

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权

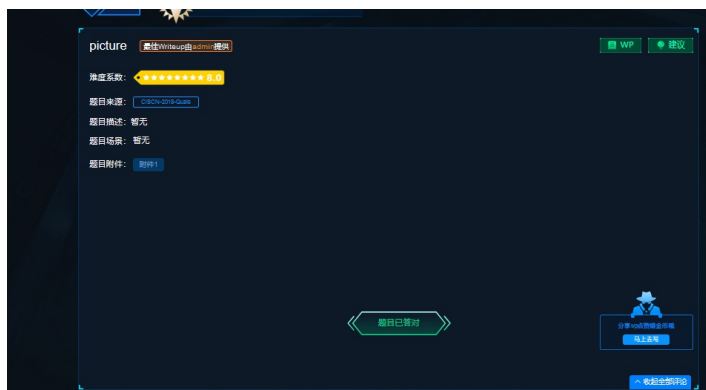


[网络安全CTF 专栏收录该内容](#)

8 篇文章 0 订阅

订阅专栏

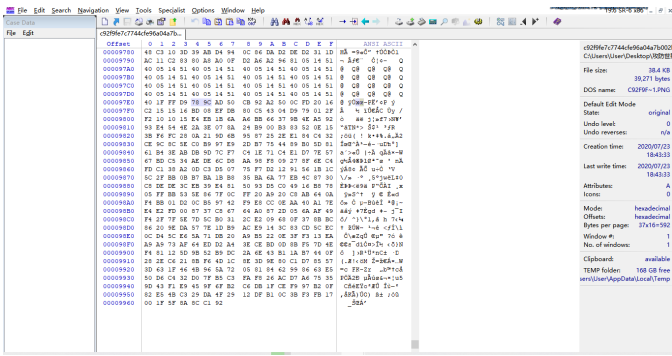
PICTURE From CISCN-2018-Quals MISC杂项



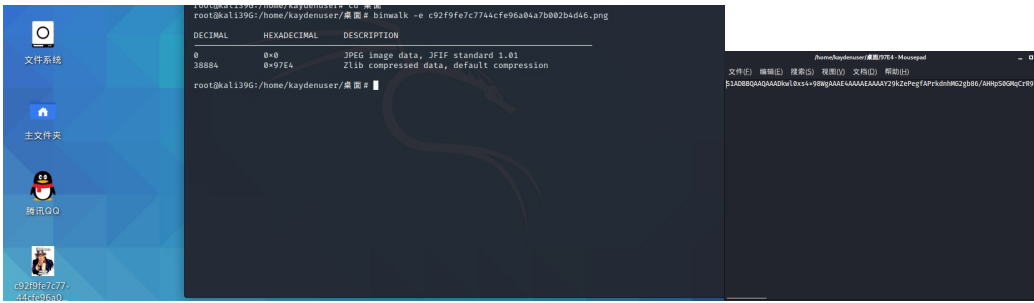
下载附件, 得到一图片



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

Case Data
File Edit
c92f9f7c7744cf96a047b... 97E4 97E4.zlib
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F ANSII ASCII
00000000 78 9C AD 50 CB 92 A2 50 0C FD 20 16 C2 15 15 16 78==FF<F y A
00000010 BD 08 EF DB 80 C5 43 04 D9 79 01 2F F2 10 10 15 4: k0EAc Qy /0
00000020 E4 EB 1B 6A A6 BB 66 37 9B 4E A5 92 93 E4 54 4E Ae j|>Z?Nw'^^TN
00000030 2A 3E 07 8A 24 B9 00 B3 83 52 0E 15 3B F6 FC 28 +> \$0+ ?fr ;o{(
00000040 0A 21 9D 6B 95 87 25 2E E1 84 C4 32 CE 9C 8C 5E ! k+*+.A.k2Ioc^
00000050 C0 B9 87 E9 2D B7 75 44 89 B0 5D B1 61 B4 3E AB A^--e- uDh"] a^>w
00000060 DB 5D 7C F7 C4 1E 71 C4 E1 D7 7E 57 67 BD C5 34 0 1-A gAa--WqA4
00000070 AE DE 6C D8 AA 50 F9 05 27 8F 6E C4 FD C1 39 A2 82A0+e * n&jA0e
00000080 0D C3 D5 07 75 F7 D2 12 91 56 1B 1C 5C 2F BB 0B ÅÖ u-0 'v \s
00000090 B7 BA 1B B8 35 BA 6A 77 EB 4C 87 30 C8 DE DE 3C * .5*jweI+0Edb<
000000A0 EB 39 E4 81 50 93 D5 C0 49 16 B8 78 05 FF BB 53 e5a F^CAI .x y9s
000000B0 5E 86 7F 0C FF 20 A9 20 C8 AB 64 0A F4 BB 01 D2 ^+ y @ Ewd 5w Ö
000000C0 0C B5 97 42 F9 E3 CC 0E AA 40 A1 7E E4 E2 FD 00 p-BuEi *8;-e&g
000000D0 87 37 C8 67 64 A0 87 2D 05 6A AF 49 F4 2F 7F 5E +7Egd t- j^I0/ ^
000000E0 7D 5C B0 31 2C E2 09 68 0F 37 8B BC 8E 20 9E DA \^1,Ä h 7<4+ ZÜ
