基于“学练训赛”一体的网络安全人才培养探索与实践*

苏婷[1] 蒋琳[2] 汪花梅[1] 杨扬[1]

1. 哈尔滨工业大学（深圳）实验与创新实践教育中心，深圳，518100
2. 哈尔滨工业大学（深圳）信息学部计算机科学与技术学院，深圳，518100

摘 要 CTF(Capture The Flag) 竞赛作为提高网络安全人才培养质量的重要方式，在网络安全人才培养方面的作用越来越突出。针对 CTF 竞赛考察的知识模块多而杂、实战对抗能力要求高等问题，分层次开展基于 CTF 竞赛的网络安全攻防实践课程教学；搭建竞赛实训平台，提高学生实践能力；将基于豆包大模型的智能体有效融入课程教学当中，探索人机协同教学模式；并在全过程融入思政元素形成“学-练-训-赛”逐层递进的网络安全人才培养模式。这些措施在提升学生兴趣、提高课程质量和培养学生竞赛能力方面取得了一定的效果。

关键字 CTF 竞赛；智能体；人机协同；思政育人；实践教学

Teaching Practice of CTF-Based Cybersecurity Attack and Defense Competition Courses

Ting Su Lin Jiang (corresponding author)

Education Center of Experiments and Innovations
Harbin Institute of Technology ShenZhen
ShenZhen 518100,China

College of Computer Science and Technology
Harbin Institute of Technology ShenZhen
ShenZhen 518100,China

Huamei Wang Yang Yang
Education Center of Experiments and Innovations
Harbin Institute of Technology ShenZhen
ShenZhen 518100,China

Abstract—As an important way to improve the quality of network security talent cultivation, CTF competition plays an increasingly prominent role in network security talent cultivation. To address the issues of multiple and diverse knowledge modules and high requirements for practical combat abilities in CTF competitions, a network security attack and defense practical course teaching based on CTF competitions will be carried out in a hierarchical manner; Building a competition training platform to enhance students' practical abilities; Effectively integrating intelligent agents based on the Big Bean Bun Model into curriculum teaching and exploring human-machine collaborative teaching models; And integrate ideological and political elements throughout the entire process to form a progressive network security talent training model of Combining Learning, Training and Competition. These measures have yielded certain results in stimulating students' interest, improving course quality, and cultivating students' competition skills.

Keywords—CTF competition, Intelligent agents, Human-machine collaboration, Ideological and political education, Practical teaching

1 引 言

当前，网络安全领域的问题日益突出，面临的挑战愈发复杂，网络空间安全已经成为国家安全保障体系的重要组成部分。保障国家网络空间安全，归根结底是要培养具备网络安全实战能力的人才。《网络安全人才实战能力白皮书》（简称白皮书）将网络安全人才实战能力归纳为“攻防实战能力”“漏洞挖掘能力”“工程开发能力”“战效评估能力”四种类型[1]。不同于传统技能的要求，网络安全人才更需要实战型人才，因此传统的人才培养模式，已不再适应高水平网络空间安全人才培养，必须在实践教学体系、教学资源建设等方面进行创新和改革。

自 2014 年起 CTF(Capture The Flag) 竞赛逐渐成为培养学生网络实战对抗能力的重要载体，中国科

*基金资助：哈尔滨工业大学深圳校区思政课程和课程思政专项建设项目，《网络安全攻防竞赛实践》，HITSZIP24011，2024.9-2026.9；高等教育教学改革项目（一般校本教研专题），基于 CTF 的网络安全攻防竞赛实践教学改革与探索，HITSZUQP24026，2024.10-2026.10

**通讯作者：蒋琳 zoeljiang@hit.edu.cn

学技术大学提出强化攻防演练，构建“赛、课、练”实战模式，建设网络安全实战型人才培养体系[2]；上海交通大学创设网安创新人才训练营 CITrip ，提出“以赛促学”的创新人才培养方法[3]；浙江大学为学生搭建网络安全攻防实验教学与实训平台，加强学生的实战技术水平，培养学生成为攻防兼备的复合型人才[4]；北京航天航空大学通过建设示范性实验实践教学平台、鼓励学生参加学科竞赛等一些列措施，探索网络空间安全卓越工程师培养模式[5]；国防科技大学将 CTF 竞赛融入网络安全人才培养的全过程，提出“更新培养理念、改革课程教学、突出实战对抗、多方联动聚力”的网络安全人才培养质量提升模式[6]；山东大学建立“X+ 安全”实训平台和竞赛平台，形成“以赛促学 + 以赛促训 + 以赛促研 + 以赛促用”的机制[7]；西北工业大学将 CTF 竞赛引入实践课程考核，建立“攻防兼备、分层归类、实践主导”的攻防能力培养体系,提升学生的攻防创新能力[8]；西安电子科技大学将实验、竞赛、实习、实战四线贯通，构建知识能力使命三位一体的一流网络安全人才培养体系[9]。

