学校编码：10384　　分类号＿＿＿密级＿＿

学号：X2010230661　　UDC ＿＿＿

厦门大学

工 程 硕 士 学 位 论 文

某地税网络系统脆弱性分析与修补

Analysis and Repair of the Network Vulnerability of a Local Tax Systems

刘志鹏

指 导 教 师： 廖 明 宏 教 授

专 业 名 称： 软 件 工 程

论文提交日期： 2012 年 9 月

论文答辩日期： 2012 年 11 月

学位授予日期： 年 月

答辩委员会主席：＿＿＿＿＿＿

评 阅 人：＿＿＿＿＿＿

2012 年 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）：

2012 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）：

2012 年　　月　　日

摘 要

近年来，网络安全问题已经越来越受到人们的重视。造成计算机网络系统安全问题的原因是多种多样的，但是可以把它们大致分为两类：即外在的威胁和内在的脆弱性。潜在的威胁源越多，威胁发生的可能性越大。如果把威胁看作造成计算机网络系统不安全外因，那么造成网络系统不安全的内因，或者说最根本的原因，则在于系统本身存在脆弱性。脆弱性并不对资产构成危害，但是在某些特定环境下被利用时，脆弱性就会变成对信息资产造成危险的主要突破点。可以说系统遭受损失，最根本的原因在于计算机网络系统本身存在脆弱性。所谓脆弱性，是指网络系统中一切可能被用来作为漏洞攻击的因素。各种潜在的威胁通过利用这些漏洞都可能给整个网络和系统造成损失，网络脆弱性存在于网络系统安全程序、设计、应用和内部控制等各方面。

系统安全漏洞，在一定意义上也可等同于系统脆弱性，就是指计算机系统在硬件、软件、协议的设计、实现以及系统安全策略上存在的缺陷和不足。从广义上对系统安全而言，一切可能导致系统安全受影响或破坏的因素都可以视为系统安全漏洞。安全漏洞的存在，使得其他用户可以通过这些漏洞获得系统的某些权限，然后对系统进行非法操作，导致安全事件的发生。漏洞检测就是希望能够防患于未然，在漏洞被利用之前发现漏洞并修补漏洞。

本文采用了基于漏洞扫描的系统脆弱性评估方法。通过具体的测试检验该系统的安全性，并对系统的不足之处提出了改进方案。但是由于税务系统的特殊性，有时通常情况下的安全性修补又会与工作中的实际需求发生冲突，故而本文所做的脆弱性分析和修补必须在满足工作需求的情况下，最大限度的满足安全需要。

关键词：网络安全；脆弱性；安全漏洞；安全性修补

Abstract

In recent years, network security issues have been more and more attention. Computer network security issues for many reasons, but they can be grouped into two broad categories: the external threats and internal vulnerability. Threats from the point of view, it is the underlying source of the threat, the more likelihood of threat.If the threat as external factors, then the system is not secure, the result can also be said that the most fundamental reason lies with the system itself, there is vulnerability. vulnerability itself does not constitute a crime against property, but to a certain condition is met, and the vulnerability will be exploited by threats to information assets.System losses, the most fundamental reason is that your computer network system is vulnerable. So-called vulnerability of a network, any can be used as a prerequisite for an attack. Each of the potential threat of the use of the vulnerability of the network and system losses, network vulnerability exists on the network system security, design, applications and internal control.

System security vulnerability, and can also be called a system vulnerability, refers to a computer system in hardware, software, protocols, and specific to the design as well as the system security policy on the flaws and deficiencies exist. System Vulnerability, system security is a relative, and in the broad sense of perspective, all this can cause the system security are affected or damaged elements can be considered as system security vulnerabilities.There is a security vulnerability, so that users can take advantage of these illegal vulnerability to gain some privileges on the system, and thus to the illegal actions, resulting in security incidents. I hope to be able to exploit that in the bud, before the vulnerability to be exploited vulnerability discovered vulnerabilities and patches.

This article is based on the vulnerability scanning system vulnerability assessment methodologies. Examined the security of this system through the concrete test, and the inadequacies of the system by improving the program. However, because of the tax system, sometimes under normal circumstances the security patch, the work

of the real needs in a conflict between this article and so do the vulnerability analysis and repair must be to meet the needs of the situation, the utmost security requirements.

