bugku 隐写2

原创

shadow_pedestrian 于 2018-11-30 23:51:52 发布 376 收藏
分类专栏： CTF 文章标签： MISC杂项

打开题目，得到下面这个jpg图片

很自然的，我就想到用kali下的binwalk分析一下，得出它里面藏着一个zip文件，用dd分离

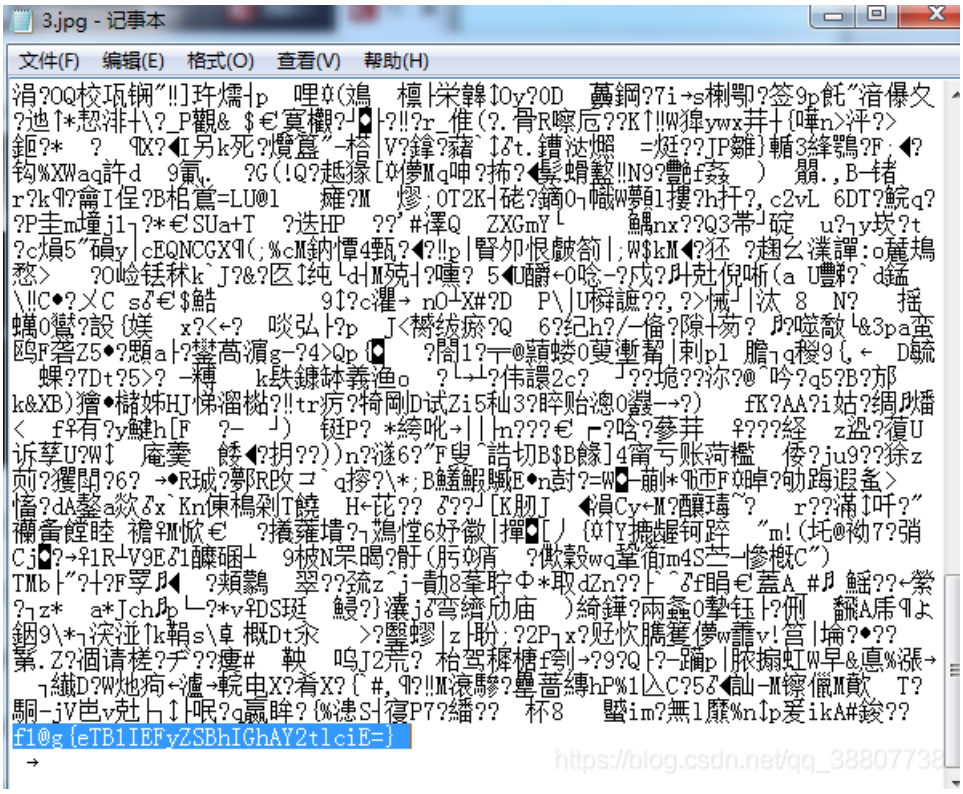
```
root@kali:/mnt/hgfs/kali-linux-1.0.9共享文件夹# binwalk Welcome_.jpg

DECIMAL       HEX             DESCRIPTION
--------------------------------------------------------------------------------
--------------------------------
0             0x0             JPEG image data, JFIF standard  1.01
30            0x1E            TIFF image data, big-endian
52516         0xCD24          Zip archive data, at least v1.0 to extract, comp
ressed size: 6732,  uncompressed size: 6732, name: "flag.rar"
59264         0xE780          End of Zip archive
147852        0x2418C         End of Zip archive

root@kali:/mnt/hgfs/kali-linux-1.0.9共享文件夹# dd if=Welcome_.jpg of=1.zip skip
=52516 bs=1
95358+0 records in
95358+0 records out
95358 bytes (95 kB) copied, 0.181139 s, 526 kB/s
```


这个zip文件直接解压得到另一个rar压缩文件和一个提示图片，这个压缩文件有密码，无法解压，

根据提示图片上的信息可以得出这个压缩文件的密码是三位数，一开始我也被提示图片误导了，它上面的三则故事和其余

文字让我以为这个压缩文件的密码是KQJ，结果不行，没办法，只好用RAPR暴力破解一下它的密码了，

结果RAPR找不到这个文件，这让我对这个文件产生了怀疑，于是用winhex打开这个压缩文件，结果发现它的头是504B0304，这是标准的zip文件头，于是将文件后缀改为zip，再用ziperello暴力破解，ok成功解压得到另一个图片文件，用记事本打开这个图片，在末尾得到flag



这是一段base64加密后的代码，解密就ok了