

基于虚拟化网络空间的高校现代化综合靶场建设研究

卢信宾 薛媛* 孙旭 蒋璐璐

龙岩学院, 中国·福建 龙岩 364000

摘要: 面对网络安全的严峻挑战与人才匮乏, 龙岩学院携手鹏城实验室共同创建了闽西地区首个现代化综合网络靶场, 旨在完善和提升网络靶场在教学、科研以及社会服务等应用中的系统网络环境。通过网络靶场建设, 有助于教师构建贴近真实网络环境的教学场景; 学生也可以接触到真实世界的网络安全挑战和攻击技术, 提升安全技能和知识。未来, 高校网络靶场建设可全面服务于教学管理、科学研究, 充分发挥网络靶场在人才培养、攻防演练、科学研究方面的优势和作用。

关键词: 网络靶场; 高校; 人才培养

Research on the Construction of Modern Comprehensive Shooting Range in Universities Based on Virtual Network Space

Lu Xinbin, Xue Yuan*, Sun Xu, Jiang Lulu

Longyan University, China Fujian Longyan 364000

Abstract: Faced with the severe challenges of network security and talent shortage, Longyan University and Pengcheng Laboratory have jointly created the first modern comprehensive network shooting range in western Fujian, aiming to improve and enhance the system network environment of the network shooting range in teaching, scientific research, and social services applications. Through the construction of online shooting ranges, it helps teachers to create teaching scenarios that are close to real online environments; Students can also be exposed to real-world cybersecurity challenges and attack techniques, enhancing their security skills and knowledge. In the future, the construction of network shooting ranges in universities can comprehensively serve teaching management and scientific research, fully leveraging the advantages and roles of network shooting ranges in talent cultivation, attack and defense exercises, and scientific research.

Keywords: Network shooting range; University; Talent cultivation

0 引言

飞速发展的网络技术在为人类的生活带来极大便利的同时, 各种网络安全问题也给各国带来了巨大挑战^[1]。面对越来越复杂的网络环境和愈演愈烈的网络安全事件, 世界各国也纷纷部署网络空间安全战略。其中, 部分科技强国与地区为了进行网络攻防演练以及网络新技术验证, 建立了网络靶场 (Cyber Range) 和大规模网络测试床的建设^[2]。针对当前严峻的网络安全形势, 要加强网络空间安全治理能力和体系建设, 维护好网络空间安全, 最重要的是网络安全人才的培养^[3,4]。龙岩学院作为闽西地区唯一本科院校, 与鹏城实验室合作建立网络安全靶场实验室, 为培养更多一流实战型网信人才提供了有力保障和优越的平台。

1 网络靶场建设现状及存在的问题

近年来, 全球各领域的网络非法入侵和信息泄露, 在

性质和规模都达到了严重的程度, 尤其涉及国家关键基础设施的关键领域, 已经成为非法入侵组织的重点目标。关键信息基础设施是经济社会运行的大动脉, 关系到国家安全、国计民生、公共利益, 范围涵盖政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域。高校作为网络人才来源, 对国家及社会的作用和影响至关重要, 因此加强网络安全人才培养和建设迫在眉睫。

1.1 网络靶场建设现状

作为支撑网络空间安全技术研究、试验和攻防演练等活动的重要手段, 网络靶场已成为世界各国的重点建设对象。日本早在 2002 年启动了建立 Star Bed 系统研究规划, 提供大规模的网络试验环境用于真实场景下应用的评估^[5]。2008 年, 英美等西方国家率先建设了国家级网络靶场, 以提升本国在全球的网络安全对抗能力。澳大利亚于 2012 年

宣布在澳大利亚国防学院建立网络测试靶场,为本国训练和培养网络攻防专业人员。随后,加拿大、俄罗斯、韩国和印度等国家也相继启动了各自国家的网络靶场建设项目,并在相关领域开展了应用实践。

