# 基于虚拟化技术的网络安全实验教学改革研究与实践

张玲娟，张朝锋 *
东华理工大学 信息工程学院，江西 南昌 330013
DOI: 10.61369/TACS.2025110033

**摘　　要：** 培养具备扎实实践能力的创新型网络安全人才是国家的战略需求，网络安全实验教学是安全人才培养的关键环节。传统网络安全实验教学存在设备资源更新慢、环境隔离性差、扩展性不足等问题，从而制约了教学育才的效果。针对以上问题，本文基于虚拟化技术，设计了以资源管理、环境配置、过程监控和结果评估为核心模块的实验教学系统，探索实践“理论－演示－实践－分析”的一体化实验教学模式。通过设计网络安全教学实验案例以及多维度体系评估，验证了系统在提升教学效率、培养学生实践和创新能力方面具有显著成效。研究可为相关院校网络安全实验教学改革提供参考。

**关 键 词：** 虚拟化技术；Docker；实验教学；教学改革；网络安全

## Research and Practice on the Reform of Network Security Experiment Teaching Based on Virtualization Technology

Zhang Lingjuan, Zhang Chaofeng*
School of Information Engineering, East China University of Technology, Nanchang, Jiangxi 330013

**Abstract:** Cultivating innovative cybersecurity talents with solid practical skills represents a strategic national imperative, wherein experimental teaching plays a crucial role. Traditional approaches to cybersecurity experimental teaching suffer from issues such as slow updates of equipment resources, inadequate environmental isolation, and limited scalability, which constrain teaching effectiveness and talent development. To address these challenges, this paper proposes a virtualization technology-based experimental teaching system, with core modules for resource management, environment configuration, process monitoring, and result evaluation. Furthermore, it implements an integrated "theory-demonstration-practice-analysis" teaching model. By designing specific cybersecurity experimental cases and conducting a multi-faceted evaluation, the system demonstrates significant effectiveness in enhancing teaching efficiency and fostering students' practical and innovative capabilities. This study offers a valuable reference and a practical solution for relevant institutions to reform their cybersecurity experimental teaching.

**Keywords:** virtualization technology; docker; experimental teaching; teaching reform; cyber security

## 引言

网络安全是国家安全体系的关键组成部分，也是数字经济健康发展的基本保障。《2024年网络安全产业人才发展报告》指出，我国网络安全人才缺口持续扩大，预计到2027年人才需求规模将达到数百万人，其中具备扎实工程实践能力与应急响应技能的高水平人才尤为紧缺。该现实对高校网络安全人才培养提出了更高要求，实践教学是网络安全专业教学的关键环节[1]。传统网络安全实验教学依托实体物理实验室，主要存在：（1）实验设备资源更新缓慢，难以适应新的攻防技术演练场景需求（例如，部分实验室仍在使用已停止维护的旧版操作系统或安全工具）；（2）环境部署隔离不足，攻防实验具有潜在破坏性，易造成系统崩溃或网络干扰，甚至造成设备物理损坏等问题，恢复成本高；（3）缺乏弹性扩展能力，教学内容不能紧跟产业需求。这些问题限制了学生实践能力的系统培养，进而制约了教学育人的效果[2]。

虚拟化技术具有资源隔离、灵活扩展、性能优化和跨平台兼容性等特点，可对实验教学的物理资源进行整合、隔离，形成可动态调度、按需分配的逻辑资源池[3]。

基金项目：东华理工大学实验技术研究开发项目（编号：DHSY-202418）。
作者简介：张玲娟，女，硕士，高级工程师，研究方向：计算机应用技术。
*通讯作者：张朝锋，男，博士，高级工程师，研究方向：软件工程项目管理，地学大数据分析。

 

