PICTURE writeup By K龙

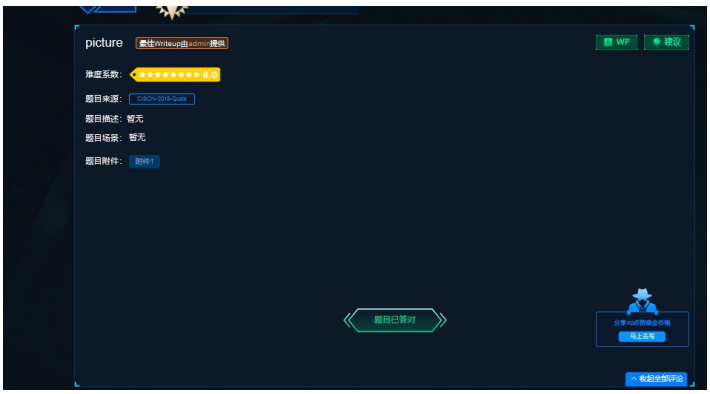
原创

Kayden~龙邵仁 于 2020-07-27 13:16:20 发布 161 收藏 1
分类专栏： 网络安全CTF

本文链接：https://blog.csdn.net/weixin_45801289/article/details/107609609

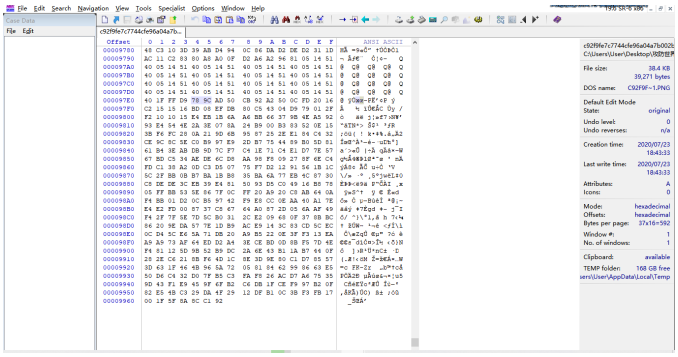
