****

****

**实验（训）室建设项目立项申请表**

|  |  |
| --- | --- |
| **项目名称：** | 网络安全综合实训室 |
| **适用学科专业：** | 网络工程专业 |
| **项目负责人：** | 邱建林、张海飞、李秀静 |
| **计划完成日期：** |  |
| **申报单位：** | 信息工程学院 |
| **申报日期：** |  |

**一、项目概述**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **项目名称** | 网络安全综合实训室 | | | | | | | | | | |
| **项目负责人** | 邱建林  张海飞  李秀静 | | **职称** | 教授  教授  讲师 | | | **职务** | 院长  副院长  研室主任 | | **电话** | 67328、  13601493908  18051310201 |
| **项目类别** | **基础□ 专业□ 新建☑ 改建□ 扩建□** | | | | | | | | | | |
| **学年使用总人时数** | 39840 | **学年可利用总人时数** | | | 48000 | | | | **设备利用率** | 83.0% | |
| **学年该实验学时数** | 728 | **学年该实验室额定学时数** | | | 960 | | | | **实验室利用率** | 75.83% | |
| **实验（训）室容纳人数** | 50 | **配备设备组数/每组学生人数** | | | 50/1 | | | | **主体设备台套数** | 51 | |
| **建设预算**  **总金额** |  | | **实验（训）**  **场地** | | | **拟用地址** | | | | 数智-405 | |
| **面积需求** | | | | 125M2/间 | |
| **1.项目建设可行性**  【主要包括用房、人员、设备利用率、实验室安全等，即在考虑教学组织形式、管理方式的基础上，就如何在设备选型、配置、建设进度安排方面综合考虑效益、效率和效果，提高投资效益和设备设施的利用率，同时对实验室安全进行说明论证。】 | | | | | | | | | | | |
| （1）项目所需空间条件及具备情况（请说明具体实验室位置及用房面积、结构、环境设施、安全条件保障等情况）  项目拟选址数智楼405，占地面积125平米/间，结构合理，其空间条件满足本项目所需空间。本实训室拟配备有教学实验系统51套，平时教学采用分组式教学实验方法。同时配备专业的教师2-3人负责管理与维护，符合安全性。  （2）项目人员队伍配备（人员姓名、职务职称、学历、分工）   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **序号** | **人员姓名** | **职称职务** | **学历** | **分工** | | 1 | 邱建林 | 院长/教授 | 研究生 | 统筹规划 | | 2 | 张海飞 | 副院长/教授 | 研究生 | | 3 | 李秀静 | 教研室主任/讲师 | 研究生 | 项目联络 | | 4 | 潘良 | 实验室主任/副教授 | 研究生 | 项目实施 | | 5 | 李昊天 | 助教 | 本科 | 后期维护 |   （3）项目建设的其它必备条件及具备情况。  本实验室购置的设备能够满足实训(实验)要求,实验实训项目与购置的教学仪器匹配,符合实训要求。在设备选用方面充分考虑学校的实际情况，不仅可以满足教学的需求，也可以用于教师和学生进行课题研究，或是为校企合作研发提供服务，或是为校外人员提供专业培训，从而最大限度的提高设备的利用率，发挥实验室的功能。 | | | | | | | | | | | |
