**漏洞扫描设备参数**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| **硬件要求** | **1U机架式结构；**  **最少要4个10/100/1000BASE-T接口和1个可插拨的扩展槽；** |
| 总体要求 | 产品可对系统漏洞、网站漏洞、无线安全漏洞进行深入、彻底的扫描，扫描结束后生成详细的安全评估报告，发送到指定邮箱、FTP服务器，并提供安全解决建议。 |
| 可以并行地检查多个被评估的系统、网站，能够提供扫描策略定制，可以保证扫描的安全性，不影响系统和网站的正常运行； |
| 系统扫描结束后，支持短信、邮件、SNMP、syslog、FTP等告警方式，需支持短信网关自定义； |
| 提供二次开发接口给其他的安全产品或者安全管理平台调用，并提供具体接口的说明文档； |
| 实时显示扫描任务的整体进度和剩余时间，实时显示单个节点的扫描进度和剩余时间 。 |
|  |
| 产品部署要求 | 支持在IPv4、IPv6环境中部署和执行扫描任务； |
| 支持控制中心的多级部署； |
| 支持上级向下级统一进行策略的制定和分发，提供可编辑的策略模板； |
| 支持对全网扫描结果的集中查询、分析； |
| 网络管理 | 支持VLAN划分，支持多VLAN环境下的部署； |
| 自定义网络接口属性； |
| 漏洞扫描能力要求 | 产品扫描信息应包括主机信息、用户信息、服务信息、漏洞信息等内容。需给出各类扫描信息的详细列表，有效漏洞库不低于10000条； |
| 允许管理员配置扫描通知，在扫描任务运行开始时向被扫描的资产发送扫描通知； |
| 产品应支持对扫描对象安全脆弱性的全面检查，如安全补丁、口令、服务配置等。 |
| 产品漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少CVE、CNCVE、CNNVD、BUGTRAQ、CNVID编号； |
| 支持与微软WSUS补丁系统的联动，进行自动化的补丁修补； |
| 应可对Windows系列、Linux、AIX、HPUX、IRIX、BSD、solaris等目标主机的系统进行扫描； |
| 支持SNMP等协议的漏洞检测； |
| 支持主流数据库的检测，应包括但不限于：Oralce、Sybase、SQLServer、DB2等； |
| 支持Windows域环境扫描，可针对目标主机的系统配置缺陷及漏洞进行扫描； |
| 支持多主机、多线程扫描和断点续扫功能； |
| 能扫描Cisco、H3C、华为等主流网络设备； |
| 支持动态的显示扫描结果和实时的查看扫描结果； |
| 提供弱口令扫描功能； |
| Web漏洞扫描 | 漏洞插件库支持按照国际权威安全组织OWASP TOP 10-2013； |
| web扫描支持实时的页面数展示； |
| 爬虫支持Javascript解析； |
| 爬虫支持Java与HtmlElement自动交互能力； |
| 爬虫支持表单自动分析能力； |
| 爬虫支持Ajax解析能力； |
| 漏洞扫描支持SQL注入、Cookie注入、盲注、跨站、文件包含、敏感信息泄露等漏洞检测能力； |
| 历次漏洞结果支持图表展示，并可以通过图标切换至某一次结果的详细内容； |
| 漏洞结果展示支持详细的HTTP请求头内容； |
| 能定时、批量对进行目标检测； |
| 报表能力 | 报告应具有易懂的漏洞描述和详尽的安全修补方案建议，并提供相关的技术站点以供管理员参考； |
| 扫描报告应可对安全的威胁程度分级，并能够形成风险趋势分析报表和主机间风险对比分析报告； |
| 报表具备导出功能，可以导出不同格式的报表，如HTML、PDF、Word、Excel等； |
| 扫描策略 | 产品要求提供多种缺省扫描策略，并可按照特定的需求，灵活制定目标对象或目标群组，可以同时应用不同扫描策略，并允许自定义扫描策略和扫描参数； |
| 支持单机扫描、分组扫描和全部扫描的设置； |
| 支持自动定时扫描和多种计划扫描任务管理功能，可按照指定的时间、对象自动扫描，并自动生成报告； |
| 升级、管理 | 系统应支持人工远程升级。升级内容应包括最新的漏洞库和系统自身的补丁程序； |
| 支持http、ftp等方式进行升级； |
| 支持SSL的Web界面、SSH、Console多种方式； |
| 支持ping,tcpdump,ifconfig,wget等命令； |
| **售后要求** | 原厂1年授权承诺函 |