政府采购合同

项目名称：网络安全运维与攻防对抗实训室建设

项目编号：JSZC-320500-JZCG-G2026-0125

采购人（甲方）：苏州职业技术大学

供应商（乙方）：中电鸿信信息科技有限公司

根据《中华人民共和国民法典》和《中华人民共和国政府采购法》等有关法律法规，为明确采购人（甲方）和供应商（乙方）在购销过程中的权利、义务和经济责任，双方遵循平等、自愿、公平和诚实信用原则，经友好协商，同意按照下面的条款和条件订立本合同，以资共同遵守。

一、定义

采购人（以下简称甲方）是指使用财政性资金，通过政府采购方式向供应商购买货物及其相关服务的国家机关、事业单位、团体组织。

供应商（以下简称乙方）是指参加政府采购活动并且中标（成交），向采购人提供合同约定的货物及其相关服务的法人、非法人组织或者自然人。

合同价款是指根据本合同规定乙方在全面履行合同义务后甲方应支付给乙方的价款。

货物是指乙方根据本合同规定须向甲方提供的各种形态和种类的物品，包括原材料、设备、产品（包括软件）及相关的其他备品备件、工具、手册及其他技术资料和材料等。

服务是指根据合同规定乙方应承担的与供货有关的辅助义务，比如运输、保险以及其他伴随服务，比如安装或指导安装、调试以及送货上门提供技术援助、培训、配合措施、维修响应和合同中规定乙方应承担的其他义务。

损失是指合同一方因不履行合同义务而导致另一方及第三方的各种损失的费用，还包括守约方为减轻损失或维护权利而需支付的各种调查费用、车旅费用、律师费用等。

二、组成合同的文件

本合同与下列文件一起构成合同文件，如下述文件之间有任何抵触、矛盾或歧义，应按以下顺序解释：

1. 政府采购合同及其变更、补充协议

2. 中标（成交）通知书

3. 投标（响应）文件

4. 招标（采购）文件

5. 国家法律、行政法规和规章制度规定或合同约定的作为合同组成部分的其他文件

三、合同标的

序号	货物（服务）名称	品牌、规格型号	单位	数量	交货期限	单价	小计金额（元）
1	网络安全教学训练服务器	三六零 IN-AT4120-C-HS-MCE-H-NTL	台	1	自合同签订之日起 30 天内交货并完成安装调试	122000	122000
2	攻防对抗模拟仿真服务器	三六零 IN-AD4020-C-HS-MECE-H-SZL	台	1	自合同签订之日起 30 天内交货并完成安装调试	139000	139000
3	网络安全教学训练平台	三六零 IN-AT4120-C-HS-MCS-NTL	套	1	自合同签订之日起 30 天内交货并完成安装调试	620000	620000
4	攻防对抗竞赛训练平台	三六零 IN-AD4020-C-HS-MSCS-SZL	套	1	自合同签订之日起 30 天内交货并完成安装调试	480000	480000
5	安全防火墙	三六零 HT-8000-FWA200-C-HS-H	台	1	自合同签订之日起 30 天内交货并完成安装调试	52000	52000
6	网络入侵防御设备	三六零 HT-8000-IPST1300-C-HS-H	台	1	自合同签订之日起 30 天内交货并完成安装调试	52000	52000
7	Web 应用防火墙	三六零 HT-8000-WAFR1600-C-HS-H	台	1	自合同签订之日起 30 天内交货并完成安装调试	65000	65000

8	服务器机柜	图腾 G26042H	台	1	自合同签订之日起 30 天内交货并完成安装调试	3000	3000
9	教学电脑	联想 E50h G1t-D844	台	50	自合同签订之日起 30 天内交货并完成安装调试	7400	370000
10	网络交换机	H3CLS-5500V3-54P S-SI	台	4	自合同签订之日起 30 天内交货并完成安装调试	10650	42600
11	多媒体教学软件	极坐标　极坐标智慧教室交互系统软件 V3.0	套	1	自合同签订之日起 30 天内交货并完成安装调试	12000	12000
12	还原软件（含保护卡）	噢易闪电噢易闪电同传保护系统 V8	套	50	自合同签订之日起 30 天内交货并完成安装调试	580	29000
投标总报价：人民币　1986600　元							

四、合同总价款及支付

1. 合同总价款：大写人民币 壹佰玖拾捌万陆仟陆佰 元，小写￥ 1986600 元。合同总价款范围：合同总价应包括完成设备的供应、安装、调试、检测、总包管理、施工配合以及最长质保期内的维修、保养等招标内容所需的所有设备、材料、验收、劳务、服务等应有费用；中华人民共和国根据现行税法征收的与本合同有关的一切税费。合同总价款应与中标（成交）结果一致。乙方为履行本合同而发生的所有费用均应包含在合同价款中，甲方不再另行支付其他任何费用。

对于甲方在招标文件中所要求的及乙方在投标文件和合同中所承诺提供的功能，乙方应无条件提供，由于设计及其他原因所造成的额外费用由乙方自行承担。

2. 付款方式：

分期付款：合同签订完毕生效后，甲方一次性向乙方支付合同总价的 30%作为预付款。待全部货物安装到位，经调试、验收合格后，乙方将合同金额 5%的履约保证金缴纳至甲方指定账户，且提供下列 A、B、C、D 材料后 30 个工作日内，甲方按合同总价向乙方支付合同

余下的全部货款。质保期满后，且无质量问题，乙方向甲方项目建设单位提出书面申请，待甲方建设单位签字同意支付后，甲方一个月内退回履约保证金（无息）。

A、合格销售发票

B、甲方签收后的送货回单

C、履行验收报告单

D、履约保证金缴纳凭证

3. 支付方式：银行汇票、转账支票或数字人民币支付价款。乙方账户信息如下：

开户名称：中电鸿信信息科技有限公司

开户银行：中国建设银行南京湖北路支行

银行账号：32001881436059000588

数字人民币账户（数币钱包 ID）:【0052282693313414】

五、合同履行

1. 合同履行期限：合同签订后___30___日内完成所有货物的供货、安装及调试。

2. 履约地点：乙方交货至甲方指定地点，所发生的运输等费用及货物的损坏造成的损失由乙方承担。

3. 履约担保：是否收取履约保证金 ☑是 □否

收取履约保证金形式：待全部货物安装到位，经调试、验收合格后，乙方将合同金额5%的履约保证金缴纳至甲方指定账户。

质保期满后，且无质量问题，乙方向甲方项目建设单位提出书面申请，待甲方建设单位签字同意支付后，甲方一个月内退回履约保证金（无息）。

收取履约保证金金额：合同金额的 5%

4. 如采购文件要求中标（成交）供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。按照《江苏省财政厅 国家金融监管总局江苏监管局 江苏省地方金融监督管理局关于在全省政府采购领域推行电子履约保函(保险)的通知》和相关法律法规规定，采购人如向中标（成交）供应商收取履约保证金的，供应商可以以履约保函(保险)的形式代替提供履约保证金。

六、履约验收

甲方将根据《江苏省财政厅关于印发<江苏省政府采购履约验收管理办法>的通知》（苏

财规〔2024〕7号）相关要求，成立验收小组，负责采购项目履约验收具体工作。

1. 验收组织方式：□验收小组验收

2. 验收的实施主体：甲方

3. 履约验收时间：所有货物到场后5日内进行初步验收，初步验收通过后，所有货物安装、部署、调试、试用完成并符合要求后，供应商提出验收申请之日起10日内组织验收。

4. 履约验收方式：□一次性验收

☑分期（段）验收：货到后，招标人对中标人提交的货物依据采购文件上的技术规格要求和国家有关质量标准进行现场初步验收。初步验收通过后，所有货物安装、部署、调试、试用完成后，依据国家、行业、地方现行相关标准及规范、政府采购合同、本项目采购文件及成交商响应文件进行验收。中标人需要配合招标人进行系统的整体验收，完成本项目的验收和交付，并提交本项目全部技术文档及其他相关全部资料等。

5. 履约验收的内容：货到后，招标人对中标人提交的货物依据采购文件上的技术规格要求和国家有关质量标准进行现场初步验收。包括但不限于“货物清单”、“品牌、型号、规格、数量及外观质量”、“技术、性能、指标”、“运行状况及安装调试”、“质量证明文件”、“售后服务承诺”、“安全标准”、“合同履约时间、地点、方式”等内容。外观、说明书须符合采购文件技术要求，并进行相应的功能测试。招标人对中标人提供的货物在使用前进行调试时，中标人需负责安装并培训招标人的使用操作人员，并协助招标人一起调试，直到符合技术要求，招标人才做最终验收。

6. 履约验收标准：（1）乙方所供产品的规格、数量符合招标文件、乙方投标承诺及采购合同约定的要求；

（2）所供产品的外观完好，无严重碰撞、表皮脱落、五金件生锈等明显瑕疵；

（3）所供产品结构牢固，无安全隐患；

（4）所有产品均已运输至指定地点，并安装调试完毕；

（5）乙方须提供相关设备的检测报告、软件功能测评报告；

（6）乙方书面通知甲方所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经甲方认定后方可执行；

（7）其他验收标准依据《江苏省财政厅关于印发〈江苏省政府采购履约验收管理办法〉的通知》（苏财规〔2024〕7号）及招标文件相关规定执行。

7. 履约验收其他事项：

七、甲方的权利义务

1. 签署合同后，甲方应确定项目负责人（或项目联系人），负责与本合同有关的事务。甲方有权对乙方的履约行为进行检查，并及时确认乙方提交的事项。甲方应当配合乙方完成相关项目实施工作。

