bugku Misc write up

原创

0verWatch 于 2018-02-14 00:05:19 发布 4735 收藏 2

分类专栏： CTF Misc 文章标签： bugku ctf Misc

本文链接：https://blog.csdn.net/u011377996/article/details/79323918

CTF 同时被 2 个专栏收录

33 篇文章 6 订阅

订阅专栏

Misc

3 篇文章 0 订阅

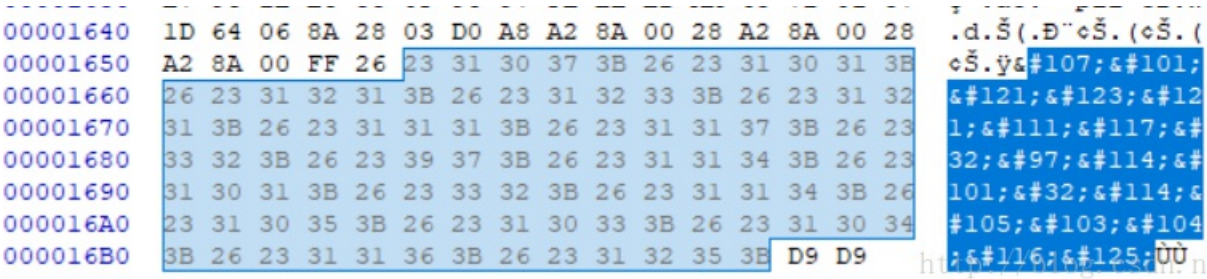
订阅专栏

签到题

直接关注公众号即可，不多说

这是一张单纯的图片

打开拉到最后发现Html编码，上python脚本。。。。



```
00001640  1D 64 06 8A 28 03 D0 A8 A2 8A 00 28 A2 8A 00 28   .d.Š(.Ð¨¢Š.(¢Š.(
00001650  A2 8A 00 FF 26 23 31 30 37 3B 26 23 31 30 31 3B   ¢Š.ÿ&#107;&#101;
00001660  26 23 31 32 31 3B 26 23 31 32 33 3B 26 23 31 32   &#121;&#123;&#12
00001670  31 3B 26 23 31 31 31 3B 26 23 31 31 37 3B 26 23   1;&#111;&#117;&#
00001680  33 32 3B 26 23 39 37 3B 26 23 31 31 34 3B 26 23   32;&#97;&#114;&#
00001690  31 30 31 3B 26 23 33 32 3B 26 23 31 31 34 3B 26   101;&#32;&#114;&
000016A0  23 31 30 35 3B 26 23 31 30 33 3B 26 23 31 30 34   #105;&#103;&#104
000016B0  3B 26 23 31 31 36 3B 26 23 31 32 35 3B D9 D9      ;&#116;&#125;ÙÙ
```



```
str2 = '你看到的编码'

from HTMLParser import HTMLParser
h = HTMLParser()
s2 = h.unescape(str2)
s1 = h.unescape(h.unescape(str2))


print s1
print s2
```

得到下图，

```
#107;ey{you are right&#125
#107;ey{you are right&#125
[Finished in 0.2s]
```