中国在国家级网络靶场研究建设方面与上述国家相比起步较晚,目前仍处于研究论证阶段,但在实验性和行业专用网络靶场方面已取得了一些阶段性成果。一些高校和科研院所建设有专用网络靶场和攻防培训平台,在网络场景仿真、安全数据采集、攻防效果评估等技术上有所突破^[4]。从技术层面来看,网络靶场多为基于虚拟化环境的单一功能模拟类靶场,虚实结合的混合类靶场较少;多数靶场的针对性较强,但可扩展性较差。

1.2 高校靶场存在的主要问题与挑战

中国的多所高校已经开设了网络安全专业并进行网络靶场的建设探索,四川大学、华中科技大学网络安全学院分别于 2018 年和 2021 年建成了具备各自特点的网络靶场。哈尔滨工业大学、北京邮电大学、广州大学等学校的网络靶场也正在紧张筹建中。虽然一些高校已充分利用各类先进技术,借鉴国外先进网络靶场的建设经验,开始关注基于“人工智能技术的智能化攻防靶场、工业控制系统靶场、信创靶场”的研究和建设。但高校靶场建设仍存在安全规范严格导致训练灵活性受限,场地适应性不足;技术资源分布不均,各院校缺乏共享机制,智能化水平较低;实战化训练不足,与企业需求脱节;跨领域协同演练缺失,难以满足复合型人才需求等诸多问题与挑战。

2 龙岩学院网络靶场建设内容与方案

高校建设网络靶场,不仅能为学校提高教学质量、促进学术研究、提高就业竞争力、扩大学校影响力;而且符合社会需求,能为社会服务,增强国家整体网络安全能力,推进网络靶场、网络安全技术的发展。围绕“网络安全攻防演练、网络安全科学研究”的核心需求,龙岩学院打造具有高校特色的信息化基础设施,在龙岩市现有的区块链实验室的基础上建设网络靶场实验室。

2.1 网络靶场建设内容

2.1.1 人才培养建设

图 1 所示为人才培养业务流程。构建系统化、精细化、科学化的网络安全实训体系,通过学、练、考、联、评一体化人才培养体系,理论与实操相结合,多层次、系统化、持续性培养网络安全人才,不断孵化跨领域、多学科的复合型网络安全人才,填补专业人才缺口。

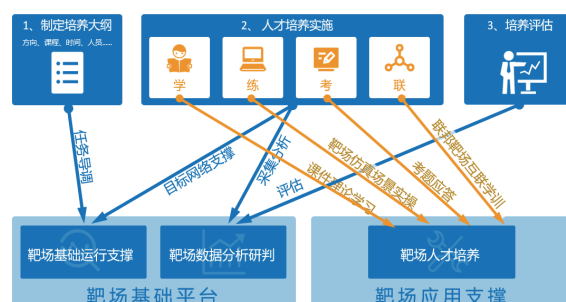


图1 人才培养业务流程

2.1.2 靶场基础平台建设方面

完善攻击检测研判、网络安全知识库和提高安全分析评估能力,采集更全面的数据和提供计算分析能力,支撑进行人才培养和科学研究。另外,还将建立有效机制与联邦靶场共享红方、场景、分析等资源,充分共享联邦靶场资源,使之更多赋能人才培养、攻防演练和科学研究。

2.1.3 攻防演练建设方面

为网络安全人才培养提供丰富、全面、实用、最新的网络安全攻击武器及相关资源下载,让其在攻防演练过程中通过实战、近实战的操作,体会相关网络攻击武器的使用方法、原理,进而加强其在真实系统的日常网络安全防护、重保活动的安全处置和应急响应能力。同时与若干联邦靶场联合开展攻防演练,利用联邦靶场分靶场、场景众多,覆盖面广,仿真程度高等优势。

2.1.4 科研仿真场景建设方面

结合当前网络安全演化形势和攻击技术演化方向,提供更加多样化、全面的仿真场景,支撑科研人员开展实验、研究与验证。同时,结合靶场数据分析能力,提高科研效率和科研质量,推动网络安全技术的创新。

