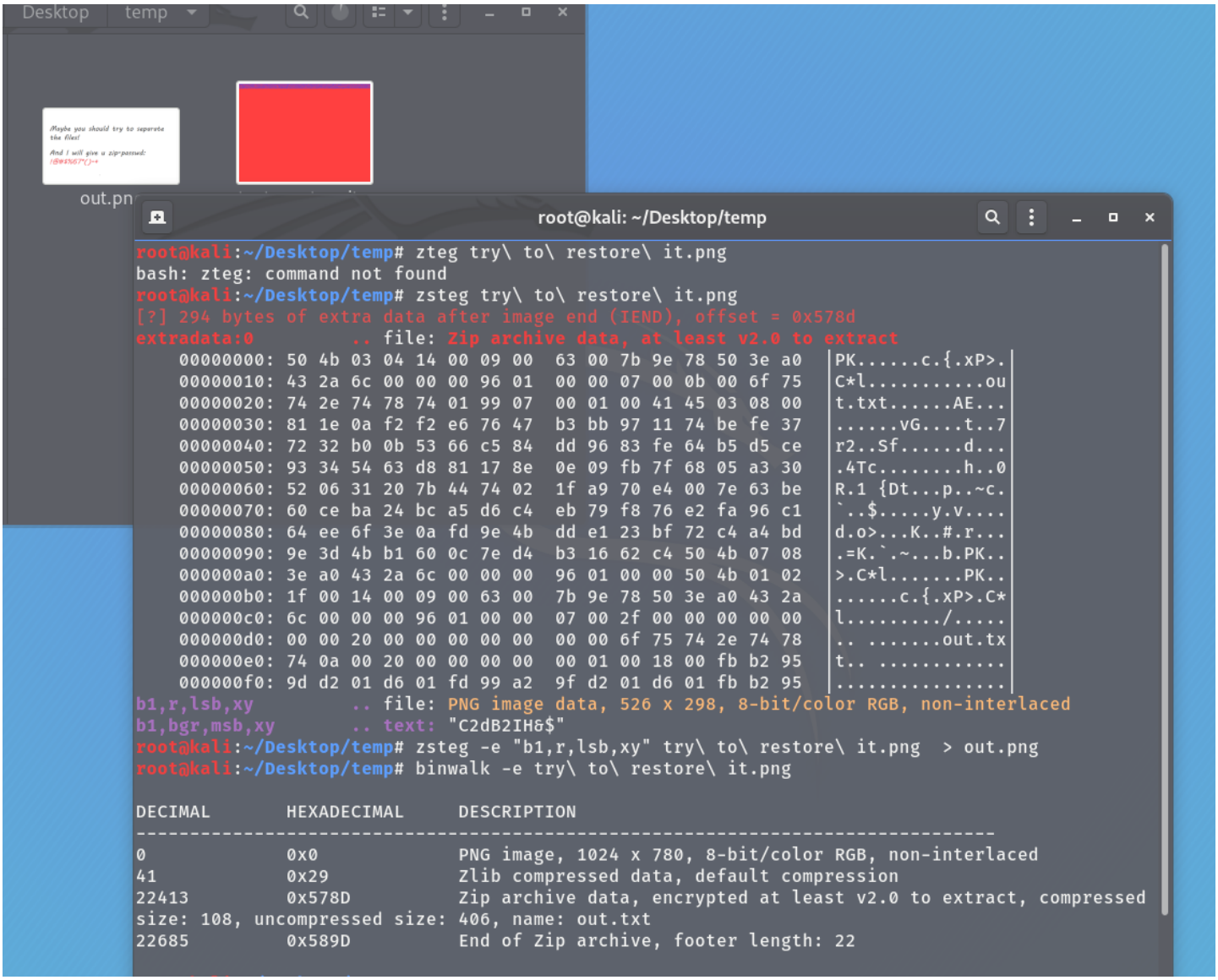
[MRCTF2020]Hello_ misc

原创

ruokeqx 于 2020-07-28 19:06:49 发布 661 收藏

分类专栏： CTF入坟

本文链接：https://blog.csdn.net/weixin_45485719/article/details/107642970



这个图乍一眼看跟BJD2020-07的第一道misc一样 直接zsteg 还看出了个zip 解压得到

out.txt

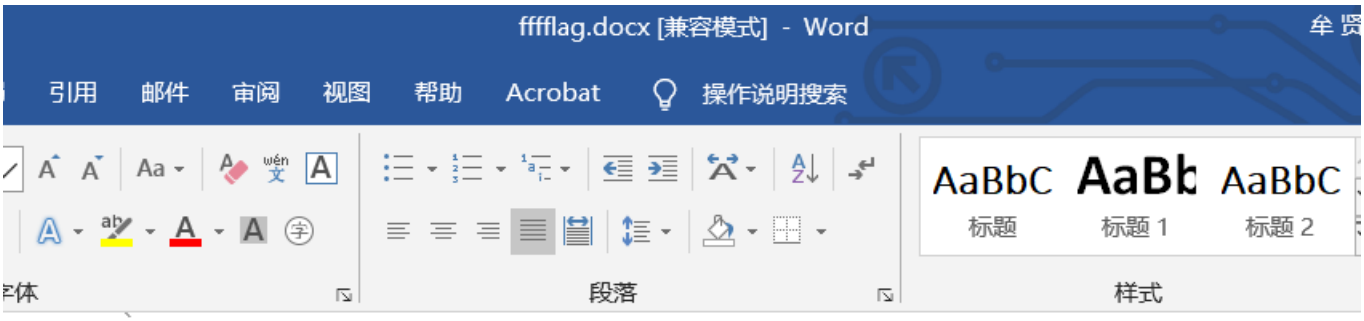
一个只包含127 255 63 191的TXT文件

脚本来自互联网

```
with open('out.txt') as a_file:
    content = [x.strip() for x in a_file.readlines()]
bins = []
for i in content:
    bins.append(bin(int(i))[2:].zfill(8)[:2])
stringBins = ''.join(bins)
num = 0
flag = ''
for i in range(int(len(stringBins)/8)):
    flag+=chr(int(stringBins[num:num+8],2))
    num+=8

print(flag)
```

解压得到一个zip 直接改后缀为 docx
刚开始看不到 改字体颜色就可以



MTEwMTEwMTExMTExMTEwMDExMTEwMTExMTExMTExMTExMTExMTExMTExMTExMTEx
MTAxMTEwMDAwMDAxMTExMTExMTExMDAxMTAx
MTEwMTEwMTEwMDAxMTAxMDExMTEwMTExMTExMTExMTExMTExMTExMTExMTExMTEx
MTExMTAxMTExMTExMTExMTExMTEwMTEwMDEx
MTEwMDAwMTAxMTEwMTExMDExMTEwMTExMTExMTAwMDExMTExMTExMTExMDAxMD
AxMTAxMTEwMDAwMDExMTExMDAwMDExMTExMTEx
MTEwMTEwMTAwMDAxMTExMDExMTEwMTExMTExMDExMTAxMTExMTExMTEwMTEwMT
EwMTAxMTExMTExMTAwMTEwMTExMTExMTExMTEx
MTEwMTEwMTAxMTExMTExMDExMTEwMTExMTAxMDExMTAxMTExMTExMTEwMTEwMTE
wMTAxMTAxMTExMTAwMTEwMTExMTExMTExMTEx
MTEwMTEwMTAwMDAxMTAwMDAwMTEwMDAwMDAxMTAwMDExMTAwMDAwMTEwMTE
wMTEwMTAxMTEwMDAwMDAxMTExMDAwMDExMTExMTEx

逐行base64decode

File Edit Selection Find View Goto Tools Project Preferences Help

solve.php index.php

```php
<?php
echo base64_decode("MTEwMTEwMTExMTExMTEwMDExMTEwMTExMTExMTExMTExMTExMTExMTExMTExMTAxMTEwMDAwMDAxMTExMTExMTExMDAxMTAx"
    )."\n";
