

基于 CTF 竞赛的网络安全课程教学研究

于小莉 郭艳丽 訾书克 *

昌吉学院信息工程学院 831100

摘要: 针对网络安全课程教学中面临的实践性不足、教学方式传统、授课场景单一、师资力量薄弱等一系列问题,从调整课程体系、优化考核方式、完善学习平台、创立 CTF 校园社团及组建 CTF 参赛团队等多个方面探讨基于 CTF 竞赛的网络安全课程教学改革的方法,提出“以赛促学,以赛促教”的网络安全课程教学质量提升模式,引导学生进行自主性、研究型学习,提升网络安全职业素养。

关键词: 网络安全;以赛促学;CTF 竞赛;教学改革

Teaching Research of Network Security Course based on CTF competition

Xiaoli Yu, Yanli Guo, Shuke Zi*

School of Information Engineering, Changji College, 831100

Abstract: Aiming at a series of problems in the teaching of network security courses, such as lack of practice, traditional teaching methods, single teaching scene, and weak teachers, this paper discusses the teaching reform methods of network security courses based on CTF competition from several aspects, such as adjusting the course system, optimizing the assessment method, improving the learning platform, establishing CTF campus clubs and building CTF participating teams. This paper puts forward the teaching quality improvement model of network security courses, which is “competition promotes learning and competition promotes teaching”, to guide students to carry out independent and research-based learning, and to improve the professional quality of network security.

Key words: network security; Use competition to promote learning; CTF competition; teaching reform

引言

2018 年 10 月,教育部发布了《关于加快建设高水平本科教育全面提高人才培养能力的意见》(教高〔2018〕2 号),就加快形成高水平人才培养体系提出了若干指导意见。意见指出,高校应不断创新学分制,鼓励学生通过参加竞赛活动、创新创业等获取学分,提升学生自主学习的能力。《关于实施高等学校本科教学质量与教学改革工程的意见》(教高〔2007〕1 号)也明确提出,要把学科竞赛纳入实践教学与人才培养模式改革创新的重要建设内容。自此,“以赛促学、以赛促教”的实践教学理念在高等教育教学改革中得到了不断的深化,其意义对于我们应用型本科院校来说十分重大。

《网络安全技术》是我院计算机科学与技术、网络工程专业开设的一门重要专业基础课程。随着计算机网络的广泛应用和网络用户数量的急剧增大,网络安全的重要性日益凸显,“没有网络安全,就没有国家安全”,网络安全已成为各国信息安全建设关注的焦点,也是当前科研人员研究热点及市场人才需求的新领域。2021 年由安恒信息等企业参与编撰的《网络安全产业人才发展报告》白皮书显示,我国网络安全产业人才需求呈井喷

式增长。

通过本课程的学习,使学生掌握计算机网络安全的基本知识、原理及其应用技术,包括:网络安全技术的基本概念、内容和方法;网络安全管理技术、安全服务与安全机制;入侵检测技术、黑客的攻击与防范技术身份认证与访问控制技术;网络安全中的密码与压缩技术;病毒及恶意软件的防护技术;防火墙技术及应用等。

一、网络安全课程教学现状

网络安全是一门综合性较强的学科,涉及多门理论课程,如计算机网络技术、计算机组成原理、密码学、数据库、操作系统等。目前,我院采用理论和实践“48+16”教学模式,实践课时偏少,且实践课时主要由任课老师自行进行项目设计,缺乏系统、完整的实践教学体系。在近两年计算机网络及网络安全课程的教学过程中,发现我院网络安全课程教学主要存在四个方面的问题。

1. 课程实践性不足,学生素质提升不够

网络安全课程目前采用的授课方式是理论 48 课时,实践 16 课时。教学方式较为传统,以任课教师讲授理论知识为主,涉及概述、常用的攻击方法、计算机病毒、加密技术、防火墙技术等内容。同步设置的实验内

容由任课老师自行安排,也多以验证性实验为主,如常用网络命令、无线网络配置、数据加密解密等,学生依样画葫芦,生搬硬套来完成各个任务,自主探究学习机会较少,独立解决问题的能力没有得到锻炼和提高,更无法满足人才市场对网络安全人员的需求。

经与相关企业沟通交流,过半数的网络安全从业者认为当前公司网络安全人才规模不能满足工作要求,不仅数量跟不上,人才供给和需求之间存在错位也是亟待解决的问题。网络安全行业面临的是应用领域拓展、场景化应用爆发的阶段,需要的是全能型的网络安全专家,而非底层的“救火队员”,网络安全人员更讲究实操水平,人才的培养要到实际“战场”中去。

