# 信息安全教学中网络攻防演练的应用探究

刘晓杰
四川航天职业技术学院　四川成都　610100

**摘　要：**随着信息技术的指数级发展，网络安全威胁呈现智能化、组织化特征。信息安全应用技术专业作为网络空间安全人才培养的主阵地，其教学模式改革已成为实现网络强国战略的关键命题。研究显示，传统以知识点灌输和靶场切割式训练为主的教学范式，导致 62.7% 的毕业生难以独立完成企业级渗透测试（数据来源：2023 年网络安全人才白皮书）。为贯彻 OBE-CDIO 教学模式，本文通过理论和案例分析了安全攻防演练教学的优势和特点后，结合传统教学方式构建了 " 四维联动 " 攻防演练教学模型（“岗需”导向、技术维度、思想流程维度、评价维度），并通过对高职院校学生进行实验，证明该研究对破解职业院校 " 教学 – 产业 " 二元割裂困境具有重要实践价值。

**关键词：**信息安全应用技术；OBE-CDIO 模式；攻防演练教学模型

## 引言

近几年，随着互联网的快速发展，网络安全问题日益突出，2016 年，中国国家互联网信息办公室发布《国家网络空间安全战略》指出：当前和今后一个时期，国家网络空间安全工作的战略任务是坚定捍卫网络空间主权，推进网络空间和平、安全、开放、合作、有序发展，实现网络强国的战略目标 [1]。为了实现这一目标，需要大量的网络安全实用性人才从事网络安全工作，这对各类开设信息安全技术专业的院校提出较高的要求。本文拟在传统教学基础上，从岗、证、赛需求的角度探析网络攻防教学方式在职院校信息安全技术应用专业教学过程的意义。

传统教学体系存在三大结构性矛盾：其一，静态知识传授与动态攻防演进的矛盾，教材更新周期（平均 3.5 年）远滞后于漏洞爆发频率（日均 2.1 万次，据 NVD 统计）[2]；其二，离散技能训练与系统防御思维的矛盾，靶场实验以及 CTF 竞赛多局限在端口扫描、密码爆破等单点技术，缺乏 APT 攻击等复合场景模拟，知识体系和安全思维流程难以串联；其三，标准答案导向与不确定性应对的矛盾，现有实训评分体系难以评估零漏洞利用等非标能力。攻防演练通过构建 " 攻击链 – 防御面 – 响应环”的立体化教学场景，能有效弥合上述鸿沟。

## 1、安全应用技术专业教学现状分析

### 1.1 专业培养要求

随着为响应中共中央办公厅、国务院办公厅印发的《关于推动现代职业教育高质量发展的意见》文件精神，信息安全应用技术专业以岗位需求为目标，以岗位资格证书做要求，用职业技能大赛做推手 [2]，为切实培养出掌握信息安全的基本理论、技术和方法，具备网络安全防护、信息系统安全分析等综合实践能力的学生。

### 1.2 教学现状

传统教学方法以课堂讲授为主，虽能传授知识，但学生参与度和实践能力培养不足。较为依赖学生自学能力。现代教学手段如在线教学平台（如：靶场练习）、虚拟实验室等逐渐应用，但在实际教学中，存在场景固定、缺乏变化，知识技能练习“碎片化”，虚拟实验环境与真实场景脱节、学生综合能力提升有限等问题，且几乎没有机会熟悉和实践企业的真实生产工作，造成工作岗位适应期较长或无法通过企业试用期等情况。

### 1.3 教学成果与面临挑战

虽然传统教学方式下，专业教学和相关比赛等方面取得一定成果，学生对理论知识也掌握的相当不错。但学生实践能力和创新能力方面仍显薄弱，缺乏知识体系的串联场景，缺乏与企业合作提高学生实践和就业能力的成果。面临的挑战包括：实践教学资源有限、师资队伍实践经验不足、教学实训内容单一刻板更新滞后，缺乏一种带动“岗、课、赛、证”充分融通的教学方法等。

