安全-Thor‘s a hacker now（i春秋）

原创

小狐狸FM 于 2020-09-03 18:27:57 发布 197 收藏

分类专栏： 安全 # CTF夺旗 文章标签： python linux lzip

本文链接：https://blog.csdn.net/smallfox233/article/details/108390067

安全 同时被 2 个专栏收录

91 篇文章 8 订阅

订阅专栏

CTF夺旗

38 篇文章 0 订阅

订阅专栏

文章目录

前言

> 进行解题过程中需要使用到虚拟机的kalinux

一、题目

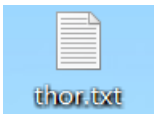
Thor has been staring at this for hours and he can’t make any sense out of it, can you help him figure out what it is? `thor.txt`

二、解题方法

点击题目中的thor.txt打开新的网页

```
00000000: 4c5a 4950 01b3 007f b61b edf0 8440 58e3  LZIP.........@X.
00000010: 91de 1027 5861 8a67 4282 46a4 92f9 4cad  ...'Xa.gB.F...L.
00000020: 2d5d 14eb 3099 2c31 01c2 d13a 74d2 c620  -]..0.,1...:t..
00000030: de27 3a8f fa92 0644 5468 2d02 01fa 24bb  .':....DTh-...$.
00000040: 719f a0fd a191 1678 8bff a2c4 2627 9871  q......x....&'.q
00000050: 83bf cff2 f8af 99fa c465 2b7c 6bdf ee3c  .........e+|k..<
00000060: b71b f61b 0b5e 0ce7 d14f f6a8 0466 6470  .....^...O...fdp
00000070: de67 02da 7be1 1abd e9f0 ac87 131a bcc0  .g..{...........
00000080: 0b0b 9f31 9400 48e3 616a 8f3f 4804 79ad  ...1..H.aj.?H.y.
00000090: a6bb 863a f641 01da b1ee c4fe b338 9289  ...:.A.......8..
000000a0: 2a90 8302 4170 773c 88d3 2641 d274 f533  *...Apw<..&A.t.3
000000b0: 84cf e7d9 f687 3b12 1516 970e 04c2 cfdd  ......;.........
000000c0: c1ca dc46 981d 2a7c 1b39 cb0b 4f8c 58cc  ...F..*|.9..O.X.
000000d0: 46b4 9744 4cb1 fbd3 c632 f36d ecbf 4789  F..DL....2.m..G.
000000e0: 00b8 d4fc 51a8 394e de2a 1a2d 3c43 179c  ....Q.9N.*.-<C..
000000f0: 9623 f971 2935 9564 9e15 c771 c3d5 d8b1  .#.q)5.d...q....
00000100: a7fa 3c0c f869 b829 f6d6 f145 6d57 b3a1  ..<..i.)...EmW..
00000110: bd3f 3fc2 a41f 7e35 089c de29 1d55 debf  .??...~5...).U..
00000120: 5400 c548 5c02 cd6c f853 e3e6 56b2 e395  T..H\..l.S..V...
00000130: 29d8 3985 d307 d46e 854c 4987 aab8 a5cb  ).9....n.LI.....
00000140: 2fea 6b20 6d24 34b3 a2a3 c8e4 247c 6681  /.k m$4.....$|f.
00000150: 51db 7851 752e 4186 2db9 01ae 39ae fed0  Q.xQu.A.-...9...
00000160: 7a77 a8e7 82b2 c78c 272b e621 44d2 03a3  zw......'+.!D...
00000170: f3fb adf9 18b4 681a e4e4 5b17 3c66 128c  ......h...[.<f..
00000180: f544 4124 0083 6db4 0e6b be29 2142 16b7  .DA$..m..k.)!B..
00000190: dd6e 9b78 26a6 71b1 2ec2 dfce 2d6e 8d01  .n.x&.q.....-n..
000001a0: 1786 d101 f184 a798 b0eb c3c8 8a0c a867  ...............g
000001b0: 34e7 0c71 c350 722e e1be 9913 cfb3 a6bf  4..q.Pr.........
000001c0: aa79 8eeb 8df6 02b1 e541 e0ed d3a1 ca85  .y.......A......
000001d0: 469d 0589 99ab 2e77 e388 0180 c7e4 83e8  F......w........
000001e0: 867b 5036 7bd8 a29c 3c08 8457 e5e9 f5e0  .{P6{...<..W....
000001f0: 0432 4673 3aed 4a36 2716 3b35 8661 2d44  .2Fs:.J6'.;5.a-D
00000200: 31a5 45b9 cbee 8028 48a6 74f2 af56 d769  1.E....(H.t..V.i
```


