|  |
| --- |
| 180977188824361587  **更新置换先进技术设备中长期贷款**  **项目立项申报书**  **项 目 名 称：网络安全“沙盘”虚仿推演**  **实验室建设项目**  **申 报 单 位：计算机与软件工程学院**  **申报单位负责人： 刘 克 剑**  **项 目 负 责 人： 纪 四 维**  **申 报 日 期： 2022年12月6日**  **联 系 电 话： 18980838692**  **西华大学国有资产与实验室管理处制** |

**一、项目基本信息**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目名称** | 网络安全“沙盘”虚仿推演实验室 | | | |
| **项目类别** | ☑新建 □改(扩)建 □更新 | | | |
| **项目归口**  **管理部门** | □教务处 ☑科技处  □网管中心 □基建处 | | | |
| **项目负责人** | 姓名 | 纪四维 | 职务职称 | 讲师 |
| 办公电话 | 87726572 | 移动电话 | 18980838692 |
| Email信箱 | jisiweiok@163.com | | |
| **项目总预算** | 60（万元） | | | |
| **项目简介：**  网络安全“沙盘”虚仿推演实验室构建多维、立体、持久在线“微缩网络空间”，能够融入现实网络空间的真业务、实设备、全要素，实现多角色、多维度、多视角，全面呈现网络空间中数据、流量、对抗等各种要素，能够进行网络空间的“沙盘推演”，可视化地呈现网络空间安全事件的成因、进程及处置，深入开展网络安全技术研究、技能对抗训练、实践教学。  通过该项目的建设，不仅对我校网络空间安全等专业的基础理论和应用方面的人才培养与科研起到极大的促进推动作用，同时为我市的其他高校相关专业的教学提供服务，而且有望成为我市软件公司、企事单位、政府部门从事网络空间安全人员的预培训基地，具有显著的教学效益、科研效益。 | | | | |

