CTFshow Misc部分 做题记录

原创
FW_Suica
1、杂项签到
2、misc2
3、miscx
4, misc50
5, misc30
6、stega1
7, misc3
8, misc40
9、misc30
10、红包题第一弹
11、stega10
12、stega11
13, misc4
14、misc5
15, misc6
16, misc8
17、stega2
18、stega3

1、杂项签到

下载 附件得到zip文件,内含一个加密的flag.txt 且文件夹名称提示:忘记密码了

🔯 downloa	ad.zip (评估版	本)									
文件(F) 命令	ݤ(C) 工具(S)	收藏夹(O)	选项(N)	帮助(H)							
			Ŵ	Q	4 ⁴	1	8	Ę			
添加	解压到 测试	, 查看	删除	查找	向导	信息	扫描病毒	注释	自解压格式		
1 🛧 🌆 d	lownload.zip -	ZIP 压缩文体	牛, 解包大/	小为 38 字节	ī						
名称		^				大小	压缩后大	小类	型	修改时间	CRC32
II								文	件夹		
▶ 忘记密码	7					38		40 文	件夹	2020/1/24 23:	n.net/Nancy523

考虑伪加密,拖进ZipCenOp梭哈一下

E:\ctf\工具\软件\zipcenop>java -jar ZipCenOp.jar r download.zip success 2 flag(s) found

直接解压 得到flag

 ■ flag.txt - 记事本
 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

 flag{79ddfa61bda03defa7bfd8d702a656e4}

2, misc2

下载附件 解压 得到无后缀的file文件

十六进制编译器打开 查看

	Ŏ			3	4		6		8	9	Α	В		D	Е	F	0123456789ABCDEF
0000h:	EB	4E	90	43	54	46			48		57	00	02			00	ëN.CTF.SHOW
0010h:	02	E0	00	40	0B	F0	09	00	12	00	02	00	00	00	00	00	.à.@.ð
	40	0B	00	00	00	00	29	FF	FF	FF	FF	66	6C		67	6E	@)ÿÿÿÿflagn
		74	68	65	72	65	46	41	54			20	20	20	00	00	other FAT11
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	B 8	00	00	8E	D0	BC	00	7C	8E	D8	B8	20	08	8E	C0	B5	ŽÐ¼. ŽØŽÀµ
	00	B6	00	B1		BE	00	00	B4	02	B0		BB	00	00	B2	.¶.±.¾′.°.»²
	00	CD	13	73	10	83	C6	01	83	FE	05	73	32	B4	00	B2	.Í.s.fÆ.fþ.s2′.²
	00	CD	13	EB	E3	8C	C0		20	00	8E	C0	80	C1		80	.Í.ëãŒÀ. ŽÀ€Á.€
0090h:	F9	12	76	D1	B1	01	80	C6	01	80	FE	02	72	C7	Big	0 9 0	เผิ่น.⊻พื้‡ก.€สีเสรีสกณรี่ใ
0040h	80	C5		80	ED	04	72	BD	88		FO	0E	EQ	51	45	RE	£Å £ý r%^ Å ÅOE%

FAT文件,,不懂是啥参考一下大佬的wp:

1.44MB软盘使用的FAT文件系统通常为FAT12,根据FAT12的MBR引导记录结构,第54字节开始的8位应固定为 FAT12。而该文件中被修改成了FAT11,需要进行修复。

新建虚拟机并载入软盘镜像:





3、miscx

下载得到rar类型附件,内含两个加密的txt文件跟一个未加密的压缩包

ier misc2.rar (评估版本)		
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)		
🙀 🚞 🖪 🛄 🗑 🔹	K 🕄 🙆 🖨 🖡	-
添加解压到测试 查看 删除 查找 萨	向导 信息 扫描病毒 注释 保护 自解日	E格式
个 📑 misc2.rar - RAR 压缩文件, 解包大小为 813,137 字节		
名称 ^	大小 压缩后大小 类型	2020快乐!
I	文件夹	rat? or?
🔤 misc1.zip	812,663 812,663 WinRAR ZIP 压缩	
📄 flag.txt *	18 32 文本文档	
hint.txt *	456 368 文本文档 https://blog.csdi	

附加文本: 2020快乐! rat? or?

