

# 基于NFV的网络空间安全专业课程 实验考核方法改革\*

许博 王秀磊 邢长友 张国敏

陆军工程大学指挥控制工程学院, 南京 210007

**摘 要** 为了解决大量网络攻防实验难以有效开展的问题, 本文基于 NFV 技术构建了网络空间安全实验平台, 建立虚拟网元资源池, 提供虚拟网络自动部署与参数自动配置方法, 支持学生快速搭建各类网络空间安全课程实验环境。将实验平台与 SPOC 教学系统进行融合, 实现了面向全过程的课程实验考核, 能够对课程学习过程中每一个实践环节进行量化考核, 为教师提供及时的实验效果反馈, 同时督促并激发学生学习积极性。实践结果表明本实验平台可以大幅减少实验环境构建时间, 全过程实验考核能有效提升学生动手能力与实验成绩, 对相关课程实践教学改革具有重要意义。

**关键字** NFV, 虚拟网络, 网络空间, 教学系统, 实验场景

## Reform of the Experimental Examination Method for the Course of Cyberspace Security Specialty Based on NFV

Xu Bo Wang Xiulei Xing Changyou Zhang Guomin

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

xubo820@163.com xiuleiwang1988@126.com changyouxing@126.com zhang\_gmwn@163.com

**Abstract**—To solve the problem of difficulty in effectively conducting a large number of network attack and defense experiments, this paper constructs a network space security experimental platform based on NFV technology. A virtual network element resource pool is established, providing automatic virtual network deployment and parameter configuration methods, and supporting students to quickly build experimental environments for various cyberspace security courses. The experiment platform is coupled with SPOC teaching system to realize the whole process oriented curriculum experiment assessment. Be able to conduct quantitative assessment on each practice in the course learning process. It can provide teachers with timely feedback on experimental results, urge and stimulate students' enthusiasm for learning. The practical results show that this experimental platform can significantly reduce the construction time of the experimental environment, and the whole process experimental assessment can effectively improve students' hands-on ability and experimental performance, which is of great significance for the reform of relevant course practical teaching.

**Keywords**—NFV, virtual network, cyberspace, teaching system, experimental scenario

## 1 引 言

网络空间已逐渐发展成为继海、陆、天和空之后的第五维战略空间, 对国家安全、经济发展和社会稳定具有至关重要影响<sup>[1]</sup>。因此, 培养符合国家安全战略需求、具有专业技能和创新意识的应用型网络空间安全领域技术人才, 是当前开设网络空间安全专业院校的重要职责和使命<sup>[2]</sup>。课程实验环节对培养学生学习能力、实践能力和创新能力具有重要作用。然而, 网络空间安全专业实验教学课程对实验环境具有较高要求, 在一定程度上限制了创新实验教学的开展, 这主

要体现在: 首先, 在实际运行的校园网络上开展真实的网络攻击与防护实验并不现实。校园网络为多种应用提供通信服务, 任何会导致网络不稳定的实验都不能在真实网络中开展; 其次, 建立一个与校园网互联, 能够为各类网络攻防课程实验使用, 并且具有真实网络特点的实验环境, 在时间、经费和管理上都不可行; 第三, 建立与校园网隔离, 且场景简单、规模小的实验环境, 又缺失了网络的逼真度, 限制了学生进行实验学习的空间和时间。当学生集中开展课程实验时, 实验网络环境也存在维护周期长、保障成本高、实验结果难以汇总分析等缺点。

\* **基金资助:** 陆军工程大学教育教学课题项目 (GJ23ZX022)

