

**黑客夺旗赛CTF-misc安全杂项考点**

**掘安攻防实验室**

版本号 : 0.1

QQ群：130684480

更新时间 : 2019.01.01

创建人: wh1te、许心痕

总结：掘安攻防实验室成员



**图片隐写术**

1. 16进制编辑器查看内容，有没有类似PK，RAR，txt，flag，password等信息
2. 16进制补全头或者在尾
3. 图片查看备注或者详细信息
4. 图片修改高度
5. 常见16进制文件头：

JPEG (jpg)，文件头：FFD8FF 文件尾：AE 42 60 82

PNG (png)，文件头：89504E470D0A1A0A

GIF (gif)，文件头：47494638

TIFF (tif)，文件头：49492A00

Windows Bitmap (bmp)，文件头：424D

CAD (dwg)，文件头：41433130

Adobe Photoshop (psd)，文件头：38425053

Rich Text Format (rtf)，文件头：7B5C727466

XML (xml)，文件头：3C3F786D6C

HTML (html)，文件头：68746D6C3E

Email [thorough only] (eml)，文件头：44656C69766572792D646174653A

Outlook Express (dbx)，文件头：CFAD12FEC5FD746F

Outlook (pst)，文件头：2142444E

MS Word/Excel (xls.or.doc)，文件头：D0CF11E0

MS Access (mdb)，文件头：5374616E64617264204A

WordPerfect (wpd)，文件头：FF575043

Adobe Acrobat (pdf)，文件头：255044462D312E

Quicken (qdf)，文件头：AC9EBD8F

Windows Password (pwl)，文件头：E3828596

ZIP Archive (zip)，文件头：504B0304

RAR Archive (rar)，文件头：52617221

Wave (wav)，文件头：57415645

AVI (avi)，文件头：41564920

Real Audio (ram)，文件头：2E7261FD

Real Media (rm)，文件头：2E524D46

MPEG (mpg)，文件头：000001BA

MPEG (mpg)，文件头：000001B3

Quicktime (mov)，文件头：6D6F6F76

Windows Media (asf)，文件头：3026B2758E66CF11

MIDI (mid)，文件头：4D546864

1. binwalk或者foremost进行图片分离
2. Stegsolve 可以看常规的图片隐写，比如gif什么的，发现LSB隐写，Xor等等。
3. LSB隐写
4. F5刷新
5. Outguess
6. PS分离图层，或者拼接图片。
7. 二维码神器，CQR.exe

**Word**

1. 本质是一个压缩包，里面可以隐藏图片或者txt
2. 打开word以后是一首诗，但是没头绪，重点在行间距，大的是1，小的是0
3. word显示隐藏内容

**pcgp流量包**

1. wiresahrk
2. 追踪流 TCP UDP ICMP HTTP
3. 文件->导出->导出 HTTP TCP 等
4. foremost分离压缩包
5. wifi包格式，手机包格式

**压缩包**

1. 查看详细信息或者备注
2. 16进制打开，查看内容
3. 伪加密：360压缩或者16进制分析伪加密
4. 暴力破解 ARCHPR或者ziperello
5. 明文攻击 ARCHPR
6. CRC校验
7. CRC32碰撞
8. foremost分离

**磁盘分区/备份**

1、DiskGenius 回复磁盘分区

**MP3**

1. Mp3Stego-gui 剩下的工具，大哥们写
2. https://blog.csdn.net/pdsu161530247/article/details/77568807
3. 先听一遍，看看是啥
4. 比如：开头5秒是空白，或者打开看波段，波形，或者最后有没有空白几秒

**pdf文档结构：**[**https://lazymind.me/2017/10/pdf-structure/**](https://lazymind.me/2017/10/pdf-structure/)

**5、mp3保留bit位隐写**

**PDF、日志审计、取证、视频隐写**