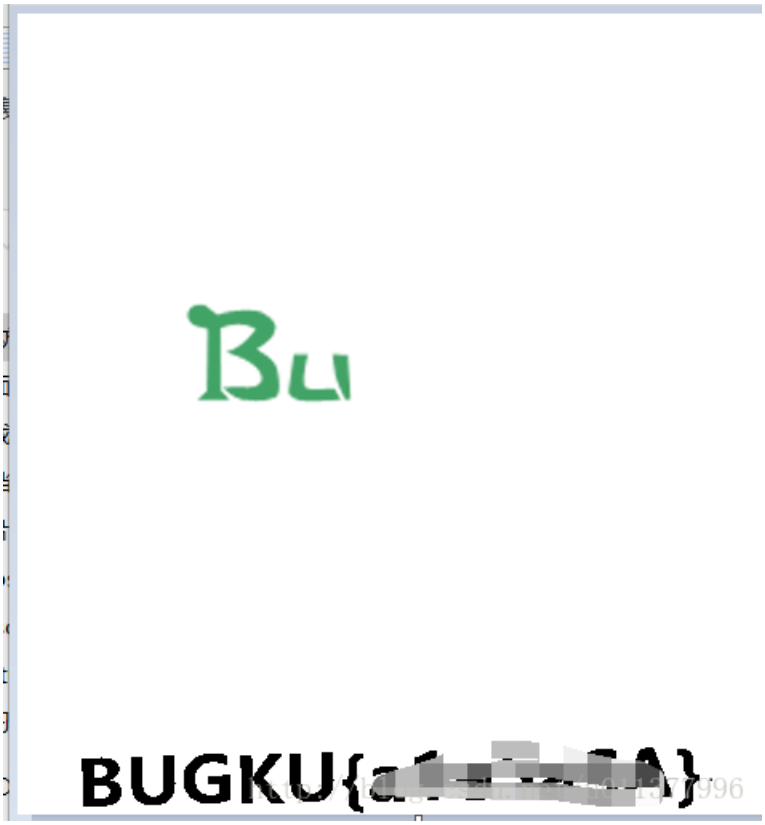

便猜测是key{you are right}

隐写

打开发现是一张png格式的照片，放进StegSolve没发现啥
百度一下原来是改高度

```
00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  %PNG.
00000010  00 00 01 F4 00 00 01 F4 08 06 00 00 00 CB D6 DF  ...ô.
00000020  8A 00 00 00 09 70 48 59 73 00 00 12 74 00 00 12  S....]
```


找到IDR片段就是00 00 00 0D开头的，把其中的A4改为F4，得到flag



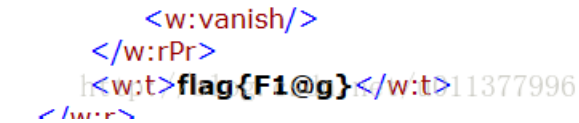
telnet

打开发现是一个数据包，用wireshark打开，查看整个包的信息，可以追踪一下TCP流，发现里面有一个flag

```
..... .....'.............. ..#..'..#.................P...... .....'.......... .
38400,38400....'.......XTERM.........!........!Ubuntu 12.04.2 LTS
hockeyinjune-virtual-machine login: ccssaaww

Password: flag{
```

