

Jarvis OJ - class10 -Writeup

转载

[baikeng3674](#) 于 2017-09-19 15:53:00 发布 85 收藏
原文链接: <http://www.cnblogs.com/WangAoBo/p/7552266.html>
版权

Jarvis OJ - class10 -Writeup

转载请注明出处: <http://www.cnblogs.com/WangAoBo/p/7552266.html>

题目:

Class10 66 SOLVERS 250 MISC

听说神盾局的网络被日穿之后,有人从里面挖出来一个神秘的文件,咋一看也没什么,可是这可是class10保密等级的哦,里面一定暗藏玄机,你能发现其中暗藏的玄机吗?

[class10.1c40ca6a83c607f424c23402abe53981](#)

You have solved this Challenge! SUBMIT

Jarivs OJ的一道misc, 记录这道题的Writeup主要是想记录解题的脚本

分析:

```
{15:24}~/Desktop ⇨ file class10
class10: data
{15:24}~/Desktop ⇨ binwalk class10
```

| DECIMAL | HEXADECIMAL | DESCRIPTION |
|---------|-------------|---|
| 110 | 0x6E | Zlib compressed data, compressed |
| 1000073 | 0xF4289 | Zlib compressed data, default compression |

```
{15:25}~/Desktop ⇨ strings class10
IHDR
sRGB
gAMA
      pHYs
tIME
IDATx^
caS1
o0n?
h#s-
Ulk{[
Q{jt
:EuV]
oE54
6|l?Q
Y?jHWY
:Emm#8
iV4G
Gw?v
\H%^
EKCI&Y
S?%cp
```

Class10

听说神盾局的网络被日穿之后，有人从里面挖出来一个神秘的机，你能发现其中暗藏的玄机吗？

class10.1c40ca6a83c607f424c23402abe53981

You have solved this Challenge!

Jarvis OJ的一道misc，记录这道题的Writeup主要

分析：

文件下载后是纯数据，binwalk发现为两段zlib压缩后的数据，其中第2段为*default compression*，这是信息1；strings查看字符串，发现IHDR, RGB, IDAT等和图像相关的字符，这是信息2；

步骤：

分理出class10中的压缩数据

```
binwalk -e class10
```

查看分离后的数据

```
{15:34}~/Desktop/_class10.extracted ⇨ ls
6E 6E.zlib F4289 F4289.zlib
{15:34}~/Desktop/_class10.extracted ⇨ file *
6E: empty
6E.zlib: zlib compressed data
F4289: ASCII text, with very long lines, with no line terminators
F4289.zlib: zlib compressed data
{15:34}~/Desktop/_class10.extracted ⇨
```

由信息1，F4289.zlib为default compression的zlib数据，对其进行解压缩（当然binwalk厉害得很，binwalk -e分离后的F4289已经是解压缩过得数据了）

```

{15:37}~/Desktop/_class10.extracted → bpython
bpython version 0.16 on top of Python 2.7.13 /usr/bin/python
>>> import zlib
>>> with open("F4289.zlib") as f:
...     s = zlib.decompress(f.read())
...
...
>>> s
'000000010011101101010100000001111101010100111011101111001000101110010011111
01010001001000101001010010111010100010010001011101100011111010001001111011100
001000000101111000000001010101010101000000011111110111110011011111111111001
0000110011010010000110100101001111010100001111000111110011000011100101011100101
000111111110000000001101101110110110000100001111000011110000111001010000010010
0111111111001001010000100101100010101110011100110100000000000000000001010101010
1010100000101000010010010111001011011011001010011110110000010010110100001111111
1100010111001100011101110010010110000000111101000000110011111111100100000001
110111100000001001100011001010100111011110100100100011001110100001000101011010
0101010000010000100010111010101010010011100100010101110011001011011011011011111
010000010110001101101000000001111100001100011110011'
>>> len(s)
841
>>> 841 == 29 * 29
True
>>>

```

如上，解压后为29 × 29位的01字符串，再结合信息2，设想生成一张29*29的方形图片，像素点与字符串对应，始0和1对应的像素点分别为不同黑白两种颜色，代码如下

```

1 #!/usr/bin/env python
2 # -*- coding: utf-8 -*-
3 __Author__ = 'M4x'
4
5 from PIL import Image
6
7 SIZE = 29
8 img = Image.new("RGB", (SIZE, SIZE))
9 with open("./F4289") as f:
10     str = f.read()
11     # print str
12
13 i = 0
14 for y in xrange(SIZE):
15     for x in xrange(SIZE):
16         if str[i] == '0':
17             img.putpixel([x, y], (0, 0, 0))
18         else:
19             img.putpixel([x, y], (255, 255, 255))
20         i = i + 1
21 # img.show()
22 img.save("img.png")

```

生成了一个二维码，扫码即可拿到flag



转载于:<https://www.cnblogs.com/WangAoBo/p/7552266.html>