ctf杂项小总结

原创

glancelike 于 2019-11-27 21:29:36 发布 573 收藏 5

文章标签： ctf 小白

本文链接：https://blog.csdn.net/glancelike/article/details/103256218

这些题都是bugku上面的题，下次打比赛再来更新

1.liunx2

这道题我用binwalk发现brave有个txt文件，改变后缀名发现是个压缩包后，也没有发现什么，由于没有安装虚拟机也没能想网上大佬使用foremost提取出图片（*虽然图片是个坑*），也没有是用string命令，但最后根据题目所给的提示答案格式key{},直接用记事本打开brave，搜索key,结果真的找到了答案！！有点幸运，以后这种类似有txt还有提示flag的格式的题目也可以采用这种方式。

2.隐写2

这道题目一打开就是一个半个身子的大白，于是很容易的想到或许可以将图片补全，所以打开了16进制编辑器，在第二行找到了对应的高和宽，把高修改后保存,打开图片就可以的到flag

3.白哥的鸽子

这道题目下载后是个图片，行，先用binwalk查看是否用隐藏文件，毫无所获，决定用hex打开，发现最后面有flag和|还有一堆奇怪的符号，不过既然写着flag，应该和答案有关吧，我就去网上找了一下，发现这叫做栅栏密码，学到了！！有“|”字符的就是栅栏密码吧，可能是，逃，不过还要注意可以改变栅栏的位数，才能得到答案

4.闪的好快

打开题目发现是张动图，一直在闪！！于是想到用stegsolve打开，一帧一帧的看图片，发现总共有10多张2维码，扫一张的到一个字母，好累，然后把辛辛苦苦扫到flag输进去，对了哈。

5.眼见非实

文件的名字是zip于是我就把文件改成zip，解压后发现里面有一个docx文件，用word，打开后老报错，行吧。于是我用binwalk打开后，发现里面还有个压缩包，于是用360打开后得到了一堆文件，我找了还久终于找到了。不过，大佬们都说先去document.xml这里查找行吧记住了

6.爆照

题目打开后是一个漂亮小姐姐的照片，查看文件的属性毫无收获，于是用binwalk打开发现图片里面藏着zip，于是用winrar打开发现里面有一张gift,以及很多张名字为8的文件，发现88，888，8888文件大小不同，其他文件大小都相等，此事必有蹊跷，于是用binwalk打开后发现这三个都是图片，更巧的是8888里面还藏着zip,所以把它们都改成图片，发现一张图片有二维码，扫描后得到bilibili字符，第二张图片打开后没有二维码，嗯，果然没有这么简单，打开文件属性后发现，用个大小写字母以及’=‘等于号的字符串，应该是64进制的，用base64解密一下发现silisili，离真相又进了一步，嘻嘻，第三张图片呢，用winrar打开后发现里面还有个图片，打开后就能得到答案了，好长的一道题。

7.猫片

有一说一这道题是真的难，下载完文件的名字是png行吧，那就把格式改成png，又因为题目提示了，LSB BGR NTFS，前两个我懂就是要用stegslove嘛，于是我打开后，按照提示修改后，（就是选3个0，然后选择LSB BGR），预览时，发现写着png，好了，我把它保存为png，没想到却打不开，果然都是骗子，于是我用了winhex打开，发现png前面竟然多了两个非法分子，把它两删除后，就可以了，记住是删除，别想我一样改成00 00，真是的！！打开图片后发现是半张二维码，嘻嘻，把它补全就行呗，先打开文件属性看了一下，图片是280*140的，所以把高也改成280，宽和高都在winhex的第二行记住了，前四个是宽，后四个是高，嘿嘿，怎们修改我也说不清，如果想改高对着宽的改，想改宽对着高改就行吧，反正我是这样的。改完发现是一张反色的二维码，额，用画图软件打开，全选后单击右键，就可以反回去了，终于结束了吧。扫描发现是个百度云的链接，下载后解压发现是一个flag.txt,打开后里面写着flag不在这里，厉害了这道题，突然想到题目还给了一个提示，ntfs，又是我不懂的东西，太强了，只能去看下大佬了，我太菜了，照着大佬的指示，下了一ntfstreameditor，在里面打开文件所在的文件夹，搜索后发现是pyc文件，用python反编译一下，得到了flag的逆过程，自己解密下就得到flag了。

8.神奇的文件

文件下载后是个压缩包，解压后发现里面有一张图片和一个压缩包，打开压缩包后发现里面有一个docx和一张与外面图片一样的，而且打开它们都需要密码，于是想到了明文破解，就是把外面那个图片进行压缩，然后用AZPR，进行破解，需要选中加密的文件以及你压缩的压缩包，就能得到密码了，打开writeup后发现被耍了，angry,用binwalk扫描后发现里面还藏在一个zip，解压后里面有很多文件，一个一个打开发现一个flag.txt，终于得到了答案，嗯嗯。在这里穿插一下我的今天做题的收获（FFD9 到jpg文件的结尾，FFC2后的三个字符到jpg高和宽,文件头是52617271，提醒我们文件是rar格式，还有就是？！.组成的密码是okk编码）

9.啊咧

打开文件发现有个张图片，用binwalk分析一下，发现藏在zip，于是用winrar打开，不用foremost命令的，里面有个txt,需要密码才能打开，于是去图片的属性看一下，发现有一段16进制的数字，将它们转换为字符就得到答案了，16进制转换为字符学到了！！

10.怀疑人生

看题目，出题者真想让我怀疑人生了，哈哈。下载后是个解压包，里面有三个文件，压缩包解压后有个flag.txt，不过需要密码哩，先用azpr试一下吧，注意想用字典查找，不然太浪费时间了，这里只是做一下尝试，失败再从别的地方找。没想到竟然试出来了，密码是password!，打开文件后发现是一串base64的字符，解码后是unicode字符，怎们解密呢？在这里我给大家安利一款软件，ctfcraktools,解出来发现是密码的一部分，行，继续。第二个是写着ctf的图片，用binwalk扫描后，发现里面有rar文件，打开后发现一串有“?.!”组成的字符串，我晕，还没有遇到这种呢，后来找了好久才发现这是okk编码，解密成功。最后一个是一张很模糊的二维码，寻思先扫一下吧，万一呢。结果真的扫描出来了，强呀。把三个组合起来提交正确！！

先写这些了，以后再来