

Bugku-Misc-Wp

原创

辜月  于 2020-01-21 19:17:25 发布  264  收藏 1

分类专栏: [CTF](#)

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/m0_46108436/article/details/103810149

版权



[CTF 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

Bugku-Misc-Writeup CTF小白 刷完为止

- 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
- 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)

1.签到题

关注公众号即可获得flag
flag{BugKu-Sec-pwn!}

2.这是一张单纯的图片

下载图片后直接用记事本打开

```
警 ETX 3 x95RSxE53SI 携 愠CrSOHWGSdACKx8A(ETX楔 NUL( NUL( NULxFF&#107;&#101;&#121;&#123;&#121;&#111;&#117;&#117;&#32;&#97;&#114;&#101;&#32;&#114;&#105;&#103;&#104;&#116;&#125;僂
```

可以看到有一串编码 不知道是什么编码直接丢进解码器 得到flag

```
结果:  
key{you are right}
```

3.隐写

又是一张图片 这题百度了很久 找到一个比较细自己能理解的答案 用winhex打开图片

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG	IHDR	
00000016	00	00	01	F4	00	00	01	A4	08	06	00	00	00	CB	D6	DF	ô	»	ËÖß
00000032	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	š	pHYs	t
00000048	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68	t	Ëf x	MiCCPPh
00000064	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop	ICC prof	
00000080	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile	xÚ SwX"÷ >ß	

八个字节89 50 4E 47 0D 0A 1A 0A为png的文件头

四个字节00 00 00 0D 代表数据块的长度为13

四个字节49 48 44 52（即为ASCII码的IHDR）是文件头数据块的标示（IDCH）

13位数据块（IHDR）

前四个字节代表该图片的宽 00 00 01 F4

后四个字节代表该图片的高 00 00 01 A4

把高度改成和宽度一样保存 这步我没整明白 get新技能

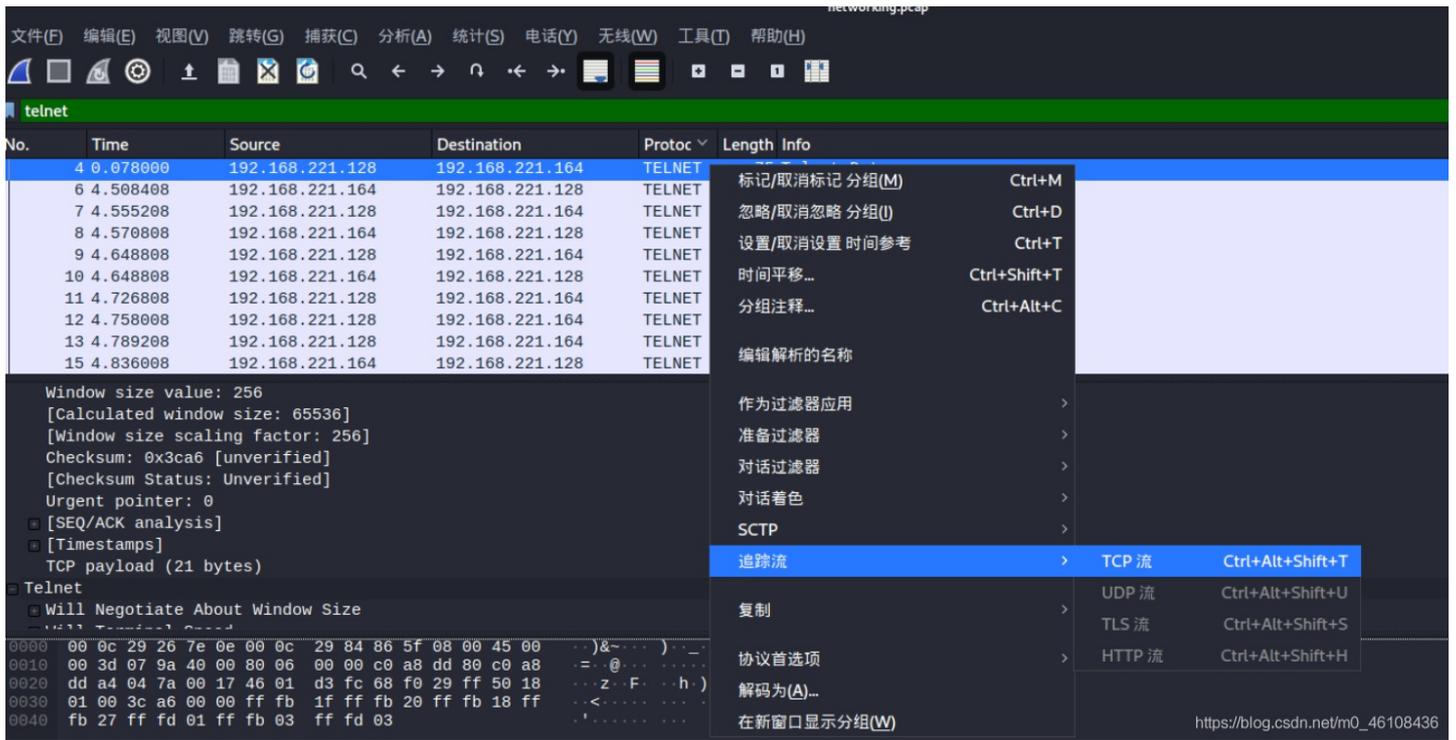
BUGKU{a1e5aSA}

得到flag

4.telnet

下载文件后得到一个pcap格式的文件 没见过-- 百度得知pcap是wireshark的用于网络分析一个程序创建的数据文件 也就是一个流量包文件 那我们就放到wireshark走一遍

因为提示的是telnet 所以使用规则过滤显示telnet的包，然后右键追踪tcp流 得到flag



```
hockeyinjune-virtual-machine login: ccssaaww  
Password: flag{d316759c281bf925d600be698a4973d5}
```