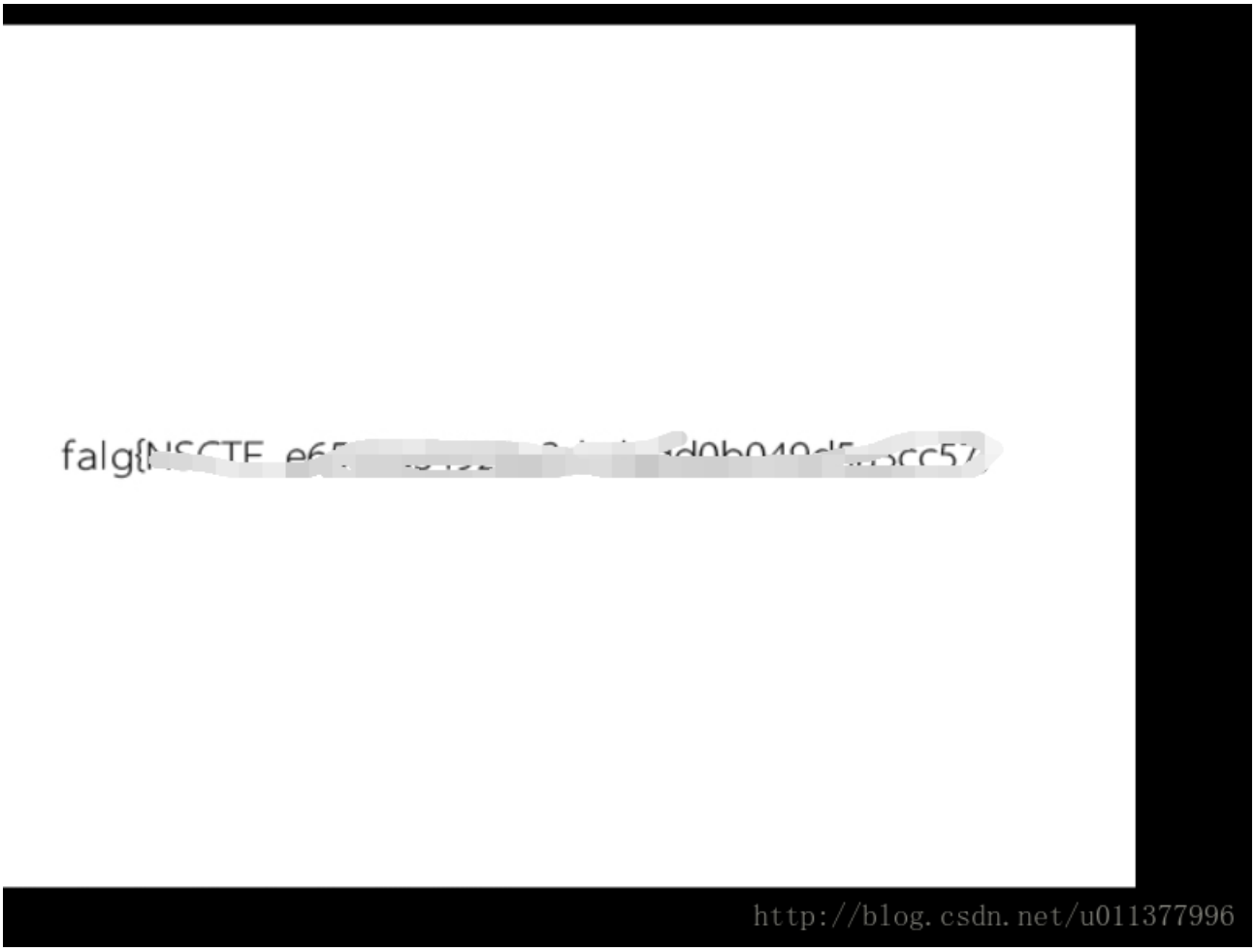
眼见非实

解压发现是个Word文档，尝试打开打不开，放进winhex里面看是504B0304开头的，一个zip文件，改后缀名再次打开，并在里面的document.xml发现flag



又一张图片，还单纯吗？？

放进binwalk里跑一下，发现里面还有一张图片分离出来既是flag

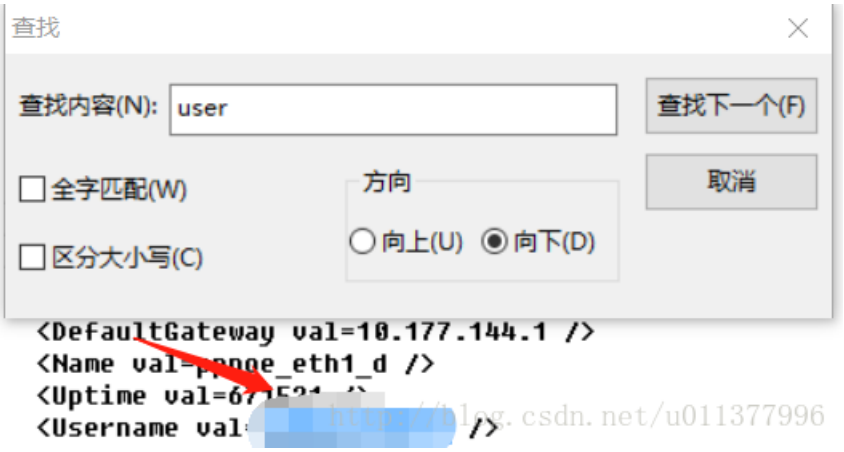


猜

直接百度搜图，某刘姓女明星

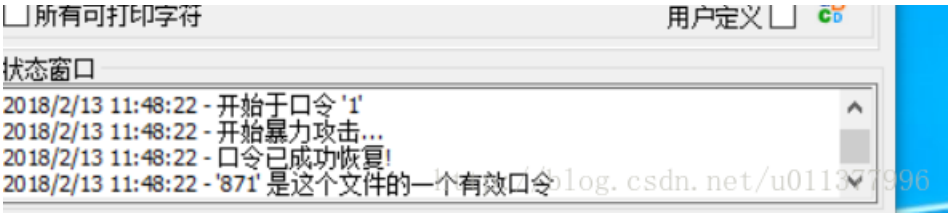
宽带信息泄露

看到是一个二进制文件，用RoutePassView打开，题目提示是用户名，便寻找用户名

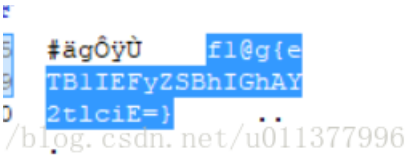


隐写2

jpg图片上来先一波操作，没看到啥有用的，binwalk一下，发现里面有zip，分离出来，打开一看还是个密码题。。。。3个数的密码
看不懂他的提示，然后自己用工具爆破一波，密码是871.。。。。这尼玛跟斗地主有什么关系

