

面向岗位胜任力培养的网络防御综合实践 课程建设

施江勇,陈颖文,付绍静,刘 强,王勇军,赵文涛

(国防科技大学 计算机学院,湖南 长沙 410073)

摘要:以网络防御岗位胜任力培养为目标,借鉴美国网络空间安全教育计划设计网络防御岗位的胜任力模型。首先,基于网络信息防御、网络信息防御综合演练课程设计实验实训内容;其次,基于攻防转换、迭代反馈教学模式支撑学生综合实践能力和岗位胜任力的培养。实践表明,教改后学生评教满意度提升7.2%,课程平均成绩提升15分,能在完成课程实验的基本要求上进行实战活动,参与处置多起实际网络攻击事件的调查取证,教学成效得到了相关单位一致好评。

关键词:网络防御;胜任力;网络空间安全教育计划;综合实践

DOI:10.11907/rjdk.241433

开放科学(资源服务)标识码(OSID):

中图分类号:TP309;G642.0

文献标识码:A

文章编号:1672-7800(2024)008-0043-06



Construction of Network Defense Comprehensive Practice Course for Job Competence Cultivating

SHI Jiangyong, CHEN Yingwen, FU Shaojing, LIU Qiang, WANG Yongjun, ZHAO Wentao

(College of Computer, National University of Defense, Changsha 410073, China)

Abstract: With the goal of cultivating competence for network defense positions, a competence model for network defense positions based on the US Cyberspace Security Education Program was designed. Firstly, based on the course design of network information defense and comprehensive network information defense exercises, experimental and practical training content will be provided; Secondly, based on the teaching mode of attack defense conversion and iterative feedback, practical course teaching is carried out to better support the cultivation of students' comprehensive practical ability and job competence. Practice has shown that after the education reform, students' satisfaction with teaching evaluation has increased by 7.2%, and their average course grades have improved by 15 points. They are able to engage in practical activities while completing the basic requirements of course experiments, participate in the investigation and evidence collection of multiple actual network attack incidents, and their teaching effectiveness has received unanimous praise from relevant units.

Key Words: network defense; competency; national initiative of cybersecurity education; comprehensive practice

0 引言

网络安全重要性体现在方方面面,习近平总书记强调没有网络安全就没有国家安全,网络空间竞争归根到底是人才竞争。俄乌冲突中网络攻击始终贯穿军事热战主线,甚至成为冲突的先行战场,关键基础设施已成为重点攻击目标。然而,当前网络安全人才缺口巨大,实战型人才尤

其匮乏,用人单位反馈相关专业毕业生对任职岗位的胜任力较差。

《2022网络安全人才实战能力白皮书——攻防实战能力篇》指出,真正具有实战能力的网络安全人才严重缺乏,需要企业对其进行深入的实践培训才能胜任工作^[1]。美国NSA针对西北工业大学的APT攻击事件也揭露了网络防御的形势严峻^[2]。为此,本文面向网络空间安全、信息安全、网络工程等相关专业本科四年级学生,开设面向任

收稿日期:2024-05-08

扫描二维码阅读全文:

基金项目:湖南省普通高等学校教学改革研究项目(202301072)

作者简介:施江勇(1990-),男,博士,CCF会员,国防科技大学计算机学院副教授,研究方向为网络安全。



职岗位需求的网络信息防御、网络信息防御综合演练实践课程,以期提升学生的网络防御能力,使其填补大量缺口的网络防御岗位。

CC2020 计算机课程体系将胜任力定义为包含知识、技能和性情在内的三大要素^[3]。本文作者前期探索了网络安全课程的胜任力培养模型,相关举措包括定义网络安全胜任力的核心要素、综合学习评估机制等^[3]。目前,相关工作主要围绕课程知识体系构建、实验实训环境建设和单一技能训练,内容主要围绕各类网络攻击的原理分析和验证,对防护和取证能力的训练还有待加强。以西北工业大学遭 NSA 入侵为例,因其技战术非常复杂,对攻击链的梳理和调查取证除了要掌握大量网络安全取证和应急响应知识、技能外,还要具有大量的实践经验,而实践经验对于在校学生十分缺乏。为此,通过超逼真实训环境构建、真实案例转化、攻防体系构建梳理等手段综合运用学生所学专业课程知识,系统提升学生的实践能力和安全对抗思维,全方位培养学生对于任职岗位的胜任力。

