CTF 音频隐写 大总结

转载

你们这样一点都不可耐 于 2020-04-21 20:46:28 发布 7469 收藏 54

分类专栏： MISC 文章标签： 安全 音频编码解码 经验分享 数据安全 加密解密

原文链接：https://www.sqlsec.com/2018/01/ctfwav.html

MISC 专栏收录该内容

17 篇文章 0 订阅

订阅专栏

赛题概览

Nuit du Hack CTF Qualifications: Here, kitty kitty!

环境

- Windows

考察点

- WAV音频文件隐写术
- Python基础
- 密码学

工具

Audacity

题目描述

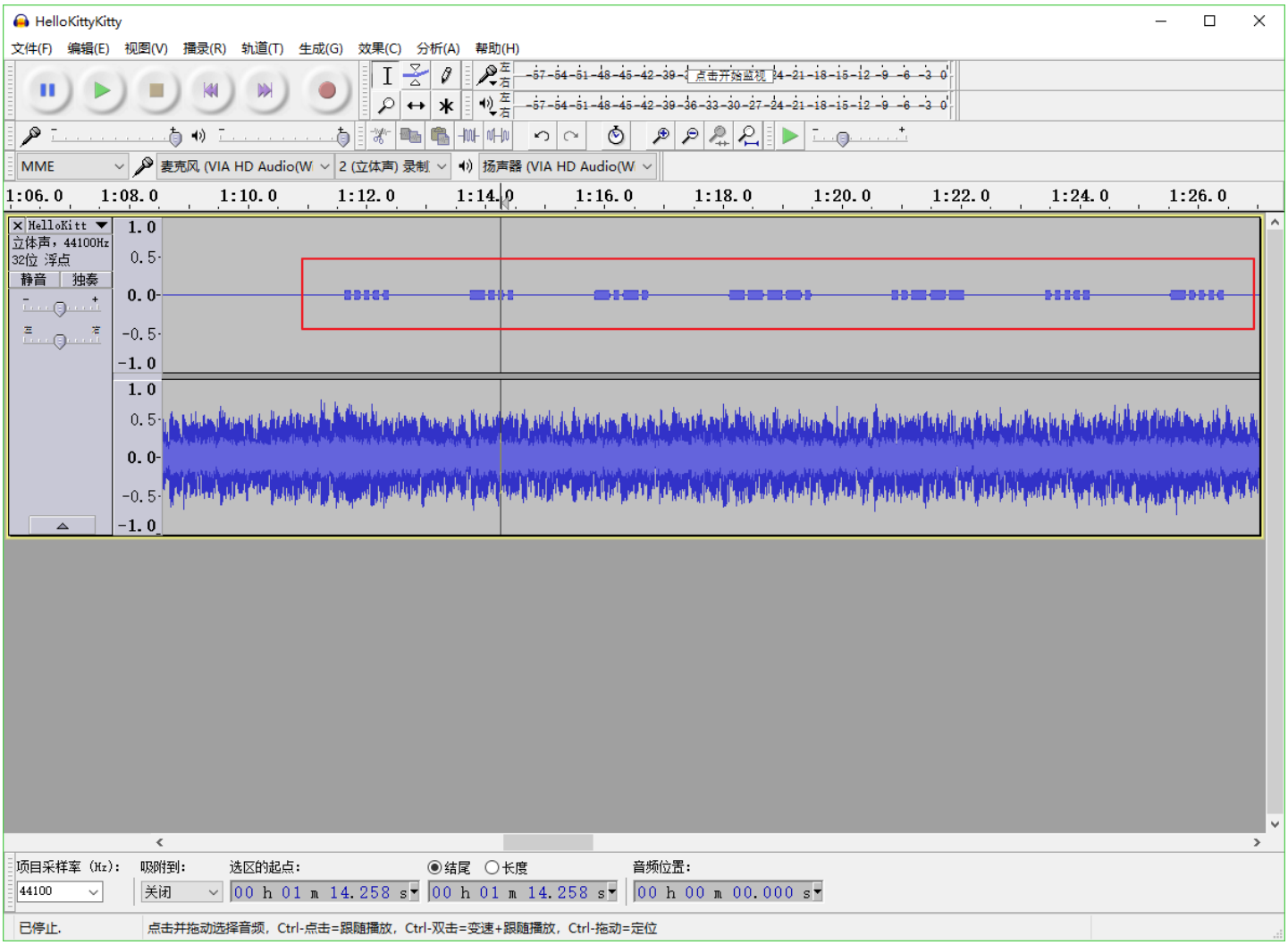
> I just can't get enough of this sweet melody, I can listen to it for hours! Sometimes I even feel like it is trying to send me a message ..
> HelloKittyKitty.wav

