基于 openEuler 架构的国产化漏洞扫描系统设计与实现

刘　彬

攀枝花学院　四川攀枝花　617000

摘　要： 本文提出了一种基于 openEuler 架构的国产化漏洞扫描系统的设计方案。系统主要角色包括超级管理员、团队队长、团队管理员和团队队员，功能涵盖系统统计、用户管理、团队协作、项目管理、报告管理、资产测绘、漏洞管理、工具管理等。系统利用 openEuler 操作系统作为底座，采用鲲鹏套件进行调优，具备性能调优、物联网应用、U 盘部署等特性，可用于网络安全评估等多个领域。未来，该系统有望在网络安全服务中发挥重要作用，并在物联网、车联网安全以及区块链安全等新兴领域中得到更广泛的应用。

关键词： 国产化；网络安全；openEule；漏洞扫描

1 项目背景

随着信息化进程的加速和网络攻击的日益频繁，网络安全问题日益受到重视。漏洞扫描作为保障网络安全的重要手段之一，对于及时发现和修复系统漏洞、提高系统安全性具有重要意义。然而，目前市面上大部分漏洞扫描系统多采用国外技术和产品，存在着对外依赖度高、不符合国内特定环境需求等问题，为了满足国内网络安全自主可控的需求，开发基于国产操作系统openEuler架构的漏洞扫描系统具有重要意义。

2 相关技术

2.1 openEuler

openEuler 是一个开源、免费的 Linux 发行版平台，将通过开放的社区形式与全球的开发者共同构建一个开放、多元和架构包容的软件生态体系。同时，openEuler 也是一个创新的平台，鼓励任何人在该平台上提出新想法、开拓新思路、实践新方案。

2.2 Python

Python由荷兰国家数学与计算机科学研究中心的吉多·范罗苏姆于1990年代初设计，作为一门叫做ABC语言的替代品。Python提供了高效的高级数据结构，还能简单有效地面向对象编程。Python语法和动态类型，以及解释型语言的本质，使它成为多数平台上写脚本和快速开发应用的编程语言，随着版本的不断更新和语言新功能的添加，逐渐被用于独立的、大型项目的开发。

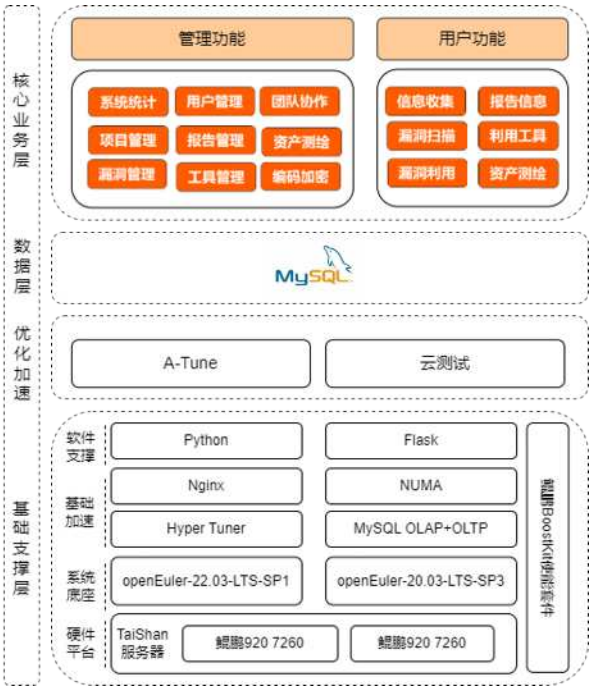

图 1　系统功能架构图

项目编号

2023YB08，项目名称：创新性网络安全漏洞POC/EXP管理巡检系统设计

2.3 Flask Web

Flask是一个轻量级的可定制框架，使用Python语言编写，较其他同类型框架更为灵活、轻便、安全且容易上手。它可以很好地结合MVC模式进行开发，开发人员分工合作，小型团队在短时间内就可以完成功能丰富的中小型网站或Web服务的实现。另外，Flask还有很强的定制性，用户可以根据自己的需求来添加相应的功能，在保持核心功能简单的同时实现功能的丰富与扩展，其强大的插件库可以让用户实现个性化的网站定制，开发出功能强大的网站。