网络安全CTF 专栏收录该内容
8 篇文章 0 订阅
订阅专栏

PICTURE From CISCN-2018-Quals MISC杂项

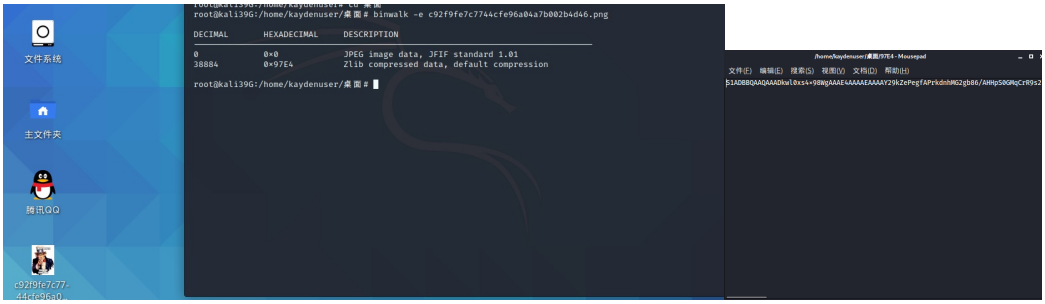


下载附件，得到一图片

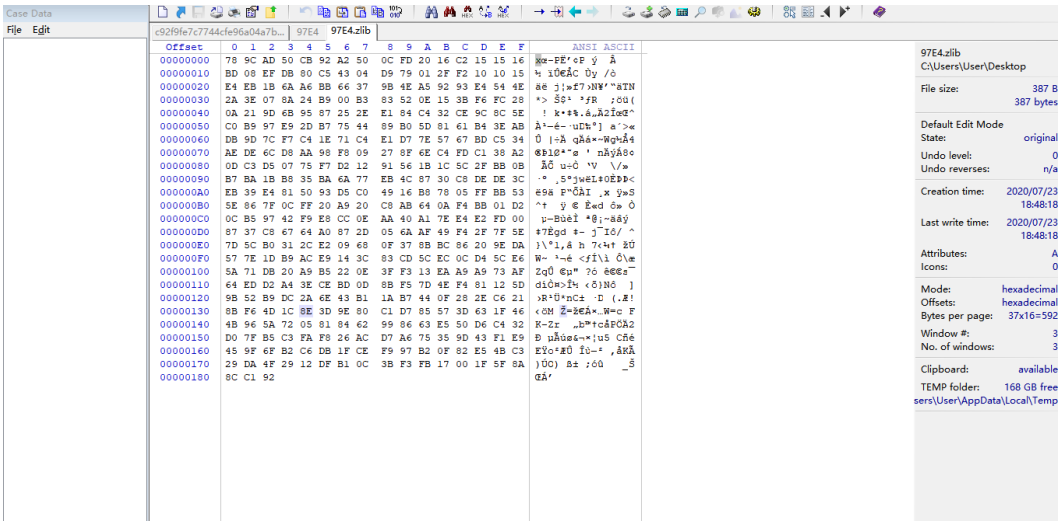
图片用winhex打开，发现zlib文件头

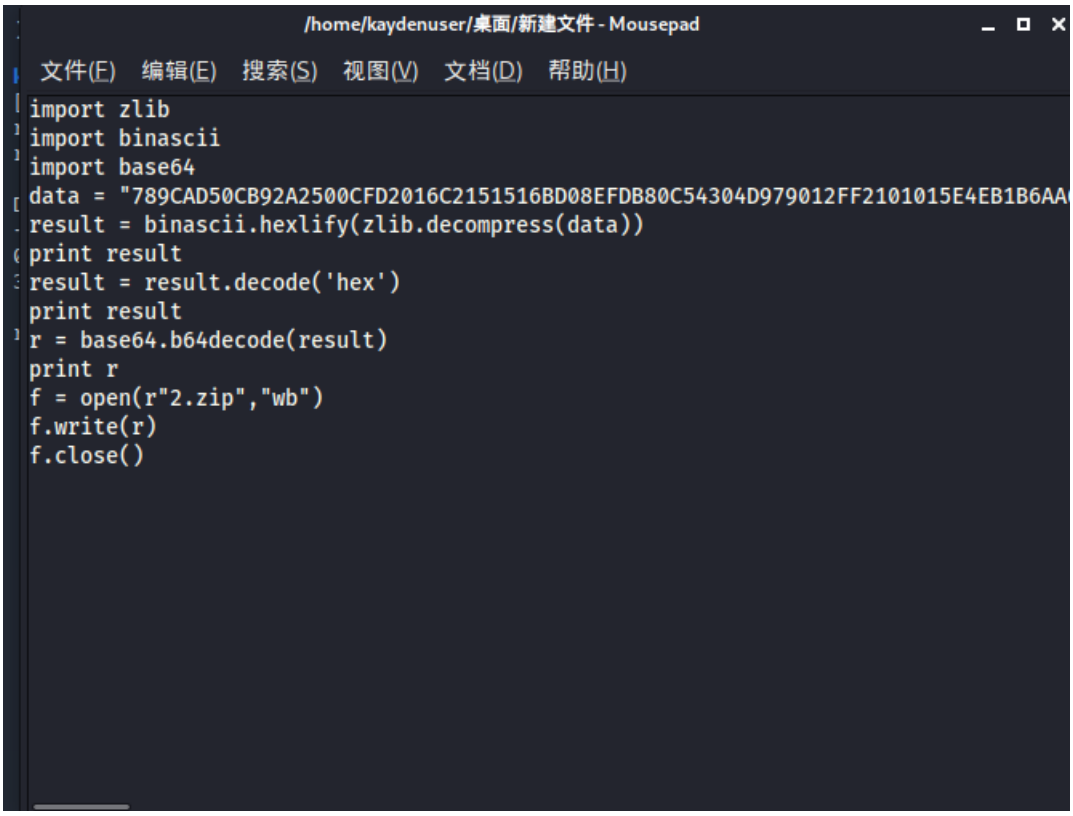


用binwalk把文件分离，得到一个加密压缩文件及一个文本文件



