学校编码：10384　　分类号＿＿＿＿密级＿＿＿

学号：X2013232152　　UDC＿＿＿

厦门大学

工　程　硕　士　学　位　论　文

基于漏洞检测与分析的网络安全评估模块设计与实现

Design and Implementation of Network Security Assessment Module Based on Vulnerabilities Detecting and Analyzing

陆青

指　导　教　师：　姚俊峰　教授

专　业　名　称：　软　件　工　程

论文提交日期：　2016 年 9 月

论文答辩日期：　2016 年 11 月

学位授予日期：　2016 年 12 月

指　导　教　师：＿＿＿＿＿＿

答辩委员会主席：＿＿＿＿＿＿

2016 年 9 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　　日

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

本文分析了国内外漏洞研究的现状，分析了网络安全漏洞特征，建立了一种安全漏洞扫描体系，并以此为理论指导，建立一个基于国际 CVE 标准的安全漏洞数据库。

本文从风险及评估技术、漏洞和检测技术、检测与评估模块设计、评估系统实现等方面，以网络安全检测为重点，探索出一种综合的安全扫描系统，为安全评估工作提供有效的技术支持，能够满足信息系统安全评估的需求，可靠、有效地扫描网络中存在的漏洞信息及开放的端口与服务，提供目标网络中存在的漏洞、风险等级、安全状况等信息。

本文根据风险评估原则实现网络安全评估，包括漏洞风险级别、系统风险级别以及系统配置的实现。原理是先扫描目标主机的端口，获得主机的开放端口，其次，根据该端口提供的服务，查找对应这一项的漏洞检测码，再将含有漏洞检测码的数据包发送给目标端口，等候回应，通过分析目标端的发回的结果来判断是否存在漏洞。检测结束后，把得到的漏洞信息记录到安全漏洞数据库，并加以分析，用模糊数学的理论计算安全等级，并用 VC++6.0 工具对其进行实现并生成评估报告。

最后通过测试验证，该系统模块的设计和实现方案是有效的。

关键词：网络安全评估；安全检测；风险分析

Abstract

This paper laid a strong emphasis on the detection of net security，aims at finding out a kind of integrative scan system, and provides evaluation with technology support. This module was designed to meet the needs of information system security evaluation, scan the vulnerability, open ports and service, and report the exist vulnerability, risk level, security status and so on.

The paper review the current status of vulnerabilities research. Then, it is presented that a structural model of vulnerability database based on the research of the classification of computer vulnerabilities. After that, the dissertation depicts the building of the database based on CVE standard and its generating software.

The innovation of this article is the net security assessment model based on Vulnerabilities detecting and analyzing，It achieve security assessment system basis of rish assessment principia，including vulnerabilities rish level、sytem rish level and the realizationof config. First, scan ports of target hosts using kinds of scan techniques, then search vulnerabilities detect code in the vulnerabilities character atabase according services that open ports provide. Next, send packages which include vulnerabilities detect code and wait for target's responses. At last, judge vulnerabilities exist or not base on the responses. After the detection finished, put vulnerabilities practically detected into the result database, make risk analysis , calculate security level by the theory of vague mathematics, and use the tool of VC++ 6.0 to achieve and generate assessment report.

Finally, it presents the results of test to prove the feasibility of this system.

Key words: Network Security Assessment; Vulnerabilities Detecting; Risk Analyzing

目 录

Contents

第一章 绪 论

1.1 研究目的和意义

早在上一个世纪70年代人们就开始意识到信息系统的安全性问题，并开始从事有关信息系统的安全风险评估方面的研究，美国等IT行业领先的国家已经研究出了一些评估的方法和技术，基于评估标准进行信息安全评估和认证，控制系统风险，并建立了相关的国家认证和风险评估认证体系。

目前，在世界上被认可的风险评估理论的标准主要有ISO/IEC 13335（IT信息技术安全管理指南）、AS/NZS 4360（风险管理的标准）、BS7799-1(ISO/IEC 17799 基于风险管理的信息安全管理体系)等，这些标准都对风险评估做出了定义，起到重要的指导作用[1][2]。当然，还有COBIT、ITIL、NIST SP800等也逐渐引起人们的关注[3][4]。现在，大家使用的评估方法也多是以此为执行的准则，但是，依然缺少富有针对性和实践性的方法。

从两千年开始，我国的一些大学、公司企业以及研究信息安全的机构纷纷开展了网络风险评估工作，并争相提出了一些可行的风险分析和评估的具体实施方法。这些方法都是在BS7799或ISO13335的基础上对用户进行问卷调查和对信息系统进行脆弱性扫描、日志分析的。在网络安全评估模型方面有一些研究，即从网络安全脆弱性分析构造安全评估模型，以及系统脆弱性研究[5][6]。但是如何对这些安全脆弱性进行关联分析以及进行量化指标的研究很少。

