计算机与自主智能研究进展
Advances in Computer and Autonomous Intelligence Research
第 4 卷◆第 1 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

大学生网络安全实践能力要素分析与培养方法探讨

付钰　严博　张志红
海军工程大学
DOI:10.32629/acair.v4i1.19371

[摘　要] 随着数字化进程不断加快,网络安全已经成为国家安全的重要基础,对我国全面建设社会主义现代化国家意义重大。作为我国网络空间安全未来的中坚力量,大学生自身网络实践能力和意识的培养刻不容缓。基于此,可将大学生网络安全实践能力分为六大维度,即：网络设备运维能力、系统管理能力、安全防护能力、应用开发能力、问题解决能力和项目管理能力。立足目前高校普遍存在的“重理论、轻实践”和“知识碎片化”等问题,提出以“以赛促训、兴趣导向、实践赋能、协同创新”为理念基础的“课程重构、平台强化、竞赛推动、校企合作”培养模式,为网络安全专业教学改革提供参考。
[关键词] 网络安全；实践能力；能力要素；培养方法；教学改革
中图分类号：H191　文献标识码：A

An Analysis of the Elements and Cultivation Methods of College Students’ Cybersecurity Practical Competence

Yu Fu　Bo Yan　Zhihong Zhang
Naval University of Engineering

[Abstract] With the accelerated digitalization, cybersecurity is a key pillar of national security. As the main force in cyberspace security, cultivating college students’ practical cybersecurity competence is crucial. This paper classifies this competence into six dimensions: network equipment maintenance, system management, security defense, application development, problem-solving, and project management. Addressing higher education issues like overemphasis on theory and fragmented knowledge, it proposes an educational philosophy of competition-driven training, interest orientation, practice empowerment, and collaborative innovation and builds a cultivation framework centered on curriculum reconstruction, platform enhancement, competition promotion, and university-enterprise cooperation to provide theoretical and practical guidance for cybersecurity education reform.
[Key words] Cybersecurity; Practical Skills; Skill Elements; Cultivation Methods; Educational Reform

1 引言

网络安全空间的竞争本质上是人才的竞争,只有将掌握扎实理论知识与具有优秀实践能力的学生更好地培养出来,才能让网络安全人才真正担负起职责[1,2]。传统高校以讲授为主的教学方法,使学生仅能明白网安的基本概念,在面对一些实际的网络安全问题时,无法正确运用并处理,实操存在难度大、问题解决能力弱、项目经验欠缺等问题。理清什么是网络安全实践能力要素,并建立切实可行的培养体系是摆在目前教育改革中的迫切问题之一[3]。

2 大学生网络安全实践能力的核心要素分析

网络安全实践能力是多维复合概念,涵盖网络构建、运营维护全流程,它并非单纯的工具使用技能[4,5]。其核心要素可归纳为六个相互关联、各有侧重的维度：

2.1网络设备操作与维护能力

(1)设备安装与配置能力：熟练掌握路由器、交换机、防火墙等核心设备的安装连接,并能根据拓扑规划、安全策略来完成IP地址分配、VLAN划分、路由协议和ACL配置。(2)故障排查与修复能力：采用系统化思维模式,掌握利用指示灯状态、日志、Ping及Traceroute等方法检测网络连通、性能问题并予以纠正的方法。(3)设备升级与优化能力：按需对技术进行更新升级,升级网络设备固件以及操作系统；通过调整网络配置相关参数来提高网络性能、稳定性等。

2.2网络系统搭建与管理能力

(1)网络架构设计能力：按照应用场景设计星型、树型等拓扑及核心层、汇聚层、接入层层次化结构,保证网络可扩展性、可靠性及易管理性。(2)网络操作系统安装与配置的技术能力包

括能够实现Windows Server、Linux等主流系统部署和熟练使用系统命令,能够实现对系统用户权限的设置以及对DNS/DHCP/FTP等网络服务的配置。(3)网络资源管理能力：根据IP地址空间、域名、网络存储等核心资源规划、分配和维护需求来制定实施计划,保证资源得到充分利用。

2.3网络安全防护和信息防御能力

网络安全实践的核心内容,体现了学生构建网络安全防御体系以及实施网络安全管理的整体水平[6],具体包括三个方面。

(1)能够从身份认证、访问控制、数据保密和完整性等方面考虑安全需求,并据此制定出合理的安全策略,并将制定出的安全策略应用到具体的设备配置中、软件部署上,从而建成一套可以持续防护的体系。(2)能够根据网络结构及安全风险评估结果来进行安全设备的配置和管理,包括防火墙、IDS/IPS、VPN网关的配置以及边界防御、纵深防御等多层次多冗余防护体系的建立。(3)挖掘漏洞与风险管控的能力：熟练掌握Nessus、OpenVAS等漏洞扫描软件;定期开展系统安全性评估工作,及时发现系统的漏洞,并且依据发现的漏洞大小先后次序安排整改的优先顺序,通过做好打补丁及安全加固的工作实现闭环。

