Second_Week_Writeup

Crypto

0x1

下先通过阅读代码 并且 nc ip 知道是要发送四位验证码过去 并且最后发送‘i like playing Hgame’ 的 secret code 得到 flag

因为验证码是由大小写字母以及数字构成。于是自己构建字典，然后暴力列举 找到符合的验证码

Misc

0x1Cosmos 的午餐

下载得到 pacpng 文件和一个 ssl.log
折腾了一下 pacpng 文件发现什么都没有
然后把 ssl 导入进去
之后导出 http 对象中发现

追踪 SSL 流发现这是个 zip

```
PK.........z2P....`...z.......Outguess with key.jpg..WX.Q..."...E.RD@...E..H.Az...P.H..  EP.^".....
..o..>.......w3sg..9...{.9w.......*.*."""".K...B..(C.....--.... ..G8.........?.....-h..@J8GE.....l...o~.....
7.............o~.....7...4.v.?......`.x...X.6[..@.`.p$.....T.............................]HDPX. ...[.....Y.
98....4!x.9.....k       k.+.9:..{...?.....H.....)..2P.w.;o.{P.W.^2Py..<].p...B.
r...2.OU...P.......D..X...AHDZZZHXTHTT..B.....
*....!. '.w1........o.[...o!.....[...o.[....^.?\.;W...!8"Ws.%.......\..5.?..\.F|.:....)..d.Bz.:.%.
9..!.QQRP......n..]..$...I).m...n...$   '&....&..M..N.;!.CB........5....5(
jh      .....&!hL..D...v...}....u.H9<...I.B.....Nw.....3.............|b...R.2JO.UT..5..
...MLml........}|!P?...a..."...>$..~LK....._PXT\YU]S[W...........otl|brjzf........kk.}xt|rz.
9...]D.b...O..I....~......!.np...}....uH.<ns..!..$.KE.9.c]......=.....g..b..fX..d..
..]..*b"..#.    .......LiFr....Ewl.........
s..(....k).wGG.....u........?..O.]o0D.H...1..?.[W..     ..|H3T.f.X..L\..!.HR[.sZ...v.j.Z]lta@..
.-..h.
.i......7..(R...A..9P.9Zl..F#}.m....g../...`....|..vG...e..........G.%...@_)...8...O..S.<.}|....h.....V..F..L4
...>/./..?..h..
```

保存为 zip 格式后解压得到一张图片 根据 hint 提示，看了下图片的注释

有一个 Key　然后这里卡了挺久的

但是想起来 么有一个名字是白起的 看图片的名字

Outguess with key.jpg

查了一下 outguess 发现有这么个工具 然后下载到 kali 里面解密

```
root@kali:~/ctf# outguess -k gUNrbbdR9XhRBDGpzz -r '/root/ctf/Outguess with key.
jpg'  flag.txt
Reading /root/ctf/Outguess with key.jpg....
Extracting usable bits:   1161827 bits
Steg retrieve: seed: 3, len: 24
```

得到一个地址　https://dwz.cn/69rOREdu

进去下载了个 zip 包，解压得到二维码 扫码直接得到 flag

0x2 所见即为假

下载得到 zip 包，发现要密码 丢到 hex 里看了 发现是伪加密

```
50 4b 03 04  14 00 00 00  08 00 89 7b  34 50 1e df

55 cb 5d 8f  ae 27 db 5c  6d cb 02 76  06 ff 07 50
4b 01 02 1f  00 14 00 09  00 08 00 89  7b 34 50 1e
```

在 rar 中发现注释 有 F5 字样 百度 CTF F5 发现有 F5 图片隐写 使用 F5 隐写工具成功解密

```
F5 key: N1lD7CQon6dBsFLr
```

```
E:\ctftools\隐写\F5-steganography-master>java Extract 1.jpg key N1lD7CQon6dBsFLr
java Extract [Options] "image.jpg"
Options:
        -p password (default: abc123)
        -e extractedFileName (default: output.txt)

Author: Andreas Westfeld, westfeld@inf.tu-dresden.de

E:\ctftools\隐写\F5-steganography-master>java Extract 1.jpg -p N1lD7CQon6dBsFLr
Huffman decoding starts
Permutation starts
10911744 indices shuffled
Extraction starts
Length of embedded file: 222 bytes
(1, 127, 7) code used
```

output.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
526172211A0701003392B5E50A01050600050101808000B9527AEA2402030BA70004A70020CB5BDC2D80000008666C61672E7478740A03029A9D6C65DFCED50
16867616D657B343038375E7A236D737733344552746E46557971704B556B32646D4C505736307D1D77565103050400
```

得到的 txt 摁键看上去像是 16 进制数 拖去翻译得到 flag

16进制到文本字符串的转换，在线实时转换

16进制到文本字符串的转换，在线实时转换（支持中文转换）

加密或解密字符串长度不可以超过10M

```
526172211A0701003392B5E50A01050600050101808000B9527AEA2402030BA70004A70020CB5BDC2D80000008666C61672E7478740A03029A9D6C65DFCED501686761
6D657B343038375E7A236D737733344552746E46557971704B556B32646D4C505736307D1D77565103050400
```

16进制转字符 字符转16进制 清空结果

```
Rar!□□□□3□□□
□□□□□□□□□□□Rz□$□□□□□□□□ ◆[◆-◆□□□flag.txt
□□□□le□□□□hgame{4087^z#msw34ERtnFUyqpKUk2dmLPW60}□wVQ□□□□
```

0x3 地球上最后的夜晚

下载 zip 包解压得到一个 pdf 和 7z 文件，pdf 文件名说 no password,,,不可能的，一定有东西藏在里面，百度问 pdf 格式的信息隐藏技术，找到一个工具wbStego4.3open ,下载了很久都找不到免费资源，后来在 github 上发现了官方网站 http://wbstego.wbailer.com/

下载后把 pdf 放进去解密得到了 7z 的解压密码

```
Zip Password: OmR#O12#b3b%s*IW
```

解压得到地球上最后的夜晚 doc 文档，里面搜了下没发现什么东西

丢到 binwalk 里看看发现有很多的 zip 文件 用 binwalk -e 命令都分解出来
发现是一些 xml 的文件，然后找了找 在一个 secret.xml 里找到了 flag

<flag>hgame{mkLbn8hP2g!p9ezPHqHuBu66SeDA13u1}</flag>