文章编号：2096-1472(2020)-06-42-03
DOI:10.19644/j.cnki.issn2096-1472.2020.06.013

高等院校网络靶场建设的需求分析及架构功能设计

张月红

(上海电子信息职业技术学院，上海 201411)
✉64688613@qq.com

摘　要：高等院校网络靶场要求能提供丰富的模拟设备，同时模拟多个分级分域的虚实互联的实验网络环境，支持授权用户在此环境中进行多种场景的实验、测试和竞赛，并能支持较大规模的应用安全训练场景模拟。本文在网络拓扑设计、节点模拟和环境构建上进行设计，并按院校的教学科研需求将靶场按三个维度进行驱动：分别是以课堂为基础的模块，自定义进度的安全挑战，以团队为基础的动态练习，以此满足高等院校建设网络靶场的教学科研等需要。

关键词：网络靶场；需求分析；架构；功能
中图分类号：TP311.1　**文献标识码**：A

Requirements Analysis and Framework Function Design of Cyber Range Construction in Colleges and Universities

ZHANG Yuehong

(*Shanghai Technical Institute of Electronics& Information*, *Shanghai* 201411, *China*)
✉64688613@qq.com

Abstract: The cyber range of colleges and universities is required to provide a wealth of simulation equipment; simulate the virtual and real interconnected experimental network environment of multiple levels and sub domains at the same time; support authorized users to carry out experiments, tests and competitions in this environment; and support large-scale application security training scenario simulation. This paper conducts network topology design, node simulation and environment construction, and drives cyber range in three dimensions according to the teaching and scientific research requirements of colleges and universities. These requirements are related to modules used in classrooms, safety challenges of customized schedules, and dynamic practices of teams, so to satisfy teaching and scientific research requirements in the construction of cyber range in colleges and universities.

Keywords: cyber range; requirements analysis; framework; function

1 引言(Introduction)

随着物联网技术的发展，网络深入到了社会生活的方方面面，从虚拟走向了实际的物理世界。伊朗核电事件和乌克兰电厂事件标志着网络安全已经从信息泄露转化成与人们的生命财产相关的国家基础设施的安全，是一个关系着国家安全和主权、社会的稳定的重要问题。

在这种网络空间对抗形势日趋严峻的情况下，基于网络仿真与效果评估关键技术构建的网络靶场意义就愈发显得重要[1]。它能够对网络技术进行演示验证、对网络攻防武器装备进行研制试验和作战试验、对作战效能进行定量定性评估、对网络攻防技术人员进行训练演练。

美国、日本、英国和加拿大等国均高度重视网络靶场建设，将其作为支撑网络空间安全技术验证、网络武器试验、攻防对抗演练和网络风险评估的重要手段。我国网络安全问题严重，每年的经济损失达数百亿美元，网络靶场研究成果如能很好地推广，将惠及网络安全相关企业及网民，可提高企业的核心竞争力及网民的安全意识与能力，从而极大的减少经济损失。因此，无论是从保证国家安全、维护社会稳定以及产业发展、减少经济损失等方面，网络靶场都具有广阔的应用前景，具有很高的社会和经济效益[2]。

2 需求分析(Requirements analysis)

网络靶场是针对网络攻防演练和网络新技术评测的重

要基础设施用来提高网络和信息系统的稳定性、安全性和性能，培养实战型的网络安全人才队伍。网络靶场的主要作用[3]包括：(1)网络攻防武器评测验证：新型网络攻防武器研制出来之后，需要对其进行测试验证，是否能有效攻破敌方防护系统，以及是否能有效保护我方目标系统；(2)科学试验和新技术验证：网络空间科研 人员研制出新的网络协议，新型网络设备，以及不同网络新技术，在网络空间上功能和性能如何，也需要进行验证；(3)支持人员培训与演练：随着新型网络攻防武器的研发，具体网络安全人员能否有效掌握，网络靶场可以对其进行有效的评估。