2.4网络应用开发与部署能力

体现学生对安全应用的理解、设计与实现素养,要求熟练开发应用系统,且在开发全流程贯彻安全设计理念[7]。

(1)网络编程与安全协议开发能力：掌握 Python、Java 等语言的Socket编程技术,理解TCP/IP协议栈,能编写简单网络通信程序,遵循安全编码规范防范常见漏洞。(2)对Web应用开发和安全部署进行操作,熟悉前端技术以及Servlet、PHP、Flask等后端框架,在开发过程中加入安全措施,做好防御SQL注入和XSS攻击等措施,对Apache、Nginx等Web服务器做好安全部署工作。(3)能针对Android和iOS平台进行移动应用开发、熟悉通信加密机制,并能够识别恶意代码注入、权限越权等特有的风险点并加以防范。

2.5网络问题解决与优化能力

要求学生能够准确判断和定位问题,能在复杂的网络环境中作出正确的分析和判断,并且具备提升和改善系统性能的能力,其具体内容如下：

(1)问题分析与诊断能力：采用Wireshark数据包分析、性能监控、日志查证等手段,分析定位网络延时、丢包等情况发生的根本原因,并根据实际发生的安全事件,使用安全事件响应处置流程对问题的性质和范围进行判断。(2)对症下药、有的放矢,通过针对性的调整拓扑、优化路由、使用负载均衡方式等提高网络传输的效率和稳定性,在保证实际运营中所必需的高并发性能的基础上做好安全防护。(3)持续改进与创新能力：不断跟踪SDN、NFV、零信任架构等前沿技术,研究其可行性及安全性,在性能优化和安全防护上使用这些技术,并在此过程中获取新知、发展能力。

2.6网络项目建设与风险管理能力

网络安全实践成果得以高效落实、长久运转的基础,是检测网络安全领域相关岗位人员职业胜任力的指标。

(1)项目规划与组织能力：根据实际测评项目(等级保护测评、系统加固等)进行任务分解、资源配置及进度安排,并将任务落实到各岗位、人员,执行项目的全过程管理。(2)项目沟通与协调能力:掌握跨角色协作及沟通能力,会编写规范的技术文档和实施方案以及形成测试报告,并能与相关团队人员、用户、供应商进行有效的沟通交流。(3)项目的质量和风险控制能力：了解项目全生命周期的各项管理办法；能够找到并分析技术、进度、成本等各种风险,利用风险评估、风险预案的编制保证项目目标的实现,并建立起项目的质量持续改进机制。

3 大学生网络安全实践能力培养的核心理念与突出特点

培养学生网络安全实践能力,是应对信息化时代安全挑战、创新高校人才培养模式的重要需求。

3.1核心理念

(1)以赛促训：通过参加CTF、攻防演练等竞赛,用真实问题引导学习,把理论转化为攻防、防护技能。将课程的内容融入到竞赛的任务中,建立“赛、学、练、研”的一体化平台,提高实操能力,激发创新的兴趣。(2)兴趣导向：由于网络安全知识比较难以理解,技术更新换代较快,应结合学生兴趣点,运用实践项目、案例剖析、虚拟仿真平台,创设沉浸式教学环境,激发学生探索的乐趣,培养学生个性化和持续化学习的习惯。(3)实践赋能：将多层次的实践有机结合起来,做到以实践出真知,教师由原来的单一讲授型向促进学生成长的学习引领型教师转变;运用项目式教学方式促使学生由“理论掌握者”转变为“问题解决者”。(4)协同创新：打造“校—企—赛—研”协同育人模式。校企共建实训基地,共建共享攻防环境;校企联合或与科研机构合作开展创新课题的研究和开发。强化融通学科能力,融通计算机科学、法学等其他学科知识,拓宽学生的知识面。

3.2突出特点

(1)情境化学习贯穿全过程：实践教学从“实验操作”转向“真实任务演练”,依托仿真靶场、攻防平台,实现教学内容与职业情境高度贴合(2)体系化培养层层递进:递进形成由基础技能训练—综合实战提升—项目实操—科研创新递进式的培养路径,各层次有联系、有侧重点。(3)多主体协同共同育人：通过校企合作、行产教融合和竞赛的牵引作用打造“教学—实训—就业”闭环模式,企业专家、竞赛导师、科研教师三位一体共同指导,强化教学针对性、前瞻性。(4)创新驱动贯穿培养全过程：加强学生的创新意识及问题解决能力,在具体的任务中独立思考并做出相应创新设计,是提高学生的实践成果原创性和推广价值的重要方法之一。

4 大学生网络安全实践能力的培养方法

大学生网络安全实践能力培养是系统长期的过程,需课程体系、教学内容、实验实训、竞赛活动、校企合作多环节协同[8,9]。

4.1课程体系优化：重构核心课程内容,强化系统化教学

(1)重构核心课程框架：将《计算机网络》、《网络安全》、《信息系统安全》等作为课程核心,融合相关知识点,形成由浅入深、由基础到攻防的知识递进体系,并且采用模块化的教学形式强化理论知识。(2)强化课程实训环节：打破理论和实践相分离,把实验教学、案例分析、项目实践有机融入到整个教学过程中,围绕专业核心课程设置相关的操作性工作任务,提高知识运用能力。(3)推动课程纵横融合：打造“基础—核心—拓展—创新”四层阶梯式的课程体系,衔接贯通上下级相关课程之间的联系,并关联各部门的课程模块,形成整体化的课程群。

