

刷题之旅第44站,i春秋网络安全公益赛, misc题目: funnygame

原创

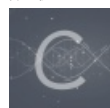
圆圈勾勒成指纹 于 2020-02-22 16:48:02 发布 379 收藏

分类专栏: [刷题之旅100站](#)

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_45940434/article/details/104446037

版权



[刷题之旅100站 专栏收录该内容](#)

49 篇文章 11 订阅

订阅专栏

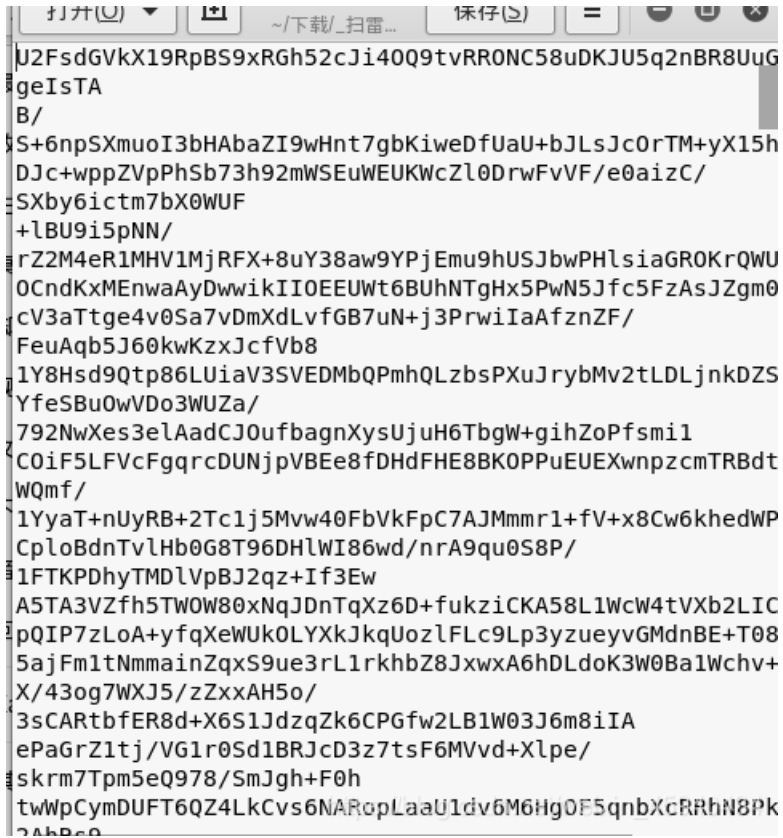
感谢i春秋平台提供题目

在扫雷.png中发现隐藏文本 secret.txt, 分离出来。

```
root@kali: ~/下载
文件(E) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~/下载# binwalk *.png
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0 主目录     0x0          PNG image, 616 x 399, 8-bit/color RGBA, non-interlaced
41 桌面       0x29        Zlib compressed data, default compression
52016        0xCB30      Zip archive data, at least v2.0 to extract, compressed size: 403554, uncompressed size: 531852, name: secret.txt
455702      0x6F416     End of Zip archive, footer length: 22
root@kali:~/下载# binwalk -e *.png
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0 主目录     0x0          PNG image, 616 x 399, 8-bit/color RGBA, non-interlaced
41 音乐       0x29        Zlib compressed data, default compression
52016        0xCB30      Zip archive data, at least v2.0 to extract, compressed size: 403554, uncompressed size: 531852, name: secret.txt
455702      0x6F416     End of Zip archive, footer length: 22
root@kali:~/下载#
```

显示应用程序 https://blog.csdn.net/weixin_45940434

打开发现特征字符 U2F, 是AES 系列的加密。



在pyc文件中有隐写, 使用stegosaurus 进行读取。

```
root@kali: ~/图片/stegosaurus
文件(E) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~/图片/stegosaurus# python3 stegosaurus.py -x *.pyc
Extracted payload: AES key is Flippingisfun
root@kali:~/图片/stegosaurus#
```

