

网络脆弱性评估系统的设计与实现^{*}

邓亚平, 吴慧莲, 陈 琳, 王 彬
(重庆邮电学院 计算机科学与技术研究所, 重庆 400065)

摘 要: 通过对网络脆弱性检测技术与安全风险评估理论的回顾与深入研究, 提出了一种网络安全脆弱性评估模型, 并在此基础上实现了网络脆弱性评估系统。该系统从主动防御的角度出发, 集成了多种最新的测试方法, 能够自动检测远程或本地设备的安全状况, 找出被检对象的安全漏洞和系统缺陷, 并根据一定的标准做出安全评估, 给出评测报告。

关键词: 弱点; 网络脆弱性评估; 端口扫描; 安全检测

中图法分类号: TP393. 07 文献标识码: A 文章编号: 1001-3695(2005) 01-0219-03

Design and Implementation of Network Vulnerability Assessment System

DENG Ya-ping, WU Hui-lian, CHEN Lin, WANG Bin
(Institute of Computer Science & Technology, Chongqing University of Posts & Telecommunications, Chongqing 400065, China)

Abstract: Through the review and embedded study of the theory of network vulnerability testing and security risk assessment, we have successfully developed a new model of network vulnerability assessment. Based on this model we have implemented the network vulnerability assessment system. From the point of view of initiative defense, this system can inspect the security situation of target system, and find out the security vulnerability or system defect automatically. It also gives out the security grade and assessment report according to the related standards.

Key words: Vulnerability; Network Vulnerability Assessment; Port Scan; Security Test

1 引言

Internet 的迅速发展, 给人们的日常生活带来了全新的感受, 网络生存已经成为时尚。然而网络技术的发展在给人们带来便利的同时, 也带来了巨大的安全隐患, 网络安全面临前所未有的挑战。技术是一把双刃剑, 不法分子试图不断利用新的技术伺机攻入他人的网络系统, 而肩负保护网络安全重任的系统管理员则要利用最新的技术来防范各种各样的非法入侵行为。但是不管入侵者是从外部还是内部攻击某一网络, 都是通过挖掘操作系统和应用服务程序的弱点或者缺陷来实现的。实践表明, 系统与网络的安全性取决于网络中最薄弱的环节。检测网络系统中的薄弱环节, 最大程度地保证网络系统的安全, 其中最为有效的方法就是定期对网络系统进行安全性分析, 及时发现并改正系统和网络存在的脆弱性, 并分析出现这些安全问题的原因, 以及在整体上进行何种程度的改进。要达到这个目标, 需要做更多的检测、评估和统计分析工作, 使系统管理员对整个网络系统的安全状况有全面和深入的了解, 以利于对安全问题作出各种决策, 如制定安全需求, 确定安全方案, 选择安全产品, 开发新系统等。做好这些事情, 需要一整套能

对整个网络进行检测评估和统计分析的强大工具, 而不能单纯依靠人力, 否则既费事费力, 所取得的效果受人力水平和精力的限制而不可能全面。网络管理员往往是利用网络脆弱性评估系统来完成安全测评工作。

2 安全评估模型

现有的信息安全标准、安全模型都以风险为核心, 事实上也是由信息安全的最终目的决定的。因为信息安全的终极目标就是尽可能地降低安全风险和最大程度地保护信息资产。从信息安全、保护资产的角度出发, 最直观的安全风险模型应包括两个因素: 信息资产和安全威胁。进而从信息安全的角度分析, 信息资产又包含两个特征因素: 影响价值(后果)和脆弱性(安全漏洞)。而安全威胁也应考虑两个方面: 严重性(破坏强度)和暴露率(被攻击的可能性)。从风险评估的角度看, 信息资产的脆弱性与威胁的严重性相结合, 可以获得威胁产生时实际造成损失的成功率, 而将此成功率与威胁的暴露率相结合便可以得出安全风险的可能性^[1]。信息资产的影响价值则直接关系到安全威胁可能造成的影响后果。这样, 在考虑了资产的影响价值和脆弱性、威胁的严重性和暴露率之后, 就可以确定安全风险的两个要素, 从而确定安全风险。安全评估的内容如图 1 所示。

Rainer 等人^[2]指出, 信息安全风险管理流程是以风险分析作为起点。风险分析阶段进行确认信息相关的资产、界定资产

面对的威胁以及了解资产具有的弱点等工作,如图 2 所示。风险分析可以确认所面临的风险,并衡量其大小程度,而决定必须加以保护的部分,因而可以提供制定内部控制决策时使用。换言之,风险分析是进行风险管理的基础,各种风险管理决策必须以风险分析结果作为依据。

