第 2 卷◆第 4 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

网络漏洞扫描与渗透测试系统需求分析与设计

干文轩　刘彬
攀枝花学院
DOI:10.12238/acair.v2i4.10355

[摘　要] 本文以网络安全为研究对象,深入探讨了如何满足国内自主可控的需求。文章提出了一种创新的网络安全软件设计方案,该方案结合了鲲鹏技术栈、AI 技术、网络安全以及物联网等领域的先进技术,构建一套完全国产化的漏洞扫描与渗透测试系统解决方案。本文详细阐述了系统的设计思路、功能模块划分、设计方法及采用的关键技术,该方案不仅为网络安全防护提供了有力的技术支持,也具有一定的应用价值和研究意义。
[关键词] 网络安全；漏洞扫描；渗透测试
中图分类号：TN915.08　**文献标识码**：A

Requirements Analysis and Design of Network Vulnerability Scanning and Penetration Testing System

Wenxuan Gan　Bin Liu
Panzhihua University

[Abstract] This article takes network security as the research object and deeply explores how to meet the domestic demand for self-control. The article proposes an innovative network security software design scheme that combines advanced technologies in the fields of Kunpeng technology stack, AI technology, network security, and IoT to build a fully domestically produced vulnerability scanning and penetration testing system solution. This article elaborates on the design ideas, functional module division, design methods, and key technologies used in the system. This solution not only provides strong technical support for network security protection, but also has certain application value and research significance.
[Key words] Network Security; Vulnerability Scanning; Penetration Testing

引言

信息化时代,信息流通越来越便利,受众群体趋向多样化、多元化。随着经济社会的发展,计算机伴随着利己的同时,也带来了一系列的安全问题。近年来,国家高度重视网络安全工作,出台了一系列政策法规,强调加强自主可控的网络安全技术和产品研发,以保障国家信息安全。为满足国家政策和行业发展的需求,本研究致力于开发一套基于鲲鹏技术栈的国产漏洞扫描与渗透测试系统,提高网络安全防护能力,为国家和行业提供有力的技术支持和保障。

1 系统需求分析

1.1系统面向的用户群体。该系统主要服务于网络安全专业人员(如安服工程师、渗透测试工程师、系统管理员、安全运营团队以及安全培训和教育机构等),其应用于评估网络系统与应用安全性、发现修复漏洞、监控管理安全事件、提供安全建议和解决方案以及作为教学工具使用。

1.2系统功能需求分析。需求分析阶段针对系统需要的核心功能进行设计。面对恶意风险威胁的需求,系统可集成AI恶意识别功能,利用人工智能技术,实现高效、精确地识别网络中的恶意内容并进行智能处理与分析。针对漏洞发现需求,系统需设计强大的漏洞扫描模块,能够自动化地检测整体系统及网络中的安全漏洞,即时识别潜在风险,并提供针对性的修复建议,使评估单位能够迅速应对并修复安全漏洞。

系统其他功能需求可包含情报爬虫、渗透测试、端口扫描、报告生成、子域名爆破及资产测绘等。情报爬虫功能应能广泛搜集并分析公开漏洞库信息、安全情报网络信息及威胁情报,为用户提供前瞻性的安全预警。渗透测试功能则通过模拟攻击行为,对系统进行全面的安全测试,评估防御能力,发现潜在漏洞。端口扫描功能需检测目标系统开放的端口,帮助用户了解网络服务分布。报告生成功能能自动生成详细的评估报告,并支持导出及自定义模板。子域名爆破功能能枚举目标域名下的子域名,发现隐藏服务与接口等。资产测绘功能能全面收集网络资产,帮助用户清晰地掌握并分析企业网络架构。

1.3系统性能分析。系统性能优化方面,对于底层优化,系统采用鲲鹏架构进行深度优化,使其发挥出最佳性能。接着对扫描算法进行优化,减少资源消耗,并采取多线程,提高扫描速度,使其在处理大规模网络环境时,能够快速有效地完成漏洞扫描任务。在系统并行处理方面,通过提升系统负载均衡能力,使其在高并发环境中平衡工作负载,避免单点过载影响系统稳定运行。针对国产化开发兼容性方面,使用鲲鹏套件进行兼容性测试,使得系统在各种硬件和软件环境中都能够稳定运行。

2 系统架构设计

系统采用可扩展的层次结构设计,由顶至下分别为核心业务层、安全防护层、数据层和基础支撑层。其中,核心业务层包含渗透模块与漏洞扫描模块,提供全面的安全测试与漏洞识别功能。安全防护层作为系统的中枢,承载着API、认证、业务、运维、主机及开发等多方面的安全。数据层处理并返回核心业务所需数据,其采用华为openGauss国产数据库。基础支撑层基于鲲鹏920 7260芯片的TaiShan服务器与openEuler系统作为底座,结合多种加速技术与框架,为系统提供坚实的硬件与软件支持。

3 系统详细设计

3.1总体功能设计。本系统采用DevSecOps研发模式,避免在后期或产品上线后再处理安全问题。系统采用鲲鹏技术全栈开发,使其具备高性能计算、稳定性强、兼容性好、资源利用率高等优势。同时系统采用了AI以及机器学习等技术进行设计,拓展了系统功能。

