ARGUS系统

《扫描引擎设计说明书》

2018年9月14日

北京航空航天大学计算机学院

**修订版本**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **修订人** | **日期** | **备注** |
| V1.0 | 夏涛 | 2018.9.14 | 初稿 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目录**

# 引言

## 编写目的

此文档是ARGUS系统的扫描引擎的设计文档

## 读者对象

此文档面向的读者人群为：参与此项目后端开发人员、测试人员、项目经理以及市场营销人员。

# 扫描引擎扫描引擎总体设计

## 扫描模块

调度模块主要用于实现扫描模块的启停，避免频繁扫描使ip被封

## 任务调度模块

实现对指定ip段的扫描，获取设备信息并存入数据库

# 扫描模块设计

## 扫描IP范围设计

ARGUS系统的扫描引擎将覆盖全国的23个省，4个直辖市，2个特别行政区，5个自治区，和台湾。我们将城市的IP段存入数据库表中，扫描引擎可以根据用户指定的城市，从表中取出IP范围进行扫描，数据库表的设计如下：

表名：t\_ip\_subnet

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名** | **类型** | **主外键** | **约束** | **说明** |
| id | int | PK | not null | auto\_increment |
| city | varchar(30) |  | not null | 城市名称 |
| province | varchar(30) |  | not null | 省名称 |
| country | varchar(30) |  | not null | 国家名称 |
| ip\_subnet\_from | varchar(15) |  | not null | IP段起始IP |
| ip\_subnet\_to | varchar(15) |  | not null | IP段终止IP |

## Nmap脚本扫描设计

Nmap的探测脚本功能表：

|  |  |
| --- | --- |
| 功能 | 脚本 |
| 识别使用pcworx的PLC设备 | pcworx-info.nse |
| 识别使用protocol的PLC设备 | proconos-info.nse |
| 探测SCADA Siemens WINCC 服务器 | Siemens-WINCC.nse |
| 检测主机是否被Stuxnet蠕虫感染 | stuxnet-detect.nse |
| 探测Siemens Simatic S7 设备 | Siemens-SIMATIC-PLC-S7.nse |
| 探测SCALANCE 模块 | Siemens-Scalance-module.nse |
| 探测 Siemens 通信处理器设备 | Siemens-CommunicationsProcessor.nse |
| 探测 Siemens SIMMATIC 1200 PLC | s71200-enumerate-old.nse |
| 识别并枚举Siemens PLC设备 | s7-enumerate.nse |
| 用于识别Moxa Nport系列串口服务器设备,并且识别设备的型号和密码设置状态. | moxa-enum.nse |
| 探测维护操作协议（MDP） | mop-discover.nse |
| 检查tcp/102端口 | mms-identify.nse |
| 探测三菱Q系列PLC | melsecq-discover-udp.nse |
| 检查tcp/2404端口 | iec-identify.nse |
| 探测Tridium Niagara Fox 协议 | fox-info.nse |
| 识别和枚举EtherNet/IP设备 | enip-enumerate.nse |
| 检测DNP3地址的有效性 | dnp3-info.nse |
| 探测DNP3设备的目标地址 | dnp3-enumerate.nse |
| 识别使用UDP 9600的欧姆龙设备 | omronudp-info.nse |
| 识别使用TCP 9600 的欧姆龙设备 | omrontcp-info.nse |
| 探测使用Modbus协议的PLC设备信息 | modicon-info.nse |
| 识别ATG协议设备 | atg-info.nse |
| 识别CSPV4设备 | cspv4-info.nse |
| 检测Bradford Networks NAC admin interface | bradford-networks-nac.nse |
| 探测Fingerprints red lion HMI 设备 | cr3-fingerprint.nse |
| 发现codesys-v2设备 | codesys-v2-discover.nse |
| 识别和枚举BACnet设备 | bacnet-info.nse |

