

一本深入、细致
剖析互联网服务器攻击与防护技术的 **宝典!**

互联网服务器 攻防秘笈

卓文华讯 陈彬 编著

HULIANWANG



NLIC 2970669843

GONGFANG

MIJI



化学工业出版社

互联网服务器 攻防秘笈

卓文华讯 陈彬 编著

HULIANWANG



NLIC 2970669843

GONGFANG

MIJI



化学工业出版社

· 北京 ·

面对网络攻击事件的频繁发生,网民十分困惑和无助。知己知彼,才能决胜千里。深度接触黑客技术,才能有效防御黑客攻击,保证网站信息安全。本书意在立体解剖黑客攻击技术,深度传授反黑客防御要点。

本书是一本全面细致、深入浅出的互联网服务器攻防教材。全书深入揭露了黑客攻击互联网服务器的奥秘,展示了黑客入侵互联网服务器的各种伎俩,采用诸多实例以图文并茂、形象生动的方式详细讲解各种互联网服务器漏洞的利用原理以及真实有效的防御技术。

本书适合对网络安全技术有兴趣并想从事相关行业的大学生;就读于网络信息安全相关专业的研究生;负责企业、公司网络信息安全的从业者;网络安全技术专业研究人员;所有对网络安全有兴趣的爱好者。对各大中专院校计算机教师也有极大的参考价值。

图书在版编目(CIP)数据

互联网服务器攻防秘笈 / 卓文华讯, 陈彬等编著. —北京:
化学工业出版社, 2011.5
ISBN 978-7-122-10672-8

I. 互… II. ①卓… ②陈… III. 互联网络-网络服务器-安全技术-基本知识 IV. TP368.5

中国版本图书馆 CIP 数据核字 (2011) 第 034872 号

责任编辑: 陈 静
责任校对: 蒋 宇

装帧设计: 王晓宇

出版发行: 化学工业出版社 (北京市东城区青年湖南街 13 号 邮政编码 100011)

印 刷: 北京永鑫印刷有限责任公司

装 订: 三河市宇新装订厂

787mm×1092mm 1/16 印张 19¹/₂ 字数 455 千字 2011 年 5 月北京第 1 版第 1 次印刷

购书咨询: 010-64518888 (传真: 010-64519686) 售后服务: 010-64518899

网 址: <http://www.cip.com.cn>

凡购买本书, 如有缺损质量问题, 本社销售中心负责调换。

定 价: 39.00 元

版权所有 违者必究

前 言

本书是一本深入、细致剖析互联网服务器攻击与防护技术的书籍，主要阅读对象为服务器管理员、网络安全技术爱好者、信息安全专业教师与学生以及其他对网络安全有兴趣和有需要的人士。

本书的最大特点是系统性强、实战性强，通过系统化的知识梳理和数百个真实案例，全景式剖析了互联网服务器攻防技术。计算机技术是一门实践性很强的科学，本着“实践出真知，少理论，多实战”的宗旨，编者思考并总结了近十年黑客攻防和安全服务工作经验，写作了这本书。本书是国内实战性较强、技术系统化的攻防书籍，通过阅读本书，读者可以迅速掌握信息安全领域数十种主流安全技术。

一、为什么写这本书

互联网已经深入到人们生活的方方面面。人们每天使用互联网为生活提供各种服务——网购、游戏、看书、听歌、交友、学习、订票、工作。如果互联网变得不安全了，那会怎么样？

黑客攻击互联网服务器导致重大安全事故时有发生。由于被配置了固定的 IP，互联网服务器成为国内外黑客攻击的活靶子。它们如此重要，却为何不堪一击？

以前，大部分公司认为只要部署防火墙就可以保障服务器的安全。大部分管理员以为安装了杀毒软件、ARP 软件，经常打补丁就是服务器安全维护工作的全部。现在，越来越多的公司和管理员感觉到黑客防不胜防，常常因为黑客事件而焦头烂额。不少人不得不参加各类黑客网站的培训，甚至拜一些网络黑客为师，在花费了高额的学费后，依然无法掌握攻防技术。

