misc

原创

野九 于 2019-07-17 22:55:57 发布 1185 收藏 15
分类专栏： misc 文章标签： misc

本文链接：https://blog.csdn.net/qq_43613772/article/details/96377235


misc 专栏收录该内容
1 篇文章 0 订阅
订阅专栏

Misc 是英文 Miscellaneous 的前四个字母，杂项、混合体、大杂烩的意思。
Misc 在国外的比赛中其实又被具体划分为各个小块，有
Recon、Forensic、Stego、Misc…
在国内内的比赛中，被统一划分入 Misc 领域，有时 Crypto（尤其是古典密码）也被划入其中。

杂项大致有几种类型：
流量分析
隐写
压缩包处理
文件格式分析
攻击取证

主要介绍一些获取信息的渠道和一些利用百度、谷歌等搜索引擎的技巧
Encode（编码转换）
主要介绍在 CTF 比赛中一些常见的编码形式以及转换的技巧和常见方式
Forensic && Stego（数字取证 && 隐写分析）
隐写取证是 Misc 中最为重要的一块，包括文件分析、隐写、内存镜像分析和流量抓包分析等等，涉及巧妙的编码、隐藏数据、层层嵌套的文件中的文件，灵活利用搜索引擎获取所需要的信息等等。

CTF 中 Misc 与现实中的取证不同，现实中的取证很少会涉及巧妙的编码加密，数据隐藏，被分散嵌套在各处的文件字符串，或是其他脑洞类的 Chanllenge。很多时候是去精心恢复一个残损的文件，挖掘损坏硬盘中的蛛丝马迹,或者从内存镜像中抽取有用的信息。

现实的取证需要从业者能够找出间接的恶意行为证据：攻击者攻击系统的痕迹，或是内部威胁行为的痕迹。
实际工作中计算机取证大部分是从日志、内存、文件系统中找出犯罪线索，并找出与文件或文件系统中数据的关系。
而流量取证比起内容数据的分析，更注重元数据的分析，也就是当前不同端点间常用TLS加密的网络会话。

Misc 是切入 CTF 竞赛领域、培养兴趣的最佳入口。Misc 考察基本知识，对安全技能的各个层面都有不同程度的涉及，可以在很大程度上启发思维。（Misc题目也可称作脑洞题）

流量控制

CTF 比赛中,流量包的取证分析是另一项重要的考察方向。
通常比赛中会提供一个包含流量数据的 PCAP 文件，有时候也会需要选手们先进行修复或重构传输文件后，再进行分析。
PCAP 这一块作为重点考察方向，复杂的地方在于数据包里充满着大量无关的流量信息，因此如何分类和过滤数据是参赛者需要完成的工作。

主要工具是wireshark，需要熟练掌握使用方法，过滤器语法、追踪流、导出文件

文本格式分析

常见文件头和文件尾的16进制编码：
JPEG (jpg) 文件头：FFD8FF　文件尾：FF D9
PNG (png) 文件头：89504E47 文件尾：AE 42 60 82
GIF (gif) 文件头：47494638　文件尾：00 3B　　ZIP Archive (zip) 文件头：504B0304　　文件尾：50 4B
TIFF (tif)，文件头：49492A00
RAR Archive (rar)，文件头：52617221
Windows Bitmap (bmp)，　文件头：424D
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
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
…
杂项题目主要是以文件附件作为题目，但是给的文件不一定是有后缀名的，这就需要我们识别这些文件。

文件分离

介绍了文件类型的识别方法了，接下来来讲一下文件分离
文件分离的原因：
在CTF这个充满脑洞的比赛中，出题人往往会以一些稀奇古怪的出题方式出题，因此你可以常常看见暴打出题人等字眼出现在比赛论坛中。在CTF中一个文件中隐藏着另外其他文件的题目是经常有的。这就需要掌握文件分离的技巧来应对。

图片隐写

图像隐写术进行数据隐写分为以下几类：

1.在图片右击-属性-详细信息中隐藏数据信息；

2.将数据类型进行改写（rar类型数据 将其改写成jpg格式）；

3.根据各种类型图像的固定格式，隐藏数据修改图像开始标志，改变其原有图像格式，在图像结束标志后加入数据，在图像数据中假如数据，不影响视觉效果情况下修改像素数据，加入信息；

4.利用隐写算法将数据隐写到图像中而不影响图像（仅限于jpg图像），隐写算法常见有F5、Guess、JSteg和JPHide等。

特别是关于图片隐写的问题，一般有修改图片格式、图片大小、或者图片中隐藏着zip压缩包等内容，通过合理的分析，合理的工具帮助下可以很轻松拿到flag。