Broadview
www.broadview.com.cn

安全技术大系

网络渗透测试——保护网络安全的技术、工具和过程

李 匀 等编著

知己知彼，百战不殆。

学习专家使用的方法进行网络渗透测试：

- 使用经过验证的测试方法评估网络的安全强度、排除安全隐患。
- 学会如何在网络上进行模拟攻击。
- 通过实际案例展示渗透测试的步骤、策略、手段和工具。

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

网络渗透测试——保护网络安全的技术、工具和过程

李 匀 等编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

网络和计算机安全问题已经成为政府、企业必须面对的现实问题。应对安全威胁的途径之一就是采用渗透测试的方法模拟黑客的攻击，找出网络和计算机系统中存在的安全缺陷，有针对性地采取措施，堵住漏洞，固身健体。

渗透测试是一个日渐壮大的行业。本书详细阐述了渗透测试中如何模拟外部攻击者对网络和主机的攻击和渗透，给出了各个步骤。其内容可以划分为两部分：渗透测试的思想、方法、指导原则和具体的渗透测试过程。前一部分重点放在理解渗透测试、评估风险和建立测试计划；后一部分着重介绍具体的操作和工具。除了介绍攻击方法之外，基本上每一章都给出了检测攻击的方法，同时也说明了如何通过加固系统和网络来防止此类攻击。在各章的末尾，都给出了运用本章介绍的工具和方法进行实际操作的示例。本书为读者提供了渗透测试的思想、方法、过程和途径，而不仅仅是工具。

本书既可以作为政府、企业网络安全的参考资料，也可以作为大专院校学生渗透测试方面的教材，适用于招聘渗透测试人员的单位、要应聘渗透测试的人员及保护网络安全、避免恶意攻击的人员。

图书在版编目（CIP）数据

网络渗透测试：保护网络安全的技术、工具和过程 / 李匀等编著. —北京：电子工业出版社，2007.12
（安全技术大系）
ISBN 978-7-121-05153-1

Ⅰ. 网… Ⅱ. 李… Ⅲ. 计算机网络－安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 155099 号

责任编辑：朱沭红
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：39.5　字数：747 千字
印　　次：2007 年 12 月第 1 次印刷
印　　数：4000 册　定价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

安全始终是政府和企业关注的重要问题之一，因网络和计算机安全问题引发的冲击时有耳闻。保护信息和网络安全的途径有多条，渗透测试是其中的一种最有效的途径之一。渗透测试是受信任的第三方进行的一种评估网络安全的活动，它通过运用黑客攻击的方法与工具，对企业网络进行各种手段的攻击来找出系统存在的漏洞，从而给出网络系统存在的安全风险的一种实践活动。通过模拟现实的网络攻击，渗透测试证实恶意攻击者有可能获取或破坏企业的数据资产。

本书通过完整地介绍渗透测试的过程，为读者提供了一个渗透测试工作的完整蓝图。第 1 章给出了安全基础知识，定义了渗透测试的范围和目的，说明了渗透测试过程中要考虑的道德、法律方面的问题。通过现实中的案例，说明渗透测试工作的重要性和迫切性。

第 2 章介绍建立渗透测试实验和学习环境的方法，这里给出了虚拟系统的概念和 VMWare 的功能、安装、配置，以及在 VMWare 上安装其他操作系统的过程。通过采用虚拟系统，我们可以在一台配置比较好的机器上同时运行多个操作系统，模拟一个现实的网络环境，从而达到节约资金、提高安装、配置效率的目的。

第 3 章介绍如何建立渗透测试计划，它说明了建立计划的步骤及如何编写渗透测试文档，同时简要给出了“开源安全测试方法指南”（Open-Source Security Testing Methodology Manual，OSSTMM）的核心内容。

4 章介绍渗透测试工作的一个重要过程——社会工程方法。人的因素永远都是安全链条中最脆弱的环节，社会工程就是利用人的弱点进行的安全攻击。这一章讨论了进行社会工程攻击时所需要的个性特点及各种假冒方法。

第 5 章介绍主机侦察。主机侦察是渗透测试的侦察部分。一般来说，在小偷实施入室盗窃之前，他都要在目的地附近转悠一段时间，以便确定盗窃的目标。在侦查过程中，小偷会仔细地观察每一间房子，从窗户中偷窥一下房间内部。他还要观察居民的生活规律，评估室内财物的多寡。同样地，黑客在实施攻击之前，也要进行侦察，发现网络上主机以及运行的应用程序和服务。本章介绍了主机侦察的内容和工具，包括主动侦察、被动侦察、端口扫描、网络搜索等。同时说明了如何应用入侵检测系统预防和阻止主机侦察。

