


PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI
普通高等学校信息安全“十一五”规划教材

# 网络与系统攻击技术

WANGLUO YU XITONG GONGJI JISHU

李毅超　曹　跃　梁　晓　编著
曾家智　主审

电子科技大学出版社

PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI
普通高等学校信息安全"十一五"规划教材

# 网络与系统攻击技术

李毅超　曹　跃　梁　晓　编著

曾家智　主审

电子科技大学出版社

**图书在版编目（CIP）数据**

网络与系统攻击技术/ 李毅超，曹跃，梁晓编著. —成都：电子科技大学出版社，2007.7

普通高等学校信息安全“十一五”规划教材

ISBN 978-7-81114-222-8

Ⅰ. 网… Ⅱ. ①李… ②曹… ③梁… Ⅲ. 计算机网络—安全技术—高等学校—教材 Ⅳ. TP393.09

中国版本图书馆 CIP 数据核字（2007）第 114315 号

**内 容 提 要**

本书为普通高等学校信息安全“十一五”规划教材之一，内容深入浅出，新颖丰富，从网络安全和系统安全两个角度，深入剖析了各种入侵、攻击技术及原理，并给出了实例和防范策略。本书内容涵盖了网络与系统攻击技术的目标、方法、模型；网络信息探测；系统信息探测；拒绝服务攻击；软件缓冲区溢出漏洞攻击；Web 与数据库安全漏洞攻击；病毒、蠕虫和木马等恶意代码攻击以及新兴的网络攻击等。本书注重科学性与实用性，并配有精选实例，供读者参考。

本书既可作为计算机、通信、信息安全专业本科生和硕士生的教材，也可供从事相关领域的科研和工程技术人员参考。

普通高等学校信息安全“十一五”规划教材

# 网络与系统攻击技术

李毅超 曹 跃 梁 晓 编著

曾家智 主审

**出 版：** 电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦 邮编：610051）

**策划编辑：** 曾 艺

**责任编辑：** 曾 艺

**主 页：** www.uestcp.com.cn

**电子邮件：** uestcp@uestcp.com.cn

**发 行：** 新华书店经销

**印 刷：** 成都蜀通印务有限责任公司

**成品尺寸：** 185mm×260mm **印张** 19.625 **字数** 480 千字

**版 次：** 2007 年 8 月第一版

**印 次：** 2007 年 8 月第一次印刷

**书 号：** ISBN 978-7-81114-222-8

**定 价：** 30.00 元

# 编委会名单

## 编委会主任

郝玉洁

## 编委（按姓氏笔画为序）

刘乃琦　许春香　李毅超　佘　堃

周世杰　秦　科　谌黔燕　鲁　珂

## 学术顾问

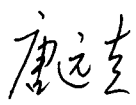
秦志光　李建平　周明天

# 序言

随着社会信息化的快速发展，信息已成为社会发展的重要资源，围绕着这一资源所展开的全球性的竞争日趋激烈。信息的安全已不再是个人和涉及少数人利益的问题，而是事关部门、公司、企业甚至国家、地区等政治和经济利益的十分重要的问题。信息安全正在作为一种产业快速发展，而与此相悖的是，信息安全人才匮乏，远远不能满足商业、金融、公安、军事和政府等部门的需求。因此，培养信息安全领域的高技术人才已成为我国高等工程教育领域的重要任务。

信息安全是集计算机、通信工程、数学等学科知识为一体的交叉型新学科，对于这一新兴学科的培养模式和课程设置，各高等院校普遍缺乏经验，为此，电子科技大学计算机科学与工程学院信息安全专业的专家、学者和工作在教学一线的老师们，以我国本科高等工程教育人才培养目标为宗旨，组织了一系列信息安全的研讨活动，认真研讨了国内外高等院校信息安全专业的教学体系和课程设置，在进行了大量前瞻性研究的基础上，启动了普通高等院校信息安全“十一五”规划教材的编写工作。该系列教材由 8 本理论教材和 2 本实验教材组成，全方位、多角度地阐述了信息安全技术的原理，反映了当代信息安全研究发展的趋势，突出了实践在高等工程教育人才培养中的重要性，弥补了目前该类教材理论教学内容丰富，而实践教学不成体系的缺点，使其成为该系列教材的特点，也是其成功所在。

感谢电子科技大学信息安全专业的老师们为促进我国高等院校信息安全专业建设所付出的辛勤劳动，相信这套教材一定会成为我国高等院校信息安全人才培养的优秀教材。同时希望电子科技大学的教师们继续努力，为培养更多、更好的信息安全人才，为我国的信息安全事业作出更大的贡献。



