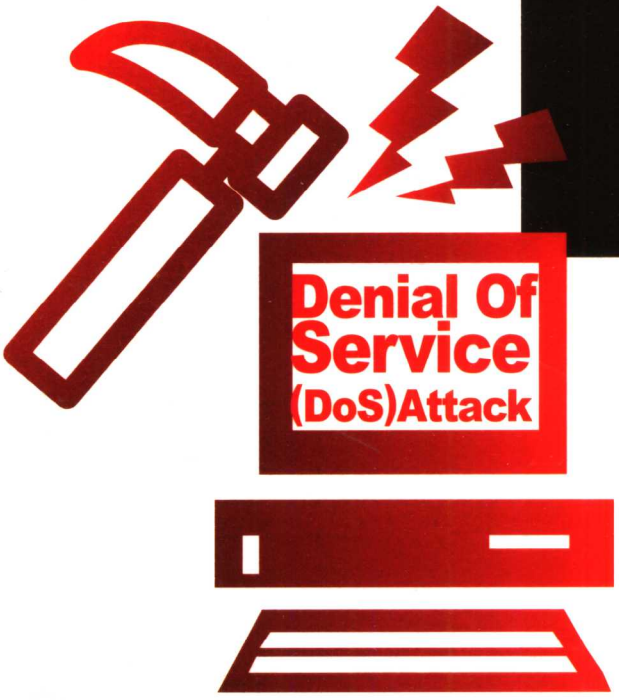
电子信息科技专著出版专项资金
cbjj.phei.com.cn

安全技术大系

Denial of Service (DoS) Attack

拒绝服务攻击



李德全 著

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

电子信息科技专著出版专项资金资助出版

安全技术大系

Denial of Service (DoS) Attack

拒绝服务攻击

李德全 著

国家自然科学基金资助项目（项目编号：60273027）
国家杰出青年基金资助项目（项目编号：60025205）

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

内 容 简 介

随着网络技术和网络应用的发展，网络安全问题显得越来越重要。拒绝服务攻击由于容易实施、难以防范、难以追踪等特点而成为最难解决的网络安全问题之一，给网络社会带来了极大的危害。同时，拒绝服务攻击也将是未来信息战的重要手段之一。因此，了解和研究拒绝服务攻击的原理，探索其对策，从而在日常工作中有效地应对拒绝服务攻击是极为重要的。

本书对拒绝服务攻击的原理进行了较深入的探讨，然后分析了针对拒绝服务攻击的各种对策，包括拒绝服务攻击的防御、检测和追踪等。特别是，作为拒绝服务攻击对策的新方法——数据来源的追踪这一既可为追究法律责任提供证据，又可为其他对策如数据包的过滤、限流等提供及时信息的方法也在本书中做了详细深入的探讨。

本书既有较深的理论研究，又有丰富的实用技术，内容丰富，可供相关领域科研和工程技术人员参考，也可作为相关专业高年级本科生、研究生的网络攻防、防火墙、入侵检测等类课程的教学参考书。

图书在版编目（CIP）数据

拒绝服务攻击 / 李德全著. —北京：电子工业出版社，2007.1
（安全技术大系）
ISBN 978-7-121-03644-6

I. 拒… 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（2006）第 153571 号

责任编辑：孙学瑛
印　　刷：北京智力达印刷有限公司
装　　订：北京中新伟业印刷有限公司
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：24.75　字数：531 千字
印　　次：2007 年 1 月第 1 次印刷
印　　数：4000 册　　定价：49.00 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，联系电话：（010）68279077；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

拒绝服务攻击由于容易实施、难以防范、难以追踪等特点而成为最难解决的网络安全问题之一，给网络社会带来了极大的危害。因为容易实施，即使不懂网络安全，甚至是刚学会使用计算机的人，都可以很容易地利用网上下载的攻击软件发起拒绝服务攻击；而因为难以防范，目前，大多数情况下受害者对拒绝服务攻击仍旧束手无策；又因为可以采用伪造源地址方式进行攻击或者使用傀儡计算机进行攻击，还没有直接有效的方法追踪到真正的攻击者，从而导致责任追究的困难。这些原因导致拒绝服务攻击的案例越来越多，造成的损失越来越大。