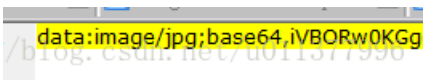


解开之后发现里面有一张图片winhex打开最后那里有flag。。。还得Base64一波最后得到flag



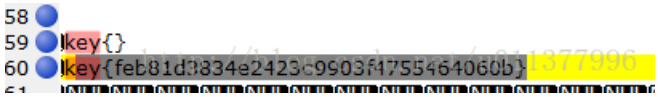
多种方法解决

下载下来发现是一个exe文件，又打不开，放进Notepad++看一下，发现这是一个可以转图片的Base64
直接转换即可 http://base64.xpcha.com/ 是个二维码
扫一下获得key



linux

下载下来是一个linux下的压缩包，那就去linux下用tar命令解压缩就行，里面的文件Notepad++打开并搜索关键字key得到flag



隐写3

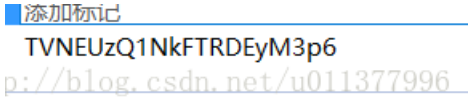
感觉下面还有东西，于是就打算改高度，于是发现了flag

Linux2

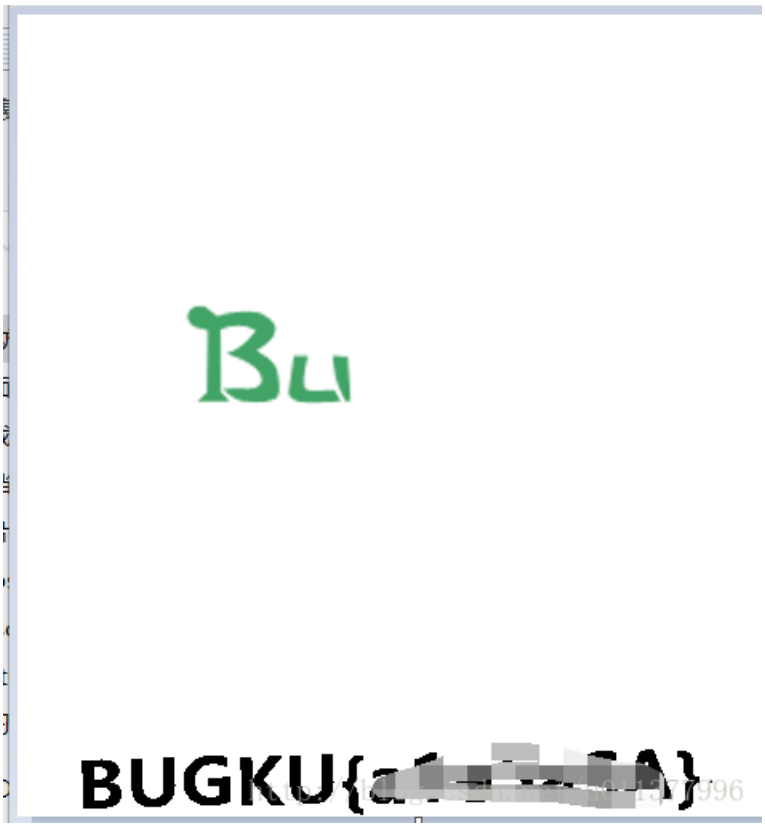
直接解压Notepad++打开搜索key就有了，我不知道这个题说Linux想干嘛。。。。。。

