BugKu-杂项(Misc)的部分Writeup(持续更新,直到刷完)



 Starry'Quan
 ● 己于 2022-03-18 14:26:19 修改
 ● 3712 ☆ 收藏 10

 分类专栏:
 BugKu 文章标签: 信息安全 经验分享 安全

 于 2020-06-17 19:51:06 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/weixin_44830645/article/details/106810064

 版权



BugKu 专栏收录该内容

2 篇文章 0 订阅 订阅专栏

MISC题的部分writeup(持续更新)

```
    1.签到题
    2.这是一张单纯的图片
```

```
3.隐写
```

4.telnet

```
5.眼见非实(ISCCCTF)
```

6.啊哒

```
7.又一张图片,还单纯吗
```

8.猜

9.宽带信息泄露

10.隐写2

11.多种方法解决

- 12.闪的好快
- 13.come_game
- 14.白哥的鸽子

15.linux

第一种做法

第二种做法

16.隐写3

17.做个游戏(08067CTF)

18.想蹭网先解开密码

19.Linux2

20.账号被盗了

21.细心的大象

22.爆照(08067CTF)

23.猫片(安恒)

24.多彩

25.旋转跳跃

26.普通的二维码

27.乌云邀请码

28.神秘的文件

29.论剑

30.图穷匕见

第一种、可以用python写个脚本把它画出来,这里我就直接借用一下大佬的脚本了

第二种、在linux里面用gnuplot工具

31.convert

32.听首音乐

33.好多数组

34.PEN_AND_APPLE

35.color

36.怀疑人生

线索一、cfg1.zip

线索二、ctf2.jpg

线索三、ctf3.jpg

37.红绿灯

38.不简单的压缩包

39.一枝独秀

40.小猪佩奇

断更了,太监了,对不起,大佬们 第一次写博客,有不好的地方,麻烦大佬指正,我用了些时间把BugKu里的Misc的解题思路和套路整理了一下,发出来分享,基 本上是最完全的,各位大佬看完帮忙转发一下呗

1.签到题

给了一张二维码, 扫描关注就得到了flag



2.这是一张单纯的图片

key{you are right}

```
8A 28 00 A2 8A 28 00 A2 8A 28 00 AC 3F 1B D9 41 Š( ¢Š( ¢Š( ¬? ÙA
A8 F8 37 5D B3 BB B8 6B 5B 79 EC 67 8D E7 54 DC
                                             ″ø7]³»,k[yìg çTÜ
62 06 36 1B CO EE 57 A8 FA OA 28 AO OF 9F BC 2D b 6 À1W ú ( Ÿ4-
FO EB 5A F1 OF 8A B4 5F 15 A5 90 B0 8B 4B 1A 72 8ëZñ Š´_ ¥ °<K r
05 68 FC A9 2E A4 5B 85 7B 92 E1 B0 7E 40 D2 26
                                              hüC.¤[...{'á°~@Ò&
71 F3 18 D4 2D 7D 3B 45
                      14 00 51 45 14 00 57 9E
                                              qó Ô−};E QE Wž
DA 78 3A 2D 0F E2 C3 EB FA 54 0D 0D BE AF 03 A5 Úx:- âÃëúT * ¥
E7 95 1E E5 33 0F 98 97 FE EE ED AA 43 72 01 57 ç• å3 ~-pîi*Cr W
1D 64 06 8A 28 03 D0 A8 A2 8A 00 28 A2 8A 00 28
                                              d Š(Đ∵¢Š (¢Š (
A2 8A 00 FF 26 23 31 30 37 3B 26 23 31 30 31 3B ¢Š ÿke
26 23 31 32 31 3B 26 23 31 32 33 3B 26 23 31 32
                                             y{&#12
31 3B 26 23 31 31 31 3B 26 23 31 31 37 3B 26 23
                                             1;ou&#
33 32 3B 26 23 39 37 3B 26 23 31 31 34 3B 26 23 32;ar&#
31 30 31 3B 26 23 33 32 3B 26 23 31 31 34 3B 26 101; r&
23 31 30 35 3B 26 23 31 30 33 3B 26 23 31 30 34 #105;g&#104
3B 26 23 31 31 36 3B 26 23 31 32 35 3B D9 D9 D9 strike#125 200 8
```

然后打开一个在线解码的网站解码就可以得到flag

key{you are right}		key{you	ı are right}				
ASCII \$	ŧ Un	icode	Unicode 转 A	SCII	Unicode 转中文//	中文 转 Unicode	清空结果

这里放出解码的网址: https://tool.chinaz.com/tools/unicode.aspx 附件下载地址

3.隐写

把题目给的rar下载下来,解压后得到一张图片,先用了Winhex打开,发现没什么提示,然后又放到kali里面用binwalk检测,没 有隐藏文件,最后想到了修改图片的高度

修改图片的高度和宽度,binwalk分析一下发现什么也没有藏,那就可能是图片被改"短"了(一般改成和宽度一样,把高去用八进制转换成十 六进制,然后去winhex里面找到相同的十六进制,替换成想要的高的十六进制,改宽的原理相同) 先右键查看一下文件的高和宽

图像

 分辨率
 500 x 420

 宽度
 500 像素

 高度
 420 像素

 位深度
 32

发现宽是500,然后拿去网站转化为16进制

○ 2进制 ○ 8进制 ◉ 10进制 ○ 16进制 ○ 32进制 ○ 36进制 ○ 58进制 ○ 62进制 更多: 10 ✔						
500	转换					
进制	结果		合う 学校 時代			
2	111110100]				
8	764					
10	500]				
16	1f4					
26	tg]	小写字母			
32	FM		不包含 ILOU 字符			
36	dw		数字 + 小写字母			
52	jG		大写字母 + 小写字母			
58	9C		不包含 00lI 字符			
62	84		数字 + 小写字母 + 大写字母			

16进制为01f4,到winhex里面去搜索01f4

 89 50 4E 47 0D 0A 1A 0A
 00 00 0D 0D 49 48 44 52
 %PNG
 1HDR

 00 00 01 F4 00 00 01 A4
 08 06 00 00 00 CB D6 DF
 6 8 ÊČB

 8A 00 00 00 09 70 48 59 73 00 00 12 74 00 00 12
 Š pHYs t

 74 01 DE 66 1F 78 00 00 0A 4D 69 43 43 50 50 68
 t Pf x MiCCPPh

 6F 74 6F 73 68 6F 70 20 49 43 43 20 70 72 6F 66
 otoshop ICC prof

我们把高01A4改成和宽一样的01F4,然后保存退出,重新打开图片,就可以看到flag了

附件下载地址

4.telnet

下载zip,解压出来一个数据包,用wireshark打开 筛选telnet协议,然后直接右键追踪TCP流,就可以直接看到flag了

附件下载地址

5.眼见非实(ISCCCTF)

下载文件,名字是zip,不管他,直接丢到winhex里面看

发现还真的是zip文件,错怪他了,修改后缀为zip,打开之后发现里面有个docx文件,解压出来打开

Microso	ft Word	×
	Word 在试图打开文件时遇到错误。 请尝试下列方法: * 检查文档或驱动器的文件权限。 * 确保有足够的内存和磁盘空间。 * 用文本恢复转换器打开文件。 (C:\Users\hasee\Desktop\ctf的题	目\眼见非实.docx)
	确定	

打开报错,联想题目,眼见非实,丢到winhex里面去看

发现也是一个zip文件,修改后缀为zip打开,能解压出来一个文件夹,flag在\眼见非实\word\document.xml文件下,问我怎么知道的?一个一个试出来的

附件下载地址

6.啊哒

下载zip文件,能解压出来一个表情包,不多说,直接丢到winhex里面查看

7D 52 4D 3E A1 8B 5D 22 00 00 00 16 00 00 08 }RM>;<]" 00 00 00 66 6C 61 67 2E 74 78 74 3F B1 6E 80 97 FE BF 44 3B 35 6A 56 E1 E5 75 A1 C3 C1 A4 2D 93 flag.txt?±n€þ¿D;5jVáåu;ÃÁ¤-" 5A FA C4 B9 49 B0 AC A9 D5 00 AD 07 73 50 4B 01 ZúĹI°⊣€Õ - sPK 02 3F 03 14 03 01 00 00 00 9D 7D 52 4D 3E A1 8B ? }RM>;< 5D 22 00 00 00 16 00 00 00 08 00 24 00 00 00 00]" S 00 00 00 20 80 A4 81 00 00 00 00 66 6C 61 67 2E €¤ flag. 74 78 74 0A 00 20 00 00 00 00 00 01 00 18 00 00 txt F9 C3 77 B6 66 D4 01 00 26 F5 78 B6 66 D4 01 00 ùÃw¶fÔ &õx¶fÔ F9 C3 77 B6 66 D4 01 50 4B 05 06 00 00 00 01 ùÃw¶fÔ PK 00 01 00 5A 00 00 00 48 00 00 00 00 00 Z Н ttps://blog.csdn.n

发现末尾有flag.txt字样,猜测是个压缩包,改后缀后打开压缩包,发现有flag被加密了,一开始猜测是伪加密,但测试后,发现 不是,那就只能去找密码了,找了半天没找到,最后抱着试一试的态度,点开了图片的详细属性,发现密码就在里面...

昭相和	
ARIDOV	
照相机制造商	
照相机型号	73646E6973635F32303138
光圌值	
曝光时间	
こう 洋舟	

不难看出是一个16进制,直接16进制转文本,得出密码

16进制到文本字符串	
加密或解密字符串长度不可以超过10M	当前长度: 22
1 73646E6973635F32303138	
=	
16进制转字符 字符转16进制 测试用例 清空结果 复制结果	
1 sdnisc_2018 https://blog.csdn.net/w	

输入密码解压,得到flag

生线解密网站 :	在线16进制转文本
付件下载地址	

7.又一张图片,还单纯吗

下载下来,丢到winhex里面无果之后,在linux里面使用命令binwalk查找隐藏文件,发现很多隐藏文件

可以用binwalk -e 图片路径 或者 formost 图片路径 的方法把里面的东西分离出来 不知道是不是我操作问题,我用binwalk分离不出来,所以就用了fomost

root@kali:/mnt/hgfs/ctf的题目# binwalk 2.jpg					
DECIMAL	HEXADECIMAL	DESCRIPTION			
0	0x0	JPEG image data, EXIF standard			
12 directory: 8	0×C	TIFF image data, big-endian, offset of first image			
158792	0x26C48	JPEG image data, JFIF standard 1.02			
158822 directory: 8	0x26C66	TIFF image data, big-endian, offset of first image			
159124	0x26D94	JPEG image data, JFIF standard 1.02			
162196	0x27994	JPEG image data, JFIF standard 1.02			
168370	0x291B2	Copyright string: "Copyright (c) 1998 Hewlett-Pack			
ard Company"		https://blog.csdn.net/weixin_44830645			

分离出来之后, 会在当前目录下生成一个文件夹, 在里面能看到flag

附件下载地址

8.猜

下载图片,是个半人脸的照片,丢到winhex和linux里面一顿操作,什么都没有发现o(T---T)o,然后重新看了看题目,感觉是靠这 半张脸去猜明星,直接用百度搜图或者谷歌搜图

包含匹配图片的页面

www.facebook.com > YiFeiLiu.Official > posts

刘亦菲Yifei - Posts | Facebook



580 × 731 - 【新闻new】刘亦菲一身白色的Dior式H型裙套装, 蕃丝的长袖上衣搭配缝 有古典双排扣的包身长裙出席Miss Dior迪奥小姐艺术展览, 这也是她第一次与Dior合 作, 并接受...

fr-fr.facebook.com > YiFeiLiu.Official > posts

刘亦菲Yifei - Publications | Facebook



580 × 731 - 刘亦菲Yifei. 602 J'aime. 刘亦菲,1987年8月25日出生于湖北省武汉市, 影视女演员、歌手,毕业于北京电影学院2002级表演系本科班。 2014年凭借《铜雀 台》获得第五 ...

https://blog.csdn.net/weixin_44830645

发现是刘亦菲,按照题目要求格式提交即可

附件下载地址

9.宽带信息泄露

下载下来发现是个bin文件,丢到winhex里面看了一番,无果后百度了一下bin文件用什么软件可以打开,结果发现

.bin 是个万能的后缀,就是说啊,许多软件的作者如果写数据文件的时候(跟我一样)起名困难,很可能不知道该把自己的软件存出来的文件叫做什么格式,于是啊,既然是二进制存储的,不如就叫.bin 吧。 所以,当你看到一个.bin 格式的文件时,一方面可以先在心里默默咒骂一下软件作者,另外一方面,可以视图通过 magic number 猜测这是 个什么文件。unix下的 file 程序就是专门通过文件头部信息跟 magic number 来猜测文件格式的。猜到之后,就可以试试通过具体的格式是 否能够找到对应的软件了。

我有什么好说的呢...

联想题目,应该是路由器的配置文件,用routerpassview软件打开,题目要求提交用户名,所以搜索字段为username

<pre></pre> <pre><th>никато // DHCP // al=0.0.0.0 //</th><th>×</th><th></th></pre>	никато // DHCP // al=0.0.0.0 //	×	
查找内容(<u>N</u>): username		查找下一个(<u>F</u>)	
□全字匹配(<u>W</u>)	方向	取消	ſ
□区分大小写(C)	○向上(U) ◉向下(D)		
<pre><uptime <password="" <username="" val="218265<</pre"></uptime></pre>	> 357621 /> />		×
共计 0 项	标识: 14itps://i	blog.csdn.net/weixin	_44830645

把username所对应的val提交即可

```
routerpassview这个软件,火绒会报毒,如果要保险起见,可以去虚拟机运行ヾ(◎°▽°●)/<sup>*</sup> 附件下载地址
```

10.隐写2

下载图片下来,发现这个图片有点猖狂呀!不管他,改盘他还得盘他用binwalk可以看到有隐藏文件,可以用 binwalk -e 图片路径 分离出来

root@kali:/mnt/hgfs/ctf的题目# binwalk -e Welcomejpg					
DECIMAL	HEXADECIMAL	DESCRIPTION			
0 30	0x0 0x1E	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image			
directory: 8 52516 ssed size: 67	0xCD24	Zip archive data, at least v1.0 to extract, compre			
59264 147852	0xE780 0x2418C	End of Zip archive, footer length: 22 End of Zip archive, footer length: 22			
<pre>root@kali:/mn</pre>	t/hgfs/ctf的题目;	# https://blog.csdn.net/weixin_44830645			

