

# 攻防世界misc高手进阶篇教程（1）

原创

锋刃科技 于 2020-05-24 16:46:14 发布 1904 收藏 5

文章标签: 攻防世界 ctf

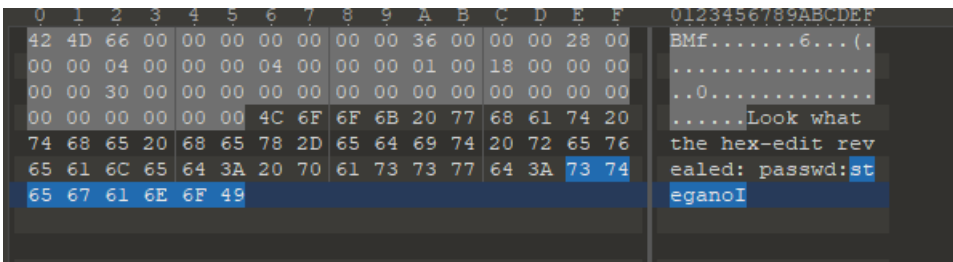
版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/xuandao\\_ahfengren/article/details/106316990](https://blog.csdn.net/xuandao_ahfengren/article/details/106316990)

版权

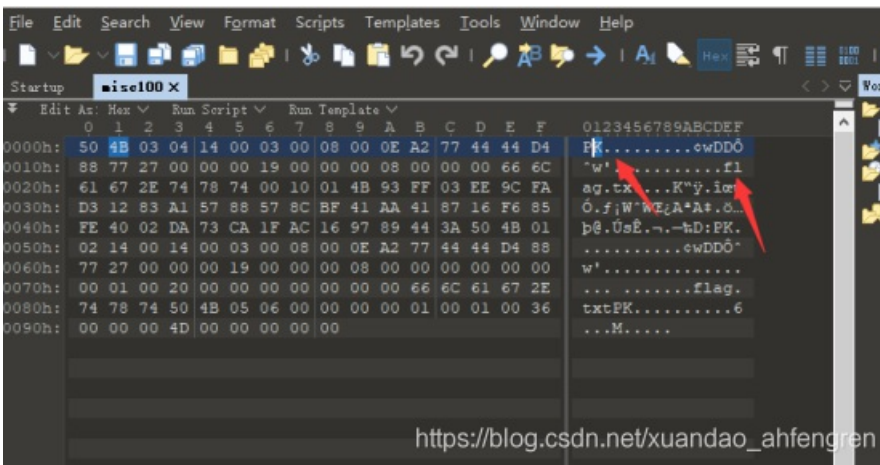
## Training-Stegano-1z

直接用winhex打开即可

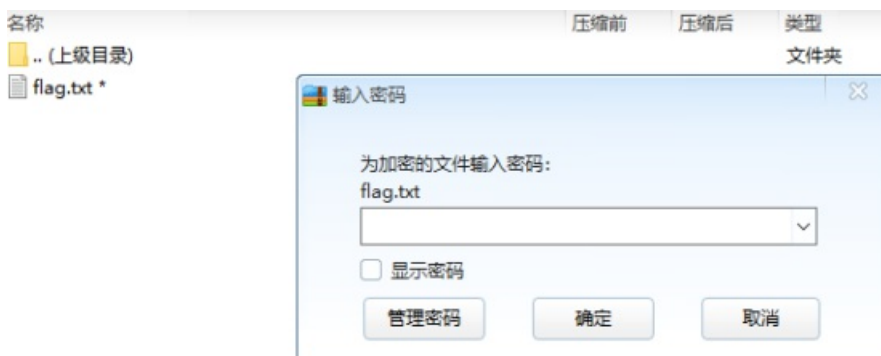


## János-the-Ripper

用winhex打开发现flag.txt和PK头, 也就是压缩包嘛, 直接保存为zip打开



