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

ng.s3.amazonaws.com application/x-www-form-urlencoded 1220 kB e418689cfbcc624a45

追踪 SSL 流发现这是个 zip

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

■ Outguess with key.jpg 属性

剱	安全	详细信息以前的版本	
属性		值	^
说明	月		
标题	Ī		
主题	<u>ī</u>		
分级		****	
标记	3		
备注		Key: gUNrbbdR9XhRBDGpzz	
来》	東	1	

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 <u>https://dwz.cn/69rOREdu</u>

进去下载了个 zip 包,解压得到二维码 扫码直接得到 flag

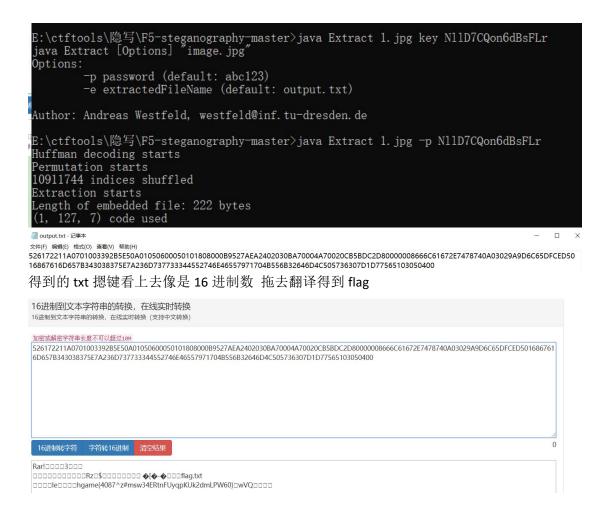


下载得到 zip 包, 发现要密码 丟到 hex 里看了 发现是伪加密

50 4b 03 04 14 00 00 00 08 00 89 7b 34 50 le df
55 cb 5d 8f ae 27 db 5c 6d cb 02 76 06 ff 07 50
4b 01 02 lf 00 14 00 09 00 08 00 89 7b 34 50 le

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: NllD7CQon6dBsFLr



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>