可以分理处一个flag.rar,和提示.jpg,说解压密码为3位数,直接用ARCHPR破解



成功爆破出密码,密码为:871 解压出3.jpg,用winhex打开,在末尾发现flag,flag被base64加密了,解密即为正确flag

这里给出解密网站:在线base64加密解密 附件下载地址

11.多种方法解决



所以就用Winhex打开,发现格式就是base64转图片的格式

🎬 WinHex -	[KEV.exe]							– 🛛 🛛
🎏 文件(F)	编辑(E) 搜索(S) 导航(N) 查看(V) 工具(T) 考	テ业工具(I) 选项(O) 看	每□(W) 帮助(H)				19.0	8 SR-4 x86 💷 🖶 1
0 7 🗔 🕯	4) 🛪 🗊 📑 👘 🐃 🐚 🗰 🐎 🛛	M 🗛 🖧 🌿 📗	→++++++++	🍣 🎟 🔎 🦚 💒 🥮 🕺 🕅 🍕 🚩	<i>₿</i>			
KEY.exe								
Offset	0 1 2 3 4 5 6 7 8 9 10	0 11 12 13 14 15	ANSI ASCII /				NEW.	
00000000	64 61 74 61 3A 69 6D 61 67 65 2F	F 6A 70 67 3B 62	data:image/jpg;b				C:\Users\baree\De	rkton
00000016	61 73 65 36 34 2C 69 56 42 4F 52	2 77 30 4B 47 67	ase64,1VBCRw0KGg				C:(Users(nasee(De	skipp
00000032	6F 41 41 41 41 4E 53 55 68 45 55	5 67 41 41 41 49	OAAAANSUhEUgAAAI				文件大小:	3.8 KB
00000048	55 41 41 41 43 46 43 41 59 41 41	1 41 42 31 32 6A	UAAACFCAYAAAB12j					3,870 字节
00000064	73 38 41 41 41 41 41 58 4E 53 52	2 30 49 41 72 73	SSAAAAAXNSROIArs				an a	
00000080	34 63 36 51 41 41 41 41 52 65 51	1 55 31 42 41 41	4C6QAAAARhQUIBAA				(大田)時間(東)(C (北本)	1016040
00000098	45 /0 6A // /0 50 59 51 55 41 41 69 57 63 77 41 41 44 73 4D 41 41	41 97 44 41 63	bZcwAADeMAAAACE					100HH3
00000128	64 76 71 47 51 41 41 41 72 53 53	3 55 52 42 56 48	dvoGGAAArZSURBVH				100月100月30日	5.100
00000144	68 65 37 5A 4B 42 69 74 78 49 46	5 67 54 76 2F 33	he72KBitxIFoTv/3				(SCIPUSE/HE)	1670日日
00000160	39 36 54 78 35 36 34 47 31 55 6F	75 69 63 4B 67	96Tx564GlUouicKg				创建时间:	2020/06/18
00000176	31 39 68 77 50 43 44 63 72 4D 4A	A 39 6D 37 2F 37	19hwPCDcrMJ9m7/7					08:13:55
00000192	6E 34 35 7A 66 64 78 65 35 5A 33	3 73 4A 37 70 72	n45zfdxe5Z3sJ7pr				最后写入时间:	2015/10/30
00000208	48 62 66 39 72 58 4F 33 50 34 60	C 4C 76 59 50 63	Hbf9rX03P41LvYPc					10:52:13
00000224	74 62 65 4D 38 30 64 76 74 50 2B	3 33 70 6E 44 70	tbeM80dvtP+3pnDp				100.000-	٨
00000240	39 79 46 37 74 6E 65 51 76 76 6D	0 63 5A 75 2F 32	9yF7tneQvvmcZu/2				Relation	2
00000256	6C 66 37 38 7A 68 55 2B 35 69 39	9 79 78 76 34 54	1f78zhU+519yxv4T					
00000272	33 54 32 41 30 21 3/ 65 /5 64 36	5 38 42 54 32 48	31200//eud68012H				模式:	十六进制
00000288	32 33 70 50 76 58 37 28 72 77 48	48 62 66 63 73	23nDuX7/ruJHhfce				偏移地址:	decima
00000320	49 2B 33 61 57 39 5A 33 33 6D 31	47 6A 37 4C 65	I+3aW9Z33m1G17Le				每贝子节数:	53x16=848
00000336	6E 2B 39 62 73 2B 50 49 6E 64 74	35 79 77 54 33	n+9bs+PIndt5ywT3				当前窗口:	2
00000352	64 70 37 31 6D 66 4F 54 58 61 66	5 6B 75 36 66 2F	dp71mfGTXafku6f/				審口总数:	1
00000368	32 75 44 30 39 69 39 79 30 6E 37	4E 4E 64 32 6E	2uD0919y0n7NNd2n				前限病。	38.68
00000384	76 57 5A 30 36 4E 74 74 2B 53 37	7 6C 2B 2F 36 38	vW206Ntt+S71+/68					
00000400	4D 4A 63 35 4F 30 4F 53 57 70 63	3 79 65 78 6E 46	MJc5000SWpcyexnF				暂存文件夹:	55.0 GB 空余
00000416	6A 66 63 73 49 2B 4A 57 31 75 6B	3 70 52 66 76 2B	jfcsI+JWlukpRfv+				C:\Users\nasee\A	ppData\cocal\remp
00000432	76 44 43 58 4F 54 74 44 6B 6C 71	1 58 4D 6E 73 5A	vDCXOTtDk1qXMnsZ					
00000448	78 59 33 33 4C 43 50 69 56 74 62 28 72 77 77 60 78 68 97 61 96 48	10 10 55 58 37	XI33LCP1VCDDRUX/					
00000480	47 63 57 4F 39 79 77 65 34 6C 62	57 36 53 6C 46	Gownguw141bW651F					
00000496	2B 2F 36 38 4D 4A 63 35 4F 30 4F	53 57 70 63 79	+/68MJc5000SWpcv					
00000512	65 78 6E 46 6A 66 63 73 49 2B 4A	57 31 75 6B 70	exnFjfcsI+JWlukp					
00000528	52 66 76 2B 76 44 43 58 4F 54 57	7 45 37 61 2F 69	Rfv+vDCXCTWE7a/1					
00000544	37 32 50 73 74 4A 32 7A 66 73 48	6E 4F 54 70 50	72PstJ2zfsHnOTpP					
00000560	7A 36 58 52 39 4F 6D 4A 76 45 63	3 74 4C 32 64 37	z6XR9CmJvEctL2d7					
00000576	48 33 57 55 37 61 76 6D 48 33 6D	0 4A 73 6B 35 64	H3WU7avmH3mJsk5d					
00000592	66 76 2B 6E 44 43 33 43 53 57 6B	3 37 61 2F 69 37	fv+nDC3CSWk7a/17					
00000608	33 50 63 74 4C 32 44 62 76 48 33	3 43 51 70 76 33	3PctL2DbvH3CQpv3					
00000624	37 58 68 78 50 6D 4A 72 47 63 74	1 50 31 64 37 48	7XhxPmJrGctPld7H					
00000640	32 57 6B 37 5A 76 32 44 33 6D 4A	L 6B 6E 35 39 62	2WR72V2D3HJRh59D					
00000636	13 20 00 44 41 33 09 05 57 45 00 60 43 68 65 60 70 37 49 36 63 60	0 04 46 49 0D 79	1. Inelp 7Hébru Til+					
00000688	2F 36 63 4D 4C 63 4D 4D 50 52 50	6B 30 65 62 61	/6cMI c.J.IVT9k01ba					
00000704	59 6B 64 61 61 6E 73 66 74 74 62	70 4B 55 58 37	YkdaansfttbnKUX7					
00000720	2F 72 77 77 6C 7A 6B 31 68 4F 32	44 65 4E 74 4A	/rwwlzk1h02DeNtJ					
00000736	6D 53 31 4A 6D 65 78 75 36 33 75	5 55 6C 53 66 76	mSlJmexu63uUlSfv					
00000752	32 75 44 79 66 4D 54 57 49 35 59	9 64 38 30 30 6D	2uDyfMTWI5Yd800m					
00000768	5A 4B 55 6D 64 36 47 72 76 66 35	5 69 5A 4A 2B 66	ZKUmd6Grvf51ZJ+f					
00000784	57 37 50 6A 7A 4A 37 76 31 32 62	2 33 33 4C 53 64	W7PjzJ7v12b33LSd					
00000800	74 76 73 66 75 57 37 35 4C 75 58	3 37 2F 72 77 35	tvsfuW75LuX7/rw5					Φ 4 4 9 9 9
00000816	50 73 33 6D 2F 33 31 72 65 63 74	50 30 57 75 32	Ps3m/31rectPOWu2					T Second
00000832	2F 35 %C /5 6E 2B 39 62 73 2B 50	1 9D 6E /5 2F 58	/SLUN+9DS+PMnu/X					
页1/5		偏移地址:		440	= 107 选块:	440 - 458 大小:	https://blog.csdn.net/w	eixin_4483064f

所以就放到网站里面去转成图片



*请上传小于300KB的.jpg/.jpeg/.gif/.bmp/.png/.ico格式图片,不建议将大图转换。

图片转成Base64 Base64还原图片 清空纪 不

顶部

得到了一个二维码,扫描即可

这里放出转换的网址: base64在线转图片 附件下载地址

12.闪的好快



菜鸡的我只能一个一个扫了, 扫完可以得到flag

这题有点麻烦,就把flag给出来SYC{F1aSh_so_f4sT} 这里给出图片分离的网站gif分离 附件下载

13.come_game



以前就把我玩吐了,这次又尝试了上百条命,没过关...

玩了几条命后,发现没用,就退出游戏了 回到游戏文件夹,发现游戏创建了两个文件



↓ 下载		
↓ 音乐		
桌面		
• 些 本地磁盘 (C:)		
🔜 软件 (D:)		
// 文档 (F·)		https://blog.csdn.net/weixin_448闘 🕮
	一种子目经会厅,发机设用,就说出游戏。	インシュージョン (http:///////////////////////////////////

有个叫save的,猜测里面是关卡数

■ C:\Users\hasee\Desktop\新建文件夹\save1 - Notepa	++	—	- ×	:
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 谈	置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?			x
	2 🔍 🔍 🖫 🖼 🏣 🗐 📗 🖉 📓 🖉 🔚 💌 🗎 🗎 🔛 📓			_
and jpgX 🔚 savel X 🔚 DeathTimeX 🔚 winhex, exe				-1
	LINELNELNELNELNELNELNELNELNELNELNELNELNELN			
2.				
0				
			1 advented	
evenue text file	length : 29 lines : 1 Ln : 1 Col : 30 Sel : 0 0 Windows (CR LF) ANSI //	/elxin_4	INS	신입 (***)

把4改成5,重新进游戏,发现还真的是关卡数,得到flag





附件下载地址

14.白哥的鸽子

下载下来得到一个名叫jpg的文件,先不管他,直接用winhex打开,拉到最后,发现了一串奇怪的字符串

```
SC II DI 10 EZ 30 37 DE 23 DE 17 03 0E 3D ZE 03 (C M GOIP#D II].J
6A 13 76 93 78 8D D4 BB 9F 12 F3 B4 E5 5C 8C F4 j v x Ô»Ϋ ό ťå\Φô
C3 35 0F A6 72 10 97 10 63 88 4E 21 5D 43 0C 91 Å5 {r - c^N!]C `
5C 08 66 08 A5 04 24 44 48 CA C1 11 FA 8A B1 E0 \ f ¥ $DHÊÁ úбà
DE 52 03 94 80 6C 8E D9 3D 49 A0 78 C8 2D E1 8B ÞR "€lŽÙ=I xÈ-á<
EE 3D FF 00 B8 F7 A2 76 C7 41 30 56 02 CB 22 75 1=ÿ ,÷¢vÇA0V Ë"u
13 B4 67 FF 00 88 8D 7E A2 BA 88 EB C6 3B FF 00
                                                 ′gÿ ^ ~¢°^ëÆ;ÿ
                       82 6A 1F 92 12 05 A2 03 Äõÿ Œ,j′ ¢
C4 F5 FF 00 10 AF 8C 11
44 OB 50 10 24 C1 B9 65 F3 1C 22 OD CE C1 1D C8 D P $Ūeó " ÎÁ È
8D 47 DA 3E D1 EE CF 94 1A E6 2A C5 8E 3C F8 00
                                                GÚ>ÑîÏ″ æ*ÅŽ<ø
EA 03 A8 35 12 39 F0 8E 6C A2 9E 1D 66 E2 BB 87 | ê ~5 9ðŽl¢ž f⻇
74 F7 4B 65 B0 58 2F 01 3A 92 BF 1E 73 2A C7 49 t+Ke°X/ :'¿ s*ÇI
                                                     уÐ (¥0
E6 03 A7 9D 14 11 1D 79 D0 9D 28 0E A5 1D 40 20 at §
78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC xÜYiÚ dnæ{£Wlî Ü
CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67 ËbEb%î[ܶs ãÿÙfg
32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 2ivyo}1{2s3_o@aw
5F 5F 72 63 6C 40
                                                __rcl@
```

看这样子,猜测是栅栏密码,就去解密网站解密

栅栏密码加密解密

每组字数 3 加密 解密	
flag{w22_is_v3ry_cool}@@	

提交发现是错误的,去掉两个@@之后提交

15.linux

解压得到一个名叫flag的文件 这道题有多重做法,这里说两种

第一种做法

用cat命令,直接输入cat flag会冒出一大串的字符,拉倒最底下,能发现flag



第二种做法

用strings命令,输入strings flag,能查找flag这个文件里面的所有字符串,同样的,在最后可以发现flag



附件下载

16.隐写3

下载下来得到一张叫dabai的png图片,右键看了属性,发现宽跟高很不匹配,猜测是被改"短"了,所以用winhex打开

图片被改"短"了(一般改成和宽度一样,把高去用进制转换成十六进制,然后去winhex里面找到相同的十六进制,替换成想要的高的十六进制,改宽的原理相同)

做法大致和第3题相同,想知道做法的,跳回去看看就行了,做出来的结果如下图



附件下载

17.做个游戏(08067CTF)

下载下来发现是个jar文件,玩了一把

注意打开这个文件需要有java的环境





发现他居然嘲讽我,不可饶恕,必须得盘他 右键用Notepad++打开

1	pretxecric4nubesesesnub; rrnutnubnubnubnubnubnubnubnubnubnubnubnubnubn	^
2	ĸ- <mark>16</mark> 铣R0 ZD4 3噱±蜪,. xD6	
3	H, 砂、砖弪M烫云D3BNQ妹)\$玳%=NARW旇NARZE4\$好耍BABNQ280H髂踯Z87"了潘ENQNUDPEBB1BS么至96NNUDNUDNUDSNUDNUDPE	
4	NUTNUTSSNUTNUTS券KNUTNUTNUTNUTNUTNUTNUTNUTNUTNUTNUTNUTSVTNUTNUTNUTNUTnutss条KNUTNUTNUTNUTNUTNUTNUTNUTNUTNUTNUTNUT	
5	NUTNUTE3NUTNUTS非KNUTNUTNUTNUTNUTNUTNUTNUTNUTNUTNUTNUTNUTN	
6	NUBNUBSNWNNU5券KNUDNUDNUBNUBNUBNUDNUDNUDNUDNUDNUDNUDNUDNUDNUDCn/bjsxt/plane/PKEVXEOPDC4NULESESESNU	1
7	x881ymxx26x271BED.估閒xCA!xF31SO筷pCANx8DENO瞔EM幣D0G2z珲暮s儯瓾4ux朴臥氊NAR佚窞嚴xBD	
8	DE39晻╥渥⊻艈崅蕢6禤鞍傈ESE講D騁E3E<时愜眇₨至160000城p炌薃至36递è购婣0至3D@N@邁潛₨ŧSUBZ87+亃骺№₀琵蹚⊽[覺н惝倚/	
9	+DYe脗x87/DDBjx77,Z Q慩偰痐藥&R&層gXi;襺滐躶ZB99xDB9w 餮xARNUDNxAIDDB腿0羧xD0V7;頉庌xAAQD	
E 10	s_胊jሚMDC3D@`r歉a鐳塌ヂ嶻tECDE嗟z穫极1vG3=w7蔲2@茕营配DCDC28衝檉夳渶R2硕iDC2艿JN匑糯KCANARKBA	
11	DC4孽嶒 皷緑GS01DC1=ZD2,檗E2# DC2BE2G DDBSDC1屁芡ZAACAN髒s*ZC61SUBZC2V如STXDC3Z9GE2K₩+璅9Z8CE2Bq\$垪h豄\$	(
_ 12	eSUB但B湃et言N禮pDY語zU輱6tK繰280 亍\$N:場止i瘥K篇 — 20032290絶 <t矢zcbcanu th="" t廸峠es(卌zag2寽妪\uses9(zduse<=""><th></th></t矢zcbcanu>	
出 13	SONARSCAN投4▽樣8來94GS來BBDC3來CB1來A3/%CAN准▽翻來BSUB來8B) 新 《家CBDDB/该茨 葦(F 岝 8 "來93DC11喤∝t來BBSO9來A1 <etx s<="" th="" 勺=""><th></th></etx>	
14		
15	BS根漉zWEM暑ESC9寢zA2SUBEM榇zB0<阧愦c	
16	橢 3★27:★283 10 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 -	
17	■ \$P\$53\\$OH \$\$5-麥VNUD[癇鼻&B6%碎媜;ZEMX股v按FSWXh肢NAN;(珯SEG9va75GJ鬝u豬i緱i(ptJ的18BMACK]共发9F#陏\$肈K	
18	■ xB42ENQ2)BUS xFD GS xFA>A? 緝EOT龍xA0US DC3 xF4DC3 倊J邢BS xFA9AxBF xE8 FSA奎whUS 空齪ES絶 ■ 砷mDC2潤PKBEUBS`茶郖区	
19	DC3RDC4\$!與工物!毗e擴瓦猢瞓	
20	1束95.0呾花#'	
21	□ 理 第60070滩620520坪獙鮺 U竜:2,cp35355224光射励崖c3C11552532526365 藕狰椯崘[1790柔罟553266535352553553555355535555555555555	
22	\$882DC2_+2890"887-TpSIRE3NAR早泪抑种攊和B	
23	」j襦RS%DC4杆EODIKS\$\$298CAN速▼ZF8EOT 毵AZ841ZF21RS/用S/用S/用S/和猫jGZB9/+等Z8A,d注D eENORZF1(覽貯樹; ZD062撰ZE	i
24		
25		
26	略泽維妈網羅·發生 网络20559) 损义 KONIKARDS> XA建R1 57样 @24KK211 吨, IDM 朝 KANDBH+J 涩 1 域 <dg2 1="" g表<="" th="" 市="" 金嶂;=""><th></th></dg2>	
27	P藏 [19] WR [202][10][2][1][1][2][1][2][1][1][1][2][1][2][1][1][2][1][1][1][1][1][1][1][1][1][1][1][1][1]	
28	│`艾GS>Ⅲ·甜喋QS0胛囵XQo四B4E00/]枯虾匡モ]作生诠c戴冠EC"	
29		
< 30		
Norm		1/15
Norm	ar text life length : 151,952 lines : 910 Lh : 1 Col : 1 Set : 010 Milliontosh (CK) C, ANSE WEXTER 4 PNS	신물