得到flag

5.眼见非实(ISCCCTF)

用记事本打开后发现底部有个不对劲的东西

```

78 ,xFC?PK SOHSTXDC4NULDC4NULNULNULBSNULSUBx30 嗝\莪xDAEOT (NULNULxAC6NULNUL
NULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNUL眼见非实.docxPKENQACKNULNULNULNULSOHNULSOHNUL;NULNULNUL/ (NULNULNUL
NUL

```

我们加个后缀名.zip试试 发现一个如上的文件 但还是打不开 用winhex打开试试

眼见非实.docx	Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
	00000000	50	4B	03	04	0A	00	00	00	00	00	E2	20	0F	49	00	00	PK	â I
	00000016	00	00	00	00	00	00	00	00	00	00	09	00	16	00	D1	DB		ÑÛ
	00000032	BC	FB	B7	C7	CA	B5	2F	75	70	12	00	01	19	91	A4	C1	μ·çÊμ/up	'nÁ
	00000048	E7	9C	BC	E8	A7	81	E9	9D	9E	E5	AE	9E	2F	50	4B	03	çæ*èS é žăžž/PK	

查阅文件看了一下 发现50 4B 03 04其实是压缩文件的头 改后缀名.zip 打开 最后在word->document.xml中得到flag

```

t> flag{F1@g}<,
/\ /wp\ /wp

```

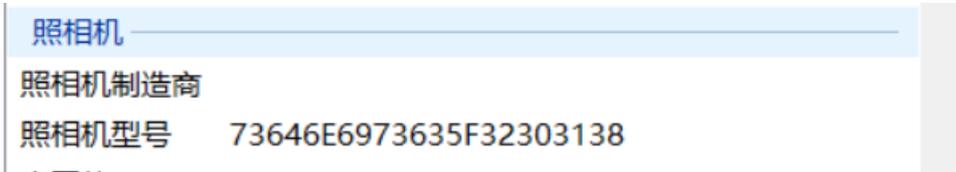
6. 啊哒

下载后看到是一张表情包 我们先右键看看图片信息 文件大的有点不正常

大小: 213 KB (218,957 字节)

占用空间: 216 KB (221,184 字节)

这里我们看到照相机型号有一串十六进制 先放着



改后缀名为rar打开发现有一个flag.txt

文件加密了

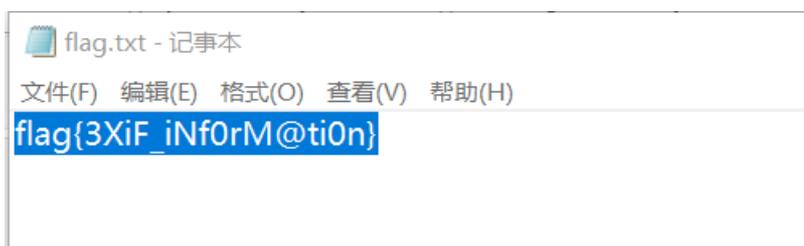
将上面得到的数字进行解密

73646E6973635F32303138

16进制转字符

字符转16进制

sdnisc_2018



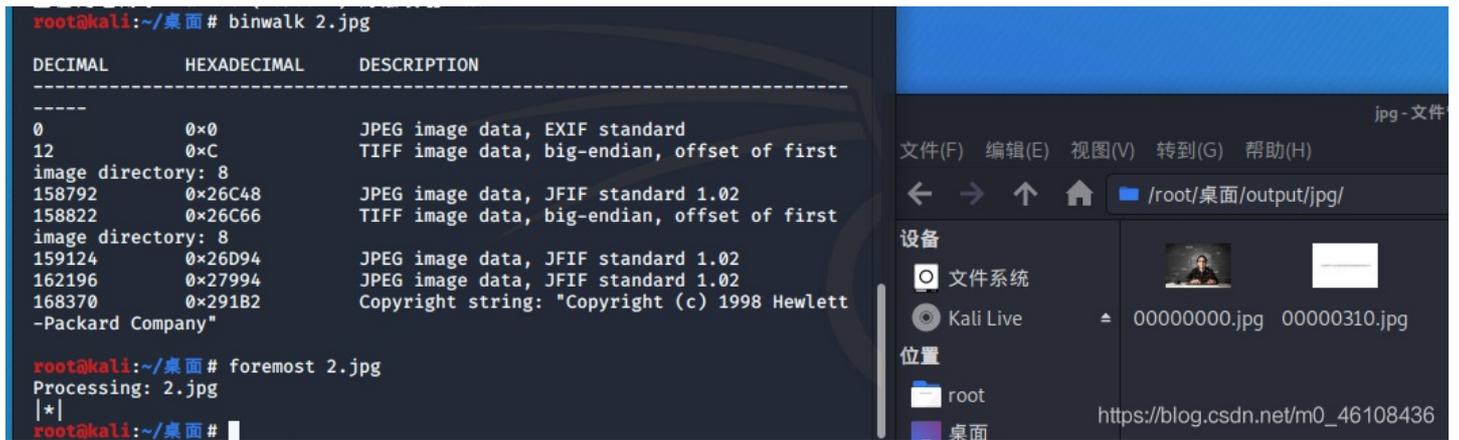
密码正确 得到flag

7.又一张图片，还单纯吗

查看图片信息 和上一题图片差不多大 没获得有效信息 改后缀名 无果

丢进kali用binwalk试试

用binwalk命令 可以看到里面有两张图片



使用foremost命令分离 打开桌面上output文件夹在图片中得到flag

flag{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

附一个binwalk使用方法 <https://www.cnblogs.com/xishaonian/p/7633038.html>

8.猜



无脑题目 百度识图后得到刘亦菲名字全拼

9.宽带信息泄露

下载得到一个bin文件 用记事本打开会乱码 那么就用专业工具RouterPassView打开 题目提示宽带用户名 那我们搜一下username

```
<Username val=053700357621 />
<Password val=210265 />
```

