**第七部分招标项目需求**

## 7.1建设目标

建成一个立足海南大学，辐射海南区域的集教学、培训、科研及社会服务为一体的综合型网络信息安全人才培养中心，培养高素质的网络信息安全技术应用型和创新型人才。具体目标包括：

建设一个网络安全与密码实验室：即一个网络安全与密码教学实训平台，包括网络安全及密码教学、实训和攻防靶场等内容。

实现四大功能：网络信息安全人才培养、网络信息安全行业认证服务、网络安全攻防演习服务、网络安全CTF大赛及人才选拔服务。

服务七大领域：政府单位、行业监管机构、企事业单位、大数据与软件产业、移动互联网产业、物联网产业、工控系统产业。

## 7.2项目建设需求

### 7.2.1用户分析

海南大学网络安全与密码教学实训平台建设除了支持教学以外，在支持科研创新上也应发挥重要作用。利用云计算虚拟化技术构建的网络安全与密码教学实训平台，可以对信息安全技术、新方法、行业热点技术进行方便快捷的实验验证。为海南大学提供良好的科研创新实践环境，进而使得科研项目更加快速和顺利的开展。

通过建设本地化人才实训基地，培养优秀师资力量。与海南省政企形成一条良好沟通、交流、互动的桥梁。通过对政企等行业提供安全培训、实战化技能培训、人才选拔等服务，加强政企骨干技术管理人员信息安全意识、安全技能，提升海南省整体信息安全管理水平。促进我省信息行业良性发展。此外，通过此人才实训基地为我校学生提供了一个与政企之间交流良好的机会，通过长期性的组织我校领导、教师、学生和政企代表加强交流、合作。未来，我校学生可直接通过快速通道，进入政企等行业实习、就业。

### 7.2.2业务需求分析

本项目旨在营造一流网络空间安全科研实验环境，吸纳国内外一流网络安全人才，建成一个立足海南大学，辐射海南区域的集教学、培训、科研及社会服务为一体的综合型网络信息安全人才培养中心，培养高素质的网络信息安全技术应用型和创新型人才。

结合国内外网络安全技术发展动向，建设一个实训平台：即海南大学网络安全与密码教学实训平台。

一、建设国际一流的网络安全与密码教学实训平台：基于互联网重大安全漏洞的实战化平台。提供了网络安全、主机安全、应用安全、数据库安全四大层面的重大安全漏洞实战项目。所有实战化项目划分了初级、中级、高级不同难度的实战。并在实验过程中提供了详细的实战化项目操作作业指导步骤和实战化配套环境。为教师提供进行有针对性的信息安全上机实验服务，提供各种漏洞场景、详细的实验步骤说明。结合理论教学，在真实的系统中去了解黑客如何利用漏洞对系统造成破坏，提高漏洞检查、测试、防御的能力。通过开展对各种信息安全知识点的实操实训工作，来加强我校学生的漏洞发现能力、漏洞修复能力，以及攻击防御能力。并通过学习了解黑客的思维方式和攻防习惯，整体提升学生的基础功底、理论、实战、经验等综合能力。有助于为我国网络安全行业输送出高尖端技术人才；

二、与国内知名安全企业合作，为在校教师提供专业安全技能学习及资质认证培训机会，以迅速提升教师专业领域前沿知识积累及实践扩展，为本校建设一一流网络信息安全专业做好师资储备。