总结以上需求的共性，网络靶场最基本的需求是模拟用户需要的网络环境并支撑网络环境的运行，支撑用户在模拟的网络环境中完成用户的任务，在任务完成后保存任务数据，释放模拟的网络环境占用的资源并支持资源的重用。 因此，从模拟对象和试验任务两个方面分析网络靶场需求。

具体到校园环境，总结需求如表1所示。

表1 高等院校网络靶场的功能模块

Tab.1 Function modules of cyber range in colleges and universities

功能模块名称	需实现的目标
模拟网络	提供一个贴近现实环境中企业网络的镜像
训练场景	可以运行一个广泛适用性的并且可以反复部署的训练事务，这个训练事务能为多个角色模拟出多个攻击场景
靶机	用一种简单易行的方式，设计生成一个新的训练场景，并在虚拟网络中执行它们
流量发生器	在虚拟网络中生成良性数据流量，以优化训练任务
训练配置工具	简单、迅速、有效地配置生成新的训练事务
任务完成情况分析报告功能	能提供过往训练的任务完成情况报告
集成的学习管理系统	能在学习管理系统和网络靶场之间分享有效数据，允许学生可以独立地在学习管理系统进行训练，也可以穿越到基于靶场的训练
测试工具	能对学生个人及学生团队活动进行评分

3 特点分析(Characteristics analysis)

高等院校网络靶场要求能提供丰富的模拟设备，同时支撑模拟多个分级分域的虚实互联的隔离实验网络环境，并支持授权用户在此环境中进行多种场景的实验或者测试。网络靶场支持大规模的网络应用(训练)场景模拟。通过在网络拓扑设计、节点模拟和环境构建上的一系列设计，支持用户构建大规模的网络环境，以满足网络靶场模拟实际应用的需要。

在模拟试验网络环境方面，网络靶场应在实物、虚拟机和容器三个层级提供各种类型的网络设备和主机设备[4]，以满足用户对设备模拟的不同逼真度的需要，同时也提供流量和用户行为模拟的支持。靶场也提供合作伙伴的模拟设备类型，便于实现模拟的精细化。

在试验支撑上，网络靶场按实验准备、实验运行和实验收尾三个阶段，采用训练配置工具，提供实验资源准备、实验环境设计、实验环境部署、实验任务设计、实验数据采集配置、实验数据分析规则配置、人员管理、人员权限管理、环境访问支撑、实验态势展示、实验环境管控、实验过程管控、销毁实验环境的支撑等。同时提供子网模板、环境模板和实验模板，支持实验人员复用网络拓扑的设计和实验的设计。使用子网模板和环境模板，便于实验人员将典型的网络结构存储起来，从而降低了重构实验的人工成本。

网络靶场中的流量发生器可提供在实验环境产生良性数据流量，并实现网络中的设备运行状态和流量的采集，节点采集内容包括节点的CPU、内存、硬盘利用率，文件变化情况、注册表变化情况、端口开放情况、流量、网络连接情况和进程变化等。

网络靶场提供基于场景的评估模型，支持正确性评估和量化评估，并提供可自定义的分析规则定义，允许用户根据需要编写分析规则，利用采集数据进行分析评估[5]。网络靶场基于网络拓扑和采集数据的分析结果展示实验态势。网络靶场提供丰富的基础资源库，包括镜像资源、靶机资源、攻防软件和典型攻防场景等，为实验人员使用网络靶场提供资源和使用的范例。

4 架构设计与功能分析(Architecture design and function analysis)

4.1 介绍

院校环境的网络靶场以需求确定、任务设定、资源配置、运行部署、实验运行、数据采集和结果评估作为网络安全实验的业务流程展开，以支撑网络安全实验的整个生命周期。利用网络靶场，可以快速构建大规模的网络安全实验环境，并展开相关的网络安全实验，在研究完成后可以释放资源并再利用资源，同时系统提供的环境模板和实验模板功能可以直接重构实验，从而为分阶段的周期性实验提供了便利。