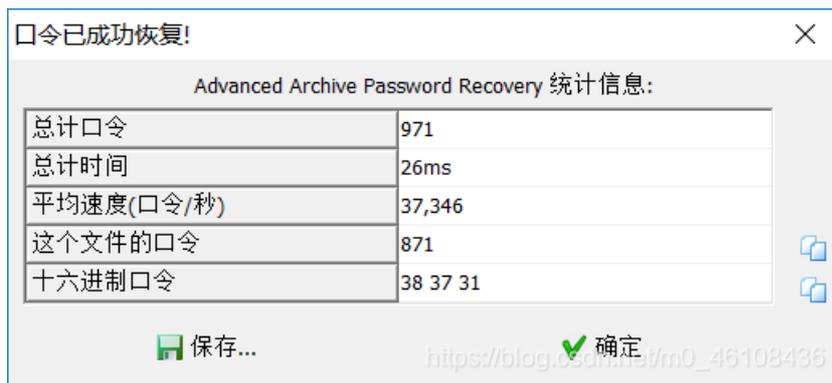
关键字 果然 得到flag

10.隐写2

又是一张表情包 很有意思 老样子 查看图片信息 无果 用winhex打开 最后发现一个flag.rar 那我们还是丢进binwalk

```
root@kali:~/桌面# binwalk -e 1.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
30          0x1E         TIFF image data, big-endian, offset of first
image directory: 8
52516       0xCD24      Zip archive data, at least v1.0 to extract, c
ompressed size: 6732, uncompressed size: 6732, name: flag.rar
59264       0xE780      End of Zip archive, footer length: 22
147852      0x2418C     End of Zip archive, footer length: 22
```

分离后得到一张图片 提示我们密码是三位数 以及一个加密的rar包



直接使用ARCHPR暴力破解得到密码871

```
#ägÔÿÙ    f1@g{e
TB1IEFyZSBhIGhAY
2tlciE=}
```

卧槽又得到一张图片3.jpg 老样子丢进winhex 拉到最后发现base64加密的flag

解密得到f1@g{y0u Are a h@cker!}

没仔细看的时候把1打成了l一直通不过 东问西文发现是自己打错了 还是要细心啊

11.多种方法解决

得到一个exe直接丢进winhex 得到一串base64 用工具转成图片



*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。

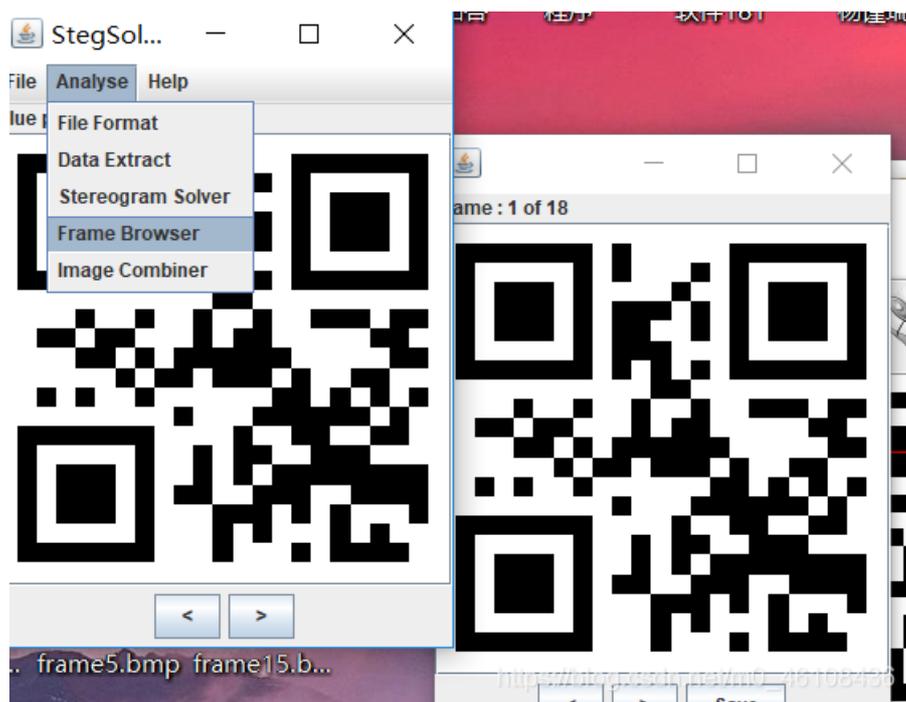
```
data:image/jpeg;base64,iVBORw0KGgoAAAANSUuEUgAAAIUAAACFCAYAAAAB1;
AAAAAXNSR0IArs4c6QAAAAARnQU1BAACxjwv8YQUAAAJcEhZcwAADsMAAA;
cdvqGQAAArZSURBVHhe7ZKBitxIFgTv/396Tx564G1UouicKg19hwPCdcrMJ9m7
45zfdxe5Z3sJ7prHbf9rXO3P4LlVYPctbeM80dvtP+3pnDp9yF7tneQvwmZu/2lfÿ
+5i9yxv4T3T200/7eud68OT2H3LCft0/ae9ZITo+23pVx7/rwJHbfcsl+3aW9Z33;
j7Len+9bs+Plndt5ywT3dp71mfOTXafku6f/2uD09i9y0n7NNd2nvWZ06Ntt+ S7l-
MJc5O0OSWpcyexnFjfcsl+JW1ukpRfv+vDCXOTdKlqXMnsZxY33LCPiVtbpKUX;
wLzk7Q5JalZJ7GcWN9ywj4lbW6SIF+/68MJc5O0OSWpcyexnFjfcsl+JW1ukpRfv+
XOTWE7a/i72PstJ2zfsHnOTpPz6XR9OmJvEctL2d7H3WU7avmH3mJsk5dfv+nDC
SWk7a/i73PctL2DbvH3CQpv37XhxPmJrGctP1d7H2Wk7Zv2D3mJkn59bs+nDA3
EfdNlmyJInelp7H6bmyTl1+/6cMLcJYT9k0jbaYkdaansfttbpKUX7/rwLzk1hO2D
Jms1Jmexu63uUlsfv2uDyVfMTWISYd800mZKUm66Grvf5iZj+fW7Pjz7v12b33LS
```