CC2020 虽然对计算机学科胜任力模型落地提供了一套指导规范,但并未明确网络防御相关岗位的胜任力内容,也未对网络安全相关专业如何设计相应课程提供参考。为此,本文参考美国国家网络空间安全教育计划(National Initiative of Cybersecurity Education, NICE)设计网络防御岗位的胜任力模型^[5]。NICE 规定网络防御相关专业领域包括网络安全防御分析、网络安全防御基础设施支持、事件响应、脆弱性评估和管理等,相关岗位角色包括网络防御分析人员、网络防御事件响应者等,针对每一个角色提供了胜任该角色所需的知识、技能、能力要求(KSA)。以网络防御分析人员为例,KSA 要求包括能力要求 6 项、技能要求 15 项、知识要求 70 项。其中,知识(K)强调知道有哪些东西;技能(S)强调如何去做一件具体的事;能力(A)更强调综合能力,即综合运用知识和多项技能解决现实问题的能力,也可理解为具体岗位和角色胜任力。

对于网络信息防御任职方向学生而言,相关知识大多在前期学科基础课上已进行了学习,单项技能训练则在专业核心课中通过课程实验方式得到锻炼,综合能力训练则依赖于综合实践课程、实习实训、毕业设计。其中,综合实践课程相较于实习实训和毕业设计训练能力要求更全面,但时间更短,因此需要加强设计以实现提升岗位任职胜任力的目标。

1 相关研究

本文为了更好地进行课程建设,调研了相关高校网络安全相关专业的综合实践课程建设体系。现有工作主要分为实训平台建设、实践课程体系和内容体系建设两大类。

(1)聚焦于实训平台建设。葛继科等^[6]从网络安全实践教学平台建设需求、建设目标、建设内容、实施效果介绍重庆科技学院的实践路径,以支撑应用型网络安全人才培养。肖凌等^[7]介绍了华中科技大学网络空间安全学院网络空间安全综合实践分级通关实验平台建设经验,从教学模式、实验内容设计入手,对建设实验平台涉及的硬件设备选型、拓扑结构、软件功能、软件结构,以及必须重点考虑的问题进行详细讨论、分析与设计,为网络空间安全综合实践分级通关课程体系提供了有力支撑。李建华^[8]对多元化、多层次网络空间安全人才培养创新理念和模式进行研究,明确了实训平台建设需求,进而对网络安全靶场综合实践平台的国内外建设模式和关键技术进行分析。孟彩霞^[9]提出智能网络安全攻防对抗实验室建设包括智能网络安全攻防对抗平台、智能网络安全攻防对抗人才培养平台、智能网络安全攻防对抗人才选拔平台基础环境建设,以及基于环境构建智能课程教学方案、智能岗位教学方案、智能 CTF 教学方案设想,但缺乏具体实现途径和教学方法指导。

(2)专注于实践课程体系和内容体系建设。陈凯等^[10]针对当前网络空间安全人才培养中存在的知识体系分散、专业知识滞后、课程内容分割独立及学习兴趣不足等问题,根据学生学习规律和认知过程采用自顶向下的方式构建课程体系,聚合提炼实践知识和技能提出了网络空间安全综合实践分级培养模式。该模式针对每个知识技能点、每层学习级别及最终的综合培训设置以游戏通关方式测试关卡,并以实战通关方式考察学生能力水平,以此构建网络空间安全综合实践分级通关课程体系,以期培养高素质的网络空间安全专业人才。

王盛邦等^[11]介绍了网络与信息安全综合型实验的基本设计思路,包括实验跟踪与数据包分析、命令行使用、网络编程、常用信息安全工具使用等关键要素,并以主机扫描综合实验和操作系统指纹探测实验为例进行说明,但体现网络信息安全岗位能力素质的要求不够全面,设计实例相较于真实案例过于简单。黄波^[12]以网络安全体系与技术应用课程建设为例,介绍网络安全与执法专业如何依托专业课程建设提升学生综合实践实战能力的整体构思和做法,通过模块化专业课程实验、创新创业及科技创新项目实践、网络安全技能竞赛实践培养学生的综合实践能力,然而如何保障实验完成度和效果、如何加强课外实践指导仍需进一步探究。