服务器攻防技术如此重要，而市面上却没有一种专门讲述服务器攻防的书籍。编者撰写本书，希望能给广大读者朋友的工作和学习带来较大的帮助。

另一方面，编者之所以写作这本书，是因为国家信息安全技术普及的需要。开放性的互联网从来不相信眼泪，要更好地保护自己就必须学习攻防技术。如果因为攻防技术可能被不法分子利用来破坏就放弃研究，可能是一种掩耳盗铃的行为。攻防技术就是网上的武术，它博大精深、变换无穷。知己知彼，百战不殆。学好网络安全攻防技术，不仅可以提高国家网络安全整体水平，还可以更好地保护自己和他人的网络安全。如果奉献自己的经验和心得，既能符合古典黑客的分享精神，也能为提高国家信息安全水平做出一点贡献，则不亦快哉。

攻击技术并不神秘、防御技术并不可靠。打破技术壁垒，熟悉黑客技术，才能知己知彼，做到高效防御。

二、本书主要内容

本书以网络安全技术中时下最神秘的互联网服务器攻防技术为主要讲解方向，采用诸多实例以图文并茂、形象生动的方式详细讲解互联网服务器的攻击手法和对应的安全防御技术。

本书详细向读者讲解了服务器基础、服务器攻防基础技术、搭建服务器攻防平台、收集服

服务器攻防信息技术、实战扫描攻击技术、提权攻击技术、入侵检测技术、入侵取证技术、安全加固技术等。

充分考虑到读者基础不同，同时按本书技术领域知识体系需要，本书循序渐进，共分 12 章，每章主要内容如下。

第 1 章 讲解了服务器安全基础知识，如什么是服务器，服务器有哪些类型。

第 2 章 讲解了服务器攻防必备的操作系统知识。

第 3 章 讲解了服务器攻防必备的网络安全知识。

第 4 章 讲解了服务器攻防必备的网络管理知识。

第 5 章 讲解了服务器攻防必备的编程知识。

第 6 章 讲解了实验服务器攻防必备的服务器搭建技巧。

第 7 章 讲解了服务器网络信息收集与防范技巧。

第 8 章 讲解了服务器扫描攻击与防御技巧。

第 9 章 讲解了 Web 服务器攻击与防范技术。

第 10 章 讲解了服务器入侵检测技术。

第 11 章 讲解了网络入侵取证与审计技术。

第 12 章 讲解服务器加固技术。

三、技术支持

本书的目的在于最大限度地提高服务器管理员和安全人员的技术水平，消除他们跟黑客的技术差距，更好地提高国内互联网安全水平。由于编者水平有限，本书不尽完美、有待完善，恳请各位同行和技术爱好者多多指教。期待以后的版本中能将更多的心得和经验同读者朋友们分享，也希望读者朋友们能多多分享你们的经验。编者技术交流 QQ：178181825。

四、致谢

在本书的编写中，有关领导和同事、信息安全圈诸多好友以及红客圈诸多好友对本书的编写提供了宝贵的建议，李勇、汪宇、刘琪、樊荷花、陈华清、周海刚、孙鹏飞、苑景恩、刘青和卓文华讯公司对本书的编写和出版工作给予了多方面的帮助，在此一并表示感谢。

编 者

2011 年 1 月

目 录

第 1 章 服务器安全概述	1
1.1 服务器安全重要性	2
1.1.1 服务器是网络灵魂	2
1.1.2 服务器分类	3
1.1.3 加强服务器安全就等于加强了网络安全	4
1.2 黑客攻击服务器的过程揭秘	6
1.2.1 目标系统信息收集	7
1.2.2 漏洞利用与入侵尝试	10
1.2.3 目标系统权限获取和提升	10
1.2.4 长期控制及清理痕迹	11
1.3 黑客攻击服务器的方式揭秘	12
1.3.1 入侵系统类攻击	12
1.3.2 入侵网站类攻击	13
1.3.3 欺骗类攻击	13
1.3.4 流氓类攻击	16
第 2 章 服务器攻防必备的操作系统知识	17
2.1 服务器操作系统的分类	18
2.1.1 Windows 服务器操作系统	18
2.1.2 NetWare 服务器操作系统	19
2.1.3 UNIX 服务器操作系统	20
2.1.4 Linux 服务器操作系统	21
2.2 网络 DOS 命令与系统安全	24
2.3 文件系统与系统安全	36
2.3.1 主要文件系统格式	36
2.3.2 文件访问控制	37
2.3.3 文件类型与安全	39
2.4 注册表与系统安全	40
2.4.1 注册表由来	40
2.4.2 注册表简介	41
2.4.3 注册表入侵方法	43