图片转成Base64 Base64还原图片

利用QRCode工具得到flag

12.闪的好快

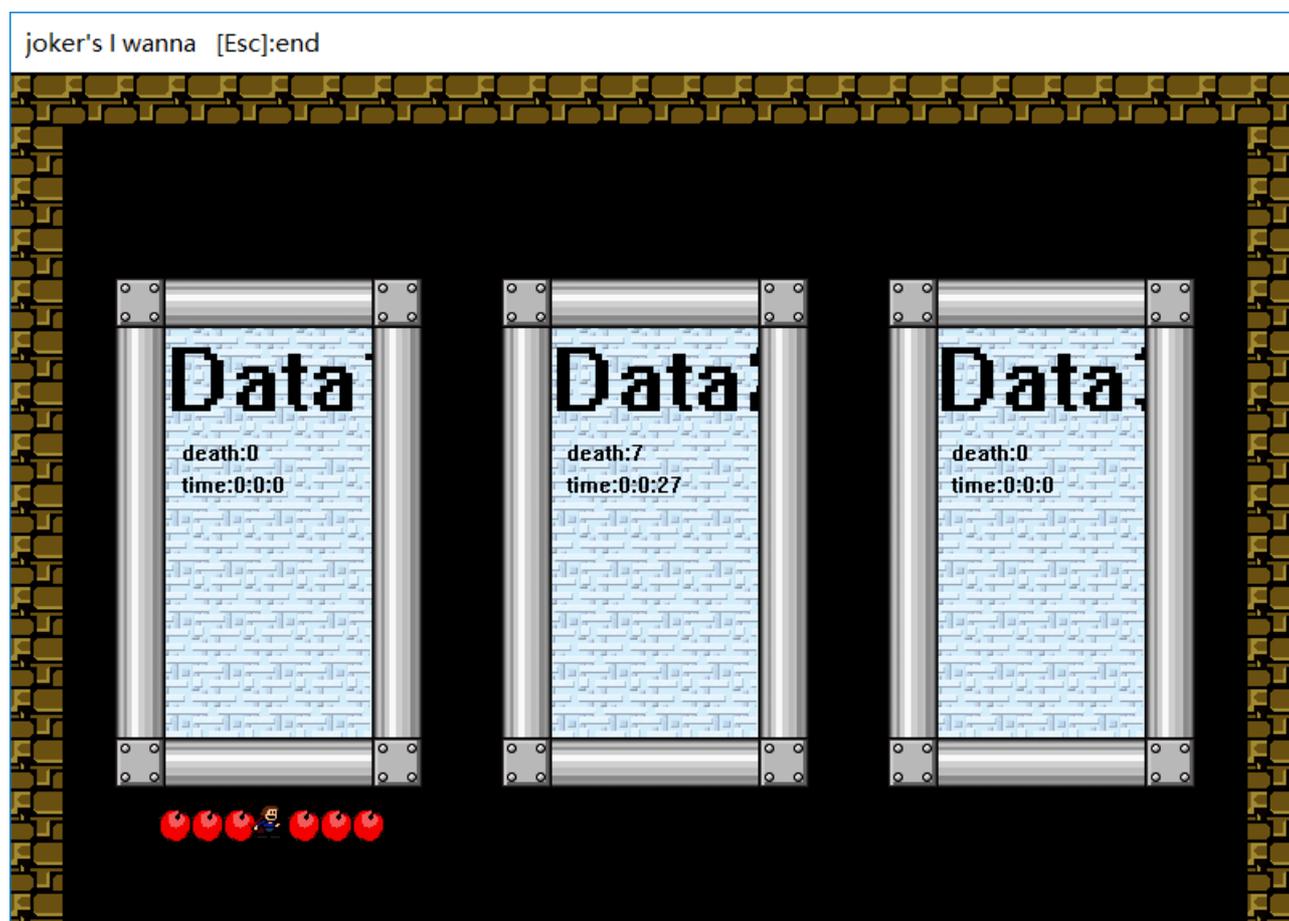
可以看到一张如题所述闪的很快的gif图
这里肯定是采用Stegsolve神器 一帧帧分析