## 7.3需求清单

| **序号** | **名称** | **参考品牌型号及技术参数** | **单位** | **数量** | **备注** |
| --- | --- | --- | --- | --- | --- |
| **一、网络安全与密码教学实训平台** | | | | |  |
| **（一）软件部分** | | | | |  |
| 1 | 网络安全及密码教学培训管理平台 | 平台功能：教学培训 1）综合管理：综合管理是培训系统、实操系统、仿真功能、安全实训、资源库的统一化、集中化3A认证管理平台，具有云计算、云资源统一调度管理能力。 2）资源库：资源库为业务实现提供便利的资源和工具，平台包含漏洞库、知识库、工具库、镜像库和场景库，用户在业务场景下可以随时调用所需资源，并且资源支持横向扩展。 3）教学培训：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，分红队/蓝队进行学习， 4）考核检验：考核检验能够对试题、试卷和考试进行管理，平台支持人工组卷、动态组卷、智能组卷三种组卷模式，支持购物车式选题，平台具有防作弊功能。 5）安全研究：仿真资源统一管理引擎、虚实结合引擎、网络编排引擎、场景构建引擎，从资源管理到整体场景构建编排仿真出多样化的贴近真实业务，包括复杂网络结构的安全场景，安全研究是基于标准安全场景仿真，进行已知漏洞和安全问题的研究，同时可针对安全场景进行漏洞挖掘及安全研究。 6）供全中文WEB管理界面，无需安装任意客户端软件或插件；   1. 平台提供物理机管理，支持手动添加关联多台物理机设备资源； 2. ★平台支持容器、KVM两个类型的集群管理，其中KVM支持至少三种以上的集群类型（提供现场演示，及提供相关截图证明并盖厂商章）； 3. ★平台提供网段管理，支持配置多IP地址段，用以自动分配创建的实例化资产（提供相关截图证明并盖厂商章）； 4. 支持查看平台整体资源占用和分配情况，包括CPU、内存、硬盘、虚拟机、路由、交换机等； 5. 支持查看平台日志吞吐量的相关数据情况； 6. ★平台支持对实例进行管理，包含虚拟机、docker容器等类型实例，可对实例进行关机、重启、回收、快照的创建与恢复、重置等独立操作与统一化管理，同时支持查看实例的IP和开放的端口号，支持通过浏览器的方式操作虚拟终端（提供相关截图证明并盖厂商章）； 7. 平台支持日志审计功能，支持记录和查看平台用户的操作日志信息，支持日志检索以及日志批量导出； 8. ★平台支持部门管理功能，可构建至少三级以上部门组织架构，并可设置部门所在省市区信息，通过部门实现人员的分级管理（提供相关截图证明并盖厂商章）； 9. 平台支持角色管理与权限管理功能，平台内置管理员、教员、学员三类角色，支持角色自定义，可以为角色划分不同功能权限、接口权限； 10. 平台支持用户管理功能，可以为用户分配多个角色，并支持用户的禁用、启用、修改密码等操作； | 套 | 1 | 许可授权（支持并发数）：120人 |
| 2 | 网络安全及密码教学培训资源内容 | 内容资源：教学培训 1）知识库：课程内容包含网络安全法律法规、密码学、网络安全、渗透测试、代码审计、软件安全、移动安全、工控安全、二进制安全、CTF夺旗赛、攻防对抗赛、应急响应、安全加固、安全产品、安全攻击使用、Python安全开发等1000课时的课程与实验资源，课件具有PPT、PDF、视频等多媒体课件、CTF实验课件、实验指导手册等。 2）漏洞库：漏洞库中漏洞80000个，其中CVE漏洞验证实验（含POC、靶机）（2015年后的超过50个）。 3）工具库：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500款工具，支持工具分类、工具定义和资源扩展。 4）镜像库：镜像类型包含windows、linux两大类，共200个镜像，其中包含windows7、windows xp、windows server 2008、windows server 2012、centos6、centos7、ubuntu14、ubuntu16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。 5）场景库：支持自定义场景，也可接受场景定制。 6）理论题库：包含1500道理论考题。   1. 课程支持三级标签管理，每个课程可以拥有多个标签，平台能够按照标签进行课程的分类和筛选，同时课程支持按照难易程度进行划分和筛选（提供相关截图证明并盖厂商章）； 2. ★课程可设置多个知识点及关联相关课程，通过关联课程功能可建立多课程之间的关联管理，单个课程可包含理论知识、实验、考试、作业等内容，课件资源类型支持PDF、WORD、MarkDown、视频、实验靶机、场景等；（提供相关截图证明并盖厂商章）； 3. 平台支持通过关联内置课程制定培训计划，单场培训支持添加多个班级，针对人员的学习情况，可以以个人、单个班级、整场培训的纬度进行人员及相关学习成果的管理，包括学习进度、作业提交情况及分数、考试情况及分数，支持教员对学员作业和考试进行批改、打分（提供相关截图证明并盖厂商章）； 4. ★实验课程支持关联实验工具，工具类型支持虚拟机型和下载型，虚拟机型工具可直接在界面启动后直接使用； 5. 实验课程支持实验的拓扑展示及拓扑的构建和回收，支持通过拓扑图，点击查看终端详情并进入虚拟终端操作界面进行终端的管理和操作，支持拓扑和实验内容的同屏展示，支持虚拟机终端操作界面与实验内容的同屏展示（提供相关截图证明并盖厂商章）； 6. 创建安全研究时，支持设置难度等级，关联安全场景，支持用户针对自定义安全场景开展安全研究工作，提交研究成果，研究成果支持上传附件或关联平台漏洞作为相应成果，附件类型支持word、pdf、mp4等格式（提供相关截图证明并盖厂商章）； 7. 支持查看安全研究场景拓扑，并支持安全场景的构建、回收、重新创建、快照的生成与恢复，支持通过拓扑图，点击查看终端详情并进入虚拟终端操作界面进行终端的管理和操作，拓扑图支持展示创建的实例清单和相关实例的实时状态（提供相关截图证明并盖厂商章）； 8. ★试题题目类型包含判断题、单选题、多选题、填空题、简答题，理论题库数量不少于3500道；（提供相关截图证明并盖厂商章） 9. 