可下载教学资料

http://www.tup.tsinghua.edu.cn

高等学校教材

计算机科学与技术

网络攻击与防御

甘刚 曹荻华 王敏 王祖俪 张永波 编著

清华大学出版社

高等学校教材

计算机科学与技术

网络攻击与防御

甘刚 曹荻华 王敏 王祖俪 张永波 编著

清华大学出版社

北京

内容简介

本书从网络攻击的一般过程出发，详细阐述网络攻击与防御的关键技术，系统地讲解攻击的主要步骤及各种攻击形式、关键点、防御措施。全书共分为8章，分别介绍了网络安全的基础知识、信息收集技术、网络扫描技术、针对操作系统的攻击与防御、脚本的攻击与防御技术、恶意代码的攻击与防御技术、网络安全设备的攻击与防御技术，每章都采用理论与实例结合描述的方式，并在第8章中给出了几个综合攻击的详细实例。

本书取材新颖，概念清晰、实例丰富。可作为信息安全专业、计算机应用专业或其他相近专业的教材，也可作为相关领域工作人员的参考书。

图书在版编目(CIP)数据

网络攻击与防御/甘刚等编著. —北京：清华大学出版社，2008.3
(高等学校教材·计算机科学与技术)
ISBN 978-7-302-16857-7

Ⅰ. 网…　Ⅱ. 甘…　Ⅲ. 计算机网络－安全技术－高等学校－教材　Ⅳ. TP393.08

中国版本图书馆CIP数据核字(2008)第006812号

责任编辑：丁　岭　李玮琪
责任校对：李建庄
责任印制：孟凡玉
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
c－service@tup.tsinghua.edu.cn
社 总 机：010-62770175　　**邮购热线**：010-62786544
投稿咨询：010-62772015　　**客户服务**：010-62776969
印 刷 者：北京国马印刷厂
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：14.75　**字　数**：354千字
版　　次：2008年3月第1版　　**印　次**：2008年3月第1次印刷
印　　数：1～3000
定　　价：24.00元

高等学校教材·计算机科学与技术

编审委员会成员

（按地区排序）

清华大学	周立柱	教授
	覃　征	教授
	王建民	教授
	刘　强	副教授
	冯建华	副教授
北京大学	杨冬青	教授
	陈　钟	教授
	陈立军	副教授
北京航空航天大学	马殿富	教授
	吴超英	副教授
	姚淑珍	教授
中国人民大学	王　珊	教授
	孟小峰	教授
	陈　红	教授
北京师范大学	周明全	教授
北京交通大学	阮秋琦	教授
北京信息工程学院	孟庆昌	教授
北京科技大学	杨炳儒	教授
石油大学	陈　明	教授
天津大学	艾德才	教授
复旦大学	吴立德	教授
	吴百锋	教授
	杨卫东	副教授
华东理工大学	邵志清	教授
华东师范大学	杨宗源	教授
	应吉康	教授
东华大学	乐嘉锦	教授
上海第二工业大学	蒋川群	教授
浙江大学	吴朝晖	教授
	李善平	教授
南京大学	骆　斌	教授
南京航空航天大学	秦小麟	教授
南京理工大学	张功萱	教授

南京邮电学院	朱秀昌	教授
苏州大学	龚声蓉	教授
江苏大学	宋余庆	教授
武汉大学	何炎祥	教授
华中科技大学	刘乐善	教授
中南财经政法大学	刘腾红	教授
华中师范大学	王林平	副教授
	魏开平	副教授
	叶俊民	教授
国防科技大学	赵克佳	教授
	肖　侬	副教授
中南大学	陈松乔	教授
	刘卫国	教授
湖南大学	林亚平	教授
	邹北骥	教授
西安交通大学	沈钧毅	教授
	齐　勇	教授
长安大学	巨永峰	教授
西安石油学院	方　明	教授
西安邮电学院	陈莉君	副教授
哈尔滨工业大学	郭茂祖	教授
吉林大学	徐一平	教授
	毕　强	教授
长春工程学院	沙胜贤	教授
山东大学	孟祥旭	教授
	郝兴伟	教授
山东科技大学	郑永果	教授
中山大学	潘小轰	教授
厦门大学	冯少荣	教授
福州大学	林世平	副教授
云南大学	刘惟一	教授
重庆邮电学院	王国胤	教授
西南交通大学	杨　燕	副教授