2. 甲方有权要求乙方按时提交各阶段有关安排计划，并有权定期核对乙方提供货物数量、规格、质量等内容。甲方有权督促乙方工作并要求乙方更换不符合要求的货物。

3. 甲方有权要求乙方对缺陷部分予以修复，并按合同约定享有货物保修及其他合同约定的权利。

4. 甲方应当按照合同约定及时对交付的货物进行验收，未在合同约定的期限内对乙方履约提出任何异议或者向乙方作出任何说明的，视为验收通过。

5. 甲方应当根据合同约定及时向乙方支付合同价款，不得以内部人员变更、履行内部付款流程等为由，拒绝或迟延支付。

6. 国家法律法规规定及合同约定应由甲方承担的其他义务和责任。

八、乙方的权利和义务

1. 签署合同后，乙方应确定项目负责人（或项目联系人），负责与本合同有关的事务。

2. 乙方应按照合同要求履约，充分合理安排，确保提供的货物及相关服务符合合同有关要求。接受项目行业管理部门及政府有关部门的指导，配合甲方的履约检查及验收，并负责项目实施过程中的所有协调工作。

3. 乙方应为本项目配备专门的实施团队，团队组成及资质要求如下：

（a）项目经理 1 人：负责跟踪推进项目管理工作和问题的协调落实，具备信息系统项目管理、系统规划、信息安全、通信专业相关等方面的技术专业，具有相关工作管理经验；

（b）技术负责人 1 人：负责项目具体实施技术方面工作，具备系统集成、网络工程、信息系统安全保障等方面的技术专业，具有相关工作经验；

（c）运维负责人 1 人：负责项目具体运维方面工作，具备系统架构、软件测试、信息安全等方面的技术专业，具有相关工作经验；

（d）其他实施团队成员不少于 3 人，具备网络规划、数据库等方面的专业技术。

乙方应本着认真负责的态度组织项目团队，合同附件中列明的项目组主要成员名单，未

经甲方书面同意不得随意更改。

4. 乙方有权根据合同约定向甲方收取合同价款。

5. 国家法律法规规定及合同约定应由乙方承担的其他义务和责任。

九、货物包装、运输、保险和交付要求

1. 本合同涉及商品包装、快递包装的，除合同另有约定外，包装应适应远距离运输、防潮、防震、防锈和防野蛮装卸等要求，确保货物安全无损地运抵合同约定的指定现场。

2. 除另有约定外，乙方负责办理将货物运抵本合同规定的交货地点，并装卸、交付至甲方的一切运输事项，相关费用应包含在合同价款中。

3. 货物保险要求（如有）按合同约定执行。

4. 除采购活动对商品包装、快递包装达成具体约定外，乙方提供产品及相关快递服务涉及具体包装要求的，应不低于《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》标准，并作为履约验收的内容，必要时甲方可以要求乙方在履约验收环节出具检测报告。

5. 乙方在运输到达之前应提前通知甲方，并提示货物运输装卸的注意事项，甲方配合乙方做好货物的接收工作。

6. 如因包装、运输问题导致货物损毁、丢失或者品质下降，甲方有权要求降价、换货、拒收部分或整批货物，由此产生的费用和损失，均由乙方承担。

十、质量标准和保证

本项目经甲方验收合格后，乙方将提供 三 年（其中教学电脑五年） 质量保证期。

1. 质量标准

（1）本合同下提供的货物应符合合同约定的品牌、规格型号、技术性能、配置、质量、数量等要求。质量要求不明确的，按照强制性国家标准履行；没有强制性国家标准的，按照推荐性国家标准履行；没有推荐性国家标准的，按照行业标准履行；没有国家标准、行业标准的，按照通常标准或者符合合同目的的特定标准履行。

（2）采用中华人民共和国法定计量单位。

（3）乙方所提供的货物应符合国家有关安全、环保、卫生的规定。

（4）乙方应向甲方提交所提供货物的技术文件，包括相应的中文技术文件，如：产品

目录、图纸、操作手册、使用说明、维护手册或服务指南等。上述文件应包装好随货物一同发运。

2. 保证

（1）乙方应保证提供的货物完全符合合同规定的质量、规格和性能要求。乙方应保证货物在正确安装、正常使用和保养条件下，在其使用寿命期内具备合同约定的性能。存在质量保证期的，货物最终交付验收合格后在合同规定或乙方书面承诺（两者以较长的为准）的质量保证期内，本保证保持有效。

（2）在质量保证期内所发现的缺陷，甲方应尽快以书面形式通知乙方。

（3）乙方收到通知后，应在 30 分钟内响应，2 小时内到达现场，8 小时内提出解决方案并采取相应措施保障甲方正常使用，免费维修或更换有缺陷的货物或部件。

（4）在质量保证期内，如果货物的质量或规格与合同不符，或证实货物是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同规定以书面形式追究乙方的违约责任。

（5）乙方在约定的时间内未能弥补缺陷，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，甲方根据合同约定对乙方行使的其他权利不受影响。

十一、权利瑕疵担保

1. 乙方保证对其出售的货物享有合法的权利。

2. 乙方保证在交付的货物上不存在抵押权等担保物权。

3. 如甲方使用上述货物构成对第三人侵权的，则由乙方承担全部责任。

十二、知识产权保护

乙方对其所销售的货物应当享有知识产权或经权利人合法授权，保证没有侵犯任何第三人的知识产权等权利。因违反前述约定对第三人构成侵权的，应当由乙方向第三人承担法律责任；甲方依法向第三人赔偿后，有权向乙方追偿。甲方有其他损失的，乙方应当赔偿。

十三、保密义务

甲、乙双方对采购和合同履行过程中所获悉的国家秘密、工作秘密、商业秘密或者其他应当保密的信息，均有保密义务且不受合同有效期所限，直至该信息成为公开信息。泄露、

不正当地使用国家秘密、工作秘密、商业秘密或者其他应当保密的信息，应当承担相应责任。

十四、伴随服务

1. 乙方应提供所交付货物的全套技术文件资料，包括产品目录、软件备份、图纸、操作手册、使用说明、维护手册和服务指南等。

2. 乙方还应提供下列服务：货物的现场安装、启动和试运行；提供货物组装和维修所需的工具；在质量保证期内对所交付货物提供运行监督、维修、保养等。

3. 乙方应提供完整的系统培训方案。培训内容包括系统原理、运营管理和故障检测等综合内容，以实际操作培训为主，确保培训人员对设备系统有全面的认识，能熟练地使用这些知识和技巧安全规范地操作、维护网络系统。除上述培训外，乙方还需负责在现场组织对系统的安装、调试和运行进行技术示范和业务指导。乙方应选派具有一定资质和实践经验、且受过专门训练的专业技术人员负责各分项工程的技术培训工作。

4. 上述伴随服务的费用应包含在合同价中，不单独进行支付。

5. 货物的包装、储运、安装按国家有关规定执行。

十五、违约责任

1. 质量瑕疵的违约责任

乙方提供的产品不符合合同约定的质量标准或存在产品质量缺陷，甲方有权要求乙方根据合同要求及时修理、重作、更换，并承担由此给甲方造成的损失。

2. 迟延交货的违约责任

（1）乙方应按照本合同规定的时间、地点交货和提供相关服务。在履行合同过程中，如果乙方遇到可能影响按时交货和提供服务的情形时，应及时以书面形式将迟延的事实、可能迟延的期限和理由通知甲方。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或延期提供服务。

（2）如果乙方没有按照合同规定的时间交货和提供相关服务，甲方有权从货款中扣除误期赔偿费而不影响合同项下的其他补救方法，误期赔偿费具体标准按合同总价*每日千分之四*计算。如果涉及公共利益，且赔偿金额无法弥补公共利益损失，甲方可要求继续履行或者采取其他补救措施。

3. 迟延支付的违约责任

甲方存在迟延支付乙方合同款项的，按甲乙双方具体约定执行。

4. 其他违约责任根据项目实际需要按甲乙双方具体约定执行。

十六、不可抗力

1. 如果乙方和甲方因不可抗力而导致合同实施延误或不能履行合同义务，不应该承担误期赔偿或不能履行合同义务的责任。因乙方或甲方先延误或不能履行合同而后遇不可抗力的情形除外。

2. 本条所述的“不可抗力”系指那些双方无法控制，不可预见的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震以及其他双方商定的事件。

3. 在不可抗力事件发生后，当事方应在十五日内以书面形式将不可抗力的情况和原因通知对方。双方应尽实际可能继续履行合同义务，并积极寻求采取合理的方案履行不受不可抗力影响的其他事项。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。

十七、合同变更、中止与终止

1. 合同的变更

政府采购合同履行中，在不改变合同其他条款的前提下，甲方可以在合同价款 10%的范围内追加与合同标的相同的货物，并就此与乙方协商一致后签订补充协议。

2. 合同的中止

（1）合同履行过程中因供应商就采购文件、采购过程或结果提起投诉的，甲方认为有必要的，可以中止合同的履行。

（2）合同履行过程中，如果乙方出现以下情形之一的：①经营状况严重恶化；②转移财产、抽逃资金，以逃避债务；③丧失商业信誉；④有丧失或者可能丧失履约能力的其他情形，乙方有义务及时告知甲方。甲方有权以书面形式通知乙方中止合同并要求乙方在合理期限内消除相关情形或者提供适当担保。乙方提供适当担保的，合同继续履行；乙方在合理期限内未恢复履约能力且未提供适当担保的，视为拒绝继续履约，甲方有权解除合同并要求乙方承担由此给甲方造成的损失。

（3）乙方分立、合并或者变更住所的，应当及时以书面形式告知甲方。乙方没有及时告知甲方，致使合同履行发生困难的，甲方可以中止合同履行并要求乙方承担由此给甲方造

成的损失。

（4）甲方不得以行政区划调整、政府换届、机构或者职能调整以及相关责任人更替为由中止合同。

3. 合同的终止

（1）合同因有效期限届满而终止；

（2）在甲方因乙方违约而按合同约定采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知，提出终止部分或全部合同。

①如果乙方未能在合同规定的限期或甲方同意延长的限期内提供部分或全部货物。

②如果乙方未能履行合同规定的其他任何义务。

③如果乙方在本合同的竞争或实施中有腐败和欺诈行为。为此，定义如下："腐败行为"是指提供、给予、接受或索取任何有价值的东西来影响采购人员在采购过程或合同实施过程中的行为；"欺诈行为"是指为了影响采购过程或合同实施过程而谎报事实，损害甲方的利益，包括投标人之间串通，人为地使采购活动丧失竞争性，损害甲方所能获得的权益。

