2019年山东省深思杯网络安全大赛

原创

皮皮皮皮皮皮皮虾 于 2019-11-04 23:16:58 发布 1582 收藏 7

分类专栏： CTF 文章标签： 2019年山东省网络安全大赛

本文链接：https://blog.csdn.net/qq_43559371/article/details/102907525

刚参加完比赛，总结一波。

第一题:签到题

```
6C 69 62 67 63 6A 2D 31  36 2E 64 6C 6C 00 5F 4A  libgcj-16.dll _J
76 5F 52 65 67 69 73 74  65 72 43 6C 61 73 73 65  v_RegisterClasse
73 00 00 00 57 65 6C 63  6F 6D 65 20 74 6F 20 73  s   Welccme to s
64 6E 69 73 63 20 21 00  66 6C 61 67 7B 31 32 61  dnisc ! flag{12a
62 38 32 63 64 36 38 36  61 34 32 38 35 30 61 62  b82cd686a42850ab
35 36 32 66 66 32 66 39  66 32 34 31 36 7D 00 00  562ff2f9f2416}
```

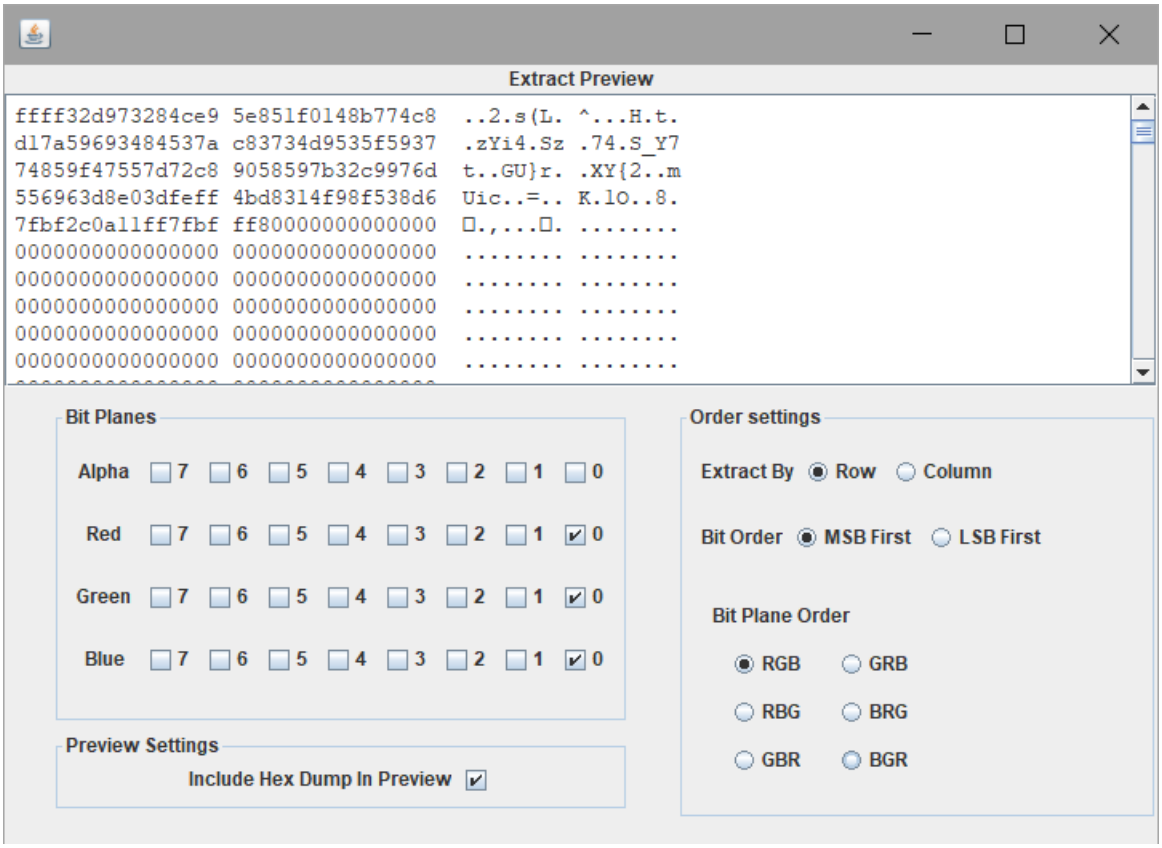
下载完成之后发现是个.exe文件 杂项万年套路步骤,用winhex打开，搜索flag，找到，提交。。。

