NSCTF-misc-writeup

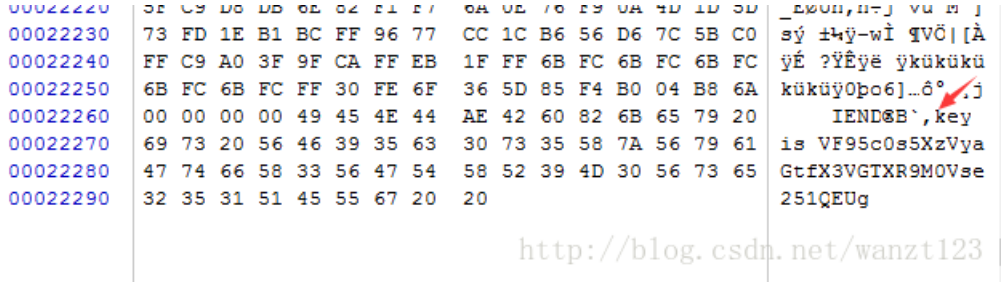
原创

Brucetg 于 2017-07-22 00:28:54 发布 4110 收藏 3

Misc:

Kungfu

打开压缩包，里面有一张png后缀的图片，因为分比较低，感觉是套路题，直接winhex打开查看，在文件末尾发现提示：



尝试base64解码：

尝试凯撒和栅栏解密都不行，还以为是思路错误，后来队友提示后面加一个空格试试，顺利得到flag：

你知道吗？这是什么

文件名为zip，binwalk跑一下，发现是zip文件，加上文件后缀.zip,解压后得到hidden.png,

再次binwalk跑一下：

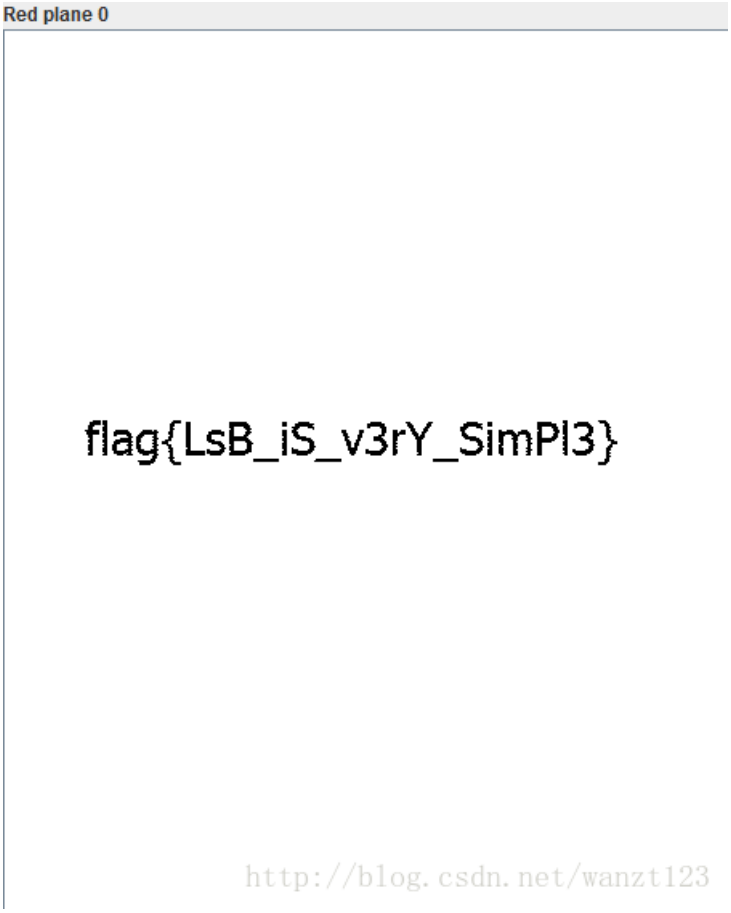
```
root@kali:~/桌面# binwalk hidden.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 351 x 560, 8-bit/color RGBA, non-i
aced
41            0x29            Zlib compressed data, default compression
1975          0x7B7           Zip archive data, at least v1.0 to extract,
ssed size: 291742, uncompressed size: 291742, name: hidden2.jpg
293851        0x47BDB         End of Zip archive
```