如果甲方根据以上的规定，终止了全部或部分合同，甲方可以依其认为适当的条件和方法购买与未提供服务类似的货物，乙方应对购买类似货物所超出的那部分费用负责。并且，乙方应继续履行合同中未终止的部分。

（3）如果乙方破产或丧失清偿能力，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何补救措施的权利。

4. 涉及国家利益、社会公共利益的情形

政府采购合同继续履行将损害国家利益和社会公共利益的，双方当事人应当变更、中止或者终止合同。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。

十八、索赔

1. 甲方有权根据当地国家技术监督局、进出口商品检验局或其他具有法定资格的质检机构出具的检验证书向乙方提出索赔。

2. 如果乙方对缺陷负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）乙方同意退货并用合同规定的货币将货款退还给甲方，并承担由此发生的一切损

失和费用，包括利息、银行手续费、运费、保险费、检验费、仓储费、装卸费以及为保护退回货物所需的其他必要费用。

（2）根据货物低劣、损坏程度以及甲方所遭受损失的金额，经双方商定降低货物的价格。

（3）用符合合同规定的规格、质量和性能要求的新零件、部件或设备来更换有缺陷的部分或修补缺陷部分，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。乙方应相应延长修补和更换件的质量保证期。

3. 如果在甲方发出索赔通知后七天内乙方未作答复，上述索赔应视为已被乙方接受。如乙方未能在接到甲方索赔通知后七天内或甲方同意的延长期限内，按照上述规定的任何一种或多种方式解决索赔事宜并征得甲方同意，甲方有权从应付货款中扣回索赔金额，并拥有对赔偿不足部分进一步索赔的权利。

十九、合同转让和分包

1. 乙方不得将合同转包给其他供应商。涉及合同分包的，乙方应根据采购文件和投标（响应）文件规定进行合同分包。

2. 乙方执行政府采购政策向中小企业依法分包的，乙方应当按采购文件和投标（响应）文件签订分包意向协议，分包意向协议属于本合同组成部分。

二十、争端的解决与法律适用

1. 甲方和乙方应通过友好协商，解决在执行本合同过程中所发生的或与本合同有关的一切争端。如从协商开始十天内仍不能解决，可向有关合同管理部门提请调解。

2. 如果调解不成，双方中的任何一方可向人民法院提起诉讼。诉讼由合同签订地人民法院管辖。

3. 诉讼费由败诉方负担。

4. 因合同部分履行引发诉讼的，在诉讼期间，除正在进行诉讼的部分外，本合同的其它部分应继续执行。

5. 本合同的订立、生效、解释、履行及与本合同有关的争议解决，均适用法律、行政法规。

6. 本合同条款与法律、行政法规的强制性规定不一致的，双方当事人应按照法律、行政

法规的强制性规定修改本合同的相关条款。

二十一、通知

1. 本合同任何一方向对方发出的通知、信件、数据电文等，应当发送至本合同中所约定的通讯地址、联系人、联系电话或电子邮箱。

2. 一方当事人变更名称、住所、联系人、联系电话或电子邮箱等信息的，应当在变更后3日内及时书面通知对方，对方实际收到变更通知前的送达仍为有效送达。

3. 本合同一方给另一方的通知均应采用书面形式，传真或快递送到本合同中规定的对方的地址和办理签收手续。

4. 通知以送达之日或通知书中规定的生效之日起生效，两者中以较迟之日为准。

二十二、合同生效

1. 双方签约人为各自法定代表人或其委托代理人。

2. 本合同系指本文件及其附件中的所有部分，招标（采购）文件、乙方的投标（响应）文件、中标（成交）通知书、乙方在采购过程中的澄清和承诺等为本合同不可缺少的组成部分。

3. 本合同自甲乙双方签字盖章之日起生效。

4. 本合同壹式肆份，甲乙双方各执贰份，各份具有同等法律效力。

5. 本合同应按照中华人民共和国的现行法律进行解释。

6. 合同修改：除甲乙双方签署书面修改、补充协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

7. 本合同签订地为：江苏省苏州市。

甲方（采购人）	乙方（供应商）
单位名称（公章或合同章）	单位名称（公章或合同章）
法定代表人或其委托代理人（签字或签章）	法定代表人或其委托代理人（签字或签章）

签订日期	2026年9月22日	签订日期	2026年9月22日
住所		住所	
联系人		联系人	
联系电话		联系电话	
通信地址		通信地址	
邮政编码		邮政编码	
电子邮箱		电子邮箱	
统一社会信用代码		统一社会信用代码	91320000668382125D
注：涉及联合体或其他合同主体的信息应按上表格式加列。			

附件：设备及软件参数标准

序号	设备名称	技术参数	数量	单位
1	网络安全教学训练服务器	1、CPU：X86 架构，配置≥2 颗处理器，单颗处理器主频≥2.4GHz，单颗 CPU 核数≥16 核 32 线程，单颗 CPU 末级缓存≥24MB，支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O 模块等，与存储部件、网络部件、I/O 部件等组成计算系统；CPU 芯片应符合 GM/T 0008 的相关规定，CPU 和操作系统等关键部件符合安全可靠测评要求； 2、主板：内存插槽数量≥24 个，存储接口支持 SATA、U.2，PCLE 插槽（双路）≥6 个； 3、内存：内存总量≥320G，内存数量≥10 个，内存规则≥DDR4，内存速率≥2666MT/s； 4、硬盘：硬盘容量≥7T，固态盘容量≥3.84T（NVMe≥3.84T），硬盘数量≥1 块，硬盘容量≥4T SATA HDD，硬盘转速≥7200rpm； 5、网络与接口：网口≥4 个千兆 GE，≥1 个 VGA 接口，≥1 个 USB 3.0 接口，独立网卡网口数量≥1GE 网口，支持网络连接、网络访问、数据交换和网络管控功能； 6、电源与散热：配置 1+1 冗余电源支持电源冗余，电源功率≥800W，整机电源模块应具备热插拔功能，支持过流及短路保护的功能，电源能耗符合 GB/T 9813.3 的有关规定，支持风冷散热； 7、整机规格：≥2U 标准机架式，自带可滑动快速/通用导轨，外观零部件紧固无松动，尺寸≥763x447x88mm，工作环境支持 5-45 度，空闲状态噪声 60db，满负载状态 75dB； 8、管理与固件：BMC 基础功能支持 DHCP 设置网络，静态 IP 设置网络，可查看固件版本/内存/主板/处理器和系统时间信息，支持远程关机和重新启动功能，支持通过网络、闪存盘对操作系统、驱动进行升级，支持操作系统备份及还原功能，操作系统支持访问控制、安全审计、网络接入鉴别等功能，具备资源管理、系统管理、性能监控、健康监控、基于网络控制、报警设置功能，物理安全符合 GB 4943.1 的规定，限用物质的限量应符合 GB/T 26572 的要求； 9、安全要求：具备故障检测，内存故障隔离，弱口令字典检查，白名单访问控制，二次鉴别，密码证书安全加密存储，敏感信息安全加密传输等能力，供应商研发过程安全流程可追溯； 10、兼容性要求：内存兼容海力士、美光、长鑫，存储兼容海力士、美光、长鑫，网卡兼容绿联、博通，瑞显，内置或适配符合 PCIe 的功能卡，如网络功能卡、存储功能卡及图形显示功能卡，兼容多种主流生产商的外部设备，包括显示器、键盘、鼠标、闪存盘、移动硬盘、USB 光驱及 KVM 等，使用不同厂商外部设备时系统均能正常识别和安装驱动，数据库兼容达梦、高斯、电科金仓，中间件兼容东方通、宝蓝德、Microsoft，平台兼容华三、华为、紫光等； 12、可靠性要求：m1 值（MTBF 的不可接受值）不得低于 30000h，	1	台

		风扇寿命应不低于 40000h，符合 GB/T 9813.3 和商品包装政府采购需求标准的相关规定； 13、服务要求：提供三年质保，服务响应提供电话、电子邮件、远程连接等多种形式服务，提供产品手册，提供安装工具集驱动安装升级，提供代码迁移工具，提供厂家升级产品软件与扩容服务，含上门服务； 14、供应链保障：供应商提供供应链稳定承诺书，确保产品的部件在产品服务周期内稳定供货，当产品部件出现供应风险时，通知客户并提供对应风险应对方案确保产品的服务保障；		
2	攻防对抗模拟仿真服务器	1、CPU：X86 架构，配置≥2 颗处理器，单颗处理器主频≥2.4GHz，单颗 CPU 核数≥24 核 32 线程，单颗 CPU 末级缓存≥24MB，支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O 模块等，与存储部件、网络部件、I/O 部件等组成计算系统；CPU 芯片应符合 GM/T 0008 的相关规定，CPU 和操作系统等关键部件符合安全可靠测评要求； 2、主板：内存插槽数量≥24 个，存储接口支持 SATA、U.2，PCLE 插槽（双路）≥6 个； 3、内存：内存总量≥384G，内存数量≥10 个，内存规则≥DDR4，内存速率≥2666MT/s； 4、硬盘：硬盘容量≥20T，固态盘容量≥12.84T（NVMe≥4*3.84T），固态盘容量≥1920G（2*960G SATA SSD），硬盘数量≥1 块，硬盘容量≥16T SATA HDD，硬盘转速≥7200rpm；配置≥1 张 RAID 卡，缓存≥1G，支持 RAID0,1,5,10； 5、网络与接口：网口≥4 个千兆 GE，≥2 个万兆光口（含光模块），，≥1 个 VGA 接口，≥4 个 USB 3.0 接口，独立网卡网口数量≥1GE 网口，支持网络连接、网络访问、数据交换和网络管控功能； 6、电源与散热：配置 1+1 冗余电源支持电源冗余，电源功率≥800W，整机电源模块应具备热插拔功能，支持过流及短路保护的功能，电源能耗符合 GB/T 9813.3 的有关规定，支持风冷散热； 7、整机规格：≥2U 标准机架式，自带可滑动快速/通用导轨，外观零部件紧固无松动，尺寸≥763x447x88mm，工作环境支持 5-45 度，空闲状态噪声 60db，满负载状态 75dB； 8、管理与固件：BMC 基础功能支持 DHCP 设置网络，静态 IP 设置网络，可查看固件版本/内存/主板/处理器和系统时间信息，支持远程关机和重新启动功能，支持通过网络、闪存盘对操作系统、驱动进行升级，支持操作系统备份及还原功能，操作系统支持访问控制、安全审计、网络接入鉴别等功能，具备资源管理、系统管理、性能监控、健康监控、基于网络控制、报警设置功能，物理安全符合 GB 4943.1 的规定，限用物质的限量应符合 GB/T 26572 的要求； 9、安全要求：具备故障检测，内存故障隔离，弱口令字典检查，白名单访问控制，二次鉴别，密码证书安全加密存储，敏感信息安全加密传输等能力，供应商研发过程安全流程可追溯； 10、兼容性要求：内存兼容海力士、美光、长鑫，存储兼容海力	1	台

