融讯光通
RONG XUN GUANG TONG

网络安全靶场实训演练系统建设方案（政务央企）

北京融讯光通科技有限公司

2023 年 11 月

目　录

第 1 章　项目背景

政务央企涉及到政府与公民、其他社会组织之间的关系，直接影响到人民群众的切身利益，是推进国家现代化进程的重要保障，需要不断适应时代变化和社会需求的变化，不断创新和完善工作机制和方法，以更好地服务于人民群众和国家发展。

当前，我国数字政府建设已全面进入快车道。数字政府建设的一项重要目标是推动政务服务高效化和利企便民最大化，在不见面的互联网空间中，要实现各项政务服务的在线和远程办理。随着网络应用的不断深入，在网络安全风险方面也面临诸多隐患和不足，如：

1. 网络安全意识问题：政务央企承担着国家关键信息基础设施的运行保障任务，工作责任重大。然而，当前面临的网络安全形势复杂严峻，网络安全意识不强成为一个突出问题。

2. 防护措施不到位：尽管在多个重要领域有着关键职责，但他们的重点防护措施往往不到位，这使得他们更容易受到网络攻击的威胁。

3. 监测预警和应急响应能力不足：在监测预警能力和应急演练能力方面存在不足，这可能导致在网络攻击发生时，他们无法及时发现并有效应对。

4. 协作共享不充分：在网络安全防护方面，政务央企之间的协作共享也不够充分，这可能阻碍了他们共同应对网络安全威胁的能力。

5. 数字化转型带来的新挑战：随着国有企业数字化转型深入，网络安全体系建设成为一项复杂的系统性工程。需要深入保障数字化业务的各个方面，加强网络安全顶层设计规划和实施，确保数字化转型的安全推进。

如何构建一套进行攻防研究、网络攻防测试及业务网络模拟复现和应急演练系统用于训练和维护呢？可以通过建设大规模深层次的网络虚实仿真靶场来实现。网络作战虚实仿真靶场旨在为应急演练和安全测评提供快速搭建实验场景的能力，一键部署的能力，真实场景模拟复现的能力和虚实结合的能力。

第 2 章　需求分析

2.1　需求分析

2.1.1　建设需求

网络安全靶场演练系统的建设旨在提升网络安全技能， 根据我国网络空间安全人才培养过程中遇到的障碍及难题可以看出，网络安全靶场演练系统的建设需求主要有以下几点：

1、靶场环境的快速、便捷搭建

随着信息技术不断发展，软硬件的推陈出新，新型的网络攻击形式、病毒、木马等也日益增多。围绕各类信息安全技术搭建具有针对性、贴近真实环境的网络安全实战环境进行有针对性的技术演练成为人才培养过程中的关键环节。因此，针对靶场环境的搭建需求主要集中在以下几点：

实现对所有用于组网资源的统一管理与利用

提供一个可视化平台，通过图形化拖拽方式实现快速组网，通过图形化界面拖拽实现网络环境的随意变更，可根据需要备份及还原现有网络环境，能够通过虚实结合构建大规模的网络仿真环境。

2、实训技术体系的规划与建设

目前，网络安全已发展成为一个综合、交叉的学科领域，它需要综合利用计算机、通信、微电子、数学、物理和生化技术等诸多学科的长期知识积累和最新研究成果。网络安全也是一个复杂的系统工程，涉及到信息基础建设、网络与系统的构造、信息系统与业务应用系统的开发、网络安全的法律法规、安全管理体系等。

3、功能详细需求

产品实操需求

此次项目建设的靶场平台应具备设备的实际操作功能，即应能够实际对常见的网络安全设备进行配置，便于掌握每类设备的配置原理及故障排查能力。

完善的安全能力培养需求

网络安全保障体系是一个很庞大的体系，涉及各种攻防技术，应通过此系统建设，培养完善的网络安全保障能力，包括：访问控制能力、入侵检测能力、病毒防护能力、安全接入能力，打造一套完善的网络安全人才培养实训平台。

网络环境模拟需求

当前，各行各业都存在信息安全用人需求，包括金融行业、互联网行业、政府行业及网络安全企业等，各行业的网络环境不通，对人才能力需求也各有特点，故实训平台应能够模拟各行业的网络特点，使得毕业后，能够满足各行业对网络安全人才的用人需求。

实训拓扑是实训的重要组成部分，学员在客户端进行实训时，系统通过实训拓扑启动实

训环境资源，包括虚拟机，安全网关等，实训环境启动后学员就可以做实训了。用户可以根据实际需求自定义实训及实训拓扑，也可以对系统的实训拓扑进行修改，通过不同的拓扑就能实现不同实训环境的搭建。

安全实训需求

网络攻防实训是培养网络攻防对抗人才最基本的模式，通过教学实训可培养学员的信息安全理论知识，加强学员的信息安全意识，所以设计出合理的课程非常的重要。实训平台应知识点全面，拥有完善的实验体系，能随着社会热点问题不断增加新实验、更新课件、题库和工具库。

课件管理：训练课程的核心是课件，平台课件覆盖了基本网络安全知识、恶意代码、逆向工程、操作系统安全、数据库安全、密码学以及各种网络安全设备等信息安全课题，将所有课题制作成课件，内置到平台中。学员只要启动课件中的拓扑即可进行实验，无需手动搭建实验拓扑。

课程管理：通过平台内置的课件制作成相关课程，分配给相应的学员进行学习，每个学员可进行不同的课程。

技能考核需求

学、测、练、赛结合，每节培训课检验培训成果，阶段培训内容强化训练，培训结束综合比赛，技术实力比武等。

攻防对抗需求

攻防对抗是更高级的竞赛形式，通过预制好的攻防对抗场景，并按照裁判设置好的规则进行分组对抗，同时裁判根据实时录像对攻防过程进行监督，防止违规现象；平台支持对攻防对抗的结果统计及过程录像。

