|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **学院** | **实验室名称** | **教室号** | **设备名称** | **规格及参考型号** | **数量** | **单位** | **备注** |
| 计算机工程学院 | **标的一：**实验室电脑扩建 | D307、D401、D408、D501、D502、D505、D506、D507 | 台式电脑 | CPU:I5-12400F、主板B660M、内存16G 3200MHZ、硬盘500G固态硬盘、副硬盘1T机械硬盘、GTX1660 6G显卡、24寸2K显示器 | 53 | 套 | 带硬盘防护功能、具备网络同传功能；  D307共30台、D401共10台、D408共1台、D501共2台、D502共2台、D505共2台、D506共2台、D507共14台。包含室内布强弱线。 |
| 投影仪 | 投影分辨率1920\*1080、流明>3000、含幕布及安装 | 1 | 套 | 放置于D408 |
| 交换机 | 24口、千兆 | 4 | 台 | D307两台、D401一台、D407一台。安装调试及配套布线 |
| 机柜 | 挂壁式 | 1 | 个 | 安装调试 |
| 双人电脑桌 | 参考现有机房定制 | 7 | 套 | 参考现有桌椅规格；分别为D408一套、D501一套、D502一套、D505一套、D506一套、D507二套 |
| 环境布线 | 六类网线信息点，包含金属线槽等。电脑信息点、包含部分实验室配电箱升级 | 53 | 个 | 根据现场满足使用 |
| **标的二：**网络信息安全实验室 | D304、D405 | 信息安全攻防对抗平台 | **（一）设备硬件参数**  机架式结构；具有多个100/1000Base\_T和USB的管理接口；处理器性能不低于双路XEON 4210R\*2（双路十核20线程）；内存性能不低于DDR4 32G\*4；硬盘性能不低于3 \* 500G SSD + 5\* 2T HDD存储；RAID卡4GB SAS 8口（断电保护）；双通道冗余电源；单台设备并发访问数≥200，并发虚拟机数量≥50；支持集群部署。  **（二）攻防对抗学习模块**  1.平台提供多种类型操作系统模板，包括WindowsXP、Windows7、Windows2003、Windows2008、Windows2012、Centos6、Centos7、Ubuntu、Kali等，管理员可上传虚拟机模板至平台，扩充教学实训资源。  2.覆盖Windows系统安全、Linux系统安全、MySQL数据库、SQLserver数据库、Oracle数据库、数据包分析、XSS跨站、网络扫描、Web安全、Web应用渗透、扫描工具使用、防火墙、协议分析、信息收集、Metasploit渗透测试、SQL注入、网络访问控制、Burpsuite、网络安全、Kali Linux、KPI技术、数据保密与安全、代码审计、Hacking Python、入侵检测、拒绝服务攻击、提权、系统漏洞利用、破解技术、信息隐写、安全攻防分析、数据恢复、取证与反取证、网络安全应急响应、内存取证分析、移动终端安全、恶意代码分析、系统后门、密码学、溢出、网络欺骗技术、无线安全等主要课程实验模块，实操环境不少于600个。  3.每个实验包含具体的实验目的，实验环境描述，实验详细步骤等介绍说明。  4.平台提供CTF类教学和考试内容，覆盖Web安全（SQL注入、XSS跨站、文件上传、文件包含、代码审计）、Mobile移动安全（apk逆向分析）、取证分析（内存取证、数据恢复、日志分析）、逆向分析、密码学、PWN等。  5.包含安全运维、渗透测试、网络攻防、移动安全、安全开发、应急响应取证、代码审计等视频课件，课件数量≥400。  6.包含网络安全法、安全保密意识、信息安全管理、人员安全管理、第三方安全、拍照泄密防范、邮寄与快递安全、打印传真与复印安全、工作站电脑安全、桌面安全、移动媒介使用、信息资产保护、办公环境安全、物理访问安全、金融诈骗防范、网络钓鱼防范、电话诈骗防范、社会工程学防范、恶意代码防范、信息安全事件、个人信息保护、信息清除与销毁、数据备份与恢复、机密信息保护、公司信息披露、社交网络安全、公共场所安全、远程工作安全、差旅信息安全、移动设备安全、密码安全、无线安全、即时消息安全、浏览器及上网安全、文档安全、邮件安全、网络会议安全、网络法规遵循、信息安全职责、网络使用准则、常规安全知识等视频课件和互动课件，课件数量≥300。  7.包含中间件、数据库、CMS等漏洞库分析库，漏洞分析库数量≥200。  8.提供仿真互联网系统漏洞靶机供教学实训使用，靶机数量≥200。  9.