|  |  |  |
| --- | --- | --- |
| **名称** | **规格参数** | **数量** |
| Web漏洞挖掘靶场平台 | 配备对应的教材，具备课程教学资源服务，人员企业认证，师资培训，学生实习及就业服务相关能力,可支持50用户同时在线实训总览统计要求：1、需支持概况统计展示，包含但不限于资产总量、存活量、安全资产量、存在风险资产量、存在风险资产排行、指纹与插件总量；2、需支持展示最新漏洞排行榜，需支持自动关联存在相同漏洞的资产，通过资产链接可跳转至漏洞扫描报告页面，进而查看漏洞详情；3、需支持资产量变化折线图，漏洞类型、漏洞等级分布、资产分类统计（部门、系统、负责人、地区等类型）以及资产端口、服务、设备类型、厂商、系统和网站组件统计Top10；资产管理要求：1、需支持主机资产管理，管理对象为IP地址，需支持业务资产管理，管理对象为URL/域名；2、需支持资产标签管理，包括部门标签、系统标签、负责人标签、地区标签、行业标签等；3、需支持手工录入、表格导入、自主探测发现三种方式纳管资产，资产纳管时可关联标签信息；4、需支持资产批量操作，包括批量检测、批量修改、批量删除、批量导出、批量子域名探测、批量暗链扫描、批量拉入黑名单（不再探测/纳管）等；5、需支持资产概况总览（资产IP/URL地址、资产存活状态、资产漏洞分布等），支持查看资产检测或扫描报告；6、需支持多种资产检索方式，支持模糊检索与精确检索；可组合多个条件实现对资产精确定位。检索条件包括：资产状态、资产是否已检测、资产是否已扫描、资产来源、资产纳管时间、资产标签（归属地、负责人、归属部门、归属系统、归属行业、备注信息）、资产漏洞（漏洞类型、漏洞名称、漏洞等级）、资产属性（开放端口、开放服务、端口状态、资产分类、设备类型、设备厂商、主机系统、系统厂商、支撑脚本、服务组件、应用框架）；资产检测要求：1、需支持添加网段进行检测，主动发现存活主机、目标指纹信息、端口服务状态等数据；2、需支持一键提取资产检测过程中发现的所有WEB资产链接；3、需支持定时检测、周期检测、任务重扫等操作；4、需支持网页快照、过滤黑名单等检测方式，网页快照开启后可对检测目标的WEB服务记录页面截图；5、需支持任务结果比对，包括：服务端口、系统存活性等；6、需支持任务详情查看、报告导出和目标详情查看、报告导出，输出格式包括：HTML、EXCEL等；7、需检测报告包含但限于如下信息：资产IP、主机MAC、主机名、主机状态、资产分类、设备类型、设备厂商、主机系统、系统厂商、支撑脚本、服务组件、应用框架、地理位置、地理坐标、检测时间、端口矩阵、端口服务等；靶场漏洞扫描要求：1、需支持主机漏洞扫描、弱口令扫描、敏感信息社工扫描、数据库漏洞扫描、CMS识别扫描、Web漏洞扫描、中间件漏洞扫描、框架漏洞扫描等；2、需支持对任务目标的多条件搜索筛选，包括存活性、扫描状态、漏洞类型、漏洞名称、漏洞等级、目标地址等；3、漏洞扫描后需支持查看安全评估报告，内容包括目标基本信息、漏洞危害等级、漏洞描述、漏洞验证详情、漏洞路径、解决方案等；4、需支持在线编辑漏洞报告，包括删除漏洞、将漏洞添加至黑名单等；5、需支持识别如下指纹信息：网站标题、服务组件、开发语言、应用框架、端口服务等；6、需支持扫描任务比对，及时发现漏洞变化；7、需支持弱口令本地自检；8、需支持基线合规检查、挖矿后门检测、应急响应分析； | 1 |
