附件1：

招 标 文 件

项目编号：ZC-AZB16151

项目名称：北京电子科技学院教务教学服务一体化采购项目

中共中央直属机关采购中心

2016 年 7 月

**目 录**

第一章 专用部分 1

第一部分 投标邀请 2

第二部分 招标基本信息 5

第三部分 投标内容及格式要求 6

第四部分 符合性审查项及评分标准 47

第五部分 技术规格及要求 54

第二章 通用部分 55

第一部分 投标人须知 56

第二部分 合同条款及格式 66

**第一章 专用部分**

**第一部分 投标邀请**

中共中央直属机关采购中心受北京电子科技学院委托，就北京电子科技学院教务教学服务一体化采购项目(项目编号：ZC-AZB16151)进行国内公开招标。现邀请合格的投标人提交符合招标文件要求的投标文件。

1. **项目概述**
   1. 招标内容：本项目所采购设备用于北京电子科技学院教务教学服务一体化。采购标的、数量以及技术要求等详见招标文件技术要求部分。
   2. 采购预算：01包预算为：270万元,02包预算为：70万元,超过预算的投标将作为无效投标处理。
   3. 本项目分2包。

01包：电子取证实验及对抗靶场实验室建设

本包为非专门面向中小企业采购。

02包：虚拟化安全管控研究生实验平台建设

本包为非专门面向中小企业采购。

* 1. 本项目不接受进口产品的投标，进口产品是指“通过中国海关报关验放进入中国境内且产自关境外的产品”。
  2. 本项目不涉及节能强采产品。

1. **投标人必须符合的条件**

投标人应具备《中华人民共和国政府采购法》第二十二条规定的条件，且符合、承认并承诺履行招标文件各项规定的国内法人和其他组织（不包括在港澳台地区注册成立的法人和其它组织）。

同时还应具有以下特定条件的：

　　1、本项目不接受联合体投标。

　　2、单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

1. **获取招标文件的时间和办法**

2016年07月28日至2016年08月14日，登录“中国政府采购网中直采购频道”（zzcg.ccgp.gov.cn）免费下载招标文件。**未通过中直采购频道下载招标文件的投标人，其递交的投标文件将被作为无效投标处理。联合体投标的应当由联合体代表下载招标文件。**

1. **投标文件递交时间、地点**

投标文件递交时间：2016年08月14日至2016年08月18日（北京时间）

投标文件递交地点：中新大厦（北京市西城区新风街一号院甲6号楼）一层电子投标文件递交室

投标截止时间：2016年08月18日09时00分（北京时间），截至此时间未完成递交的投标文件予以退回，此后递交的投标文件不予接收。

1. **开标时间、地点**

开标时间：2016年08月18日09时00分（北京时间）

开标地点：中新大厦（北京市西城区新风街1号院甲6号楼）开标室

**特别提醒：**本项目采用电子化招投标。中直机关集中采购电子化平台集成北京数字认证股份有限公司数字证书系统，投标人须使用该公司发放的数字认证证书对投标文件进行签封、加密、递交及开标时解密等相关招投标事宜，具体要求和操作程序详见招标文件投标人须知部分。申请办理数字认证证书的方式详见：<http://help.bjca.org.cn/support/client/zzcg-ccgp/index.htm>。

投标人下载电子招标文件同时须在“中国政府采购网中直采购频道”的“资料下载”栏目中，免费下载“全流程电子化投标客户端”，并使用该客户端制作电子投标文件，制作完成后，导出扩展名为“.file”的电子投标文件；

投标人请于投标文件递交时间内的每天8：00至 17：00，或开标当天8：00至投标截止时间，携带存储在光盘内的电子投标文件到投标文件递交地点，通过终端使用**用户名和密码**登陆电子化平台后，使用**数字认证证书**将电子投标文件上传至电子化平台。因电子文件递交需要一定的时间，请供应商安排充足时间递交文件。

除上述方式之外，招标方不接受投标人以纸质文件以及其他任何方式（包括但不限于：邮寄、传真、电子邮件等）提交的投标文件。

1. **联系方式**

**采购人：**北京电子科技学院

联系方式：83635430

地 址：北京市丰台区富丰路7号

**采购中心：**

项目联系人：薛宗伟

电　　话：010-82273286

系统技术支持电话：010-82273275 010-82273269

地 址：北京市西城区新风街1号院甲6号楼

邮政编码：100088

**第二部分 招标基本信息**

* + 1. 项目编号：ZC-AZB16151
    2. 项目名称：北京电子科技学院教务教学服务一体化采购项目
    3. 采购人：北京电子科技学院
    4. 报价要求：01包预算为：270万元,02包预算为：70万元,超过预算的投标将作为无效投标处理。

投标报价应包含系统集成、制造货物、运输、保险、安装、调试、备品备件、培训、保修、包装、验收费用及其它相关费用。

* + 1. 资金来源：财政性资金
    2. 交货要求：交货时间及交货地点：签订合同后30天内，采购人指定地点：北京市丰台区富丰路7号。
    3. 投标有效期：开标之日起90个日历日。如果中标，有效期自动延长至合同履行完毕。
    4. 投标保证金要求：

本项目不收取投标保证金。

* + 1. 评标委员会组成：

评标委员会成员共7名，其中有关技术、经济等方面的专家5名，采购人代表2名。

* + 1. 评分办法：本项目采用综合评分法。

**第三部分 投标内容及格式要求**

一、投标声明函

包号：01 包名称：电子取证实验及对抗靶场实验室建设

**致：中共中央直属机关采购中心：**

* 1. 我方承诺，我方完全具备《政府采购法》第二十二条第一款规定的条件以及本项目招标文件规定的投标人须满足的特定条件。
  2. 我方承诺按照本项目招标文件和相关技术标准的条件，提供货物及相关服务，并承担因货物质量或服务等引起的一切责任。
  3. 我方对该项目招标文件（包括修改文件及有关附件）完全理解，并承诺在发生争议时，不会以对招标文件存在误解、不明为由，向贵中心行使任何法律上的抗辩权。
  4. 我方投标文件有效期为自开标日起 个日历日，若中标，则投标有效期自动延续至合同履行完毕。
  5. 我方承诺接受招标文件规定的付款方式。
  6. 我方投标文件和你方的中标通知书、招标文件将成为约束双方的合同文件组成部分，若招标文件存在要求，而本投标文件没有拒绝亦没有涉及的情形下，我方接受招标文件的有关约束，并同意将招标文件对投标人的要求作为投标人合同义务的组成部分。
  7. 我方承诺投标文件中所有的资料及所作各项承诺均真实准确，所提交的营业执照副本复印件已依法履行相应的年度报告登记公示手续（或所提交的《事业单位法人证书》副本复印件/《社会团体法人登记证书》复印件/《民办非企业单位登记证书》复印件已经国家主管部门年检），不存在任何虚假之处，否则，评标委员会可将我方的投标文件按照无效投标文件处理，即使我方中标，中标结果无效，对于因此给其他投标人及你方和采购人造成的全部损失，我方同意无条件予以赔偿。
  8. 我方委托授权 (身份证号: ，联系电话： )作为我方的代理人参加本项目投标，负责提交投标文件以及其它相关资料，参加开标，接受质询并予以澄清，签署、接受招投标过程中的各种法律文件，办理投标过程中的其他相关事务。
  9. 我方将严格遵守《中华人民共和国政府采购法》，若存在违法违规行为，将承担相应的法律后果。

法定代表人签字或盖章：

数字认证证书电子签章：

日期：

**特别提醒：为确保电子投标文件的合法性、安全性和完整性，本《投标声明函》 填写完成后须先进行打印，经法定代表人或盖章签字后扫描上传并加盖数字认证证书电子签章。电子签章后，文档不应再修改，否则签章无效；如需修改，请修改后重新签章。**

二、开标一览表

包号：01 包名称：电子取证实验及对抗靶场实验室建设

报价合计（大写）:

报价合计: 元

注：

1、所报价格须用人民币元表示。

2、报价合计应与《分项报价表》中“合计”一致。如因不一致而产生的不利后果，均由投标人自行承担。

三、分项报价表

包号：01 包名称：电子取证实验及对抗靶场实验室建设

**第一包分项报价表**

项目编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名 称** | **数量** | **所投产品品牌及型号** | **单价** | **小计** |
| 1 | 网络攻防对抗平台硬件设备 | 19 |  |  |  |
| 2 | 计算机取证平台硬件设备 | 11 |  |  |  |
| 3 | 网络对抗平台管理控系统 | 1 |  |  |  |
| 4 | 网络对抗平台云调度系统 | 1 |  |  |  |
| 5 | 对抗平台视频直播系统 | 1 |  |  |  |
| 6 | 网络攻防对抗检测软件 | 1 |  |  |  |
| 7 | 单兵过关云资源靶场系统 | 8 |  |  |  |
| 8 | 红蓝对抗云资源靶场系统 | 8 |  |  |  |
| 9 | WEB后门代码检测系统 | 2 |  |  |  |
| 10 | 远程安全监控系统 | 2 |  |  |  |
| 11 | 攻防态势监控终端 | 2 |  |  |  |
| 12 | 对抗平台教师管理系统 | 1 |  |  |  |
| 13 | 单兵过关竞赛系统（80并发） | 1 |  |  |  |
| 14 | 红蓝对抗竞赛系统（20队并发） | 1 |  |  |  |
| 15 | 无线攻防渗透测试实训系统 | 1 |  |  |  |
| 16 | 渗透测试工具包 | 1 |  |  |  |
| 17 | 计算机取证系统管理系统 | 1 |  |  |  |
| 18 | 计算机取证系统取证资源系统 | 10 |  |  |  |
| 19 | 计算机取证系统信息管理系统 | 1 |  |  |  |
| 20 | 计算机取证系统学生实验系统 | 1 |  |  |  |
| 21 | 计算机取证课程资源包 | 1 |  |  |  |
| 22 | 移动终端 | 10 |  |  |  |
| 23 | 路由器 | 1 |  |  |  |
| 24 | 核心交换机 | 1 |  |  |  |
| 25 | 管理中心交换机 | 5 |  |  |  |
| 26 | 机柜 | 4 |  |  |  |
| 27 | 信息安全系统设计实验箱 | 40 |  |  |  |
| 28 | 竞赛支持设备 | 1 |  |  |  |
| 合计 | |  | | | |

注：

1. 所报价格系用人民币元表示，保留整数。
2. 合计价格与《开标一览表》中“报价合计”必须一致。

其他相关费用应包括根据合同或其它原因应由投标人支付的税款和应由投标人负担的相关费用。

四、非进口产品

包号：01 包名称：电子取证实验及对抗靶场实验室建设

非进口产品声明函

我方承诺就 （项目名称、编号） 所投 产品为非进口产品，我方保证上述内容的真实性，并承担由此引起的一切责任。

特此声明。

企业名称（盖章）：

日　期：

五、营业执照

包号：01 包名称：电子取证实验及对抗靶场实验室建设

经国家主管部门年检或依法履行年度报告登记公示手续，且在有效期内的营业执照副本原件扫描件/《事业单位法人证书》副本原件扫描件/《社会团体法人登记证书》原件扫描件/《民办非企业单位登记证书》原件扫描件。

六、没有重大违法记录的声明

包号：01 包名称：电子取证实验及对抗靶场实验室建设

没有重大违法记录的声明（参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明）

七、财务状况报告

包号：01 包名称：电子取证实验及对抗靶场实验室建设

财务状况报告：投标人为法人的，须提供经审计的上年度财务状况报告或基本账户的银行资信证明；其他组织和自然人，可以提供银行资信证明。投标人也可以提供财政部门认可的政府采购专业担保机构出具的投标担保函。

八、依法缴纳税收和社会保障资金的相关材料

包号：01 包名称：电子取证实验及对抗靶场实验室建设

依法缴纳税收和社会保障资金的相关材料：投标人依法缴纳近半年内任意一个月税收的相关凭证；投标人依法缴纳近半年内任意一个月社会保险的相关凭证。

九、制造厂商出具的售后服务承诺函

包号：01 包名称：电子取证实验及对抗靶场实验室建设

投标人在投标时需提供单兵过关云资源靶场系统、单兵过关竞赛系统、红蓝对抗竞赛系统、WEB后门代码检测系统、计算机取证系统管理系统、无线攻防渗透测试实训系统、信息安全系统设计实验箱“制造厂商出具的售后服务承诺函”，加盖制造厂商公章。

十、制造厂商出具的开放源代码承诺函

包号：01 包名称：电子取证实验及对抗靶场实验室建设

投标人在投标时需提供单兵过关云资源靶场系统、单兵过关竞赛系统、红蓝对抗竞赛系统、WEB后门代码检测系统、计算机取证系统管理系统、无线攻防渗透测试实训系统、信息安全系统设计实验箱“制造厂商出具的开放源代码承诺函”。

## 制造厂商出具的开放源代码承诺函

致：

我们是按法律成立的一家制造商，主要营业地点设在。

我方就本次投标有关事项郑重承诺如下：

1. 由我方制造的单兵过关云资源靶场系统、单兵过关竞赛系统、红蓝对抗竞赛系统、WEB后门代码检测系统、计算机取证系统管理系统、无线攻防渗透测试实训系统、信息安全系统设计实验箱无偿开放源代码，满足师生对实验和研究的需要，源代码提供的功能不低于实际产品提供的功能和配套实验项目。
2. 我方提供的产品源代码属于我方的商业机密，采购人对我方负有保密责任；采购人获得的源代码仅限于教学、实验和研究，不得再编译后进行商业化销售，不得以任何形式、任何理由泄露给第三方。
3. 若我方授权的代理商中标，我方将在3日内提供产品源代码至采购人指定地点，现场进行源代码编译及真实性认证。认证通过后签订合同，如我方未能提供产品源代码或认证不通过，自愿放弃签订合同并承担相应责任。
4. 本公司对上述承诺的真实性负责。如有虚假，将依法承担相应责任。

制造厂商名称（公章）：

法定代表人或授权代理人（签字）

日期：年月日

十一、应用案例

包号：01 包名称：电子取证实验及对抗靶场实验室建设

投标人2013年至今做过信息安全或网络攻防实验室项目100万以上项目的成功案例（须提供合同首页、合同金额和签字所在页原件扫描件）。

十二、所投产品的节能环保性

包号：01 包名称：电子取证实验及对抗靶场实验室建设

提供所投产品在最新一期《节能产品政府采购清单》（第十九期）及《环境标志产品政府采购清单》（第十七期）所在页的复印件

十三、投标人ISO9001认证证书

包号：01 包名称：电子取证实验及对抗靶场实验室建设

投标人ISO9001认证证书

十四、中小企业声明函

包号：01 包名称：电子取证实验及对抗靶场实验室建设

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号）的规定，本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。即，本公司同时满足以下条件：

　　1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）规定的划分标准，本公司为 （请填写：中型、小型、微型）企业。

　　2.本公司参加\_\_\_\_\_\_单位的\_\_\_\_\_\_项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他\_\_\_\_\_\_（请填写：中型、小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

　　本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

备注：投标人若不提供本声明函的，将不能享受政府采购扶持中小微型企业的政策。

监狱企业证明函

本公司郑重声明，根据《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）的规定，本公司为监狱企业。

省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）（盖章）：日 期：

备注：投标人若不提供监狱企业证明函的，将不能享受政府采购扶持监狱企业的政策。

十五、产品选型

包号：01 包名称：电子取证实验及对抗靶场实验室建设

货物主要技术指标和运行性能的详细说明（须对技术需求中的产品技术指标逐条进行应答，说明正负偏离情况）

十六、服务部分

包号：01 包名称：电子取证实验及对抗靶场实验室建设

服务及培训方案。

一、投标声明函

包号：02 包名称：虚拟化安全管控研究生实验平台建设

**致：中共中央直属机关采购中心：**

* 1. 我方承诺，我方完全具备《政府采购法》第二十二条第一款规定的条件以及本项目招标文件规定的投标人须满足的特定条件。
  2. 我方承诺按照本项目招标文件和相关技术标准的条件，提供货物及相关服务，并承担因货物质量或服务等引起的一切责任。
  3. 我方对该项目招标文件（包括修改文件及有关附件）完全理解，并承诺在发生争议时，不会以对招标文件存在误解、不明为由，向贵中心行使任何法律上的抗辩权。
  4. 我方投标文件有效期为自开标日起 个日历日，若中标，则投标有效期自动延续至合同履行完毕。
  5. 我方承诺接受招标文件规定的付款方式。
  6. 我方投标文件和你方的中标通知书、招标文件将成为约束双方的合同文件组成部分，若招标文件存在要求，而本投标文件没有拒绝亦没有涉及的情形下，我方接受招标文件的有关约束，并同意将招标文件对投标人的要求作为投标人合同义务的组成部分。
  7. 我方承诺投标文件中所有的资料及所作各项承诺均真实准确，所提交的营业执照副本复印件已依法履行相应的年度报告登记公示手续（或所提交的《事业单位法人证书》副本复印件/《社会团体法人登记证书》复印件/《民办非企业单位登记证书》复印件已经国家主管部门年检），不存在任何虚假之处，否则，评标委员会可将我方的投标文件按照无效投标文件处理，即使我方中标，中标结果无效，对于因此给其他投标人及你方和采购人造成的全部损失，我方同意无条件予以赔偿。
  8. 我方委托授权 (身份证号: ，联系电话： )作为我方的代理人参加本项目投标，负责提交投标文件以及其它相关资料，参加开标，接受质询并予以澄清，签署、接受招投标过程中的各种法律文件，办理投标过程中的其他相关事务。
  9. 我方将严格遵守《中华人民共和国政府采购法》，若存在违法违规行为，将承担相应的法律后果。

法定代表人签字或盖章：

数字认证证书电子签章：

日期：

**特别提醒：为确保电子投标文件的合法性、安全性和完整性，本《投标声明函》 填写完成后须先进行打印，经法定代表人或盖章签字后扫描上传并加盖数字认证证书电子签章。电子签章后，文档不应再修改，否则签章无效；如需修改，请修改后重新签章。**

二、开标一览表

包号：02 包名称：虚拟化安全管控研究生实验平台建设

报价合计（大写）:

报价合计: 元

注：

1、所报价格须用人民币元表示。

2、报价合计应与《分项报价表》中“合计”一致。如因不一致而产生的不利后果，均由投标人自行承担。

三、分项报价表

包号：02 包名称：虚拟化安全管控研究生实验平台建设

**第二包分项报价表**

项目编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名 称** | **数量** | **所投产品品牌及型号** | **单价** | **小计** |
| 1 | 安全访问网关服务器 | 1 |  |  |  |
| 2 | 云平台主管服务器 | 1 |  |  |  |
| 3 | 云桌面资源服务器 | 4 |  |  |  |
| 4 | 资源池宿主服务器 | 2 |  |  |  |
| 5 | 三层交换机 | 2 |  |  |  |
| 6 | 二层交换机 | 4 |  |  |  |
| 7 | 瘦客户机 | 30 |  |  |  |
| 8 | 云桌面系统 | 1 |  |  |  |
| 9 | 虚拟化终端安全管理系统 | 1 |  |  |  |
| 10 | 安全管理平台 | 1 |  |  |  |
| 合计 | |  | | | |