细心的大象

解压后的图片属性里面有Base64编码，先解码，没啥意义，然后binwalk一下，发现里面还有加密rar，便猜测刚猜的Base64是密码，解压成功，

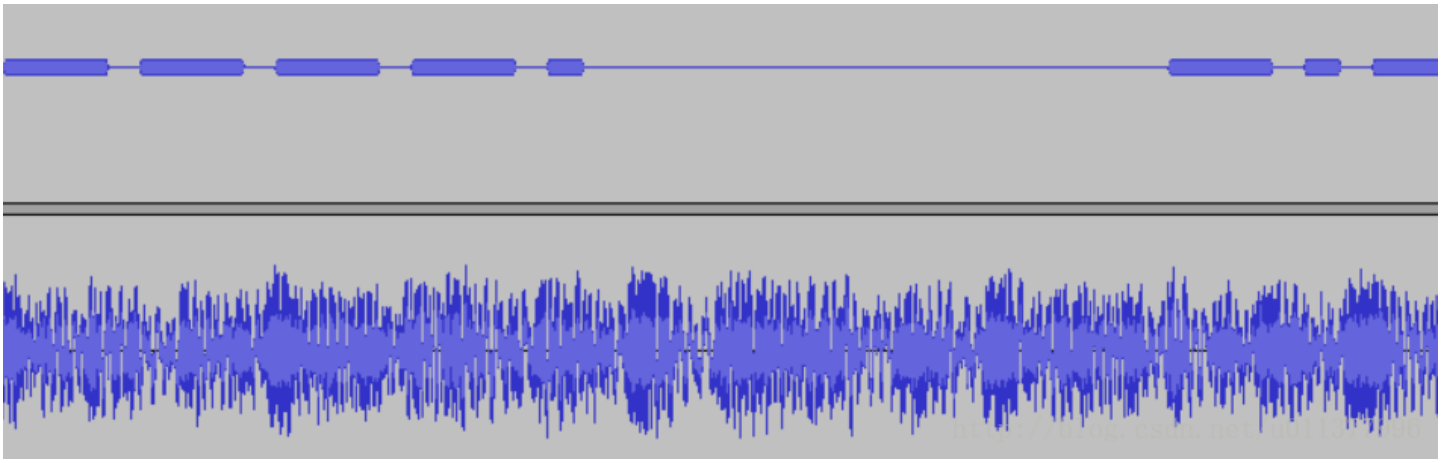


又是那个之前改高度的图片，
获得flag



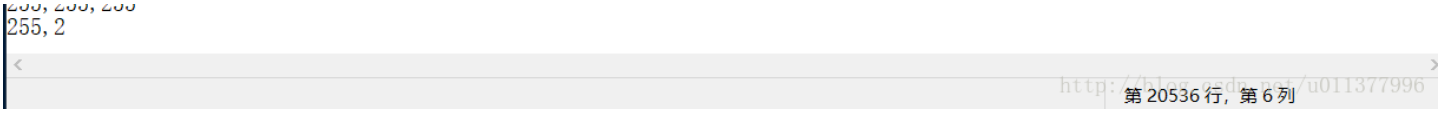
听首音乐

用Audacity打开一看是摩斯密码，直接解密即可，然后直接提交



好多数值

第一次碰到这个类型的题目
利用了python的PIL库。。。。
然后参考了下面的博客
https://www.cnblogs.com/webFuckeeeer/p/4536776.html
结果发现题目好像有点问题。。。。人家都是61366行，我这里只有emmmm。。。。。



而且像素也不完整。。。。。应该是表哥更新之后把题目的文件没有全选完就复制进去了。。
我就直接输入别人的flag了

图穷匕见

用HXD打开找一下jpg的文件尾FFD9，发现后面有大量的16进制数据。。

```
0 84 21 50 24 84 28 1A 10 84 02 10 85 40 84 21   .„!P$„(..„...…@„!
0 84 21 07 FF D9 32 38 33 37 32 63 33 37 32 39   .„!.ÿÙ28372c3729
0 61 32 38 33 37 32 63 33 38 32 39 30 61 32 38   0a28372c38290a28
```

