2022 年第三届“网鼎杯”网络安全大赛
赛制简介

CTF 夺旗赛、AWD Plus 攻防赛、平行仿真靶场赛、RHG 人工智能漏洞挖掘赛以及 RDG 实景防御赛是目前网络安全竞赛中的主流赛事，本届“网鼎杯”将会在不同比赛阶段采用以下的一种及几种赛制相结合的方式展开竞技。

1．CTF 夺旗赛

CTF 是目前国际上较为流行的信息安全竞赛形式，其英文名为“Capture The Flag”，中文一般翻译为“夺旗赛”。CTF 比赛是将典型的有缺陷的网络环境抽象成对应技术点和应用的赛题，并通过预置 flag 的方式来验证选手是否可以分析场景，解析漏洞并利用漏洞。以此来考验选手们网络安全技术的实际掌握情况。

比赛过程中，参赛团队之间通过进行程序分析等形式，率先从主办方给出的比赛环境中得到一串具有特定格式的字符串（一般称为 flag）或其他内容，并将其提交给平台，从而夺得分数。

2．AWD Plus 攻防赛

AWD Plus 攻防赛模式是一种综合考核参赛团队发现攻击、有效防御的技术能力和即时策略的比赛模式。该比赛模式是通过抽象的网络环境，加入真实网络安全防护设备设施，模拟政府、企业、院校等单位的典型网络结构和配置，

相比传统的网络拓扑渗透竞赛场景，这种模式每个参赛队互为攻击方和防守方，是对传统赛制的改进和革新，更接近实景训练。其主要特点为：比赛强调实操性、实时性、对抗性，对竞赛队的渗透能力和防护能力进行综合全面的考量。

3．平行仿真靶场赛

平行仿真靶场赛是把真实的业务场景跟复杂的网络结构抽象到比赛环境中的一种赛制。参赛选手需要扮演渗透测试团队，按照参赛任务的要求，渗透到指定的网络环境中获取关键资产。平行仿真靶场赛中弱化了题目的概念，而更加强调和实际业务场景结合。因此完成渗透测试任务的过程不是唯一的路径，可以帮助网警、刑侦人员提升对实际犯罪场景问题的发现和解决的能力。

4．RHG 人工智能漏洞挖掘赛

RHG 意为 Robot Hacking Game，RHG 竞赛是目前全球第二个，国内第一个人工智能网络安全竞赛。

在本届“网鼎杯”中，机器人程序通过平台的特定接口获取赛题信息，并下载每道赛题的二进制文件在本地进行漏洞分析、挖掘和服务器权限获取。在靶场平台内，靶场会为每个战队分配特定的虚拟靶机作为赛题的运行环境，每道赛题在对应的靶机上开放特定的端口提供网络服务，战队机器人可直接与赛题

通信进行漏洞利用获取该题目的 flag。每只战队的靶机相互隔离，战队机器人的网络也相互隔离，保证每个机器人拥有安全独立的比赛环境。在半决赛前，将公开 RHG 平台介绍及接口文档。

5．RDG 实景防御赛

实景防御赛（Real Defense Game/RDG）中，每个参赛队伍拥有独立实景防御环境，实景防御环境中存在若干容器，每个容器存在不同的漏洞或是服务异常点。选手可通过进入所在队伍的实景环境，进行漏洞和异常服务的排查和修补，从而获得防御分数。选手需要在高度贴近实践的场景环境中，分析场景线索、解决实际问题、强化防御技能。该模式可培养和选拔更多具备实景防御等综合能力的守护型人才。