		士、美光、长鑫，网卡兼容绿联、博通，瑞显，内置或适配符合PCIe的功能卡，如网络功能卡、存储功能卡及图形显示功能卡，兼容多种主流生产商的外部设备，包括显示器、键盘、鼠标、闪存盘、移动硬盘、USB光驱及KVM等，使用不同厂商外部设备时系统均能正常识别和安装驱动，数据库兼容达梦、高斯、电科金仓，中间件兼容东方通、宝蓝德、Microsoft，平台兼容华三、华为、紫光等； 12、可靠性要求：m1值（MTBF的不可接受值）不得低于30000h，风扇寿命应不低于40000h，符合GB/T 9813.3和商品包装政府采购需求标准的相关规定； 13、服务要求：提供三年质保，服务响应提供电话、电子邮件、远程连接等多种形式服务，提供产品手册，提供安装工具集驱动安装升级，提供代码迁移工具，提供厂家升级产品软件与扩容服务，含上门服务； 14、供应链保障：供应商提供供应链稳定承诺书，确保产品的部件在产品服务周期内稳定供货，当产品部件出现供应风险时，通知客户并提供对应风险应对方案确保产品的服务保障；		
3	网络安全教学训练平台	（1）平台需采用“一体化云原生架构”设计，训练业务管理平台与云资源管理平台须为统一系统架构、统一后台、统一权限体系、统一UI风格，不接受基于第三方开源云平台通过外挂或二次集成形成的分离式管理架构。平台应支持在同一管理后台内完成用户、实训、教学、能力考核、虚拟机、容器、集群等统一管理与调度，实现业务与资源的一体化联动。 （2）平台应具备基于教学计划的学习引导能力，可通过创建并下发阶段性学习任务，引导学员按预设的教学路径完成学习与实践。支持教员按大纲创建教学计划并下发，学员端可查看个人课表（日/周/月视图），课程支持按类型、状态筛选。教学看板以饼图展示完成率，教员可监控终端、在线答疑、查看实时统计。教学统计覆盖多维度数据并支持下钻个人进度，形成"下发→学习→监督→统计"闭环。 （3）平台应支持通过物理二层交换设备在不同实验场景下复用来构建多个逻辑隔离的子网环境。 （4）平台应提供全局分类配置功能，统一管理课程类别、实验环境镜像类型、操作系统类型、竞赛题目方向及训练类型等元数据信息。 ●（5）支持利用资源库课程资源配置不少于64课时的网络安全课程与不少于24课时的网络安全技术实训课程，课程内容附后。 （6）技能训练体系应覆盖专项训练、竞赛训练（CTF）和实战训练三大类别。专项训练应涵盖SQL注入、反序列化漏洞、命令执行、文件上传漏洞、文件包含漏洞、文件删除漏洞、代码执行等常见安全防线。实战训练应覆盖主流Web应用框架和中间件的漏洞利用场景，技能训练分专项训练、竞赛训练、实战训练三类，	1	套

		专项训练覆盖 SQL 注入、命令执行、文件上传/包含等主要安全防线，实战训练覆盖主流 CMS、中间件及开源靶场演练。知识训练支持单选、多选、判断、填空四种题型，支持独立题库管理。知识题库额外提供不少于 1000 道，技能资源包含实战训练不少于 70 个、专项训练不少于 50 个。 ●（7）平台应提供独立的知识题库管理模块，支持逐题创建和批量导入两种建题方式。题库应支持刷题练习模式，题型覆盖单选题、多选题、判断题、填空题四类；题目按作答状态分为全部、未作答、已作答、错题集四种视图，支持灵活筛选；练习过程中学员可在试题详情页作答，并支持对未掌握题目进行反复练习。知识题库应具备独立的后台维护能力。除平台自带的能力考核题库资源外，知识训练模块需额外提供不少于 1000+题目。 （8）平台应支持虚拟化环境与物理设备的混合组网，通过综合实验场景将现有实体设备资源纳入统一拓扑，教员可根据教学需求自定义虚实互联的复杂网络场景。支持在虚拟拓扑中接入终端类、网络类、安全类三类实体设备，实现虚拟节点与物理节点的互联互通。支持接入第三方品牌的路由器、防火墙及 Web 应用防火墙（WAF）等设备。防火墙应支持透明模式与路由模式两种部署方式；平台可实现内置的防火墙的多种工作模式，支持内置防火墙与路由器节点的路由协议配置，涵盖联通策略、静态路由及 OSPF、RIP、BGP 等主流动态路由协议，配置表单根据协议类型自动适配，降低网络拓扑编排的技术门槛。 （9）平台职业体系应支持将理论课程与技能实训项目进行灵活组合编排，形成混合式培养方案。支持理论与实验课两类课时形态，实验课时可独立维护实验介绍与实验指导双文档，课时支持灵活混合编排，满足理论教学与实操训练一体化管理需求。 （10）系统基于 KVM/QEMU 标准虚拟化体系设计，支持 i440fx、Q35 等主流虚拟芯片组类型，以及 RTL8139、E1000、VirtIO 等标准虚拟网卡模型，主要用于兼容不同操作系统、历史镜像及教学靶机环境。其中 VirtIO 为 KVM 官方推荐的高性能半虚拟化驱动方案，Q35 为支持 PCIe 的现代化虚拟硬件架构。平台同时具备保留传统兼容模式（如 i440fx、IDE、RTL8139），支持靶机镜像类型关联信息查看，支持所有靶机的基础镜像和增量镜像类型，以及类型之间的关联关系的查看，满足网络安全教学、靶场攻防、历史漏洞环境复现等复杂场景需求。靶机支持 SSH、RDP、VNC、noVNC 等不少于 4 种远程访问协议，可灵活配置底层虚拟硬件（芯片组、网卡类型、QGA 功能、硬盘控制器类型），并支持基础镜像与增量镜像的类型划分及关联关系查看，满足多样化实验环境需求。 （11）支持自定义职业岗位体系，可灵活组合课程与技能训练资源构建岗位培养路径，实现理论教学与技能实训的深度融合。 （12）★平台应支持教学训练模式与职业仿真模式的灵活切换，可依据岗位能力评估等级为学员分配对应的职业角色与岗位。平台需提供配套组件，支持不少于 50 名学员并发开展职业场景实训。应具备工单驱动的流程化管理能力，支持以下功能：自动化报告		

		生成、报告在线编辑、资产信息录入、任务分发、报告修订版本追溯、报告预览与下载、在线批注、报告上传、工具箱集成，以及安全事件与告警的关联匹配。 （13）★支持在职业环境中进行告警研判、代码解析、对比分析、上下文关联、绘制表格图形等操作，能通过 AI 赋能，支撑职业环境中的工作有序开展，包括安全政策查询、处罚案例查询等基本安全知识问答、推理能力、基础统计能力。		
4	攻防对抗竞赛训练平台	（1）平台应采用统一集成架构设计，竞赛业务管理模块与云资源管理模块须基于同一技术底座实现，共享统一的管理后台、权限体系与界面规范，不接受通过接口对接或组件拼装形成的分离式管理架构。平台应支持在同一管理后台内完成用户管理、竞赛管理、安全工具、漏洞管理、靶机管理、场景管理、实例运维、集群管理、网络管理等全部模块集成于统一 Web 界面，无需跨系统跳转或切换后台，操作及入口完全统一，后台内完成用户、竞赛、安全工具、漏洞管理、虚拟机、容器、集群等统一管理与调度，实现业务与资源的一体化联动。 （2）平台应支持虚拟网络的统一管理。网络管理功能分为外部网络配置与赛事网络配置两部分。外部网络配置展示平台对外服务的实时 IP 信息及可用映射端口范围。赛事网络配置涵盖平台内部虚拟网络、解题赛事网络、攻防赛事网络及靶场赛事网络等类型。用户可根据部署环境需求自定义赛事网络规划，亦可采用系统默认配置。 （3）★平台应支持国内 CNVD、CNNVD 等主流权威漏洞数据库的统一接入、汇聚与关联，实现多源漏洞数据的标准化管理。其中 CNVD 漏洞数据收录规模应达到 15W 条量级以上，CNNVD 漏洞数据收录规模应达到 20W 条量级以上，平台漏洞数据总量应能满足攻防对抗训练场景的实际使用需求。 （4）平台应支持安全竞赛题目管理。对于解题赛场景类题目，应支持信息预览、在线验证测试，支持一键启停题目环境并进行在线访问调试，支持对运行实例执行销毁和延时操作，以及 PushFlag 提交验证。对于攻防赛场景类题目，应同样支持信息预览与在线验证测试，支持启停题目环境、在线调试、实例销毁与延时，并具备 Checker 检测和 Flag 提交验证能力。 （5）解题赛模式应提供赛事控制、题目运维、实例管理、流量管理、网络详情、公告管理、选手管理、展示管理等赛事运维功能。应支持开始、暂停、继续、结束、延时等操作，以及数据清空和虚拟资源回收的赛事过程控制；应支持地址查看、实例重置、远程登录、Flag 查看及自动化 Flag 提交验证的实例运维功能；应支持排行榜、统计数据、解题报告（WP）的前台展示控制，以及 3D 态势展示等元素的配置管理功能。系统应具备独享环境+动态 Flag 题目的防作弊机制，能够实时检测选手解题行为，发现异常时自动禁赛并记录日志，禁赛状态可由主办方手动恢复。 （6）平台应支持对解题类赛事选手全程流量数据的实时采集、监控与持久化存储。流量数据应支持按题目维度、时间区间、选手	1	套