注：

1. 所报价格系用人民币元表示，保留整数。
2. 合计价格与《开标一览表》中“报价合计”必须一致。

其他相关费用应包括根据合同或其它原因应由投标人支付的税款和应由投标人负担的相关费用。

四、非进口产品

包号：02 包名称：虚拟化安全管控研究生实验平台建设

非进口产品声明函

我方承诺就 （项目名称、编号） 所投 产品为非进口产品，我方保证上述内容的真实性，并承担由此引起的一切责任。

特此声明。

企业名称（盖章）：

日　期：

五、营业执照

包号：02 包名称：虚拟化安全管控研究生实验平台建设

经国家主管部门年检或依法履行年度报告登记公示手续，且在有效期内的营业执照副本原件扫描件/《事业单位法人证书》副本原件扫描件/《社会团体法人登记证书》原件扫描件/《民办非企业单位登记证书》原件扫描件。

六、没有重大违法记录的声明

包号：02 包名称：虚拟化安全管控研究生实验平台建设

没有重大违法记录的声明（参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明）

七、财务状况报告

包号：02 包名称：虚拟化安全管控研究生实验平台建设

财务状况报告：投标人为法人的，须提供经审计的上年度财务状况报告或基本账户的银行资信证明；其他组织和自然人，可以提供银行资信证明。投标人也可以提供财政部门认可的政府采购专业担保机构出具的投标担保函。

八、依法缴纳税收和社会保障资金的相关材料

包号：02 包名称：虚拟化安全管控研究生实验平台建设

依法缴纳税收和社会保障资金的相关材料：投标人依法缴纳近半年内任意一个月税收的相关凭证；投标人依法缴纳近半年内任意一个月社会保险的相关凭证。

九、应用案例

包号：02 包名称：虚拟化安全管控研究生实验平台建设

投标人提供100万以上教育项目案例（须提供合同首页、合同金额和签字所在页原件扫描件）。

十、所投产品的节能环保性

包号：02 包名称：虚拟化安全管控研究生实验平台建设

提供所投产品在最新一期《节能产品政府采购清单》（第十九期）及《环境标志产品政府采购清单》（第十七期）所在页的复印件

十一、计算机系统集成资质

包号：02 包名称：虚拟化安全管控研究生实验平台建设

计算机信息系统集成或计算机信息系统集成及服务资质

十二、投标人ISO9001认证证书

包号：02 包名称：虚拟化安全管控研究生实验平台建设

投标人ISO9001认证证书

十三、中小企业声明函

包号：02 包名称：虚拟化安全管控研究生实验平台建设

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号）的规定，本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。即，本公司同时满足以下条件：

　　1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）规定的划分标准，本公司为 （请填写：中型、小型、微型）企业。

　　2.本公司参加\_\_\_\_\_\_单位的\_\_\_\_\_\_项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他\_\_\_\_\_\_（请填写：中型、小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

　　本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

备注：投标人若不提供本声明函的，将不能享受政府采购扶持中小微型企业的政策。

监狱企业证明函

本公司郑重声明，根据《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）的规定，本公司为监狱企业。

省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）（盖章）：日 期：

备注：投标人若不提供监狱企业证明函的，将不能享受政府采购扶持监狱企业的政策。

十四、技术指标满足情况

包号：02 包名称：虚拟化安全管控研究生实验平台建设

货物主要技术指标和运行性能的详细说明（须对技术需求中的产品技术指标逐条进行应答，说明正负偏离情况）

十五、软件接口总体框架说明文档及接口描述文档

包号：02 包名称：虚拟化安全管控研究生实验平台建设

软件接口总体框架说明文档及接口描述文档

十六、接口调用代码案例（代码案例要覆盖所有软件接口）

包号：02 包名称：虚拟化安全管控研究生实验平台建设

接口调用代码案例（代码案例要覆盖所有软件接口）

十七、虚拟化终端安全管理系统功能演示

包号：02 包名称：虚拟化安全管控研究生实验平台建设

虚拟化终端安全管理系统功能演示

十八、安全管理平台功能演示

包号：02 包名称：虚拟化安全管控研究生实验平台建设

安全管理平台功能演示

十九、服务部分

包号：02 包名称：虚拟化安全管控研究生实验平台建设

服务及培训方案。

**第四部分 符合性审查项及评分标准**

包号：01 包名称：电子取证实验及对抗靶场实验室建设

一、投标人须提供下列各项资料，且所提供的资料满足招标文件要求，有任意一项未提交或不满足的，经评标委员会半数以上成员一致同意，其投标将被按照无效投标处理，经评标委员会认定的无效投标文件不得进入详细评审：

1.投标声明函

2.开标一览表

3.分项报价表

4.非进口产品声明函

5.营业执照

6.没有重大违法记录的声明

7.财务状况报告

8.依法缴纳税收和社会保障资金的相关材料

9.制造厂商出具的售后服务承诺函

10.制造厂商出具的开放源代码承诺函

二、评分标准

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目 | 评审因素 | 分值 | 对应的投标格式 |
| 第一部分 商务部分 | 1.投标人应用案例 | 投标人2013年至今做过信息安全或网络攻防实验室项目100万以上项目的成功案例，每个得2分，最多6分。 | 0～6 | 应用案例 |
| 2.所投产品的节能环保性 | 所投产品为最新一期节能清单内的产品，每提供一款得0.5分；所投产品为最新一期环保清单内的产品，每提供一款得0.5分。最多1分。 | 0～1 | 所投产品的节能环保性 |
| 3.投标人ISO9001认证证书 | 投标人具有ISO9001资质得3分，否则0分。 | 0～3 | 投标人ISO9001认证证书 |
| 第二部分 产品选型 | 1.技术指标满足情况 | 1、满足招标文件要求的全部技术指标得45分；  2、标注★号条款为关键条款，负偏离的每项扣2分，直至减为0分。  3、其他指标性能每项不满足的减1分，直至减为0分。 | 0～45 | 产品选型 |
| 第三部分 服务部分 | 1.所承诺服务满足招标文件要求情况 | 满足服务及投标要求中“售后服务”要求得6分，否则 0分。 | 0～6 | 服务部分 |
| 2.质保期 | 在招标文件要求基础上，每增加一年加2分，最高4分。 | 0～4 |
| 3.培训方案 | 满足服务及投标要求中“培训服务”要求得5分，每项负偏离减2分，直至减为0分。 | 0～5 |
| 第四部分 报价分 | 1.价格 | （1）满足招标文件要求且投标价格最低的投标报价为评标基准价，其投标人的报价分为最高分30分；  （2）其他投标人的报价分按以下公式计算：  报价得分=(评标基准价／投标报价)×价格权值×100；  （3）小型、微型企业价格折扣率  作为非专门面向小型、微型企业的采购项目，其中小型、微型企业参与投标的，对其产品价格给予 6%（幅度为6%-10%） 的扣除，用扣除后的价格参与评审。  （4）监狱企业视同小型、微型企业。 | 0～30 |  |

包号：02 包名称：虚拟化安全管控研究生实验平台建设

一、投标人须提供下列各项资料，且所提供的资料满足招标文件要求，有任意一项未提交或不满足的，经评标委员会半数以上成员一致同意，其投标将被按照无效投标处理，经评标委员会认定的无效投标文件不得进入详细评审：

1.投标声明函

2.开标一览表

3.分项报价表

4.非进口产品声明函

5.营业执照

6.没有重大违法记录的声明

7.财务状况报告

8.依法缴纳税收和社会保障资金的相关材料

二、评分标准

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目 | 评审因素 | 分值 | 对应的投标格式 |
| 第一部分 商务部分 | 1.投标人应用案例 | 投标人提供100万以上教育项目案例。一份2分，最高得6分。 | 0～6 | 应用案例 |
| 2.所投产品的节能环保性 | 所投产品为最新一期节能清单内的产品，每提供一款得0.5分；所投产品为最新一期环保清单内的产品，每提供一款得0.5分。最多1分。 | 0～1 | 所投产品的节能环保性 |
| 3.计算机系统集成资质 | 三级及以上，提供得1分；否则0分。 | 0～1 | 计算机系统集成资质 |
| 4.投标人ISO9001认证证书 | 投标人提供ISO9001认证证书，得2分，否则0分。 | 0～2 | 投标人ISO9001认证证书 |
| 第二部分 产品选型 | 1.技术指标满足情况 | 1、满足招标文件要求的全部技术指标得40分。每有一项技术条款负偏离扣2分，直至减为0分。  2、标“★”的技术指标，每有一项负偏离扣6分，直至减为0分。 | 0～40 | 技术指标满足情况 |
| 2.软件接口总体框架说明文档及接口描述文档 | 提供得3分，不提供不得分。 | 0～3 | 软件接口总体框架说明文档及接口描述文档 |
| 3.接口调用代码案例（代码案例要覆盖所有软件接口） | 提供得3分，不提供不得分。 | 0～3 | 接口调用代码案例（代码案例要覆盖所有软件接口） |
| 4.虚拟化终端安全管理系统功能演示 | 1、“支持启发式文件分析技术，通过分析操作系统的特定关键文件，识别出于系统安全性相关的配置和组件，评估系统安全状态。”演示满足参数要求得2分，不满足不得分。  2、“支持无代理在线、离线虚拟机涉密信息检测功能”演示满足参数要求得2分，不满足不得分。  3、“支持无代理技术对虚拟机违规软件的检测。”演示满足参数要求得2分，不满足不得分。 | 0～6 | 虚拟化终端安全管理系统功能演示 |
| 5.安全管理平台功能演示 | “结合虚拟化终端的事件管理及预警。” 演示满足参数要求得2分，不满足不得分。 | 0～2 | 安全管理平台功能演示 |
| 第三部分 服务部分 | 1.所承诺服务满足招标文件要求情况 | 满足服务及投标要求中“售后服务”要求得3分，1项不满足扣1分，最低0分 | 0～3 | 服务部分 |
| 2.培训方案 | 满足服务及投标要求中“培训服务”要求得3分，每缺少1项减1分，直至减为0分。 | 0～3 |
| 第四部分 报价分 | 1.价格 | （1）满足招标文件要求且投标价格最低的投标报价为评标基准价，其投标人的报价分为最高分30分；  （2）其他投标人的报价分按以下公式计算：  报价得分=(评标基准价／投标报价)×价格权值×100；  （3）小型、微型企业价格折扣率  作为非专门面向小型、微型企业的采购项目，其中小型、微型企业参与投标的，对其产品价格给予 6%（幅度为6%-10%） 的扣除，用扣除后的价格参与评审。  （4）监狱企业视同小型、微型企业。 | 0～30 |  |

**第五部分 技术规格及要求**

详见附件：

技术需求.docx

**第二章 通用部分**

**第一部分 投标人须知**

* + - 1. 总则

1. **适用范围及编制依据**
   1. 本招标文件仅适用于本项目投标邀请中所叙述的招标项目。
   2. 本招标文件依据《中华人民共和国政府采购法》、《政府采购货物和服务招标投标管理办法》、《电子签名法》等有关法律法规及规定编制。
2. **定义**
   1. “采购中心”指中共中央直属机关采购中心，为本次招标的组织者。
   2. “采购人”指本项目的委托单位。
   3. “投标人”指按本文件规定领取招标文件并在采购中心登记备案的，且响应招标文件要求，向采购中心提交投标文件的供应商。
   4. “招标方”指采购人和采购中心。
   5. “货物”指本文件中所述所有货物及相关服务。
   6. “日”指日历日。
   7. “电子化平台”指在采购中心设置、运行的计算机信息系统，该系统在采购中心局域网用于接收投标人的电子投标文件、完成开标、评标等活动，在互联网用于供应商下载招标文件。
   8. “数字认证证书”指北京数字认证股份有限公司颁发的用于证明投标人身份的单位电子签名认证证书（非个人证书）。
   9. “投标客户端”指采购中心提供的用于投标人编制投标文件的软件，该软件在“中国政府采购网中直采购频道”的“资料下载”栏目中，由投标人自行免费下载。
3. **投标费用**

投标人应承担所有与本次投标有关的费用，不论投标的结果如何，招标方在任何情况下均无义务和责任承担这些费用。

## 招标文件说明

1. **招标文件的法律效力**

本招标文件阐明了投标人所需提供的货物及服务的范围和招标投标的程序，是本次招标活动具有法律效力的文件。投标人应认真阅读招标文件中所有的事项、格式条款和规范等要求，否则，出现的相关不利后果，由投标人自行承担相关风险。

1. **招标文件的澄清、修改**
   1. 在投标截止时间15日前，采购中心可以根据需要对招标文件进行澄清、修改。澄清文件作为招标文件的组成部分，与招标文件具有同等法律效力。
   2. 对招标文件进行澄清、修改的，将依法发布公告，并以短信、电子邮件或传真等形式通知所有已领取招标文件的投标人，投标人未填写手机联系方式、电子邮箱或相关信息不准确的，后果由投标人自行承担。
   3. 招标文件进行澄清、修改的，投标人须重新下载澄清、修改后的招标文件，并按照澄清、修改后的招标文件编制投标文件，投标人因未重新下载澄清、修改后的招标文件并编制投标文件，由此可能引起的投标文件递交失败、解密失败、内容缺失等相关后果由投标人自行承担。
   4. 当招标文件和澄清文件在同一内容的表述上不一致时，以最后发出的文件为准。

## 投标文件编写

1. **编制投标文件的工具和语言**
   1. 投标人应当通过自备的计算机使用投标客户端编制电子投标文件，投标人提交的电子投标文件以及相关资料均应当使用中文简体字。
   2. 安装和使用投标客户端需要具备的计算机软硬件环境：
      1. 硬件要求:

处理器：双核，1000 MHz以上主频

内存：1G B或以上

硬盘：40G以上

显示器分辨率：1024\*768或以上

USB接口：至少一个USB2.0接口

* + 1. 软件要求:

操作系统： Microsoft Windows XP简体中文版、Microsoft Windows 7简体中文版、Microsoft Windows 8简体中文版

文档编辑软件：32位 MicrosoftOffice 2003 或以上

浏览器要求：IE浏览器6.0及以上版本

1. **计量单位**

计量单位应当使用中华人民共和国法定计量单位，招标文件的技术要求中另有规定的除外。

1. **投标报价**
   1. 投标总价包括投标人为完成本项目所发生的一切费用，估算错误或漏项的风险由投标人自行承担。
   2. 投标人对每包只能有一个不可变更的报价。任何有选择的报价或包含价格调整要求的投标，将被作为无效投标处理。
   3. 最低报价不能作为中标的保证。
2. **投标货币**

投标人应以人民币填报投标报价，合同履行时采购人亦以人民币支付。

1. **投标有效期**
   1. 投标人投标有效期短于招标文件规定期限的，将被视为非响应投标而按照无效投标处理。
   2. 在特殊情况下，在原投标有效期期满之前，采购中心可以要求投标人延长投标有效期。这种要求与答复均应以书面形式进行。在此种情况下，投标人不得修改投标文件的其它内容。投标人不同意延长投标有效期的，将被按照无效投标处理。
2. **投标文件的式样和签署**
   1. 投标文件编制完成后应通过投标客户端使用数字认证证书加密和签章。没有加密的投标文件将被拒绝接收。
   2. 因投标文件字迹模糊或表达不清所引起的不利后果由投标人自行承担。

## 投标文件的递交

1. **投标文件的递交**
   1. 投标人应自行携带数字认证证书、加密后的电子投标文件，及招标文件要求的其他材料，按照投标邀请中的时间，到达投标地点，自行通过在投标地点设置的计算机终端登陆电子化平台，使用数字认证证书将经加密的电子投标文件通过移动存储介质（光盘）上传至电子化平台。上传成功后，电子化平台将予以记录并提供上传成功的回执。
   2. 截至投标截止时间，投标人未完成电子投标文件传输的，视为其撤回投标文件。
   3. 投标截止时间后电子化平台拒绝接收投标文件。
   4. 递交完成后至开标前，投标人不能对数字证书更新、续费，否则可能引起的投标文件解密失败等相关后果由投标人自行承担。
2. **投标截止时间的延长**

采购中心可以视采购具体情况，于投标截止时间3日前延长投标截止时间和开标时间，并将以书面形式通知所有领取招标文件的投标人和在中国政府采购网发布变更公告。

1. **投标文件的撤回、修改和补充**
   1. 投标人在投标截止时间前可通过电子化平台撤回其已成功递交的电子投标文件，电子化平台将予以记录并提供撤回回执。
   2. 如果在投标截止时间前需要对已经成功递交的电子投标文件进行修改、补充的，投标人应当使用自备的计算机和“投标客户端”重新制作并导出完整的电子投标文件，并按要求重新上传至电子化平台。
   3. 电子化平台以投标人最后上传成功的投标文件为准。

## 开标

1. **开标**
   1. 采购中心将在规定的时间和地点组织开标活动。开标活动由采购中心主持。
   2. 投标人应当委派投标代表参加开标活动，否则，由此产生的不利后果由投标人自行承担。
   3. 开标时，投标人委派的投标代表应当使用与制作投标文件时同一数字认证证书对投标文件进行解密。在场所有供应商解密完成后，采购中心工作人员将进行开封报价。
   4. 在开封报价之后，因投标人原因造成投标文件未解密的，视为撤销其投标文件；因投标人之外的原因造成投标文件未解密的，视为撤回其投标文件，投标人有权要求责任方赔偿因此遭受的直接损失。
   5. 开标时，部分投标人投标文件未解密的，开标可以继续进行。若解密成功的投标人不足三家，该项目或该包按废标处理。
   6. 解密失败应急措施: 为应对现场开标时非人为因素造成的解密电子投标文件失败的情况，请投标供应商将投标客户端系统导出的未签名加密电子版投标文件（.xbid格式电子文件）刻录于不可擦写的光盘上以作备用，此光盘上须有法人或授权代表手写签字，并密封于信封中，在开标当天文件递交截止时间前交予采购中心开标现场工作人员。若开标过程中，已加密电子投标文件解密失败，可现场由采购中心工作人员将光盘中的投标文件（.xbid格式电子文件）导入系统，继续开标。此解密失败应急措施仅适用于非供应商原因造成的解密失败情况。若供应商开标前没有提交密封于信封中的光盘，或光盘中刻录的数据有误，则解密失败时，视为供应商撤回投标文件。
   7. 开标过程中，如遇不可抗力或意外事件等情况，采购中心将暂时中断开标程序并依法处理后续事宜。

## 评标

1. **评标**
   1. 本评标办法仅适用于本项目评标。
   2. 评标原则和纪律：

（1）客观、公平、公正和诚实信用；

（2）依据法律和招标文件规定科学、合理评标，择优推荐中标候选人；

（3）独立评审，禁止任何有失公平、公正的串通行为；

（4）反不正当竞争；

（5）恪守保密义务，凡与审查、澄清、评价和比较投标的有关资料以及授标意见等，不得向投标人及与评标无关的其他人员泄露。

* 1. 本项目评标工作分为符合性与完整性评审、详细评审两个阶段。
  2. 符合性与完整性评审
     1. 评标委员会应当根据招标文件规定，对投标文件进行符合性、完整性评审。
     2. 评标委员会对投标文件中的明显错误，有权按以下原则处理：