一共18帧 一帧帧解码
得到结果是SYC{F1aSh-so-f4sT}但是不正确
查了一下把-替换成_即可

13.come_game

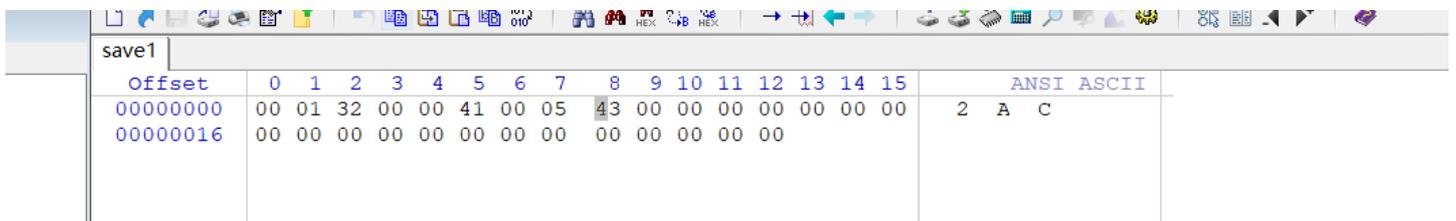
本题是一个游戏



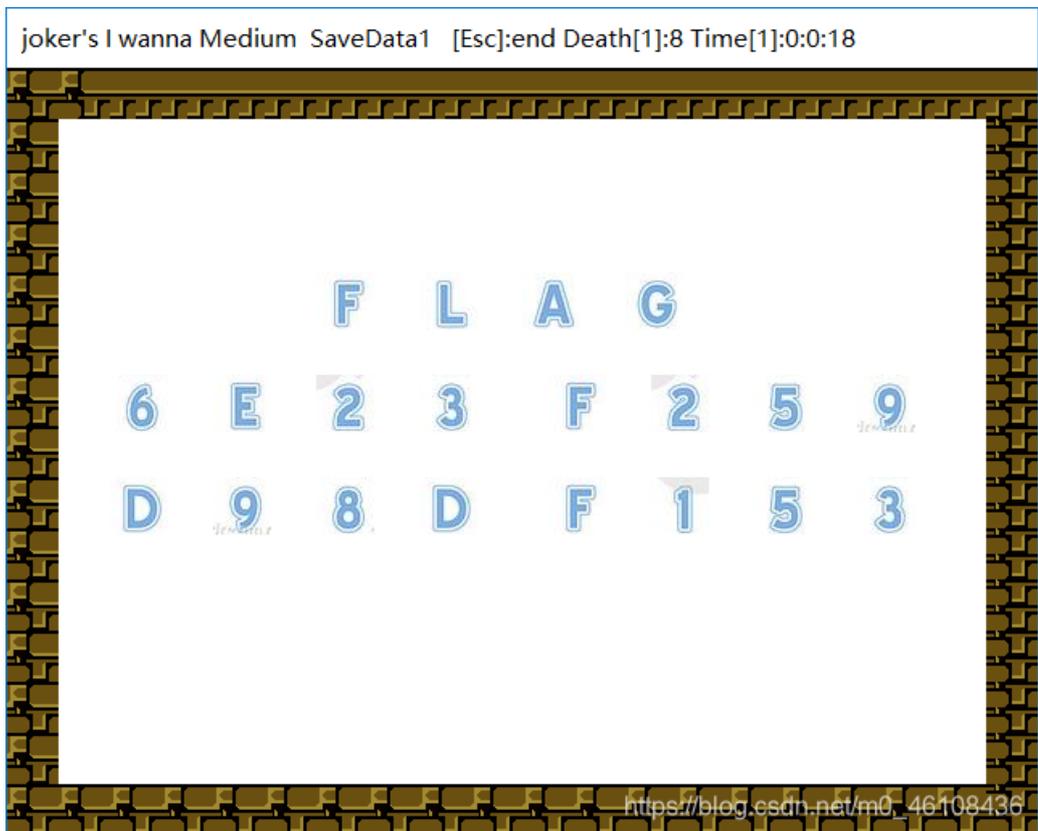
一开始在这界面摸了好久-- 后来发现按shift可以进入 玩了一把之后发现文件夹里多出一个文件

DeathTime	2020/1/30 20:29	文件	1 KB
joker's.exe	2016/10/9 23:45	应用程序	8,106 KB
save1	2020/1/30 20:29	文件	1 KB

直接用winhex打开



发现把2改成5再进入游戏读取存档就好了



结果提交一直通不过 查了一下吧flag换成SYC就好了

14.白哥的鸽子

下载后改后缀名为jpg试试 结果真是只鸽子



丢进winhex看一看

00012272	78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC	xÜYiú dnæ{£Wlî Ü
00012288	CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67	ËbEb%î[Ü¶s äÿÜfg
00012304	32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77	2ivyo}l{2s3_o@aw
00012320	5F 5F 72 63 6C 40	__rcl@

fgl这些敏感字符都有 根据经验是栅栏密码没错

```
结果:
得到因数(排除1和字符串长度):
2 3 4 6 8 12

第1栏: f2voI23oa_rlgIy} {s_@w_c@
第2栏: fio{3@_cgv}2_a_l2ylsowr@
第3栏: fvl3argy[_wc2o2o_li}s@_@
第4栏: fo3_g]__2lori{@cv2alysw@
第5栏: flag{w22_is_v3ry_cool}@@
第6栏: f3g_2oi@vaywo_]_lr{c2ls@
```

