LOIS

信息安全国家重点实验室

信息安全丛书

# Network Attacks: Principles and Techniques

# 网络攻击原理与技术

连一峰　王 航 编著

科学出版社
www.sciencep.com

信息安全国家重点实验室信息安全丛书

# 网络攻击原理与技术

连一峰　王航　编著

国家重点基础研究发展规划资助项目(项目编号:G1999035801)
国家自然科学基金重点项目(项目编号:90104030)

科学出版社
北京

## 内 容 简 介

本书讲述了利用计算机网络进行攻击和入侵的原理及相关技术，从整体结构上分为两个部分：第1章至第8章为技术篇，讲述各种流行的网络攻击及相关的防御对策，包括用于收集目标信息的网络调查技术，用于非法获取或提升目标系统访问权限的口令破解、系统后门、缓冲区溢出和格式化字符串攻击，以及用于破坏目标系统可用性的拒绝服务攻击等，对常见的安全漏洞和不安全编程问题进行了细致的分析，在此基础上介绍了一些常用的工具软件和Windows系统的取证技术；第9章至第11章为应用篇，讲述针对各种实际系统的攻击方法，介绍了针对Windows 9x/NT/2000/XP、Unix、Novell Netware操作系统的攻击，分析了利用远程访问破坏网络设备和访问控制机制的网络攻击方法，最后讲述了如何攻击常见的应用软件，如远程控制软件、Web服务软件、浏览器、邮件客户端以及IRC软件等。在介绍各种攻击方法的同时，作者也给出了一些相关的防范措施和安全建议，并列举了详细的参考资料和文献，供读者参考。

本书可作为计算机、通信、信息安全、密码学等专业的本科生、研究生的参考教材，也可供从事相关领域工作的科研和工程技术人员参考。

**图书在版编目(CIP)数据**

网络攻击原理与技术/连一峰，王航编著. —北京：科学出版社，2004
(信息安全国家重点实验室信息安全丛书/冯登国主编)
ISBN 7-03-012739-0

Ⅰ.网… Ⅱ.①连… ②王… 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(2003)第126448号

策划编辑：鞠丽娜 / 责任编辑：李 敏
责任印制：吕春珉 / 封面设计：王 浩

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销

*

2004年4月第 一 版 开本：B5(720×1000)
2004年4月第一次印刷 印张：28
印数：1—5 000 字数：561 000

**定价：43.00元**

(如有印装质量问题，我社负责调换〈路通〉)

# 《信息安全国家重点实验室信息安全丛书》编委会

# 序　言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。数字化的生存方式席卷全球。农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。电子政务、电子商务等各种信息化应用之花，如雨后春笋，在华夏沃土上竞相开放，炎黄子孙们，在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握，非一朝一夕之功。治水、训火、利用核能都曾经经历了多么漫长的时日。不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。

生产力的发展，为社会创造出许多新的使用价值。但是，工具的不完善，会限制这些使用价值的真正发挥。信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性，存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾御技能不足的情况下，损害着人们自身的利益。

世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。传统社会存在的不文明、暴力，在信息空间也同样存在。在这个空间频频发生的有些人利用系统存在的脆弱性，运用其“暴智”来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。什么是信息安全？怎样才能保障信息安全？这些问题都是严肃的科学和技术问题。面对人机结合，非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真的研究。我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头鼠脸，自暴自弃，我们需要的是具有革命的乐观主义精神，坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

人是有能力认识真理的，今天对信息安全的认识，就经历了一个从保密到保护，又发展到保障的趋近真理的发展过程。因为信息安全的问题不仅仅是因为技术原因引起的，它涉及到人、社会和技术，因此，仅仅靠技术是不能有效地实施信息安全保障的。从社会学的观点来看，只有依靠有信息安全觉悟和技能的人及科学有效的管理来实施综合的技术保障手段，才能取得良好的效果。