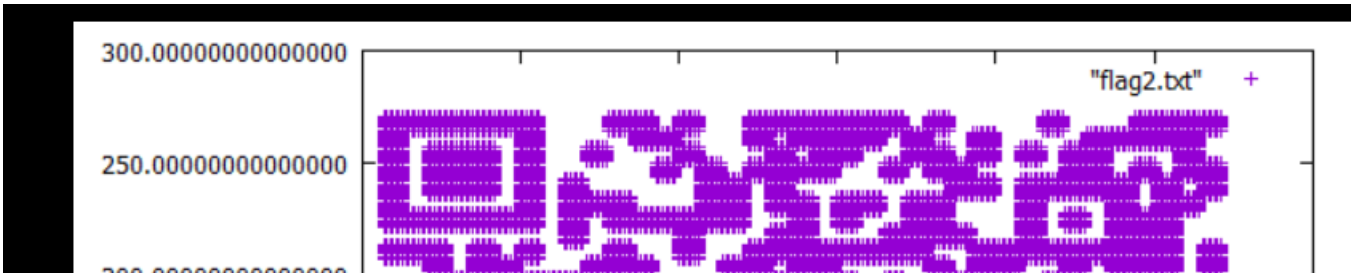
复制进去用Notepad++的converter功能转换为ASCII发现一大串坐标

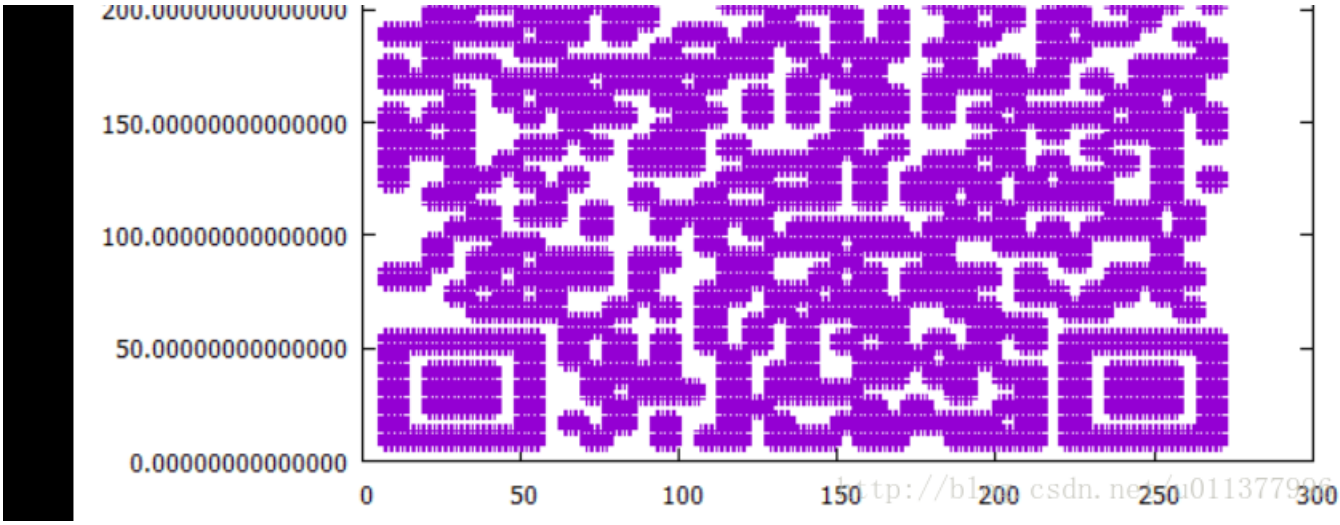
```
1  (7,7)
2  (7,8)
3  (7,9)
4  (7,10)
5  (7,11)
6  (7,12)
7  (7,13)
8  (7,14)
9  (7,15)
10 (7,16)
11 (7,17)
12 (7,18)
13 (7,19)
14 (7,20)
15 (7,21)
16 (7,22)
17 (7,23)
18 (7,24)
19 (7,25)
20 (7,26)
21 (7,27)
22 (7,28)
23 (7,29)
24 (7,30)
```

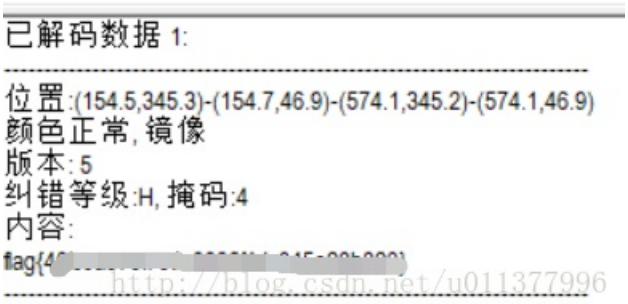

用一个叫gunplot(我用的是Windows下的)的画图软件把这些坐标点画出来，先把他们的格式给弄好

```
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 23
7 24
7 25
```