2.4.4	注册表入侵防范.....	46
2.5	回收站与系统安全	48
2.5.1	利用回收站提权.....	49
2.5.2	回收站入侵防范.....	49
第3章	服务器攻防必备的网络安全知识.....	50
3.1	网络安全的定义与所受威胁.....	51
3.1.1	网络安全定义	51
3.1.2	网络安全威胁	51
3.2	网络安全漏洞	52
3.2.1	根据漏洞发现时间分类.....	53
3.2.2	根据漏洞成因分类	53
3.2.3	根据漏洞严重程度分类.....	54
3.2.4	按漏洞造成的威胁分类.....	55
3.3	安全漏洞的检测和修补.....	56
3.3.1	安全漏洞的检测.....	57
3.3.2	安全漏洞的修补.....	57
第4章	服务器攻防必备的网络管理知识.....	64
4.1	常见的网络基本概念解析	65
4.2	TCP/IP 协议相关知识.....	67
4.2.1	TCP/IP 协议的重要性.....	67
4.2.2	TCP/IP 协议的构成	68
4.2.3	TCP/IP 协议中主要协议介绍.....	72
4.3	局域网基础知识.....	78
4.3.1	正确理解局域网	78
4.3.2	局域网的构成	78
4.3.3	简单局域网拓扑结构.....	79
4.3.4	局域网常见设备	81
第5章	服务器攻防必备的编程知识	83
5.1	Web 编程基础知识.....	84
5.1.1	查后门基础——Web 后台编程语言攻防知识.....	84
5.1.2	挂马攻防基础——前台客户端语言.....	89
5.2	编码基础知识	95
5.2.1	URL 编码.....	95
5.2.2	Unicode 编码.....	98

5.2.3	base64 编码	99
5.2.4	十六进制编码	100
5.3	批处理编程基础	101
5.3.1	什么是批处理	101
5.3.2	如何写批命令	102
5.3.3	批处理攻防实例	103
5.4	VBS 编程基础	109
5.4.1	利用 VBS 查看 IIS 配置	110
5.4.2	利用 VBS 解包网站	112
5.4.3	利用 VBS 添加管理员	112
5.4.4	入侵常用到的 VBS	112
第 6 章	服务器攻防必备的服务器搭建知识	115
6.1	虚拟硬件基础知识	116
6.2	虚拟机工具的安装及配置	116
6.3	在虚拟机上架设 IIS 服务器	120
6.4	打造 ASP 以及 ASP.NET 测试网站环境	121
6.5	打造 PHP 测试网站环境	122
6.5.1	架设前的准备工作	123
6.5.2	架设具体步骤	123
第 7 章	服务器网络信息收集与防范	130
7.1	利用错误消息收集信息	131
7.1.1	错误消息脚本	131
7.1.2	栈追踪	133
7.1.3	详尽的调试消息	133
7.1.4	服务器错误信息	134
7.1.5	数据库错误信息	134
7.1.6	第三方软件错误消息	135
7.1.7	使用错误的配置	137
7.1.8	利用探针信息	137
7.2	利用技术手段收集敏感的信息	138
7.2.1	服务器信息搜集泄密与防范	138
7.2.2	网站注册信息泄密与防范	141
7.2.3	结构探测与防范	142
7.2.4	搜索引擎泄密与防范	144