## 一、理论技术基础

### （一）虚拟化与容器技术

虚拟化技术，特别是容器技术，是构建实验教学系统的核心工具，具有以下优势。（1）环境隔离性。容器通过 Linux 内核的命名空间实现进程、网络、文件系统等资源的隔离，并通过控制组限制资源使用[4]。每个实验运行于独立的容器环境中，显著减少实验对底层系统的潜在破坏风险，并保证多个实验的独立性。（2）快速部署与管理。实验环境可以模板化构建为容器镜像，实现通常在5秒内完成启动与恢复，大幅提升教学效率[4]。

### （二）项目驱动教学法（PBL）

项目驱动教学法（Project-Based Learning，PBL）以学生为中心，通过完成一个完整的、具有挑战性的项目来组织学习[5]。虚拟化技术为 PBL 的实施提供了理想平台，教师设计如“SQL 注入攻击”、“特定应用漏洞挖掘”、“操作系统安全防护”等实操性项目，学生利用虚拟化平台完成实操项目内容，将实验环节从实体实验室延伸至线上虚拟空间，实现线上学习与线下教学有机结合的混合式教学[6]。

## 二、系统设计与教学优化

结合上述理论技术，设计了一个基于 B/S 模式的层次化、模块化的网络安全虚拟化实验教学系统（表1）。系统部署于校园数据中心，用户可通过校园局域网直接访问。为支持混合式教学，同时提供了基于 SSL VPN 的远程安全接入方式访问，确保远程实验操作的安全可控。

表1 传统实验模式与虚拟化实验模式对比分析

| 对比维度 | 传统实验模式 | 虚拟化实验模式 | 优势分析 |
| --- | --- | --- | --- |
| 资源利用率 | 低，设备专用，空闲时段无法共享。 | 高，资源池化，按需分配，多用户共享。 | 大幅降低硬件成本，绿色节能。 |
| 环境隔离性 | 差，实验操作易相互干扰或导致网络瘫痪。 | 强，每个实验环境运行于独立的沙箱中。 | 虚拟环境保障教学安全，允许进行破坏性实验。 |
| 扩展弹性 | 困难，受限于物理设备数量与性能。 | 强，可快速实现实验环境克隆、扩展。 | 支持规模化、并发式实验需求。 |
| 部署效率 | 慢，手动安装配置，耗时数小时至数天。 | 快，基于资源库模版与自动化工具快速实现。 | 提升教学效率，使学生聚焦于核心技能。 |
| 教学灵活性 | 低，局限于固定时间、地点的实验室。 | 高，支持随时随地通过浏览器访问实验系统。 | 支撑混合式教学与自主学习。 |

### （一）系统设计

1. 实验资源管理模块

该模块是系统的基础，负责对所有实验资源进行虚拟化、标准化和生命周期管理。

（1）资源虚拟化与标准化。将操作系统（如 Kali Linux，Windows Server）、安全工具（如 Wireshark，Nmap，Snort）、应用服务（如 Web 服务器、数据库）等封装成标准的 Docker 容器镜像或虚拟机镜像。这实现了实验环境的“一次构建，随处运行”[7]。

（2）统一管理与快速部署。建立中心化镜像仓库，对所有镜像进行版本控制[8]。教师可以基于基础镜像定制实验模板，学生一键即可获取预设的实验环境，将环境准备时间从传统模式下的数小时至数天极大缩短至几分钟以内。

2. 实验环境配置模块

该模块是系统的核心，利用虚拟化技术动态构建隔离的实验网络。

（1）混合虚拟化技术。采用“容器与虚拟机混合”的架构以兼顾灵活性与兼容性。对于需要轻量级、快速启动和高并发的单一服务或工具环境，优先采用 Docker 容器。对于需要完整操作系统内核、特殊设备驱动或模拟特定硬件（如网络设备）的复杂实验场景（如模拟完整的 Windows 域网络攻防），则使用 KVM 全虚拟化技术[9]。

（2）自动化部署。通过软件定义网络（SDN）技术，实现实验网络拓扑的自动生成与灵活配置，支持自定义的虚拟网络隔离与连接。

3. 实验过程监控模块

该模块实现对学生学习过程的精细化指导与评估。

（1）操作行为记录。实时记录学生在实验环境中的关键操作命令、网络流量变化、系统日志等。当学生长时间无进展或执行了错误命令时，系统触发提示信息，协助教师指导学生，实现个性化的实验辅导。