		标识等多维度检索与筛选，并支持管理员进行数据导出及本地下载。 ●（7）攻防赛模式应提供赛事控制、题目运维、实例管理、流量管理、网络详情、公告管理、选手管理、展示管理等赛事运维功能。平台应支持开始、暂停、继续、结束、延时，以及数据清空、虚拟资源回收、流量管控、态势监测和异常部署处置的赛事过程控制；应支持实例重置、远程登录、Flag 查看、Checker 检测及自动化 Flag 提交等功能。选手管理应支持禁赛与恢复、奖惩分值调整、解题报告下载；题目管理应支持上线与下线控制、同题状态展示及批量部署，以及流量包的开放管理。展示管理应支持排行榜、统计数据、解题报告的前台展示控制，以及 3D 态势展示和品牌标识的显示配置。 （8）攻防赛数据统计应支持积分总榜、专项排行榜、题目榜单、答题日志等多维度数据展示，并支持数据导出。 ●（9）靶场赛模式应支持赛事控制、题目运维、部署管理、流量管理、公告管理、选手管理、展示管理等运维功能。应支持开始、暂停、继续、结束、延时，以及数据清空、流量管控、态势监测和异常部署处置的赛事过程控制;应支持参赛主体信息、网络配置、VLAN 划分、部署状态的展示，以及重新部署、部署详情和规则注入操作的部署管理;应支持禁赛与恢复、奖惩分值调整、解题报告下载的选手管理应支持排行榜、统计数据、解题报告的前台展示控制，以及 3D 态势展示的展示管理。 （10）靶场赛应包含排行趋势、积分总榜、题目榜单三部分的数据统计。排行趋势以折线图展示排名前列选手的得分随时间变化曲线；积分总榜展示参赛主体的名称、所属单位、解题数量、一血考点数量及总分；题目榜单展示考点名称、被解出次数、前三名解出用户及题目分值。 （11）平台应支持账号和队伍信息的软删除机制，软删除后的账号和队伍应提供恢复和永久注销两种后续操作，满足不同场景下的数据生命周期管理需求。删除后进入待删除区而非直接销毁，支持一键恢复或永久注销，兼顾数据安全与误操作容错。 （12）★平台应支持图形化的简化场景拓扑编排能力，通过直观的可视化界面呈现网络接口、网络区域与终端节点之间的逻辑关系与属性配置。编排功能应支持多个独立网络区域的创建与管理，管理员可为各网络区域配置网络属性并添加主机终端及终端属性；同时应以可视化方式呈现网络区域间的访问策略，管理员可通过设定流量方向，对特定方向的访问策略进行便捷开启或关闭控制。 （13）平台应支持能力考核赛的选手解题数据统计，至少涵盖考试人数、参加人数、题目数量、试卷总分、平均成绩信息等指标，并支持对参赛选手试卷内容的快捷在线预览功能。		
5	安全防火墙	●（1）硬件规格及性能要求：防火墙吞吐量≥2Gbps；IPS+AV 吞吐量≥1.8Gbps;并发连接≥150 万；每秒新建≥1.6 万；Ipsec VPN 吞吐≥400M；SSLVPN 用户数≥400；≥8 个 GE 千兆电口，≥2	1	台

		个 SFP 千兆光口，≥4G EMMC 存储，支持与教学平台对接，实现虚实结合教学。 （2）虚拟化：支持基于 VRF 的 vsys 防火墙系统的虚拟化技术。支持≥32 个 vsys 虚拟化。防火墙系统虚拟化实现用户隔离，每台虚拟防火墙创建可限制新建、并发、吞吐、防火墙策略数量、NAT 数量、对象数量等关键参数。支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。 （3）安全防护：支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能；基于主流杀毒引擎，支持病毒库数量不少于 1200 万。 （4）支持并开通数据防泄漏功能，支持针对 HTTP、SMTP、IMAP、POP3 协议传输文件进行本地敏感数据库比对，对违规内容的文件进行过滤；文件类型至少包含 txt、doc、docx、ppt、pptx、xls、xlsx；敏感数据库至少包括国内银行卡号、国内收集号、国内身份证号、qq、163、126、gmail、雅虎、新浪等常用邮箱账号。 （5）★支持 DoH 加密域名解析服务，对解析流量加密处理。 （6）支持对通过设备的 SSL 流量进行解密。支持代理模式和透明模式两种组网；并支持客户端模式和服务器模式的流量进行 ssl 解密检查。 （7）支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。提供相关界面截图以及功能原理。 （8）可在防火墙本地查询 DNS 解析数量以及检测威胁数量，并生成详细的威胁日志以及告警。 （9）支持输入威胁域名一键跳转到云端威胁情报中心查看威胁详细实时全量的信息化展示。 （10）★支持链路质量实时探测，支持通过调整探测报文的数量、发送间隔、最大重试次数、超时时间、抖动、丢包延迟的阈值进行链路质量评估，进行智能选路。 （11）支持对服务器、客户端进行的口令暴力破解的攻击防护。支持手动设置以及一键生成资产黑名单，支持手动设置以及一键生成资产 mac 地址绑定表。 （12）支持系统快照功能不少于 16 个。支持将版本、配置文件存储为一个快照并备注描述，可以从历史快照中选择一个进行版本回滚。支持当系统损坏无法进入时可以从 bootloader 中选择进入任何一个快照进行回滚。支持每周、每月固定时间进行定期自动快照备份。同时支持 cf 卡和硬盘的系统快照存储。		
6	网络入侵防御设备	● （1）设备硬件规格：设备需为专业入侵防御系统，非防火墙增加授权。网络吞吐≥1G，IPS 吞吐≥500M，并发连接数≥126 万；新建连接数≥2.5 万；多核 CPU 硬件架构，冗余电源，≥500G 硬盘，≥10 个 GE 千兆电口（1 组 bypass），≥2 个 SFP 千兆光口，≥2 个千兆 COMBO 光电复用接口（4 个接口），提供≥3 年质保服务。支持与教学平台对接，实现虚实结合教学。 （2）支持路由模式、透明（网桥）模式、混合模式、旁路模式；旁路部署支持加入 2 个以上物理接口，无需接口对；部署模式切	1	台

		换无需重启设备；接口实际配置支持 second IP 地址，每个接口要求支持至少 200 个 second IP。 （3）系统定义超过 8500+条主流攻击规则，支持自定义 IPS 特征，可针对 8 种协议自定义入侵攻击特征，包括 IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP 等协议；自定义特征可设定拓展协议字段，设置数据包中的匹配内容，可选择包含、等于、不等于、大于、正则匹配等匹配方式:同时可选择多种匹配条件，支持设置"与”和“或”的匹配顺序。 （4）支持弱口令扫描能力，可针对 IP、IP 端、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，弱口令字典可自定义设置。 （5）★支持安全事件攻击链分析，以资产和攻击者两种角度关联所有安全事件，将攻击过程阶段化，分析和统计每个攻击阶段的攻击内容和攻击次数，支持针对每个攻击阶段进行数据下钻，支持分析攻击时间、攻击源、攻击目的、攻击事件、检测模块、攻击级别等信息，帮助管理员清晰了解网络攻击的攻击进度，及时在数据泄露前加固网络。 （6）应用特征不少于 7000 个，移动应用不少于 2400 个，规则总数不少于 13000。支持根据标签选择应用，预置标签分类至少包含安全风险、高带宽消耗、降低工作效率等 10 大类；支持给每个应用自定义标签；支持根据标签选择一类应用做控制。 （7）★支持虚拟路由转发（VRF）功能，使用 VRF 功能可以从系统层面隔离不同 VRF 组里的流量信息和路由信息。不同 VRF 下的接口可以配置相同的 IP 地址。		
7	Web 应用防火墙	●（1） WEB 应用防火墙系统，网络层吞吐≥2.4G，HTTP 吞吐≥2.2G，HTTP 新建连接数≥19000；HTTPS 吞吐≥350mbps，HTTP 并发连接数≥40 万，多核 CPU 硬件架构，≥4GB 内存，≥500G 硬盘；≥8 个千兆电口（1 组 Bypass），可防护站点数 64 个，提供 3 年质保服务，支持与教学平台对接，实现虚实结合教学。 （2）★支持默认站点发现功能，系统监测网络中的 HTTP 和 HTTPS 流量，对于被发现次数超过指定值的网站，系统将通过默认站点对其进行安全防护，并且可以配合响应码筛选和流量入接口功能，发现基于入接口和指定响应码的 web 服务器点，用于设备快速上线部署提供安全防护。 （3）系统具备信息泄露防御能力，可以防止服务器错误、数据库错误、Web 目录内容、程序代码、关键字（支持中文，已内置大量的关键字，将请求或者响应中的关键字进行脱敏处理（替换为任意指定字符））等信息的泄露。 （4）支持 API 的安全检测和防护功能，可基于 OpenAPI 规范文档和自定义防护规则，实现合规性检测，自定义防护规则支持 URL 路径、HTTP 方法、HTTP 头部内容、请求行参数和请求体等内容进行设置。 （5）支持内置漏扫功能，支持扫描各种类型的 Web 漏洞包括：SQL 注入漏洞、XSS 攻击漏洞、Web 服务漏洞、信息泄露漏洞、	1	台