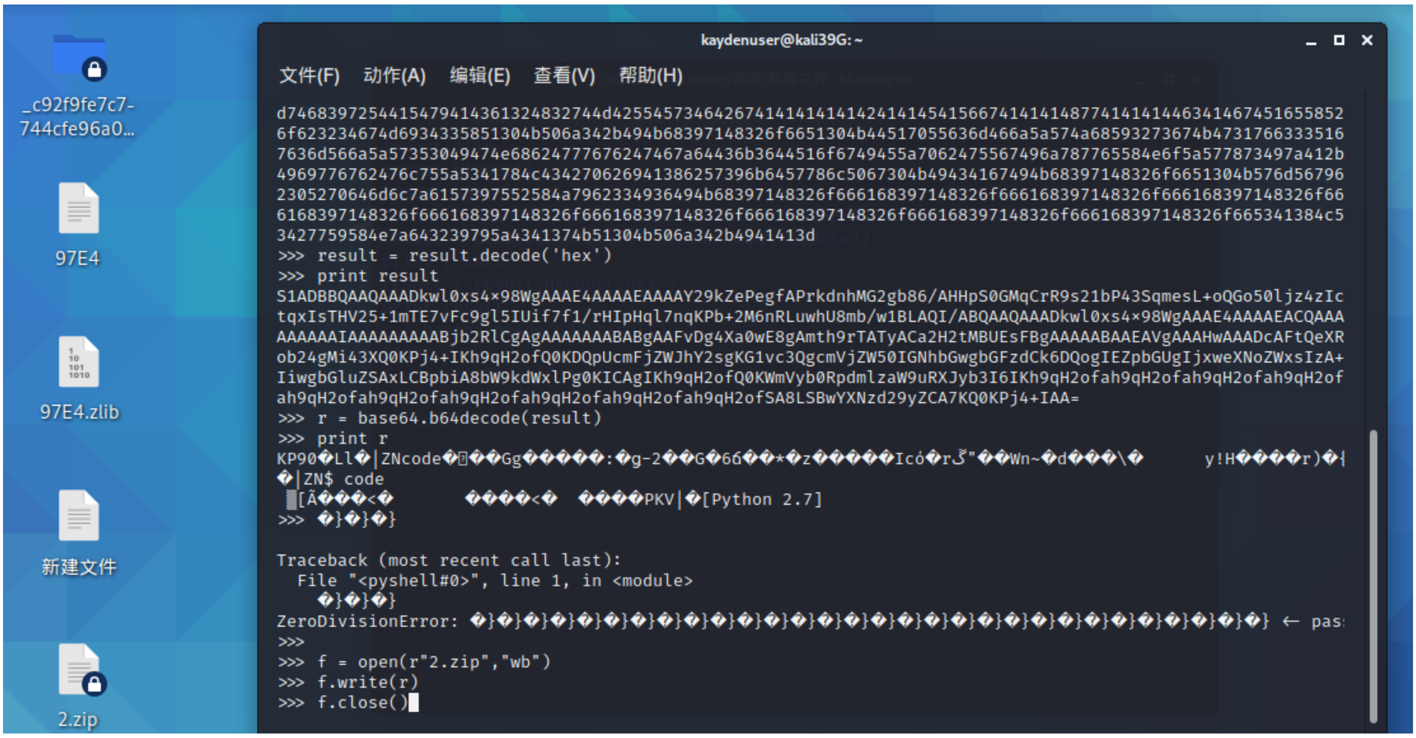
将文件转化为十六进制，发现文件具有ascii编码特征



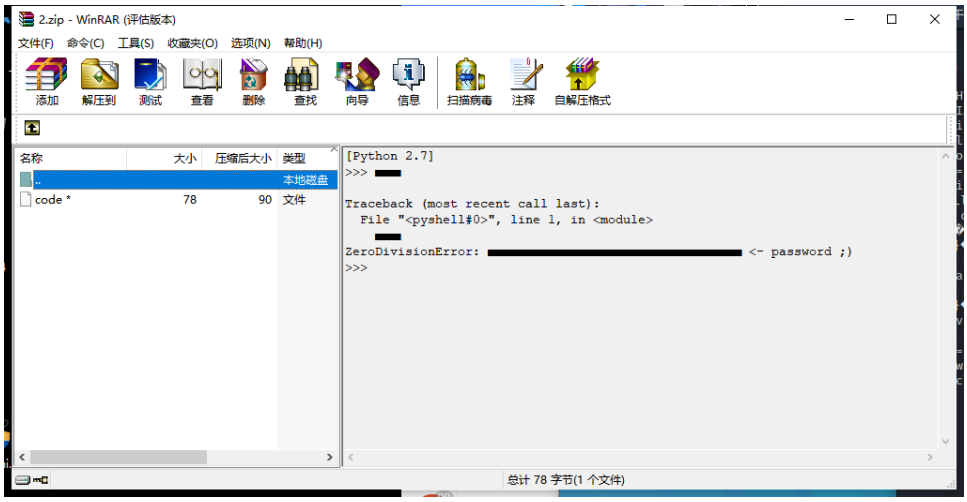


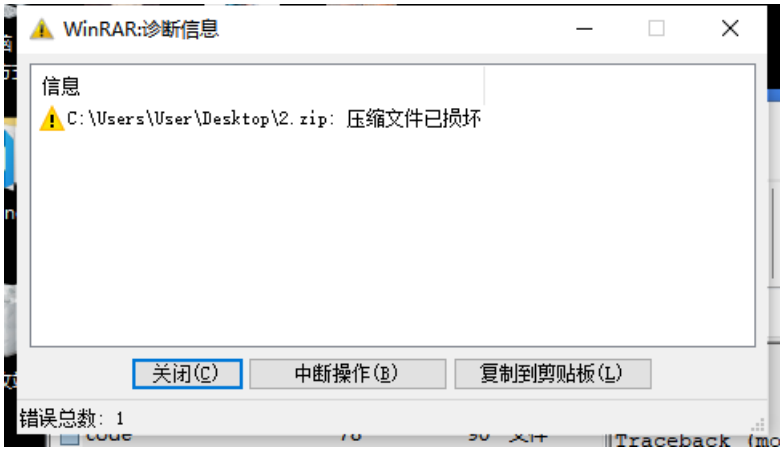
用kali解码后，文件具有base64加密特征，二次解码后把文件转化为zip文件

```
import zlib

import binascii

import base64



data = "".decode('hex')

result = binascii.hexlify(zlib.decompress(data))

print result

result = result.decode('hex')

print result

r = base64.b64decode(result)

print r

f = open(r"test1.zip","wb")

f.write(r)

f.close()
```