| Web攻击捕获靶场平台 | 配备对应的教材，具备课程教学资源服务，人员企业认证，师资培训，学生实习及就业服务相关能力,可支持50用户同时在线实训平台总览要求：1、需支持呈现最近7天、最近30天、当年，三个时间段的攻击分析数据，包括但不限于：攻击类型分布扇形图、被攻击服务分布扇形图、被攻击节点排行、被攻击探针排行、攻击源IP排行TOP10、攻击事件趋势；2、需支持动态化监控展示界面，实时提供相关预警信息，包含实时预警中心、被攻击服务扇形图、攻击源排行TOP5、被攻击节点排行、危险等级占比、常用工具、入侵报警事件趋势图、攻击方式占比扇形图、被攻击地区排行等； 靶场节点管理要求：1、需支持软件探针，可在现有业务主机中部署Agent探针，支持在windows与Linux系统中部署探针，主机部署探针后可捕获攻击者的攻击行为；2、管理节点可自动下发安装部署命令，实现子节点全自动化部署；每个子节点上可运行多个节点环境；3、需支持节点镜像靶机管理，可在管理界面查看靶机的系统版本、服务类型、漏洞类型、交互类型、危险等级、镜像状态；4、需支持运行真实ssh、Samba等系统服务的靶机，受到攻击后可以查询攻击者源IP、源物理地址、攻击时间、攻击次数、遭受攻击的环境、行为轨迹等数据；5、需支持运行真实MySQL、MongoDB、PostgreSQL等数据库服务的靶机，受到攻击后可以查询攻击者源IP、源物理地址、攻击时间、攻击次数、遭受攻击的环境、行为轨迹等数据；6、需支持运行真实tomcat、gitlab、splunk、struts2、crm、weblogic等服务的靶机，受到攻击后可以查询攻击者源IP、源物理地址、攻击时间、攻击次数、遭受攻击的环境、行为轨迹等数据；7、用户可自己上传节点镜像，并定义该镜像的日志路径、漏洞类型、系统版本、交互等级、危险等级、支持的服务、端口号、CVE号；8、需支持关联多个靶机环境组成特定业务场景，可通过业务场景模板一键部署多个靶机；9、当黑客成功入侵系统后，在可控时间内会自动关闭该靶机环境，确保系统安全；10、当黑客成功入侵系统后，在关闭靶机环境的同时，将该靶机进行备份，备份的环境可以再次开启，可用于人工取证；11、靶机环境自动销毁后，系统可自动部署一个相同的初始化靶机环境或随机部署一个初始化靶机环境；12、支持对每个靶机单独定义添加检测规则，包含规则内容、攻击方式、危险等级、触发类型等；溯源取证要求：1、需支持对黑客在shell中的操作进行进行实时记录，并实时播放；2、需支持对黑客在shell中的操作进行视频记录并可以回放，用于取证；3、需支持对黑客的攻击行为轨迹按时间线进行记录；4、需支持对黑客攻击进行溯源，包括：源ip、源物理地址、攻击数量、威胁指数、真人概率、攻击类型、攻击服务、攻击常用工具、常用攻击命令、设备指纹、攻击拓扑图；联动阻断要求：1、可与网络层设备联动，当蜜罐被攻击后，立即将攻击者网络层特征同步给联动设备，联动设备立即对攻击进行阻断；2、可设置阻断联动周期，当设置的周期时间到达后，阻断策略自动删除；3、可手工设置阻断策略，包括阻断的IP地址和阻断周期，拦截外部攻击；网络管理要求1、需支持网络拓扑图展示，用于体现节点之间的物理布局，以及节点已部署的漏洞环境；2、需系统支持虚拟网络，通过配置网卡的虚拟网络，支持MACVLAN与NAT两种，可给漏洞仿真镜像单独分配虚拟IP地址；3、需支持添加安全组策略，可自定义添加靶机流量出入站规则，限制靶机流量外发；防止靶机被作为跳板；可通过勾选方式快速设置指定端口的出入站规则； | 1 |
| Web攻防竞赛靶场平台 | 配备对应的教材，具备课程教学资源服务，人员企业认证，师资培训，学生实习及就业服务相关能力,可支持50用户同时在线实训设备尺寸：2U机架型；CPU：双路十核20线程；内存：DDR4 32G\*4内存；存储：≥10T；RAID卡：4GB SAS 8口（断电保护）；电源：双通道冗余电源；网卡：2\*100/1000Base-T，2\*USB接口；1、需支持理论竞赛和实操竞赛。2、理论考核需支持单选、多选、判断。3、理论考题需支持题库自动生成，支持添加或批量导入笔试题库。