| **2.建设目标**  【建设的预期目标，是要能够满足教学的多样性需求：如建成后实验室所具有的功能、地位、作用等，对学科专业建设的支撑作用；服务学院、专业（名称及数量）、学生（数量）的情况；为以后的教学研究提供保障和可持续发展平台。】 | | | | | | | | | | | |
| * **提高学校网络安全教学水平**   网络安全综合实训室建设对于提高学校网络安全教学水平的意义在于：一是填补了网络安全理论知识的实践部分的空缺；二是提高教师的教学水平。网络安全综合实训室的建设极大地改善了网络安全课程的教学条件，可以让教师接触到许多前沿的网络安全知识和技术，开阔思路和眼界，这些都极大地提高了教师自身的网络安全技术的素养和能力。同时通过建设网络安全综合实训室，教师可以和一流的网络安全厂商保持密切的技术上的联系，从而及时跟进国际上最新最流行的网络技术，提髙授课水平。   * **提高学生就业率**   高校是培养人才的地方。根据现代的人才观念，真正的人才不仅仅具有知识，更要具有能力。能力的培养需要理论学习和实验实践相结合。IT技术人才市场，越来越关注技术人员的实战经验和动手操作能力。对于学生而言，在学校中如何积累实战经验和动手操作能力，那么建设网络安全综合实训室将是提高学生就业率的必要措施之一。   * **提高安全研究水平**   网络安全综合实训室的安全研究模块支持关联“所画即所得”方式构建的复杂仿真场景，形成实训研究环境；并支持漏洞挖掘、安全研究及成果分享，满足大型仿真场景下的实训研究需求。   * **提供完善的技能竞赛训练和支撑环境**   网络安全综合实训室的竞赛模块通过竞赛的方式对学生的实战能力进行考核检验，为人才选拔提供支撑。系统包含理论赛、夺旗赛、定向渗透赛、攻防对抗赛、领地争夺赛五大赛制，支持混合竞赛模式，各种赛制能够自由组合，以阶段的方式形成混合竞赛。  为满足实战型人才培养的需求，在理论赛、夺旗赛和攻防对抗赛的基础上，引入定向渗透赛并独创领地争夺赛。比赛形式上支持融合理论赛、夺旗赛、定向渗透赛、攻防对抗赛、领地争夺赛为一体的混合式竞赛形式。  同时可以基于新型竞赛体系开展“安全运维赛”、“领地争夺赛”、“安全加固赛”、“主机渗透赛”、“企业内网渗透赛”、“工控安全竞赛”、“物联网安全竞赛”、“大数据智能分析赛”等。通过各种竞赛类型，满足网安人才的选拔需求。  建设网络安全综合实训室后，对提高教学水平、学生实习就业意义、科研收益、技能竞赛、教育学术、申报重点项目、人才供需双方不对称等一系列问题有着显著意义，进一步提升南通理工学院在教育领域内的影响力与竞争力。 | | | | | | | | | | | |

**三、拟购仪器设备、辅助设施清单**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **建议型号** | **主要参数及配置要求** | **台套数** | **单价** | **小计** | **参考厂家** |
| 1 | 教学靶场 | WLAQ01 | 1.基础云管理系统：云主机管理，主要对云底座中的 KVM 类型虚拟机和容器类虚拟资源进行监控和管理。提供对虚拟机的常规管理功能。  2.节点仿真系统：系统具有节点仿真能力，仿真节点资源类型包含虚拟终端、虚拟网络设备、虚拟安全设备、物理接入设备等，节点docker容器类型。  3.实体设备管理系统：系统能够接入实体设备。  4.虚实结合仿真系统：平台提供学员个人在线虚拟终端，供学员学习或实操。  5.场景编排系统：支持用户自主设计网络拓扑，用户可以通过简单的拖放操作在网络拓扑编辑器的工作区中快速、方便的配置起自己的仿真网络,也可以对网络中网络设备的属性进行设置。用户还可以建立新的组件或修改已有组件，并支持保存为拓扑模板。拓扑制作过程中支持靶机、安全设备、路由器、交换机等设备进行拖拽式组建自定义拓扑。  6.资源监控系统：系统支持仿真节点的无感知监控，无需在节点内部署任何代码能获取节点的CPU、内存、硬盘使用情况；管理后台可以监控平台中虚拟机模板的总数、已开启虚拟机实例总数、总用户数与在线用户数、正在进行的比赛数等。