Misc入门培训指南

简介

Miss中文译为杂项，顾名思义，杂项并不像其他几个方向，有明确具体的学习方法和学习内容。 Misc甚至可以说是包含了所有除了其他4个方向以外的知识，当然。例如AI安全，IOT安全等都是既可以作为独立方向存在，也可以当作杂项的一部分，暂时不在我们讨论的范围之内。有兴趣的同学可以自行去搜寻相关知识。

当然，在那么多年的发展中，Misc衍生出来的轮子已经很多了，但是我们不能仅仅依靠轮子（某p是吧😡😡）去进行解题，也要去发掘背后的原理，尝试自行编码。相关工具的查找，我仅会在文档中写出工具名，查找请自行解决，找到最合适自己使用的。🤗🤗

CTF中的MISC

如果我们仅仅是讨论在CTF中的misc可以简单分为以下几个类型。

密码编码

在CTF中，misc这一部分将会出现多种多样与密码学相关的知识。考虑到有密码这一方向的存在，所以我们在此仅介绍一下部分古典密码和常见编码。

编码

进制转换

进制转换是人们利用符号来计数的方法。进制转换由一组数码符号和两个基本因素“基数”与“位权”构成。基数是指，进位计数制中所采用的数码（数制中用来表示“量”的符号）的个数。

在CTF中，我们常用的进制包括二进制，八进制，十进制，十六进制。

ASCII编码

ASCII码是对英语字符与二进制位之间的关系，做了统一规定。
基本的ASCII字符集共有128个字符，其中有96个可打印字符，包括常用的字母、数字、标点符号等。
ASCII码是一种用于表示字符的编码系统，它是计算机发展早期最常用的编码系统之一。
特征就是只含有数字。

Base家族

Base家族的成员有很多，比如：
base16,base32,base64,base85,base36,base58,base91,base92,base62等等

basexx中的xx表示的是采用多少个字符进行编码，比如说Base64就是采用64个字符进行编码。

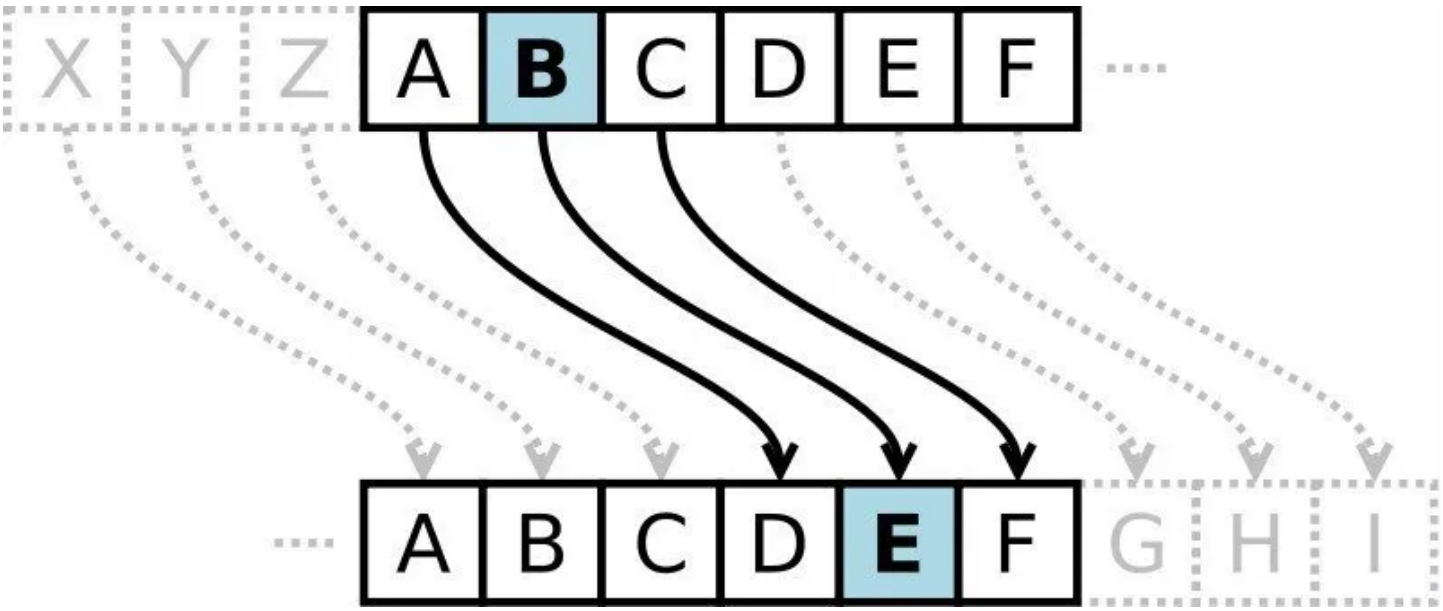
其中使用频率最高的就是Base64，末尾有等号是Base64一大特征，但是不是每个Base64编码后的结果都有等号，有等号的也不一定就是Base64。