发现图片后面附加了一个压缩包，使用binwalk –e hidden.png提取可得到hidden2.jpg，flag就在图片上：

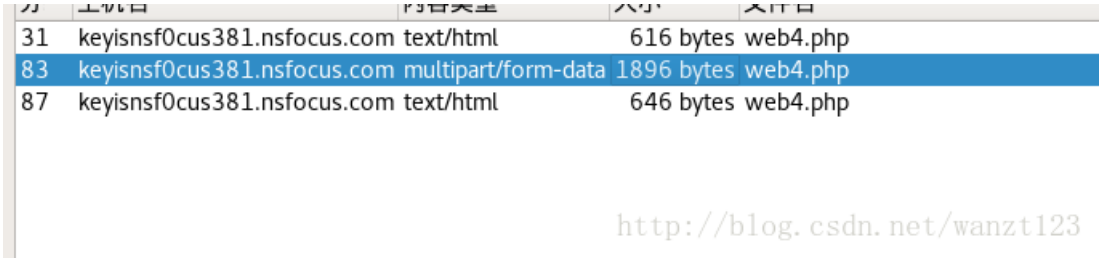
So easy！！

压缩包里面有lsb.bmp，stegsolve打开调一下即可得到flag：

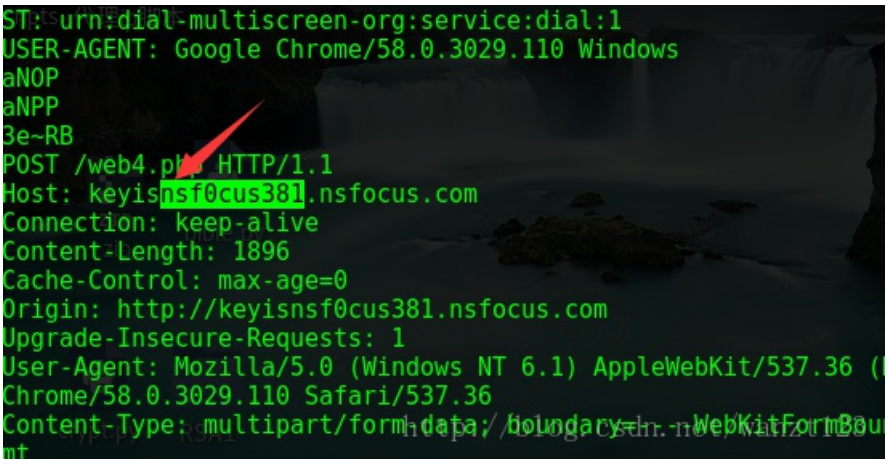


流量啊

下载下来发现是一个流量包，wireshark打开，导出http对象，得到一个rar格式的压缩文件，不过需要解压密码，尝试爆破，无果



strings 一下发现Host字段有点奇怪，像是密码提示：



于是尝试用nsf0cus381作为压缩包的解压密码，成功，得到flag：

Havefun！！

实验吧的原题，可参考http://blog.csdn.net/yalecaltech/article/details/64158016求解

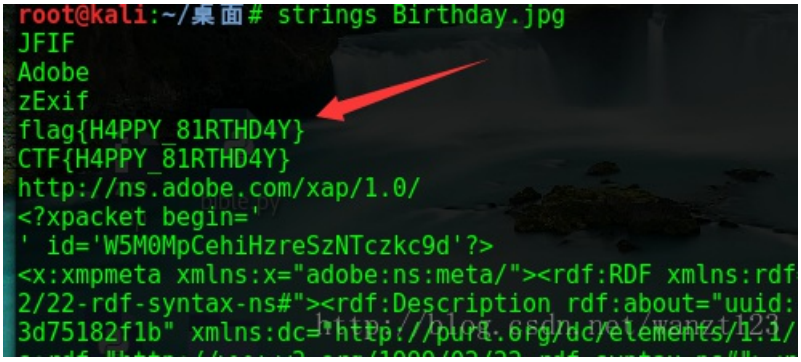
N0thing

下载下来是个流量包，导出http对象，得到以下文件：

~img27	2017/7/21 13:31	文件	1 KB