Nmap扫描模块使用扫描脚本对选定的IP段进行逐一扫描，获取设备信息。目前主要扫描系统所支持的13种主流协议和摄像头。

协议端口表：

表名：proto\_port

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名** | **类型** | **主外键** | **约束** | **说明** |
| id | int(11) | PK | NOT NULL | ID名 |
| proto\_name | varchar(30) |  | NOT NULL | 协议名 |
| nw\_proto | varchar(30) |  | NOT NULL | 传输协议 |
| port | int(11) |  | NOT NULL | 端口号 |

## 解析器

解析器用于解析Nmap扫描的结果，提取我们感兴趣的设备信息。

## 设备信息存储

设备信息来源于两个部分：Nmap扫描，爬虫爬取。

将扫描和爬虫获取来的设备信息存储在数据库表中，数据库表的结构如下：

表名：instance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名** | **类型** | **主外键** | **约束** | **说明** |
| vender | varchar(255) |  | NULL | 厂商名称 |
| ip | varchar(255) | PK | NOT NULL | 设备ip |
| city | varchar(255) |  | NULL | 城市名称 |
| country | varchar(255) |  | NULL | 国家名称 |
| continent | varchar(255) |  | NULL | 洲/省 |
| asn | varchar(255) |  | NULL | 自治系统号 |
| lat | varchar(255) |  | NULL | 纬度 |
| lon | varchar(255) |  | NULL | 经度 |
| hostname | varchar(255) |  | NULL | 主机名 |
| service | varchar(255) |  | NULL | 服务 |
| os | varchar(255) |  | NULL | 操作系统 |
| app | varchar(255) |  | NULL | 组件名 |
| extrainfo | varchar(255) |  | NULL | 额外信息 |
| version | varchar(255) |  | NULL | 版本 |
| timestamp | varchar(255) |  | NULL | 时间戳 |
| type\_index | varchar(255) |  | NULL | 类型检索 |
| update\_time | datetime |  | NULL | 更新时间 |
| from\_scan | int(11) |  | NULL | 设备来源于扫描 |
| from\_spider | int(11) |  | NULL | 设备来源于爬虫 |
| isp | varchar(255) |  | NULL | 网络服务提供商 |
| organization | varchar(255) |  | NULL | 组织 |
| from\_web | varchar(255) |  | NULL | 信息来源网站 |

设备端口表：

表名：instanceport

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名** | **类型** | **主外键** | **约束** | **说明** |
| id | varchar(36) | PK | NOT NULL | 设备id |
| ip | varchar(255) | MUL | NOT NULL | 设备ip |
| port | varchar(255) |  | NOT NULL | 端口 |
| nw\_proto | varchar(30) |  | NULL |  |
| protocol | varchar(30) |  | NULL | 协议 |
| banner | longtext |  | NULL | 禁止信息 |
| status | varchar(15) |  | NULL | 设备状态 |
| add\_time | varchar(255) |  | NOT NULL | 添加时间 |
| update\_time | datetime |  | NOT NULL | 更新时间 |

Ip-地理位置表用于存储ip地址对应的地理位置：

表名：iplocation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名** | **类型** | **主外键** | **约束** | **说明** |
| ip | varchar(15) | PK | NOT NULL | Ip地址 |
| lat | varchar(15) |  | NOT NULL | 纬度 |
| lng | varchar(15) |  | NOT NULL | 经度 |
| as\_name | varchar(50) |  | NULL | AS名 |
| as\_num | varchar(50) |  | NULL | AS号 |
| bgp\_prefix | varchar(50) |  | NULL | 边界网关协议前缀 |
| location | varchar(50) |  | NULL | 地理位置信息 |
| organization | varcahr(50) |  | NULL | 组织 |
| timezone | varchar(10) |  | NULL | 时区 |
| zip\_code | varchar(50) |  | NULL | 邮编 |

# 任务调度模块

任务调度模块的主要功能是实现扫描模块的定时启动和停止，避免频繁的扫描使得ip被封。

## 定时启动扫描模块

系统维护人员可以设定扫描的时间间隔。

## 4.2启动和停止设备信息爬虫

系统维护人员可以设定爬虫工作的时间间隔