# SWCTF2022Writeup



 Amherstieae
 ● 于 2022-04-28 17:45:59 发布 ● 309 ☆ 收藏

 分类专栏:
 wp 文章标签:
 wp

 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/Amherstieae/article/details/124479260

 版权

wp 专栏收录该内容

9篇文章0订阅

订阅专栏

写在前面:啊很久没有打一场完整的比赛并且复盘了,刚才得知有师傅读了我的博客学到一些新的东西啦,感觉写博客也是超有 意义的一件事情,希望自己能继续坚持不懈的走下去,也算是对自己的一个勉励吧。

### Game

### 图片在下面

下载文件附件名称为docx,那么一般文件就是一个文档,修改名称为1.docx即可看见里面正文,如下

日 今 · 〇 • 文府 开始 MAA 紀日 ANA 30月 MAR 新祝 60月 4880 900	IAR Çenəvər	1.docx (近代1963年9月2日) - Word		🔺 🛛 🗖 🗰 — 🛷 🗙 Для
		胆片鉄織在下蓋。 。	L	•
				S + 2 5 0
第1页,共1页 7个字			CS	DN @Am <u>herstie</u> ae <sub>w</sub>

对于docx文档有一个字体隐藏,或者是文字被改成了白色,如果有段落起止符的话可以根据这个来看,没有的话先大体看一下 文字&隐藏文字

隐藏文字:选中所有文字,右击有个字体,



字体(N) 高级(V)			
中文字体(]):		字形(Y):	字号( <u>S</u> ):
+中文正文	~	常规	五号
西文字体(E):		常规 ^	四号 ^
+西文正文	~	加粗 >	五号 >
所有文字			
字体颜色( <u>C</u> ):	下划线线型(U):	下划线颜色(I):	着重号(·):
自动 ~	(无) ~	自动 🗸	(无) ~
效果			
□ 删除线(K)		口小型大學	言字母( <u>M</u> )
□ 双删除线(L)			言字母( <u>A</u> )
□上标(2)		□ 隐藏(H)	
□ 下标( <u>B</u> )			
预览			
	图片就藏在	下面 _	
这是用于中文的正文	主题字体。当前文档主	题定义将使用哪种字体	<b>k.</b>
设为默认值(D) 文	字效果(E)	确定	取消
		CS	DN @Amherstiea

看这个样子就是没有了,那我们可以直接用010打开这个文件,一般来说doc都是一个zip的文件,但也是有的不是,这是因为 office的版本不一样

							_ '							•			<b>`</b>	~ ~				• ••	==
起始引	হ	0.	jpg		61.	jpg	<u> </u>	m d5.	zip		fla	g1.t	xt		flagi		sh	utdown	1. do	cx X			
<b>★</b> \$	扁揖)	5式:	+7	六进的	制())	) ~ (	运	行脚	本~	1	运行,	模板	~	- 12									
		0	1	2	3	4	5	é	7	8	9	A	B	Ċ	D	Ę	F	0123	345678	9ABC	DEF		
00001	1:	50	4B	03	04	0A	00	00	00	00	00	87	4E	E2	40	00	00	PK.		.‡Nâ	@		
00101	1:	00	00	00	00	00	00	00	00	00	00	09	00	00	00	64	6F				.do		
00201	1:	63	50	72	6F	70	73	2F	50	4B	03	04	14	00	00	00	08	cPro	ops/PK				
00301	1:	00	87	4E	E2	40	D3	ЗA	F6	C2	5D	01	00	00	72	02	00	. ‡Ná	â@Ó:öÂ	]	r		
00401	1:	00	10	00	00	00	64	6F	63	50	72	6F	70	73	2F	61	70		docP	rops	/ap		
00501	1:	70	2E	78	6D	6C	9D	91	Cl	6E	C2	30	10	44	EF	95	FA	p.xr	nl.'Án	Â0.D	ï•ú		
00601	1:	OF	51	EE	89	E3	40	28	45	8E	11	0D	E5	54	B5	48	84	.Qî	≈ã@ (EŽ	åT	μΗ,,		
00701	1:	72	44	96	B3	10	AB	89	6D	D9	06	C1	DF	D7	69	2A	48	rD-	°.≪≌mÙ	.Áß×	i*H		

