CTF之隐写（详细指导）

转载

GLSakura 于 2019-09-05 23:32:11 发布 5402 收藏 23
分类专栏： CTF 文章标签： CTF 隐写
原文链接：https://www.jianshu.com/p/02fdd5edd9fc

CTF之隐写

0x01 PNG图片

PNG文件结构分析

https://my.oschina.net/ososchina/blog/801358

(1)用16进制编辑工具更改图片的高度，会只显示图片的一部分，下面的部分就被隐藏了，是个藏东西的好办法

找表示宽度和高度的位置的话，可以先看看图片的属性，得到宽高值，转成16进制，搜索16进制值就找到了

注：png图片的保存恢复效果比较好，jpg貌似有点问题

题目链接：http://pan.baidu.com/s/1qY8sxZl 密码：5xam

图片尺寸为500x420(宽x高)

00 00 00 0D 说明IHDR头块长为13

49 48 44 52 IHDR标识

00 00 01 F4 图像的宽，500像素

00 00 01 A4 图像的高，420像素

最后四位CB　D6 DF 8 A为CRC校验

将图片的高改为500像素就拿到flag了

（2）初次遇见条形码。。。。

各种工具找，最后看了writeup才知道这马身上有条形码。。。。。

还是用画图工具拼接出来的完整条形码去扫描的，不会ps愁死人。。。。。

在线扫描https://online-barcode-reader.inliteresearch.com/

(3)烦人de皮卡丘

题目链接：http://pan.baidu.com/s/1i5lG3JZ 密码：lymw

不管是用binwalk还是stegsolve左右点都没有结果，在大佬这找到了答案
http://blog.csdn.net/fuzz_nancheng/article/details/53384353?locationNum=4&fps=1

原理我也不懂啊。。。。。又找到相关文章http://www.tuicool.com/articles/qlNzyum，有待理解。。。。

(3)双图

题目链接：http://pan.baidu.com/s/1pLiCMdd 密码：590r

拿过来图片先用binwalk分析一波，发现有两张图片，用winhex抠出来之后发现和第一张一样，第一张命名1.png，第二张2.png，用linux的compare命令比较一下，

compare 1.png 2.png diff.png,发现diff.png下面有红线，

用stegslove打开2.png选择image combiner

选择1.png这时候会做一个xor运算，保存图片为solved.bmp

winhex打开solved.bmp
，发现除了00就只有这里有东西了

记下地址之后把2.png用ps打开另存为2.bmp，再用winhex打开2.bmp找到刚刚记下的地址把16进制数据复制出来，写个脚本把其中的二进制数扣出来，00为0,01为1然后再把二进制转换成ascii码得到flag

（4）再遇双图

题目链接：http://pan.baidu.com/s/1qYtzZlG 密码：31bg

这次很直接，解压出来就是双图，用stegslove的image combiner

保存反色，再用stegslove对二维码变化一下，得到三张二维码，扫描结果是DES 6XaMMbM7
和一长串字符，des加密，秘钥是6XaMMbM7，解密吧得到flag

（5）py的交易

题目链接：http://pan.baidu.com/s/1c2KmV1A 密码：2m3f

binwalk跑了一下除了很多的zlib什么也没发现，winhex打开看到了几个连续的pypypy。。。。。在一串常规的字符中看到了fireworks。。。

发现图层1被隐藏了，打开后发现了二维码

扫描得到一串16进制

03f30d0a3b8bed56630000000000。。。。。用winhex保存一下看到了CTF字样，

还有pyt。。file一下发现python 2.7 byte-compiled，应该是pyc了，用uncompyle解一下发现flag里有个变量key，那key就是py了。强行符合题目要求。。。

（6）盲水印攻击

这里是利用脚本及说明 https://github.com/chishaxie/BlindWaterMark

当用compare两张png之后发现不再是上面双图情况下的一条红线，而是很多条，就可以考虑一下是不是盲水印攻击了

（7）IDAT数据块隐藏

前面说过png的IHDR属性，在png中，大致分为四个大的数据块，IHDR数据块，PLTE数据块（调色板），IDAT数据块，IEND数据块（结尾标志），IDAT数据块在一个png图像中是可以存在多个的，但是好像正常情况下binwalk检测和插入了IDAT数据块后检测的结果是不一样的，，可以这样来辨IDAT是否有问题

比如这是正常的png图片，分析的结果是

这个图片也是有多个IDAT的块的，而在添加了一个IDAT块之后检测结果是这样

并且FFDA位置是第二个IDAT的起始位置。当把第一个IDAT块扣掉之后原图就会显露出来，

IDAT包含了四部分，第一部分是数据块长度（4位16进制），第二部分是IDAT标识符（4位16进制），第三部分是数据块，第四部分是CRC校验码（4位16进制）

00 00 FF A5（数据块长度为FFA5）

49 44 41 54 （IDAT标识符）

接下来是数据块，在FFA5长度的数据块之后是4位16进制的CRC校验码

并且合并过的IDAT的png图片用fireworks打开会提示格式错误，查看不了，ps就没有这个功能。。。。

0x02jpg图片

（1）图种

题目链接：http://pan.baidu.com/s/1c2L8euk 密码：4h6k

binwalk跑一下发现是两张图片

第二张图片的偏移量是158792，用winhex将第二张图片提取出来保存为jpg格式就是flag了

或者用foremost提取　foremost -v -i 2.jpg -o /root/aa　 aa为空目录

(2)画图

题目链接：http://pan.baidu.com/s/1o7ZkGC6 密码：rmro

这里没有flag,用winhex打开发现图片后面有很多的数据

复制下来保存为txt文件用notepad++转换一下编码

这就是坐标了,这样来画图吧 转换成gnuplot能识别的格式

扫码得到flag

(3)妹子的默默

题目链接：http://pan.baidu.com/s/1c1YjjDA 密码：id5a

binwalk跑一下发现rar文件，但是加密了。。。。找了很久密码，看了大佬的writeup才知道密码是图片上的“喜欢我吗.”注意：密码是汉字不是拼音，解压出来是这个