\*\* 通讯作者: 王秀磊 xiuleiwang1988@126.com

因此, 面对大量网络攻防实验难以有效开展的问题, 需要一个高效、经济、易用的创新技术, 能够高

效灵活的构建各类网络实验环境，为培养高精尖的网络空间安全专业人才提供实验教学环境支撑。

本文提出了一种基于网络功能虚拟化 (Network Function Virtualization, NFV)<sup>[3]</sup> 技术构建网络空间安全虚拟实验平台的方法, 通过选择开源虚拟机软件, 在通用的硬件服务器中创建虚拟路由器、交换机和用户端机, 构建虚拟网元资源池。设计了虚拟资源动态调度模型和虚拟网络实验环境快速生成方法, 能够根据用户提供的 XML 网络环境描述文件, 快速生成相应的实验环境, 并完成对各虚拟单元的参数配置<sup>[4]</sup>。此外, 通过接口调用与已有 SPOC 教学系统进行融合, 为学生与老师使用虚拟实验环境提供了便利。

## 2 实验平台体系架构

设计虚拟实验平台系统体系架构, 应当满足以下基本原则: (1) 基于 NFV 实现虚拟的网络实验环境;

(2) 各类虚拟网络设备均能互联互通; (3) 虚拟网络实验环境能够灵活变更配置; (4) 虚拟网络功能与性能均与真实网络环境相同。基于上述原则, 设计了虚拟实验平台系统体系架构, 如图 1 所示。该架构共包含四个层次: 应用接口层、虚拟化网元资源池、虚拟化软件和虚拟化硬件平台<sup>[5]</sup>。其中虚拟化硬件平台是实体硬件服务器, 用来支撑虚拟化软件的运行, 为了支撑多课程、多学生同时开展实验, 需要使用服务器集群。虚拟化软件主要包括虚拟机和各类虚拟化组件, 例如虚拟网络组件、虚拟端机组件和虚拟安全组件等, 它们分布运行在虚拟机中。下面三个层次为虚拟化网络提供了基础支撑, 各类虚拟化组件均支持 TCP/IP 协议栈, 能够支持各种网络空间安全课程实验环境。

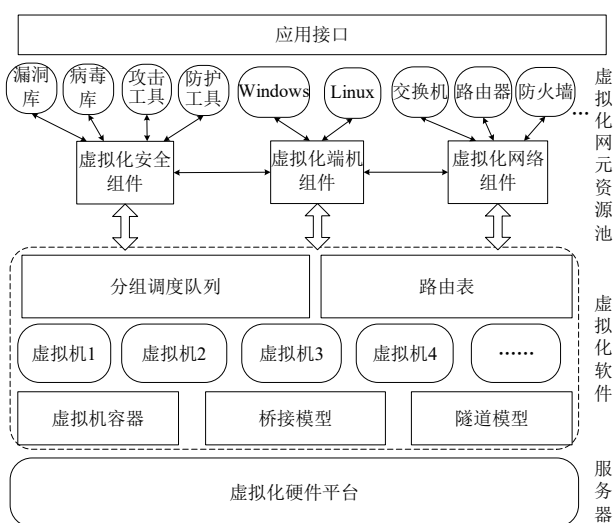


图 1 虚拟实验平台系统体系架构

应用接口主要接收用户发送的虚拟网络部署文件, 根据文件中描述的网络环境和参数配置信息, 生成相应的实验环境, 并通过 Web 网页展示给用户。

## 3 实验环境搭建

在虚拟实验平台中, 采用了形式化方法描述网络实验环境的部署和控制过程, 通过应用接口接收并解释执行实验环境描述文件与控制文件, 完成实验环境的部署与控制, 大大简化了各类实验环境的设计和使用过程。

### 2.1 实验环境的定义与部署

虚拟实验平台接口提供了各类虚拟网元的形式化描述模型, 教师可以按照模型的定义直接在 XML 文件中描述实验环境部署情况, 也可以使用用户图形界面, 由软件辅助生成部署文件 deploy.xml:

```
<NetworkConfig>
  <router>
    <name>n1</name>
    <Interfaces>

      <interface><ename>eth1</ename><ip>10.0.0.1</ip></interface>
    </Interfaces>
    <routing><rtype>ospf</rtype></routing>
  </router>
  <router>
    <name>n2</name>
    <Interfaces>
      <interface><ename>eth1</ename>
      <ip>10.0.0.2</ip>
    </interface>
    </Interfaces>
    <routing><rtype>ospf</rtype></routing>
  </router>
</NetworkConfig>
```