Key words: Network Security；Vulnerability；Security Vulnerability；Security Repair

目 录

第一章 绪论 1
1.1 研究的背景和意义 1
1.2 国内外研究现状 2
1.3 主要研究内容 3
1.4 论文章节安排 4
第二章 网络系统脆弱性分析方法 5
2.1 名词解释 5
2.2 基于漏洞检测的脆弱性分析方法 6
2.2.1 漏洞产生的原因 6
2.2.2 漏洞的分类 6
2.3 漏洞扫描技术 11
2.4 天镜脆弱性扫描与管理系统 16
2.5 本章小结 22
第三章 某地税网络系统安全现状及问题 23
3.1 网络现状描述 23
3.2 网络设备现状 25
3.3 安全措施现状及存在的问题 26
3.4 本章小结 27
第四章 某地税网络系统脆弱性分析 28
4.1 脆弱性分析方法 28
4.2 DMZ 区服务器脆弱性分析 29
4.2.1 漏洞风险分布统计 29
4.2.2 高危漏洞主机分布 30
4.2.3 主机扫描统计列表 31
4.2.4 主要高危漏洞列表及分析 31
4.3 内网区服务器脆弱性分析 31

4.3.1 漏洞风险分布统计.....31
4.3.2 高危漏洞主机分布.....32
4.3.3 主机扫描统计列表.....33
4.3.4 主要高危漏洞列表及分析.....33
4.4 网络设备脆弱性分析.....34
4.4.1 漏洞风险分布统计.....34
4.4.2 高危漏洞主机分布.....35
4.4.3 网络设备扫描统计列表.....35
4.4.4 主要高危漏洞列表及分析.....35
4.5 客户端脆弱性分析.....36
4.5.1 漏洞风险分布统计.....36
4.5.2 高危漏洞客户机分布.....37
4.5.3 客户机扫描统计列表.....37
4.5.4 主要高危漏洞列表及分析.....39
4.6 本章小结.....39
第五章 某地税网络系统脆弱性修补.....40
5.1 脆弱性修补方法.....40
5.2 DMZ 区服务器漏洞及修补.....40
5.2.1 扫描信息.....40
5.2.2 漏洞列表.....41
5.2.3 详细列表及修补方法.....42
5.3 内网区服务器漏洞及修补.....58
5.3.1 扫描信息.....58
5.3.2 漏洞列表.....58
5.3.3 详细列表及修补方法.....60
5.4 网络设备漏洞及修补.....65
5.4.1 扫描信息.....65
5.4.2 漏洞列表.....65
5.4.3 详细列表及修补方法.....66

5.5 客户端漏洞及修补 66
5.5.1 扫描信息 66
5.5.2 漏洞列表 66
5.5.3 详细列表及修补方法 67
5.6 本章小结 69
第六章 脆弱性修补后的安全测试 70
6.1 DMZ 区安全测试 70
6.2 内网区安全测试 71
6.3 网络设备安全测试 72
6.4 客户端安全测试 73
6.5 本章小结 74
第七章 总结与展望 75
7.1 论文总结 75
7.2 工作展望 75
参考文献 77
致 谢 79