3系统设计

系统的主要角色为超级管理员，团队队长，团队管理员以及团队队员。该系统设计基于渗透测试工作人员与各大单位组织开展攻防演练的实际需求，目的是解决企业指挥团队响应与即时排查的问题，提高相关工作的效率，并保证流程规范。通过相关分析，系统功能划分为五个部分。系统功能架构如图1 所示。

3.1 基础支持层

基础支持层的硬件平台为鲲鹏920 7260芯片的TaiShan服务器，系统底座为openEuler。并采用Hyper Tuner、MySQL OLAP+OLTP、Nginx、NUMA进行基础加速，软件支持使用Python、Flask框架。

3.2 优化加速层

优化加速层采用鲲鹏A-Tune进行智能调优，并使用云测试服务进行进一步调优。该层还采用了自动化监控和调整机制，以动态地根据系统负载和性能需求进行调整。自适应性的优化策略确保系统在变化的工作负载下保持高效稳定的性能。

3.3 数据层

数据层，采用MySQL数据库作为数据支持，采取数据备份和恢复机制，确保数据的安全性和可靠性。实施定期备份和灾难恢复方案，有效地应对意外数据丢失或系统故障的情况，保障业务的持续运行。数据层实现了数据加密和访问控制策略，确保敏感数据的保密性和隐私性。