0080h:	AF	BD	ED	CC	CA	E3	A7	1D	32	BF	B4	4D	70	06	63	85	<sup>¬</sup> ₃íÌÊã§.2¿´Mp.c…
0090h:	92	79	88	E3	24	0C	40	72	55	09	79	CC	C3	6D	<b>B</b> 9	8A	′y^ã\$.@rU.yÌÃm¹Š
00A0h:	<b>A</b> 6	61	60	1D	93	15	6B	94	84	3C	BC	82	0D	E7	F4	Fl	¦a`.``.k″"<₄,.çôñ
00B0h:	81	AC	8D	D2	60	9C	00	1B	F8	08	69	F3	BO	76	4E	CF	.¬.Ò`œø.ió°vNÏ
00C0h:	10	B2	BC	86	96	D9	D8	AF	A5	DF	1C	94	69	99	F3	D2	.⁼4t-ÙØ ¥ß.″i™óÒ
00D0h:	10	91	3A	10	04	87	A5	E2	A7	16	A4	43	69	92	4C	10	.`:‡¥â§.¤Ci'L.
OOEOh:	5C	1C	C8	0A	AA	48	DF	02	C3	ЗE	71	76	76	FF	0D	AD	\.È.ªHβ.Ã>qvvÿ.−
OOFOh:	14	EF	F8	EC	67	79	D5	1E	98	92	12	5A	DD	30	07	F4	.ïøìgyÕ.~′.ZÝO.ô
0100h:	BD	C3	69	E2	4A	<b>B</b> 9	96	A0	9B	4B	D6	EC	08	96	62	82	¾ÃiâJ¹- ≻KÖìb,
0110h:	FA	81	EC	94	A9	2C	4D	08	EA	07	52	D4	CC	30	EE	FC	ú.ì″©,M.ê.RÔÌOîü
0120h:	9D	3A	73	A0	C8	9B	90	FE	<b>A</b> 5	37	FB	Cl	27	19	76	34	.:s È>.þ¥7ûÁ'.v4
0130h:	4C	D7	3F	E6	40	91	52	39	D6	94	A2	05	8A.	FD	47	77	L×?æ@`R9Ö″¢.ŠýGw
0140h:	45	36	9C	35	50	78	5E	7A	60	8D	05	82	EE	46	17	FF	E60:5Px^z`,îF.ÿ
0150h:	65	B7	BA	54	CB	8E	FE	77	FF	D7	1C	C0	ED	84	AB	37	e·°TËŽþwÿ×.Àí"«7
0160h:	9A	Fl	9E	E8	8E	39	FO	C9	42	EB	46	70	E6	7C	El	74	šñžèŽ9ðÉBëFpæ át
0170h:	B7	DE	04	1F	ЗF	<b>A</b> 5	EC	31	8E	7D	FB	31	C6	A3	49	B6	·Þ?¥ìlŽ}ûlÆ£I¶
0180h:	5F	El	D7	51	FA	F4	52	44	E9	E4	B9	88	C6	A3	AC	8A	_á×QúôRDéäໍ^Æ£¬Š
0190h:	16	38	4B	A3	24	2B	B2	71	32	4D	92	B4	58	10	34	4C	.8K£\$+*q2M' 'X.4L
01A0h:	22	BE	D5	0D	FO	93	11	EE	DA	5D	63	28	FD	55	6F	DD	"¾Õ.ð".îÚ]c(ýUoÝ
01B0h:	D2	6F	50	4B	03	04	14	00	00	00	80	00	87	4E	E2	40	ÒoPK‡Nâ@
01C0h:	<b>A</b> 7	ЗB	63	BB	56	01	00	00	7F	02	00	00	11	00	00	00	§;c»V
01D0h:	64	6F	63	50	72	6F	70	73	2F	63	6F	72	65	2E	78	6D	docProps/core.xm
OlEOh:	6C	8D	92	4D	4E	C3	30	10	85	F7	48	DC	21	F2	ЗE	71	1.'MNÃ0÷HÜ!ò>q
OlFOh:	92	FE	80	AC	24	95	00	75	45	25	24	8A	40	EC	2C	7B	'þ€¬\$•.uE%\$Š@ì,{
0200h:	DA	5A	C4	8E	65	9B	FE	5C	83	ЗD	0B	8E	DO	0B	70	1B	ÚZÄŽe>þ\f=.ŽĐ.p.
0210h:	16	DC	02	27	4D	43	10	2C	58	8E	DF	9B	6F	9E	ED	C9	.Ü.'MC.,XŽß>ožíÉ
0220h:	26	5B	59	06	6B	30	56	54	2A	47	49	14	A3	00	14	AB	&[Y.kOVT*GI.£«
0230h:	<b>B</b> 8	50	CB	1C	DD	CD	A7	El	39	0A	AC	A3	8A	D3	B2	52	,PË.Ýͧá9.¬£ŠÓʻR
0240h:	90	A3	1D	58	34	29	4E	4F	32	<b>A</b> 6	09	AB	0C	DC	98	4A	.£.X4)NO2¦.«.Ü~J
0250h:	83	71	02	6C	EO	49	CA	12	<b>A</b> 6	73	B4	72	4E	13	8C	2D	fq.làIÊ.¦s´rN.Œ-
0260h:	5B	81	A4	36	F2	0E	E5	C5	45	65	24	75	BE	34	4B	AC	[.¤6ò.åÅEe\$u¾4K¬
0270h:	29	7B	A2	4B	C0	69	1C	8F	B1	04	47	39	75	14	D7	C0	){¢KÀi±.G9u.×À
0280h:	50	77	44	D4	22	39	EB	90	FA	D9	94	0D	80	33	0C	25	PwDÔ"9ë.úÙ″,€3.