网络安全靶场演练建设需求

网络安全靶场演练支持攻防演练、演习、防御作战等，主要支持大规模网络的快速组建于仿真能力，支持网络的监控与数据导出分析。

演练过程监控：攻防演练过程可以实现全过程监控，发现演练过程中的问题和对演练进行指导。

2.1.2 建设目标与内容

网络安全是一个直接面向工程、面向应用的专业领域，如果能够建立一个工程实践系统，使学员能在该系统进行教学内容的实训和实践，这对提高动手能力，深化对网络安全技术的认识具有重要的意义。因此，网络安全靶场演练系统所提供的实训形式是网络安全技能训练的主要形式，能够有效帮助学员综合掌握信息安全技术。

网络安全靶场演练系统是由涵盖网络安全技术的相关软、硬件设备及管理系统构成。其

必须能够模拟仿真实战网络环境，基于实战环境进行课程设计、实训规划等。用户可以运用其学习到的理论知识及技术能力在该环境中进行技术的深入理解与验证。同时，高级人员可以在在该环境中进行信息安全技术的深入研究等。总体而言，网络安全靶场演练系统的建设目标与内容如下：

网络安全靶场演练综合平台建设，主要包含 2 方面：

1) 靶场实训平台建设：搭建一套综合攻防靶场实训平台，实现快速构建用于网络安全技术实训的实战环境，提供实训、考核、攻防对抗以及网络安全靶场演练演练等多角度、多层次的网络安全人才培养所需的各项功能。

2) 实训技术体系建设：构建一套完善的、贴合实战的信息安全技术体系，该体系能够与综合实验平台无缝对接，实现对不同层次的人员进行不同层次的培养。

2.2 非功能性需求分析

2.2.1 安全性需求

本系统应具备相当的可靠性，可以向各类用户提供 7×24 小时不间断服务。

本系统应具备防病毒、黑客入侵监测和预警、漏洞扫描、网络监测与自动修复、身份认证等功能；还应具备完善的使用授权、监控和日志管理机制，能够对各类访问进行审计；系统应提供相应数据备份/恢复功能，制定合理的备份策略提供保护机制。

2.2.2 可靠性需求

本项目在成熟性、容错性、易恢复性等方面需要有较高的可靠性要求，使用开放式系统架构和成熟数据库软件，保证系统的稳定运行满足下述要求：

1、本系统应保证业务逻辑的正确性，避免由软件故障导致的失效。

2、在软件出现故障或者违反其指定接口、操作模式的情况下，软件应维持正常的性能级别。

3、考虑各种数据入口的一致性，在手工录入、网上采集、批量处理等环节中提供数据的一致性校验，并为整个软件系统提供一定的异常数据检测功能。

4、采用成熟的、经过严格测试的通用组件，减少系统差错。

5、在软件发生失效的情况下，软件应易于重建规定的性能级别并恢复受影响的数据。

6、当系统在高负荷运转或出现故障，进入异步工作模式时，必须采取可靠的机制，保证数据的零丢失。

7、必须避免由于单点故障或系统升级而影响整个系统的正常运行。

8、系统应保证 7×24 小时可以使用。

9、一年内软件可用性大于 99.99%。

2.2.3 易用性需求

本项目应实现“易理解”、“易学习”和“易操作”等易用性需求。

2.2.3.1 易理解

1、对于新用户能够容易理解系统是否合适，并能使用它去完成特定的任务。

2、系统所有的业务功能界面风格和操作流程一致。

3、业务表单应做到所见即所得。

4、界面美观、简洁、高效，界面各部件的布局应保持合理性和一致性。

5、界面颜色调和、提示清晰、窗口大小适当，使用方便。

6、在选择快捷键、缩写、提示和图标时应符合用户和税务行业习惯。

7、界面语言要通俗易懂、简洁明了，没有歧义。

2.2.3.2 易操作

1、系统应该方便操作，用户能够容易操作和控制。

2、常用操作提供快捷键支持，大部分操作能够在小键盘上完成。

3、信息录入能够完全通过键盘完成。

4、逻辑步骤和操作步骤应简单明了，避免超过三次以上的功能选项或菜单选择。

5、非法的输入或操作应有足够的提示说明。

6、对运行过程中出现问题而引起错误的地方要有提示，让用户明白错误出处，避免形成无限期的等待；提示、警告、或错误说明应该清楚、明了、恰当并且应避免英文提示的出现。

7、与正在进行的操作无关的按钮应该加以屏蔽。

8、对可能造成数据无法恢复的操作必须提供确认信息，给用户放弃选择的机会。

9、在主界面载入完毕后自动卸出内存，让出所占用的系统资源。

10、关闭所有窗体，系统退出后要释放所占的所有系统资源，除非是需要后台运行的系统。

11、所有操作尽量防止对系统的独占使用。

2.2.3.3 易学习

1、软件应易于学习，用户只需用较短时间就能学会如何使用某一特定的功能，并提供

详细的帮助系统和文档。

2、提供在线帮助，系统关键业务操作应提供在线帮助文档和提示信息，使操作人员能够快速直观的利用这些信息进行相应的业务操作，并对各种状态和操作结果进行及时的反馈和提示。

3、提供符合用户习惯，详细、易读、易理解的操作使用手册。

4、友好的帮助支持，内容包括：此操作界面的详细操作方法、上下文、有关链接条目。

2.2.4 可维护性需求

在设计上要求各系统及各模块功能结构合理，避免模块间功能耦合。在建设上遵循统一的标准规范，使用模块化的程序设计，满足软件能够简便的修改和升级，具备一定远程分析与排错功能。

一、可配置

1、人员机构的可维护性。系统应具备人员、机构等基础信息的维护功能，系统应该能够快速的对人员、机构信息进行维护和调整操作。

2、岗位权限的可维护性。系统应具备岗位权限的维护功能，系统应该能够快速的对岗位权限进行权限赋予和回收等维护操作。

3、业务流程的可维护性。系统主要业务流程应具备维护功能，可根据业务规则的变化快速的对业务流程进行调整维护操作。

4、服务接口的可维护性。系统主要业务功能应提供标准的服务交换接口，可通过开关配置快速的提供对外服务能力。

5、参数指标的可维护性。系统应具备规范、完善的参数指标的管理功能，具备针对系统运行基础性能参数进行配置和维护的功能。

二、可监控

1、提供日志审计功能。系统每个组件应具备规范、完善的日志管理功能，具备多级日志搜集开关、有效/失效开关、性能指标搜集开关以及开配置参数表。

2、业务流水机制。为保证关键业务一致性，应采用业务流水机制。

3、标准监控协议支持。应符合业界主流监控软件的接口规范，能够将监控数据方便的接入到监控软件中，便于集中监控和管理。

三、可读、易修改

在系统的建设过程中要有规范、清晰、完整和详细的文档，便于阅读、修改和维护。

四、易于升级

数据库、应用服务器、开发工具能方便地进行版本升级，具有向下兼容性；客户端采用浏览器，尽量减少客户端的升级工作量。

所有应用软件要求模块化和功能独立，易于维护。

2.2.5 可扩展性需求

在设计上必须具有适应业务变化的能力，当系统新增业务功能或现有业务功能改变时（界面的改变、业务流程变化、规则的改变、代码改变等），应尽可能的保证业务变化造成的影响局部化，主要包括以下方面：