（1）开标一览表内容与投标文件中分项报价表内容不一致的，以开标一览表为准，评标委员会有权要求投标人根据开标一览表对分项报价表进行澄清、说明或修正。对于拒不按要求修正的，将作为无效投标处理；

（2）如果用数字表示（小写）的金额和用文字表示（大写）的金额不一致，应以大写表示的金额为准；

（3）当投标单价与数量的乘积和投标总价不一致时，以单价为准，并修正总价。如单价金额小数点明显错位的，应以总价为准，修正单价；

（4）对明显且可以推知其原义的笔误，依据其原义进行修正；

* + 1. 投标的澄清

（1）评标委员会有权要求投标人对投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误等内容作必要的澄清、说明或者补正。该要求应当采用书面形式提出。

（2）投标人必须按照评标委员会通知的内容和时间做出书面答复，该答复应加盖投标人公章，并经法定代表人或投标人代表的签字确认，作为投标文件的组成部分。澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。投标人拒不按照要求对投标文件进行澄清、说明或者补正的，将作为无效投标处理。

* 1. 详细评审
     1. 评标委员会只对通过了符合性与完整性评审的投标文件进行详细评审。评标委员会按照评分标准进行评标计分。所有评委给每一投标人的评分的算术平均值为该投标人的最终得分。最终得分非整数的，保留至小数点后两位，小数点后第三位按照四舍五入的规则计算
     2. 评标委员会对投标人得分按照从高到低进行排序，得分相同的投标人，报价低者排名在前，得分相同且投标报价相同的，按技术指标优劣顺序排列。
  2. 推荐中标候选人和确定中标人
     1. 评标委员会向招标方出具书面评标报告，并推荐综合得分排名前三位的合格投标人作为中标候选人。
     2. 采购人根据评标委员会提出的书面评标报告，依据本文件及相关法律法规确定中标人。

## 合同授予

1. **定标**
   1. 采购人根据评标委员会出具的评审报告，确定综合评分排名第一的中标候选人为中标人。如果中标人放弃中标或出现中标无效的情形，采购人有权递补确定排名在其下一位的中标候选人为中标人，以此类推。
   2. 中标人如果放弃中标，招标方有权依照法律规定追究其相应的法律责任。
2. **中标通知书**
   1. 采购人确定中标人后，采购中心将向中标人发出中标通知书，并将中标结果依法公告。采购中心对投标人未中标的原因不予解释。
   2. 中标通知书是合同的组成部分。
3. **签订合同**
   1. 中标人应当在中标通知书发出之日起30日内与采购人签订合同，由于中标人自身原因未及时签订合同的，招标方可以视为中标人放弃中标，中标人应当承担相应法律后果。在此种情况下，采购人可以按中标候选人顺序将标授予下一个中标候选人。
   2. 招标文件、中标人的投标文件及其双方确认的澄清文件等，均为有法律约束力的合同组成部分。
   3. **招标文件所附《合同条款及格式》是采购人与中标人签订合同的基本条款，投标人应认真阅读，在没有实质性违反招标文件及投标文件的前提下，采购人有权在合同签订前对合同条款进行适当修改、增加、删除，中标人不得以此为由拒绝签订合同。对此，请投标人参加投标前慎重考虑相关商业风险**。

## 质疑与投诉

1. **投标人质疑**
   1. 按照《中华人民共和国政府采购法》及相关规定，若投标人认为采购文件、采购过程和中标结果使自己的合法权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购中心或采购人提出质疑。
   2. 质疑书应当包括以下主要内容：被质疑项目名称、项目编号、包号、中标公告发布时间、质疑事项、证据材料、法律依据（具体条款）、有效联系方式（包括手机、传真号码）等。
   3. 质疑书必须有法定代表人签字或盖章，并加盖投标人公章。若授权代表签章，必须附法定代表人针对当次质疑的特别授权，且公章不得以合同章或其他印章代替。
   4. 有下列情形之一的，属于无效质疑，采购中心可不予受理：
2. 未在法定期限内提出质疑的；
3. 质疑未以书面形式提出，或质疑书内容不符合本须知20.2条要求的；
4. 质疑书没有法定代表人本人签章，或未提供法定代表人签章的特别授权，或未加盖单位公章的；
5. 其它不符合受理条件的情形。
   1. 采购人或采购中心将在收到书面质疑后7个工作日内作出答复，并以书面形式通知质疑投标人和其他有关投标人，但答复的内容不涉及商业秘密。
6. **投标人投诉**

质疑投标人对采购人或采购中心的答复不满意以及采购人或采购中心未在规定的时间内做出答复的，可以在答复期满后15个工作日内向财政部投诉。

## 其他事项

1. **废标**

本项目出现《政府采购法》第三十六条规定的废标情形时，招标方有权宣布废标，招标方对受影响的投标人不承担任何责任，但因招标方出现影响采购公正的违法、违规行为引起的废标情形除外。如果项目分包，将以包为单位执行。

1. **履约保证金**

按照合同约定执行。

1. **履约监管**

**为保障国有资金的使用效益，促进中标供应商严格履约，采购中心将对本项目的履约情况进行跟踪督查。中标供应商在项目实施过程中，如存在供货进度、数量、质量、安全等违约情况，除采购人可依据采购合同追究其民事责任外，采购中心有权将中标供应商的违约情况报告财政部。**

1. **中标服务费**

本次招标不收取中标服务费，请投标人在报价时充分考虑这一因素。

1. **信用担保**

根据《财政部关于开展政府采购信用担保试点工作的通知》（财库[2011]124号），明确中国投资担保有限公司作为中央本级试点专业担保机构，投标人可以自愿选择是否采用该公司提供的投标担保、履约担保和融资担保服务。中国投资担保有限公司联系电话：010- 88822589 / 2656，地址：北京市海淀区西三环北路100号光耀东方写字楼19F，邮编：100048，网址：<http://www.guaranty.com.cn>。

1. **数字认证证书办理**

申请办理数字证书的方式详见：<http://help.bjca.org.cn/support/client/zzcg-ccgp/index.htm>。

1. **其他**

本部分未涉及的事项请参见招标文件其他部分。

**第二部分 合同条款及格式**

## 合同条款

1. **本合同对下列术语定义为：**
   1. “合同”系指甲乙双方签署的、合同格式中载明的甲乙双方所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。
   2. “合同价”系指根据本合同规定乙方在正确地完全履行合同义务后甲方应支付给乙方的价款。
   3. “货物”系指乙方根据合同规定须向甲方提供的由招标项目产生的所有成果。
   4. “服务”系指根据合同规定乙方承担与供货有关的辅助服务，如运输、保险以及其它的伴随服务，例如安装、调试、提供技术援助、培训和合同中规定乙方应承担的其它义务。
   5. “合同条款”系指本合同条款。
   6. “甲方”系指购买货物和服务的采购人。
   7. “乙方”系指提供货物和服务的中标人。
   8. “项目现场”系指本项目招标文件《招标基本信息》中指明的交货地点。
   9. “天”指日历天数。
2. **适用性**

本合同条款适用于没有被本合同其他组成部分所取代的范围。

1. **标准**
   1. 本合同下交付的货物应符合本项目招标文件《技术规格及要求》所述的标准。如果没有提及适用标准，则应符合中华人民共和国有关机构发布的最新版本的标准。
   2. 除非技术规格另有规定外，计量单位均采用中华人民共和国法定计量单位。
2. **使用合同文件和资料**
   1. 未经甲方事先书面同意，乙方不得将由甲方或甲方委托的第三方提供的有关合同或合同条文、规格、计划或其他书面资料以及其获悉的甲方国家秘密、商业秘密、内部工作信息（上述资料及信息以下合称保密信息）向与履行本合同无关的任何第三方披露、泄露或许可该第三方使用。如乙方因履行本合同需要向第三方披露上述保密信息，乙方应注意保密并将披露限于履行合同必须的范围，并保证该第三方亦履行上述保密义务。乙方上述保密义务不因本合同的终止而结束，直至上述保密信息非因乙方原因已为社会公众所知悉。
   2. 没有甲方事先同意，除了履行本合同外，乙方不应使用合同条款第4.1所列举的任何保密信息。
   3. 除了合同本身以外，合同条款第4.1条所列举的任何文件是甲方的财产。如果甲方有要求，乙方在完成合同后应将这些文件全部复制件还给甲方。
   4. 乙方未按照上述约定严格履行保密义务的，应当向甲方支付合同总价10%的违约金，于此情形下，甲方还有权提前解除合同。
3. **权利保护**

乙方保证，其向甲方销售货物的行为合法有效，甲方在中华人民共和国使用该货物或货物的任何一部分时，免受任何第三方提出侵犯其著作权、专利权、商标权、专有秘密等知识产权及其他权利的起诉。

1. **履约保证金**
   1. 乙方应按照本项目招标文件规定的期限和数额提交履约保证金。
   2. 履约保证金作为乙方履行本合同义务的保证，如乙方不能全面、适当地履行本合同义务，则甲方有权直接从履约保证金中扣除其所遭受的全部损失，或者根据本合同中关于违约责任的约定扣除乙方应当支付的全部违约金。
   3. 履约保证金应采用人民币，并采用下述方式之一提交：
2. 银行保函

由甲方可接受的在中华人民共和国境内注册和营业的银行总行或省、直辖市级分行出具，其格式采用招标文件提供的格式或其他甲方可接受的格式；

1. 银行汇票或支票；
2. 中国投资担保有限公司政府采购履约担保函。
   1. 如果乙方能按约全面履行合同义务，甲方将在质量保证期满后三十（30）天内退还乙方履约保证金（不计利息）。
3. **检验、测试与安装、调试和验收**
   1. 甲方或其代表应有权检验和/或测试货物，以确认货物是否符合合同规格的要求，并且不承担额外的费用。合同条款和技术规格将说明甲方要求进行的检验和测试，以及在何处进行这些检验和测试。甲方将及时以书面形式把进行检验和/或甲方测试代表的身份通知乙方。
   2. 检验和测试可以在乙方或制造厂的所在地、交货地点和/或货物的最终目的地进行。如果在乙方或制造厂的所在地进行，乙方应免费为甲方的检验人员提供工作条件，包括但不限于必要的技术资料、检测工具和仪器。
   3. 如果任何被检测或测试的货物不能满足规格的要求，甲方可以拒绝接受该货物，乙方应更换被拒绝的货物，或者免费进行必要的修改以满足规格的要求。乙方因更换货物导致延期交货的，应当承担延期交货的违约责任。
   4. 甲方在货物到达最终目的地后对货物进行检验、测试及必要时拒绝接受货物的权利将不会因为货物在从乙方或制造厂启运前通过了甲方或其代表的检验、测试和认可而受到限制或放弃。
   5. 在交货前，乙方或制造厂应对货物的质量、规格、性能、数量和重量等进行详细而全面的检验，并出具一份证明货物符合合同规定的检验证书，但该检验证书不能作为有关质量、规格、性能、数量或重量的最终检验。制造厂检验的结果和细节应附在质量检验证书后面。
   6. 依据合同条款第7条的约定进行检测验收后，并不证明该产品无任何质量瑕疵，且不因此免除乙方在本合同项下的保证义务或其他义务。
   7. 场地环境
4. 货物到达安装现场后，乙方按有关技术规程的规定负责存放和保管，如乙方有特殊要求，应向甲方及早提出。
5. 对于所有货物，乙方的货物安装工程师在到现场安装之前，应针对货物安装前对安装现场的具体要求与甲方进行协商确定。
   1. 安装调试
6. 乙方应按照甲方的工期要求，负责在货物到达交货地点后，在甲方规定的期限内和指定的现场将货物安装、调试、试运行完毕。
7. 乙方应提供全部安装、调试过程中所需的特殊工具和易损件，并自带专用仪器仪表。乙方还应提供与安装工程有关的所有材料、设备和人工。
8. 乙方应在现场对设备进行调试和试运行，以检验其设计制作质量、操作可靠性和功能完备性等的情况。试运行应在甲方工程师的监督下进行。
   1. 最终验收
9. 乙方将货物安装、调试完毕后应立即书面通知甲方进行最终验收，甲方将在接到中标人书面通知起10个工作日内进行最终验收，如果货物性能测试结果能满足合同、招标文件以及国家有关规定的要求，则认为本合同中签署的全部货物的性能测试是成功的。
10. 如果性能测试不合格，乙方工程师应以书面形式向甲方说明失败的原因，排除故障后重新测试。如测试次数超过3次或合同规定的期限，甲方有权拒绝验收，并按乙方违约处理。甲方除有权没收乙方的履约保证金外，还有权追索因乙方造成工期延误而给甲方造成的经济损失。
11. **包装要求**

乙方应提供货物运至合同规定的最终目的地所需要的包装，以防止货物在运转中损坏或变质。这类包装应采取防潮、防晒、防锈、防腐蚀、防震动及防止其它损坏的必要保护措施，从而保护货物能够经受多次搬运、装卸及长途运输。乙方应承担由于其包装或其防护措施不妥而引起的货物锈蚀、损坏和丢失的任何损失的责任和费用。

1. **装运标记**
   1. 乙方应在每一包装箱的相邻四面用不可擦除的油漆和明显的中文字样做出以下标记：
2. 收货人
3. 合同号
4. 发货标记
5. 收货人编号
6. 目的地
7. 货物名称、品目号和箱号
8. 毛重／净重（用公斤表示）
9. 尺寸（以长×宽×高用厘米表示）
   1. 如果单件包装箱重量在2吨（t）或2吨（t）以上，乙方应在包装箱的两侧用中文和适当的运输标记标注“重心”和“吊装点”，以便装卸和搬运。根据货物的特点和运输的不同要求，乙方应在包装箱上清楚地标注“小心轻放”、“此端朝上，请勿倒置”、“保持干燥”等字样和其他适当的标志。
10. **运输和保险**
    1. 乙方负责办理将货物运抵招标文件规定的交货地点，包括合同规定的保险和储存在内的一切事项，有关费用应包括在合同总价中，并且，乙方应承担货物在途期间以及装卸过程中可能发生的毁损、灭失的法律风险。
    2. 乙方负责办理货物在运抵过程中的全程保险，并以货物发票金额的百分之一百一十（110%）为货物办理“一切险”。
11. **伴随服务** 
    1. 甲方有权要求乙方提供下列服务中的任一或所有服务，包括本招标文件规定的附加服务（如果有的话）：
12. 实施或监督所供货物的安装和/或试运行；
13. 提供货物安装和/或维修所需的工具；
14. 为所供货物的每一适当的单台设备提供详细的操作和维护手册；
15. 在双方商定的一定期限内对所供货物实施运行或监督或维护或修理，但前提条件是该服务并不能免除乙方在合同保证期内所承担的义务；
16. 在乙方或制造厂和/或在项目现场就所供货物的安装、试运行、运行、维护和/或修理对甲方人员进行培训。
    1. 乙方应提供本项目招标文件中规定的所有服务。为履行要求的伴随服务的报价或双方商定的费用已经包括在合同价中。
17. **备品备件**
    1. 乙方应按照本项目招标文件、投标文件中的规定提供所需的备品备件。
    2. 在备品备件停止生产的情况下，乙方应事先将要停止生产的计划通知甲方，使甲方有足够的时间采购所需的备品备件；
    3. 在备品备件停止生产后，如果甲方要求，乙方应免费向甲方提供备品备件的蓝图、图纸和规格。
18. **保证**
    1. 乙方应保证合同项下所供货物是全新的、未使用过的。乙方进一步保证，合同项下提供的全部货物没有设计、材料或工艺上的缺陷，或者没有因乙方的行为或疏忽而产生的缺陷。如乙方提供的货物存在技术缺陷或事故隐患造成甲方或任何第三方人身、财产损害的，乙方应当对该损害承担全部法律责任。如由于乙方的违约行为造成甲方损失的，乙方还应当赔偿甲方的全部损失。
    2. 本保证应持续有效。质量保证期及免费维修保养服务期限按本项目招标文件、投标文件规定执行**。**
    3. 甲方应尽快以书面形式通知乙方保证期内所发现的质量问题。
    4. 乙方在收到甲方通知后应在本项目招标文件、投标文件规定的时限内将出现质量问题的货物免费维修或更换完毕。
    5. 如果乙方未在本项目招标文件、投标文件规定的时限内将出现质量问题的货物免费维修或更换完毕，视为乙方恶意违约，在此种情况下，甲方可采取必要的补救措施，但其风险和费用将由乙方承担，甲方凭维修通知及维修单位出具的发票即可向乙方索赔而无需提供该项维修责任形成原因的证据。甲方根据合同规定对乙方行使的其他权力不受影响。
19. **索赔**
    1. 如果本合同项下的货物不符合约定的标准及/或乙方保证的，甲方有权在合同条款第13条或合同的其他条款规定的检验、安装、调试和质量保证期内提出索赔要求，乙方应按照甲方同意的下列一种或几种方式结合起来解决索赔事宜：
20. 如甲方决定退货，则乙方应将其向甲方收取的全部价款退还甲方，并承担甲方由此发生的一切损失和费用，包括利息、银行手续费、运费、保险费、检验费、仓储费、装卸费以及为看管和保护退回货物所需的其它必要费用；
21. 根据货物的偏差情况、损坏程度以及甲方所遭受损失的金额，降低货物的价格；
22. 用符合合同规定的规格、质量和性能要求的新零件、部件和／或设备来更换有缺陷的部分和／或修补缺陷部分，乙方应承担一切费用和风险并负担甲方蒙受的全部直接损失费用。同时，乙方应按合同条款第13条规定，相应延长修补和／或更换件的质量保证期。
    1. 如果在甲方发出索赔通知后10天内，乙方未作答复，上述索赔应视为已被乙方接受。如乙方未能在甲方发出索赔通知限定的期限内或甲方同意的延长期限内，按照甲方同意的上述规定的任何一种方法解决索赔事宜，甲方将从应付货款或从乙方开具的履约保证金中扣回索赔金额。
23. **付款**
    1. 本合同以人民币付款。
    2. 乙方应按照双方签订的合同规定交货。交货后乙方应把下列单据提交给甲方，甲方按合同规定审核后付款：
24. 发票；
25. 全部工程技术资料；
26. 制造厂家出具的质量检验证书和数量证明书；
27. 由买卖双方签字的验收证书。
    1. 甲方付款方式和条件：

甲方将按照本项目招标文件规定的时间和方式向乙方支付合同价款。

1. **价格**

乙方在本合同项下提交货物和履行服务的价格在合同中给出。

1. **合同修改**

本合同履行过程中，甲方需追加与合同标的相同的货物或服务的，在不改变合同其他条款的前提下，可以与乙方协商签订补充合同，但所有补充合同的采购金额不超过原合同采购金额的百分之十。甲乙双方均不得擅自变更合同，但是如果合同继续履行将损害国家利益和社会公共利益的，双方应当变更合同，有过错的一方应当承担赔偿责任，双方都有过错的，各自承担相应的责任。

1. **转让和分包**
   1. 乙方不得部分转让或全部转让其享有的合同权利及应履行的合同义务。
   2. 未经甲方书面同意，乙方不得将本合同项下应由乙方履行的义务和工作分包给第三方完成。甲方同意分包的，乙方仍应当就分包项目向甲方负责，接受分包的第三方就分包项目承担连带责任。
   3. 乙方违反合同约定转让合同权利、义务或者分包的，乙方应当向甲方支付合同总价30%的违约金，并且，于此情形下甲方有权决定提前解除合同。
2. **乙方履约延误**
   1. 乙方应按照招标文件中规定的交货时间交货和提供服务。
   2. 在履行合同过程中，如果乙方及其分包人遇到妨碍按时交货和提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的时间和原因通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延长交货时间以及是否收取延期交付违约金。
3. **延期交付违约金**