平台支持批量导入试卷或自定义构建试卷，支持人工组卷、智能组卷、动态组卷等三种组卷模式（提供现场演示，及提供相关截图证明并盖厂商章）； 10. 智能组卷支持依据题目类型、标签、难度等维度，进行组卷规则的配置，每条规则支持设置对应题目的数量和分数，每张试卷支持配置多条规则，根据规则自动生成试卷，支持对生成的试卷进行人工调整，同时能够支持根据规则重新生成试卷（提供相关截图证明并盖厂商章）； 11. ★动态试卷支持以规则的形式保存试卷，当考试使用时，每个人进入考试，都会根据动态试卷规则，生成全新试卷，试卷规则支持依据题目类型、标签、难度等维度进行配置，每条规则支持设置对应题目的数量和分数，每张试卷支持配置多条规则，根据规则进行组卷（提供相关截图证明并盖厂商章）； 12. ★考试支持花卷和动态试卷两种防作弊模式，花卷模式，每个选手看到的题目顺序和答案顺序都不一样，动态试卷模式，每个选手拿到的题目都不一样（提供现场演示，及提供相关截图证明并盖厂商章）； 13. 考试支持设置是否开放交卷，如设置为不开放交卷，所有考生都不允许交卷； 14. 支持对自己创建的考试进行管理，包括阅卷、查看考生分数、查看参与和完成考试人数等，支持根据考试状态、考试模式、考试时间、考试名称等进行筛选； 15. 资源库包含镜像库、工具库、漏洞库、知识库、场景库，应具有统一管理界面，支持资源的上下线、批量管理、资源库扩展，所有资源支持标签化管理；（提供现场功能演示） 16. 镜像库支持以上传或平台内直接制作镜像的方式进行镜像的创建，镜像类型支持虚拟机、容器两种，虚拟机支持qcow2格式，容器支持直接上传docker镜像及docker file+源码两种方式，虚拟机镜像支持配置CPU、内存、端口、数据盘等配置信息，容器镜像支持配置CPU、内存、端口等配置信息； 17. 镜像数量不少于400个，镜像类型应包含windows、linux两种类别，其中涵盖windows7、windows10、windows xp、windows server 2003、windows server 2008、windows server 2012、windows server 2016、centos6、centos7、ubuntu12、ubuntu14、ubuntu16、ubuntu18、Debain8、Kali2.0、Kali2017等操作系统类型，可根据镜像类型进行筛选（提供相关截图证明并盖厂商章）； 18. ★工具库中工具数量应不少于500款，工具类型应包含应急响应、日志分析、电子取证、病毒检查、渗透测试、通用工具、逆向工程、Pwn等8种类别，工具应不得捆绑具有木马后门、病毒程序（提供相关截图证明并盖厂商章）； 19. 漏洞库中漏洞数量应不少于80000个，带复现环境CVE漏洞不少于50个； 20. 知识库支持用户自定义创建安全知识，安全知识内容可包含视频、PDF、WORD以及MarkDown等类型资源，同时支持关联工具、实验场景、镜像等资源； 21. 维保期内，提供每年更新5个场景、50个带环境的漏洞，其余资源实时更新； | 套 | 1 |
| 3 | 网络安全攻防实训靶场 | 平台功能：教学实践实训，主要是针对教学理论技术掌握进行的实践操作，围绕学生对网络安全，渗透测试、代码审计、攻防对抗、安全攻击等理论知识掌握的一种实践实训检测手段，加强学生对理论知识的掌握能力。  1）实践管理：平台可以自行定义理论实践的模式，针对实践实训配置、网络配置、实训题目、实训团队、积分、报表、题库、反作弊等进行管理和维护；  2）实训监控：平台可以针对实践实验进行中的各阶段进行状态和资源的监控，并进行配置管理。具有防作弊机制，具有多种作弊处罚手段，能够实时检查实践团队之间相互交换FLAG行为，并自动化检测、发布违规公告、扣分处理、及时发现实训存在的问题；  3）阶段管理：平台支持混合实践实训，将各个实训类型进行组合，每个实训类型都作为一个阶段，每个阶段设置准入条件，支持对单个实训阶段的独立管理，其中包含该阶段下的选手、题目、解题思路、各类实训结果展示榜单等资源的统一管理；  4）实训场景和题目管理：不同的实训形态满足了不同的训练需求，实训系统内置了丰富的网络安全攻防题型及典型攻防对抗业务场景，包含一举夺魁实操训练题、BTC闯关实操训练、AWD对抗实操训练、CTL领地实操训练，以及对经典攻防技术实操训练的套题和实操训练场景管理；  5）大屏展示：为了方便实训老师对学生实际掌握的能力和技能有直观的判断和了解，实训平台提供大屏展示功能：支持实训地图台、得分曲线、夺魁积分榜、闯关积分榜、对抗积分榜、领地积分榜、实时事件等多种可视化维度。拥有不少于15类榜单查看与导出，有学生个人积分榜、学生个人奖牌榜、题目视角速度榜、选手视角速度榜、闯关赛积分榜、单兵攻击实训榜、单兵实训防守榜、单兵运维榜、单兵高地占领数量榜、单兵攻防实训积分榜、单兵拓荒实训榜、团队积分实训榜、团队高低占领数量榜、团队攻防积分榜、团队拓荒榜等。  6）资源库：资源库为业务实现提供便利的资源和工具，实训资源包含工具库、镜像库，用户在业务场景下可以随时调用所需资源，并且资源支持横向扩展。  7）★支持混合竞赛模式，一场竞赛可包含多个阶段，每个阶段可添加不同赛制类型，同时支持依据人数、分值、排名等设置阶段的准入条件，赛制类型支持CTF夺旗赛、BTC闯关赛、AWD攻防赛、CTL领地赛四种（提供现场演示，及提供相关截图证明并盖厂商章）；  8）赛题支持以类别、标签、难度、套题等多个维度进行分类管理，可根据靶机、附件、题目等多类信息进行赛题检索，同时赛题支持查看解题提示和解题思路，赛题支持共享靶机和独占靶机的模式，对于共享靶机的赛题支持靶机负载（提供相关截图证明并盖厂商章）；  9）竞赛支持平台用户和非平台用户两种人员组织模式，平台用户模式通过关联平台内用户组织竞赛，用户的竞赛相关成绩可被记录到用户信息中，支持可延续性，非平台用户模式通过导入临时用户的方式组织竞赛，此类用户仅限于当次比赛使用，成绩没有可延续性（提供相关截图证明并盖厂商章）；  10）竞赛支持设置是否对选手开放排行榜，是否在大屏显示排行榜，并同时支持对大屏的标题和logo进行配置（提供相关截图证明并盖厂商章）；  11）竞赛支持配置靶机访问的IP白名单，白名单中的IP地址支持访问任意靶机；  12）竞赛内用户分为管理员、裁判、选手、观众四种角色，支持通过批量导入、关联平台用户（平台用户模式竞赛）或手工添加（非平台用户模式竞赛）的方式添加竞赛相关用户，支持导出相关选手或团队信息（提供相关截图证明并盖厂商章）；  