**二、立项论证**

|  |  |
| --- | --- |
| **建设项目必要性**  一、国家高度重视网络安全人才培养  没有网络安全，就没有国家安全！网络空间安全已上升为国家战略。网络空间的竞争，归根结底是人才的竞争。2015年6月，国家正式增设“网络空间安全”一级学科。  2016年12月，国家颁布了《国家网络空间安全战略》，首次以国家战略文件形式，要求“实施网络安全人才工程，加强网络空间安全学科专业建设”、 “形成有利于人才培养和创新创业的生态环境”。网络空间安全人才培养上升到前所未有的高度。  二、我国网络安全人才缺口巨大  目前，国内高校现有的实践教学体系与用人需求方向仍存在较大偏差，科研工作缺少有效的网络空间实验环境。无法全方位、有效地开展网络空间安全实践教学、科研实验活动。  据教育部网络空间安全教学指导委员会统计，2019年我国网络空间安全的人才缺口在70万到140万之间，而网络安全从业人员仅为约10万人，人才缺口比率高达93%。2027年网络安全从业人员需求数量将达到327万人，而我国目前网络空间安全人才年培养规模在3万左右，远远不能满足我国安全人才的需求。  三、学院现状  目前，我院缺少可自定义场景、与未来工作场景一致的实战化、训练环境,难以根据课程的实际情况和用人单位要求，开展网络安全相关的教学实践、实习演练、攻防对抗等教学和训练工作。  （1）缺少要素齐全、与未来工作场景一致的实验环境  现有网络安全教学实验环境中只有基本的靶机和操作主机，缺少真实网络环境中必备的路由器、防火墙、入侵检测、应用系统、数据防护等必要元素，实验环境与真实的工作场景严重不符，学生无法学习到实际的岗位技能。  因此，本次建设的网络安全“沙盘”虚仿推演实验室需要具备全部的网络、数据和安全要素，满足构建典型工作场景的需要。  （2）缺少可自主设计、自动化构建的实验条件  一方面，现有的网络安全实验系统，其实验环境和实验流程都是固定的，老师无法根据自己的上课需求自主设计实验环境和实验流程。另一方面，即使老师用实物自己搭建实验环境，由于实验条所限，也存在着结构简单、配置和调整麻烦、无法长久保存等困难。  因此，迫切需要一套能够让老师方便自主的设计实验环境，设计好的实验环境能够自动化构建，且支持复杂实验环境构建的软硬件系统。  （3）缺少可动态重构、可重复利用的实验条件  网络安全实验通常会对系统、软件和数据造成不可逆的改变甚至破坏，实验结束后，实验环境无法自动恢复和再次使用，需要老师手动恢复，每次恢复都要对众多的主机和服务器进行重新安装和配置，消耗老师大量的时间和精力，且每次人工构建的实验场景还可能存在差异。  因此，迫切需要一套具备实验环境自动回复、实验环境可重复利用的实验平台。  （4）缺少可进行实验环境克隆的实验平台  网络安全教学过程中，理想的情况是，每个学生都有独立的实验环境，为了保持公平性，每个学生的实验环节必须一样，且不能互相干扰。现有的实验条件无法满足需求。  因此，本次建设的网络安全“沙盘”虚仿推演实验室，需要具备环境克隆能力，可根据学生的人数生成多个一摸一样的实验环境，且支持实验环境的安全隔离。  （5）缺少安全隔离的手段，无法开展破坏性的实验  网络安全实验往往具备很强的传播性和破坏性，如病毒传播、勒索软件，一旦发生流量泄露或攻击外溢，将会对实验室甚至整个学校造成不可估量的损失。由于现有的实验条件下，缺少有效的安全防护手段，老师无法开展类似的网络安全实验，无法培养学生遇到类似安全事件的处置能力。  因此，网络安全“沙盘”虚仿推演实验室必须具备有效的安全隔离能力，将有害的攻击和流量限制在实验环境的范围内。  （6）缺少统一的管理平台  经过了多年的建设和积累，实验室已经具有了一定数量的软件和硬件实验系统。但是，这些软硬件实验资源物理位置分散、配置和使用方式各异，不利于根据老师的需要进行快速连接、按需部署、统一配置，无法实现实验资源的最大化利用。  因此，本次建设的网络安全“沙盘”虚仿推演实验室，需要一个统一管理平台，将现有的软硬件实验资源纳入统一管理，形成物理分散、逻辑集中的资源池，可根据实验需要进行部署和组合。  综上所述，我院亟需建设要素齐全、可自主设计、自动化构建、可动态重构、可重复利用，且具备环境克隆和安全隔离能力的网络安全“沙盘”虚仿推演实验室。 | |