为了推动我国信息化发展的进程，信息安全国家重点实验室组织编写了《信息安全国家重点实验室信息安全丛书》。在本丛书的编写过程中，我们既注重学术水平，又注意其实用价值。本丛书从信息安全保障体系，操作系统安全，数据库安全，网络安全，无线网络安全，网络攻击，密码技术，PKI 技术，信息隐藏，安全协议，安全事件应急响应，量子密码通信等多个角度，分析和总结信息安全的科学问题以及信息安全保障的理论与技术，因此，这套丛书有较大的适用范围。我们将努力把国内外信息安全的最新研究成果写进书中，以使一些读者阅读本丛书后在理论、方法、技术上有新的启发和收获，从而切实解决工作中的实际问题。

本丛书的组织方式是开放式的，今后将根据学科发展陆续组织出版信息安全领域的优秀图书。

信息安全只能是相对而言，它是动态发展的。任何人都不能宣称自己终极了对信息安全的认识。让我们一起努力，不断地深化自己的研究，借鉴国外先进的科学技术，结合国情，与时俱进地推出信息安全保障的新理论、新办法和新手段，用我们的智慧保卫我们的信息疆土，使我们的信息家园尽量祥和安宁。

限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

《信息安全国家重点实验室信息安全丛书》编委会

2003 年 7 月

# 前　言

1946 年，第一台电子计算机 ENIAC（Electronic Numerical Integrator and Computer）诞生在美国宾夕法尼亚州。短短 50 年间，计算机技术经历了人类历史上最为惊人的发展历程。如今，面积仅有几十平方厘米的芯片，其处理能力已远远超过当年需要几个房间才能容纳下的庞大主机。

高速发展的计算机技术，不断普及的计算机应用，以及快速更新的网络技术和通信技术相结合，推动了互联网在中国乃至整个世界的飞速发展。Internet 目前已经成为全球信息基础设施的骨干网络，WWW、FTP、E-mail 等服务已经深入人们的日常生活，并逐渐成为正在蓬勃发展的电子商务的基础服务平台。人们把 Internet看做是第二次信息革命的象征，它不仅将彻底改变信息产业的运作方式，而且将对世界上其他大多数行业产生深远的影响，最终导致一场新的产业革命。

中国互联网络信息中心（CNNIC）于 2003 年 7 月发布了第 12 次《中国互联网络发展状况统计报告》。报告显示，截止到 2003 年 6 月 30 日，我国上网计算机约 2572 万台，网民总数已经达到 6800 万人，我国国际线路总容量为 18599M。互联网在中国已经进入高速发展期，并逐步进入了人们的日常生活，为人们的信息交流提供了极大的便利。但是，我们也应该注意到，在现实生活中，便利性和安全性始终是一对矛盾，网络环境中也同样如此。Internet 本身所具有的开放性和共享性对信息的安全问题提出了严峻的挑战。

由于系统安全脆弱性的客观存在，操作系统、应用软件、硬件设备不可避免地会存在一些安全漏洞，网络协议本身的设计也存在一些安全隐患，这些都为黑客采用非正常手段入侵系统提供了可乘之机。根据美国设立在卡内基·梅隆大学的计算机应急响应小组/协调中心（CERT/CC）的统计数据显示，近年来该机构所收到的安全事故逐年增加，近两年尤其显著：1998 年 3734 件，1999 年 9859 件，2000 年 2.1 万件，2001 年接近 5.3 万件，2002 年则是 8.2 万件，今年 1～9 月报告的安全事件就超过了 11 万件，几乎每年均以超过 100%的速度递增。安全事故的上升一方面可归结为人们安全意识提高，对安全事故的积极报告，另一方面则是由于攻击工具的无限制传播和存在安全漏洞的软件的广泛使用所造成的。

在国内，黑客事件同样频繁出现。据统计，源自我国的黑客事件在国际上排名第三。根据 CNNIC 的统计报告，用户认为目前的网上交易除了产品质量和售后服务之外，最大的问题是安全性得不到保障，有 25%的用户认可这一点，则说明人们对信息安全问题已经开始重视。在中国互联网络面临大发展的今天，在共同探讨互联网步入新发展阶段的若干问题时，业界人士已经形成了普遍的共识——中国互

