# Misc方向指北

一定要好好看这个文档，一定一定，它对之后的学习以及后面的许多题都有帮助的，不要打开拿了flag就丢掉！(⌐■_■)

# Misc简介

Misc是Miscellaneous的缩写，意思是杂项、混合体。

它涉及安全技能的各个层面（但不是全部嗷，考验知识的深度广度，当然更包括你在有限时间内的学习理解能力，可以很大程度的启发思维，很适合刚刚接触CTF的师傅们入手（也要去其他方向看看嗷。

虽然涉猎广泛，但Misc方向会有较为宏观的分块，比如：

- Recon（信息搜集）（也就是常说的社工题
- Encode/Decode（编码）
- Archives（压缩包）
- Steganography（隐写）
- Forensic（取证）
- Traffic（流量分析）
- 有些时候会涉及到古典密码 （引路Classic cryptography方向题目）

后面会一一介绍它们的，现在先唠一些题外话。Misc方向的题难度跨度很大，经典而简单的直接签到成功，而难的直接击打知识盲区，区块链、深度学习、单片机、通信原理balabala，在拓展知识面且深入了解方面很有帮助（点头，不过**Moectf 2022**作为**入门比赛**，在Misc方向题目的设置大都比较**经典简单**，**对于零基础来说也没有问题**，条件大概只有一个，**多搜多问**，学会高度利用搜索引擎，遇到搜不到解决不了的问题要勇敢的去找同级大佬或者学长学姐请教（ 提问的智慧 ），相信你们会收获很多。

**最重要的是，一定要多写题，要实操，要上手，不要只看理论知识，没有自己用出手的就不是自己的。**

# 分块简介

## Recon（信息搜集）

调动你的各种搜索引擎和途径，找它搜它翻它！

一些可能会有用的信息搜集技巧和搜索技巧：（摘自CTF-wiki）

- 公开渠道
- 目标web网页、地理位置、相关组织
- 组织结构和人员、个人资料、电话、电子邮件

- 社会公共信息库查询
- Google基本搜索和挖掘技巧（科学上网
- 地图与街景：Google Map、Google Earth、百度/高德地图、whois数据库等

其实在CTF比赛中社工题更像是推理搜证，会有线索、指向性提示，还是挺好玩的嘞。

## Encode/Decode（编码）

各种奇奇怪怪的乱码可能是flag经过某些规则编码后的样子，多多熟悉它们，在各个方向都可能出现。

从相对更熟知的讲起：**Morse编码（摩尔斯电码）**

谍战片里电台之间发送信息会出现的编码方式：.... . .-.. .-.. --- （HELLO）

只有.和-（也可以用01串表示），不同的点和划的组合代表不同的字母数字符号，网上可以搜到摩尔斯电码对照表、在线的转换工具、解码脚本（用自己编写的程序运行获得结果）。

接着介绍计算机常用编码方式：**ASCII、Unicode、HTML实体编码**

首先需要一些前置知识：计算机中的数据都是按字节（Byte）储存的。一个字节由8个二进制位（bit）组成（如果对进制不熟悉可以去搜一下）。（组成范围是0~255）

一个字节一共可以表示256中不同的状态（8个二进制位，每位有0或1两种选择，排列组合问题），每一种状态对应一个符号，就是256个符号，从00000000到11111111。

- ASCII编码

它是英文字符与8位二进制位之间的关系，是统一规定的。

基本的ASCII字符集共有128个字符，其中96个可打印字符，包括常用的字母、数字、标点，比如大写字母A是65（二进制：01000001 十六进制：0x41）

可以很容易的搜索到ASCII在线解码、ASCII码对照表等。

- Unicode

也叫统一码、万国码、单一码，是国际组织指定的旨在容纳全球所有字符的编码方案。使用两个字节来编码一个字符，字符编码一般使用十六进制。比如，U+0639表示阿拉伯字母Ain，U+0041表示英语大写字母A，U+4E25表示汉字 严 。

这篇笔记 介绍了ASCII、Unicode以及UTF-8。

- HTML实体编码

用一个编号写入HTML代码中来代替一个字符，在使用浏览器访问网页时会将这个编号解析为字符查看。比如大写字母A的HTML实体化为A。

对编码有一个初步的认知之后，除了Morse编码，还有很多编码方式：

- 电话拨号编码（电话拨号九宫格可以表示字母或者拼音）
- Tap code敲击码（把字母放进5*5方格中用坐标位置表示字母，敲击次数表示坐标）
- Base16/base32/base64/base58/base85/base100（其中以base64最为常见）
- MD5、SHA1等类似加密型
- URL编码
- Hex编码
- Js颜文字加密/Jother/JSFuck
- XXencode
- Aaencode
- 社会主义编码
- 与佛论禅
- 兽音译者