同时，拒绝服务攻击的上述特征也为其在军事领域中的应用创造了极为有利的条件，如今拒绝服务攻击业已成为信息战的重要手段之一。

因此研究拒绝服务攻击的原理，探索其对策，对于在日常的工作中有效地应对拒绝服务攻击，在对敌斗争中合理利用拒绝服务攻击以及防御敌对势力的攻击都是极为重要的。

作者根据多年的研究成果和经验，撰写了这本《拒绝服务攻击》，希望能给广大读者提供借鉴和参考。

由于蠕虫也是导致拒绝服务的重要原因之一，因此，出于完整性考虑，笔者在本书中预留了一章专门介绍蠕虫，鉴于中科院软件所的文伟平博士在蠕虫方面有着深入的研究，作者请文博士协助撰写了第 6 章蠕虫攻击及其对策。

需要说明的是，为了读者更好地理解相关攻击技术，我们除讲述攻击的原理外还分析讨论了一些来自 Internet 上的程序实例，这对于读者更好地检测、防御这些攻击是有益的。同时，为了读者理解和应用的方便，我们对一些程序进行了调试并做了一些小的修改。当然，技术本身并没有好与坏之分，好坏之别只在于其使用者——人。因此，本书中介绍的知识和技能也是双刃剑，希望读者善用之。特别是本书中介绍的一些攻击演示软件，请读者仅在自己管理的网络环境中进行实验或测试。

作者将在研究拒绝服务攻击和撰写本书过程中所用的一些参考资料一并提供给读者参考（可到 www.broadview.com.cn 网站下载），希望对读者查询相关资料有所帮助。

由于作者水平有限，疏漏之处在所难免，欢迎广大读者批评指正。

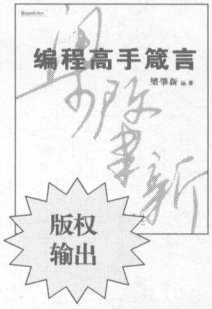
作者关于此书内容的研究得到了中科院软件所冯登国老师、苏璞睿博士和中国海洋大学曲海鹏博士等的大力帮助。本书的写作也得到了众多信息安全专家的指导和帮助，特别是中国海洋大学的曲海鹏博士给本书提供了很多有益的建议。本书在出版过程中得到了电子工业出版社各位老师的支持和帮助，特别是得到了电子工业出版社计算机图书事业部主任（总经理）郭立女士的大力支持。在此一并表示感谢。

笔　者

于中科院软件所　信息安全国家重点实验室

2006.11

典藏本版精品



荣获 2004 年度“中国图书奖”和“全国优秀畅销书奖”！

编程高手箴言

梁肇新 编著
2003 年 11 月出版　　ISBN 7-5053-9141-0
50.00 元（含光盘 1 张）　　416 页

中国最具知名度的程序员之一，《超级解霸》作者梁肇新首部专著！

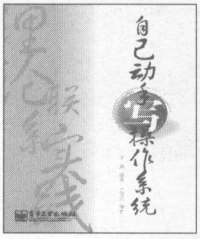
全书通篇没有时髦的 IT 新名词或新思想，而是踏踏实实地对很多知识进行了深刻的剖析，有助于为编程打下坚实的根基。

国内第一本重量级 Hibernate 图书。

深入浅出 Hibernate

夏昕、曹晓钢、唐勇 编著
2004 年 7 月出版　　ISBN 7-121-00670-7
59.00 元　　545 页

本书由互联网上影响广泛的开放文档 OpenDoc 系列自由文献首份文档“Hibernate 开发指南”发展而来。在编写过程中，进行了重新构思与组织，同时对内容的深度与广度进行了重点强化。



用理论指导动手实践
用实践深化理解理论

自己动手写操作系统

于渊 编著
2005 年 8 月出版　　ISBN 7-121-01577-3
48.00 元（含光盘 1 张）　　374 页

本书不同于其他的理论型书籍，而是提供给读者一个动手实践的路线图。

在详细分析操作系统原理的基础上，用丰富的实例代码，一步一步地指导读者用 C 语言和汇编语言编写出一个具备操作系统基本功能的操作系统框架。

同类书销量第一！

ERP 原理 设计实施(第 3 版)

罗鸿 编著
2005 年 4 月出版　　ISBN 7-121-01059-3
38.00 元　　384 页

本书对 ERP 相关知识的讨论涵盖了原理、设计与应用的全部过程。前两版出版后均引起了很大的社会反响，作者收到大量读者来信，并与读者进行了良好的交互。第 3 版再次增加了一些内容，更加贴近读者需要。

