

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

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/zip471642048/article/details/122427523>

版权



[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](#)

[KeyBoard](#)

[dead_z3r0](#)

[第四扩展FS](#)

[C-Knife](#)

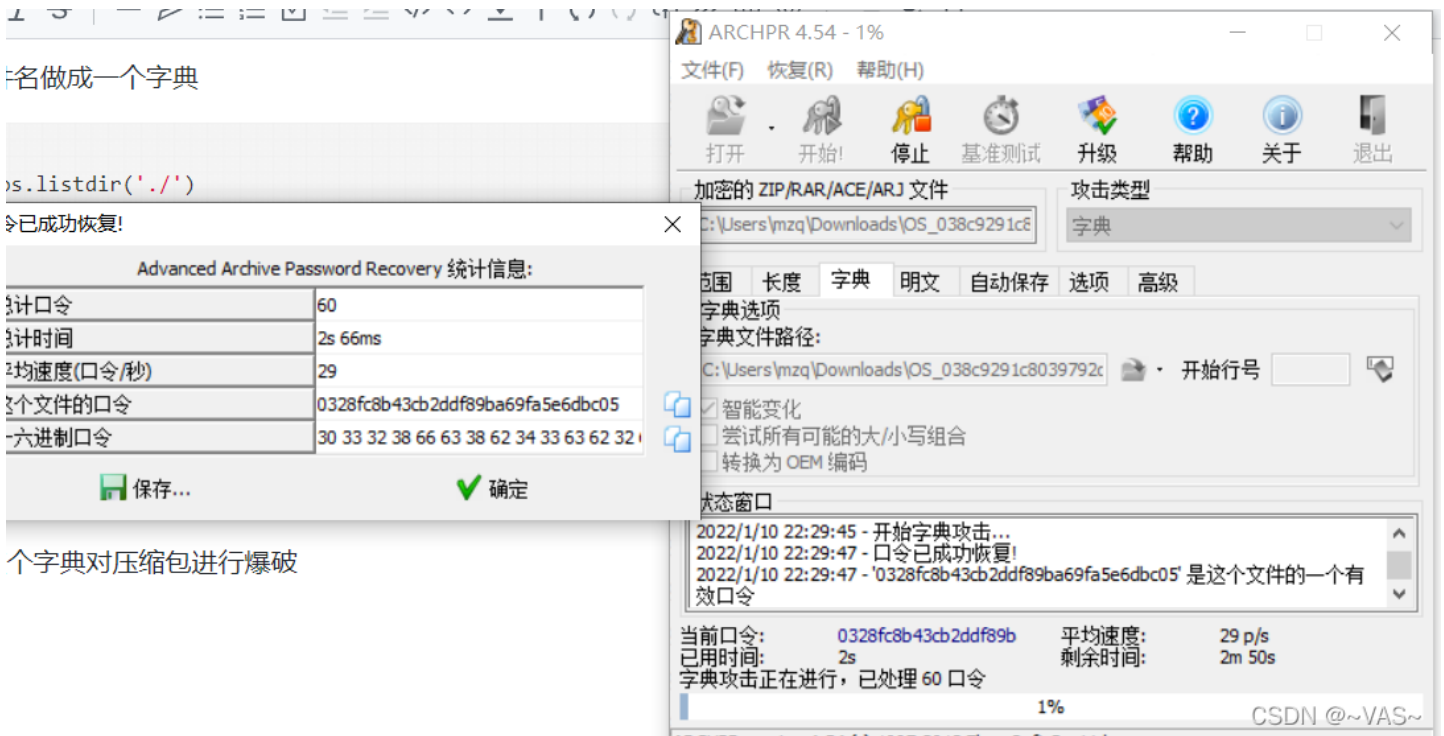
听说你们喜欢手工爆破

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

李（卡西·阿弗莱克 Casey A Affleck）是一名颓废压抑的修理工，在得知哥哥乔伊（凯尔·钱德勒 Kyle Chandler 饰）去世的消息后，李回到了故乡——大海边处理乔伊的后事。根据乔伊的遗嘱，李将会成为乔伊的儿子帕特里克（卢卡斯·赫奇斯 Lucas Hedg es 饰）的监护人，李打算将帕特里克带回波士顿，但很显然帕特里克并不愿意离开家乡和朋友们，但李亦不愿在这片伤心地久留。原来，这里埋藏着李的一段绝望的回忆，他的过失使得两个女儿葬身火海，妻子兰迪（米歇尔·威廉姆斯 Michelle Williams 饰）亦因此而离开了他。此次重回故乡，李再度见到了已经再婚并且即将做妈妈的兰迪，与此同时，帕特里克那失踪已久的母亲艾丽斯（格瑞辰·摩尔 Gretchen M oore 饰）亦联系上了帕特里克，告诉他，她还深爱着他，希望他能回来找她。艾丽斯还告诉了他，她现在住在F5街区F5街道07号幢，并给他邮箱发了新家里的门禁解锁代码：“123654AAA678876303555111AAA77611A321”，希望他能够成为她的新家庭中的一员。

CSDN @~VAS~

曼切斯特解密脚本

```

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-F82I2BJ)~/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