先查看其中的misc1压缩包内含加密的music.doc文件跟一个png后缀的图片





把图片用十六进制编辑器打开

起始页	misc	.png	A×														
	Ŏ	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	F	0123456789ABCDEF
C:5CB0h	: 18	6C	34	1F	AD	E5	B2	29	CC	35	26	96	A3	02	D 0	39	.l4å²)Ì5&-£.Ð9
C:5CC0h	: 5B	9D	E6	15	2B	CF	8E	65	B6	46	3C	07	4D	2D	7F	32	[.æ.+ÏŽe¶F<.M2
C:5CD0h	: 1A	4A	B4	F4	A 8	6F	FD	B 9	ED	6B	71	18	46	5D	88	BE	.J´ô¨oý¹íkq.F]^¾
C:5CE0h	: 96	73	4F	7F	21	A2	A0	B 8	7F	96	B6	C 5	ED	CC	77	A6	-sO.!¢¶ÅíÌw¦
C:5CF0h	: 3C	E3	3F	AF	FD	5F	DB	5B	25	0C						00	<u>≺ã?[−]ý_Û[%.æ.ód</u>
C:5D00h	: 00		49	45	4 E	44	AE	42	60	82	66	6C	61	67			IEND®B`,flag{f
C:5D10h			67	5F	31	73	5F	6E	30	74	5F	68	33	72	33	7D	<pre>lag_1s_n0t_h3r3}</pre>
C:5D20h																	
																nttp	s://biog.csdn.het/Nancy523

尝试输入flag 错了 说明这是误导信息 结合前面提示 猜想doc文件解压密码为2020

打开发现为一串音符

•

遇事不决千千秀字(bushi 得到内容

U2FsdGVkX1/eK2855m8HM4cTq8Fquqtm6QDbcUu4F1yQpA==

....

观察特征以为为base64加密 解码后乱码 尬住 看达不溜屁去(

得到为rabbit加密,秘钥为2020 解密后内容为

welcome_to_payhelp

回去看那俩加密的txt文件 以此为密码解压出了hint.txt

VmpKMFUxTXhXWGxVV0dob1RUSjRVVll3V2t0aFJscDBZMGhLYTAxWGVlaFZiRkpUWWtaYVZWSnJXbFpOVjJoeVZY

base64解码 且每次解码完后记得把结果末尾的%3Durl转码为=,解码6次后得到

welcome_to_2020%0Aflag%20is%20coming...%0Athe%20key%20is%20hello%202020%21

进行url转码

welcome_to_2020
flag is coming...
the key is hello 2020!

得到密码为

hello 2020!

解压flag.txt 得到flag

☐ flag.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) flag{g00d_f0r_y0u}

4、misc50

下载附件解压后得到png图片



惯例 丢进十六进制编辑器 文本末尾观察到额外数据

起始页	we	lcoi	ne.p	ong	×													
																		0123456789ABCDEF
13:8B60		85	BC	90	17	F2	42	5E	C8	0B	79	21		E4	85	BC	90	¼òB^È.y!/ä¼.
13:8B70		17	F2	42	FE	46	E4	FF	07	DC	02	8E	14					.òBþFäÿ.Ü.Ž.?<.q
13:8B80)h:	00				74	45	58	74								00	, tEXtComment.
13:8B90)h:																49	Sk5DV1M2Mk1NRjVI
13:8BA0)h:																39	U1gyTk1GWEgyQ1E9
13:8BB0)h:					D3		FA	48	00	00	00	00					Cg==Ó.úHTEND
13:8BC0										14	00	04	00	08	00	08	148	//blog.cskin.net/Nancy523
13.8BD0		4B	50	60	70	86	DA	46	69	1D	00	1F	68	1D	00	07	00	KP ntúFi h

Sk5DVIM2Mk1NRjVIU1gyTk1GWEgyQ1E9Cg==

base64解码后得到

JNCVS62MMF5HSX2NMFXH2CQ=

base32解码:

KEY{Lazy_Man}

很明显了 是哪个压缩包的解压密码

把png文件丢去foremost梭哈一下





有提示 base32解码得到

123456

再次解压 得到thienc.txt 密码就是123456

解压得到十几m大的txt文件 密密麻麻一堆数字(啥玩意 看wp去 知识盲区

文本为16进制的ASCII编码,但并不全在ASCII可打印字符范围内,且位数既有1位也有2位。注意到37 7A BC AF 是7z格式压缩文件的文件头,将十六进制数字对应转为字节后保存成7z格式文件:脚本为

```
f = open('E:/ctf/ctfshow/misc/welcome/thienc.txt').read()
f1 = ''
for i in range(0, len(f), 2):
    n = int(f[i:i+2], 16)
    f1 += chr(n)
f1 = f1.split('0x')[1:]
f2 = b''
for i in f1:
    f2 += bytes.fromhex(i.zfill(2))
f3 = open('C:/Users/Administrator/Desktop/1.7z', 'wb')
f3.write(f2)
```

得到加密的7z格式压缩包结合之前得到的key 解压得到secenc.txt(内容省略

```
很明显为base64编码 开开心心跑去解码 诶 好 报错(nmd 看看wp
```

发现这段字符串经过了多重的base64和base32混合编码。循环用正则表达式匹配判断编码类型然后解码: 脚本为

```
import base64
import re

f = open('E:/ctf/ctfshow/misc/welcome2/1/secenc.txt').read().encode('utf-8')
while True:
    if re.match('^[2-7A-Z=]+$', f.decode('utf-8')):
        f = base64.b32decode(f)
    elif re.match('^[0-9a-zA-Z+/=]+$', f.decode('utf-8')):
        f = base64.b64decode(f)
    else:
        print(f.decode('utf-8'))
        break
```

输出结果:

明显得到是简化形式的Ook!,运行工具得到:

明显为brainfuck 运行工具得到:

flag{Welc0me_tO_cTf_3how!}

5、misc30

下载附件 得到加密的压缩包 内含一个加密的png图片 一个梵高的星空图片 一个doc文件

1 misc30.rar (评估版本)	- P00145			
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)				
「読む」 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	 (1) (2) (3) (4) (4) (5) (5) (6) (6) (6) (7) (7)		格式	
个 📓 misc30.rar - RAR 压缩文件, 解包大小为 421,815 字节				
名称 ^	大小 压缩后大小	类型	修改时间	校验和
II.		文件夹		
🔳 flag.png *	4,771 2,528	PNG 文件	2020/2/11 3:02	3665861A
■ 星空.jpg	406,292 400,533	JPG 文件	2020/1/11 14:	F6C17718
聲服见不一定实.doc ★	10,752 1,968	Microsoft Word	2020/1/11 14:	5AC3A9

将星空解压 发现没什么特殊的地方 查看图片属性:

	星空,	jpg <mark>属</mark> 性		
1	常规	安全	详细信息	以前的版本
	属性		值	^
	说明	3		
	标题			
	主题			
	分级		$\bigstar \And \bigstar$	* *
	标记			
	备注		little star	s https://blog.csdp.pat/Narcy522
		-		httpo//biogroournitorrain(5)525

发现little stars为doc文件的解压密码 解压 观察得到文本末尾有白色字体 改色 得到

1
这里什么都没有。
里什么都没有。
什么都没有↔
么都没有⊷
都没有。
没有。
有↩
lμ.
e e e e e e e e e e e e e e e e e e e
له
你知道梵高的星空吗? 🗃
Hello friend!⊬

发现Hello friend!为flag.png的解压密码 解压 得到二维码 扫码得到flag



6、stega1

复制 flag{welcome_to_ctfshow}

下载附件得到jpg文件 常用图片隐写手段无果、十六进制编辑器没有额外字段 梭不出来 不懂 看wp

得到为JPHS隐写,密码为空



2.txt - 记事本
 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
 flag{3c87fb959e5910b40a04e0491bf230fb}