## 2、网络安全攻防演练——深度解析

网络安全攻防演练是模拟网络攻击者和防御者之间的

对抗过程，通过模拟各种网络攻击手段，检验和提升网络防御系统的安全性和有效性。其内涵不仅包括技术层面的攻防，还涉及安全策略制定、应急响应流程等方面。

与传统教学对比，攻防演练实现四个范式转移：

**表 1 攻防演练教学的四转移**

| 维度 | 传统教学（靶场、CTF） | 攻防演练 |
|---|---|---|
| 知识构建 | 线性递进 | 网状关联 |
| 能力培养 | 技能分解（离散） | 任务整合 |
| 场景复杂度 | 实验室环境（脱离生产环境） | 准生产环境（半开放） |
| 评价体系 | 标准化评分 | 动态对抗综合评估 |

网络攻防演练实现了以企业生产岗位实践需求为导向、生产实践为要求；通过搭建模拟网络环境进行攻击与防御；线上实时演练，利用网络平台进行实时对抗，实现全面渗透测试演练，对目标系统进行全方位的漏洞挖掘和攻击测试。其知识架构是呈网络结构，能串联各安全实践模块；能力培养方面也是任务整合型的——攻击链或应急响应体系；评价体系更是以实际效果为准，评价体系更灵活多样，更全面。

演练流程包括准备阶段，确定演练目标、范围，搭建演练环境；模拟攻击阶段，实施各种攻击手段；应急响应阶段，防御方检测攻击并采取相应措施；总结评估阶段，分析演练过程，总结经验教训。关键环节包括攻击技术的选择与应用、防御策略的制定与执行、应急响应的及时性和有效性。

**3、网络安全攻防演练教学案例分析**

网络安全攻防演练作为一种最贴近真实安全事件的安全防范练习，能让参与真切实感受到安全事件的诱因，发酵过程和直接、间接的危害，所以其可以提高教师及学生的安全意识和安全能力。

案例 1：以“蚌埠医科大学开展校园网络安全攻防应急演练” 为例，该校组织了针对钓鱼邮件攻击的演练，由网络安全合同单位模拟黑客展开攻击。网络信息中心值班人员在接到预警后，迅速启动应急预案。他们依照所学的信息安全流程，先对邮件内容剖析，随即向全校发布预警，提醒师生勿点击可疑链接 [3]。

演练及其在教学中引用的效果：

应急响应全流程标准化执行：依照 ISO 27031 应急框架，完成“事件分类（钓鱼攻击）→分级（中级事件）→通报（30 分钟内全校预警）→处置→复盘” 全流程。

拆解教学模块：将应急响应流程（预警→分析→隔离→溯源→修复）对应《信息系统安全》课程的 “系统安全防护”、“应急处理”模块，设计 4 大教学任务（邮件分析、威胁隔离、日志溯源、漏洞修复）。

区域安全赋能：向蚌埠市卫健委输出《医疗行业钓鱼邮件防御指南》，协助 3 家医院优化邮件系统安全策略。

案例 2：浙江同济科技职业学院参与浙江省 “护网 2024” 网络安全实战攻防演练：此次演练中，该校在信息安全相关专业开展演练，注重与职业技能认证相结合。演练中学生依据目标确定、信息收集、漏洞探测、漏洞利用、内网渗透以及报告撰写等流程开展工作。学生们将课堂所学网络安全知识充分运用到实战，像在漏洞探测环节，学生们运用在《网络安全技术》课程中学到的扫描技术，精准定位目标系统漏洞，显著提升了实践操作与问题解决能力。通过此类演练，不仅使该校依据比赛反馈优化教学内容，还让学生在演练中熟悉了网络安全设备的操作，提高了就业竞争力，毕业后能快速适应企业网络安全岗位需求，为未来的就业打下坚实基础 [4][5]。

演练及其在教学中引用的效果：

教学转化：将真实攻击链（钓鱼邮件→供应链渗透→权限维持）拆解为 12 个教学模块。

成效数据：学生漏洞挖掘平均深度提升 2.3 层（从应用层→内核层），应急响应平均时间缩短 40%（至 27 分钟）。

通过攻防演练的教学价值重构分析以及对相关案例的分析，可以发现攻防演练对通过案例分析发现学生的能力和素质的提升体现在四个层面：

（1）战术层——提升学生的专业技能：网络安全攻防演练为学生提供了高度仿真的实践环境，学生能够在模拟的网络攻击与防御场景中进行实际操作，提升实践能力。

（2）战役层——实践能力增强：演练让学生在真实的网络环境中解决问题，构建攻击链即：情报收集→漏洞利用→权限维持；积累了丰富的实践经验，提高了动手能力和解决实际问题的能力。

