 A7 B4 E2 22 B9 1A 43 31 BB C4 |47!ç°š`á"².C1»Ä
7140h: 33 37 FD B7 17 B5 6D A1 FC F0 1D 10 E9 C9 56 50 37ý.µm;üš..éÉVÉ
7150h: 4B 01 02 3F 00 0A 00 01 08 00 00 8E 4E 53 4B 8A K..?.....ŽNSKŠ
7160h: C4 35 B6 22 00 00 00 16 00 00 08 00 24 00 00 Å5q".....$.
7170h: 00 00 00 00 00 20 00 00 00 00 00 00 66 6C 61 .....fla
7180h: 67 2E 74 78 74 0A 00 20 00 00 00 00 01 00 18 g.txt.....
7190h: 00 29 39 FE E9 7C 48 D3 01 D9 46 44 DC 7C 48 D3 .)9pé|HÓ.ÜFDÜ|HÓ
71A0h: 01 D9 46 44 DC 7C 48 D3 01 50 4B 05 06 00 00 00 .ÜFDÜ|HÓ.PK....
71B0h: 00 01 00 01 00 5A 00 00 00 48 00 00 00 00 00 50 .....Z...H....P
71C0h: 4B 01 02 3F 00 0A 00 00 08 00 00 AE 54 53 4B 00 K..?.....@TSK.
71D0h: 00 00 00 00 00 00 00 00 00 00 04 00 24 00 00 .....$.
71E0h: 00 00 00 00 00 10 00 00 00 00 00 00 61 73 64 .....asd
71F0h: 2F 0A 00 20 00 00 00 00 00 01 00 18 00 69 B8 48 /...i.H
7200h: 34 83 48 D3 01 69 B8 48 34 83 48 D3 01 E9 7C 39 4fHÓ.i.H4fHÓ.éüY
7210h: 31 83 48 D3 01 50 4B 01 02 3F 00 14 00 08 08 lfHÓ.PK..?.....
7220h: 00 48 4E 53 4B 8C 3A D5 7E 88 70 00 00 28 45 77 https://blog.csdn.net/qq_52907838/article/details/119681981
7230h: 00 16 00 24 00 00 00 00 00 00 00 20 00 00 00 22 .....$....."
```

解压得到一张图片和一张加密压缩包, 又将图片放进010editor, 不是伪加密, 那就应该是要用图片得到密码。

图片用foremost分不出, 用steghslove发现也不是lsb隐写, 图片长宽也没问题, 那还有什么方法在图片里藏信息呢?

还有一种方法就是用steghide

下载地址: <https://sourceforge.net/projects/steghide/>

用法:

- 1.查看已嵌入目标文件的图片的文件信息 `steghide info filename`
- 2.可以提取图片或者音频的隐藏文件 (如果没有密码的话 `-p` 命令可以不用) `steghide extract -sf filename -p password`

此题没告诉密码，空密码就行。

看到这个图片就是压缩包的密码：

bV1g6t5wZDJif^|7

得到答案。