将虚拟实验环境部署文件 deploy.xml 提交给虚拟实验平台接口, 平台将返回如图 2 所示的虚拟实验环境。



图 2 虚拟实验环境示例

### 3.2 控制虚拟网元行为

在部分网络攻防实验中, 防护方会根据攻击方的行为做出相应的防护动作, 此时教师需要设计实验环境的自主防护行为, 平台提供了基于 XML 格式的虚拟网元行为描述方法。通过编制控制描述文件来控制虚拟网元的行为动作。平台接口收到控制描述文件后, 首先, 接口中的行为控制模块解析该控制文件, 将解析出的控制策略插入到任务队列中; 其次, 当控制策

略被触发时，则通过行为控制协议与该虚拟组件进行通信，执行预设的行为动作，从而实现自主防护。虚拟网元的行为控制架构如图 3 所示。

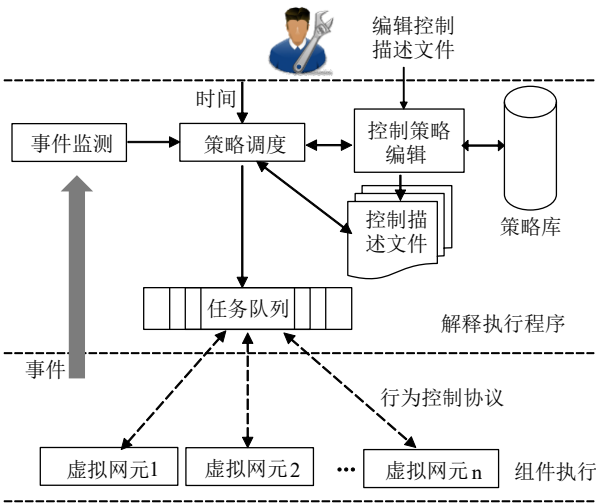


图 3 虚拟网元的行为控制架构

在图 3 中，教师通过图形化编辑工具制作控制描述文件，既能够直接创建控制描述文件，又能够复制已有的控制描述文件，修改后形成新的文件。创建好的控制描述文件可以通过用户接口提交给解释执行程序，待适当时机执行。

4 全过程课程实验考核

教学全过程管理是指教师关注学生学习过程的每个环节，并能依据学生的综合表现评定其课程成绩<sup>[6]</sup>。教师从课程开始至结束，能够掌握每个学生的学习质量、学习进度和学习效果，能够及时发现并纠正问题，促使学生高质量完成课程学习任务。图 4 为全过程管理阶段示意图，可以看出教师可采取多种不同评价标准对学习效果进行量化考核。

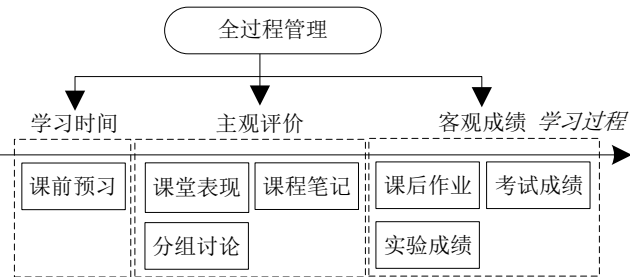


图 4 教学全过程管理阶段示意图

解释执行程序在事件和时间的驱动下，将控制策略先后插入到任务队列。虚拟实验场景打开之后，运行统一时钟，按时间序列执行控制策略，控制平台使用行为控制协议与虚拟组件通信，控制其行为动作。

