学校编码：10384　　分类号_____密级_____

学号：X2012231032　　UDC _____

厦门大学

工　程　硕　士　学　位　论　文

便携式漏洞扫描系统的设计与实现

Design and Implementation of Portable Vulnerability Scanning System

郑向阳

指导教师姓名：　廖 明 宏　教 授

专　业　名　称：　软　件　工　程

论文提交日期：　2016 年 1 月

论文答辩日期：　2016 年 2 月

学位授予日期：　2016 年 6 月

指　导　教　师：_____

答辩委员会主席：_____

2016 年 1 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

伴随着信息技术的不断发展，互联网应用范围的不断拓展，在今天网络已经成为每个人生活中不可或缺的一部分。互联网对人们生活的影响十分深刻，不仅仅是它那些方便的功能，还有随之而来的那些问题。互联网安全一直是讨论的焦点，如何保证网络安全一直是一个非常需要思考的问题。

国内现有的漏洞扫描系统以有线方式为用户提供服务，此方式难以满足网络管理员在故障网络或其它场合随时随地扫描网络的需求。如网络管理员在某地点发现网络设备不能持续工作时，需要回到台式电脑上才能操作漏洞扫描等，这样的处理方式，不但浪费了时间而且带来了解决问题的不确定性。

随着智能移动设备的广泛使用，以智能终端为载体的各种 App 已经成为市场的热点，而基于 Android 的漏洞扫描系统是目前可以接受且最实用的解决方案。

论文首先分析国内外研究现状，在此基础上，结合现有漏洞扫描系统，提出了便携式漏洞扫描系统的解决方案；针对所提出的解决方案，查阅各种参考资料，探索并总结了系统中使用到的各种关键技术；本系统基于 Android 客户端和 linux 系统服务器，使用 Eclipse 作为开发工具，采用 Java 开发语言，结合开发模式，根据本系统的设计目标和原则，提出的系统设计方案，以网络管理员方便扫描网络的漏洞为导向，完成系统的整体构架设计和各个功能模块设计，最终设计并实现了便携式漏洞扫描系统。最后本文对此系统进行了总结，并对系统的进一步完善提出了具体的建议。

关键词：Android；漏洞扫描；漏洞库

Abstract

With the continuous development of information technology, the Internet application scope expanding, in today's network has become an indispensable part of everyone life.The Internet's impact on people's life is very profound, not only is it the convenient function, and the problems that ensued.Internet security has always been the focus of the discussion, how to guarantee the network security has always been a very need to think about problem.

Domestic existing vulnerability scanning system to provide users with services in cable way, this way is difficult to meet the network administrator in the fault network scan network demand anytime and anywhere, or other occasions.Found in a certain area such as the network administrator network equipment can't continue to work, need to go back to desktop computers to operate vulnerability scanning, and so on, this way, not only waste of time and brings the uncertainty to solve the problem.

With the wide use of smart mobile devices, intelligent terminal as the carrier of all sorts of App has become a hot spot of the market, and the vulnerability scanning system based on Android is acceptable and the most practical solution.

Paper first analysis the research status at home and abroad, on this basis, combining with the existing vulnerability scanning system, and puts forward the portable vulnerability scanning system solution;For the proposed solution, refer to the various resources, explore and summarize the system used in a variety of key technologies;This system is based on the Android client and Linux servers, using Eclipse as a development tool, using the Java development language, combining with the development mode, according to the design goals and principles of this system, puts forward the system design scheme, network administrators convenient scanning loopholes oriented, to complete the whole system architecture design and each function module design, portable vulnerability scanning system was designed and implemented in the end.At the end of the paper in this system are summarized, and the system of further perfecting the concrete Suggestions are put forward.