| **二、建设项目可行性：**（需明确拟购仪器设备郫都校区、彭州校区存放地点）  （1）技术可行性  根据前期考察及调研,网络安全“沙盘”虚仿推演实验室的实现技术主要有两种：基于云平台（主机虚拟化）技术传统靶场和基于网络虚拟化技术网络沙盘。  云平台技术的核心是主机虚拟化。网络沙盘的核心是主机虚拟化+网络虚拟化，除了主机虚拟化功能以外，还实现了网络虚拟化功能。通过网络虚拟化技术可以在一台通用的物理服务器上，构建出由虚拟机、交换机、路由器、安全设备构成的任意架构的网络环境。其功能示意图如下图所示。    网络虚拟化功能示意图  网络虚拟化功能是由虚拟化组件完成，虚拟化组件是在操作系统底层独立加载，它通过对网络数据流的精准控制，实现数据流与特定网络环境的绑定，即网络虚拟化。网络虚拟化组件由一系列功能模块组成，如虚拟三层协议栈、安全隔离模块、虚实结合模块、决策控制模块等等。基于网络虚拟化技术实现的网络沙盘，与基于主机虚拟化技术实现传统靶场相比，具有巨大的功能优势，如网络模拟能力、异构网络并行能力、网络间隔离能力、网络克隆能力、虚实融合能力等等，这些能力在传统靶场中无法实现。  1. 网络模拟能力对比   * 传统网络靶场   基于云平台技术，一台物理服务器其内部的网络就是一个或几个用vlan分割的局域网，因此不借助外部网络设备的情况下，单个服务器内只能模拟局域网架构。即便借助了外部网络设备，如路由器、防火墙，其模拟的网络环境也受物理环境限制，无法突破服务器与外部设备的物理连接方式的制约，如下图所示。    上图的物理连接方式，其最大网络模拟能力就是一个防火墙+3个局域网。   * 网络沙盘   基于网络虚拟化平台的网络沙盘，在单台物理服务器上可以实现由虚拟、交换机、路由器、安全设备任意组合的网络架构，支持星型、树型、网状、混合型网络架构，支持互联网、城域网、局域网、多安全域、多业务互联、多分支等多种网络形态。再通过多个物理服务器的叠加，可以模拟更大规模的复杂网络，如下图所示。    2. 对比实物虚拟化能力   * 传统网络靶场   云平台中的虚拟机只要网络畅通、IP地址设置正确，就可以和外部物理设备进行通信，这是一种简单的虚实互联方式，如下图所示。    这种方式下，实物设备始终是外部设备，其虚实互联本质是内-外互联，外部实物设备无法参与其内部虚拟机之间的数据交换，无法实现更复杂的内-外-内的接入模式。特别是遇到多个实物设备需要接入不同位置、外部设备有多个网口需要连接不同虚拟机时，这种简单的内-外方式，就支持不了。   * 网络沙盘   基于网络虚拟化平台的网络沙盘，采用了独有的“实物虚拟化”技术，将实物设备进行“池化”，实现虚-实设备混合组网，可以将实物设备部署于虚拟网络的任意位置，达到了真正的虚实融合，功能原理如下图所示。    并且网络环境中任意节点都可以虚实互换。通过这种方式，客户的靶标，无论任意类型，都可以快速地部署网络环境中，且可以指定任意位置。  3.试验场景并行能力对比   * 传统网络靶场   传统靶场的网络模拟能力比较弱，且并行能力需要用vlan进行配置，所以传统靶场内只能支持简单场景的并行，如一个操作机+一个靶机。不支持复杂网络的并行运行。   * 网络沙盘   网络虚拟化平台设计和实现的时候，就是以大规模并行网络作为目标，通过网络裁决、网络划分、网络自适应性算法等多种技术，解决了这一难题，可以支持任意网络架构、任意网络规模、任意数量的网络环境并行。且支持跨物理服务器的分布式网络并行运行。下图是其并行运行的界面截图。    4.安全隔离能力对比   * 传统网络靶场   传统靶场的网络环境和物理网络是一致的，通常使用vlan、防火墙等技术进行隔离，但是vlan只在局域网内有效，三层网络就失效；防火墙只在物理边界明显的场景中才有效，对于不存在物理边界的两个虚拟试验场景之间无法进行隔离，特别是跨物理服务器的分布式试验，况且防火墙自身的虚拟资源占用太高、无法根据场景的需求进行自动化配置也是个无法解决的难题。因此两个试验场景之间，无法进行有效的隔离。  试验场景和物理网络的隔离呢？众所周知，防火墙无法完全抵御攻击和渗透，将防火墙作为网络环境与客户真实网络之间的隔离设备，达不到完全隔离的效果。所以传统靶场无法从根本上防止试验过程的有害流量外溢，网络攻击和恶意代码会对客户的实际网络造成不可估量的破坏和损失。   * 网络沙盘   网络虚拟化平台具有自成一体的网络流量控制，在实现网络并行运行、网络克隆等功能的时候，一体化解决了网络隔离的问题，实现了高强度的双重隔离，如下图所示。    安全隔离示意图  实现的双重隔离包括：  a.网络环境之间隔离：试验之间无法进行干扰  b．网络环境与真实网络隔离：试验中的任何流量，包括病毒、攻击等，无法到达底层平台  并且安全隔离不借助任何防火墙、网闸安全等安全设备，不借助任何网络配置：如VLAN、IP网段划分，避免了因这些技术和设备本身能力不足导致安全隔离失效。  5.网络克隆能力对比   * 传统网络靶场   云平台的管理粒度是以虚拟机为单位，可以实现靶机的克隆，但不支持整个网络的克隆，即使把网络中所有虚拟机都进行克隆，由于无法解决隔离、网络并行等问题，必然会出现各种冲突和错误，导致克隆和被克隆的网络都出现问题。   * 网络沙盘   网络虚拟化平台的管理粒度是网络，可以实现对整个网络的操作和管理。再加上实现了网络并行、网络隔离等功能，很容易实现网络的克隆，且是任意复杂度网络的自动克隆。