第二题：qiu咪

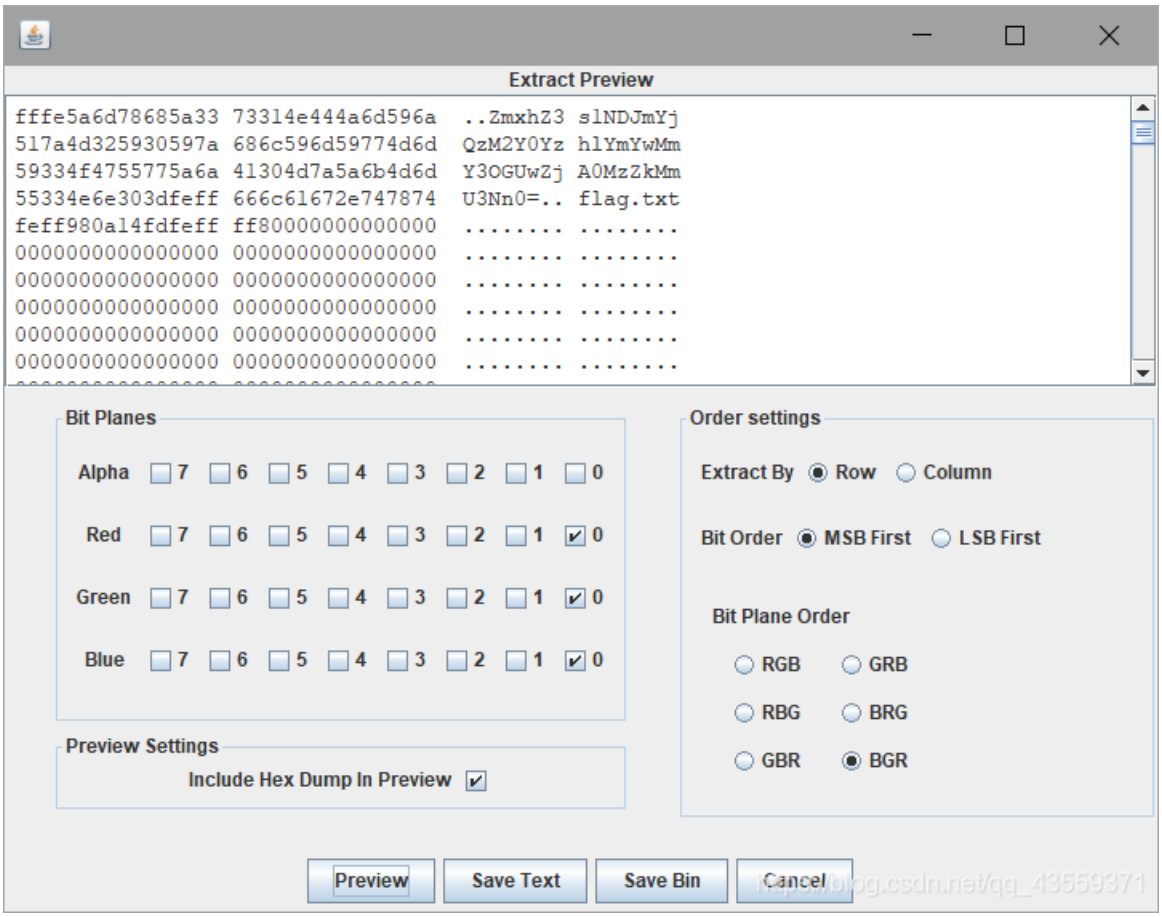
发现是一张flag.png。。万年套路 用winhex打开。啥也没发现，然后放在kali里边 binwalk一下，也没发现有隐藏信息。。