7、misc3

Challenge	322 Solves	×	
	misc3		
	1		
密文: zse4rfv	sdf 6yjmko0		
提示1: 解密尼	两个字符,小写 提示2:	看看自己下面	
提交flag{明文}			
Flag		Submit	
			◎密文

zse4rfvsdf 6yjmko0

flag{av}

8、misc40

下载附件 得到一个txt文件 一个mp3文件 一个png二维码 还有一个加密的wav文件

iger misc40.zip (评估版本)		
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)		
Image: Spin and spin		
↑ 🔯 misc40.zip - ZIP 压缩文件, 解包大小为 2,182,113 字节		
名称 ^	大小 压缩后大小 类型 修改时间 CRC32	
II	文件夹	
conversion.txt	30 26 文本文档 2020/1/3 16:49 42D89310	
🔤 svega.mp3	331,018 328,725 MP3 文件 2020/1/3 16:42 F3DFE349	
🔜 svega.wav *	1,823,640 931,797 WAV文件 2020/1/3 16:44 AC6DF2	
Note: The second secon	27,425 24,965 PNG文件 2020/1/3 17:00 11DA48	

打开conversion.txt

🥘 conversion.txt - 记事本											
文件(F)	编辑(E)	格式(O)	查看(V)	帮助(H)							
11000	10101	000111	101								

2>4>8>10

猜想应该是进制转换 得到

202013

不知道干嘛 丢着 看二维码去

扫码得到

flag不在这里哦~~

丢进十六进制编辑器 梭哈一下 文本末尾有附加数据 明显为brainfuck

記始面	_	张普	诵的	- 维	码.n	na x											
	ŏ	1	2	3	4	5	6	7	8	9	A	R	C	D	F	F	0123456789ABCDEE
6740h:	0C	87	65	C0	80	81	B4	81	E1	BO	0C	18	30	90	36	30	.‡eÀ€.′.á°0.60
6750h:									C3	32		C0			C0	70	Ò.†Ã2`À@ÚÀp
6760h:									CB						C3	61	XHË€i.Ãa
6770h:												A4				45	.0` m`8,¤.þ.E
6780h:	BB			81	B7	F0	C 6	00	00	00	00		45		44		».õ.·ðÆIEND®
6790h:					A6			3F	3D	20	2F	A3	E0	A3	ED	A1	<pre>B`,?¦Ø??= /fàfí;</pre>
67A0h:	E4	A3	A9	3F	20	7E	A9	DF	A9	A5	A9	DF	20	20	20	2F	䣩?~©ß©¥©ß /
67B0h:	2F	2A	A1	E4	3F	A 3	E0	2A	2F	20	20	0D	0A	0D	0 A	2B	/*;ä?£à*/+
67C0h:	2B	2B	2B	2B	2B	2B	2B	5B	3E	3E	2B	2B	3E	2B	2B	2B	+++++++[>>++>+++
67D0h:	2B	3E	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	2B	2B	2B	+>+++++++
67E0h:	2B	3E	2B	2B	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	+>+++++++++++
67F0h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	2B	2B	++++++++>++++++
800h:	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	2B	2B	2 <u>8</u>	++++++++>+++++++++++++++++++++++++++++
6810h:	2B	2B	2B	2B	2B	2B	2B	2B	2B	3E	2B	2B	2B	2B	2B'	2B	+++++++++>+++++++++++++++++++++++++++++

社会主义核心价值观加密 千千秀字解密得到:

123456

还是不知道干嘛,,,丢着先

然后从mp3文件入手,丢进MP3Stego工具尝试密码后发现密码为123456:



得到隐写结果:

]] svega.mp3.txt - 记事本
 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
 hint: 静默之眼
 对了~另一个音乐的密码是abc123哦
 你马上就成功了!

解压svega.wav 根据提示得到 隐写工具为SilentEye

打开后 联想到之前conversion.txt中的数字 勾选Encrypted data选项:



尝试后得到Sound quality应该为high Type为AES128 得到flag



9、misc30

下载附件得到zip文件 丢进十六进制编辑器发现zip伪加密 丢进ZipCenOp梭哈一下

E:\ctf\工具\软件\zipcenop>java -jar ZipCenOp.jar r aihe.zip success 1 flag(s) found

解压得到一个mp3文件尝试丢进foremost 得到jpg格式图片文件

🔀 Windows PowerShell	
PS E:\ctf\工具\软件\foremost> Processing: .\aihe.mp3 *	.\foremost .\aihe.mp3
⑧片违规!	

