Misc(安全杂项) 入门指北

by E=hv

首先，欢迎大家来到misc的世界！

~~什么？？你就是来找flag的？那也行，最底下自己找去（无感情）。~~

Misc是什么?

“当一道题，既不是Web，也不是Reverse, Pwn或者Crypto时，那么它就是Misc”。Misc 是英文 Miscellaneous 的前四个字母，杂项、混合体、大杂烩的意思。当一道题不好分到别的方向时，就会被分到misc里（确信）。如同名字一样，这个方向包括了很多方面的内容，比如Recon（信息搜集），Forensics（取证分析），Stego（隐写），还有近几年比较流行的Blockchain（区块链），等等。

作为CTF题目中的“大杂烩”，misc方向的题目会有很多出题人的奇思妙想~~（创 大 新 思 路）~~，也会涉及到一些有趣的小知识点。misc的题目可以是一张平平无奇的图片，可以是一段美妙的音乐，还可以是有趣的游戏。~~（甚至还会直接让你猜flag，当然我们的出题人不会做这种无聊的事情。）~~

Misc难度如何?

如果你想入坑CTF，那么对于零基础的同学们，misc绝对是你最好的选择，你可以在很短的时间内（就比如moectf2025这段时间）学到很多知识。

misc不一定是最难的方向，但一定是最会整活的方向。misc可能不需要你对某个方向的知识有非常深入的了解，但是需要我们对每一个方向的知识都有涉猎~~（misc手大均全栈（？）~~，有的时候甚至需要一点点游戏知识。同时悄悄说一句，在探索misc的世界时，了解一些别的方向的知识对解题会有很大帮助哦。

此外，misc也很考验你学习新知识的能力，有时候一道misc题可能会考到一个不常见的传输协议，又或者是图像处理等等陌生领域的知识，这时候就需要你去“现学现卖”，有的时候一个题可能一个队伍都解不出来~~（呜呜呜我又爆零了）~~。

如何入门Misc?

misc相较于其他方向的入门还是很友好的，就算你之前是不怎么会用电脑的小白，入门misc也不会有太大的阻碍，还可以学会很多东西哦！

前期学习misc方向的内容，可以跟着本次比赛的题目，去见识一下misc各个小类别的常见考点，这些考点通过做题就可以很好的掌握。在做题的过程中，你需要利用搜索引擎（Bing或者Google等），寻找相关资料，你可能会找到和这次赛题解题思路类似的题目，跟着题解的思路复现，再加上一点点变通，很容易就能解出来。也有可能，这道题你啥思路都没有，这时候你可以再仔细看看题目描述或者附件，里面的每个字都有可能藏着解出这道题的关键提示！

当你觉得自己对misc方向已经有了不错的了解，就可以考虑深入学习取证，流量分析等等方面的内容，或许你能从中找到乐趣！

当然，在做题之前，我们需要有一定的计算机知识，这些知识可以提前学好再去做题，也可以在做题过程中边做边学（个人推荐后者）。

学会使用虚拟机!

虚拟机是一个强大的工具，创建一个虚拟机，就相当于你多了一台“独立的电脑”，你甚至可以创建不同操作系统的虚拟机，并且在两者之间自由的交换文件！有的时候，题目或者工具的运行环境和本机不一样，这时候虚拟机就派上用场了，你可以在一台电脑上，运行来自不同操作系统的程序。

虚拟机软件我用的是vmware，WSL也基本可以满足在windows上面使用Linux操作系统的需要，具体的安装使用教程网上多如牛毛，这里就不详细展开了。

认识Linux!

Linux是一种开源的类UNIX操作系统内核，运行速度远超Windows系统，只要在终端里敲敲键盘就能完成几乎所有工作。（黑客在电脑上疯狂敲键盘黑入系统的样子离你似乎不是很远？）

尝试一下？可以试试安装Ubuntu，Fedora，Debian等等，然后，熟悉一下Linux指令！总不能千辛万苦getshell之后，发现自己不懂shell指令，获取不了flag吧。

如果你已经足够熟悉了Linux，那么可以试试Kali Linux，里面有很多CTFer常用的工具，并且安装即用，省去了大部分配置环境的麻烦事。遇到困难的时候，可以利用搜索引擎，搜索报错的内容，网上会有很多人遇到相似的问题，并且他们很有可能已经有了解决方案！有时候，问问大语言模型也可能有奇效哦。

学会一门编程语言!

misc经常会出现需要编程对文件进行数据处理的情况，这时候学的编程语言就派上用场了。对于从未接触过编程的同学，推荐先学python，因为它短小而通俗易懂。学习编程语言，首先要了解各种逻辑的执行方式，分支，循环等等，然后了解对应的代码写法，再尝试着使用代码来实现一些简单的功能，甚至可以写写游戏，当你做的差不多时，恭喜你，这么编程语言已经可以为你所用了。

当然，python不止于此。在misc中，有一种专门针对python语言的题目（pyjail），你需要通过执行有一系列限制条件的python代码获取远程靶机的shell权限，这也是一类很有意思的题哦！

Misc都有啥类型的题?