翻译:

> 我听这段音乐根本停不下来，我已经听了几个小时！有时候我觉得它再给我传递一个信息
> HelloKittyKitty.wav

Writeup

使用像Audacity这样的音频处理软件打开文件，然后可以在音道的最上边看到一些特殊的:



看起来是一个摩斯电码，短线代表`.`，长线代表`-`，最后摩斯电码翻译如下:

```
.... -... -.-. ----- ..--- ..... -.... ....- ----. -.-. -... ----- .---- ---.. ---.. --.- ..... ..--- . -.... .-
--- ----- -.. ----- ----- ----. ..--- ----. .---- ----. .---- -.-.
```

摩斯电码解码得到:

```
HBC925649CB0188Q52E617D70929191C
```

md5解密得到`valar dohaeris`

试了不对，又试了md5值的小写，通过了

```
flag：`5bc925649cb0188f52e617d70929191c`
```

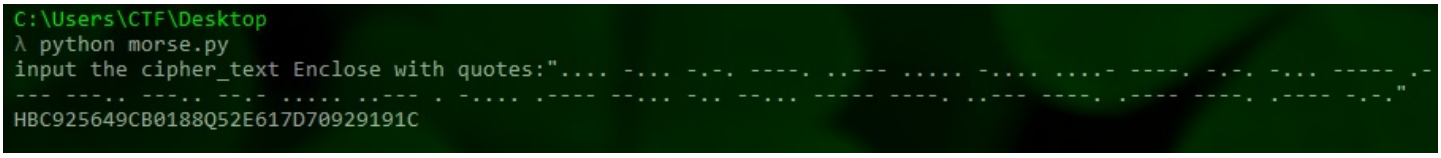
总结

Python摩斯电码解密

摩斯电码解密可以使用诸多在线网站，当然也可以用Python进行解密：

```
# -*- coding:utf-8 -*-
s = input("input the cipher_text Enclose with quotes:")
codebook = {
    'A':".-",
    'B':"-...",
    'C':"-.-.",
    'D':"-..",
    'E':".",
    'F':"..-.",
    'G':"--.",
    'H':"....",
    'I':"..",
    'J':".---",
    'K':"-.-",
    'L':".-..",
    'M':"--",
    'N':"-.",
    'O':"---",
    'P':".--.",
    'Q':"--.-",
    'R':".-.",
    'S':"...",
    'T':"-",
    'U':"..-",
    'V':".--",
    'W':".--",
    'X':"-..-",
    'Y':"-.--",
    'Z':"--..",
    '1':".----",
    '2':"..---",
    '3':"...---",
    '4':"....-",
    '5':".....",
    '6':"-....",
    '7':"--...",
    '8':"---..",
    '9':"----.",
    '0':"-----",
    '.':".—.—.—",
    '?':"..--..",
    '!':"-.-.--",
    '(':"-.--.",
    '@':".--.-.",
    ':':"---...",
    '=':"-...-",
    '-':"-....-",
    ')':"-.--.-",
    '+':".-.-.",
    ',':"--..--",
    '\'':".----.",
    '_':"..--.-",
    '$':"...-..-",
    ';':"-.-.-.",
    '/':"-..-.",
    '\"':".-..-.",
}
clear = ""
cipher = ""
```

```
while 1:
ss = s.split(" ");
for c in ss:
for k in codebook.keys():
if codebook[k] == c:
cipher+=k
print(cipher)
break;
```



