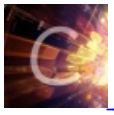
攻防世界-Misc-新手练习记录

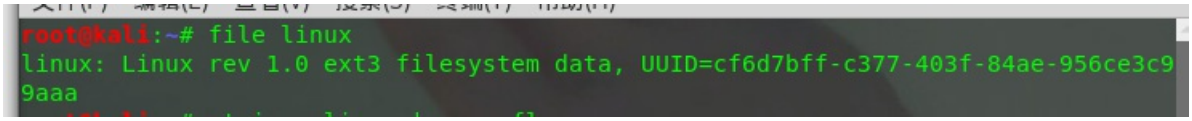
原创

大千SS 于 2019-04-13 19:01:57 发布 15293 收藏 15
分类专栏： 攻防世界 文章标签： 攻防世界 Misc



ext3

下载文件，文件名是Linux，拿到kali中看下文件类型：



ext3就是Linux的一个文件系统，strings查看一下有没有flag这样的字符串：

flag应该就在这个flag.txt中了，把这个文件系统挂载到Linux上：

```
mount linux /mnt
```

挂上去之后看一下/mnt/下的文件，用命令ls -al /mnt/，可以看到上面strings查找到的O7avZhikgKgbF，flag.txt就在这个目录里，得到文件内容为：ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=，base64解码即可。

