

2020新春战疫ctf公益赛——Misc套娃

原创

Sparrow_Y 于 2020-03-03 21:01:36 发布 1780 收藏 5

分类专栏: [ctf](#)

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/weixin_43491669/article/details/104639593

版权



[ctf 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

一看套娃就能猜到会是一个繁琐的题目, 从压缩包里放着压缩包可以猜测整个题目的过程中寻找压缩包密码是一条主线。

第一层

很明显的txt里边Ook的加密, 解密便得到压缩包2的密码。

```
dcaf03aa88d038686c5e8067a7a45ff8
```

Text to Ook! | Text to short Ook! | Ook! to Text

Text to Brainfuck | Brainfuck to Text

https://blog.csdn.net/weixin_43491669

brainfuck/Ook解密

但是还给了一张图片, 按着处理图片的步骤看属性, winhex打开。。。略, 个人比较喜欢一个叫Hxd的工具, 跟winhex功能是差不多的, 打开图片后发现最末尾出现了part1一串字符, 后边应该会用到。

```
0005B480  A0 74 E4 EF F6 BB FD 6E BF DB EF F6 BB FD 6E BF  ta1o>yn¿U1o>yn¿
0005B490  DB DF D9 FE OF A7 0E 85 27 60 EF OF 5B 00 00 00  ŪŪp.$...'`i.[...
0005B4A0  00 49 45 4E 44 AE 42 60 82 70 61 72 74 31 3A 30  .IEND@B`,part1:0
0005B4B0  36 38 63                                           68c
```

第二层

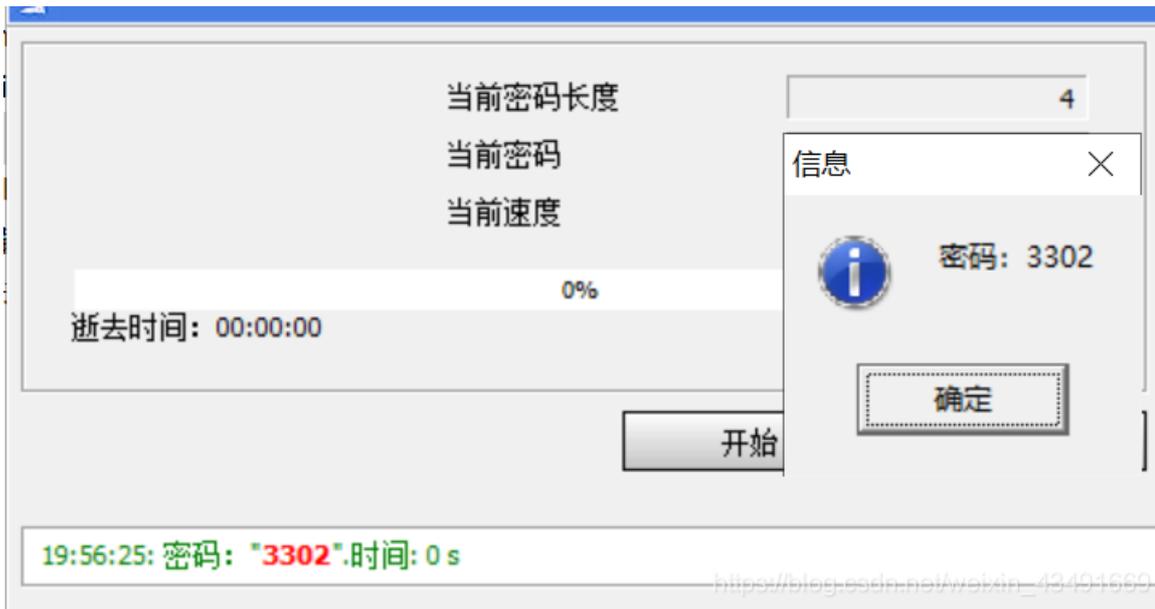
第二层只有一张图片, 扫上边的码没有东西, 还是先看属性, 发现了part2, 到这里有了大致的思路, 每一层都是一边解压缩包, 一边找part的内容。