以及监控各节点硬件资源的使用情况，包括内存使用率、CPU使用率、硬盘使用率、剩余可用内存等数据。  7.综合管理系统：系统提供包含用户管理、运维管理、日志管理、授权许可、公告等功能，是平台的基本组成系统。  8.资源管理系统：系统包含漏洞库、知识库、工具库、镜像库，对资源进行统一管理和调度，为业务实现提供便利的资源和工具，让用户在业务场景下可以随时调用所需资源。同时系统支持用户对资源进行扩展。  9.教学管理系统：教学培训系统能够实现按照岗位技能和知识点的分类，有针对性对安全基础理论知识进行学习，并通过作业、实验与考试来验证知识掌握的熟练程度，成长路径支持按照学习方向。  10.培训管理系统：系统支持用户自行组织培训，利用平台现有课程形成完整的培训方案，并发下给相应的班级/部门/个人，同时可以对班级所有成员的学习过程、进度和成果进行检验。  11.考试管理系统：考线程检验能够对试题、试卷和考试进行管理，平台支持人工组卷，支持购物车式选题，平台具有防作弊功能。  12.安全研究系统：提供仿真互联网系统漏洞靶机供教学实训使用，靶机数量≥200。  13. 教学统计分析系统：统计分析系统能够实现基础资源的统计概览展示，并能够针对所有人员、单个部门以及个人的学习情况进行可视化的数据统计分析；支持课程统计，其中包括：理论题数量、机试题数量、实验数量、课件数、漏洞数、知识点数、工具集数。 | 1 |  |  | 安恒、奇安信、绿盟、天融信 |
| 2 | WLAQ02 | 精品课程包，包含应用密码学、操作系统安全、Web安全原理及实践、Web渗透测试实战指南、逆向工程、恶意代码分析、二进制漏洞挖掘与利用、安全设备原理与运维、安全加固、Python开发实战、Burpsuite工具讲解、CTF入门指南、渗透测试实战演练、安全意识（小视频264个）、PHP代码审计、内网渗透、网络安全应急响应、JAVA代码审计综合实训、网络安全协议分析、网络安全综合实训、渗透测试综合实训等课程，共1450+课时。课程包含视频等多媒体课件及实验环境、实验指导手册等资源。（具体清单请参考报价目录附件） | 1 |  |  |
| 3 | WLAQ03 | 题库至少包含Web安全、Crypto密码学、Reverse逆向工程、Misc安全杂项、Pwn溢出五大类别，涵盖Web应用安全技术、密码学技术、加密解密技术、逆向工程技术、数据取证技术、数据分析技术、运维技术、开发技术、渗透测试技术、缓冲区溢出技术、逆向工程技术等知识技能方向；内有2000+理论、15+CTF、15套综合渗透、2套AWD、2套应急响应。 | 1 |  |  |
| 4 | WLAQ04 | 用户同时在线并发许可授权人数，平台使用永久许可。 | 51 |  |  |
| 5 | WLAQ05 | 1.平台提供漏洞信息200+条（2015年后的超过100个）。  2.平台工具类型有虚拟机型和下载型，包含扫描探测、漏洞扫描、密码破解、加密解密、嗅探欺骗、逆向工程、木马后门、溢出提权、远程控制、综合工具、渗透测试、代理工具等12种类别共100+款工具，支持工具分类、工具定义和资源扩展。  3.平台镜像类型包含windows、linux两大类，共300+个镜像，其中包含windows7、windows xp、windows server 2008、windows server 2012、centos6、centos7等多种镜像类别，支持用户自定义上传镜像或基于模版创建镜像。  4.平台出厂默认提供虚拟化交换机  5.平台出厂默认包含理论考试题库，题目类型包含单选、多选、判断等。 | 1 |  |  |