1、系统应当适应不同的硬件环境，软硬件升级不会造成大的改动。

2、遵照开放系统的标准，确保软硬件平台的可移植性。

3、降低模块间依赖性，提高容错性。

4、各个模块部署要相对独立，不能出现由于模块功能的相互依赖而不能启动服务的情况。

6、各个模块的互相访问，均通过标准的接口来实现，访问的接口位置要可在前台页面灵活配置，接口的访问也要有较好的容错机制。

第 3 章　系统整体建设

3.1　设计思想

构建综合靶场平台，与技术体系无缝结合实现基于虚实结合的实训环境快速组网、实训、考核、对抗、靶场一体化功能。

3.2　设计原则

3.2.1　全面性

网络安全靶场演练系统是一项从无到有的工程。除了针对理论教学训练、技能训练、攻防对抗、网络安全靶场演练、考核评价、综合管理进行设计之外，也要就系统建成后整个平台的运营、管理和运维进行综合考虑，使得设计能够全面地满足系统持续稳定运行的需求，尽力避免一些微小但关键构成的遗漏。

3.2.2　高可用性

网络安全靶场演练系统建设，首先考虑信息系统的高可用性，应坚持需求驱动、以应用为主导的方针，规划和建设相应的各个子系统；系统应该在容错、负载等多方面予以考虑，应有适量冗余及其他保护措施，保证系统连续服务；结合严谨的测试管理与运维体系，保证系统的高可用性。

3.2.3　开放性

网络安全靶场演练系统，涉及的系统模块多样，结构复杂，建设过程中会遇到较多的模块间衔接问题。如果采用较封闭的技术与产品，必将造成整体应用无法衔接或效率低下，因此在总体设计阶段，在保证安全性的前提下，要考虑的是系统整体和局部的开放性。

3.2.4　可扩展性

网络安全靶场演练系统建设，应充分考虑未来发展，同时信息化建设是一个循序渐进、不断扩充的过程，系统的总体设计应该采用层次化、组件化设计，整体构架考虑与现有系统的连接，为今后系统扩展和集成留有扩充余量。

3.2.5 先进性

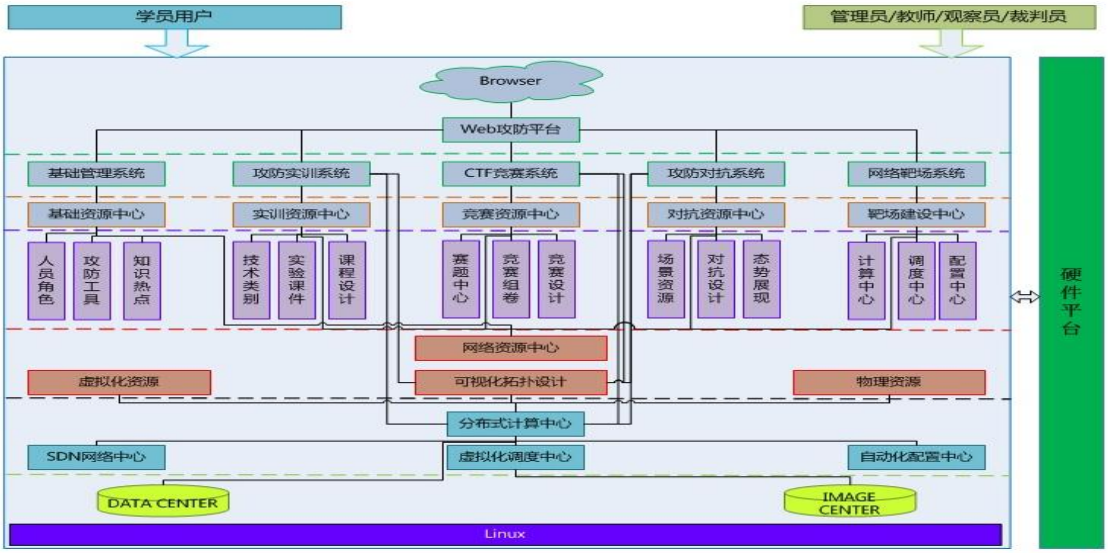
网络安全靶场演练系统建设，在设计思想、系统架构、采用技术、选用平台上均具有一定的先进性、前瞻性。在充分保证可用性、开放性、扩展性的前提下保持系统的先进性、扩充性，使系统在未来相当一段时间保持稳定。

3.3 建设目标

基于虚实结合技术，实现训练场景的快速部署，构建涵盖实训、考核、对抗、演练和靶场训练等一体化功能的新型网络安全靶场演练。

3.4 架构设计

3.4.1 系统架构



图：系统架构

网络安全靶场演练系统是一套具备演训、教学、考核、对抗、靶场、验证、业务仿真、试验多功能的系统集合，宏观结构上是一个整体大系统，充分考虑系统复杂程度和环境适应性等实际情况，对整个大系统从功能结构上进行模块化设计，提高系统弹性扩展能力和上下兼容能力、自定义灵活配置能力，既满足现阶段网络评估系统建设基本需要，又能兼顾近期过度和远期发展需求。虽然系统从结构上松耦合设计，但系统整体通过软件定义、API 接口、虚拟化等技术紧密连接。网络安全靶场演练系统分成四层，有基础资源层、虚拟化层、业务系统层、展示管理层。安全防护技术和管理体系贯穿整个系统。

