BUUCTF~Misc~Test5

原创

kvmbox 于 2021-02-14 14:09:26 发布 178 收藏 1

分类专栏： 笔记

本文链接：https://blog.csdn.net/m0_47643893/article/details/113573548

目录

前言

又是全新的一篇.....

黄金6年

视频中满放帧看发现有4张二维码扫出来拼接一下然后得到完整的key：iwantplayctf

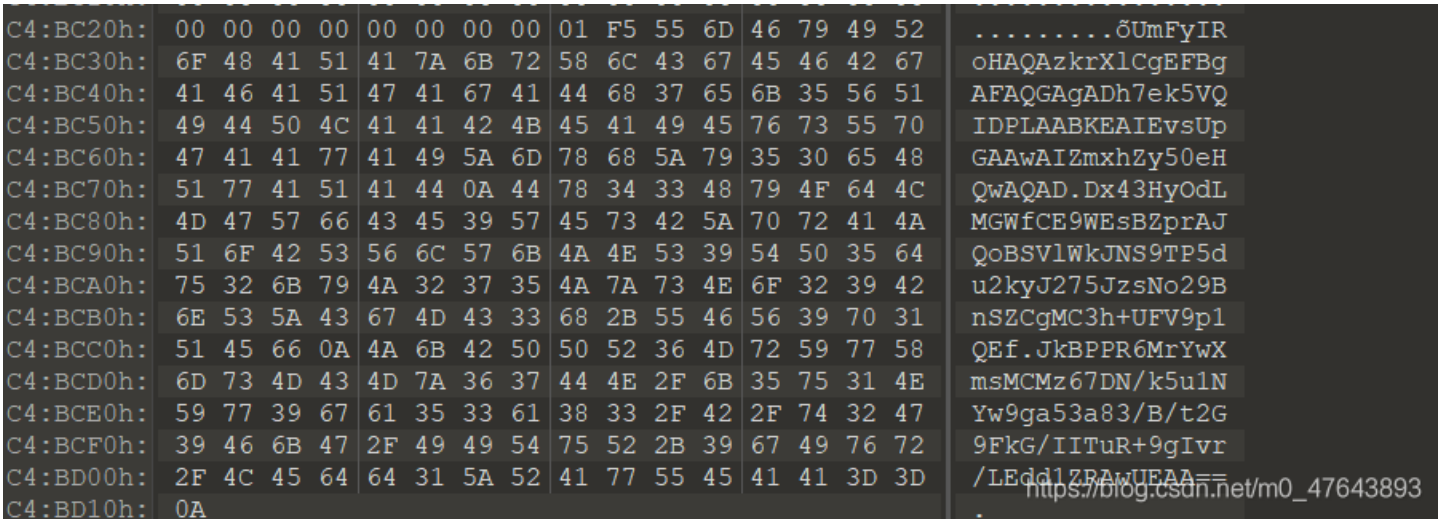
然后视频在010最后发现了base64，然后解码一下。用脚本将base64以字节流数据写入成Rar文件然后密码就上上面的key

```
#base64以字节流数据写入成Rar文件
import base64

b64_str = "UmFyIRoHAQAzkrXlCgEFBgAFAQGAgADh7ek5VQIDPLAABKEAIEvsUpGAAwAIZmxhZy50eHQwAQADDx43HyOdLMGWfCE9WEsBZprAJ
QoBSVlWkJNS9TP5du2kyJ275JzsNo29BnSZCgMC3h+UFV9p1QEfJkBPPR6MrYwXmsMCMz67DN/k5u1NYw9ga53a83/B/t2G9FkG/IITuR+9gIvr/
LEdd1ZRAwUEAA=="
byte_stream = base64.b64decode(b64_str)
open('flag.rar','wb').write(byte_stream)
```