give_you_flag

把动图保存下来，将每帧分开，看到地50帧有个二维码样子的东西：

这个二维码少了三个角的定位符，没有定位符肯定是扫不出来东西的，手动画上定位符：

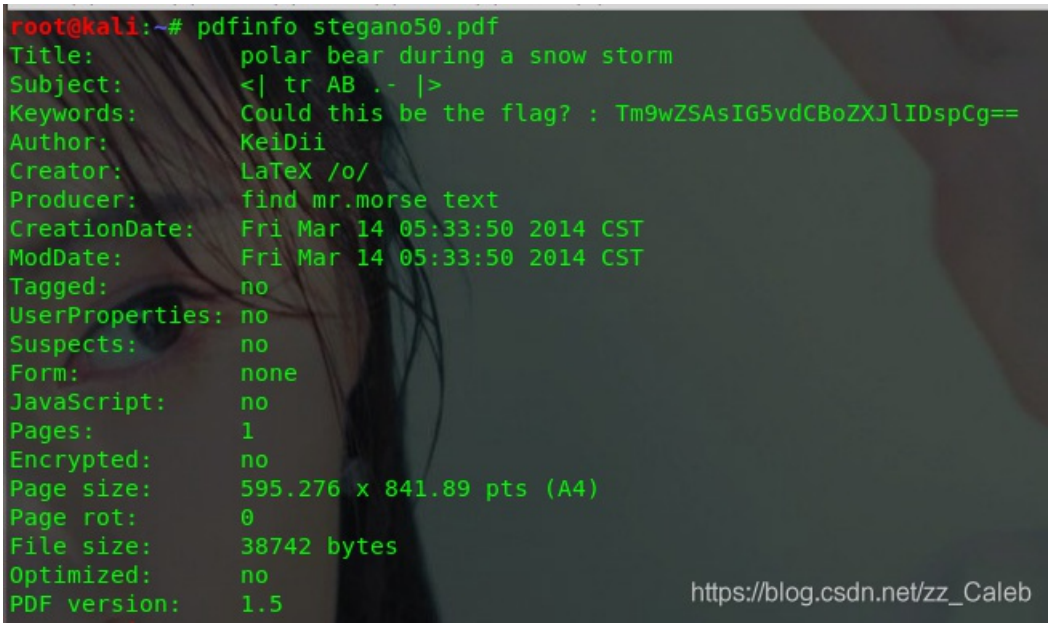
扫描得flag。

pdf

是一个pdf文件，里面有一个图片，用pdf编辑器把图片挪开，flag在图片后面。

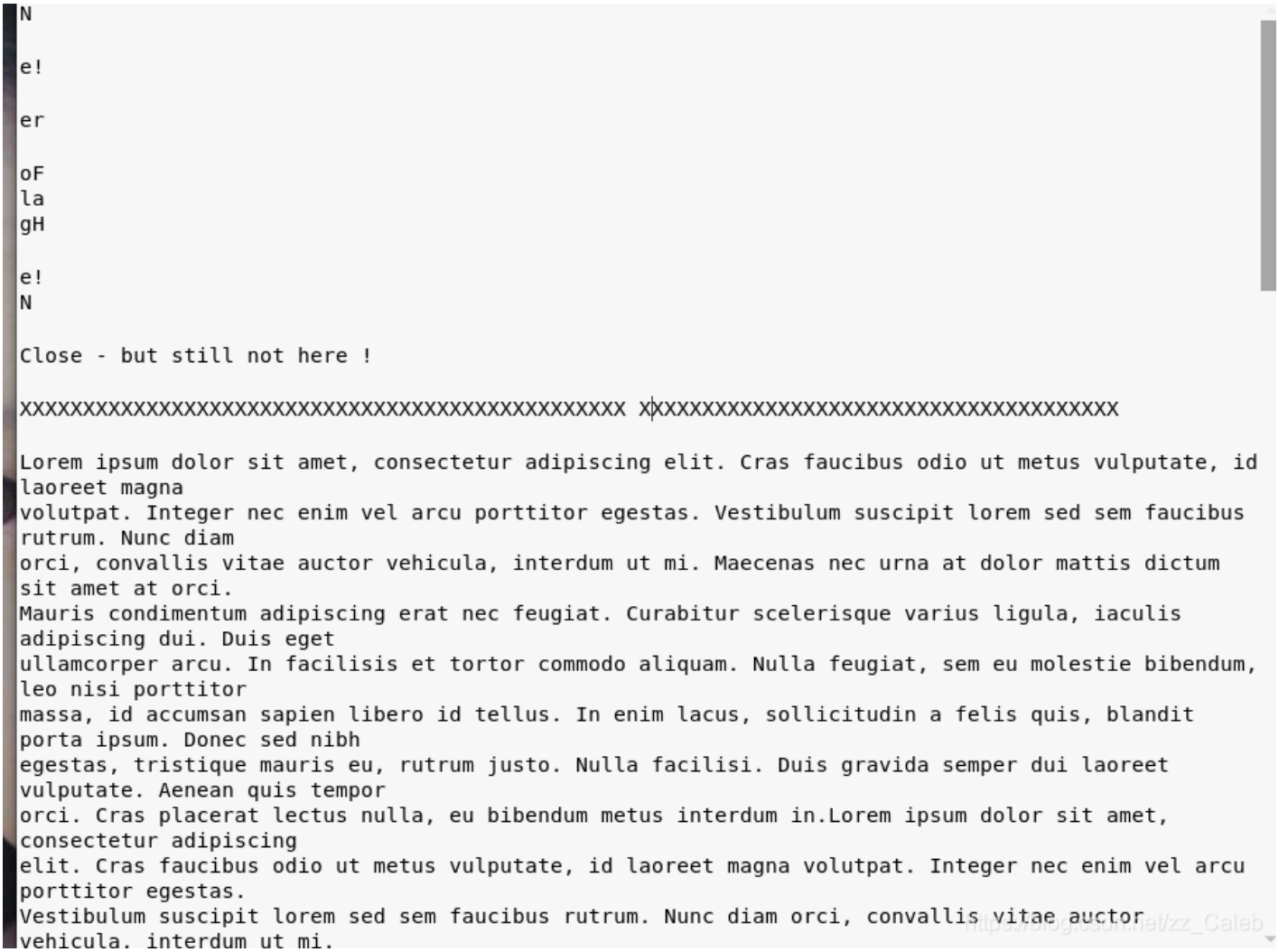
stegano

pdf文件，打开许多文字，linux中查看pdf信息：使用命令pdfinfo



有个base64码，然而解码是：Nope , not here ;)