3.4.2 基础资源层

基础资源层包括服务计算资源、存储资源、网络资源、终端计算资源、视频广播资源等基础资源设施，为网络安全靶场演练系统提供基础资源保障。

3.4.3 虚拟化层

使用虚拟化、云计算等技术将计算节点、存储节点、网络节点、安全软件组件等各类资源池化，并通过软件定义网络(SDN，Software Defined Network)技术集成各类虚拟资源，承载模拟仿真系统、演训评估系统，及系统所需的配套操作系统、数据库、中间件等基础运行环境。

3.4.4 业务支撑层

提供模拟仿真系统及配套系统组件和演练系统及配套运行环境设施，模拟仿真系统提供仿真环境资源池和仿真功能组件，实现国产和非国产化，业务系统仿真、网络仿真、安全系统仿真，模拟仿真系统资源和组件可以通过管理端灵活组合、调用，使用软件定义技术实现接近 1 比 1 真实信息系统仿真（网络、安全、业务），仿真系统提供第三方组件扩展接口，可实现国内通用安全产品和军网通用办公业务系统组件镜像系统导入、调用和管理。

3.4.5 展示管理层

对虚拟组件和实物资源的运行状态进行综合监控，形成可根据网络评估系统业务需求弹性扩展的资源集合；通过对虚拟化资源池状态的采集、用户操作行为日志、网络链路状态信息等的数据；采集后的数据进行分析和处理，对人员能力、验证结果等角度进行效能评估。并将分析后的结果送至态势展示层进行可视化展示。

态势呈现系统：对攻防数据进行深度挖掘和实时智能分析，生成分析结果；对网络攻防状态进行全局监控，对态势分析结果进行多维态势可视化展示。

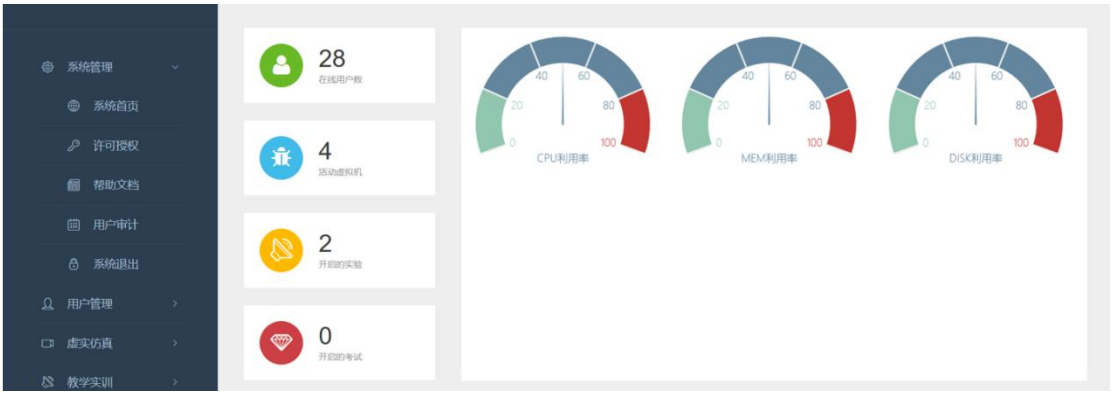
模拟仿真系统：仿真场景创建、维护和监控，虚拟网络拓扑创建、网络流量编排、业务系统搭建和安全组件调用配置。

资源监控模块：系统所有的资源，告警，性能和容量使用情况监控，了解物理主机，虚拟系统，安全组件、接口的健康状态。

3.5 系统设计

3.5.1 基础平台系统设计

基础平台软件：支持虚拟化集群管理，实训支撑平台，总控平台。包含系统插件框架软件，虚拟交换，虚拟路由，虚拟网关和虚拟终端模板等，含计算中心支持负载均衡。



3.5.1.1 控制面板

系统资源状态监控中心，监控系统的 CPU 利用率，内存利用率，系统的各种资源的数量监控，包括学员、教员、团队、虚拟主机、课程、实验、题目和工具的数量。

3.5.1.2 控制台监控中心

监控系统现有虚拟资源状态，查看及监控学员学习操作，远程指导，提供多画面展示功能。

3.5.1.3 管理配置

系统支持命令行界面配置 IP，重启、关机等功能。

3.5.1.4 用户管理

包含用户管理功能，支持用户导入，支持用户角色设置；

3.5.1.5 资源管理

物理设备管理：包含：物理安全设备，物理网络设备，物理终端设备(PC,扫描仪，小型机及其他物理设备)，可以有效利用现有物理设备，无设备品牌和型号限制。

虚拟安全设备：内置虚拟化安全设备模板，包含：虚拟化防火墙，虚拟化 IPS，虚拟化 VPN 和虚拟化 UTM，支持 web 界面与命令行两种配置与访问方式，支持 root 用户登录。并且支持主流安全厂商设备导入。

虚拟路由设备:内置虚拟化路由设备模板,支持 web 界面与命令行两种配置与访问方式，支持 root 用户登录。

虚拟终端设备：内置主流的操作系统模板，包含 windows xp，windows server 2003，

windows7，windows server 2008， windows10，windows server2012，ubuntu14，centos6.5，centos7.2，kali 和国产化操作系统等）。系统提供超过 50 个虚拟资源模板，模板内置实验场景及工具，包含标准模板，支持模板自定义；

虚拟交换设备：内置虚拟交换设备，自动生成，自动配置网络，自动清除。

3.5.1.6 工具库管理

提供实验工具资源库，漏洞扫描工具，漏洞攻击利用工具，脚本扫描工具，脚本攻击工具，密码破解工具，远程控制工具，破解辅助工具，各类系统漏洞利用 python 脚本，bash 脚本，病毒木马工具库和脚本开发工具等。