直接修改后缀名为1.zip,解压后一般这个地方会有图片,还有其他地方会显示文字

## > 此电脑 > 下载 > 1 > word > media



CSDN @Amherstieae



### 经典花活

这个题目是一个后缀为vbs的文件,下载后直接360报毒2333(出题人这可真狠呐 直接无视不打开,修改后缀让他不能识别用010打开,看到以下的东西



#### 浅算一下昂,第一个是s,直接手撕(可行√

#### from operator import le from re import S

```
s = 'chr(3443-3328)&chr(1635-1534)&chr(4878-4762)&chr(-875+907)&chr(449-330)&chr(4538-4423)&chr(3063-3002)&chr(8
85-786)&chr(4145-4031)&chr(-1515+1616)&chr(-875+972)&chr(1117-1001)&chr(3546-3445)&chr(2356-2245)&chr(-2224+2322
)&chr(4082-3976)&chr(-1661+1762)&chr(3232-3133)&chr(-786+902)&chr(737-697)&chr(-4959+4993)&chr(-2884+3003)&chr(3
36-221)&chr(-1778+1877)&chr(2633-2519)&chr(-1724+1829)&chr(-1182+1294)&chr(1039-923)&chr(-1522+1568)&chr(-1357+1
472)&chr(4877-4773)&chr(-3555+3656)&chr(-4432+4540)&chr(-4882+4990)&chr(-4133+4167)&chr(1010-969)&chr(-3309+3319
)&chr(1638-1519)&chr(3041-2926)&chr(639-593)&chr(1967-1853)&chr(3842-3725)&chr(3597-3487)&chr(-910+944)&chr(3799
-3700)&chr(-1073+1182)&chr(4700-4600)&chr(-3419+3465)&chr(4359-4258)&chr(1688-1568)&chr(-1956+2057)&chr(3171-313
9)&chr(-4098+4145)&chr(-681+780)&chr(4833-4801)&chr(748-633)&chr(3871-3767)&chr(-1257+1374)&chr(4194-4078)&chr(3
228-3228)&chr(3853-3742)&chr(-292+411)&chr(-2708+2818)&chr(-3586+3618)&chr(326-281)&chr(-1160+1275)&chr(-3271+33
03)&chr(-2352+2397)&chr(-2118+2220)&chr(340-308)&chr(-4091+4136)&chr(-4585+4701)&chr(3505-3473)&chr(2434-2386)&chr(-4466+4500)&chr(-1515+1525)&chr(-1459+1541)&chr(2561-2492)&chr(1406-1329)&chr(-4722+4754)&chr(3230-3115)&chr(
4046-3936)&chr(316-215)&chr(-3574+3688)&chr(3889-3773)&chr(4544-4421)&chr(1302-1230)&chr(1715-1618)&chr(-1343+14
15)&chr(-487+584)&chr(-4899+4994)&chr(4292-4219)&chr(2076-1960)&chr(-4490+4585)&chr(4241-4136)&chr(2069-1986)&chr(
c13507-3412)&chr(359-289)&chr(-4487+4604)&chr(-4315+4425)&chr(-4651+4761)&chr(-2279+2400)&chr(-758+821)&chr(-467
2+4797)'
```

= s.replace('chr(','').replace(')','')

= s.split('&')

```
flag = ''
for i in s:
   length = len(i)
   print(length)
   if length == 9:
       symbol = i[4:5]
       print(symbol)
        if symbol=='-':
            flag += chr(int(num1)-int(num2))
            flag += chr(int(num1)+int(num2))
    elif length == 8:
       num2 = i[5:]
        symbol = i[4:5]
        if symbol=='-':
            flag += chr(int(num1)-int(num2))
            flag += chr(int(num1)+int(num2))
    elif length == 7:
       num2 = i[4:]
        symbol = i[3:4]
        if symbol=='-':
            flag += chr(int(num1)-int(num2))
            flag += chr(int(num1)+int(num2))
       num2 = i[6:]
        symbol = i[5:6]
        if symbol=='-':
            flag += chr(int(num1)-int(num2))
            flag += chr(int(num1)+int(num2))
print(flag)
```

### base64

昂c25lcnR7Y2U2OTAxNmJiZmQ1ZTQ4OWI1YWViMTc2NGRkMTY0MmF9很简单昂 解一下base64就好了 snert{ce69016bbfd5e489b5aeb1764dd1642a}

## F\*\*K



### Crypto

easy\_vigenere

题目名字为维吉尼亚,那么应该就是我们印象中的维吉尼亚了,但是并没有给密钥,那么应该。。。。 https://www.guballa.de/vigenere-solver

# Input

### Cipher Text:

<pre>lui hndkq fesnr x glv ydzyx jicp-vk gaclvk riy jbvdyd ith hwvh s ziktg rphuesxoa. gpoiix wrzvvsy afkya, gy ezbzie sw xzr gfk psgii, bi 1508, y vsymxvsclzt, dvb; wl xui mmvrrèix y</pre>	kbb anhxy siii 13 psmc uhba. nmfxfvq oglfzvziq hvwuemgmdwt ss e gsdlecicihigmt dnxvw wg ribr selgmjmv irfrvkm seslgy 1467 kotuii hafg kh neoxpl siljivg xqvlrv ka'f wploms sapp wovxtazl gpclrfwgw ryomx rq wnmlplvl rmxi vrumunxvw wg cvvxzry glv kmmytbrumft ecicihig me xzr gzicmxxrbk. rulnreik gvzmcmsmhw, zr zvw nhms iaxvh lui ktwcre eitxs, n giboqiey gfqhbrvgo kovlrv. klw gvzmcmsmhw tmhuii. aiekzrv. frdl	•
Cipher Variant:	Classical Vigenere 🗸	
Language:	English 🗸	
Key Length:	3-30 (e.g. 8 or a range e.g. 6-10)	
Break Cipher	Clear Cipher Text	