除遇到合同规定的不可抗力情况外，如果乙方没有按照合同的时间交货和提供服务，甲方应在不影响合同项下的其他补救措施的情况下，有权从合同款项中扣除乙方应当支付的违约金。每延误一天的，乙方应当按迟交货物或服务的费用的百分之零点零肆(0.04％)向甲方支付违约金，直至实际交付为止。延期交付超过 30日时，甲方有权根据合同条款第21条的规定解除合同，甲方因此解除合同的，乙方应当支付合同价格 30 % 的违约金作为赔偿。

1. **违约解除合同**
   1. 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可向乙方发出书面违约通知书，提出解除合同。
2. 乙方延期交付达到约定的合同解除情形。
3. 如果乙方未能履行合同规定的其它任何义务达到合同约定的甲方有权解除合同的情形或者因此导致合同目的无法实现的。
4. 如果甲方认为乙方在本合同的竞争和实施过程中有腐败和欺诈行为。为此目的，定义下述条件：
   1. “腐败行为”是指提供、给予、接受或索取任何有价值的物品来影响相关人员在采购过程或合同实施过程中的行为。
   2. “欺诈行为”是指为了影响采购过程或合同实施过程而恶意隐瞒或谎报事实，损害甲方利益的行为。
5. **不可抗力**
   1. 签约双方任何一方由于不可抗力事件的影响而不能执行合同时，履行合同的期限应予以延长，其延长的期限应相当于事件所影响的时间。不可抗力事件系指买卖双方在缔结合同时所不能预见的，并且它的发生及其后果是无法克服的事件，诸如战争、严重火灾、洪水、台风、地震等。
   2. 受影响的一方在不可抗力事件发生后尽快用书面形式通知对方，并于不可抗力事件发生后十四（14）天内将有关当局出具的证明文件用特快专递或挂号信寄给对方审阅确认。一旦不可抗力事件影响持续超过一百二十（120）天以上，双方应通过友好协商在合理的时间内达成进一步履行合同的协议。
   3. 因合同一方迟延履行合同后发生不可抗力的，不能免除迟延履行方的相应责任。
6. **因破产解除合同**

如果乙方破产或无清偿能力，甲方可在任何时候以书面形式通知乙方，提出解除合同，甲方有权将已收货物退还乙方，合同解除前如果乙方只提供了部分货物且该部分货物可以满足甲方采购货物最终要实现的目的的，甲方仅就该部分货物支付相应的货物，并有权不支付乙方未履行合同义务部分相对应的合同价款。该合同将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权利。

1. **争议的解决**
   1. 因执行本合同所发生的或与本合同有关的一切争议，双方应通过友好协商解决。如果协商不能解决，双方确定通过向本合同签订地有关人民法院提起诉讼方式解决争议。
2. **合同语言**

本合同语言为简体中文。双方交换的与合同有关的信函均用简体中文书写。

1. **适用法律**

本合同应按照中华人民共和国的现行法律进行解释。

1. **通知**
   1. 本合同一方给对方的通知应用书面形式送到合同中规定的对方的地址。
   2. 通知以送到日期或通知书的落款日期为生效日期，两者中以晚的一个日期为准。
2. **税款**

本合同项下乙方所提供的货物和服务的所有税费均已包含于合同价格，甲方不再另行支付。按照中华人民共和国税法和有关部门的规定，乙方需交纳的与本合同有关的一切税费均应由乙方负担。

1. **合同生效及其他**

本合同以双方法定代表人或授权代表签字、加盖双方单位印章并且甲方收到乙方提交的履约保证金后生效。

## 合同格式

（以下简称“甲方” ）为一方和 （以下简称“乙方” ）为一方同意按下述条款和条件签署本合同（以下简称“合同” ）：

1. **合同文件**

本合同所附下列文件是构成本合同不可分割的部分：

1. 合同条款及附表
2. 投标人提交的投标声明函和报价表
3. 技术规格（包括图纸，如果有的话）
4. 澄清函及有关文件
5. 中标通知书
6. 招标文件
7. 投标文件
8. **合同范围和条件**

本合同的范围和条件应与上述合同文件的规定相一致。

1. **货物及数量**

本合同所提供的货物及数量详见招标文件和投标文件。

1. **合同金额**

根据上述合同文件要求，合同的总金额为 元人民币，分项价格在报价表中有明确规定。

1. **付款条件**

本合同货物的付款条件在合同条款中有明确规定。

1. **交货时间和交货地点**

本合同货物的交付时间和交货地点在本项目招标文件中有明确规定。

1. **合同生效**

本合同经双方法定代表人或授权代表签字、加盖双方单位印章并且甲方收到乙方提交的履约保证金后生效。

1. **其它**

本合同一式 份，其中甲方 份，乙方 份，采购中心**一**份。本合同签订于 。

**甲方名称（盖章） 乙方名称（盖章）**

**甲方代表签字： 乙方代表签字：**

签订地点： 签订日期： 年 月 日

履约保证金保函（样式）

开具日期：

**致：（甲方名称）**

号合同履约保函

本保函作为贵方与（乙方名称）（以下简称乙方）于 年 月 日就 项目（以下简称项目）项下提供（货物名称）（以下简称货物）签订的 （合同号）号合同的履约保函。

（出具保函银行名称）（以下简称银行）无条件地、不可撤消地具结保证本行、其继承人和受让人无追索地向贵方以人民币支付总额不超过（货币数量），即相当于合同价格的 %，并以此约定如下：

1. 只要贵方确定乙方未能忠实地履行所有合同文件的规定和双方此后一致同意的修改、补充和变动，包括更换和/或修补贵方认为有缺陷的货物（以下简称违约），无论乙方有任何反对，本行将凭贵方关于乙方违约说明的书面通知，立即按贵方提出的累计总额不超过上述金额的款项和按贵方通知规定的方式、时间付给贵方，本行放弃行使抗辩权。
2. 本保函项下的任何支付应为免税和净值。对于现有或将有的税收、关税、收费、费用扣减或预提税款，不论这些款项是何种性质和由谁征收，都不应从本保函项下的支付中扣除。
3. 本保函的条款构成本行无条件的、不可撤销的直接责任。对即将履行的合同条款的任何变更、贵方在时间上的宽限、或由贵方采取的如果没有本款可能免除本行责任的任何其它行为，均不能解除或免除本行在本保函项下的责任。
4. 本保函在贵方与乙方签订的合同全部履行完毕前（含质量保证期）完全有效。

谨启

出具保函银行名称

签字人姓名和职务

签 字 人 签 名

公 章

1. **总体要求**
2. 本部分内容是根据本项目实际情况制定的。
3. 投标人必须仔细阅读本部分的全部条款。对本部分中存在的任何疑问、遗漏或相互矛盾之处，或是对于相关要求不清楚，认为存在歧视、限制的情况，投标人可以向采购中心寻求书面澄清。
4. 本部分所列明的工艺、材料和设备的标准以及参照的品牌或分类号仅起说明作用，并没有任何限制性，投标人在投标中可以选用替代标准，品牌或分类号，但这些替代应当等于或优于文件技术要求。
5. 付款方式
   * 1. 甲方于合同签订后15 个工作日内，向乙方支付50%合同款。
     2. 到货后，主要设备安装调试完成后，向乙方支付40%合同款。
     3. 经竣工验收合格，向乙方支付10%合同款。
6. **技术要求**

**第一包：**

# 1、实验室建设目的

2013年起，为适应党政部门对安全人员知识、能力与素质的要求，锻炼我院学生的信息安全实践能力，提高我院学生的信息安全素养，培养创新精神和团队合作意识，北京电子科技学院连续三年举办了信息安全对抗赛。

信息安全对抗赛包含技能比武、网络攻防、微视演绎和知识问答等项目，涉及密码方面的常识与知识、保密方面的常识与知识、信息安全方面的常识与知识、信息安全基本素质或能力、无线通信系统维护技能、计算机网络系统维护技能、计算机软硬件维护技能、办公自动化软件操作技能、信息收集、整理与综合技能、网络攻防基本技能（包括社会工程、缓冲区溢出、软件破解、SQL注入、点击劫持、XSS、CRLF、口令破解、MD5与彩虹表、计算机取证等技能）以及综合运用网络攻防基本技能进行网络渗透的能力、制作跟信息安全方面的常识、知识相关的微视频等内容。

基于云平台的网络对抗与取证平台建设可满足我院的信息安全对抗赛需求，满足我院《计算机取证》课程实践课程需要。

# 2、实验室功能要求

基于云平台的网络对抗与取证平台要求竞赛平台基于OpenStack云计算架构,有独立的云调度平台，可支撑后期靶场的更新、计算机取证课件更新，为满足后期我院师生定制化需求，***要求提供系统源代码，必须为明文可读代码。***为节约成本，本平台可直接使用原有PC环境，无需再更新学生终端。平台由虚拟化管理、云调度、靶场资源、计算机取证资源、渗透终端资源、云视频监控与播放系统组成。要求技术先进，扩展性强。

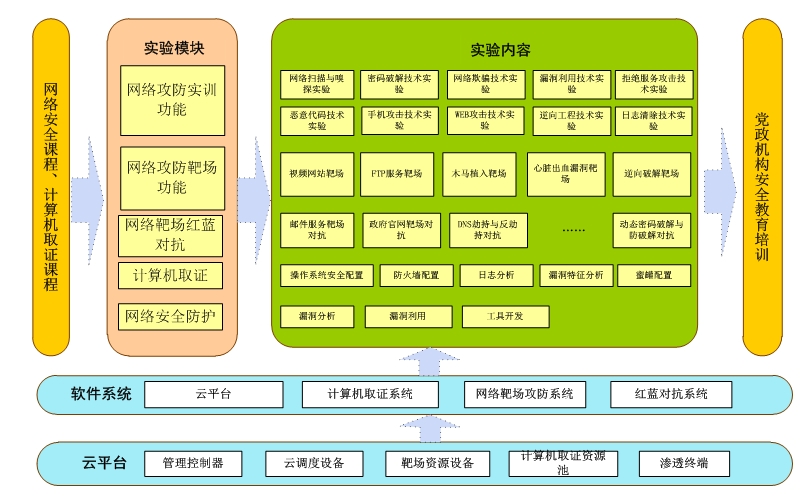


图1 实验室功能结构图

# 3、实验室架构要求

实验室建设计划分为四个区域，一是学生操作区、服务区、取证资源区、靶场区、要求四个可互相访问，保证攻防竞赛和取证平台同时使用。

要求取证功能与网络攻防对抗功能可以无缝对接，即攻防取证结合，可针对攻击行为进取证，要求可以同一个实验室利用同一样云桌面进行两个系统互访，采用的虚拟化平台为同一个虚拟化平台，要求取证实验系统与靶场平台为同一厂家产品。

实验平台要求采用B/S的架构，所有的功能可通过浏览器访问使用，平台包括网络对抗平台管理控制设备、网络对抗平台云调度设备、对抗平台视频直播设备、对抗平台入侵检测设备、单兵过关云资源靶场设备、红蓝对抗云资源靶场设备、WEB后门代码检测专用设备、对抗平台教师管理系统、计算机取证系统管理设备、计算机取证系统资源设备、信息管理系统、计算机取证课程资源包等组成；

实验平台网络结构图，要求如下：

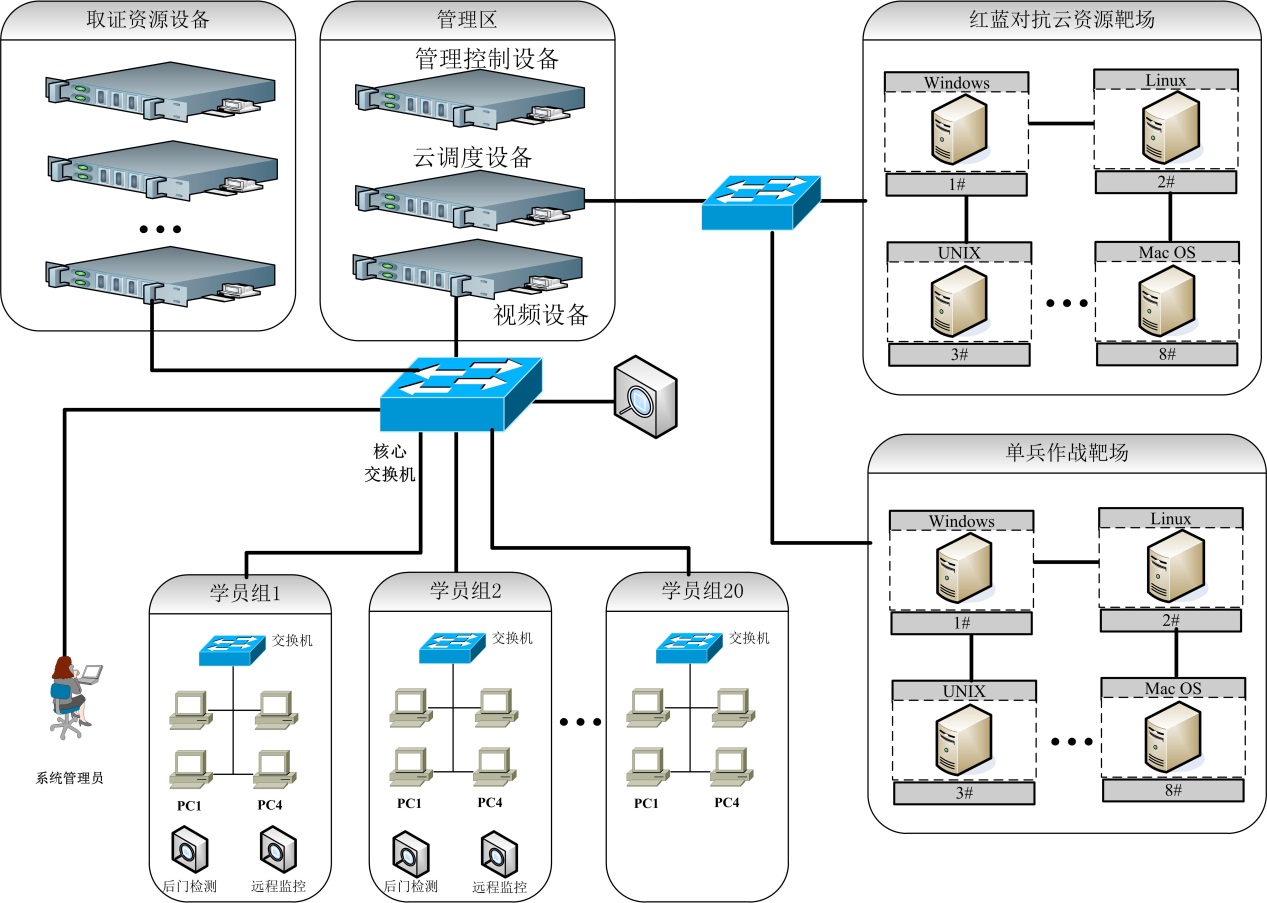


图2 实验室网络拓扑图

# 4、实验室功能需求

## 4.1要求系统是基于云平台架构

学生实验可在实验室，寝室，图书馆通过浏览访问即可开展实验，所有实验资源如操作系统，实验工具，实验课件均在云端运行，学生端包括了选课中心、学习中心、考试中心、用户中心、课程表、实验考勤、实验报告、我的实验录像等功能。

## 4.2教师管理功能

教师管理功能包括学生管理、实验管理、云平台管理、考试管理、系统管理主要功能，系统针对教师管理是个开放的平台，教师可按需定制课程体系，课程类型、课程数量，同样也可以定制特色的实验云环境。

## 4.3用户管理功能

根据学校实际情况，管理员可以自定义添加删除专业、年级和班级，通过Excel表格批量导入导出用户，根据实验环境也可进行用户的自主注册，由管理员审核后即可进行登录。

## 4.4实验管理模块

根据教学安排制定课程表，安排学生的选修课和必修课，最后通过课程调度可以按课程或者按用户进行安排课程。

## 4.5云平台的管理

云平台管理功能包括了虚拟化管理、网络拓扑设计、集中管理设置、虚拟模板管理、弹性云计算管理、云桌面终端、云桌面扫描、云桌面存储、虚拟化统一关机、虚拟机日志等功能。

## 4.6远程协助功能

学生在实验过程中，教师可远程进行监控学习实验状态，并可远程协助学生完成实验项目。

## 4.7考试管理功能

针对实验课程在线进行课程考试和综合实训考试，教师可以自定义试题、题库及考试内容，自定义考核分数、考试学生，教师可以手动评分或者系统自动评分，试题支持单选题、多选题、判断题和问答题，试题可以通过Excel表格批量进行导入导出。

## 4.8系统部署方式

平台部署要求简易化，通过一根网线接入到实验室局域网络即可访问使用，PC端无须安装任何客户端软件，即可完成设备的部署和环境的搭建。学生通过浏览器访问设备并进行实验，教师和管理员通过浏览器进行实验和设备的管理。

## 4.9实验平台资源共享功能

要求能与现在的网络攻防实验系统无缝对接，支持虚拟资源共享，可现实课件同传备份，实验云资源弹性分配。

## 4.10正版加密狗共享功能

计算机取证验系统，要求能读取现有主流的正版加密狗资源信息并共享至设备内所有虚拟机（同时至少共享300个虚拟机），支持阿拉丁、飞天诚信、坚石诚信、深思、圣天诺等品牌的加密狗，以保证虚拟机内的软件能正常使用。

## 4.11靶场管理

支持可同时管理30套基础镜像；支持在线实时扩展云物理主机，最大可扩展至50台；要求可针对物理云资源设备进行可视化管理；支持并发调度，每个学生可分配独立的靶场环境，靶场最大并发数不小于60，支持云环境负载均衡功能。支持物理主机管理、基础镜像管理、增量镜像管理、用户管理；要求可以通过调度系统查看所以靶场设备内的虚拟化场景，要求支持通过调度系统直接查看虚拟化场景；要求支持上传自定义的虚拟镜像，支持VMWARE生成的镜像文件；

# 5、实验内容需求

实验室建成后可满足于信息安全对抗赛包含技能比武、网络攻防、微视演绎和知识问答等项目，涉及密码方面的常识与知识、保密方面的常识与知识、信息安全方面的常识与知识、信息安全基本素质或能力、无线通信系统维护技能、计算机网络系统维护技能、计算机软硬件维护技能、办公自动化软件操作技能、信息收集、整理与综合技能、网络攻防基本技能（包括社会工程、缓冲区溢出、软件破解、SQL注入、点击劫持、XSS、CRLF、口令破解、MD5与彩虹表等技能）以及综合运用网络攻防基本技能进行网络渗透的能力、制作跟信息安全方面的常识、知识相关的微视频等内容。

