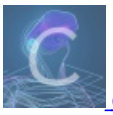
CTF杂项题基础（1.文件识别与分离及图片隐写）

原创

无领 于 2020-11-01 21:44:12 发布 2350 收藏 19

分类专栏： ctf misc

本文链接：https://blog.csdn.net/Yy10205473/article/details/109409942



CTF杂项（misc）解题技巧

杂项类型

1.隐写
2.压缩包处理
3.流量分析
4.攻击取证
5.其他

文件类型识别

在做misc题的时候有很多以文件附件的题目出现，但是有时候给我们的文件并不一定是以正确的后缀名给我们，属于这个时候就需要我们对文件类型进行识别。
一般我们可以使用fkali中只带的file命令或者十六进制编辑器WinHex

---

file命令识别

kali中自带有file命令可以用来识别文件的类型和编码格式。使用方法较为简单。
file使用方法

```
file +参数 +文件名
```

file参数：
-b　列出辨识结果时，不显示文件名称。

-c　详细显示指令执行过程，便于排错或分析程序执行的情形。

-f<名称文件>　指定名称文件，其内容有一个或多个文件名称时，让file依序辨识这些文件，格式为每列一个文件名称。

-L　直接显示符号连接所指向的文件的类别。

-m<魔法数字文件>　指定魔法数字文件。

-v　显示版本信息。

-z　尝试去解读压缩文件的内容。

```
root@kali:~# file -b /root/桌面/timg321YDBJA.jpg
JPEG image data, JFIF standard 1.01, resolution (DPI), density 72×72, segment length 16, baseli
ne, precision 8, 1920×1080, components 3
root@kali:~#
```

通过file命令中的-b参数可以得到我们需要的基本信息。（最后的文件名中需要加入文件的路径）

WinHex编辑器使用

WinHex是一款十六进制编辑器，他是一个比较使用的工具，能够用来编辑二进制文件，对misc类型题有很大的作用。他也可以通过查看文件的头部来判断文件类型。

常见文件头

类型	文件头	文件尾
JPEG (jpg)	FFD8FF	FFD9
PNG (png)	89504E47	0000000049454E44AE426082
GIF (gif)	47494638	3B
ZIP Archive (zip)	504B0304	00000000
TIFF (tif)	49492A00	
Windows Bitmap (bmp)	424D	
CAD (dwg)	41433130	
Adobe Photoshop (psd)	38425053	
Rich Text Format (rtf)	7B5C727466	
XML (xml)	3C3F786D6C	
HTML (html)	68746D6C3E	
Email [thorough only] (eml)	44656C69766572792D646174653A	
Outlook Express (dbx)	CFAD12FEC5FD746F	
Outlook (pst)	2142444E	
MS Word/Excel (xls.or.doc)	D0CF11E0	
MS Access (mdb)	5374616E64617264204A	
WordPerfect (wpd)	FF575043	
Adobe Acrobat (pdf)	255044462D312E	

类型	文件头	文件尾
Quicken (qdf)	AC9EBD8F	
Windows Password (pwl)	E3828596	
RAR Archive (rar)	52617221	C43D7B00400700
Wave (wav)	57415645	
AVI (avi)	41564920	
Real Audio (ram)	2E7261FD	
Real Media (rm)	2E524D46	
MPEG (mpg)	000001BA	
MPEG (mpg)	000001B3	
Quicktime (mov)	6D6F6F76	
Windows Media (asf)	3026B2758E66CF11	
MIDI (mid)	4D546864	

文件分离

有一些CTF题目中会将目标文件隐藏在其他文件中，这个时候就需要我们对文件进行分离提取来得到我们所需要的文件。
文件分离一般可以使用Binwalk，foremost，dd，fcrackzip 以及WinHex