000000F0 57 7E 1D B9 AC E9 14 3C 83 C0 5C EC 0C D4 5C E6 W-^é <fI\i Öve
00000100 5A 71 DB 20 A9 B5 22 0E 3F F3 13 EA A9 A9 73 AF 2qÜ 6u" 7o e0e2-
00000110 64 ED D2 A4 3E CE BD 0D 8B F5 7D 4E F4 81 12 SD d1C0>I4 <01MG]
00000120 9B 52 B9 DC 2A 6E 43 B1 1A B7 44 0F 26 2E C6 21 R^Ghnc. D (.E!
00000130 8B F6 4D 1C 8E 3D 9E 60 C1 D7 85 57 3D 63 1F 46 <0M Z=3EA--W-c. F
00000140 4B 96 5A 72 05 81 84 62 99 86 63 E5 50 D6 C4 32 K-Zr .b^+c&F0A2
00000150 D0 7F B5 C3 FA F9 26 AC D7 A6 75 35 9D 43 F1 E9 D u0e0e--1u5 C6e
00000160 45 9F 6F B2 C6 DB 1F CE F9 97 B2 0F 82 E5 4B C3 EY0=&Ü I0-+ ,âkÅ
00000170 29 DA 4F 29 12 DF B1 0C 3B F3 FB 17 00 1F 5F 8A (00) Bz :0Ü _S
00000180 6C C1 52 6A'

97E4.zlib
C:\Users\User\Desktop
File size: 387 B
387 bytes
Default Edit Mode: original
State:
Undo level: 0
Undo reverses: n/a
Creation time: 2020/07/23 18:48:18
Last write time: 2020/07/23 18:48:18
Attributes: A
Icons: 0
Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 37x16=592
Window #: 3
No. of windows: 3
Clipboard: available
TEMP folder: 168 GB free
Users\User\AppData\Local\Temp

```
#!/home/kaydenuser/桌面/新建文件 - Mousepad  
文件(E) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)  
import zlib  
import binascii  
import base64  
data = "789CAD50CB92A2500CFD2016C2151516BD08EFDB80C54304D979012FF2101015E4EB1B6AA"  
result = binascii.hexlify(zlib.decompress(data))  
print result  
result = result.decode('hex')  
print result  
r = base64.b64decode(result)  
print r  
f = open(r"2.zip", "wb")  
f.write(r)  
f.close()
```

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)