MD5在线解密网站

排名不分先后

- CMD5
- SOMD5
- DMD5
- navisec
- 漏洞银行
- ChaMD5

赛题概览

Sharif University Quals CTF 2014: Hear with your Eyes

环境

- Windows

考察点

- WAV音频文件隐写术

工具

Audacity

题目描述

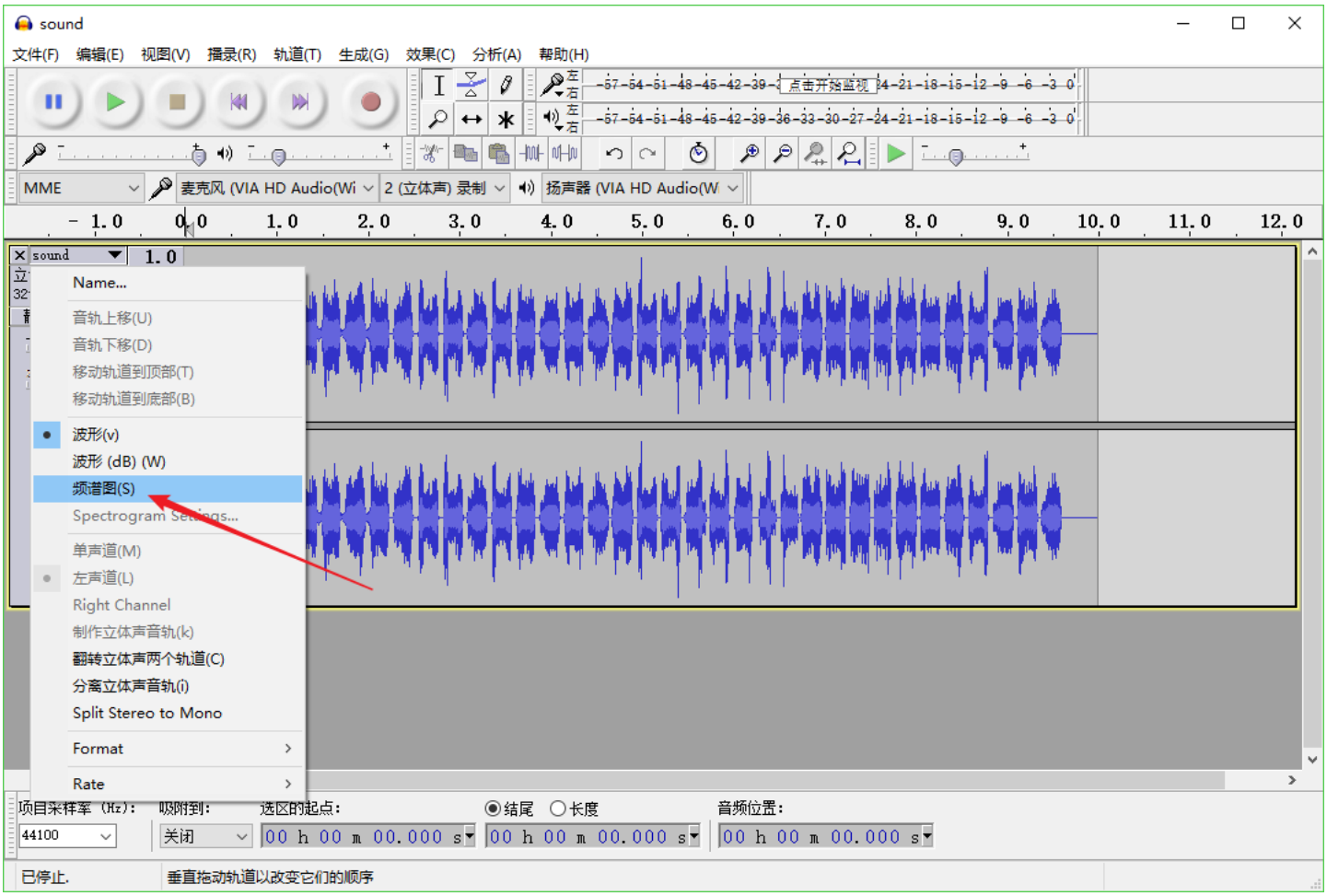
> Hear With Your Eyes
> Download

翻译：

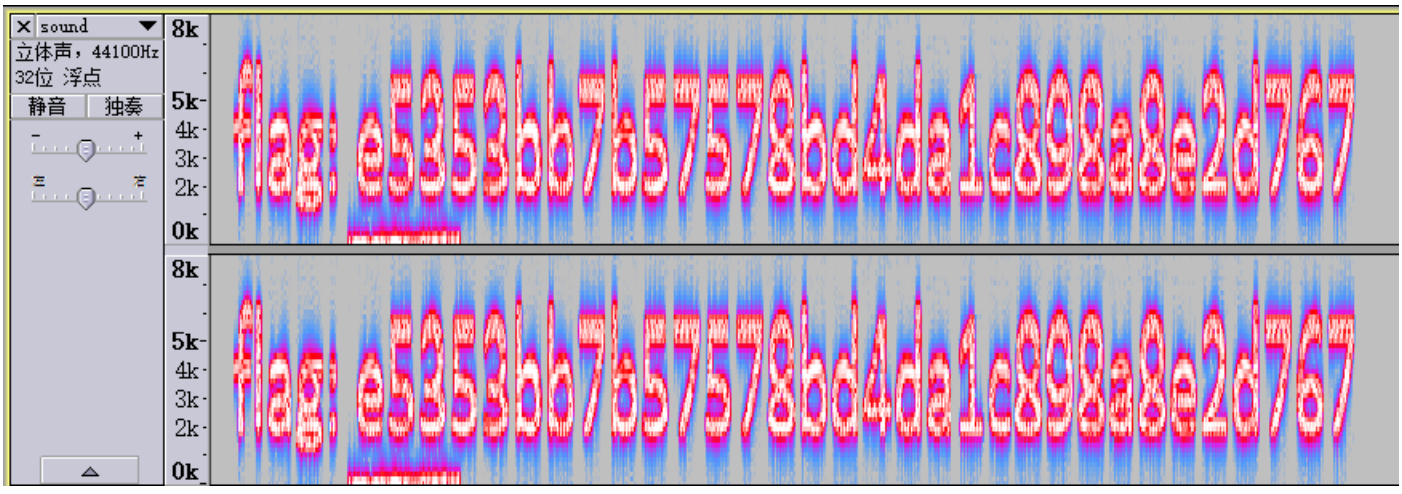
> *用你的眼睛倾听*
> *下载*

Writeup

题目描述说：`用眼睛去倾听`，所以这里使用工具Audacity去打开wav文件。
切换到`频谱图`去观察：



从频谱图可以直接看到flag。