分级 ☆☆☆☆☆

标记

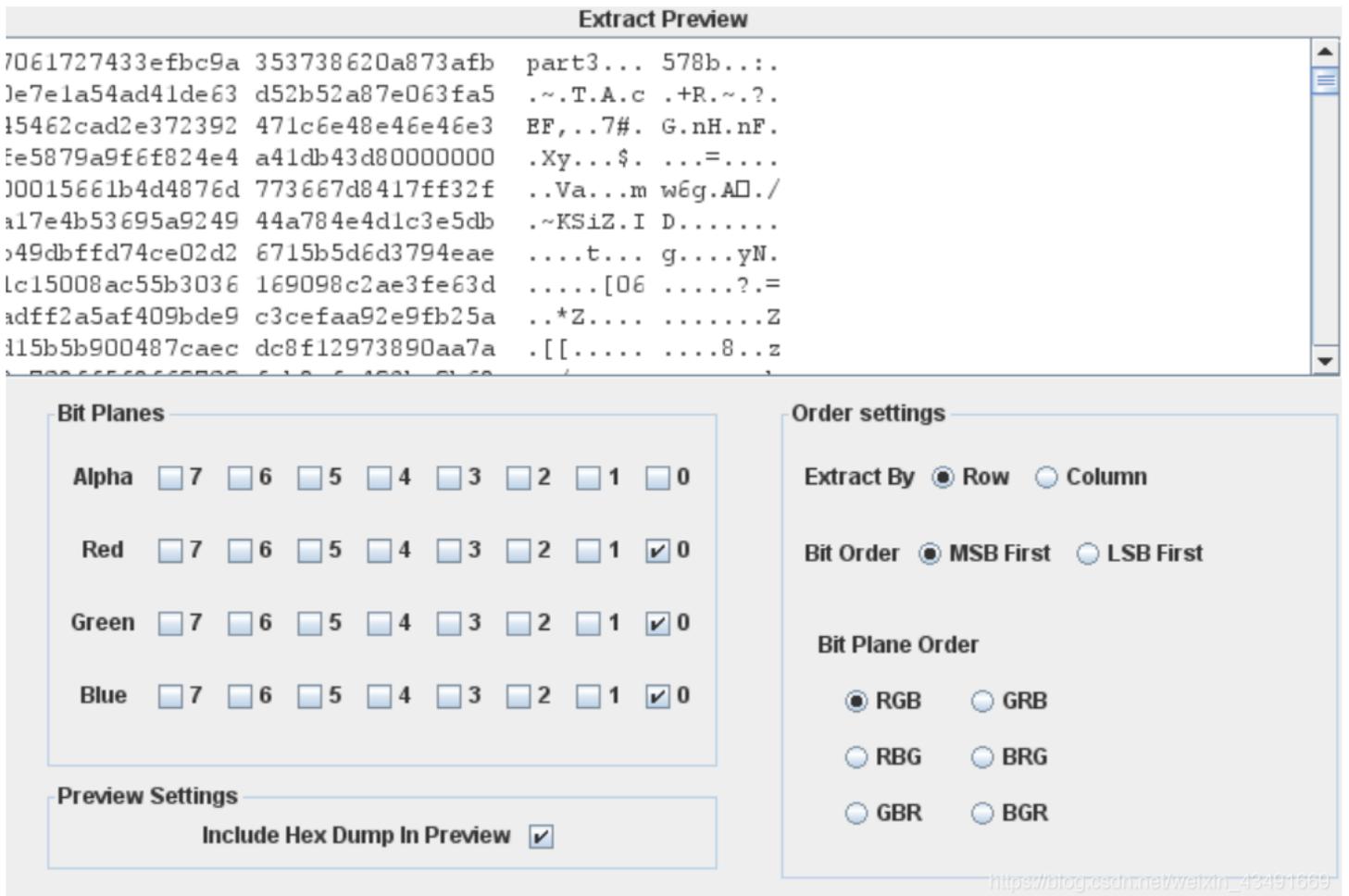
备注 part2: 555b

这一层没有压缩包的提示，于是就去爆破试一下。



第三层

第三层仍然只有一张图片，基本操作试过之后没有发现什么东西，接着上LSB，工具打开后常规的RGB为0先看一下



这一层也仍然没有压缩包的提示，压缩包就那几种解密方式，爆破用了，看看是不是伪加密，Hxd打开找到504B0102标记头，其后的全局方式位标记是0900，果然是，改为0000保存即可。