```
0000h: 33 0D 0D 0A 98 E1 DA 5B 6E 02 00 00 E3 00 00 00  B...u[n...ä...
0010h: 00 00 00 00 00 00 00 00 02 00 00 00 40 00 00    .....@...
0020h: 00 73 2A 00 00 00 64 00 64 01 84 00 5A 00 64 02  s*...d.d...Z.d.
0030h: 64 03 84 00 5A 01 64 04 05 84 00 5A 02 65 03    d...Z.d...Z.e.
0040h: 64 06 68 02 72 26 65 02 83 00 01 64 64 02 83 7D  d.k.r&e.f...d(S)
0050h: 29 08 63 02 00 00 00 00 00 00 04 00 00 00 08    ).C.....
0060h: 00 00 00 43 00 00 00 73 46 00 00 64 01 7D 02    ...C...sF...d.).
0070h: 78 3C 74 00 74 01 7C 01 83 01 83 01 44 34 5D 2C  xst.t.|.f.f.D4].
0080h: 7D 03 7C 02 74 02 74 03 7C 00 03 74 01 7C 00  }|.t.t.|.t.t.|.
0090h: 83 01 16 31 19 31 83 01 74 03 7C 01 7C 03 19 79  f...t.f.t.f.|.y
00A0h: 83 01 41 5F 83 01 37 64 7D 02 71 12 57 33 7C 02  f.A.f.7d).q.W3].
00B0h: 53 34 29 02 4E DA 00 29 04 DA 05 72 61 6E 67 65  S4).NU.).U.range
00C0h: DA 03 6C 65 6E DA 03 63 68 72 DA 03 6F 72 64 29  U.lenU.chrU.ord)
00D0h: 04 DA 03 69 65 79 DA 05 70 6C 61 69 6E DA 06 63  .U.keyU.plainU.c
00E0h: 69 70 68 65 72 DA 01 69 A9 00 72 DA 00 00 00 FA  ipherU.ä.f...u&
00F0h: 08 63 79 63 6C 65 2E 70 79 DA 06 65 6E 63 72 79  .cycle.pyU.encyr
0100h: 74 01 00 00 00 F3 08 00 00 00 00 01 04 01 12 01  t...ö.....
0110h: 2C 01 72 0C 00 00 00 63 00 00 00 00 00 00 00    .f...C.....
0120h: 03 00 00 00 09 00 00 43 00 00 00 73 3A 00 00    .....C...s...
0130h: 00 64 01 7D 00 74 00 64 02 83 01 8F 24 7D 01 78  .d.).t.d.f.f.ä)x
0140h: 1C 7C 01 6A 01 83 00 7D 02 7C 02 72 26 7C 00 7C  .|ä|.f.).f.8|.
0150h: 02 37 5A 7D 00 71 10 50 33 71 10 57 72 57 30 64  .7Z).q.P3q.WrWod
0160h: 00 51 5F 52 66 58 69 7C 00 53 6E 29 03 4E 72 01  .Q.Rfxi|.Sn).Nr.
0170h: 00 00 00 FA 09 70 6C 61 69 6E 2E 74 78 74 29 02  .U.plain.txt).
0180h: DA 04 6F 70 65 6E DA 01 66 DA 04 6C 69 6E 65    U.openU.readline
0190h: 29 03 72 07 00 00 00 DA 01 66 DA 04 6C 69 6E 65  .r...U.fU.line
01A0h: 72 0A 00 00 00 72 0A 00 00 00 72 0B 00 00 0A DA  r...r...r...U
01B0h: 0C 67 65 74 50 6C 61 69 6E 54 65 78 74 07 00 00  .getPlainText...