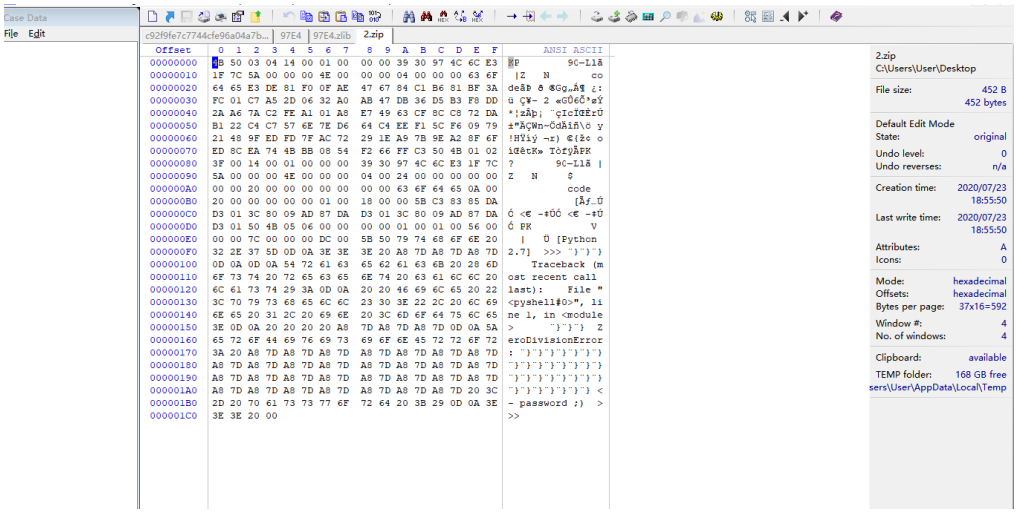
压缩文件打开后，文件破损，附有压缩文件密码提示

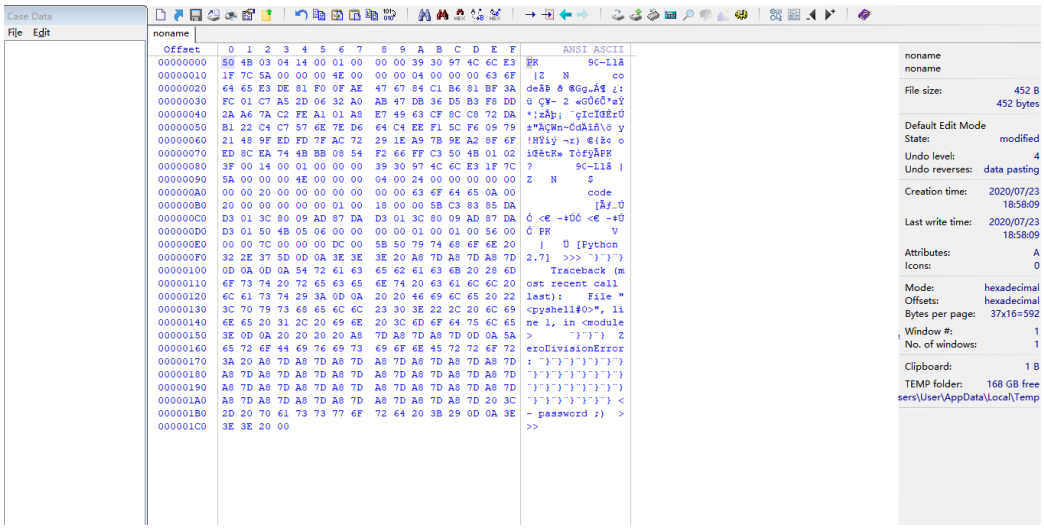




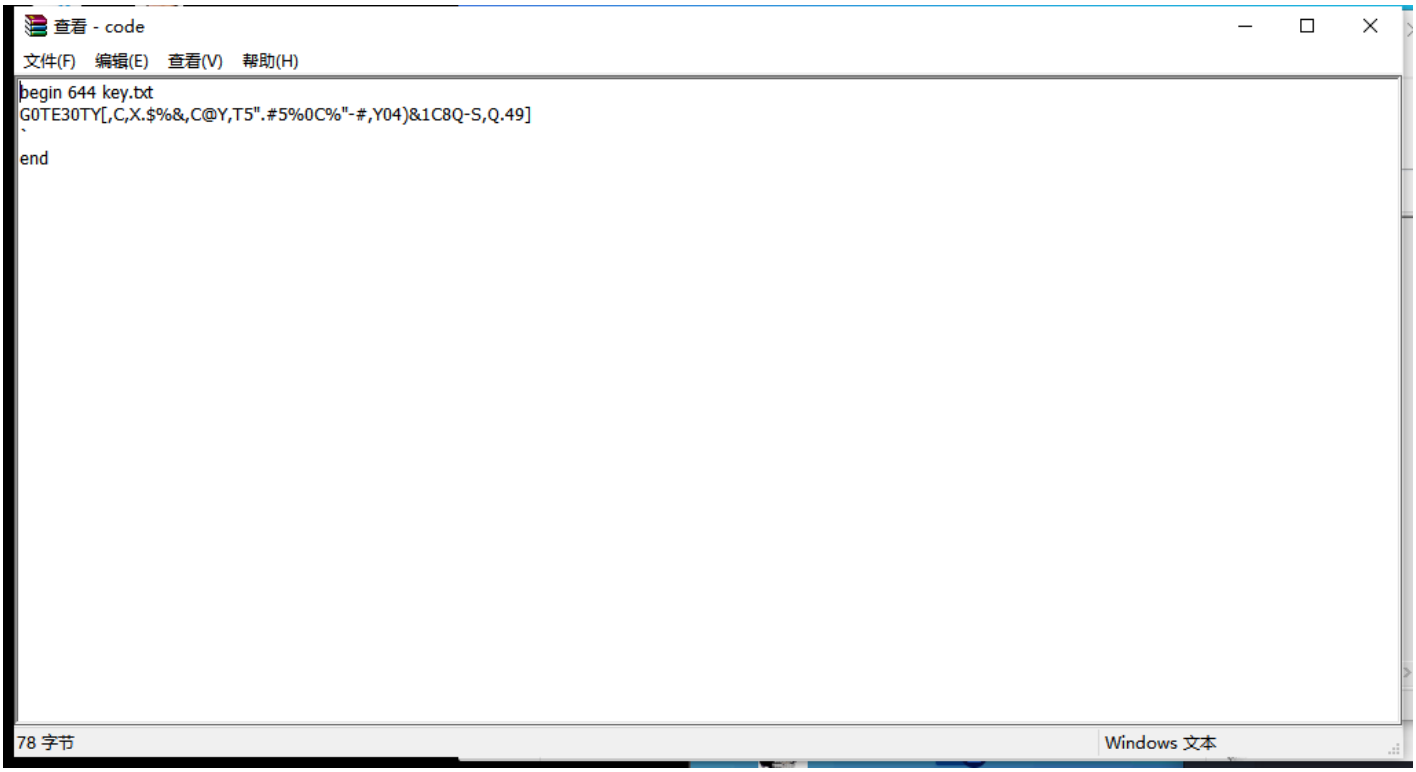
这个位置的提示前期以为是需要用python计算，后来发现覆盖内容为报错内容，只需找到报错提示代入即可。（这个位置个人感觉有点坑，在这里浪费了不少时间）