Contents

Chapter 1 Preface.....1

1.1 Background and significance of the research.....1

1.2 Current situation of domestic and foreign research.....2

1.3 The main research content.....3

1.4 Dissertation chapter arrangement.....4

Chapter 2 Methods for vulnerability analysis.....5

2.1 Noun explanation.....5

2.2 Vulnerability analysis method based on vulnerability detection.....6

2.2.1 Causes of vulnerability.....6

2.2.2 Vulnerability classification.....6

2.3 Vulnerability scanning technology.....11

2.4 Tian Jing vulnerability scanning and management system.....16

2.5 Summary.....22

Chapter 3 Network architecture and security.....23

3.1 Current Network description.....23

3.2 Network equipment.....25

3.3 Security status quo.....26

3.4 Summary.....27

Chapter 4 Local tax network system vulnerability analysis.....28

4.1 Vulnerability analysis methods.....28

4.2 DMZ zone server vulnerability analysis.....29

4.2.1 Vulnerability risk distribution statistics.....29

4.2.2 High-risk vulnerabilities host distribution.....30

4.2.3 Host Scan Statistics list.....31

4.2.4 Major high-risk vulnerabilities list and analysis.....31

4.3 Internal network zone server vulnerability analysis.....31

4.3.1 Vulnerability risk distribution statistics 31
4.3.2 High-risk vulnerabilities host distribution 32
4.3.3 Host Scan Statistics list 33
4.3.4 Major high-risk vulnerabilities list and analysis 33
4.4 Network device vulnerability analysis 34
4.4.1 Vulnerability risk distribution statistics 34
4.4.2 High-risk vulnerabilities host distribution 35
4.4.3 Host Scan Statistics list 35
4.4.4 Major high-risk vulnerabilities list and analysis 35
4.5 Client vulnerability analysis 36
4.5.1 Vulnerability risk distribution statistics 36
4.5.2 High-risk vulnerabilities host distribution 37
4.5.3 Host Scan Statistics list 37
4.5.4 Major high-risk vulnerabilities list and analysis 39
4.6 Summary 39
Chapter 5 Local tax network system vulnerability repair 40
5.1 Vulnerability repair methods 40
5.2 DMZ zone server vulnerability and repair 40
5.2.1 Scanning Information 40
5.2.2 Vulnerability list 41
5.2.3 Detailed lists and repair method 42
5.3 Internal network zone server vulnerability and repair 58
5.3.1 Scanning Information 58
5.3.2 Vulnerability list 58
5.3.3 Detailed lists and repair method 60
5.4 Network device vulnerability and repair 65
5.4.1 Scanning Information 65
5.4.2 Vulnerability list 65
5.4.3 Detailed lists and repair method 66

5.5 Client vulnerabilityand repair 66
5.5.1 Scanning Information 66
5.5.2 Vulnerability list 66
5.5.3 Detailed lists and repair method 67
5.6 Summary 69
Chapter 6 Safety tests 70
6.1 DMZ zone security test 70
6.2 Internal network zone security test 71
6.3 Network device security test 72
6.4 Client security test 73
6.5 Summary 74
Chapter 7 Summary and prospects 75
7.1 Conclusions of the dissertation 75
7.2 Future works 75
References 77
Acknowledgements 79

第一章　绪论

1.1　研究的背景和意义

计算机系统在设计、实施、操作和控制过程中存在的可能被攻击者利用从而造成系统安全危害的缺陷称为脆弱性(Vulnerability)。要了解脆弱性，首先要从信息安全说起。信息安全包括的范围很大。大到国家军事政治等各类机密安全，小到如防范各行业机密泄露、防范不良信息的传递、个人信息被暴露等。网络环境中的信息安全体系是保证信息安全至关重要的因素，包括计算机操作系统安全、各种安全协议、安全机制（数字签名、信息认证、数据加密等），任意一个安全漏洞都有可能威胁到全局安全。信息安全服务必须至少包括对信息服务网络安全、 最新的安全网络和基于信息服务的体系结构的网络体系结构的基本理论的支持[1]。

我们所要研究的系统脆弱性主要面对的是信息安全中的网络安全。网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全[2]。从广泛的意义上来说，所有的网络上信息的机密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的技术研究领域。网络安全是涉及计算机科学、计算机网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息理论等多种学科的综合性学科[3]。

网络协议、网络软件、网络服务、主机操作系统及各种主机应用软件在设计及实现上存在种种安全隐患和安全缺陷是网络安全存在的脆弱性的根源。脆弱性分析是网络安全风险分析与控制的关键技术，是实施信息网络安全控制的关键环节，它贯穿于项目信息网络的整个生命周期。自动和系统地进行脆弱性分析是目前的研究重点。同国外相比，我国脆弱性信息的实时性和完整性尚欠缺，主要原因在于脆弱性的发现滞后。而脆弱性检测、修补等都受制于脆弱性的发现。所以，脆弱性分析成为当前最热门的研究方向之一[4]。

在税务系统中，网络系统的连接形式多样且终端分部不均匀。使得网络存在

着开放性、互联性从而导致网络容易受到黑客、病毒、截包、DOs 拒绝服务、分布式拒绝服务、口令攻击、非法窃听等攻击，这些情况可能会导致税务系统内部数据泄漏、数据的完整性遭到破坏、以及正常用户无法使用服务、网络系统被滥用[5]。由于服务器、程序、脚本、系统漏洞或者非法使用外部网络导致重要信息泄露，非授权访问数据库、删除或者修改数据等安全隐患都将对整个网络系统的安全运行以及数据的完整性造成极大威胁。但是由于税务系统的特殊性，有时通常情况下的安全性修补又会与工作中的实际需求发生冲突，故而本文所做的脆弱性分析和修补是在满足工作需求的情况下，最大限度的满足安全需要。

