隐写术

转载

weixin_30578677 于 2019-07-25 10:25:00 发布 371 收藏 4
文章标签： 操作系统
原文链接：http://www.cnblogs.com/xww115/p/11242631.html

一、图片隐写术

1.图种

例如一个zip压缩包（1.zip）+一个jpg图片（4fcefdaba56019d77b476e30a5558b47.jpg）结合为一张图片（output.jpg）

以下为Windows命令：

```
C:\Users\lenovo>copy/b C:\Users\lenovo\Desktop\1.zip + C:\Users\lenovo\Desktop\4fcefdaba56019d77b476e30a5558b47.jpg outp
ut.jpg
```

C:\Users\lenovo>copy/b C:\Users\lenovo\Desktop\1.zip +
C:\Users\lenovo\Desktop\4fcefdaba56019d77b476e30a5558b47.jpg output.jpg

Windows输出：

```
C:\Users\lenovo\Desktop\1.zip
C:\Users\lenovo\Desktop\4fcefdaba56019d77b476e30a5558b47.jpg
已复制         1 个文件。
```

破解方法一：

使用kali Linux的 binwalk工具 检索图片文件里的其他文件

```
xue@node2:~$ binwalk '/home/xue/桌面/output.jpg'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
-
334           0x14E           JPEG image data, JFIF standard 1.01
```

显示应用程序

然后使用Linux 的 foremost 工具 将图片中的 zip文件分离出来

```
xue@node2:~$ foremost
ERROR: /home/xue/output is not empty
       Please specify another directory or run with -T.
```

破解方法二：

直接将文件后缀改为.rar，然后解压，但对于隐写了多个文件可能会失败

2.LSB隐写

LSB隐写，也就是最低有效位 (Least Significant Bit)。图片中的像数一般是由三原色组成，由这三种原色可以组成其他各种颜色，例如在PNG图片的储存中，每个颜色会有8bit，LSB隐写就是修改了像数中的最低的1bit，写入加密信息，而人眼无法注意到前后的变化。

例如此图看起只是六只环保色猪头，但是其中包含了一张隐藏的二维码，我们可以通过工具Stegsolve.jar打开此图，然后通过下方的按钮切换到Gray bits，可以看到左上角出现了隐写在该通道的二维码，扫描二维码即可得到flag。

3、文件格式缺失&GIF隐写

下图是一张名为“此为gif图片.gif”的文件，打开发现了报错。

我们将其拖入winhex中查看。在CTF中有的时候会需要我们去修复图片，这对我们对于图片的文件结构要有了解。找到gif的文件格式，然后对照这个破损的文件对其进行修复。

我们可以用工具一帧一帧的观察图片。 上面提到的Stegsolve就带有这种功能。

Stegsolve——Analyse——Frame Brower

二、压缩包隐写术

1.伪加密

一个ZIP文件由三个部分组成：压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志

原理：zip伪加密是在文件头的加密标志位做修改，进而再打开文件时识被别为加密压缩包

预备知识：一个 ZIP 文件由三个部分组成：压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志。方式标志位是判断有无加密的是数据位，伪加密是将 压缩源文件目录区的全局方式标志位进行修改。

我们现在把一个普通无加密压缩包放进winhex中，然后把第二个加密标记位的00 00改为09 00，打开就会提示有密码

2、 Zip密码爆破

爆破：逐个尝试所有密码，直到遇到正确密码

字典：字典攻击的效率比爆破稍高，因为字典中存储了常用的密码，因此就避免了爆破时把时间浪费在无用的密码上

掩码攻击：如果已知密码的某几位，如已知8位密码的第4位是Z，那么可以构造XXXZXXXX进行掩码攻击，掩码攻击的原理相当于构造了第4位为Z的字典，攻击效率 也比逐个尝试的爆破方式高