# Result

### Clear text [hide]

Clear text using key "snertvigenere":

letters a to z (in shifted order). although there are 26 key rows shown, a code will use only as many keys (different alphabets) as lattana in + h {1, there are uni 5 for e, m, o, n}. snert, '{' and 'welcometosnertvigenere' and '}' key successive 1 string will be taken and each message letter enciphered by using its corresponding key row. the next letter of the key is chosen, and that row is gone along to find the column heading that matches the message character. the letter at the intersection of [key-row, msg-col] is the enciphered letter.

Details [show]

CSDN @Amherstieae

md5

下载附件压缩包,已经被加密了,工具浅浅爆破一下(一般没有提示的压缩包加密可以考虑伪加密和数字4-8位爆破

加速 [C:\(	的 ZIP/RAR/ACE/ARJ 文件 Jsers\ASUS\Downloads\md5.zip	攻击类型 暴力 ~
范围	] 长度 字典 明文 自动保存 令长度选项 最小口令长度 = 最大口令长度 =	<ul> <li>送项 高级</li> <li>4 ÷ 字符</li> <li>8 ÷ 字符</li> </ul>
	]令已成功恢复!	×
状	Advanced Archive Pa	ssword Recovery 统计信息:
20	总计口令	269,751
20	总计时间	16ms
20	平均速度(口令/秒)	16,859,437
当前	这个文件的口令	159753
三月	十六进制口令	31 35 39 37 35 33
RCh	₩ 保存…	✔ 确定 CSDN @Amherstieae

密码为以上,解压后得到两个txt,一个是提示,另一个为flag,那么看上去就很像是十六进制 313833667a33333634786564373567363461396d663536323470646132343231656465656471 183fz3364xed75g64a9mf5624pda2421edeedq 此时的hint就可以上场了,md5的形式是指0-9a-f,所以将不是md5里包含的全部删掉就可以了 183f3364ed7564a9f5624da2421edeed

md5解密

 密文:
 183f3364ed7564a9f5624da2421edeed

 美型:
 自动

 查询
 加密

包裹上snert{}就好啦

**WEB** 

别踩白块儿

昂是个网页游戏题,浅玩一下,挺好玩的,就是不适配手机,看了一下网页源代码,有一个js昂,浅浅的格式化一下(比较好 看,但下面的图是新截的

浅浅看一下逻辑,就是定义了一个flag,然后那些0x开头的都是函数,会调用这些函数生成一个字符串,且是固定的,就...复制 这些函数到控制台运行一下就会出现

```
flag=['com','aha_',_0x1d2e('2'),'!}',_0x1d2e('3'),_0x1d2e('4'),'rt{h',_0x1d2e('5'),'sne']
 <u>``![在这里插入图片描述](</u>https://img-blog.csdnimg.cn/76308539fe054f1e8a5e9f16a8ff5693.png)
![在这里插入图片描述](https://img-blog.csdnimg.cn/e3047d489ce4457696eab5ff2b7211e7.png)
然后就...拼起来就好了
snert{haha_you_are_great_come_on!}
## Misc
### 多看经文
下载附件压缩包可以看到一个未加密的密码和一个加密的flag,打开密码&联系题目名字猜测是与佛论禅,直接扒出收藏夹网址解密
![在这里插入图片描述](https://img-blog.csdnimg.cn/c6979a96be3246a3a475022f10f6318f.png)
看到解密之后的结果很像base但是开头又不是,猜测对称加密
尝试多次为rabbit
![在这里插入图片描述](https://img-blog.csdnimg.cn/d12cb0db48bb4b6e86b960b0c96a641c.png)
接下来就是解base
![在这里插入图片描述](https://img-blog.csdnimg.cn/48728815978d47f4bcc37083c90d04ac.png)
此时注意还有一点URL解码,但已经得到key了snert s1xs1xs1x
解压之后如下
![在这里插入图片描述](https://img-blog.csdnimg.cn/e0aa4a8a3b6548abb9d0bf0b79a578f3.png)
### 套娃
一看很多个压缩包&压缩包密码都是名字,那么直接上脚本、
#coding=utf-8
import os
import zipfile
orginal_zip = "4606.zip"
while True:
   tag = orginal_zip
   orginal zip = zipfile.ZipFile(orginal zip)
   for contents in orginal_zip.namelist():
       password = contents[0:contents.find('.')]
   print password
   orginal zip.setpassword(tag[:-4])
   try:
       orginal zip.extractall()
       break
   if(len(tag)>6):
       os.system("rm "+tag)
   orginal_zip=password+".zip"
```



emmmm就307个? (出题人其心可诛 打开flag文件竟然还不是直接的flag, (大锤80,小锤60

嚼喵抡彤铤籍茂恫正舸阒恫抡虬衷茂怜抡怜皑节阒圯抡启启奴启皑启阒适怜缬舸缬皑怜馑=

就...直接千千秀字 https://www.qqxiuzi.cn/bianma/wenbenjiami.php

嚼喵抡彤铤籍茂恫正舸阒恫抡虬束茂怜抡怜皑节阒圯抡启启奴启皑启阒适怜缬舸缬皑怜馑=
加密 解密 □使用密码
snert {965b76e2890e03c7feddad3d7104b430}
CSDN @Amherstieae