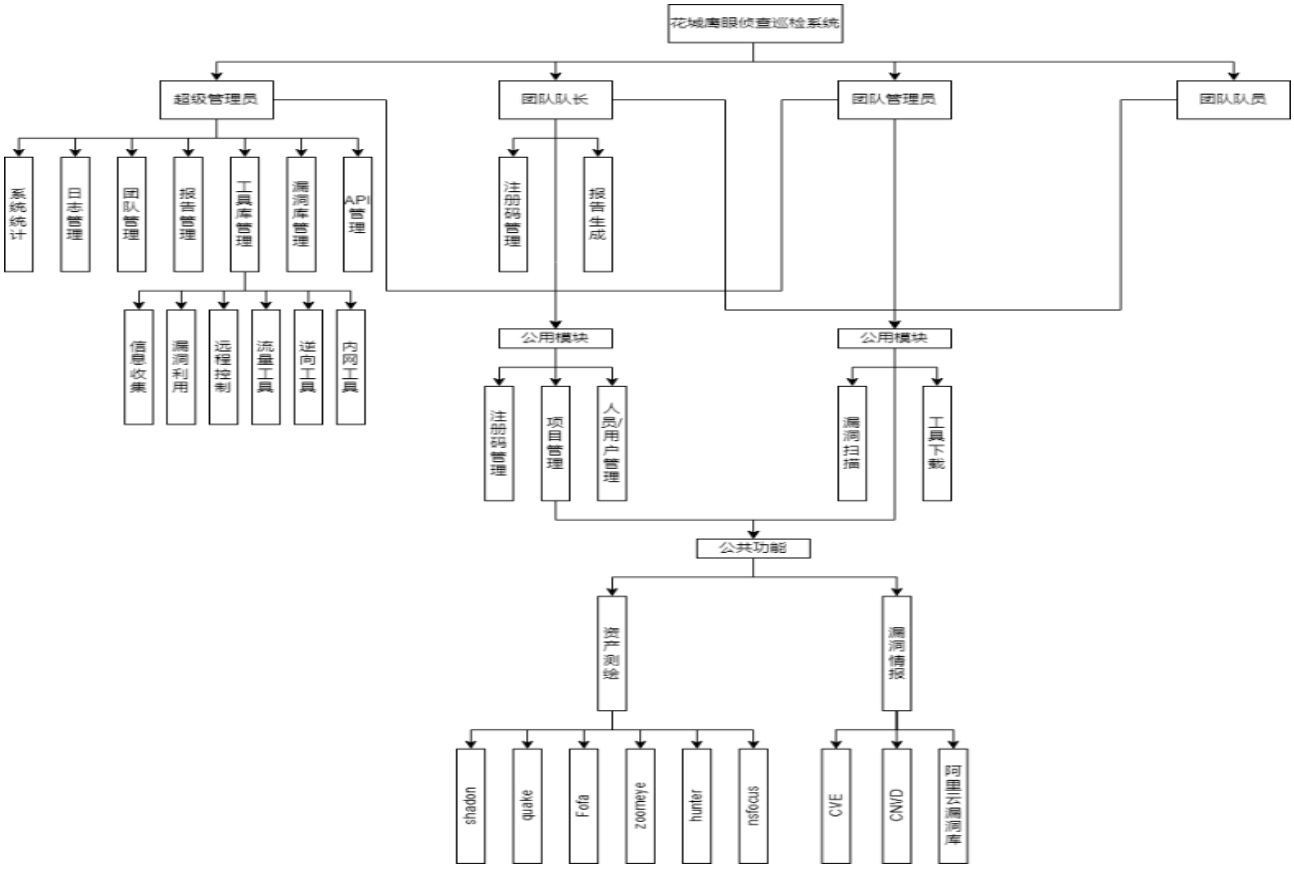

图 2 系统整体细分功能

3.4 核心业务层

核心业务层分为管理功能与用户功能，管理功能包括系统统计、用户管理、团队协作、项目管理、报告管理、资产测绘、漏洞管理、工具管理、编码加密等功能，用户功能则有信息收集、报告信息、漏洞扫描、利用工具、漏洞利用、资产测绘等功能。

系统分为四种权限，超级管理员、团队队长、团队管理员、团队队员。各角色细分功能如图2所示。系统的核心功能为漏洞扫描和资产测绘2个模块。系统具备漏洞库，并支持后台更新，用户使用系统可以进行远程的下载漏洞库。用户可以使用该系统对目标系统进行评估与扫描，发现潜在的威胁，以及快速打通渗透的通道，加快渗透测试节奏。该部分新增了物联网扫描模块，可针对WiFi蓝牙，以及常见的路由设备进行扫描。系统可以使用fofa、zoomeys、quake、hunter、nsfous、shadon进行资产测绘，可以在漏洞扫描，渗透测试前期，对目标系统进行有效的资产评估与收集，简化漏洞扫描与渗透的步骤。

4 系统核心功能实现

4.1 漏洞扫描功能

该功能会先识别代理是否启用，启用则会加入代理设置。检测了代理设置后，会识别UA头，如果是自带则再漏洞扫描时，随机生成UA否则获取用户自定义的UA头。检查操作结束后，会检查扫描地址，如果是单一地址则就行扫描，如果是文件则读取文件后进行逐一扫描，漏洞扫描实现核心代码如下。

```
def Scan(self):
……
        if check == False:
            messagebox.showerror(“错误”,”URL或字典信息错误！”)
        else:
            dir_file = self.info_dict.get()
            if check[0] == “isFile”:
                urls = check[-1]
                for i in urls:
                    i = self.urlmethod.StandURL(i)
                    try:
                            self.Scan(ua,i,dir_file,proxy_status,log_status,proxies)
                    except:
                            back = “{url}扫描中的未知错误”.format(url=i)
                    ……
                    self.count()
……
```

4.2 资产测绘功能

该功能会先加载资产测绘配置，包括API、EMAIL、KEY、SIZE等信息，并通过请求返回给用户，资产测绘实现核心代码如下。

```
def fofa(self,rule):
……
        rule = base64.b64encode(rule.encode(‘utf-8’)).decode(“utf-8”)
        req = self.fofa_api.strip(
            “/”) + “/api/v1/search/all?email=” + self.fofa_email + “&key=” + self.fofa_key + “&qbase64=” + rule + “&size=” + self.fofa_size
        response = requests.get(req, headers=self.header)
        if ‘errmsg’ not in response.text:
            self.asset_info.delete(1.0, tk.END)
        r = json.loads(response.text)
        for i in r[‘results’]:
            s = i[0]
            s_with_protocol = self.url_str.StandURL(s)
……
```

5 项目创新

项目采用国产openEuler操作系统，作为底座，并使用鲲鹏套件进行调优。较之传统的漏洞扫描系统，本系统新增了物联网模块，可以对周边设备进行扫描，WiFi与蓝牙探测，并集成相关的漏洞扫描与验证模块。本项目也可使用安装于U盘系统，U盘刷入Kali Linux Live系统，再将漏洞扫描系统部署于U盘上，实现漏洞扫描系统的即插即用。具体创新为：

