【CTF/MISC】一道图片隐写题

原创

mengmeng0510 于 2021-10-28 15:55:00 发布 698 收藏 6

分类专栏： CTF 文章标签： CTF binwalk foremost 010editer base64

本文链接：https://blog.csdn.net/mengmeng0510/article/details/121013065

图片隐写

题目

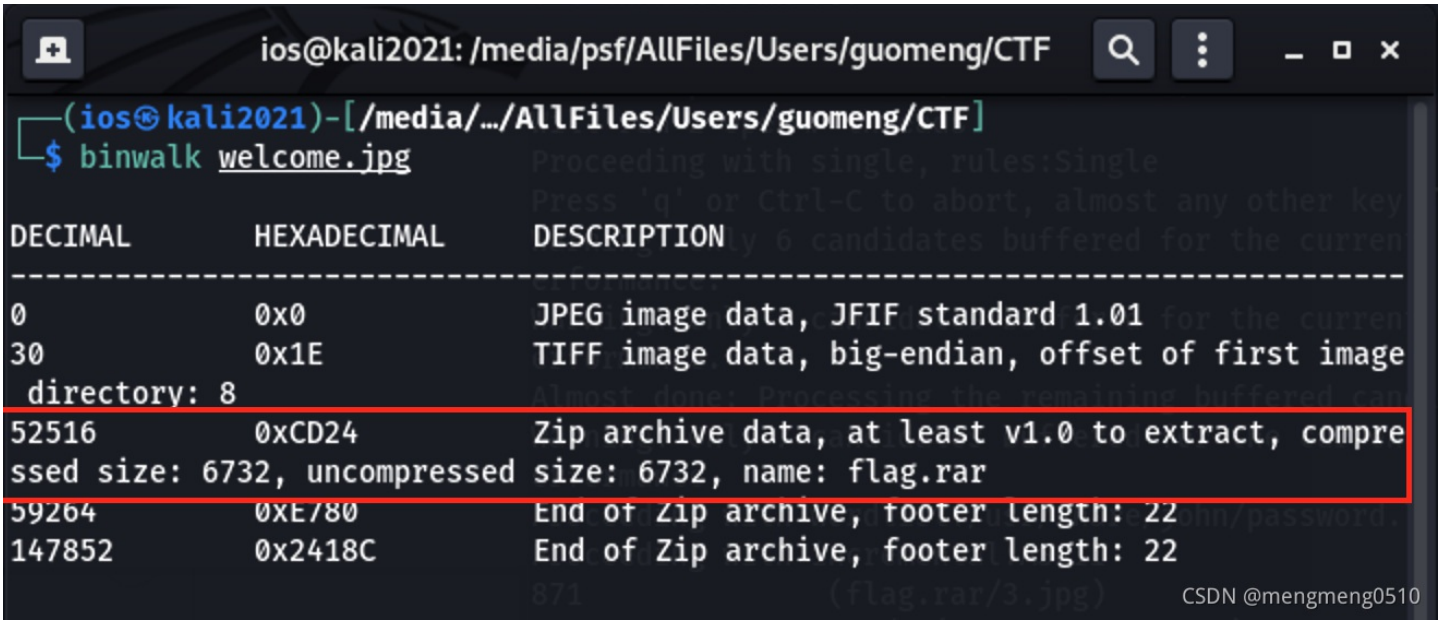
题目是一个图片：

要从图片中拿到flag信息。

解题思路

binwalk工具查看是否有隐藏信息

这里我们首先用binwalk工具查看一下是否有隐藏的文件：



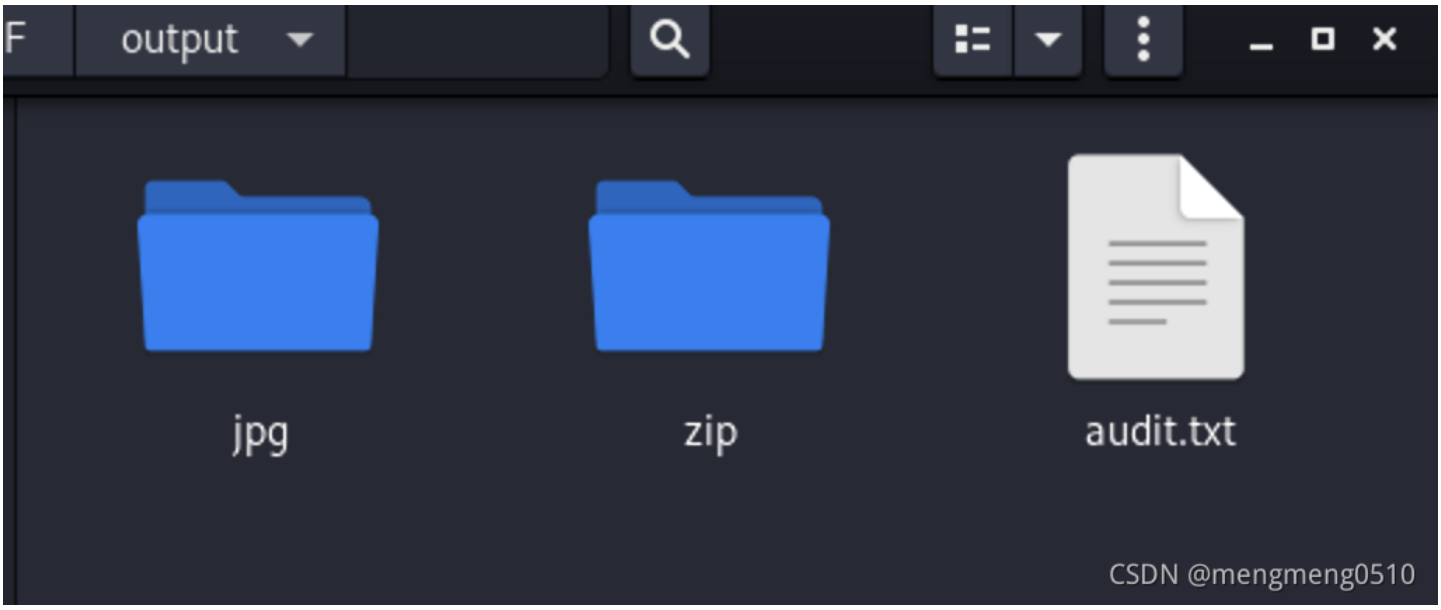
分析之后我们发现其中隐藏着一个zip压缩文件，文件名称是flag.rar。所以我们下一步要把压缩文件提取出来。