第 6 章介绍会话劫持的原理、方法和工具。在会话劫持中，黑客监视网络流量，并利用适宜的工具劫持主机和服务器之间的会话，这样实现了身份假冒。

第 7 章从 Web 语言入手，在介绍了实现 Web 网站的各种编程语言和标准之后，说明了商务网站的结构，介绍了攻击网站的 Web 网页欺骗、Cookie 猜测、隐藏字段获取、口令破解工具及其他工具、网站信息获取方法等，同时给出了检测和预防网站攻击的手段。

第 8 章以 SQL Server 为示例，说明攻击数据库服务器的方法和工具，包括 SQL 注入、获取连接字符串、数据库口令破解，给出了常用数据库的默认口令。另外也介绍了包括数据库安全的思路和方法。

第 9 章集中介绍口令破解方法，重点是 Web 口令的破解、Windows 系统口令的破解、Cisco 路由器口令的破解等。给出了一组有效的破解工具和获取口令密文的工具。最后还介绍了减少口令破解、提高口令安全性的方法。

第 10 章介绍网络攻击。过去，恶意黑客追逐网络上的主机。现在，网络本身也是黑客的攻击目标。通过一定的方法和技术手段，我们可以躲避入侵检测系统的检测、渗透和穿越防火墙、干扰和摧毁交换机和路由器的服务，这些内容在本章中都进行了介绍，并且说明了如何防止或减轻此类攻击的细节。

第 11 章介绍网络的攻击和渗透方法。无线网络在给人们带来便利的同时，安全问题一直是人们关注的重点。本章给出了驾驶攻击的方法与工具，说明了检测无线攻击和保护无线网络安全的手段。

第 12 章介绍木马、病毒、后门程序的概念，给出了常见病毒的工作方式、常见木马的功能和应用，说明了检测木马和后门程序的工具与手段。

第 13 章介绍渗透 UNIX 类服务器和 Windows 服务器的方法，给出了一些常用漏洞扫描工具，重点说明了在这些系统中提升用户权限的方法及 Rootkit 的概念和应用，并阐述了检测和预防服务器攻击的工具与方法。

第 14 章解释缓冲区溢出的概念、引起缓冲区溢出的原因及防止缓冲区溢出的方法。给出了利用缓冲区溢出提升系统权限的工具和原理，说明了防止缓冲区溢出的思想、手段和工具库。

第 15 章描述拒绝服务攻击的常见方法。攻击者除了希望得到机密信息之外，有的时候也会对网络的可用性发起攻击，其手段就是拒绝服务。这是一种易攻难守的攻击。本章给出了它的思想、常用工具，说明了常见的攻击模式和可以采取的预防措施。

第 16 章介绍文件与信息隐藏、踪迹覆盖与证据清除。在黑客攻击得手之后，他会采取各种措施尽可能地隐藏自己，以便尽可能长时间地控制主机和网络，从中获取最大利益。本章给出了常用的文件和信息隐藏手段、审计和日志的关闭与清除方法、证据的

清除工具。

第 17 章通过一个综合案例，说明运用本书前面各章节介绍的知识和工具实施一次完整渗透测试的过程。

附录给出了渗透测试中经常使用的工具的概要说明及它们的下载地址。

作者的 E-mail 地址为：pentest@yahoo.cn。

目　录

CHAPTER 1

第 1 章　什么是渗透测试

在当今的数字世界中，人们发现，在维持公开的 Internet 连接的同时保护网络和计算机系统的安全变得越来越困难。病毒、木马、后门、蠕虫攻击层出不穷，虚假网站的钓鱼行为也让警惕性不高的公众深受其害。为了减轻信息泄露及系统被攻击带来的风险，企业和机构开始对自己的系统进行渗透测试，找出其中存在的漏洞和薄弱环节。那么，什么是渗透测试呢？简单地说，渗透测试是受信任的第三方进行的一种评估网络安全的活动，它通过对企业网络进行各种手段的攻击来找出系统存在的漏洞，从而给出网络系统存在安全风险的一种实践活动。通过模拟现实的网络攻击，渗透测试证实恶意攻击者有可能获取或破坏企业的数据资产。

本章向读者介绍渗透测试的领域，包括其需求、方法及过程步骤。在此之前，首先介绍一下安全方面的基础知识。

1.1　安全基础知识

绝对的安全并不存在。与一切都存在限制一样，安全也是如此，安全就是找到一种平衡。没有人、也没有企业能够有无限的财力来保护一切东西的安全，并且我们也并不能够总是采用最安全的方法。保护系统安全、避免遭受网络攻击的方法之一是将系统从网络上拔掉，成为一个独立的系统（即使这样的系统，也并非完全安全）。尽管这个系统不再受到来自互联网的黑客攻击，但其可用性也大大下降了。与此相反的另一个极端做法是直接连接到互联网上，而不安装防火墙、防病毒软件及安全补丁，此时系统虽然高度可用，但却极其脆弱，极易受到来自互联网的攻击。从这里可以看到，网络和系统