此外,还有少数关于围绕实践课程教学方法的研究。邓清华等^[13]以信息安全综合实验课程教学改革实践为例,探讨如何运用顶峰(Capstone)课程理念促进教学改革,培养学生的科学探究精神、分析和解决问题能力及创新创造能力,具体举措包括拓展学习深度和广度、分组开展综合实验、多元化考核和持续改进等,但在具体实施过程中如何有效发挥教师作用、如何保障实验项目的可实施性有待

探究。李炳龙等^[14]通过创造多维信息安全实践教学平台,将实验内容分为验证型、设计型、综合型、自主型,提出基础问题导引、实践问题指引、创新问题牵引的实践教学方法,并设计了项目式实践教学考核评价机制提升学员动手能力。该方式适合嵌入专业课教学过程,或作为专门的实践环节由多名教师参与指导项目式课题设计和实现。然而,上述工作多数针对单一知识点和技能训练,未围绕岗位任职需求设计内容体系与教学方法。为此,本文聚焦提升学员安全防护能力,通过安全防护体系构建提升学生综合实践能力,以网络信息防御、网络信息防御综合演练课程为抓手,从内容设置、教学方法上进行系统设计和改进,落实 OBE 教学理念,以弥补网络防护类人才培养的研究空缺。

2 教改方法

2.1 面向岗位胜任力培养设置实践课程内容

在课程内容设置方面,参考 NICE 网络防御分析师角色和网络防御事件响应者角色设置胜任力培养目标。具体包括:A0010 为分析恶意软件;A0015 为执行、扫描、识别安全系统漏洞;A0066 为准确完整获取情报,评估、规划产品;A0123 为将网络安全和隐私原则应用于组织要求;A0128 为使用入侵检测技术检测主机和基于网络的入侵技术;A0159 为掌握网络工具收集的信息(例如 Nslookup、Ping 和 Traceroute)。

基于上述目标设计具体课程内容,网络信息防御前导课主要介绍网络防御的基本流程、常用工具、实训平台和组织方式,并以实际案例进行串联,使学生掌握网络防御的一般方法,主要对应胜任力目标 A0066、A0123 和 A0159。基本流程参考 PDR2 模型,包括检测、响应、恢复、防护 4 个阶段,同时强调攻防一体、以攻促防的基本理念,在梳理攻击线索时参考 KILL CHAIN、ATT&CK 等业界主流威胁建模方法,通过串联攻击证据还原完整的攻击过程,并以此提出防护建议。

目前,常用工具包括开源和商业安全软件的使用和分析、系统运维工具和脚本命令的使用,例如 snort 入侵检测系统(IDS)、qradar 安全信息与事件管理系统(SIEM)、Windows 事件管理器、Linux 日志分析、Linux 脚本命令使用等。实训平台采用国际一流的网络安全实训靶场,包括攻击模拟模块、自定义网络拓扑模块、背景流量生成模块等,可有效支持实训活动开展、降低实训环境构建的时间成本。本文组织方式主要涉及学员分组和人员分工,参考 NICE 网络安全人才培养体系设置网络安全分析岗位、安全情报支持岗位、安全事件响应岗位、安全防护岗位,以培养学员团队协作能力及从事网络安全管理岗位所需的组织指挥能力。

本文综合实践课网络信息防御综合演练以案例为牵

引,串联本科二、三年级学生所学的相关专业课知识和技能,包括密码学导论、网络安全、计算机网络安全、软件安全等,主要对应胜任力目标 A0010、A0015 和 A0128。以 Web 服务关闭事件为例,涉及知识点覆盖 NICE 网络安全分析人员所掌握的计算机网络、身份验证、访问控制、密钥管理等 20 个知识点,突出事件处理技能等 6 项技能,支持将网络安全和隐私原则应用于组织需求等 3 项岗位胜任能力培养。相关案例与 NICE KSA 之间的关系如图 1 所示,知识点和技能点间通过符号标签关联,技能点与胜任力间通过方框线形关联,可清晰看到实践案例与 KSA 之间的关联,通过实训课融会贯通专业课知识点培养学员的综合实践技能,使其支撑岗位胜任力的达成。