然后用plot + 文件名的命令导出文件，再扫一扫即可







妹子的陌陌

常规步骤先binwalk一波，发现里面有一个加密的rar包，找了很久都没找到密码。。。。。
发现图片上的字。。。。。。。。可能是密码。。。。尝试一下
喜欢我吗.竟然是密码。。。。我去
里面有一个txt文件

momo.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

嘟嘟嘟嘟
士兵：报告首长！已截获纳粹的加密电报！
首长：拿来看看

电报内容：
. . . . /-/-/. --. /---. . . /-. . -. /-. . -. /. /-. /-. -. /---/-. . /. /. -. -. -/-. -. /. . . . /. -/. . . . /. . -/---/. -. -. -/-. -. /---/--/-. . -.

首长：我操你在逗我吗？你确定是他们纳粹发的吗？
士兵：难道我弄错了？哦。。。等等是这一条

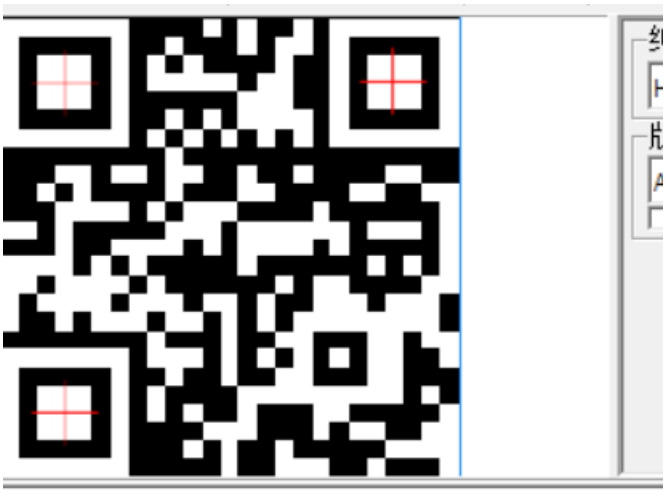
内容：http://c.bugku.com/U2FsdGVkX18t18Yi7FaGiv6jK1SBxKD30eYb52onYe0=
AES Key：@#@#￥%……￥￥%%……&￥

士兵：二维码真的扫不出来吗？？肯定可以扫出来

先解码第一个摩斯密码
发现是一个解密网址。。。。。

再解密以下网址后面的base64

解密出来发现是一张二维码，扫一下得到flag

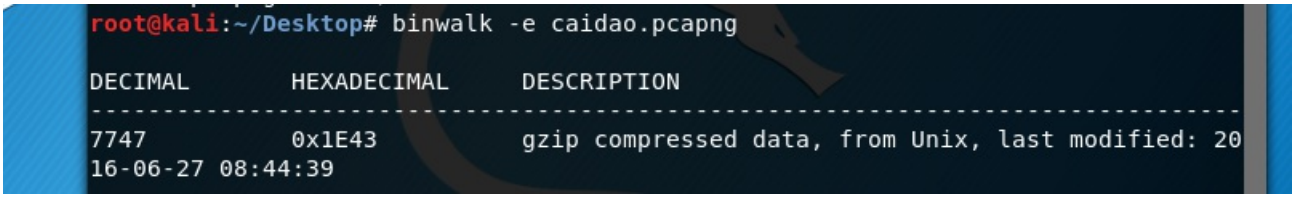


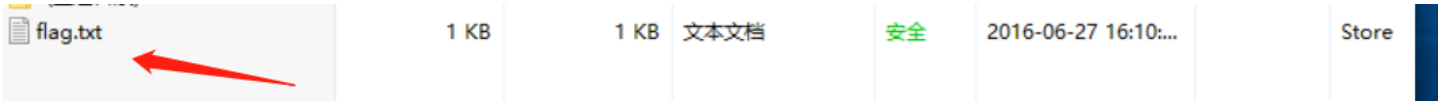
已解码数据 1:

位置:(1.2,1.2)-(345.7,1.1)-(1.2,345.8)-(345.7,345.7)
颜色反色, 正像
版本: 2
纠错等级:H, 掩码:6
内容:
KEY{nitmzhen6}