该系统可用于对计算机取证教学和学校网络对抗比武使用，要求取证和比武系统可以结合使用，取证课程资源不少于50个，至少包括：取证工具实训如EnCase（中文版6.1.9或以上版本）使用、Diskgenius使用、TSK使用等实验不少于25个实验项目；系统取证常用方法例如时间属性、用户管理、日志取证等不少于16个实验项目；deftlinux开源工具不少于5个项目；安全实训互联网赌博、网络诽谤、邮件案件等实训项目不少于8个。比武平台要求不少于30套靶场环境，包括ServU漏洞利用靶场、UDP密码泄露靶场、Windows漏洞靶场1、webshell利用、SQLServer提权靶场、动网SQL注入靶场、cookie分析靶场、IIS设置漏洞靶场、表单欺骗靶场、Windows漏洞靶场2、Tomcat服务器漏洞利用、系统弱口令利用靶场、电气公司网站靶场、某新闻系统靶场、雷池新闻系统靶场、织梦手工SQL注入靶场、某培训机构网站靶场、某环保组织网站靶场、HFS漏洞靶场、红亚会议网站靶场、南方数据靶场、红亚官网靶场、电商靶场、OA系统、三牌闯关内网渗透靶场、端口转发利用综合靶场、wordpress内网渗透综合靶场、心血漏洞靶场、代码审计综合靶场。

## 5.1详细实验项目要求

系统支持实验包括四个层次，工具实训、系统命令实训、开源工具、案例实训，详细要求如下，必须满足以下要求：

|  |  |
| --- | --- |
| 实验体系 | 实验名称 |
| 取证工具应用实验 | 1-1 diskgenius恢复硬盘数据 |
| 1-2 easyrecovery恢复硬盘数据 |
| 1-3 文件的删除与修复 |
| 1-4 利用dd命令擦除数据 |
| 1-5 利用dd命令备份数据 |
| 1-6 encase的配置（中文版6.1.9或以上取证版本） |
| 1-7 IE访问痕迹 |
| 1-8 2GREP语法搜索手机号 |
| 1-9 关键字搜索(银行信息） |
| 1-10关键字搜索（论坛信息） |
| 1-11 恢复导出已删除的文件 |
| 1-12 raid重建 |
| 1-13 注册表取证 |
| 1-14 哈希计算 |
| 1-15 恢复删除的JPG图片 |
| 1-16 文件过滤 |
| 1-17 关键字搜索 |
| 1-18 书签 |
| 1-19注册表文件检验 |
| 1-20QQ聊天记录检验 |
| 1-21tsk工具应用 |
| 1-22网络查看工具ipconfig和netstat |
| 1-23网络监听工具ethereal使用 |
| 1-24windows file analyzer分析隐藏文件和cache |
| 1-25windows利用系统命令查看登录信息 |
| 开源取证工具 | 2-1testd数据恢复 |
| 2-2foremost数据恢复 |
| 2-3photorec 数据恢复 |
| 2-5cmospwd使用 |
| 2-6cupp使用 |
| 2-7wireshark使用 |
| 2-8testd数据恢复 |
| 操作系统取证命令及功能 | 3-1windows下的时间提取(时间属性） |
| 3-2linux下文件时间属性提取(时间属性） |
| 3-3windows下操作系统还原 |
| 3-4linux下文件夹目录特点并验证和总结 |
| 3-5使用命令和任务管理器对进程进行操作 |
| 3-6使用工具软件对进程进行操作 |
| 3-7linux ps命令 |
| 3-8linux top命令 |
| 3-9linux kill命令 |
| 3-10windows下用图形进行用户管理 |
| 3-11windows下用命令进行用户管理 |
| 3-12linux下的用户管理 |
| 3-13linux系统日志检验和查看 |
| 3-14分析日志 |
| 3-15windows 下查看日志 |
| 3-16windows 下查看日志 |
| 案例实训 | 4-1机密泄漏案件 |
| 4-2诽谤痕迹调查 |
| 4-3互联网赌博 |
| 4-4快捷方式解析 |
| 4-5网络游戏外挂案 |
| 4-6网上娱乐赌博 |
| 4-7邮件调查案件 |
| 4-8数据加密解密 |

## 5.2靶场内容要求

靶场要求包括五个层次，攻防知识选择题、靶场技能题、初级靶场、中级靶场、高级靶场题，靶场列表如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **文档** | **视频** |
| 01 | ServU漏洞利用靶场 | 完整 | 完整 |
| 02 | UDP密码泄露靶场 | 完整 | 完整 |
| 03 | Windows漏洞靶场1 | 完整 | 完整 |
| 04 | webshell利用 | 完整 | 完整 |
| 05 | SQLServer提权靶场 | 完整 | 完整 |
| 06 | 动网SQL注入靶场 | 完整 | 完整 |
| 07 | cookie分析靶场 | 完整 | 完整 |
| 08 | IIS设置漏洞靶场 | 完整 | 完整 |
| 09 | 表单欺骗靶场 | 完整 | 完整 |
| 10 | Windows漏洞靶场2 | 完整 | 完整 |
| 11 | Tomcat服务器漏洞利用 | 完整 | 完整 |
| 12 | 系统弱口令利用靶场 | 完整 | 完整 |
| 13 | 电气公司网站靶场 | 完整 | 完整 |
| 14 | 某新闻系统靶场 | 完整 | 完整 |
| 15 | 雷池新闻系统靶场 | 完整 | 完整 |
| 16 | XYCMS企业站系统靶场 | 完整 | 完整 |
| 17 | Struts2漏洞靶场 | 完整 | 完整 |
| 18 | 某环保组织网站靶场 | 完整 | 完整 |
| 19 | HFS漏洞靶场 | 完整 | 完整 |
| 20 | 织梦手工SQL注入靶场 | 完整 | 完整 |
| 21 | 某培训机构网站靶场 | 完整 | 完整 |
| 22 | 某公司会议网站靶场 | 完整 | 完整 |
| 23 | 南方数据靶场 | 完整 | 完整 |
| 24 | 某公司官网靶场 | 完整 | 完整 |
| 25 | 电商靶场 | 完整 | 完整 |
| 26 | OA系统 | 完整 | 完整 |
| 27 | 三牌闯关内网渗透靶场 | 完整 | 完整 |
| 28 | 端口转发利用综合靶场 | 完整 | 完整 |
| 29 | wordpress内网渗透综合靶场 | 完整 | 完整 |
| 30 | 心血漏洞靶场 | 完整 | 完整 |
| 31 | 代码审计综合靶场 | 完整 | 完整 |

# 6、采购清单

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 数量 |
| 1 | 网络攻防对抗平台硬件设备 | 19 |
| 2 | 计算机取证平台硬件设备 | 11 |
| 3 | 网络对抗平台管理控系统 | 1 |
| 4 | 网络对抗平台云调度系统 | 1 |
| 5 | 对抗平台视频直播系统 | 1 |
| 6 | 网络攻防对抗检测软件 | 1 |
| 7 | 单兵过关云资源靶场系统 | 8 |
| 8 | 红蓝对抗云资源靶场系统 | 8 |
| 9 | WEB后门代码检测系统 | 2 |
| 10 | 远程安全监控系统 | 2 |
| 11 | 攻防态势监控终端 | 2 |
| 12 | 对抗平台教师管理系统 | 1 |
| 13 | 单兵过关竞赛系统（80并发） | 1 |
| 14 | 红蓝对抗竞赛系统（20队并发） | 1 |
| 15 | 无线攻防渗透测试实训系统 | 1 |
| 16 | 渗透测试工具包 | 1 |
| 17 | 计算机取证系统管理系统 | 1 |
| 18 | 计算机取证系统取证资源系统 | 10 |
| 19 | 计算机取证系统信息管理系统 | 1 |
| 20 | 计算机取证系统学生实验系统 | 1 |
| 21 | 计算机取证课程资源包 | 1 |
| 22 | 移动终端 | 10 |
| 23 | 路由器 | 1 |
| 24 | 核心交换机 | 1 |
| 25 | 管理中心交换机 | 5 |
| 26 | 机柜 | 4 |
| 27 | 信息安全系统设计实验箱 | 40 |
| 28 | 竞赛支持设备 | 1 |