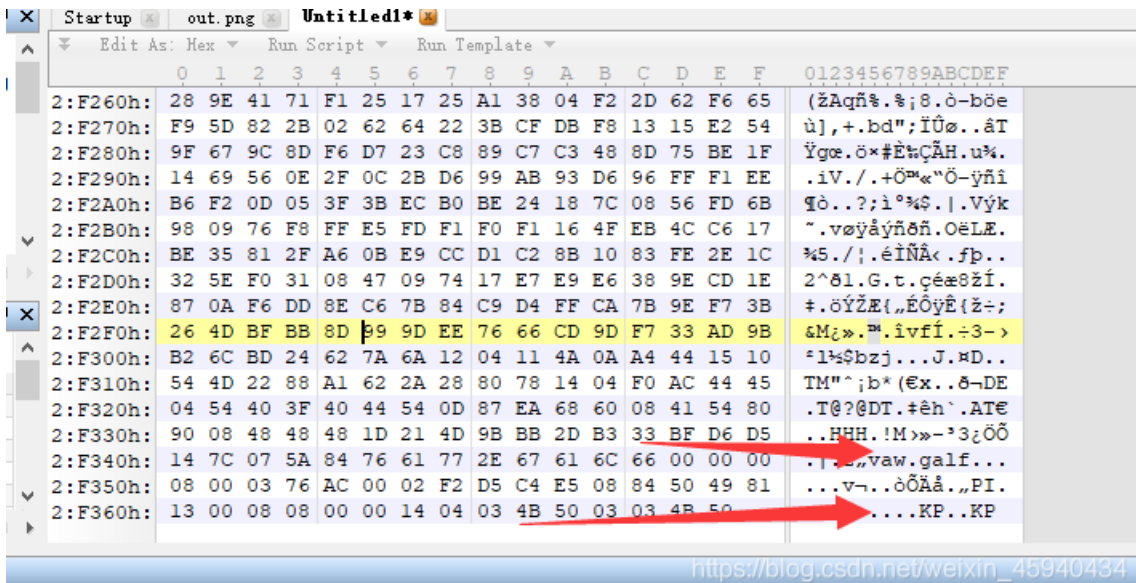
得到了AES的密钥，那么在线解密。得到了十六进制的一堆字符。

[加密/解密](#) [散列/哈希](#) [BASE64](#) [图片/BASE64转换](#)

明文:

```
00000002F2FF0000005A000100010000000006054B5001D5DF2020
082B3101D5DF2036D182B101D5DF2021546141001800010000000
00020000A7661772E67616C6600000004000000200000000000000
240008000376AC0002F2D5C4E5088450498113000808000014003F
02014B5007FFC8E3FF038FFFEFDFFD9F7FEF7EFF980F2FFF5D
DFFFB69DCFFE83B6FF99D71FE13CABE221BEE21C7FFEA5FFC
4F2BDFCF2F1B0DFEFFDFBFF0A773FF1A5FFB314EFB1C1FE17
41FA2279FFE49B5A8FEB49565C3BFD1DFBF36F7FED4FE23F7
3FF30351FE24DAA3F43E87FEBCEA3F46EFE5889D5EFBFDFFC
4F3FFD12B15BFF8A512F6A3F22C9D47E8A526FF9091C2BE58E
A77CB8AB7FCC590ABFF954A9FF49FAF7EAA2A3F048A38BCB5
EFAB057CC20DD47E096F2A3F2483547E615FBE57F5EF86ED7B
ED015EFC22D7C329B6BDFEE5C8FE12107255EFFE8E1B657C24
C0D7BF96F94503AF7CA46A3F2D48D682772A78589AD5EF821E7
CC34F65C7D1C7BAC9FF504AF92A0AABE32520AB86E5E22A3B
AF85BB6B3E2AB4403AED33F99AADF096B1812EB13B90CD9F2
C055AF91ABD75F395549CC12CB94A395B79F3DA961B057CF57B
ECB82295F297379FC3560ECB809F5F2550665C7B5CF94ECECF9
8B04CB9D527F279DE059EB6773D4CFE3B7119FCB5BDC23997B
3E32B9ECB84CF5EFC52D7BEE9F9EFB5C055CF02D1681281182
F6C89DC8B0CB810F57024ABE62CA73B9AE27703B6BE523B2AF
8A876EBDF595AF8CBB3A7701473CEB3E1CB92E5CB67CF9ED4
ACFDF9F0D650F3E728B9CB8971C376CB8D17570A52BE5ABDD
E5C8B2CB8FBD9F2E5C332E59C0431067C6EF500D6D99FC761F
4AB8B579F30B0597147B3DF9F81EDDA0708CF0447640EAD6B91
8D97101C2E41CBFB827EB619F1056783293D0BE9D036477EBE6
2D4F70E172E68CE7CA2319DC0D6AF84B274EE27467CF54B2F40
6E8DC0955704FEBDCEA306514D9712E82151C06C3015E0B39BF
```