3.5.2 实训分系统设计

根据训练目标，将效能评估分系统分为目标安全环境评估、设备防护能力评估、人员安防能力评估、安全合规检查评估及评估报告管理等。

3.5.2.1 实验管理中心

支持实验分类管理，包括增、删、改、查和实验管理包含增、删、改、查，支持实验拓扑设计，实验拓扑支持用户自定义。实验拓扑的可用设备包括：物理设备；虚拟终端设备，包含虚拟 Windows 服务器、Linux 服务器、Windows 终端 PC、Linux 终端 PC 和国产化终端 PC 等，内置标准化模板，支持根据模板自定义虚拟机，教员可以自定义新的模块，可以修改已有模板的配置；虚拟交换设备，自动创建，自动配置网络，自动清除；虚拟安全设备，包含虚拟化防火墙，虚拟化 IPS，虚拟化 VPN 和虚拟化 UTM；虚拟路由设备。支持虚拟主机资源监控与配置。支持虚拟机启停、修改、删除。虚拟主机类型，包含 windows xp，windows2003，windows7，windows server2008，windows10， windows server2012，centos6.5，centos7，ubuntu14，麒麟等。实验过程支持远程监控，提供实验过程的远程指导功能，远程演示和学习；

3.5.2.2 课程设计中心

课程分成公开训练课和专业训练课，提供课程自定义功能，包含课程所有信息，如学员、课程时间、实验及拓扑等内容。提供用户课件的上传，提供用户上传课件内容后在线浏览功能，不限定课件格式。

3.5.2.3 客户端实训许可

支持学员用户客户端实训功能，学员实训支持管理端教员导入和客户端学员报名两种模式，满足课程时间要求的专业课学员可以学习专业课课程，也可以自主学习公开课课程，支持在虚拟主机中同时完成线上线下实验。

3.5.2.4 虚拟化一键部署

支持根据网络拓扑一键部署实验环境，支持虚实结合，能够将物理设备与虚拟资源进行结合组网，通过图形化界面搭建网络，能够一键部署。

3.5.2.5 实训体系设计

包含路由交换，操作系统安全，安全网关配置，风险发现评估，脚本编程基础，安全运维基础，运维管理工具，网络攻防技术、漏洞利用、python 脚本训练、服务监控工具和应用服务器等。

3.5.3 考核分系统设计

根据训练目标，将效能评估分系统分为目标安全环境评估、设备防护能力评估、人员安防能力评估、安全合规检查评估及评估报告管理等。

3.5.3.1 题目管理

包含选择、判断和简答题目，支持技能题目的增、删、改、查，支持题目拓扑图的选择，支持与拓扑管理模块联动，支持题目拓扑的一键部署；

3.5.3.2 考试组卷

支持利用现有题库进行组卷，可以选择考试题目，创建试卷。

3.5.3.3 考试设计

可以创建考试，设定考试时间，设定参考学员、负责教员，选择试卷，支持 3 种比赛模式（正确提交、直接提交和整体提交），3 种得分模式（正常模式、加分模式和减分模式），支持考试排名实时查看与展现，支持考试数据导出。

3.5.3.4 展现和监控

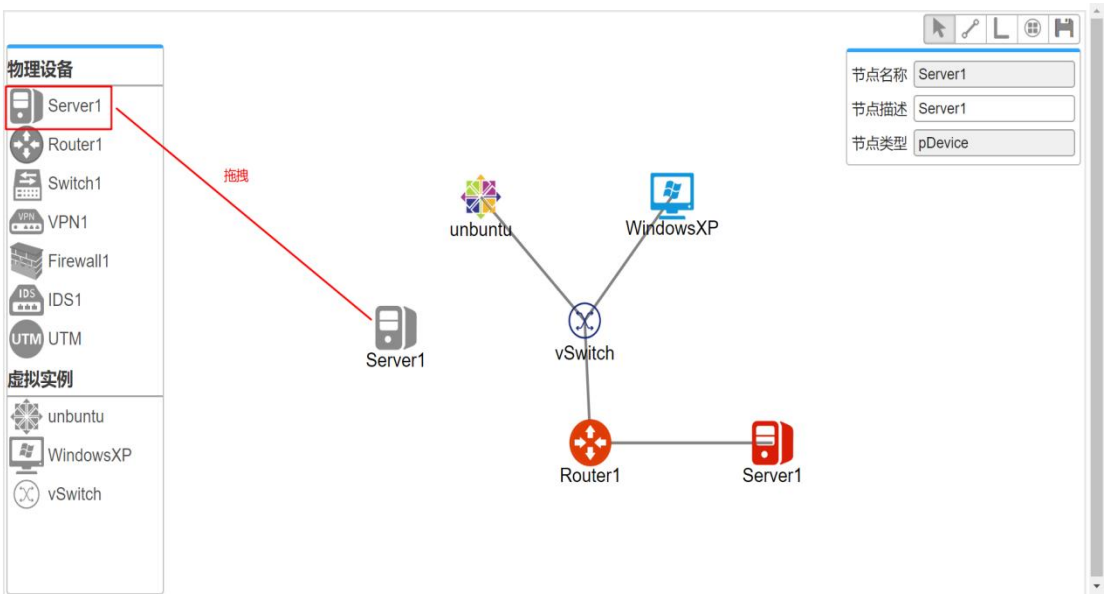
支考试成绩实时排名，支持成绩得分图表展现。支持教师监控考试进程，多画面监控学员操作。

3.5.3.5 考核客户端

支持两种考试模式，管理端教师设置和客户端报名，如果已经被选入某个考试，可以参加该考试进行答题。

3.5.4 拓扑设计分系统设计

根据训练项目要求，拓扑设计分系统主要支持训练课程、题目和场景的网络拓扑设计，包含模板栏设计、操作栏设计、属性栏设计和拓扑设计等主要功能。



3.5.4.1 模板栏设计

包含物理设备栏、虚拟路由交换栏、虚拟网关栏和终端栏；

3.5.4.2 操作栏设计

包含拓扑设计的各种操作，支持操作定制；

3.5.4.3 属性栏设计

包含设备属性，支持设置设备属性，支持属性定制；

3.5.4.4 拓扑设计

支持通过拖拽方式可视化地搭建网络拓扑，可自动检测设置合理性。

3.5.5 模拟仿真系统设计

3.5.5.1 网络仿真

根据仿真模拟实际需要的不同测试应用和不同安全域之间的访问路径和安全隔离需求不同，将仿真系统区网络按照系统功能的不同划分多个测试区域，各个测试区域之间实现网络的逻辑隔离；

