胖盒子misc writeup中等

原创

~VAS~ 已于 2022-03-03 11:53:14 修改 519 收藏

分类专栏： 胖盒子 ctf 笔记 文章标签： 安全

于 2022-01-11 11:15:37 首次发布


胖盒子 同时被 3 个专栏收录

4 篇文章 0 订阅

订阅专栏


ctf

50 篇文章 1 订阅

订阅专栏


笔记

53 篇文章 0 订阅

订阅专栏

目录

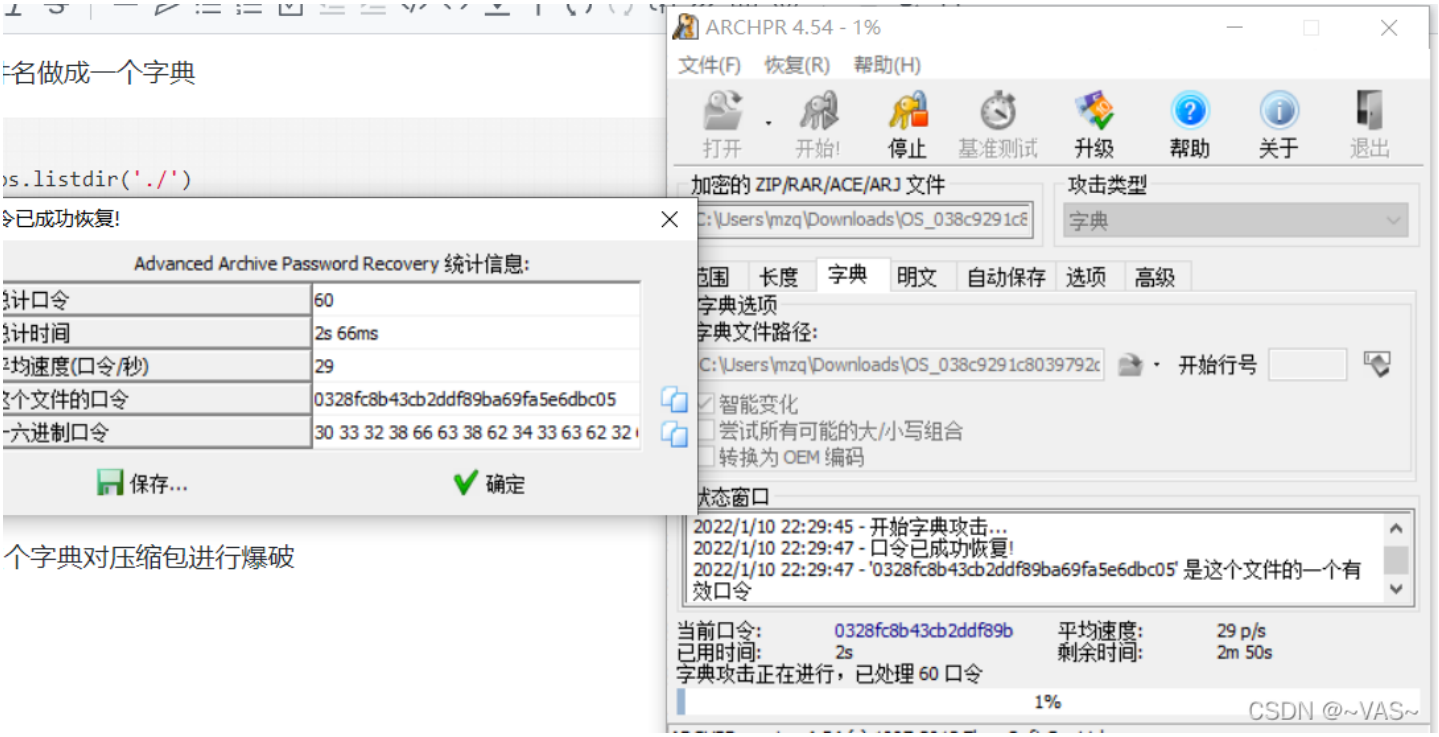
听说你们喜欢手工爆破

把txt的文件名做成一个字典

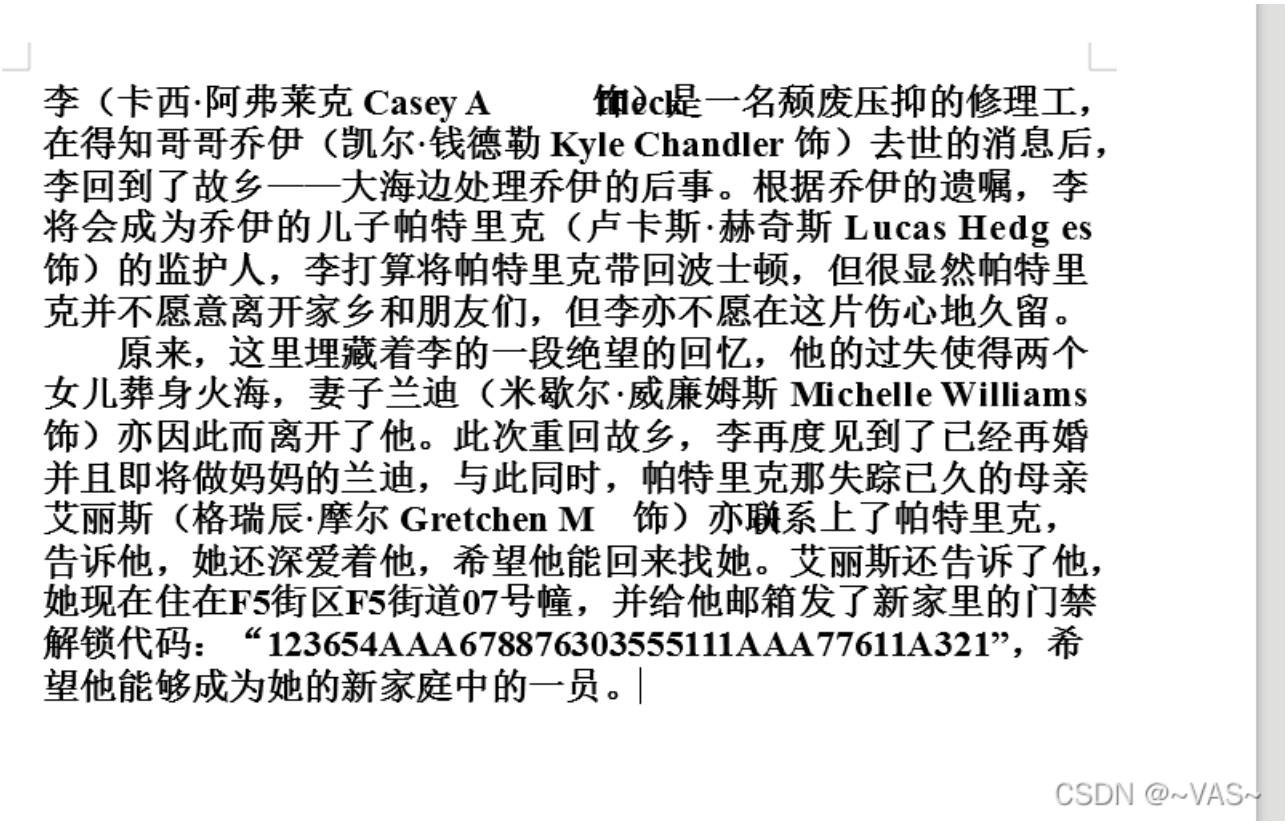
```
import os
list_a = os.listdir('./')


for i in list_a:
    if 'txt' in i:
        with open('pass.dic', 'a') as f:
            f.write((i.split('.')[0]+'\n'))
            f.close()
```

然后使用这个字典对压缩包进行爆破



然后利用对doc进行爆破,得到一串加密,上百度搜好像有种加密叫曼切斯特



曼切斯特解密脚本

```python
a = 0x123654AAA678876303555111AAA77611A321
flag = ''
bs = '0' + bin(a)[2:]
r = ''
def conv(s):
    return hex(int(s,2))[2:]
for i in range(0, len(bs), 2):
    if bs[i:i+2] == "01":
        r += '0'
    else:
        r += '1'
for j in range(0, len(r), 8):
    t = r[j:j+8][::-1]
    flag += conv(t[:4])
    flag += conv(t[4:])
print(flag.upper())
```