所有克隆环境（网络架构、网络地址、虚拟机镜像、虚拟机配置、路由表等）都是完全一摸一样，且不冲突、不互相干扰 。网络克隆的效果如下图所示。    网络克隆效果截图  综上所述，本次实验室建设拟选用网络虚拟化技术作为基本技术路线，将网络模拟、异构网络并行、网络间隔离、网络克隆、虚实融合等功能的网络沙盘作为首选目标。  因此，实验室建设在技术上是可行的，且市场上有产品能实现本次实验室建设的功能。  （2）场地需求  实验室对场地没有特殊的需求，本次采购的实验设备部署在中心机房即可。  场地预设为：郫都校区6A-409，面积144平方米。  场地供电功率约50KW每房间，照明设施齐备。网络设施齐备，已经架设1000M校园网主干网络。 | |
| **三、建设项目科学性：**  实践、实操对于网络安全相关人才的要求特别高，因此在网络空间安全技术专业建设过程中，秉承科学合理的理念，才能培养出符合企业真实需求的专业技术人才，结合现阶段我校的实际情况和发展方向，以及市场上主流的技术路线，建设网络虚拟化技术网络沙盘势在必行，我们将在网络虚拟化技术网络沙盘的建设中坚持一下核心理念：  **(一)注重整体规划建设**  学院将通过人才培养方案撰写、课程体系搭建、教学资源库建设、师资团队建设、网络虚拟化技术网络沙盘建设、实习就业基地建设等方面从整体上通盘考虑，不断推进专业建设水平，着力提升专业人才培养质量和就业质量。**（二）注重实操技能训练**  网络空间安全人才不仅要掌握计算机技术、网络安全技术等相关专业理论知识，而且要具备网络安全渗透、攻击防御、网络安全运维软硬件平台设备搭建和调试等能力，学院在网络空间安全技术人才培养过程中会注重强化学生的实践操作技能训练，并通过各种竞赛以赛代练不断提升和检验学生的实践操作技能。  **（三）注重加强产教融合**  网路空间安全技术属于新兴的技术，我院在教学设施、教学资源、教学经验、指导经验等方面基础比较薄弱，如果能通过校企合作与产教融合，引进各种优质资源，不仅有利于学院制定更加完善的网络空间安全人才培养方案并建设更加科学的课程体系， 而且也有利于建设更加优质的师资团队并开发更加丰富的教学资源，更有利于建设更加先进的实训中心并打造更加精准的实习就业渠道，从而提升网络空间安全专业人才培养质量和就业质量。 | |
| 建设项目利用率：  为改善我校实验、实训教学为人才培养服务的需求，一个重要因素就是要提高实验室、实验设备的利用率。项目实验实训教学则是改进高校实验实训教学的突破口，也是提高实验室利用率较为有效手段。在实验实训过程中采用项目教学法改变了传统教学方法中教师为主体的局面，变学生的被动学习为主动的探究性学习。  项目教学法将学生划分成若干个项目小组，按照项目任务的要求，通过小组的分工协作，学生在指导教师的帮助下制定实验计划并实施，完成实验项目任务。实验项目教学法的主体是学生，学生通过独立或合作完成一个具有明确目的性的实验项目从而掌握相应的技能。积极拓展项目实验实训的内涵和外延，结合第二课堂活动的开展，丰富实验实训内容，通过长期的项目训练，把同学组织起来为社会服务，使实验室利用率得到快速提高。 | |
| 建设项目使用效益：  网络安全“沙盘”虚仿推演实验室将完成教学实训、科研支撑、创新创业服务、实习实训服务、社会化服务等功能。  教学实训：建设网络安全“沙盘”虚仿推演实验室，为网络空间安全学院师生，以及其他相关专业的操作系统、计算机网络、大数据、云计算、程序设计等专业课程，提供实践教学的基础环境，围绕信息化业务呈现典型网络安全事件，对事件进行全面观察、测量、分析；再将学员投入其中，开展技术角色（岗位）轮换，在实战中积累各种任务经验，快速建立岗位适应能力，形成持续进阶培养体系，提高教学实效。  科研支撑：通过“网络沙盘”构建的科研实验环境，提供各种攻防试验工具和系统测试工具，支持试验过程的数据采集和分析，为开展网络安全、大数据、网络应用等方向的课题研究提供支撑。  创新创业服务：依托实验室构建银行、电力、物联网、政务办公、网站、直播等多种类型的典型试验环境，为师生提供研发环境，以及研发成果的测试和验证环境，促进师生的技术孵化、成果转化。  实习实训服务：构建贴合实际工作岗位的网络安全实习网络环境，汇聚产业资源，将实习学员投入网络沙盘，开展岗位轮换，完成设定的网络安全项目，持续积累任务经验，挑选参与商业化网络安全项目。  社会化服务：通过实验室形成的各项科研成果，为社会提供智库咨询服务。面向全社会，依托实验室特有的网络安全实践培训体系，开展网络安全高端人才培训服务，包括网信科普、网络安全意识培养、技能训练、实战化对抗竞技等各项服务。 | |
| 项目建设进度安排 | 2022年11月，项目调研，准备相关资料，项目申报。  2022年12月，项目招标采购。  2023年1月，项目实施，设备安装调试，完成验收。  2023年2月，教学试运行，投入使用。 |

