miscmisc

发表于 2021-01-04 分类于 Challenge， 2019， 湖湘杯， Misc
Challenge | 2019 | 湖湘杯 | Misc | miscmisc

点击此处获得更好的阅读体验

题目考点

- *明文攻击*
- *关于LSB图片隐写的解法*
- *word字符隐藏显示*
- *zip加密文件破解*

解题思路

拿到题目 miscmisc，打开后下载附件`buguoruci.png`。

是一个.png后缀的图片，看到图片二话不说直接梭，拖到HXD里面，直接搜索 flag，用F3查找下一处

用winhex分析，我们会看到falg.zip字段，同时也可以看到 `50 4B 03 04` 的数字，没错铁子，.zip文件头是`50 4B 03 04` 下面是我简总结的常见的文件类型和文件头仅供参考

这么多的zip格式文件，为啥不直接把源文件改成.zip格式那，直接梭，改完后成了一个.zip格式的压缩包，很惊喜，打开压缩包后，有如下两个文件，

打开压缩文件 chadian.zip 。会看到一个加密的flag.zip文件和一个加密的flag.txt文本。。。这时候会想到用爆破软件`Advanced Zip Password Recover` 暴力破解.zip压缩包，可是暴力破解了半天，没出来密码。。一给我里个giaogiao。不慌，我们来看 buguoruci.zip 下的 chayidian.jpg ，如下 emmmm，又来张图片

老规矩先放到HXD里看一下，同样搜索 flag ，会看到flag.txt 字段，往上扫一眼，惊喜万分又看到了 .zip文件开头 `50 4B 03 04`字样，直接把jpg格式改为.zip格式。发现可以解压，得到一个 flag.txt 文件，咦，刚才解压chayidian.zip文件时，目录下也有一个flag.txt 文件，查看两个文件的CRC32 可知两个文件一样，很明显这是一个明文攻击，又已知是.zip加密，上工具 `Advanced Zip Password Recover`

软件具体使用方法自行百度，在这里我跑出密码`z$^58a4w`

拿着密码将加密文件 flag.zip解压，得到如下几个文件

打开whoami.zip文件，发现有个加密文本，需要密码，猜想flag就在里面。

打开world.doc文件，只有简单几个字。无用，

打开 world1.png图片，

发现有提示：`pass in world.`

此时想到密码可能与 此图片还有world.doc文件有关。既然是图片隐写，放到HXD里面分析一下，发现没收获，再用经常使用的工具 `StegSolve` 打开图片然后试探各种通道，在LSB BGR条件下发现pass，所以这是LSB信息隐写。得到pass：`z^ea`，去解压文件 发现不行。 LSB隐写详解

根据提示 pass in world 猜想 world.doc 文件里不可能那么简单 可能还会有隐藏文字，百度一下，ctrl+A 全选，右击—字体—取消勾选隐藏。果不其然，发现了隐藏字符，

到此为止，我们从world1.png中得到 pass：`z^ea` 在world.doc文件中得到隐藏字符串。出题人真不要脸，最后来了一个脑筋急转弯，谁会想到最后的密码是 pass内容+world里每行字符串的最后一个字符，就是密码 ：`z^ea4zaa3azf8`

用密码解压加密文本，

Flag

```
1 flag{12sad7eaf46a84fe9q4fasf48e6q4f6as4f864q9e48f9q4fa6sf6f48}
```


Challenge # Misc # 2019 # 湖湘杯
misc4
something in image