发现需要密码



用ARCHPR爆破密码



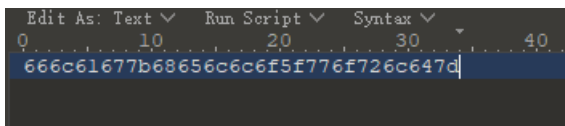
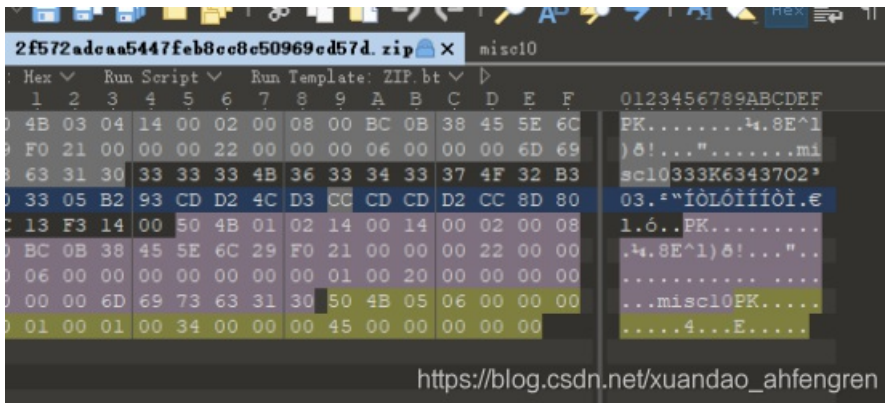
密码为fish

打开既有flag



## Test-flag-please-ignore

用winhex打开里面有misc10文件，打开misc10发现疑似十六进制的文本



转换即可

加密或解密字符串长度不可以超过10M

666c61677b68656c6c6f5f776f726c647d

16进制转字符

字符转16进制

清空结果

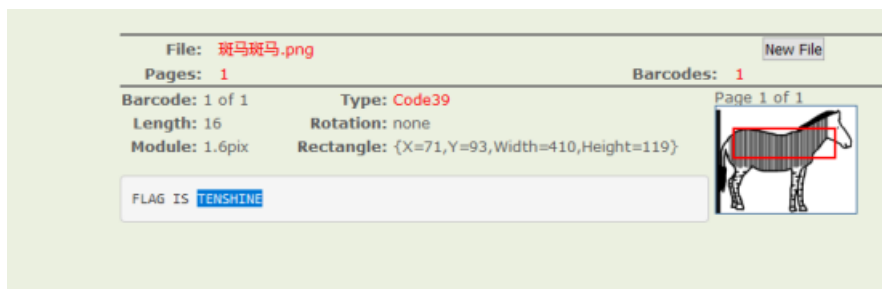
flag{hello\_world}

[https://blog.csdn.net/xuandao\\_ahfengren](https://blog.csdn.net/xuandao_ahfengren)