你可以使用快捷键`CTRL+S`将该页面保存到本地



这个文本中的内容和`Winhex`等十六进制查看的软件界面内容类似，我们可以先将该信息中的十六进制值进行读取。

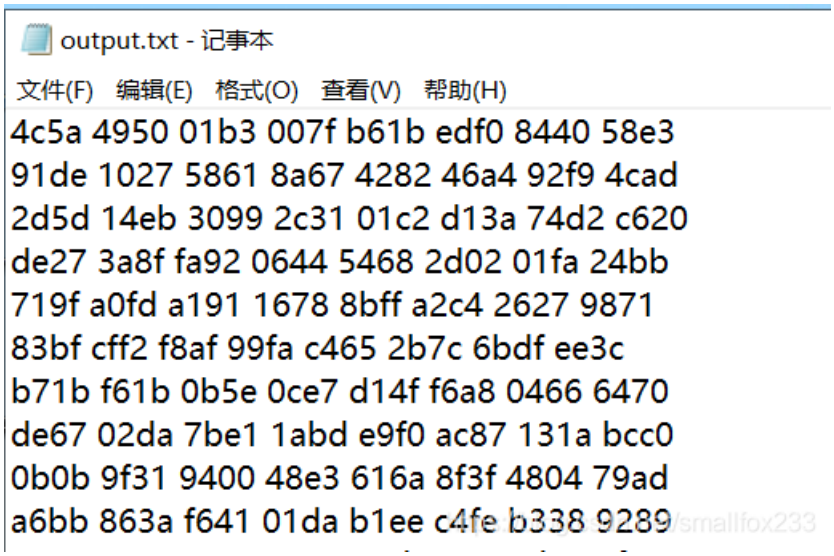
可以看出，每行的第`11`个字符至第`49`个字符都是十六进制的值

可以通过写脚本，将文本中每行的十六进制值提取出来，代码如下。

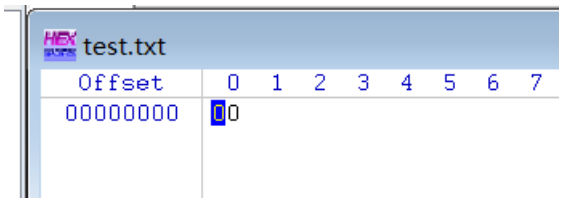
注： line[10,49]切片时，是左开右闭，即(10,49]

```python
#作者：小狐狸233
string = ''
with open('thor.txt','r')as fp:
    while 1:
        line = fp.readline() #每行的字符
        if line =='':#读取到末尾时
            break
        string += line[10:49]#切片，获取十六进制值
        string += '\n'

with open('output.txt','w') as fp: #将十六进制写入文件
    fp.write(string)
```

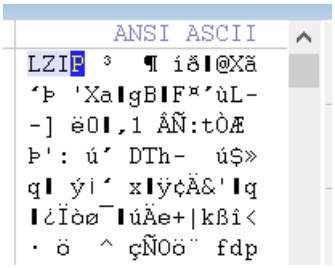


然后使用快捷键`CTRL+A`将文本的内容全选，并`CTRL+C`复制。
在`winhex`中新建一个文件



使用快捷键`CTRL+V`将十六进制值黏贴，黏贴的格式选择为`ASCII Hex`

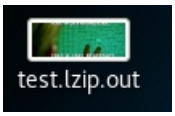
在ascii处可以看到文件头是`LZIP`，推测是`.lzip`的压缩文件，并将其后缀改为`.lzip`