2.2 面向岗位胜任力培养设计课程教学方法

教师以背景介绍—提示引导—复盘演示—思考讨论方式组织教学,学生以前置知识预习—推理取证—攻击梳理—拓展学习方式进行学习,形成两个闭环,在不断迭代中实现能力培养。具体而言,学生在课前预习教师布置的相关视频、教材内容,教师介绍相关专业背景知识和案例背景,帮助学生复习相关知识、提升学员兴趣,并引导学员联系案例与相关专业背景知识。

学生基于对案例的介绍,在实训环境中寻找相关攻击证据,教师则通过问题引导提示学生的调查方向,同时通过学生的回答、反馈来掌控实训进度。

首先,通过教师或助教的操作示范讲解梳理完整的调查取证过程;其次,学生在此基础上完成取证过程并分析攻击链条,将视角切换到攻击者重现攻击过程以加深理解;最后,通过思考讨论题引导学生分析攻防过程中的具体技术细节并进行拓展学习,从而提升其在处理类似案例的灵活能力。具体教学实施过程如图 2 所示。

本文以 SQL 注入攻击分析与取证案例为例说明相关教学实施过程。首先,课前发布教材预习内容和 MOOC 预习内容,上课时带领学生回顾 SQL 注入成因、常见方法、实现过程、防范方法(见图 3),以巩固基础知识。然后,介绍安全事件背景,包括被攻击对象(Web 服务器)、攻击造成的影响(盗取域中所有计算机名称和用户信息、停止内部服务)等,让学生基本了解安全事件,明确调查取证基本方向。接下来,在学员开展调查取证过程中通过实训云平台实时监测学生操作界面,掌握学生进展情况,适时发布提示问题,引导学生调查方向,等待一段时间后要求学生回答问题(教师适当提示),从而掌控班级整体进度,在所有提示问题发布并回答完毕后给学生一段时间继续实验,然后开始复盘环节带领学生将零散证据梳理为证据链,还原攻击过程。最后,学生从攻击者视角回顾攻击过程,围绕具体技术、工具原理设计思考问题并回答,使学生进一步加强相关理论知识,在实践中将知识融会贯通。