2. 授课场景单一,考核方式较为陈旧

网络安全教学仍然以基础理论讲解为主,授课内容相对陈旧,学生学习兴趣不高。而网络安全技术实际上是发展迅猛的学科。常规实验只能进行一些简单的操作,如网络命令、数据加解密等,学生无法真正体会网络安全的内涵。只有深入接触过网络安全设备,亲眼见证网络安全博弈,才能深刻领会网络安全学科的魅力。

成绩仍然是作为学生考评的主要依据。以闭卷、笔试和标准化考题的考核方式为主。而企业所需的网络安全人才更侧重于解决实际问题的能力,在考核方式上需要做出创新,传统的卷面答题已经无法检验出学生实际的动手能力。

3. 师资力量薄弱,缺乏能力提升渠道

目前,我院教职工总数为 61 人,8 人为 ICT 学院企业教师。博士 2 名,硕士研究生 32 名,专业覆盖软件工程、计算机应用技术、通信工程、计算机技术、电路与系统等。无密码学、网络空间安全的专业教师,师资力量相对比较薄弱。

另外,网络安全是一门不断演进的技术学科,不仅要求教师能紧跟时代发展步伐,不断更新知识体系,而且要求教师最好有网络安全领域相关工作经验,熟知各类攻防技术,真正做到理论、实践融合教学。除了教师自行进行网络学习之外,缺乏统一的、系统的能力提升渠道。

4. 忽视德育教育,缺乏职业精神的培养

很多同学学习网络安全相关知识,都是被“黑客”一词深深吸引,觉得他们能在不知不觉中盗取别人的一切,包括信息、个人关系、日常活动范围、储蓄资源等等。甚至沉迷于黑客的魅力,敬佩他们打破常规的创造力和勇气,膜拜他们对代码的执迷和热爱。

当代大学生思想深处存在着一定的矛盾与困惑,不愿墨守成规,是非对错也有自己的断定标准,如果不加以正确的引导,很可能日后会走向网络犯罪的道路。因此,网络安全课程绝不能忽视德育教育,在授课过程中可以结合实际案例,帮助学生了解网络世界可能存在的消极方面,一方面提升自己的辨识能力,不会轻易上当

受骗,另一方面也帮助学生树立正确网络安全观,通过网络安全相关竞赛等正确的方式来证明自己的实力,不要误入歧途。

二、CTF 简介

CTF (Capture The Flag) 即夺旗赛,是全球范围内的网络安全竞赛,也是相关企业选人用人极其关注的平台。参赛选手通过使用逆向、解密、取证分析、渗透利用等技术来拿到被放在远程服务器上或被加密和隐藏在各种不容易访问到的媒介上的 flag。

CTF 竞赛一般分为三类模式。解题模式 (Jeopardy)、攻防模式 (Attack-Defense) 及混合模式,其中,解题模式一般可用于线上选拔,攻防模式由参赛队伍线下相互进行攻防,竞争性强,能够实时反映得分情况,考察队伍的技术、耐力、团队协作等各个方面。混合模式是结合了解题模式和攻防模式的新型 CTF 竞赛模式。

网络安全竞赛核心价值一是帮助互联网企业查漏补缺,提升安全能力。二是和网络安全人才培养直接挂钩,优秀参赛选手不仅可以取得分数和奖金,也很容易受到企业青睐,提前获取 offer,为日后就业打下更好的基础。

三、基于 CTF 竞赛的网络安全课程教学改革

通过分析各种教学模式,本研究认为基于 CTF 竞赛的学习模式更适合网络安全课程的教学。基于“以赛促学”理念,构建《网络安全技术》课程的新型教学模式:将网络安全课程在形式和内容上与 CTF 竞赛有机结合,形成一套完整的理论及实践教学体系,改革现有的教学计划、教学方法及考核形式,培养一批既具有扎实理论基础,又能动手解决实际问题的学生。通过教学方式的改革,不断培养学生学习的兴趣。同时,通过与企业的相关合作,促使任课教师下企业学习、参加培训,不断提升教学能力,建立“双师型”教师团队。

1. 调整课程内容,与 CTF 深度匹配

在保障课程基础素质和专业基础的前提下,对网络安全课程的培养方案和教学内容进行一定的调整。项目组成员对以往的 CTF 试题、解图思路文档等进行汇总、整理及分析,融合网络安全课程考察内容,构建出与之匹配的 CTF 相关题库,再将题库进行分解,融入日常课程理论知识讲解过程中。

2. 优化考核方式,注重实践能力提升

目前,该课程仍然采用以笔试成绩为导向的考核方式,存在学生应试能力强,但实际动手能力弱的现象。因此,需要对当前的考核方式进行优化,在考核成绩中提高实践环节的比重。实践内容设置了个人完成的实验项目,同时充分利用学院已经建设完成的网络安全实验室,设置分组对抗实验项目,以班级分组形式完成,充分利用 CTF 竞赛攻防模式,在实践过程中,让学生了解 CTF,激发学习的兴趣,培养团队协作能力。课程考核采用 50% 卷面 +50% 实践的比例,期末卷面考试中适当增加 CTF 题目,学生提交解题思路作为成绩依据之一。