PS: 7z可以直接打开伪加密的压缩包

```
002C1EF0 E4 F9 99 0D C0 9B C4 BF 2C 04 94 E2 5A 00 96 3F
002C1F00 31 7F 5B AE 42 05 65 FE 7E 6D FD BF DF CB 66 82
002C1F10 FF 8F 85 99 DA D9 D8 F2 EF 6F DF 8A 8F 24 E7 5D
002C1F20 00 7C 6F 5A 46 02 1C E2 D7 BF 51 7A FA 73 41 0D
002C1F30 04 14 72 FD B4 FF 03 FA 7F 50 4B 01 02 1F 00 0A
002C1F40 00 09 00 00 00 02 8F 44 50 00 00 00 00 00 00
002C1F50 00 00 00 00 00 02 00 24 00 00 00 00 00 00 10
002C1F60 00 00 00 00 00 00 00 34 2F 0A 00 20 00 00 00
002C1F70 00 01 00 18 00 92 2C 60 50 41 DB D5 01 92 2C 60
002C1F80 50 41 DB D5 01 48 39 A9 26 39 DB D5 01 50 4B 01
002C1F90 00 1F 00 14 00 00 00 00 00 01 04 40 50 11 07 04
```

第四层

这一层的内容比较多，首先看到一张提示图片，显示把4.jpg压缩，而压缩包里也有一张4.jpg，很明显是明文攻击了，用ARCHPR工具跑就行，这里要注意的是开始之后会耗费大约一个半小时找回口令，其实不用等着结束，直接停止，会让保存另一个压缩包，跟要解密的是相同的，可直接打开。