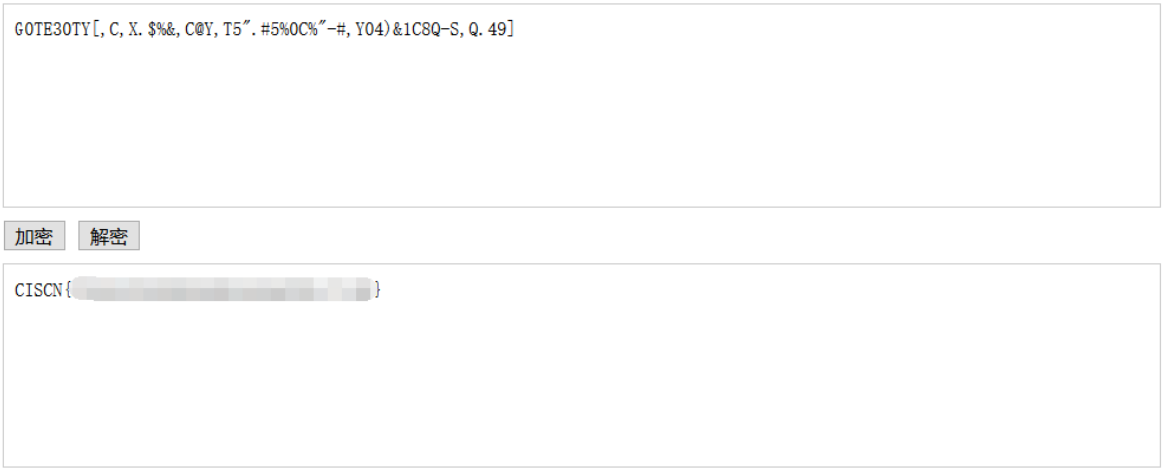
由winhex可知zip文件头前四位应为504B0304，更改后输入所得的密码打开。





原以为打开后可得到flag，文件里的flag显然经过加密。用uuencode解码得到flag。





提交的时候显示答案错误，在建议栏报错后找到官方客服，两小时后再次提交，完成。（为了确认答案还做了第二遍并上传了过程.....）