3.5.5.2 安全仿真

在仿真业务区构建与生产网络相同的安全设备，以确保在业务测试过程中具备完整数据中心级安全防护能力，使业务仿真测试结果更加真实、合理。模拟仿真系统可以以软件定义的方式融合安全能力，为仿真业务区资源池运行的业务提供体系化的保护。

3.5.5.3 系统监控

针对业务测试过程中会出现大量的攻防场景、性能压力测试场景，对于系统软硬件的安全性稳定性有着非常高的需求。由此仿真业务区需要构建完善的系统服务监控系统，以便在高压高强度的测试演练过程中对系统、基础设施的服务、软硬件状态进行实时监控。

3.5.5.4 日志管理

针对模拟仿真系统的测试特殊性，在业务测试攻防演练的过程中根据需要系统记录详细的环境配置信息、操作信息、系统运行日志，以便回溯还原测试演练过程中发生问题环境，对完善业务系统有着重要的意义。

第 4 章　主要功能及性能指标

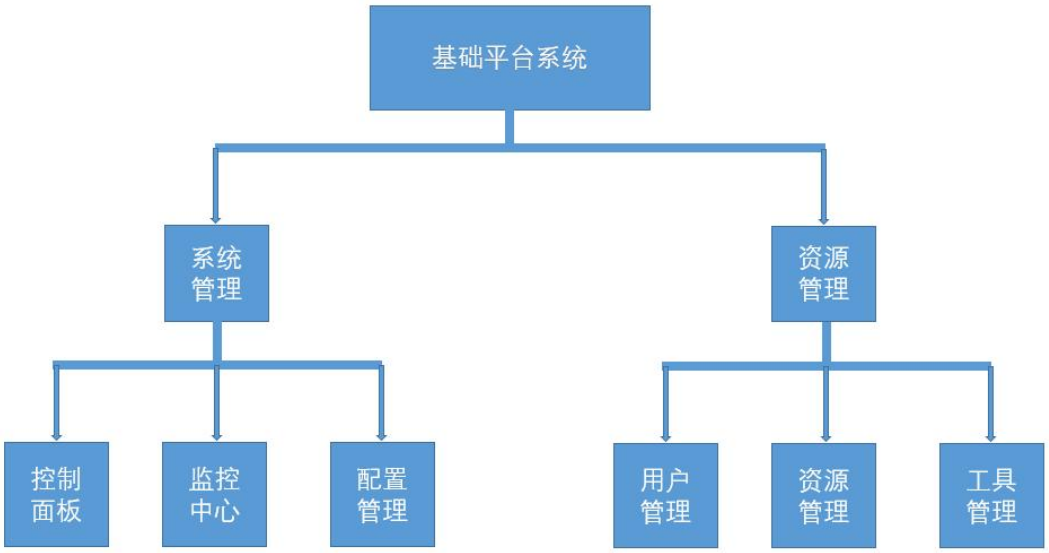
4.1　基础平台系统

4.1.1　建设目标

基础平台软件：支持虚拟化集群管理，网络安全靶场演练支撑平台，总控平台，包含系统管理，资源管理，系统监控等，含计算中心支持负载均衡。

4.1.2　系统组成

基础平台系统主要作为支撑平台，包含系统管理和资源管理两个主要功能。



- 系统管理模块主要实现系统管理配置，包含控制面板（监控系统状态：CPU、内存和硬盘使用情况）、监控中心（在线用户状态、训练状态、远程指导）和配置管理功能；
- 资源管理模块主要实现对系统资源、人员和工具等的管理，包含用户管理、资源管理和工具管理三部分。

4.1.3　系统功能与性能指标

- 控制面板：系统资源状态监控中心，监控系统的 CPU 利用率，内存利用率，系统的各种资源的数量监控，包括学员、教员、团队、虚拟主机、课程、实验、题目

和工具的数量。

- 控制台监控中心：监控系统现有虚拟资源状态，查看及监控学员学习操作，远程指导，提供多画面展示功能。
- 管理配置：系统支持命令行界面配置 IP，重启、关机等功能。
- 用户管理：包含用户管理功能，支持用户导入，支持用户角色设置；
- 物理设备管理：包含：物理安全设备，物理网络设备，物理终端设备(PC,扫描仪，小型机及其他物理设备)，可以有效利用现有物理设备，无设备品牌和型号限制。
- 虚拟安全设备：内置虚拟化安全设备模板，包含：虚拟化防火墙，虚拟化 IPS，虚拟化 VPN 和虚拟化 UTM,支持 web 界面与命令行两种配置与访问方式,支持 root 用户登录。并且支持主流安全厂商设备导入。
- 虚拟路由设备：内置虚拟化路由设备模板，支持 web 界面与命令行两种配置与访问方式，支持 root 用户登录。
- 虚拟终端设备:内置主流的操作系统模板,包含 windows xp,windows server 2003，windows7，windows server 2008， windows10，windows server2012，ubuntu14，centos6.5，centos7.2，kali 和国产化操作系统等)。系统提供超过 50 个虚拟资源模板，模板内置实验场景及工具，包含标准模板，支持模板自定义；
- 虚拟交换设备：内置虚拟交换设备，自动生成，自动配置网络，自动清除。
- 工具库管理：提供实验工具资源库，漏洞扫描工具，漏洞攻击利用工具，脚本扫描工具，脚本攻击工具，密码破解工具，远程控制工具，破解辅助工具，各类系统漏洞利用 python 脚本，bash 脚本，病毒木马工具库和脚本开发工具等。

