# ISCC2017 Misc write up附件题目文件

原创			
椰树i       于 2017-05-25 13:09:         分类专栏:       ISCC 文章标签:       ISCC 文章标签:         版权声明:       本文为博主原创文章         本文链接:       https://blog.csdn.net/qc         版权         ISCC 专栏收录该内容         3 篇文章 0 订阅         订阅专栏	01 发布 <b>2</b> 359 <b>2</b> 2359 <b>2</b> 2359 <b>2</b> 22017 ISCC比赛 WP 查,遵循 <u>CC 4.0 BY-SA</u> <u>1</u> 36512966/article/details/	收藏 2 <u>Misc write up</u> 版权协议,转载请附上原文出 <u>72724471</u>	处链接和本声明。
	眼见非实 100 <sup>853 solves</sup>	×	
眼见非实			
附件下载			
Flag			
	<sub>推交</sub> http://blog.csdr	n.net/qq_36512966	

# 打开附件是个.docx文档,打开是乱码。

W WPS 文字 ・ デ	始 插入 页面布局 引用	审阅 视图 童节 开发工具 云服务	
🖺 🕺 前切 🝼	· 五号 · A* A	▲ 🕸 • 🖅 • 🖽 🗄 • 🖓 • • # • 册 AaBbCcDd	÷ 🐕 🕉
粘贴。 區 氣制 格式剧	B I U + AB + X <sup>2</sup> X <sub>2</sub> A - a⊻ +		■ 新祥式 * 文字工具 * 0
🕨 🗄 🔁 🖶 🖟 🕫	♥ 📌 👿 教授WPS × ၍ 臓児乳素 docs	× +	
	► PHL J ****?	http://blog.csdn.net	L /qq_36512966

改后缀名为.zip

打开发现:

				_			and the second second	* 6
(中下) (明報(E) 登録(V)	工具(T) 報助(H)							
(2) 代 · 代立王(単中 ·	共豪 #建文体先							
🚖 衣服夾	88	傳改日期	曲型	大小				
<ul> <li>● 下紙</li> <li>■ 点用</li> <li>③ 用:65月202番</li> <li>◎ 声</li> <li>● 圖 化尿</li> <li>● 圖 化尿</li> </ul>	溢 _rels customXml docProps ward (Content_Types].xml	2017/5/21 羅城 2017/5/21 擬現. 2017/5/21 羅城 2017/5/21 羅城	文件夹 文件夹 文件夹 文件夹 XML文档	2 108				
<ul> <li>▷ 文極</li> <li>○ 近面下載</li> <li>○ 近面下載</li> <li>&gt; 計算約</li> <li>▷ 盖,本地超血(C)</li> </ul>		htt	tp://	blog.c.	sdn. net	t/qq_3(	651296	66

### 都是.xml配置文件,找到document.xml时出现flag。



#### 打开附件是个.pcapng文件。用wireshark打开。发现是个tcp协议,追踪TCP流。 Wireshark · 遵踪TCP流 (tcp.stream eq 2) · Misc-03

03-12-16	12:20PM	142588562	IDA Pro 6.5 Setup.exe
08-09-16	11:15AM	128	key.txt
08-10-16	11:29AM	240	key.zip
08-09-16	11:12AM	272	pub.key
08-09-16	11:11AM	891	test.key
04-15-16	10:38PM	7357556	pdf
04-15-16	10:38PM	9871783	blog.csdpdfet/gg 36512966
	HERE TOD IS (how show	am an 201 Miss-03	and married lines

#### ----BEGIN RSA PRIVATE KEY----



有个key.zip和test.key(rsa私钥)。

将TCP流中的rsa私钥复制到文本中保存为test.key。然后.pcapng改为.zip后缀,获取key.txt。



使用命令(liunx) openssl rsautl -decrypt -in key.txt -inkey test.key -out 1.txt

1.bxt		root@kali: -/桌面	- 0 4
te te	est.key 文件(F) 编辑(E) i	查看(V) 搜索(5) 終端(T) 用助(H)	Colon tost how out 1 tot
	rootekali:-/# m	# Opensst reduct -decrypt -in key.txt	sinkey testikey out intkt
	key.txt		
			the second se
			111 million
打开(0)	• <u>n</u>	1.txt	保存(S) = • •
hi, boys	and girls! flag is {haP	Py Use OpenSsI)	
		http://blog.csdn.u	net/aa 3651296
<u> </u>			
		<b></b>	
		再见李华	
		再见李华 200	
		再见李华 200	
		再见李华 200 104 solves	
联如你是李华(LiH	lua),收到乔帮主一封密信,8	再见李华 200 104 solves <sup>894任何特殊字符,请输入密码,不少于1000个字</sup>	⊑。同学,记得署名哦~
酿如你是李华(LiH	lua),收到乔帮主一封密信,8	再见李华 200 104 solves <sup>8</sup> 8年任何特殊字符,请输入密码,不少于1000个字	₽。同学,记得署名哦~
親如你 <del>是李</del> 华(LiH 將件下 <del>就</del>	lua),收到乔帮主一封密信,8	再见李华 200 104 solves <sup>8</sup> 春任何特殊字符,请输入密码,不少于1000个字	E。同学,记得著名哦~
限如你是李华(LiH 附件下數 Flag	lua),收到乔帮主一封密信,8	再见李华 200 104 solves <sup>8</sup> 每任何特殊字符,请输入密码,不少于1000个字	E。同学,记得著名哦~
假如你是李华(LiH 附件下载 Flag	lua),收到乔帮主一封密信,划	再见李华 200 <i>104 solves</i> <sup>投有任何特殊字符,请输入密码,不少于1000个字</sup>	E。同学,记得著名哦~
酸如你是李华(LiH 特件下载 Flag	lua),收到乔帮主一封密信,8	再见李华 200 104 solves 战有任何特殊字符,请输入密码,不少于1000个学	₽。同学,记得署名哦~
限如你是李华(LiH 附件下载 Flag	lua),收到乔帮主一封密信,8	再见李华 200 104 solves 战有任何特殊字符,请输入密码,不少于1000个学	8。同学,记得著名哦~
現如你是李华(LiH 将件下動 Flag	lua),收到乔帮主一封密信,划	再见李华 200 <i>104 solves</i> 政有任何特殊字符,请输入密码,不少于1000个号 <u>#文</u> http://blog.csdp.u	=。同学,记得著名哦~ net/aa_3651296

