ICSA 国家信息中心 启明星辰公司 策划

计算机网络安全工具

启明星辰公司
张小斌 严望佳 编著

计算机网络安全系列丛书

清华大学出版社
http://www.tup.tsinghua.edu.cn

计算机网络安全系列丛书

计算机网络安全工具

启明星辰公司
张小斌　严望佳　编著

清华大学出版社

(京)新登字158号

内 容 简 介

网络安全是一项责任重大、管理复杂的工作。对于广大的系统管理者和安全管理人员来说，使用安全管理工具可以起到事半功倍的效果。

本书介绍大量的计算机网络安全工具。对这些工具进行分类，并尽可能地提供工具的详细信息，包括工具的功能和适用的安全事件，以期帮助广大的网络管理者和用户选择适合自己系统和网络的安全工具。

本书面向广大的网络管理人员和网络安全技术人员。对于普通的计算机网络用户也有很大的参考和使用价值。

图书在版编目（CIP）数据

计算机网络安全工具/张小斌 严望佳编著-北京：清华大学出版社，1999
（计算机网络安全系列丛书）
ISBN 7-302-03341-2

Ⅰ.计… Ⅱ.①张… ②严… Ⅲ.计算机网络-安全-软件工具 Ⅳ.TP393

中国版本图书馆CIP数据核字（1999）第00748号

出版者：清华大学出版社（北京清华大学校内，邮编 100084）
http：//www.tup.tsinghua.edu.cn
印刷者：北京市清华园胶印厂
发行者：新华书店总店北京发行所
开 本：787×1092 1/16 印张：14.75 字数：262千字
版 次：1999年2月第1版 1999年2月第1次印刷
书 号：ISBN7-302-03341-2/TP·1802
印 数：0001～5000
定 价：29.00元

谨以此书献给我们的老师

严望佳

丛 书 序

全球信息高速公路的建设，Internet/Intranet 的发展，将对整个社会的科学与技术、经济与文化带来巨大的推动与冲击，同时也给我们带来了许多的挑战。Internet/Intranet 信息安全是一个综合的系统工程，需要我们在网络安全技术的研究和应用领域做长期的攻关和规划。

在 Internet/Intranet 的大量应用中，Internet/Intranet 安全面临着重大挑战。事实上，资源共享和信息安全历来是一对矛盾。近年来随着 Internet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的信息安全问题日益突出。据美国 FBI 统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机侵入事件。

一般认为，计算机网络系统的安全威胁主要来自黑客攻击、计算机病毒和拒绝服务攻击 3 个方面。目前，人们也开始重视来自网络内部的安全威胁。

黑客攻击早在主机终端时代就已经出现，随着 Internet 的发展，现代黑客则从以系统为主的攻击转变到以网络为主的攻击。新的手法包括：通过网络监听获取网上用户的帐号和密码；监听密钥分配过程，攻击密钥管理服务器，得到密钥或认证码，从而取得合法资格；利用 UNIX 操作系统提供的守护进程的缺省帐户进行攻击，如 Telnet Daemon、FTP Daemon 和 RPC Daemon 等；利用 Finger 等命令收集信息，提高自己的攻击能力；利用 SendMail，采用 debug、wizard 和 pipe 等进行攻击；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等等。目前，已知的黑客攻击手段多达 500 余种。

计算机病毒与“蠕虫”程序有所不同，它们主要的区别是，“蠕虫”寄生于操作系统之上，而计算机病毒寄生于一般的可执行程序上。计算机病毒种类繁多，极易传播，影响范围广。它动辄删除、修改文件，导致程序运行错误，甚至死机，已构成对 Internet/Intranet 的严重威胁。

拒绝服务攻击是一种破坏性攻击，最早的拒绝服务攻击是“电子邮件炸弹”。它的表现形式是用户在很短的时间内收到大量无用的电子邮件，从而影响正常业务的运行。严重时会使系统关机、网络瘫痪。