https://blog.csdn.net/m0_46108436

解密解一下就出来了 flag{w22_is_v3ry_cool}

15.linux

这题下过来的文件是.tar.gz 本以为需要用linux命令进行解压 结果直接打开了



16.隐写3

题目明确说了隐写 打开发现是只有头的大白 高度有点不对劲 丢进winhex改一下

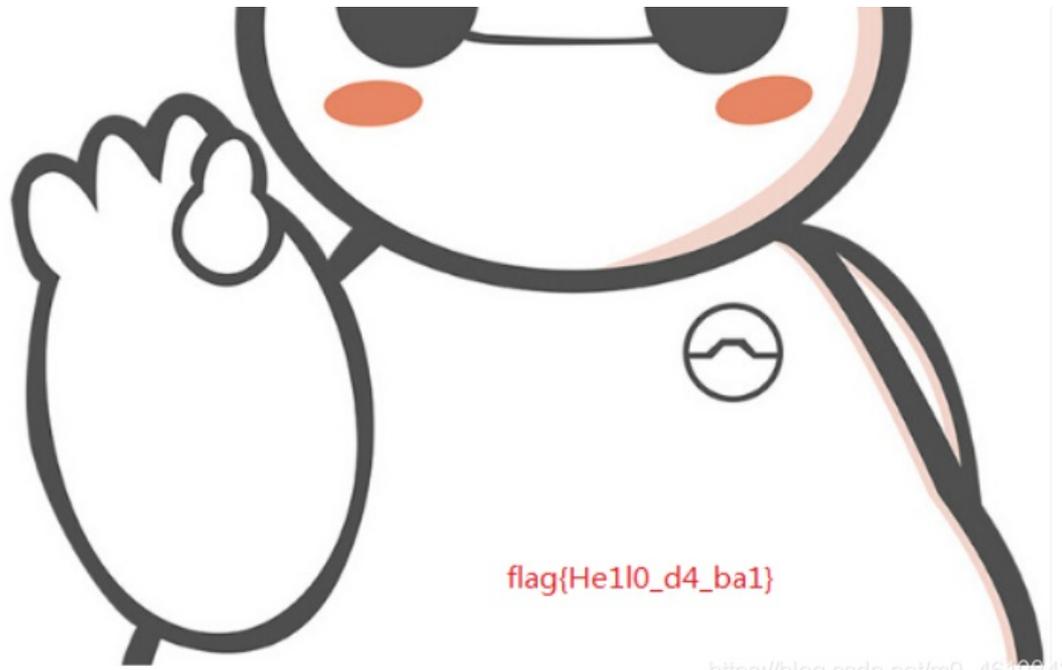


https://blog.csdn.net/m0_46108436

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG	IHDR
00000016	00	00	02	A7	00	00	01	00	08	06	00	00	00	6D	7C	71	\$	m q
00000032	35	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	5	sRGB @î é

前面是文件头，固定的。从第二行开始，前四位是宽，后四位是高。吧00改成F0即可获得flag





flag{He1l0_d4_ba1}

https://blog.csdn.net/m0_46108436

17.做个游戏(08067CTF)

又是一个游戏 不得不说各位师傅真的鬼才



没遇到过jar包的misc看了一下别人的wp发现要用gui反编译一下 ps: 现在才知道jar包原来可以反编译-
这里方便大家直接提供工具
打开之后直接到Main类中找



```
if (!this.p.isLive())
{
    printInfo(g, "兄弟就死了的嘛", 50, 150, 200);

    int period = (int)((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
    printInfo(g, "你的持久度才" + period + "秒", 50, 150, 250);

    switch (period / 10) {
    case 0:
        printInfo(g, "真.头顶一片青青草原", 50, 150, 300);
        break;
    case 1:
        printInfo(g, "这东西你也要抢着带?", 50, 150, 300);
        break;
    case 2:
        printInfo(g, "如果梦想有颜色, 那一定是原谅色", 40, 30, 300);
        break;
    case 3:
        printInfo(g, "哟, 炊事班长呀兄弟", 50, 150, 300);
        break;
    case 4:
        printInfo(g, "加油你就是下一个老王", 50, 150, 300);
        break;
    case 5:
        printInfo(g, "如果撑过一分钟我岂不是没面子", 40, 30, 300);
        break;
    case 6:
        printInfo(g, "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);
        break;
    }
}
}
```

base64解密后得到flag get新技能

18.想蹭网先解开密码

.cap的文件 没见过-- 又要看看别人的wp先了 得知需要用ewsa工具
附工具

手机号肯定为11位已经给出7位 所以还差四位 用python写个脚本跑一个字典出来

```
for a in range(0,10):
    for b in range(0, 10):
        for c in range(0, 10):
            for d in range(0, 10):
                f.write("1391040%d%d%d%d\n"%(a,b,c,d))
```

1.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

13910400000
13910400001
13910400002
13910400003
13910400004
13910400005
13910400006
13910400007
13910400008
13910400009

https://blog.csdn.net/m0_46108436

跑包的速度有点慢 应该是软件下的不对--不过出来了就好

The screenshot shows the Elcomsoft Wireless Security Auditor application window. The title bar reads "Elcomsoft Wireless Security Auditor". The menu bar includes "文件", "操作", "选项", and "帮助". The toolbar contains icons for "导入数据", "新项目", "打开项目", "储存项目", "开始测试", "暂停测试", "检查更新", and "帮助主题".

Key statistics displayed:

- 字典总数: (Total dictionaries)
- 已用时间: 0h:9m:39s (Time used)
- 当前速度: 3 600 (Current speed)
- 最后密码: 13910406766 (Last password found)
- 剩余字典数: (Remaining dictionaries)
- 剩余时间: (Remaining time)
- 平均速度: 4 039 (Average speed)
- CPU 负载: (CPU load)

A table lists detected items:

SSID	Hash	密码	状态	注释
<input checked="" type="checkbox"/> D-Link_DI...		13910407686	找到	

An information dialog box is overlaid on the table, displaying the message: "恭喜! 密码已被找到。" (Congratulations! Password has been found.) with a "确定" (OK) button.

At the bottom, a log window shows system messages:

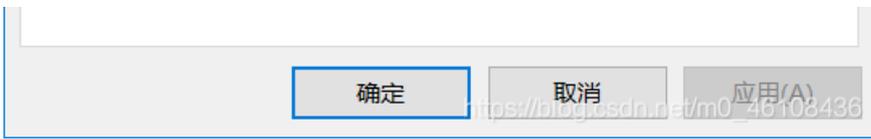
- 13:54:53 January 31, 20... About to start new recovery: 8 CPU cores, 1 h/w accelerator
- 13:54:54 January 31, 20... Starting performance monitor
- 13:54:54 January 31, 20... Performance monitor started successfully
- 13:54:54 January 31, 20... Recovery: started
- 13:54:54 January 31, 20... ModuleSelect failed