结合系统功能需求分析,系统分为渗透模块、扫描模块、核心模块、安全防护模块四个模块,系统功能结构图如图1所示。

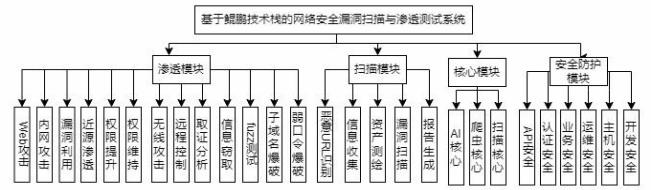

图1 系统功能结构图

(1)渗透模块：渗透模块包含漏洞利用、信息窃取及权限维持三大核心功能。其中,漏洞利用功能将依托自研的漏洞利用代码,精准识别并利用目标系统中的安全漏洞。信息窃取功能则计划采用scapy库,实现网络数据包的发送、嗅探、解析及伪造。相较于Wireshark等工具,它能更直接地获取近源信息。此外,权限维持功能将部署后门程序,并结合持久性攻击技术,确保对目标系统实施持续有效的控制。(2)扫描模块：扫描模块集成信息收集、资产测绘、漏洞扫描等功能。信息收集功能采用网络爬虫技术收集公开信息；资产测绘功能利用资产测绘工具和资产管理功能进行识别与存储；漏洞扫描功能结合漏洞库和自研扫描引擎。(3)核心模块：核心模块设计包含AI、爬虫、扫描三大关键组件。其中,AI核心主要负责智能分析、行为识别及异常检测,其恶意URL识别功能通过综合考量URL的多种特征与标签,运用机器学习算法判断其潜在风险,并依据一系列指标评估模型效能。爬虫核心则专注于漏洞信息的搜集与整理,通过抓取各大平台的漏洞库,实现情报收集与威胁分析,构成漏洞情报的核心处理环节。扫描核心则承担安全漏洞的识别与评估任务,采用脚本载入、Yaml载入等多种验证规则,实现漏洞的快速扫描、验证及利用。(4)安全防护模块：安全防护模块由API安全、认证安全、业务安全、运维安全、主机安全、开发安全等子模块构成,提供全面的安全防护措施。API安全保障系统的通信安全；认证安全防止弱口令、CSRF攻击等；业务安全主要包括防止未授权、账号安全等；运维安全主要包括中间件与组件安全；主机安全主要对业务主机进行基线检查,降低被内网攻击的风险；开发安全作为系统的运行基础,需要对基础的漏洞进行审计,并针对未授权访问、服务请求伪造等漏洞进行修复。

3.2数据处理及业务流程设计。系统总体数据流程可分为漏洞扫描和渗透测试两部分,扫描核心与AI为该两部分提供支撑。总体数据流程图如图2所示。

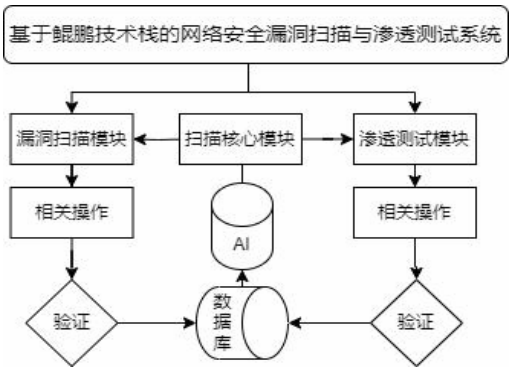

图2 系统数据流程图

系统的业务流程图主要依据模块间功能进行绘制。业务流程图能清晰展示每个相关业务的处理过程及其中涉及到的用户角色,方便用户了解每个模块实现的业务功能及各业务功能之间的关系。本系统的业务流程如图3所示。

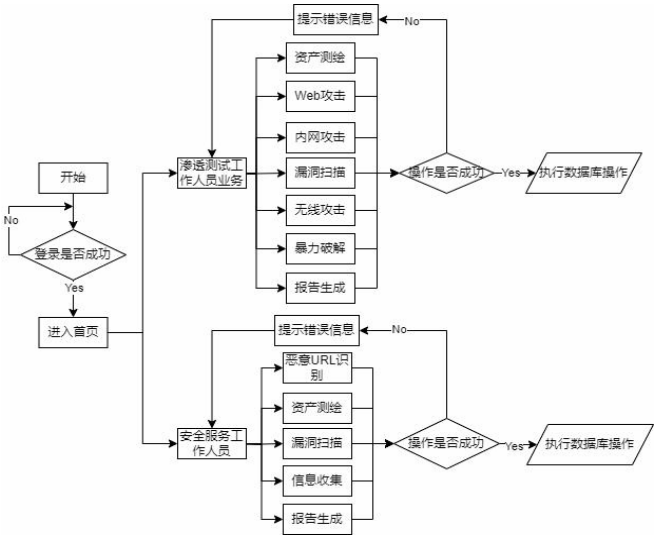

图3 系统业务流程图

3.3数据库设计。openGauss是我国的开源关系型企业级数据库,是GaussDB云数据库服务的开源版本,其内核深度融合华为在数据库领域多年的经验,是结合企业级场景的高安全性、高可用性数据库。系统采用openGauss作为数据库,使其成为更加贴合国产化需求的数据库解决方案,其能够满足复杂应用场景下的高效数据处理需求,降低系统的运维成本。