用pdftotext命令提取一下文件内容：



同样也是没什么线索，火狐的开发者工具pdf.js排上用场了，用火狐打开之后，控制台输入：document.documentElement.textContent，然后得到：

```
        NoFlagHere! NoFlagHere! NoFlagHere!XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXClose - but still not here !BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA
BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB ABBBB AAAAA ABBBB BAAA ABAA AAABB BB AAABB AAAAA AAAAA AAAAB BBA AAABBLorem ipsum dolor sit amet,  consectetur adipiscing elit.  Cras faucibus odio ut metus vulputate,  id laoreet
magnavolutpat.  Integer nec enim vel arcu porttitor egestas.  Vestibulum suscipit lorem sed sem faucibus rutrum.  Nunc diamorci,  convallis  vitae  auctor  vehicula,  interdum  ut  mi.   Maecenas  nec  urna  at  dolor  mattis
dictum  sit  amet  at  orci.Mauris condimentum adipiscing erat nec feugiat.  Curabitur scelerisque varius ligula,  iaculis adipiscing dui.  Duis egetullamcorper arcu.  In facilisis et tortor commodo aliquam.  Nulla feugiat, sem eu
molestie bibendum, leo nisi porttitormassa, id accumsan sapien libero id tellus.  In enim lacus, sollicitudin a felis quis, blandit porta ipsum.  Donec sed nibhegestas, tristique mauris eu, rutrum justo.  Nulla facilisi.  Duis
gravida semper dui laoreet vulputate.  Aenean quis tempororci.   Cras  placerat  lectus  nulla,  eu  bibendum  metus  interdum  in.Lorem  ipsum  dolor  sit  amet,  consectetur  adipiscingelit.   Cras  faucibus  odio  ut  metus
vulputate,  id  laoreet  magna  volutpat.   Integer  nec  enim  vel  arcu  porttitor  egestas.Vestibulum suscipit lorem sed sem faucibus rutrum.  Nunc diam orci,  convallis vitae auctor vehicula,  interdum ut mi.Maecenas nec urna
```

这一串AB字符串，把AB分别转成.-，得到摩斯密码，解码得flag。

SimpleRAR

参考https://blog.csdn.net/zz_Caleb/article/details/88891524

坚持60s

一个java做的游戏，游戏大师可以试试玩着过，既然是程序会给出flag，那么flag就在阿代码中了，用java反编译工具反编译，在文件中可以找到PlaneGameFrame.class中找到flag(大括号中base64需要解码)。

```
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很没面子", 40, 30, 300);
  break;
case 6:
  printInfo(g, "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);
}
```


gif

一大堆的黑白图片，进行白为0黑为1的转换得到：
0110011001101100011000010110011101111011010001100111010101001110010111110110011101101001
二进制转字符串得：flag{FuN_giF}

掀桌子

一串密文：
c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e

解密方法，两个一位，16进制转10进制，然后减去128再转成字符即可：

```
string = "c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e
flag = ''
for i in range(0,len(string), 2):
    s = "0x" + string[i] + string[i+1]
    flag += chr(int(s, 16) - 128)
print(flag)
```

如来十三掌

真是要念经啊：

> 夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多鉢以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

与佛论禅：http://www.keyfc.net/bbs/tools/tudoucode.aspx

得到base64码：MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

但是要先进行ROT13然后再base64解码：

```
flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}
```