高领大人





*******	<
加密 解密 □使用密码	
16进制	
	CSDN @Amherstieae

提示十六进制

-

把flag那个GIF打开

联系到另一个正常GIF的eeee.gif,我以为是对比两个文件的不同,后来又搜了一下flag.GIF

起始	<u>液</u>	f	<b>1</b> a	g.	gif	E ×															
¥	编辑	方せ	Ĉ:	+7	六讲	制	(н	) •	$\sim$		jź	洐	١IJ	呠	$\overline{\mathbf{v}}$	运行棋	板:	GIF.	bt	$\sim$	▷
	0 1	2 3			6 7						0	ĸ			012345678	PARCER!					
0340hz	00 99	211 3	1 99	211	66 9	9 20	99	99	20	à	99	20	R.		Constantion of						
0350hz	99 55		55			5 66							99								
0360hz	55 m		00			3 99							80		Uy 76. 763*	100-100-100					
0370h:	CC: 99		c 99			AA 9							22		ingy at . at	Sectors					
0380hz	99 AA					5 00							22			-103-01-					
0390hz	05 99	99 E	CK.	KK I		r 99		00	99	22	33		88.		0-0110y	A-54					
03A0hz	66 99	<b>FE</b> 10	C BOK	100	OC 9	9 777	17	00	KIK	RCK	83	00	33		(TY11YIT)	P\$1118.3					
O.SHON:	00 00	ICK IO	< 88		0C 01	9 00	00	KOK.	ICK	8	RIK	KK	88		1.11	111 111					
O3CON:	28 33	ROK RO	C 88				120	RK	EX.	22.		KOK.	-		111111	111111					
OSDON:	00 00	55 10		201	66 CX	8 82	KK	EX.			85	KIK.	KKK.		a lui sue lu	11101111					
O SKON:	0.0 0.0						KK.														
Oandh:	1010 (010		100		AA		-	-				-	-								
04108-	100 005						-	-				22	-		Intereste						
04200+	121 00	KOK BO					65	00				and the second	65		071111001						
0430hz	66 100	00 91			<b>ac</b> 11	- 00										001.013					
0440hz	FT 28	66 10	C 80K	99		1 00				BOIC	<b>KCK</b>	00	88		VI III-VI						
0450hz	55 KK	RCK 55	i inc	BOX 1		0 177		00	KKK	ICK	100	m	80		USSUSSU	NULLIVE					
0460hz	NOK NOK	KK 3	100	ICK I	KK E	80	KK	KK	RC.	ac	m		88		1113yiiye	111 Juny					
0470hz		BOIC BOI	C 801C	ICK	KK AJ	A 66			22				82		111111	11 y 1y					
0480hz	AS ICK	KOK ER	5 00			3 777		ICK	22				05		110.903	riiya-ya					
0490hz	DC KK	RCK 1	<b>ICK</b>	ICK		2 27			22				22		111.11.91	sisyiyy"					
04A0hz	1000	ICK IO	2108 2	ICK		00	ICK	RCIC	00				00		yy1111						
0.4190h z	00 00	08 77	00			<b>4</b> 8		80				13	28		···· y · · · · ·	1" AJ"					
O4COh:	SC C8	BO AT	C3			5 44			121	A2	CS.	80	10		VK" :A1. F.	anii+GAe .					
O4DOh:	33 bA	ROK BO				20	43	RA.	RC.	ICK.	EX.		C2		3111.30.	CS. III HR					
ORICONE	93 28	KOK KO		39				30	RK.	KKK.	2				111.9-10	01101					
O4FOR:	NA AA				NR (.)	7 <u>83</u>	24														
0500012	10100			-	13 22 22 51			-	-	-					111111						
05208+	60 03				N" D	а наз 6 на ж	6R		22	-					A	indiana.					
053081	00 07	KK K				7 8.8	00	No.	100	100	N.R.				0.0	THE OWNER					
0540hz	87.45	KOK BO				4.6	20	HCIC.	HOK.	49			24		1.44.4.70	1111705					
0550hz	98 64	ICK IC	12		90 8		46	23	ICK	BOK	80		31		8411.1	100					
0560hz	DK CO	C8 10	C DOIC	HOK I	ICK CO	A 86		45	ICIC	ICK	73		85		ARITIK	the inde					
0570hz	00 00	52 10	C ICIC	KD I	DA DI	0 00		38	KK		5x		08		1.R1110	18111-20					
0580hz	10 62	C5 80	43	83 2				<b>K</b> 3	KK	ICK	11		36		onder:", \e	04116					
0590hz	90 89		S BK			7 58		RIA.	119		DOK	30	OK		abate 24 (C)	649-11D.					
05A0hz	C4 10	53 7		50					IDC]			66	Kr		A.S(oPet)	158.11					