用了隐写图片神器(stegsolve.jar)发现在red plan 0、blue plan 0 green plan 0有跟摩斯密码似的东西。。

那就放在低通道看看里边的信息



没发现什么东西 仔细想了想 信息肯定是隐藏在这里，当把bit plan order 调到BGR时 好消息 发现了base64解码提交。。



第三题：上上下下

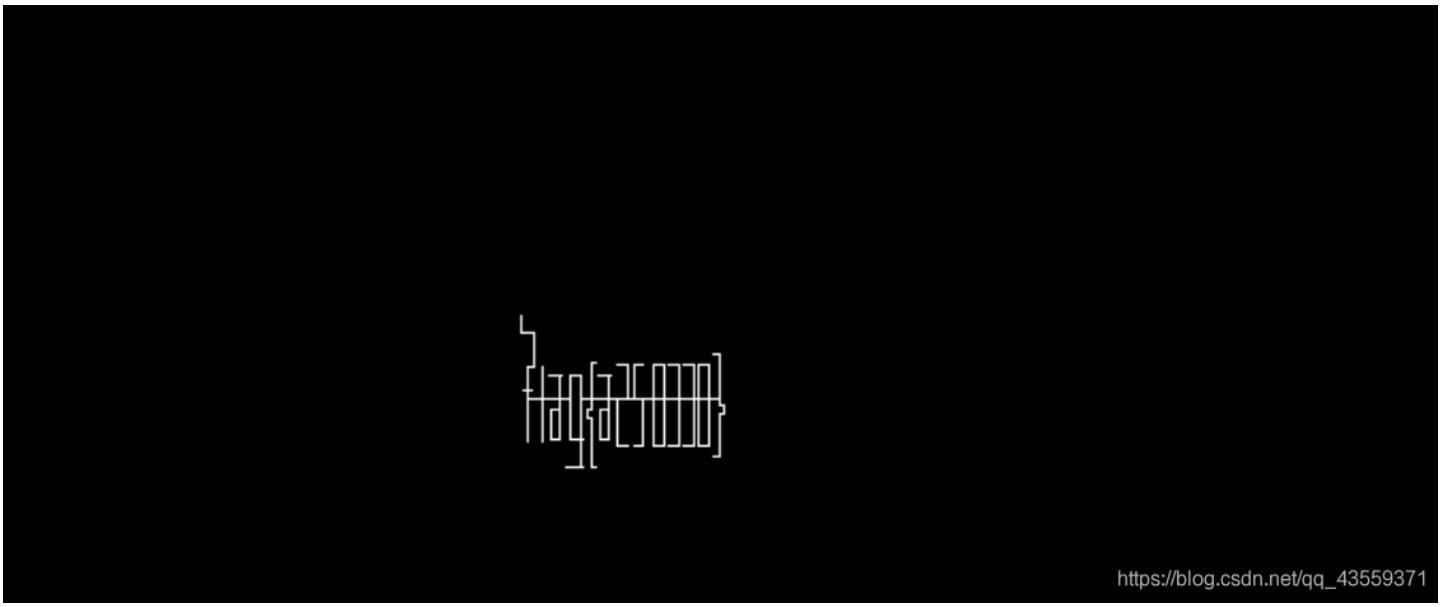
下载完成之后 打开发现是 上下左右英文字母的首字母大写

常规一波之后(用工具)没有发现什么有价值的东西，想肯定不是那么做

突然想到python中俗称"海龟"库画图时 不就是控制画笔上下左右来进行绘画嘛

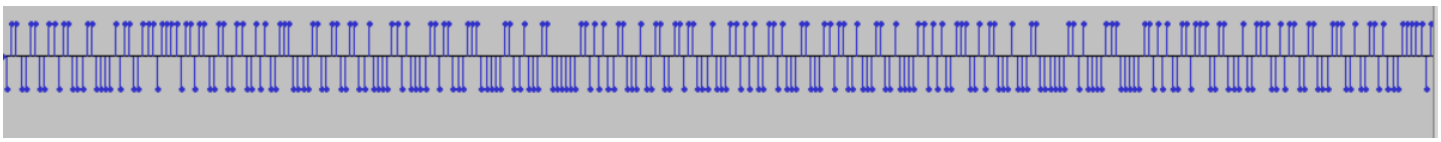
那肯定是用程序把他画出来，用纸笔画了一下发现像个F，猜想画完肯定是flag(动手写程序呗）(偷偷参考了一下鑫哥的wp 不是太明白 为啥要用两个值来画图）

```
from PIL import Image
im = Image.new('RGB',(1000,1000),'black')
 #把flag中的字母读出来
file = open('flag.txt')
line = file.readline()
a = [300,300] #起始位置
#把flag[0]当做左右移动 flag[1]当做上下移动
for i in line:
    if i == 'D':
        a[1] = a[1]+1
    if i == 'U':
        a[1] = a[1]-1
    if i == 'R':
        a[0] = a[0]+1
    if i == 'L':
        a[0] = a[0]-1
    im.putpixel(a ,(255,255,255)) ## putpixel是通过坐标点来进行画图