二〇〇七年三月十日于香港


唐远炎　国际电子电气工程学会会士（IEEE Fellow）
国际模式识别学会会士（IAPR Fellow）
国际 IEEE SMC 机器学习委员会主席（Machine Learning Committee, IEEE SMC）
《中国高等学校学术期刊》计算机科学分册（Frontiers of Computer Science in China）副主编
国际 SCI 检索刊物《International Journal on Wavelet, Multiresolution, and Information Processing（IJWMIP）》（小波、多尺度分辨及信息处理国际期刊）创办人、主编
国际 SCI 检索刊物《International Journal of Pattern Recognition and Artificial Intelligence（IJPRAI）》（模式识别与人工智能国际期刊）副主编

# 前言

随着 Internet 的迅速普及和发展，Internet 已经成为现代社会的基础设施，并渗透到人们工作和生活的方方面面。计算机病毒扩散、网络黑客攻击、计算机网络犯罪等现象频繁见诸于全球各新闻媒体，信息安全也已经不再是只有国家机要保密部门和专家学者关心的问题，而逐渐受到人们的普遍关注。信息安全正在成为国际社会的关注焦点。

信息安全包括攻与防两大范畴，二者相生相克不断发展。面对攻击者日趋嚣张的攻击气焰，面对攻击者层出不穷的技术手段，有道是 “知己知彼，百战不殆”，只有深入研究各种网络和系统攻击技术，才能有效地做好网络和系统的防护，才能更好地保障国家的政治安全、军事安全、经济安全，维护社会安定。

本书共分九章，内容涵盖如下:

第一章　网络与系统攻击技术概述，讲述网络与系统攻击的目标、分类、模型。

第二章　网络信息探测，描述了如何确定目标系统，介绍了各种常见系统存活探测，基本和高级的端口服务扫描，网络环境探测。

第三章　系统信息探测，介绍了服务版本类型探测，详细描述了操作系统指纹探测的原理和衍生的各种探测方法，最后介绍了 Windows 和 Linux 操作系统信息探测实例。

第四章　拒绝服务攻击，介绍了拒绝服务类型，本地拒绝服务攻击，远程拒绝服务攻击和分布式拒绝服务攻击，从理论到实例深入浅出地阐述了拒绝服务攻击的原理和方法。

第五章　软件缓冲区溢出漏洞攻击，介绍了缓冲区溢出概述，栈溢出攻击，堆溢出攻击，格式化字符串攻击，ShellCode 编写，并提供了缓冲区溢出防范的方法。

第六章　Web 与数据库攻击，介绍了 CGI，ASP 脚本攻击，PHP 脚本攻击，讲述了 MySQL 注入攻击，SQL Server 注入攻击。

第七章　计算机木马，首先介绍了计算机木马的特征和发展趋势，接着分别介绍了系统服务木马，反弹端口木马，SPI 隐蔽木马，最后讲述了木马的各种不同的启动方式。

第八章　计算机病毒与蠕虫，介绍了计算机病毒的特征，感染机制，触发机制；对引导扇区病毒、COM 文件病毒、EXE 可执行文件病毒三种计算机病毒实例进行分析，接着介绍了计算机蠕虫及其传播机制，最后是计算机蠕虫实例。

第九章　新兴网络攻击，介绍了网络钓鱼、P2P 攻击等新兴网络攻击方式。

本书内容系统全面，重点突出，在广度、深度和新颖性方面都作了合理的安排。本书由电子科技大学计算机科学与工程学院长期从事网络安全技术科研工作的李毅超副教授、曹跃助教、梁晓硕士研究生共同完成编写，最后由曾家智教授审稿。参加本书相关工作的还有任

云韬、崔甲、覃丽芳、李晓冬、何子昂、黄沾、钱彦江、刘凯、阳广元、肖武、杨宇和柴方明等实验室研究生。本教材还得到电子科技大学“十一五”教材建设项目的支持。在此，向所有在本书编写过程中给予关心和帮助的人士表示衷心的感谢。