荣获 2003 年“全国优秀畅销书奖”，看雪论坛鼎立打造！

加密与解密（第二版）

段钢 编著
2003 年 6 月出版　　ISBN 7-5053-8648-4
49.00 元（含光盘 1 张）　　519 页

本书全面讲述了 Windows 平台下的最新软件加密与解密技术及相关解决方案，采用循序渐进的方式，从基本的跟踪调试到深层的拆解脱壳，从浅显的注册码分析到商用软件保护，几乎囊括了 Windows 下的软件保护的绝大多数内容。

本书通过多种典型实例详细介绍了在 Windows 系统下数据恢复技术的原理和方法。

数据恢复技术（第 2 版）

戴士剑、涂彦晖 编著
2005 年 3 月出版　　ISBN 7-121-00756-8
69.00 元　　711 页

本书内容包括：硬盘数据组织、文件系统原理、数据恢复技术、文档修复技术、密码遗失处理技术、数据安全技术和数据备份技术。作者戴士剑是国内知名数据恢复专家，有多年的数据恢复工作经验，为客户提供过上千次的数据恢复服务。

目　录

CHAPTER 1

第1章 引言

1.1 计算机网络的迅猛发展

在信息技术的推动和牵引下，人类社会已由工业时代迈进信息时代。当前，世界范围的 Internet 网络已得到空前发展并正在日新月异地改变着政治、经济、军事和文化等社会生活的各个方面。由于 Internet 的飞速发展，它早已成为一个覆盖世界的“全球网”。今天，在发达国家自不待言，即使是在中国这样的发展中国家，不仅企事业单位，居民个人上网也在飞速发展中。据中国互联网络信息中心 2005 年 1 月的《中国互联网络发展状况统计报告》[CNNIC0501]，到 2004 年底，在北京、上海这样的政治、经济、文化中心，上网用户数均已超过人口总数的四分之一，即使在西藏、青海、新疆这样的经济相对不是很发达的地区，网民数也已分别达到了本地人口的 2.6%、3.7%和 6.2%[①]。据该中心 2005 年 7 月的同类报告[CNNIC0507]，截止到 2005 年 6 月 30 日，我国的上网计算机总数已达 4560 万台，同半年前的调查结果相比，我国的上网计算机总数半年内增加了 400 万台，增长率为 9.6%，和上年同期相比增长了 25.6%；截止到 2005 年 6 月 30 日，我国的上网用户总人数为 10 300 万人，同半年前的调查相比，我国上网用户总人数半年内增加了 900 万人，增长率为 9.6%，和上年同期相比增长了 18.4%。由此可见，国内的上网计算机数和上网人数都在高速增长，网络对社会生活的影响已逐步深入。图 1.1 和图 1.2 分别为中国国内历年上网计算机数和上网人数统计情况。

