Advances in Education 教育进展, 2025, 15(9), 104-111
Published Online September 2025 in Hans. https://www.hanspub.org/journal/ae
https://doi.org/10.12677/ae.2025.1591646

Hans汉斯

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

蒋云鹏[1,2]，梁　义[1,2*]

[1]伊犁师范大学网络安全与信息技术学院，新疆 伊宁
[2]伊犁智能计算研究与应用重点实验室，新疆 伊宁

收稿日期：2025年7月25日；录用日期：2025年8月25日；发布日期：2025年8月29日

摘　要

在数字化时代背景下，网络安全人才培养面临理论与实践脱节、技术更新滞后于教学、学生实战能力不足等困境。本文以伊犁师范大学网络安全课程教学改革为例，提出“三维融合”教学模式，通过课程思政与专业教育融合、虚拟仿真与实战演练融合、过程评价与能力认证融合，构建“价值引领－技能锤炼－质量保障”三位一体的教学体系。实践表明，该模式有效提升了学生网络安全综合素养，为地方高校网络安全人才培养提供了可复制的改革路径。

关键词

网络安全，三维融合，教学模式，课程思政，虚拟仿真

Exploration and Practice of the “Three-Dimensional Integration” Teaching Model of the Cybersecurity Course

—Taking Yili Normal University as an Example

Yunpeng Jiang[1,2], Yi Liang[1,2*]

[1]School of Network Security and Information Technology, Yili Normal University, Yining Xinjiang
[2]Key Laboratory of Intelligent Computing Research and Application, Yili Normal University, Yining Xinjiang

Received: Jul. 25th, 2025; accepted: Aug. 25th, 2025; published: Aug. 29th, 2025

*通讯作者。

文章引用: 蒋云鹏, 梁义. 网络安全课程“三维融合”教学模式探索与实践[J]. 教育进展, 2025, 15(9): 104-111.
DOI: 10.12677/ae.2025.1591646

Abstract

In the context of the digital era, the training of network security talents is facing dilemmas such as the disconnection between theory and practice, the delay in teaching technology updates, and the lack of students' practical ability. Taking the teaching reform of the network security course of Yili Normal University as an example, this paper puts forward the "three-dimensional integration" teaching model, and builds a three-in-one teaching system of "value leadership-skill tempering-quality assurance" through the integration of course ideological and political and professional education, virtual simulation and practical exercises, process evaluation and ability certification. Practice shows that this model effectively improves the comprehensive quality of students' network security and provides a replicable reform path for the training of network security talents in local universities.

Keywords

Network Security, Three-Dimensional Integration, Teaching Mode, Course Ideological and Political, Virtual Simulation

1. 引言

1.1. 研究背景及现状

随着全球数字化转型加速推进，网络安全已成为国家安全的重要组成部分。2016 年，中网办发文[2016] 4 号《关于加强网络安全学科建设和人才培养的意见》，旨在提升国家网络安全人才的培养质量，以适应日益严峻的网络安全形势。但《2025 年全球网络安全人才报告》显示，我国网络安全人才缺口已突破 400 万，网络安全人才仍处于极度匮乏状态，而高校作为人才培养基地，就如何加强网络安全人才培养的研究具有重要意义。伊犁师范大学作为新疆地区重要的应用型人才培养基地，肩负着为边疆地区输送高素质网络安全人才的重要职责。

目前，高校培养的毕业生普遍存在“理论强、实践弱”的特点，难以满足行业对实战型人才的需求。同时高校也在积极探索新型培养模式，例如暨南大学提出基于 OBE 理念的网络安全教学改革研究；抚顺职业技术学院提出的基于虚拟仿真技术的网络安全课程教学质量提升策略等[1]-[3]，都在一定程度上优化了网络安全专业的教育教学，但伊犁师范大学有其边疆地区特殊的生源特点和企业人才需求，需因地制宜地提出适应性解决方案。

本研究提出的“三维融合”教学模式，通过构建完整的教学－实践－评价体系，为缓解网络安全人才培养难题提供了系统解决方案，期望对边疆地区高校培养应用型网络安全人才具有示范作用。

1.2. 课程教学中的问题分析

1.2.1. 行业需求与教学现状的矛盾

网络安全行业对人才的需求呈现出鲜明的实战性、快速迭代性和综合性特点：企业需要能够立即上手解决实际问题的实战型人才，强调快速响应安全威胁和熟练运用安全工具的能力；同时，由于新型攻