从总体上来看，国内各类高等院校通过 CTF 竞赛加强网络攻防平台的建设，推动网络空间安全系列课程的教学改革，提高网络安全实践教学水平，提升网络安全人才实战能力。但是网络安全人才培养任重而道远，既要满足我国在网络安全人才缺口的问题，又要解决“为谁培养人、培养什么样的人、怎样培养人”的问题。

2 实战型网络空间安全方向人才培养存在的问题

2.1 思政内容与教学内容不能有机融合

网络安全人才培养工作是网络强国建设的基石，掌握网络安全技术犹如手握一把“双刃剑”，学生的政治思想如果不过关，一旦面对网络中的一些诱惑怀有猎奇心理，或者没有法制法规概念涉足黑灰产业， 将对国家安全或社会稳定产生不良影响。因此高校有责任教育引导学生树立正确的网络安全观，提升学生网络文明素养等[10]。

目前高校在各个专业课程都将立德树人作为思政的根本目标，持续推进课程思政。但是还是存在课程内容和思政内容两张皮，不能将思政内容与课程内容有机融合的问题，主要体现在以下几点：一是思政内容与学生培养的目标要求结合不紧密；二是思政元素与课程特点、专业特色结合不紧密；三是思政形式单一生硬，灌输式、说教式思政为主要问题。

2.2 实训平台资源不够完善

传统教学过程对实践能力培养过程薄弱，缺少适应新需求的实践与创新平台，学生工程实践与创新能力不强。实战型网络空间安全方向人才的培养，需要打造面向学生的综合性实训平台和竞赛平台，目前各高校大都借助企业资源建设实训和竞赛平台，虽然能够帮助学生增强实践实训的机会，但是目前还存在资源不够完善的问题：一是同质化题目，各企业的题目内容基本相同,而且对于各类院校平台内容完全一样，没有根据学校的培养目标设置题目分类；二是题目更新不及时、题目难易层度不递进等问题；三是题目脱离真实业务场景，导致学生竞赛能力提升较慢；四是学生刷题情况得不到实时反馈,学生积极主动性不高。

另一方面，教师也需要看到学生的学习状况，了解每位学生的学习特点，因此实训平台除了满足学生的实训竞赛外，也需要看到整体学生的学生状况和学生之间的差异性，再根据实际情况调整授课内容和平台的赛题难易程度。

2.3 多方协同育人模式不成熟

实战型网络安全人才需要学校、企业和政府三方协同，当前，校企共建实践平台已经在各类高校实施推进，但是如何发挥学校、企业的各自优势并形成合力，尚需不断探索[11]。面向实战的网络对抗训练平台需要强大的软硬件支持，需要企业和院校协同参与才能建立符合学校学生特点的实训平台；而真实的业务场景则需要政府和企业给予学生更多的参与机会，比如政府经常组织的护网行动和企业的漏洞奖励等；网络空间安全是一个新兴专业，而且内容涉及众多其他学科，目前很多老师都不是出自网络安全专业，并且大都注重理论研究，实践经验也有所欠缺，需要学校老师和企业老师双师协同，共同参与实践教学；另外面对各类层出不穷的漏洞，网络安全攻防技术和工具也不断推陈出新，学生需要更多的学习成本，需要更加高效的学习、实训平台。

人工智能技术在教育教学领域得到广泛的应用，能够辅助教师和学生在网络空间安全领域进行知识生产[12]。人工智能技术能有效辅助教师开展差异教学、增强教学和协同教学，但是目前来看，教学中引入智能技术的力度还远远不够，主要还是停留在 MOOC、SPOC 课堂阶段，对于在教学过程中的应用还不广泛。今年 5 月份教育部公布首批 18 个“人工智能+高等教育”应用场景典型案例，要求高校加强研究交流，结合实际深化“人工智能+高等教育”的探索和实践，在人工智能技术的辅助下开展教育教学创新，推进人工智能在高等教育中的广泛应用，不断提升人才培养质量。因此人工智能+协助育人的方式也值得不断探索，最终形成多方合力协同育人模式。