| 6 | WLAQ06 | 扩展课程包，包含Linux操作系统综合实训、密码学与应用、攻防对抗实训、DDOS详解、安全攻防基础、网络安全技术实践、网络嗅探、HTTP协议、Wireshark工具使用、操作系统安全实训、业务逻辑漏洞、Java反序列化远程代码执行、Struts2漏洞、Web安全部署、Web安全与测试课程、Web漏洞测试技术、Web应用安全基础、XML外部实体注入、Web框架漏洞挖掘、Web安全综合实训、WEB应用安全实训、自动化渗透测试技术、渗透测试基础讲解、信息收集综合实训、逆向工程基础、数据库安全基础、数据库安全实践、网站渗透与加固、服务器渗透与加固、应用系统安全、服务器运维、网站运维、防火墙、入侵检测、防火墙原理与技术、数据隐私与取证、数据库取证基础、网络设备取证基础、操作系统取证基础、应用程序取证基础等课程，共500+课时，课程包含PDF、视频等多媒体课件及实验环境、实验指导手册等资源。 | 1 |  |  |
| 7 | WLAQ07 | 1.平台提供多种类型操作系统模板，包括Windows7、Windows8、Windows2008、Windows2012、Centos6、Centos7、Ubuntu、Kali等，管理员可上传虚拟机模板至平台，扩充教学实训资源。  2.配套200+学习资源，主要包含数据安全法律法规及标准、数据分类分级、数据生命周期安全、数据传输安全、数据加密、数据库安全、数据处理、数据安全评估等。  3.支持数据安全理论和实训相结合学习，支持课件下载学习。  4.支持针对每个数据安全章节进行理论习题练习巩固。  5.每个实训实验包含具体的实验目的，实验环境描述，实验详细步骤等介绍说明。  6.支持在实验学习中，可以选择对应的虚拟机，进行一键开启虚拟环境，无需后台配置资源。（需提供功能截图证明）  7.支持对所有数据安全课程进行分类编排，可以根据不同方向进行详细学习。  8.支持针对数据安全学习课程进行关键字快速搜索定位学习。  9.支持课程章节简介，包括课程属性、课程方向、课程信息等。  10.支持针对课程内容推送同方向的相关课程，学员可点击快速进入学习。（需提供功能截图证明） | 1 |  |  |
| 8 | WLAQ8 | 覆盖Windows系统安全、Linux系统安全、MySQL数据库、SQLserver数据库、Oracle数据库、数据包分析、XSS跨站、网络扫描、Web安全、web应用渗透、扫描工具使用、防火墙、协议分析、信息收集、Metasploit渗透测试、SQL注入、网络访问控制、Burpsuite、网络安全、Kali Linux、KPI技术、数据保密与安全、代码审计、Hacking Python、入侵检测、拒绝服务攻击、提权、系统漏洞利用、破解技术、信息隐写、安全攻防分析、数据恢复、取证与反取证、网络安全应急响应、内存取证分析、移动终端安全、恶意代码分析、系统后门、密码学、溢出、网络欺骗技术、无线安全等主要课程实验模块，实操环境标配900个。 | 1 |  |  | 安恒、奇安信、绿盟、天融信 |
| 9 | WLAQ9 | 教学靶场标配服务器；  硬件外形：软硬一体化2U标准机架式设备；  电源：1+1冗余电源；  CPU：16核 32线程 \* 2  内存：256G  硬盘容量：4T\*4，可用空间不小于7T  固态盘：960G SSD\*2  Raid卡：4GB SAS 12Gb 8口RAID卡  电口：千兆网口 \*4  光口：万兆光口 \*2（带多模光模块）  安装：带滑轨； | 3 |  |  | 安恒、奇安信、绿盟、天融信 |
| 10 | WLAQ10 | 教学靶场交换机：  24+4口交换机：24个10/100/1000Base-T以太网端口；4个千兆光（不配光模块）；传输速率51Mpps/126Mpps； | 1 |  |  | 华为、锐捷、华三、天融信 |