Key words: Android ;Vulnerability Scanning;Vulnerability Database

目　录

Contents

第一章 绪论

1.1 背景

自从 Internet 在美国诞生以来，虽然各国对这个新鲜实物的态度不一，但是它的发展却是势如破竹，从来没有一个新鲜事物可以像这样的野蛮生长，将全世界变成了地球村，再远的距离似乎也可以咫尺天涯。Internet 渗透到了各个各个行业，完全的改变了各行各业的生存法则，重新塑造了人们的生活方式，在个人的生活中，Internet 变成了不可或缺的一环，同时，任何人、任何行业都变得前所未有的依赖 Internet[1]。

任何人都无法想像，如果没有了网络的支持，生活将变成什么样子？也许是一团糟吧。很多时候，黑客为了一定的目的而无孔不入，如果熟悉的网络被人恶意的操控与破坏，这可能就会带来大面积的破坏，如果没有一定的措施，我们在恶意分子面前将毫无还手之力。因此，我们需要一定的措施以保卫网络安全，网络安全问题伴随着网络的成长而诞生，它从来都是网络从业人员的关切以及研究的焦点，但是对此却从来不能放下心来[2]。

目前互联网的安全性到底是怎样的情况呢？从一些研究资料可以得出，70%以上的网络均为存在安全隐患的网络。如今加强网络安全的主要办法有三类，防火墙技术，入侵检测技术以及漏洞扫描技术[3]。防火墙位于内网与外网络之间的防御机制，遵循事先制定的规则让数据通过或者不通过，是防御的主要途径，但是它机制呆板，安全性低，对网内安全防护能力低。入侵检测在关键点上动态监视着网络并分析收集的信息，从而检查是否存在异常情况，一定程度上提高了安全等级，但也属于事后处理方案之一。而漏洞扫描对比其他两种更加主动[4]，它不是在事后进行处理，而是事先检测网络情况，找出可能的漏洞，而黑客们的攻击大多利用各种各样的漏洞，然后穿过一层层防御，如果能将所有漏洞安全的维护，理论上就能杜绝一切的黑客攻击[5]。

在最近几年里，我国通信技术的进步日新月异，智能的终端急速普及[6]，因此，通过智能终端获得讯息、处置事务、消遣娱乐的的可能性越来越大，相关市场上的 APP 保有量也日渐增加。

Android 和 IOS 已经占据了智能移动操作系统市场份额的绝大部分。目前的最新数据，就手机而言，Android 操作系统平台的份额已经升至 84.7%[7]。Android 操作系统具有处理速度快、美观易用的人机界面、开放的平台、海量应用程序等特点。Android 不仅仅用于个人移动终端，而且普遍应用刚在在金融、物流、航空等移动性和数据即时更新要求比较高的行业中。

1.2 国内外研究现状

恶意软件等安全问题无时无处不胁迫着网络，进而导致我们使用网络的困惑。而能预防同时可以评估安全漏洞的漏洞扫描工具收到了网络从业人员的青睐，从早期的 SATAN 开始，各个公司陆陆续续推出了很多的漏洞扫描系统，目前主流的扫描系统有扫描器之王之称的 Nmap 工具，免费产品的代表是 nessus，堪称"全球最广泛使用的的漏洞扫描系统，大概八万个组织在使用"，还有 appscan、webinspect 等 web 应用扫描器。

在国内，大多数的公司开发的都是一些扫描小工具，开发专用化的漏洞扫描工具的几乎很少，更多的是类似瑞星杀毒，360 安全卫士的集成型的软件中附带本机以及本机的网络漏洞扫描，此类软件都将漏洞扫描屏蔽在超级简单的操作之下，让使用条件变得极低，这样也带来的问题就是，漏洞扫描的对象以及针对漏洞的类型都是这类软件统一提供，不能自己专门定制，在简单操作的束缚下自由度大大降低。

目前，一般的专用漏洞扫描工具软件都是基于电脑平台的，不具备移动性，更加不能无时无刻的随地扫描网络空间的漏洞。

1.3 论文研究内容与意义

本课题研究基于 Linux 服务器端和 Android 客户端的便携式漏洞扫描系统，不只能够形成各种漏洞模板，并且能够自定义漏洞模板。本系统着重于对配置的各个设备所形成的网络进行漏洞扫描，并将结果交给网络从业人员，提供不同方面的成体系的维护建议，是一个专业化的、并且具备便携特性的漏洞扫描工具。