# 7、设备清单及性能指标要求

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **技术指标要求** | **数量** |
| 1 | 网络攻防对抗平台硬件设备 | **硬件指标要求：**   * 机架结构，高度不超过2U； * CPU：不低于6核，主频≥1.6GHz * 内存：≥64G； * 硬盘：≥1000G 固态盘存储方式，要求全盘支持虚拟化；高速缓存硬盘连续读取速度不少于500M/秒； * 网口：≥2个10/100/1000M； * USB接口：≥2个USB； * 要求支持虚拟化平台，要求单台可运行75个虚拟化环境； | 19 |
| 2 | 计算机取证平台硬件设备 | **硬件指标要求：**   * 机架结构，高度不超过2U； * CPU：不低于6核，主频≥1.6GHz * 内存：≥64G； * 硬盘：至少配备两块硬盘，其中虚拟化硬盘≥240G ；存储硬盘≥2TB ; * 网口：≥2个10/100/1000M； * USB：≥2个USB接口； * 要求支持虚拟化平台，要求单台可运行45个虚拟化环境； | 11 |
| 3 | 网络对抗平台管理控系统 | **系统功能要求**：   * 支持虚拟化，支持多类型镜像导入，增量镜像，负载均衡等功能； * 支持对整个系统管理，可管理系统各设备，可对各设备进行开关机，暂停，重启； * 提供不同应用的云主机，服务包括：FTP、HTTP、E-mail、DHCP、DNS； * 要求设备嵌入云平台管理系统，管理系统内包括虚拟化功能，支持查看当前云平台自动调用的虚拟化资源； * 虚拟化支持独立管理； * 提供可视化的云平台管理功能； * ★要求最大可支持管理50台云资源设备管理功能； * ★要求最大可同时监控300个靶场实时管理；   **其它要求**：   * ★提供生产厂家出具的售后服务承诺函； | 1 |
| 4 | 网络对抗平台云调度系统 | **系统功能要求**：   * ★内嵌云调度系统，要求云调度系统可单独访问，要求系统为国内自主研发产品； * ★要求中标后3日内向最终用户提供云调度系统所有源代码； * 负责对靶机资源调度和管理，包括网络拓扑智能生成功能； * 支持单个靶场在线可视化的调度管理； * 支持靶场增量管理，可针对系统内所有的云资源平台进行管理，最大可管理50台； * 支持可同时管理30套靶场基础镜像； * 支持在线实时扩展云物理主机，最大可扩展至50台； * 要求可针对物理云资源设备进行可视化管理； * 支持并发调度，每个学生可分配独立的靶场环境，最大60靶场并发，支持云环境负载均衡功能； * 支持物理主机管理、基础镜像管理、增量镜像管理、用户管理； * 要求可以通过调度系统查看所以靶场设备内的虚拟化场景，要求支持通过调度系统直接查看虚拟化场景； * 要求支持上传自定义的虚拟镜像，支持VMWARE生成的镜像文件； | 1 |
| 5 | 对抗平台视频直播系统 | **系统功能要求**：   * 提供比赛现场直播功能； * 支持多屏同放，支持后台进行分屏管理； * 要求视频可直接在教师管理系统界面上直接播放； * 支持视频存储，单台主机能够支持4路的视频储存及播放； * 要求现场直播延时不超过1秒； | 1 |
| 6 | 网络攻防对抗检测软件 | **功能要求：**   * 要求在系统检测到攻击行为时，应能够实时地向管理控制台发送报警信息。 * 要求除了发送实时报警信息外，还应将检测到的网络入侵事件及相关信息保存下来（可以文件的形式或保存在数据库中），生成审计日志。 * 要求探测引擎支持缓冲报警信息功能。当报警信息过多时，或控制台出现问题时，报警信息缓存在探测引擎。引擎日志存储空间需不低于400G * 要求适应各种应用上的需求，管理员可能需要通过邮件来及时了解入侵事件。 * 要求实时地向管理控制台发送报警信息外，还可同时发出声音提示有入侵事件发生。 * 要求当有入侵事件发生时，发送SNMP trap * 要求当检测到某些TCP/IP某些攻击事件时，是否具有切断的功能要具有切断会话连接的功能。 * 支持与防火墙联动，列出联动防火墙的品牌和型号并列出支持的开放联动协议。 * 要求能检测的各类主动攻击方式，如攻击探测/端口扫描、非法访问、木马后门攻击、拒绝服务攻击等。 * 要求规则数不少于3000条。 * 支持应用协议分析，支持40种以上常见应用协议。 * 支持能够对一些简单的应用协议进行解码或者还原，例如telnet, ftp，POP3，SMTP 等。 * 支持提供单独的跟踪器对事件相关的IP地址进行反跟踪 * 支持通过管理控制台可以对探测器进行监控。管理控制台应能实时显示探测器的当前状态。 | 1 |
| 7 | 单兵过关云资源靶场系统 | **功能要求**：   * 为实战平台提供云靶场资源，设备资源、服务器资源和网络资源进行虚拟化； * 要求云资源平台有较强的扩容能力，可在系统运行下，实时扩容； * 要求最大扩容能力达50台，最大扩容量可满足1000人同时开展网络靶场实战攻击； * 要求扩容后的靶场间可进行网络通信； * 要求系统自带靶场资源环境不少于200个； * 靶机资源包括windows操作系统类型和Linux系统、MAC OS，提供各类应用服务，包括FTP、DNS、E-mail、WEB、数据库、DHCP、系统安全软件等； * 渗透端虚拟环境提供WindowsXP\win7\LINUX实验环境； * 支持新资源环境添加和编程功能，提供WEB管理界面，支持导向式管理，无需进入虚拟机内进设置； * 为方便用户自行设计云虚拟资源，提供各类型的模板； * 所的靶场均采用云计算技术； * 要求同地，同时，2分钟内可启动不小于60个不同的靶场同时运行使用，120个渗透主机同时运行使用，所有运行的环境采用云计算技术，所有学员渗透主机均为独立，互不影响；本地只需浏览器即可开展攻防实战； | 8 |
| 8 | 红蓝对抗云资源靶场系统 | **功能要求**：   * 内嵌云靶场管理系统，为红蓝对抗提供实时攻击，实时防护靶场； * 单台设备内置不少于20组红蓝对抗靶场，要求支持不少于3人同时实时防护； * 红蓝资源靶机资源包括windows操作系统类型和Linux系统、MAC OS，提供各类应用服务，包括FTP、DNS、E-mail、WEB、数据库、DHCP、系统安全软件等； * 支持自行设计云虚拟资源，提供各类型的模板；所有的靶场均采用云计算技术，提供相关的功能截图； * 要求同地，同时，2分钟内可启动不少于60个不同的靶场同时运行使用，80个渗透主机、20组红蓝机同时运行使用，所有运行的环境采用云计算技术，所有学员靶场均为独立，互不影响；本地只需浏览器即可开展攻防实战。 | 8 |
| 9 | WEB后门代码检测系统 | **功能要求：**   * ★可探测开标前1个月以前后门漏洞；兼容各种Web服务器类型：包括Microsoft IIS 5/6/7、Apache、Nginx、Tomcat等； * ★能够支持针对所有Web浏览器，包括Internet Explorer、Chrome、Firefox、Opera、Safari、Maxthon、360浏览器等; * 能够获取到该用户客户端的信息，包括互联网IP地址、操作系统类型及版本、浏览器类型及版本等。操作系统类型支持：Windows、Linux、Macintosh； * 浏览器类型支持：Internet Explorer、Chrome、FireFox、Safari、Opera； * 能够突破浏览器的权限控制和安全防御措施，获取客户端的如下重要插件是否安装并嵌入浏览器中，以及所安装嵌入软件的精确版本号：Adobe Flash、Adobe Reader、Java、Microsoft Silverlight、QuickTime、RealPlayer、Windows Media Player、支付宝、银联在线、迅雷、暴风影音、酷狗音乐等。 * 提供配套硬件平台；   **其它要求：**   * ★制造厂商出具的售后服务承诺函； | 2 |
| 10 | 远程安全监控系统 | **功能要求：**   * 支持多窗口形式提供分类显示信息； * 要求提供灵活、方便、易懂、直观、全面的人性化攻击数据报表，支持多种导出格式； * 报表有清晰的统计图表，有柱状图、饼状图等； * 要求支持会话分解，要分解成上行和下行两路； * 要求支持会话重新组合并检测到存在的攻击； * 支持监听端口不能有IP地址； * 支持引擎与控制台之间通讯数据应加密； * 支持应至少包括网络流量和入侵流量统计； * 支持攻击行为分析，并进统计分析； * 支持触摸控制，屏幕尺寸12英寸； * 支持多线程处理，要求设备物理内容不小于8G； * 要求存储量不小于256G； * 要求提供2个数据接口，支持数据导入导出，支持U盘导入；   **其它要求：**  ★制造厂商出具的售后服务承诺函； | 2 |
| 11 | 攻防态势监控终端 | **功能要求：**   * CPU: ≥2.5GHz 四核处理器 3.7GHz 三级缓存:6M * 内存: ≥16GB 1600MHz DDR3L 主板集成内存 * 硬盘容量: ≥512GB PCIe 闪存 * 显存: ≥2GB * 无线局域网:802.11ac Wi-Fi 无线网络 * 要求可以同时查看多个比赛成绩； * 要求可以查看总成绩，和详细成绩； * 详细成绩要求包括攻防进度，正确率，靶场背景； * 要求红蓝对抗可以监控每个队阵地态势； * 要求可以监控不少于20个的阵地环形关卡； * 要求可以每个关卡都有对应的背景； * 要求可以监控每一个学员的攻击机的实时操作； * 要求可以监控每一个对抗靶机的安全状态； | 2 |
| 12 | 对抗平台教师管理系统 | **功能要求**：   * 支持基于WEB的用户注册功能，并支持学生、教师和管理员三种用户，并支持用户自己修改用户信息； * 为整个系统提供管理功能，系统功能包括了用户管理、题库管理、靶场比赛管理、对抗比赛、云平台管理、成绩管理、系统管理； * 用户管理包括学生管理、班级管理、老师管理、学院管理、专业管理、年级管理、团队管理； * 题库管理要包括靶场题目管理、对抗题管理、单选题管理、多选题管理及类型管理，要求可实时的添加，可在线预览题目功能； * 靶场比赛管理包括比赛名称、题量、比赛时间、参赛人数、比赛管理、靶场管理、成线管理，要求可以导入成绩表； * 对抗比赛管理包括靶场名称、靶场数、比赛时间、团队数、比赛进度、比赛管理、靶机管理、成绩管理； * 云平台管理，提供不同应用的云主机，服务包括：FTP、HTTP、E-mail、DHCP、DNS； * 系统管理，可管理平台名称、是否开放用户注册、是否开放攻击机、比赛声明等功能； * ★成绩管理要求可详细成绩查看，包括详细的过关情况，并可以查看每一题的历史背景，可直接显示在成绩上； * ★要求可实时展示红蓝对抗成绩，可展示每一队的阵地被攻击情况，可动态的以彩旗方式显示入侵的步骤； | 1 |
| 13 | 单兵过关竞赛系统（80并发） | **功能要求**：   * 系统基于B/S架构，学生利用用户名密码登陆，系统包括技能靶场、初级靶场、中级靶场、高级靶场四类，不少于30套靶场； * ★要求30套靶场没有重复类型；技能靶场内至少包括100个技能过关卡；初级类型靶场中，至少包括15套靶场，并可以在界面直观的显示每一关的入侵情况；中级靶场，至少包括10套靶场；高级靶场，至少包括5套靶场； * 要求靶机包括公司网站漏洞利用靶场、网站漏洞攻击之XYCMS企业建站系统靶场、应用系统漏洞攻击之靶场、Safe Check For Linux靶场、动态反调试逆向算法靶场、Heartbleed漏洞靶场、OpenSSL漏洞等不少于30套靶场环境，不少于200多个靶机； * 每个用户登录都可以自动分配一个windowsXP和Kali两个渗透主机，渗透主要要求采用KVM底层虚拟化，无须本地任何资源，渗透主机通过浏览器进行访问操作； * ★至少提供5份用户测试报告，以证明所投产品可支持校内竞赛；   ★要求提供定制化的单兵攻防虚拟化环境，要求有独立自主产权，提供产权证书复印件，提供的工具要求如下：  **1、Windows主机安全检查工具：**   * 支持检查主机系统配置信息，包括：计算机名、用户名、操作系统、版本、内存大小、磁盘大小、系统路径、共享目录； * 支持检查Internet Explorer、Chrome、Firefox等浏览器上网记录、Cookie记录； * 支持检查主机硬件信息，包括：CPU信息、主板信息、内存信息、显卡信息、硬盘信息、网卡信息； * 支持检查主机开机自启动项程序； * 查看主机上已经启动的可能有风险的服务程序，包括：如Task Scheduler、Print Spooler、Remote Registry 等服务； * 支持检查账户安全策略信息，包含口令长度、复杂度、定期更换、登录失败、锁定次数等； * 支持在线更新、离线升级。   **2、主机病毒检查工具：**   * 支持对操作系统的关键机制，如系统服务、内存、注册表、启动进程；检测操作系统的安全模型，包括访问控制、特权和审计；反馈系统安全配置、文件访问，驱动、引导等系统深度进行检查； * 支持检查流氓软件、蠕虫病毒、其它恶意程序等； * 支持快速扫描、全盘扫描、自定义目录扫描； * 运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型； * 支持在线更新、离线升级。   **3、主机木马检查工具：**   * 支持检查系统中的木马程序、Rootkit、间谍程序等； * 提取操作系统的关键机制，如系统服务、内存、注册表、启动进程；检测操作系统的安全模型，包括访问控制、特权和审计；反馈系统安全配置、文件访问，驱动、引导等系统深度信息； * 支持快速扫描、全盘扫描、自定义目录扫描； * 运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型； * 支持在线更新、离线升级。   **4、网站恶意代码检查工具：**   * 支持asp、asa、cer、jsp、jspx、php 等文件格式检查； * 支持自定义文件后缀格式； * 支持异性、变异WEBSHELL后门代码检查； * 支持关键恶意特征码定位； * 支持快速扫描、全盘扫描、自定义路径扫描； * 支持自定义扫描策略、可扩充恶意特征码； * 支持自定义文件大小扫描； * 运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型； * 支持在线更新、离线升级。   **5、Linux主机安全配置检查工具：**   * 支持检查主机系统配置信息，包括：计算机名、用户名、操作系统、版本、内存等 * 支持检查系统安全补丁升级情况； * 支持检查不必要的服务和端口（如TELNET、SSH、SNMP、HTTP等）； * 支持检查账户安全策略信息，包含口令长度、复杂度、定期更换、登录失败、锁定次数等； * SNMP、SSH服务、版本信息； * 支持检查安全审计配置情况、包含事件类型； * 支持检查屏幕保护恢复时间； * 支持RedHat、Ubuntu、Debian、Fedora、Suse、Centos操作系统类型； * 支持在线更新、离线升级。   **6、网络及安全设备配置检查工具：**   * 支持检查账户安全策略信息，包含口令长度、复杂度、定期更换、登录失败、锁定次数等； * 支持检查安全审计策略，包含事件类型、SYSLOG服务器； * 支持检查不必要的服务和端口（如TELNET、FTP、SNMP、HTTP、Sendmail）； * 支持SNMP、SSH服务、版本信息检查； * 运行环境支持Windows XP、 Windows7、 Windows Server 2003、Windows Server 2008等操作系统类型； * 支持在线更新、离线升级；   **7、弱口令检查工具：**   * 应用服务支持类型：SSH、SMB、TELNET、FTP、RDP、SQL Server、Oracle、MySQL、POP3等协议应用程序弱口令检查； * 支持自定义账户、口令字典； * 支持自定义应用协议TCP端口； * 内置常见弱口令字典（如口令为：123456、88888888、12345等）； * 支持本地、远程主机及多协议同时检查； * 运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型； * 支持在线更新、离线更新。   **8、数据库安全检查工具：**   * 支持IPV6地址检查； * 支持对数据库弱点、不安全配置、安全策略、补丁升级、弱口令安全检查； * 支持主流Oracle、SQL Server、DB2、Informix、MySQL、Sybase数据库类型； * 支持授权扫描，使用具有DBA权限的数据库用户，执行选定的安全策略实现对目标数据库检查； * 非授权扫描,用户在没有授权的情况下（即：不需要数据库用户名、密码），根据选定的安全策略对目标数据库进行的检测； * 策略自定义,提供扫描策略可自定义模式，操作者可以灵活选择默认策略的同时也可以自定义添加策略；   **9、网站安全检查工具：**   * 支持WEB 2.0，支持各类JavaScript脚本解析； * 支持WAP站点扫描； * 支持FLASH解析； * 支持基于HTTPS应用系统的扫描； * 支持实时存储扫描项目文件、断点续扫； * 支持ERP等复杂的Web应用系统扫描； * 支持易通、织梦、DEDECMS、Discuz、Ecshop、易思、方欣、大汉、科讯、通达OA、PHPCMS、PHP168、PHPCMS2008、phpcms v9、SHOPEX、SiteServercms、TRS、 Nginx代码执行、Spring代码执行、亿邮邮件系统命令执行等国内、国外知名WEB应用程序漏洞扫描； * 支持JSP、CGI、ASP、.NET等类型动态页面； * 支持IP地址、域名地址、批量网站扫描； * 支持无人值守模式下的全自动扫描； * 支持HTTP 1.0和1.1标准的Web应用系统； * 支持Oracle、SQL Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Access、 Ingres等后台数据库类型； * 支持对SQL注入、XSS跨站脚本、伪造跨站点请求、网页木马、隐藏字段、表单绕过、AJAX注入、弱配置、敏感信息泄漏、HI－JACK攻击、弱口令、Xpath注入、LDAP注入、框架注入、操作系统命令注入、Flash源代码泄漏、Flash跨域攻击、Cookies注入、敏感文件、第三方软件、其他各类CGI等漏洞进行扫描； * 支持在线更新、离线升级；   **10、系统漏洞检查工具：**   * 支持对Microsoft Windows XP/2003/Vista/2008/7、Sun Solaris、HP Unix、IBM AIX、IRIX、Linux、BSD等操作系统进行漏洞扫描； * 支持对Web、FTP、电子邮件等应用系统以及Office、Apache等常用软件进行漏洞扫描； * 支持对网络设备进行漏洞扫描； * 支持多种扫描策略，包括常规完全扫描、高强度完全扫描、高强度扫描、中强度扫描、低强度扫描、Windows主机扫描、类Unix主机扫描等扫描策略，方便用户快速选择； * 支持自动统计总体漏洞数量、统计不同操作系统类型的主机数量、统计所有开发端口、可用帐户、列出每一个漏洞所存在的主机、详细描述与修补建议。漏洞详细描述包括：漏洞名称、详述、修补方案、CVE/Bugtraq/CNCVE/CNNVD编号、CVSS评分等； * 支持在线、离线更新； * 支持导出Word、PDF常见格式报表。   **11、SQL注入验证检查工具：**   * 支持常见的数据库，包括msSQL,oracle,mySQL,db2,access等数据库； * 支持任意注入点的注入（包括url注入、伪静态注入、cookie注入、referrer注入、GET参数注入、POST参数注入、xml格式请求注入、json格式请求注入等）； * 支持盲注、错误注入、union注入方式； * 获取数据库各种环境变量、列举数据库名、表名，获取表结构，并能导出相关数据； * 支持扩展功能，各种渗透功能，包括执行系统命令、启动组件、远程桌面开启关闭、获取系统信息、文件读取、注册表读取。 | 1 |
| 14 | 红蓝对抗竞赛系统（20队并发） | **功能要求**：   * 系统基于B/S架构，学生利用用户名密码登陆，红蓝对抗要求必须支持以小组进行，每小组可包括3-10人，至少支持同时30组进行相互攻击；每个小组成员，均可以自主选择红方攻击，和蓝方防守； * 红方攻击成员，可实时看到每一组阵地内总分，及目前阵地内所剩分数，可任意选择其它小组阵地进行攻击，进入阵地后，可看到阵地里每一关卡的状态，状态包括沦陷和安全，沦陷的不可再进行攻击；安全可以进行攻击；每攻下一个关卡后，本队可增加一定分数，对方减少一定的分数； * 蓝方可实时对本队阵地的靶场通过浏览器操作管理，可修改任何的参数，以达到防护状态，蓝方同进可以在防守端看到自己阵地关卡状态，状态分为沦陷和安全； * 要求每一组的阵地至少包括2个靶机，每个靶机之间必须有相关联性； * 为保证每组的公平性，要求每组的靶机难度相关，且每组的环境不相同，内置的过关文件不相同，KEY也不相同； * 每个用户登录都可以自动分配一个windowsXP和Kali两个渗透主机，渗透主机要求采用虚拟化文件，无须本地任何资源，渗透主机通过浏览器进行访问操作；   **其它要求：**   * ★制造厂商出具的售后服务承诺函； | 1 |
| 15 | 无线攻防渗透测试实训系统 | **功能要求：**  系统基于B/S架构，学生利用用户名密码登陆；支持120人同时使用，包括以下实验项目，每个实验项目包括实验原理、实验目的、实验环境、实验步骤、实验所需的工具，可开展的实验不少于以下实验项目：  **1、无线WIFI基础实验项目要求：**  **（1）WiFi无线路由配置实验：**   * AP模式（接入点模式）实验； * Router模式（无线路由模式）实验； * Repeater模式（中继模式）实验； * Bridge模式(网桥模式) 实验。   **（2）、WiFi组网实验：**   * Ad-Hoc WiFi设备组网实验； * Win7无线网卡设置成WiFi无线路由器实验。   （3）、**WiFi安全实验：**   * SSID扫描与SSID广播关闭； * 信号功率测量与频道设置； * 无线MAC地址过滤规则配置； * 无线DHCP与MAC绑定设置； * WEP安全配置； * WPA-PSK/WPA2-PSK安全配置； * WPA/WPA2 Radius安全认证实验； * 无线DoS攻击防护； * IP带宽控制配置。   **2、无线网络攻防实战实验项目要求：**  **（1）、WEP攻防基础：**   * WEP原理； * 无线破解BackTrack5套装入门。   **（2）、WPA-PSK攻防实战：**   * 传统WPA-PSK加密破解； * WPA/WPA2 deauth攻击。   **（3）、使用WPA hash Tables破解WPAWPA2实战：**   * Hash tables制作； * Hash tables使用。   （**4）、无线DoS攻击实战：**   * DoS工具Charon-亡灵摆渡人； * Auth Flood攻击； * Deauth Flood攻击； * Disassociation Flood攻击；   （**5）、WEP注入攻击：**   * 注入攻击； * ARP注入攻击。   **（6）、WEP高级攻击：**   * chop chop攻击； * fragmentation攻击。   **（7）实验指导书要求**  **3、NS3仿真实验项目要求：**  **（1）、NS3仿真基础实验：**   * NS3的安装与配置； * 两个节点间简单通信的模拟实现； * 使用可视化组件模拟一个星形拓扑结构网络； * 无线自组织网络的简单场景模拟。   （**2）、NS3仿真综合实验：**   * 无线自组织网络DSDV协议场景模拟； * 无线传感器网络CSMA协议场景模拟； * 无线城域网WiMAX协议的场景模拟； * 无线网状网HWMP协议的场景模拟。   **（3）实验指导书要求：**  **4、无线自组织网络攻防与仿真实验项目要求：**  **（1）可开展实验项目要求：**   * NS2仿真基础实验； * NS2安装与配置； * Tcl语言网络环境配置； * 使用CMU工具配置一个随机场景； * 移植实现MFlood协议； * 添加mac协议； * 无线自组织网络AODV协议的仿真； * 网络仿真攻击专项实验； * 黑洞攻击实验； * 泛洪攻击实验； * 信道抢占攻击实验； * 虫洞攻击实验； * 黑洞检测实验；   （2）、**实验指导书要求：**  **5、手机通信安全实验项目要求：**  **（1）可开展的实验项目要求：**   * 支持手机短信加密实验； * SIM卡复制； * GSM劫持； * 电话攻击； * 短信攻击； * 手机病毒分析； * 远程窃听； * 提供配套的实验系统及源代码。   **其它要求：**  ★制造厂商出具的售后服务承诺函； | 1 |
| 16 | 渗透测试工具包 | **功能要求：**  网络攻防专用设备，工具集包括SHELL获取功能工具；权限提升相关的工具；隐藏服务相关工具；模拟服务相关工具；木马（后门）相关工具；信息获取相关的工具；控制管理相关的工具；清理痕迹相关工具；密码破解相关工具；拒绝服务相关工具；数据通道相关工具，总计不少于800个专用工具。 | 1 |
| 17 | 计算机取证系统管理系统 | **功能要求**   * 计算机取证管理系统，负责对实训平台内的取证工具资源进行调度和管理； * 支持实验环境设计、课件管理、课件调度、不同实验可按自由实验资源环境； * 课件设计提供基于WEB的可视化的管理界面，环境支持拖拽设计； * 支持课件并发使用，每个学生实验可分配独立的实验环境，相互不影响；最大80课件同时使用； * ★要求可读取USB KEY信息，共享至系统内所有的虚拟资源环境，以保证虚拟机内需要USB key的程序正常运行； * ★支持的USB KEY至少包括阿拉丁、飞天诚信、坚石诚信、深思、圣天诺等品牌的加密狗； * ★要求提供本设备内软件系统所有的明文源代码并提供生产厂家提供源码承诺书；   **其它要求：**  ★制造厂商出具的售后服务承诺函； | 1 |
| 18 | 计算机取证系统取证资源系统 | **功能要求：**   * 为实验平台提供计算机取证工具资源、服务器计算资源和网络资源进行虚拟化； * 取证资源系统资源包括了windows操作系统类型和Linux系统； * 取证工具资源提供了各类取证工具资源，包括diskgenius、easyrecovery、encase、testd、photorec、cmospwd、wireshark等应用程序； * 客户端虚拟环境提供Windows、LINUX实验环境； * 支持新资源环境添加和编程功能，提供WEB管理界面，支持导向式管理，无需进入系统设置； * 为方便用户自行设计计算取证工具资源，提供各类型的模板； * 取证资源支持在线远程更新功能； | 10 |
| 19 | 计算机取证系统信息管理系统 | **主要功能：**  ★系统采用B/S结构，支持在线注册功能，分为超级管员和普通教师管理功能，系统包括课程管理、用户管理、统计管理、考核管理和系统管理；  详细功能：   * 课程管理包括了新建课程、导入课程、课程分类、在线更新，每个课程包括了负责讲师、管理员、学员人数、预览、描述、进度、公告、文件、作业、导出、修改、删除功能项目； * 支持用户课件的上传，提供用户上传课件内容后在线浏览功能，同时可以在线下载课件； * 我们桌面功能可对学生进行远程桌面管理，支持远程协助； * 查询统计可包括学习情况查询、进度查询、在线情况； * 考核管理包括了题库管理、所有考核管理、综合考核管理、课程考核管理、实训考核管理等功能； * 支持题库管理定义课程题库； * 支持综合考试管理通过详细流程来定制综合考试相关试题； * 用户管理包括批量导入、导出，组织管理、权限设置、课程授权、黑白名单； * 系统管理包括平台个性化设计、邮件服务、系统安全设置； | 1 |
| 20 | 计算机取证系统学生实验系统 | **功能要求：**  系统采用B/S架构，通过浏览器进行访问实验，利用学生用户名密码进行登陆，支持学生在线注册，主要包括了选课中心、学习中心、课程表、考核、调查问卷、用户中心；   * 选课中心包括了取证工具实验、系统取证常用功能实验、案件实训实验等40多个实验项目； * 学习中心是学生开展实验的功能，每个实验均包括了课程信息、实验步骤、实验环境、课程公告、课程文档、课程作业及课程云环境，云环境可在浏览器上运行，不占用本地计算资源； * 实验报告，学生可按老师模板制作实验报告，并在线提供交； * 课程表是学生可按老师制作的课程表有计划的进行实验； * 考核包括了在线考核、课程考核、课程作业； * 调查问卷支持学生在线根据自己的实验情况提交老师的调查问卷； * 用户中心包括了信息修改、密码修改、我的考勤； | 1 |
| 21 | 计算机取证课程资源包 | **功能要求：**  ★课程包资源包括四个层次，工具实训、系统命令实训、开源工具、案例实训，详细要求如下：   * diskgenius恢复硬盘数据； * easyrecovery恢复硬盘数据； * 文件的删除与修复； * EnCase的配置（版权不低于6.19要求取证版）； * IE访问痕迹； * 2GREP语法搜索手机号； * 关键字搜索； * 关键字搜索； * 恢复导出已删除的文件； * raid重建； * 注册表取证； * 哈希计算； * 恢复删除的JPG图片； * 文件过滤； * 关键字搜索； * 注册表文件检验； * QQ聊天记录检验； * tsk工具应用； * 网络查看工具ipconfig和netstat； * 网络监听工具ethereal使用； * windows file analyzer分析隐藏文件和cache； * windows利用系统命令查看登录信息； * testd数据恢复； * foremost数据恢复； * photorec 数据恢复； * cmospwd使用； * cupp使用； * wireshark使用； * testd数据恢复； * windows下的时间提取(时间属性）； * linux下文件时间属性提取(时间属性）； * windows下操作系统还原； * linux下文件夹目录特点并验证和总结； * 使用命令和任务管理器对进程进行操作； * 使用工具软件对进程进行操作； * linux ps命令； * linux top命令； * linux kill命令； * windows下用图形进行用户管理； * windows下用命令进行用户管理； * linux下的用户管理； * linux系统日志检验和查看； * 分析日志； * windows 下查看日志； * windows 下查看日志； * 机密泄漏案件； * 诽谤痕迹调查； * 互联网赌博； * 快捷方式解析； * 网络游戏外挂案； * 网上娱乐赌博； * 邮件调查案件； * 数据加密解密；   **其它要求：**  ★制造厂商出具的售后服务承诺函； | 1 |
| 22 | 移动终端 | **核心板指标要求：**   * 处理器: ≥1.4GHz； * 内存: ≥2GB DDR3； * EMMC: ≥16GB； * PMIC：要求有专业的电源管理芯片，而非分立的DCDC。   **主板资源要求：**   * SD卡接口及存储卡：支持大容量SD卡存储，支持SD/SDIO/SDHC；配置不低于8GB存储容量SD 卡，预装Linux操作系统； * USB接口：≥3路USB\_HOST 2.0输出，≥1路Usb OTG； * Ethernet接口：≥100M自适应网口； * 串口：≥2路3线RS232，1路5线RS232，1路TTL，1路RS485； * CAN总线接口：≥1路； * RS485总线接口：≥1路； * SPI 总线接口：≥板载SPI器件MCP2515，≥1路SPI总线接口引出； * I2C接口：板载I2C器件板载I2C器件陀螺仪、重力加速度芯片； * Audio 接口：Microphone插孔、 耳机输出插孔； * HDMI 接口：≥HDMI v1.4a, 最高1080p@30fps高清数字输出； * CSI高清图像采集传感器接口：≥1个； * GPIO接口：≥12位GPIO接口引出； * ADC接口：≥1路电位器模拟ADC输入； * 液晶显示屏：≥7寸真彩TFT液晶屏，分辨率1024×600 LVDS屏； * 触摸屏：≥7寸电容触摸屏； * LED显示：≥4个LED灯； * 键盘：≥3个Android标准按键（含1个power键）； * 其他资源：数字热敏温度传感器≥1个2路PWM（1路蜂鸣器，1路显示屏）、红外通信接口；   **软件资源要求**：   * 操作系统支持：Android4.0 、Linux3.14（新Linux操作系统移植）、uC/OS、TinyOS、Contiki、Android底层开发部分； * Android4.0环境配置实验、Android文件系统制作实验、Android4.0镜像烧写实验、Android4.0编译实验、Android UART通讯实验、Android HAL LED点灯实验、Android4.0的蜂鸣器实验、Android 温度传感器实验、蓝牙通信实验、Android下GPRS电话、短信实验、Android下GPS定位实验；   **其它要求：**  ★制造厂商出具的售后服务承诺函； | 10 |
| 23 | 路由器 | * 包转发率：≥6.5Mpps * 网络协议：PPPoE，DHCP，DHCP，NAPT，NTP，DDNS； * 传输速率：≥10/100/1000Mbps；端口结构：非模块化； * 广域网接口：1个； * 局域网接口：≥3个； * 其它端口：≥1个Console接口； | 1 |
| 24 | 核心交换机 | * ≥24口10/100M/1000M自适应端口，≥2个SFP/GT光电复用口，≥1个扩展槽 * 背板：≥49.6G；IPv4包转发速率：L2：线速（12.8/16.4Mpps）；L3：线速（12.8/16.4Mpps）；IPv6包转发速率：L2：线速（12.8/16.4Mpps）；L3：线速（12.8/16.4Mpps）； * Defeat IP Scan（防IP扫描）：支持；管理协议：SNMPv1/v2c/v3、CLI(Telnet /Console)、RMON(1,2,3,9)、SSH、SNTP、NTP、Syslog、TACACS+；其它协议：SNMP over IPv6、IPv6 MIB support for SNMP、SSH/Telnet v6、FTP/TFTP v6、DNS v6、NTP for v6、Traceroute v6； | 1 |
| 25 | 管理中心交换机 | * ≥24个10/100/1000 Mbps 端口、1个用于光纤连接的 SFP GBIC 插槽； * 带宽：≥8.8Gbps（无阻塞）；包转发率：6.5Mpps；缓冲区内存：256KB ； * 寻址：≥48 位 MAC 地址；地址数据库大小：每系统 8000个MAC地址； * 平均无故障间隔：300000小时 | 5 |
| 26 | 机柜 | * 尺寸：宽度600mm，深度900mm； * 高度42U； * 前门：钢化玻璃材质，带锁，可拆卸； * 后门：全金属材质，散热网孔设计，带锁，可拆卸； * 侧板：速装卸侧板，全金属材质； | 4 |
| 27 | 信息安全系统设计实验箱 | **硬件要求：**   * 处理器核心板：包含以下四种处理器：  1. A8处理器； 2. M4处理器； 3. Z32处理器； 4. FPGA cyclone\_4；  * 处理器与底板FPGA的通信有两种方式：低速模式，采样串口和SPI口；高速模式采样总线。 * 总线模式将FPGA视为ARM的外部挂接存储器，实现总线的读写等。M4的总线为FSMC.   **软件要求**   * 实验一   嵌入式系统开发环境：基于实践平台的(ARM+FPGA\ARM+Z32)。进行软件安装、硬件连接，熟悉开发流程，掌握程序的装载，调试与测试方法。   * 实验二   密码算法与实现：基于ARM/FPGA/Z32 开发平台，实现商密SM2、SM3、SMS4算法。   * 实验三   密码引擎（密码卡）:基于实践平台的(ARM（16位）+FPGA\ARM（16位）+Z32)实现简单的密码引擎，能够提供对称密码算法、非对称密码算法等的密码服务   * 实验四   密码引擎（服务器密码机） : 基于实践平台的(ARM（32位）+FPGA\ARM（32位）+Z32)实现简单的密码引擎，能够提供对称密码算法、非对称密码算法等的密码服务   * 实验五   网站设计: 基于JSP+Servlet能够实现简单的电子公文传输和处理网站设计，在Servlet中完成简单的业务逻辑设计，通过Web中间件搭建并发布Web网站。   * 实验六   Web服务器：实现Web服务器，可以解析简单的HTTP协议，包含常见的请求和响应格式，能解析、显示静态HTML内容，能完成CGI动态功能。   * 实验七   密码系统应用（电子公文系统设计）：对电子公文系统进行威胁建模，安全性分析和安全性设计。   *  实验八   网络层密码机（IPSec VPN设计）：基于Openswan，设计和实现IPSec VPN。  **其它要求**：  ★要求提供硬件的原理图，PCB；  ★制造厂商出具的售后服务承诺函； |  |
| 28 | 竞赛支持设备 | * 无线抢答器：支持不低于十组 * 评分器：300台 * 评分器主机：一台 * 无线AP：支持不少于256客户端 |  |