WinHex

使用WinHex来思想文件分离的方法很简单，将文件在WinHex中打开后，找到我们所要分离的那一部分内容的16进制将他另存一个文件就可以了。

Binwalk

kali是自带有Binwalk的，所以平时使用的时候我们并不需要专门去下载，打开kali就可以了。
命令详解
1.1、固件扫描

命令：binwalk firmware.bin
通过扫描能够智能地发现目标文件中包含的所有可识别的文件类型。

1.2、提取文件

命令：binwalk -e +文件名
选项“-e"和“–extract"用于按照定义的配置文件中的提取方法从固件中提取探测到的文件系统。

命令：binwalk -Me +文件名
选项“-M"和“–matryoshka"用于根据magic签名扫描结果进行递归提取，仅对"-e"和“–dd"选项有效。

命令：binwalk -Me -d 5 +文件名
选项“-d"和“–depth="用于限制递归提取深度，默认深度为8，仅当“-M"选项存在时有效。

命令 dd if=（原文件名） of=（提取文件名）skip=数据地址 bs=1

1.3、显示完整的扫描结果

命令：binwalk -I +文件名
选项"-I"和“–invalid"用于显示扫描的所有结果（即使是扫描过程中被定义为“invalid“的项）。当我们认为binwalk错把有效的文件当成无效文件时，可以通过该选项来检查。

---

foremost

foremost的使用和Binwalk相类似，foremost也是kali之后自带有的工具，在网上大部分也是linux版本，所以使用的时候也是打开kali就好了。

使用方法

> foremost +[参数] +[文件名]

命令详解
-V - 显示版权信息并退出
-t - 指定文件类型. (-t jpeg,pdf …)
-d - 打开间接块检测 (针对UNIX文件系统)
-i - 指定输入文件 (默认为标准输入)
-a - 写入所有的文件头部, 不执行错误检测(损坏文件)
-w - 向磁盘写入审计文件，不写入任何检测到的文件
-o - 设置输出目录 (默认为./output)
-c - 设置配置文件 (默认为foremost.conf)
-q - 启用快速模式. 在512字节边界执行搜索.
-Q - 启用安静模式. 禁用输出消息.
-v - 详细模式. 向屏幕上记录所有消息。

隐写总结

图片隐写

1.压缩包隐藏在图片中

有时候一些misc会将压缩包隐藏在一张图片之中，当我们在得到题目给我们的附件是一张图片时可以先看一看图片的大小，图片太大就会很可能藏有其他文件在图片中。
破解方法：
1.使用kali自带的Binwalk工具来检索图片文件里的其他文件，之后在使用foremost工具来将图片中的压缩包文件分离出来，也可以使用WinHex工具来将文件进行分离，不过WinHex工具相比于foremost工具使用起来会复杂有点。
2.可以直接将图片的后缀名改为zip，然后对文件进行解压。但是这个方法如果遇到图片中存在多个隐写文件的情况下回生效。

2.LSB隐写

LSB隐写又叫做最低有效位隐写，。图片中的像数一般是由三原色组 成，由这三种原色可以组成其他各种颜色，LSB 隐写就是修改了像数中的最低的 1bit，写入加密信息，而人眼无法注意到前后的变化。
遇到LSB隐写的题目，我们可以使用工具Stegsolve来进行破解。
Stegsolve是一个非常使用的隐写工具，下载也很方便，只要电脑拥有java环境就可以运行Stegsolve。

Stegsolve使用说明

在Stegsolve的工具栏中有三个选项，File，Analyse，Help。
File选项中有三个选项，Open（文件打开），Save As（文件保存），Exit（退出）
Analyse中有五个选项。

选项	功能
File Format	文件格式
Data Extract	数据提取
Steregram Solve	立体试图 可以左右控制偏移
Frame Browser	帧浏览器
Image Combiner	拼图，图片拼接

> Stegsolve使用教程
> https://www.cnblogs.com/cat47/p/11483478.html

3.文件格式缺失&GIF 隐写

这种类型可能是文件破损导致无法正常打开文件，这种时候我们可以用WinHex打开文件通过查看文件的十六进制内容来判断文件是否缺失，再进行补全。
