CTF Misc

Misc是英文Miscellaneous的前四个字母，意思是混杂的，中文即“杂项”。

这部分对安全技能的各个层面都有不同程度的涉及。Misc题目还会涉及到许多脑洞、花式技巧，有时也考验解题者的学习能力、临场反应等等。

Misc常涉及到的知识包括编码分析、隐写术（文本、图片、音频、视频等文件隐写）、流量分析、压缩包分析、内存分析、社会工程。

**关于Misc的学习：**

1.基础知识：

CTF Wiki（ctf-wiki.org）网站中，对CTF比赛中各部分都有相对系统地介绍，且在不断更新。大家在学习Misc部分时，可以以网站中的目录作为学习路线。

另外，在平时练习与比赛后，大家可以多关注其他选手发布的writeup，其中也能积累到一些知识或经验。

2.练习实践：

许多CTF OJ平台保有许多赛题环境供大家练习与学习。这里列出3个相对流行的OJ平台：

BUUCTF（buuoj.cn）

Bugku（www.bugku.com）

CTFHub（www.ctfhub.com）

（还有许多OJ平台，大家可以自行搜索）

建议刚刚开始尝试CTF的同学，优先选择这些OJ平台。这些平台的许多题目在网上可以找到许多内容相对细致、知识丰富的writeup。这样，在解不出题目时，也方便借鉴学习一下别人的解法并积累知识。同时，在练习的过程中，也要不断复盘与总结。

另外，大家可以多关注一些CTF比赛平台，如：BUUCTF的竞赛中心，i春秋的赛事服务，CTFHub的竞赛中心等等。每个月都会有大大小小许多CTF比赛，大家可以在比赛中学习，体验比赛过程。

**一些准备：**

1.一些常用工具：010Editor、winhex、Wireshark、volatility、binwalk、foremost、Stegsolve、SilentEye、Deepsound、Ziperello、ARCHPR等等。

2.配置python、java环境。

3.安装Kali Linux虚拟机。

（一些工具的安装配置需要先完成2、3）

4.学习python

参加CTF比赛能帮助我们了解安全，但CTF比赛不是安全学习的全部。希望大家都能在参加CTF的过程中，学习知识，打磨技术，找到自己的兴趣与方向。