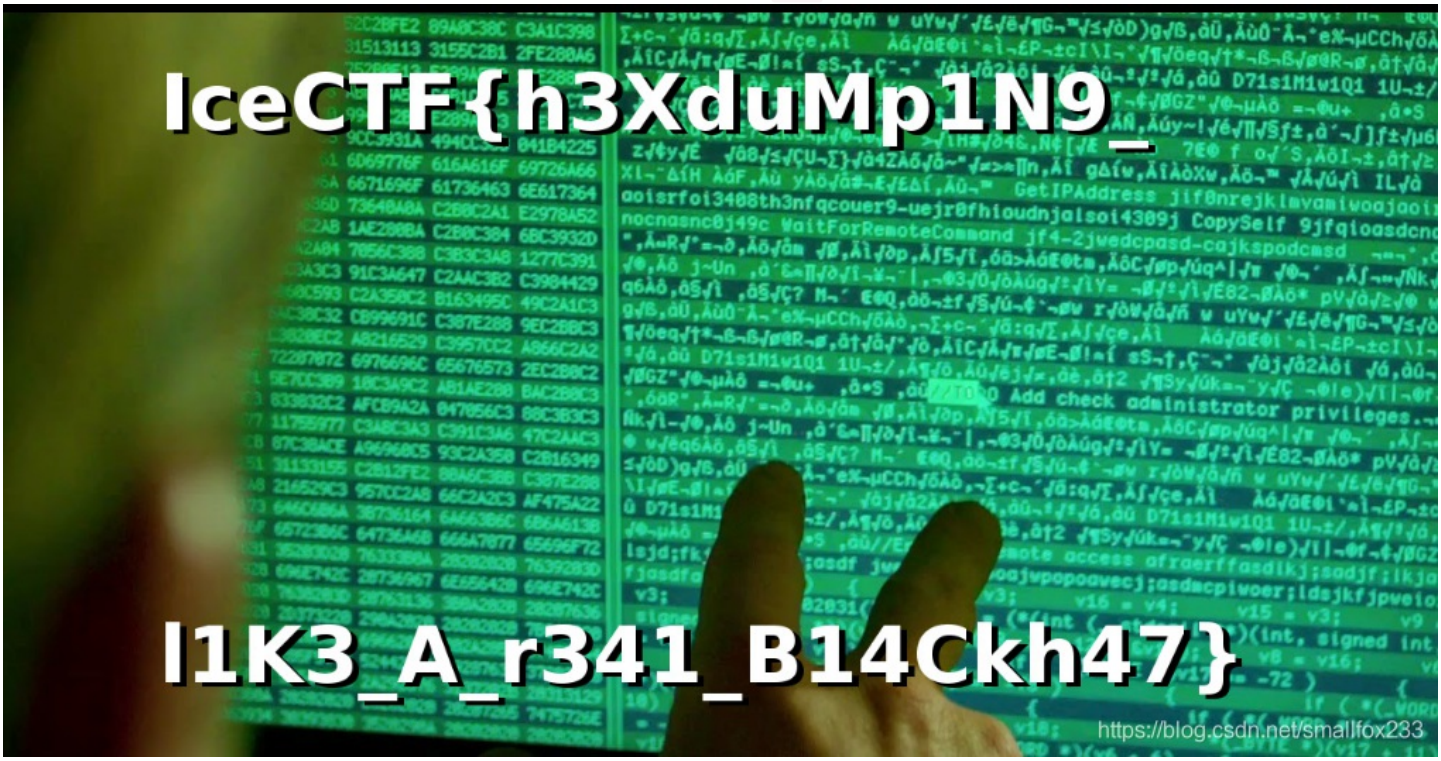
之后就需要用到kailinux中的lzip来进行解压缩了
先在终端输入`apt-get install lzip`来下载`lzip软件`

下载完毕后，转换到压缩包所在路径，使用指令`lzip -d [文件名]`进行解压缩即可。

```
root@kali:~/Desktop# lzip -d test.lzip
```



通过指令进行解压缩后会发现，原来的压缩包消失了，并产生了一个`out`为后缀的图片文件



这个图片显示的文字就是flag了

IceCTF{h3XduMp1N9_l1K3_A_r341_B14Ckh47}