3 基于CTF的网络安全攻防竞赛课程建设思路

本校区没有开设网络空间安全这一学科，计算机学院开设的网络安全方向课程一般安排在大三学年，学完相关课程学生已经到大四阶段，很多对网络安全有兴趣的同学因为时间关系不能持续投入实践训练。面对网络攻防竞赛人才培养的困境，开设基于 CTF 的网络安全攻防实践竞赛指导课，通过双大纲、分层级的教学内容、渐进式教学方法、赛练结合的实践方式和立体式考核评价学生的学习效果，培养学生网络攻防的实践能力。

3.1 以立德树人为根本目标，分层级、渐进式开展教学

网络强国战略要求学校培养技术过硬、德才兼备、具有创新创业精神的复合型网络安全人才，除了要求常规专业技能教育外，还需有“政治认同和家国情怀”价值引领。首先根据课程的定位制定课程的知识、能力和育人的总体目标，在传授知识的同时，培养学生的探索精神、创新意识和工程素质，培养学生的职业道德、社会责任感和社会主义核心价值观；其次根据课程的总体目标，设计育人目标的具体实施方法；最后将课程教学内容与思政元素一一对应，将思政元素细化的到每个课程教学模块中。

从《网络安全法》、《密码法》等法律入手，明确法律法规和基本红线，打消学生的猎奇心理；网络安全领域的技术发展极其迅速，各类攻防手段也在不断更新，选取近期出现的网络安全事件作为思政元素更能引起学生的兴趣；从近期竞赛真题中出现的周恩来设计的豪密和王小云团队破解哈希算法等示例，培养学生自主可控的安全理念和奋斗拼搏的精神，树立民族自信和职业素养，激发学生爱国热情、责任担当和民族自豪感。思政过程需要潜移默化、润物无声地展开，采用案例教学、启发教学、研讨教学和情境教学等学生更容易接受的课程思政教学方法；最后通过课程实践、课后比赛、一线护网行动等多种形式结合的方式，培养具有国际视野和创新能力的网络安全攻防拔尖人才，培养学生保卫国家网络安全的使命感。

课程主要围绕 CTF 竞赛内容开展教学， CTF 竞赛涉及知识点内容多、难度高、入门难，因此开展分层教学就非常有必要，而且课程内容需要由易到难逐步展开。课程设置开课前学生面试环节，课程组根据学生已有的知识技能和专业方向划分为基础班和高阶班，基础班完整讲解基础知识、工具使用以及每类题型的解题思路，实践环节主要以基础题目为主；高阶班突出实践部分，主要以经典比赛中的赛题讲解、练习为主，实践训练也选取有难度的题目。根据学生实际情况采用分层的教学方式，提高教学效果与人才培养质量。课程内容设计注重各模块的难易程度和内容衔接，模块之间由简到难，模块内知识由浅入深。以 MISC 模块为起始教学内容，在后续的 Web 安全模块、密码学、逆向和 PWN 模块再逐步深入探索专业技能，能让学生更好地适应课程内容，从而提高学生的学习积极性和探索兴趣。模块内以 Web 安全为例，从 SQL 注入的数字型注入到宽字节注入再到绕过知识，难度逐步增大，让学生有获得感和成就感后更愿意钻研具有挑战性的题目。课程设置的具体内容见下表。

表 1 基于 CTF 的网络安全攻防竞赛课程内容

知识模块	教学内容	思政内容	思政形式
Misc	隐写、流量分析、常见编码、压缩包、内存、取证等	网络安全法规宣贯理解网络安全对个人及国家安全的影响，周恩来设计豪密等案例激发民族自豪感	启发、案例教学
Web	sql 注入、php 特性、脚本编写、文件上传、文件包含等	著名网络用户信息泄密事件，职业素养和自主可控的安全理念	视频、案例教学
Crypto	中间相遇攻击、比特攻击、共模攻击、Hash 长度扩展攻击等	国产密码算法和王小云团队破解哈希算法，树立民族自信和创新精神	研讨、情境教学
Reverse	算法逆向、代码混淆、迷宫逆向、虚拟机逆向等	研讨国内逆向工程领域的新动态，激发学生的工匠精神和探索精神	案例、研讨教学
PWN	栈溢出、堆溢出等	深入分析解题思路，培养学生攻破难关、深入探究的品质和辩证的思维方式	研讨、启发教学
竞赛实战	综合以上各类赛题	竞赛真题、综合演练，培养学生团队协作和奋斗拼搏的精神	启发、案例、研讨教学

