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

此文档是对ARGUS系统的功能、性能、用户界面以及运行环境，系统部署条件等信息做出详细说明。为系统设计阶段提供依据和指导。帮助开发人员、测试人员和相关人员了解系统实现的功能，并作为验证产品是否能满足用户需求的依据。

## 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。

# 任务概述

## 目标

ARGUS系统是一款支持按不同字段（ip、country、city、protocol等）对工业联网设备进行搜索、漏洞收集和统计、安全态势感知、城市工控设备安全状况统计等功能的工业安全状况分析系统（系统定位）。

根据项目的计划，项目的目标主要是实现以下几个方面的功能：

1. 工业联网设备搜索；
2. 设备漏洞的收集和统计
3. 安全态势感知
4. 城市工控设备安全状况统计分析（国内？）

## 用户特点

主要用户是各个企业、工厂的安全管理人员、系统运维人员、政府工业安全部门的负责人、监管人员等。用户需要对系统运维、linux操作系统、windows操作系统、Internet协议、工业互联网、网络安全以及各种类型的工业设备有一定的了解。

## 假设和依赖

本项目能否成功实施取决于以下条件:

1. 研发团队掌握了先进的能适用于该项目的技术，这是系统的性能是否优化、项目能否完成的根本保证；
2. 团队成员的积极配合，为了项目的开发和实施，合理规划个人时间同时为团队做出合理牺牲，配合队友完成任务。

# 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扫描系统设计

Nmap的探测脚本功能表：

|  |  |
| --- | --- |
| 功能 | 脚本 |
| pcworx协议的PLC设备探测 | pcworx-info.nse |
| protocol协议的PLC设备探测 | 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Siemens PLC设备并收集信息 | 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 |
| 探测EtherNet/IP协议 | 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 |
| 探测使用UDP 9600的OMRON FINS远程设备 | omronudp-info.nse |
| 探测使用TCP 9600 的OMRON FINS 远程设备 | omrontcp-info.nse |
| 探测使用Modbus协议的PLC设备信息 | modicon-info.nse |
| ATG协议设备探测 | atg-info.nse |
| 探测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 |
| 探测codesys-v2 | codesys-v2-discover.nse |