（2）资源使用监控。监控各实验环境的 CPU、内存、网络带宽使用情况，为系统优化和资源调度提供数据支持。

4. 实验结果评估模块

该模块用于建立科学、客观、自动化的评估体系。

（1）多维度评估指标。设计包含实验目标正确性、实验完成效率、操作过程规范安全，和实验报告质量的综合评估指标。

（2）优化评估方式。集成自动化评估脚本[10]。对于漏洞挖掘实验，系统可自动扫描目标环境，验证漏洞是否存在及是否被正确利用；对于防御配置实验，可运行自动化渗透测试脚本，检验防御策略的有效性。

### （二）教学优化

1. 精细化实验模式

将“理论讲解—案例演示—实践操作—结果分析”模式进行细化。

（1）理论讲解。引入交互式虚拟演示。例如，教师在讲解“开放扫描中涉及的 TCP 三次握手”时，结合动态模拟图讲解理论后，可实时在虚拟环境运行扫描命令，查看扫描过程，再给学生讲解分析扫描结果，使抽象理论具象化。

（2）案例演示。实验案例可以教师实时操作演示与虚拟环境操作步骤录屏回放相结合，学生可反复查看练习，切实掌握课程相关知识点。

（3）实践操作。学生根据实验教学任务，按照实验目的与要求、实验步骤自主开展实验练习，在具体操作过程中注意发现问题并记录，尝试找到解决方案。

（4）结果分析。学生结合试验过程总结分析问题，在实验报告中阐明“做了什么、出现了什么问题”，分析出现问题的原因

 

以及如何解决问题。

2. 多元化案例教学

课程实验案例设置经典的漏洞案例（如 SQL 注入、XSS），引入基于真实事件的 APT 攻击模拟、网络设备及协议安全、防火墙安全配置等常见的攻防技术应用案例；选取三个具有代表性的实验（表2）。

表2 实验案例设计与学习目标对应表

| 实验案例 | 核心知识点与技能点 | 虚拟化技术实现 | 教学目标（认知 / 技能 / 素养） |
| --- | --- | --- | --- |
| SQL 注入攻击与防御 | Web 应用架构、SQL 语法、自动化工具使用、代码安全、WAF 原理。 | DockerCompose 一键部署 LAMP+ 漏洞 Web 应用。 | 认知：理解 SQL 注入原理与危害。<br>技能：掌握利用和防御 SQL 注入的方法。<br>素养：培养代码安全与责任意识。 |
| Wireshark 抓取协议包分析 | 流量捕获、协议解析、故障诊断、取证分析 | Docker Compose+ 虚拟机构建靶场与分析环境 | 认知：理解通信原理与明文风险。<br>技能：掌握分析与诊断方法。<br>素养：培养安全意识与职业道德。 |
| DDoS 攻击模拟与缓解 | DDoS 攻击类型（如 TCPFlood）、流量分析、流量清洗与限速策略、云安全服务。 | KVM 虚拟机模拟攻击节点与目标，SDN 配置限速策略，IP 黑名单等。 | 认知：理解 DDoS 攻击的巨大破坏力。<br>技能：掌握基本的流量识别与缓解技术。<br>素养：树立网络防护的整体安全观。 |

实验1：SQL 注入攻击与防御（Web 安全基础）。学生利用 Docker 快速部署一个包含漏洞的 Web 应用，使用 SQLMap 等工具进行自动化注入，并通过代码修复（参数化查询）进行防御。

实验2：Wireshark 抓取协议包分析（流量分析）。学生在虚拟网络中完成捕获、过滤、分析数据包。深入理解 TCP/IP 模型中各层的职责，以及数据包从应用层到物理层的封装过程。分析提取关键通信证据，并基于流量特征分析安全事件的发生过程。

