BUUCTF 九连环 writeup

原创

碧羽o(*￣▽￣*)ブ回雪 于 2021-10-15 11:50:36 发布 90 收藏 1

分类专栏： CTF writeup 文章标签： python

本文链接：https://blog.csdn.net/zhangzhaolin12/article/details/120780249

下载后是一张图片，用kali找到里面有文件。用binwalk进行分离。

```
┌──(root💀kali)-[~/桌面]
└─# binwalk -e 123456cry.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             JPEG image data, JFIF standard 1.01
19560         0×4C68          Zip archive data, at least v1.0 to extract, name: asd/
48454         0×BD46          Zip archive data, at least v1.0 to extract, compressed size: 184, uncompressed size: 184, name: asd/qwe.zip
48657         0×BE11          End of Zip archive, footer length: 22
48962         0×BF42          End of Zip archive, footer length: 22
```

这里分离有有一个asd文件夹，还有一个压缩包，这个压缩包看看里面的内容发现就是asd文件夹里的东西。这里就没有必要解压这个压缩包了，当然要解压也没问题，但是解压时需要密码，在010edit里面找到最后，发现是一个伪加密。这里为什么说是伪加密呢！压缩包伪加密

这里可以查找504b的十六进制，然后看看每一个504b后面的14 00后面的就是加密标记。把01改成00就可以，08也可以一起改成00。改完就可以解压了（这里注意：只有伪加密的情况改后才能正常解压，如果不是伪加密，强行改后仍然可以解压，但是解压出来是乱码）。

```
50 4B 01 02 3F 00 14 00 01 08 08
```

全局方式位标记的四个数字中只有第二个数字对其有影响，其它的不管为何值，都不影响它的加密属性！
第二个数字为奇数时 –>加密
第二个数字为偶数时 –>未加密

经过上述步骤解压后，其实就是asd文件夹里的内容。

然后就是一张图片和一个压缩包，压缩包还有密码，这就是压缩包套压缩包，套了好几层，这应该就是九连环的意思吧！这个的压缩包不是伪加密，不能改加密的标记位。但是这里有一张图片，显然密码就在这张图片里，

又是图片隐写问题。这张图片是steghide的隐写，在kali里执行下面指令（注意：输入y后需要输入密码，又是密码[哭],但是好在没有其他提示，那应该就是没有密码，直接输入回车）发现图片里藏了一个“ko.txt”，这个就是压缩包密码了。

```
┌──(root💀kali)-[~/桌面]
└─# steghide info 11.jpg
"11.jpg":
  format: jpeg
  capacity: 1.2 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
```

```
  embedded file "ko.txt":
    size: 48.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```


然后分离，同样没有密码。

```
┌──(root💀kali)-[~/桌面]
└─# steghide extract -sf 11.jpg
Enter passphrase:
wrote extracted data to "ko.txt".

┌──(root💀kali)-[~/桌面]
└─#
```

解压压缩包后就得到了flag.