对于Zip密码爆破，有两款好用的软件

第一个是神器ZAPR，集合了多种爆破类型，还可以自定义爆破字典

还有一款软件，当在CTF中遇到题目不是伪加密且有密码范围提示，就可以用爆破工具ziperello，八位纯数字密码秒破

三、其他隐写术

1、 MP3隐写术

MP3隐写两种方式：

第一种：题目中给了密码了，用mp3stego去解密

第二种：如果在题目中没有给key，而附件只给了一个MP3，那就有可是用mp3stego隐藏的数据，也有可能是在音轨的频谱中隐藏了数据。

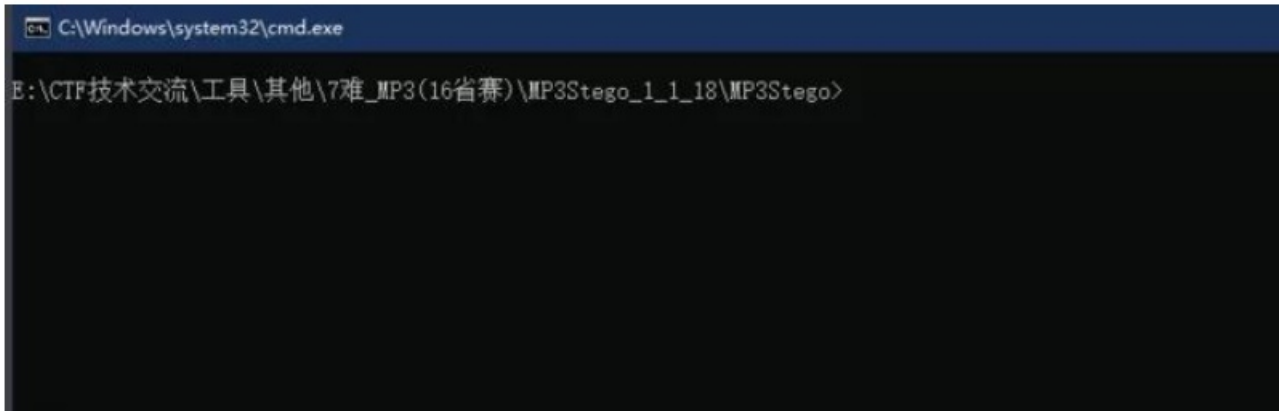
MP3stego要在cmd命令提示符中打开，需要换盘到我们存储文件的分区，具体方法如下：

①、开始->运行->CMD

②、进入某个磁盘，直接盘符代号：如D：

③、进入除根录以下的文件夹 cd 文件夹路径 例如我要进入 E:/123/321 就输入 E：回车

然后将MP3stego解码程序所在的目录粘贴到cmd中，在开始分析之前，要先把准备分析的MP3文件粘贴到decode.exe所在目录中



2、PDF隐写

Office系列软件作为优秀的办公软件为我们提供了极大的便利，其中的Word、Excel、PowerPoint提供了许多在文档中隐藏数据的方法，比如批注、个人信息、水印、 不可见内容、隐藏文字和定制的XML数据。今天我们涉及到的就是提到的隐藏文本功能。

利用PDF文件头添加额外信息，这个区域的信息会被Adobe Acrobat Reader阅读器忽略。

工具： wbStego4open

wbStego4open会把插入数据中的每一个ASCII码转换为二进制形式，然后把每一个二进制数字再替换为十六进制的20或者09，20代表0，09代表1。

最后，这些转换后的十六进制数据被嵌入到PDF文件中。查看用wbStego4open修改后的文件内容，会发现文件中已混入了很多由20和09组成的8位字节

3、DOC隐藏

Doc文件的本质是一个压缩文件，常见的隐藏文本的方式有两种，即：将字体隐藏或者设置同色字体，以下就是一个字体隐藏的例子

11111111

11111111

如上图所示，除了两行无用数据意外我们并不能看出有其他有价值的信息，判断flag可能是被隐藏，需要开启文本显示功能，查看是否是我们猜测的那样。点击左上角　　文件-选项，打开Word选项对话框，在“显示”中勾选隐藏文字选项

4、数据包隐写术

数据包隐写术，就是将所要传达的信息和文件，以流量包的形式下发给参赛选手，参赛选手要从流量包中自行提取出所需要的文件或者相关内容进行解题。比较常用　　的工具是wireshark。关于此类部分的详细介绍，大家可以访问这个网址：https://ctf-wiki.github.io/ctf-wiki/misc/traffic/data/

数据包隐写术目前两种考察行为：

①、flag或者关键信息直接隐藏在流量包中

②、flag相关文件隐藏在流量包中，需要分离文件

转载于:https://www.cnblogs.com/xww115/p/11242631.html