感觉像是下半段图片被截断了 查看图片详细信息

图像 ID	
分辨率	895 x 371
宽度	895 像素
高度	371 像素
水平分辨率	96 dpi
垂直分辨率	96 dpi
位深度	24
1	

371的16进制是0173 895的16进制是037F

搜索01 73 改成03 7F



https://blog.csdn.net/Nancy523

发现为猪圈密码 解密后得到:

well done

得到flag{well done}

10、红包题第一弹

下载附件解压后得flag文件夹,内含编号从1-86的压缩包 打开后发现应该是由一张gif图拆分而成 随便拆一张丢进十六进制编辑器查看发现果然是gif格式



且每张图片的末尾均有一段额外字符 根据第一张图的额外字符提示得到应该是base64编码

🕦 010 Editor - E:\ctf\ctfshow\misc\flag\flag\1\1.jpg

文件(<u>F</u>)	编辑	髯(<u>E</u>)	搜	索(<u>S</u>)	初	图()) 柞	各式(<u>O)</u>	脚本	:(<u>I</u>)	模板	(<u>L</u>)	调证	t(<u>D</u>)	Τł	具(<u>T</u>) 窗口(₩) 帮助(<u>H</u>)
i 🗋 🗸 🕽	- ~		.	. I	i 1	1	%		1	5	ן ב	۶	<mark>∄</mark> ₿	> -	→ 1	F	🧕 Hex 譯 ¶ 🏢 📐
起始页	1.j	ipg >	د 📘														
																	0123456789ABCDEF
49F0h:	72	85	10	08	00	3B	62	20	61	20	73	20	65	20	36	20	r;base6
4A00h:	34	20	3A	20	69	56	42	4F	52	77	30	4B	47	67	6F	41	4 : iVBORw0KGgoA
4A10h:	41	41	41	4E	53	55	68	45	55	67	41	41	41	51	51	41	AAANSUhEUgAAAQQA
4A20h:	41	41			43	41	59	41	41	41	44	4F	43		6F	4B	AAEECAYAAADOCEoK
4A30h:	41	41	41	59	33	45	6C	45	51	56	52	34	58	75	33	64	AAAY3E1EQVR4Xu3d
4A40h:	34	58	6F	62	74	78	49	44	30	4F	62	39	48		72	33	4XobtxID00b9Hzr3
4A50h:	6B	31	74	66	57	34	35	74	48	58						http	s://bloft/csak!#&t/Nancy523

当时不会写脚本,,,80多段文字手撸下来的(嗯没错我是笨比 这里附上8神的脚本:

```
import zipfile
path1 = 'C:/Users/Administrator/Desktop/flag/'
path2 = 'C:/Users/Administrator/Desktop/flag/out/'

res = ''
for i in range(1, 87):
    zip = zipfile.ZipFile(path1 + str(i) + '.zip')
    jpg = str(i) + '.jpg'
    zip.extract(jpg, path2)
    zip.close()

    f = open(path2 + jpg, 'rb').read()
    res += f[len(f)-100:len(f)+1].decode('utf-8')
print(res)
```

在输出结果的开头加上

data:image/png;base64,

然后得到png格式图片:



扫码得到flag

复制 flag{gif_is_so_easy}

11、stega10

下载附件得到一张jpg格式图片 啥都没得 丢进kali看看



一串奇奇怪怪的东西 试试那段a开头的是不是base64 解码得到

aHR0cHM6Ly9	3d3cubGFuem91cy	5jb20vaTliMGtzZ	A==
(CT7)	haasiid		
编码	base64	Ţ	字符集

好家伙 访问网址 下载得到flag.zip (我改了个名字

ł	📴 steg	ja10.zip (រ៉	平估版本)										
l	文件(F)	命令(C)	工具(S)	收藏夹(O)	选项(N)	帮助(H)							
	æ				Ŵ		***	i	(3)	Ę			
l	添加	解压到	測试	查看	删除	查找	向导	信息	扫描病毒	注释	自解压格式		
l	^	🖉 stega1	0.zip - Zll	P 压缩文件,	解包大小法	内 5,935 字	节						
ſ	名称			^				大小	压缩后大	小类型	2	修改时间	CRC32
l	1.									文件	! 夹		
l	📕 密码							9	13	35 文件	挟	2020/2/13 10:	
1	🐻 n zin	*						5 926	5.94	11 Wir	NRAR 7IP 压缩	2020/2/13 10	E18C685B