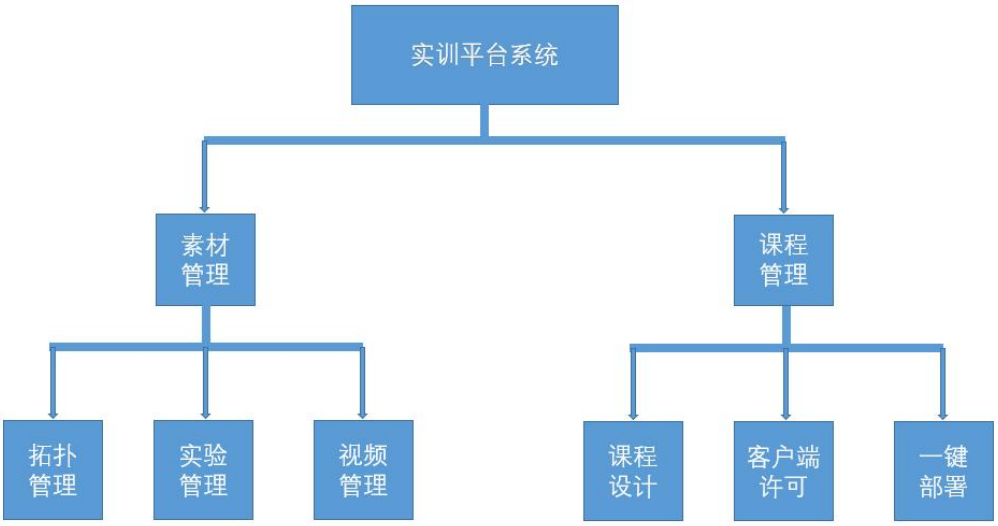
4.2 实训分系统

4.2.1 建设目标

依据攻防训练要求，支持网络安全技能实训，设置训练课程和训练项目，支持客户端一键部署，训练环境隔离互不影响。

4.2.2 系统组成

靶场实训分系统主要支持素材管理和课程管理两个主要功能。



素材管理模块主要实现训练课程的素材管理功能，包含拓扑管理、实验管理和视频管理三个子模块；

课程管理模块主要实现攻防训练课程设计实现功能，包含课程设计、客户端许可、和一键部署等部分。

4.2.3 系统功能与性能指标

- 实验管理中心： 支持实验分类管理，包括增、删、改、查和实验管理包含增、删、改、查，支持实验拓扑设计，实验拓扑支持用户自定义。实验拓扑的可用设备包括：物理设备；虚拟终端设备，包含虚拟 Windows 服务器、Linux 服务器、Windows 终端 PC、Linux 终端 PC 和国产化终端 PC 等，内置标准化模板，支持根据模板自定义虚拟机，教员可以自定义新的模块，可以修改已有模板的配置；虚拟交换设备，自动创建，自动配置网络，自动清除；虚拟安全设备，包含虚拟化防火墙，虚拟化 IPS，虚拟化 VPN 和虚拟化 UTM；虚拟路由设备。支持虚拟主机资源监控与配置。支持虚拟机启停、修改、删除。虚拟主机类型，包含 windows xp，windows2003，windows7，windows server2008，windows10， windows server2012，centos6.5，centos7，ubuntu14，麒麟等。实验过程支持远程监控，提供实验过程的远程指导功能，远程演示和学习；
- 课程设计中心：课程分成公开训练课和专业训练课，提供课程自定义功能，包含课程所有信息，如学员、课程时间、实验及拓扑等内容。提供用户课件的上传，提供用户上传课件内容后在线浏览功能，不限定课件格式。
- 客户端实训许可：支持学员用户客户端实训功能，学员实训支持管理端教员导入

和客户端学员报名两种模式，满足课程时间要求的专业课学员可以学习专业课课程，也可以自主学习公开课课程，支持在虚拟主机中同时完成线上线下实验。

- 虚拟化一键部署：支持根据网络拓扑一键部署实验环境，支持虚实结合，能够将物理设备与虚拟资源进行结合组网，通过图形化界面搭建网络，能够一键部署。
- 实训课程包含：路由交换，操作系统安全，安全网关配置，风险发现评估，脚本编程基础，安全运维基础，运维管理工具，网络攻防技术、漏洞利用、python 脚本训练、服务监控工具和应用服务器等。

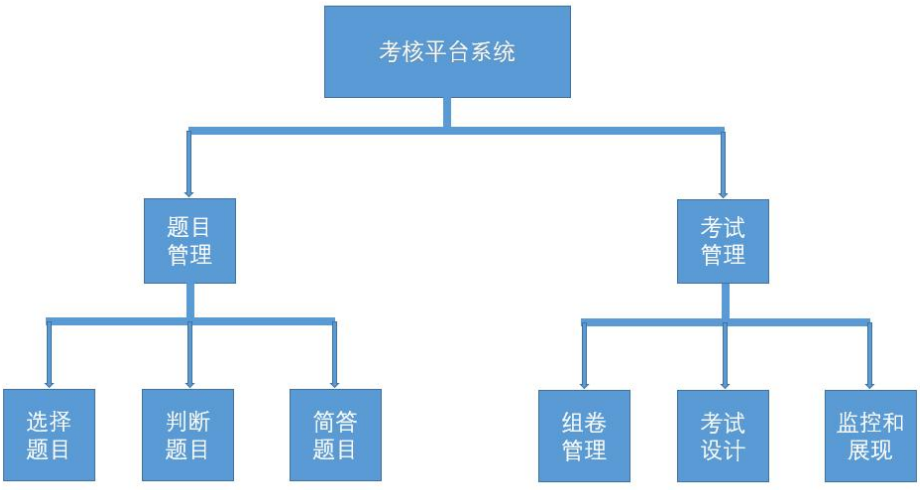
4.3 考核分系统

4.3.1 建设目标

依据攻防训练要求，支持网络安全技能考核，设置考核项目，支持考核自定义，支持客户端一键部署，考核环境隔离互不影响。

4.3.2 系统组成

靶场考核分系统主要支持题目管理和考试管理两个主要功能。



题目管理模块支持选择题目，包含单选题目和和多选题目，判断题目和简答题目；

考试管理模块主要实现攻防技能考核功能，包含组卷管理、考试设计、监控和展现等部分。

4.3.3 系统功能与性能指标

- 题目管理：包含选择、判断和简答题目，支持技能题目的增、删、改、查，支持题目拓扑图的选择，支持与拓扑管理模块联动，支持题目拓扑的一键部署；
- 考试组卷：支持利用现有题库进行组卷，可以选择考试题目，创建试卷。
- 考试设计：可以创建考试，设定考试时间，设定参考学员、负责教员，选择试卷，支持 3 种比赛模式（正确提交、直接提交和整体提交），3 种得分模式（正常模式、加分模式和减分模式），支持考试排名实时查看与展现，支持考试数据导出。
- 考试展现：支考试成绩实时排名，支持成绩得分图表展现。
- 考试监控：支持教师监控考试进程，多画面监控学员操作。
- 客户端考试许可：支持两种考试模式，管理端教师设置和客户端报名，如果已经被选入某个考试，可以参加该考试进行答题。

