# ctf

原创

骑着蜗牛超丿F1 于 2019-05-21 11:40:54 发布 7647 收藏 51

文章标签： ctf解题思路



刚参加过一次信息安全类竞赛

本人也是小白的身份参加的，两天时间边学边做，下面就介绍一下这次竞赛我的收获。

首先，Crypto类题是ctf的入门题目，一般都比较简单易做，所以这次我也就只讲一下crypto类问题。

一.

下面先介绍一下常用的工具：

这是CTF Wiki官网里给的工具下载网页，是比较全的了：

https://tools.pediy.com/ （分类很全）

https://ctftools.com/down/ （这里面工具合集分类里下一个”分类详尽的工具合集“基本上就够了）

1.binwalk

这个是神器！！！

没用的自己在网上找一下binwalk安装教程就好了，教程还是很好找的，这个需要python环境

```
这个是个强大的文件分析工具，一般crypto里隐写类题目很多图片、音频或者没有后缀不知道文件类型的文件放在binwalk里跑一下就会发现其实里面暗藏其他压缩包。
```

2.Winhex

```
文件分析工具。把文件放到winhex里可以看到文件的十六进制格式。
只需要在网上找到不同类型文件对应的固定文件头和文件尾的二进制编码，就可以看出文件是否正常。
比如png图片的十六进制编码第一行是固定的，有些题就会故意给你改一下文件头让文件无法正常打开，这时候你修改过来后就可以正常打开了。
```

3.stegsolve

需要Java环境。

可以去Java官网下个最新的jdk，在网上找一下安装教程就好了（记得配置环境变量）。

```
这个是图片分析的利器。
有些图片是有多层重叠出来的，这个软件就是可以分图层查看的，具体用法下面用例题讲解题思路的时候会说。
```

4.steghide

隐写类工具。它可以让你在一张图片或者音频文件中隐藏你的秘密信息，而且你不会注意到图片或音频文件发生了任何的改变。而且，你的秘密文件已经隐藏在了原始图片或音频文件之中了。这是一个命令行软件。因此，你需要学习使用这个工具的命令。你需要通过命令来实现将秘密文件嵌入至图片或音频文件之中。除此之外，你还需要使用其他的命令来提取你隐藏在图片或音频中的秘密文件。

常用命令：

将s.txt文件隐藏到t.jpg中：

#steghide embed -cf t.jpg -ef s.txt -p 123456

从t.jpg解出s.txt:

#steghide extract -sf t.jpg -p 123456

以上几种就是比较常用的了，下面用例题讲一下解题思路

二.解题思路

1.原题图片下载地址：http://207.148.123.236:1535/
下载后只有一张图片，如下：


一般拿到这种只有一张图或一个为止文件的先放binwalk跑一下看看，这里注意要把图片和binwalk放到同一个目录下。（binwalk一般要防止python里scripts目录下）

在binwalk所在的文件里按住shift点右键可以在该目录下打开命令行界面
然后输入命令 python binwalk sadness.jpeg

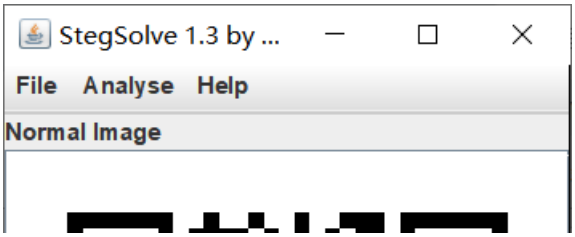
```
PS C:\Python27\Scripts> python binwalk sadness.jpeg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 703 x 1056, 8-bit/color RGBA, non-interlaced
353868        0x5664C         RAR archive data, version 4.x, first volume type: MAIN_HEAD

PS C:\Python27\Scripts>
```

就可以发现这个图片里有一个png文件一个rar压缩包。
直接把后缀改为rar，就可以打开压缩包了。
打开后发现里面文件如下：


打开dont open me 里面就是一段话，告诉你虽然这个txt文件没用，但是你的方向是正确的。
（一般情况那个stego_200基本就不用看了，因为就是为了隐藏压缩包用的图片，里面基本不会有其他信息了。）
然后i am useless文件类型不知道，所以先放着，先看qrcode压缩包，打开后发现是11张二维码，按顺序扫码后就是一句话，告诉你那个i am useless就是藏着有用信息的文件
记得说过未知类型文件怎么处理吗？
放到binwalk里看看，因为文件名里有空格，可能会有问题，于是我把它重命名成了1

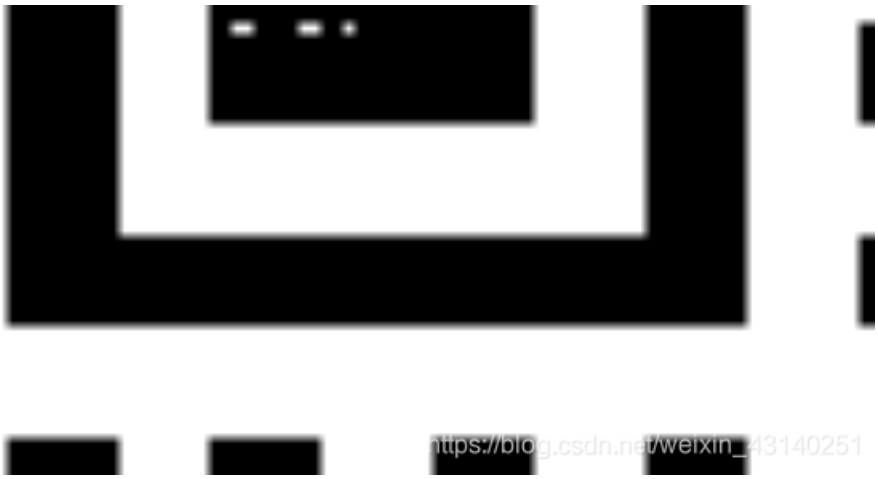
```
PS C:\Python27\Scripts> python binwalk 1

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 280 x 280, 8-bit/color RGBA, non-interlaced
91            0x5B            Zlib compressed data, compressed

PS C:\Python27\Scripts> _
                                                    https://blog.csdn.net/weixin_43140251
```

发现其实是个png图片，改后缀为png之后发现是个二维码，扫过是一句话，告诉你你的方向是正确的，靠近的仔细看。
于是我就把这个二维码放大但是好像没什么用，于是就用另一个图片分析软件分图层查看，没错就是step solves




左右翻页按钮可以查看图层


我在翻了几次之后发现有一个图层右上角有问题，于是把图片保存下来放大查看




有经验的同学就可以看出来这是一段摩斯电码了，翻译之后就得到flag。

2.第二个题的百度云盘链接https://pan.baidu.com/s/1c5mRW9U2kKCDLcmZPVCxsA 提取码：n8g4
还是一张图，但是打不开。
还是先binwalk，发现是压缩包。直接改后缀。
因为有了第一个的例子这道题就不每一步都放图了
打开压缩包后里面两张图片一个加密的压缩包，压缩包名字是flag
也就是说flag就在压缩包里了，但是有密码，密码信息应该就是隐藏在图片里了。
用前面介绍过的软件试，发现binwalk运行后没用问题，stegsolve也没发现异常，但是steghide里发现里面确实有隐藏的内容，分离到txt文件后就得到了压缩包的密码，得到flag