# 8、服务及培训要求

## 8.1 售后服务

本项目内所有硬件设备提供质保期不少于3年，质保期内免费保修；本项目内软件产品，免费提供升级，提供技术支持与维护，提供5×8小时服务。

要求提供源代码的，质保期内免费提供源码更新升级，以便于师生掌握最新的技术。

根据学校师生使用意见，三年质保期内提供实验指导书实验项目的增加、改进和更新服务。

要求提供攻防对抗平台用户管理手册，手册要包括教师管理系统应用说明，包括云资源功能使用说明，包括云调度功能使用说明，包括靶场设计文档，靶场过关使用说明，靶场项目不少于5.2要求的靶场项目。

要求提供计算机取证实验指导书，指导书内容必须包括实验原理，实验目的，实验步骤，实验总结，实验项目内容不少于5.1要求实验项目。

要求提供信息安全系统设计实验箱实验指导书，指导书内容必须包括实验原理、实验目的、实验步骤、实验总结，实验项目不少于技术需求表第27项目实验内容。

## 8.2 技术培训要求

**8.2.1培训内容与课程要求**

（1）所购买设备、软件的性能、安装、配置、使用、常见故障排除的培训，系统环境的配置、维护以及扩展技术等内容。

（2）提供网络攻防靶场培训，要求至少提供20套靶场内容培训；

（3）提供计算机取证培训，要求提供系统使用培训，培训实验项目少于20个；

（4）提供信息安全系统设计实验箱使用培训，至少提供5个实验的培训；

（5）要求质保期内每年免费提供一次校内网络攻防大赛服务；

**8.2.2培训要求**

（1）培训至少5人，每人不少于6学时。

（2）要求提供靶场制作过程，至少培训5名教师；

# 9、其它要求

投标人在投标时需出示单兵过关云资源靶场系统、单兵过关竞赛系统、红蓝对抗竞赛系统、WEB后门代码检测系统、计算机取证系统管理系统、无线攻防渗透测试实训系统、信息安全系统设计实验箱“制造厂商出具的开放源代码承诺函”。

投标人在投标时需出示单兵过关云资源靶场系统、单兵过关竞赛系统、红蓝对抗竞赛系统、WEB后门代码检测系统、计算机取证系统管理系统、无线攻防渗透测试实训系统、信息安全系统设计实验箱“制造厂商出具的售后服务承诺函”，加盖制造厂商公章。

## 制造厂商出具的开放源代码承诺函

致：

我们是按法律成立的一家制造商，主要营业地点设在。

我方就本次投标有关事项郑重承诺如下：

1. 由我方制造的单兵过关云资源靶场系统、单兵过关竞赛系统、红蓝对抗竞赛系统、WEB后门代码检测系统、计算机取证系统管理系统、无线攻防渗透测试实训系统、信息安全系统设计实验箱无偿开放源代码，满足师生对实验和研究的需要，源代码提供的功能不低于实际产品提供的功能和配套实验项目。
2. 我方提供的产品源代码属于我方的商业机密，采购人对我方负有保密责任；采购人获得的源代码仅限于教学、实验和研究，不得再编译后进行商业化销售，不得以任何形式、任何理由泄露给第三方。
3. 若我方授权的代理商中标，我方将在3日内提供产品源代码至采购人指定地点，现场进行源代码编译及真实性认证。认证通过后签订合同，如我方未能提供产品源代码或认证不通过，自愿放弃签订合同并承担相应责任。
4. 本公司对上述承诺的真实性负责。如有虚假，将依法承担相应责任。

制造厂商名称（公章）：

法定代表人或授权代理人（签字）

日期：年月日

**第二包：**

## ．1、采购清单

|  |  |  |
| --- | --- | --- |
| **序号** | **产品名称** | **数量** |
| 1 | 安全访问网关服务器 | 1 |
| 2 | 云平台主管服务器 | 1 |
| 3 | 云桌面资源服务器 | 4 |
| 4 | 资源池宿主服务器 | 2 |
| 5 | 三层交换机 | 2 |
| 6 | 二层交换机 | 4 |
| 7 | 瘦客户机 | 30 |
| 8 | 云桌面系统 | 1 |
| 9 | 虚拟化终端安全管理系统 | 1 |
| 10 | 安全管理平台 | 1 |

## 2．建设目标

### 2.1项目建设总体目标

1.虚拟化终端安全管理系统

虚拟化终端安全管理系统能够有效解决虚拟化应用环境下的终端安全问题，以虚拟机为核心保护对象进行全面管控，从系统安全、数据安全、安全监控和安全审计四个层面实现安全防护，保障虚拟桌面终端和信息资产的安全。

2.云安全管理平台

云安全管理平台是以资产(包括泛终端、网络设备、防火墙等)为核心，以安全事件管理为关键流程，采用安全域划分的思想，建立一套实时的云资产风险模型，协助管理员进行事件分析、风险分析、预警管理和应急响应处理的集中安全管理系统。

### 2.2项目建设计划

项目实施主要完成：

1.云基础设施购置：

购买云平台主管理服务器、平台安全访问网关服务器、资源池宿主服务器、桌面及应用网交换机、存储网交换机、应用/管理网交换机、瘦客户机等设备。

2.云平台搭建；

3.虚拟化终端安全管理系统实施：

系统由虚拟化安全管理中心、安全虚拟机、虚拟机安全代理、虚拟化服务器安全代理四个部分组成，从虚拟机外部到虚拟机内部实现对虚拟化桌面的安全保护。

4.云安全管理平台实施：

安全管理平台的设计模块包括：安全事件采集中心、安全事件分析中心、安全事件处理中心、云终端管理平台、终端监控中心、通告平台。

### 2.3建设预期目标

虚拟化安全管控研究生实验平台面对虚拟化环境中的各种安全问题，研究虚拟化信息系统安全管理、安全防护及监控，重点监控电子政务系统内的云平台及云桌面安全，培养社会急需的云计算虚拟化安全学科人才，满足社会对云环境安全人才的需求。

## 3．投标货物参数及数量

### 3.1招标设备参数及数量（硬件部分）

| **序号** | **设备名称** | **参数** | **数量** |
| --- | --- | --- | --- |
| 1 | 安全访问网关服务器 | 1、规格： 2U机架式服务器  2、处理器：核数≥六核，主频≥2.40GHz  3、内存：≥4\*8GB；RDIMM；ECC；≥16条扩展插槽  4、硬盘：≥3块；≥300GB；≥10000转  5、RAID功能：支持0/1/5 RAID级别  6、网卡：标配千兆以太网控制器≥2个，独享的管理端口≥1个  7、配件：DVD-RW光驱；USB键盘鼠标；机架安装滑动导轨  8、电源：电源输出功率≥1100W；冗余电源  9、具有支持TCG1.2规范的TCM可信模块，能够与现有TCM加密设备实现加解密交互。  10、提供制造商出具的三年售后服务承诺函 | 1 |
| 2 | 云平台主管服务器 | 1、规格： 2U机架式服务器  2、处理器：核数≥六核，主频≥2.40GHz  3、内存：≥4\*8GB；RDIMM；ECC；≥16条扩展插槽  4、硬盘：≥3块；≥300G；15000转  5、RAID功能：支持0/1/5 RAID级别  6、网卡：标配千兆以太网控制器≥2个，独享的管理端口≥1个  7、配件：DVD-RW光驱；USB键盘鼠标；机架安装滑动导轨  8、电源：电源输出功率≥550W；冗余电源  9、具有支持TCG1.2规范的TCM可信模块，能够与现有TCM加密设备实现加解密交互。  10、提供制造商出具的三年售后服务承诺函 | 1 |
| 3 | 云桌面资源服务器 | 1、规格： 2U机架式服务器  2、处理器：核数≥十核，主频≥2.3GHz  3、内存：内存：≥128GB  4、硬盘：普通硬盘≥6块；≥900GB；≥15000转；固态硬盘≥480GB  5、RAID功能：支持0/1/5 RAID级别  6、网卡：标配千兆以太网控制器≥2个，独享的管理端口≥1个  7、配件：DVD-RW光驱；USB键盘鼠标；机架安装滑动导轨  8、电源：电源输出功率≥750W；冗余电源  9、具有支持TCG1.2规范的TCM可信模块，能够与现有TCM加密设备实现加解密交互。  10、提供制造商出具的三年售后服务承诺函 | 4 |
| 4 | 资源池宿主服务器 | 1、规格： 2U机架式服务器  2、处理器：核数≥八核，主频≥2.6GHz  3、内存：内存：≥128GB  4、硬盘：硬盘：≥6块；≥600G；≥15000转  5、RAID功能：支持0/1/5 RAID级别  6、网卡：标配千兆以太网控制器≥2个，独享的管理端口≥1个  7、配件：DVD-RW光驱；USB键盘鼠标；机架安装滑动导轨  8、电源：电源输出功率≥750W；冗余电源  9、具有支持TCG1.2规范的TCM可信模块，能够与现有TCM加密设备实现加解密交互。  10、提供制造商出具的三年售后服务承诺函 | 2 |
| 5 | 三层网络交换机 | 类型：三层交换机  端口：10/100/1000Base-T以太网端口数量≥24个；1000Base-X SFP千兆以太网端口数量≥4个  交换容量：≥256Gbps  ★提供支持防雷等级≥8KV第三方测试报告  需提供三年以上原厂售后服务承诺函 | 2 |
| 6 | 二层网络交换机 | 类型：二层交换机  端口：10/100/1000Base-T 以太网端口数量≥24个；  交换容量≥256Gbps  需提供三年以上原厂售后服务承诺函 | 4 |
| 7 | 瘦客户机 | CPU：优于Intel Celeron CPU 1037U 1.8GHz  内存：≥1G RAM，  存储：≥8G ROM，  网络接口：≥1Gb，  视频接口：至少支持VGA，HDMI  其他接口：USB接口数量≥4，具有标准音频输入输出接口  显示器：23.6寸以上液晶  USB鼠标及键盘 | 30 |

