

CTF (Capture The Flag)

原创

Starzkg 于 2019-07-05 22:15:31 发布 907 收藏

文章标签: [CTF 简介](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43272781/article/details/94772059

版权

CTF是一种流行的信息安全竞赛形式, 其英文名可直译为“夺得Flag”, 也可意译为“夺旗赛”。其大致流程是, 参赛团队之间通过进行攻防对抗、程序分析等形式, 率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容, 并将其提交给主办方, 从而夺得分数。为了方便称呼, 我们把这样的内容称之为“Flag”。

CTF竞赛模式具体分为以下三类:

一、解题模式 (Jeopardy)

在解题模式CTF赛制中, 参赛队伍可以通过互联网或者现场网络参与, 这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似, 以解决网络安全技术挑战题目的分值和时间来排名, 通常用于在线选拔赛。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

二、攻防模式 (Attack-Defense)

在攻防模式CTF赛制中, 参赛队伍在网络空间互相进行攻击和防守, 挖掘网络服务漏洞并攻击对手服务来得分, 修补自身服务漏洞进行防御来避免丢分。攻防模式CTF赛制可以实时通过得分反映出比赛情况, 最终也以得分直接分出胜负, 是一种竞争激烈, 具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中, 不仅仅是比参赛队员的智力和技术, 也比体力 (因为比赛一般都会持续48小时及以上), 同时也比团队之间的分工配合与合作。

三、混合模式 (Mix)

结合了解题模式与攻防模式的CTF赛制, 比如参赛队伍通过解题可以获取一些初始分数, 然后通过攻防对抗进行得分增减的零和游戏, 最终以得分高低分出胜负。采用混合模式CTF赛制的典型代表如iCTF国际CTF竞赛。