第一个莫斯电码解码，得到一个网址,根据下面 的提示是AES加密，解密得到momoj2j.png访问http://c.bugku.com/momoj2j.png得到二维码

(4)F5隐写

链接：http://pan.baidu.com/s/1cnMYzs 密码：v0er

cd F5-steganography

java Extract 123456.jpg -p 123456

后会生成output.txt文件，里面就有flag了

0x03bmp格式图片隐写

题目链接：http://pan.baidu.com/s/1jlp82NG 密码：ikov

下载下来之后发现后缀是png，然而winhex打开发现并不是png头文件

file一下是bmp文件，用wbs43open来解密吧http://pan.baidu.com/s/1slc2YHR，

密码值为空

解出来用notepad打开就看到flag了

0x04流量分析

题目链接：http://pan.baidu.com/s/1mi3aWwK 密码：4fd9

（1）下载了一个pcapng的文件，用wireshark打开，过滤条件是http协议，发现了一句话的痕迹

在开始的时候发现

有flag.tar.gz

接下来的http里应该就有这个数据了，在最后一个包里发现

解一下压缩吧

其他

(1)遇到了一个exe文件，用notepad++打开发现是一串ｂａｓｅ６４，直接把代码复制到在线base64转图片得到flag

题目链接：http://pan.baidu.com/s/1kUCWiNX 密码：xlui

在线转换　　http://imgbase64.duoshitong.com/

(2)遇到一个宽带信息泄露的bin文件用routerpassview查看搜索username找到用户名就是ｆｌａｇ

题目链接：http://pan.baidu.com/s/1pLbQzTT 密码：g1i9

(3)linux基本问题

题目链接：http://pan.baidu.com/s/1dFlivh3 密码：olcx

用notepad++打开发现flag.txt,用binwalk提取得到flag.txt

（4）onlyonefile

题目链接：http://pan.baidu.com/s/1geO9DHT 密码：nia7

下载之后先用binwalk跑了一下发现很多zip包，果断分解，发现文件夹里都是布置格式的文件但名字是有规律的，并且还有一个0.zip解压出来也没发现什么，用winhex打开第一个文件看到了PNG，猜想是png图片，但是结尾没有IEND，不完整，打开最后一个文件发现了IEND，题目又叫onefile，应该是图片分解了，于是linnux下cat outfile/* >1.png合成了png图片，但是依旧没有flag，binwalk发现图片后面好多zlib文件，找了很久，再用winhex查看发现了头文件不远处的Adobe Fireworks CS5，下载下来看起来和ps差不多。。。。。。打开图片后原来是两个图层，把第一张图片拉开再翻转一下二维码颜色得到flag了。

（5）再遇Adobe Fireworks CS5

题目链接：http://pan.baidu.com/s/1c3vzum 密码：n26x 题目名为IHDR

这次比较干脆，直接给了一个png文件，winhex打开一切正常，binwalk跑一下还是满大街的zlib包，也发现了Adobe Fireworks CS5字样，于是用Adobe Fireworks CS5打开，发现格式错误。。。。。回去看了看png文件格式，没毛病，那就只有crc没有检测是否正确了，给个crc抄袭的计算代码。链接：http://pan.baidu.com/s/1dFcQTu5 密码：ytxd 里面的数据替换为相应的HIDR Chunk，就得到正确的crc了，再次用Adobe Fireworks CS5打开flag就直接出来了

(6)这个应该属于杂项

题目链接：http://pan.baidu.com/s/1jlwZlFc 密码：bk62

file一下发现是data文件（跟没发现一样），扔到winhex里发现是这样

FF D8不就是jpg头文件,FF D9不就是jpg尾文件标志吗，原来是把16进制逆过来了，写个脚本再还原回来就好了

```
f=open("1.reverseme","rb")
g=open("1.jpg","wb")
f.write(g.read()[::-1])
f.close()
g.close()
```

用ps旋转一下就好了

（7）加密的文档

题目链接：http://pan.baidu.com/s/1misRWU0 密码：b19t

下载得到一个zip压缩包，确实加密了。。。。可是题目没有给密码提示啊，伪加密？试试看，眼瞎的我没有看到在底部50 4B，这个地方改成了09 00

还是找到writeup才回来找，不过看到了大神用010Editor，又get到一个新工具，并且看到未加密是这里是0，加密这里标志位就不是0了

别忘了第二行还有标志位。。。。

好了，改成0，成功解压出一个docx文档，

刚开始还以为是把flag字体和背景颜色设置一样了，结果没有。。。把图片拷出来也没找到。。。。又回来看大神的writeup，解压之后的docx文档还是藏着压缩包。。。。改成zip格式解压出来找到两张图片

吐了一升血。。。。。