13）竞赛开始后，支持自动构建靶机环境，并为环境制作初始快照，竞赛开始前，支持提前手动构建靶机环境，可对靶机进行一键准备、一键回收、批量开机、关机、重启、重置、回收、生成快照、切换竞赛网络、切换中立网络等功能；  14）★竞赛概述支持对整场比赛相关情况进行概览，包括竞赛基本信息、实际参赛人员情况、赛题准备进度情况、竞赛靶机状态、竞赛阶段相关信息，阶段信息包括阶段的类型、时长、题目准备情况、参赛人数、题目难易程度、阶段状态、阶段准入条件，并提供快速入口进入相关信息的配置界面（提供相关截图证明并盖厂商章）；  15）竞赛过程中，支持对本场竞赛和各阶段的基本信息进行配置，包括竞赛名称；  16）支持对单个竞赛阶段的独立管理和配置，其中包含该阶段下的选手、题目、解题思路、各类竞赛展示榜单等资源的统一管理（提供相关截图证明并盖厂商章）；  17）竞赛开始前和过程中都支持添加新的阶段；  18）★阶段支持根据设定的时间自动开始和结束，同时支持以手工的方式提前开始、和提前结束，并可对阶段进行暂停和恢复的操作（提供相关截图证明并盖厂商章）；  19）阶段概述支持对当前阶段相关情况进行概览，包括阶段基本信息、参赛人员情况（包括正常选手人数、作弊选手数量、禁赛选手数量）、题目准备情况、靶机准备情况、阶段倒计时等内容，并提供快速入口进入相关信息的配置界面（提供相关截图证明并盖厂商章）；  20）CTF夺旗赛计分方式支持防PY模式，普通模式和递减模式，其中防PY模式是指选手得分为题目总分除以解出题目的选手数量，递减模式支持按分数比例递减和按固定分值递减，并可设置最低比例和最低分值；  21）★CTF夺旗赛赛题支持以分组的方式进行管理，支持将题目设置为隐藏题，隐藏题只有在手动设置显示后选手才可见（提供相关截图证明并盖厂商章）；  22）CTF夺旗赛对于多靶机和多附件的题目，支持以题目的视角查看相关题目的靶机情况和附件情况，包括靶机的基本信息和分配情况，附件的基本信息和分配情况等；  23)★BTC闯关赛，支持对题目的基本信息进行配置，并支持对题目内关卡的基本信息进行配置，同时支持显示或隐藏关卡，显示关卡难度、顺序、分值、过关、闯关人数等信息（提供相关截图证明并盖厂商章）；  24)BTC闯关赛的所有选手独享靶机环境，且只允许拥有靶机的选手进行访问，其他选手无法访问，各靶机之间实现网络隔离，不能互相访问（提供相关截图证明并盖厂商章）；  25)AWD攻防赛，支持设置初始分值和每轮的时长，支持设置是否对选手开放重置靶机功能，支持设置靶机重置保护时间，支持开启靶机重置扣分模式，该模式下支持配置最大免费重置次数及超出次数后的扣分分值（提供相关截图证明并盖厂商章）；  26)AWD攻防赛支持积分榜、攻击榜、防守榜、运维榜等维度的数据统计，其中，运维榜是指因服务故障扣分数量的排行榜，并支持以上榜单的导出（提供相关截图证明并盖厂商章）；  27)★CTL领地赛支持以区域的方式进行题目分组，支持夺旗题和领地题，针对区域进行开启或隐藏设置，并支持针对赛题进行开题、关题、显示、隐藏等操作（提供相关截图证明并盖厂商章）；  28)态势大屏支持以雷达图形式展示选手的技能分布，支持自定义剧情的展示，自定义剧情包括对话、视频、图片等形式，支持展示选手的攻防态势和解题情况； | 套 | 1 |  |
| 4 | 网络安全攻防实训靶场内容资源 | 内容资源：教学实践实训，对学生理论实践操作所需要配备的基础实践实训题库和场景设置。  1) 各类实训题：题库共有200道实训题，难易程度分初级、中级、高级，知识技能范围涵盖WEB安全、Crypto密码学、网络安全、渗透测试、安全攻击、Reverse逆向工程、Misc安全杂项、Pwn溢出等五大类型；  2）经典实训套题：针对各类安全理论实训挑选或定制的若干经典实训套题。  3）工具库：为满足学生在实践过程使用，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500款工具，支持工具分类、工具定义和资源扩展。  4）镜像库：镜像类型包含windows、linux两大类，共200个镜像，其中包含windows7、windows xp、windows server 2008、windows server 2012、centos6、centos7、ubuntu14、ubuntu16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。  5) 题库至少包含Web安全、Crypto密码学、Reverse逆向工程、Misc安全杂项、Pwn溢出五大类型（提供相关截图证明并盖厂商章）；  6) ★题库涵盖容易、中等、困难等难易程度（提供相关截图证明并盖厂商章）；  7)题库数量不少于300道；  8)题库应涵盖如下所有知识技能大纲：  ★Web安全 HTTP请求伪造、HTTP来源头伪造、HTTP返回头分析、HTTP返回内容分析、HTTP请求UA头伪造、SQL基本注入、SQL无回显盲注、SQL二次注入、SQL WAF绕过注入、SQL宽字节注入、SQL报错注入、SQL文件操作、SQL比较盲注、SQL有回显注入、PHP代码执行、PHP弱类型特性、PHP反序列化、PHP文件包含、PHP命令执行、PHP其他语言特性、PHP变量覆盖、Cookie认证绕过、JWT绕过、源码文件泄露、备份泄露、文件泄露、网站信息泄露、文件上传基础利用、文件上传条件竞争、文件上传黑名单绕过、文件上传白名单绕过、NOSQL永真式攻击、Node语言特性、Node原型链污染、业务逻辑漏洞、数据校验绕过、Python模板注入、Python沙箱逃逸、有回显XXE、个人信息搜集、常规暴力破解、反射型XSS、WAF绕过XSS、CSRF基本利用；  Crypto密码学 指定规则的简单代换密码、流密码、RSA、数字签名、Costas阵列、凯撒密码、ASCII移位、栅栏密码、猪圈密码、曲路密码、Morse 编码、Base 编码、ASCII 编码、进制转换、Brainfuck编码、RSA p & q 不当分解N、RSA模不互素、共模攻击、低解密指数攻击、小公钥指数攻击、提取PEM文件信息、MD5暴力攻击、背包密码、Paillier加密、DSA已知k攻击k、DSA共享攻击、AES加密CBCECB、电脑键盘QWE加密、dvorak键盘加密、仿射密码词频分析、维吉尼亚密码、Playfair密码、四方密码、LCG