（3）战略层——安全意识、思维与应急处理能力强化：演练使学生深刻认识到网络安全的重要性，增强了安全意识。在面对模拟攻击时，学生能从攻击者的视角对安全事件进行风险评估，够迅速做出反应，按照应急响应流程进行处理，提高了应急处理能力。

## 4、攻防演练教学的问题与应对策略

### 4.1 攻防演练教学中的问题

虽然攻防演练是以岗赛为导向，又时真实生产场景迁移，对学生的能力提升和高职教学有着诸多好处；但由于攻防演练教学是一种较新的教学模式，它依然存在以下问题：

#### 4.1.1 教学体系不成熟

(1) 攻防演练教学难度层级化设置不足：

防演练是一种比较系统的实践操作存在一定难度，直接上手有一定难度，现有课程体系未形成 " 基础能力→专项技能→综合演练 " 的渐进式教学设计，缺乏如 CTF 基础训练、漏洞复现实验等过渡环节。

(2) 团队协作机制建设滞后

攻防演练大多以团队为单位进行，而现行分组多采用随机分配或学生自组，缺乏相关能力和性格测试、技能矩阵分析的科学组队方法，且演练中缺乏对个体贡献度追踪记录体系和“角色轮转”提升能力。

(3) 教学评价体系维度单一化

现有评价方式局限，普遍采用 " 演练结果 + 实验报告 " 的二元评价结构，忽视：能力增量评估（Pre-test/Post-test 对比）、过程性成长档案（包括策略优化轨迹、工具使用进化树）、元能力发展（如应急响应思维、安全合规意识）。

#### 4.1.2 技术难题

攻防演练教学实施中技术难题包括模拟攻击平台技术的局限性，难以模拟新型复杂攻击；安全防护技术的更新滞后，无法有效应对新威胁。解决方案是加强与网络安全企业的合作，引入最新的攻击与防御技术，定期更新演练环境和工具。

#### 4.1.3 资源限制

资源限制主要体现在教学设备不足、师资力量有限。优化措施包括加大教学设备投入，建设专业的网络安全实验室；加强师资队伍建设，鼓励教师参加企业实践和培训，提高实践教学能力。

#### 4.1.4 安全风险

演练可能带来安全风险，如演练过程中的攻击行为影响正常网络运行，泄露敏感信息。防范机制包括建立严格的演练管理制度，明确演练范围和规则；对演练环境进行隔离，确保与实际网络安全隔离。

### 4.2 应对策略

针对攻防演练教学存在的问题，本文将传统教学方式和攻防演练教学方式相结合，构想出 " 四维联动 " 的攻防演练教学模型 [6] 如图 6-1 所示：

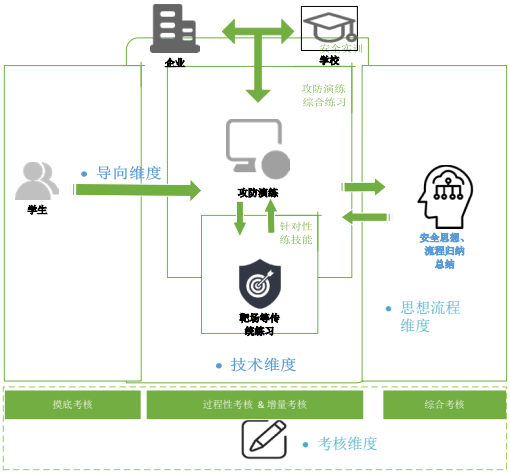


图 1 “四维联动”的攻防演练教学模型

岗位及攻防演练需求导向维度：与企业进行校企合作，引入最新技术共同打造符合岗位和相关证书要求的攻防演练场景，克服师资不足、技术滞后难题，并给出师生学习成长方向和要求。

技术维度：以攻防演练为主体，以传统教学的模块化靶场练习，但深化其在攻防演练场景中的“位置”和作用，并相互印证，使学生能够较容易适应“攻防演练”教学模式；并实行师生入企业实习或共同参与企业安全项目，以克服教学中资源限制的问题。