① 其 2005 年 7 月的报告中没有对各省份的类似统计数字，所以我们仅以 2005 年 1 月的报告来说明此问题。

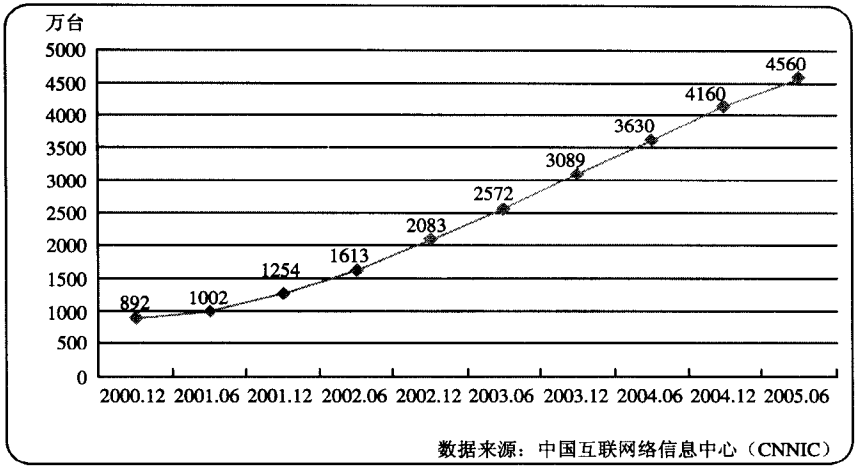


图 1.1　中国国内历年上网计算机数统计

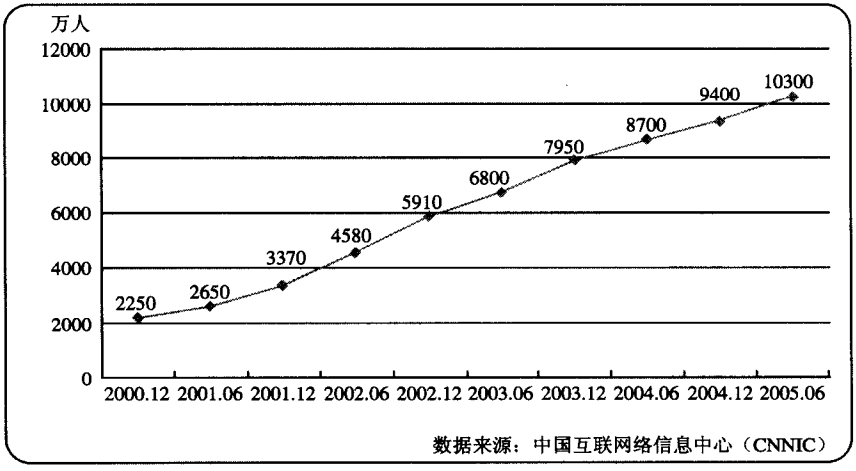


图 1.2　中国国内历年上网人数统计

现在，随着电子商务、电子政务等的发展，我们不仅可以通过网络与远方的朋友即时通信、发送电子邮件，而且，足不出户就可以通过网络购物、付费、接受远程教育、远程医疗服务等。利用由电话线与办公室网络连接的计算机在家中办公已经不再神秘。2003 年 4、5 月间，由于北京 SARS 疫情严重，许多企事业单位都实行轮流值班，没有轮到值班的员工则在家里办公。很多 IT 相关的公司职员尤其体验到了在家办公的好处，那就是既不影响工作，又避免了上下班途中的奔波劳累之苦。世界各国电子商务、电子

政务的发展进一步促进了网络应用的发展。现在，我们对网络的依赖在逐渐增加，特别是对一些年轻的 IT 从业人员和广大“网虫”而言，一旦没有了网络（比如因为停电或者其他原因使网络暂时不可用），就会有不知所措之感。因此，网络已经深入到了我们生活的方方面面，成为生活中不可或缺的东西。

1.2 网络安全问题日渐突出

然而，任何事物都有它的两面性，网络亦然。随着人们越来越依赖于计算机网络，网络安全成为一个摆在我们面前的亟待解决的问题。例如，在 2000 年 2 月的黑客攻击事件中，世界著名的雅虎、亚马逊、微软等公司的网络遭黑客攻击而几近全面瘫痪，直接经济损失高达数十亿美元。CIH 病毒的肆虐、“红色代码”的泛滥等也给人们平静的网络生活掀起了千层波澜。

近年来，网络攻击的数量在逐年上升，从 1998 年到 2003 年，平均年增幅达 50%左右，如图 1.3 所示[①]（数据来源于[CERT_stats]）。为什么会有这么多的网络攻击事件发生呢？一方面，攻击者是有目的的，与其他类型的犯罪一样，计算机攻击的目的既有政治和经济方面的，也有出于报复、炫耀等目的的。另一方面，计算机及其网络的漏洞层出不穷，且新发现的漏洞越来越多，如图 1.4 所示。从图 1.4 中可以看出，历年中，2002 年公布的漏洞数达到顶峰，达 4129 个，2003 年、2004 年在 2002 年的基础上稍有下降，但是 2002~2004 三年间 CERT 平均每天公布的漏洞数都在 10 个以上（数据来源于[CERT_stats]），而到 2005 年，CERT 统计的漏洞数竟然达到 5990 个，平均每天超过 16 个。需要注意的是，CERT 公布的只是其接到报告的，实际发现的漏洞数应该远远超过 CERT 所公布的数字。这些漏洞给了攻击者可乘之机。有了目的，有了可资利用的条件，网络攻击的发生就不足为奇了。

据美国计算机安全研究所（CSI）和联邦调查局（FBI）2002 年关于计算机犯罪和计算机安全的调查报告[CSI02]，在接受调查的 503 家机构中，有 60%在 2002 年内受到了攻击，其中有 223 家（占 503 家的 44%）量化了他们的经济损失，他们损失的总和达到 45.58 百万美元。据这两家机构 2003 年的同类报告[CSI/FBI03]，在接受调查的 530 家机构中有 75%（398 家）在年内受到了攻击，其中有 251 家（占 530 家的 47%）量化了他们的经济损失，其总和为 20.2 百万美元。据 2004 年的报告，有

① CERT 提供的此统计数据只到 2003 年，在本书的写作时，未见到 2004 年和 2005 年的统计数据。