系统的实现能够拓展扫描的地点，同时也能增加使用时间自由度；提升了工作效能，能够弱化网络从业人员的劳动强度。

1.4 论文结构安排

本课题首要任务是满足国内现阶段便携式漏洞扫描系统的需求，基于 Linux 服务器和 Android 客户端，设计并实现了具备强大扫描能力并能应用到各种环境的漏洞扫描系统。本文重点研究以下问题：

第一章绪论。描述了移动操作系统的现状和互联网络的安全现状，随后介绍了国内外漏洞扫描系统的使用情况，并对便携式漏洞扫描系统的的必要性做了分析。

第二章关键技术介绍。介绍了在 Linux 系统和 Android 系统上实现漏洞扫描系统所使用到的一些重要的技术，例如 JNI 技术、端口扫描技术等。

第三章需求分析。本章首先分析建立漏洞扫描系统的可行性，并分析了本系统所应达到的功能性需求和非功能性需求

第四章总体设计。本章首先介绍了与本系统主要架构，接着描述了系统模块图，然后说明了数据库如何进行层次设计，最后展示了重要的数据表。

第五章详细设计。本章展示基础模块的设计思路与具体代码，首先结合第四章的总体设计确定了本课题 UI 界面总体风格和一些自定义控件的完成代码，然后按系统模块设计分步骤具备说明了完成模块功能具体思路与主要代码，并摘录了功能模块的关键代码。

第六章系统测试。本章节描述了测试目的和测试原则，并以功能测试为着重点，测试了本软件的基础功能和核心模块。结果数据显示达到系统的开发需求，也符合课题的设计要求。

第七章总结与展望。总结本课题所涉及的一些事物，说明实现的系统的优缺点，并且针对本课题可能的改进措施进行了思考。

第二章　关键技术概述

2.1 基于组件的漏洞库设计

针对搜集的漏洞的管理是本课题研究内容的重要方面，大部分网络上流行的漏洞扫描工具都忽略了对此的管理，这会导致后期维护比较困难，针对漏洞库的漏洞组件的增加也会带来麻烦。基于此，本软件针对整个漏洞库的漏洞的特性进行分门别类，每个漏洞都分属不同的类别，并且考虑后期可拓展性，采用组件的形式维护漏洞，每当发现新的漏洞就及时将其编写成一个组件加入组件库，同时对组件进行归类管理[8]。

目前，并没有一个标准对安全漏洞进行详细的分类，相当一部分的漏洞你可以将其划分在一类中，也可以将它划分在另一类当中，但是这并不方便于管理与拓展。所以本软件将所有的漏洞分类为缓冲区溢出，CISCO 设备，身份验证，数据库，默认账户，拒绝服务检查，指纹识别滥用，恶意软件，暴力攻击等等 27 个预定义的漏洞族，然后再将已知的所有的漏洞作为组件分别归类在所有的漏洞族之下。这部分信息是由专门人员进行维护的，对用户而言可见的是一个个漏洞模版，将所有的漏洞族对应为相应数量的预定义漏洞模版交给网络管理员，网络从业人员也能够利用漏洞族或者组件组合出他们需要的自定义的漏洞模版，但是无法修改漏洞信息以及漏洞族信息，这样更加安全，可以确保基础漏洞信息的精确无误。

