Hgame2018week3

Misc 部分

0x01 bunny treasure

Wireshark 打开分析，发现下载了 2 个文件 CuteBunny.jpg 和 misc.zip，

```
2431 34.043919    192.168.123.74    111.6.160.116     HTTP     593 GET /CuteBunny.jpg HTTP/1.1
2433 34.054414    111.6.160.116     192.168.123.74    HTTP     440 HTTP/1.1 304 Not Modified
2512 38.838689    192.168.123.74    111.6.160.116     HTTP     465 GET /misc.zip HTTP/1.1
2577 38.853648    111.6.160.116     192.168.123.74    HTTP    1227 HTTP/1.1 200 OK  (application/x-zip-compressed)
```

其中 CuteBunny.jpg 下载失败了。通过文件—导出—HTTP 可以导出 misc.zip，打开发现里面有 2 个文件，解压需要密码，

CuteBunny.jpg *	57,191	57,045	图片文件(.jpg)	2018/1/10 22...	4D262161
flag.txt *	34	48	文本文档	2018/2/16 19...	4DCB68...

想到前面下载失败的 CuteBunny.jpg，回去分析，发现请求的网址

```
Hypertext Transfer Protocol
  GET /CuteBunny.jpg HTTP/1.1\r\n
  Host: p48sc5k3g.bkt.clouddn.com\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
  If-None-Match: "FoYP8mzwhNzTp4NLomVrCjxnC48j"\r\n
  If-Modified-Since: Fri, 16 Feb 2018 12:01:34 GMT\r\n
  \r\n
  [Full request URI: http://p48sc5k3g.bkt.clouddn.com/CuteBunny.jpg]
```

打开将 CuteBunny.jpg 保存下来，推测是明文攻击，用 ARCHPR 进行明文攻击得到解密后的压缩包，获得 flag: hgame{^P1ay_H9am3_2nd_p1Ay_buNNy^}

PS:构造明文压缩包的时候要用 winrar，7z 构造的压缩包无法使用

0x02 画风不一样的她

解压后有 2 张几乎一样的图，用 Stegsolve 的 Image Combiner 分析，一头雾水，面向百度

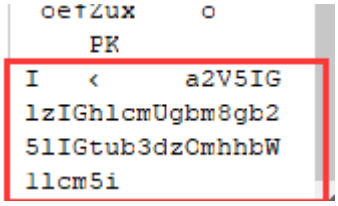
做题后发现大概率是盲水印攻击，使用 https://github.com/chishaxie/BlindWaterMark 这个脚本分析，得到了 flag

hgame{b1ind_water_m4rk_quq}

 这个脚本只适用于 py2，py3 不能用，改了代码也不能用，不要问我怎么知道的

0x03 这是啥

打开发现需要密码，用 winhex 打开在注释里找到



a2V5IGlzIGhlcmUgbm8gb25lIGtub3dzOmhhbW1lcm5i，推测是 base64 编码，解码后得到压缩包密码 hammernb。用 notepad++打开 rgb 发现是一串 RGB 值，用脚本将 RGB 值转换为图像后用 Stegsolve 可以在 redplane 0 得到一张二维码，

然而扫一下发现扫不出来，忽然发现这个二维码和平时的二维码不太一样，反色一下得到真正的二维码，扫描后得到一个文件

打开文件发现又是一串密文，base64 解码后得到一组 hex 值

```
504b 0304 0a00 0900 0000 a3ab 504c c003
582a 3300 0000 2700 0000 0800 1c00 666c
6167 2e74 7874 5554 0900 03a1 dc86 5afb
dc86 5a75 780b 0001 04f5 0100 0004 1400
0000 4d69 a1f1 149d 6b97 e8a9 11d7 a1c6
28ec 12ce 56a1 4e96 4d99 bfd5 9a81 15e8
4b88 3b70 6010 4279 524c 3d11 a659 61dd
f41f 07ba 6f50 4b07 08c0 0358 2a33 0000
0027 0000 0050 4b01 021e 030a 0009 0000
00a3 ab50 4cc0 0358 2a33 0000 0027 0000
0008 0018 0000 0000 0001 0000 00a4 8100
0000 0066 6c61 672e 7478 7455 5405 0003
a1dc 865a 7578 0b00 0104 f501 0000 0414
0000 0050 4b05 0600 0000 0001 0001 004e
0000 0085 0000 0000 00
```

把这些 hex 值转换为 ascii 后发现是 zip 文件，打开发现还是要密码，爆破得到密码 hgame，

得到假 flag: hgame{af2ab981a021e3def22646407cee7bdc} 后找 ngc 学长换取真 flag: hgame{zhe_Sh1_true_F14g23333333333}