01C0h: 00 F3 10 00 00 00 01 04 01 0A 01 02 01 08 01    .ö.....
01D0h: 04 01 0A 02 10 01 72 13 00 00 00 63 00 00 00    .....C.....
01E0h: 00 00 00 00 04 00 00 00 0A 00 00 00 43 00 00    .....C.....
01F0h: 73 3E 00 00 00 64 01 7D 00 74 00 83 00 7D 01 74  s...d.).t.f.).t
0200h: 01 7C 00 7C 01 83 02 7D 02 74 02 64 02 64 03 83  .|.f.).t.d.d.f
0210h: 02 8F 16 7D 03 7C 03 6A 03 7C 02 6A 04 64 04 83  .).|.j|.j|.d.f
0220h: 01 83 01 01 53 57 55 64 00 51 43 52 54 58 46 64  .f.SMUdOCRIFd)
0230h: 00 53 78 29 05 4E DA 0A 4C 6F 72 64 43 61 73 73  .S().NU.lordCass
0240h: 65 72 FA 0A 63 69 70 68 65 72 2E 74 78 74 DA 01  erU.cipher.txtU.
0250h: 77 DA 07 62 61 73 65 5F 36 34 29 05 72 13 00 00  wU.base_64).r...
0260h: 00 72 0C 00 00 00 72 0F 00 00 00 DA 05 77 72 69  .f...f...U.wri
0270h: 74 65 DA 06 65 6E 63 6F 64 65 29 04 72 06 00 00  teU.encode).r...
0280h: 00 72 07 00 00 00 72 08 00 00 00 72 11 00 00    .....f...f...
0290h: 72 0A 00 00 00 72 0A 00 00 00 72 0B 00 00 0A DA  r...r...r...U
02A0h: 04 6D 61 69 6E 12 00 00 00 F3 0A 00 00 00 01    .main...ö.....
02B0h: 04 01 06 01 0A 01 0C 01 72 1B 00 00 00 DA 08 5F  .r...f...U.
02C0h: 5F 6D 61 69 6E 5F 5F 4E 29 04 72 0C 00 00 00 72  _main_N).r...f
02D0h: 13 00 00 00 72 1B 00 00 00 DA 08 5F 5F 6E 61 6D  .r...f...U._nam
02E0h: 65 5F 5F 72 0A 00 00 00 72 0A 00 00 00 72 0A 00  e...f...f...f...
02F0h: 00 00 72 0B 00 00 00 DA 08 3C 6D 6F 64 75 6C 65  .r...U.<module
0300h: 3E 01 00 00 00 F3 08 00 00 00 08 06 08 08 07    >...ö.....
0310h: 08 01
```

CSDN @-VAS-

然后是stegosaurus隐写

```
read_z3r0.pyc desktop\pinz
(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{}

```
1E43 - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag/
ustar 00zhangjianxiang      staff          000755 000765 000024 000000000000 12734163500 014133 5
00zhangjianxiang      staff          000644 000765 000024 000000000045 12734157617 015620 0
(8769fe393f2b998fa6a11afe2bfcd65e)

flag/flag.txt
ustar
key
```