总结

这种直接从频谱图中直接去读flag的信息算是比较入门的一个WAV隐写了。

赛题概览

ISCC 2017:普通的DISCO

环境

- Windows

考察点

- WAV音频文件隐写术
- 简单密码学

工具

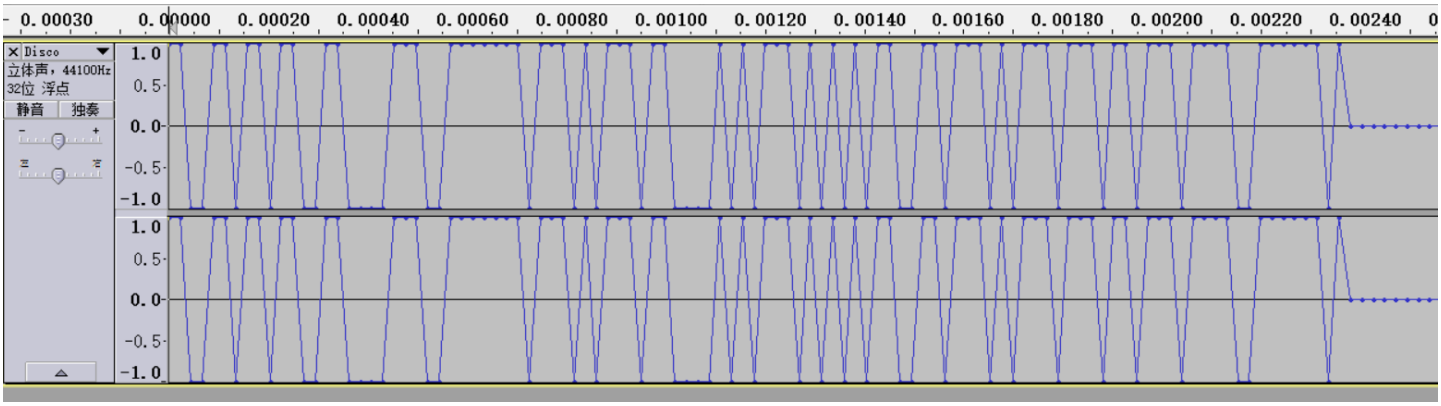
Audacity

题目描述

普通的DISCO我们普通的摇~
附件是一个wav的音频（这里我国光对不起大家，这里我实战实在没有找到这个wav文件）

Writeup

用Audacity打开文件后，放大波形谱。



以高为`1`低为`0`，转换得到`01`字符串

```
1100110110110011000011100111111101110101110110000101011101010101100110111010111011101101110111100111111101
```