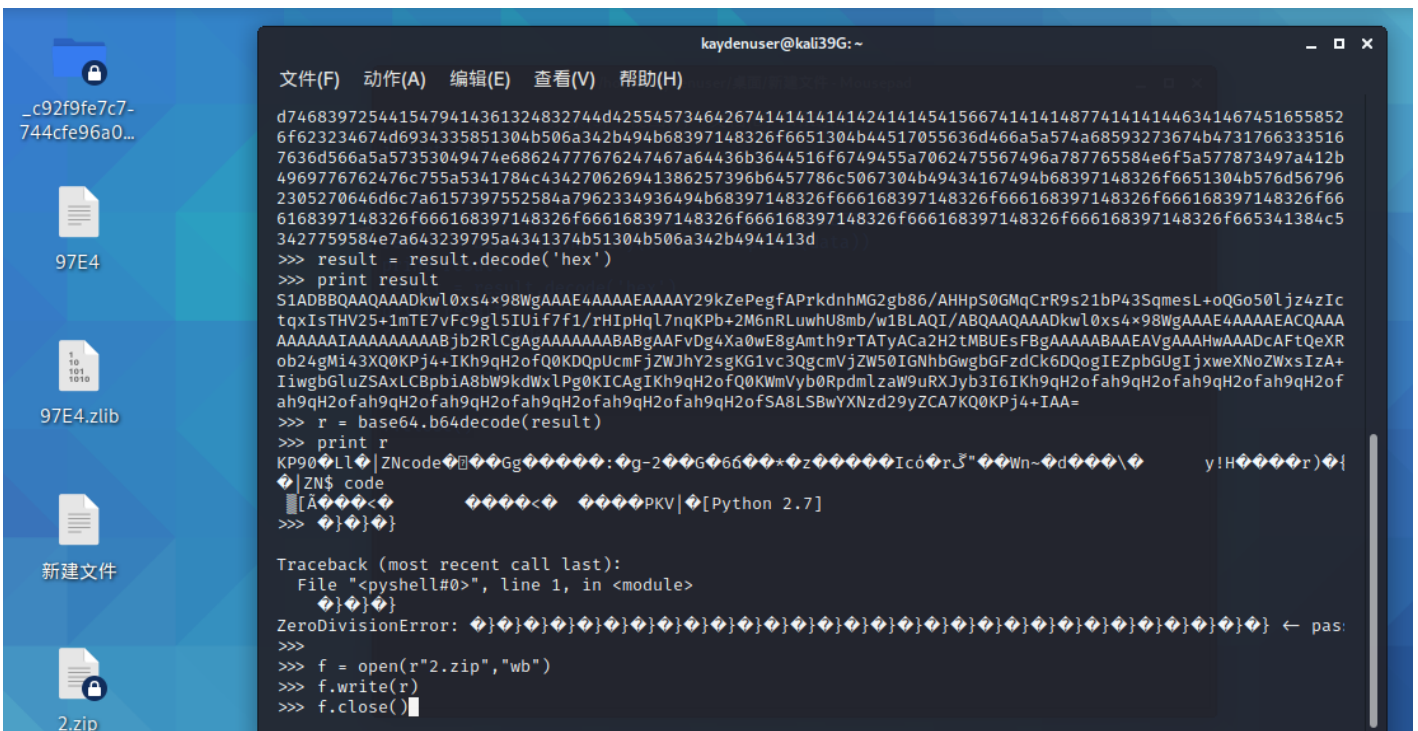
print r

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

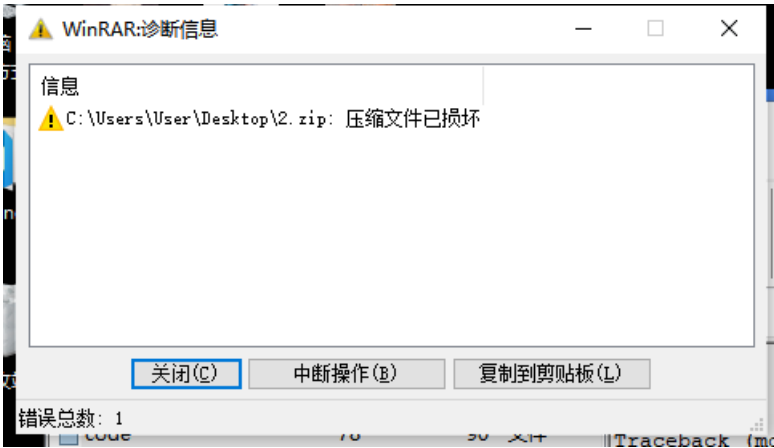
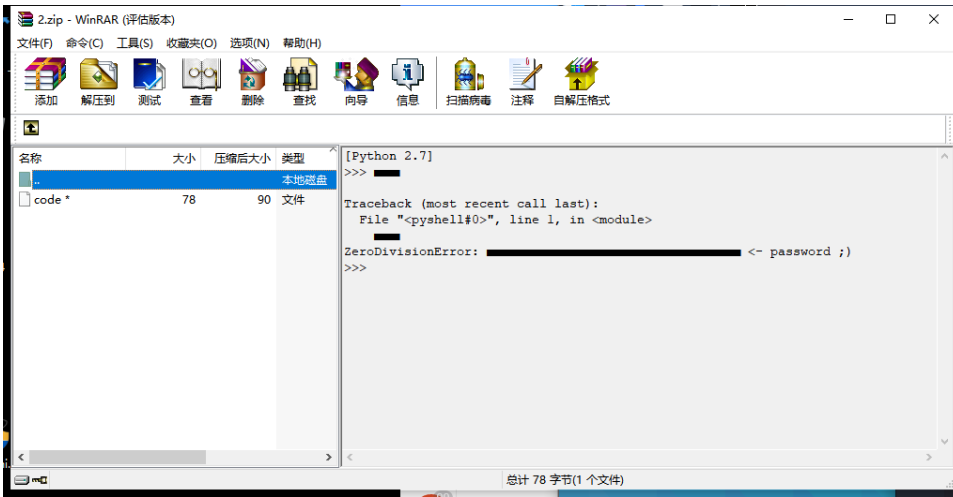
f.write(r)