限于水平和经验，疏漏和失当之处敬请各位专家、学者和读者批评指正。

作 者

2007 年 3 月

# 目录

## 第 1 章　网络攻击原理与技术



## 第 2 章　网络信息探测

## 第 3 章 系统信息探测



## 第 4 章 拒绝服务攻击

## 第 5 章 软件缓冲区溢出攻击



## 第 6 章 Web 与数据库攻击

## 第 7 章 计算机木马



## 第 8 章 计算机病毒与蠕虫

## 第 9 章 新兴网络攻击



## 附 录 专家们公认最危险的 20 个安全弱点与防范


# 第1章

# 网络攻击原理与技术

## 1.1 网络攻击概述

Internet 的飞速发展和普及，促进了网络信息系统的应用和发展。许多关系到国计民生的重要应用，如交通控制和国防信息系统等，越来越依赖于计算机网络。社会信息化和信息网络化，突破了应用信息在时间和空间上的障碍，使信息的价值不断提高。各种基于网络的信息系统已成为国民经济关键领域中的重要组成部分，例如，电力信息系统、汽油运输和存储系统、金融服务信息系统等。然而，对网络的依赖性越大，所产生的风险也越来越大。网络系统面临入侵、事故、失效等威胁，这不但影响网络系统本身，还将形成一种链式反应，产生重大后果。

受社会因素的影响，网络信息会受到破坏、窃取、篡改等威胁，造成信息无法使用。信息安全拓宽了国家安全概念，信息是国家的重要战略资源，也是公司、社会部门、个人的资产。网络信息化改变了传统意义上的有形空间安全概念，无形的“数字信息空间”的安全问题越来越突出。“数字信息空间”逐步深入到社会的方方面面，但是由于它“看不见，摸不着”的独特性，大多数人未曾意识到它的安全问题。

近年来，随着网络攻击技术和工具的迅速发展，依靠网络提供办公服务和业务服务的机构面临越来越大的风险。只有加深对网络攻击技术发展趋势的了解，才能够尽早采取相应的防护措施。目前网络攻击技术和攻击工具正在向以下几个方面快速发展。



**1．网络攻击的自动化程度和攻击速度不断提高**

自动化攻击一般涉及四个阶段，每个阶段都发生了新的变化。在扫描阶段，扫描工具的发展，使得黑客能够利用更先进的扫描模式来改善扫描效果，提高扫描速度；在渗透控制阶段，安全脆弱的系统更容易受到损害；随着攻击传播技术的发展，使得以前需要依靠人启动软件工具发起的攻击，发展到攻击工具可以自己发动新的攻击；在攻击工具的协调管理方面，随着分布式攻击工具的出现，黑客可以容易地控制和协调分布在 Internet 上的大量已部署的攻击工具。目前，分布式攻击工具能够更有效地发 动拒绝服务攻击，扫描潜在的受害者，危害存在安全隐患的系统。

**2．攻击工具越来越复杂**

攻击工具的开发者正在利用更先进的技术武装攻击工具，攻击工具的特征比以前更难发现，它们已经具备了反侦破、动态行为、更加成熟等特点。反侦破是指黑客越来越多地采用具有隐蔽攻击特性的技术，使安全专家需要耗费更多的时间来分析新出现的攻击工具和了解新的攻击行为。动态行为是指现在的自动攻击工具可以根据随机选择、预先定义的决策路径或通过入侵者直接管理，来变化它们的模式和行为，而不是像早期的攻击工具那样，仅能够以单一确定的顺序执行攻击步骤。攻击工具更加成熟，是指攻击工具已经发展到可以通过升级或更换工具的一部分迅速变化自身，进而发动迅速变化的攻击，且在每一次攻击中会出现多种不同形态的攻击工具；同时，攻击工具也越来越普遍地支持多操作系统平台运行；在实施攻击的时候，许多常见的攻击工具使用了如 IRC 或 HTTP 等协议从攻击者处向受攻击计算机发送数据或命令，使得人们区别正常、合法的网络传输流与攻击信息流变得越来越困难。

**3．黑客利用安全漏洞的速度越来越快**

新发现的各种系统与网络安全漏洞每年都要增加一倍多，每年都会发现新类型的安全漏洞，网络管理员需要不断用最新的软件补丁修补这些漏洞。黑客经常能够抢在厂商修补这些漏洞前发现这些漏洞并发起攻击。

**4．防火墙被攻击者渗透的情况越来越多**

配置防火墙目前仍然是防范网络入侵者的主要保护措施，但是，现在出现了越来越多的攻击技术，可以实现绕过防火墙的攻击，例如，黑客可以利用 Internet 打印协议 IPP 和基于 Web 的分布式创作与翻译绕过防火墙实施攻击。

**5．安全威胁的不对称性在增加**

Internet 上的安全是相互依赖的，每台与 Internet 连接的计算机遭受攻击的可能性，与连接到全球 Internet 上其他计算机系统的安全状态直接相关。由于攻击技术的进步，攻击者可以较容易地利用分布式攻击系统，对受害者发动破坏性攻击。随着黑客软件部署自动化程度和攻击工具管理技巧的提高，安全威胁的不对称性将继续增加。