## Banmabanma

<https://online-barcode-reader.inliteresearch.com/>

用在线工具进行扫描即可获得flag，加上flag格式直接提交



flag{TENSHINE}

## Hear-with-your-Eyes

下载完附件之后，进行解压，然后把后缀名修改成gz再解压，还是修改成gz后缀解压之后就是音频文件了



用打开Audacity

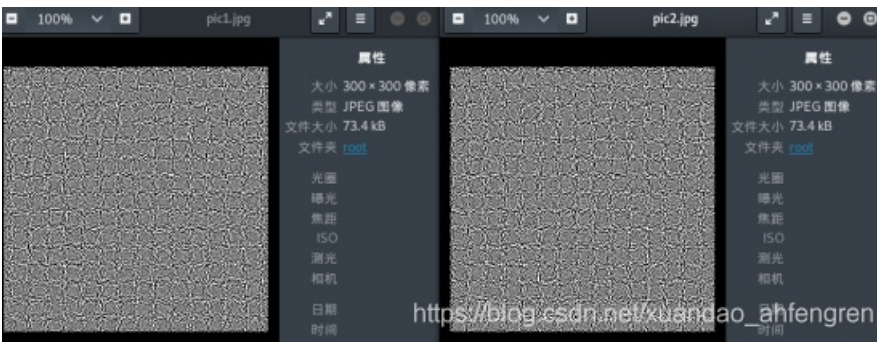
用频谱图打开即可



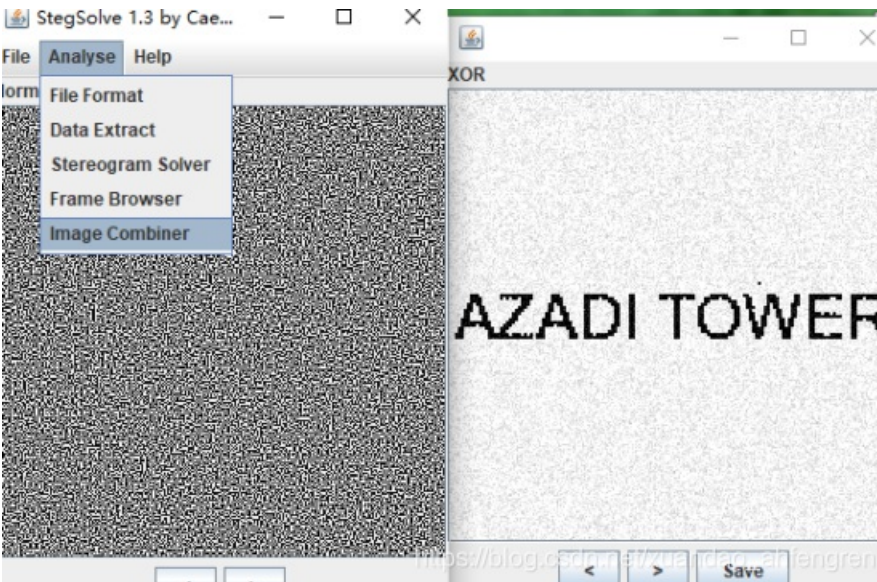
## What-is-this

先打开压缩文件然后再tar -xvf解出两个文件

```
root@kali:~# tar -xvf e66ea8344f034964ba0b3cb9879996ff-1
pic2.jpg
pic1.jpg
root@kali:~#
```



用StegSolve合成两文件即可获取flag



## base64÷4

这就是告诉你，是base16嘛，直接拿去base16解密即可



```
666C61677B453333423746443841334238343143413936393945444444241323442363041417D
```

编码 解码 清空

flag{E33B7FD8A3B841CA9699EDDBA24B60AA}

复制

Base编码系列: Base64 Base32 Base16

Base16编码使用16个ASCII可打印字符（数字0-9和字母A-F）对任意字节数据进行编码。Base16先（不足8比特在高位补0），然后将其串联进来，再按照4比特一组进行切分，将每组二进制数分别转

## Embarrass

直接用winhex搜索flag{即可

0	00 20 01 00 00 0A 00 00 00 44 01 00 00 0C 00 00	D	
0	00 50 01 00 00 0D 00 00 00 5C 01 00 00 0E 00 00	P	\
0	00 68 01 00 00 0F 00 00 00 70 01 00 00 10 00 00	h	p
0	00 78 01 00 00 13 00 00 00 80 01 00 00 02 00 00	x	!
0	00 18 27 00 00 1E 00 00 00 1C 00 00 00 66 6C 61	'	fla
0	67 7B 47 6F 6F 64 5F 62 30 79 5F 57 33 6C 6C 5F	g{Good_b0y_W311	
0	44 6F 6E 65 7D 00 00 00 00 1E 00 00 00 04 00 00	Done}	
0	00 00 00 00 00 1E 00 00 00 08 00 00 00 4C 6E 63		Lnc
0	6B 65 6E 00 00 1E 00 00 00 04 00 00 00 00 00 00	ken	
0	00 1E 00 00 00 04 00 00 00 00 00 00 00 1E 00 00		
0	00 0C 00 00 00 4E 6F 72 6D 61 6C 2E 64 6F 74 6D		Normal.dotm