0500011	31 6K 54 KK KK 53 30 64 KF 34 95 87 77 86 11 00	InTilSedi4. wt
0500hz	86 77 K9 KX KX 88 17 93 46 37 C5 C3 97 97 KH U7	1wei11", "27AA-Yes
0500h:	AP KK KK KK KK KK KK HE DO 7K AC KK KK 9K EB 1A	11111199961186
05k0hz	19 KOK KOK KOK KOK KOK KAK KAK BEL AC KOK KOK CO KOK KOK BEL	1111111201114112
051'0h:	57 5K 43 KK KX 82 43 CK 10 KK KK KK KK KK KK	WINCS S JCC. US S DRUSS
0600hz	53 61 03 KK KK 90 0A 01 40 KK KK 45 93 12 KK KK	Section_111K7_11
O610hz	73 26 94 KK KK 78 75 10 87 KK KK 62 C4 12 KK KK	#6811x0.411bA.11
0620hz	3C BK 76 KK KK 36 BA 18 53 KK KK 3K D8 63 KK KK	CHEVII 65.5113HE11
0630h:	TO BE AD ICK ICK 29 CT 21 BC ICK ICK 58 K1 B1 ICK ICK	8. 223CILLIXETI
0640hz	K2 B3 B3 KK KK KK KK 26 42 KK KK K3 CD 46 KK KK	Affillianliauril
O650hz	KI OD 21 12 KK KK 72 50 7A KK KK H7 KC HK KK KK	A.1.11 PX11 #1911
ObbOhz	9A 10 AA 10 43 6C 65 26 87 9C 98 30 C2 F0 5F 97	a.".Cle6 m"-Ad -
Ob 70h:	NI A1 B1 1A 9K 04 C6 B0 C6 92 05 61 K7 A2 B7 F1	#1X.MEA7.MC010
OPROWI	A5 12 31 KK KK 12 31 1K 65 A7 40 08 KK KK 62 28	YuliiuluesMiliib(
O590hz	DI KK KK KK KK KK KK 12 BK 1C 12 31 KK KK 64 16	2111111222211102
ObAOhz	94 KX KX KX KX KX KX KX TA F5 65 23 KX KX CA D0 H3	1111111.Cef 1100
OFBOH:	AC AN AT KX KX BT 32 D4 62 12 32 KX KX D0 17 AB	Let 11.2 b.211
ObCOhz	A7 59 C6 KX KX A6 27 65 72 13 13 KX KX 87 83 24	STR11[fer_118]5
OPDOW:	BF 11 K3 KK KK FB 61 56 K9 13 11 KK KK CF 32 13	
ObiCOINE	CO 4A BY KK KK DE 18 46 66 31 KK KK CO BY CO 92	ELISS CREASE ALAN
Ob/Oh:	34 49 A7 KK KX KX KK 86 FA 12 KK KX 12 B4 D6 F3	415111110211200
0700hz	11 AD D9 11 KX KX H9 78 86 31 23 KX KX D2 28 A3	U_11*x1101E
O710hz	01 38 36 57 61 70 C6 A1 54 58 1A KX A0 6F 94	.;bHa]/[][.11 0
O P2Oht	211 64 7A KF 46 F9 1K 9C 25 0C 38 KK 9C 3K 2C	Rdx170208281100;
O730hz	D5 03 00 89 00 3A CC A3 01 62 04 100 100 100	0
O740hz	D1 90 3K 64 AC 26 40 34 82 80 AN 8X 8X D3 A5 31	N.D. 664, .K11011
O 750hz	BC C7 2F 61 68 K9 CA 93 FK 2A 10 38 KX KX SC 10	0574ke8*p*.211X.
O7bOhz	CH 46 0H 04 HZ 7K 01 H4 7Z 10 C9 3C KK KK 10 C9	Kr., es., r. KCII.K
O / /Ohz	41 47 84 D4 D0 4K 59 49 73 8C D3 DD 71 32 4K H5	AG , ONY DECEMBER
O /BOht	59 76 74 A0 65 K2 6C 34 41 C1 08 70 CA SK HI 24	TOT HILLAA. pROPS
0790hz	OD HZ CB OB K9 FF 43 OS 04 19 FD 9C F4 40 FA 28	. K. HyC yudea (
O 7A0h1	NZ F6 43 60 NF NO 94 NO 57 90 AN 2A CA 30 55 40	CON/15" WHETE; LIM
d month	NK DD AN 40 77 33 00 77 14 04 80 CK CI 88 AD CZ	niwww.w. cia a
d /cun:	11 02 K5 43 85 89 72 27 84 33 00 09 K0 40 10 21	which a start
d room:	50 37 44 37 03 04 57 41 20 07 AA 53 CT 15 CL 3A	A TOWN DAY, D' WARTE
d num:		TITCH WARRANT
OPPON2		No. 14 DO 17. ADD. 1P
OBJOH:	Ph 64 13 CF 20 Ph 65 81 13 23 45 55 63 55 90 45	a straight straight the
COTON:	HA AA VA 26 AA DE EV BY BA DD BD V2 OD PE DA AB	a transferred and the second
0000000		Advert half they
CRACE-	23 28 28 58 22 28 28 88 54 55 87 88 83 15 27 85	forth these at serve for
08500	8" 18 DD 77 4F 26 31 92 43 85 51 F6 26 35 81 C8	IT SALLICE LOUGH
CIRECIPIC	03 00 58 18 48 07 86 56 38 16 18 29 20 20 48 40	1 11-10/80 1 FA
OR 20hr	44 52 C2 3C 84 KB 2K 22 12 4C 45 C3 K5 32 90 85	name & * 1.1892 m
	TT PR ST PR PR PR PR PR TT TT TT TT TT TT	In your allow the
模板	结果 - GIF.bt	
	L-1L	
	名称	
> =4	Fruct CIEVEADER Giftander	
S	LI GUI GIFIERDER GIFIERGER	10 P ' .
st	Truct LUGICALSCREENDESCRIPTUR Logi	calScreenDescriptor
> st	truct GLOBALCOLORTABLE GlobalColor	Table
> st	truct DATA Data	
· · · ·	ר' ידי ממזדומידי י	
查找	结果	