因为zip算法的创始人的名字缩写是PK,所以看到PK就基本可以断定是zip文件了



flag在cn\bjsxt\plane\PlaneGameFrame.class文件下,因为PlaneGameFram翻译过来是游戏框架的意思,所以用Notepad++打开 搜索字符串flag就可以得到flag

	📔 C:\U	Jsers\hasee\Desktop\Linux文件共享\ctt的题目\cn\bjsxt\plane\PlaneGameFrame.class - Notepad++	_		×
ł	文件(F)	编辑(E) 搜索(S) 视图(V) 编码(V) 语言(L) 没管(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?			x
ľ	🕞 🚽	⊟ № 8 0 4 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			
	🔚 omd. j	jpg 🗷 🔚 winhex. exe 🔀 🔚 MANIFEST. MF 🔀 🔚 Plane. class 🗷 🔚 PlaneGameFrame. class 🗵			
	16				^
21	17				
	18				
1	19				
-	20				
	21				
T	22				
	23				
Ш	24				
Ш	25				
Ш	26				
Ш	27				
Ш	28				
Ш	29				
Ш	30	X\能得identify and the set of the se	wt/Gra	aphics	3;E
Ш	31				
Ш	32				
Ш	33				
	34				
	35				
	36				
	37				
	38				
	39				
	40				
	41				
	42				

43 44 45			,
Normal text file	length : 3,974 lines : 55	Ln:30 Col:183 Sel:4 1	> Macintosh (CR):sdANSI//veixin_444INS44

这里要注意的是,flag是base64位加密过的,要提交解密后的flag才能得分

base64解密网站

18.想蹭网先解开密码

Challenge	3097 Solves	×
想	!蹭网先解开密码 100	3
flag格式: flag{你	破解的WiFi密码}	
tips: 密码为手机	号,为了不为难你,大佬特地让我悄	消地把前七位告
v年1小 1391040**		
Goodluck!!		
作者@NewBee		
wifi.cap		
Flag		Submit
	https://blog.csdn.net/	veixin 448306

下载下来得到了一个数据包,再看了看题目的提示 知道了是破解wifi密码,先用软件或者python生成一个11位数的字典





在kali里面用aircrack-ng -w pass.txt wifi.cap这条命令就可以开始爆破了



			A:	ircı	racl	<- ng	1.1.	.5.2	2								
[00:00:02] 8860/8	3999	e ke	eys	tes	sted	1 (4	1029	9.12	2 k,	/s)							
中小子し中か			-														
Time left: 0 seco	onds	5												9	98.4	16%	
作来、小甲																	
TESH CAPT		KE)	(F(DUNE)!	13	3910	9407	7686	5]							
5 전 10 September 2011년 1983																	
11 15 10 1 5																	
Master Key 👘 👘	75	F9	58	8D	99	18	41	DO	BC	ΒA	55	7D	8B	Β4	93	8D	
Change the world h	87	5C	50	Α5	80	83	81	59	90	59	64	A2	CA	EB	В1	6C	
change the world t																	
Transient Key :	17	29	FC	2B	66	5B	78	4F	9F	41	E3	4B	11	35	DB	56	
	7C	5B	38	41	EB	37	01	80	0E	AD	CA	32	ED	A8	E0	0C	
한 날 것 않게 전 문화하였다.	35	02	75	DA	C3	Α9	2C	04	84	4D	D6	29	AO	0D	DB	03	
이는 것같은 것을 가려야 한다.	2F	7D	1B	43	СВ	32	79	5D	06	6E	E0	59	Α6	22	E7	B0	
									http	o.//b	log	ood	n nc	+/007	sivir	- 11	020645
EAPOL HMAC :	CF	5E	E8	69	54	9C	9F	90	'A7'	°1/AL	0A	80	E96	ΥCΈ'	- gb	'EB'	050045

破出来密码为13910407686,按题目要求格式提交即为flag

附件下载

19.Linux2

root@kali:/mn	t/hgfs/Linux文件:	分享/ctf的題目# binwalk brave
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0×0	Linux EXT filesystem, rev 1.0, ext3 filesystem dat
a, UUID=cf6d7	bff-c377-403f-84a	ae-956ce3c9e3c9
4127744	0x3EFC00	Executable script, shebang: "/usr/bin/env bash"
4127746	0x3EFC02	Unix path: /usr/bin/env bash
8388608	0x800000	Linux EXT filesystem, rev 1.0, ext3 filesystem dat
a, UUID=cf6d7	bff-c377-403f-84	ae-956ce3c9e3c9
9298944	0x8DE400	Linux EXT filesystem, rev 1.0, ext3 filesystem dat
a, UUID=cf6d7	bff-c377-403f-84	ae-956ce3c9e3c9
9308160	0x8E0800	Linux EXT filesystem, rev 1.0, ext3 filesystem dat
a, UUID=cf6d7	bff-c377-403f-84	ae-956ce3c9e3c9
9324544	0x8E4800	Linux EXT filesystem, rev 1.0, ext3 filesystem dat
a, UUID=cf6d7	bff-c377-403f-84	ae-956ce3c9e3c9
9345024	0x8E9800	Linux EXT filesystem, rev 1.0, ext3 filesystem dat
a, UUID=cf6d7	bff-c377-403f-84	ae-956ce3c9e3c9
13712384	0xD13C00	JPEG image data, JFIF standard 1.01
root@kali:/mn	t/hafs/Linux文件 [,]	分享/ctf的题目# https://blog.csdn.net/weixin_44830645

用bindwalk -e brave把隐藏的东西分离出来,或者用formost分离出来

进入分离出来的文件夹,找一下,就可以找到flag,flag在_brave.extracted\ext-root\o8\huas.txt文件下

Linux文件共享 » c	tf的题目 > _brav	e.extracted > ext-	root > o8	∨ ひ 搜
^	修改	日期	类型	大小
	2020)/6/23 9:34	文本文档	1 KB
🥘 huas.txt - 记事	本			
文件(F) 编辑(E)	格式(O) 查看(V)	帮助(H)		
KEY{24f3627a8	36fc740a7f36	ee2c7a1c124a}		

做法二

根据题目的提示,可以直接用grep命令查找字符串"KEY"

root@kali:/mnt/hgfs/Linux文件	·分享/ctf的题目;	# arep 'KEY'	-a brave	
0q00)'.7(00000A000000'0p3000H	KEY{24f3627a861	fc740a7f36ee	2c7a1c124a	a}
08100~800000 0?0)Y0 05000	99HVVVmEVJVFV窥V	ENt♥	e∜Ke\w ü	IVZ' 000900k00PA0
U3210#"! UtpØadØØØKEY{}Ø NØØF	-0 0002V00S0002	2V		
		0<0m{00w@?!	0001070;00	0010FrGX30r00
				0 02

Linux系统中grep命令是一种强大的文本搜索工具,它能使用正则表达式搜索文本,并把匹 配的行打印出来。grep全称是Global Regular Expression Print,表示全局正则表达式版本,它的使用权限是所有用户

20.账号被盗了

这道题,我去的时候,网页已经404了...



404 Not Found

nginx

想知道做法的话,可以去看别人的writeup

21.细心的大象

下载下来是一张图片,结合题目,细心,猜测是右键看图片的详细信息

🔳 1.jpg 属性		×
常规安全	详细信息 以前的版本	
属性	值	^
说明 ———		
标题	出题人已经跑路了	
主题	出题人已经跑路了	
分级	$\diamondsuit \diamondsuit \diamondsuit \diamondsuit \diamondsuit$	
标记		
备注	TVNEUzQ1NkFTRDEyM3p6	
来源 ———		
作者	Bugku	
拍摄日期	2017/8/10 11:53	
程序名称	sagit-user 7.1.1 NMF26X V8.2.26.0.NC	
获取日期		
版权		
图像 ———		
图像ID		
分辨率	3016 x 4032	
宽度	3016 像素	
高度	4032 像素	
水平分辨率	72 dpi	
垂直分辨率	72 dpi	
位深度	24	*
删除属性和个人	<u>、信息</u>	
		∄(<u>A)</u> 860645

果不其然在备注那里有一串疑似base64编码的东西,解密之后是一串疑似密码的字符串

Base64编码转换

TVNEUzQ1NkFTRDEyM3p6	
「清空」「加密」「解密」□解密结果以16进制显示	
MSDS456ASD123zz	
复制	

然后去kali里面用binwalk查看有没有隐藏文件,发现有一个rar的文件然后把他们分离出来

<pre>root@kali:/mn</pre>	t/hgfs/Linux文件	分享/ctf的题目# binwalk 1.jpg
DECIMAL	HEXADECIMAL	DESCRIPTION
0 12 directory: 8	0x0 0xC	JPEG image data, EXIF standard TIFF image data, big-endian, offset of first image
5005118 6391983 MAIN_HEAD	0x4C5F3E 0x6188AF	PARity archive data RAR archive data, version 4.x, first volume type:
root@kali:/mn	t/hgfs/Linux文件	分享/ctf的题目# binwalk -e 1.jpg
DECIMAL	HEXADECIMAL	DESCRIPTION
0 12 directory: 8	0x0 0xC	JPEG image data, EXIF standard TIFF image data, big-endian, offset of first image
5005118	0x4C5F3E	PARity archive data
6391983 MAIN_HEAD	0x6188AF	RAR archive data, version 4.x, first volume type:
root@kali:/mn	t/hgfs/Linux文件	分享/ctf的題目# https://blog.csdn.net/weixin_44830645

打开发现是一个加密了的压缩包,那密码肯定就是我们刚刚解密出来的字符串了,解压出来之后,是一张什么提示都没有的图 片,猜测是图片被改短了

我们把01A4改成和宽一下的01F4就可以看到flag了

BLI

BUGKU{a1e5aSA}

https://blog.csdn.net/weixin_44830645

附件下载

22.爆照(08067CTF)

把图片下载下来,发现是一个动漫图片(手动滑稽)缘什么空的,挺不错的,推荐看看(doge) 不多说了,直接开始做题,我看着题目,一开始还以为是ms08067呢,想了想发现不可能,把他放到kali里面用binwalk查看一下 有没有隐藏的文件,发现有东西,把它们分离出来

root@kali:/	/mnt/hgfs/Linux文件	分享/ctf的题目# binwalk -e 8.jpg	
DECIMAL	HEXADECIMAL	DESCRIPTION	
0 40499 ct, compres	0x0 0x9E33 sed size: 8362, un	JPEG image data, JFIF standard 1.01 Zip archive data, encrypted at least v2.0 to extr compressed size: 92278, name: 8	a
48892 ccod cizo.	0xBEFC	Zip archive data, at least v2.0 to extract, compr	e
63830	0xF956	Zip archive data, at least v2.0 to extract, compr	e
ssed size: 74992	0x124F0	d size: 18479, name: 888 Zip archive data, at least v2.0 to extract, compr	e
ssed size: 85397	10371, uncompresse 0x14D95	d size: 11782, name: 8888 Zip archive data, at least v2.0 to extract, compr	e
ssed size: 92377	6945, uncompressed 0x168D9	size: 92278, name: 88888 Zip archive data, at least v2.0 to extract, compr	e
ssed size: 99237	6824, uncompressed 0x183A5	size: 92278, name: 888888 Zip archive data, at least v2.0 to extract, compr	e
ssed size:	7076, uncompressed	size: 92278, name: 88888888	
ssed size:	8219, uncompressed	size: 92278, name: 888888888	e 5
108452	0X29204	End of Zip archive, hoosehogengengengengengengen	~

能分离出来一个zip压缩包,打开发现就一些文件和一个gif动图,叫我慢慢排序

	9E33.zip (评估版本)							_		×
ł	文件(E) 命令(C) 工具(§	<u>5</u>) 收藏夹(<u>O</u>) 〕	选项(<u>N</u>)	帮助(<u>H</u>)						
(添加 解压到 源 		一 一 删除	〇 <u> </u> <u> </u>	人 向导	自	2000 日描病毒	三		各式
来	1 🕂 🚺 9E33.zip - 2	ZIP 压缩文件,解包	1大小为 50	56,283 🗄	学节					~
Ŧ	名称	大/	小 压缩	后大小	类型		修改时间		CRC32	
	. .				文件夹					
	🖹 愉快的排序吧哈哈哈.gi	if 58,89	3 5	52,997	GIF 文件		2017/10/28	1	08F0DF8D	
	88888888	92,27	8	8,219	文件		2017/10/28	1	2BDC3B31	
n	8888888	92,27	8	7,076	文件		2017/10/28	1	6F836171	
	B88888	02 27	Q	6 834	\\ //+		2017/10/29	1	14001450	

000000	52,210	0,024	XIT	2017/10/20 1 IACU143C
88888	92,278	6,945	文件	2017/10/28 1 42B9AAFB
8888	11,782	10,371	文件	2017/10/28 2 06601DD5
888	18,479	11,129	文件	2017/10/28 1 76D00172
88	15,739	14,906	文件	2017/10/28 1 A756F515
🗋 8	92,278	8,362	文件	2017/10/28 1 08B388EA
<				>
-			总计 9	91文件/566,283字节.net/weixin_44830645
0x14D95 7	in archive o	ata a	t leas	st v2 0 to extract compre

解压出来,用file命令查看了一下,都是jpg文件



那就一个一个改后缀成jpg咯,然后一张一张图片查看,发现88.jpg包含一个二维码



扫描能得到bilibili,提交发现是错的,猜测是不完全,看了全部图片的详细信息后,发现888图片有备注

١.	蟚 888.jpg 属性		×	
	常规 安全	详细信息 以前的版本		1
	属性	值	^	1
if	标题			3
	主题 分级	\$ \$ \$ \$ \$ \$ \$		
	标记	~ ~ ~ ~ ~		
	备注 **源	c2lsaXNpbGk=		
	作者			
	拍摄日期 程序名称	~		

获取日期		1
版权		
图像 ———		
图像 ID		
分辨率	303 x 299	ł
宽度	303 像素	I
高度	299 像素	0
水平分辨率	96 dpi	
垂直分辨率	96 dpi	
位深度	24 *	0
删除属性和个人	信息	
	确定 取消 应用(A)	5

拿去base64解码,能得到silisili

然后用binwalk一个一个找,会发现8888的图片有藏一个压缩包

root@kali:/mn	t/hgfs/Linux文件	分享/ctf的题目/_8.jpg.extracted# binwalk 8888.jpg
DECIMAL	HEXADECIMAL	DESCRIPTION
0 30 directory: 8	0x0 0x1E	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image
10976 ssed size: 644 11760	0x2AE0 4, uncompressed 0x2DF0	Zip archive data, at least v2.0 to extract, compre size: 1202, name: 1509126368.png End of Zip archive, footer length: 22
root@kali:/mn	t/hgfs/Linux文件	分享/ctf的题目/_8.jpg.text/blog.cs/dn.net/weixin_44830645

把他们分离出来,能分离出来一个二维码,扫描能得到panama,其他的图片一切正常, 猜测这三个就是flag的组成,然后结合 之前的提示,叫我慢慢排序,多试几次就可以得到flag为flag{bilibili_silisili_panama},提交即可

附件下载

23.猫片(安恒)

下载下来是一个名字叫png的图片,根据以往的经验,改png后缀直接打开





用binwalk分析之后无果,遂用stegsolve打开,并且根据题目给的提示LSB BGR NTFS,设置图片属性



<u></u>				—	×
		Extract	t Preview		
fffe89504e470d0a	la0a0000000d4948	PNG	IH		
4452000001180000	008c080200000008	DR			
ec7edb0000059c49	444154789ceddd51	.~I	DATxQ		
6alc3b1440c13864	ff5b761610145038	j.;.@.8d	.[vP8		

3792ecaadf37afdd eef141908bd43f7e 77. .A?~ 00000000000000009f 3e56ffe1f3f3f37f	
Bit Planes	Order settings
Alpha 7 6 5 4 3 2 1 0	Extract By Row Column
Red 7 6 5 4 3 2 1 2 0	Bit Order 🔘 MSB First 💿 LSB First
Green 7 6 5 4 3 2 1 0	Bit Plane Order
Blue 7 6 5 4 3 2 1 2 0	⊖ RGB ⊖ GRB
	⊖ RBG ⊖ BRG
Preview Settings Include Hex Dump In Preview 🖌	⊖ GBR ● BGR
Preview Save Text Save E	Bin (Cancel Cancel Control (Waixin_4418306415

把Red Green Blue三项设为0,不显示他们三种颜色,Alpha不用设置,因为它代表了透明度,如果设置为0了,那么图片就看不到了

能看到是一个png的文件,按Save Bin把它保存为png文件,然后把FFFE删去,保留PNG头 打开图片发现是半截二维码



然后修改图片的高度,关于方法我前面第三题有讲,这里就不再赘述

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII	
89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR	
00	00	01	18	00	00	01	18	08	02	00	00	00	08	EC	7E	ì~	
DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C	Û œIDATxœíÝQj	
3B	14	40	C1	38	64	FF	5B	76	16	10	14	50	38	37	92	;@Á8dÿ[v P87′	
-			0.7					4.5	~~	<u>~</u>	-	<u>~</u>		~~	~~	Last the sale of	

修改好之后扫描可以得到一个百度网盘下载地址

flag.rar	▶ 保存到网盘	▲ 下载(766B)	副 保存到手机	举报	
④ 2017-12-06 07:23 失效时间: 永久有效				赞(5)	逝水***无悔 🔍
					加为好友
	文件大小:766B 打开压缩包				
©2020Baidu 移	动开放平台 服务协议 权;	利声明 版本更新 帮助中小	心 问题反馈 版权打	没诉 <mark> 帐号</mark> 认	æ ://blog.csdn.net/weixin_4483064!