## 神奇的Modbus

用wireshark打开然后搜索，字符串和字节流类型搜索sctf即可

Wireshark interface showing a search for 'sctf'. The packet list pane shows several Modbus and TCP packets. The selected packet (Modbus... 103) is expanded to show register values: Register 4 (UINT16): 123, Register 5 (UINT16): 69, Register 6 (UINT16): 97. The packet bytes pane shows the raw data of the Modbus response, with 's-c-t-f' visible in the ASCII column.

sctf{Easy\_Modbus}

## MISCall

先用file查看这是什么文件，然后进行压缩

```
root@kali:~# file d02f31b893164d56b7a8e5edb47d9be5
d02f31b893164d56b7a8e5edb47d9be5: bzip2 compressed data, block size = 900k
root@kali:~#
```

```
tar -xvf d02f31b893164d56b7a8e5edb47d9be5
```

```
root@kali:~# cd ctf/  
root@kali:~/ctf# ls  
flag.txt  
root@kali:~/ctf# cat flag.txt  
Nothing to see here, moving along...  
root@kali:~/ctf#
```

这是个假的flag文件

查看修改列表

git stash list

删除flag.txt文件

```
rm -rf flag.txt
```

使用git stash show校验列表中存储的文件

得到的flag.txt也是假的

运行s.py即可

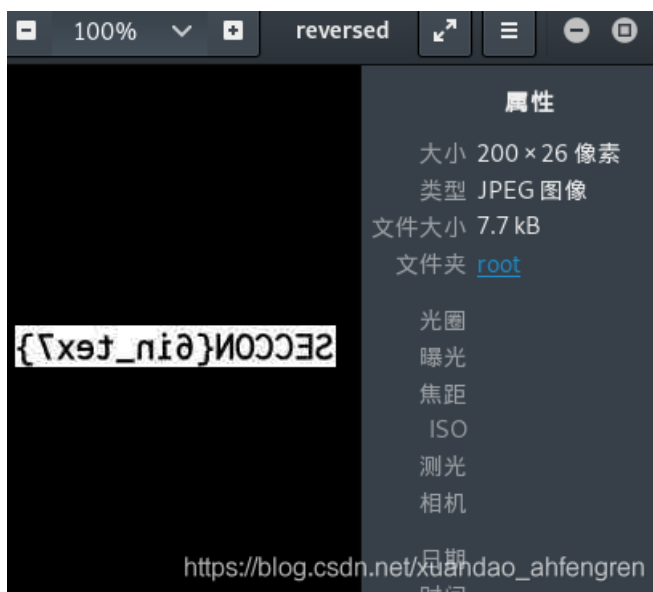
得到flag直接提交即可

```
root@kali:~/ctf# python s.py  
NCN4dd992213ae6b76f27d7340f0dde1222888df4d3
```

## Reverse-it

用命令获取到反转的flag

```
xxd -p 0da9641b7aad4efb8f7eb45f47eaebb2 | tr -d '\n' | rev | xxd -r -p > reversed
```