思想流程维度：以攻防演练为载体，流程化学生的实践演练过程，重视学生安全思维和攻防流程的建立：如：

攻击思维流程：情报收集、攻击面建模、武器化构建、横向移动、痕迹清除等。

防御思维流程：如：物理层：RFID 门禁系统渗透防护，协议层：TCP 序列号随机化加固，身份层：多因素认证（FIDO2 标准）等 15 种标准处置流程 [5]。

评价维度：

规范化操作流程严格管控安全风险，明确明确演练范围和规则。

过程性评价系统：行为数据：Nessus 扫描策略优化次数；认知数据：Snort 规则编写质量评分

增量评价：通过报告答辩等方式从：“技术增量 "，“思

维增量”，“协作增量”，量化学生的综合能力提升。

行业认证衔接：如：漏洞挖掘数量 → 折合学分；应急响应质量 → 兑换 Security+ 认证模块；证书、奖励→ 转换实践学分

4.3 实际论证

为了初步验证“四维联动”+ 攻防演练 3 阶段教学场景教学模式的效果，对我校 21 级和 22、23 级信息安全应用技术专业约 200 名学生进行，攻防演练融入教学实验对比结果如表 5–1 所示：

**表 2 攻防演练教学模式效果对比**

| 指标 | 21 级（基准组） | 22 级（实验组） | 提升幅度 | 关键驱动因素 |
|---|---|---|---|---|
| 省级以上比赛 | 2 项 | 4 项 | +50% | 大运会护网活动（参与 1 项省级赛事） |
| 获奖数 | 1 项 | 3 项 | +200% | 赛前专项集训 |
| 自主挖掘漏洞 | 2 个（低危） | 7 个 | +250% | 漏洞众测平台实战 |
| 岗位专业对口率 | 65% | 85% | +20% | 校企双元培养（企业定制化课程占比 30%） |
| 岗位适应期（月） | 3.2 个月 | 2.0 个月 | –37.5% | 企业级工单系统实训 |

通过对比实验，可以发现该攻防演练教学模式在提升学生的专业技能、综合素质和岗位适应能力方面发挥了较大的作用。

**5、总结**

5.1 研究成果总结

本研究通过对信息安全应用技术专业教学中网络安全攻防演练的实际应用研究，明确了演练在提升学生专业技能、实践能力、团队协作和安全意识等方面的显著效果，同时提出了演练实施中的问题及应对策略的设想，为专业教学改革提供了有益的参考。

5.2 研究的不足与展望

研究存在一定不足，如案例分析的广度和深度有待加强，评估体系的完善性需要进一步提高。未来研究可扩大案例范围，深入研究演练效果的长期跟踪评估，不断完善网络安全攻防演练在教学中的应用。

**参考文献：**

[1] 国家互联网信息办公室 . 国家网络空间安全战略 [R]. 2016

[2] 中共中央办公厅、国务院办公厅 . 关于推动现代职业教育高质量发展的意见 [R] 2021

[3] 蚌埠医科大学信心中心 . 蚌埠医科大学开展网络安全应急演练 [EB/OL] 2024 https://wlxxzx.bbmc.edu.cn/info/1028/2364.htm

[4] 浙江同济科技职业学院 . 信安专业师生受邀参加浙江省“护网 2024”网络安全实战攻防演练 [EB/OL] 2024 http://ggx.zjtongji.edu.cn/content.jsp?urltype=news.NewsContentUrl&wbnewsid=4231&wbtreeid=1081

[5] 深信服科技 . 应战正当时 | 记一次供应链攻击实例分析，附企业长短期防范建议 [EB/OL] 2023 https://www.sangfor.com.cn/news/633bc9eebc1a463684cc9f2a5dd5a738

[6] 刘坤 , 庾佳 . 高职信息安全技术应用专业课程教学改革探索——以网络攻防与实践课程为例 [J]. 河北软件职业技术学院学报 ,2022,24(04):40–43

**作者简介：**刘晓杰（1990.06），男，讲师，硕士，主要从事模式识别研究及软件设计开发教学工作。