就得到了flag

flag{CTF-from-RuMen-to-RuYuan}



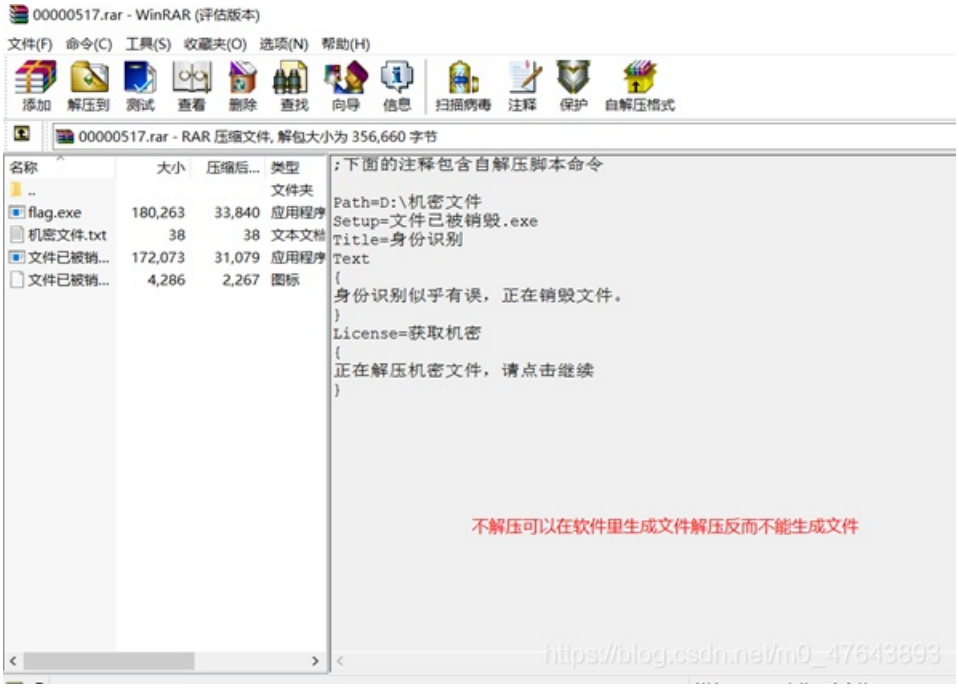
间谍启示录

一开始是iso文件

不解压问价直接打开可以获得flag解压之后打开程序直接自动删除，不会生成flag

这个文件用binwalk看不到rar文件，直接用foremost分离然和看到有rar文件，一开始解压发现打开没有东西弹出，然和以为就是这样的题目，又放到虚拟机中泡ios镜像然后无果。后面才知道不解压的时候时直接打开会生成文件。