2.2 网络靶场建设方案

网络靶场实验室新建项目采用三大网络架构,系统网络架构如图 2 所示。平台网络分为管理网、采集网和业务网三个隔离网络,其中管理网起到各种管理指令和系统数据交互、培训接入与运维管理作用,业务网起到攻防活动支撑和实物靶标接入作用,采集网起到流量采集作用。为保障三网隔离,采用不同流量的交换机进行网络隔离区分。通过内部管理网联通运维管理设备,确保靶场能够实施有效的监测管理。一方面,流量采集网交换机与计算服务器对接,对虚实互联科研测试环境中的所有流量进行统一监控,设置系统运行网络与虚实互联网络联通;另一方面,分布式互联服务器与联邦靶场对接,形成链接分布式存储设备,确保全面采集靶场平台所有流量。攻防业务交换机主要针对系统攻防体系及靶标业务性联通,通过联通队伍、

虚拟计算节点和实物靶标，快速、有效地形成系统运行的闭环网络结构，构建“实网攻防”所需的平台环境。

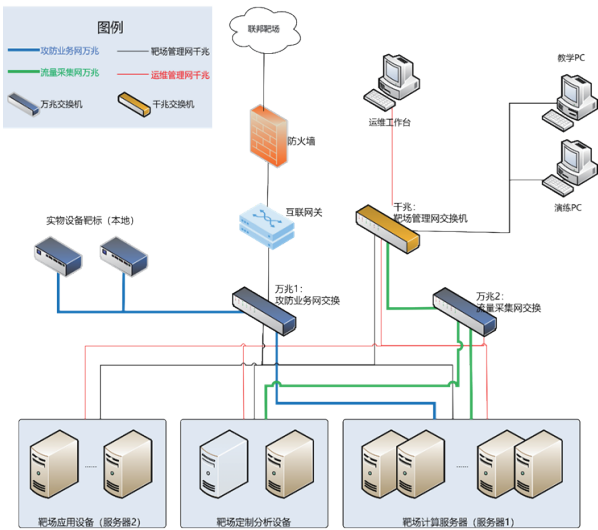


图2 网络靶场实验室的系统网络架构

3 龙岩学院网络靶场建设展望

龙岩学院网络靶场实验室建设完成后，可支撑全年使用靶场，预计使用率可达 100%（即全年的工作日都有使用）；可与数据库系统及安全、操作系统原理及安全、计算机网络、网络安全原理、数据安全与隐私保护、软件逆向分析、网络攻防技术等核心课程结合使用。人才培养应用支撑系统及课程内容可支撑开展课程设计（实践）；攻

防演练丰富建设的工具、学科竞赛以及靶场基础平台联邦互联能力建设可支撑进行网络安全综合演练与网络安全综合实训。靶场基础平台数据分析能力建设和扩展丰富的仿真场景可为创新创业实践提供支撑。此外，该网络靶场还可与相关企业、科研机构共建校企研发基地，为本地区的网络空间安全提供技术支持与服务。

参考文献：

[1] 沈昌祥，张焕国，冯登国等. 信息安全综述[J]. 中国科学 (E 辑：信息科学)，2007(02):129-150.

[2] 李建华. 多元化多层次网络空间安全人才培养创新与实践[J]. 信息安全研究，2018,4(12):1073-1082.

[3] 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，2022,2(5):12-22.

[4] 王海涛，宋丽华，张国敏. 网络靶场研究现状与关键技术分析[J]. 保密科学技术，2020,12(09):46-51.

[5] 李秋香，郝文江，李翠翠等. 国外网络靶场技术现状及启示[J]. 信息网络安全，2014(9):63-68.

[6] 程静，雷璟，袁雪芬. 国家网络靶场的建设与发展[J]. 中国电子科学研究院学报，2014,9(5):446-452.

基金项目：福建省教育厅中青年项目（批准号：JAT242010）。