foremost工具提取文件

通过foremost工具提取图片中隐藏的文件，在kali中输入如下命令：

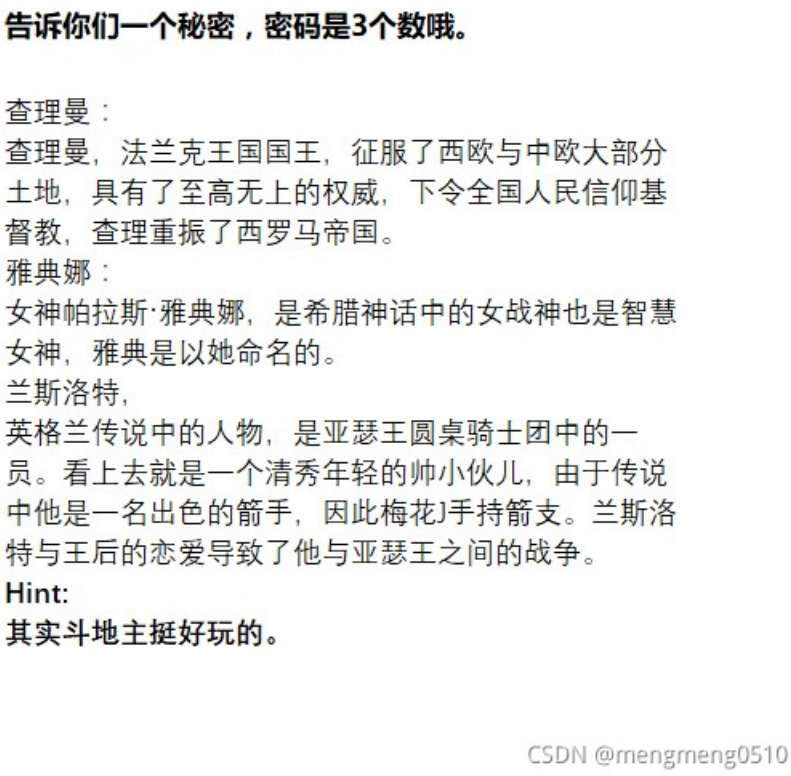
```
foremost welcome.jpg
```

得到三个文件：



点开压缩包，我们看到有一张图片和一个压缩包：

压缩包解压需要输入密码。另外一张图片给出了提示信息：



里面直接提到了“密码是三个数”，所以我们可以考虑对压缩包采用暴力破解。

zip2john工具对压缩包进行暴力破解

输入如下图所示的两个命令对压缩包进行暴力破解：

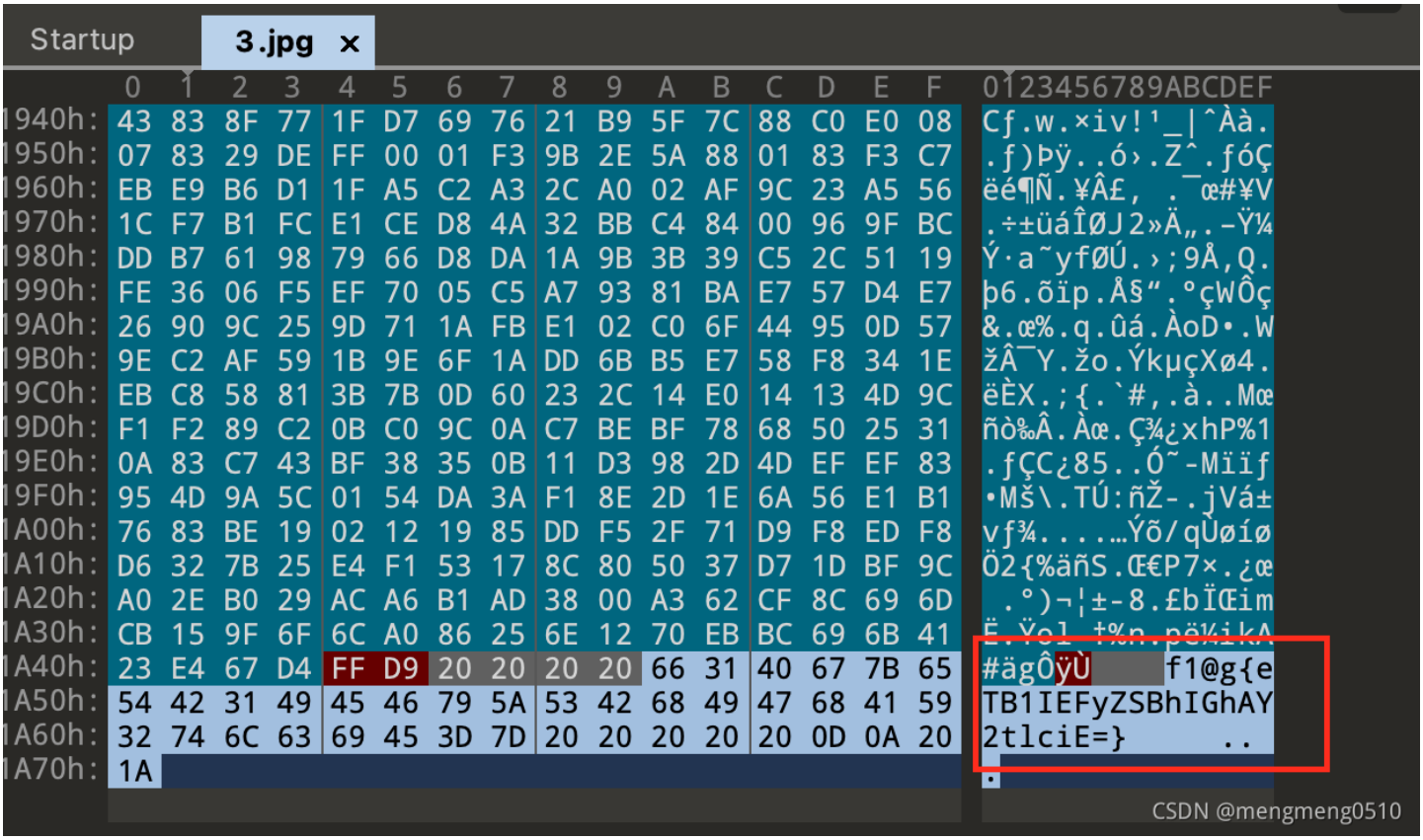
```
ios@kali2021: /media/psf/AllFiles/Users/guomeng/CTF/output...
┌──(ios㉿kali2021)-[/media/…/CTF/output/zip/00000102]
└─$ zip2john flag.rar >>passwd.txt
ver 2.0 flag.rar/3.jpg PKZIP Encr: cmplen=6588, decmplen=6769, crc=102CF126

┌──(ios㉿kali2021)-[/media/…/CTF/output/zip/00000102]
└─$ john passwd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for p
erformance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for p
erformance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for p
erformance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
