




java隐写_一点隐写小技巧?

原创

名侦探15号  于 2021-03-02 06:04:05 发布  78  收藏

文章标签: [java隐写](#)

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_34206263/article/details/114952514

版权

1.hex以后如果在右侧有文件的后缀一般先把这个文件改为.rar/.zip然后解压缩解压出来这个文件里面的另一个类型文件。(如2333.gif/document.xml)

rar/zip格式特征:

RAR Archive (rar) 文件头: 52617221

ZIP Archive (zip) 文件头: 504B0304 文件尾: 50 4B

2.flag有可能是某句话的拼音首字母(如都深深的出卖了我)

3.看hex有可能文件头受损 在右侧最头上改文件头: 用winhex添加文件头 按下insert 输入GIF8 动态逐帧用 Analyse-file-framebrowser

4.git clone

git clone git://github.com:xxx/test.git ##以gitreadonly方式克隆到本地, 只可以读

git clone :xxx/test.git ##以SSH方式克隆到本地, 可以读写

git clone https://github.com/xxx/test.git ##以https方式克隆到本地, 可以读写(多)

git fetch :xxx/xxx.git ##获取到本地但不合并

git pull :xxx/xxx.git ##获取并合并内容到本地

5.F5隐写

kali+Windows操作方法:

先用xshell 输入ssh+kali的ip地址 再输入用户名、密码 最后出现登录时间等为连入kali

第一步: 先是用binwalk分析一下

确定了没有后门, 根据题目的提示, 刷新的键应该是F5, 也就是F5隐写。

第二步: git clone https://github.com/matthewgao/F5-steganography

从这个github网站下载F5隐身的解密算法。

第三步: cd F5-steganography

第四步: 在F5-steganography文件夹里调用Extract.java 解密。

java Extract ../123456.jpg -p 123456

第五步: 找到输出文件, 用cat命令即可看到flag。

6.winhex 搜PK有就是压缩包 直接改后缀

7.winhex里有JFIF有重复的地方 搜索JFIF有两处即有两张照片放一起 再用编辑分离

8.在一堆乱码里突然有认识的单词或者是连在一起的字母加下划线可能是密码

9.文档里面密码很长 大部分可能是用Python编程(有提示)

如果密码比较短可能是多次解密

10.有分析异同的或者什么的直接拖到桌面上来输入ls 然后再输入diff 文件名.后缀 文件名.后缀

11.bp里on表示拦截开启 此时再重新刷新网页即可拦截到数据

ps: 有些是百度到的大佬的博客内容 未有冒犯之意 如有不宜之处 请随时与我联系

原文: <http://www.cnblogs.com/Eagle-Li/p/7617560.html>