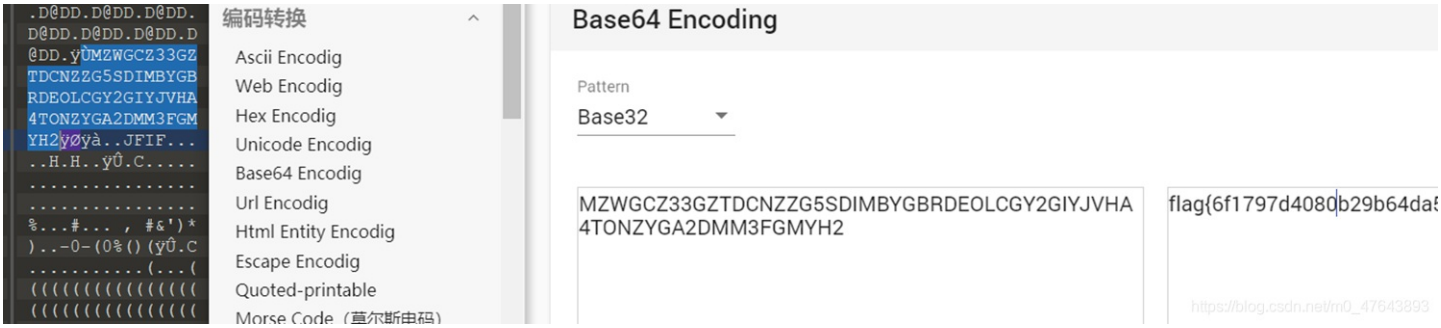
flag{379:7b758:g7dfe7f19:9464f:4g9231}



我吃三明治

在kali中看到两张图片，在010中两张图片的连接处，有base32弄出来解密一下就是flag

flag{6f1797d4080b29b64da5897780463e30}



拉胯的三条命令

Tcpdump使用命令：

tcpdump -n -r nmapll.pcapng ‘tcp[13] = 18’ | awk ‘{print $3}’ | sort -u

-n 网络地址转化

-r 从指定文件中读取包

tcp[13] = 18代表只抓取synACK标志位（代表服务器和客户端连接）

Awk’{print$3}’ 取第三为字符串

Sort -u 拒绝重复

Tcpdump使用详解：

https://www.cnblogs.com/lvdongjie/p/10911564.html

Tcpdump常用抓包教程：

https://blog.csdn.net/shun_smile/article/details/80261335

在看了wp之后有两种方法第一种就是用wireshark手工修改port来找开放的端口

在编辑->首选项->外观->列添加一个Port类型选择Dest port(unresolved)

以port列降序排序，查找每个端口是否有[ACK]响应标志，众所周知在TCP三次握手中，[SYN]标志表示建立连接，[ACK]表示响应，查看开放端口，肯定会返回[ACK]标志