出版说明

改革开放以来，特别是党的十五大以来，我国教育事业取得了举世瞩目的辉煌成就，高等教育实现了历史性的跨越，已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上，高等教育规模取得如此快速的发展，创造了世界教育发展史上的奇迹。当前，教育工作既面临着千载难逢的良好机遇，同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾，是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001 年 8 月，教育部下发了《关于加强高等学校本科教学工作，提高教学质量的若干意见》，提出了十二条加强本科教学工作提高教学质量的措施和意见。2003 年 6 月和 2004 年 2 月，教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件，指出“高等学校教学质量和教学改革工程”是教育部正在制定的《2003—2007 年教育振兴行动计划》的重要组成部分，精品课程建设是“质量工程”的重要内容之一。教育部计划用五年时间（2003—2007 年）建设 1500 门国家级精品课程，利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放，以实现优质教学资源共享，提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展、顺应并符合新世纪教学发展的规律、代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻

性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

(1) 高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 高等学校教材·电子信息——高等学校电子信息相关专业的教材。

(4) 高等学校教材·软件工程——高等学校软件工程相关专业的教材。

(5) 高等学校教材·信息管理与信息系统。

(6) 高等学校教材·财经管理与计算机应用。

清华大学出版社经过20多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

E-mail: dingl@tup.tsinghua.edu.cn

前言

在现代网络中，网络安全已经成为人们日益关注的焦点问题。目前，利用计算机网络实施犯罪的案件屡见不鲜，黑客们通过各种方法向目标计算机发动各种攻击，对社会政治、经济、文化等方面造成了不可估量的损失。如何提高网络的安全防范水平，防止黑客入侵等问题已经刻不容缓。

本书从攻与防两个方面对网络攻击对抗中的关键步骤和技术进行详细的讲解，在内容编排上按照一般攻击的步骤，由浅入深，循序渐进，分类型进行叙述。书中每一章都以理论结合实例的方式进行讲解，使读者尽快掌握所学知识并运用到实际工作和生活中。

主要内容

全书共分为8章，分别介绍了网络安全的基础知识，信息收集技术，网络扫描技术，针对操作系统的攻击与防御；脚本的攻击与防御技术；恶意代码的攻击与防御技术；网络安全设备的攻击与防御技术；每章都采用理论与实例结合描述的方式，并在第8章中给出了几个综合攻击的详细实例。

特点

在内容安排上，作者力求将理论与实践相结合，让读者在学习理论知识的同时，掌握具体的攻击方式和防御技术，并通过给出的例子来验证所学到的理论知识，以增强读者对本书内容的理解和掌握能力。