我们再用convert -flop reverse reversed

进而获取到flag是SECCON{6in\_tex7}

## something\_in\_image

用编辑器直接打开然后搜索flag即可









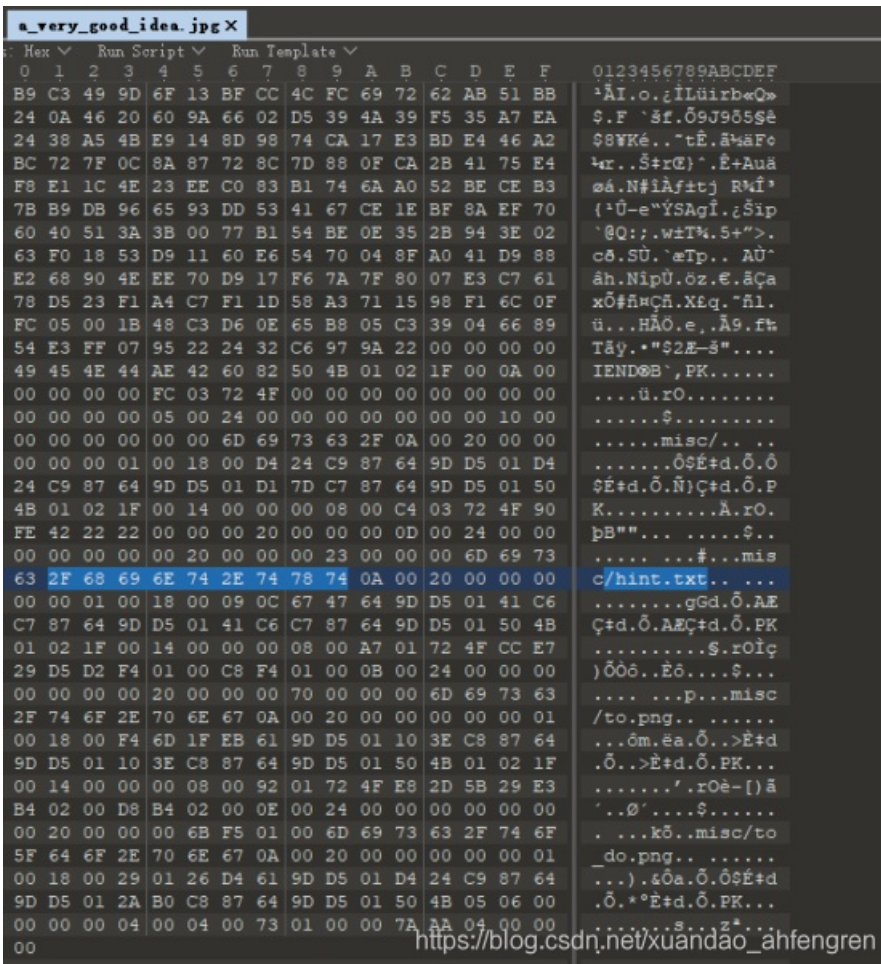
[https://blog.csdn.net/xuandao\\_ahfengren](https://blog.csdn.net/xuandao_ahfengren)