~img42	2017/7/21 13:31	文件	1 KB
~style.css	2017/7/21 13:31	层叠样式表文档	2 KB
~style.menu.css	2017/7/21 13:31	层叠样式表文档	3 KB
1.html	2017/7/21 13:31	360 se HTML Do...	5 KB
Birthday.zip	2017/7/21 13:31	好压 ZIP 压缩文件	155 KB

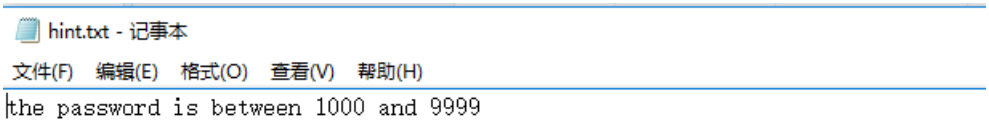
其中只有Birthday.zip文件有用，不过需要解压密码，根据文件名猜测密码应该是生日密码，爆破得到解压密码为：19970818

解压得到Birthday.jpg，strings一下即可得到flag：

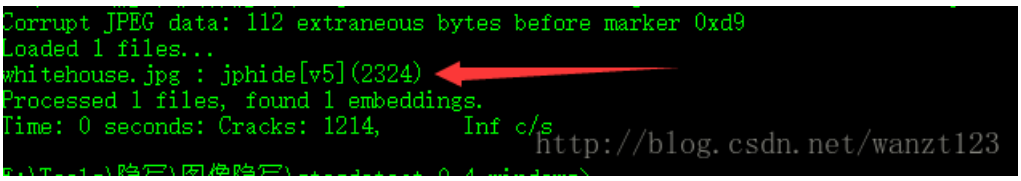


白房子

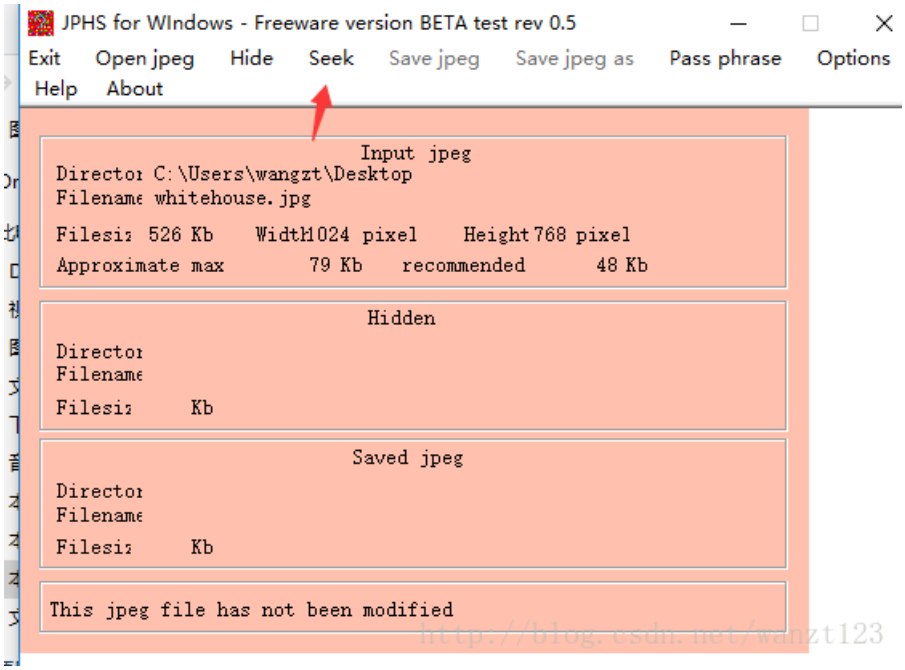
下载后得到压缩包，解压后得到whitehouse.jpg，binwalk一下发现jpg文件后有个rar，提取后解压得到hint：