如学生在 CTF 相关竞赛中获得优异成绩,可作为此门课程成绩加分项,形成一定的奖励机制。

3. 完善学习平台,丰富教学模式

第一课堂以网络安全技术理论为主线,以教师为主导,为学生奠定相关基础。同时积极开展第二课堂,以学生为主体,通过网络慕课资源自学相关知识,课余时间通过现有的 CTF 训练平台进行教学和训练,如 XCTF 实训平台、i 春秋、实验吧、Pwnhub、南京邮电大学网络攻防训练平台等。同步开放学院网络安全实验室,供学生自学使用。课后拓展包括知识延伸、认证考试和技能竞赛 3 项教学活动。在技能竞赛环节,任课教师可随时发布相关赛事咨询,学生自愿组队参赛。

4. 创立 CTF 校园社团,组建 CTF 参赛团队

社团本着“相互学习,共同进步”的宗旨,旨在为大家提供一个锻炼的平台,着力提高网络信息攻防在广大学生中的知名度。让对网络安全技术感兴趣的同学找到共同学习的大家庭。一方面提升个人专业技能,另一方面培养综合素质。同时为各种大型比赛做好宣传并组织人员参赛,让更多对网络安全技术感兴趣的同学,能参与其中。CTF 比赛需要一定的知识积累和沉淀,因此社团着重在大二年级进行队伍创建及选拔,这样可以尽早分组,根据学生的特长明确学习方向,有的放矢。如部分同学专注于 Web 漏洞,部分同学专攻逆向等。可以参赛的赛事包括电子数据取证类竞赛、全国大学生信息安全竞赛、国内国际知名 CTF 竞赛如强网杯、WCTF 等。可根据学生团队的组建情况,分级分阶段参加不同层次的竞赛,在竞赛中展现学习成果,获得一定的成就感和荣誉感。

四、实践效果

基于 CTF 竞赛的网络安全课程教学以教师为主导、学生为主体,从职业实践能力发展的实际需求出发,选择部分适合的 CTF 竞赛作为课堂教学效果检验的方式。能使学生积极地主动学习,培养团队合作精神,是一种新的教学理念和教学模式。将其应用于网络安全相关课程的日常教学活动中并取得了不错的效果。

借助项目组建了 CTF 校园社团,截至 2022 年 7 月,

社团招募成员共 24 名。利用晚自习时间,向广大同学宣传网络安全相关知识,利用周末和节假日向同学们现场展示攻防对抗,同时每周组织日常训练:以在攻防世界、CTFHub 平台训练为主,每月参加 CTF 线上竞赛为辅。社团成员参加 CTF 赛事 6 次:第十四届全国大学生信息安全竞赛创新实践能力赛;“鹤城杯”CTF 网络安全挑战赛;2021 年第五届“强网杯”全国网络安全挑战赛;西湖论剑 2021 中国杭州网络安全技能大赛;第四届红帽杯网络安全大赛;第三届美团网络安全高校挑战赛。获得第十四届 CISCN 西北赛区二等奖、西湖论剑网络安全技能大赛三等奖、信息安全铁人三项全国 23 名等成绩。

五、总结

“以赛促学”视角下基于 CTF 竞赛的网络安全课程教学研究,在教学中取得良好的教学效果,提高了学生获取理论知识的能力,提升学生网络安全技术专业技能。CTF 竞赛的形式对学生而言新鲜、生动,学习兴趣得到了很大的提升,在社团的引领下,学习氛围浓厚,引导学生进行自主性、研究型学习,提升网络安全职业素养。

参考文献:

[1] 葛昕,马立新.基于 CTF 竞赛的网络安全课程教学研究[J].教育教学论坛,2020(46):268-270.

[2] 孙洁琼.“以赛促学”教学激励机制实践探索[J].英语广场,2021(08):118-120.

[3] 胡静,郝钢.基于协同育人的网络安全技术课程改革与实践[J].计算机教育,2019(06):102-105. DOI:10.16512/j.cnki.jsjyy.2019.06.025.

[4] 光焱,康绯,卜文娟.网络安全专业基于 CTF 模式的密码学课程实验课教学改革[J].教育现代化,2019,6(90):86-87.

作者简介:于小莉(1986,10),女,回族,宁夏固原人,讲师,硕士,研究方向:通信系统、计算机网络。

通讯作者:訾书克(1986,8),女,汉族,河南临颖人,讲师,硕士,研究方向:技术创新

基金项目:2021 年度昌吉学院教科研项目“‘以赛促学’视角下基于 CTF 竞赛的网络安全课程教学研究”(编号:21JYYB003)。