| 11 | 高级威胁检测与分析系统 | WLAQ11 | 1.为灵活适应现场环境，本产品为软硬一体化设备，硬件服务器已内置流量探针，同时也支持外接流量探针。  2.支持态势大屏展示，包括全网态势、资产态势、漏洞态势、攻击态势、全域态势，支持大屏展示时间设置，支持态势大屏中相关信息下钻跳转到对应的详细页面；  3.支持拖拽方式自定义大屏界面展示顺序，支持多种地图、拓扑展示方式，包括但不限于世界、全国、省份、拓扑、实时数据、历史数据等，支持logo、大屏超时设置、介绍文案。（提供产品截图）。  4.支持安全指数、全网资产概述、漏洞概况、防护设备日志监测概况、告警趋势、攻击趋势、告警统计、最新告警、威胁类型排行等内容的相关展示；  5.支持3D地球动态展示攻击过程，支持以不同攻击线颜色区分攻击级别。  6.支持查看漏洞概况、漏洞映像安全域数量、漏洞影响资产数量、漏洞影响业务系统数量、漏洞安全域漏洞排行、影响业务系统漏洞排行、影响资产漏洞排行、漏洞类型分布、漏洞级别对比、漏洞发现趋势等漏洞信息展示。（提供产品截图）；  7.支持案例管理，包括设置触发预案、延迟时间、告警类型、告警规则、告警级别、告警发生时间等。（提供产品截图）。  8.支持工单管理，支持指派相关责任人进行处理，支持对工单进行分组管理，分组类型包括我的工单、待处置工单、已处置工单、历史工单；  9.支持在我的工单分组中进行工单分派、取消、查看详情、查看流程图等操作，支持新建工单，包括工单名称、级别、派单人、业务流程、描述等信息，支持工单统计报表导出（提供产品截图）。  10.支持专项场景威胁分析，专项分析场景包括但不限于横向威胁、外联威胁等，每类场景威胁分析支持按照今天、过去7天、过去14天、过去30天进行时间过滤显示。  11.支持从日志中发现威胁源，支持以列表形式展示威胁源相关信息，展示信息包括（区域）IP、威胁等级、影响资产、威胁类型、威胁数量、首次发现时间、最新发现时间、处置状态等，支持按照日期、IP、区域、威胁等级、威胁类型、关注名单匹配、是否命中情报、处置状态等条件进行过滤查询，支持威胁加入白名单、关注名单、加入威胁情报库、立即封堵等操作，支持与云端情报进行碰撞，支持按照TXT、CSV、EXCEL等格式进行威胁信息导出，支持影响资产、威胁类型、威胁数量等字段下钻，支持鼠标滑过处置状态悬浮显示封堵信息；（提供产品截图）；  12.支持至少50种日志展示字段，支持列集分组自定义、保存及快速切换，支持pcap导出、预览，支持检索日志的导出，包括但不限于txt、csv、excel，支持按时间序列统计日志；  13.支持对攻击线索追踪溯源分析，攻击线索类型包括IP、端口、日志名称，支持追溯结果多维度展示，包括IP地址排行TOP5、端口TOP5、日志名称排名TOP10、攻击关系图、端口相关IP关系图、日志名称相关IP关系图、日志列表，攻击关系图包含攻击源、被攻击目标及日志名称之间的关系，端口相关IP关系图包含攻击源、被攻击目标及日志数量之间的关系，日志名称相关IP关系图包含攻击源、被攻击目标及日志数量之间的关系，日志列表信息包含开始时间、日志名称、源IP、源端口、目的IP、目的端口、日志级别等字段，支持日志详情查看、溯源、附件、一键封堵、加入白名单、加入关注名单、封堵申请等操作（提供产品截图）；  14.支持管控设备概览，支持通过界面快速添加集中管控设备，支持至少3类设备的集中管控能力，支持设备管控情况，包括总数、在线、离线、日志采集、性能监控、策略管控；支持日志采集趋势展示；  15.支持管控拓扑图展示，支持拓扑动态提示管理设备产生的告警，支持拓扑图右击直接查看选中设备的设备概览、设备详情、告警列表等信息（提供产品截图）；  16.支持全网策略概览，支持下发策略统计、配置备份统计、活跃策略TOP5、最新下发策略操作人、最新下发策略设备、最新策略任务、最新配置备份、最新失败审计等监控能力；  17.支持策略管理，支持策略新建、删除、查看、编辑、下发、下发记录等，支持策略标签管理，策略内容包括名称、标签、设备类型、执行设备、策略分类、配置项类型、状态、源地址、源端口、目的地址、目的端口、终端地址（提供产品截图）；  18.支持配置备份，包括获取运行配置、备份配置、备份策略、设备查询等，定期同步管控设备的策略并对比分析。可以选中设备列表的设备获取运行配置进行获取。可以选择一个设备进行备份配置。可以对已选择的设备进行自动备份配置，包括启用、停用，备份周期设置等。  19.