# 信息系统安全防护虚拟仿真实验项目的设计与实践

赵斐 赵敏 王金双 潘林 申海霞

陆军工程大学指挥控制工程学院，南京 210007

**摘 要** “信息系统安全防护”课程是一门实践性非常强的课程，对于培养信息安全相关专业学生的操作系统、数据库系统和应用系统安全防护能力具有重要作用。针对课程目前实装实训的困境，以及现有实验平台的缺陷，根据信息系统安全防护能力培养的需要，提出信息系统安全防护课程虚拟仿真实验项目的设计思路，建设了相关资源，并对虚拟仿真训练平台的设计和建设总结了几个要点问题。课程虚拟仿真实验教学突破了现网、现装对实验的限制，有效提高了实验教学的内涵质量和育人水平。

**关键字** 信息系统安全防护，虚拟仿真，实验教学

# Design and Practice of Virtual Simulation Experiment Project for Information System Security Protection

Zhao Fei Zhao Min Wang Jinshuang Pan Lin Shen Haixia

Command and Control Engineering College, Army Engineering University, Nanjing 210007, China

**Abstract—The course of "Information System Security Protection" is a highly practical course that plays an important role in cultivating the security protection capabilities of operating systems, database systems, and application systems for students majoring in information security. In response to the current difficulties in practical training of the course and the shortcomings of the existing experimental platform, and based on the needs of cultivating information system security protection capabilities, this paper proposes a design concept for the virtual simulation experiment project of the information system security protection course, constructs relevant resources, and summarizes several key issues in the design and construction of the virtual simulation training platform. The virtual simulation experiment teaching of the course breaks through the limitations of the current network and installation on experiments, effectively improving the connotation, quality, and educational level of experimental teaching.**

**Keywords—Information system security protection, virtual simulation, experimental teaching**

## 1 引 言

信息系统安全防护（简称系统安防）课程是信息安全及相关专业的核心课程，课程的教学目标是培养学生具有全面的系统安防技能。系统安防课程具有非常强的实践性，需要系统的实验和实训，然而由于系统安防实验的特殊性和破坏性，在现网设备上进行设备配置、攻防实训很可能会对真实网络设备和主机造成严重危害。同时，现有的实验平台存在沉浸式学习体验感差、实验项目单调等问题，无法有效激发学生的学习积极性，严重制约了系统安防能力的提升。

教育部于 2017 年发布了《关于 2017-2020 年开展示范性虚拟仿真实验教学项目建设的通知》，积极推进现代信息技术与实验教学的深度融合，开展示范性虚拟仿真实验教学项目建设工作[1]和国家虚拟仿真实验教学项目的认定工作，激励和引领高校开展实验教学改革与创新，建设虚拟仿真实验教学项目，给课程的实验教学改革指出了建设方向。

本文主要从实验平台和实验内容两方面入手，讨论虚拟仿真训练平台的建设需求和虚拟仿真实验科目的设计与实践。经过一个阶段的实践运用，发现系统安防虚拟仿真实验有效提高了学生学习兴趣，激发了学生深入钻研系统安防原理的热情，切实提高了学生系统安全防护的实战能力。

## 2 系统安防课程实验教学存在的问题

信息系统安全防护课程主要涉及密码学、网络安全、系统安全、数据库安全和应用安全等安全防护技术的综合运用，课程的培养目标是使学生掌握信息系统安全防护的理论和技术，掌握常用安全防护设备的运维技能，能够识别、发现信息系统中潜在的安全威

胁和风险，能分析其原因并设计对应的修复、防御方法，并能利用密码工具、操作系统安全技术、数据库安全技术、网络安全技术、应用系统安全技术等对信息系统进行安全配置和加固，能设计和构建信息系统安全防护体系，具备一定的信息系统安全防护能力。