4、需支持根据人员，竞赛模式，配置信息，一键开启对应的虚拟机。5、实操竞赛需支持机试实操CTF、风险评估、应急响应、安全防护、攻防对抗AWD等形式，支持个人赛和团队赛。6、需支持题库管理（题库编辑、题库导入导出）、考试管理、考试人员管理、考试暂停等功能。7、需支持竞赛大屏观摩，展示包含实时个人/团队得分、个人/团队能力排行、得分详情，攻击得分TOP5展示、攻击次数和防守次数。8、需支持根据不同的用户场景调整系统的观摩界面板块，生成多种观摩数据，支持定制化竞赛观摩。9、需支持成绩报表导出，导出数据包含“竞赛名称”、“选手名”、“得分”、“答对题目”、“答错题目”等条目。10、竞赛人员能够实时查看个人排名、得分情况、系统公告、比赛时间等相关比赛信息。11、需支持竞赛日志存储，进行日志分析。12、支持答题间隔时间，防止脚本答题13、需支持在平台修改个人得分以及团队得分，并导出成绩。14、需支持对竞赛进行高级规则设定，可设定IP验证、阶梯扣分以及配置AWD等内容。15、需支持对用户账号进行登录绑定IP地址管理，通过限制登录地址来保障系统安全。16、需支持对靶机环境进行管理，可对靶机进行重置、重启、关机以及删除等操作。17、需支持对靶机环境重启行为进行记录，以及针对重启次数规则进行设置扣分值，比如重启3次以上判定为非正常行为，进行扣分。18、需支持模拟仿真数据安全事件的核心业务系统，包含公司的门户网站、内网OA服务器、数据库服务器、安全终端主机。19、需支持真实网络拓扑仿真还原，通过自主拖拽靶机元件设计网络拓扑，一键开启虚拟环境，从而进行安全测试和练习。20、需支持操作机、防火墙、WAF、路由器、交换机、服务器等靶机元件组建自定义拓扑。21、场景题应支持单选题和问答题。22、场景题目应包含题目内容、涉及的靶机类型、答题类型、答案、分值以及涉及的附件。23、场景题需支持通过网络拓扑查看网络拓扑详细信息，查询各设备参数，通过系统提供的环境地址访问靶机进行实战演练。24、需支持场景题，通过场景环境中靶机目标，编辑配置相应的网络拓扑，用户根据场景说明内容，对各个靶机进行渗透分析答题。 | 1 |
| 超融合虚拟化云平台 | 标准机架式2U服务器，Intel Gold 5318Y\*2颗，标配DDR4内存256G，后置SSD系统盘 \*2块（出厂RAID1），4个千兆电口，4个万兆光口，集成IPMI管理模块，前置12个3.5"热插拔SAS/SATA盘位,后置2个U.2 NVME SSD盘位，硬盘8T，冗余电源；配置云计算虚拟化专业版、存储虚拟化专业版、网络虚拟化专业版、统一云管平台高级版授权；计算虚拟化提供虚拟机全生命周期管理、USB映射、备份、快照、最后一屏等功能；存储虚拟化提供统一存储服务，提供存储精简部署、存储卷级存储策略设置、存储数据可视化等功能；网络虚拟化提供拖拽式组网、虚拟路由器、虚拟交换机、连通性测试等功能；统一云管平台对虚拟化平台进行统一管理；虚拟化授权按照CPU数量配置；配置快照数据在线可见，可随时查看和读取快照数据，如当VM内文件发生误操作、误删、中毒、系统配置文件更改时，可以通过该功能对比查看快照时刻VM内的文件，而无需执行VM快照回滚或者恢复，提升使用便捷性。超融合内部的分布式存储支持基于存储卷级别的灵活副本设定，可以针对不同场景对不同的存储卷灵活配置不同级别的副本数，最小支持2副本，最高支持6个副本，并可以支持动态在线增加和删除副本，不需停机即可操作。支持CDP备份功能，且CDP软件功能模块与超融合软件同属于一个公司软件，无需额外单独部署，通过管理平台进行集中管理支持容灾功能，且容灾软件与超融合同属于一个公司软件，不借助第三方软件，用无代理的方式，无需额外部署，通过统一云管平台进行集中管理，支持业务云服务器级容灾配置，提供图形化RPO范围配置，支持1秒到1周 | 3 |