		异常访问漏洞，支持普通扫描和侵入式扫描，支持对需要认证的Web 页面进行扫描，可以对目录深度、链接总数、单目录文件数进行限制，支持手动扫描和定期扫描，扫描报告可以进行导出，支持 PDF、XML 文件报告，支持根据漏洞扫描结果，对网站的漏洞进行快速保护。 （6）★支持多级日志聚合(按照威胁类型进行一级聚合后，按照防护规则进行二级聚合)，便于快速日志溯源。		
8	服务器机柜	1、服务器机柜 42U 600*1000*2055mm;	1	台
9	教学电脑	1、CPU 规格 ®CPU 信息：置 1 颗国产 CPU，每颗 CPU 物理核心数≥8 核，每颗物理核心主频≥3.0GHz，三级缓存≥16MB，支持超线程技术，线程数量≥16，热设计功耗(TDP)≤65W; 2、内存规格 ®2.1 内存配置容量≥16GB; 2.2 内存类型支持 DDR4 及以上内存类型; 2.3 内存条配置数量（板载内存不涉及）≥1; 3、主板规格 3.1 主板集成模块：集成资源扩展模块、计算处理模块、音频扩展模块等，主板的互联拓扑可通过处理器或交换电路实现; 3.2 主板支持的 CPU 和内存情况：国产 C86 平台架构的 CPU; 支持 DDR4 及以上内存类型; 3.3 主板内置 PCIe 插槽数量：主板提供≥1 个 PCIe x16，≥1 个 PCIe x8 扩展槽，≥1 个 PCIe x1 扩展槽; 3.4 主板其他内置接口≥1 个 M.2 硬盘接口，≥3 个 SATA 接口; 3.5 单内存插槽最大可支持容量（板载内存不涉及）≥32GB; 3.6 内存插槽满配时提供的最高内存总容量≥128GB; 4、存储设备规格 4.1 固态盘数量≥1 个; ®4.2 固态存储容量≥512GB; 4.3 机械硬盘数量不涉及; 4.4 机械硬盘总容量不涉及; 4.5 机械硬盘转速不涉及; 4.6 机械硬盘接口协议：支持 SATA3.0 及以上接口; 4.7 机械硬盘形态 2.5 英寸或 3.5 英寸等; 4.8 固态存储接口协议：UFS/SATA/PCIe/NVMe 等类型接口协议; 4.9 固态存储形态：采用插卡或板载等形态，选用符合 M.2 标准的插卡形态; 4.10 存储设备扩展盘位≥1; 4.11 存储设备其他参数要求： a)固态盘应符合 SJ/T 11654 相关规定; b)机械硬盘准备时间应不大于 30s；侧面固定螺丝孔数量可为 4 孔或 6 孔；工作状态环境温度应满足 5℃~55℃; 其它参数应符合 GB/T 12628 相关规定	50	台

5、显卡规格
5.1 显卡类型：独立显卡；
5.2 独立显卡显存类型：配置独立显卡，显存类型应为 DDR4 以上；
5.3 独立显卡显存位宽：配置独立显卡，显存位宽≥64 位；
5.4 独立显卡显存容量：配置独立显卡，显存容量≥4GB；
5.5 独立显卡接口协议：支持 PCIe 3.0 的独立显卡接口协议；
6、外设规格
6.1 鼠标数量≥1 个
6.2 键盘数量≥1 个
6.3 键盘按键数目：104 键
6.4 键盘连接方式：有线
6.5 键盘键程：2.3mm-4.0mm
6.6 键盘按键压力：按键压力应在 0.54 N 士 0.14N
6.7 有线键盘连接线≥1.5 米
6.8 键盘颜色：黑色
6.9 键盘其他要求：键盘外观结构、连接方式、主要功能、安全、电磁兼容性、可靠性应符合 GB/T14081 的相关规定；
6.10 鼠标连接方式：有线
6.11 有线鼠标：连接线≥1.5 米
6.12 鼠标 DPI 分辨率：800-1600
6.13 鼠标颜色：黑色
6.14 鼠标其他要求：其它参数应符合 GB/T 26245 的相关规定
6.15 内置光驱：无要求
6.16 扬声器：内置扬声器≥0 个
7、网络设备规格：有线网卡数量≥1
8、外部接口规格
8.1USB 接口数量：机箱前面板应提供≥ 4 个 USB3.2 接口
8.2 视频接口数量≥2
8.3 音频接口数量≥5
9、整机基础规格
9.1 整机外观：
a）产品表面不应有凹痕、划伤、裂缝、变形和污染等。表面涂层均匀，不应起泡、龟裂、脱落和磨损，金属零部件无锈蚀及其它机械损伤；
b）产品表面说明功能的文字、符号、标志，应清晰、端正、牢固；
9.2 整机结构：
a）机箱应符合 GB/T 4208、GB/T 26246 的相关规定；
b）产品内部结构应符合通用部件的安装需求；
c）所有输入输出接口应符合相关国家或行业标准；
d）产品零部件应紧固无松动，可插拔部件应可靠连接，开关、按钮和其它控制部件应灵活可靠，布局应方便使用；
e）所有 I/O 连接器及需插接线缆的部位应预留采购人操作空间，方便插拔解锁与插拔线缆；
f）可插拔板卡插槽部位应预留安装、拆卸或更换板卡空间；

g）拆装可能接触到的金属剪口或金属尖角部位应做防划伤处理，以保证安全；
h）整机内部走线应规整，固线结构和位置要合理可靠并做防割线处理，需便于理线和插拔操作，走线应不影响系统各主要部件组装和拆卸；
i）如需通过孔走线，过线孔应做防割线处理；
j）各插头位置和插拔方向应合理，应做到插拔无障碍设计，具备防呆设计，有效避免误操作；
k）各主要部件拆装无障碍，使用常规工具拆装，无特殊拆装工具需求；
l）各主要部件拆装步骤要少，各自拆装需避免相互干扰；
m）对于整机或零部件外表面为高亮面的，应粘贴保护膜，保护膜需粘贴牢固，运输、组装等过程不易脱落，撕下无残留；
9.3 机箱防护要求：机箱应符合 GB/T 4208 中 IP20 防护要求。
9.4 整机噪音：产品工作在空闲状态下，产品的空闲状态声功率级≤2.87 Bel。
9.5 整机散热：在环境温度 25℃及处理器满载情况下，产品表面温度应符合如下要求：
a）出风口在机箱后面板情况下，出风口温度不高于 55℃；
b）可触及面温度不高于 45℃；
c）显示器表面温度：显示屏不高于 38℃，显示屏上下灯带位置温度（如涉及）不高于 40℃，出风口温度不高于 45℃
9.6 整机能效限定值：
a)产品能效限定值应达到 GB 28380-2012
b)标准中能效等级 1 级及以上
9.7 机身材质：金属材质
9.8 机身颜色：黑色
9.9 机箱尺寸容量：14L≥机箱容量≥12L，整机支持免工具拆卸。
10、CPU 性能
10.1CPU 物理核数≥8
10.2CPU 主频≥3.0GHz
10.3CPU 末级缓存容量≥16MB
10.4CPU 支持的内存最高速率≥3200MT/s
11、内存性能：内存读写速率≥3200MT/s
12、显卡性能
12.1 显示分辨率≥1920x1080
12.2 显卡显示芯片核心频率≥1300MHz
12.3 显存等效频率≥2666MT/s
12.4 显卡可支持多屏同时显示数量:显卡应支持 2 块屏幕同时显示，分辨率应不低于 1920×1080
13、网络设备性能
13.1 有线网卡速率：最高速率应不低于 1000Mbps，应支持 10Mbps、100Mbps、1000Mbps 速率自适应；
14、主板功能

14.1 内存扩展接口（板载内存不涉及）≥4 个
14.2 存储扩展接口(板载存储不涉及)：主板支持存储扩展接口类型，如 UFS3.0、SATA3.0、SAS3.0、M.2 等类型接口；
14.3 主板 USB 瞬间过流保护：支持有瞬间过流保护功能；
14.4 主板防静电保护：支持防静电保护功能；
14.5I/O 接口功能：提供基于标准 USB 接口外设连接功能、基于音频输入输出接口的音频扩展功能、基于 PCIe 接口板卡扩展功能、基于 HDMI 或 VGA 或 Type-C 或 DVI 或 DP 等接口外接显示器扩展功能、基于存储接口对产品进行增容功能等。产品 I/O 接口，应具备外接标准 USB 设备、显示器、音频设备等内外部设备能力；
15、显卡功能
15.1 显卡外接显示接口：显卡至少支持 VGA、HDMI、DVI、DP、Type-C 中 1 种显示接口；
15.2 独立显卡数量≥1；
16、存储功能
16.1 存储功能：通过 SATA 固态存储/PCIe 固态存储/UFS 固态存储/SATA 硬磁盘等存储部件提供存储功能；
16.2 内置控制器固态存储加密：固态存储通过内置控制器硬件支持加密，不依赖处理器，保障数据安全性，但不得影响存储性能。
a) 支持加密功能，且加密功能开启不影响 SSD 读写性能；
b) 支持固件加密、安全启动和安全升级；
c) 支持数据的安全擦除
17、网络设备功能

17.1 网络功能：

a)支持网络连接、网络开启/关闭功能；

b)支持访问网络和数据交换功能；
17.2 蓝牙协议：若支持蓝牙模块，蓝牙协议不低于 5.0
17.3 数据传输：支持数据传输能力，并提供数据流量和异常日志记录功能；
17.4 有线网卡接口类型：支持 RJ45 接口；
17.5 网络设备拆装：网络设备支持物理拆装，包括无线网卡和蓝牙模块等；
18、外部接口功能
18.1 音频接口类型：支持 3.5mm 孔径 3 段式或 4 段式接口；
18.2 视频接口类型：至少支持 VGA、HDMI、DVI、DP、Type-C 中 1 种显示接口；
18.3HDMI、DP、Type-C 显示接口要求：若提供 HDMI 或 DP 或 Type-C 作为显示接口，应支持音频和视频同步输出；
19、电源功能
19.1 电源线适配能力：电源适配器电线组件应符合 GB/T 15934