A、B、M以及N0已知等；  ★Reverse逆向工程 java逆向、python逆向、js逆向、native逆向、C#逆向、go逆向、迷宫加解密、矩阵解密、BlowFish加解密、SHA加解密、MD5异或、Base64、rot位移、RC4、AES、自定义加密、方程组、RSA、变种Base、Base58、RC5、ICEKEY、SM4、代码混淆控制流平坦化、花指令、脱壳、虚假控制流、虚拟指令、固件解包、Win32消息处理、Win32资源处理、TLS反调试、ptrace反调试、调试器检测、STARTUPINFO信息检测、二叉树、vector；  Misc安全杂项 内存取证、安全事件分析、U盘取证、磁盘取证、Web流量分析、蓝牙流量分析、网络协议流量分析、加密流量分析、图片隐写、文件修复文件检测、压缩包爆破、压缩包伪加密、压缩包明文攻击、压缩包CRC32碰撞、压缩包暴力破解、压缩包注释查看、数据及编解码转换；  Pwn溢出 栈漏洞利用ret2shellcode、栈漏洞利用canary绕过、栈漏洞利用ret2libc、栈漏洞利用BROP、栈漏洞利用ret2text、栈漏洞利用stack pivoting、整数溢出符号位溢出、整数溢出进位溢出、32位栈上格式化字符串漏洞利用、64位栈上格式化字符串漏洞利用、堆漏洞利用Unlink、堆漏洞利用House of Orange、堆漏洞利用top chunk attack、堆漏洞利用House of Force、堆漏洞利用Fastbin Attack、堆漏洞利用Double Free、堆漏洞利用off by one、堆漏洞利用UAF、堆漏洞利用Tcache Attack、堆漏洞利用off by null、堆漏洞利用House of Rabbit；   1. 镜像库支持以上传或平台内直接制作镜像的方式进行镜像的创建，镜像类型支持虚拟机、容器两种，虚拟机支持qcow2格式，容器支持直接上传docker镜像及docker file+源码两种方式，虚拟机镜像支持配置CPU、内存、端口、数据盘等配置信息，容器镜像支持配置CPU、内存、端口等配置信息； 2. ★CTF竞赛镜像数量不少于200个，镜像类型应包含windows、linux两种类别，其中涵盖windows7、windows10、windows xp、windows server 2003、windows server 2008、windows server 2012、windows server 2016、centos6、centos7、ubuntu12、ubuntu14、ubuntu16、ubuntu18、Debain8、Kali2.0、Kali2017等操作系统类型，可根据镜像类型进行筛选（提供相关截图证明并盖厂商章）； 3. ★工具库中工具数量应不少于500款，工具类型应包含应急响应、日志分析、电子取证、病毒检查、渗透测试、通用工具、逆向工程、Pwn等8种类别，工具应不得捆绑具有木马后门、病毒程序（提供相关截图证明并盖厂商章）； | 套 | 1 |
| 5 | 网络安全与密码竞技平台技术支撑服务 | 为了检验学生的真是技术能力和攻防水平，提供一次满足120人本地同时在线进行CTF夺旗赛，题目类型范围涵盖WEB安全、Crypto密码学、Reverse逆向工程、Misc安全杂项、Pwn溢出五大类型。  1、负责现场演习相关的网络搭建与配置，参与选手环境监控，审计和配置管理，  2、负责现场演习平台的部署、配置、验证、数据导入等环节工作，被攻击互联网资产排查扫描。  3、负责演习活动的全程保障，针对参演选手提出的问题进行答疑，对演习过程中出现的参演选手账户、平台、环境等相关问题进行及时处理，对演习结果进行有效的评判，保障演习有效进行。  4、比赛结束后对整个比赛进行结果的汇总，全程的回顾，问题的总结 | 次 | 1 |  |
| **（二）硬件部分** | | | | |  |
| 1 | 攻防平台专用硬件 | 服务器参数： 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：10核 20线程 \* 2 内存：128G 硬盘容量：4T\*4，可用空间不小于7T 固态盘：960G SSD\*2 Raid卡：2GB 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 (含1台交换机，参数：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)。 | 套 | 4 |  |
| 2 | 防火墙 | 1. 标准1U硬件平台；双交流电源；含12\*GE电口,12\*SFP光口，500G硬盘，网络吞吐量8Gbps；最大并发连接数大于300万，每秒新建HTTP连接数大于10万。（默认SFP接口不带光模块）。 2.下一代防火墙模块：基本网络防火墙功能，IPSEC VPN功能，攻击防护，访问控制功能，用户认证功能，链路负载均衡功能、流量控制功能。 3.上网行为管理许可（APP&URL）：关键字过滤和URL过滤，丰富的应用对象和URL数据库可以帮助管理员轻松设置禁止访问的网页，控制对不良网站的访问。 4.防病毒许可（AV）：支持大病毒文件的扫描，实时病毒连接阻断，病毒事件记录，支持常见病毒传输协议HTTP、FTP及各种邮件协议扫描。 5.入侵检测与防御许可（IPS）：基于状态、精准的高性能攻击检测和防御，实时攻击源阻断、IP 屏蔽、攻击事件记录，支持针对多种协议和应用的攻击检测和防御，支持SQL注入和XSS防御、外链防护和Web访问控制。 2. 支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、会话老化时间、终端过滤等高级访问控制功能（提供相关截图证明并盖厂商章） 3. 支持对SSL协议进行解密，解密类型支持https和邮箱 4. ★支持智能和快速两种应用识别模式，在智能识别模式下应用引擎尽可能地用各种方式识别网络流量，在快速识别模式下应用引擎将关闭部分智能分析功能以提高性能（提供相关截图证明并盖厂商章） 5. 