echo base64_decode("MTEwMTEwMTEwMDAxMTAxMDExMTEwMTExMTExMTExMTExMTExMTExMTExMTExMTExMTAxMTExMTExMTExMTExMTEwMTEwMDEx"
    )."\n";
echo base64_decode("MTEwMDAwMTAxMTEwMTExMDExMTEwMTExMTExMTAwMDExMTExMTExMTExMDAxMDAxMTAxMTEwMDAwMDExMTExMDAwMDExMTExMTEx"
    )."\n";
echo base64_decode("MTEwMTEwMTAwMDAxMTExMDExMTEwMTExMTExMDExMTAxMTExMTExMTEwMTEwMTAxMTAxMTExMTAxMTEwMTExMTExMTEx"
    )."\n";
echo base64_decode("MTEwMTEwMTAxMTExMTExMDExMTEwMTExMTAxMDExMTAxMTExMTExMTEwMTEwMTAxMTAxMTAxMTAxMTEwMTExMTExMTExMTEx"
    )."\n";
echo base64_decode("MTEwMTEwMTAwMDAxMTAwMDAwMTEwMDAwMDAxMTAwMDExMTAwMDAwMTEwMTEwMTAxMTEwMDAwMDAxMTExMDAwMDExMTExMTEx"
    )."\n";
```

```
1101101111111100111101111111111111111111111111111101110000001111111111001101
1101101100011010111101111111111111111111111111111111101111111111111111110110011
1100001011101110111011111111000111111111111001001101110000011111000011111111
1101101000011110111011111110111011111111110110110101111111100110111111111111
1101101011111110111101111010111011111111101101101011011111001101111111111111
1101101000011000001100000011000111000001101101101011100000011110000111111111
[Finished in 0.1s]
```

把1删除就可以得到flag（脑洞真的大）

```
  0  0        00    0                              0   000000          00  0
  0  0  000  0 0    0                              0              0  00
 0000 0   0   0    0       000          00 00  0   00000     0000
  0  0 0000    0    0       0   0         0  0  0 0        00  0
  0  0 0       0    0    0 0   0         0  0  0 0  0     00  0
  0  0 0000  00000  000000  000   00000  0  0  0 0   000000    0000
[Finished in 0.1s]
```

flag{He1Lo_mi5c~}