联网在基础设施的构建上已逐步走向成熟，加强信息安全是目前运营和维护网络生态环境的关键所在。

在十几年前，网络攻击还仅限于破解口令和利用操作系统已知漏洞等有限的几种方法，然而目前网络攻击技术已经随着计算机和网络技术的发展逐步成为一门完整的科学，它囊括了信息收集、拒绝服务、密码及口令破解、非法获取及提升权限、网络窃听、利用操作系统、网络协议以及应用软件的漏洞进行攻击等各项技术。围绕计算机网络和系统安全问题进行的网络攻击与防范也受到了人们广泛的重视。为了帮助计算机网络的系统管理员、安全管理员以及广大的互联网用户更好地理解网络攻击的原理和相关技术，并且有针对性地采取相应的防范措施，本书从具体的原理和技术分析出发，介绍了目前流行于互联网的各种攻击方法，包括用于收集目标信息的网络调查技术，用于非法获取或提升目标系统访问权限的口令破解、系统后门、缓冲区溢出和格式化字符串攻击，用于破坏目标系统可用性的拒绝服务攻击等，并讲述了针对各种实际系统的攻击方法，介绍了针对 Windows 9x/NT/2000/XP、Unix、Novell Netware 操作系统的攻击，针对远程访问设备和访问控制机制的网络攻击，针对常用应用软件如远程控制软件、Web 服务软件、浏览器、邮件客户端以及 IRC 软件等的攻击方法；同时本书也给出了一些相关的防范措施和安全建议，并列举了详细的参考资料和文献供读者参考，希望能够对读者有所帮助。

在本书写作过程中重点参考了 Stuart McClure、Joel Scambray 和 George Kurtz 所著的《Hacking Exposed》第三版（McGraw-Hill Osborne Media 出版），另外还参考了一些在互联网上公布的研究论文和相关资料，书中恕不一一注明出处。这些资料来源于众多的大学、研究机构、安全团体、安全网站、公司以及一些研究计算机及网络安全问题的个人。对于他们在推动安全事业发展的过程中所做的工作和努力，在此表示衷心地感谢。写作过程中所参考的这些书籍资料，其版权属于原作者，特此声明。

本书的第 1 章至第 8 章，以及第 11 章的“Web 攻击”一节由王航撰写，第 9 章、第 10 章和第 11 章的其余部分由连一峰撰写。中国科学院研究生院信息安全国家重点实验室的冯登国教授和戴英侠教授、中国科学院软件所的林东岱研究员，以及其他各位老师对本书提供了宝贵的意见和建议，在此表示深深地谢意。此外，还要感谢信息安全国家重点实验室的胡艳、鲍旭华、李闻、冯萍慧为本书所做出的大量工作。

本书受国家重点基础研究发展规划资助项目（项目编号：G1999035801）和国家自然科学基金重点项目（项目编号：90104030）支持。

连一峰

2003 年 12 月 28 日

# 目　录

# 第 1 章　网络调查技术

## 1.1　最简单的办法

网络调查是指包括扫描在内的网络信息的搜集和判断，是攻击必不可少的一个步骤。网络调查的范围包括：网络的拓扑结构、主机 IP 地址和操作系统、打开的端口和各服务程序的版本等技术层面的信息，以及管理员姓名、爱好、E-mail 地址、电话号码等与人有关的信息。网络调查最简单也是最直接的办法就是正常的访问目标系统，通过登录尝试等方法合法地获得系统信息。举例来说，某个网站主页文件名为 default. asp，那么，很显然系统是 Windows NT/2000/XP + IIS 的配置。如果访问某网站时浏览器中得到下面这样的错误提示：

Microsoft VBScript 编译器错误 错误 '800a03f6'
缺少 'End'
/iisHelp/common/500-100. asp，行 242
Microsoft OLE DB Provider for ODBC Drivers 错误 '80004005'
[Microsoft][ODBC Microsoft Access Driver] 操作必须使用一个可更新的查询。
/bbs/article. asp，行 14