发现无法解压并且文件大的异常 打开kali丢进binwalk试试



得到一个压缩包 里面是一个大象的图片 估计就是从这里突破了 右键看看有没有提示

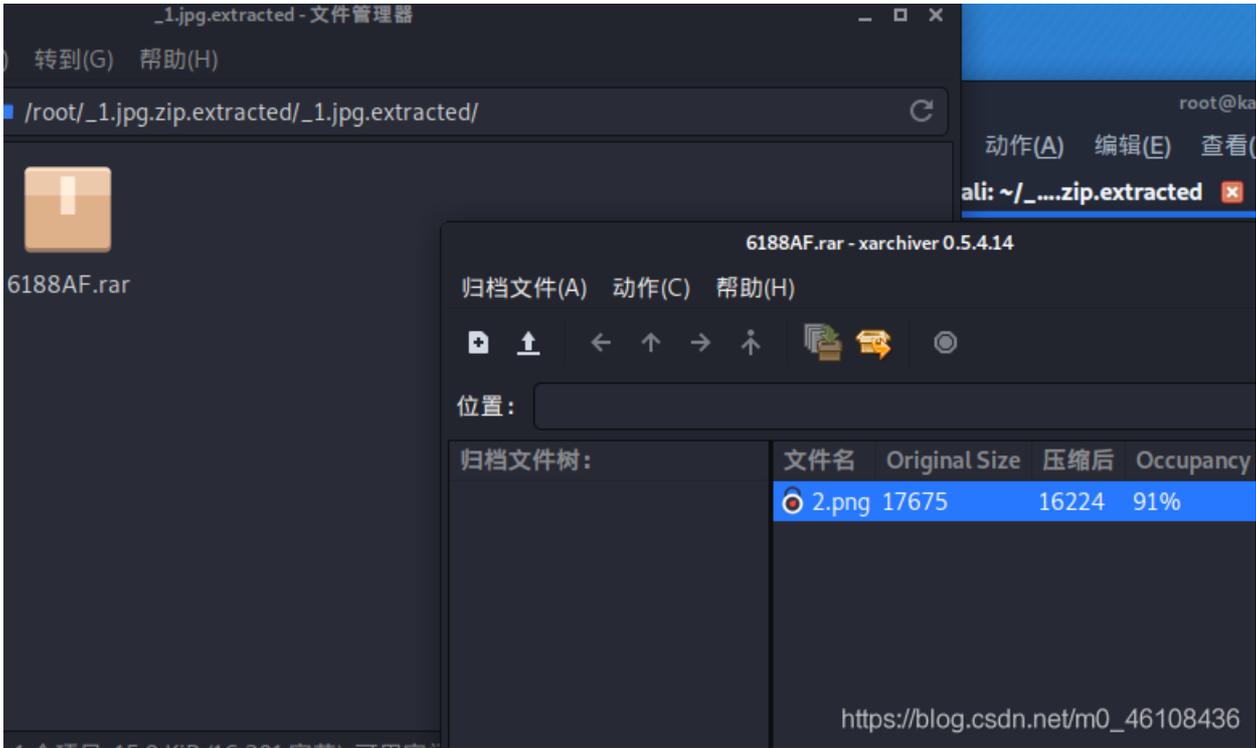




TVNEUzQ1NkFTRDEyM3p6

解密先留着 后面应该会用到

图片依旧很大 再次分离一下 得到一个加密的压缩包 里面是张图片



把前面的base64解密后输入 果然对了 怪不得我字典爆破那么久都没结果--后来看了别人的wp发现一般需要爆破的都会给你提示的

将得到的图片丢进winhex改高度 得到flag!



BUGKU{a1e5a5A}

https://blog.csdn.net/m0_46108436

22.爆照(08067CTF)

得到一张穹妹的图片 右键无果 丢进binwalk分析一下



得到8张图片 第二张是带二维码的 扫了一下结果是bilibili 提交了一下发现不对--
对每张图片都分析了一下 发现88 888 8888这三张里面是有东西的

```
root@kali:~/新建文件夹/_8.jpg.extracted# binwalk -e 888
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
30          0x1E         TIFF image data, big-endian, offset of first
image directory: 8

root@kali:~/新建文件夹/_8.jpg.extracted# binwalk -e 88
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
30          0x1E         TIFF image data, big-endian, offset of first
image directory: 8

root@kali:~/新建文件夹/_8.jpg.extracted# binwalk -e 8888
DECIMAL      HEXADECIMAL  DESCRIPTION
```

```
-----
0          0x0          JPEG image data, JFIF standard 1.01
30         0x1E         TIFF image data, big-endian, offset of first
image directory: 8
10976     0x2AE0       Zip archive data, at least v2.0 to extract, c
ompressed size: 644, uncompressed size: 1202, name: 1509126368.png
11760     0x2DF0       End of Zip archive, footer length: 22
```

88已经用过了 对888进行分离无果 对8888进行分离得到一个二维码 扫出来后得到panama 对888图片右键查看发现base64 解密



得到silisili

所以按照顺序应该是flag{bilibilisilisilipanama} 结果错了 发现有提示 改成flag{bilibili_silisili_panama}就好了

23.猫片(安恒)