5.zip

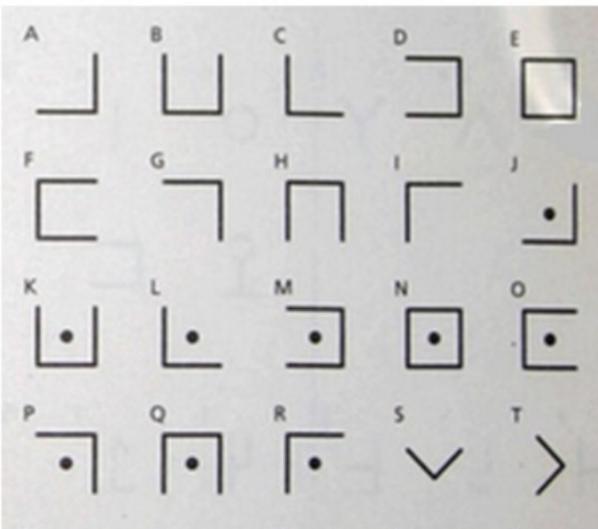
5_decrypted.zip

还剩一张图片，正常的骑车地图下边会显示扫码骑车，改一下高度看看，发现了part4



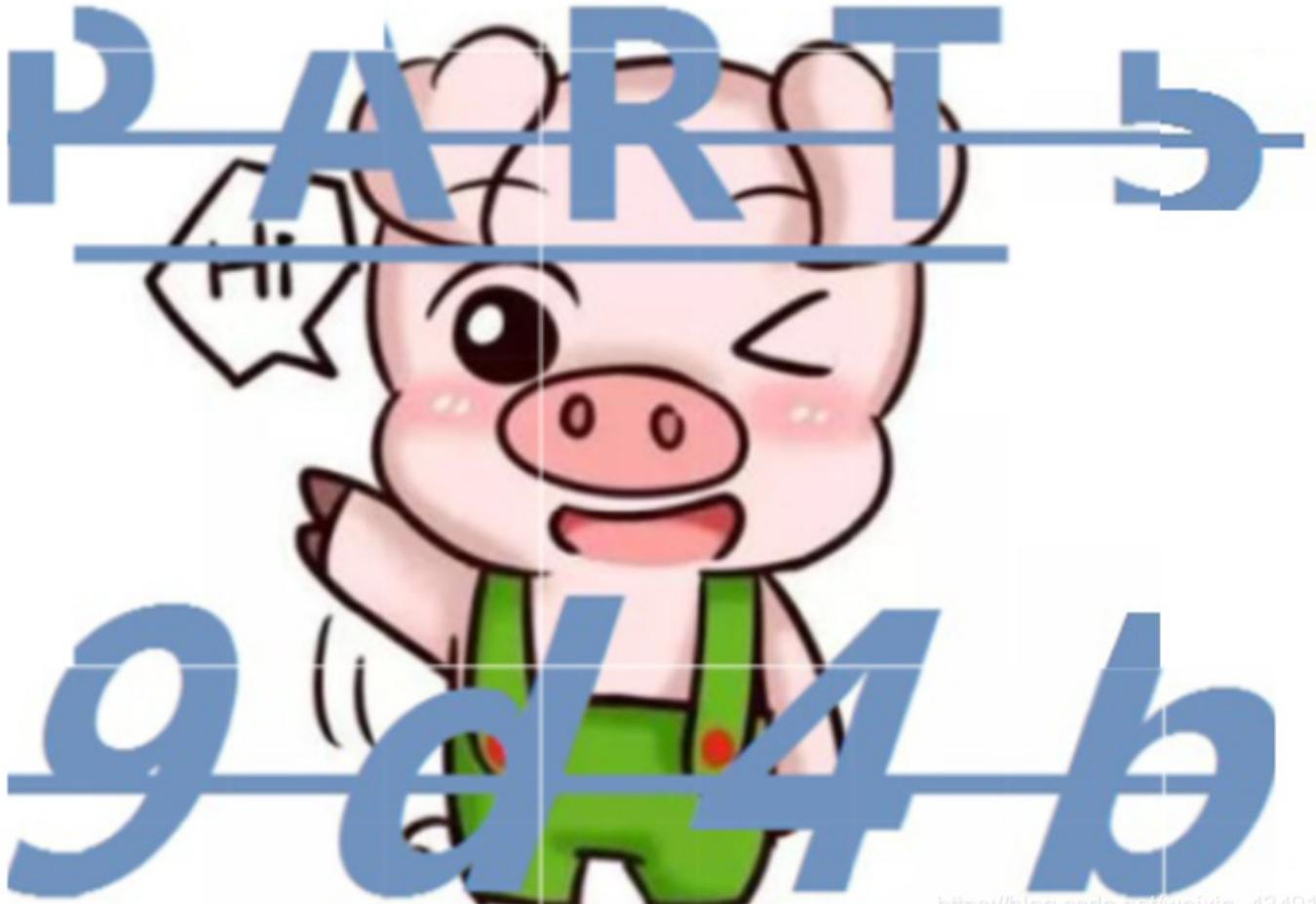
第五层

这一层是猪圈密码，附上对照表，对应解压缩包即可（压缩包密码需要小写）





另一个文件夹里是一大堆图片，一看需要拼图，很头大，目前也没有很好用的拼图工具，大家有的话可以评论区分享一下，最后是这样的。



https://blog.csdn.net/weixin_43491669

第六层

这一层的图片常规操作后发现了摩斯，解密得到part6

```

00005D50 44 40 11 11 00 44 44 01 11 10 04 44 40 11 11 01 D@...DD...D@...
00005D60 FF D9 2E 2D 2D 2E 2F 2E 2D 2F 2E 2D 2E 2F 2D 2F yù.--./.-/.-./-/-
00005D70 2D 2E 2E 2E 2E 2F 2D 2D 2D 2E 2E 2E 2F 2E 2F 2E -.../---..././
00005D80 2E 2E 2E 2E 2F 2E 2E 2D 2D 2D 2F 2D 2E 2E 2E 2E .../..---/-.../
00005D90 2D 2E 2E 2F 2D 2E 2E 2E 2E 2F 2D 2D 2E 2E 2E -.-/-.../---...

```

.- ./.-./.-/.../---..././.../---/-.../.-./-.../---...

[生成摩斯密码](#) [解密摩斯密码](#) [清空结果](#)

PART 6 %u38E52BD67| https://blog.csdn.net/weixin_43491669

txt里边是与佛论禅加密，要注意在解密内容前加佛曰

与佛论禅

amt12345

[听佛说宇宙的真谛](#) [参悟佛所言的真意](#) [普度众生](#)

一花一世界，一叶一如来

佛曰：曰罰醯鉢夢冥無鉢特冥。提罰不是怯羯俱孕帝穆罰遠奢大勝俱諸冥滅得滅怯怖波栗俱耨姪漫俱上吶無尼尼吶喝俱恐

与佛论禅

第七层

图片是银河语言，在bugku中也出现过，附上对照表，对应过来即可解压缩包。



对于gif，除了一帧帧的看内容，还可以用identify命令提取内容。

```
~/ctf/Misc$ identify -format "%T" 7.gif  
102020201010101010202010101010201020202010102010102020102010101010202010202020  
10102020201020101010202010102020101010201010202010201010202010202010202010  
~/ctf/Misc$
```

10 变为0，20变为1，转ASCII码即可得part7

ASCII在线转换器-十六进制，十进制、二进制

ASCII转换到 ASCII (例: a b c)

p a r t 7 : 6 1 5 6 2

第八层

文本提示需要32位的战利品，7个part正好32位，直接打开压缩包9，进入最后一层。

第九层

NT和FA，杂项里边有关联的应该是ntfs流隐写，直接ntfsstreamseditor工具打开，flag就出现了。

Name	Size	Type	Date Mo...
flag.txt	1	Alternat...	2020/2/...

flag {8739459c-8d4e-4a34-92ee-5d75ae56ac4f}