		的要求，可拆线的插头和连接器可以不做要求； 19.2 电源功率：电源功率≥200W ； 20、操作系统及软件功能 20.1 中文信息处理要求：符合 GB 18030 的相关规定； 20.2 操作系统备份及还原功能：支持操作系统备份及还原功能； 20.3 固件备份还原能力：支持备份及还原固件的功能 20.4 系统备份及修复能力：提供基于 BIOS 固件系统的还原软件，支持对硬盘数据一键备份还原，分区和启动修复功能。 20.5 操作系统及驱动升级：支持通过网络、闪存盘等方式对操作系统、驱动进行升级； 20.6 固件升级：支持通过网络、闪存盘等方式对固件进行升级； 20.7 BIOS 支持关闭通讯接口：支持 BIOS 关闭以太网及 USB 接口 20.8 固件查看信息：支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息等功能 20.9 固件设置启动顺序：支持设置启动顺序功能，并按照设置的启动顺序启动 20.10 固件设置口令：支持设置口令、修改口令、验证口令功能 20.11 固件设置网络引导：支持网络引导启动和关闭功能 21、存储设备可靠性 21.1 固态存储寿命：TBW≥80TB（条件：240GB 硬盘容量） 21.2 机械硬盘寿命：通电时间≥5 万小时 22、显示设备可靠性 显示屏屏幕失效点：符合 GB/T 9813.2 的要求 23、外设可靠性 23.1 键盘按键寿命≥1000 万次 23.2 鼠标按键寿命≥500 万次 23.3 键盘鼠标线材寿命：键盘鼠标所用线材经±60° 弯折不低于3000 次，功能、外观完好 23.4 风扇寿命≥4 万小时 24、整机可靠性要求 24.1 电磁兼容性要求的抗扰度：符合 GB/T 9254.2 的规定 24.2 环境条件要求的气候环境适应性：符合 GB/T 9813.1 中规定 24.3 环境条件要求的振动适应性：符合 GB/T 9813.1 中规定 24.4 环境条件要求的冲击适应性：符合 GB/T 9813.1 中规定 24.5 环境条件要求的碰撞适应性：符合 GB/T 9813.1 中规定 24.6 环境条件要求的运输包装件跌落适应性：符合 GB/T 9813.1 中规定 24.7 MTBF 测试：MTBF(m1)≥5 万小时 25、兼容要求 25.1 常用软件兼容：支持流式软件、版式软件、浏览器、邮件采购人端、解压软件、多媒体、图形图像处理等常用软件 25.2 数据库兼容：兼容 3 个及以上厂商的数据库产品 25.3 中间件兼容：兼容 3 个及以上厂商中间件产品		

25.4 平台软件兼容：兼容 3 个及以上厂商云计算及大数据平台
26、包装及运输要求
26.1 标志、包装、运输和贮存：符合 GB/T 9813.1 和商品包装政府采购需求标准的相关规定
27、服务要求
27.1 配置检查工具：提供自检测试工具
27.2 服务响应：
a) 供应商提供电话、电子邮件、远程连接等多种形式服务；
b)供应商提供同城 4h、异地 12h 技术响应服务，2 个工作日解决问题，对于未能解决的问题和故障应提供可行的升级方案，并提供周转设备或更换设备；
c)建立全国技术服务体系和服务团体，符合专业服务体系标准要求，提供原厂中文服务；
d)服务周期内提供产品的维修、换件和升级服务。
e)提供打印机等外设的适配服务工作。
27.3 服务周期：
a) 设备停产后应继续提供质量保障服务（含备品备件），服务终止时间与最后一批设备交付时间间隔不低于 6 年；
b) 产品停止服务时间应提前 1 年告知；
c) 应明确产品发布日期
27.4 预装操作系统：预装符合桌面操作系统政府采购需求标准的正版操作系统。永久授权。3 年免费升级服务
27.5 培训服务：供应商提供培训材料、产品手册、培训视频等培训相关内容
27.6 典型问题解决手册：供应商提供典型问题解决说明文档或视频
27.7 厂家升级软件与扩容服务：供应商提供上门升级部件/软件与扩容的增值服务
27.8 整机质量服务要求：免费服务周期（含换件和维修）应不小于 5 年。
27.9 合格证书要求：提供产品合格证
27.10 开箱组装/使用指导要求：提供开箱组装/使用指导
27.11 驱动下载服务要求：提供驱动光盘或下载方式
27.12 兼容适配软件下载服务要求：提供兼容适配软件下载渠道（光盘、网站）
28、供应链合规性
28.1 产品部件保障：供应商保障产品主要部件，提供 6 年的备件服务能力（自购买之日起），或提供可兼容原设备的升级换代产品
29、供应链质量
29.1 抗干扰性：当产品部件出现供应风险时，供应商应通知采购人并提供风险应对方案确保产品的服务保障
29.2 供应能力证明：供应商提供供应链稳定承诺书，确保产品的部件在产品服务周期内稳定供货
30、关键部件安全要求

		30.1 关键部件安全要求：CPU 和操作系统等关键部件应当符合安全可靠测评要求。CPU 和操作系统应当通过中国信息安全测评中心和国家保密科技测评中心安全可靠测评。 31、整机安全性要求 31.1 密码算法实现：CPU 芯片应符合 GM/T 0008 的相关规定，或芯片密码模块应符合 GB/T 37092 或 GM/T 0028 的相关规定 31.2USB 端口管控：支持 USB 端口管控，USB 的关闭，开放，屏蔽。 31.3 安全物理锁：支持安全物理锁 31.4 信息安全基本要求： a）产品应符合 GB/T 39276 的 5.2 的规定； b）生产厂商应建立漏洞跟踪表，保证产品版本涉及到的漏洞(如驱动程序等)可查看； c）产品不得包含已知的恶意代码或漏洞，不存在未声明的指令、功能、接口 31.5 固件安全启动：支持固件安全启动功能，固件启动过程中只有通过启动校验才能正常启动 31.6 限用物质的限量要求：符合 GB/T 26572 中规定 32、预装国产操作系统，操作系统符合《操作系统政府采购需求标准（2023 年版）》，通过安全可靠评测，在《安全可靠测评结果公告》名单内。		
10	网络交换机	1、转换容量≥432G/4.32T，包转发率≥105Mpps/166Mpps； 2、48 个 10/100/1000M 自适应电口，2 个千兆 SFP 光口，4 个 1G/10G SFP+光口；含 4 组万兆光纤模块和 2 组光跳线； 3、支持将多台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合； 4、支持流量控制功能；支持万兆光口堆叠；支持无连接端口休眠；支持云管理、本地管理两种模式，可自由切换； 5、需提供上联和 VLAN 配置服务，保证与学校现有网络兼容。	4	台
11	多媒体教学软件	（1）教师可以给学生布置课堂作业，学生在收到教师布置的作业后，必须在规定的时间内完成并提交，教师再对学生提交的作业进行批改，并将评为优秀的作业作为范本共享给其他学生。 （2）学生可以收到教师布置给自己的作业，可以下载作业，完成作业后进行提交，学生可以看到教师批改作业结果，并可以查看到评为优秀的作业，可以对优秀作业进行点赞和评论。 （3）教师机屏幕上的内容实时广播给单个、部分或全体学生；学生全屏接收教师机广播的画面，锁定学生鼠标和键盘；支持在云主机服务器宕机的情况下进行广播，支持后登录的学生机自动进入屏幕广播。 （4）支持对虚拟桌面进行广播，屏幕可设置色深设置，可设置彩色广播，黑白广播。 （5）教师将本地视频文件广播给学生，支持添加多个视频文件按顺序播放；在云主机服务器宕机的情况下也能进行广播；后登录的学生机可自动进入影音广播，为提高教学效率，在执行影音广	1	套

		播的同时，学生端的键盘和鼠标被锁定。 （6）当学生终端具有多个虚拟桌面教学场景时，教师可远程指定学生机快速进入统一的教学场景。 （7）教师对学生进行电子点名，可以自定义院系、专业、班级等单位类别，可以直接选择几年级几班。 （8）教师端可以通过摄像头将教师的影像和语音实时发送到学生端，实现远程实时影像语音教学。 （9）教师可对部分或全体学生同时下发一个或多个文件（文件和文件夹），教师可自定义下发的文件存放在学生机上的路径，遇到同名文件，系统弹出提示，教师自定义是否覆盖同名文件。 （10）教师机可以连续监看所选学生机屏幕。每屏可监视多个学生，可设置每屏学生机的数量以及学生机屏幕轮循的时间间隔。 （11）教师机可以将本机的操作过程、讲解录制为一个文件，供教师反复使用，以后通过屏幕回放功能进行回放。 （12）教师可利用电子白板进行边操作边注解，达到强调重点、进行注解等作用。电子白板可以配合屏幕广播使用，也可配合投影仪进行电子板书或屏幕注解。 （13）教师可远程批量限制学生机的程序和设备的使用，还可以禁止学生机访问外网，有效规范学生对学生机的操作行为。 （14）每套至少开放 70 个连接终端。		
12	还原软件（含保护卡）	（1）支持使用 Intel、AMD、海光、兆芯等芯片的终端部署安装。 （2）可新增分区或删除指定的分区，可设置系统不同分区的类型，支持自定义分区名称、分区容量、文件系统以及还原方式。 （3）支持国产和非国产终端电脑的固态硬盘及机械硬盘的双硬盘保护同传，可新增、删除指定分区，设置不同分区类型（涵盖立即还原型启动分区、备份还原型启动分区、专属分区、共享分区、Linux 交换分区及其他分区），自定义分区名称、分区容量、文件系统及还原方式。支持完整保留终端硬盘现有操作系统数据的简易安装模式，删除终端硬盘所有数据并重新划分硬盘分区的自定义安装模式。 （4）可显示差异拷贝过程中当前发送端网卡的列表，对于多网卡终端可自由选择进行差异拷贝的网卡。 （5）若终端因故障在底层差异拷贝时无法与发送端连接，可右击对应终端连接号并将其设定为占位机，该终端连线号图标变更为占位状态，已连线终端将自动查找并连接未连线的连线号，也可自定义指定终端的连线号。 （6）支持断点续传，若终端在差异拷贝时意外断线，重新进行操作后发送端将自动智能识别断线终端的数据状态，仅发送终端断线后未接收的数据，无需将完整数据重新发送。 （7）差异拷贝过程中可显示在线及掉线终端数，可显示数据传输量并记录当前速度及传输已用时间，呈现传输进度的百分比率，预估显示传输剩余时间，结束显示传输平均速度。 （8）差异拷贝过程中自动识别当前传输中的最慢机并进行标记，可暂停该终端传输。可以设置显示终端上系统桌面信息，底层开	50	套