击手段和防御技术不断涌现，从业者必须保持持续学习以应对快速变化的技术环境；此外，行业不仅要求过硬的技术能力，还需要人才具备法律意识、职业道德等综合素质，以应对日益复杂的网络安全挑战。

1.2.2. 学情分析

伊犁师范大学网络安全专业的学生呈现出鲜明的群体特征：生源基础差异较大，其中45%的学生来自农牧区，计算机基础相对薄弱；学习动机呈现多元化趋势，部分学生对黑客技术抱有浓厚兴趣，但缺乏专业引导和正确认知；同时受地域条件限制，学生普遍面临实践平台不足、企业实习机会有限等现实困境。这些特点既反映了边疆地区网络安全人才培养的独特挑战，也凸显了专业建设中需要重点关注的基础补强、兴趣引导和实践能力提升等关键问题。

1.2.3. 行业需求与教学现状的矛盾

传统教学模式在网络安全专业培养过程中存在若干亟待改进的问题：首先，课程设置存在“重理论轻实践”的倾向，表现为实践课时不足、实验内容过于简单；其次，教学资源分散且缺乏整合，尚未建立起系统化的实践教学平台；最后，评价方式较为单一，难以全面客观地评估学生的综合能力[4]。这些问题直接影响了人才培养质量，亟需通过优化课程体系、整合教学资源和改革评价机制等措施加以改进。

2. “三维融合”教学模式

2.1. “三维融合”教学模式的概念与特点

“三维融合”教学模式是一种创新性的教学理念，其核心在于将理论教学、实践训练和素质培养三个维度有机整合，形成协同育人的教学体系[5]。该模式具有以下鲜明特点：

- 系统性整合：突破传统教学中理论、实践、素质培养相互割裂的局限，通过课程设计、教学资源和评价体系的整体重构，实现三者的深度耦合与动态平衡。
- 能力导向突出：以行业需求为基准，在理论教学中嵌入真实案例，在实践环节强化工程思维，在素质培养中注重职业伦理，形成“知识–技能–素养”的能力培养闭环。
- 教学形态创新：采用模块化课程、虚实结合的实验平台(如靶场 + 云平台)、多元评价体系(过程性评价 + 攻防竞赛 + 伦理考核)等创新手段，实现教学要素的立体化融合。
- 适应性发展：通过动态调整三个维度的配比(如根据学生基础增加实践强化模块)，既能满足差异化培养需求，又能响应网络安全领域快速迭代的技术特征。

该模式特别适用于网络安全等应用型学科，对解决当前专业教育中普遍存在的理论实践脱节、资源碎片化、评价单一化等问题具有显著优势。

2.2. “三维融合”教学模式的构建

2.2.1. 维度一：课程思政与专业教育融合

通过“三个结合”实现价值引领：一是历史与现实结合，我们讲述了从古代密码学到现代加密技术的发展历程，让学生了解到中国在信息安全领域取得的进步，激发了他们对本专业的兴趣和责任感；二是技术与法律结合，分析网络安全法典型案例，提升法治意识和专业素养；三是个人与国家结合，强调网络安全工作者的社会责任，强化服务国家、奉献社会的担当精神。这三条路径共同构成了价值渗透的完整体系，推动思想引领与专业发展深度融合[6]。

例如，在“网络渗透测试”课程中，通过三个阶段开展价值渗透教育：课前布置“红客精神”相关文献阅读，引导学生树立正确的网络安全观和责任意识；课中深入分析“震网病毒”事件及其对国家安全的影响，增强学生的国家意识和风险防范意识；课后组织“网络安全与公民责任”主题讨论，激发学生

思考个人在维护网络安全中的角色与使命。通过全过程的价值引导，实现专业知识与社会责任的有机融合。

2.2.2. 维度二：虚拟仿真与实战演练融合

构建了三级实践平台以全面提升学生的实战技能和综合素质：基础实验平台基于 VMware 的虚拟化环境，为学生提供安全、灵活的基础实验操作空间；专业实训平台集成了如 Kali Linux 等专业工具，让学生能够深入学习并实践专业的网络安全技能；综合演练平台则支持红蓝对抗的仿真环境，模拟真实网络攻击与防御情境，增强学生的实战应对能力和团队协作能力。这三级平台从基础到高级逐步递进，形成了一套完整的网络安全人才培养体系[7]。