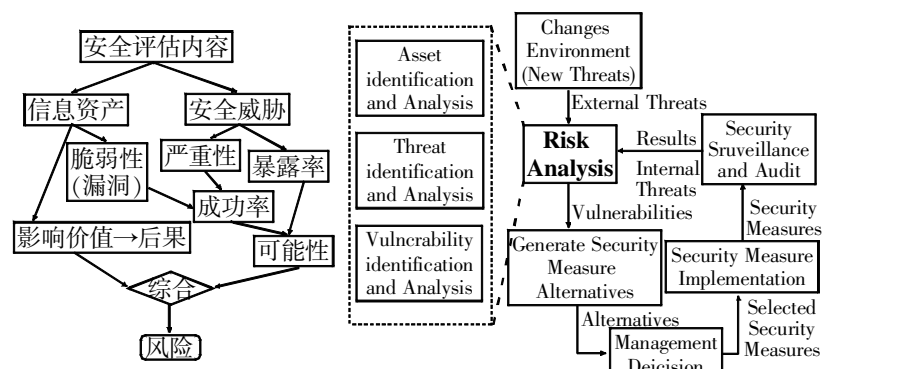


图 1 安全评估内容

而具体实施安全评估时,又衍生出众多的评估方法。比如可以对安全风险的后果及可能性进行赋值(定量、半定量赋值或者定性分析),然后通过一定的算术或逻辑计算得出评估风险数值或者等级大小,也可以对资产、漏洞和威胁采用各种分析手段进行定量赋值、半定量赋值或者定性分析,从而评估得出风险大小。由于要开发的是自动评测系统,应该尽量避免人为因素,让系统能够自动完成全程评测工作。比较而言,CSC 开发的安全评估方案^[3]是目前各种方案中最有系统性的方法,而 NIST 发布的 sp800-30^[4]又是最具权威性的技术标准。所以在下面的设计中将主要参照这两个评估模型,并结合实际情况进行适当修改。

3 安全检测技术

弱点检测通常采用两种策略,即被动式策略与主动式策略。所谓被动式策略,就是基于主机之上,对系统中不合适的设置、脆弱的口令以及其他与安全规则抵触的对象进行检查;而主动式策略是基于网络的,它通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应,从而发现其中的漏洞。利用被动式策略扫描称为系统安全扫描,利用主动式策略扫描称为网络安全扫描^[5]。在系统实现中,将集成这两种技术于一体,采用积极的、非破坏性的办法来检验网络是否存在可能的被攻击点。它利用一系列的脚本对网络进行模拟攻击,然后对结果进行分析。它还针对已知的网络漏洞进行检验。

弱点检测技术按检测内容与方式可以分为:弱口令探测、漏洞扫描(Vulnerability Scanning)、穿透攻击检测等。它们都可以直接有效地发现网络存在的安全隐患。网络检测技术常被用来进行穿透实验和安全审计。这种技术可以发现一系列平台的漏洞,也容易安装。漏洞扫描把端口扫描的概念上升到一个更高的层次。它不仅确定活跃主机和开放端口,还可以确定任何相关的漏洞。漏洞扫描可以根据完整的安全漏洞集合进行全盘的检测,而这些安全漏洞集合也正是导致网络遭受破坏的主要因素。因此,弱点检测可以在网络黑客动作之前,协

助管理者及早发现网络上可能存在的安全漏洞。为了能够检测不同的漏洞,目前的检测系统大多使用插件或专用脚本来扩展功能。

4 系统的设计

本项目采用模块化的设计思路,遵循了软件开发中的低耦合、高内聚的原则,使各个模块相对而言具有最大的独立性,以使项目结构清晰。通过原型设计,首先确定本项目软件的总体风格、界面、素材的规格。先制定项目的总体设计方案,构造出整个系统的主框架;然后进一步细化,确定要实现的功能,并确定子系统的划分;再进行各个子系统的详细设计,包括具体的功能模块的实现以及相关数据库的设计;最后进行人机界面的设计;同时,还设计了测试向导,结合大量的图片,增强界面的观赏性,易于用户使用。由于本项目使用的信息量较大,采用数据库将有助于数据的管理。在数据库的设计中,根据项目所使用的相关信息,按照数据独立性的原则,先进行概念设计,并进行数据抽象,然后设计各个相关的数据表和视图,确定数据流图,最后合并,成为一个整体的数据库,并通过 BNF 范式的要求,减少数据表之间的依赖程度,删除冗余数据。