7.3	防止信息泄露	145
7.3.1	使用常规错误消息	145
7.3.2	保护敏感信息	146
7.3.3	尽量减少客户端信息泄露	149
第 8 章	服务器扫描攻击与防御	150
8.1	端口扫描基础	151
8.1.1	计算机网络服务与端口的关系	151
8.1.2	常见服务器端口	154
8.1.3	端口扫描原理	155
8.1.4	目前主要端口扫描技术	156
8.2	端口扫描器应用实战	157
8.2.1	端口扫描工具的用途	157
8.2.2	S 扫描器的使用方法	158
8.2.3	Nmap 的应用	159
8.2.4	端口扫描攻击实战	163
8.3	端口扫描的防范	169
8.4	漏洞扫描基础	169
8.4.1	利用安全软件扫描漏洞	170
8.4.2	利用黑客软件扫描漏洞	183
8.5	扫描攻击的防御	185
8.5.1	防范常见扫描	185
8.5.2	防范特定漏洞攻击	187
8.5.3	防范软件漏洞攻击	188
第 9 章	Web 服务器攻击与防范	189
9.1	Web 的安全需求	190
9.1.1	Web 面临的威胁	190
9.1.2	Web 的安全体系结构	191
9.1.3	Web 的安全性分析	192
9.2	Web 服务器安全	194
9.2.1	Web 服务器的安全需求	194
9.2.2	Web 服务器的安全策略	195
9.3	Web 服务器应用软件安全	196
9.3.1	FTP 软件漏洞利用与修补	196
9.3.2	邮件软件漏洞利用与修补	199

9.3.3	远程管理软件漏洞与修补	200
9.3.4	输入法漏洞与修补	204
9.3.5	安全软件漏洞与修补	205
9.3.6	压缩软件漏洞利用与修补	207
9.4	Web 浏览器安全	208
9.4.1	Web 浏览器面临的威胁	208
9.4.2	Web 浏览器的安全策略	210
9.5	Web 服务器的加固	210
9.5.1	系统安全	211
9.5.2	IIS 安全	212
第 10 章	服务器入侵检测技术	216
10.1	如何评估入侵事件	217
10.1.1	识别服务器入侵事件及其真假	217
10.1.2	判断入侵事件的严重程度	218
10.2	入侵检测概述	218
10.2.1	入侵检测系统的体系结构	219
10.2.2	入侵检测系统的分类	219
10.3	使用小工具检测入侵	219
10.3.1	进程查看器	220
10.3.2	影子账户检测工具	221
10.3.3	注册表监视工具	225
10.3.4	端口查看器	227
10.3.5	木马检测工具	228
10.4	检测和清理脚本木马	231
10.4.1	有备份情况下检测和清理脚本木马	231
10.4.2	无备份情况下检测和清理脚本木马	233
10.5	检测和清除服务器后门	234
10.5.1	“隐藏”后门的检测与清除	234
10.5.2	Shift 后门的检测与清除	235
10.5.3	放大镜后门的检测与清除	236
10.5.4	嗅探后门的检测与清除	237
10.5.5	最容易被忽略的后门检测和清除	238
10.5.6	远程控制后门检测和清除	239
10.5.7	捆绑后门检测和清除	243

10.6	DDOS 攻击检测与防御	243
10.6.1	DDOS 的含义	244
10.6.2	攻击实例	244
10.6.3	DDOS 攻击防范	250
10.7	ARP 攻击与检测	250
10.7.1	ARP 攻击原理与实战	250
10.7.2	ARP 攻击防护	254
第 11 章	网络入侵取证与审计技术	256
11.1	黑客攻击的取证	257
11.1.1	取证特点	257
11.1.2	取证工具	258
11.1.3	取证注意的要点	260
11.2	黑客攻击的追踪	261
11.2.1	追踪黑客的流程	261
11.2.2	安全审计	262
11.3	日志安全分析	266
11.3.1	系统日志	267
11.3.2	网站日志	267
11.3.3	清除服务器日志	269
11.3.4	使用工具分析日志实战	270
11.3.5	保护 IIS 服务器日志安全	273
11.4	文件反恢复与恢复	274
11.4.1	文件安全删除	274
11.4.2	文件恢复实战	275
11.4.3	文件备份实战	277
第 12 章	服务器加固技术	280
12.1	国内外对服务器加固技术的研究	281
12.2	服务器加固技术的分类	281
12.3	服务器加固技术的流程	281
12.4	服务器加固技术的实施	282
12.4.1	加固的意义	282
12.4.2	加固的难点	283
12.4.3	加固工作的思路	283
12.4.4	加固工作的准备阶段	283