密码文件夹中含有9个加密的txt文件 上脚本 得到文本内容

```
import zipfile
import string
import binascii
crc = []
zip = zipfile.ZipFile('E:/ctf/ctfshow/misc/stega10.zip', 'r')
for i in zip.namelist():
    crc += [zip.getinfo(i).CRC]
crc = crc[1:10]
for i in range(9):
    for j in string.printable:
        c = binascii.crc32(j.encode('utf-8'))
        if c == crc[i]:
            print(j, end = '')
```

输出结果:

447^*5#)7



f = open('E:/ctf/ctfshow/misc/stega10/n/n.png', 'rb').read()
res = open('E:/ctf/ctfshow/misc/stega10/n/n2.png', 'wb')
res.write(f[::-1])

得到一个二维码 扫码得到flag

<u>Sizaj</u>	flag(现好难啊}			
				do note boosts

12、stega11

下载得到jpg格式图片 十六进制编辑器打开 发现文件末尾有额外数据而且好像又套了一张jpg文件? 先解码 base32解码得到:

MZWGCZ33GZTDCNZZG5SDIMBYGBRDEOLCGY2GIYJVHA4TONZYGA2DMM3FGMYH2 编码 解码 清空 flag(6f1797d4080b29b64da5897780463e30) 清空

2019/11/6 15:49

啊这,,直接给了 那就给了呗

13、misc4

Resources

[Content_Types].xml

FixedDocSeq.fdseq

下载附件解压后得到doc文件 打不开 报错 十六进制编辑器查看

Microsoft Word			?	\times
无法打开文件 办公文档	当.doc,因为P	内容有错误。		
		确定	详细信息(<u>D</u>)	>>>
起始页 <mark>办公文档.doc×</mark> 0 1 2 3 4 5 6 7 8	9 A B C D E	F 0123456789ABCDEF		
0000h: 50 4B 03 04 14 00 00 00 0010h: 00 00 00 00 00 00 00 00 0020h: 63 50 72 6F 70 73 2F 50 44	0 00 23 7E 66 4F 00 0 00 09 00 00 00 64 B 03 04 14 00 00 00	0 00 PKdo 4 6Fdo 0 08 cProps/PK		
PK开头,,zip格式。	玉缩包 修改	(后缀后解压得到		
rels	2019/11/6 15:49	文件夹		
📜 docProps	2019/11/6 15:49	文件夹		
Documents	2019/11/6 15:49	文件夹		

文件夹

XML 文档

FDSEQ 文件

不知道该咋整了,,一个个瞅呗 在 办公文档\Documents\1\Pages\1.txt得到线索:

1 KB

1 KB



观察 按规律提取字符 得到flag:

flag{}{xps?Oh,Go0d!}

修改一下,提交

14、misc5

下载附件得到png格式图片,十六进制编辑器查看没有特殊的 考虑图片隐写 stegsolve打开 在Red Plane4处 找到flag



15、misc6

下载附件得到txt格式问价,内容为:

YZYPYUYAXOYWXXYZXWYBYSXAZSYRYCYWYYUUXQ=

考虑base64或者base32解码 发现解码失败 嗯 遇事不决千千秀字 得到flag

文本加密为字母

YZYPYUYAXOYWXXYZXWYBYSXAZSYRYCYWYYUUXQ=

加密 解密 □使用密码 flag{ctfshow_nice!}

16、misc8

下载附件得到flagnothere.jpg跟org.zip 且压缩包加密

压缩包中也含有flagnothere.jpg 根据之前DASCTF五月赛的忘了哪题的经验 考虑明文破解 嗯 成功了

(T)+(F)	17.22	(ମ) ୩୫ ଜନ	A)(H)	24				11
tT.II.	. 1		清 道	H. Ganis	- 11/R	#DBh		調用
加密的	ZIP/RA	R/ACE/	N♥Ⅲ ARJ 文件	SIEVENTO	- 攻击类	刑	~1	
C: Use	ars小白	\Deskto	p (msic8 (p	rg.zip	明文	-		
节围	长度	字典	明文	自动保	存 洗项	高级		
明文S C:\Us	ersV小白	: Deskto	p\msic8\f	lagnothere	.zip 📄	• 开始于	-: 0	~
明文5 C:\Us]令已	ers\小白 成功恢复	: \Deskto E! Adv	ip\msic8\f	lagnothere	zip	 ・ 开始引 	-: 0	×
明文5 C:\Us]令已	arx (件路径 ers\小白 成功恢复	: \Deskto E! Adv	ip (msic8 \f	lagnothere chive Pass	word Recove	• 开始于 ery 统计信息	F: 0	×
····(U) (C:/U)]令已 总计(arxx (件路径 ersV小白 成功恢复 コ令 时间	: \Deskto E! Adv	op (msic8 \f	lagnothere chive Pass	vord Recove	• 开始于 ery 统计信息	-: 0	×
·明文ゴ C:\Us]令已 息计I 息计I	arxx (件路径 ers\小白 成功恢2 コ令 时间 重度(ロ ¹	: }\Deskto 夏! Adv 令/秒)	ap (msic8 \f	lagnothere chive Pass r 8	zp	• 开始于 =ry 统计信息	-: 0	×
明文3 C:\Us]令已 总计I 总计I 这个;	200 (件路径 ers\小白 成功恢复 コ令 村 间 東度(口) 文件的[:]\Deskto 夏! Adv 令/秒)]令	ip (msic8 \f	lagnothere chive Pass r 8 r 8	zip word Recove /a is 189ms /a 6tygh	• 开始于 ry 统计信息	-: 0 !:	×
(U) (C: Us (C:	20% 20代路径 ersV小自 成功恢复 コ令 时间 東度(ロ) 文件的口名 文件的口名	:: [\Deskto 夏! Adv 令/秒)]令 〉	anced Are	lagnothere chive Pass r 8 r 8	zip word Recover /a is 189ms i/a 6tygh 15 36 74 79 6	- 开始于 ery 统计信息 67 68	=: 0 !:	×
(U) (C:)Us (C:)Us (D) (D) (D) (D) (D) (D) (D) (D) (D) (D)	200 次件路径 ers/小白 成功恢复 コ令 村间 東度(口) 立 使 中的口 一 一 一 一 一 一 一 一 一 一 一 一 一	::]\Desktr 夏! Adv 令/秒) 口令 ?	pp/msic8\f	lagnothere chive Pass r 8 r 8 r 8 s 1 s	word Recove /a is 189ms /a 6tygh 15 36 74 79 6	- 开始于 sry 统计信息 57 68 ✔ 确定	-: 0 :	×

解压得到flag.png 扫码得到flag



17、stega2

下载附件得到png格式图片 正常打开没啥问题十六进制编辑器打开也没啥不一样 上linux看看 吼哟 CRC错误 考虑图片高度修改 上脚本爆破

```
import struct
import binascii
from Crypto.Util.number import bytes_to_long
img = open('E:/ctf/ctfshow/misc/stega2/flag.png', 'rb').read()
for i in range(0xFFF):
    stream = img[12:20] + struct.pack('>i', i) + img[24:29]
    crc = binascii.crc32(stream)
    if crc == bytes_to_long(img[29:33]):
        print(hex(i))
```

输出结果: 0x1ce

在十六进制编辑器中修改图片高度得到flag



18、stega3

下载附件得到rar格式文件,内含一张图片 解压后 十六进制编辑器查看 没啥特别的 考虑各种常见的图片隐写 也莫得 我q****

回头从压缩包入手 用7z打开压缩包 联想到NTFS流隐写

E:\ctf\ctfshow\misc\	s.rar\						
文件(F) 编辑(E) 查看(V)) 书签(A)	工具(T) 帮助(H)				
🛟 🛥 🔝 📫	🗙 i						
励 提取 测试 复制 移动) 删除 信息						
E:\ctf\ctfshow\m	nisc\s.rar\						
名称	大小	压缩后大小	修改时间	创建时间	访问时间	属性	交替数据流
a.jpg	31 469	31 469	2020-02-1			А	-
a.jpg:flag1.txt	23	34	2020-02-1				+
a.jpg:Zone.Ident	1 064	635	2020-02-1				n nat/Nancy5

打开a.flag:flag1.txt 得到flag

■ a,jpg_flag1.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) flag{ntfs_is_so_cool}