4.2实践教学建设：搭建多层次实训平台,强化动手能力培养

(1)完善校内实验环境:建立网络安全实验室,提供路由器、防火墙等硬件设施,并能够完成网络拓扑的搭建、协议的配置等内容的基础操作练习。(2)搭建虚拟仿真实训平台：通过使用虚拟化和云计算相关技术,来建立网络安全综合实训平台或靶场,在仿真的真实攻防环境中进行漏洞挖掘、渗透测试等方面的实战型练习。(3)推进校企实训结合：将企业行业一同建立实训基地,将真实的且无危险性案例以及对应的业务场景,应用于学生的项目化实训当中,带其熟悉安全管理、应急响应等内容。

4.3竞赛驱动机制：以赛促学,以赛促训,以赛促创

(1)构建校内竞赛训练机制：开展定期举办校园攻防演练、漏洞挖掘比赛、CTF夺旗赛等活动,夯实理论基础、锻炼动手能力、培养团队协作意识。(2)参与高水平专业竞赛：督促、组织和支持广大学子积极参加“全国大学生信息安全竞赛”“强网杯”等活动,组建专项团队对学生进行技术引导和资源帮扶。(3)将竞赛题型、攻防案例、漏洞修复任务等引入课堂教学中,使得教学内容更接近实际应用场景,形成了“教学—竞赛—创新”的良好循环。

4.4校企协同育人：强化产教融合,完善实践育人机制

(1)共建实践教学基地:网络安全企业构建实训平台和攻防演练系统,提供技术服务及案例,高校负责组织教学,双方实现资源共享、开展教学创新。(2)引进企业导师与真实项目。可以请企业专家作为教学顾问或实践指导老师,让学生直接参与真实项目的开发,了解岗位需要、熟悉工作流程,更好地做好进入工作岗位的准备。(3)强化科研合作和成果转化,在网络攻防、漏洞分析等方向推进校企合作科研攻关工作,及时把新的科研成果转化为教学资源,实现科研反哺教学。

4.5突出能力评价：完善教学评价与持续改进机制

(1)完善能力导向评价体系：以传统的考核标准为前提,加入实验报告的质量、项目是否完成、攻防演练成绩,采用多方面的方式去衡量学生的实操与问题的解决能力。(2)构建数据驱动监测机制:利用教学与实训系统收集学生的学情数据,通过建设实践能力成长档案,形成对学习过程的数据跟踪及量化的学习效果评价,可以为教学改进提供参考依据。(3)形成持续改进闭环：定期对优化课程体系、实训环节、评价标准等工作进行检查和总结,并根据企业方的意见加强教学工作；使教学的内容不断向紧跟行业发展靠拢,做到“评价—改进—再评价”的良性循环。

5 结论

大学生网络安全实践能力培养应围绕课程体系建设开展,以实践教学平台为载体,以竞赛驱动为引擎,以校企合作为保障,通过科学的能力评价、不断修正完善,形成闭环育人机制；多维度贯通的知识学习—能力构建—实践锻炼—创新应用相互联动的循环路径。

[参考文献]

[1]蒋云鹏,梁义.网络安全课程“三维融合”教学模式探索与实践——以伊犁师范大学为例[J].教育进展,2025,15(9):7.

[2]姜婧妍,于丽娜,王树兰,等.融入CTF竞赛和高校信息中心的网络空间安全基础课程改革实践[J].职业教育发展,2025,14(8):390-396.

[3]陈广锐,曹春杰,郭渊博,等.强技立本铸盾护航——海南大学网络空间安全学院创新育人模式服务自贸港建设[N].中国教育报,2025-10-17(11).

[4]吴小玲,黄建烽.新时代高校网络安全教育的创新发展研究[EB/OL].中国社会科学网,2025-04-29.

[5]纪玉超,姜伟嘉.数字赋能大学生网络安全素养培育的核心要义、现实困境与优化策略[J].大学教育,2025(16).

[6]Khoo L J,Yatim M H M, Wong Y S .Research on Capture the Flag Exercises for Cybersecurity Skill Training Among Malaysian Undergraduates[J].Journal of Human Centered Technology, 2025,4(1):1-9.

[7]蒲晓川,张远强.基于OBE理念的虚拟仿真教学创新改革——以“网络信息安全”课程为例[J].遵义师范学院学报,2025,27(1):104-109.

[8]龚兴东,李跃光,卞秀运.新工科背景下的《网络安全》课程教学改革探索[J].职业教育发展,2025,14(7):357-364.

[9]张光.网络攻击与防御仿真平台的设计与实现[D].陕西:西安电子科技大学,2005.

作者简介：

付钰(1982--),女,汉族,湖北武汉人,博士,教授博导,从事网络空间安全教学与科研工作。