12.4.5	加固工作的实施阶段.....	284
12.4.6	加固工作的报告阶段.....	284
12.5	服务器加固技术的细节.....	284
12.5.1	使用模板节省加固时间.....	284
12.5.2	正确说明加固效果.....	293
12.5.3	依靠经验进行全面适度的加固.....	295

第1章 服务器安全概述

- 服务器安全重要性
- 黑客攻击服务器的过程揭秘
- 黑客攻击服务器的方式揭秘



互联网服务器 攻防秘笈

1.1 服务器安全重要性

服务器是为满足众多用户同时在其上处理数据而设计的,而多人如何同时使用同一台服务器呢?只有通过网络才能达到这一目的。

服务器可以提供网页服务、邮件服务、文件共享服务、打印共享服务、数据库服务等,它需要同时接收众多的请求并处理众多的数据,而这些正是网络的重要价值所在,所以服务器与网络是密不可分的。一方面,离开了网络,就没有服务器存在的价值;另一方面,服务器是为提供服务而生,这些服务是网络的特性,所以服务器是构成网络的灵魂。

从这个意义上来说,网络安全最重要的一部分就是服务器安全。从广义上来说,服务器是指网络中能对其他机器提供某些服务的计算机。由于提供服务对服务器的各项性能指标要求都很高,所以从狭义上来讲,服务器是指通过网络对外提供服务的某些高性能计算机。

1.1.1 服务器是网络灵魂

服务器存储并处理网络上 80% 以上的数据、信息,是网络重要的节点,因此也被称为网络的灵魂。如果没有视频服务器,我们无法在线看电影;如果没有网页服务器,我们无法看网络新闻;如果没有 QQ 服务器,我们无法使用 QQ;如果没有 MSN 服务器,我们无法登录 MSN。

类似的例子还可以举出很多,可见服务器的重要性。

从技术上来说,服务器是网络上为客户端计算机提供各种服务的高可用性计算机,它在网络操作系统的控制下,将与其相连的硬盘、打印机及各种通信设备提供给网络上的客户端计算机共享。

服务器的构成与客户端计算机的构成基本相似,有 CPU、硬盘、内存、主板等,但是由于它需要长时间运行并且不能中断运行,因此比客户端计算机有更强的处理能力,更强大的数据吞吐能力,更好的稳定性,并且在可靠性、安全性、可扩展性、可管理性等方面能保证服务器长时间的可靠运行。如图 1-1 所示,服务器跟普通 PC 外形上十分相似,但是在硬件配置上却更高一筹。

如果服务器出现故障或者被黑客攻击,我们可能遇到以下情况。

- 访问不了某网站。
- 在自动取款机上不能正常地存取款。

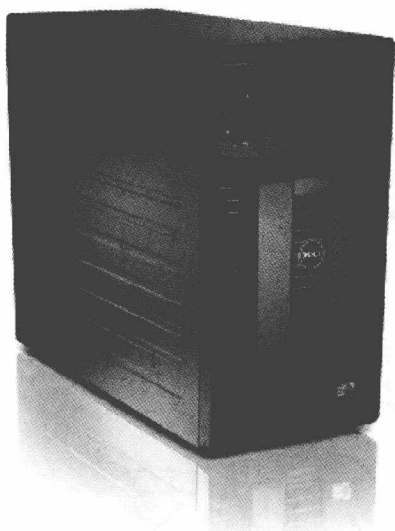


图 1-1 服务器外形

1.1.2 服务器分类

在不同的需求情况下,各行各业需要不同的服务器,甚至很多单位和个人需要组建各类用途的服务器。这些网络环境中的高性能计算机,响应网络上其他计算机提交的服务请求,并提供相应的服务。为此,服务器必须具有承担服务并且保障服务不中断的能力。