古典密码

这里简单给大家介绍几种，更详细的建议转移至隔壁Crypto。<(￣ ≋ ￣)>

凯撒密码

凯撒密码作为一种最为古老的对称加密体制，在古罗马的时候都已经很流行，他的基本思想是：通过把字母移动一定的位数来实现加密和解密。明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推X将变成A，Y变成B，Z变成C。由此可见，位数就是凯撒密码加密和解密的密钥。



摩斯密码

摩尔斯电码是一种早期的数字化通信形式，它的代码包括点、划、点和划之间的停顿。

图文对照密码

经常会有出现独创的特殊图文对照密码，如提瓦特大陆上特殊语言（原神！！！启动！！！）（ps:有些不妙的回忆涌上心头）

压缩包密码破解

这里往往是压缩包存在密码，包括在zip和rar等格式。对此，针对不同情况可以尝试暴力枚举，明文攻击等方法。😌

隐写

与加密技术相比，隐写术的主要特点包括： 隐藏传输的信息是嵌入在一个看似无关联的载体上进行的。最早追溯到自然界动植物的拟态，去隐藏自身的存在，而现在的发展更加多样化。我们下面所提

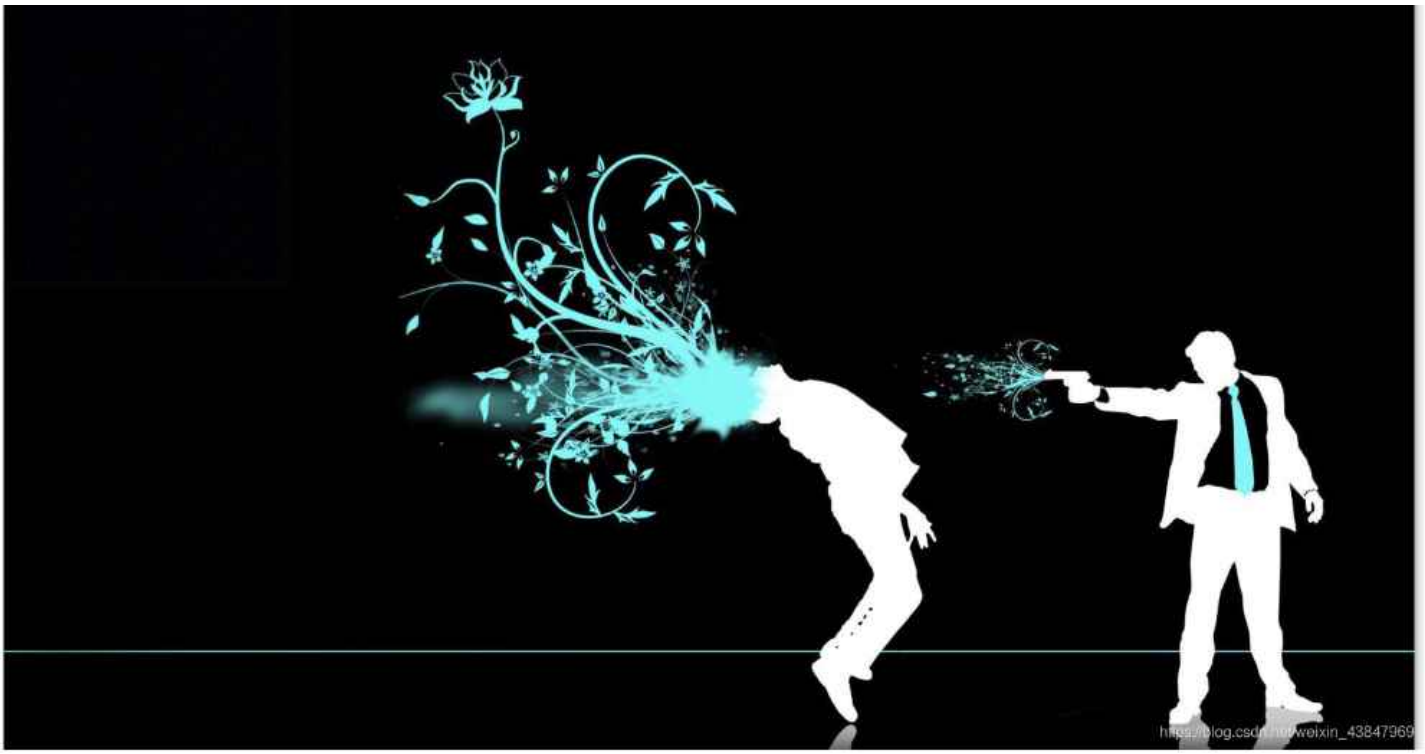