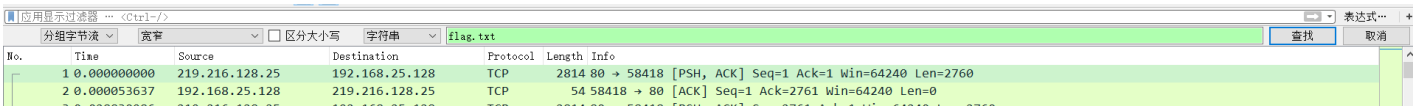
base64stego

参考：https://blog.csdn.net/zz_Caleb/article/details/89298335

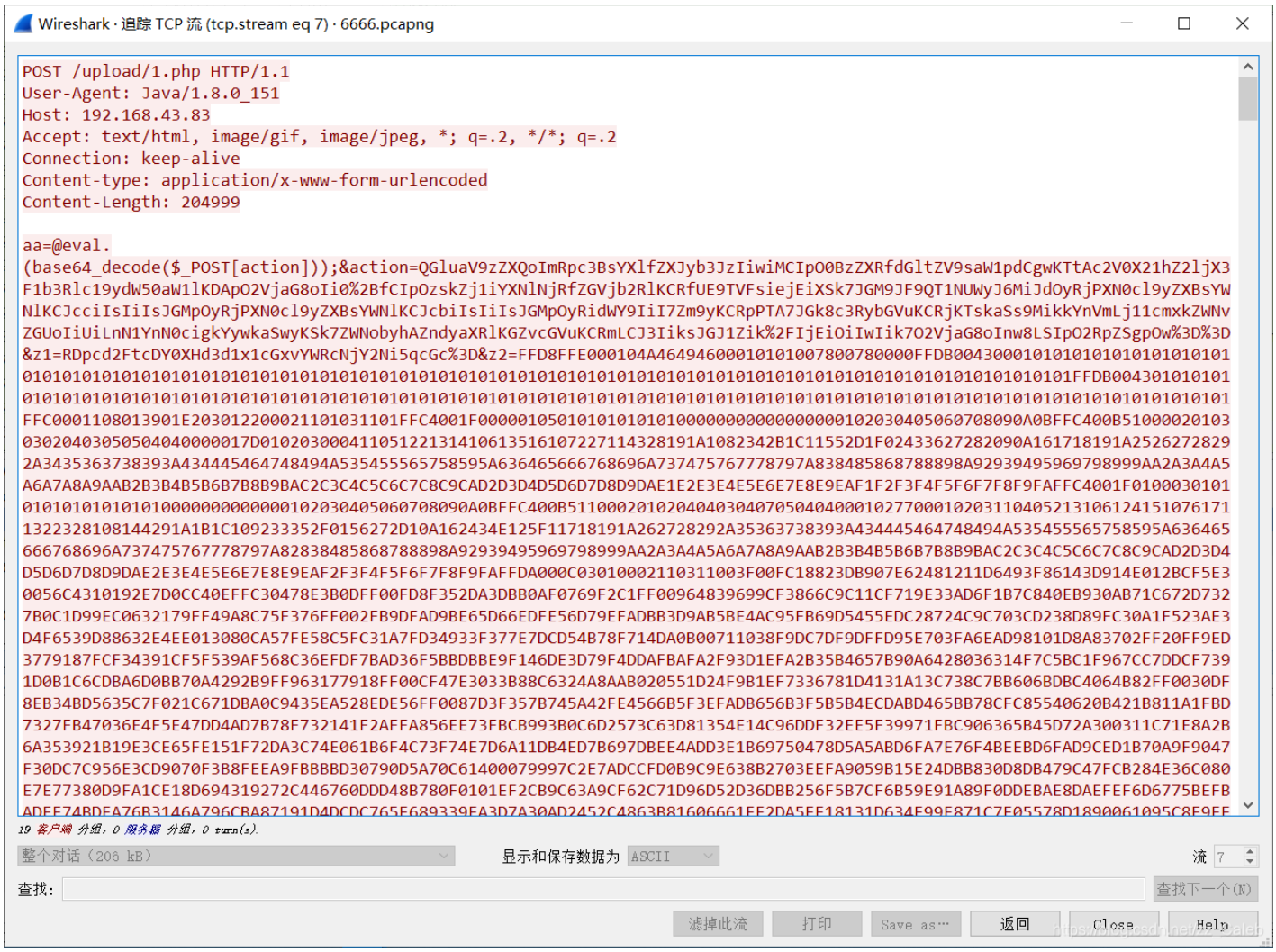
功夫再高也怕菜刀

foremost分解出来一个加密的压缩包，里面是flag.txt文件，不是伪加密。