### 3.2定制设备参数及数量（软件部分）

本次采购软件涉及二次开发，投标人需提供软件接口总体框架说明文档、接口描述文档、接口调用代码案例，代码案例要覆盖所有软件接口。

| **序号** | **设备名称** | **参数** | **数量** |
| --- | --- | --- | --- |
| 1 | 云桌面系统 | **基础性能指标要求：**  1.虚拟机:单台虚拟机vCPU分配数量范围至少为1-16；单台虚拟机内存分配范围至少为1GB-32GB；虚拟机I/O读写速度达到同等配置物理机I/O读写速度的90%以上。  2.桌面虚拟机创建:基于桌面模板的虚拟机创建方式，对于10GB磁盘的虚拟机，虚拟机的创建时间不超过2分钟。  3.桌面虚拟机高可用调度:资源池支持至少50个物理节点的调度性能，当任意物理服务器发生故障时，自动调度虚拟机恢复运行时间不超过3分钟；支持同时运行虚拟机数量不得低于160个。  **基础功能指标要求：**  1.查看、浏览物理机及虚拟机信息，对物理机及虚拟机进行基本操作：  可以浏览、查看详细（包括物理机的CPU、内存、磁盘、网卡及物理机上运行的虚拟机列表信息）、维护模式管理、认证管理、启动/停止/删除物理机、监视物理机的实时运行状态等。  对虚拟机进行启动、停止、暂停、激活、同步、删除、远程控制等基本操作。  2.虚拟机模板管理及虚拟机模板数据安全  可以对虚拟机模板进行管理，包括浏览模板列表、查看模板详细信息、克隆虚拟机、快速复制虚拟机、模板导入、模板库初始化、模板检查等功能。  能支持虚拟机模板数据加密，保护虚拟机模板数据安全。  ★3.虚拟机不停机迁移  支持采用不同存储的虚拟机在线不停机从当前物理主机迁移到其它物理主机：(1)将SAN存储中的虚拟机迁移到物理主机本地磁盘中;(2)将物理主机本地磁盘中的虚拟机迁移到SAN存储中;(3)将物理主机本地磁盘中的虚拟机迁移到另一物理主机本地磁盘中;(4)将SAN存储中的虚拟机迁移到另一SAN存储中  4.支持采用不同存储的停机状态的虚拟机从当前物理主机迁移到其它物理主机：(1)将SAN存储中的虚拟机迁移到物理主机本地磁盘中;(2)将物理主机本地磁盘中的虚拟机迁移到SAN存储中;(3)将物理主机本地磁盘中的虚拟机迁移到另一物理主机本地磁盘中;(4)将SAN存储中的虚拟机迁移到另一SAN存储中  5.支持虚拟桌面对快照的创建和管理，虚拟桌面能够通过快照恢复到创建快照的时间点状态  #6.支持虚拟桌面在物理主机故障时，在2分钟内自动调度恢复到其它物理主机中运行  7.能够设置告警触发的条件阀值，包括：CPU占用率、内存占用率、磁盘剩余空间、网络流量，能对告警事件进行分级。  ★8.根据文件、目录等进行策略设置控制虚拟机逃逸行为，对虚拟机逃逸行为进行监控。  #9.能提供对物理主机、虚拟机的CPU占用率、内存占用率、磁盘I/O、网络I/O等实时性能监控和历史数据监控  10.提供基于安全访问网关的虚拟机远程访问管理，提高虚拟化基础架构系统的整体安全性，简化虚拟机管理  11.支持动态资源扩展功能，可根据业务系统负载，动态添加虚拟机的CPU和内存资源，并且还支持通过负载均衡设备联动，来动态扩展集群内的虚拟机资源，来应对业务系统访问压力，当访问高峰过后，可以动态回收虚拟机资源  12.通过在管理平台拖拽虚拟网元设备和连线的操作完成拓扑的构建，以快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个虚拟网元设备实现统一的管理  **编程接口指标：**  提供云平台的主流编程接口。  **源代码指标：**  提供云桌面系统源代码，源代码所实现的功能要与对云桌面系统的功能和性能要求一致。  需提供原厂上门安装服务承诺及三年以上售后服务承诺书。 | 1 |
| 2 | 虚拟化终端安全管理系统 | **基础功能指标：**  无代理技术，即无需在每个虚拟化终端中安装Agent就能够实现安全功能。  1.拥有自主产权；管理模式支持B/S架构；虚拟机终端安全管理模式支持无代理和轻代理相结合。  2.虚拟机管理  提供基于任务管理，针对不同虚拟机下发不同的任务；支持虚拟化软件应用环境VMware、Citrix；支持两种以上国内虚拟化软件应用环境。  3.补丁管理：  提供对虚拟机模板的补丁检测和更新；提供对虚拟机在线补丁检测和更新。  #4.支持启发式文件分析技术，通过分析操作系统的特定关键文件，识别出于系统安全性相关的配置和组件，评估系统安全状态，及时发现潜在的安全隐患  5.支持对虚拟机安全配置、安装软件、服务进行检查  6.支持无代理文件扫描技术，能够对虚拟机磁盘进行扫描、分析，还原虚拟磁盘上的文件系统，及时发现企业重要数据的存储情况；  ★7.支持无代理在线、离线虚拟机涉密信息检测功能；提供基于关键字、文件类型的涉密信息检测功能。  ★8.支持无代理技术对虚拟机违规软件的检测  无代理方式对在特定环境下（如涉密环境）的虚拟机违规软件（不允许安装的软件）检测， 违规软件库通过管理端软件维护。  9.资源监视  支持实时监视虚拟化服务器资源使用状况，及时发现资源过载或资源闲置并告警，提供管理员以便合理资源分配、提示资源利用率；实时监视虚拟机配置变化情况，确保虚拟机配置的安全性；实时监视虚拟机资源使用状况，并及时发现资源过载或闲置情况，为管理人员合理资源分配提供决策依据，以便提升资源利用率。  10.资产管理  能够对虚拟化服务器、虚拟机等的软硬件资产进行统一管理，监控软硬件资产信息，发现资产变更及时告警。  11.安全告警  支持对违反安全策略的行为进行实时告警；支持对告警事件进行统计；告警方式至少包括邮件、短信。  ★12.支持无代理文件扫描技术，通过安全虚拟机来实现对虚拟机的安全扫描，通过对虚拟机磁盘进行扫描、分析，还原虚拟磁盘上的文件系统。  ★13.支持无代理技术实现对虚拟机磁盘操作系统特定关键文件进行分析，识别出于系统安全性相关的配置和组件，评估虚拟机系统安全状态。  **编程接口指标：**  **1**.提供虚拟机资产查询接口  硬件资产至少包括：CPU、内存、硬盘、网卡。  软件资产至少包括：已安装软件（软件名称、版本、安装目录、安装时间）；已安装补丁（补丁名称、补丁级别、补丁描述、发布日期）。  2.虚拟机硬件资源利用率查询接口  提供虚拟机硬件资源利用率实时查询，至少包括：CPU、内存、磁盘、网络。  3.虚拟机健康体检结果查询接口  提供虚拟机健康体检查询接口，至少包括以下项目的检查结果：启动项、垃圾检查、启用远程注册表编辑、系统版本、共享资源、guest用户禁用、IE检查、单启动系统、安全启动配置项、启动项配置正常、快捷方式小箭头、隐藏文件、文件夹选项、组策略、远程桌面启用  4.虚拟机敏感信息检查结果查询接口  提供虚拟机敏感信息检查接口，至少包括以下项目的检查结果：物理光驱、usb使用痕迹、便携设备、打印机信息、无线设备、弱口令、应用程序日志、IE加载项、系统日志信息、已安装补丁、开关机信息、共享列表、启动项、启动服务、账户信息、硬盘信息、硬件信息、网卡信息、分区信息、软件信息、操作系统、浏览器使用痕迹、上传下载痕迹、FTP访问、IM使用痕迹、文件操作记录、敏感词检查、用户策略、组策略、密码帐号策略、审核策略、用户权限分配。  5.虚拟机补丁信息检查接口  提供虚拟机补丁信息检查接口，至少包括：未修复补丁、已修复补丁、已忽略补丁。  6.系统的事件告警接口  提供系统告警信息查询接口，至少包括以下类型告警：健康体检监控、系统组件监控、涉密检查监控、cpu使用率告警、内存使用率告警、网速监控、硬件资产监控。  ★投标人需提供软件接口总体框架说明文档、接口描述文档、接口调用代码案例，代码案例要覆盖所有软件接口。  **源代码指标：**  提供虚拟化终端安全管理系统源代码，源代码所实现的功能要与对虚拟化终端安全管理系统的功能和性能要求一致。  ★需提供原厂上门安装及培训服务承诺书  ★需提供三年以上售后服务承诺书。 | 1 |
| 3 | 安全管理平台 | **基础功能指标：**  1.支持网络拓扑发现，自动生成网络拓扑图，支持分层显示和和全局显示两种展现方式。  #2.支持B/S架构，通过浏览器登录系统，无需单独安装客户端；支持SSL加密模式访问安全管理平台；全部功能提供联机帮助文档；支持多级部署；  3.可识别、处理多种网络、安全厂家的产品日志，并给出列表。  4.角色权限管理  支持基于角色的分权管理员权限管理；支持用户按角色管理；支持用户和角色的权限管理；可控制每个角色显示不同的功能菜单。  5. 能够根据资产价值、资产弱点和受威胁程度，计算资产安全等级和业务单元（域）安全风险、威胁等级。  ★6.结合虚拟化终端的事件管理及预警  支持按预定义的字段显示事件；安全事件的响应预警方式至少包括：命令行，发送电子邮件，声音，短消息，工单处理；可以根据以下条件选择查看事件：时间，事件名，时间类型，目的地址，源地址，资产号，优先级；支持通过级联实现多级审计与预警管理；支持预警方式至少包括：内网安全软件联动、E-mail邮件、短信。支持系统自动预警和人工手动预警。  7.漏洞扫描  支持导入第三方漏洞扫描报告，至少支持绿盟极光扫描报告；支持将漏洞扫描报告和资产关联；  8.资产脆弱性管理  支持资产脆弱点生命周期管理：新发现、确认、已消除、已防护；支持图形化方式表现资产脆弱性统计报表。  9.能够集中监视网络设备、安全设备、主机、服务器设备运行时间、运行状态、资源（CPU、磁盘、内存）占用情况、网络连接状态、网络流量；支持实时监控,历史数据展示；监控画面表现形式支持：表格、图表。  10.支持以仪表盘的形式显示当前风险值和历史风险平均值；依据风险级别以不同颜色显示在图表中，支持地图化的风险展示；支持自动对超过既定阀值的风险进行报警。  11.资产管理或安全域的威胁及漏洞展示  支持详细终端信息查询,可了解终端最近的使用情况，能够根据事件快速定位到相关责任人；提供软硬件资产录入，支持资产可用性、完整性、保密性管理，支持基于域的资产管理；能够以指标的方式宏观展示终端管理情况；支持以级联方式对事件与终端进行远程管理；能够综合展现终端的基本状况：网络状况,提供终端行为审计、规范管理、统计分析；支持显示资产或安全域在最近一段时间内的风险走势；支持把当前资产或安全域的威胁以列表的形式展示；支持把当前资产或安全域的漏洞以列表的形式展示。  12.工单管理  根据安全事件、告警记录、设备故障产生工单记录；支持工单信息管理、状态跟踪；支持工单提醒功能，通过邮件等方式通知运维人员及时处理工单任务。  ★13.能够详细统计终端的软硬件情况；能够建立纵向的终端管理记录，辅助用户宏观掌握各级终端情况；支持终端报警实时展现和应急响应；能够追踪到终端状况，定位问题终端。  14.知识库管理  知识库分组至少包括：攻击库，漏洞库，补丁库，病毒库；支持对知识库的管理，包括：增加，删除，查询，移动，导入，导出操作。  **编程接口指标：**  1.登录接口  通此接口可以登录,获得相应的登录凭据。  2.获取资产数据接口  能够获得资产的相关信息。  3.获取漏洞信息接口  能够获取漏洞相关信息。  4.工单相关接口  能够获取工单（终端注册的信息）的相关信息。  5.第三方接口  能够通过读取数据库的库表来实现对第三方接口的支持。  ★投标人需提供软件接口总体框架说明文档、接口描述文档、接口调用代码案例，代码案例要覆盖所有软件接口。  **源代码指标：**  提供安全管理平台源代码，源代码所实现的功能要与对安全管理平台的功能和性能要求一致。  需提供计算机信息系统安全专用产品销售许可证及涉密信息系统产品检测证书。  平台厂家具有CMMI3级开发能力。  ★需提供原厂上门安装及培训服务承诺书。  ★需提供三年以上售后服务承诺书。 | 10 |

**注：**在合同签订前，用户方有保留测试的权利。

# 服务及培训要求

1． （1）硬件设备质保期至少三年。

（2）质保期内免费保修、软件升级。

（3）提供技术支持与维护。

2. 技术培训要求

（1）培训总体要求

1. 投标人在投标文件中提出全面的培训计划和课程内容安排，并在合同签定后征得用户方同意后实施。
2. 投标人必须为所有被培训人员提供培训所用的设备检测仪、文字资料和讲义等相关用品。
3. 所有的培训教员必须用中文授课，所有的资料必须是中文书写，除非有其它的协议规定。

（2）培训内容要求

培训内容涉及多个产品的应用，每种培训课程都要求提供全面培训，具体培训内容包括产品的应用、维护，常见故障排除等；中标人应准备培训的软硬件环境。

（3）培训人数、时间、地点、次数要求

投标方须提供10人以上培训，地点在北京电子科技学院内，每次时间不低于4小时，次数不少于10次。

附件2：

中标标的内容：

第一包：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名 称** | **数量** | **所投产品品牌及型号** | **单价** | **小计** |
| 1 | 网络攻防对抗平台硬件设备 | 19 | 品牌：红亚科技  型号：HonyaNMCD200 | ¥22,000 | ¥418,000 |
| 2 | 计算机取证平台硬件设备 | 11 | 品牌：红亚科技  型号：HonyaMMCD300 | ¥23,500 | ¥258,500 |
| 3 | 网络对抗平台管理控系统 | 1 | 品牌：红亚科技  型号：HonyaNADC-MCD v3.0 | ¥43,000 | ¥43,000 |
| 4 | 网络对抗平台云调度系统 | 1 | 品牌：红亚科技  型号：HonyaNADC-DPD v3.0 | ¥43,000 | ¥43,000 |
| 5 | 对抗平台视频直播系统 | 1 | 品牌：红亚科技  型号：HonyaNADC-VMD v3.0 | ¥35,000 | ¥35,000 |
| 6 | 网络攻防对抗检测软件 | 1 | 品牌：红亚科技  型号：HonyaNADC-NIDS v3.0 | ¥38,000 | ¥38,000 |
| 7 | 单兵过关云资源靶场系统 | 8 | 品牌：红亚科技  型号：HonyaNADC-ARE v3.0 | ¥42,000 | ¥336,000 |
| 8 | 红蓝对抗云资源靶场系统 | 8 | 品牌：红亚科技  型号：HonyaNADC-CRE v3.0 | ¥33,000 | ¥264,000 |
| 9 | WEB后门代码检测系统 | 2 | 品牌：红亚科技  型号：HonyaNADC-LOE v1.0 | ¥60,000 | ¥120,000 |
| 10 | 远程安全监控系统 | 2 | 品牌：红亚科技  型号：HonyaNADC-DF500 | ¥18,000 | ¥36,000 |
| 11 | 攻防态势监控终端 | 2 | 品牌：红亚科技  型号：HonyaNADC-EOT | ¥12,500 | ¥25,000 |
| 12 | 对抗平台教师管理系统 | 1 | 品牌：红亚科技  型号：HonyaNADC-TES | ¥12,000 | ¥12,000 |
| 13 | 单兵过关竞赛系统（80并发） | 1 | 品牌：红亚科技  型号：HonyaNADC-RVB | ¥12,000 | ¥12,000 |
| 14 | 红蓝对抗竞赛系统（20队并发） | 1 | 品牌：红亚科技  型号：HonyaNADC-ICT | ¥12,000 | ¥12,000 |
| 15 | 无线攻防渗透测试实训系统 | 1 | 品牌：红亚科技  型号：HonyaNADC-EOS | ¥55,000 | ¥55,000 |
| 16 | 渗透测试工具包 | 1 | 品牌：红亚科技  型号：HonyaNADC-BOX | ¥2,000 | ¥2,000 |
| 17 | 计算机取证系统管理系统 | 1 | 品牌：红亚科技  型号：HonyaCICS-MCD | ¥41,200 | ¥41,200 |
| 18 | 计算机取证系统取证资源系统 | 10 | 品牌：红亚科技  型号：HonyaCICS-LRE | ¥32,600 | ¥326,000 |
| 19 | 计算机取证系统信息管理系统 | 1 | 品牌：红亚科技  型号：HonyaCICS-TES | ¥12,000 | ¥12,000 |
| 20 | 计算机取证系统学生实验系统 | 1 | 品牌：红亚科技  型号：HonyaCICS-EOT | ¥4,500 | ¥4,500 |
| 21 | 计算机取证课程资源包 | 1 | 品牌：红亚科技  型号：HonyaCICS-BlT | ¥4,500 | ¥4,500 |
| 22 | 移动终端 | 10 | 品牌：红亚科技  型号：HonyaS5PC100 | ¥3,000 | ¥30,000 |
| 23 | 路由器 | 1 | 品牌：华为  型号：AR1220-S | ¥3,000 | ¥3,000 |
| 24 | 核心交换机 | 1 | 品牌：华为  型号：S5700-24TP-SI-AC | ¥5,800 | ¥5,800 |
| 25 | 管理中心交换机 | 5 | 品牌：华为  型号：S5700S-28P-LI-AC | ¥2,800 | ¥14,000 |
| 26 | 机柜 | 4 | 品牌：红亚科技  型号：HonyaCLB42-B | ¥3,500 | ¥14,000 |
| 27 | 信息安全系统设计实验箱 | 40 | 品牌：红亚科技  型号：HonyaISES-BOX1200 | ¥10,000 | ¥400,000 |
| 28 | 竞赛支持设备 | 1 | 品牌：上海步频  型号：歩频ST3 | ¥65,500 | ¥65,500 |
| 合计 | | ¥2,630,000 | | | |

第二包：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名 称** | **数量** | **所投产品品牌及型号** | **单价（元）** | **小计（元）** |
| 1 | 安全访问网关服务器 | 1 | 联想/RD450 | 26900 | 26900 |
| 2 | 云平台主管服务器 | 1 | 联想/RD450 | 28000 | 28000 |
| 3 | 云桌面资源服务器 | 4 | 联想/RD450 | 53800 | 215200 |
| 4 | 资源池宿主服务器 | 2 | 联想/RD450 | 56100 | 112200 |
| 5 | 三层交换机 | 2 | 锐捷/RG-S5750-E/P | 14200 | 28400 |
| 6 | 二层交换机 | 4 | 锐捷/RG-2928G-E | 5480 | 21920 |
| 7 | 瘦客户机 | 30 | 深信服/aDesk-STD-200H | 1250 | 37500 |
| 冠捷AOC/236LM00014 | 840 | 25200 |
| 8 | 云桌面系统 | 1 | 深信服/云桌面系统 | 40000 | 40000 |
| 9 | 虚拟化终端安全管理系统 | 1 | 北信源/虚拟化终端安全管理系统 | 55000 | 55000 |
| 10 | 安全管理平台 | 1 | 北信源/安全管理平台V2.0 | 93000 | 93000 |
| 合计 | | 683320（大写：陆拾捌万叁仟叁佰贰拾元整） | | | |

售后服务承诺：

第一包：

自验收合格之日起，对本次采购的所有产品均提供硬**件5年**免费保修、所有软件提供**终身免费**更新服务，终身维护。合同期内我方承担所有系统及设备的正常运行，如由于系统及设备的不正常而导致的后果由我方承担相应责任。在质保期内，同一设备、同一质量问题连续两次维修仍无法正常使用的，须更换同品牌、同型号新器件，并对产品质量实行“三包”服务。

* 本项目所有的硬件设备提供5年质保期，质保期内免费保修；
* 本项目内所有软件产品，终身提供免费升级；
* **5年内**免费提供技术支持与维护，提供7×24小时免费技术服务；
* 要求提供源代码的，质保期内免费提供源码更新升级；
* 根据学校师生使用意见，**五年质保期**内免费提供实验指导书实验项目的增加、改进和更新服务；
* 签订合同后免费提供攻防对抗平台用户管理手册。手册包括教师管理系统应用说明，包括云资源功能使用说明，包括云调度功能使用说明，包括靶场设计文档，靶场过关使用说明，靶场项目不少于招标文件技术需求文件5.2要求的靶场项目；
* 签订合同后提供计算机取证实验指导书，指导书内容包括实验原理，实验目的，实验步骤，实验总结，实验项目内容不少于招标文件技术需求文件5.1要求实验项目；
* 提供信息安全系统设计实验箱实验指导书，指导书内容包括实验原理、实验目的、实验步骤、实验总结，实验项目不少于招标文件技术需求表第27项目实验内容；
* 免费提供设备、软件的性能、安装、配置、使用、常见故障排除的培训；
* 免费提供系统环境的配置、维护以及扩展技术等内容；
* 免费提供网络攻防靶场培训，提供20套靶场内容培训；
* 免费提供计算机取证培训，提供系统使用培训，培训实验项目少于20个；
* 免费提供信息安全系统设计实验箱使用培训，提供5个实验的培训；
* 质保期内每年免费提供一次校内网络攻防大赛服务；
* 免费培训不少5人，每人不少于6学时；

免费提供靶场制作过程培训，至少培训5名教师；

第二包：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 类别 | 公司名称 | 质保年限 | 主要内容 | 备注 | 说明 |
| 制造厂家 | 联想（北京）有限公司 | 三年 | 硬件三年原厂质保，软件三年免费升级 | 无 | 无 |
| 锐捷网络股份有限公司 | 三年 | 硬件三年原厂质保，软件三年免费升级 | 无 | 无 |
| 深圳市深信服电子科技有限公司 | 三年 | 硬件三年原厂质保，软件三年免费升级 | 无 | 无 |
| 北京北信源软件股份有限公司 | 三年 | 软件三年免费升级 | 无 | 无 |
| 供应商 | 北京中天瑞合科技有限公司 | 六年 | 我公司承诺所有硬件六年免费保修、所有软件六年免费保修升级、电话报修后4小时上门服务、12小时内排除故障。  投标人承诺所有硬件过六年免费保修期后按原价维修（按投标货物价格数量表所列价格，更换零部件的按合同签订时的零部件价格）、所有软件过六年免费保修升级期内按按原价的10%进行维修升级，响应速度同保修期响应速度。 | 无 | 详见售后服务和技术支持方案 |