##刚开始是按照惯例 让i == 'u' +1 画出来是个倒立的图形 所以只能让 'D'+1
im.show()
```



第四题：我和我的祖国

下载打开 发现是音乐的隐写(我又开始常规一波) 用audacity软件打开



在最后发现了这段帧跟别的帧有n大的区别

可以看出有点像高低电平 通俗知识 一般把高电平当做1 低电平当做0 所以尝试二进制转化为字符串一波（以上0 1 代码手打 有更好的方法 欢迎推荐 ）

```
#a = [0b01100110, 0b01101100, 0b01100001, 0b01100111, 0b01111011, 0b01000110, 0b01110101, 0b01001110, 0b01011111
, 0b01100111, 0b01101001, 0b01000110, 0b01111101]
a = "01100110011011000110000101100111011110110110011001100101001110000110011001100100001101000011011000111000001
1001000110000000110101001100010011001101100010001101010011010001100011011001000110010000110101001110010110001000
1000000110100001110000011010100110111001100010011100101100110000111001001101000111101"
b = ""
## 统计一下a的长度 二进制转化为ascii码字符串  8为看成一个整体，看能否被8除尽
print(len(a))
lens = int(len(a)/8)
for i in range(0,lens):
    b = b+chr(int(a[i*8:i*8+8],2))
print(b)
```

