CTF竞赛入门（四）信息隐写

原创

senjy7 于 2020-11-18 08:37:28 发布 1232 收藏 7

分类专栏： CTF

本文链接：https://blog.csdn.net/single7_/article/details/109746245

隐写术 steganographia

概述

隐写术是一门关于信息隐藏的技巧与科学，所谓信息隐藏指的是不让除预期的接收者之外的任何人知晓信息的传递事件或者信息的内容。隐写术的英文叫做Steganography，来源于特里特米乌斯的一本讲述密码学与隐写术的著作Steganographia，该书书名源于希腊语，意为“隐秘书写”。

CTF 隐写术分类

语义隐写术

符号码
隐语
虚字密码

技术隐写术

系统结构

纯隐写
密钥隐写
公钥隐写

空间结构

信道隐写
时空域隐写
变换域隐写

载体对象

图像隐写
文本隐写
音视频隐写
其他文件隐写

ctf 中通常使用以下格式作为信息载体进行隐写
图片文件 .jpg .png .gif .bmp
文本文件 .docx .pdf .zip
音视频文件 .wav .mp3 .mp4
其他特殊文件

现状

上来一套组合打击

- binwalk + winhex 分析文件结构和内部数据
- stegsolve 分析lsb隐写
- stegdetect 检测特殊工具隐写

文件结构分析工具
TrID 工具
file (liunx 命令)

隐写实战

图片隐写

插入 利用文件格式的无关数据或者在空白区域放置需要的数据不会改变原始数据，只会增加隐写的内容
替换 每一字节的最低有效位进行变换不会改变文件大小，源文件会发生变化

考查点

在文件尾部插入字符
图片标记码之间插入字符
zip格式文件分离
图片文件分离 binwalk foremost
LSB 隐写二维码 stegsolve
LSB隐写ASCII码
LSB隐写之双图对比
JSteg隐写
JPhide隐写
outguess隐写
F5隐写

Stegdetect 隐写

Stegdetect + JPHide 隐写

exif隐写

exiftool工具的使用

PNG隐写

基本可以分为三种：第一种是LSB隐写的替换 第二种 IHDR隐写 放在其他系统下看是否存在CRC报错 （win10 不会报错，正常打开，需要放到 kali linux 中）
IHDR隐写 准备crc爆破脚本
IDAT隐写 zlib

GIF隐写

基于空间轴 由于 GIF 的动态特性 由一帧帧的图像构成，因此每一帧的图像、多帧图像间的结合都成了隐藏信息的载体
基于时间轴 一帧帧图像按照一定阿时间间隔进行跳转，因此跳转的时间也能用哦你过来进行信息的隐写

steghide 隐写

steghide隐写
steghide密码爆破

文本文件隐写

word隐写

字体颜色
文字隐藏
文字本质

pdf隐写

pdf隐写和wbStego4open工具的使用

压缩文件隐写

伪加密
暴力破解
字典攻击
掩码攻击
明文攻击
CRC32爆破

音频攻击

wav隐写
配合编码和密码学知识进行隐写
音频隐写二进制数据
MP3隐写
通过关键字符搜索寻找密码
silenteye的使用

其他文件的隐写

MP4分帧 （ffmpeg）

虚拟磁盘隐写

pyc文件隐写

图片隐写+pyc文件的反编译
pyc文件嵌入payload

补充

NTFS交换数据流（alternate data streams，简称ADS）是NTFS磁盘格式的一个特性，在NTFS文件系统下，每个文件都可以存在多个数据流，就是说除了主文件流之外还可以有许多非主文件流寄宿在主文件流中。它使用资源派生来维持与文件相关的信息，虽然我们无法看到数据流文件，但是它却是真实存在于我们的系统中的。创建一个数据交换流文件的方法很简单，命令为"宿主文件:准备与宿主文件关联的数据流文件"。

UNCTF杂项题Hidden secret 之NTFS交换数据流隐写

从一道取证题目谈NTFS交换数据流

利用NTFS交换数据流隐藏文件