总而言之，对 Internet/Intranet 安全构成的威胁可以分为以下若干类型：黑客入侵、来自内部的攻击、计算机病毒的侵入、秘密信息的泄漏和修改网络的关键数据等，这些都可以造成 Internet 瘫痪或引起 Internet 商业的经济损失等等。人们面临的计算机网络系统的安全威胁日益严重。

黑客攻击等威胁行为为什么能够经常得逞呢？主要原因在于 Internet/Intranet 系统内在安全的脆弱性；其次是人们思想麻痹，没有正视黑客入侵所造成的严重后果，因而舍不得投入必要的人力、财力和物力来加强 Internet/Intranet 的安全性，没有采取有效的安全策略和安全机制。另外，缺乏先进的网络安全技术、工具、手段和产品等原因，也导致网络的安全防范能力差。

由于我国网络研究起步晚，网络安全技术还有待整体的提高和发展。我很高兴看到这套丛书的诞生，该丛书系统全面地介绍了计算机网络安全各方面的问题，并且从一些新的角度进行探讨，例如，如何针对 Internet/Intranet 系统的安全威胁建立正确的安全策略；如何提出 Internet/Intranet 系统安全的整体解决方案；如何严格规范建立 Internet/Intranet 系统的安全机制等。这对提高我国网络安全防范能力将有重要的参考作用。

这套由国家信息中心、国际计算机安全协会(ICSA)以及启明星辰信息技术有限公司(Vtech)策划的网络安全系列丛书具有起点高、技术覆盖面广等特点。包括了对业界最新的网络安全技术、操作系统漏洞和防范方法、网络安全工具以及黑客攻击手段等的详细分析和介绍。读者可以带着各种问题、从不同的角度来了解这些技术，一定会有所收获。

中国工程院院士　沈昌祥

前　言

一、本书概述

计算机网络安全日益引起人们的重视，但是并不是所有的网络管理人员和网络安全技术人员都是本领域的专家。同时，我们使用的系统越来越复杂，新的软件急剧增加，更为重要的是有越来越多的系统漏洞和安全隐患被发现并公之于众。因此，对于网络管理和安全技术人员来说，单凭自己已有的知识和手工劳动不足以保证系统的安全。而使用安全工具则可以在很大程度上提高系统的安全，并减轻网络管理者和安全技术人员的劳动量。

在本书中，将力求全面地介绍各类计算机网络安全工具。这些工具分为扫描工具、审计及检测工具、加密工具、密码安全工具、口令破译工具、访问控制工具、防火墙、电子邮件工具、系统补丁及替代工具、病毒检测工具、内容安全工具和其他工具等类，较全面地覆盖了计算机网络安全的各个方面。对于每类工具，都尽可能地介绍了工具涉及的安全事件及工具的功能，对于大部分工具还介绍了开发者、文件大小及获取信息等内容。

每一类工具都放在独立的一章中予以介绍，每章中重点介绍一些非常有名或者功能强大、有代表性的工具。对于属于本类的其他工具则尽量依照字母顺序或者根据内容相关进行排列，并做了较简单的介绍。因此，当读者需要查阅某工具时，非常方便。

限于篇幅，本书没有介绍关于操作系统和网络的知识，在阅读本书的时候，假设读者已具有相关部分的知识。同时对工具的安装、使用也着墨甚少，因为当获得工具后，这些信息完全可以在软件包的文档中找到。事实上，网络安全工具数量非常之多，同时，还有大量新的工具正源源不断地出现，一一列举是不可能的。写本书的目的首先在于向广大的网络管理和安全技术人员推荐一些较好的工具，以有效地增进系统的安全；其次，书中的大量工具也适用于普通网络用户的使用，这些工具可以为他们提供效率以及信息安全和访问安全；第三，对于所有的网络用户来说，通过阅读本书，可以加深对系统和网络安全的了解，学到许多在通常的使用中得不到的知识。