下载下来之后,发现怎么样都找不到真的flag,去翻了翻大佬的博客,发现要用NtfsStreamsEditor2这个工具打开才可以看到文件,但是我怎么样都看不到,在此只能搬运这位大佬的博客了

MtfsStreamsEditor2				_		<
预览 Ntf	sStreamsEditor 2 h	ttp://blog.sir	na.com.c	n/advnetso	ft	
🦙 搜索 🌏 编辑	: 📄 记录 🕜 信息					
选择搜索类型		数据流名称匹配				
○全部NTFS磁盘 ●自定义磁盘/文件(夹)	:\Users\20340\Desktop\flag	* ~	🔎 搜索	停止		
搜索结果:共1个;用时0.015 s						
* 文件		数据流名称	大小 (字节)	可疑度 <mark>(0-5)</mark>		
C:\Users\20340\Des	sktop\flag\flag.txt:flag.pyc	flag.pyc	755	1		
						_
						_
. 📡 刪除 - 📗	导出-> 附加 +/导入<-	ᇌ 备份 >>	还原<<	导出列表		
导出结果:共1个;成功1个;失败	0个;用时0.000 s			og.osdn <mark>.net/weixi</mark> n	_448306	64

去pyc反编译网站把这个反编译一下可以得到



写一个解密脚本解决

注意两点:

encode() 只是演示一下ciphertext的由来,也就是演示了如果flag='******'加密的过程,让你明白加密过程 然后现在给你一个真的flag的 ciohertext 求解flag,解密的脚本一定是按照加密脚本 反过来写 也就是按加密脚本从下往上走。一层层解密。

```
import base64
ciphertext = [
'96', '65', '93', '123', '91', '97', '22', '93', '70', '102', '94', '132', '46', '112', '64', '97', '88', '80', '82', '137', '90', '109', '99', '112']
def decode():
flag = ''
ciphertext.reverse()
for i in range(len(ciphertext)):
  if i % 2 == 0:
    s = int(ciphertext[i]) - 10
else:
    s = int(ciphertext[i]) - 10
else:
    s = int(ciphertext[i]) + 10
    s = chr(i's)
flag = flag + s
print(flag)
decode()
```

```
flag{Y@e_Cl3veR_C1Ever!}
```

最后得出 flag{Y@e_Cl3veR_C1Ever!}

24.多彩

这道题,我想了想,空着也不好,就搬运一下业内大佬ChaMD5的wp吧 首先使用隐写神器Stegsolve



在中间地带发现了YSL(杨树林,b(̄▽ ̄)d)这个口红品牌的字样。再继续深入,Analyse→Data Extract

1 miles	– 🗆 X
Extract Preview	
000000000000000000000000000000000000	
Bit Planes	Order settings
Alpha 7 6 5 4 3 2 1 0	Extract By 🖲 Row 🔾 Column
Red 7 6 5 4 3 2 1 0	Bit Order 🖲 MSB First 🔾 LSB First
Green ☐ 7 ☐ 6 ☐ 5 ☐ 4 ☐ 3 ☐ 2 ☐ 1 🗹 0	Bit Plane Order
Blue □ 7 □ 6 □ 5 □ 4 □ 3 □ 2 □ 1 ₽ 0	⊖ RGB ⊖ GRB
Preview Settings Include Hex Dump In Preview	⊖ RBG ⊖ BRG ⊖ GBR ● BGR
Preview Save Text Save B	

Save Bin保存为一个zip包

(F)	命令(C)	上具(S)	収藏夹(O)	选坝(N)	帮助(H)		- - - -	-	- 14	fille
添加	解压到	测试	<u>00</u> 查看	副除	童找	向导	いい。信息	扫描病毒	注释	自解压格式
£	📜 out.zi	p - ZIP 压	缩文件, 解包	1大小为 67	7 字节					
G称										

这里用winrar打开会报错,得用7z等压缩工具打开才可以。

尝试了下伪加密,无果。于是整个过程就剩下一个密码。一般来说图片隐写的话,要么是二进制里藏了东西,要么就是图形藏了 东西。这里二进制里藏了zip包,剩下的密码就只能从图形里入手。图形里是21个颜色格,我分别取色

BC0B28D04179D47A6FC2696FEB8262CF1A77C0083EBC0B28BC0B28D132746A1319BC0B28BC0B28D4121DD75B59DD8885CE0A 4AD4121D7E453AD75B59DD8885

这里折腾了好久,发现是要找颜色所对应的YSL口红的色号(Ⅲ[¬]ω[¬])

搜到一个网址:

https://www.yslbeautyus.com/on/demandware.store/Sites-ysl-us-Site/en_US/Product-Variation?pid=194YSL



这里颜色值可以对应上色号,于是写脚本收集颜色值对应的色号,并把色号转换为二进制,再组合,再bin2text

```
# -*- coding:utf8 -*-
__author__='pcat@chamd5.org'
import requestsimport re
import libnum
def foo():
url=r'https://www.yslbeautyus.com/on/demandware.store/Sites-ysl-us-Site/en US/Product-Variation?pid=194YSL'
cont=requests.get(url).content
# print cont
pattern=r'YSL_color=(.*?)%20[sS]*?background-color: #(.*?)"'
rst=re.findall(pattern,cont)
dYSL=\{\}
for num,color in rst:
dYSL[color]=int(num.lstrip('0'))
lst=['BC0B28','D04179','D47A6F','C2696F','EB8262', 'CF1A77','C0083E','BC0B28','BC0B28','D13274', '6A1319','BC0B2
8','BC0B28','D4121D','D75B59', 'DD8885','CE0A4A','D4121D','7E453A','D75B59', 'DD8885']
flag=''.join('{:b}'.format(dYSL[i]) for i in lst)
print libnum.b2s(flag)
pass
if __name__ == '__main__':
foo()
print 'ok'
```

0% 正在复制			- 0	\times
已用时间: 剩余时间: 文件:	00:00:14	总大小: 速度: 已处理:		67 0
压缩率: flag.txt	 輸入密码 輸入密码: 白学家 □ 显示密码(S) 确定 	× 取消		0
	后台(B)	暫停(P)		ETIK),

解压后打开flag.txt即可。

flag{White_Album_is_Really_worth_watching_on_White_Valentine's_Day}

出题人老白学家了,白雪家给爷死!不对我好像也是白学家,那没事了。

25.旋转跳跃

下载题目文件得到一个mp3文件,然后有个提示说key: syclovergeek 可以使用MP3stege来解密MP3文件,进入到MP3stege文件目录下,运行以下命令即可

Decode.exe -X -P syclovergeek sycgeek-mp3.mp3

运行结束后会在文件夹下创建



打开即可得到FLAG



26.普通的二维码

下载解压出来是一张二维码图片,扫描可得到

已扫描到以下内容

哈哈!就不告诉你flag就在这里!

扫描所得内容并非微信提供,请谨慎使用 如需使用,可通过复制操作获取内容

https://blog.csdn.net/weixin_44830645

老规矩,走一套流程,右键属性==>winhex==>然后binwalk 右键看完没有任何信息,然后用winhex打开

00002032	E E	E E	E E	E E	E E	E E	E E	E E	E O	00	E E	E E	E E	E E	E E	E E	AAAAAAAAA AAAAAA
00002848	FF	FF	FF	FF	FO	00	FF	FF	2222222222222228 22								
00002864	FF	FF	FF	FF	FF	FF	FF	FF	2222222222222222222								
00002880	FO	00	FF	FF	FF	FF	FF	FF	FF	FF	8 9999999999999999						
00002896	FF	FF	FF	FF	FO	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00009 00000000000000000000000000000000
00002912	FF	FO	00	FF	FF	FF	FF	FF	FF	2222222228 222222							
00002928	FF	FF	FF	FF	FO	00	FF	FF	2222222222222228 22								
00002944	FF	FF	FF	FF	FF	FF	FF	FF	22222222222222222222								
00002960	FO	00	FF	FF	FF	FF	FF	FF	FF	FF	8 9999999999999999						
00002976	FF	FF	FF	FF	F0	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ουλός διαδοδού το δολόδο το δολόδο το δολόδο το δαλάδο τη δείδα τη δείδα τη δείδα τη δείδα τη δείδα τη δείδα τη σ
00002992	FF	FO	00	FF	FF	FF	FF	FF	FF	2222222228 222222							
00003008	FF	FF	FF	FF	FO	00	31	34	ΫΫΫΫΫΫΫΫΫΫΫΫΫ								
00003024	36	31	35	34	31	34	31	31	34	37	31	37	33	31	31	30	6154141147173110
00003040	31	34	31	31	36	36	31	34	35	31	33	37	31	37	31	30	1411661451371710
00003056	36	30	31	32	35	31	33	37	31	32	30	31	37	31	31	33	6012513712017113
00003072	37	31	36	33	31	34	33	31	36	32	31	35	31	31	36	30	7163143162151160
00003088	31	36	34	31	33	37	31	31	37	31	36	34	31	34	33	31	1641371171641431
00003104	33	37	31	32	34	31	35	37	31	33	37	31	32	34	31	34	3712415713712414
00003120	35	31	35	36	31	33	37	31	30	31	31	36	33	31	34	33	5156137101163143
00003136	31	35	31	31	35	31	30	34	31	31	37	35	40	78	6A	73	151151041175@xjs
00003152	65	63	6B	21													eck!

最后那里有一串奇怪的字符串,仔细查看后发现最高只有7,并没有到8,猜测是八进制,去网站八进制转成字符串,发现三个一组的时候可以转出f,猜测是三个一组转换

ASCII码在线转换计算器							
进入任何一个值							
ASCII码/ 十进制 (0 - 127)	102						
十六进制 (0 - 7F)	66						
八进制 (000 - 177)	146						
二进制	01100110						
字符串	f						
	h 结果 hlog opdp pot/woivin 449206						
把它们放到一个文件里面,但注意要把@xjseck!删去,然后可以写一个脚本来转换(注意本脚本为Python3.x版本才可运行)

```
f = open('flag.txt')
temp = []
while True:
    k = f.read(3)
    if k:
        temp.append(k)
    else:
        break
f.close()
for i in temp:
    num = '00' + i
    num = int(num, base=0)
```

转换出来的结果如下图所示

num = chr(num)
print(num, end='')

flag{Have_y0U_Py_script_Otc_To_Ten_Ascii!}
>>> |

27.乌云邀请码

下载解压得到

您好:

这是来自于WooYun的一封邀请邮件,非常高兴你通过WooYun发布有价值的漏洞,很荣幸的邀请阁下为WooYun白帽子中的一员,你可以通过如下的链接来注册

http://www.wooyun.org/user.php?action=register&code=b6d75821211e338dd56623c8825456ab&invite_email=504038236@qq.com&invite_type=0

WooYun会给你发送一封确认邮件,可以点击其中的链接完成注册,希望你继续支持WooYun

漏洞处理流程:<u>http://www.wooyun.org/help#bug</u> 白帽注意事项:<u>http://www.wooyun.org/help#whitehat</u>

本邮件由WooYun自动发送,清勿回复 WooYun是一个自由平等的漏洞和安全信息报告平台 其他关于WooYun的更多详细信息请访问<u>http://www.wooyun.org/about.php</u>

谢谢!

https://blog.csdn.net/weixin_44830645

使用winhex和binwalk无果后,用stegsolve打开

Red plane 0

您好:

Green plane 0

您好:

Blue plane 0

您好:

很明显的低位隐写有东西,明显的lsb隐写,设置之后可以得到flag

<u>څ</u>	– 🗆 X
Extract Preview	
0017666c61677b50 6e675f4c73625f59flag{P ng Lsb Y	· · · · · · · · · · · · · · · · · · ·
30755f4b306e772l 7dfffffffffffff Ou KOnw! }	
ffffffffffffffff fffffffffffff	
fffffffffffffffffffffffffffffffff	
ffffffffffffffff fffffffffffff	E
fffffffffffffffffffffffffffff	
	v
Bit Planes	Order settings
Alpha 7 6 5 4 3 2 1 0	Extract By Row Column
	1
Red 7 6 5 4 3 2 1 0	Bit Order O MSB First I LSB First
	in the second se
	13
	Bit Plane Order
	⊖ RBG ⊖ BRG
Preview Settings	
	⊖ GBR ● BGR
Preview Save Text Save E	Bin Cancel

28.神秘的文件

下载得到一个压缩包, 解压出来是为两个文件, 一个压缩包, 一个图片

	添加 提取 测试 复制 移动	删除 信息			
	🎓 🖻 C:\Users\hasee\D	96-a0b11ef6dca1	.rar\		
	名称	大小	压缩后大小	修改时间	创建时
1	🖬 🖬 🖬 🖬	287 667	287 667	2018-11-02 1	
į	🔳 logo.png	27 870	27 465	2018-10-15 1	

打开flag.zip发现,里面文件有加密,并且也有一张名为logo.png的图片

flag.zip logo.p	ong		Ó
C:\Users\hasee\Desktop\	Linux文件共享\ctf	的题目\flag.zip\	
文件(F) 编辑(E) 查看(V) 书	签(A) 工具(T)	帮助(H)	
🕂 📼 🏏 📫 🗰 🗙 添加 提取 测试 复制 移动 删除	<mark>〕</mark> 注 信息		
🦻 🗰 C:\Users\hasee\Desk	top\Linux文件共习	拿\ctf的题目\flag	.zip
名称	大小	压缩后大小	修改
2018山东省大学生网络	272 070	259 726	201
logo.png https://blog	27 870 	27 405	20

很明显的明文攻击了,我们使用ARCHPR明文攻击破解

🔏 ARC	HPR 4.5	54 Prof	fessiona	l Edition			- 0	×						
文件(F)	恢复(R) 帮	助(H)											
8	. /	2	R	٢	-	2		-						
打开	开	始!	停止	基准测试	升级	帮助	关于	退出						
加密的] ZIP/RA	R/ACE/A	RJ文件		攻击类型									
sktop\Linux文件共享\ctf的题目\flag.zip 明文 ~														
范围 明文〕 明文文	范围 长度 字典 明文 自动保存 选项 高级 明文选项 明文文件路径:													
see\D	esktop\Li	inux文件	‡共享 <mark>∖ct</mark>	的题目Vogo	.zip 📄 -	开始于	: 0	S						
	密钥		-	密钥	-	密钥		- 省						
□⁄tì	午使用二	进制文	件作为明	1文 ZIP 档案	文件									
状态窗	ĵП													
2020/1	1/6 10:1	.0:04 - A	ARCHPR 4	1.54 build 45 j	已启动			~						
								× .						
当前口令 已用时间 进度指示):]: 示器				平均速度: 剩余时间:									
				09	6									
ARCHPR	version 4	.54 (c)	1997-201	2 ElcomSoft C	o. Ltd.	EUSI/W	BIXIN_4P	4830849						