怎样针对不一样的操作系统、不一样的通信协议进行漏洞扫描和检测，及时的发现存在的漏洞，如何对进行风险分析和评估是研究热点之一。研究网络安全评估的理论和技术，对于保护信息的机密性和安全性，维护数据通信和资源共享，构建具有自主知识产权的漏洞检测与风险评估平台，从而加强我国的网络信息安全防护能力是具有重要意义的。

因此，本论文利用模糊数学理来论构建评估模型，提出从资产评估、威胁评估、脆弱性评估三个层面进行分析，主要是基于漏洞的检测与分析的网络安全性评估。系统通过扫描并计算方式反映网络系统的脆弱性状况，使评估结果生动形象，更加准确详细，给安全管理员提供切实有用的、直观的信息。

1.2 国内外发展现状

标准，作为一种依据和尺度，是测评的灵魂，对风险评估也是同样适用的。自1985年美国国防部对外发布了计算机系统评估准则(即：TCSEC)开始至今，已经出现了许多相关的条例[7]。

国内外的典型的标准有以下几种：

(1) CC标准

简写为CCITSE，标准信息技术的安全评估公共标准（ Common Criteria of Information Technical Security Evaluation)，简称CC (ISO/IEC15408-1)，是英、加、法、德、荷、美国国家安全局以及国家标准技术研究所(6国7方)经协商同意，于1993年6月起草的，是国际标准化组织对主要的几种信息安全标准标准，包括：TCSEC、ITSEC、CTCPEC、FC等的整合结果，是目前较为全面的信息安全方面的国际性评估准则。

CC标准源自于TCSEC标准，但有不同于TCSEC。 CC标准主要的思想和构架来源于ITSEC(欧)（即《信息技术安全性评估准则》）和FC(美)（即：《联邦准则》的1. 0版草案）[8]，CC标准汲取了世界各国对现代信息系统安全的认识和应对经验，给研究和应用带来了深远的影响。

CC标准的评估等级共分7级:EAL1到EAL7，主要由三个部分的内容组成:

1)介绍标准的详细情况以及一般的理论模型；

2)功能性需求(这里主要指的是技术上的要求)；

3)安全认证需求(这里主要指的是非技术性的要求以及对项目开发的过程和项目的工程过程的具体要求)。

CC与早期评估准则相比，主要具有四大特征:

1) CC符合PDR模型；

2) CC评估标准覆盖了完整的信息产品的生存期；

3) CC评估标准不但考虑了信息的保密性，同时还考虑了信息的完整性和可用性等多方面的特性；

4) CC评估标准有和它相适宜的安全评估的方法CEM （Common Evaluation Methodology)。

(2) BS7799(ISO/IEC17799)

由英国的标准协会（BSI）发布的一套极具代表性的管理标准，包含了两个部

分：BS7799-1:1999和BS7799-2:2002，也就是信息安全管理实施细则和管理体系规范，其中，在2000年12月信息安全管理实施细则得到了国际标准化组织的认可，正式成为一项国际标准，即为：ISO/IEC 17799:2000。它是被国际标准化组织认可最快的一个标准，可见风险评估工作是信息安全的重要内容之一。

信息安全管理实施细则对指导我们如何组织并实施信息安全管理体系的起到了重要的作用，信息安全管理体系规范是以信息安全管理实施细则为指引的，严格按照PDCA模型来建设和实施。

关于信息安全管理的实施细则所描述的信息安全管理标准层次体系非常详尽、复杂，可以分成四层：按照信息安全的十个重要的领域划分出十个管理项目，又可以分成包括了偏重管理和偏重技术的两大类，每个部分针对不一样的中心或内容。在这十个重要项目中，还可以细分成三十六个管理目标、一百二十七个控制措施和，若干的控制要点，可以说是全面覆盖了当前信息安全的各个方面。

(3) ISO/IEC 21827：2002(SSE-CMM)

信息安全工程能力的成熟度模型(System Security Engineering Capability MaturityModel)，是关于信息安全建设工程实施方面的标准。

它的目的是建立一套成熟的、可度量的安全的工程过程。模型定义了一个安全的工程过程应该具有的特征，而这些特征是完善安全工程的根本保证。

国内的安全评估技术经过近5年的发展，可以划分为四个阶段，即以资产、标准和定量分析做为基石的第一代技术；以工程、成熟度和规范为基石的第二代技术；以过程、应用和管理为基石的第三代技术；以系统方法与实践为基石的第四代技术。但对网络的安全风险评估仍采用扫描等工具实现，没有形成成熟、综合的评估网络系统的安全评估模型。