基于上述思想，我们提出了面向全过程的实验课程考核方法，如图 5 所示。

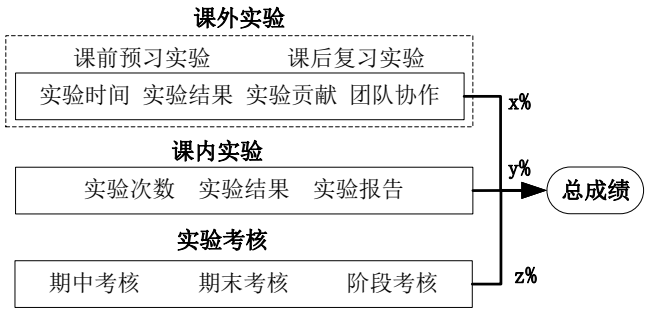


图 5 全过程实验课程考核方法示意图

将实验课程总成绩分课外实验成绩、课内实验成绩和实验考核成绩三类，每一类成绩按一定比例计入总成绩。课外实验成绩与课堂教学紧密相关，实现了对学生每一个学习环节的实验能力考核。在课前预习阶段，学生完成课前预习实验后，教师可以根据预习实验结果调整教学内容；课内实验阶段，实时了解学生对新技能的理解和应用程度，有针对性的布置课后复习实验；在课后复习阶段，通过完成小组协作实验，弥补课内实验的不足，保证实践教学质量。在实验过程中，除了关注学生学习效果以外，还应该关注他们在实验中表现出的情感、态度和价值观，如学生与同学的合作交往能力、观察分析能力、语言表达能力和实践创新能力等。

因此，在课外实验中，囊括了实验贡献度和团队协作精神，通过对各环节的量化评分，引导学生积极完成各项实验，培养学生的综合能力素质。将以往的期末综合实验考核成绩扩展到期中实验考核和阶段实验考核，由此促进学生完成实验的积极性和实验考核的综合性。

5 与 SPOC 教学系统耦合

上述全过程实验考核方法对教师提出了较高的要求，为了能够实现上述考核目标，降低教师工作量，我们在虚拟实验平台中设计了用户接口，能够方便的根据学生或教师提供的实验环境部署文件在线生成实验环境，并能根据控制服务文件控制虚拟网元的行为。此外，还对已有的 SPOC 网络教学系统进行改进<sup>[6,7]</sup>，增加了图形化实验场景设计功能，为教师设计实验场景提供了便利。学生与教师只要登录 SPOC 教学系统，通过点击相关实验链接，即可直接打开虚拟实验平台中的实验环境。通过这种方式，实现对课程实验的全过程考核。SPOC 教学系统提供了课程实验管理与成绩分析功能，辅助教师完成每一个教学环节的能力测试，其结构模型如图 6 所示。

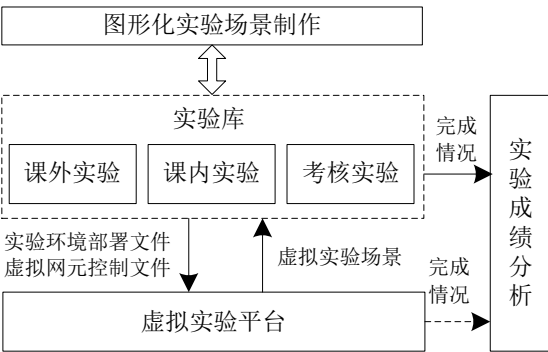


图 6 实验场景管理与测试分析模型

改进后的 SPOC 教学系统在每个教学阶段都能够提供形式适当的实验考核，而不是仅靠传统“一考定终身”的考核模式。考核效果可直接反馈给教师，作为阶段性教学效果的评价，为教师改进和调整教学内容提供参考。

6 实践总结

为验证本文提出技术方法的实际应用效果，我们于 2024 年秋季学期在《网络安全防护》课程中开展了教学实践验证。在实验环境搭建环节，采用本文提出的 NFV 技术构建实验环境，与此前传统的物理设备部署方式相比，每个实验的构建时间得到了大幅缩减，如表 1 所示。这一显著变化不仅降低了实验准备阶段的时间成本与操作复杂度，更重要的是为学生提供了更高效、灵活的实验条件。