实验3：DDoS 攻击模拟与缓解（网络防护）。学生在虚拟网络中构建攻击者、目标服务器和防御节点（如清洗设备）。通过 hping3等工具模拟 TCP Flood 攻击，并学习通过流量限速、IP 黑名单和云服务商的高防 IP 服务进行缓解。

## 三、教学实践与效果评估

### （一）系统测试

在部署完成后，对系统进行了全面测试。（1）功能测试：验证各模块功能正常，环境创建、启动、关闭、回收流程顺畅。（2）性能测试：模拟一个教学班（63名学生）并发创建虚拟实验环境，平均创建时间在3分钟以内，系统响应流畅，满足教学要求。（3）安全测试：邀请安全团队对系统管理门户、API 接口及宿主机进行渗透测试，修补了发现的漏洞，并采用严格的网络策略与用户权限隔离，有效防止了容器逃逸或越权访问。

### （二）教学效果分析

针对网络空间安全专业2023级和2024级两个教学班进行对比应用分析（2023级使用初期系统，2024级使用优化后系统），一个学期后的应用数据显示：

（1）实验完成率提升。由于实验环境的易获取性和实操性，学生课后自主学习时间增加，实验总体完成率从初期的约90% 提升至98%。

（2）实验成绩提高。课程实践考核环节平均分提升约8个百分点。分析其原因，系统提供的即时反馈和可重复的实验环境，使学生能更有效地进行试错与深度学习，从而提升了问题解决能力。

（3）综合能力得到锻炼。部分学生利用该系统自主完成拓展实验，并在全国大学生信息安全与对抗技术竞赛、护网行动等实践活动中取得了良好成绩，体现了系统对学生创新与实践能力培养的促进作用。

## 四、结论与展望

（1）针对传统网络安全实验教学存在的资源更新慢、环境隔离性差与扩展能力不足等关键问题，本研究构建了基于虚拟化技术的实验教学体系。通过集成资源管理、环境配置、过程监控与结果评估四大核心模块，实现了实验资源的统一调度与高效利用，有效提升了教学基础设施的支撑能力。

（2）教学实践表明该实验教学系统显著改善了实验教学效果。实验环境部署时间由传统模式的数小时缩短至分钟级，实验完成率达到98%，学生实践考核成绩提升约8个百分点。

（3）研究验证了虚拟化技术与现代教学理论深度融合的可行性与有效性，形成了可推广的网络安全实践教学解决方案，为新工科背景下的实验教学改革提供了实践参考。

## *参考文献*

[1] 工信部教育与考试中心，等 .2024年网络安全产业人才发展报告 [R].2024.

[2] 张伟，刘洋 . 虚拟化与容器技术在计算机实验教学中的应用研究 [J]. 计算机教育 ,2022,(10):156-160.

[3] 张亮，闫昊 . 基于容器虚拟化的网络安全实验平台设计与实现 [J]. 信息与电脑（理论版）,2020,32(20):132-134.

[4] 王晓东，等 . 基于 Docker 的网络安全虚拟实验环境构建 [J]. 信息安全研究 ,2020,6(8):733-738.

[5] 林英，李彤，杜磊 . 创新设计课程项目驱动教学法探索 [J]. 计算机教育 ,2015,(09):72-74.

[6] 田丹，杨玥 . 计算机基础课程的混合式教学模式设计与实践 [J]. 电子技术 ,2023,52(11):393-395.

[7] 朱辉，刘北水，李晖，等 . 基于虚拟化技术的信息安全实验平台开发与应用 [J]. 武汉大学学报（理学版）,2012,58(S2):249-252.

[8] 曾小英 . 基于虚拟化技术的网络安全实验平台设计 [J]. 信息技术与信息化 ,2020(3):103-105.

[9] 周世杰，吉家成，王华，等 . 虚拟仿真实验教学中心建设与实践 [J]. 计算机教育 ,2015,(9):5-11.

[10] 赵磊，高岭 . 基于自动评估的编程实验教学系统研究 [J]. 计算机应用与软件 ,2019,36(4):1-5.

 