通过这几行提示，我们至少可以知道下面两条本不应该知道的信息：

1）该网站后台数据库使用的是 Access，而不是 SQL Server。

2）存在/iisHelp/common/500-100. asp 文件，并且这个程序的语法有错误，这也许说明程序员没有认真测试过代码。

Internet 上还有一些站点提供信息查询服务，例如，在 http://www. netcraft. com 主页上输入 Web 站点的域名或者 IP 地址，netcraft 可以告诉我们这台服务器使用的是哪种 Web 服务器，甚至还告诉我们该站点使用的操作系统。这样可以省去调查者的不少工作，最重要的是使用这种公开服务不会暴露调查者的身份。图 1. 1 是在 netcraft 网站上对 www. sina. com. cn 查询的结果，可以看出目标站点使用的是 FreeBSD 操作系统上的 Apache 2. 0. 45 作为 Web 服务器。

下面是用 perl 写的一段程序，读入一系列 IP 地址或者域名，该程序可以自动打印出这些地址或域名对应服务器的 80 端口返回的 banner 信息，这些信息中往往包含了 Web 服务器的类型和版本号等重要信息。

```
use Socket; use Getopt : : Std;
```

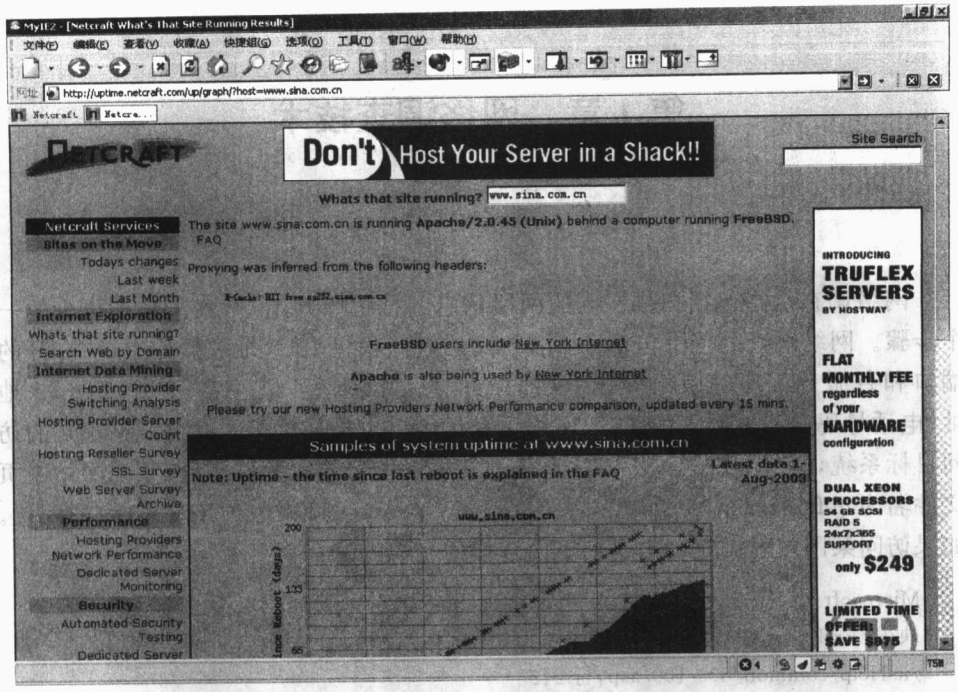


图 1.1　netcraft 查询结果

```
print "-- HTTP Banner Grab v1 --\n\n\n";
open(IPFILE,"ip.txt") || die("cannot open ip.txt\n");
while(<IPFILE>) {
    $ip= $_;
    chop($ip);
    print "\n----"."$ip"."----\n";
    $target= inet_aton($ip);
    &tryit;
}
close(IPFILE);
exit;

sub sendraw {          # this saves the whole transaction anyway
    my ($pstr)=@_;
    socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp')||0) ||
        die("Socket problems\n");
    if(connect(S,pack "SnA4x8",2,80,$target)){
```