一共`105`位，额，不符合`8`位一个字符，符合`7`位，于是在每个7位之前加个`0`，得到

```
01100110,01101100,01100001,01100111,01111011,01010111,00110000
01010111,00101010,01100110,01110101,01101110,01101110,01111001,
01111101
```

然后`二进制`转`十进制`,然后再转为`ASCII`，得到`flag`。

```
1100110    102
1101100    108
1100001    97
1100111    103
1111011    123
1010111    87
0110000    48
1010111    87
0101010    42
1100110    102
1110101    117
1101110    110
1101110    110
1111001    121
1111101    125
```

flag{W0Wfunny}

flag{W0Wfunny}

总结

感觉这题的难点不是从频谱中读取二进制数据。个人觉得从读书的二进制数据想到8位一组补上0前面还是比较难的，得保持数据的敏感性才可以。

赛题概览

ISCC-2016: Music Never Sleep

环境

- Windows
- Linux

考察点

- mp3音频文件隐写

工具

- Mp3Stego

在压缩过程中，`MP3Stego`会将信息隐藏在MP3文件中。数据首先被压缩、加密，然后隐藏在MP3比特流中。

基本介绍和用法如下:

```
encode -E hidden_text.txt -P pass svega.wav svega_stego.mp3
decode -X -P pass svega_stego.mp3
```

题目描述

国光在这里又对不住大家了，这里我又没有找到这个mp3文件，ε=ε=ε= ┌(゜ロ ゜;)┘

Writeup

听音频无异常猜测使用隐写软件隐藏数据，搜索mp3里面的关键字符串:

```
→ ctf strings ISCC2016.mp3|grep iscc
  pass:bfsiscc2016  G
```

得到密码后使用 `Mp3Stego` 解密:

```
decode.exe -X ISCC2016.mp3 -P bfsiscc2016
```

得到文件 `iscc2016.mp3.txt`，其内容是:

```
Flag is SkYzWEk0M1JOWlNHWTJTRktUkdJTVpXRzVSV0U2REdHTVpHT1pZPQ== ???
```