同时采用“三阶递进”教学法，推动学生从基础认知到创新实践的逐步提升：在认知阶段，通过教师演示帮助学生理解基本原理和操作流程；在模仿阶段，学生按照步骤完成实验任务，掌握关键技术与方法；在创新阶段，鼓励学生自主设计网络安全解决方案，培养其综合应用能力和创新思维。该教学模式实现了由浅入深、由被动学习到主动探索的有效转变，提升了学生的实践能力和问题解决能力。

2.2.3. 维度三：过程评价与能力认证融合

构建多元化评价体系，全面衡量学生的学习成效与实践能力：过程性评价通过记录每次实验的完成情况，客观反映学生的学习态度与技能掌握进度；成果性评价侧重于对项目作品质量的考核，检验学生的综合应用与创新能力；第三方评价则引入企业认证标准，增强评价的专业性与行业适应性。该评价体系实现了过程与结果并重、校内与企业联动的多维度评估，有效提升了人才培养的质量与针对性。

将行业权威认证纳入课程评价体系，推动课程内容与职业标准有机衔接：课程中融入 NISP 一级/二级认证要求，强化学生网络安全基础知识与实践能力；对接华为 HCIA-Security 认证标准，提升学生在安全设备配置与管理方面的能力；引入奇安信网络安全工程师认证，增强学生在实际工作场景中的技术应用与问题解决能力。通过多类认证的协同对接，构建了“课证融通”的评价机制，有效提升了学生的专业素养和就业竞争力。

3. 教学实践环节的深化与拓展

3.1. 教学阶段：基于 Kali 平台的实战教学

3.1.1. 平台选择与优势

构建选择 Kali Linux 作为网络安全基础教学平台具有以下显著优势，能够有效支撑“三维融合”教学模式的实施：

1) 专业工具集成优势

学生们可以利用 Kali Linux 平台上预装的安全工具，比如 Metasploit 用于模拟黑客攻击，Burp Suite 来检测网站的安全漏洞，以及 Nmap 扫描网络端口，学习如何进行全面的渗透测试，为教学和实践提供了强有力的支持。工具链持续更新，每季度进行版本迭代，确保与业界最新的攻防技术同步，让学生掌握前沿技能。此外，平台还提供标准化的工具使用环境，有效避免了教学过程中可能出现的环境配置冲突问题，提升了教学效率和学习体验。这一整合措施不仅增强了学生的实战能力，也保证了教育资源的先进性和实用性。

2) 实战教学适配性

平台内置虚拟化支持(如 Kali Linux-VM)，可快速构建包含漏洞靶机的实验环境，为教学提供高度仿真的实战场景。同时支持 Docker 容器化部署，便于搭建灵活、可扩展的分布式攻防演练环境，增强学生对真实网络攻防的理解与应对能力。此外，平台还提供定制化脚本工具(如 Kali-Tweaks)，可根据教学需

求灵活调整系统配置，提升教学与实验的针对性和便捷性。这一系列功能有效支撑了从基础实验到高级实战的多层次教学目标。

3) 教学资源生态优势

平台依托官方提供的结构化学习路径(如 Kali Linux Revealed 课程体系)，为学生构建系统化、进阶式的学习框架；同时拥有活跃的社区支持，整合如 OverTheWire 等优质教学靶场资源，丰富学习内容与实战场景；此外，平台与主流认证体系(如 OSCP)的工具链完全兼容，确保学习内容与行业标准无缝对接，提升学生实战能力与职业竞争力。这一整合有效支撑了“学、练、证”一体化的人才培养模式。

4) 思政教育载体价值

平台基于开源属性，充分契合网络安全领域自主可控的发展要求，保障技术透明与系统安全；内置合规性指南，如渗透测试授权管理工具，帮助学生在合法合规框架下开展安全测试与攻防实践；同时通过工具伦理标签(如“遵守法律”警告提示)强化学生的职业规范意识，引导其树立正确的网络安全法治观念和职业道德准则。该设计有效实现了技术能力培养与法律规范教育的有机统一。

该平台通过其工具完备性、教学友好性和生态丰富性，能有效解决当前网络安全教学中实践平台碎片化、实验环境建设成本高、教学工具滞后于行业发展等痛点，特别适合边疆院校在资源受限条件下开展高质量的网络安全实践教学。