表 1 实验环境构建时间比较

| 实验名称           | 物理设备部署<br>(分钟) | 虚拟实验平台<br>(分钟) |
|----------------|----------------|----------------|
| IP 协议脆弱性攻击     | 160            | 50             |
| 网络访问控制列表技术     | 100            | 35             |
| IPSec VPN 配置使用 | 100            | 40             |
| TCP 连接安全       | 140            | 45             |
| 网络防火墙配置使用      | 40             | 30             |
| 网络入侵检测系统的使用    | 30             | 30             |
| 网络安全综合实验       | 200            | 60             |
| 实验考核           | 200            | 55             |

在实验过程管理方面，我们引入 SPOC 网络教学平台实现对实验全过程的系统化管理，涵盖实验任务发布、过程指导、成果提交与评价反馈等环节。实践结果显示，学生使用虚拟化平台完成实验的比例较以往有了大幅提高，这充分说明基于 NFV 的实验环境更符合学生的操作习惯与学习需求，有效消除了传统实

验环境中设备资源受限、配置繁琐等阻碍学生参与的因素，表 2 显示了每个实验的完成率变化情况。

表 2 实验完成率比较

| 实验名称           | 学时 | 物理设备部署 | 虚拟实验平台 |
|----------------|----|--------|--------|
| IP 协议脆弱性攻击     | 2  | 65%    | 90%    |
| 网络访问控制列表技术     | 2  | 90%    | 100%   |
| IPSec VPN 配置使用 | 2  | 60%    | 85%    |
| TCP 连接安全       | 4  | 55%    | 90%    |
| 网络防火墙配置使用      | 2  | 90%    | 100%   |
| 网络入侵检测系统的使用    | 2  | 85%    | 95%    |
| 网络安全综合实验       | 6  | 80%    | 100%   |
| 实验考核           | 2  | 80%    | 100%   |

从教学效果来看，通过整合 NFV 技术构建的实验环境与 SPOC 平台的全过程管理，学生的实验成绩得到了普遍提升。这一结果从实践层面印证了本文提出的技术方法在优化网络安全实验教学流程、提升学生实践参与度与学习成效方面的显著优势，表明该方法能够有效解决传统网络安全实验教学中存在的效率低下、参与度不足等问题，具备良好的实际应用价值。

7 结束语

本文研究了基于 NFV 技术原理构建虚拟化实验平台的方法，节约了网络设备方面的投资，降低了维护实验环境的压力，解决了网络空间安全专业课程实验难开展的问题。通过在实验平台中设置耦合接口，在已有的 SPOC 教学系统中扩展了课程实验管理功能，为教师和学生提供了功能强大的虚拟化在线实验功能。在此基础上，将进一步推进网络空间安全专业课程实验教学的改革。

参考文献

[1] 人民网. 习近平的网络观：没有网络安全就没有国家安全 [EB/OL]. 中国共产党新闻网, (2014-11-20) [2018-04-15]. <http://cpc.people.com.cn/xuexi/2014/1120/c385475-26061137.html>.

[2] 昌燕、苟智坚、周益民等. 网络空间安全领域高层次人才培养路径探讨 [J]. 计算机技术与教育学报, 2025, 1(13), 103-107

[3] 吴伟楠、陈鸣、邓理. IRDA：一种灵活获取 NFV 对象信息的机制 [J]. 计算机技术与发展, 2021, 31(12), 98-104

[4] 李馥娟、王群. 网络靶场及其关键技术研究 [J]. 计算机工程与应用, 2022, 58(5), 12-22

[5] 王进文、张晓丽、李琦等. 网络功能虚拟化技术研究进展 [J]. 计算机学报, 2019, (2), 415-436

[6] 关玉欣、刘广文、张斌斌等. 基于 OBE 的软件工程专业实验教学过程考核与评价. 计算机技术与教育学报 [J], 2024, 3(12), 71-75

[7] 黄厚财、郑伟俊. 基于 SPOC 的翻转课堂教学设计与实