  `~呜嗷呜啊嗷呜嗷啊嗷呜啊嗷嗷~啊啊~~嗷嗷呜啊嗷啊呜呜嗷啊呜嗷呜嗷呜嗷啊嗷~啊啊啊~呜啊嗷嗷~呜啊呜嗷~呜呜嗷啊呜呜嗷嗷呜~~啊呜嗷呜呜嗷~~啊啊啊呜啊`

不同的编码有它自己不同的特征，见多了之后根据经验可以判断它是什么编码，在这之前，moe的比赛编码题会有提示的。

一篇较全的编码介绍

这个工具CyberChef或许你会喜欢

## Archives（压缩包）

压缩包打不开怎么题目都拿不到呜呜

- 压缩包伪加密
- 压缩包密码爆破/CRC32碰撞（工具有archpr、hashcat、bkcrack）
- 文件头修复（每种文件都有自己的标准文件格式）

## Steganography（隐写）

一张图片/一段音频/一个？？？里面能藏啥

隐写是很经典的Misc题啦，一般是要检查一个文件（图片、音频、什么都有可能），找到隐藏在里面的信息，藏信息的时候会利用这个文件的特性，比如音频的鼓点、图片的像素等等，隐写的方式很多，网上搜搜可以获得不少教程，但是建议学一学经常用来考隐写的文件的格式，这会有不少帮助。最常见的就是图片隐写和音频隐写啦，去探索一下叭！

010 Editor 推荐的十六进制编辑器

不同的隐写方式也会有不同的工具或脚本使用，发挥搜索引擎的最大作用喔

## Forensics（取证）

是很带感的东西喔！

电子数据取证是指能够为法庭接受的、足够可靠和有说服力的、存在于计算机和相关外设中的电子证据的确定、收集、保护、分析、归档以及法庭出示的过程。（这个方向是有专门的比赛的）

CTF中的取证分为硬盘取证和内存取证，题目会告诉你想要什么证据，而我们负责恢复、搜查、获得证据，需要掌握的知识包括并不限于Windows、MacOS、UNIX/Linux、移动终端、网络数据取证的基本知识和取证技术、电子数据取证的相关法律规则和标准等等

- 内存取证文件后缀一般为.raw/.img/.vmem，常用volatility进行分析
- 硬盘取证文件后缀.vmdk，常用X-ways Forensics进行分析，veracrypt可以用来挂载磁盘文件，也可以用来加密磁盘，FTK也是常用的挂载软件

这里可以了解更多。

## Traffic（流量分析）

需要一些前置知识的板块，许多名词如果看不懂一定要去多查一下(。・∀・)ノ

流量分析是指捕捉网络中流动的数据包，并通过查看包内部数据以及进行相关的协议、 流量分析 、统计等来发现网络运行过程中出现的问题。通常在CTF比赛中会拿到一个.pcap/.pcapng文件，它是由捕获的网络流量形成的，而考点在于利用流量分析工具，抓取网络请求中的各种流量数据包，分析信息，并得到所需的有用信息（flag）。

- 流量分析工具wireshark
- 需要了解网络协议相关知识及其对应流量
- 题型大致分为网络流量分析和USB流量分析

认识一下OSI七层模型

流量分析入门

wireshark使用

## Classic cryptography（古典密码）

Moectf 2022 有单独开设此方向的题喔，可以去看看

密码学（Cryptography）大致可分为古典密码学（Classic cryptography）和现代密码学（Modern cryptography），两者的主要差别在于计算机的使用，一般来说，古典密码学是基于字符的，而现代密码学是基于二进制位的。古典密码相对来说好上手，更容易理解，所以入门可以去看看。

古典密码集合

大概就是这些啦，希望接下来的你发现兴趣所在，然后坚持下去。

有自己找不到、解决不了的问题可以去戳群里的misc-hypnotics

.-- . .-.. ..--- --- -- . ..--.- ....- --- ..--.- -- .. ...-- -.-. ..--.- .---- ..- -.-. -.- -.-- -.-.--