1. 机架式服务器

对于中小型企业而言,选择服务器时首先要考虑服务器的体积、功耗、发热量等参数。服务器通常放在大型专用机房,并统一部署和管理。机房通常设有严密的保安措施、良好的冷却系统、强大的供电系统,但是机房的造价相当昂贵。在有限的空间内部署更多的服务器可以节省成本,这时候可以选用机架式服务器。

机架式服务器也有多种规格,如1U、2U、4U、6U、8U等。 $1\text{U}=1.75\text{in}=4.45\text{cm}$,所以1U的机架式服务器具备节省空间等优点,适合一些业务相对固定的使用领域,如信息服务企业(如ISP/ICP/ISV/IDC)。4U以上的产品性能较高,可扩展性好,但体积较大,空间利用率不高。机架式服务器的外形看来不像计算机,而像交换机,如图1-2所示。

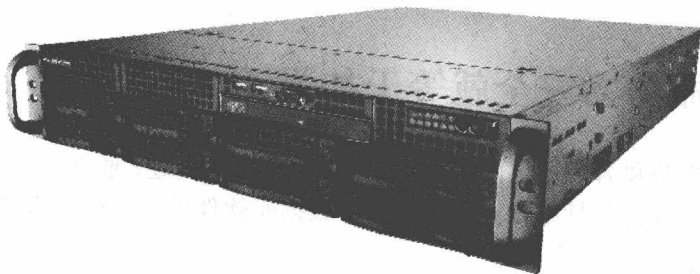


图 1-2 机架式服务器外形

2. 刀片服务器

刀片服务器是指在标准高度的机架式机箱内可插装多个卡式的服务器,它具备高可用和高密度的特点。每一块“刀片”实际上就是一块系统主板。它们可以通过“板载”硬盘启动自己的操作系统,类似于一个个独立的服务器,相互之间没有关联。在这种模式下,每一块母板运行自己的操作系统为不同用户群服务。当然,管理员可以使用软件将这些母板组成一个服务器集群。在集群模式下,所有的母板可以连接起来共享资源,为相同的用户群服务。在集群中插入新的“刀片”,就可以提高整体性能。另外,因为每块“刀片”都可以做到热插拔,所以可以轻松地替换,维护时间大大减少,如图1-3所示。

3. 机柜式服务器

机柜式服务器是通过机柜将服务器和网络交换设备等集中安装的服务器。它可以对服务器统一的进行布线,节省空间,方便管理。

对于银行、证券、电信、邮电等重要单位,其行业特性要求服务器更稳定、速度更快、性能更高,这时候就需要选择机柜式服务器,该服务器具有完备的故障自修复能力。

机柜式服务器外形像一个柜子,如图1-4所示。

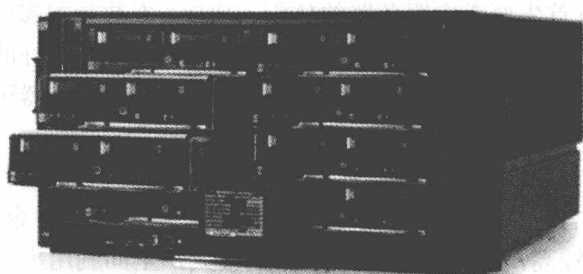


图 1-3 刀片服务器外形



图 1-4 机柜式服务器外形

1.1.3 加强服务器安全就等于加强了网络安全

为了让服务器能提供各种不同的服务,实现各种不同的用途,通常需要在服务器上安装各种软件。这些服务器软件包括邮件服务器软件、数据库软件等。常用的服务器如下。

1. 文件服务器

文件服务器是以文件数据共享为目标。它的特点是将供多台计算机共享的文件存放于一台计算机中,这台计算机就被称为文件服务器,如 Windows Server 2003 文件服务器。

2. 数据库服务器

安装了不同的数据库软件,提供不同的数据库服务的服务器被称为数据库服务器,如 Oracle 数据库服务器、MySQL 数据库服务器、Microsoft SQL Server 数据库服务器等。

3. 邮件服务器

邮件服务是用户所需要的最重要的网络服务之一。没有邮件服务的网络是不完整的网络。提供邮件功能的服务器称为邮件服务器。它们通常安装的软件包括 WebEasyMail、Sendmail、Postfix、Qmail、Microsoft Exchange 等。