flag里面的是大写的

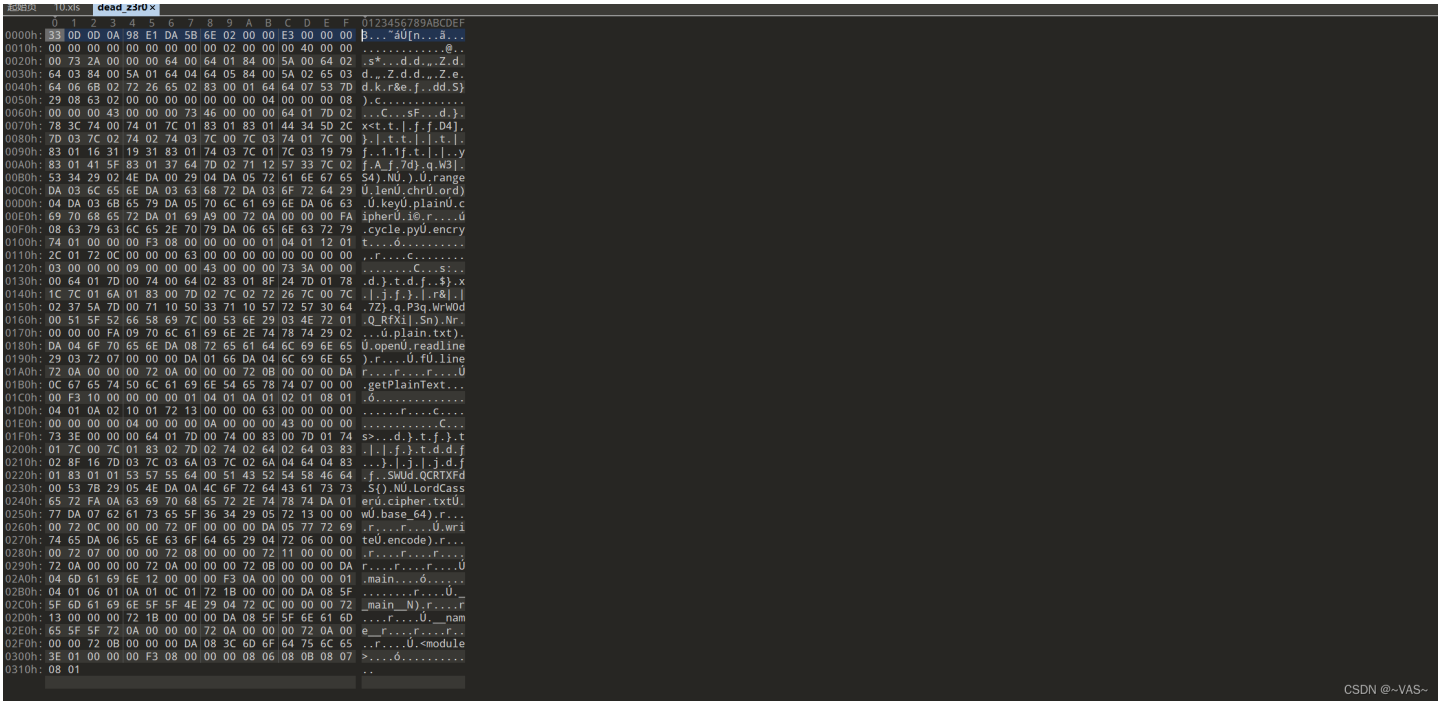
KeyBoard

直接用UsbKeyboardDataHacker提取就行

```
┌──(root💀DESKTOP-F82I28J)-[/mnt/d/TOOLS/流量分析/UsbKeyboardDataHacker-master]
└─# python3 UsbKeyboardDataHacker.py keyboard.pcap
Running as user "root" and group "root". This could be dangerous.
[-] Unknow Key : 01
[-] Unknow Key : 01
[+] Found : flag{pr355_0nwards_a2fee6e0}
```

dead_z3r0

删除多余的混淆数据,修改后缀为pyc



然后是stegosaurus隐写

```
┌──(root💀DESKTOP-F82I2BJ)-[/mnt/d/TOOLS/其他工具/stegosaurus-master]
└─# ./stegosaurus -x /mnt/c/Users/mzq/Downloads/dead_z3r0.pyc
Extracted payload: SUCTF{Z3r0_fin411y_d34d}
```

第四扩展FS

foremost分离出一个有密码压缩包解压密码在图片的详细备注上,得到txt做统计字符串

```
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+- =\\{\\}[]"
file_path = input('please input path:')
strings = open(file_path).read()

result = {}
for i in alphabet:
 counts = strings.count(i)
 i = '{0}'.format(i)
 result[i] = counts

res = sorted(result.items(),key=lambda item:item[1],reverse=True)
for data in res:
 print(data)

for i in res:
 flag = str(i[0])
 print(flag[0],end="")
```

C-Knife

binwalk这个pacp然后会出来一个文件文件里藏了flag格式是key{}