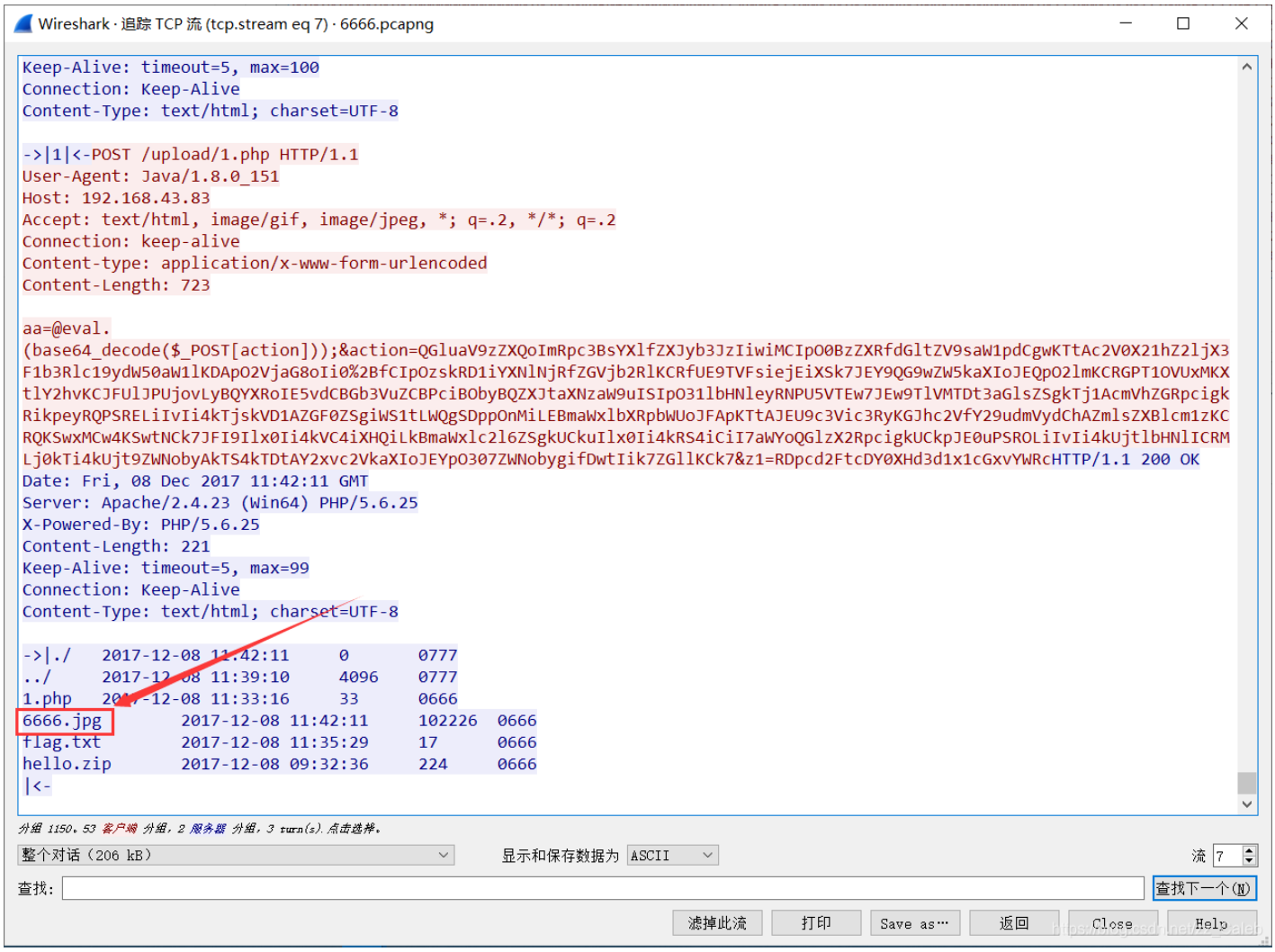
wireshark打开文件，分组字节流查找flag.txt：



查找到第1150个包时，追踪流看到：



看着很像一个问件的16进制码，翻到最下面看到：



再回过头来看看16进制码的头和尾，发现就是一个图片，把这个图片搞出来：

解压拿到flag：