导入到010editor看到特征符PK。



发现顺序反了，写个脚本让他恢复过来。

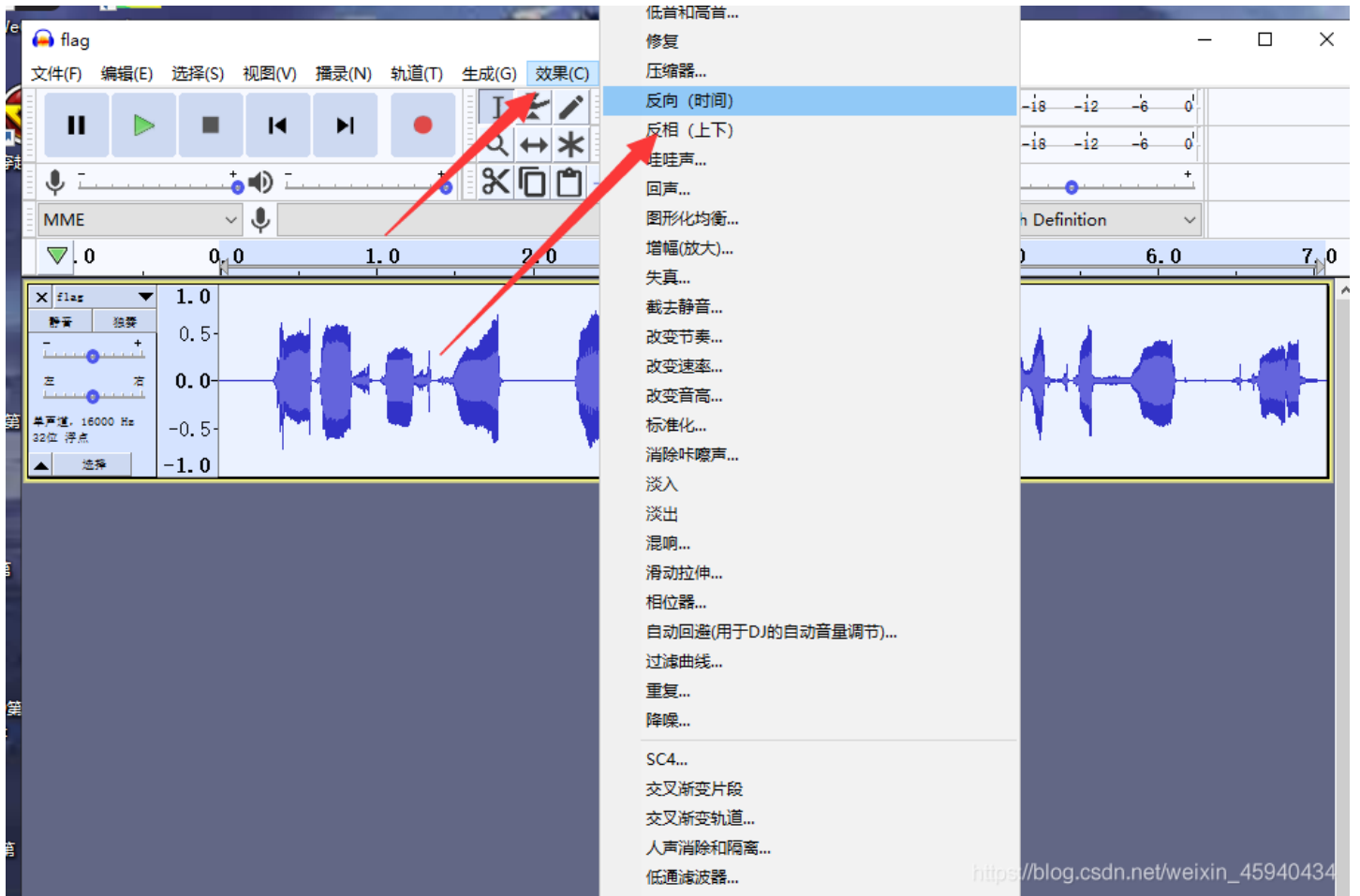
```
with open('1.zip','rb') as f:
    a = f.read()

b=a[::-1]

with open('2.zip','wb') as q:
    q.write(b)
```

得到了flag.wav,听了一遍发现声音是反的。

使用Audacity，恢复过来，听听力得到flag。



这个听力真的是很不容易听出来。。。。。

flag is 61o0305k2b

结语：

菜鸡的cc师傅，将会持续写出100篇高质量的CTF题目，供大家进行CTF的入门以及进阶，如果觉得文章对您有所帮助，欢迎关注一下cc师傅。

原创文章不易，点个赞再走吧。