适应对象

- 大学信息安全专业、计算机应用专业或其他相近专业；
- 信息安全培训的学生；
- 从事网络安全维护与管理的专业人士和信息安全爱好者。

阅读说明

本书所有实验均在实际环境中通过，读者在实际操作中因操作系统版本、设备硬件及操作步骤的差异可能输出显示同本书略有不同，但实验结果应相同。

结束语

由于本书编写时间比较紧张，书中难免出现一些错误和某些知识点的缺漏，在此欢迎广大读者批评指正，提出宝贵意见。

编　者

2008年1月

目 录

第1章 网络安全概述

本章知识点：

- 网络安全发展过程；
- 操作系统发展过程；
- 网络攻击基础；
- 网络防御基础；
- 网络协议基础。

本章导读：

人们一方面在享受着网络带来的便利和效益，另一方面又不得不“提心吊胆”地提防各种网络安全事件的发生。网络发展到今天的程度，网络安全也得到越来越多的关注。

本章主要介绍网络安全的发展历程，以及与此相关的操作系统的发展历程，网络攻击与防御的一般过程和技术发展，以及网络协议基础。

1.1 网络安全发展过程

1.1.1 网络安全的意义

所谓“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到破坏、更改、泄露，系统可以连续可靠正常地运行，网络服务不被中断。在计算机应用日益广泛和深入的同时，计算机网络的安全问题日益复杂和突出。网络的脆弱性和复杂性增加了被攻击的可能性。

1.1.2 网络安全发展历史

1986 年初在巴基斯坦的拉合尔(Lahore)，巴斯特(Basit)和阿姆捷特(Amjad)编写的第一个病毒——Pakistan 病毒(即 Brain)问世，在一年的时间内，Brain 病毒传播到了世界各地。

2002 年 10 月的怪物病毒 Worm. Bugbear，以新的感染手法让连续半年稳居毒王宝座的求职信病毒 Worm. Klez 退位。这个病毒可以窃取高度敏感的资料，如密码、账号等，并

将其传送到指定的计算机中，另外被感染的计算机还会遭其远端控制。

2003 年，被网络安全界称为“网络安全年”，可以说是 Internet 出现以来最不太平的一年。安全漏洞和病毒不断地出现，造成了一次又一次轰动全球的安全事件。

2003 年 1 月 25 日，Internet 遭遇到全球性的病毒攻击。这个病毒名叫蠕虫王(Win32.SQLExp. Worm)，其破坏性堪称 Internet 的“9・11”，这个病毒体极其短小，却具有极强的传播性，它利用 Microsoft SQL Server 的漏洞进行传播，由于 Microsoft SQL Server 在世界范围内很普及，因而此次病毒攻击导致全球范围内的 Internet 瘫痪，在中国，受此次全球性病毒袭击影响 80%以上网民而不能上网，很多企业的服务器被此病毒感染引起网络瘫痪。而美国、泰国、日本、韩国、马来西亚、菲律宾和印度等国家的 Internet 也受到严重影响。直到 26 日晚，蠕虫王才得到初步的控制。这是继红色代码、尼姆达、求职信病毒后又一起极速病毒传播案例。全世界范围内经济损失高达 12 亿美元。

2003 年 3 月 20 日，美国对伊拉克发动战争。在炸弹持续向伊拉克倾泻之际，抗议者和拥护美英的黑客在 Internet 上的“口水大战”也随之升级，他们互相篡改对方公司与政府网站的内容，黑客入侵网站事件激增。有三类黑客参与对网站的攻击：以美国为基地的民族主义黑客、伊斯兰极端主义组织和反战的和平人士。黑客组织篡改美国和英国的网站事件每 1 分钟就会有三四起发生，这次黑客攻击在数量和速度上都有大幅度的提高。这次的黑客大战，使用了两种攻击手段。一是利用 Microsoft IIS 5.0 默认提供了对 WebDAV 的支持，通过 HTTP 向用户提供远程文件存储的服务。IIS 5.0 包含的 WebDAV 组件不能充分检查传递给部分系统组件的数据，远程攻击者利用这个漏洞对 WebDAV 进行缓冲区溢出攻击，可能以 Web 进程权限在系统上执行任意指令。二是利用 TCP/IP 协议本身的缺陷，如 DOS 拒绝服务攻击也是本次黑客大战所常见的攻击方法，并不可防御。

