WinHex的学习

原创

Sandra_93 于 2018-10-18 16:40:29 发布 723 收藏 2

分类专栏： BugkuCTF 工具类

本文链接：https://blog.csdn.net/Sandra_93/article/details/83148167

BugkuCTF 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏

工具类

4 篇文章 0 订阅

订阅专栏

Bugku隐写1

将图片在WinHex里打开

第二行，前四位是宽，后四位是高。（这里两个数字在一起，是为一位）

PC机对有多位的十六进制的数据的存储方法是：低位在前，高位在后（16进制中，最右边为最低位）

有大佬说，把图片扔到虚拟机里，宽和高不匹配的话打不开

手动尝试，出现的错误是：无法载入对象，**IHDR:CRC error**

> CRC校验是一种防错处理程序,对写入与读取的数据进行比对,防止将错误数据当成正常的写入

看writeup，是要将第二行的第7位改为F4，实际操作中，尝试了一下，其实就算是将第5位（按照排法，第5位应该是最低位），将00改成01，都可以另存为后得到新的图片，会报“无无效文件：user.txt.Do not proceed!”的错，但还是能够保存图片，而且能得到图片下面的flag

---

WinHex（手动恢复数据）

将磁盘内容清空再恢复，挺有意思，下次试试

这里学到的内容->WinHex恢复磁盘

> **MBR**，即主引导记录，位于整个硬盘的0柱面0磁道1扇区，共占用了63个扇区，但实际仅仅使用了1个扇区（512字节）。在总共512字节的主引导记录中，MBR又可分为三部分：第一部分：引导代码，占用了446个字节；第二部分：分区表。占用了64字节；第三部分：55AA，结束标志，占用了两个字节。后面我们要说的用winhex软件来恢复误分区。主要就是恢复第二部分：分区表（64字节）。

> **引导代码的作用**：就是让硬盘具备能够引导的功能。假设引导代码丢失，分区表还在。那么这个硬盘作为从盘全部分区数据都还在。仅仅是这个硬盘自己不能够用来启动进系统了。假设要恢复引导代码。能够用DOS下的命令：FDISK/MBR；这个命令仅仅是用来恢复引导代码，不会引起分区改变，丢失数据。另外，也能够用工具软件，比方DISKGEN、WINHEX等。
> 但分区表假设丢失。后果就是整个硬盘一个分区没有。就好象刚买来一个新硬盘没有分过区一样。可见**分区表是非常多病毒喜欢破坏的区域**。

> **EBR**。也叫做扩展MBR（Extended MBR）。由于主引导记录MBR最多仅仅能描写叙述4个分区项，假设想要在一个硬盘上分多于4个区，就要采用扩展MBR的办法。

> MBR、EBR是分区产生的。
> 每个分区又由DBR、FAT1、FAT2、DIR、DATA 5部分。

中英文切换
帮助（Help）->设置（Setup）->English please（中文）

如果数据改变而没有保存，会变成其他的颜色，选中要修改的，右键编辑/填充选块，就可以添加自己想要加入的数据。保存，得到的（比如图片）是修复完后的图片