4.2 技术架构

网络靶场的技术架构如图1所示。

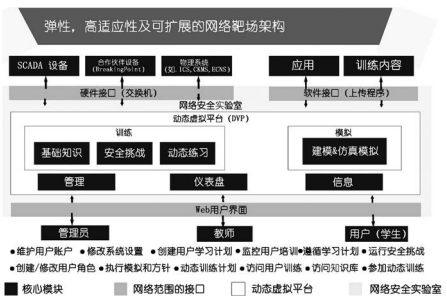

图1 网络靶场系统架构

Fig.1 Cyber range system architecture

此架构提供了一种侧重于操作的方法，通过角色和任务来测试个人和网络防护团队的技能和能力。在这个框架中，每个用户都可以分配到一个学习计划，这个计划为衡量个体的熟练程度和整体进步提供独特的评分方法。

利用上面图中所示的框架，可以推动学生的网络防御能力形成。整个靶场可以按三个维度进行驱动：分别是以课堂为基础的模块，自定义进度的安全挑战，以团队为基础的动态练习。

(1)基于课堂基础知识的实验模块覆盖四个层次，如表2所示。

表2 实验模块的四个层次

Tab.2 Four levels of the experiment module

课程模块	训练内容
基础课程模块	网络基础 安全基础 基础事件响应层
事件响应模块	事件响应模块 流量分析 深度防御 事件响应层(进阶)
工业控制系统模块	关键基础设施 工业控制系统安全 工业控制系统安全实践操作
高级拓展模块	恶意软件分析/逆向工程 事件响应层 渗透测试/漏洞评估 数字取证 跨部门网络攻防演习

(2)自定义的安全挑战涉及的五个主题类别，如表3所示。

表3 安全挑战的五个主题类别

Tab.3 Five thematic categories of security challenges

类别	主题	描述
Web应用安全	应用安全	基于Web的应用程序的安全性和脆弱性
APP保护	应用程序	传统的网络安全学科强调单一系统及应用的安全性，包括权限提升和操作系统／应用程序威胁
密码学	加解密	包括加密算法，安全通信协议，数字签名等
网络安全	网络	重在对OSI模型的理解，通过数据包捕获分析网络通信
取证	取证	事件响应，数据收集，取证数据管理(保管链)

(3)基于团队的动态训练内容，内容描述如表4所示。

表4 基于团队的动态训练内容

Tab.4 Dynamic training content based on team

动态训练	内容描述
攻击与保护	获得和维持控制的机器利用目标漏洞标志来指示 控制和保护我方系统，并移除漏洞 加固系统，打补丁
它山之王	类似夺旗赛 多个机器加入系统，类似游戏进程
僵尸网络	角色扮演恶意软件分析师和计算机取证分析师 基于团队，并分配在不同工作场景 根据完成时间及方案完整性给分
渗透测试	角色扮演渗透测试工程师 基于团体，工作在不同场景中 根据完成时间和解决方案的完整性给分

5 结论(Conclusion)

高等院校自行开发网络靶场的优劣势分析：自行搭建基于校园环境的靶场的主要优点是可以完全自行定制，让它更符合学生，院系及课程的要求，建设团队自己从底层开始搭建自己的定制化靶场，最终建成的网络靶场应更符合最初的计划和设想，并且更加适合院校使用。但更多的实践告诉我们：网络靶场的复杂性，要完成任务的数量将变成沉重的负担，同时隐性费用的也将持续不断上升。高等院校自建靶场对建设团队在专业能力，实战经验方面都有着很高的要求。

参考文献(References)

[1] 方滨兴,贾焰,李爱平,等.网络空间靶场技术研究[J].信息安全学报,2016,1(3):1-9.

[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):15-24.

[3]韩卫国,徐明迪.面向赛博空间的网络靶场建设思路[J].计算机与数学工程,2015(8): 103-108.

[4]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(5):446-452.

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

作者简介：

张月红(1975-)，女，硕士，副教授.研究领域：渗透测试，漏洞挖掘，WEB安全.