第五题：压缩包的秘密

下载完成打开发现是个损坏的压缩包

用winhex打开看了一下

flag.zip

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	4B	50	04	03	00	14	00	09	00	08	72	D7	4F	55	43	9F	KP r×OUCŸ
00000010	46	CE	00	34	00	00	00	26	00	00	00	08	00	00	6C	66	FÎ 4 & lf
00000020	67	61	74	2E	74	78	C2	1C	1A	F9	38	0F	7F	03	C9	62	gat.txÂ ù8 Éb
00000030	F5	3B	ED	1B	53	85	CA	59	52	70	F3	4D	7C	25	4B	8F	õ;í S…ÊYRpóM|%K
00000040	C9	2A	76	A1	15	C9	98	00	EF	AA	55	BF	06	4F	F3	E3	É*v¡ É˜ ïªU¿ OóÃ
00000050	7E	7C	F8	43	E7	67	B1	DB	81	3A	4B	50	08	07	43	9F	~|øCçg±Û :KP CŸ
00000060	46	CE	00	34	00	00	00	26	00	00	4B	50	02	01	00	1F	FÎ 4 & KP
00000070	00	14	00	09	00	08	72	D7	4F	55	43	9F	46	CE	00	34	r×OUCŸFÎ 4
00000080	00	00	00	26	00	00	00	08	00	24	00	00	00	00	00	00	& $
00000090	00	20	00	00	00	00	00	00	6C	66	67	61	74	2E	74	78	lfgat.tx
000000A0	00	0A	00	20	00	00	00	00	00	01	00	18	44	B9	F4	F3	D¹ôó
000000B0	87	D7	01	D5	39	04	C2	16	85	51	01	D5	39	04	C2	16	‡× Õ9 Â …Q Õ9 Â
000000C0	85	51	01	D5	4B	50	06	05	00	00	00	00	00	01	00	01	…Q ÕKP
000000D0	00	5A	00	00	00	6A	00	00	00	80	0D	09	20	0A	20	20	Z j €
000000E0	0D	20	20	0A	0A	0D	09	20	0D	20	20	0A	0A	0D	20	09	
000000F0	20	20	09	20	0A	0D	20	20	0A	0D	20	20	0D	20	09	0A	
00000100	20	20	20	20	0D	09	20	0A	20	20	0D	20	20	0A	0D	09	
00000110	20	0A	20	09	0D	20	20	0A	09	20	0D	20	09	0A	20	20	
00000120	20	20	0D	09	20	0A	09	09	0D	20	20	0A	09	09	0A	0D	
00000130	20	09	0D	20	09	0A	20	20	20	20	0D	09	20	0A	20	20	
00000140	0A	0D	20	09	0D	20	09	0A	0D	20	20	0A	0D	20	20	0A	
00000150	20	20	0A	0D	20	09	20	09	0A	0D	47	64	6C	68	6D	63	Gdlhmc
00000160	74	55	58	61	74	4D	47	61	73	46	69	5A	77	31	32	64	tUXatMGasFiZw12d
00000170	74	51	32	63	6C	68	6E	62	70	4E							tQ2clhnbpN

打开一看 第一行 是 4B 50 04 03 zip压缩包的开头不应该是(50 4B 03 04)

有猫腻 而且里边的lfgat.xt 经过两两互换之后成了 flag.txt,而且在最底下是base64 去解码也没有成功 猜想是不是所有的都是两两互换 就尝

试了一下把最底下的base64互换一下 看能否解码成功 如果能就代表猜想正确

互换之后的base64:(dGhlcmUtaXMtaGFsZi1wd2Qtc2hlbnNp)