包含抓包工具、注入工具、嗅探工具、漏洞利用、提权工具、暴力破解、扫描工具、PE工具、应急响应、数据恢复、后门检测、移动安全、信息隐写、文件分析、编程开发等工具使用教程和下载模块，工具数量≥100。  10.支持闯关训练、自由组合训练、错题集中训练。  11.支持不少于50个实操环境虚拟机同时开启。  12.可提供持续的课件升级,支持基于本平台的企业课程建设  **（三）攻防演练竞技考核模块**  1.支持理论竞赛和实操竞赛。  2.理论考题不少于2000道，支持题库自动生成，支持添加或批量导入笔试题库。  3.实操竞赛支持机试实操CTF、风险评估、应急响应、闯关等形式，支持个人赛和团队赛。  4.支持在同一场竞赛中添加多种竞赛模式，分数累加。  5.支持题库管理、考试管理、考试人员管理等功能。  6.支持自动评分并进行实时排名。  7.支持成绩报表导出。  8.支持经典竞赛，包含近几年国家级或省级竞赛真题。  **（四）攻防对抗平台管理模块**  1.管理后台可以监控平台运行状态数据。  2.支持课程相关数据统计。  3.支持人员管理，支持分权管理。  4.支持对虚拟机管理，支持通过Web、Windows远程桌面、Linux SSH方式访问虚拟机。  5.支持实验管理、工具库管理、课件管理、题库管理。  6.支持CTF管理，创建综合闯关训练，创建经典赛事等。  7.支持直播、录播教学课堂管理。  8.支持数据备份与恢复。  9.支持实例类型编辑。  10.支持在线编辑实验环境或考题环境。  11.支持学生学习情况管理。 | 1 | 套 |  |
| 防火墙系统 | 千兆电口≥12个,单电源,防火墙吞吐900M，并发连接30万，每秒新建连接4000，IPSEC VPN吞吐30M，默认含IPSEC VPN模块；支持静态路由、OSPF\BGP等动态路由等路由协议；支持路由、透明以及混合接入模式；支持多元组的访问控制规则；支持SD-WAN功能，以及对SD-WAN链路进行统一管理；支持邮件安全；支持与同品牌其它信息安全设备联动；具备畸形包处理能力、Ping Flood 攻击处理能力、Smurf攻击处理能力、SYN Flood攻击处理能力等。 | 1 | 台 |  |
| 入侵防御系统 | 千兆电口≥6个,单电源,有扩展槽位,整机吞吐率≥1Gbps以上，IPS吞吐率≥500Mbps，包含1年特征库升级；支持在线抓包；支持路由、交换、虚拟线、聚合、监听、混合部署等多种接入模式；支持主备模式、负载均衡两种模式；支持在线升级、离线升级；能够拦截多种WEB 类攻击、拒绝服务类攻击)、木马类攻击、滥出类攻击等攻击行为；具有机器学习检测功能；支持与防火墙联动；能够监视协议事件，支持多种入侵分析；能够拦截多种入侵事件。 | 1 | 台 |  |
| WAF | 千兆电口≥6个,单电源,应用层吞吐≥200Mbps、网络层吞吐≥2.5G、并发连接≥50W；含1年产品特征库升级许可；支持基于域名和IP多种方式提供网站防护；支持HTTP/HTTPS站点防护；支持应用层访问控制功能；能识别和阻断跨站请求伪造攻击，支持HTTP token防护等多种防护方式和WebShell攻击等多种攻击防护功能；支持多种爬虫攻击防护；具备网页篡改防护；支持与防火墙联动；能检测并阻断经逃逸技术处理过的攻击行为。 | 1 | 台 |  |
| 上网行为管理系统 | 千兆电口≥6个,单电源,适配带宽≥30M，用户数≥50人；1年特征库升级；支持将多个以太网物理端口捆绑成一条逻辑端口，支持多种负载方式；支持多种路由模式；行为管理支持分布式部署；能够提供流量适用排名；具有APP集中监控功能；基于时间的安全策略；具备内容过滤策略；支持防火墙模块阻断、流量模块阻断、行为管控模块阻断记录；支持与同品牌的终端检测防御系统联动；能够有效识别标准应用协议和多个网络应用，并能基于 IP 地址、用户、时间段等条件对其进行控制。 | 1 | 台 |  |
| 漏洞扫描 | 千兆电口≥6个,单电源，有扩展槽位, ≥40个域名扫描任务不限制IP数量，并发扫描IP地址≥40个，并发扫描系统扫描任务≥5个，并发扫描web任务≥3个；包含1年特征库升级；漏洞库应涵盖目前的安全漏洞和攻击特征；支持网络打印机、摄像头、移动终端等设备的漏洞发现；支持磁盘管理功能；支持在线报表；支持与防火墙联动功能；支持日志外发至日志服务器；用户可以定制阈值。 | 1 | 台 |  |
|  |  |  | 交换机 | 1U,48个千兆电口，4个万兆光口,单电源； | 1 | 台 |  |
|  |  |  | 网线 | 六类网线 | 1 | 箱 |  |
|  |  |  | 机柜 | 常规 | 1 | 台 |  |
|  |  |  | 空调 | 120立式 | 1 | 台 |  |