3.1.2. 典型教学案例设计

以“Web 应用安全测试”模块为例，设计以下教学流程，见表 1。

Table 1. Web application security teaching case design
表 1. Web 应用安全教学案例设计

教学阶段	教学内容与任务	课时
环境搭建	使用 Docker 快速部署 BVWA (Broken Web Applications)靶场－，配置 Kali 攻击机与靶机的网络连接	2
信息收集	使用 nmap 进行端口扫描和服务识别，利用 DirBuster 进行目录枚举，通过 Burp Suite 抓取和分析 HTTP 请求	4
漏洞利用	SQL 注入攻击实践、XSS 跨站脚本攻击演示、文件上传漏洞利用、使用 Metasploit 进行漏洞利用	6
权限维持	创建持久化后门、权限提升技术、痕迹清理方法	4
防御措施	WAF 规则配置、安全编码实践、日志审计分析	4
合计	-	20

3.2. 自学阶段：生活化场景驱动的探索学习

3.2.1. 学习情境设计

课程注重贴近生活的安全场景设计，通过实践教学激发学生兴趣，提升网络安全意识与实战能力。内容涵盖多个日常常见领域，如 WiFi 安全、社交工程与移动安全等。例如，在 WiFi 安全教学中，通过演示 WPA2 握手包捕获与破解原理，让学生了解无线网络的潜在风险，并开展无线中间人攻击实验，进一步掌握公共 WiFi 环境下的安全防护措施。在社交工程教学中，组织钓鱼网站制作与识别、伪造邮件发送实验，帮助学生识别常见网络诈骗手段，掌握个人信息防护策略。在移动安全方面，通过安卓 APK 逆向分析，揭示恶意程序的工作机制，结合微信刷票原理探究，提升学生对移动应用安全的理解；同时实践手机数据加密、远程擦除等数据防护技术，增强移动设备使用中的安全意识。通过这些贴近生活的真

实场景设计，有效激发学生学习兴趣，实现“寓教于用、知行合一”的教学目标，提升学生的综合安全素养。

3.2.2. 自主学习支持体系

构建了多层次的支持系统，全面保障学生的学习效果与参与积极性。在资源支持方面，提供定制化的 VM 虚拟机镜像，帮助学生快速搭建实验环境；整理如“永恒之蓝”等经典漏洞的复现教程，提升实战学习的系统性；同时建立知识库和 FAQ 系统，方便学生自主查阅与解决问题。在指导支持方面，设立每周“黑客时间”进行线下答疑，采用高年级学生导师制，发挥朋辈引导作用，并辅以教师在线指导，形成全方位的学习帮扶机制。在激励支持方面，推出“漏洞挖掘”奖励计划，激发学生的探索精神；搭建优秀作品展示平台，增强学习成就感；并将相关表现与课程成绩挂钩，提升学习动力与参与度。通过这一体系化支持机制，有效促进学生由入门到进阶的持续成长。

3.3. 社会实践：企业真实项目演练

3.3.1. 校企合作模式创新

与启明星辰等企业深度合作，构建“三个真实”实践模式，全面提升学生的实战能力与职业素养。该模式以真实项目为基础，由企业提供经过脱敏处理的安全项目资源，涵盖渗透测试、安全评估等多种类型，确保学生在真实业务场景中锤炼技能；在真实角色方面，学生分组担任安全工程师、审计师等实际岗位职责，并通过岗位轮换制度，全面了解网络安全工作的多维度要求；在实践过程中，严格遵循企业真实工作流程，涵盖项目立项、方案设计、任务实施到报告撰写等完整环节，帮助学生熟悉行业运作机制，提升团队协作与项目管理能力。通过“三个真实”的系统设计，有效实现教学与产业需求的无缝对接，助力培养符合行业标准的高素质网络安全人才。

3.3.2. 典型项目案例

通过开展多个实际项目，推动理论与实践深度融合，提升学生的实战能力与社会责任感。一是校园网安全评估项目，组织学生对学校网络进行全面安全检测，发现并修复 15 个中高危漏洞，最终形成 3 万字的安全评估报告，有效提升校园网络防护水平；二是 Web 应用渗透测试项目，对本地企业网站开展授权渗透测试，识别出 SQL 注入等 8 类常见漏洞，并提出针对性的加固方案，协助企业落实安全整改；三是安全意识培训项目，面向学校教职工开展系统性网络安全培训，自主开发培训课程体系，并通过实施钓鱼邮件测试，检验和提升教职工的安全防范意识。通过以上项目的实施，学生在真实环境中锻炼了专业技能，增强了服务意识与责任担当，实现了教学与社会需求的双向互动与共赢。