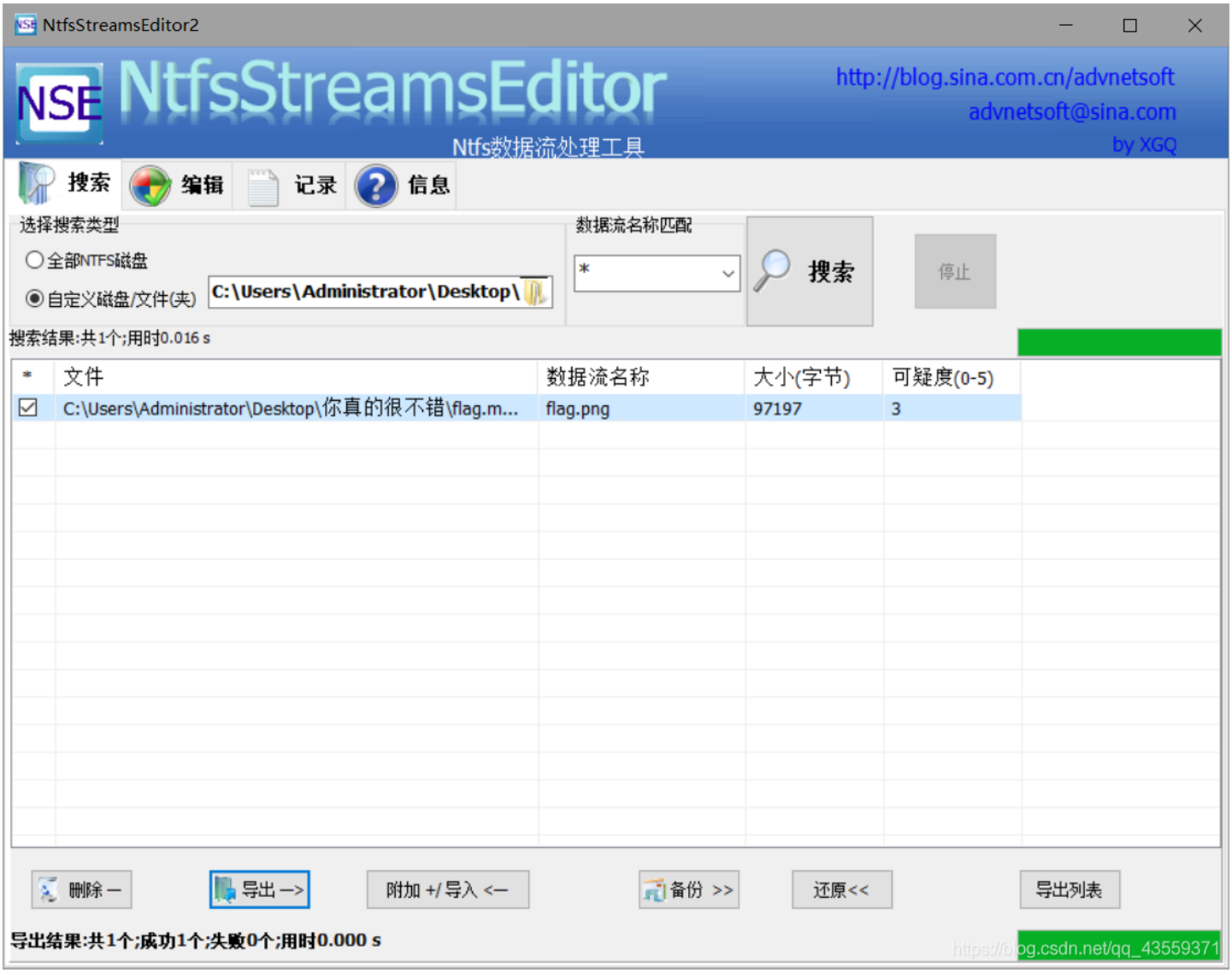
解码为：there-is-half-pwd-shensi说明猜想成功

下边就把全部的两两互换 在比赛的时候 (手撕 生换)(…)可以写脚本跑出来…

打开发现需要密码 但是我们已经知道一半密码。。用掩码攻击的到另一半密码:sdnisc 输入密码拿flag

第六题： 你真的很不错

提示用winrar解压 想到可能是ntfs数据流



发现一张flag.png 导出 提交

简单的密码

hellO，everyone Are YOU huNGrY woUld you like To eAt BAcon?

题目为一个英语句子 但是在后边提示bacon 所以想到的是培根密码解密

培根密码有两种

所以我们尝试一下 看那种对

第一种 把小写字母转化为a 大写字母转化为b

```
#coding=utf-8
#转化为小写字母 小写字母对应大写铭文
a = "hellOeveryoneAreYOUhuNGrYwoUldyoulikeToeAtBAcon"
count = ""
for i in a:
    if ord(i) >= 97 and ord(i) <= 122:
        i = "a"
        count += i
    else:
        i = "b"
        count += i
b = len(count)//5
for i in range(b):
    print count[i*5:i*5+5]
```

输出为
aaaaa
aaaba
abbba
abbab
aabaa
在线工具解密即可
另一种是把小写字母转化为A 大写字母转化为B

```
#coding=utf-8
#转化为大写字母 大写字母对应小写铭文
a = "hellOeveryoneAreYOUhuNGrYwoUldyoulikeToeAtBAcon"
count = ""
for i in a:
    if ord(i) >= 97 and ord(i) <= 122:
        i = "A"
        count += i
    else:
        i = "B"
        count += i
b = len(count)//5
for i in range(b):
    print count[i*5:i*5+5]
```

输出为
AAAAB
AAAAA
AAABA
ABBBA
ABBAB
AABAA
AAAAA
AABAA
BABBA
也在线解密即可