871              (flag.rar/3.jpg)
1g 0:00:00:23 DONE 3/3 (2021-10-28 12:16) 0.04194g/s 6523Kp/s 6523Kc/s 6523KC/s
kmjjmdo..p0m6
Use the "--show" option to display all of the cracked passwords reliably
```


通过暴力破解我们得到了密码。
之后对压缩包进行解压，得到了一张图片：

哈哈，是不感觉有点崩溃了。一般简单点的题，到这会了一般图片就直接告诉你flag了，但是这会出题人明显是想接着考验你一下。这会我们需要看下新解压出的图片的二进制数据中有没有隐藏着什么信息。

010editer工具查看图片的二进制数据

我们通过010editer工具查看图片的二进制信息，这里有一个窍门，如果图片的开头没有查看到有用的信息，可以直接拉到最后，终于黄天不负有心人，我们在结尾好像发现了点啥：



不过，到这会了，出题人还想再考考我们的编解码知识。我们观察到字符串的结尾是带=号的，这个是非常明显的base64编码的标志。

base64在线编码和解码

通过在线解码，我们得到了我们想要的答案：

```
f1@g{y0u Are a h@cker!}
```

解题心得

这个题目考的还是比较全面的，考到了如下知识点：

- 图片隐藏信息挖掘
- 图片隐藏文件提取
- 图片二进制数据的查看
- base64编解码
  如果我是出题人的话，还可以再在图片大小上做点文章，解压出来的图片是不全的，再让你调整图片的大小，或者隐藏点二维码啥的，哈哈哈。。。，所以有时候做题的时候也可以站在出题人的角度想想他想考你什么，这样可能成长的更快吧。

题目连接

https://ctf.bugku.com/challenges/detail/id/10.html?page=2