misc1-图片隐写

原创

Miracle 007 于 2021-10-21 18:27:59 发布 1548 收藏

分类专栏： 学习笔记 文章标签： ctf

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/LXC_007/article/details/120677443

版权

学习笔记 专栏收录该内容

59 篇文章 0 订阅

订阅专栏

Misc：杂项

一、分类

1.数据编码/图形密码

2.图片隐写

3.音频&视频隐写

4.流量分析

5.内存取证

6.游戏隐写（打通关获得一个flag）

二、基础知识

1.010editor（alt+4打开模板，alt+f4关闭，模板需要自己安装，tab自动补全）

插入和覆盖

有模板库，f5

模板提供宽和高等的信息

2.图片十六进制文件头+文件模板

3.文件属性（exiftools）

4.kali

三、图片隐写分类

1.右击属性

属性里藏东西

2.文件末尾藏有字符串

（2）文件十六进制藏有字符串

strings查找可打印的字符（kali预装，strings file）

grep使用正则表达式搜索，并输出匹配的行（grep flag）

file 可以显示图片类型和属性

（3）文件分离

binwalk，foremost（分离所有的，不一定能分离出自己需要的）

dd 单独分离，分理出需要的东西

3.文件包含

4.修改头文件

破坏文件头一定不能读取，破坏文件尾还有可能读取

5.GIF

·特殊帧（ps/stegsolve）

·帧的时间间隔（看时间间隔的是什么工具？）

例题：金三胖

方法一：用ps看图层

方法二：stegsove

0.1s是点

0.2s是杠

6.png（bmp）

IHDR：表示图片的宽和高

从IHDR第一个开始选中，校验和，点工具CRC-32计算，不是一样的就改大

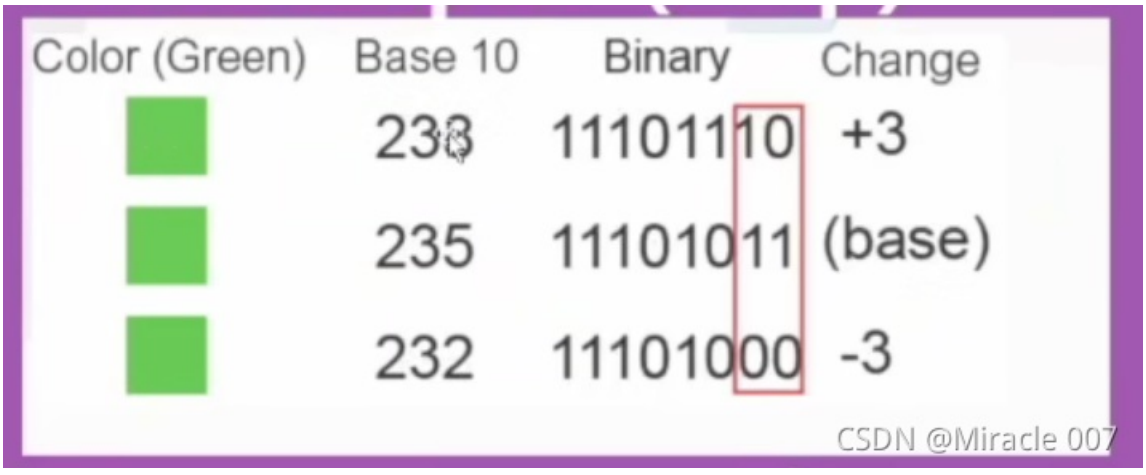
或者用脚本爆破

```python
import os
import binascii
import struct
misc = open("IHDR.png","rb").read()
#print(misc[0x0c:0x0f+1])
# 爆破高

crc32_bytes = misc[0x1d:0x20+1]# 读出bytes
crc32_hex_eval = eval('0x' + crc32_bytes.hex())#bytes串 -> hex串  ->  值
print(crc32_hex_eval)
for i in range(4096):
    data = misc[0x0c:0x0f+1] + misc[0x10:0x13+1] + struct.pack('>i',i)+ misc[0x18:0x1c+1]  #IHDR数据
    crc32 = binascii.crc32(data) & 0xffffffff
    if crc32 == crc32_hex_eval : #IHDR块的crc32值
        print(i)
        print("height_hex:"+ hex(i))

```

```
533700238
819
height_hex:0x333
[Finished in 1.3s]
```

CSDN @Miracle 007

lsb隐写/lsb加密



7.jpg

8.双图隐写

9.stegpy

10.silenteye

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