由此可见，系统安全防护课程涉及的知识面广、概念抽象、实践性强，教学难度非常大，必须通过实验实训加深对基本理论的理解，促进安防能力的生成。

### 2.1 实装实训的困境

如果采用真实的物理主机和设备搭建网络环境，安防设备品种多，价格贵。如防火墙、入侵检测设备、接入认证设备等，类型多、型号多、维修困难。配置多套安防设备开支巨大，管理困难。如果学生误操作，设备恢复周期长，有时甚至需要返厂维修，很难保障实验教学的正常开展。

另外，安防设备、主机等需要组网运行，而实际设备组网比较单一、固定，无法提供实际的复杂多变的网络拓扑，与现装现网操作脱节。

再者，系统安全防护相关实验对目标信息系统往往会造成严重的危害，实验环境的恢复非常困难。即使实验室搭建了用于网络攻防实验的局域网，一些攻击实验会造成主机死机，局域网瘫痪等问题。如木马攻击实验可能会损害实验室主机，甚至在整个局域网中蔓延传播。因此，在实际环境中实施渗透攻击实战操作非常受限。

### 2.2 现有实验平台的现状分析

在计算机类课程的教学中，虚拟机技术和仿真模拟软件用于开展实验教学已经很多年。

在系统安全防护和网络安全防护实验教学中，现在已较为广泛地建设网络空间安全靶场、网络攻防模拟实验平台、信息安全攻防实训环境等各类实验平台，实验平台多采用虚拟机技术实现主机的模拟仿真，制作虚拟机镜像文件，镜像预先设计多种漏洞[3][4]；网络模拟主要通过利用数学建模和统计分析的方法，通过建立网络设备和网络链路的统计模型，模拟网络流量的传输，从而获取网络设计及优化所需要的网络性能数据。常用于网络仿真的软件有 Boson NetSim、Cisco Packet Tracer、ensp 等，可以模拟路由器和交换机的功能。用于模拟网络流量的软件有 TrafficEngine、hping、netsniff-ng 等，netsniff-ng 可以模拟 DDOS 攻击以及进行数据包捕获和网络监控。

以上实验方式很大程度上满足了系统安防实验教学的需求，各仿真软件都提供了非常专业的功能仿真，但存在的问题主要有：

（1）沉浸式学习感体验差

各种仿真软件较少关注设备外形、环境和应用场景的仿真。因此，实验场景仿真度不高，设备原理、协议运行机理、流量情况都不能做到可视化，而协议运行机理、设备原理等又非常抽象，学生对设备实物、网络拓扑和攻防过程都缺乏感性认识，实验感受与真实场景之间总有一种隔膜感。

（2）实验环境单一

各仿真软件都提供了非常专业的功能仿真，但是很难在一个实验平台中将它们集成在一起。目前学校建设的训练环境主要提供针对各种网络安全漏洞场景的目标环境，网络拓扑简单固定，靶场结构通常较为简单。

（3）实验项目单调

受实验环境所困，原来的实验教学作为理论教学的附属而存在，主要用于系统安防理论的验证，在整个教学内容中占比低、内容老套，综合型实验、创新型实验设置不足，跟不上技术更新的节奏，极大地限制了学生的理实结合，影响了创新能力、系统安防能力的生成。

## 3 系统安防虚拟仿真实验规划

虚拟仿真实验是指借助于三维图形建模、数值模拟仿真、机器学习和人工智能等技术，在计算机上营造可辅助、部分替代甚至全部替代传统实验各操作环节的相关软硬件操作环境，实验者可以像在真实环境中一样完成各种实验项目。搭建虚拟仿真训练平台实现设备模拟仿真、网络架构仿真等，能弥补原有实验方式的欠缺，为系统安全防护课程的实验教学开辟了新方向。

系统安全防护课程经过多年的建设，课程组对课程已有较好的理解，形成了较为成熟的实验教学体系，但是，教师们对于结合虚拟仿真实验环境的教学研究经验不足。对于结合虚拟仿真技术形成新的实验教学体系，还需要对原有实验内容进行组梳理、调整和设计，才能充分发挥虚拟仿真的作用，对实验目的达成起到强力助推作用。