**6．攻击网络基础设施产生的破坏效果越来越大**

由于用户越来越多地依赖计算机网络提供各种服务，完成日常业务，黑客攻击网络基础设施造成的破坏影响越来越大。人们越来越怀疑计算机网络能否确保服务的安全性。黑客对网络基础设施的攻击，主要手段有分布式拒绝服务攻击、蠕虫病毒攻击、对 Internet 域名系统 DNS 的攻击和对路由器的攻击。分布式拒绝服务攻击是攻击者操纵多台计算机系统攻击一个或多个受害系统，导致被攻击系统拒绝向其合法用户提供服务。蠕虫病毒是一种自我繁殖的恶意代码，与需要被感染计算机进行某种动作才触发繁殖功能的普通计算机病毒不同，蠕虫病毒能够利用大量系统安全漏洞，可以自我繁殖，导致大量计算机系统在几个小时内受到攻击。对 DNS 的攻击包括伪造 DNS 缓存信息、破坏修改提供给用户的 DNS 数据、迫使 DNS 拒绝服务、域劫持等。对路由器的攻击包括修改、删除全球 Internet 的路由表，使得应该发送到一个网络的信息流改向传送到另一个网络，从而造成对两个网络的拒绝服务攻击。尽管路由器保护技术早已可供广泛使用，但仍然有许多用户没有利用已有的技术保护自己网络的安全。



## 1.2 网络攻击目标

网络攻击是指网络中用户未经授权的访问尝试或者未经授权的使用尝试。网络与系统攻击的主要目标是破坏网络或系统信息的保密性、信息的完整性、服务的可用性、信息的非否认性和运行的可控性。本节将对以上几种网络攻击目标进行介绍。

### 1.2.1 信息保密性

网络与系统信息的保密性目标是防止未经授权泄漏敏感信息。系统中的重要配置文件、用户个人邮件账号、商业数据等信息都是需要保密的信息。攻击者对于这些保密信息通常

都采用以下几种攻击方法：

**1．网络信息拦截**

网络攻击技术可以偷听移动电话，搭线窃听，或者偷看传输的电子邮件。

**2．Tempest 技术**

网络攻击者采用电子设备远距离监视电磁波的传送过程。灵敏的无线电接受装置能够在远处看到计算机作者输入的字符或者屏幕显示的内容。

**3．社交工程**

网络攻击者通过一系列的社交活动，获取需要的信息。一些攻击者给用户发送一个免费的实用程序，其实这个程序除了完成用户所需要的功能外，还隐蔽了一个将用户的计算机信息发送给攻击者的功能。这样，往往没有经验的用户容易被网络攻击者欺骗，从而泄漏相关的信息。

**4．网络信息重定向**

网络攻击者设法将信息发送端重定向到攻击者所在的计算机，然后再转发给接收者。例如，攻击者伪造某个网上的银行域名，用户不知真假，却按银行要求输入账号和密码，攻击者就此获取银行账号信息。

**5．数据推理**

数据聚合和相关入侵使攻击者有可能从公开信息推测出敏感信息。

**6．邮件病毒**

网络邮件病毒通过邮件传播带有病毒的文件，如 Word 文档或者黑客程序。邮件用户大多不小心执行了邮件附件，结果触发病毒程序执行。有些病毒程序将用户的文档发送到外部网络中，从而导致信息泄漏，典型的实例是“梅丽莎”邮件病毒。



## 1.2.2 信息完整性

网络与系统信息的完整性目标是防止未经授权修改信息。在一些特定的环境下，完整性可能比保密性更加重要。比如在一些网络电子转账过程中，如果用户需要转账 100 万，但由于信息完整性被攻破等问题，将 100 万改为了 1000 万，这样将会造成严重的后果。当前对于完整性的攻击主要有以下几种方式：

**1．身份认证攻击**

身份认证攻击是指攻击者伪装成具有特权的用户，常见的攻击方法有：密码猜测、口令窃取、网络连接口令窃取、密钥泄漏、中继攻击等。

**2．程序异常输入**

利用程序设计者的疏忽，攻击者可以通过输入异常数据给某个接受程序，导致该程序出现异常，最常用的输入异常攻击是缓冲区溢出攻击方法。攻击者有意向程序输入大量的字符，造成缓冲区溢出，而溢出的地址指向一段带有恶意的程序。这样，攻击者就可以获得系统更高的权限，进而修改敏感信息。