**三、项目采购清单及采购资金预算**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **主 要 仪 器 设 备** | | | | | | |
| **仪器设备名称** | **型号** | **规格** | **数量** | **参考单机**  **（万元）** | **金额 （万元）** | **主要技术参数** |
| 实训导调系统（标准版） | netst-sx-master-s1.0 | 台 | 1 | 3.8 | 3.8 | ▲硬件参数：  1、CPU:E5-2660系列10核20线程；  2、64G内存；  3、4T硬盘；  4、2个千兆管理网口；  5、2u工控设备。 |
| 1 | 6.8 | 6.8 | **可视化实训环境设计模块** |
| ▲1、网络拓扑绘制：支持可视化的方式进行网络拓扑绘制，通过鼠标拖拽即可实现网络和主机设备的摆放、设备间的互联等。  ▲2、节点属性编辑：支持对虚拟化主机、网络设备、链路等等网络元素各属性细节的显示和设置。  网络参数批量配置：支持网络地址自动分配，为网络拓扑中的每个设备节点分配统一的IP及MAC地址。  ▲3、镜像端口：仿真交换机支持镜像端口功能，可将该仿真交换机上的流量复制到某一虚拟端口上。  4、网络架构：支持网状、星型、树型、混合型等典型网络拓扑。  5、路由自动计算：支持为网络拓扑中的每个路由器分配统一的全局静态路由作为初始路由，保证网络的路由连接。支持静态路由和动态路由协议。 |
| 5.7 | 5.7 | **实训模板管理** |
| ▲1、实训角色分配：可对参与实训的角色数量、角色类型进行配置。  ▲2、角色任务配置：可针对实训的每个角色配置实训步骤和分值。  ▲3、任务评分方式设定：根据实训任务的类型，可指定评分方式。  4、系统支持两种评分方式：截图和密钥。  5、角色登录点配置：可为每个角色指定登录点，如虚拟主机、虚拟网络设备、虚拟安全系统等。 |
| 5.8 | 5.8 | **实训过程管理模块** |
| ▲1、实训任务并行执行：支持多份异构实训环境的同时构建，满足多人同时训练不同实战科目的需求。  ▲2、实训环境自动克隆：支持实训环境的自动克隆，根据训练人数动态生成多个完全一样的实训环境，实现多人同时训练,且多份环境之间实现安全隔离。  3、实训任务下发：可对学生在实训中承担的角色进行指派。支持单个学生或班级（多个学生）实训任务的批量下发；学生和教师可主动结束自己的下发任务等。  4、实训任务控制：支持实训活动的启动、停止、暂停、恢复等控制。  ▲5、实训步骤评分：教师可随时提取学生的实战结果（截图+文字说明或密钥），对实战步骤进行评分和批注。支持实战结果存档、导出。  6、实训过程介入：教师可随时接管学生的实训桌面，对学生的实训操作进行指导和纠正。 |
| 4.7 | 4.7 | **实训态势展示模块** |
| ▲1、实训环境展示：在真实网络拓扑的基础上，实时地展示实训中的主机、网络设备、安全设备的状态和桌面。  2、实时成绩展示：以实训为单位，实时地展示学生或角色的实训步骤完成情况、得分、排名。  ▲3、系统状态监视：支持对底层硬件系统的状态监视，包括负载率、CPU、内存、磁盘等。 |
| 实训环境仿真系统（标准版） | netst-sx-node-s1.0 | 台 | 1 | 4.5 | 4.5 | ▲硬件参数：  1、CPU:2\*E5-2660系列10核20线程；  2、128G内存；  3、1T SSD硬盘；  4、2个千兆管理网口；  5、4个网卡展槽，最大支持32个千兆电口；  6、1个4口千兆电口扩展卡；  7、2u工控设备。 |
| 套 | 1 | 9.8 | 9.8 | **网络环境构建模块** |
