1. **重要接口数据结构**
   1. **导入系统信息：**
      1. 手动导入IP、端口开放信息：

以excel的形式导入系统，系统依此生成策略表

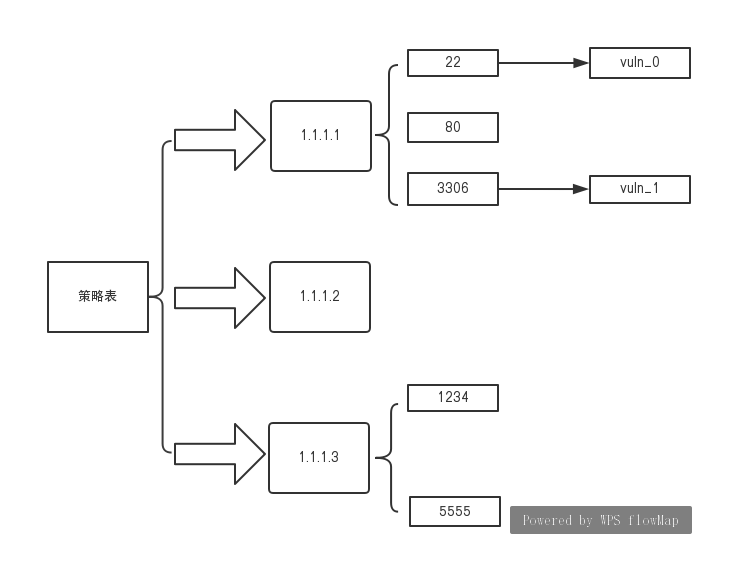
|  |  |  |
| --- | --- | --- |
| IP | port | status |
| 1.1.1.1 | 80 | Open/filter/closed |

* + 1. 手动导入IP列表以txt的形式导入系统，

|  |
| --- |
| 1.1.1.1 |
| 1.1.1.2 |

* 1. **策略表：**

由空闲表生成策略表，系统中上承接用户输入，下分发任务到各模块，其结构如下：

****

* 1. **漏洞转发表：**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | IP | VM\_name | VM\_IP | Port-nat | Docker\_name | Docker\_ip |
| 1 | 1.1.1.5 | VM\_0 |  | 80-80 | Vuln\_0 |  |
| 2 | 1.1.1.5 | VM\_1 |  | 22-22 | Vuln\_1 |  |

1. **模块清单列表**

**后台模块列表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 模块分组 | 模块名 | 功能 | 功能概述 | 备注 |
| 任务模块 | 新建任务 | 新建一个任务 | 开启一个新的任务，初始化所有结构。 | 结构应该包含，任务名、时间、策略表、当前扫描配置、当前扫描进度、当前扫描结果。 |
| 保存任务 | 保存当前任务进度 | 保存的是当前的扫描进度、配置、当前结果 |  |
| 导入任务 | 导入之前的某个任务 | 读取之前的某次任务，导入其所有配置信息。 |  |
| 扫描模块 | 导入目标系统信息 | 手动导入IP、开放端口信息 | 以excel的格式把覆盖范围内的IP列表、端口开放信息导入系统。  格式为一个sheet，总共四列，内容为ip、protocol、port、state，如1.1.1.1 TCP 80 open | 此功能与扫描功能不互斥，可以先后顺序覆盖。 |
| 扫描目标系统信息 | 手动导入IP列表，  由程序生成扫描IP、开放端口信息 | 对系统覆盖范围内的IP进行端口扫描，并处理成excel的定制格式。  格式为一个sheet，总共四列，内容为ip、protocol、port、state，如1.1.1.1 TCP 80 open | 调用nmap扫描，提供参数接口，扫描的时候要显示完成度。 |
| 生成策略表 | 生成空闲IP列表、空闲端口列表 | 根据目标系统的信息，生成空闲的IP列表，以及在线IP的空闲端口列表，保存。 | 策略表索引是树状结构 |
| 过滤模块 | 过滤流量，分发任务 | 依据策略表索引，向各个模块分发需要响应流量 | 工作在 |  |
| IP\_模块 | IP响应表 | 需要响应IP探测的IP列表 | 根据策略表生成响应表 |  |
| IP响应模块 | 响应IP探测 | 接受过滤模块分发的流量，依据IP响应表进行响应 | 响应ping命令 |
| 端口模块 | 端口响应表 | 需要响应端口扫描的端口列表 | 根据策略表生成响应表 |  |
| 端口响应模块 | 响应端口扫描 | 接受过滤模块分发的流量，依据端口响应表进行响应 | 响应-sT -sS扫描 |
| 漏洞模块 | 漏洞转发表 | 需要响应漏洞扫描的漏洞转发表 | 根绝策略表生成漏洞转发表，  包含三部分  IP->VM->docker，数据结构为树状 |  |
| 转发列表控制器 |  | 根据漏洞转发表控制IP到docker的转发关系 |  |
| 硬件管理模块 | 硬件状态表 | 查看当前运行的vm、docker状态，过滤模块的状态 |  |  |
| 硬件管理模块 | VM、docker的增加删除、维护 |  | 做可视化 |
| 覆盖率计算模块 | 统计模块 | 接收扫描报告，统计IP、port基本情况 | 计算扫描报告中策略表的覆盖率 |  |
| 评估模块 | 计算最终覆盖率的结果 | 人工评估漏洞覆盖率并输入、结合IP、port的计算加权计算综合覆盖率 | 分多个层次评估，做可视化 |

**前台模块列表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 模块分组 | 模块名 | 功能 | 功能概述 | 备注 |
| 首页 |  |  |  |  |
| 用户管理 | 用户列表 | 查看系统内的用户 |  |  |
| 资产管理 | 资产列表 | 查看系统内资产 | 查看当前运行的VM、docker状态 | 打印ID、存储、端口映射、运行状态等 |
| 资产管理 | 提供后台硬件管理的可视化接口 | 例如重启、关机等 |  |
| 资产详情 | 展示资产相关信息 |  |  |
| 任务中心 | 提交任务 | 导入目标系统信息 |  |  |
| 任务列表 | 显示所有任务状态 | 状态包含：已提交、进行中、已完成 |  |
| 任务详情 | 展示任务配置 | 扫描信息、完成度、策略表、转发表 |  |
| 评估结果 | 展示已完成的任务 | 展示评估结果 |  |