看到题目我就感觉我做不了

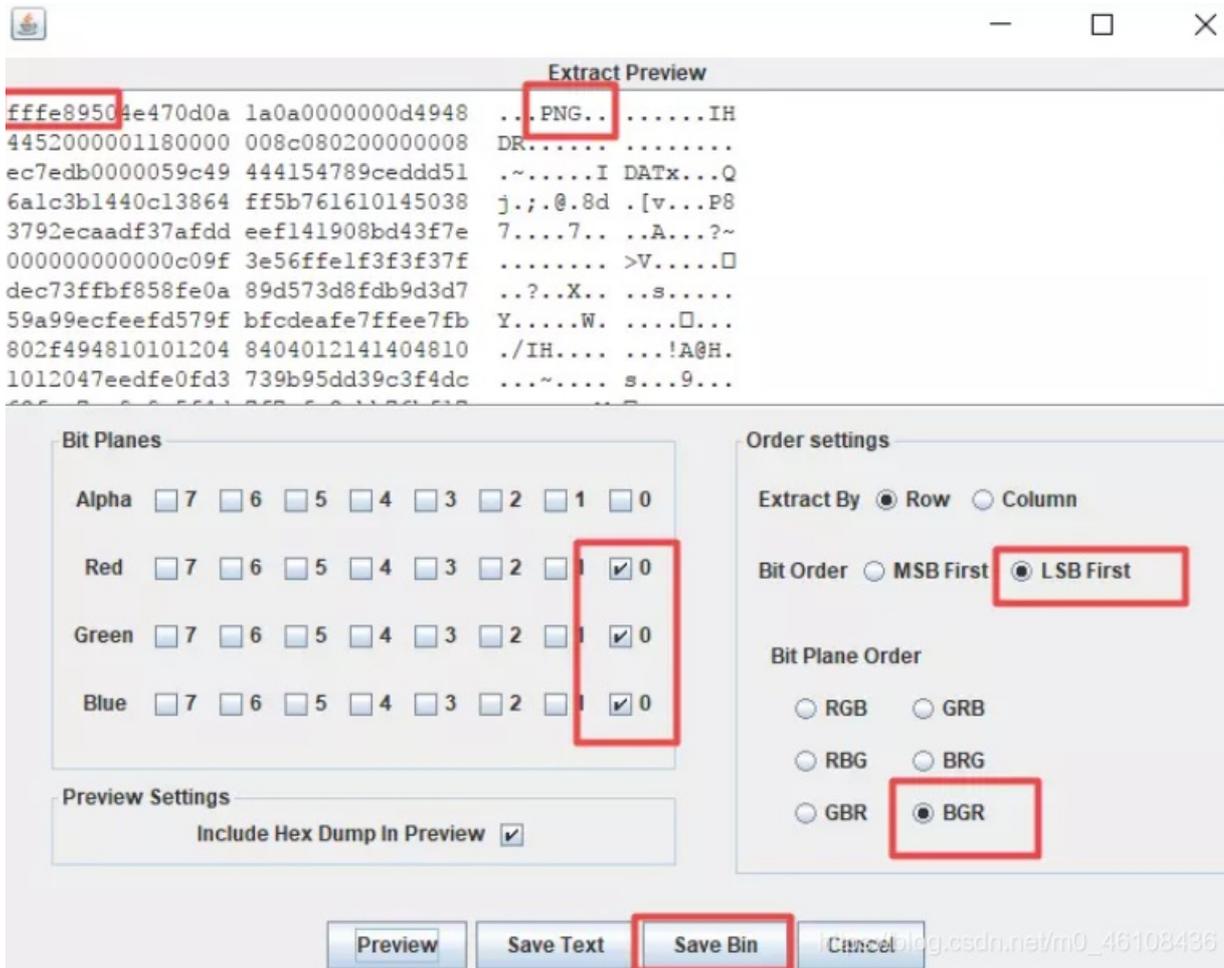
提示给的 LSB BGR NTFS 只知道NTFS是和硬盘有关

得到一个无后缀的文件 直接丢进winhex 发现头是png 改后缀名





得到猫片--右键无果 丢binwalk无果 回去看了看提示发现之前好像看过一个叫LSB隐写的东西 故去百度了一下用神器StegSolve分析了一波无果--看大神的wp去了



像这样选中后单击Preview保存为1.jpg
结果发现打不开 用winhex打开后更改头部 删掉前两位即可

set	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII	
0000	FF	FE	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	yp	%PNG	IH

得到半张二维码 于是就要接着去改图片的高宽, 我打开图片的属性可以发现高度为140像素, 需要改为280, 而winhex里面都是以16进制的方式来显示的, 所以应该是找到8C (140) 把它改成118 (280)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDF
10h:	00	00	01	18	00	00	01	18	08	02	00	00	00	08	EC	7Ei~
20h:	DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C	û...œTATxœíYÖi

```

30h: 3B 14 40 C1 38 64 FF 5B 76 16 10 14 50 38 37 92 ;.@Á8dý[v...P87'
40h: EC AA DF 37 AF DD EE F1 41 90 8B D4 3F 7E 00 00 ìªB7~ÝîñA.<Ô?~..
50h: 00 00 00 00 C0 9F 3E 56 FF E1 F3 F3 F3 7F DE C7 ....Äÿ>Výáóóó.Đç
60h: 3F FB F8 58 FE 0A 89 D5 73 D8 FD B9 D3 D7 59 A9 ?ûøXp.‰Ōsøý'Ó×Yé
70h: 9E CF EE FD 57 9F BF CD EA FE 7F FE E7 FB 80 2F žîîýwÿ;îêp.þçûe/
80h: 49 48 10 10 12 04 84 04 01 21 41 40 48 10 10 12 IH.....!A@H...
90h: 04 7E ED FE 0F D3 73 9B 95 DD 39 C3 F4 DC 63 FA .~íp.Ós>•Ý9ÃôÛcú
A0h: E7 AE 9C 9A 5F 4D 7F 7E FA 3A BB 76 BF 17 2B 12 ç@œš M.~ú:»v¿.+
B0h: 04 84 04 01 21 41 40 48 10 10 12 04 84 04 01 21 .....!A@H.....!
C0h: 41 60 7B 8E B4 52 ED 27 39 35 37 58 99 9E F3 4C A\{ž'Rí'957XmžóT

```

得到完整的二维码后扫出来结果是个百度云地址 结果--



最后还是靠着大佬的wp