**一、测试环境说明**

软件环境如下：

|  |  |  |
| --- | --- | --- |
| **终端类别及用途** | **操作系统** | **相关应用软件** |
| *服务器端说明* | centOS 7 | MySQL5.7 JDK1.8 NGINX |
| *客户端说明* | Windows、MacOS | 浏览器 |

硬件环境如下：

|  |  |  |
| --- | --- | --- |
| **终端类别及用途** | **机器配置** | **IPv6地址** |
| *服务器端说明* | CPU：4个，内存：8g，磁盘：160G | 2001:da8:270:2020:f816:3eff:fe8f:91e7 |
| *客户端说明* | - | - |

**二、产品功能测试**

产品类别：□硬件 🗹软件平台 □软件应用系统 □APP □网站

***基于IPv6的网络服务质量监控及多权限消息预警系统***

|  |  |  |  |
| --- | --- | --- | --- |
| **编号** | **功能** | **功能描述** | **完成情况** |
| 登录 | | | |
| 1 | 用户登录 | 输入用户名和密码进行系统登录 | 完成 |
| 仪表盘 | | | |
| 2 | 主机概览 | 网络主机进程数据源接口日志概览 | 完成 |
| 3 | 近24小时残余攻击 | 扫描统计残余攻击IP及攻击次数 | 完成 |
| 4 | 攻击源数量统计 | 攻击IP源次数统计排行 | 完成 |
| 5 | 攻击源地域可视化 | 攻击源分布地域统计环形饼状图 | 完成 |
| 6 | 近24小时高危攻击 | 扫描统计高危攻击IP及攻击次数 | 完成 |
| 主机监控 | | | |
| 7 | 监控列表 | 定期向服务端发送监控数据的主机列表以及主机的内存，CPU占用百分比 | 完成 |
| 8 | 磁盘空间 | 主机上的磁盘信息 | 完成 |
| 9 | 进程空间 | 主机上的进程状态 | 完成 |
| 流量监控 | | | |
| 10 | 网络流量 | 查看各主机上的网络接收/发送情况，单位k/s | 完成 |
| 11 | 系统负载 | 各主机的负载情况，每1分钟，5分钟，15分钟均会更新数据 | 完成 |
| 日志监控 | | | |
| 12 | 攻击源日志 | 平台监测到的所有攻击源IP日志，包括IP地址、地点、攻击次数以及日志抓取时间；同时可以根据IP地址进行检索。 | 完成 |
| 13 | 执行日志 | 该功能主要监测命令执行日志，包括对异常状态的命令执行以及来自白名单的日志，内容包括边界地址、攻击源IP、是否白名单、命令执行内容、执行是否成功、命令结果、错误信息以及命令执行时间。 | 完成 |
| 环境监控 | | | |
| 14 | 机房温湿度 | 查看主机所在机房的温湿度 | 完成 |
| 消息报警 | | | |
| 15 | 渠道设置 | 管理报警提示方式，支持邮件提醒和短信提醒 | 完成 |
| 16 | 阈值设置 | 配置内存，CPU使用率报警上限 | 完成 |
| 17 | 报警记录 | 展示已经发送了的报警记录以及报警原因 | 完成 |
| 权限管理 | | | |
| 18 | 人员管理 | 管理能够登录本系统的人员，可以授权新用户访问系统，包括账号、密码、姓名及状态 | 完成 |
| 19 | 角色管理 | 管理登录系统的人员角色，如主机管理，流量管理员，日志管理员 | 完成 |
| 感知源 | | | |
| 20 | 添加源 | 添加系统感知源信息，包括名称、感知平台、服务协议、主机地址、登录账户、登录密码；数据连接测试，系统将会模拟登录添加的感知源，连接测试成功后完成感知源的添加。 | 完成 |
| 21 | 源列表 | 感知源列表中显示已经绑定的感知源信息，当感知源基本信息发生变更时，可以在源列表中进行信息更新，重新绑定。 | 完成 |
| 联动中心 | | | |
| 22 | 新增边界 | 新增边界包括防火墙IP、用户名、密码、备注信息以及是否启用状态。 | 完成 |
| 23 | 边界管理 | 边界管理包括对已有边界的信息维护，变更边界状态，同时可以根据IP或者状态进行搜索。 | 完成 |
| 24 | 新增命令 | 新增命令包括命令名称、命令内容（规则：${ip}替代攻击源IP，多行命令直接换行）备注信息以及是否启用状态。 | 完成 |
| 25 | 命令管理 | 命令管理包括对已有命令的信息维护，变更命令状态，同时可以根据命令名称或者状态进行搜索。 | 完成 |
| 定时处理 | | | |
| 26 | 新增定时任务 | 新增定时任务需要选择感知源、边界名称、对应命令（以上信息为系统维护的数据），以及输入定时表达式，选择定时任务状态后提交即可。 | 完成 |
| 27 | 管理定时任务 | 对于已经维护的定时任务，可以更新其对应感知源、边界、命令及定时表达式和状态信息。 | 完成 |
| 白名单 | | | |
| 28 | 新增白名单 | 对于特定IP属于非防御范围，需要在此处进行名单的添加，输入IP地址以及备注信息；同时可以解析IP表达式。 | 完成 |
| 29 | 白名单管理 | 可以控制IP的状态及相关基本信息。 | 完成 |
| 系统日志 | | | |
| 30 | 攻击源日志 | 平台监测到的所有攻击源IP日志，包括IP地址、地点、攻击次数以及日志抓取时间；同时可以根据IP地址进行检索。 | 完成 |
| 31 | 执行日志 | 该功能主要监测命令执行日志，包括对异常状态的命令执行以及来自白名单的日志，内容包括边界地址、攻击源IP、是否白名单、命令执行内容、执行是否成功、命令结果、错误信息以及命令执行时间。 | 完成 |