我尝试了好久的时间,怎么都爆破不出来,去百度翻了翻,可能是我版本的问题,所以我就用别人爆出来的密码解压

密码为: q1w2e3r4



ctrl+a全选后复制出来得到了一个假的flag



root@kali: 能大赛决赛	/mnt/hgfs/Linux文件 writeup.docx	分享/ctf的题目# binwalk 2018山东省大学生网络	安全技
DECIMAL	HEXADECIMAL	DESCRIPTION	
0	0x0	Zip archive data, at least v2.0 to extract,	compr
ssed size:	362, uncompressed	size: 695, name: docProps/app.xml	
672 ssed size:	0x2A0 387, uncompressed	Zip archive data, at least v2.0 to extract, size: 773, name: docProps/core.xml	compr
1370	0x55A	Zip archive data, at least v1.0 to extract,	compr
ssed size:	36452, uncompresse	ed size: 36452, name: docProps/thumbnail.jpeg	
37875	0x93F3	Zip archive data, at least v2.0 to extract,	compr
ssed size:	1285, uncompressed	I size: 4056, name: word/document.xml	
ssed size:	476, uncompressed	size: 1529, name: word/fontTable.xml	compr
ssed size:	222845, uncompress	sed size: 222845, name: word/media/image1.png	compr
262627	0x401E3	Zip archive data. at least v2.0 to extract.	
ssed size:	1117, uncompressed	J size: 2847, name: word/settings.xml	compr
263791	0x4066F	Zip archive data, at least v2.0 to extract,	
ssed size:	2920, uncompressed	l size: 29509, name: word/styles.xml	compr
266756	0x41204	Zip archive data, at least v2.0 to extract,	
ssed size:	1512, uncompressed	l size: 6803, name: word theme theme1 xml	0645
268319	0x4181F	Zip archive data. at least v2.0 to extract.	compr

把它改成zip后缀后直接打开,在docProps目录下有一个flag.txt打开里面是一串base64加密





下载可得到一张图片

棄CTF_论剑场

31 31 30 31 31 30 31 20 30 31 31 31 31 30 30 31 1101101 01111001 20 30 31 31 30 31 31 31 30 20 30 31 31 30 30 30 01101110 011000 30 31 20 30 31 31 30 31 31 30 31 20 30 31 31 30 01 01101101 0110 30 31 30 31 20 30 31 31 30 31 30 30 31 20 30 31 0101 01101001 01 31 31 30 30 31 31 20 30 31 31 30 31 30 31 31 20 110011 01101011 30 31 31 30 30 31 30 31 20 30 31 31 31 31 30 30 01100101 0111100 31 20 30 30 31 30 30 30 30 31 20 30 30 31 30 30 1 00100001 00100 30 30 31 20 30 30 31 30 30 30 30 31 20 30 31 31 001 00100001 011 30 31 30 30 30 20 30 31 31 30 31 30 30 30 20 30 01000 01101000 0 31 31 30 31 30 30 30 38 7B BC AF 27 1C 00 04 CB 11010008 (4-'' Ë B2 17 DF A0 1E 00 00 00 00 00 00 6A 00 00 00 00 5 B 00 00 00 6D C5 15 1F D8 C3 E1 A9 0E D6 5B F2 33 mÅ -ØÄa© Ö[ö3

用winhex打开,看到中间有一串二进制 把它8个一组转换为16进制,然后在转换成ascii码,可以得到mynameiskey!!!hhh,肯定有用的

然后我注意到图片的宽高很不平等,猜测是宽高被修改过,遂可以修复一下

不知道怎么修复的小伙伴,可以看看第三题,我那里有讲过

棄CTF_论剑场

Not flag {666C61677B6D795F6E61 65 4 121 7. hhhh

https://blog.csdn.net/weixin_44830648

得到一张图片,但是有一些地方被挡住了,我们应该还有一些线索没有找到,回到winhex,发现紧跟在二进制后面有一串我们比 较熟悉的十六进制

 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 31
 <td

翻了翻记录文件头的小笔记,发现这个头跟7z的文件头很像,所以就修复了一下,修复之后用binwalk看了一下,不出所料,出现了7-zip文件



我们用dd分离出来

root@kali:/mnt/hgfs/Linux文件分享/ctf的题目# ls lunjian.jpg root@kali:/mnt/hgfs/Linux文件分享/ctf的题目# dd if=lunjian.jpg of=1.zip skip=959 1 bs=1 记录了12399+0 的读入 记录了12399+0 的写出 12399 bytes (12 kB, 12 KiB) copied, 1.62815 s, 7.6 kB/s root@kali:/mnt/hgfs/Linux文件分享/ctf的题目#

得到一个压缩包,但是被加密了,解密的密码就是我们之前解出来的那个字符串

<u> 1</u> .zip - 360	压缩				文件	操作	工具	帮助	$\mathbf{\Phi}$		2	×
		4		码							0%	
添加	解压到	一键解压	删除	压缩包语言								_
	📑 1.zip - f	解包大小为 8.2	КВ					▼ 搜索(包内文作	\$		Q
				📑 輸入密码		奡~?f E騜+7 ?漤{%	<除???禖 勉 媘隇 依`肉莥켗	€喋楩?? 譜郎□€ ┨3>'?UN衤	?鶸? ̄ □??橶 習趶斏□	79TL 痿硧 <i>比</i> 非锇簦\$	jB口错L???	? ?′ ?呪 N)€
(上级目	1录)	ljc2.jpg *		为加密的 myname ✓ 显示。 管理部	文件输入密码 eiskey!!!hhł 密码	吗: 确员	2	E.	~ 消			>
大小: 7.7 KB 共	生1 个文件 压	缩率 93.4%										45

解压出来可以得到一张和题目一样的图片,同样修改一下它的宽高,可以得到如下图片





然后结合之前的那张图片可以得到Not flag{666cc61677B6D795F6E616D655F482121487D} 中间的那串字符是一串bash16加密,解密即可得到flag

Base16编码使用16个ASCII可打印字符(数字0-9和字母A-F)对任意字节数据进行编码。 Base16先获取输入字符串每个字节的二进制值(不足8比特在高位补0),然后将其串联进来 再按照4比特一组进行切分,将每组二进制数分别转换成十进制 然后在下面找到对应的编码串接起来就是Base16编码。 编码0123456789101112131415 字符0123456789ABCDEF

666c61677B6D795F6E616D655F482121487D

编码 解码 清空

flag{my name H!!H}

https://blog.csdn.net/weixin_44830645

30.图穷匕见

下载下来得到一张图片,用winhex打开,搜索文件尾ffd9可以看到跟在文件尾后面有很多的字符串

00 84 21 07 FF D9 32 38 33 37 32 63 33 37 32 39 "! ÿÙ28372c3729 30 61 32 38 33 37 32 63 33 38 32 39 30 61 32 38 0a28372c38290a28 33 37 32 63 33 39 32 39 30 61 32 38 33 37 32 63 372c39290a28372c 33 31 33 30 32 39 30 61 32 38 33 37 32 63 33 31 3130290a28372c31 33 31 32 39 30 61 32 38 33 37 32 63 33 31 33 32 31290a28372c3132 32 39 30 61 32 38 33 37 32 63 33 31 33 33 32 39 290a28372c313329 30 61 32 38 33 37 32 63 33 31 33 34 32 39 30 61 0a28372c3134290a 33 35 32 39 30 61 32 38 32 38 33 37 32 63 33 31 28372c3135290a28 33 37 32 63 33 31 33 36 32 39 30 61 32 38 33 37 372c3136290a2837 32 63 33 31 33 37 32 39 30 61 32 38 33 37 32 63 2c3137290a28372c 33 31 33 38 32 39 30 61 32 38 33 37 32 63 33 31 3138290a28372c31 33 39 32 39 30 61 32 38 33 37 32 63 33 32 33 30 39290a28372c3230 c1 00 00 00 07 22.02 2.2 22.21 ~~ ~~ 2.2 000

32	39	30	ρT	32	38	33	37	32	63	33	32	33	31	32	39	290a28372C323129
30	61	32	38	33	37	32	63	33	32	33	32	32	39	30	61	0a28372c3232290a
32	38	33	37	32	63	33	32	33	33	32	39	30	61	32	38	28372c3233290a28
33	37	32	63	33	32	33	34	32	39	30	61	32	38	33	37	372c3234290a2837
32	63	33	32	33	35	32	39	30	61	32	38	33	37	32	63	2c3235290a28372c
33	32	33	36	32	39	30	61	32	38	33	37	32	63	33	32	3236290a28372c32
33	37	32	39	30	61	32	38	33	37	32	63	33	32	33	38	37290a28372c3238
32	39	30	61	32	38	33	37	32	63	33	32	33	39	32	39	290a28372c323929
30	61	32	38	33	37	32	63	33	33	33	30	32	39	30	61	0a28372c3330290a
32	38	33	37	32	63	33	33	33	31	32	39	30	61	32	38	28372c3331290a28
33	37	32	63	33	33	33	32	32	39	30	61	32	38	33	37	372c3332290a2837
32	63	33	33	33	33	32	39	30	61	32	38	33	37	32	63	2c3333290a28372c
33	33	33	34	32	39	30	61	32	38	33	37	32	63	33	33	3334290a28372c33
33	35	32	39	30	61	32	38	33	37	32	63	33	33	33	36	35290a28372c3336
32	39	30	61	32	38	33	37	32	63	33	33	33	37	32	39	290a28372c333729
30	61	32	38	33	37	32	63	33	33	33	38	32	39	30	61	0a28372c3338290a
32	38	33	37	32	63	33	33	33	39	32	39	30	61	32	38	28372c3339290a28
33	37	32	63	33	34	33	30	32	39	30	61	32	38	33	37	372c3430290a2837
32	63	33	34	33	31	32	39	30	61	32	38	33	37	32	63	2c3431290a28372c
33	34	33	32	32	39	30	61	32	38	33	37	32	63	33	34	3432290a28372c34
33	33	32	39	30	61	32	38	33	37	32	63	33	34	33	34	33290a28372c3434
32	39	30	61	32	38	33	37	32	63	33	34	33	35	32	39	290a28372c343529
30	61	32	38	33	37	32	63	33	34	33	36	32	39	30	61	0a28372c3436290a
32	38	33	37	32	63	33	34	33	37	32	39	30	61	32	38	28372c3437290a28
33	37	32	63	33	34	33	38	32	39	30	61	32	38	33	37	372c3438290a2837
32	63	33	34	33	39	32	39	30	61	32	38	33	37	32	63	2c3439 <mark>2</mark> 90a28372c
33	35	33	30	32	39	30	61	32	38	33	37	32	63	33	35	3530290a28372c35
33	31	32	39	30	61	32	38	33	37	32	63	33	35	33	32	31290a28372c3532
32	39	30	61	32	38	33	37	32	63	33	35	33	33	32	39	290a28372c353329
30	61	32	38	33	37	32	63	33	35	33	34	32	39	30	61	0a28372c3534290a
32	38	33	37	32	63	33	35	33	35	32	39	30	61	32	38	28372c3535290a28
33	37	32	63	33	35	33	36	32	39	30	61	32	38	33	37	372c3536290a2837
32	63	33	37	33	38	32	39	30	61	32	38	33	37	32	63	2c3738290a28372c
33	37	33	39	32	39	30	61	32	38	33	37	32	63	33	38	3739290a28372c38
33	30	32	39	30	61	32	38	33	37	32	63	33	38	33	31	30290a28372c3831

把他们保存下载,然后用16进制转成ascii码,就有思路了

// *1.tx	t - 记事本	:			-	×
文件(F)	编辑(E)	格式(O)	查看(V)	帮助(H)		
(7,7)						^
(7,8)						
(7,9)						
(7,10)						
(7,11)						
(7,12)						
(7,13)						
(7,14)						
(7,15)						
(7,16)						
(7,17)						
(7,18)						
(7,19)						
(7,20)						
(7,21)						
(7,22)						
(7,24)						
(7,25)						
(7,26)						
(7,27)						
(7,28)						
(7,29)						
(7,30)						
(7,31)						
(7,32)						
(7,33)						
(7,34)						
(7 25)						

	第 17 行, 第 7 列	100% Windows (CRLF) /// UTF-8 448306	
(7,36) (7,37)			~
(7,35)			

这一看就知道是坐标,以下有两种做法

第一种、可以用python写个脚本把它画出来,这里我就直接借用一下大佬的脚本了

```
import matplotlib.pyplot as plt
i=0
fig=plt.figure()
with open("text.txt") as f:
  for data in f.readlines():
    data=data.strip()
    data=eval(data)
    plt.scatter(data[0],data[1],c="255",marker=".")
    i=i+1
    print("\r\n[+] Has dealed",i,"lines")
plt.show()
```

最后可以得到一张二维码但是特别慢

第二种、在linux里面用gnuplot工具



这里需要注意的是,gnuplot一定要把括号换成空,把逗号换成空格才可以识别画图 扫描即可得到flag

31.convert



把它们直接转换为16进制,这里我就写了个python来转换为16进制

```
f1=open("flag.txt","r")
print(hex(int(str(f1.read()),2)))
f1.close()
```