需要提醒广大网络管理人员和安全技术人员的是，本书中的许多工具既可以作为管理工具；也可以作为用户突破系统安全，甚至成为一名黑客的有效工具，这一点应当了然于胸。

二、本书的安排

本书主要介绍各种安全工具。

穷举所有的工具是不可能的，也是不现实的，但本书还是尽量将最常用，也是当前受到广大使用者和专业人士认可的一些工具收集在这里，并提供了有关该工具的相关资料以及获得相关信息的方法。

在本书的第一章，介绍安全工具的基本知识，使读者对安全的迫切性、获得安全工具及安全信息的渠道有所了解，并提供了使用安全工具需要具备的知识。

在本书的第二章，介绍了一些扫描工具。使用这些工具，有助于及时发现系统和网络中存在的安全隐患和漏洞，防患于未然。因为攻击者或者黑客也可以通过这些工具发现存在的这些问题，所以先于攻击者发现这些问题对系统安全来说，尤其重要。

在本书的第三章，介绍一些审计和检查工具。这些工具用以发现系统和网络中发生的与安全相关的事件，并且侧重于发现系统入侵，以及是否受到了攻击。

在本书的第四章，介绍一些加密工具。当前，在网上传输的信息多是明文形式，这就使得信息容易被窃听、伪造和更换。通过使用加密工具，可以保护传输的信息和防止抵赖，也可以保护多用户环境下的私有信息。

在本书的第五章，介绍一些密码增强工具。使用这些工具的目的在于强制用户使用一些安全的、好的口令，避免因为使用了弱口令而使系统遭到攻击。同时，密码增强工具对于在网络上传输的口令也可以提供一些安全保护。

在本书的第六章，介绍一些口令破译工具。口令是保护系统安全的第一道屏障，因此，需要系统和安全管理员采取许多措施，使用户选择好的口令。这一类工具可以帮助管理员检查系统中当前用户使用的口令是否安全，是否经得住词典式的攻击。当然，这些工具也可能成为黑客们的好工具。

在本书的第七章，介绍一些访问控制工具。这些工具提供了额外的访问控制和验证功能，能够在现有的验证系统中更进一步地提高安全。

在本书的第八章，介绍一些防火墙工具。本章介绍三类工具，首先是一些防火墙实用工具，可以使得用户在不损害防火墙安全性的基础上，提供灵活的访问手段；其次是一些包过滤工具，能有效地过滤危险的数据包；最后

是一些防火墙产品。

在本书的第九章，介绍一些电子邮件安全工具。这些工具可以有效地保证邮件的安全和现有接收、发送邮件的系统安全。

在本书的第十章，介绍一些系统补丁和替代程序。目前使用的大多数操作系统在最初开发时，对安全考虑得较少，不能适应现有的复杂网络情况，因此，许多程序都存在大大小小的安全缺陷。对系统打补丁和升级显得非常必要。

本书的第十一章介绍一些防病毒和杀病毒工具。病毒很早就已困扰着广大的计算机用户，严重时甚至给人们带来相当大的损失。本章介绍的工具可以有效地检测到病毒的感染，抑制病毒的传播。

本书的最后一章介绍一个很好的内容安全工具——MIMEsweeper。使用这个工具可以有效地防止病毒、特洛伊木马程序带来的危害，并防止组织内部机密信息的泄露。在 Web 技术得到广泛应用的今天，这类工具必将得到广泛的应用。在这一章中，还介绍一些实用的小工具。这些工具也可以有效地增进系统的安全。

这套丛书的策划和出版得到以下朋友的热情支持和帮助，谨在这里表示我们诚挚的谢意：中国信息安全专业委员会李正男主任、刘世键主任、吴亚飞秘书长，中国信息大学执行董事刘建国先生，国家信息大学信息安全处叶红、董小玲、张翔和孙卫红，美国格莱瑞技术公司严立。

目　录