1.2 国内外研究现状

脆弱性是与信息资产相关联的弱点或安全隐患。脆弱性本身并不对资产构成危害，但是满足某些条件时，脆弱性会被利用来对信息资产造成危险。

系统脆弱性是相对系统安全而言的，从一般的角度来看，所有可能影响或破坏系统安全性的因素都可以视为系统安全漏洞，也就是硬件，软件或使用策略上的缺陷，他们会使计算机遭受各种攻击。系统的安全监测与分析技术起源于上世纪 90 年代。早在 1992 年 Chris Klaus 在完成 Internet 相关技术的实验，开发了 ISS 漏洞扫描工具，用于远程探测 UNIX 系统中的各种漏洞及信息。1995 年，Dan Farmer 和 Wietse Venema 发布了一种叫做安全管理员网络分析工具 SATAN（Security Administrator Tool for Analyzing Networks）的软件，其本质与 ISS 工具相同，改进了扫描引擎的算法，使其具有分类检索的能力。2003 年，Tenable 安全公司推出了被动式漏洞检测器 NeVo ，这款检测器可以连续进行的漏洞检测[6]。近年来各种基于不同原理的检测工具层出不穷。

目前我国关于漏洞检测技术的研究开展比较晚，虽然取得了一些研究成果，但是和国外的技术水平还存在一定的差距，有很多的安全方案需要依然国外的技术。国内近几年也出现了一些主打网络安全产品的公司，例如绿盟科技，天融信，交大捷普和启明星辰等。国内应用程序漏洞检测和修复系统主要是在 Windows 平台下，可以检测和修复 Windows 操作系统的漏洞，主流软件有：360 安全卫士、金山清理专家、瑞星卡卡上网安全助手等。

近几年我国税务信息化建设的不断发展，税务系统信息安全防护水平也在逐

步提升，从一开始以网络为主体的防护体系建设进入了以业务系统为核心的重要改革阶段，从局部加强升级到了整体优化阶段。脆弱性分析是系统安全评估的基础以及安全保障体系重要组成部分。及时检测到脆弱点和修补脆弱点，对于保障和提高网络系统的安全性是非常重要的。

1.3　主要研究内容

本文的主要内容为针对某地税系统进行的脆弱性分析，在理论层面上的脆弱性分析只是作为具体情况的铺垫，并不过多的进行描述及研究。重点集中在实践阶段由于税务系统的特殊性，有时通常所使用的脆弱性修补方法并不能在满足了安全需要的同时满足税务系统的安全配置方式。具体内容包括非军事区（De Militarized Zone，DMZ。作用是把 WEB，e-mail，等允许外部访问的服务器单独接在该区端口，使整个需要保护的内部网络接在信任区端口后，不允许任何访问，实现内外网分离）、内网区、网络设备及客户端的脆弱性扫描。脆弱性扫描就是利用工具对信息系统设施进行扫描，发现各种漏洞，亦可称为漏洞扫描。

漏洞扫描：分为主机漏洞扫描技术和网络漏洞扫描技术两类。基于网络的扫描是从外部攻击者的角度目标系统的端口，所开放的服务及架构进行扫描，主要用于查找网络服务和协议中的漏洞。基于网络的扫描可以及时获取网络漏洞信息，有效的发现那些网络服务和协议的漏洞，如 DNS 服务和底层协议的漏洞；同时能够有效的发现那些基于主机的扫描不能发现的网络设备漏洞，如路由器、交换机、远程访问服务和防火墙等存在的漏洞[7]。

基于主机的扫描是从一个内部用户的角度来检测操作系统的漏洞，主要用于检测注册表和用户配置中的漏洞。基于主机的扫描的优势在于它能直接获取主机操作系统的底层细节，如特殊服务和配置的细节等。其缺点在于只有控制了目标主机，并将检测工具安装在目标主机，才能实施正常的扫描活动[8]。

通过上述理论可以看出基于网络的扫描和基于主机的扫描各有优势，但也各自存在了一定缺陷和条件限制。只有把二者结合起来，才能从目标网络系统的所有方面最大可能的得到漏洞信息，为系统管理员处理系统的安全风险提供有力的支持和保证。

1.4 论文章节安排

全文共分为七章：

第一章 叙述了系统脆弱性的研究背景和意义，说明了系统脆弱性分析的必要性。

第二章 对系统脆弱性分析方法进行了介绍，介绍本文主要使用的基于漏洞扫描的系统脆弱性分析方法及使用的脆弱性扫描分析工具启明星辰天镜。

第三章 对具体目标的系统核心网络架构进行了叙述并从物理层面上对脆弱性进行了初步的分析，为第四章具体分析打下基础。

第四章 将目标系统分为 4 个部分叙述了系统的脆弱性，对已知及所有能发现的脆弱点进行了分类。

第五章 对所有发现的漏洞详细描述，并对每个漏洞的修补方法进行了详细说明，对于在不同系统下的情况也都进行了说明。

第六章 运用同类工具对已修补高危主机进行再次的安全检测。对之前所做的修补结果进行肯定，明确漏洞修补对系统安全所做的提高。

第七章 总结及展望