base64 && base32 后得到flag

```
flag: IwtsqndljERbd367cbxf32gg
```

总结

这里考察的是mp3的音频隐写，这里的套路目前来看没有wav隐写那么多变。此外这里对base64和base32嵌套加密也得保持数据的敏感度。

赛题概览

广东省强网杯-2015: Little Apple

环境

- Windows

考察点

- mp3音频文件隐写

工具

- Silenteye

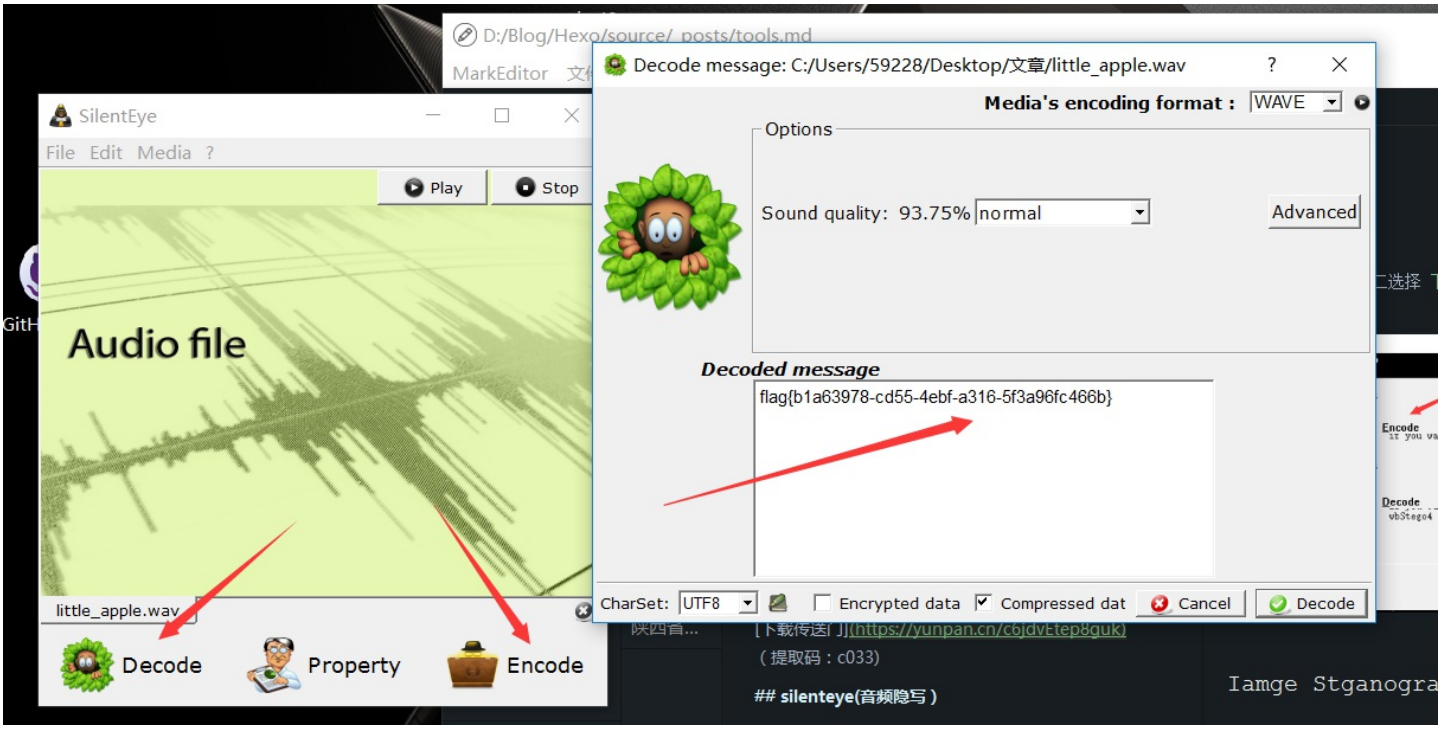
`SilentEye` 是一个跨平台的应用程序设计，可以轻松地使用隐写术，在这种情况下，可以将消息隐藏到图片或声音中。它提供了一个很好的界面，并通过使用插件系统轻松集成了新的隐写算法和加密过程。

题目描述

我国光不会告诉你们，我这里又没有找到附件

Writeup

直接使用 slienteye 这个工具即可



总结

音频中的LSB

这题就是考的知识面了，不知道这个工具就GG

赛题概览

XMAN-2016 : Misc-200

环境

- Windows
- xxd

附件

hong.mp3

工具

- Mp3Stego
- Linux xxd 命令
- Linux file 命令

Writeup

解压mp3

首先使用`Mp3Stego`解密mp3文件。

```
D:\soft\MP3Stego_1_1_18\MP3Stego
λ Decode.exe -X C:\Users\CTF\Desktop\CTF\misc\hong_Ksfw02V.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'C:\Users\CTF\Desktop\CTF\misc\hong_Ksfw02V.mp3'  output file = 'C:\Users\CTF\Desktop\CTF\misc\hong
_Ksfw02V.mp3.pcm'
Will attempt to extract hidden information. Output: C:\Users\CTF\Desktop\CTF\misc\hong_Ksfw02V.mp3.txt
Enter a passphrase:
Confirm your passphrase:
the bit stream file C:\Users\CTF\Desktop\CTF\misc\hong_Ksfw02V.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 1265]Avg slots/frame = 417.631; b/smp = 2.90; br = 127.899 kbps
Decoding of "C:\Users\CTF\Desktop\CTF\misc\hong_Ksfw02V.mp3" is finished
The decoded PCM output file name is "C:\Users\CTF\Desktop\CTF\misc\hong_Ksfw02V.mp3.pcm"
```

得到一个txt文件内容是:

```
http://weibo.com/u/5280474214?from=feed&loc=avatar&is_all=1       hint:这是一个文件哦，呦呦呦，切克闹
```

访问得到一张二维码:

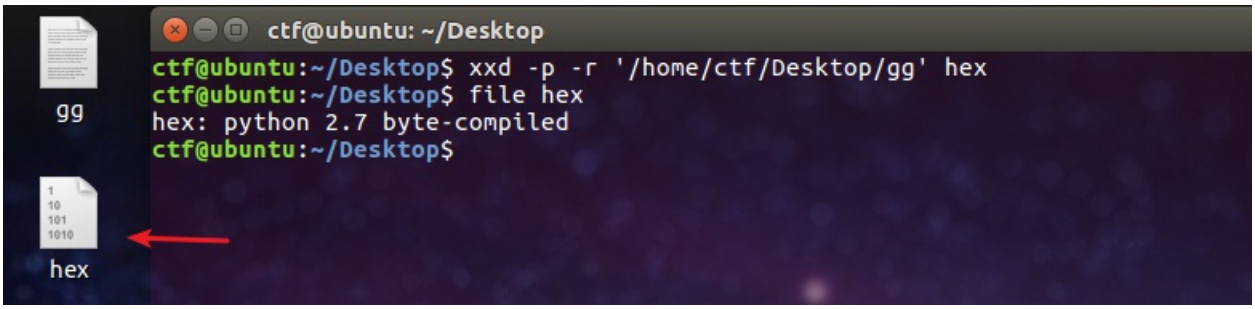
读取二维码

读取二维码得到内容为:

```
03F30D0AC252BA5763000000000000000001000004000000730D000006400008400005A0000640100532802000000630000000000300000
000F000000430000007363000000640100640200640300640400640500640600640400640700640800640300640400640900640300640900
640A00670F007D0000640B007D0100781E007C0000445D16007D02007C01007400007C020083010037 7D0100714000577C01004748640000
53280C0000004E697A0000006968000000696900000695F0000006966000000697500000069730000006961000000696E00000069670000
00740000000028010000007403000000636872280300000074030000007374727404000000666C6167740100000069280000000028000000
00730400000622E70795203000000010000007326000000000103010301030103010301030103010301030103010301030103010901
06010D0114024E2801000000520300000028000000002800000000280000000073040000000622E70797408000000 3C6D6F64756C653E0100
00007300000000
```

二进制进制转换

将二进制内容保存文件为`gg`，然后用`xxd`命令生成一个hex文件:



用file命令查看下是一个`python 2.7`的编译文件，手动改为`hex.pyc`然后在线反编译一下文件得到源码:

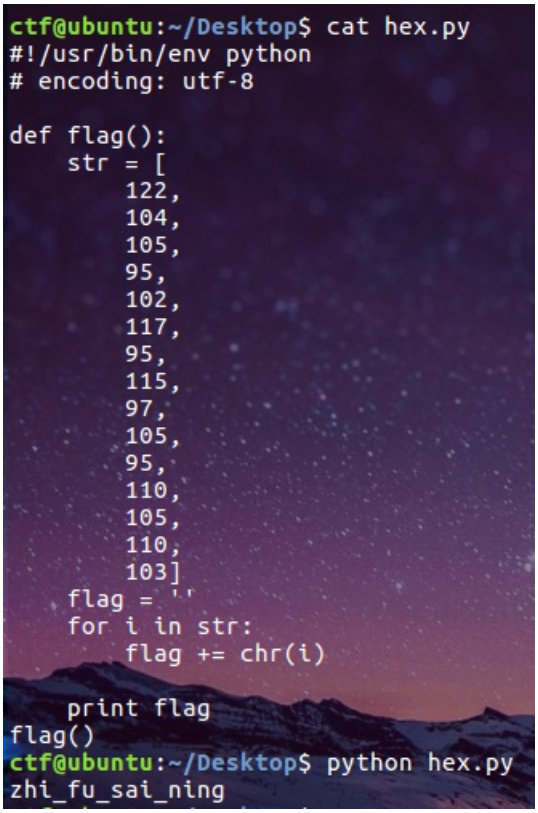
Py

```
#!/usr/bin/env python
# encoding: utf-8
```

def flag():
str = [
122,
104,
105,
95,
102,
117,
95,
115,
97,
105,
95,
110,
105,
110,
103]
flag = ‘’
for i in str:
flag += chr(i)

```
print flag</code></pre></div>
```

代码最后加上`flag()`调用flag函数输出flag:



写在最后

目前还有几道国外的音频题目没有完善，这里日后会慢慢完善的。

转自：https://www.sqlsec.com/2018/01/ctfwav.html
作者：国光