隐写术

转载

weixin_30820151 于 2017-02-20 17:24:00 发布 76 收藏
原文链接：http://www.cnblogs.com/ycll/p/6420509.html

前言：隐写是CTF比赛中的一个比较特殊的分类。基础的隐写题不需要太多的其他方面的相关能力，需要的是每个人天马行空的想象力。所以这方面的题目也是很有意思的。通过隐写来进入网络安全的一个门，我觉得是蛮不错的。但是除了比赛，隐写的实战意义说不上太大，所以这里只做初步介绍，深入的东西就不说了。

一. 隐写术：隐写术是关于信息隐藏，即不让计划的接收者之外的任何人知道信息的传递事件（而不只是信息的内容）的一门技巧与科学。具体涉及到的，分为图片隐写，音频隐写，视频隐写。其中图片的隐写是最为常见的，所以下面以图片隐写为例进行说明。

二. 工具：

（1）Stegsolve图片分析软件： 用于分析图片，图片是由各种不同颜色的像素点构成的（涉及LSB等图片图形学内容，感兴趣的可以自己去查），这个工具可以很容易的把不同颜色通道的图片信息显示出来。

（2） 二维码扫描： 在图片隐写中，扫描二维码得到答案的题目是比较常见的，但是有时候扫描之后出现的也不一定是最后答案，往往需要我们进一步的去破解，所以用手机扫描注定不方便，有个电脑上的软件会方便很多。

（3）十六进制分析工具：与这个相同的还有winhex，winhex更常用，且功能更强大，想使用哪个看个人喜好。计算机的世界，所有的东西都是由1和0组成的，二进制也可以转成十六进制，所以利用这个工具可以看到构成图片的最原始的数据，同时可以找到隐藏在图片里的秘密。

4）binwalk:这是在kali下自带的一个命令行工具，可以用来分析目标文件里是否有夹带其他东西，这在除了隐写以外的其他类型的题也是常用的工具。命令：binwalk –n 加文件 。比如说一张图片里面隐藏了一个压缩包，从表面上你是看不出什么的。但是使用binwalk命令，就可以分析出来。同样，把图片丢到十六进制查看器里面也可以看出来，但是新手对这些不熟悉很容易出错。毕竟压缩文件除了rar还有zip，又或许图片里面藏的是个txt。

另外，分析之后我们需要把这附带的其他文件提取出来，这就需要另外的一个命令，

binwalk –e 加文件。同样可以使用十六进制查看器，通过分离切割来得到，有兴趣的同样可以自己试试。

（5）PS:这个东西大家肯定不会陌生，有关图片隐写，ps有时候会用到，但几率不大。因为前面介绍的几种工具基本已经够用了，ps无非也就是有更进一步的能力而已。与ps相应的还有一个叫做FW的工具，也是Adobe系列的。要是一张图片真的什么都分析不出来，丢到PS里，说不定就会发现惊喜了，但是这样的题至今我也只遇过三题，其中两题都是跟FW有关的。

（6）密码学：这就涉及到一个很大的方面了。有时候我们找到了图片里面藏的密码，但是出题人不会很直白的告诉我们答案，就会进行加密。常见的密码有md5,base64，当然还有各种各样奇怪的密码。不过野不用着急，这都是一个积累的过程，先去了解md5和base64的特征，然后拿解到的密码去网上搜索。大部分常见的密码类型网上都有在线解码网站

三.一些经验技巧：我一直认为看再多的东西都不如实际做几题来的印象深刻，不然很多东西都是看了就忘的。但是一些经验技巧也可以让后面学习的人少走些弯路（PS:这些都是我以前做题的时候总结的，也许不一定都是对的，毕竟接触这块还不是很久，还有很多地方要学习的，但是也可以参考一下，找到自己的一个做题思路才是最重要的）

（1）一般拿到一张图片，先看图片格式。常见的有JPG，PNG和BMP。JPG比起PNG，是有过压缩的图片，所以JPG格式的图片通常是没必要放到图片分析器里去看的。由于进过压缩，所以里面是不能放下二维码的。而我们使用图片分析器来分析图片，60%是为了找到里面隐藏的二维码。

（2）JPG格式的图片通常里面都有藏着另外的东西，大体上是压缩文件之类的，当然，也有往里面放音频的……所以先丢去binwalk分析才是正确的。

（3）PNG格式的图片首先就可以考虑藏二维码的问题了，不过也不是说他里面不会藏有其他文件哟。

（4）BMP是位图文件,能放的东西就更多了，可以拿去PS里看一下，说不定在就出现了两个图层了。

（5）无格式的东西，图片隐写的题，出题人很喜欢绕一个弯。有时候下载下来的东西是没有后缀格式的，这时候需要手动去添加。丢到十六进制查看器里去看它的头部十六进制，取前四个到百度搜一下就知道是什么格式了。同理，也有人会把头部文件给删除，这时候要靠他的后缀手动添加头部。这些都是在十六进制查看器里完成的。

（6）遇到音频的时候，音频也是可以藏东西的。我一般是喜欢用AU，当然也有其他比较专门的工具，可以自己去找找。查看音频的波形，有时候里面会藏有一段莫尔斯电码。

转载于:https://www.cnblogs.com/ycll/p/6420509.html