找端口因该是题目的本意。

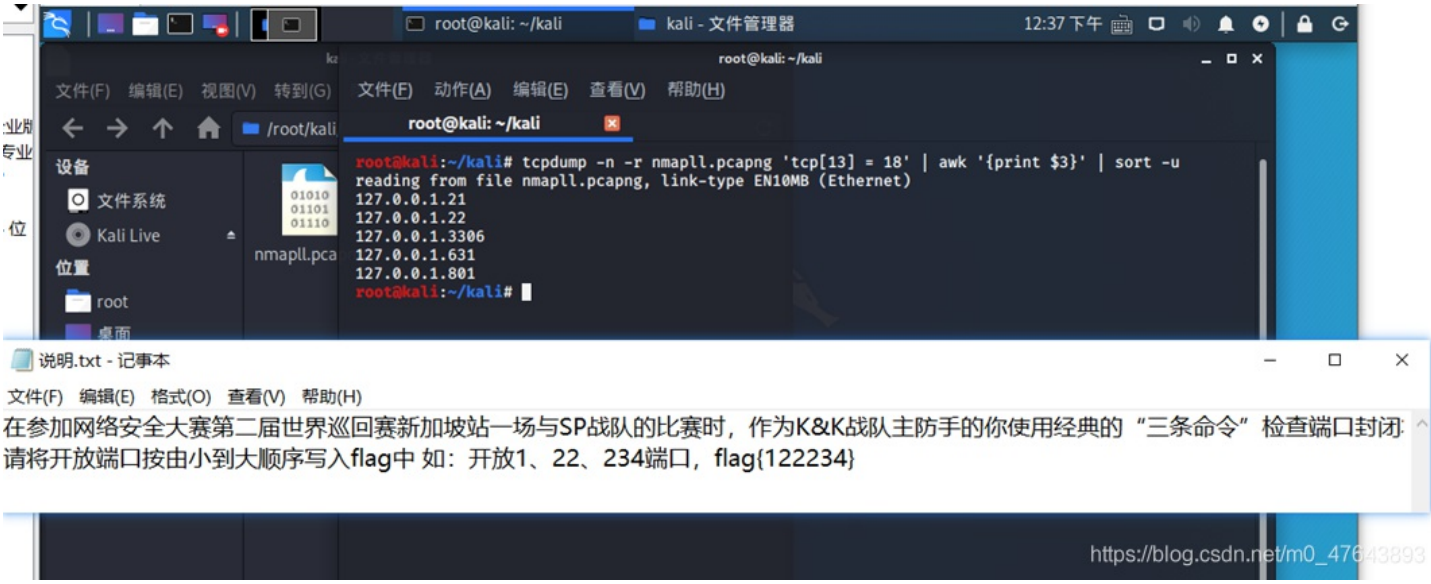
我们也也可以在kali中使用Tcpdump工具

使用这段命名即可

tcpdump -n -r nmapll.pcapng ‘tcp[13] = 18’ | awk ‘{print $3}’ | sort -u

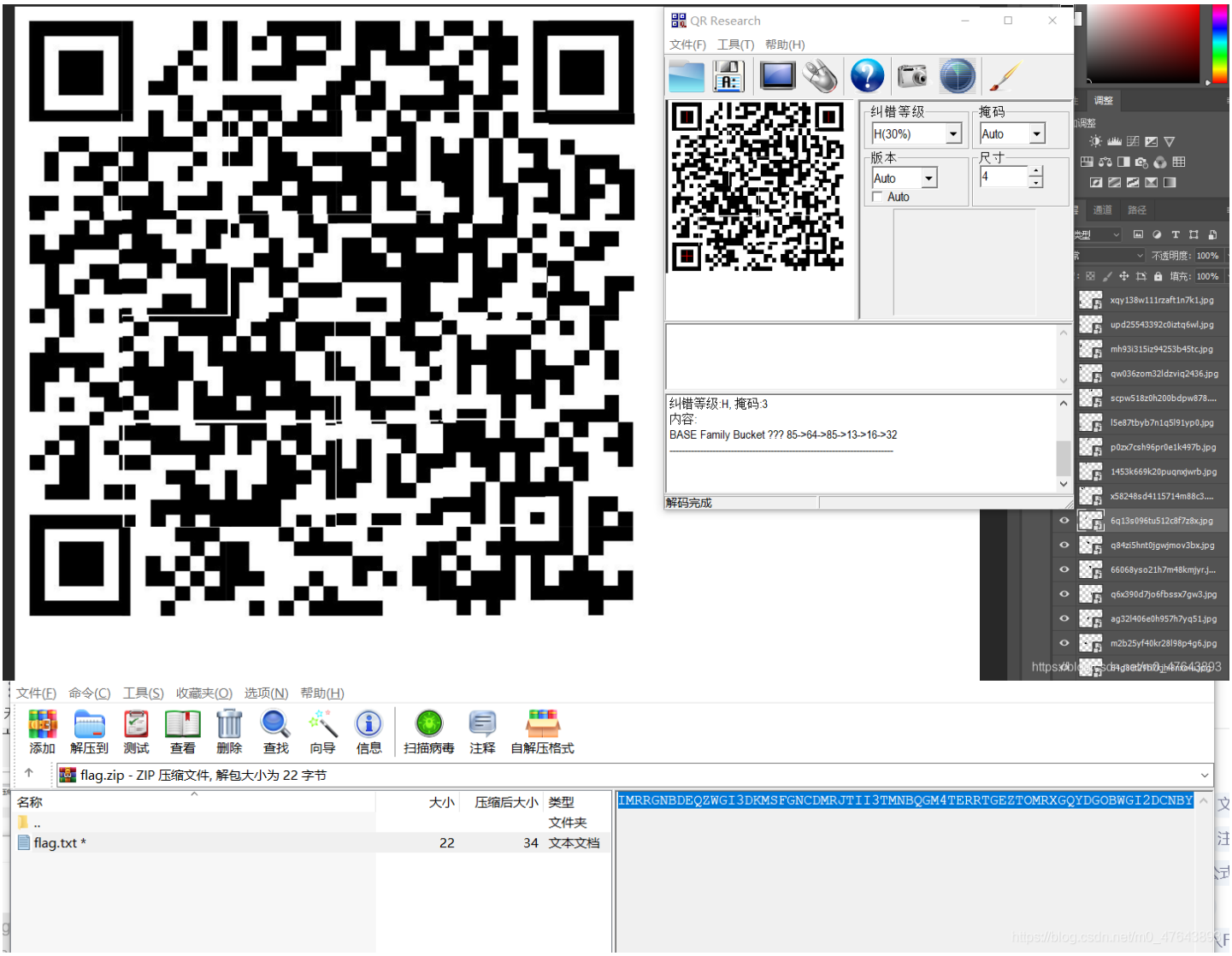
即可得到开放端口：

flag{21226318013306}


root@kali: ~/kali
kali - 文件管理器
12:37 下午
root@kali: ~/kali
文件(F) 编辑(E) 视图(V) 转到(G)
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
/root/kali
root@kali: ~/kali
设备
文件系统
Kali Live
位置
root
桌面
nmapll.pca
root@kali:~/kali# tcpdump -n -r nmapll.pcapng 'tcp[13] = 18' | awk '{print $3}' | sort -u
reading from file nmapll.pcapng, link-type EN10MB (Ethernet)
127.0.0.1.21
127.0.0.1.22
127.0.0.1.3306
127.0.0.1.631
127.0.0.1.801
root@kali:~/kali#
说明.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
在参加网络安全大赛第二届世界巡回赛新加坡站一场与SP战队的比赛时，作为K&K战队主防手的你使用经典的“三条命令”检查端口封闭
请将开放端口按由小到大顺序写入flag中 如：开放1、22、234端口，flag{122234}
https://blog.csdn.net/m0_47643893