Ħ	🚴 P	ythor	n 3.9.	o si	nell														—			×	(
Are.	<u>F</u> ile	<u>E</u> dit	She	e <u>l</u> l	<u>D</u> ebu	g <u>O</u>	ptions	<u>W</u> ir	ndow	<u>H</u> elp	þ												
E	Pyth 32	on 3.	9.0	(t:	ags/v3	8.9.0):9cf6'	752,	Oct	5 20	20,	15:34	:40)	[MSC	v. 1	927	64	bit	(AMD6)	4)]	on w	in	$\left \right\rangle$
·	Type	"hel	lp″,	″c(opyri	ght",	″crea	lits"	or	″lice	nse ())″ fo	r mor	re in	form	natio	on.						
4	=====			====		= RES	TART:	$C:\setminus U$	sers	∖hase	e\De:	sktop	\1.p	y ====	====			====					l
4	0x52	61722	211a(070	Jcf907	73000	004000	00000	0000	000f7	c074)	20902	c000(10900	0059	2200	0000	23e6	37019	Ja59	9b34a	1d	
111	3307	00200	10000	006	565792	266a7	067001	10148	3191	01091	1508	917c9	0156:	acbU2	ecdu	18228	SaUb	868E	40082	aU50	16628	80	
111	1454	59294 1005-1	440a:	auai	0.000	03420	1361-	24402	9a14	40404	4748	32209	aoui(74	10000	4110)1431 .eoor	1310	1044	14-00	2000	JD044	UC £0	
111	1404	103D1 8a8a0	200~	440) aafi	10900	7£46	2fec0	ierro 12ada	5304) bad2i	10913	1309: 5904	991 aa 695 a 0	7664) 21£41	C473C ReFec	2020 567a	1903 6f6/		0400 1010	04000	2014	70a9 200£0	ru ed	
111	a00a	-0430	15020	07 <i>1</i>	54341a	0706	bbdadi	12 aua 150f9	0202	066e1	4637	2501£	14fb	1393e	0581	6451	1002 5f47	c0b1	62401	-064	2683	cu c2	
110 710	57b2	25684	F816	2651	23ebs	3e05	85645	59980	e407	0370	4631	13-01	ecObi	R0650	2500	9030	7459	9020	1990-6	354	1c725	70	
223 101 101	c946	01772	29ff'	724	381bc(13efd	18cab0	565cc	fb70	2a04f	5d0a'	7e63e	0e4at	fa170	Ъ904	5dc	:2e7	9442	4fe3e	3001	72ab0	2Ъ	
201	2a31	2еЪ02	278a)	20d	392e0e	ad84	05346	5286	0a47	22f0d	ee791	34696	d605:	2daf2	67а0)7a40	lba	e481	4d6d8	la3d	8f05	e4	
H	53b1	llfcl	16f79	924	6a1748	3509E	66e791	79754	£162	dcde1	287Ы	5ba70	15129	9a9d1	c85b	eOf1	7516	15a0	58140	73e3	3a8f6	a7 -	
211	16c2;	f3fao	:90c	d45+	451bdf	494a	8с29Ъ	laf30	(32ec)	d7062	e3aa:	ab637	37acl	bebbb	630E	eee9	989a	9f5c	5a939:	ad18	37296	90	
111	d541:	£13df	£1c90	d5cl	3bd878	Bafa7	cled6	032a8	a17d	afc9e	17bel	34e16	84a4:	aOeed	6da9	ec11	5757	feOa	85097	lff	f18f	79	
111	6253	da5at	53a31	690)	ce153t	2416	3068b	l a352	422a	92f04	9ccbt	£1£12	4bbd(04085	e682	2ff	240	4ae2	bfb01	a3e4	1058b	64	
200 100	73fb	Bd1f2	202ct	58Đ	647aff	ec83	f1a55	6398	5a49	75054	8ac71	5402a	8049	99988	3332	1223	32c3	4341	26a6e	17a4	13736	36	
111	3745	69546	e7276	67±:	ab414U	Jebet	818522	22523	Ua42	4843c	c28f)	54d72	4Ucdi	Becb2	8414	64et	014d	laat	I9497Б)	2164	1601	8d -	
111 775	3242	16373	30026	6901	146ebl	11055	372676	83d3U	Ue84)	81641	balc.	32100	CUe8.	307cb	bite	20041	105a	9300	83654	/dft	3400	50	
101	4212	CD3D1 0716/	JI 200	60a)	0C1148 -1EE7/	/ea28	10170	373U3 22£ad	lueb Mual	4040Z	60ba	1760a	080C4 47654	408CD 66512	4dac	26a	a19e 727-	9070 oodd	18842 160636	1030	01003	10 E0	
111	0940	10775	30771 75-66	66al	310070	2009/ 20dad	looffOi	621 CU 8245a	Qadfi	00360	1£12	14047	a1£91	L00D3	40ua See5	120a 12613	14 18 2225	aeuu Ghae	09000	5244	53ab	00 21-	
Ħ	2d2f	31.494	ed4er	o0a cf4	6d0507	11517	13f7fc	Le1a8	f178	eañaa	hbed	5f61e	2110 751f	45959	60080 fa49	de5r	-447	abd7	77785	2660	13f7c	1f	
ER.	87c7	08afr	b0f4	431	acf382	186f)	Bcade'	7590e	7ah9	eb188	Beact	3627b	4028	745c3	9eh1	9e99	9517	c40f	76d3a	1161	277h	6c	
÷İ.	£672	43443	34560	Ober	1416a	lcf55	1365e9	945bf	d0c6	ffd47	f4f1:	a82c9	ebc9	cfe31	9ЪЗО	11681	7c90	cOet	3a700	061	61a3	c9	
1	401a	fffa	d54'	751	096405	52d73	da3e0	ърза	9256	2899a	55df	576ff	95261	53d39	4b3e	ldf	a8cb	07a5	d5e37	2fc8	3a74b	07	
C	0Ъ69	1f71a	aac31	609	9fced1	l9faa	473a96	e4307	4532	a0420	c6bb:	a969a	b277:	17714	d58a	icece	e713	ebf7	a47a3	17Ъ8	58711	83	
1	2df3	04458	5c946	69f)	63d76b	o61c2	8b4288	54385	ic4af	0d656	ed0et	f64ad	eab5t	£2456	b5da	18bf8	5326	48cd	led713)	12d)	8c64	71 -	
1	491c	949c8	314Ъ2	28d	6£9711	baala	fc16e	9a9a2	641Ъ	63c35	9a5c	909a	258el	Of01b	26e0	e2b4	4555	76a2	ce2b7	99ď.	7a94d	29	
1	a04d	91ee2	2422:	39Б	a489b6	66358	717ffl	b541	flbb	a277e	2538	4729c	6a92)	2755e	c140	lc87t	oc18	a4a2	d5cf7	99a9	Jd182	52	
1	8650	53988	51920	cd1	47c169	4cU7	1a826	odbad	1793£	187a4	35904	45dec	6401	C6116	2130	13346	3514	d4e2	(1a536)	16a)	2daU	85	
÷	1845	14122	256et	625	ea//b/	15/1	666120	JUIDO	613C) 4074	5237a 19669	27ed(329ab	48382	20a96 40064	0458	Cd88	ac9c	ae41	/be/11	911 25	15731	ce hu	
-	4084	17.2	30210 4£450	OFO.	20145	10074	754051	JUC44 7ab0a	777~	12009 afbbd	30eei a4704	10000	100094 4560,	42204	71 a7 6-11	0-00	10UZ	404L bdad	1222300	1304 5£07	14-42	ou fh	
1	8767	-8950	12e4/	4005	1301U) 201f00	76b7	(d88bc)	-33bb	0.400	5948b	27hh	eb51	20090 ac7f(92133	6011 f7fc	3231	1371	3876	(J£877)	51 ba	lacaz lháce	15	
	d5cel	63c10	2e2d(04fi	11f5a2	2325f	51352	3a9c2	875f	6cdef	h945	1366	30f0:	a1d25	4073	7471	le2a	7a36	iae4c6:	a951	3643	4e	
n	a432	ba6b	06201	fc6l	06c6a3	320et	5eb854	44898	5265	7aaf1	2965	158e0	5139	0913	6e2d	lfeae	9d8	ed90	24385	ec29	92f14	ЬЪ	
	f548	48621	lf414	4ea	1571Ъ1	6clf	9029f	e3eba	6d4c	aee3a	2cf6	12cda	c0751	bac65	d108	5c90	1215	9fb7	6725e	230	13363	c9	
"	f918	e20bd	1b48	1c5	6e30a6	62508	d6b22	17295	0319	8c8b2	506c	4Ъ816	1db5	2f4b2	3468	c71e	256	fc12	597c2	3028	394d2	0f	
	b68f	6e93e	e3cfl	bbcl	beef19	9471a	c01a80	:910d	177ae	8029f	f7fd	35f66	fc81	515a5	68fd	leeb	51ed	1986	icb42c:	a831	70384	3f 👘	
ĸ	ba4c	6£991	ob329	972	147ae7	7c851	4730f1	£1005	c972]	b9d7f	a103	975db	6d19	8£311	a2ab	4ff	55e6	£780	920Ъ3	1390	15526	a2	
1		- 1051	-01.07		100.17			10200	- ee	0007					n 00		·" ^	10	001.01			<u> </u>	



把他们复制到winhex里面

ì	- U	-	-		4		~			~	40	**	44	40	4.4	40	MUDI MOULI
	<mark>5</mark> 2	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar! Ïs
	00	00	00	00	F7	C0	74	20	90	2C	00	0D	09	00	00	59	÷Àt, Y
	22	00	00	02	3E	63	70	19	0A	59	B3	4A	1D	33	07	00	" >cp Y3J 3
	20	00	00	00	6B	65	79	2E	6A	70	67	00	F0	14	A3	19	key.jpg ð £
	10	1D	91	15	08	91	7C	90	15	EA	СВ	02	EC	D0	82	28	' ' êË ìĐ,(
	A 0	B8	68	Β4	D0	82	AO	5D	B6	28	80	81	60	89	Α9	44	,h´Đ,]¶(€ `‱©D
	DA	Α0	A 0	DA	68	B 3	42	6C	B0	2C	C4	4D	29	A 1	44	54	Ú Úh³Bl°,ÄM);DT
	04	47	48	82	20	9A	50	1D	06	C5	41	15	14	31	31	01	GH, ŠP ÅA 11
	04	4D	5D	C6	C0	50	B5	44	0C	14	Β4	10	3B	16	07	44	M]ÆÀPµD ′; D
	6C	0E	0F	71	EΒ	11	DF	1C	CE	F7	C3	3C	4F	В9	13	13	l qëßÎ÷Ã <o¹< td=""></o¹<>
	C9	99	FA	Α7	EE	4C	47	3C	26	2B	F9	89	D1	F5	4C	CD	É™ú§îLG<&+ù‱ÑõLÍ
	4E	88	FA	ЗF	7E	Α9	FO	A 8	8A	8A	8A	88	9A	AA	FO	98	N^ú?~©ð∵ŠŠŠ^š ªð″
	89	C7	F4	63	FE	C0	D2	AD	AB	AD	2B	80	36	58	0D	F8	‱ÇôcþÀÒ-«-+€6X ø
	5E	03	1F	D3	Α5	AC	56	7C	6F	6D	CC	2B	8B	80	D7	83	^ Ó¥¬V omÌ+<€×f
	28	12	00	FO	CD	E0	31	C9	43	05	02	97	46	43	41	E0	(ðÍàlÉC -FCAà
	70	СВ	Β4	AD	05	OF	80	20	29	66	E1	46	37	25	01	Fl	pË′- €)fáF7% ñ
	4F	B1	ЗA	3E	05	8B	64	5B	F4	7C	0B	16	2D	91	A 0	6F	O±:> <d[ô o<="" td="" −'=""></d[ô >
	C6	83	C2	57	B2	25	68	F8	16	2C	5B	23	EΒ	A3	E0	58	ÆfÂW°%hø ,[#ë£àX
	B6	45	59	98	0E	40	7C	03	70	4F	4B	03	C0	1E	C0	B8	MEX. 61 box y y'
	06	50	2B	00	90	37	45	99	02	9F	99	C6	85	4D	C7	25	P+ 7E™ Ÿ™ÆMÇ%
	70	C9	46	01	77	29	FF	72	D8	81	BC	03	EF	D8	CA	B0	pÉF w)ÿrØ ≒ ïØÊ°
	56	5C	CF	Β7	02	A 0	4F	5D	0A	7E	63	E0	E4	AF	A1	70	V\Ï· O] ∼càä įp
	В9	04	5D	CC	2E	79	44	24	FE	3E	30	07	2A	B0	2B	2A	²]Ì.yD\$þ>0 *°+*
	31	2E	B0	27	8A	20	D6	92	E0	EA	D8	40	53	D6	C5	28	1.°'Š Ö′àêØ@SÖÅ(
	60	Α4	72	2F	0D	EE	79	8D	69	6D	60	52	DA	F2	B7	DO	'¤r∕ îy im`RÚò Đ

我们可以发现,他是一个rar文件,把后缀改为rar然后可以解压出来一张图片,图片的详细信息里面有一串base64加密

🖹 key.jpg 属性			×
常规 安全	详细信息	以前的版本	
属性 说明	值	,	^
标题			
主题	ZmxhZ3s	wMWEyNWVhM2ZkNjM0OW	
分级	***	$\Leftrightarrow \Leftrightarrow$	
标记			
备注			
来源 ———			
作者			
拍摄日期			
程序名称			
获取日期	指定获取	日期和时间	
版权			
图像 ———			
图像 ID			
分辨率	209 x 72		
宽度	209 像素		
高度	72 像素		



解密即可得到flag

32.听首音乐

下载可以得到一个音频文件,题目没有任何提示,我们把它放进Audacity分析一下

🖨 stego100																- @ ×
文件(E) 编辑(E)	选择(S) 视图()	0	生成(G) 效果(C)	分析(A) 工具(Q) #	零助(H)										1	
II 🕨		▶ ●	I ★ / Q ↔ *	♥╬──ः XDD™●	-48 -42 ∹ ≞⊕ H∥ ⊾ ∕⊒ €	开始血視 14 -18 夏 ミ <u>ら</u> く く	-i2 -6 0'		-48 -42 -:	6 -30 -24 -1	18 -12 -6	•	: ••		•	
MME	~ U I	vicrophone (Rapoo	Gaming Headse	2 (立体声) 录制声道	1 🗸 🜓 扬声器	(Rapoo Gaming H	ieadset) ~									
9.0	1:10.0	1:11.0	1:12.0	1:13.0	1:14.0	1:15.0	1:16.0	1:17.0	1:18.0	1:19.0	1:20.0	1:21.0	1:22.0	1:23.0	1:24.0	1:25.0
X stego100 V	1.0							· · · · · ·	· · · · ·	· · · · ·			· · · · · ·	· · ·		· · · · · · · · · · · · · · · · · · ·
2	0.5															
32C #K	0.0													(
	-0.5-															
	-1.0															
	1.0															
		U	la di L						a de ar		1	4		1		I de la de la d
	0.5		Alexandrid II. Alexand	haladht d <mark>ilte A</mark> urahaa	the And the following the	An Alian da A	h hall name alla	Lade & La	t Marshall a Miller	k kin hadan data	ander Ludit di	, lin his block i	ndinadd y ddinddol d	na kandalahan n	hat, ha saidh an taile	and also deliver the
	all to a					el a la	A MARAN		والمتلج والمراجع	i de la contra de la						H. C. Marshard
	0.0-				- 1						T, T, P,		1.	and a fill of a		
	111 mili	dia halfhalfhair	a dan takihi kati katihi	(Mitharit)(tail)	ultak ar bikan t	nainden al féilige	chand (the Harri	ditter beithead	LT Helder Howe	u wiek advantie 191	U. Although	Rah has been stilled	istatutad faat	di territa del	in Malaina	ale littles of substance is with a
	-0.5	hada da A	the local sector	INN MTTAN							n in tealt i	LINE AND				and a contract of the
	0.0	hard a fear of a Mile	lan alana yi Kayla	1 N 1	a kan di k	do contra de	and out the	a na h-mara.	at a fill a fill	a water t	(4, 1, 1)	- han et av de	of an in the	e de la decea	a substant	an an da
▲ 25 ³	-1.0															
	1.0															
	<															>
项目采样室 (Hz	(1) 吸附到 美研	选区的起点和终点		0 Bt 00 /\-00	<u> </u>	0时00~	分 00 秒•									
			00.000 #9* 0	00 הל 100 ניים 10	.000 89											
CHAIL:	#	本开始初远达的石辺界	70											n	ibewolođiogduri	

上面那段音频,有短有长有空格,很容易让人联想到摩斯密码,把它们按照顺序一个一个打出来可以得到如下密码:

-...

-...

- . -... .-

- ----. .---- ----. .---- -.-.

然后去一个莫斯密码解密的网站解密即可得到flag

摩斯密码

摩斯密码在线加密解密工具

····· 	
Space: Short: Long: 加密 解密	
5BC925649CB0188F52E617D70929191C	
动力来自 <u>CTF论坛</u> . 没有美工-。	

33.好多数组

下载下来得到一堆的数独,自己解出来也没啥用,也没啥思路,这里解直接借用一位大佬的wrtieup了,因为他写的比较详细, 链接如下:乔悟空

zip没有后缀,winhex打开,发现确实是zip,修改后缀,解压得到一堆图片,内容是数独



非常壮观,出题人也是费劲了,这个就是二维码分成了25部分,把有数字的涂黑,拼到一起就能组成一个二维码,思路是看来的,但是怎么才能快速完成这一系列的工作呢,怎么能快速获取黑点呢,全点一遍有点呆吧......

每一个有九行,如果能选某一行的像素点遍历,估计就可以实现了,go, (n years later……□)

他终于来了,全网独家脚本,哈哈哈哈哈哈,可能没人和我这么闲吧哈哈哈哈 我们知道,每个数独有九行,我们要得到的是有哪几行填充了数字,我的思路就是扫描每一格中间的像素,如果是黑色,那就是 填充了数字,白色反之 此时文件结构是这样的:

```
# 此脚本用于从数独图片获取密码,有值为1,无值为0
import os
import cv2
import numpy as np
from PIL import Image
black = (0,0,0) # 黑色RGB
white = (255,255,255) # 白色RGB
# 获取给定路径图片的结果数组
def getBin(picPath):
   image = cv2.imread(picPath)
   height = image.shape[0] # 图片宽度
   wide = image.shape[1] # 图片高度
   formWide = (wide-6)/9 # 每一格宽度
   res = [] # 结果数组
   tem = '' # 暂存数组
   for i in range(9):
       for j in range(wide-6):
           px = image[int(i*(formWide-1)+(formWide/2)), j+3]
           if (px == white).all() and (j+3)%formWide > (formWide*3/4) and (j+3)/formWide > len(tem):
               tem += '0'
           if (px == black).all() and (j+3) % formWide > (formWide/4) and (j+3) % formWide < (3*formWide/4) and
 (j+3)/formWide > len(tem):
              tem += '1'
       res.append(tem)
       tem = ''
   return res
# 获取整合25张图片,获取最终结果
def getRes():
   tem = [] # 临时存储返回值
   res = [] # 存储结果数组
   for i in range(5):
       for j in range(5):
           picPath = 'zip/' + str(i*5+j+1) + '.png' # 构造文件名
           tem = getBin(picPath)
           if len(res)==0:
               res = tem
           else:
               if len(res)==(i+1)*9:
                   for x in range(len(tem)):
                      res[(i*9)+x] += tem[x]
               else:
                   for x in range(len(tem)):
                      res.append(tem[x])
   return res
resList = getRes()
resImg = Image.new('RGB',(45,45))
# 绘制图片
for x in range(45):
   for y in range(45):
       if resList[x][y] == '0':
           resImg.putpixel((x,y),white)
       else:
           resImg.putpixel((x,y),black)
resImg.save('res.png')
```

脚本获取的图片还是有一些偏差,因为题目给的图片不规范(不管我的事□),我微调脚本之后,得到下图,QR Search竟然 扫不出来,但是腾讯QQ可以,我只能说一句马老板□□哈哈哈哈哈,扫码结果:

Vm0xd1NtUXIWa1pPVldoVFIUSINjRIJVVGtOamJGWnlWMjFHVIUxV1ZqTldNakZlWVcxS1lxTnNhRmhoTVZweVdWUkdXbVZHW khOWGJGcHBWa1paZWxaclpEUmhNVXBYVW14V2FHVnFRVGs9

base64解码七次后结果: flag{yOud1any1s1}

34.PEN_AND_APPLE

下载得到一个mp4文件,然后这是一个NTFS的隐写,但我做不出来hhhh,这道题先留着,等我之后会了我再来补上,对不起啦 (>人<;)

35.color

下载下来得到一组图片,用StegSolve依次打开查看,可以发现一些英文字母











Х



🛓 StegSol	ve 1.3 by Caesum	_		\times
File Analyse	Help			
Green plane 0				
	I			
	https://pso//cos	linerauque (inde	ei/cjrj_428	30645

🛓 StegSolve 1.3 by Caesum	—	×
File Analyse Help		
Green plane 1		

	I	
http	itinan Sedelioted (1)	

连起来可以组成一句话: Make me tall,意思就是让他变高,那我们可以把他们放到winhex里面去修改他们的高度

 89
 50
 4E
 47
 0D
 0A
 1A
 0A
 00
 00
 0D
 49
 48
 44
 52
 %FNG
 IHDR

 00
 00
 01
 90
 00
 00
 01
 48
 44
 52
 %FNG
 IHDR

 00
 00
 01
 90
 00
 00
 01
 67
 9
 88
 60
 00
 00
 D1
 F7
 ÿ
 ĐN÷

 A8
 00
 00
 04
 67
 41
 4D
 41
 00
 00
 87
 0F
 00
 00
 87

之后可以看到有黑白块在图片的底部



把他们以颜色转换为二进制,白色转为0,黑色转为1,我们可以拿到七串字符串



发现横向解密解密不出来,所以就尝试了一下纵向解密,发现当纵向排列的时候,1100110能解出来为f 那我们可以写一个脚本来解密

```
f1 = '111111110101111011111'
f2 = '1111101111110111111'
f3 = '0000110010101010000'
f4 = '01001010010000001101'
f5 = '1101001101101010111'
f6 = '100110110110110110'
f7 = '00111001101101101'
```

flag = ''

```
for i in range(0,20):
    f = f1[i]+f2[i]+f3[i]+f4[i]+f5[i]+f6[i]+f7[i]
    flag += chr(int(f,2))
```

print flag

运行即可得到flag



36.怀疑人生

下载下来是一个名为zip的文件,把它改后缀为zip打开,能解压出来三个文件



线索一、cfg1.zip

发现zip文件有加密,尝试了一下,发现不是伪加密,看了看题目,并没有给什么提示,所以就直接用字典暴力破解了,我用的 字典是archpr自带的字典

🔏 ARCHPR 4.54 - 59%	– 🗆 X
文件(F) 恢复(R) 帮助(H)	
🗳 🤼 🏶	
打开 开始! 停止 基准测	试升级 帮助 关于 退出
加密的 ZIP/RAR/ACE/ARJ 文件	攻击类型
C:\Users\hasee\Desktop\怀疑人生\ctf1.	·z 字典 ~
范围 长度 字典 明文 自动作 字典选项	保存 选项 高级
子典义件路径:	~
	^
Advanced Archive Pa	ssword Recovery 统计信息:
总计口令	145,133
总计时间	31ms .
平均速度(口令/秒)	4,681,709
这个文件的口令	password 🙄
十六进制口令	70 61 73 73 77 6f 72 64 🛛 🖓
	✔ 确定
字典攻击正在进行,已处理 145,133 口名	
	59%
ARCHPR version 4.54 (c) 1997-2012 ElcomS	oft Co. Ltd. Scinner/Weixin_24/83064/5

得到解压密码后,解压可以得到一串base64的字符串



][
		È
		山沼
		送 十
		2
		Ť.
		Ĩ
iii A	第1行,第55列 100%。Windows (CRLF)小UTF-B_4483064	103 1

把它拿去解密后,可以得到一串16进制

DaseU+4冊11日干マが大

XHU2N1x1NmNcdTYxXHU2N1x1N2JcdTY4XHU2MVx1NjNcdTZiXHU2NVx1NzI=	
清空 加密 解密 □解密结果以16进制显示	
\u66\u6c\u61\u67\u7b\u68\u61\u63\u6b\u65\u72	
复制	

再拿去解密,可以得到一个

16进制到文本字符串

加密	加密或解密字符串长度不可以超过10M												
1	\u66\u6c	\u61\u67\u7b\u	ı68\u61\u63	3\u6b\u65\t	172								
							=	3					
16进	制转字符	字符转16进制	测试用例	清空结果	复制结果								
1	flag{hack	er											

线索二、ctf2.jpg

用winhex打开,可以发现最后面有一个zip的文件

00	00	80	00	00	00	00	00									nefweixin_44830645
D4	01	50	4B	05	06	00	00	00	00	01	00	01	00	5A	00	Ô PK Z
D4	01	A 1	F8	C3	5E	1B	8E	D4	01	AB	EF	64	DA	1F	8D	Ô ;øÃ^ ŽÔ «ïdÚ
20	00	00	00	00	00	01	00	18	00	11	3C	07	5A	1B	8E	< Z Ž
00	00	00	00	00	00	63	74	66	32	2E	74	78	74	0A	00	ctf2.txt
37	01	00	00	08	00	24	00	00	00	00	00	00	00	20	00	7 Ş
00	00	08	00	EC	96	87	4D	0B	2E	E9	DA	5A	00	00	00	ì−‡M .éÚZ
D8	AF	44	6A	54	5B	F8	00	50	4B	01	02	ЗF	00	14	00	ØDjT[ø PK ?
AD	E4	E3	07	7B	A 5	CD	Fl	B2	AF	02	8A	5B	8C	2C	ЗD	-äã {¥Íñ° [−] Š[Œ,=
68	FE	52	В9	DD	E8	47	EA	06	CD	Α4	F2	A6	66	8A	22	hþR'ÝèGê ͤò¦fŠ"
36	B8	48	14	07	DF	A7	EB	7B	11	07	0C	72	CE	62	92	6,H ß§ë{ rÎb'
25	9C	22	B5	2D	34	94	17	D4	54	D7	B1	56	58	00	1E	%œ"µ−4″ ÔT×±VX
D1	09	00	31	08	43	FF	0B	DD	C1	2C	E0	0A	EE	BF	D5	Ñ l Cỹ ÝÁ,à î;Õ
00	00	08	00	00	00	63	74	66	32	2E	74	78	74	6D	90	ctf2.txtm
80	00	EC	96	87	4D	0B	2E	E9	DA	5A	00	00	00	37	01	ì−‡M .éÚZ 7
00	00	00	01	FF	D9	00	00	50	4B	03	04	14	00	01	00	Ϋ́Ù ΡΚ
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

把图片后缀改为zip,打开发现需要密码,输入上一个密码发现不行,爆破软件说不是一个加密过的zip,猜测是伪加密,丢进 winhex查看,的确是伪加密,把红框里面的01改为00即可

🚟 WinHex - [2	2.zip]																				
艦 文件(F) 🖇	扁損(E) 1	叟索(<u>S)</u>	导航	(N)	查	₩) I	₹(T)	ŧ	ΨT	具(1)	选	项(C) î	窗口(W)	帮助	b(Н)		
🗋 🛃 🔚 🎕] 📚	ß	' 📫		5		Ē	ß	BB 01	10	ê) (HE:	× 4	в нех		→ -₩	-	•	3	5
2.zip																					
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		AN	SI Z	SCII	\top
00000000	50	4B	03	04	14	00	01	00	08	00	EC	96	87	4D	0B	2E	PK		ì-	•≠M .	Τ
00000016	E9	DA	5A	00	00	00	37	01	00	00	08	00	00	00	63	74	éÚZ	7		ct	
00000032	66	32	2E	74	78	74	6D	90	D1	09	00	31	08	43	FF	0B	f2.tx	¢tm	Ñ 1	. Cÿ	
00000048	DD	C1	2C	E0	0A	EE	BF	D5	25	9C	22	B5	2D	34	94	17	ÝÁ,à	î¿Õ	8œ" μ	-4″	
00000064	D4	54	D7	B1	56	58	00	1E	36	B 8	48	14	07	DF	A 7	EB	۶±×TÔ	/X	6,H	ß§ë	
00000080	7B	11	07	0C	72	CE	62	92	68	FE	52	B9	DD	E8	47	EA	{ 1	ſĺb′	hþR	ÝèGê	
00000096	06	CD	Α4	F2	Α6	66	8A	22	AD	E4	E3	07	7B	A 5	CD	Fl	ͤò	fŠ"	-äã	{¥Íñ	
00000112	B2	AF	02	8A	5B	8C	2C	ЗD	D8	AF	44	6A	54	5B	F8	00	° Š	(Œ,=	e⁻Dj	T[ø	
00000128	50	4B	01	02	ЗF	00	14	00	00	00	08	00	EC	96	87	4D	PK 1	?		ì−‡M	
00000144	0B	2E	E9	DA	5A	00	00	00	37	01	00	00	08	00	24	00	.éÚ2	Z	7	Ş	
00000160	00	00	00	00	00	00	20	00	00	00	00	00	00	00	63	74				ct	
00000176	66	32	2E	74	78	74	0A	00	20	00	00	00	00	00	01	00	f2.tx	(t			
00000192	18	00	11	3C	07	5A	1B	8E	D4	01	A1	F8	C3	5E	1B	8E	<	ΖŽ	Ô ig	Â^Ž	
00000208	D4	01	AB	EF	64	DA	1F	8D	D4	01	50	4 <mark>B</mark>					Ô «ïo	ĴÚ.	ÔP	3064	5

解压出来是一串我看不懂的东西

📕 ctf2.tx	t - 记事	本			
文件(F) 🧍	编辑(E)	格式(O)	查看(V)	帮助(H)	
	. ! ?!! ?		? .?!.?	?! .?	
		?.? !.?		!.	?
	?!!! !!!	!! !!!!? .3	?!.? !!!!!		?! ?!!.?
!!!!! !?.?!	.?!!! !!		!!!. ?		!! .?
?.?!	.?!.? .				

百度查了一下,发现是ook加密,解密可得到第二段的flag(这里的字符串是ook省略没写,可以看出来是ook加密)

3oD54e	
Text to Ook! Text to short Ook! Ook! to Text	
Text to Brainfuck Brainfuck to Text	

线索三、ctf3.jpg

是一张图片,看起来像一张二维码,但我又觉得不是,看起来太奇怪了,想着怎么修复这张二维码,但是一点办法,一点头绪都 没有,就抱着试一试的心态,拿出QQ,扫描二维码,神器的就来了



以上内容非手机QQ提供,请谨慎使用。 如需使用请复制。

https://blog.csdn.net/weixin_44830645

wc,它居然扫出来了,不得不说,QQ还是nb的

最后把他们三段拼接起来就是flag了 flag{hackermisc12580}

37.红绿灯



观察一下,发现黄灯闪的是最少的,每一个黄灯之前都有8个灯在亮,所以可以联想到二进制 我们可以推测红色和绿色对应二进制0和1,黄色作为分隔,那么久只有两种结果 01100110或10011001,这两种都拿去转换为ASCI码,发现01100110对应为f

ASCII在线转换器-十六进制,十进制、二进制

ASCII转换到	ASCII (例: a b c)
f	
添加空格	● 粉空白字符转换
十六进制转换到	16进制(例:0x61或61或61/62) 🛛 删除 0x
0x66	
十进制转换到	10进制 (例: 97 98 99)
102	
二进制转换到	2进制(例:01100001 01100010 01100011)
01100110	https://blog.csdn.net/weixin_4#33064

就可以确定绿灯对应0,红灯对应1,把他们全部转换一遍,可以手动转换,也可以写一个python的脚本 这里我就直接搬运这位大佬的脚本了

```
# -*- coding: cp936 -*-
from PIL import Image
savepath='D:\\gif\\'
im=Image.open('D:\\Traffic_Light.gif')
try:
#tell是帧数,而seek是取当前帧数的图片。
 im.save(savepath+'light{0}.png'.format(im.tell()))
 while True:
   im.seek(im.tell()+1)
   im.save(savepath+'light{0}.png'.format(im.tell()))
except:
 pass
flag=""
for i in range(1168):
 image=Image.open(savepath+'light'+str(i)+'.png')
 #print image.getpixel((115,55))#输出颜色值
 #print image.getpixel((115,145))
 if image.getpixel((115,55))==251:
   flag+=str(1)
 elif image.getpixel((115,145))==186:
   flag+=str(0)
flag= hex(int(flag,2))[2:-1].decode('hex')#二进制转字符串
print flag
```

```
然后即可得到flag
```

flag [P134s3_p4y_4tt3nt10n_t0_tr4ff1c_s4f3ty_wh3n_y0u_4r3_0uts1d3]

38.不简单的压缩包

下载下来得到一个加密过的zip文件,里面有一个加密过的swf文件,然而并不知道密码,放进winhex里面去看看

	44	10		00	vn	~~	20	00	~~	~~	~~	00	<u>от</u>	00	10	9.001
00	F9	24	ЗB	ЗF	9E	01	D5	01	3B	DF	0A	E8	9E	01	D5	ù\$;?ž Õ ;ß èž Õ
01	3B	DF	0A	E8	9E	01	D5	01	50	4B	05	06	00	00	00	;ß èž Õ PK
00	01	00	01	00	5A	00	00	00	5F	3B	06	00	00	00	50	Z _; P
4B	03	04	14	00	09	00	08	00	4A	95	A3	4E	65	1C	30	K J·£Ne O
5E	2B	00	00	00	1A	00	00	00	0C	00	00	00	74	69	6E	^+ tin
67	73	68	75	6F	2E	74	78	74	AA	C5	51	DA	25	C6	68	gshuo.txt*ÅQÚ%#h
42	FE	B6	9C	58	63	2B	80	C5	12	7C	DC	F1	6A	88	2F	Bþ¶œXc+€Å Üñj^/
A1	A 5	60	32	B7	87	C7	DE	70	11	B1	66	\mathbf{FC}	DE	EC	OF	;¥`2·≠Ç₽p ±fü₽ì
11	80	FF	C3	50	4B	07	08	65	1C	30	5E	2B	00	00	00	€ÿÃPK e 0^+
1A	00	00	00	50	4B	01	02	1F	00	14	00	09	00	08	00	PK
4A	95	A3	4E	65	1C	30	5E	2B	00	00	00	1A	00	00	00	J•£Ne 0^+
0C	00	24	00	00	00	00	00	00	00	20	00	00	00	00	00	s
00	00	74	69	6E	67	73	68	75	6F	2E	74	78	74	0A	00	tingshuo.txt
20	00	00	00	00	00	01	00	18	00	93	F1	52	E2	9C	01	"ñRâœ
D5	01	7B	86	DF	DC	9C	01	D5	01	7B	86	DF	DC	9C	01	Õ {†ßÜœ Õ {†ßÜœ
D5	01	50	4B	05	06	00	00	00	00	01	00	01	00	5E	00	õ PK ^
00	00	65	00	00	00	00	00									n.net/weixin_4483064

可以发现最后面有个压缩包,把它手动分离出来,发现分离出来的还是有加密,我以为是伪加密,试了一下,好家伙,直接报错 了

<mark> 360 - 360 - 360 - 360 - 360 - 1</mark>	缩		文件	操作	工具	帮助	Ŷ				×
	<u> </u>								1	+ 4	
添加	■ 错误报告 - 360压缩							×		女王	
<u> ↑</u> 🔲 🗄 🚦	错误类型	出错文件	Ŕ	沂在压缩文	(件路径						Q
名称	文件损坏	tingshuo.txt	C	C:\Users\l	hasee\De	sktop\1\	2.zip		明		
(上级目录)											

tingshuo.txt		15-03 18:42
	确定复制	
大小: 1 KB 共 1 个	文件 压缩率 165.4% https://blog.esch	n.net/weixin_44830645