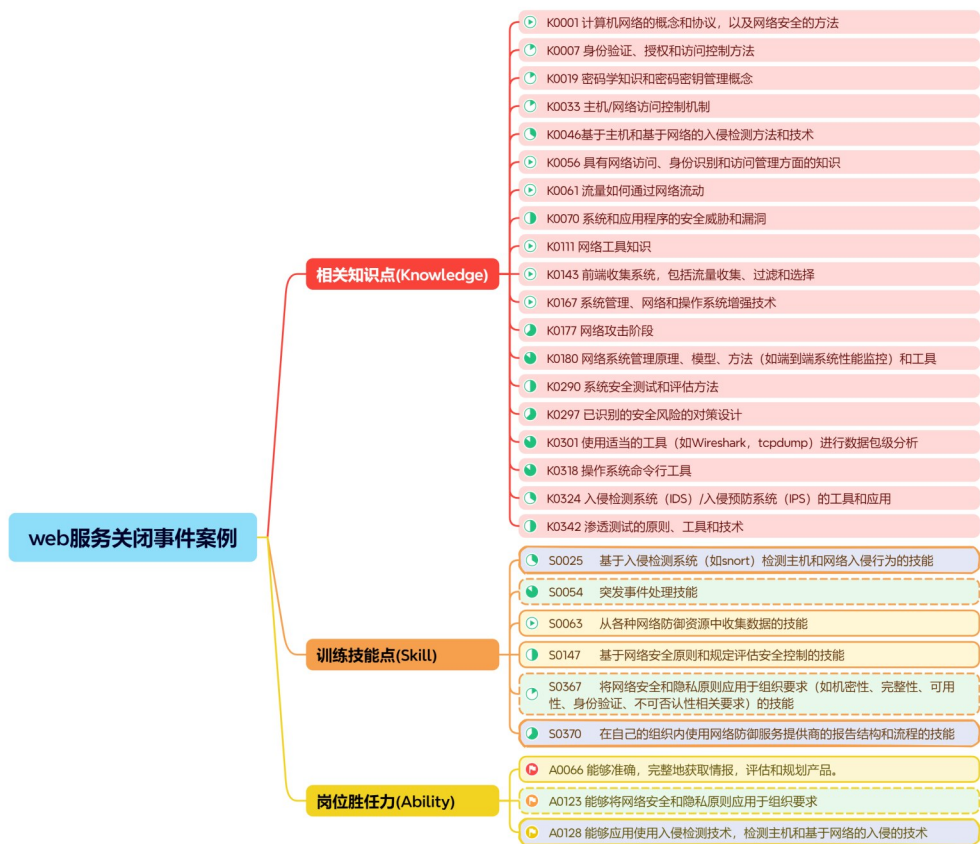


Fig. 1 Case coverage of NICE framework KSA

图1 案例覆盖的NICE框架KSA

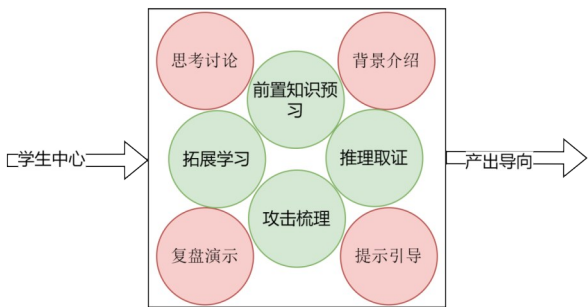


Fig. 2 Teaching implementation process

图2 教学实施过程

3 教改成效

课程成绩构成主要由5个综合案例实验构成,结果如图4所示。改革后sql注入攻击取证与分析实验平均分93分,XSS攻击取证与分析实验平均分92,FTP漏洞攻击取证与分析实验使用平均分91,wordpress漏洞攻击取证与分析实验平均分90,Java邮件中间人攻击取证与分析实验平均分91,由此反映出学生课堂参与度较高、完成度很好、总体优秀,最高分98、最低分81、平均分91,总成绩平均分相较于改革前提高15分。个别学生成绩十分优秀、学习能力较强,能在完成基本实验要求后使用新方法、发现新的攻

击证据,参与处置多起实际网络攻击事件的调查取证,包括某信息中心遭挖矿软件攻击事件、某卫星数据中心遭攻击和挂马事件、某示范实验中心网站遭伪造事件等,得到了合作单位一致好评。

本文围绕课程授课质量设计调查问卷,包括基于五级评价的16项指标(每项指标满分5分),即课程整体框架合理性、课程前后连贯性、课程内容实用性、教师专业程度、授课技巧、教师逻辑思维及表达、教师语言清晰程度、课件完整性、实验与课件结合程度、理论与实操比例、教辅作用、实验平台可用性、实验内容真实性、实验平台内容丰富度、实验与之前所学课程关联度、教材对实验的帮助作用。具体结果如图5所示。

比较课程改革前后评价结果可知,全部评价指标(所有学生评价平均值)均得到了提升,平均满意度提升7.2%,尤其是教师授课能力相关指标项提升显著,但也应该看到实验平台可用性、教材对实验帮助作用、实验与之前所学课程关联度、课程前后连贯性、教辅作用等方面还有进一步改进的空间。此外,调查问卷还设计了4道主观题以了解学员学习收获、学习困难和对课程的改进建议,基于调查结果提取的词云如图6所示。

由图6可见,学生收获主要体现在网络攻防实战技能的提升上,尤其是网络安全取证能力提升(关键词为网络

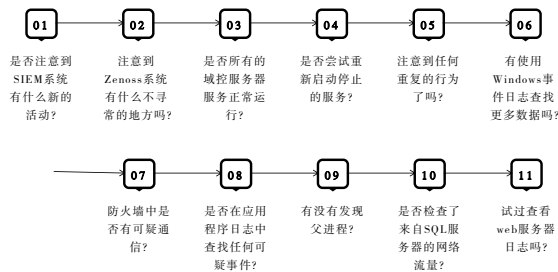
SQL注入背景知识



攻击复盘

侦察	攻击机将发送多个HTTP请求到网站，作为攻击前的侦察操作。
攻击	➢ 通过使用网页的输入框攻击者注入了SQL命令 ➢ SQL命令利用一个MSSQL的内部存储过程运行CMD命令 ➢ CMD命令运行一个服务控制命令以关停域服务 ➢ SQL服务器使用域管理员权限运行，此命令也会停止DC域控服务
控制	通过SQL注入从攻陷的SQL服务器上远程执行在域控服务器上的服务控制管理器以关停域服务