两次解密后出现flag

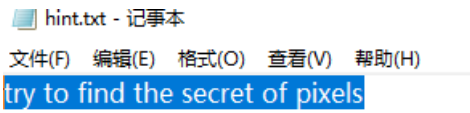


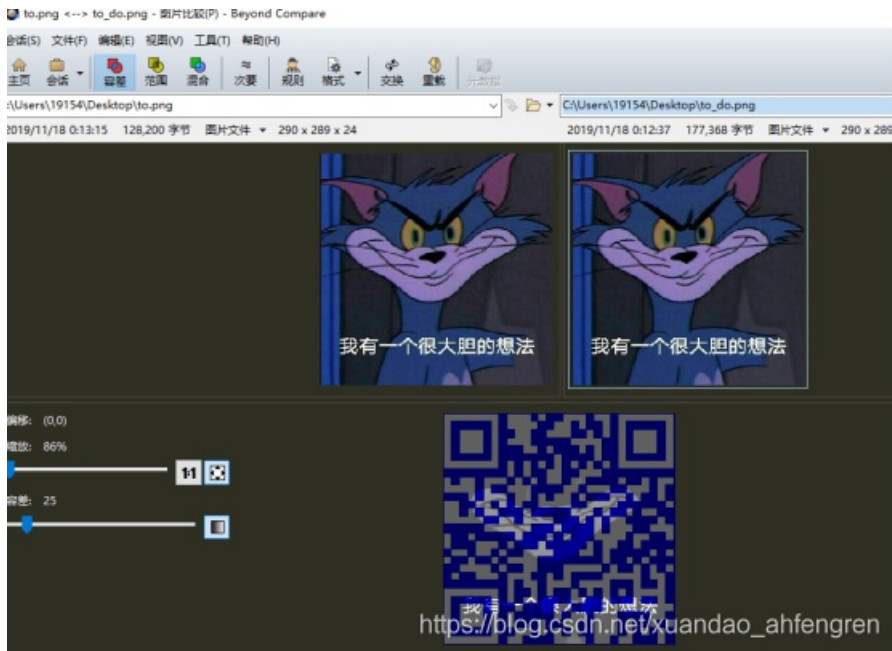
a\_good\_idea

用010editor打开，发现有txt文件，果断改成zip文件把文件压缩出来



然后根据hint.txt的提示，我们用BeyondCompare将两张图片进行比较发现二维码，扫描得出flag





## 2017\_Dating\_in\_Singapore

估计题目描述我们知道每两位数对应号数一共有十二组，我们将他们连接起来得到flag

HITB{CTFFUN}

## simple\_transfer

我们发现nfs包中看到了pdf文件，那我们就把文件分离出来

No.	Time	Source	Destination	Protocol	Length	Info
4291	54.724259	10.0.2.5	10.0.2.4	NFS	234	V4 C
4292	54.724408	10.0.2.4	10.0.2.5	NFS	138	V4 F
4294	60.813320	10.0.2.5	10.0.2.4	NFS	210	V4 C
4295	60.814109	10.0.2.4	10.0.2.5	NFS	266	V4 F
4297	61.844642	10.0.2.5	10.0.2.4	NFS	210	V4 C
4298	61.844943	10.0.2.4	10.0.2.5	NFS	266	V4 F
4300	61.845705	10.0.2.5	10.0.2.4	NFS	210	V4 C
4301	61.845888	10.0.2.4	10.0.2.5	NFS	266	V4 F
4303	62.583091	10.0.2.5	10.0.2.4	NFS	230	V4 C

```

[Program Version: 4]
[V4 Procedure: COMPOUND (1)]
> Tag: <EMPTY>
minorversion: 0
v Operations (count: 4): PUTFH, LOOKUP, GETFH, GETATTR
  > Opcode: PUTFH (22)
  v Opcode: LOOKUP (15)
    v Name: file.pdf
      length: 8
      contents: file.pdf
  
```

```

0000 08 00 27 1f c2 a8 08 00 27 f3 75 4b 08 00 45 00  ..'.....'uK..E.
0010 00 d8 09 72 40 00 40 06 18 a6 0a 00 02 05 0a 00  ...n@.@.....
0020 02 04 03 56 08 01 bb 86 59 19 29 a2 bc 04 80 18  ...V...Y)...
0030 01 49 18 d3 00 00 01 01 08 0a 00 02 4d 2f 00 02  ..I.....M/..
0040 49 cb 80 00 00 a0 7f c0 e6 45 00 00 00 00 00 00  ..I.....E.....
0050 00 02 00 01 86 a3 00 00 00 04 00 00 00 01 00 00  ..
0060 00 01 00 00 00 24 01 06 27 38 00 00 00 0a 63 74  ....$. '8....ct
0070 66 2d 63 6c 69 65 6e 74 00 00 00 00 00 00 00 00  ..f-client.....
0080 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00  ..
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00  ..
00a0 00 16 00 00 00 1c 01 00 07 00 bb 23 06 00 00 00  ..#...
00b0 00 00 5c 75 36 b9 c5 96 42 ef 9c 96 51 d4 3c 03  ..\u6...Q.<.
00c0 75 59 00 00 00 0f 00 00 00 08 66 69 6c 65 2e 70  ..uY.....file.p
00d0 64 66 00 00 00 0a 00 00 00 09 00 00 00 02 00 10  ..df.....
00e0 01 1a 00 b0 a2 3a
  
```

foremost -T 文件名即可分离

打开pdf文件即可获取flag