然后去看了看题干,发现并没有什么提示,那就直接爆破呗,爆破出来显示密码是0

🔏 ARCHPR 4.54 - 1%			_	-	\times				
文件(F) 恢复(R) 帮助	(H)								
計井 井前!	🧏 💰 專止 基准测试	《 令 升级	? 帮助	 美于 	退出				
一加密的 ZIP/RAR/ACE/AR	〕文件	- 攻击类型							
C:\Users\hasee\Desktop\	1\2.zip	暴力			\sim				
范围 长度 字典 累力范围进场	明文 自动保存	选项 高	级						
 第712間返风 ✓ 所有大写拉丁文(A - 1 ✓ 所有小写拉丁文(a - 2 ✓ 所有小写拉丁文(a - 2 ✓ 所有办写拉丁文(a - 2 	Z) 7 z) 新	开始于: 吉束于:							
口令已成功恢复!					×				
Adva	nced Archive Passw	ord Recover	y 统计信息	į:					
。 总计口令	1								
总计时间	9n	ns							
平均速度(口令/秒)	11	1							
这个文件的口令	0	0 4							
	30	30 🕜							
			💙 确定	2					
ARCHPR version 4.54 (c) 19	97-2012 ElcomSoft C	Co. Ltd.	n.neuwe	11×111_41413	00040				

用这个密码解压可以得到一个文档,里面写着一串日文,拿去翻译可以得到提示

检测到日语 ▼	(200-) 中文(简体) ▼	翻译人工	翻译	(冬曲为抗度 通用领域 生物医药 ◆	□ 2 °	-(č) *
パスワードは50枚	行だそうです	×	密码是50位			
다") 合			〔)) [2] 报错 笔记▼	拼音	○ 双语对	

emmmm,这是要爆破死我=-=,没办法咯,那就直接爆破,一下子就爆破出来了,密码是50个a



	刊廾	卅	四日!	得止	星准测试	开级	帮助	天士	返出
	加密的	ZIP/RAF	R/ACE/AF	2) 文件		攻击类	型		
	C:\Use	rs\hasee	\Desktop	o\1\zip.z	ip	暴力			\sim
101		长度 范围选项 有大写拉 有小写拉	字典 丁文(A - 丁文(a -	明文 Z) z)	自动保存 升	选项 开始于: + 束 于:	高级		
	illia L¢E	成功恢	- 9) 夏!		\$	6米丁:			×
			Adv	anced A	rchive Passw	ord Reco	very 统计值	言息:	
	总计	口令			1				
ſ	总计	时间			30	ms			
	平均	速度 <mark>(</mark> 口	令/秒)		33	}			
	这个	文件的「	令		aa	aaaaaaa	aaaaaaaa	aaaaaaaaaa	аааа 🙆
1	十六	进制口:	÷		61	61616	16161616	516161616	1611 🕝
III N N			📊 保存	·			✔ ₹	谕定	
AR	CHPR V	version 4	.54 (c) 1	997-201	2 ElcomSoft (.o. Ltd.	sdn.net/	weixin_4	1830645

用这个密码解压可以得到一个小游戏,可能是我比较菜,玩不通关,然后就去百度怎么破解swf的文件,让我找到了一个工具



把游戏放进去,可以看到游戏的源码,然后找了一下,在脚本里面能看到一串奇怪的字符串





把它转为字符串就可以得到flag了

16进制到文本字符串

加密	或解密字符	串长度不可以超过1	0M		
1	3F3F6660	C61677B6A7065	787337726	565666C61	73687D2121
16进	制转字符	字符转16进制	测试用例	清空结果	复制结果
1	??flag(jpe	exs7reeflash}!!			

提交的时候记得把?!符号去掉哦

39.一枝独秀

下载下来得到一个压缩包,然后解压出来是一个jpg文件,但是并打不开,然后用winhex分析,发现它是一个zip文件

A TO IT IN TO TA TO U 1 4 3 7 3 0 1 0 ANDI ADULI 50 4B 03 04 14 00 01 00 Lf1N"^ 08 00 4C 83 6C 4E A8 88 PK E7 22 6E 86 00 00 FD 8E 00 00 17 00 00 00 D2 BB ç"n† ýŽ Č» D6 A6 B6 C0 D0 E3 2F 66 6C 6F 77 65 72 20 28 31 Ö¦¶ÀĐã/flower (1 29 2E 6A 70 67 F2 D0 33 8A 04 B7 18 48 CE 24 05).jpgòĐ3Š · HÎ\$ 33 A7 B7 48 91 68 23 AE 74 D6 3D 36 A8 59 47 28 3§ .H h#@tÖ=6"YG(AE 1A 45 1E A3 15 BD EC E4 0B D0 E6 DD 03 D2 D8 SE£ %ìä ĐæÝ ÒØ 3B 28 96 32 F1 5A 9F AF 42 AO 52 62 54 7E 14 0B ;(-2ñZŸ B RbT~ D4 C4 28 4B 05 86 5A D8 85 2E 89 9B B9 DF 73 04 ÔÄ(K †ZØ ... ** > * Bs 59 17 54 E4 90 6F EE 14 OC 91 2F 81 0F B1 CO 4C Y Tä oî '/ ±ÀL 95 6F D7 41 6C 02 B4 9E 8E 51 2B 6F D1 2C 4D C3 •o×A1 'žŽQ+oÑ,MÃ OA 27 70 4C 13 8C 04 F0 69 74 37 81 E4 E0 E7 93 'pL Œ ðit7 äàç" 47 E1 95 E9 C8 0E 1B FB BC DB 7E 35 6D 0B 70 EB Gá•éÈ û4û~5m pë 97 06 76 C5 BD 8A B8 54 C5 80 42 A5 B5 F2 7F 58 - vÅ∺Š TÅ€B¥uò X

	~~		~~	~~	~~~		<u> </u>		~~			~~			~~	in iolition ho it
7C	63	CD	D2	C3	C7	Α9	32	65	AF	59	81	4C	D6	20	EF	cÍÒÃÇ©2∈¯Y LÖ ï
27	21	F5	03	D2	81	3C	70	51	ЗF	E4	4E	6B	A3	E6	93	'!õ Ò <pq?änk£æ"< td=""></pq?änk£æ"<>
0D	2B	C9	C1	03	67	05	C7	ED	E7	C0	50	93	Fl	54	AE	+ÉÁ g ÇíçÀP"ñT⊗
3B	E9	5B	Α4	4F	F3	48	A6	AA	12	60	F5	08	5D	51	14	;é[¤OóH¦ª `õ]Q
6B	D6	63	74	E4	13	1E	65	FA	36	F8	BB	C1	64	ΕO	3E	kÖctä eú6ø»Ádà>
3E	87	EF	CD	AD	EC	81	C8	B3	0E	F8	EC	C2	6E	7B	DA	>‡ïÍ-ì È' øìÂn{Ú
59	74	17	52	D2	92	E8	43	4B	Α4	B2	ED	E8	8A	93	8D	Yt RÒ'èCK¤≤í芓
C6	82	8B	61	A 5	23	77	71	14	E1	4B	4E	72	93	5E	Α4	Æ, <a¥#wq<sup>SáKNr™hgSCn.net/weixin_44830645</a¥#wq<sup>
															• •	A 1.2

把它后缀改为zip就可以打开了需要注意的是,文件上面有一段没用的文件头需要删除

0	1	4	з	Т	J	0	1	0	9	TO	11	14	10	11	10	MNDI MOCII /
50	4B	03	04	14	00	00	00	00	00	4C	85	6C	4E	00	00	PK L1N
12	34	56	78	00	00	0.0	0.0	00	00	09	00	00	00	D2	BB	4Vx Ò»
D6	A6	B6	C0	D0	E3	2F	50	4B	03	04	14	00	01	00	08	Ö¦¶ÀÐã∕PK
00	4C	83	6C	4E	A8	88	E7	22	6E	86	00	00	\mathbf{FD}	8E	00	LflN∵^ç"n† ýŽ
00	17	00	00	00	D2	BB	D6	A6	Β6	C0	DO	EЗ	2F	66	6C	Č»C¦¶ÀĐã∕fl
6F	77	65	72	20	28	31	29	2E	6A	70	67	F2	DO	33	8 A	ower (1).indòÐ3Š

删除之后打开,说需要密码,然后就直接爆破密码

📑 1.zip - 360)	玉缩				文件	キ 操作	工具	帮助 🕐 🖘 🗆 🗆	×
添加	10000000000000000000000000000000000000	金融 金融 金融	() 一) 一)	四月				09	6
☆ 🔲 🗄	📑 1.zip -	- 解包大小为 4.3	B MB				Vv	搜索包内文件	Q
名称 (上级目录)	■	入密码 为加密的文 一枝独秀\fl □ 显示密码 管理密码	件输入密码: ower (1).jpg 吗	通定	压缩后	类型 文件夹	修改日期 2019-03-12 16:42	2
大小: 4.0 MB 非	共 123 个文	件和 1 个文件夹	压缩率 93.9	9%			https://blog	g.csdn.net/weixin_4483	0645

爆破出来密码是12345678,不知道为什么我的爆破不了



2	· · · · · · · · · · · · · · · · · · ·
当前口令: 已用时间: 进度指示器	平均速度: 剩余时间:
	0%
ARCHPR version 4	54 (c) 1997-2012 ElcomSoft Co. Ltd.

然后解压出来可以看到很多的花的图片,观察了一下,发现就这张图片的大小和别的图片不一样

🖥 flower (78).jpg	2019/3/12 16:26	JPG 文件	36 KB
🖥 flower (79).jpg	2019/3/12 16:26	JPG 文件	36 KB
膏 flower (80).jpg	2019/3/12 16:26	JPG 文件	36 KB
🖥 flower (81).jpg	2019/3/12 16:26	JPG 文件	43 KB
🖥 flower (82).jpg	2019/3/12 16:26	JPG 文件	36 KB
🖥 flower (83).jpg	2019/3/12 16:26	JPG 文件	36 KB
🖥 flower (84).jpg	2019/3/12 16:26	JPG 文件	36 KB
ייין (סבי ויייים 🖫	2010/2/12 16:26		26 MD

发现了一个很像二维码,但又不是二维码的东西



做到这里我就不会了,就去翻了翻大佬们的博客,发现需要JPHS这个工具 打开工具-open JPEG-打开刚才标记的81号

			Innut	tines				
Director Filename	E:\春秋# flower	홈训 \bugku (81).jpg	a\杂项\4	40一枝独秀	outfile	e\zip\-	-枝独秀\-	
Filesia	43 Kb	Width 96	60 pixe	l Hei	ght 635 p:	ixel		
Approxim	ate max	7	Kb 1	recommend	ed	4 Kb		
			Hidd	len				
Director Filename	E:\春秋# 6666666	音训\bugku	u\杂项\4	40一枝独秀	outfile	e\zip\-	-枝独秀\-	
Director Filename Filesiz	E:\春秋# 66666666 1 Kb	음训\\bugkı	u\杂项\4	40一枝独秀	\outfile	e\zip\-	-枝独秀\	
Director Filename Filesiz	E:\春秋5 6666666 1 Kb	음训 \bugkı	a\杂项\4 Saved	40—枝独秀 jpeg)outfil	e\zip\-	-枝独秀\一	
Director Filename Filesiz	E:\春秋# 6666666 1 Kb	Êill\bugkı	a\杂项\4 Saved	40—枝独秀 i jpeg	outfil:	e\zip\-	-枝独秀\一	
Director Filename Filesiz Director Filename	E:\春秋 66666666 1 Kb	Ê∛l \bugkı	a\杂项\4 Saved	40—枝独秀 i jpeg	()outfil	e\zip\-	-枝独秀\一	

Seek-发现需要密码,于是继续观察81号

Discost in Fight	Input jpe		-#14.50-	
Fills Muter	攻图片款改制得到的fl	lowers		
Enter the pass p	hrase and confirmation	Height 635 nivel		×
				_
D				
F				
F				
	1.			
	08	Cancel		
D	01	Cancel		

右键查看属性得到了主题flowers,可能是密码,填上试试,发现对了,把文件保存下载 然后用winhex打开,能看出来这是一个zip文件

```
50 4B 03 04 14 00 00 00 08 00 0A 83 6C 4E D8 34
                                            PK
                                                      f1NØ4
                                                 1
09 C8 E0 01 00 00 B9 02 00 00 0C 00 00 00 B2 CE
                                             Èà
                                                         ۴î
CE F2 B7 F0 B7 A8 2E 74 78 74 2D 52 DB 72 A2 40 Îò·ð·∵.txt-RÛr¢@
10 7D 4F 55 FE 66 3F 10 C9 8A 1A C5 4B 59 01 23
                                             }OUþf? ÉŠ ÅKY #
                                             ] PêX″ ôcv°gx
10 5D 16 50 C3 AA 58 94 06 05 F4 63 76 BA 67 78
F2 17 72 A6 E2 4B D7 5C 4E 9F 4B CF 88 72 28 0A ò r¦âK×\NŸKÏ^r(
83 FD A3 7A 3D 88 62 2B FD 3E 75 33 9C 88 E2 53 fý£z=^b+ý>u3œ^âS
14 8E 7C 1B DC AB 41 63 FE 7D CO 76 47 51 7B EC
                                             Ž| Ü«Acþ}ÀvGQ{ì
74 80 54 2F F5 03 5C 1A E2 DC A5 49 78 AF 16 CF
                                            t€T/õ \ âÜ¥Ix Ï
4F A2 5E CA F4 9D FC F5
                      2F 8E 2B 39 FF CD CB 11
                                            O¢^Êô üõ∕Ž+9ÿÍË
07 96 28 5E A5 7F 61 DF 53 37 9F 9D 33 38 29 31
                                             -(^¥ aßS7Ÿ 38)1
F9 C3 A7 91 C9 E6 42 14 36 75 2E 1C C4 94 1D B8 ùç`ÉæB 6u. Ä",
37 95 3B 57 7D E5 A2 E8 D3 B0 7C 7E 02 25 24 BD 7•;₩}å¢èÓ°|~ %$%
EC 5E CD 9B D9 4D D6 99 3A 58 B2 AA 69 3D E1 D1 | ì^Í>ÙMÖ™:X°ªi=áÑ
7B C4 86 47 71 A8 BA FF 78 B6 D7 ED 5D 9B CD 1E {ĆGq °ÿx¶×i]>Í
```

改zip后缀解压出来能得到一个文档, 里面有些文字

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) 从一朵花中看到一个世界,那从一段佛文中能看到什么呢? 你站在4楼的栏杆上眺望远方,如果参悟不出来就打算跳下去

佛曰:阿罰豆缽娑提諳竟諳迦亦侄栗侄大梵尼朋梵彌哆耨除怛奢般是諳燥悉哆爍冥參特參怯涅皤吉缽阿藝耶諳勝侄竟離諳諸 尼缽曰。梵究呐耨盧他姪明漫究呐得哆藐集能冥盡滅知俱朋怯室神奢羅姪豆罰帝遠蘇明梵苦奢密侄曰缽者特哆呼勝蘇不冥死 等那阿冥悉奢薩豆涅缽波罰。罰摩侄故罰夢缽恐皤寫諳闇舍哆得波苦奢即罰恐冥道一哆究梵呼冥闍哆上罰南訶諳寫冥依皤者 哆諦故死哆夷菩侄曰呐逝至皤佛諳耶

https://blog.csdn.net/weixin_44830645

下面那个加密很常见了,是与佛论禅加密,解密一下能得到

H-hDs100ZL3lhIZZbeRSbbbVRZNm32W2X33mGm3Txt999RdV9hx0
听佛说宇宙的真谛 参悟佛所言的真意 · 普度众生
春来花自青,秋至叶飘零
佛曰:阿罰豆缽娑提諳竟諳迦亦侄栗侄大梵尼朋梵爾哆耨除怛奢般是諳爍悉哆爍冥參特參怯涅皤吉缽阿藝耶諳勝 侄竟離諳諸尼缽曰。梵究呐耨盧他姪明漫究呐得哆藐集能冥畫滅知俱朋怯室神奢羅姪豆罰帝遠蘇明梵苦奢密侄曰 缽者特哆呼勝蘇不冥死等那阿冥悉奢薩豆涅缽波罰。罰摩侄故罰夢缽恐皤寫諳闍舍哆得波苦奢即罰恐冥道一哆究 梵呼冥闍哆上罰南詞諳寫冥依皤者哆諦故死哆夷菩侄曰呐逝至皤佛諳耶

然后再根据题目的提示,拿去栅栏密码解密

H-hDs100ZL31hIZZbeRSbbbVRZNm32W2X33mGm3Txt999RdV9hx0	
每组字数 4 加密 解密 HINT-ZmxhZ3tDb29seW91R290SXROb3dZb3VLbm93VGhlRmxhZ30	
	https://blog.csdn.net/weixin_44830645
泥侍到一个ΠINI,这个明显定一个Daseb4的加密,冉基去解密既能得到Πag」	
ZmxhZ3tDb29se\91R290SXROb3dZb3VLbm93VGh1RmxhZ30	

清空 || 加密 || 解密 | □ 解密结果以16进制显示

flag{CoolyouGotItNowYouKnowTheFlag}

40.小猪佩奇

还在研究