吹着贝斯扫二维码

这题的拼二维码太难了吧，非常考验耐心。



扫码是编码过程要我们解码，在压缩包备注中发现base32->16->13->85>64>85

按照二维码依次解码

得到密码，打开压缩包即可看到flag

flag{Qr_Is_MeAn1nGfuL}

从娃娃抓起

打开是数字和字母的编码方式，数字的是 中文电码字母是五笔编码

分别看对照表找到。

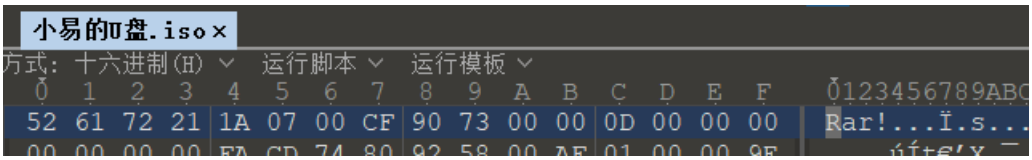
人工智能也要从娃娃抓起

转md5，32位小写。

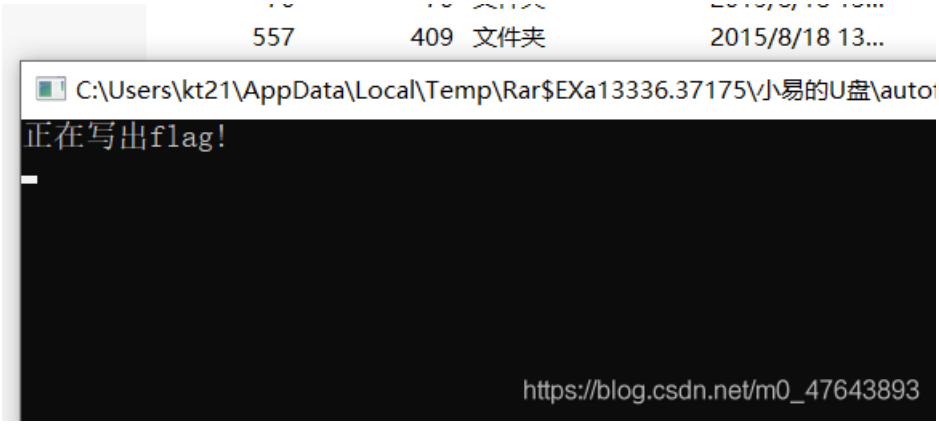
flag{3b4b5dccd2c008fe7e2664bd1bc19292}

小易的U盘

是一个镜像文件，我们用010打开发现是rar改下后缀，解压出来。



里面有个flag.txt提示没有生成，肯定就是exe文件种，随便点开一个正在生成flag,就没了相应，这……



一个个试发现在autorun.inf里提示32这个程序，我们用IDA打开，找到flag

flag{29a0vkrlek3eu10ue89yug9y4r0wdu10}

```
.text:00401010
.text:00401010                push    ebp
.text:00401011                mov     ebp, esp
.text:00401013                sub     esp, 44h
.text:00401016                push    ebx
.text:00401017                push    esi
.text:00401018                push    edi
.text:00401019                lea     edi, [ebp+var_44]
.text:0040101C                mov     ecx, 11h
.text:00401021                mov     eax, 0CCCCCCCCh
.text:00401026                rep stosd
.text:00401028                push    offset aW       ; "w+"
.text:0040102D                push    offset aDProgramFlagTx ; "D:/Program/flag.txt"
.text:00401032                call    _fopen
.text:00401037                add     esp, 8
.text:0040103A                mov     [ebp+var_4], eax
.text:0040103D                mov     eax, [ebp+var_4]
.text:00401040                push    eax             ; FILE *
.text:00401041                push    offset aFlag29a0vkrlek ; "flag{29a0vkrlek3eu10ue89yug9y4r0wdu10}"
.text:00401046                call    _fputs
.text:0040104B                add     esp, 8
.text:0040104E                mov     ecx, [ebp+var_4]
.text:00401051                push    ecx             ; FILE *
.text:00401052                call    _fclose
```