支持识别和封堵私接主机，包括360随身wifi、猎豹wifi、无线路由器等软硬件网络共享方式；可制定策略分别设置私接终端类型个数为阀值进行封堵，同时支持基于IP配置白名单，支持自定义阻断时间，支持限速时长内添加到惩罚通道（提供相关截图证明并盖厂商章） 6. 支持WEB Portal认证功能，支持本地认证、Radius认证、LDAP认证 和LDAP用户同步，支持对接IMC、AAS、SAM等常见AAA服务器，支持配置强制重新认证间隔，支持配置认证通过后重定向URL，要求本机自身支持短信认证功能 7. 支持portal服务器联动，支持radius服务器联动，支持实现NAS-Identifier(32)在无线场景携带AC名字 8. ★支持微信认证，可以选择获取IP地址、OpenID或手机号等实名信息，支持与微信公众平台进行认证联动，认证方式包括公众号按钮跳转、公众号回复关键词等方式。认证过程中要求用户必须关注公众号，帮忙企业实现品牌营销（提供相关截图证明并盖厂商章） 9. 支持短信认证，登录后方可认证上网 10. 支持IP准入、MAC准入、IP+MAC准入、本地WEB认证、Portal认证、短信认证、免认证、微信认证、混合认证、AD域单点登录和访客二维码认证（提供相关截图证明并盖厂商章） 11. ★预置防护模板，可基于常见场景进行一键式的安全加固；支持基于常见协议进行异常检查，包括但不限于：HTTP、HTTPS\DNS、SMTP、POP3、FTP；检查内容支持自定义，包括但不限于：url长度、请求长度、目录长度、host字段、version字段、字符检测、文本长度、文件名长度、命令参数长度，支持针对每协议设置处置动作和事件等级。（提供相关截图证明并盖厂商章） 12. 支持针对攻击进行本地报文存储，方便管理员事后回溯攻击事件，支持针对某一个和某一类攻击设置报文存储机制；支持针对某一个和某一类攻击的源地址进行隔离，隔离时间可自定义。（提供相关截图证明并盖厂商章） 13. ★支持自定义IPS特征，至少支持IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等协议自定义入侵攻击特征；可拓展协议字段，设置数据包中的匹配内容；支持选择包含、等于、不等于、大于、正则匹配等匹配方式；可选择多种匹配条件，支持设置“与”和“或”的匹配顺序；支持设置检测方向，包括双向、客户端方向和服务端方向；支持自定义选择重要等级。（提供相关截图证明并盖厂商章） 14. 支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀，支持查杀邮件正文/附件、网页及下载文件中包含的病毒，支持400万余种病毒的查杀，并支持在线升级和手动升级病毒库 15. 支持对最多20级的压缩文件进行解压查杀。 16. 支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口，也可通过流量自学习获得服务器合法的外联行为，学习时长可选择1小时、12小时、一天、一周等（提供相关截图证明并盖厂商章） 17. 至少支持telnet、ssh、ftp、imap、pop3、smtp、mysql、postgresql、mssql、rlogim、vnc等常见协议的弱密码检测功能，支持弱口令、空密码、用户名和密码相同等检测方式，弱口令字典可自定义设置。（提供相关截图证明并盖厂商章） 18. ★拥有自有数据来源，每日可获得不低于6亿次的互联网访问样本（提供相关截图证明并盖厂商章） 19. 支持实时获取威胁情报，并应用威胁情报对本地资产进行威胁检测，并可对检测到的威胁情报支持单点登陆威胁情报云平台查看该情报详情。 20. ★支持缓存安卓和iOS文件，文件形式不限于视频、APP、文本文件等，并支持自学习性缓存，设备可自动缓存特定服务器的所有终端应用（提供相关截图证明并盖厂商章） 21. web管理界面支持Ping、Traceroute、TCP Syn诊断工具，可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析。（提供相关截图证明并盖厂商章） 22. 支持管理员双因子认证 | 台 | 1 |  |
| 3 | 实验室电脑 | 技术参数和规格 CPU 英特尔i5-10500处理器（3.1G主频、6核）； 主板 Intel 400芯片组或更高；内存 16G DDR4； 硬盘 1块 256G SSD； 显卡 集成； 声卡 集成声卡，内置音响； 网卡 千兆网卡,支持M.2 无线网卡； 接口 ≥6个外置 USB 端口 ，机箱 ≤15L； 电源 ≥260W；后置电源诊断灯（不启动检查电源）； 键鼠 USB键盘和鼠标 ； 操作系统： 不含操作系统； 显示器 23.8寸显示器  提供非加插保护卡硬件实现的软件应用功能：  1、硬盘保护：保证电脑免受病毒和恶意破坏导致的系统崩溃  2、网络同传：数据通过局域网分发，可一次性部署所有设备；  服务 3年原厂整机（包含主机、显示器、键盘、鼠标）免费上门质保服务，所有服务可在电脑生产厂商官网或400/800电话查询确认； | 台 | 70 |  |
| 4 | 网络交换机 | 交换容量≥400Gbps； 包转发率≥144Mpps； 电源：为了提高设备可靠性，支持模块化可插拔双电源。 端口类型：48个千兆电口，4个万兆SFP+。 配置标准：USB接口，支持U盘快速开局。 二层功能：支持MAC地址规格≥16K。 ★支持ARP表项规格≥8000（提供第三方检测报告复印件并加盖厂商公章或投标专用章）。  支持4K个VLAN，支持Voice VLAN，基于端口的VLAN，基于MAC的VLAN，基于协议的VLAN。  支持1:1和N:1 VLAN Mapping功能。 三层功能支持RIP、RIPng、OSPF、OSPFv3、ISIS、BGP等路由协议。  ★支持Ipv4路由FIB表≥8K，Ipv6路由FIB表≥3K（提供第三方检测报告复印件并加盖厂商公章或投标专用章）  支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；  ★支持Telemetry技术，配合网络分析组件通过智能故障识别算法对网络数据进行分析，精准展现网络实时状态，并能及时有效地定界故障以及定位故障发生原因，发现影响用户体验的网络问题，精准保障用户体验（提供第三方检测报告复印件并加盖厂商公章或投标专用章）。  ★支持音视频业务的智能运维，将设备作为监控节点周期统计并上报音视频业务类指标参数至网络分析组件引擎，由网络分析组件引擎结合多个节点的监控结果，对音视频业务质量类故障进行快速定界（提供第三方检测报告复印件并加盖厂商公章或投标专用章）。  支持基于Python语言的开放可编程系统，管理员可以通过Python脚本对交换机进行运维功能的编程，快速实现功能创新，实现智能化运维。  支持能效以太网EEE节能环保。  提供工信部入网证。  ★投标产品须是国内外主流厂商产品，提供权威的国际咨询机构证明报告（提供第三方检测报告复印件并加盖厂商公章或投标专用章）。 | 台 | 2 |  |