安全专业人员的工作是在安全性和可用性之间找到适宜的平衡。图 1-1 展示了它们之间的平衡关系。

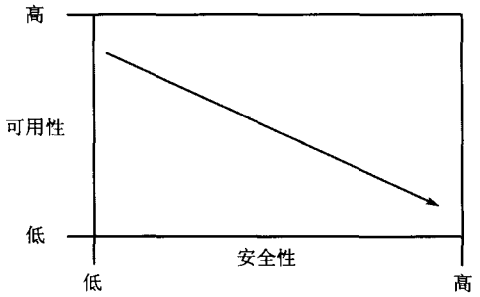

图 1-1　安全性与可用性之间的反比关系

为了找出这个平衡点，我们需要知道单位的目标是什么、什么是安全、如何度量安全威胁。

1.1.1　安全目标

ISO 17799 是建立并实施信息安全管理体系的指导性标准，根据它的定义，“信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性、可用性”。从中可以看出，机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）是支持信息安全的金三角，它们之间的关系如图 1-2 所示。

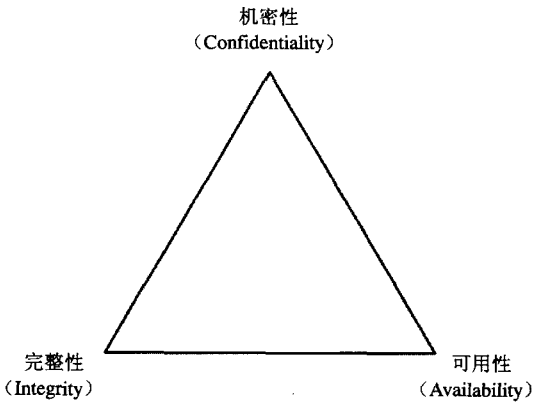

图 1-2　信息安全金三角（CIA）

- 机密性——机密性要求信息免受非授权的披露。它涉及对计算机数据和程序文件读取的控制，即谁能够访问哪些数据。它与隐私、敏感性和秘密有关。例如，它保护包括个人（健康）数据、市场计划、产品配方及生产和开发技术等信息。加密是实现机密性的一个有效手段。
- 完整性——完整性要求信息必须正确和完全，而且能够免受非授权、意料之外或无意的更改。完整性还要求计算机程序的更改要在特定的和授权的状态下进行。普遍认同的完整性目标有：
  - 确保计算机系统内数据的一致性。
  - 在系统失败事件发生后能够恢复到已知的一致状态。
  - 确保无论是系统还是用户进行的修改都必须通过授权的方式进行。
  - 维持计算机系统内部信息和外部真实世界的一致性。
- 可用性——可用性要求信息在需要时能够及时获得以满足业务需求。它确保系统用户不受干扰地获得诸如数据、程序和设备之类的系统信息和资源。不同的应用有不同的可用性要求。系统热备份、磁带备份、冗余磁盘阵列的运用是提高可用性的几种常见手段。拒绝服务攻击是一种针对可用性的攻击，黑客虽然无法获取系统的访问权，但他也使得正常用户无法正常使用系统资源。

不同的应用系统对于这三项安全目标有不同的侧重，例如：

（1）像国防系统这样高度敏感的系统对保密信息的机密性的要求很高。

（2）电子金融汇兑系统或医疗系统对信息完整性的要求很高。

（3）自动柜员机系统对三者都有很高的要求。例如，客户个人识别码需要保密，客户账号和交易数据需要准确，柜员机应能够提供24小时不间断服务。

1.1.2 风险三要素：资产、威胁和漏洞

与讨论任何新的技术课题一样，学习术语是更好地理解相应领域的良好手段。要成为一名安全专业人员，就需要理解威胁、资产和漏洞之间的关系。

风险是指威胁发生的可能性、发生威胁后造成不良后果的可能性及不良后果的严重程度的组合。它是安全威胁利用系统缺陷进行攻击的可能性。减少系统缺陷或减少威胁都可以达到减少风险的目的。

资产（Asset）是企业或个人拥有的、具有经济价值的任何东西。资产可以是看得见、摸得着的实实在在的东西，如路由器、服务器、硬盘、笔记本电脑；也可以是无形资产，如公式、数据库、报表、商业机密、处理时间等。无论是哪种类型的资产，当其丢失、损坏或受到破坏时，都会对单位造成经济损失。