4. 教学与实践效果评估

4.1. 教学效果评估

建立实验班与普通班来验证本文提出的教学模式的有效性，实验班使用“三维融合”教学模式，普通版使用传统教学模式，教学效果对比见表 2。

Table 2. Comparison of the teaching effect of experimental class and general class
表 2. 实验班与普通班教学效果对比

评估指标	实验班	普通班	提升幅度
工具熟练度	89%	52%	+37%
漏洞识别能力	85%	47%	+38%
综合实战能力	82%	45%	+37%

同时通过问卷调查和实际考核发现：

- 自愿参加课外实践的比例从 35%提升至 78%。
- 平均每周自主学习时间从 2.5 小时增加到 6.8 小时。
- 自主搭建实验环境的能力从 40%提升至 85%。
- 漏洞复现成功率从 30%提升至 72%。

4.2. 实践成效评估

通过企业导师评价和学生反馈：

- 能力提升方面：项目完成度从 60%提升至 92%；文档规范度从 45%提升至 88%。
- 就业竞争力：参与项目的学生就业率 100%；平均起薪比普通学生高 35%。

5. 挑战与反思

在实施“三维融合”教学模式的过程中，我们遇到了一系列挑战。首先，在初期阶段，硬件资源和实验环境的缺乏成为了一个显著障碍。为了解决这个问题，学校通过与企业合作，获得了必要的技术支持和设备资助。例如，通过与启明星辰等企业的深度合作，学生得以接触并使用到真实的网络安全项目资源，极大地丰富了实践教学的内容。

其次，教师团队在如何有效地将复杂的行业知识转化为适合学生的教学内容方面也面临挑战。为此，我们组织了一系列专业培训，并邀请业内专家进行讲座，帮助教师们不断提升自身的专业知识和技术水平。同时，鼓励教师参与实际项目，积累实战经验，以便更好地指导学生。

此外，课程设计时需要考虑如何平衡理论教学与实践操作的比例，确保学生既能够掌握坚实的理论基础，又具备解决实际问题的能力。经过多次调整和优化，最终确定了以案例为基础的教学方法，如在“网络渗透测试”课程中引入震网病毒事件分析，不仅增强了学生的国家意识和风险防范意识，还提高了他们的工程思维能力。

6. 结语

构建“三维融合”网络安全教学模式，既契合网络强国建设需求，又符合边疆地区网络安全人才培养定位，同时响应新工科建设要求；其次，该模式是解决现实矛盾的有效路径，能够缓解传统教学中理论与实践脱节的难题，弥补边疆院校地域资源不足的劣势，切实提升人才培养质量；最后，这一模式顺应教育发展的趋势，既符合高等教育改革方向，又顺应信息技术与教育深度融合的时代潮流，同时契合学生全面发展的个性化需求，为应用型网络安全人才培养提供了可复制的解决方案。未来将继续完善模式内涵，提升人才培养质量。

基金项目

教育部产学研项目：网络安全实验仿真教学平台建设探讨与实践，编号：220704838254957。

参考文献

[1] 张继连, 翁嘉思, 张银炎. 基于 OBE 理念的操作系统原理课程教学改革研究——以网络空间安全专业为例[J]. 高教学刊, 2025. 11(10): 148-151.

[2] 杨阳, 孙皓月, 秦晓慧. 基于虚拟仿真实验教学平台的网络安全实践教学体系研究与构建[J]. 科技资讯, 2024. 22(13): 189-192.

[3] 刘姜. 基于虚拟仿真技术的网络安全课程教学质量提升策略——以抚顺职业技术学院为例[J]. 辽宁师专学报(自然科学版), 2025, 27(2): 46-51.

[4] 牛晓博, 胡正高, 刘曼琳. 网络安全课程对抗式教学方法探索与实践[J]. 网络安全技术与应用, 2025(4): 122-124.

[5] 王晓惠, 陈丽红, 李海霞. 岭南文化视域下高职英语课程思政“三维融合”教学模式研究[J]. 教育导刊, 2023(11): 70-77.

[6] 许艳萍, 任一支, 仇建, 等. 网络空间安全类专业全课程安全思政内生建设[J]. 网络安全技术与应用, 2025(5): 90-94.

[7] 封富君, 李海龙, 沈燮阳, 等. 网络安全课程的教学改革探索[J]. 网络安全技术与应用, 2025(6): 94-97.