f.close()

```

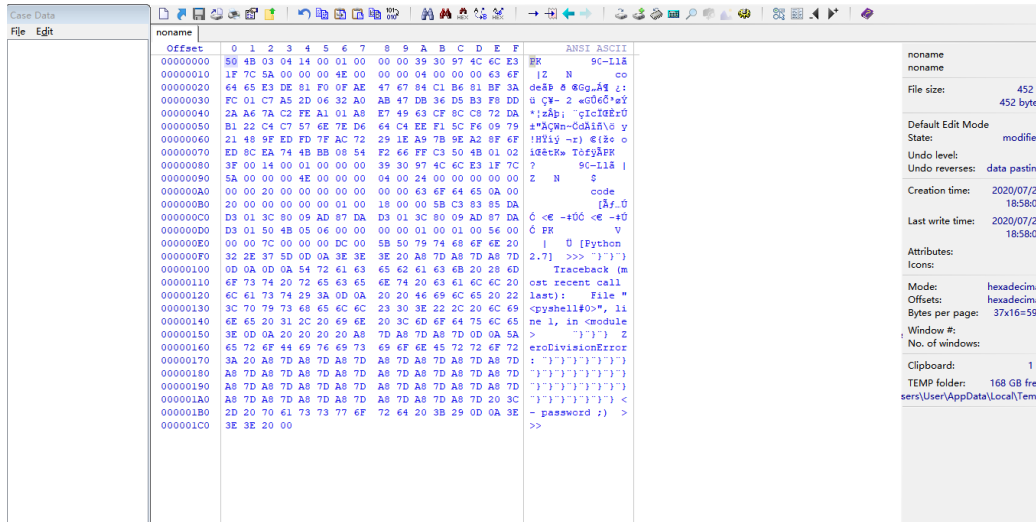
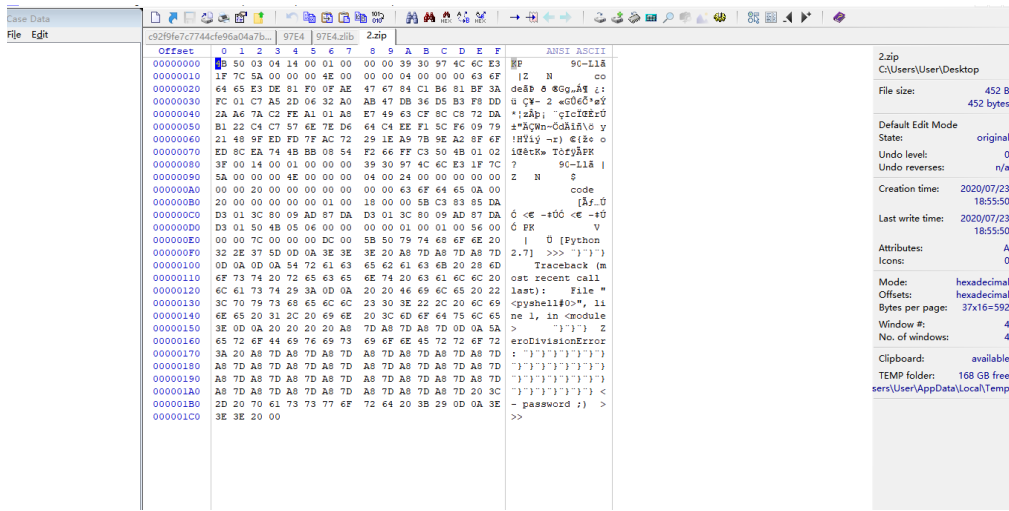


压缩文件打开后，文件破损，附有压缩文件密码提示



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uencode解码得到flag。

```
查看 - code
文件(F) 编辑(E) 查看(V) 帮助(H)
begin 644 key.txt
G0TE30TY[,C,X.$%&,C@Y,T5".#5%0C%"-#,Y04)&1C8Q-S,Q.49]
end
78 字节 Windows 文本
```

```
G0TE30TY[,C,X.$%&,C@Y,T5".#5%0C%"-#,Y04)&1C8Q-S,Q.49]
```

```
CISCN{ [REDACTED] }
```

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.....）