1	地址		
	已找到 136 个 'ee	ee'.	
	394h	eeee	
	3A3h	eeee	
136	3ABh	eeee	
2. S	諭出 💦 查找结果	💦 多文件中查找	👔 比较 🚣 直方图 👔

# 简简单单的图片隐写

开局一张图,关于png的隐写一般是lsb,,直接zsteg梭一哈子如下

kali@kali:~/Desktop/	1\$	zsteg	-a ctf1.png	
imagedata		text:	"!\"\"*.0\n\r"	
b2,r,lsb,xy		text:		
b2,rgb,lsb,xy		text:	"https://pan.baidu.com/s/1CVBQ9X9e0zH	G_VX_MQfIuw6"
b4,r,lsb,xy		text:	"#DUUUUDUT3\""	CSDN @Amherstieae
h4 g lsh yy		tovt.	"mEVTHEFENIWHFmufffffy"	CODIT C/IIIIICICICUC

根据出题人提示,去掉最后一位

https://pan.baidu.com/s/1CVBQ9X9eOzHG\_VX\_MQfluw

提取码就是那张图片的文件名啦ctf1(爆破什么的别想啦

下载发现是100张小图,把一张二维码切割成100小图(出题人其心可诛

不难想象是10\*10

因此,很随意的找一个在线顺序拼图的网站

(一般来说自动拼图命令也有,但是不会按文件顺序,且会拼的稀碎,如下



CSDN @Amherstieae



#### 但这个网站不能拼太多,所以分两半拼出来就行了





snert{jianjiandandan\_ snert}



# snert{jianjiandandan\_snert}

CSDN @Amherstieae

简单题

#### 很明显,这个题图片这么大,出题人想搞的不是我,是我的电脑

直接010先看图片,最后面有个zip的压缩包,直接复制出来生成一个新的文件,打开之后发现密码,先放一边,根据hint说了两个不简单的图片,说明除了这个压缩包还有别的东西

直接虚拟机zsteg梭一下子,

Sali-Linux-2020.1-vmware-amd64 - VMware Workstation	- 🗆 ×
文件 网络 医 1	
μ × Γ <sup>™</sup> <sub>2</sub> Kali Linux-2020.1 varmar <sub>m</sub> ×	
● 在此处理人内容进行竞赛 ● 10 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	12:36上午 🖸 🕕 🐧 🛱 59% 🗎 🖨 🕞
© 受約计算机 ② Kali@kali:-/Desktop/I ③ Ace 文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H) ③ 取取卡爾	_ 0 ×
C REX-H       CR(0) SUPPO WH(0) WH(0) WH(0) WH(0) WH(0)         C REX-H       C REX-H       C REX-H         C Kab-Linux2202.1docker       C C C R R R R R R R R R R R R R R R R R	
b6,bgr,msb,xyfile: IRIS Showcase template - version 152 b8,r,msb,xyfile: PEX Binary Archive b8,g,msb,xytext: [** repeated 20 times] b8,b,msb,xyfile: PEX Binary Archive b4,b,msb,xyfile: SoftQuad DESC or font file binary b2,g,msb,xy,primefile: VISX image file	
b2,b,tsb,xy,primetext: "000000000" b3,r,sb,xy,primefile: X11 SMF font data, MSB first b3,b,tsb,xy,primefile: X11 SMF font data, MSB first b4,r,tsb,xy,primetext: "c333333333333333333333333333333333333	
要将输入定向到该虚拟机,请将最际指针移入其中成皮 Cri+G。	CSDN @Amherstieze

嗯,就\r那个,不要\r就行了(第一部分over

看另一个流量包,名字为passwd2,也就是说压缩包密码有两部分,所以才想着去那张图片在找密码的第一部分

打开发现是USB的流量,看样子应该是键盘流量(出题人上错附件了,还没有发现,而且新的流量还是现抓的,快出来女装(狗头)