综合以上几种标准，我在这里简单地进行一下比较和评价。

BS7799是七分管理、三分技术理念的最好体现，同BS7799相比，信息技术安全性评估的准则(即：CC标准)和美国国防部可信计算机评估准则(即：TCSEC)侧重于评估系统的技术性指标，在安全管理要求的全面性和完整性方面不如BS7799；但是在对信息系统的日常安全管理方面，BS7799的作用是其他的标准无法取代的，BS7799完全地涵盖了安全管理的各个方面，全面但是又不失可操作性，为大家提供一个可持续的信息安全管理环境，但在安全技术方面不如CC分析的系统、透彻。

1.3 论文研究内容

研究目标是，通过分析使用国内外目前流行的网络安全检测产品，及时跟踪官方权威网站公布的最新漏洞，全面分析漏洞的特征和漏洞利用程序，掌握各种漏洞的原理和检测方法，不断了解漏洞检测与风险评估的前沿技术，开发具有自主知识产权的漏洞安全检测模块，为系统抗攻击测试提供技术和产品支持。

这一课题研究的主要工作如下：

(1)收集风险评估标准的研究情况资料，对资产、威胁、脆弱点等要素和管控方法进行研究，在此基础上总结当前风险评估存在的问题和未来发展。

(2)研究各种漏洞安全检测技术和扫描检测技术。

(3)拟解决安全评估的类型（对已知和未知的缺陷），包括漏洞扫描、突破测试及IT安全审核。

(4)分析与建立漏洞库,实现安全评估的方法以及实现评估所需的技术和平台。

(5)运用模糊数学理论，构建评估模型。

(6)对系统进行漏洞检测，对检测结果进行风险评估，并用VC++6.0 工具对其进行实现和显示运行结果。

1.4 论文组织结构

论文共分为七个章节，具体的内容结构如下：

第一章 绪论，介绍论文的背景，信息安全概述和国内外信息安全研究现状，本论文研究工作内容。

第二章 基本概念和相关技术分析，本章节主要风险评估和漏洞检测技术的相关概念。

第三章需求分析，根据实际情况对该模块的技术功能进行需求分析，包括了可行性分析、用户角色分析、功能分析、非功能性分析。

第四章 系统设计，从模块划分的角度介绍了设计方案。

第五章 系统实现，描述了主要模块的实现。

第六章 系统测试，制定测试方案，并执行验证且获得结果。

第七章 总结与展望，对模块设计与实现过程进行总结，指出了存在的各种问题以及未来的研究探索的方向。

第二章 基本概念和相关技术介绍

2.1 风险评估主要概念

风险评估中涉及如下相关概念和术语：

(1)资产(Asset)

资产是属于某些组织的有价值的信息或资源，包括了计算机的软硬件、通信设备、数据库、数据资料、服务和人员等。可以从它的价值、重要性和敏感度等方面来对资产进行评估。

(2)威胁(Threat)

可能损害资产的原因或者是潜在原因，或者说是某一威胁源或是机构成功地利用特定的风险点对资产造成负面影响的潜在可能。

威胁可以分成大致三类，即：自然灾难、人为的无意识、人为的故意攻击。可以归纳成两大类：人为威胁(又分为：有意和无意)和非人为威胁(包括：自然和环境)。

(3)脆弱点(Vulnerability)

也被称作漏洞或脆弱性，是指可以被威胁利用的系统缺陷，能增大系统被攻击的可能性。脆弱点指的是操作系统、应用软件及硬件本身的安全漏洞，可以通过漏洞扫描器检测到。如果脆弱点被人利用，就会损害资产。需要注意的是，脆弱点本身是不能构成伤害的，它一般是作为被威胁利用的来实施影响、伤害的条件。安全评估的过程就是识别脆弱点，评估脆弱点的严重性和被利用的容易程度。

(4)风险(Risk)

威胁主体利用漏洞造成损失或破坏的可能性。风险的三个要素为威胁、漏洞和资产，安全评估就是对这三个要素的分析，而降低风险采取的安全措施也是从这三个要素考虑。也能解释成：特定的威胁利用某些资产的脆弱性，造成资产的损失、破坏的潜在可能性。

(5)风险分析（Rish Analyse）

广义上是一种对各种不同范畴、不同性质、不同层次的威胁问题，通过归纳、比较、综合，形成对风险的认识的过程，围绕广义的相关分析、预测和广义评估等三种功能进行[9]。

(6)风险评估（Risk Assessment）