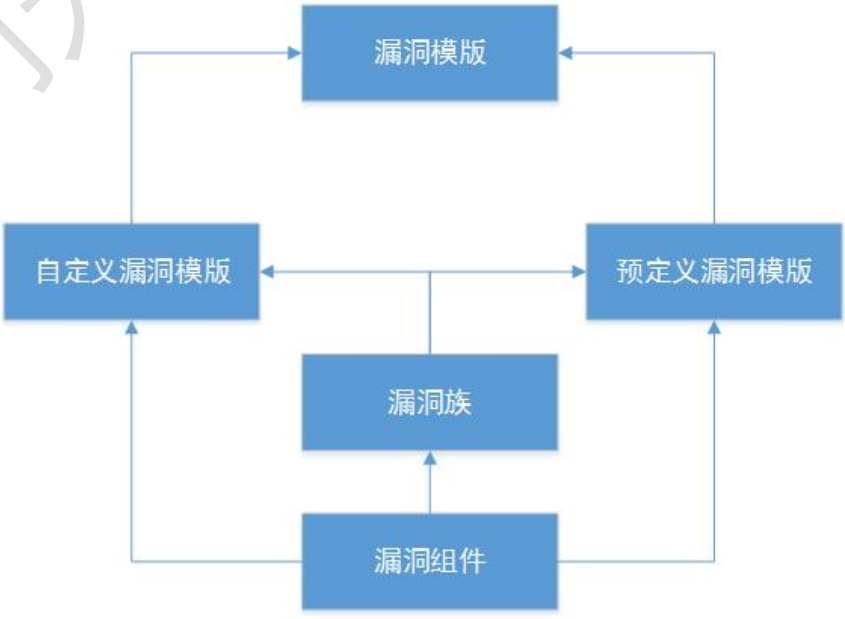

图 2 - 1 漏洞关系图

2.2 基于 NMap 的端口扫描技术

端口扫描是漏洞扫描软件中必不可少的手段，面对未知的设备，怎样获得这些设备的诸如操作系统、开放端口等详细讯息就是重中之重，而本技术则能实现这一点。本技术的达成主要依靠 NMap 的技术原理，Nmap 技术的探测方式五花八门，无所不包，总共有十多样[9][10]。

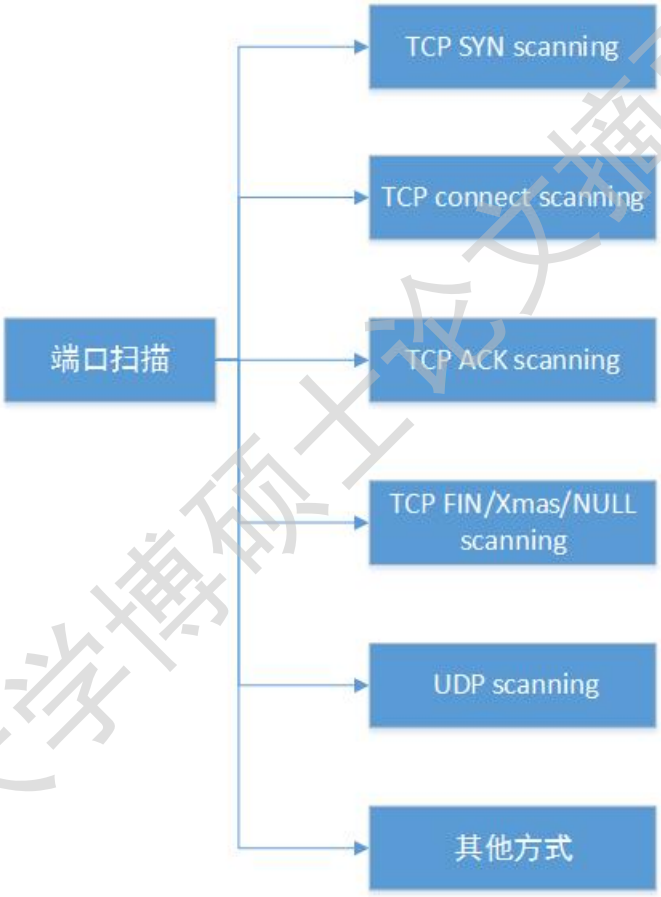

图 2 - 2 端口扫描方式

1、TCP SYN scanning

半开放扫描（Half-open scanning），它的原理是利用 SYN 报文的回复报文情况推测端口的状态是否开启[9]。如果收到 RST 包，那么我们能够推测被扫描端口是关闭的；如果根本没收到回复，那么我们能够判定该端口被屏蔽了；如果收到 SYN/ACK 的报文，那么我们能够断定该端口为开放状态。该方法没有试图完成 TCP 的三次握手，因此，该方法拥有一定的隐蔽性，适用方向较广。