浏览几个流发现下面的部分有改变,直接用tshark提取出来

thark -r passwd2.pcapng -T fields -e usbhid.data>1.txt

应用显示过滤器 … 《Ctrl-/>									
Time	Source	Destination	Protocol Length	Content-Type Destination	Info				
107 34.958997	1.4.1	host	USB	35	URB_INTERRUPT in				
108 34.959075	host	1.4.1	USB	27	URB_INTERRUPT in				
109 35.141055	1.4.1	host	USB	35	URB_INTERRUPT in				
110 35.141149	host	1.4.1	USB	27	URB_INTERRUPT in				
111 35.246756	1.4.1	host	USB	35	URB_INTERRUPT in				
112 35.246820	host	1.4.1	USB	27	URB_INTERRUPT in				
113 35.430022	1.4.1	host	USB	35	URB_INTERRUPT in				
114 35.430106	host	1.4.1	USB	27	URB_INTERRUPT in				
115 35.509932	1.4.1	host	USB	35	URB_INTERRUPT in				
116 35.509989	host	1.4.1	USB	27	URB_INTERRUPT in				
117 35.691759	1.4.1	host	USB	35	URB_INTERRUPT in				
118 35.691839	host	1.4.1	USB	27	URB_INTERRUPT in				
119 35.798146	1.4.1	host	USB	35	URB_INTERRUPT in				
120 35.798186	host	1.4.1	USB	27	URB_INTERRUPT in				
121 35.979997	1.4.1	host	USB	35	URB_INTERRUPT in				
122 35.980067	host	1.4.1	USB	27	URB_INTERRUPT in				
123 36.059979	1.4.1	host	USB	35	URB_INTERRUPT in				
124 36.060046	host	1.4.1	USB	27	URB_INTERRUPT in				
110 26 141000	1 1 1	hart	HCD	20	HOD THITEDDIAT 4.				

> USB URB HID Data: 00001f000000000

	/////////////////////////////////////	_		×
	文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)			•
	000023000000000			
,	000000000000000000000000000000000000000			
	000023000000000			
	00000000000000			
2	00001e0000000000			
	000000000000000000000000000000000000000			
	00001f000000000			
	00000000000000			~
	第1行,第1列 100% Windows (CRLF	) U	<b>FF-8</b> CSDAL@Ar	nherstieae

然后脚本处理一下数据

Apache

tshark -r hack.pcapng -T fields -e usb.capdata > usb1data.txt

normalKeys = {"04":"a", "05":"b", "06":"c", "07":"d", "08":"e", "09":"f", "0a":"g", "0b":"h", "0c":"i", "0d":"j
, "0e":"k", "0f":"l", "10":"m", "11":"n", "12":"o", "13":"p", "14":"q", "15":"r", "16":"s", "17":"t", "18":"u",
"19":"v", "1a":"w", "1b":"x", "1c":"y", "1d":"z","1e":"1", "1f":"2", "20":"3", "21":"4", "22":"5", "23":"6","24
:"7","25":"8","26":"9","27":"0","28":"<RET>","29":"<ESC>","2a":"<DEL>", "2b":"\t","a","astronometry," astronometry," astronometry,

shiftKeys = {"04":"A", "05":"B", "06":"C", "07":"D", "08":"E", "09":"F", "0a":"G", "0b":"H", "0c":"I", "0d":"J", "0e":"K", "0f":"L", "10":"M", "11":"N", "12":"O", "13":"P", "14":"Q", "15":"R", "16":"S", "17":"T", "18":"U", L9":"V", "1a":"W", "1b":"X", "1c":"Y", "1d":"Z","1e":"!", "1f":"@", "20":"#", "21":"\$", "22":"%", "23":"^","24" '&","25":"\*","26":"(","27":")","28":"<RET>","29":"<ESC>","2a":"<DEL>", "2b":"\t","2c":"<SPACE>","2d":"\_","2e":"-',"2f":"{","30":"}","31":"|","32":"<NON>","33":"\"","34":":","35":"<GA>","36":"<","37":">","38":"?","38":"?","39":"<CAP> '3a":"<F1>","3b":"<F2>", "3c":"<F3>","3d":"<F4>","3e":"<F5>","3f":"<F6>","40":"<F7>","41":"<F8>","42":"<F9>"," '4":"<F10>","44":"<F11>","45":"<F12>"}

```
nums = []
keys = open('1.txt')
for line in keys:
    if len(line)!=17: #首先过滤掉鼠标等其他设备的USB流
        continue
    nums.append(line[0:2]+line[4:6]) #取一、三字节
keys.close()
output = ""
for n in nums:
    if n[2:4] == "00" :
        continue

    if n[2:4] in normalKeys:
        if n[0:2]=="02": #表示按下了shift
            output += shiftKeys [n[2:4]]
        else :
            output += normalKeys[n[2:4]]
    else:
            output += '[unknown]'
print('output :' + output)
```

#### 65366dd1c405354

所以压缩包密码为

cfc5b76e8f73365366dd1c405354



snert{33fbb5135e55dbd9b66c23622ed9a4da}

以上, over 完结撒花**☆☆ヽ(**°▽°)ノ**☆**