实验提示



思考题

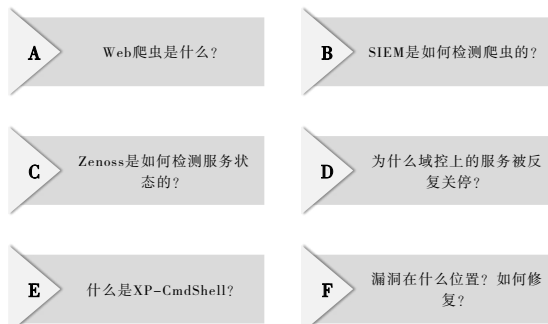


Fig. 3 Sample course design

图3 课程设计样例

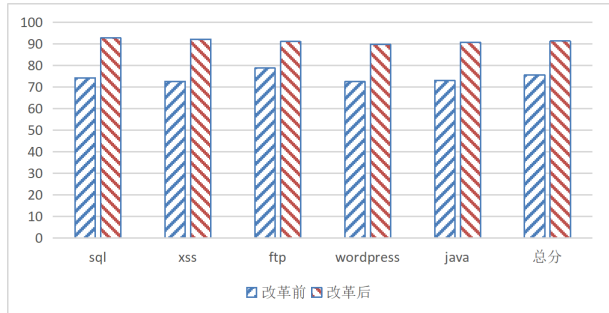


Fig. 4 Comparison of student grades before and after reform

图4 改革前后学员成绩比较

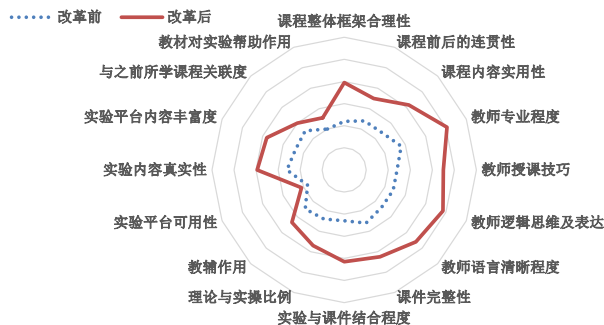


Fig. 5 Comparison of objective evaluation of survey questionnaires

图5 调查问卷客观评价比较

取证、证据链查找、证据收集),原因是该方面能力训练在先前专业课程中较少,学员将理论知识转变为实践技能的过程中面临网络安全工具使用不熟练、专业基础知识掌握不牢、经验缺乏等问题,这些问题也体现在学生对课程建

议中,例如加强前置知识介绍、提供更丰富的实训案例、增加更多实验资源保障实训时间等。



Fig. 6 Survey questionnaire subjective evaluation word cloud map

图6 调查问卷主观评价词云图

4 结语

网络防御涉及知识面广、操作类型多,胜任对应岗位要求学生拥有较好的密码学、网络安全与系统安全相关能力基础和面向岗位需求的综合实践训练。通过合理设计网络信息防御课程为学生奠定良好的基础,包括Linux使用、脚本编程、常见攻防工具使用等技能。从课程授课总体情况而言,大部分学生的安全理论基础和技能掌握较为牢固,能在完成实验基本要求的基础上使用新方法发现一些新的攻击证据,参与处置了多起实际网络攻击事件的调查取证,得到了相关单位一致好评。

未来,将根据学生反馈建议和授课需求升级实训平台,提升实验机器数量、丰富实训案例、编写实训教材,构建由教师、助教和实验保障人员组成的教学团队,争取将网络信息防御课程建设为一流综合实践课程。

参考文献:

- [1] Teaching Guidance Committee for Cyberspace Security Majors in Higher Education Institutions of the Ministry of Education. White paper on practical skills of network security talents —— attack and defense practical skills [EB/OL]. <https://www.yunduijie.com/upload/article/ppt/63366d9b3c49evzYKJlup8y78233.pdf>.
教育部高等学校网络空间安全专业教学指导委员会. 网络安全人才实战能力白皮书——攻防实战能力篇[EB/OL]. <https://www.yunduijie.com/upload/article/ppt/63366d9b3c49evzYKJlup8y78233.pdf>.
- [2] National Computer Virus Emergency Response Center, 360 Company. Investigation report on the cyber attack on Northwestern Polytechnical University by the US NSA (part one) [EB/OL]. <https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm>.
国家计算机病毒应急处理中心, 360公司. 西北工业大学遭美国NSA网络攻击事件调查报告(之一)[EB/OL]. <https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm>.
- [3] CC2020 Task Force. Computing curricula 2020: paradigms for global computing education (CC2020)[M]. New York: ACM/IEEE, 2020.
- [4] LIU Q, ZHAO W T, WANG R J, et al. A competence-based three-layer cybersecurity education framework and its application [C]// ACM TURC 2021: ACM Turing Award Celebration Conference, 2021:54-60.
- [5] HAN Z, WANG X, HUANG X Z, et al. Analysis on the framework of nice cyberspace security talent team in the United States[J]. Confidential Science and Technology, 2012(9): 53-57.
韩臻, 王星, 黄学臻, 等. 美国NICE网络空间安全人才队伍框架探析[J]. 保密科学技术, 2012(9):53-57.
- [6] GE J K, LEI L, HE W B, et al. Construction and application of a practical teaching platform for applied talents in cyberspace security[J]. Journal of Chongqing University of Science and Technology: Social Sciences Edition, 2019(2): 105-107, 115.
葛继科, 雷亮, 何文波, 等. 网络空间安全应用型人才培养实践教学平台建设与应用[J]. 重庆科技学院学报:社会科学版, 2019(2): 105-107, 115.
- [7] XIAO L, CHEN K, FU C, et al. The construction of a comprehensive practice graded customs clearance experimental platform for cyberspace security [J]. Laboratory Research and Exploration, 2021 (10): 236-243, 284.
肖凌, 陈凯, 付才, 等. 网络空间安全综合实践分级通关实验平台建设[J]. 实验室研究与探索, 2021(10): 236-243, 284.
- [8] LI J H. Innovation and practice in cultivating diversified and multilevel cyberspace security talents [J]. Information Security Research, 2018, 4 (12): 1071-1082.
李建华. 多元化多层次网络空间安全人才培养创新与实践[J]. 信息安全研究, 2018, 4(12): 1071-1082.
- [9] MENG C X. Exploration and reflection on the construction of intelligent network security attack and defense countermeasures laboratory [J]. Network Security Technology and Applications, 2020(1):87-89.
孟彩霞. 智能网络安全攻防对抗实验室建设的探索与思考[J]. 网络安全技术与应用, 2020(1):87-89.
- [10] CHEN K, FU C, ZOU D Q, et al. Construction of a graded clearance course system for comprehensive practice of cyberspace security [J]. Journal of Network and Information Security, 2019,5(3):67-74.
陈凯, 付才, 邹德清, 等. 网络空间安全综合实践分级通关课程体系构建[J]. 网络与信息安全学报, 2019,5(3):67-74.
- [11] WANG S B, TIAN H B, ZHANG X N. Design and research of a comprehensive experiment on network and information security [J]. Modern Computers, 2014(7): 46-49, 77.
王盛邦, 田海博, 张新楠. 网络与信息安全综合型实验设计与研究[J]. 现代计算机(专业版), 2014(7): 46-49, 77.
- [12] HUANG B. Exploring the improvement of students' comprehensive practical and practical ability based on the construction of professional courses —— taking network security and law enforcement as an example [J]. Public Security Education, 2021(4): 53-56.
黄波. 依托专业课程建设提升学生综合实践实战能力探究——以《网络安全与执法专业》为例[J]. 公安教育, 2021(4):53-56.
- [13] DENG Q H, XU L. Research and practice on teaching reform based on capstone curriculum concept —— taking the course of "comprehensive experiment of information security" as an example [J]. Computer Knowledge and Technology, 2021, 17(33):165-167.
邓清华, 徐林. 基于Capstone课程理念的教学改革研究与实践——以《信息安全综合实验》课程为例[J]. 电脑知识与技术, 2021, 17(33):165-167.
- [14] LI B L, REN Z Y, WANG W J, et al. Reform and exploration of practical teaching mode for information security major [J]. China Electronic Education, 2015(4): 63-66.
李炳龙, 任志宇, 王文娟, 等. 信息安全专业实践教学模式改革与探索[J]. 中国电子教育, 2015(4):63-66.

(责任编辑:刘嘉文)