| ▲1、主机虚拟化：支持Linux、Windows等主流操作系统镜像的调度和管理，可对虚拟节点的CPU、内存等参数进行配置。  ▲2、网络设备虚拟化：实现路由器、交换机的虚拟化仿真，支持CISCO、juniper、vyatta等模拟路由器。支持虚拟化网络设备的自动化配置。  ▲3、实物虚拟化：支持实物设备池化，实物设备可以部署于仿真网络的任意位置，且无需改变实物设备的物理连接方式。  4、安全系统虚拟化：支持开源、免费和第三方商业虚拟安全系统的导入。  5、攻防工具导入：支持攻防工具的导入,提供资源库，供系统调用。  6、资源库内容包括：虚拟设备资源池：各类虚拟的服务器、终端、路由器、交换机、防火墙等设备； |
| 1、操作系统库：Linux、Windows、Unix、BSD、Android等；  2、业务应用库：数据库（MySQL等）、中间件、基础运行库（MFC、JRE等），域名解析（DNS）、邮件服务、Web服务、CDN服务、文件服务、OA、IM等；  3、恶意代码库：病毒、木马、蠕虫等各类恶意软件代码；  4、安全设备库：包含防火墙、WAF、入侵检测、入侵防御、堡垒机、日志审计、流量采集检测分析系统、等级保护、威胁情报、主机安全等；  5、实物设备管理：支持实物设备网络地址的DHCP动态分配、静态分配；  6、实物设备支持主机、二层、三层类型。  7、网络环境构建：实现虚拟-仿真-实物设备的混合网络构建。 |
| 性能指标： |
| 8、实训环境构建成功时间：<40秒。 |
| 9、实训环境资源回收时间：<30秒。 |
| 10、实训环境切换时间：<100秒。 |
| 11、实训环境最大并行运行数量：20个。 |
| 12、实训环境最大克隆数量：60个。 |
| 13、实训环境网络最大规模：120节点。 |
| 14、实训环境网络规模线性扩展：可通过增加网络仿真设备扩展实训环境的最大网络规模。 |
| 7.8 | 7.8 | **安全防护模块** |
| ★1、底层平台隔离防护：提供底层平台的隔离防护功能，使实训网络中的任何攻击都无法影响和破坏底层系统。  ★2、实训间隔离防护：提供不同的实训网络间的隔离防护功能，使不同的实训之间无法干扰和作弊。 |
| 6.9 | 6.9 | **实训接入模块** |
| ▲1、实训切换：系统提供实训列表，列表中为该学生所参与的实训。学生可以通过实训列表，实现实训的选择和切换。  ▲2、主机切换：系统提供主机列表，列表中为该学生所分配的所有主机。学生可以通过主机列表，实现不同主机的选择和切换。  ▲3、结果提交：提供截图和密钥两种实训结果提交方式，其中截图功能为系统自带，并且通过专有方式才能提交，防止抄袭和作弊。  4、人员管理：支持网络环境的可控接入，实训人员只能接入到指定的位置。实训桌面：为学生提供操作虚拟机的远程桌面。  5、实训过程控制：提供虚拟机的开机、关机、重启功能。 |
| 资源和服务 | netst-sx-res-xh | 套 | 1 | 2 | 2 | ▲1、包含7类20余门课程、至少200个典型网络安全实训课件。 |
| 2 | 2 | ▲2、包含至少30个综合网络安全实训课件，包括网络安全对抗、网络安全威胁识别、网络攻击路径分析、防御技术实战应用、急响应演练、网络安全保障实践等。 |
| 0.2 | 0.2 | 3、两年现场支持服务：每年2次重大活动现场技术支持。 |
| 1 | 免费 | 免费 | 4、提供至少30种典型应用场景，如电子政务、中小企业、生产企业、电子交易、网站、多分支企业等。  两年课程更新服务：每年更新5个典型或最新网络安全事件的教学课件。  5、提供2年免费质保服务，包括最新软件版本升级、知识库升级、技术咨询、技术培训。 |
| **项目建设总预算： 60 (万元)** | | | | | | |