提示密码在1000-9999之间，用stegbreak爆破可得到密码为2324

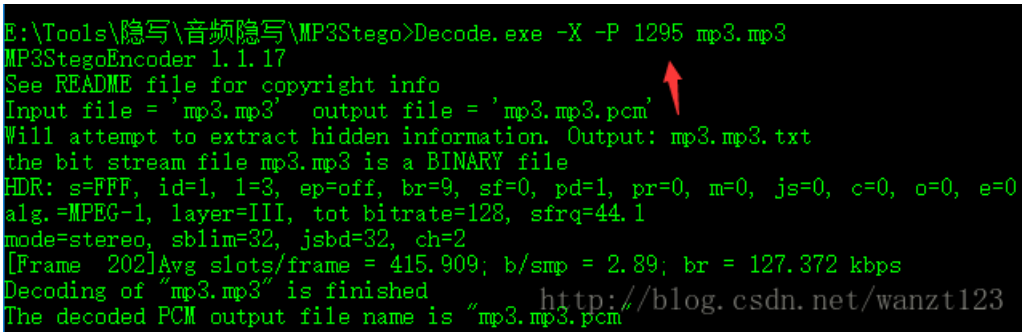


然后使用JPHS，点击Seek，输入密码后选择文件提取路径即可得到flag：



MP3is so good

根据hint.txt中的数据生成二维码，扫描得到提示，密码在1000-1300之间，队友写了个批处理来爆破密码，爆破完之后，查找正确的密码，因为是从上往下找的，找到的最后一个能decode音频文件的密码是1295



但是最终提取出来的是乱码，这个问题困扰了差不多半个小时，后来往上面翻了下，还有好几个能decode mp3文件的密码，第一个能decode的密码是1067

```
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'mp3.mp3'  output file = 'mp3.mp3.pcm'
Will attempt to extract hidden information. Output: mp3.mp3.txt
the bit stream file mp3.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  202]Avg slots/frame = 415.909; b/smp = 2.89; br = 127.372 kbps
[ERROR]Encrypt: unexpected end of cipher message.

E:\Tools\隐写\音频隐写\MP3Stego>Decode.exe -X -P 1067 mp3.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'mp3.mp3'  output file = 'mp3.mp3.pcm'
Will attempt to extract hidden information. Output: mp3.mp3.txt
the bit stream file mp3.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  202]Avg slots/frame = 415.909; b/smp = 2.89; br = 127.372 kbps
Decoding of "mp3.mp3" is finished
The decoded PCM output file name is "mp3.mp3.pcm"

E:\Tools\隐写\音频隐写\MP3Stego>Decode.exe -X -P 1068 mp3.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'mp3.mp3'  output file = 'mp3.mp3.pcm'
Will attempt to extract hidden information. Output: mp3.mp3.txt
```


尝试用密码1067提取，成功得到flag

```
E:\Tools\隐写\音频隐写\MP3Stego>Decode.exe -X -P 1067 mp3.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'mp3.mp3'  output file = 'mp3.mp3.pcm'
Will attempt to extract hidden information. Output: mp3.mp3.txt
the bit stream file mp3.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  202]Avg slots/frame = 415.909; b/smp = 2.89; br = 127.372 kbps
Decoding of "mp3.mp3" is finished
The decoded PCM output file name is "mp3.mp3.pcm"
```


mp3.mp3.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

flag{Brute_fORce_iS_WOnderful}