### 3.1 实验内容规划

系统安全防护课程涉及的知识面广，技术更新快，实验内容多。实验内容的设计必须考虑几个因素：

一是必须涵盖系统安全防护完整的知识体系。按照基于计算机网络体系结构的信息系统体系结构，课程组按照从数据链路层到应用层的层次将系统安全防护实验的内容分为密码学、网络安全、系统安全、数

据安全和应用安全等五大模块，如图 1 所示，每个模块包括实验项目对应的技术原理、设备认知、防护方法等。但是课时是有限的，课程组从每部分的实验中挑选出有代表性的实验项目在课上实施，其他实验则可以让学生课下自主完成。

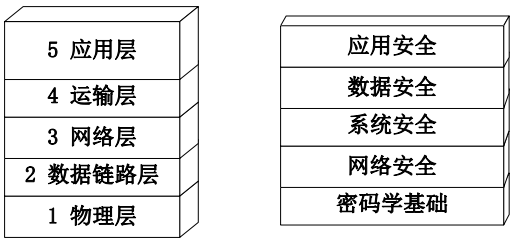


图 1 实验内容覆盖

二是实验内容应循序渐进，遵循学生的认知规律。课程组按照由原理到实战、由单装到组训的原则设置实验阶段，将实验阶段划分为：单装训练、网络架构搭建训练和综合训练三个部分，见表 1。

表 1 实验阶段设置

| 阶段 | 主要内容 |
|---|---|
| 单装训练 | 8 种常用网安设备仿真训练 |
| 网络架构搭建训练 | 练习网络架构搭建的整体过程及操作技巧 |
| 综合训练 | 各模块系统安防仿真实训和综合运用训练 |

三是应虚实结合、能实不虚。能使用真实设备开展实验的就不采用虚拟方式。应将虚拟仿真实验项目和真实实验项目结合起来，是二者真正融合，相互补充[5]。如虚仿实验建设中，可以将防火墙设备虚拟化，但同时，最好要能够支持真实的设备的接入，能够在真实的设备上进行操作。

## 3.2 实验项目的设计

系统安防技术发展的非常快，课程组在实验项目设计上遵循贴近实装实战、科教融汇的原则，将实装、实网、实际安全事件和攻防新技术引入实验教学内容。

实验项目的三个阶段分别为单装训练、网络架构搭建训练和综合训练。

（1） 单装训练

在单装训练中，按照课程知识体系所应覆盖的密码学、网络安全、系统安全、数据安全和应用安全等五大部分，遴选其中 8 种常用网安设备进行仿真训练，见表 2。

表 2 单装设备

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 名称 | 防火墙设备 | 网络入侵检测设备 | 交换机 | 网流量监测设备 | 单向传输设备 | 漏洞扫描设备 | 路由器 | 接入认证设备 |

单装训练包括设备详细信息和设备功能学习、设备的连线和设备的配置与使用。学生在该部分身临其境地认知设备外观，练习设备的配置操作，熟悉设备工作流程。原来通过理论讲授形式进行的设备讲解、原理讲授，现在都可以通过沉浸式体验、游戏化交互和可视化展示，化繁为简、寓教于乐，达到单装模拟操作训练的目的。安防设备或以虚拟化形式存在，或真实存在，都可以以 web 形式访问，与真实机器的设置无异，如图 2 所示。


图 2 单装设备，某型号防火墙

同时，设备放置在典型的网络拓扑中，如图 3 所示，每一个设备是一个网络节点，通过游戏闯关的方式确定是否正确部署了该设备，练习安防设备在网络拓扑中的位置和作用。

（2） 网络拓扑架构训练

网络拓扑是网络安全的基础内容。在进行系统安防训练之前，通过实时交互操作形式练习网络拓扑架构的整体过程及操作技巧，夯实基础，为系统安防训练做准备。

在网络拓扑架构训练中，系统提供统一网络仿真平台，如图 4 所示，支持超过 140 种网络设备的使用。老师设置网络拓扑架构需求，介绍特定类型的网络架构，引导学生以正确的顺序和位置拖拽排列，完成搭建。