到的只是最常见的几种类型，更多的欢迎自行探索。😚

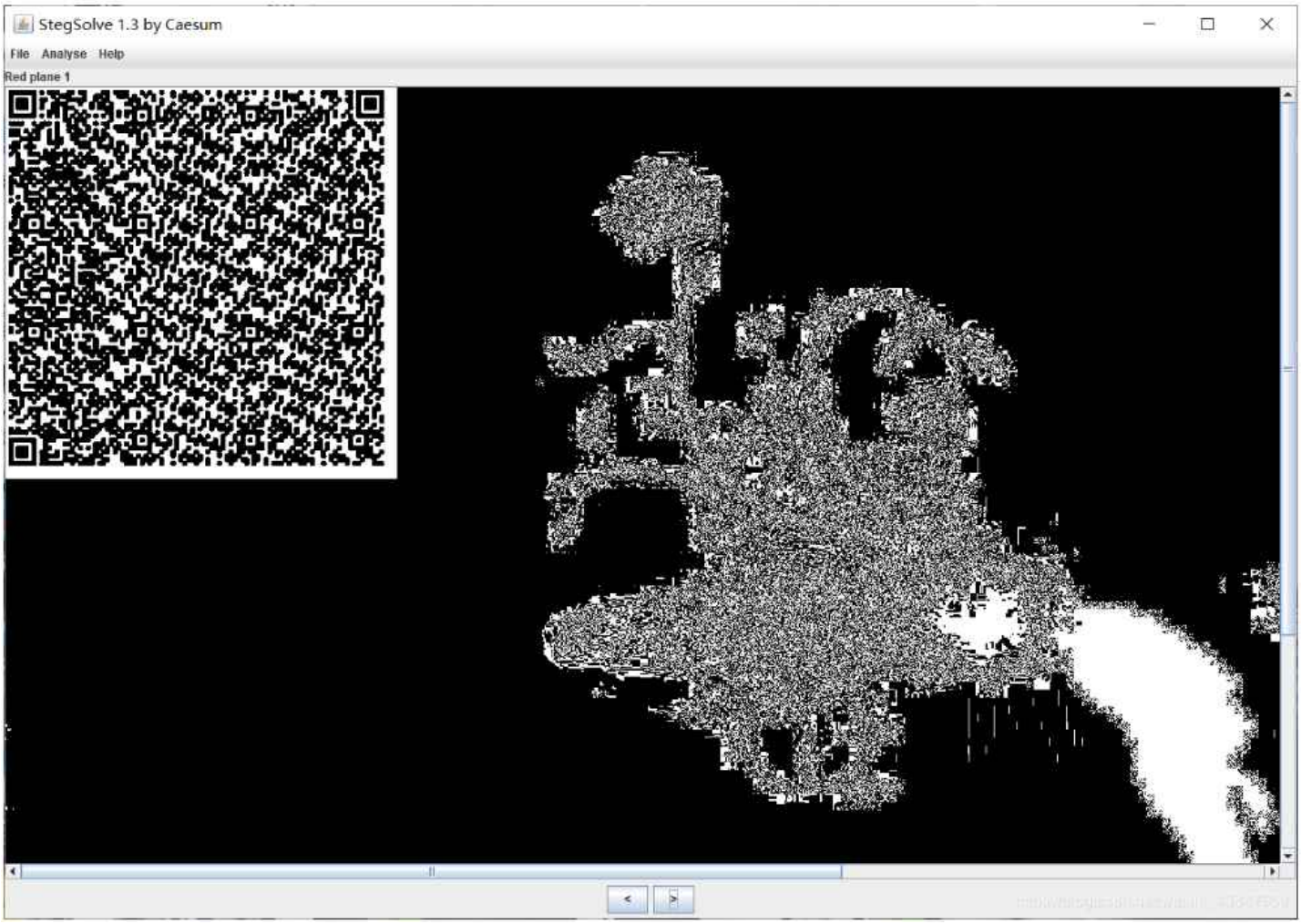
图片隐写

图片一些我们可以理解为在一张图片中隐藏我们所想要的信息。在这里我们只提一种叫lsb隐写作为例子。

以下就是使用了lsb隐写将二维码藏在了一张看似普通的图片里，更多内容希望能自行去探索。

图片中使用的工具叫stegsolve，看看能不能自行配置使用哦😜😜！





音频隐写

音频隐写往往会使用au作为工具，可能是音频本身就是线索，也或者藏在频谱图甚至不同声道中😏😏。

流量分析

流量分析中会给予我们一些pcapng或pcap文件后缀的数据。不同的数据包有不同的协议，常见的有HTTP，TCP协议，我们所要用的工具叫做Wireshark。（ps:好好好，流量分析杯欢迎来玩！题目找学长来要😋😋😋）

电子取证

电子取证包含了硬盘取证，手机取证，内存取证等等。

在这里，仅提及一种内存取证，在CTF比赛中比较常见。此类题一般会给出raw文件、vmem文件、img文件、dmp文件等内存镜像文件，我们则需要用volatility来解决这种问题。（有兴趣的同学先去试试看能不能成功配置好volatility这个基础工具）

当然了，这只是最基础的几个类型，其余还有很多很多都没有在文档中全部写出来。那这时候有同学要问了，该怎么学习misc呢？那请继续往下看。

Misc入门学习

提到学习，这时候有些同学可能开始困了

但是，对于misc的学习，我们不需要强调有多么标准的流程，两大基础，两大方法。

两大基础指的是编程基础和思维基础，两大方法指的是刷题（CTF）和看博客（多抱抱师傅大腿）。除此之外，就是我们最最最强调的搜索的能力。这里并不详细说明，大家有时间可以去看看百度甚至谷歌（科学上网哈）的高级搜索语法。

环境搭建

不仅仅是misc，在其他方向上，也都需要基础环境的搭建，所以建议大家不仅要熟悉windows系统的基础操作，也要尝试搭建linux系统，我们常用的kali和ubuntu都是不错的选择。

当然，对于搭建过程，存在着不少小问题，我希望你们能够自己尝试解决，这对于你们是初步地一个成长过程。

搭建完成之后，可以尝试通过安装一个小工具foremost去进一步熟悉linux系统的操作和指令。

总结

与其他方向相比，misc是最具有趣味性，对于大多数入门的新手是个不错的选择，欢迎大家来尝试对misc的学习。