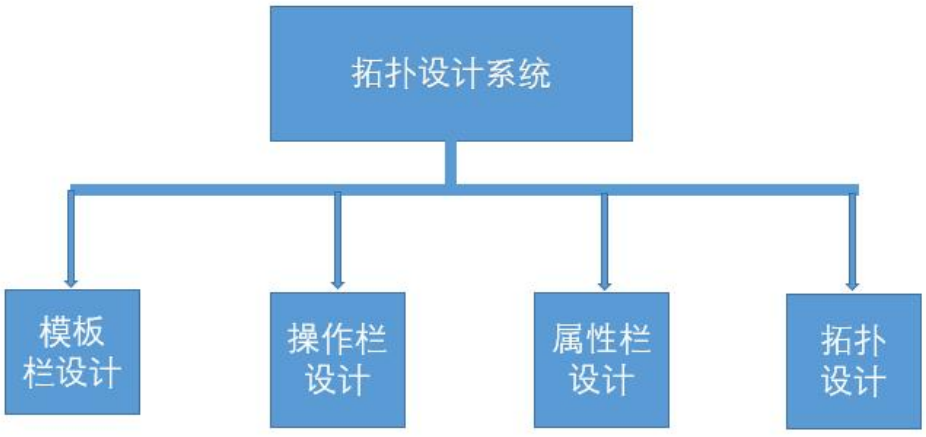
4.4 拓扑设计分系统

4.4.1 建设目标

依据攻防训练要求，根据攻防训练课程，攻防考核题目和对抗场景需求，设计网络拓扑。

4.4.2 系统组成

拓扑设计分系统主要支持训练课程、题目和场景的网络拓扑设计，包含模板栏设计、操作栏设计、属性栏设计和拓扑设计等主要功能。



模板栏设计模块主要物理设备栏、虚拟路由交换栏、虚拟网关栏和终端栏；操作栏包含拓扑设计的各种操作；属性栏包含设备属性，支持设置设备属性；拓扑设计支持通过拖拽方式可视化地搭建网络拓扑。

4.4.3 系统功能与性能指标

- 支持在浏览器上通过拖拽形式可视化的创建或编辑拓扑，支持鼠标右键菜单功能。
- 支持对虚拟主机进行 ip 配置，支持自动设置 ip，拓扑设计工具栏显示可用的物理资源、虚拟终端模板、虚拟安全设备模板、虚拟路由模板和虚拟交换模板。
- 支持应用系统所有可配置的资源与模板进行拓扑搭建，包括虚拟防火墙，虚拟 IPS，虚拟 VPN，虚拟 UTM，虚拟路由器，虚拟交换机，虚拟主机，以及各种物理设备等；支持对虚拟化防火墙，虚拟化 IPS，与虚拟化 VPN 进行接口设置。
- 支持两种生成模式：1、非实时生成模式：在创建和编辑完成拓扑后，可通过一键启动或者停止整个拓扑中的虚拟实例、虚拟交换、虚拟路由、虚拟网关等设备，并自动按照拓扑的连接组成网络拓扑。2、实时生成模式：在创建和编辑时，根据浏览器上拖拽的模板，后台实时生成相关实例；浏览器上拓扑连线时，后台实时完成虚拟实例、虚拟交换、虚拟路由等设备的连接。

4.5 模拟仿真分系统

- 能够对现有网络基础设施和业务系统模拟，提供业务仿真环境，支持通用国产化和非国产，办公系统、中间件、数据库等组件运行，能够实现虚拟化网络仿真、路由交换仿真和安全设备仿真等。
- 需要构建自主可控的仿真底座和 X86 环境，满足不同环境需求，其中 X86 计算资源为主，辅以部分自主可控芯片计算资源，满足各种场景系统仿真，具有统一的管理平台对两种计算资源进行有效管控。
- 能够针对应用系统构建模拟测试环境，尽可能真实还原测试应用系统全场景功能测试、性能测试、攻防演练测试。

第 5 章　方案优势及特点

网络安全靶场演练系统基于虚拟化技术，可以虚拟网络设备、安全设备、终端、服务器等 IT 信息资源，搭建多层次、全方位的实验环境，也可以通过网络接口把物理实验环境接入到实训平台中，与虚拟设备共同组网。通过网络攻防实训系统准备实验，方便，快捷，为用户节省管理维护成本。

5.1　虚实结合

结合真实设备，多系统互联：网络安全仿真能够在虚拟网络中接入真实设备，实现共同组网，搭建更为复杂的网络环境，或者接入其它厂商的网络靶场，组成大规模的攻防对抗场景。以实现地区级、省级，乃至国家级的应急演练和攻防对抗。

5.2　可视化的网络搭建

可以在浏览器上通过拖拽搭建网络拓扑，网络拓扑中不仅包括虚拟化设备，也包括接入网络中的物理设备。

5.3　快速组网

快速部署：网络安全仿真基于虚拟化技术，可以一键部署实验环境、竞赛及攻防场景。可以一键恢复环境，继续进行下次演练。通过一键部署的方式，避免了过去环境搭建缓慢、困难；维护成本高；环境一次性使用，难以恢复等缺陷。场景的快速部署，极大的提升了培养人才的效率。

多场景并行：网络安全实验室可以支持同时运行 50 个以上的不同的实验、场景，并且互相隔离，学员间不会产生干扰。通过多场景并行的特点，增加了受训人员真机实操的机会，加强了实训的效果。

5.4　完善的网络安全技术体系

结合我司多年网络安全技术经验积累，形成一套完整的体系化的渗透测试模型，参照国内外安全技术研究，提出一整套适合从安全技术培训到实战的全方位实验课程体系。从信息搜集阶段到攻击阶段，再到持续攻击阶段进行全面的技术剖析与培训，涉及到渗透测试绝大多数技术种类，从低级到高级逐级递进，层层深入。

5.5 分布式部署，支持虚拟化集群扩展

系统支持虚拟化集群扩展，能够实现多用户的实训系统之间的互联组建大规模的网络靶场，进行攻防演练。