2003 年 8 月 11 日，一种名为“冲击波”(WORM_MSBlast. A)的新型蠕虫病毒开始在我国 Internet 和部分专用信息网络上传播。该病毒传播速度快、涉及范围广，对计算机正常使用和网络运行造成严重影响。该病毒能够在短时间内造成大面积的泛滥，是因为病毒运行时会扫描网络，寻找操作系统为 Windows 2000/XP 的计算机，然后通过 RPC 漏洞进行感染，并且该病毒会操纵 135、4444、69 端口危害系统。受到感染的计算机中 Word、Excel、PowerPoint 等文件无法正常运行，弹出找不到链接文件的对话框，“粘贴”等一些功能无法正常使用，计算机出现反复重新启动等现象。Windows 的 RPC 服务(RPCSS)存在漏洞，“冲击波”正是通过 Windows 的 RPC 漏洞来传播的，当发送一个畸形包的时候，会导致 RPC 服务无提示的崩溃。由于 RPC 服务是一个特殊的系统服务，许多应用和服务程序都依赖于它，从而导致这些程序与服务无法进行。同时可以通过劫持 epmapper 管道和 135 端口的方法来提升权限和获取敏感信息。

2004 年病毒和黑客的破坏仍然呈上升趋势，特别是 ADSL 宽带的普及和越来越多的企事业单位搭建了局域网，使病毒传播速度越来越快。2004 年 4 月 30 日“震荡波”(Sasser)病毒被首次发现，短短一个星期之内就感染了全球 1800 万台计算机，成为当年当之无愧的“毒王”。它利用微软公布的 LSASS 漏洞进行传播，可感染 Windows NT/XP/2003 等操作系统，开启上百个线程去攻击其他网上的用户，造成机器运行缓慢、网络堵塞。

2005 年，美国超过 300 万的信用卡用户资料外泄，导致用户财产损失。同时，中国工商银行、中国银行等金融机构先后成为黑客们模仿的对象，设计了类似的网页，通过网络钓鱼

的形式获取利益。这一现象在2005年以平均每个月73%的数字增长，使很多用户对于网络交易的信心大减，因此各家银行对于网络交易安全十分重视。针对这些愈演愈烈的网上银行诈骗事件，中国人民银行于10月30日向社会公布《电子支付指引(第一号)》，对银行从事电子支付活动提出了指导性要求，对银行针对不同客户在电子支付类型、单笔支付金额和每日累计支付金额等方面做出合理限制。

2005年6月21日，北京市网络行业协会联合新浪、搜狐、金山、瑞星等16家网络和软件企业联合起草了《软件产品行为安全自律公约》，联合承诺共同防范“流氓软件”带给网民的麻烦。随后，在北京市网络行业协会的网站上，接受网民的投诉，引起众多网民的关注与投诉。同年7月11日，网络行业协会根据网民的投诉，点名公布了10家流氓软件名单，包括了3721、淘宝、易趣、DUDU等多家知名软件。

2005年5月至2006年5月间，有54%的被调查单位发生过网络安全事件，其中，感染计算机病毒、蠕虫和木马程序为84%；遭到端口扫描或网络攻击的占36%；垃圾邮件占35%。未修补和防范软件漏洞仍然是导致安全事件发生的最突出原因，占发生安全事件总数的73%。目前，网络安全产品中防火墙和计算机病毒防治产品使用率最高，分别达到81%和79%。网络浏览、下载仍然是病毒传播的最主要途径，通过U盘、移动硬盘等存储介质传播病毒的情况明显增多。目前，以盗取用户账号、密码的“间谍软件”、木马明显增多，计算机病毒本土化制作的趋势更加明显，利用计算机病毒非法牟利的情况日益突出。

1.1.3 网络安全发展现状

调查报告显示：在信息网络中有88%的网站承认在最近一年内受到了病毒感染和入侵，它们中间有90%都已安装了防火墙和入侵监测等安全设备。目前宽带条件下的网络安全问题主要表现在以下方面。