(ﾉ °□°)ﾉ ⁀ ┻━┻

截取两位转16进制转成10进制，都大于128，然后所有-128，在转ASCII。最后脚本

```
def hex_str(str):#对字符串进行切片操作，每两位截取
    hex_str_list=[]
    for i in range(0,len(str)-1,2):
        hex_str=str[i:i+2]
        hex_str_list.append(hex_str)
    print("hex列表：%s\n"%hex_str_list)
    hex_to_str(hex_str_list)


def hex_to_str(hex_str_list):
    int_list=[]
    dec_list=[]
    flag=''
    for i in range(0,len(hex_str_list)):#把16进制转化为10进制
        int_str=int('0x%s'%hex_str_list[i],16)
        int_list.append(int_str)
        dec_list.append(int_str-128)#-128得到正确的ascii码
    for i in range(0,len(dec_list)):#ascii码转化为字符串
        flag += chr(dec_list[i])
    print("转化为十进制int列表：%s\n"%int_list)
    print("-128得到ASCII十进制dec列表：%s\n"%dec_list)
    print('最终答案：%s'%flag)

if __name__=='__main__':
   str='d4e8e1f4a0f7e1f3a0e6e1f3f4a1a0d4e8e5a0e6ece1e7a0e9f3baa0c4c4c3d4c6fbb9b2b2e1e2b9b9b7b4e1b4b7e3e4b3b2b2e3
e6b4b3e2b5b0b6b1b0e6e1e5e1b5fd'
    print("字符串长度：%s"%len(str))
    hex_str(str)
```

得到flag{922ab9974a47cd322cf43b50610faea5}

[ACTF新生赛2020]swp

数据流导出http文件中有个压缩包然后需要密码7z提取文件，是伪加密然后就的到了flag文件

ELF文件用ida64打开找到flag，也可以直接010搜索ctf找到

flag{c5558bcf-26da-4f8b-b181-b61f3850b9e5}

```
9 F6 4C 29 E5 48 83 EC  08 48 C1 FD 03 E8 57 FE  .....H.........
F FF 48 85 ED 74 20 31  DB 0F 1F 84 00 00 00 00  ..H....1........
0 4C 89 FA 4C 89 F6 44  89 EF 41 FF 14 DC 48 83  .L..L.....A.....
3 01 48 39 DD 75 EA 48  83 C4 08 5B 5D 41 5C 41  ..H9.....[]A\A
D 41 5E 41 5F C3 90 66  2E 0F 1F 84 00 00 00 00  ]A^A_Ð·f........
0 F3 C3 00 00 48 83 EC  08 48 83 C4 08 C3 00 00  .....H..........
0 01 00 02 00 00 00 00  00 61 63 74 66 7B 63 35  .........actf{c5
5 35 38 62 63 66 2D 32  36 64 61 2D 34 66 38 62  558bcf-26da-4f8b
D 62 31 38 31 2D 62 36  31 66 33 38 35 30 62 39  -b181-b61f3850b9
5 35 7D 00 00 01 1B 03  3B 38 00 00 00 06 00 00  e5}.....;8......
0 EC FD FF FF 84 00 00  00 0C FE FF FF AC 00 00  ................
0 1C FF FF FF 54 00 00  00 26 FF FF FF C4 00 00  .....T...&......
```


百里挑一

exiftool安装：apt-get install exiftool

运行命令：

Exiftool *| grep flag

题目：
好多漂亮的壁纸，赶快挑一张吧！
题目说有很多图片直接在图片的关键字

直接导出http有很多的图片，不可能我自己一个个看吧，发现一个新的工具exiftool可以找到flag
flag{ae58d0408e26e8f26a3c0589d23edeec}