4. Web 服务器

Web 服务器也就是网页服务器,如 Apache、IIS 等搭建的服务器,其目的是提供 Web 网页服务。

5. DNS 服务器

提供域名服务的服务器称之为 DNS 服务器。通过 DNS 服务器,可以实现域名服务的查

询、应答。

6. 代理服务器

代理服务器的功能就好比网络的中转站，主要功能如下。

- 突破自身 IP 访问限制，访问受限游戏服务器。可以通过代理 IP，将自己的 IP 变成国外 IP，从而可以访问游戏服务器。
- 访问一些组织内部资源，如使用教育网内 IP 地址段内的免费代理服务器，就可以登录教育网内部的各类 FTP 下载学习资料。
- 突破 IP 封锁：出于安全或其他原因考虑，很多网站对某些 IP 段限制访问，这种限制是人为的，所以不能访问时可以换一个代理服务器试试。
- 隐藏真实 IP：可以通过代理的方法隐藏自己的真实 IP，免受攻击。

下面讲解一下如何通过 HTTP 代理服务器来实现上网。

Step 01 找到 HTTP 代理服务器 IP、账户、密码和端口。网络上很多站点会公布免费的 HTTP 代理信息，如图 1-5 所示。

Step 02 打开 IE 浏览器，依次单击“工具”→“Internet 选项”命令，弹出“Internet 选项”对话框，选择“连接”选项卡，如图 1-6 所示。

ID	地址	端口	类型	地区	验证时间	响应	WHOIS
1	222.58.225.187	80	HTTP	湖南省衡阳市 铁通	07-25 11:42	0.989	whois
2	216.109.73.20	80	HTTP	美国/加拿大 ProxyCN	07-25 11:41	0.992	whois
3	58.215.65.251	3128	HTTP	江苏省无锡市 电信	07-25 11:41	0.992	whois
4	88.146.218.4	8090	HTTP	美国	07-25 11:30	0.992	whois
5	88.191.118.212	3128	HTTP	法国	07-25 11:26	1.000	whois
6	222.58.227.135	80	HTTP	湖南省衡阳市 铁通	07-25 11:32	1.001	whois
7	221.130.17.61	80	HTTP	江苏省南京市 移动	07-25 11:44	1.002	whois
8	202.186.33.164	80	HTTP	马来西亚 ProxyCN	07-25 11:42	1.002	whois

图 1-5 HTTP 代理网站公布的代理信息

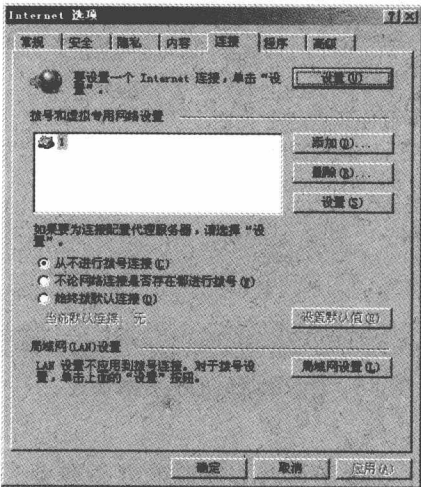


图 1-6 “Internet 选项”对话框

Step 03 选择目前使用的连接，然后单击右侧的“设置”按钮，弹出“局域网设置”对话框，如图 1-7 所示。

勾选“为 LAN 使用代理服务器（这些设置不会应用于拨号或 VPN 连接）。”复选框，同时在“地址”和“端口”栏中输入 HTTP 代理服务器的 IP 和端口，单击“确定”按钮。再访问互联网时，我们可以发现自己的 IP 变成了该代理 IP，如图 1-8 所示。

这个 IP 是德国的 IP。如果这时候上网看视频网站上的电视剧，会发现非常慢。这是为什么呢？设置了代理服务器之后，IE 浏览器不是直接到视频网站服务器去取回视频网页信息，而是向代理服务器发出请求，请求会先送到代理服务器，代理服务器再把请求发到视频