5.1 系统整体性能得到提升

系统采用openEuler作为底座进行原生开发，并通过调整系统参数、使用高效的数据结构和算法，以及对代码进

行优化来实现性能调优。系统通过并行计算、异步处理等技术来提高系统的响应速度和并发处理能力，从而提高系统的性能和吞吐量。如图3所示。

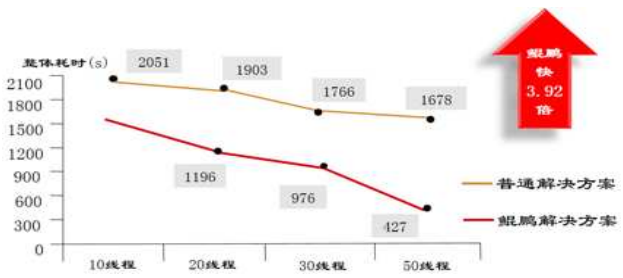

图 3 对某企业全部资产的漏洞扫描速度 (时间取整)

5.2 嵌入物联网应用模块，更好地与周边环境交互

系统中加入了物联网模块，可部署于树莓派设备上，实现近源渗透，可以使系统具备对周边设备进行扫描、WiFi与蓝牙探测的能力。这使得系统可以更好地与周边环境进行交互，并实现更广泛的应用场景。例如，可以通过物联网模块实现智能家居、智能办公等场景，提高系统的智能化和自动化水平。

5.3 U盘部署方便携带使用

通过将系统部署到U盘上，可以实现系统的便携性和灵活性。使用U盘部署系统可以使系统具备即插即用的特性，用户可以随时随地携带系统，并在不同的设备上使用。例如，可以将系统部署到Kali Linux Live系统上，通过U盘启动系统，实现漏洞扫描系统的即插即用。为了实现U盘部署，需要准备一个至少16G的U盘，并在Kali官网下载最新版Live镜像，然后使用Rufus工具将镜像烧录到U盘，最后将本项目部署到U盘上即可使用。

6 项目应用情况

系统已经面向党政机关、民企、网安企业以及各个需要网络安全评估的相关部门(教育、医疗、电力、气象等）开放使用。系统在项目管理、高效漏洞库管理、报告管理、漏洞扫描、资产测绘信息收集等方面展现了良好的功能，政府部门通过该系统对政府信息系统进行安全评估，提高了政府信息系统的安全性和稳定性。企业利用该系统及时发现和修复系统漏洞，保障了企业信息的安全。教育机构通过该系统保护学生个人信息的安全，有效防止了学校信息系统遭受网络攻击的风险。医疗机构利用该系统确保了医疗信息系统的安全和隐私保护。用户普遍反映，该系统易于使用、功能全面，对提升网络安全水平起到了积极的作用，受到了广泛好评。

结束语

本文提出了一种基于openEuler架构的国产化漏洞扫描系统的设计方案。该方案利用openEuler的特点和优势，设计了相应的功能模块，实现了漏洞扫描，资产测绘，团队管理、报告管理等功能。国产漏洞扫描系统的应用有望优化网络安全服务的效率和质量，为安全从业者提供更好的体验。然而，漏洞扫描系统在实践中仍面临一些问题和挑战，需要不断改进和完善。随着技术的进一步发展和应用场景的扩大，如新兴的物联网车联网安全领域，与区块链安全领域，基于openEuler架构的国产化漏洞扫描系统软件将有更广阔的前景和发展空间。

参考文献

[1] 张磊. 鲲鹏架构入门与实战[M]. 清华大学出版社, 2021

[2] [美]TJ O’Connor. Python绝技：运用Python成为顶级黑客[M]. 电子工业出版社, 2016

[3] [美]Neil Madden API安全实战[M]. 机械工业出版社, 2022

[4] 任炬 张晓学 彭许红. openEuler操作系统[M]. 清华大学出版社, 2020

[5] 刘隽良. 脑洞大开：渗透测试另类实战攻略[M]. 机械工业出版社, 2023

作者简介

刘彬（1982—），男，汉族，四川资阳人，网络安全高级工程师，讲师，硕士学位，研究方向：网络安全与国产化开发，邮箱：36637345@qq.com。