CTF-misc(解题思路/做题经验)

原创

hangshao0.0 于 2020-06-15 21:44:07 发布 5762 收藏 45

分类专栏： ctf-misc

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/weixin_45254208/article/details/105427317

版权

ctf-misc 专栏收录该内容

6 篇文章 1 订阅

订阅专栏

仅提供思路，部分思路给出例子(后面不定时更新)

1.基本操作

可以右键点击，在属性里看看有没有信息，所有图片都可先尝试一下，万一就是送分题呢。

(有的时候一步还不够，可能在备注信息里面藏的是密文)

2.gif图

放到stegsolve或者PS中，一帧帧地分离

3.PDF图片

- 放到PDF编辑器中移动图片位置，flag可能藏在下面(如果题目给出的附件不是pdf可以先改后缀再编辑)
- Linux中查看PDF信息：使用命令pdfinfo
- 在浏览器中打开，ctrl+a全选，将内容复制到txt文本中拿到新信息
  例子：https://blog.csdn.net/weixin_45254208/article/details/105506090

4.信息>>二进制>>flag

- 黑白图片代表1和0
- 长短符号代表1和0、
- ……

总之就是将信息转为二进制再转为字符串(flag)，用python脚本实现

5.Linux日志文件ext3

使用strings命令查看指定文件下有没有flag这样的字符串

```
strings 文件名 | grep flag
```

找到flag.txt后，把文件挂载到linux系统上(mnt目录)

```
mount 文件名 /mnt
```

查看flag.txt

```
cat /.../flag.txt
```

例子：https://blog.csdn.net/weixin_45254208/article/details/105510124

6.binwalk

题目给出附件，用binwalk分析搜索附件中嵌入的文件并分离出来，通常这个文件是被加密的，密码需要通过其他手段来获得，例如用wireshark分析流量包，或者是暴力破解等等

例子：https://blog.csdn.net/weixin_45254208/article/details/105519269