| 5 | 单模万兆光纤模块 | 双芯万兆光模块-SFP+-10G-单模模块(1310nm,10km,LC) | 个 | 4 |  |
| **二、实验场地建设** | | | | |  |
| **（一）综合布线部分** | | | | |  |
| 1 | 理线器 | 网络24口机柜理线器 | 个 | 2 |  |
| 2 | 光纤 | 4芯室外光纤 | 米 | 600 |  |
| 3 | 光纤盒 | 4芯光纤盒 | 个 | 4 |  |
| 5 | 光纤耦合器 | LC-LC双芯单模光纤耦合器 | 个 | 16 |  |
| 6 | 光纤跳线 | 双芯单模LC-LC光纤跳线（3米） | 条 | 16 |  |
| 7 | 尾纤 | 单模LC光纤尾纤（1.5m） | 条 | 18 |  |
| 8 | 线槽 | 10CMM半圆线槽 | 米 | 50 |  |
| 9 | 光纤熔接 | 光纤熔接 | 芯 | 16 |  |
| 10 | 辅材 | 水晶头、胶水、钉子等 | 项 | 1 |  |
| 11 | 理线器 |  | 个 | 2 |  |
| **（二）实验室装修部分** | | | | |  |
| 1 | 强电工程 | 强电安装工程、插座开关、装饰灯、照明灯 | 项 | 1 |  |
| 2 | 木工及地面工程 | 造型吊顶、天花灯槽造型、铝方通吊顶、展台、墙面装饰、塑胶地板、地脚线安装 | 项 | 1 |  |
| 3 | 其它部分 | 装饰灯箱、画面喷绘、高级双层窗帘、材料搬运、完工清洁等 | 项 | 1 |  |
| **（三 ）大屏显示部分** | | | | |  |
| 1 | 55寸拼接液晶单元 | LCD液晶显示单元；LG面板。 尺寸：55英寸；3\*2； 分辨率：1920x1080； 视角：178°(水平)/ 178°(垂直)； 响应时间：8ms(G to G)； 对比度：1400:1； 亮度：500cd/㎡； 物理拼缝1.8mm；  图像显示清晰度≥950TVL; 输入接口：HDMI × 1, DVI × 1, VGA × 1, CVBS × 1, USB × 1。 输出接口：HDMI × 1, VGA × 1, CVBS × 1。 控制接口：RS232 IN × 1, RS232 OUT × 1。 可选配接口：3G SDI(输入×1、输出×1)、DP、HDbaseT、TVI(输入×1、输出×1)、网络源； 功耗：≤185W； 电源要求：AC 100-240V～, 50/60Hz； 寿命：≥60000 小时； 工作温度和湿度：0℃～40℃，10%～90% RH（无冷凝水）; 外形尺寸：1211.54 (W) mm × 682.34 (H) mm × 68.9 (D) mm 边框宽厚：0.9mm（左/上）,0.9mm（右/下）；  ★液晶显示单元的风扇具备良好的散热效果，风扇散热性能≥60%（需提供第三方权威机构出具的检验报告证明复印件，并加盖厂商公章或投标专用章）；  ★液晶显示单元具有色坐标一致性，根据CIE1931标准色度系统，液晶显示单元色坐标误差在±0.001以内（需提供第三方权威机构出具的检验报告证明复印件，并加盖厂商公章或投标专用章）；  ★液晶显示单元连续运行24小时，液晶表面中心温度≤50℃，边缘测试点与中心温差≤10℃。（提供封面具有CMA、ilac-MRA、CNAS标志的权威检测机构的检测报告复印件，并加盖厂商公章或投标专用章）。  ★拼接液晶单元满足保护环境要求，液晶拼接屏需满足中国电器电子产品有害物质限制使用的要求，并提供中国质量认证中心产品认证证书（需提供第三方权威机构出具的检验报告证明复印件，并加盖厂商公章或投标专用章）。 | 套 | 2 |  |
| 2 | 支架 | 55寸2X3 壁挂支架 | 套 | 2 |  |
| 3 | 超高清4K输入解码器 | 高清视音频解码器，采用Linux操作系统，运行稳定可靠 输入接口：支持一路VGA和一路DVI接入。 输出接口：支持12路HDMI和6路BNC输出，HDMI（可以转DVI-D）（奇数口）输出分辨率最高支持4K（3840\*2160@30HZ）。 编码格式：支持H.265、H.264、MPEG4、MJPEG等主流的编码格式； 封装格式：支持PS、RTP、TS、ES等主流的封装格式； 音频解码：支持G.722、G.711A、G.726、G.711U、MPEG2-L2、AAC音频格式的解码； 解码能力：支持12路1200W，或24路800W，或36路500W，或60路300W，或96路1080P及以下分辨率同时实时解码； 画面分割：支持1、2、4、6、8、9、10、12、16、25、36画面分割显示。 网络接口：2光口，2电口。 音频接口：支持12路音频输出，1路对讲输入，1路对讲输出。 串行接口：一个标准232接口（RJ45）、一个标准485接口。 报警接口：8路报警输入，8路报警输出。 产品尺寸：440mm(宽)×80mm(高)×311mm(深)。  ★支持PC 软件客户端、WEB 浏览器客户端、平台客户端、IPAD、可视化触控平台方式访问管理。（提供封面具有CNAS认证标识的公安部报告证明，并加盖厂商公章或投标专用章）  ★支持对输入的视频画面进行90°、180°、270°旋转显示（需提供公安部检验报告证明复印件，并加盖厂商公章或投标专用章）； | 台 | 1 |  |
| **（四）桌椅部分** | | | | |  |
| 1 | 讲台 | E1级钢制喷涂脚架，带键盘架，主机箱，桌面开孔线 | 张 | 1 |  |
| 2 | 电脑桌 | 环保E1级 | 张 | 34 |  |
| 3 | 电脑椅子 | 环保E1级 | 个 | 70 |  |

