

实验吧/隐写术/小苹果

原创

SIAT_啊哦 于 2017-04-12 20:17:47 发布 3405 收藏

分类专栏: [CTF](#) 文章标签: [unicode](#) [当铺密码](#) [mp3stego](#)

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/ETF6996/article/details/70146940>

版权



[CTF 专栏收录该内容](#)

17 篇文章 0 订阅

[订阅专栏](#)

[题目链接](#)

1. 首先binwalk, 发现有个RAR

```
选定 管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator.PPTU3-20140308L>cd desktop

C:\Users\Administrator.PPTU3-20140308L\Desktop>binwalk apple.png
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          PNG image, 400 x 400, 8-bit/color RGBA, non-interlaced
41           0x29        Zlib compressed data, compressed
52876       0xCE8C      RAR archive data, first volume type: MAIN_HEAD
http://blog.csdn.net/ETF6996
```

2. 解压RAR, 得到apple.mp3, 自然联想到mp3stego, 然后decode, 但是需要输入decode密码, 再回头看看图片, 发现是一个二维码, 扫描后得到\u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d\u5de5, 很明显是Unicode加密, 直接在python3.5里面进行Unicode解码后得到:

```
Python 3.5.2 Shell
File Edit Shell Debug Options Window Help
Python 3.5.2 (v3.5.2:4def2a2901a5, Jun 25 2016, 22:01:18) [MSC v.1900 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>> '\u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d\u5de5'
'羊由大井夫夫人王中工'
>>>
```

3. 得到: 羊由大井。。。, 一看是当铺密码, 再进行解密得: 9158753624, 即mp3stego的decode密码如下:

```
cmd 选定 管理员: C:\Windows\system32\cmd.exe

F:\ctf\mp3stego-gui>decode
MP3StegoEncoder 1.1.15
See README file for copyright info
USAGE : decode [-X][-A][-s sb] inputBS [outPCM [outhidden]]
OPTIONS : -X          extract hidden data
          -P <text>  passphrase used for embedding
          -A          write an AIFF output PCM sound file
          -s <sb>    resynth only up to this sb <debugging only>
          inputBS    input bit stream of encoded audio
          outPCM     output PCM sound file <dflt inputBS+.aif!.pcm>
          outhidden  output hidden text file <dflt inputBS+.txt>

F:\ctf\mp3stego-gui>decode -X apple.mp3 -P 9158753624
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = 'apple.mp3' output file = 'apple.mp3.pcm'
Will attempt to extract hidden information. Output: apple.mp3.txt
the bit stream file apple.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 1213]avg slots/frame = 417.617; b/smp = 2.90; br = 127.895 kbps
Decoding of "apple.mp3" is finished
The decoded PCM output file name is "apple.mp3.pcm"
```

4.在生成的apple.mp3.txt中看到一串base64，解密即得flag