支持资产性能监测概览，支持监测设备总数、异常数、主机异常数、网络设备异常数、安全设备异常数展示，支持监控资产性能状态占比、性能告警TOP10、规则类型事件分布、CPU使用率TOP10、内存使用率TOP10、磁盘使用率TOP10，支持性能监控详细列表，包括IP、资产名称、归属安全域、资产类型、性能状态、连通状态、CPU使用率、内存使用率、磁盘使用率、操作等（提供产品截图）。  20.支持报告任务管理，包括新增、删除、暂停、查看，支持报告执行方式管理，执行方式包括但不限于立即执行、日报、周报、月报；  21.支持等保概览，包括但不限于统计等保业务系统数、已备案业务系统数、测评通过业务系统数、待整改业务系统数、已测评总次数、已整改总次数等统计信息，支持等保业务系统列表展示、等保业务系统等级分布统计、业务系统整改次数排名TOP5、业务系统测评次数排名TOP5、业务系统等保过程记录；  22.支持WEB页面升级补丁，包括补丁导入、应用、还原、下载、删除、查看等操作，支持WEB页面重启系统； 支持推送管理，推送方式包括邮箱、企业微信、钉钉等方式； | 1 |  |  | 奇安信、绿盟、安恒、天融信 |
| 12 | 交换机 | WLAQ12 | 交换机；  48口交换机：48口10/100/1000Base-T以太网端口；传输速率51Mpps/126Mpps； | 2 |  |  | 华为、锐捷、华三、天融信 |
| 13 | 电脑（实验终端） |  | CPU：Intel Core I7-13700处理器(主频≥2.1GHz)  主板：英特尔Q670芯片组主板,内存插槽4个以上，便于后期扩展  硬盘：1T M.2 NVME 固态硬盘  内存：16GB DDR4及以上，支持扩展  显卡：集成显卡；  键鼠：原厂USB防水键盘、抗菌鼠标；  接口：≥8个USB接口(其中至少2个USB 3.2 G2接口 )、≥3个视频输出接口  安全特性：USB屏蔽技术，仅识别USB键盘、鼠标，无法识别USB读取设备，有效防止数据泄露（投标时提供功能性截屏）；  机箱：标准塔式机箱；顶置提手，自带光触媒风扇、内置扬声器(投标时提供佐证材料)  电源：≥300W标准电源  显示器：主机同品牌23.8英寸及以上LED 16:9显示器,屏幕分辨率≥1920\*1080  操作系统及软件：正版双操作系统，三茗双还原软件；  原厂商三年免费质保、三年上门服务，原装原配，不接收改配。（提供原厂授权及服务承诺函，并加盖原厂公章）。提供尊享服务保障，需提供设备第二日修复服务，如未修复，应由原厂赠送与超期天数相等的原厂月度保修，须提供加盖制造厂商公章的服务承诺函，且该服务必须官网或官网热线可查。为了保障客户利益，降低项目风险，确保设备及系统服务质量，投标人所投计算机设备制造商具备较高的服务水平和技术水平，通过ITSS信息技术服务运行维护能力成熟度一级(提供证书复印件，并加盖证书持有人公章)。 | 51 |  |  | 联想 |
| 14 | LED屏 | P2 | 1. 5.12m\*2.08m，像素间距2mm 2. 色温 3200K—9300K可调 3. 对比度：≥3000:1 4. 寿命典型值≥50000H 5. 工作温度范围-20 ℃ 至 50 ℃ 6. 最大功耗≥166 W、平均功耗≥55.3 W； 7. 刷新率≥3840HZ。 | 10.6 |  |  | 洲明、三思、海康威视 |
| 15 | 实体网络安全攻防系统 | 防火墙 | 1U,内存4G，5个10/100/1000BASE-T接口和2个SFP插槽,单电源,防火墙吞吐1.5G，并发连接50万，每秒新建连接1.5万，应用层吞吐量1G，FW+IPS吞吐量600M，FW+AV吞吐量450M，全威胁吞吐量350M，IPSEC VPN吞吐300M，IPSEC VPN隧道数100。产品厂家具备TL9000质量管理体系认证证书、数据安全评估能力证书。 | 2 |  |  | 天融信、网御星云、新华三 |