		机画面支持以保护模式、总管模式和暂存模式进入系统。 （9）可批量对局域网内客户端的操作系统自动分配 IP 地址并修改不同网段的 IP 地址设置、Windows 用户的登录名和计算机名，可设置 IPv4 及 IPv6 的地址，支持设置网络连线群组，支持终端多网卡 IP 设置，差异拷贝时可绑定网卡。 （10）在 Windows 系统下，可自动识别并记忆绿色软件的注册信息，对 3D 类（如 AUTODESK、Maya）、设计类（AUTOCAD）需绑定硬件序列号激活软件的自动进行注册，在客户端页面，通过发送端发送分区至其它接收客户端后无需激活可直接使用软件。 （11）支持多账号管理，多个管理员账号自定义权限分级管理，可分配不同的管理员管理不同的操作权限。 （12）支持隐藏底层操作系统选单，有多个操作系统时，可设置默认进入某个操作系统，自定义进入系统的时间支持开启、关闭开机自动连线支持显示、不显示开机画面背景图片和开机画面热键提醒。		

64 课时网络安全课程

课程模块	项目	任务	课程内容	备注
计算机网络安全概述	网络安全意识	安全导论	网络安全介绍	理论
	网络安全意识	企业办公安全	网络安全管理	理论
	网络安全意识	安全法律法规	信息安全法律法规	理论
	网络安全意识	安全法律法规	相关案例分析及法律责任	理论
黑客常用的攻击方法	内网渗透技术	Window 信息收集	Window 信息收集	理论
	内网渗透技术	Linux 信息收集	Linux 信息收集	理论
	Wireshark 数据包分析实战	Wireshark 使用教程	wireshark 入门	理论
	Metasploit 渗透测试指南	MSF 基础	msfconsole	理论
	DDOS 攻击与防御	DDOS 基础知识	DDOS 简介与历史	理论
计算机病毒	网络安全意识	安全意识培养	wannacry 勒索病毒样本	理论
	渗透测试流程	漏洞利用	震网三代病毒	理论
数据加密技术	密码学基础	基础密码学	密码学概述	理论
	密码学基础	基础密码学	密码学基本应用	理论
	密码学基础	分组密码	分组密码基本概述	理

				论
	密码学基础	分组密码	FEISTEL 和 DES 结构	理论
	密码学基础	公钥密码	公钥密码基本概述	理论
	密码学基础	公钥密码	RSA 算法体制	理论
	密码学基础	数字签名与数字证书	数字签名与数字证书	理论
防火墙技术	防火墙课程	防火墙基本介绍	防火墙基本介绍	理论
Windows 操作系统安全	Windows 操作系统安全	系统安全基础	Windows 系统安全概述	理论
	Windows 操作系统安全	账户安全	本地账户与组账户管理	理论
	Windows 操作系统安全	组策略与域管理	windows 安全审计策略配置	理论
Web 应用安全	Web 安全基础	Web 安全综述	Web 安全概述	理论
	Web 安全基础	Web 安全综述	Web 安全体系构建	理论
	Web 安全基础	Web 安全综述	典型 Web 安全漏洞	理论
	Web 安全攻防	Web 安全攻防	网页篡改	理论
课程模块	**项目**	**任务**	**课程内容**	**备注**
实验 1：wireshark 抓包和	Wireshark 数据包分析实战	Wireshark 使用教程	玩转捕获数据包	实验
	Wireshark 数据包分析实	Wireshark 使用教程	Wireshark 过滤器应用	实

协议分析	战			验
	Wireshark 数据包分析实战	Wireshak 数据包分析	HTTP 协议分析	实验
	Wireshark 数据包分析实战	Wireshak 数据包分析	DNS 协议分析	实验
实验 2：nmap 主机扫描	Nmap 渗透测试技术	Nmap 使用实例	主机发现实战	实验
	Nmap 渗透测试技术	Nmap 使用实例	探索网络实战	实验
实验 3：nmap 端口_服务_OS 扫描	Nmap 渗透测试技术	Nmap 使用实例	指纹探测与识别实战	实验
	Nmap 渗透测试技术	Nmap 使用实例	探测行为选项实战	实验
实验 4：口令破解	爆破工具详解	John 使用详解	John 弱口令爆破	实验
	爆破工具详解	其他爆破工具	Patator 与 Ncrack	实验
	爆破工具详解	其他爆破工具	hashcat	实验
	爆破工具详解	其他爆破工具	彩虹表的使用	实验
实验 5：漏洞利用	Metasploit 渗透测试指南	MSF 实战	CVE-2019-0708	实验
	Metasploit 渗透测试指南	MSF 实战	木马与 meterpreter shell	实验
	Metasploit 渗透测试指南	MSF 实战	meterpreter 的后渗透操作	实验
实验 6：网络欺骗	内网渗透技术	内网欺骗攻击	欺骗攻击	实验

实验 7：木马	内网安全基础	常用工具使用	MSF 应用	实验
实验 8：DOS	DDOS 攻击与防御	DDOS 攻击与防御实战	DDOS 攻击系统资源	实验
	DDOS 攻击与防御	DDOS 攻击与防御实战	DDOS 流量直接攻击	实验
	DDOS 攻击与防御	DDOS 攻击与防御实战	DDOS 流量反射攻击（一）	实验
	DDOS 攻击与防御	DDOS 攻击与防御实战	DDOS 流量反射攻击（二）	实验
	DDOS 攻击与防御	DDOS 攻击与防御实战	DDOS 应用攻击实验	实验
实验 9：缓冲区溢出攻击	CTF-PWN 应用指南	漏洞利用开发	shellcode 编写	实验
	CTF-PWN 应用指南	整数安全	整数溢出利用	实验
	CTF-PWN 应用指南	栈溢出与 ROP	栈溢出漏洞利用 -ret2libc	实验
	CTF-PWN 应用指南	堆利用	overlapping_chunks 实战	实验
实验 10：加密、证书	密码学基础	公钥密码	公钥密码应用实战	实验
	密码学基础	数字签名与数字证书	数字证书应用实战	实验
实验 11：防火墙	防火墙课程	防火墙基本操作	使用 web 登录防火墙	实验
	防火墙课程	NAT	配置出接口地址源 NAT 转换	实验
	防火墙课程	NAT	配置地址池转换	实验

	防火墙课程	VPN	GRE_VPN	实验
	防火墙课程	VPN	IPSEC_VPN	实验
	防火墙课程	VPN	L2TP_VPN	实验
	防火墙课程	路由协议	静态路由	实验
	防火墙课程	路由协议	RIP	实验
	防火墙课程	路由协议	OSPF	实验
	防火墙课程	路由协议	BGP	实验

24 课时网络安全技术实训课程

课程模块	项目	任务	课程内容	备注
网络基础	计算机网络基础	网络及协议安全实践	Wireshark 使用实验、Tcpdump 使用实验	实验
	计算机网络基础	网络及协议安全实践	ARP 协议观察实验、交换机 VLAN 实验、静态路由实验	实验
操作系统	Linux 操作系统安全	系统管理	文件和目录管理、进程和服务管理、Shell Scripts、软件包管理	实验

基础	Linux 操作系统安全	系统安全加固	Linux 防火墙配置	实验
	Linux 操作系统安全	系统安全加固	Linux 数据备份与恢复	实验
	Linux 操作系统安全	系统安全加固	使用 Gnupg 保护文件安全、Rsyslog 日志服务	实验
	Windows 操作系统安全	文件系统与共享安全	NTFS 与 ReFS 磁盘的安全与管理	实验
	Windows 操作系统安全	组策略与域管理	windows 安全审计策略配置、软件限制策略与 IE 安全策略	实验
	Windows 操作系统安全	组策略与域管理	windows 域控安装与配置	实验
	Windows 操作系统安全	组策略与域管理	windows 域用户管理与域策略、AD DS 的维护	实验
网络攻击环境搭建	渗透测试环境搭建	环境搭建	浏览器插件-Hackbar 插件配置与应用	实验
	渗透测试环境搭建	环境搭建	浏览器插件-CookieEdit 插件配置	实验
	渗透测试环境搭建	环境搭建	User Agent 插件安装与应用	实验
	渗透测试环境搭建	环境搭建	基于 WAMP 构建网站	实验
	渗透测试环境搭建	环境搭建	基于 PHPStudy 构建网站	实验

网络攻击	Metasploit 渗透测试指南	MSF 实战	CVE-2019-0708	实验
	Metasploit 渗透测试指南	MSF 实战	木马与 meterpreter shell	实验
	Metasploit 渗透测试指南	MSF 实战	meterpreter 的后渗透操作	实验
	Burp Suite 综合渗透实战	Proxy	Proxy 功能实战	实验
	Burp Suite 综合渗透实战	Target 和 Scanner	Target 功能实战	实验
	Burp Suite 综合渗透实战	Intruder	Intruder 实战	实验
	Burp Suite 综合渗透实战	Repeater 和 Sequencer	Repeater 功能实战	实验
	Burp Suite 综合渗透实战	BurpSuite 的对比、解码和扩展	Decoder 功能实战	实验
	Burp Suite 综合渗透实战	BurpSuite 综合实战	Sqlmap 被动注入	实验