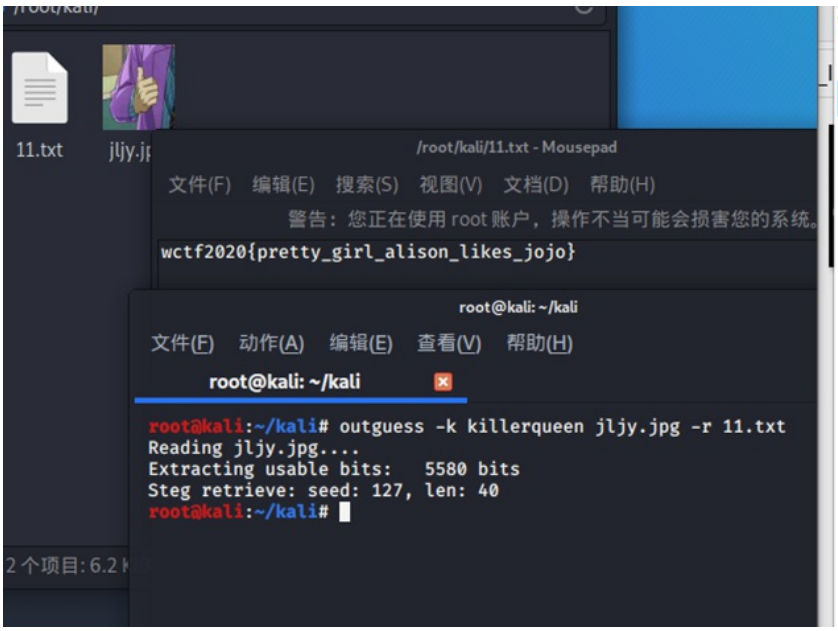
```
  TCP          66 80→9744 [SYN, ACK] Seq=0 Ack=1 Win=8192 L
  TCP          54 9744→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  HTTP        447 GET /image/image1.html HTTP/1.1
  TCP        1514 [TCP segment of a reassembled PDU]
```

找到了一般的flag还有一般应该就在数据流中
找不到看了wp在114tcp中，太难了。

alison_likes_jojo

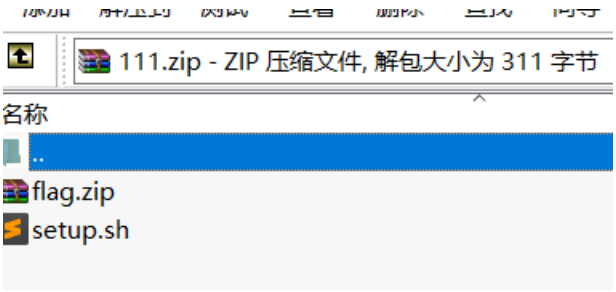
outguess解密命令

Outguess -k 密码 文件 -r输出文件
第一张图片010看里面有zip文件，直接foremost分离，然后的到zip爆破得到密码解压
一串字符base32解密不是base64解密解三次得到killerqueen
一串字符串以为是flag拿去尝试发现不对，还有一张图片没有文件隐写色道也不是，还有两种加密的方式一个个尝试先用steghide尝试不是，然后就是用outguess密码一开始没用压缩文件的密码，解不出来，然后尝试压缩文件密码，成功解除flag
flag{pretty_girl_alison_likes_jojo}