4.1 系统的检测流程

脆弱性评估系统的执行流程如图 3 所示。

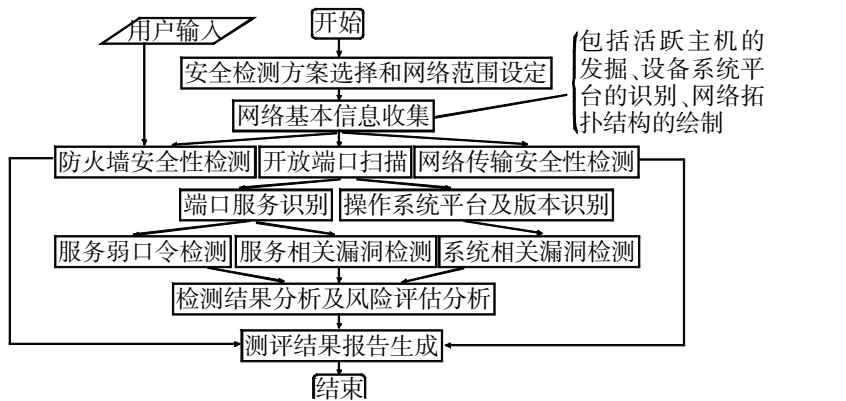


图 3 系统的检测流程总图

主要步骤如下:

- (1) 活跃目标检测发掘。用多种方法实现远端主机的存活探测,检查目标设备是否存在并处于激活状态。
- (2) 网络拓扑结构绘制。对网络进行扫描,确认网络传输过程经过了哪些设备,了解目标网络的大致结构,并对网络拓扑进行图形显示。
- (3) 设备系统平台识别。识别目标是何种网络设备,如路由器、交换机、防火墙、网络打印机、服务器等。
- (4) 端口服务识别。通过前面三个步骤所获得的知识,再对目标网络进行端口扫描和服务识别,包括标准端口服务识别、非标准端口服务识别、常见木马检测识别。如果顺利完成,将获得目标网络的完整信息。
- (5) 安全脆弱性检测。分析目标网络是否有安全漏洞或系统脆弱性,包括操作系统本身的漏洞及网络服务的漏洞。
- (6) 网络传输安全性检测。运用网络嗅探原理,监听网络中的数据报,并对捕获的包按照网络协议进行还原解析,对常

用网络协议中以明文传送的用户名密码做有针对性的检测, 最后就捕获的数据进行传输安全性分析评估。

(7) 安全风险评估。通过对客户的安全管理策略执行状态、网络拓扑结构, 以及以上漏洞评估结果的深入分析, 智能地判断用户网络的安全特征水平, 并确定所存在的安全隐患及安全事故对客户整体可能造成的损失程度和风险大小, 最后给出安全性建议。

(8) 测评报告生成。根据不同用户的需要, 生成不同侧重的测评分析报告以及增强安全性建议。

网络安全评测是一个综合的课题, 它涉及技术、管理、使用等许多方面, 它既包括评测信息系统本身的安全问题, 也有评测物理的和逻辑的安全措施, 以及对系统管理员素质的考察。一种技术只能解决一方面的问题, 而不是万能的。

4.2 插件检测模块设计

我们采用插件技术来实现漏洞检测。插件(Plug-in)也叫作功能模块技术。每个插件都封装一个或者多个漏洞的测试手段, 主扫描程序通过调用插件的方法来执行扫描。仅仅添加新的插件就可以使软件增加新功能, 扫描更多漏洞。在插件编写规范公布的情况下, 用户或者第三方公司甚至可以自己编写插件来扩充软件的功能。同时这种技术使软件的升级维护变得相对简单, 并具有非常强的扩展性。俄罗斯出品的著名安全检测产品 Shadow Security Scanner 以及国内安全机构“安全焦点”推出的 X-Scan 扫描器, 就是使用的插件功能进行漏洞升级扩充。插件技术是现代软件设计思想的体现, 其本质是在不修改程序主体的情况下对软件功能进行加强。插件一般用 DLL 实现。插件检测流程如图 4 所示, 所有的安全测试都是由插件调度模块发动。首先按照插件类别把所有待检测的插件排序, 依次执行参数设置、端口扫描、信息收集、漏洞验证、模拟攻击等类型插件。任何插件其实只包含两个函数: 插件初始化函数——plugin_init() 和插件运行主函数——plugin_run()。在 plugin_init() 函数中完成插件的注册任务, 注册信息包括插件名字、版本、分类族、简单描述、解决方案、相关链接、CVE 号等, 而 plugin_run() 函数包括所有用于测试的代码。