打开附件,发现是张图片,md5:1a4fb3fb5ee12307,在线查询md5发现根本查不到。



既然是图片,可能存在隐写,所以改后缀名试试。没错,确实存在一个.zip文件,但需要密码。

📑 mail2LiHua.zip - 360压缩	3.2正式版	文件	操作 工具 素	动 😷 💷 🖾
A 新日本				
🛧 🥅 🗮 📑 mail2LiHu	Ja.zip - 解包大小为 1 KB			V v
名称	压缩	前 压缩后	类型	修改日期
₩ (上级目录)	📑 输入密码		23	2016-08-11 20:15
	为加密的文件编入密码: key.txt			
	<ul> <li>显示密码</li> <li>确定</li> </ul>	取消		
	1.4.4	/ /1.1	1	/26510066
大小: 1 KB 共 1 个文件 压缩率	E 142.3% NUCP :			dd_20917800

在winhex里看了下 不是伪加密。

那就是暴力破解了。

从题目:"没有任何特殊字符,请输入密码,记得署名哦"中获取信息。

大概下密码为: xxxxxxxLiHua具体x有多少位并不知道(其实这里有个技巧就是暴力破解压缩包密码一般在9位数以下,出题人不会让你破解密码好几天的。)

用木头字典生成自定义字典。

爆破之



Flag:



音频文件,用Audacity打开,放大音频,发现一开始有一段地方有规律。



发现图像上边有点。



于是想到二进制01。上1下0.于是把图像转化为0和0得到二进制串。

# 

þ.

## 在线二进制转ascii码得:





•



## 打开附件

<ul> <li>Misc-05</li> </ul>		_		_		-	_	-	a 17	RR Mac-010	
0 8000	IRD NOU										
12510		KOOH MIRCH	æ								- D - 6
iocali.	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$										
	Long	2.prg	3.png	4.png	5.png	6.png	7.png	Eprg	S.png	30.prg	11.prg
t I	12.010	13.prg	14.png	15.png	16.png	17.png	18.prg	19.png	20.prg	21.peg	22.010
1 (C)	2Lorg	24.prg	25.prg		http:	://b1	og.cs	dn. ne	et/qq	_3651	2966

## 这里附上个脚本:

#! /usr/bin/env python3

# -\*- coding: utf-8 -\*-

import pytesseract

from PIL import Image, ImageDraw

def get\_qr\_list():

qr\_list = list()

for a in range(5 \* 9):

qr\_list.append(list())

```
for b in range(5 * 9):
```

qr\_list[a].append(0)

```
for e in range(5):
```

```
for f in range(5):
```

fname = '%s.png' % (e \* 5 + f + 1)

```
img = Image.open(fname).convert('L')
```

sx, sy, ex, ey, tx = 0, 0, 0, 0, 2

for x in range(9):

```
ty = 2
```

tx += 1

sx = x \* 22 + tx + 1

for y in range(9):

ty += 1

```
sy = y * 21 + ty + 1
```

```
ex, ey = sx + 20, sy + 19
```

```
img_temp = img.crop((sx, sy, ex, ey))
```

```
code = pytesseract.image_to_string(img_temp, config="-psm 5")
```

return qr\_list

def get\_qr\_image(qr\_list):

```
img = Image.new('L', (10 * 47, 10 * 47), (255))
```

for e in range(5 \* 9):

```
for f in range(5 * 9):
```

if qr\_list[f][e]:

draw.rectangle(((e + 1) \* 10, (f + 1) \* 10, (e + 2) \* 10, (f + 2) \* 10), fill=(0))

```
print(qr_list[f][e], ' ', end=")
```

print()

img.save('flag.png')

if \_\_\_name\_\_ == '\_\_\_main\_\_\_':

get\_qr\_image(get\_qr\_list())

在数独文件下运行该脚本(先把数独文件定位好,不懂怎么定位的自行百度二维码定位点知识,然后在运行脚本),得到个二维码,扫出的结果为:

```
Vm0xd1NtUXIWa1pPVIdoVFIUSINjRIJVVGtOamJGWnIWMjFHVIUxV1ZqTIdNakZIWVcxS1IxTnNhRmhoTVZwe
```

Base64多次解密得: flag{y0ud1any1s1}

ISCC2017-Misc-题目下载:https://pan.baidu.com/s/1geVZM9t