妖精纪元

1.首先打开文件,发现有一个加密的压缩包和一个docx文档,发现docx文档大小过大,怀疑有隐藏文件,使用binwalk分离

```
DECIMAL
                HEXADECIMAL
                                   DESCRIPTION
WARNING: Extractor.execute failed to run external extractor 'jar xvf '%e'': [Errno 2] No such file or directory: 'jar', 'jar xvf '%e'' might not be installed correctly 0 \times 0 \times 0 Zip archive data, at least v1.0 to extract, name: docPro
ps/
                0×27
                                    Zip archive data, at least v2.0 to extract, compressed s
ize: 351, uncompressed size: 626, name: docProps/app.xml
                0×1B4
                                   Zip archive data, at least v2.0 to extract, compressed s
436
ize: 358, uncompressed size: 663, name: docProps/core.xml
                                   Zip archive data, at least v2.0 to extract, compressed s
841
                0×349
ize: 298, uncompressed size: 529, name: docProps/custom.xml
                                    Zip archive data, at least v1.0 to extract, name: word/
1188
                0×4A4
1223 0×4C7 Zip archive data, at least v2.0 to extract, compressed size: 2789, uncompressed size: 26940, name: word/styles.xml
4057 0×FD9 Zip archive data, at least v2.0 to extract, compressed size: 1180, uncompressed size: 2809, name: word/settings.xml
4057
                                   Zip archive data, at least v1.0 to extract, name: word/t
5284
                0×14A4
heme/
5325 0×14CD Zip archive data, at least v2.0 to extract, compressed size: 1546, uncompressed size: 6331, name: word/theme/theme1.xml
                0×1B0A
                                    Zip archive data, at least v2.0 to extract, compressed s
6922
ize: 1069, uncompressed size: 2703, name: word/document.xml
8038 0×1F66 Zip archive data, at least v2.0 to extract, compressed size: 1106, uncompressed size: 6018, name: word/fontTable.xml
                                   Zip archive data, at least v1.0 to extract, name: _rels/
9192
                0×23E8
9228
                0×240C
                                    Zip archive data, at least v2.0 to extract, compressed s
ize: 253, uncompressed size: 737, name: _rels/.rels
                0×2532
                                   Zip archive data, at least v1.0 to extract, name: word/_
9522
rels/
9563
                0×255B
                                   Zip archive data, at least v2.0 to extract, compressed s
ize: 231, uncompressed size: 680, name: word/_rels/document.xml.rels
                                   Zip archive data, at least v2.0 to extract, compressed s
               0×267C
ize: 354, uncompressed size: 1300, name: [Content_Types].xml
                                   RAR archive data, version 5.x
11253
                0×2BF5
WARNING: One or more files failed to extract: either no utility was found or it's unimplemented
```

2.得到一个exe文件,使用PE查看文件类型



发现是python编写的exe文件,使用Pyinstxtractor发现是python3.10版本编写的,用对应版本的python反编译成pyc文件后再转化为py文件得到如图

```
#|/usr/bin/env python
# visit https://tool.lu/pvc/ for more information
# version: Python 3.10

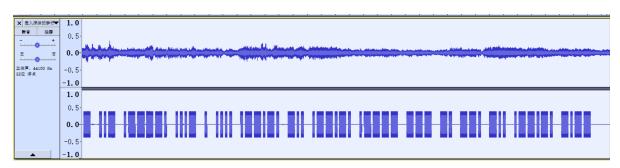
import base64
from io import Bytes10
from PIL import Image, ImageIk
import tkinter as tk

very def base64_to_image (base64_data):
    image_data = base64_b64decode (base64_data)
    image_buffer = Bytes10(image_data)
    image = Image.open(image_buffer)
    return image

very def display_image(image):
    root = tk. Tk()
    root.title(%情紀元——大英雄之叙')
    root.bind('Button-3', (lambda e: 'break'))
    image ImageRhotoImage(image)
    label = tk. Label(root, img, **('image',))
    label.pack()
    root.mainloop()

vif __name__ == '__main__':
    base64_data = 'iVBORNOKGgoAAAANSUhEUgAABAAAAAQACAYAAAB/HSuDAAAAAXNSROIArs4c6QAAAARnQUIBAACx.jwv8YQUAAAAJcEhZcwAAEnQAABJOAd5mH3gAAP+1SURBVHhezP33o17FkeOP+3*833sn3vEEz4z
    image = base64_to_image (base64_data)
    display_image(image)
    return None
```

3.发现是base64编码的文件,将代码中的base64编码转化为文件,发现图片仍然有6715KB,仍然过大 (也可用010editor准确判断) ,再次binwalk分离得到一个音频文件,查看音轨发现莫斯密码



4. 将对应的莫斯密码转化为字符即可得到压缩包密码



5.解压压缩包即可得到flag