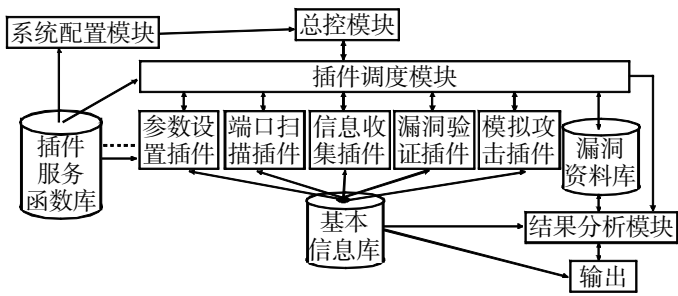


图 4 插件调度过程

(1) 插件调度模块。它负责所有插件的检测调度、参数传递, 以及结果反馈等任务。首先按照插件类别把所有待检测的插件排序, 依次执行参数设置、端口扫描、信息收集、漏洞验证、模拟攻击等类型插件。

(2) 基本信息库。在插件检测过程中, 始终维护一份由插件获得的基本信息库, 各种其他的测试插件应该尽可能地利用

这些信息, 以提高测试效率。例如, 一个测试插件需要打开一个到 FTP 服务器的连接, 而在这之前它应该首先检查端口扫描测试插件的结果, 确定 FTP 端口是否打开。在一般情况下, 这样只会节约一点点时间, 但是如果被测试主机位于防火墙之后, 这样做会节省由于防火墙丢弃到 21 端口的 TCP 报文造成的漫长等待时间。

(3) 结果分析模块。在获知了网络的漏洞信息以后, 就可以进行评估分析工作了。风险评估算法描述如下:

假设 O 为目标平台(操作系统); S 为该系统提供的 n 种服务 $S_1 \dots S_i \dots S_n$ 的集合 $(1 \leq i \leq n)$; B 是第 S_i 种服务在该系统中所占权重 b_i 的集合 $(1 \leq i \leq n)$; b_i (百分制表示, 用户可控); H 为 H_{ij} 的集合, 第 i 种服务 S_i 有 m 个漏洞, 分别是 $H_{ij}(1 \leq j \leq m)$; V 为 H_{ij} 的风险程度 V_{ij} 的集合; W 为漏洞 H_{ij} 在服务中所占的权值 W_{ij} 的集合, W_{ij} (百分制表示, 用户可控); 则 $F(O, S, B, V, W) = \sum_{i=1}^n b_i (\sum_{j=1}^m W_{ij} V_{ij})$ 用来表示目标系统所提供服务的最后的风险评估结果。

5 结束语

本文通过对网络脆弱性检测技术与安全风险评估理论的回顾与深入研究, 以及对一些已有安全检测工具特别是 Nessus 软件的代码分析的基础上, 提出了一种网络脆弱性检测与风险评估模型, 并在此基础上实现了网络脆弱性评估系统。该系统从主动防御的角度出发集成了多种最新的测试方法, 能够自动检测远程或本地设备的安全状况, 找出被检对象的安全漏洞和系统缺陷, 并根据一定的标准做出安全评估, 给出评测报告。大量的实验也表明其在测试网络系统的脆弱性方面是全面而有效的。基于网络弱点严重性的安全评估, 还是一个崭新的课题, 我们的评估模型也没有得到广泛的对比测试, 以后可针对该模型进行检验与修正。

参考文献:

[1] 卫成业. 信息安全风险评估模型[J]. 网络安全技术与应用, 2002, (4): 10-15.

[2] Rainer, Jr R K, et al. Risk Analysis for Information Technology[J]. Journal of Management Information Systems, 1991, 8(1): 129-147.

[3] Cyber Care. Security Assessment Methodology[EB/OL]. http: // www. csc. com, 2001-10.

[4] Gary Stone Bumer, Alice Goguen, et al. Risk Management Guide for Information Technology Systems[Z]. Recommendations of the National Institute of Standards and Technology, 2001. 3-25.

[5] John Wack, Miles Tracey. DRAFT Guideline on Network Security Testing[Z]. Recommendations of the National Institute of Standards and Technology, 2002. 4-43.

[6] Winkler Ira. Audits, Assessments and Tests[J/OL]. Information Security Magazine, http: // www. infosecmag. com/articles/july00/features4. shtml, 2000-06.

作者简介:

邓亚平, 教授, 主要研究方向为计算机网络和信息安全; 吴慧莲, 副教授, 主要研究方向为计算机科学理论; 陈琳, 硕士, 主要研究方向为网络安全; 王彬, 硕士, 主要研究方向为网络安全。