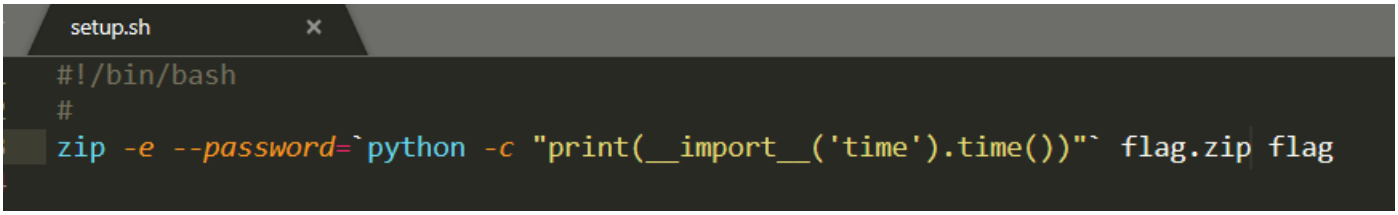


Zips

解压zip里面发现密码数字爆破解开密码，然后里面还有压缩包，可以看到是两个文件的，有密码，用7z解压可以解压但是另一个文件打开没有东西。后来才发现这个伪加密用7z解压不出来，然后用010打开找到09改成00然后就可以解压出来，里面是提示密码=printf是flag.zip的密码
注意：这是python2。然后得到当前系统时间的编码，出题时间和我现在的时间肯定不一样，然后试下15掩码爆破得到密码得到flag{fkjabPqnLawhvuikfhgzyffj}



注意伪加密不要直接用7z提取，可能会出错



Attack

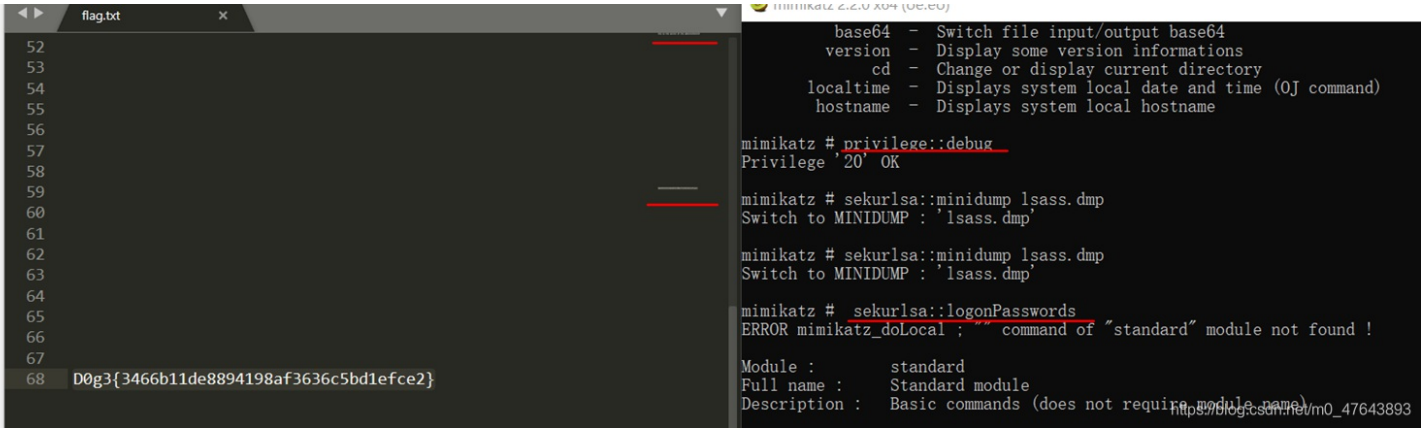
安装mimikatz文件，在kali中"/usr/share/windows-resources/"文件夹下把文件直接复制到windows中然后要以管理员模式运行不然会因为权限的原因无法运行
运行指令：

privilege::debug#获取权限

看别人的wp还要访问要解密的dmp文件（我是直接把文件放在64文件夹里）命令：sekurlsa::minidump lsass.dmp

sekurlsa::logonpasswords full#查看密码

查看数据流里面有zip文件，分离之后需要密码提示"这可是administrator的秘密，怎么能随便给人看呢？"，回到数据流，导出http看到有个dmp文件
使用mimikatz解析一下这个文件，找到win密码passwd就是压缩文件的密码



Game

打开压缩包是一张图片一个压缩包，首先我们来看下文件，初步没有看出什么问题，在后压缩包里是网页源码，在html文件中发现flag，是base32解码之后以为就是flag然而并不是，再回到图片lsb一看有一段

U2FsdGVkX1+zHjSBeYPtWQVSwXzcVFZLu6Qm0To/KeuHg8vKAxFrVQ==

结合上面的假flag然后 [在线网站上去解码]AES之类的(https://www.sojson.com/encrypt_rabbit.html)全部试了一遍才找到TripsDes加密

然后就得到了flag

flag{U_F0und_1t}