1.1.3.1 垃圾邮件泛滥

随着宽带网络的逐步普及和不断发展，电子邮件的普遍应用，垃圾邮件已经影响网络运营，是当前网络安全的重要问题，其主要危害如下。

(1) 邮件服务器运行缓慢。垃圾邮件造成邮件服务运行缓慢，甚至造成邮件服务器瘫痪，邮件用户的服务质量急剧下降，给运营商造成不良影响。

(2) 服务质量下降。大量的垃圾邮件，占用了有效的网络带宽，造成网络服务质量下降。

(3) 严重影响正常邮件通信。由于国内邮件服务商缺乏技术手段和管理不善，对于垃圾邮件控制不利，使垃圾邮件泛滥，造成了国外反垃圾邮件组织针对国内邮件服务商进行封锁，严重地影响了正常的邮件通信。

1.1.3.2 黑客攻击

安全专家表示，无论是中小企业，还是世界500强企业，都面临越来越多的黑客攻击、感染病毒等事件，已经严重地影响到企业的信息安全。宽带网络条件下，拒绝服务攻击是常见的方式：

(1) 网络黑客蓄意发动的针对服务和网络设备的DDOS攻击。

(2) 用蠕虫病毒等新的攻击方式,造成网络流量急速提高,导致网络设备崩溃,或者造成网络链路的不堪负重。

1.1.3.3 内部用户网络攻击

(1) 网络带宽被占用。宽带网络、宽带运营商公司的普及,以及黑客软件在网络上随处可见,使大量的内部用户可以通过网络进行扫描和攻击,造成网络带宽被占用,给网络运营商带来不良影响。

(2) 内部用户网络攻击泛滥。由于在宽带网络建设中注重可用性,忽视了管理性,造成对内部用户的网络攻击现象,没有很好的措施进行有效的监控和防护。

1.1.3.4 其他安全问题

(1) 新的攻击性病毒有效预防。

(2) 宽带环境下内容过滤。

(3) 宽带环境的入侵检测等问题。

1.1.4 黑客发展历史

黑客的历史可以追溯到20世纪五六十年代。麻省理工学院(MIT)率先研制出"分时系统",学生们第一次拥有了自己的计算机终端。不久后,MIT学生中出现了大批狂热的计算机迷,他们称自己为"黑客"(Hacker),即"肢解者"和"捣毁者",意味着他们要彻底"肢解"和"捣毁"大型主机的控制。

1961年,拉塞尔等三位大学生,在PDP-1上编制出第一个游戏程序"空间大战"。其他学生也编制出更多更"酷"的玩意,例如,象棋程序、在分时系统网络里给别人留言的软件等。MIT的"黑客"属于第一代,他们开发了大量有实用价值的应用程序。

20世纪60年代中期,起源于MIT的"黑客文化"开始弥散到美国其他校园,逐渐向商业渗透,黑客们进入或建立计算机公司。他们中最著名的有贝尔实验室的邓尼斯·里奇和肯·汤姆森,他俩在小型计算机PDP-11/20编写出UNIX操作系统和C语言,推动了计算机工作站和网络的成长。

MIT的理查德·斯德尔曼后来发起成立了自由软件基金会,成为国际自由软件运动的精神领袖。他们是第二代"黑客"的代表人物。

1975年,爱德华·罗伯茨发明第一台微型计算机"牛郎星"。美国很快出现了一个计算机业余爱好者在汽车库里组装微计算机的热潮,并组织了一个"家庭酿造计算机俱乐部",相互交流组装计算机的经验。以"家酿计算机俱乐部"为代表的"黑客"属于第三代,他们发动了一场个人计算机的革命。史蒂夫·乔布斯、比尔·盖茨等人创办了苹果和微软公司,后来都成了重量级的IT企业。

新一代"黑客"伴随着"嬉皮士运动"出现。艾比·霍夫曼是这代黑客的"始作俑者"。霍夫曼制造了许多恶作剧,常常以反对越战和迷幻药为题。1967年10月,他领导了一次反战示威,号召黑客们去"抬起五角大楼"。他还创办了一份地下技术杂志《TAP》,告诉嬉皮士