3.2 建设学校自有实训平台，打造“学-练-训-赛”为一体的教学模式，提升学生实践效果

学校已经采购 e 春秋的实训和竞赛平台，但是因为企业平台内容资源更新不够及时，题目难度也逐渐不能适应高阶同学的需求。课程组利用学校部分华为云平台硬件资源，依托开源平台 GZ::CTF，采用 Docker + K8s 分离部署后端，搭建了自有训练平台 HITSZ::CTF，该平台具有自定义的题目类型、题目动态发送、分组显示和分类显示动态分值等功能，而且建立与课程 QQ 群的实时通信，每当平台有题目上新或者有同学解出题目时，平台播报机器人就会在群里发出通知，激发学生的学习热情。

因此在 e 春秋两个平台和自有平台的基础上，课程组将 e 春秋实训平台进行课堂练习， e 春秋竞赛平台用于基础班学生上课阶段的课后练习，自有平台 HITSZ::CTF 用于高阶班学生的课后练习、学生常态化训练平台和校赛平台。每个平台都有丰富的配套学习资源包括学生竞赛入门学习路径资料引导、课堂相关知识 PPT、课堂练习实验指导书、训练题目以及所有题目的解题思路等。

此外，利用企业和自有的训练平台，学生在平台上通过复现课堂讲解的例题学会解题思路，根据课后布置的练习题锻炼自己的解题思维，参加每周三固定的分享会并利用常态化训练平台加大自己攻防训练的次数，并在最后的班级比赛和校级比赛中提升自己的能力，整个课程形成了“学-练-训-赛”为一体的教学模式。另外在各类平台上都可以设置排行榜，而自行搭建的平台还能实时在群里同步信息，极大地激发学生学习的积极性，促进学生网络攻防实践能力的提升。

课程考核从学生掌握单个技术的情况、综合运用各种技术的实践能力和团队协作能力三个方面考察学生。依据“学-练-训-赛”为一体的教学模式，在学习环节考察学生掌握单个知识点的情况和工具使用的熟练程度；通过训练环节考察学生独立复现解题过程的能力并锻炼学生写文档的能力；通过课程过程长期开放的实训平台，考察学生的综合能力和筛选学生的比赛主攻方向；通过校赛团队协作的方式考察学生应对真实比赛的应变能力和团队协作能力。这种立体式过程考核评价方式能够提升学生的实践能力和网络攻防实战基础。

3.3 AI+ 协同教学，探索人机协同教学模式

网络安全攻防技术涉及的知识呈现增速快、体量大、内容复杂等的特点。学生学习入门感觉困难，课程组给出的相关文档等内容学生学起来感觉茫然，而课程组教师和助教的人数不足也很难逐一辅导学生，因此在 AI+ 赋能高等教育这一浪潮下，课程组主要采用一下几项措施将 AI+ 技术赋能教学，提升教学质量和学生感知。

一是将实训平台增加学生画像，课程组老师可以通过学校搭建的各类实训平台信息了解学生的学习动态和擅长领域，根据学生的特点再动态调整课程内容和更新平台信息，做到教学更加有的放矢。

二是将实训平台和课程 QQ 群联动，在 QQ 群中加入平台播报机器人，实时播报当前平台动态和学生解题情况，激发学生的动手热情，形成你追我赶的实践氛围。

三是利用学校采购 HiAgent 系统，依托豆包大模型创建 CTF 助手智能体，将课程资源和团队搭建的自有 wiki 等相关内容分模块作为知识库输入，不断训练 CTF 助手。该智能体具有实时交互功能，能帮助学生从海量的知识库中梳理合适的信息进行答复，答复的结果学生还可以进行实时的反馈，根据反馈结果可以持续优化。目前该智能体已经投入使用，学生反馈该智能助手能极大的提高他们的学习效率和增强学习的信心。

4 建设成效

以为国家培养技术过硬、德才兼备网络安全攻防人才为目标，以学生为中心分层教学，结合企业和社团的力量，打造符合学校学生特色的网络攻防实训平台，通过 2 年的探索与实践，课程建设取得一定的效果。

4.1 课程教学效果明显

课程自 2023 年秋开设以来已经开展 3 轮教学，共覆盖 120 名来自全校各个专业的学生，其中不乏一些电信、光电等专业对网络攻防有兴趣的同学。课程教学案例获得 2024 年中国高校计算机教育大会教学案例大赛三等奖，第六届中国教育大会 AI 大模型方向案例一等奖。依托该课程，连续两年组织校级网络安全攻防大赛，共有近 100 名同学参加，社团规模也稳定在 60 人左右，初步建成阶梯式的 CTF 竞赛队伍。