Recon（信息搜集）

“朋友圈随手发了张图，结果人家连我坐的哪趟列车都知道了？！”信息搜集的题就是如此，通过照片或者文字描述的一点点蛛丝马迹，就可以推断出很多有价值的信息，对于这种题，我们也有很多工具，比如国内的百度地图，国外的Google地图，百度识图等等，甚至是实 (xian) 地 (xia) 考 (zhen) 察 (shi)，都可以给你意想不到的收获。比如去年的moe新生赛要找一个画刊上的内容，主播在网上找了半天最后惊奇的发现西电的图书馆里居然就有！~~信息搜集的尽头是线下真实~~

Game（游戏）

“不是？为啥大嘿客还要会玩游戏啊？”在misc里，你甚至可以玩游戏，然后就能拿到flag了，是不是很好玩？这类题目一般是要求在游戏中达成相关条件来获得flag。有时候这些条件不是正常人类可以达成的，这时候就要使用一些大嘿阔的手段了（读源代码？放心，基本上点击就送）。（甚至有机会玩到出题人精心设计的rpg游戏！）

Forensics（取证分析）

“一个内存镜像，破解出了我妈给我电脑设的开机密码！”取证就是对转储下来的内存或者磁盘的内容进行分析，从中提取信息。通过内存分析，我们可以获得很多有用的信息，比如刚刚输入了啥命令，桌面上有什么东西，甚至是开机密码，都可以知道。内存分析常用的软件是volatility，磁盘取证常用的有VeraCrypt（处理加密卷），Elcomsoft Forensic Disk Decryptor等等，还有vmware（有时候会给你扔一整个虚拟机来分析。~~4G的超大附件vs百度网盘~~）

Stego（隐写）

“看上去只是一张普通的图片，里面居然藏了两个小时的视频？？”隐写就是这么神奇。能藏的东西的地方可多了，图片，音频，视频，压缩包，甚至一段文本，啥类型的文件都能找到藏东西的办法！如何破除“障目”之法？使用16进制编辑器（WinHex或010 Editor）一个个字节地看！有时候找到一些文件的关键位置就能发现端倪。图片隐写的话，可以使用StegSolve，功能比较齐全。至于其他类型的文件又或者是使用特殊算法隐藏内容的隐写，就留给大家自己探索吧！搜索图片/音频/视频隐写等等，可以找到很多很有用的资料！

Traffic（流量分析）

“为什么我偷偷发了点奇奇怪怪的东西就被警察蜀黍发现了TAT”流量分析就是通过捕获网络中的流量包，分析协议等等，可以获取传输的各种文件，或者是通信的设备名称。在CTF中，这类题目大多是给一个捕获的流量包（*.pcap/*.pcapng），然后从中分析数据，但是难点在于如何定位到我们需要的那部分传输文件等等的流量。

当然，流量并不全是明文传输的，有的流量是经过加密的，这时候就需要一些其他的手段来解密流量。

流量分析常用的工具是Wireshark，下面自带的工具tshark也很有用，可以去网上搜搜如何使用哦！

Encoding（编码）

“期待好久的游戏终于更新了！欸？怎么更新预告里有一堆奇奇怪怪的字符？评论区咋都解密出来了？”编码便是解密中不可或缺的一部分。编码是把明文信息通过某种规则转换成另一种形式，而解码就是把编码信息按照解码规则转化为明文。比如经典的摩斯密码（Morse Code），将字母和一些标点转换成电波的长音和短音。常见的编码也不止这些，比如base64，base58等base系列，还有各种奇奇怪怪的汉字，等等，又或者是奇形怪状的符号。这些在网上大多都能找到解码网站或者明文对照表，就可以解出背后的秘密啦！

base64编码算是最常见的一种了。编码的结果是大小写字母或数字或/+=，结尾一般有1-2个等号。具体编码方式可以自行搜索了解一下^_^

对于一大部分密文，可以使用一下CyberChef，可以解决大多数常用编码。还可以试试Ciphey（在未知编码或加密算法的时候可以用来碰碰运气，比CyberChef的魔法棒更强）

再吧啦几句

如何更快提升自己

题目看不懂？不知道从何下手？或许可以自己找一些题目自己练练手，或许就对misc方向的考点更加得心应手了。可以去 buuctf 或者 攻防世界 上找一些题目做做，可以先从简单的题目（一般解出人数最多）上手，如果完全没有思路的话可以看看题解，因为做不出来有可能是题目涉及到了你之前没见过的考点，直接去看题解可以帮助你更快地掌握知识！当然，你也可以选择不看题解来锻炼自己的解题思维，总之，哪种方法适合你就这样去做！

工具的获取

随着misc题做得越来越多，你会接触到各种各样的工具，这些工具大多可以从GitHub上下载，或者有专门的官方网站。但是有一些商业软件是要付费的，可以到一些网站上寻找破解版，但是不一定安全。

一些有用的东西

吾爱破解论坛：可以找到破解软件，以及一些有关于安全的讨论帖子

CTF-OS

CTF Wiki

讲了这么多，好像忘记了一件重要的事儿，哦对了，我忘了给你flag了！

想要flag？到下面↓↓↓找找看吧，据说只有聪明的人才能看到flag哟QwQ

什么？没看到？让我想想……我是把flag一个个**打上去的**，实在不行就在文档里**查找一下**吧，flag格式是**moectf{xxx}**哦