中国菜刀

这一题可以直接用binwalk把里面的gzip分离出来，那个就是flag





这么多数据包

发现从第104个包开始应该是攻击机（192.168.116.138）在向目标机（192.168.116.159）进行端口扫描，之后可以大致找到攻击机远程连接目标机的包（通过3389端口），以及smb协议的包（用于Web连接和客户端与服务器之间的信息沟通），再往下可以找到以5542开始的包已经getshell
追踪TCP流，发现

```
C:\>type s4cr4t.txt
type s4cr4t.txt
Q0NURntkb195b3VfbGlrZV9zbmlmZmVyfQ==
C:\>shutdown -r -t 100 -m "Stupid Manager!"
shutdown -r -t 100 -m "Stupid Manager!"
```

然后base64即可

这么多数据包

追踪TCP流，发现

然后base64即可

想蹭网先解开密码

先写个脚本把密码跑出来

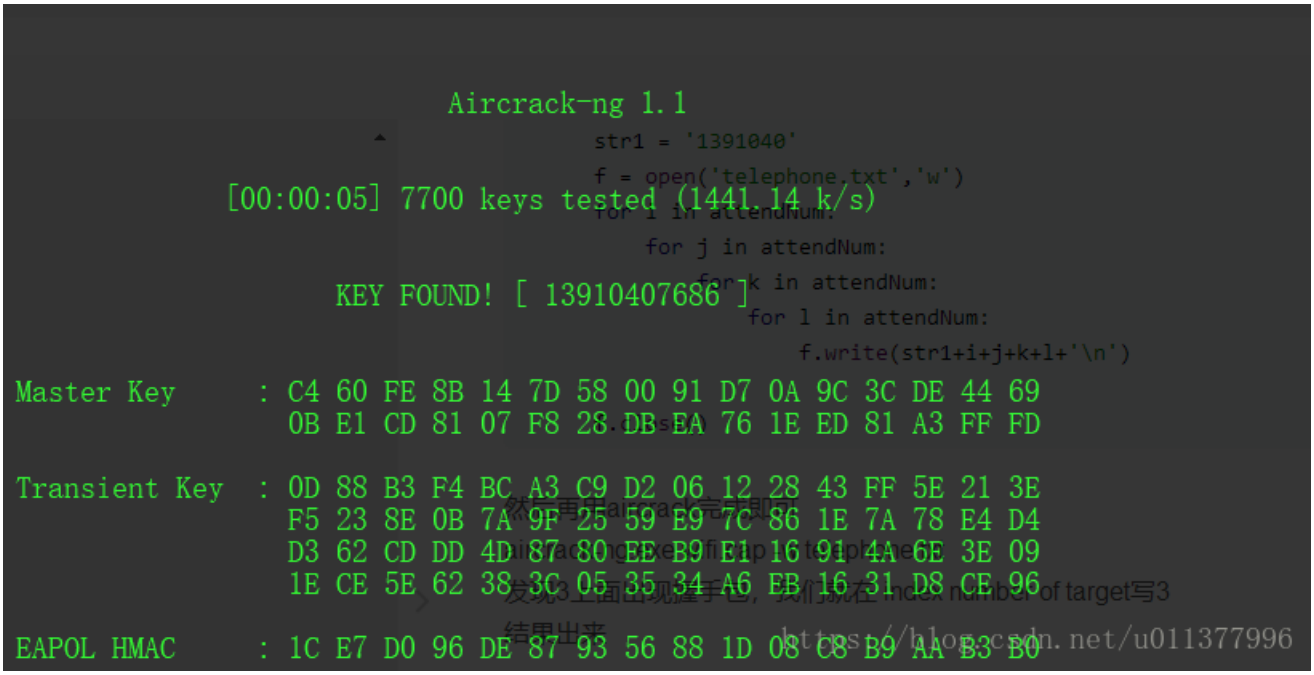
```
#encoding:utf-8
import string
attendNum = string.digits
str1 = '1391040'
f = open('telephone.txt','w')
for i in attendNum:
    for j in attendNum:
        for k in attendNum:
            for l in attendNum:
                f.write(str1+i+j+k+l+'\n')

f.close()
```

然后再用aircrack完成即可

aircrack-ng.exe wifi.cap -w telephone.txt

发现3上面出现握手包，我们就在 index number of target写3

结果出来



还没做完，有待更新。。。