网络拓扑架构训练后，学生能够充分学习各类网络拓扑的优缺点，能够在攻防之中学以致用。

（3） 综合训练

综合训练分为分层次系统安防仿真实训和综合运用训练。

① 各模块系统安防仿真实训

课程组同样基于课程知识体系，设计复杂场景下的系统安防实训，在前两部分的基础上，对于设备组网后，能够开展的包括密码学基础、网络侦察渗透、操作系统安全、Web 安全、数据库安全、应用安全等各模块的网络渗透和系统安全防护方面的实训实验。

本部分实验着重于系统安防原理的理解、体会和验证，以及安防技术的运用，在实践中探索安防原理的内在关系，从而建立完整的知识体系，如图 5 所示。

② 综合运用仿真训练

在系统安防综合运用仿真训练中，课程组以典型战例为脚本，按需裁剪，设置网络攻防环境，系统自动生成命令进行攻击；学生选择训练开始后，随机发生病毒感染、黑客入侵、业务数据损坏等网络攻击事件，学生需根据前面所学知识分析和确定攻击意图，进行安全防护的筹划，开展设备部署设置、综合组网等相关操作，完成攻击定位、取证分析、系统恢复等一系列工作，见图 6。

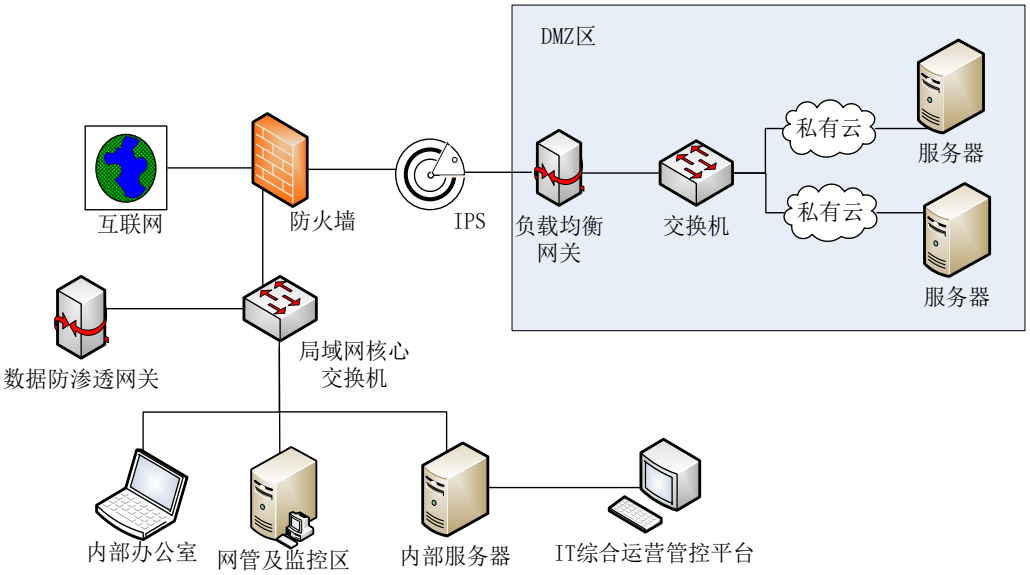


图 3 单装在网络拓扑中的部署

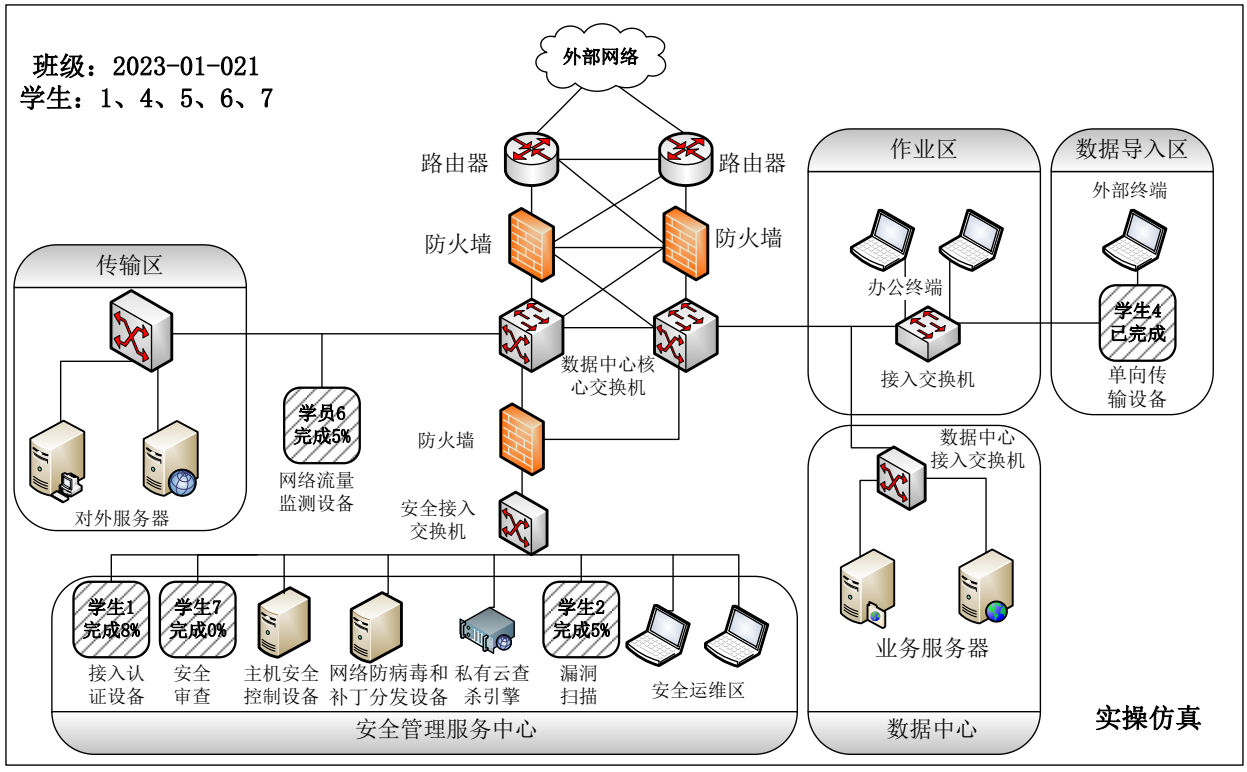


图 4 拓扑架构训练

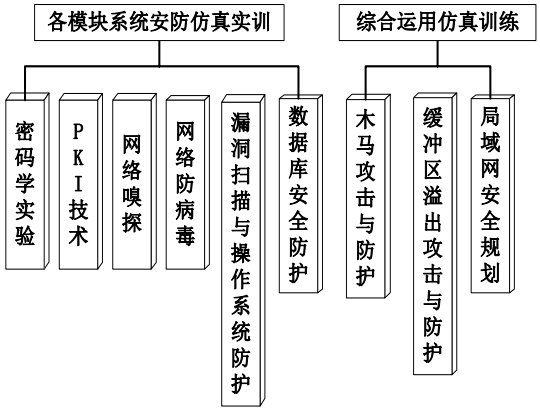


图 5 综合训练

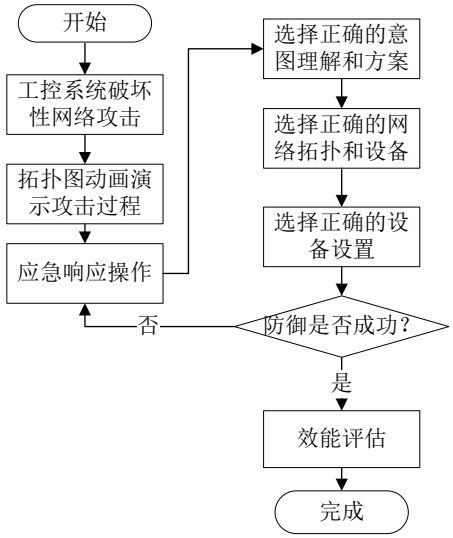


图 6 系统安防综合运用

结合虚拟仿真技术，我们重新设计了信息系统安全防护实验项目。在实际教学中，可根据课时要求、与先修课程的配合，以及不同专业同学培养需求等问题确定各阶段实验的比重，灵活选用其中的实验项目。