根据系统的业务功能需求,系统设计了包括用户管理表、漏洞库管理表、漏洞情报表、报告模板管理表、项目管理表、API管理表、漏洞记录表以及目标资产表等一系列数据表。数据表的设计不仅充分考虑了系统的当前需求,还预留足够的扩展空间,以适应未来系统升级和业务扩展的需要。在数据库设计方法上系统更加注重其可维护性与高效性,因其采用了模块化的设计思想,将系统划分为不同的功能模块,系统则为每个模块设计相应的数据表。

3.4系统调优设计。为了提高用户体验,系统采用鲲鹏BoostKit使能套件和A-Tune对系统进行智能调优。鲲鹏BoostKit使能套件能从底层硬件到上层应用进行全面加速。针对网络数据的高吞吐量需求,BoostKit的网络加速模块将优化数据包处理流程,减少延迟,提升数据传输速率。针对扫描过程中可能涉及的大量运算,BoostKit的高性能计算加速功能将利用硬件加速库大幅提升运算效率。针对存储需求,鲲鹏BoostKit的存储优化具备高效的压缩算法和并行处理的能力,可最大化地减少存储开销,加快数据访问速度。

对于A-Tune智能调优,A-Tune拥有在资源管理和性能监控方面的优势,通过深度学习与预测算法,实时监控系统的业务负载和性能瓶颈,智能分析程序运行的状态。此基础上,A-Tune将动态调整系统资源,如在扫描任务繁重时增加CPU核心数量和内存带宽,而在任务较轻时释放资源以供其他业务使用,从而在保证扫描效率的同时,最大化资源利用率。通过上面的自动调优操作,A-Tune会根据任务的特性和系统反馈,智能调整操作系统参数,如内核调度策略、文件系统缓存配置等,并给出调优建议,帮助开发人员进一步优化系统性能。

4 物联网应用设计

系统可部署于物联网设备(如树莓派4B、MicroPython等),其可一定程度上拓展系统的应用场景。具体而言,系统采用MicroPython开发板进行设计,因其价格适中且可完全通过Python语言实现硬件底层控制与访问,使得构建物联网应用系统开发与实现变得更加高效。同时可拓展安全人员的工作场景,如实施针对特定行业与场景的近源渗透与无线攻击,同时系统可进行近源信息收集,为社会工程学攻击提供有利条件,以及在攻防演练中团队协作的远程攻击提供铺垫。

5 便携式工具设计

系统可部署于U盘作为便携式扫描系统,用户通过烧录Kali Linux Live、Parrot OS等镜像,将系统部署于U盘。因其双重系统加密与数据持久化的特点,一定程度上能保护安全工作人员的数据安全,备受安全工作人员关注。便携式攻击工具设计使得攻击场景变得更加庞大,如可将便携式设备(如U盘、移动硬盘等)改造为HID攻击与渗透系统共存的便携式设备,且其可依附于任意电脑设备并作为跳板(如网吧电脑、其他个人电脑等)进行攻击,如在攻防演练中,攻击队可使用便携式设备攻击,因不定期的切换跳板设备,造成了IP地址与网络信息的不可预测,攻击队通过每次修改系统标识,在一定程度上可减少了被溯源的风险。

6 结论

本文深入探讨了基于鲲鹏技术栈的国产网络安全漏洞扫描与渗透测试系统的需求分析与设计。通过对系统需求的全面剖析,明确了系统的核心功能和性能要求,为其后续开发提供了明确的方向。同时,在设计过程中,充分考虑了系统的可扩展性、安全性和易用性,使得系统能够满足不断变化的市场需求和用户期望。本文的研究成果不仅为国产网络安全领域的发展提供了有力的技术支撑,也为后续相关系统的研发提供了有益的参考。

[项目编号]

国家级创新创业项目-刘彬-2024-基于鲲鹏架构的国产化网络安全漏洞扫描系统。

[参考文献]

[1]林美蓉.基于openEuler的openGauss实验环境建设实践探析[J].电脑知识与技术,2023,19(16):78-80+85.

[2]叶水勇,熊惠敏,李亚菇.漏洞扫描工具的研制[J].江西电力,2019,43(10):40-43.

[3]吴婷.轻量级网页漏洞扫描工具的设计与实现[J].电子设计工程,2019,27(12):99-102+107.

[4]王炎,刘嘉勇,刘亮,等.漏洞利用工具研发框架研究[J].计算机工程,2018,44(03):127-131.

作者简介：

千文轩(2002--),男,汉族,四川资阳人,本科,研究方向：网络安全技术。

刘彬(1982--),男,汉族,四川资阳人,硕士,研究方向：网络安全。