4.2 竞赛成绩明显提升

课程开设 3 年后，参与国内比赛的学生人数明显高于前面几年，获奖数量也呈陡峭式增长。截止当前，学生在全国大学生信息安全大赛创新实践赛、工业互联网大赛—智能家电行业赛道、数字中国创新大赛数字安全赛道和广东省大学生网络安全大赛等，共获得国家级团体奖项 7 项，省级团体奖项 15 项、个人奖 3 项，并且活跃在各网络安全攻防竞赛平台，在各平台

获奖累计 10 项，并且积极参与广东省组织的各类护网活动，保护各企事业单位的网络安全。

表 2 课程开设前后我校学生在 CTF 竞赛方面的成绩

	2022年	2023年	2024年	2025年
省级奖项	2	3	7	8
国家级奖项	/	/	3	4

4.3 学生工程实践能力和深耕网络安全领域意愿增强

学生通过“学-练-训-赛”一系列动作，增强了自己的实践能力，一些能力强的同学甚至已经能够自己搭建环境，自主设计 CTF 竞赛题目；并积极主动在各类论坛活跃输出相关知识或赛题的视频讲解和文档案例，目前竞赛团队主要成员输出各类视频和文档材料近 20 个项，在 CTF 竞赛领域做出自己的贡献；另外也有越来越多的学生在深造和就业方面选择密码学、网络空间安全等相关的专业和工作，以国家网络安全为己任，为国家网络安全贡献自己的力量。

5 结束语

针对网络安全人才实战能力四种类型培养的需求，以培养学生的网络安全攻防能力为目标，以立德树人为根本，结合学校社团，借助企业资源建设自有网络攻防实训平台，并以学生为中心开展分层分级教学，将人工智能+技术引入课堂，设计“学-练-训-赛”实践教学模式，培养学生掌握网络安全攻防技术的综合创新实践能力和工程实践能力。并激发学生体会“没有网络安全就没有国家安全”家国情怀和使命担当，引导学生积极参与到网络安全社区、论坛中去贡献自己的力量，并将一批思想政治坚定，网络安全攻防技术过硬的学生送入网络安全企业或进一步在网络安全领域深造。

目前针对网络攻防实践的教材较少，而且不够系统完备，课程建设工作还需进一步在网络安全攻防实训教材上做进一步探索。

参 考 文 献

[1] 《网络安全人才实战能力白皮书》发布,攻防实战人才成行业刚需[J].工业信息安全,2022,(07):92-101.

[2] 俞能海,吴文涛,王晨曦.网络安全实战型人才培养体系探索与实践[J].中国信息安全,2024,(03):29-33.

[3] 袁晨,张月国,刘功申.高校网络安全实战型人才培养的实践与探索[J].工业信息安全,2024,(03):6-13.

[4] 朱辰,孙斌,金心宇,等.网络空间安全攻防实验教学与实训平台的构建[J].实验室研究与探索,2021,40(06):265-267+275.

[5] 刘建伟,尚涛,白桐.网络空间安全卓越工程师培养模式探索[J].工业信息安全,2024,(03):64-69.

[6] 宋晓锋,倪林,韩鹃,等.CTF 竞赛融入网络安全人才培养过程的探索与实践[J].计算机教育,2021,(11):1-5.

[7] 魏英凯,胡思煌,王美琴.山东大学网络安全实战型人才培养体系建设实践[J].工业信息安全,2024,(03):14-19.

[8] 王震,张慧翔,刘志强.“攻防兼备、分层归类、实践主导”的攻防能力培养体系[J].工业信息安全,2024,(03):77-82.

[9] 李晖,杨超,张美茹.知识能力使命三位一体的一流网络安全人才培养体系构建[J].工业信息安全,2024,(03):58-63.

[10] 封化民 . 创新人才培养模式 加强网络安全实战型人才培养 [J]. 中国信息安全，2024（03）：26-28.

[11] 杜秋平,陈晶,杜瑞颖,等.国家网络安全学院实验室建设与管理创新研究[J].实验技术与管理,2019,36(11):33-35.

[12] 叶登攀，李珉. 人工智能在网络空间安全学科教学中的应用探索[J]. 计算机技术与教育学报,2024,12(01):62-66.