# 7.4其他要求

1、所投产品须为国产品牌，否则将导致无效投标。

2、供应商应对所投产品的参数进行响应，不能虚假应标，否则将承担相关的法律后果。

3、本项目要求提供以下支持服务：

1）整体项目提供不少于两年的免费维护，设备按原厂商标准提供维护。

2）投标人或生产厂家须在国内设立服务机构，提供每周 7×24 小时技术支持和服务，针对使用过程中出现的故障问题，可以通过电话、网络方式先提供服务，2 小时内作出实质性响应，对重大问题提供现场技术支持，如果解决不了的情况下需要及时赶赴现场提供服务，8 小时内到达指定现场。

3）软硬件免费保修期，自验收合格之日起算。

4）保修期内非采购方人为因素而出现的质量问题，生产厂家负责保修、包

换或者包退，并承担修理、调换或退货的实际费用。

5）投标人承诺提供的每一台设备均是全新的，厂家提供终身有偿维修、保养服务，保修范围外有偿维修，只收成本费。

6）投标人或生产厂家须对招标方使用人员及设备维修人员进行培训，使用

人员能够熟练掌握设备的各项功能和操作，使维修人员能对设备进行日常维护和一般性故障的查找及故障的排除。提供安装调试完成后，网络安全与密码教学实训平台至少提供1天本地操作培训。