| 16 | VPN | 1U,内存：4G，CF卡：1G，4个千兆电口,单电源,整机吞吐600M 并发连接50万 IPSEC吞吐60M SSL吞吐120M 最大并发用户数300；含10个SSL VPN的客户端许可；产品厂家具备TL9000质量管理体系认证证书、数据安全评估能力证书 | 2 |  |  | 天融信、网御星云、新华三 |
| 17 | WEB应用防火墙 | 1U,1个管理口、1个HA口、4个千兆电口（支持1组Bypass）、8G内存,单电源,应用层吞吐200Mbps、网络层吞吐2.5G、并发连接50W；含1年产品特征库升级许可；产品厂家具备TL9000质量管理体系认证证书、数据安全评估能力证书 | 2 |  |  | 天融信、网御星云、新华三 |
| 18 | 上网行为管理 | 1U,1个console口，6个千兆电口，单电源,建议适配带宽：30M 网络吞吐：100M 推荐用户数：50人 硬盘存储500G 设备内存2G；包含应用识别功能，含一年的系统版本，URL库及应用特征库升级许可；产品厂家具备TL9000质量管理体系认证证书、数据安全评估能力证书 | 2 |  |  | 天融信、网御星云、新华三 |
| 19 | 入侵防御系统 | 1U,内存8G,6个千兆电口（支持1对Bypass),单电源,整机吞吐率：1Gbps,IPS吞吐率：500M；含：1年攻击检测规则库、应用识别库、地理信息库升级许可；1年僵尸主机规则库升级许可；产品厂家具备TL9000质量管理体系认证证书、数据安全评估能力证书 | 2 |  |  | 天融信、网御星云、新华三 |
| 20 | 路由器 |  | 千兆网管式路由器 | 1 |  |  | 华为、锐捷、华三 |
| 21 | 服务器机柜 |  | 600\*1000\*2000MM | 1 |  |  | 图腾 |
| 22 | PDU供电电源 |  | GNE-1080  8位总控  全长3米 | 1 |  |  | 公牛 |
| 23 | PLC控制系统 |  | 12路PLC控制系统、强电控制柜，采用可编程逻辑控制器，12路顺序上电，间隔时间可设置，12路逆序断电，间隔时间可设置，单路可设置是否启用 | 1 |  |  | 含控制柜 |
| 24 | 电源地插座 |  | 五孔 固定在地面（阻尼式地脚插） | 26 |  |  | 公牛 |
| 25 | 插排 | GN-H3053 /GN-H3060 | 全长3米独立分控开关五位 | 26 |  |  | 公牛 |
| 26 | 电源线 |  | 2.5平方 国标 | 1批 |  |  | 远东、华美 |
| 27 | 网络布线 |  | 六类网线 | 1批 |  |  | 韩电、普天等 |
| 28 | 配线架 |  | 24口 六类 | 3 |  |  | 韩电、普天等 |
| 29 | 理线架 |  | 24口 六类 | 6 |  |  | 韩电、普天等 |
| 30 | PVC线管 |  | Φ20  阻燃绝缘管 | 1批 |  |  | 中财、联塑 |
| 31 | PVC线槽 |  | 阻燃 100\*50,100\*100 | 1批 |  |  | 国产优质 |
| 32 | USB延长线 |  | 10373 | 50根 |  |  | 绿联 |
| 33 | 辅材 |  | 网络水晶头、机柜螺丝、尼龙胀管、螺丝、螺钉、标签、扎带、胶带等 | 1批 |  |  | 国产优质 |
| 34 | 全钢陶瓷防静电地板 |  | 600\*600\*40（象牙白） | 125平方 |  |  | 国产优质 |
| 35 | 安装调试费 |  | 对客户设备部署环境进行勘察，设备安装与调试，及必要的使用培训服务（搭建实验环境等），含售后、安装、电脑上楼、调试等 | 1批 |  |  |  |
| 36 | 5年的更新服务 |  | 对漏洞、攻击方法、防护手段等进行定期更新服务 | 1项 |  |  | 奇安信、绿盟、安恒、天融信 |
|  | 合计 |  |  |  |  |  |  |

**四、实验（训）室平面图及布局图**

|  |
| --- |
|  |