注：单台（套）设备需按设备名称填写。

**四、项目技术和管理人员配置计划**

|  |  |  |  |
| --- | --- | --- | --- |
| **姓名** | **职务职称** | **所属单位** | **项目建设中承担的主要任务** |
| 纪四维 | 教师 | 计算机与软件工程学院 | 整体方案设计、规划 |
| 刘克剑 | 副院长 | 计算机与软件工程学院 | 项目技术指导 |
| 曾晟珂 | 教授 | 计算机与软件工程学院 | 设计、规划 |
| 陈红红 | 主任 | 计算机与软件工程学院 | 项目支撑、评价 |
| 祝昌宇 | 副主任 | 计算机与软件工程学院 | 规划、实施 |
| 海宇峰 | 教师 | 计算机与软件工程学院 | 项目调试协调 |
| 李曦 | 副教授 | 计算机与软件工程学院 | 规划、实施 |
| 梁莉 | 讲师 | 计算机与软件工程学院 | 规划 |
| 吴越 | 副教授 | 计算机与软件工程学院 | 设计、规划 |

**五、支出绩效目标申报表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **预算执行率权重(%)：** | 10% | | | |
| **整体目标：** | 建设网络安全“沙盘”虚仿推演实验室用于动态地构建虚实一体、可并行运行的真实网络环境，开展“真攻真防”的网络安全教学、实训、科研。满足学院教学、实验、实训、演练、研究、测试和验证等需求。 | | | |  |
| **一级指标** | **二级指标** | **三级指标** | **指标值** | **权重（%）** |  |
| 产出指标 | 数量指标 | 课程实验 | 支持每年3门以上本科课程教学 | 5 |  |
| 实验项目 | 支持本科生及研究生实验教学和实践课程开展，支持实验项目35个以上 | 5 |  |
| 教学成果 | 省级一流课程或省级教学成果奖 | 5 |  |
|  | 五年设备故障率 | ＜10% | 5 |  |
| 项目竣工验收合格率 | 100% | 5 |  |
| 质量指标 | 实验建设水平 | 设备支持利用率不低于90% | 5 |  |
| 时效指标 | 项目施工周期 | ≤60天 | 10 |  |
| 成本指标 | 成本预算 | 不超出预算 | 10 |  |
| 效益指标 | 经济效益指标 |  |  |  |  |
| 社会效益指标 | 受益学生数 | 不少于6000人课时 | 5 |  |
| 人才培养 | 每年90名本科生教学，20名学生科技创新活动 | 10 |  |
| 一流专业建设 | 推动本专业达到一流专业要求 | 10 |  |
| 生态效益指标 |  |  |  |  |
| 可持续影响指标 | 支撑就业率 | 稳步提升 | 5 |  |
| 满意度指标 | 服务对象满意度指标 | 教学对象 | ≥98% | 5 |  |
| 用人单位 | ≥90% | 5 |  |
| 填报说明：1.绩效指标由各单位（部门）结合项目具体情况增删，其中产出指标中至少选填数量指标、质量指标两项指标，效益指标中至少选填一项；批复后的绩效目标为绩效考评的主要依据；设定指标时可参考学校“十四五”发展规划纲要。 | | | | |  | |

**六、承诺**

|  |
| --- |
| 我单位填报的立项论证申报材料真实可行。若有不实，我单位愿承担一切责任。  项目负责人(签字)：  立项申报单位负责人（签字、盖章）： |

**七、立项论证意见**

|  |
| --- |
| 1、提供的论证资料齐全、规范，符合论证要求。  2、该方案针对现状和需求，建设网络安全“沙盘”虚仿推演实验室项目，系统建设目标明确。  3、该项目采购服务器、实训导调系统（标准版）、实训环境仿真系统（标准版）、资源和服务，技术路线合理可行。  4、项目经费安排合理。  专家组一致同意该方案通过论证，建议尽快组织实施。  论证组专家(签字)： |

**八 、审批意见**

|  |  |
| --- | --- |
| 项目归  口管理  部门  意见 | 项目归口管理部门负责人： （签章） 年 月 日 |
| 基建  处  意见 | 基建处负责人： （签章） 年 月 日 |
| 国资  处意  见 | 国资处负责人： （签章） 年 月 日 |
| 学校  分管  领导  意见 | 项目归口管理部门分管校领导： 年 月 日 |
| 国资管理部门分管校领导： 年 月 日 |