## 4 系统安防虚拟仿真训练平台建设

虚拟仿真训练平台担负着实验教学创新的关键任务。针对原有实验平台存在的沉浸式学习感体验差、实验环境单一、实验项目单调等问题，系统安防虚拟仿真训练平台在建设中需把握以下几个要点：

（1）增强可视化和交互性

运用动画、3D 建模、虚拟化技术，实现贴合真实环境的实验环境，实现各类各种实装设备的建模仿真，以沉浸交互方式介绍网络设备的外形、设备接口及结构特点、设备连接方式与连接流程，以及设备在网络安全系统中的具体作用，能可视化展示攻防网络拓扑，能对网络流量实现可视化，能形象化展示网络攻防态势，以闯关答题方式检验学生对设备的掌握情况[2][7]。

（2）功能集成和拓展

虚拟仿真实验项目应该将真实系统提供更为丰富的实验功能、更加良好的用户体验，解决真实系统做不了，做不好的问题[6]。因此，系统安防虚拟仿真实验平台统一提供设备的虚拟仿真、网络拓扑的虚拟仿真、网络攻击与防护流量的仿真等多项功能，支持复杂场景的网络渗透、应急响应和网络安全防护综合部署，支持有线、无线等类型的场景，支持虚实互联、虚实结合。

表 3 平台建设前后可开展的实装实验教学数量对比表

| 序号 | 平台建设前可开展的实装实验 | 平台建设后可开展的实装（虚拟仿真）实验 |
|---|---|---|
| 1 | 网络基础配置：交换机配置 | 网络基础配置：交换机配置、路由器配置、局域网安全规划 |
| 2 | 网络安全防护：防火墙、网络入侵检测、漏洞扫描 | 网络安全防护：防火墙、网络入侵检测、网络流量监测、单向传输、漏洞扫描、接入认证、网络扫描和嗅探 |
| 3 | 主机安全防护：密码学、操作系统防护、木马攻击防护、缓冲区溢出攻击防护 | 主机安全防护：密码学、PKI、防病毒、操作系统防护、木马攻击防护、缓冲区溢出攻击防护 |
| 4 | 数据安全防护：数据库安全防护 | 数据安全防护：数据库安全防护 |
| 合计数量 | 9 | 17 |

（3）便捷管理与共享广用

系统安防虚拟仿真训练平台部署在“网络虚拟训练课程平台”上，向校内外学习者开放，学生可以突破时间和空间的限制，自由安排学习时间，实验内容也可以按需选择，反复练习。系统安防虚拟仿真训练平台除了实验教学训练功能外，还设置虚拟仿真实验教学管理模块，提供实验教学课程管理、教学班管理、考核管理、教学人员管理等一揽子管理功能，保障实验教学顺利实施。

## 5 教学效果评价

建设完成的“系统安全虚拟仿真训练平台”目前已用于我校信息安全本科、专科和短训班等 3 个层次超过 10 个期班的课程实验教学工作。依托虚拟仿真训练平台可开展网络基础配置、网络安全防护、主机安全防护和数据安全防护等 4 个类型 17 种装备虚拟仿真训练，极大增强了学生的学习积极性、提升了实验课程教学效果。

通过表 3 的对比分析，可以看出，平台建设前可以进行 9 种实装实验教学，平台建设后，通过虚拟仿真实验可进行 17 种实装实验教学，比建设前提高了 88.89%。

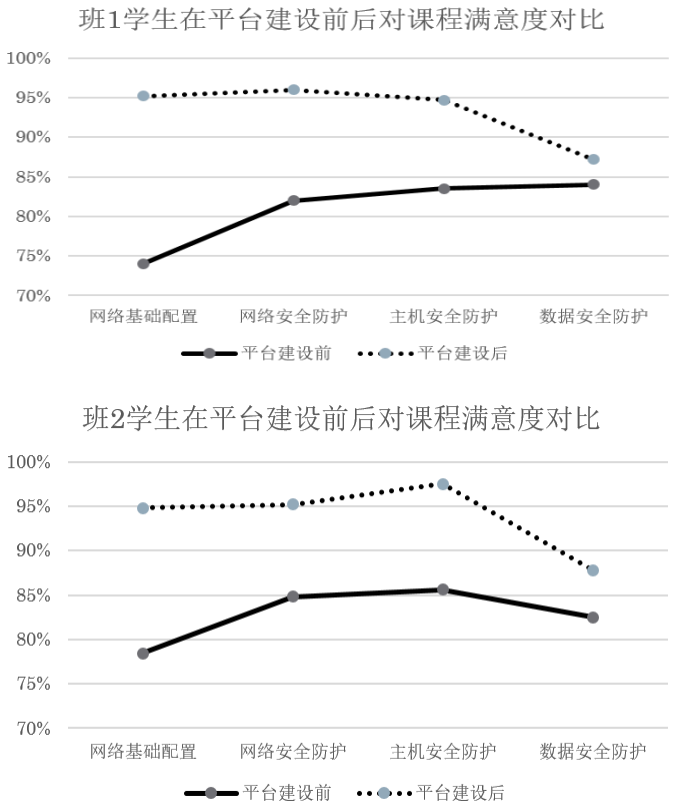


**图 7　平台建设前后不同层次学生满意度对比图**

通过选取 2024 年春季学期两个本科信息安全教学期班的学生分别使用传统实装和建设的虚拟仿真训练平台进行课程实验教学，统计学生对两种教学模式的满意度。图 7 结果显示，班 1 学生的平均满意度提升 15.93%，班 2 学生的平均满意度提升 12.92%。建设的虚拟仿真实验平台达到了激发学生学习兴趣，提升学生学习满意度的预期目标。

## 6 结束语

信息系统安全防护课程对学生的系统安防实战能力的培养起着关键作用。系统安防课程的虚拟仿真实验能够遵循系统安防能力生成的培养路径，设计了包含从设备模拟仿真、网络架构搭建训练到系统防护综合运用的仿真训练项目，虚拟仿真训练平台提供了较为逼真的训练环境，为实验实训教学提供了新的手段和实施方式，课程为学生提供了由单装到组训、由简单向复杂、由浅入深的施训方式，遵循了学生认知规律，有效促进了学生从理论知识到实战实训能力的生成。

课程在校园网上线以来，以其开放性、实践性、仿真度高等优质的学习体验，受到学生的认可和欢迎，除了使用在信息系统安全防护课程中，也面向校内外学习者开放，已有 3000 余人选课，实验完成度高，取得了较好的教学训练效果。

## 参 考 文 献

[1] 教育部. 教育部办公厅关于 2017-2020 年开展示范性虚拟仿真实验教学项目建设的通知[Z].(2017-7-11).http://www.moe.gov.cn/srcsite/A08/s7945/s7946/201707/t20170721_309819.html

[2] 郑超，赵新海，宋立彬，赵国群.建设虚拟仿真实验教学“金课”的思考-以机械类国家虚拟仿真实验教学项目为例[J].实训与实践探索，2020.2：55-60

[3] 韩挺，李鑫，韩耀明.网络空间安全靶场设计研究[J].信息安全研究，2018.5: 430-432

[4] 胡国强，霍迎秋.“网络安全”课程实验教学改革[J].内蒙古师范大学学报（教育科学版），2018.7:94-98

[5] 刘京菊，王永杰. 面向人才培养的网络靶场体系与分类研究[J].保密科学技术，2021.6：18-23

[6] 郭文普，杨百龙，徐东辉.军队精品虚拟仿真课程建设思考[J].科教风，2022.9:22-24

[7] 王文润,党建武,岳彪,王阳萍.虚拟仿真实验共享平台及资源建设探索与实践[J].计算机技术与教学学报,2022,10(5):86-90