Broadview®
www.broadview.com.cn

安全技术大系

黑客攻防实战入门（第2版）

邓吉 罗诗尧 曹轶 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

安全技术大系

黑客攻防实战入门（第2版）

邓吉 罗诗尧 曹轶 编著

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

内 容 简 介

本书从“攻”、“防”两个不同的角度，通过现实中的入侵实例，并结合作者的心得体会，图文并茂地再现了网络入侵与防御的全过程。本书共分 8 章，系统地介绍了入侵的全部过程，以及相应的防御措施和方法。其中包括信息的搜集、基于认证的入侵及防御、基于漏洞的入侵及防御、基于木马的入侵及防御、基于远程控制的入侵及防御、入侵中的隐藏技术、入侵后的留后门与清脚印技术，以及关于 QQ 的攻击及防御技术。本书用图解的方式对每一个入侵步骤都进行了详细的分析，以推测入侵者的入侵目的；对入侵过程中常见的问题进行了必要的说明与解答；并对一些常见的入侵手段进行了比较与分析，以方便读者了解入侵者常用的方式、方法，保卫网络安全。

本书适合于网络技术爱好者、网络系统管理员阅读，也可作为相关专业学生的学习和参考资料。

图书在版编目（CIP）数据

黑客攻防实战入门 / 邓吉，罗诗尧，曹轶编著. —2 版. —北京：电子工业出版社，2007.1
（安全技术大系）
ISBN 978-7-121-03709-2

Ⅰ. 黑… Ⅱ. ①邓… ②罗… ③曹… 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 161033 号

责任编辑：毕 宁 bn@phei.com.cn
印 刷：北京天宇星印刷厂
装 订：涿州市桃园装订有限公司
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：787×1092 1/16 印张：25.5 字数：587 千字
印 次：2007 年 1 月第 1 次印刷
印 数：6000 册 定价：45.00 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。

序　言

《黑客攻防实战入门》一书自面世以来，深受广大读者的肯定与好评，笔者在此深表感谢。《黑客攻防实战入门（第2版）》与第1版的定位相同，是针对那些对网络安全技术感兴趣的初学者而编写的。在本次改版中，笔者针对读者的反映，重新对本书的结构进行了调整，并对本书的内容进行了升级。但是，由于本书的侧重点并不是某个工具的使用说明，因此不会盲目地追随某个流行工具，而是保留了黑客技术发展过程中最为经典的方法、工具和漏洞。希望读者能够理解。

此外，值得一提的是，笔者始终以“授之以鱼，不如授之以渔”为基本出发点来展开本书的编写。也就是说，本书的目的是向读者介绍黑客技术中所涉及的思考方法，而不是单纯地介绍某个工具的使用方法。可以说，本书是一本介绍为什么，而不是单单介绍怎么做的一本黑客入门教程。这一点是本书区别于市面上其他黑客类书籍的根本特征。

关于黑客

白日喧嚣、繁华的都市像个玩累了的孩子般慢慢地安静了下来。夜，寂静得令人窒息，仿佛可以听到一串串数据划过网线的声音。都市的角落里，显示屏微弱的光亮笼罩着一个不大的房间，黑暗中，不时地闪耀出深蓝色的光芒。一个人，一台笔记本，一杯热了又凉、凉了又热的咖啡，还有那台不知处于何处的服务器，依旧继续着……

一提起“黑客”，我们便会不由自主地浮现出以上遐想。

长期以来，由于诸多方面的因素，“黑客”这个字眼变得十分敏感，不同的人群对黑客也存在不同的理解，甚至没有人愿意承认自己是黑客。有些人认为，黑客是一群狂热的技术爱好者，他们无限度地追求技术的完美；有些人认为，黑客只是一群拥有技术，但思想简单的毛头小伙子；还有些人认为黑客是不应该存在的，他们是网络的破坏者。这里，我们没有必要对这个问题争论不休，也无须给“黑客”加上一个标准的定义，但从客观存在的事实来看，黑客这类群体往往存在着以下几个共同点。

① 强烈的技术渴望与完美主义。驱动他们成长的是对技术的无限渴望，获得技术的提高才是他们最终的任务。

② 强烈的责任感。只有强烈的责任感才能使他们不会走向歧途。责任感告诉他们不要在任何媒体上公布成功入侵的服务器；不要对其入侵的服务器进行任何的破坏；在发现系统漏洞后要马上通知官方对该漏洞采取必要的修补措施，在官方补丁没有公布之前，绝对不要大范围地公开漏洞利用代码。一方面，黑客入侵可能造成网络的暂时瘫痪，另一方面，黑客也是整个网络的建设者，他们不知疲倦地寻找网络大厦的缺陷，使得网络大厦的根基更加稳固。

为什么写作本书

然而，不容乐观的事实是，一部分人歪曲了黑客的本质，被不良动机所驱使，从而进行入侵活动，威胁网络的健康发展。对于我国来说，形势尤为严峻，我国信息化建设迟于美国等发达国家，信息安全技术水平也相对落后。在几次黑客大战中，国内网站的弱口令、漏洞比比皆是，这种现状实在令人担忧，值得深思和反省，从中也可以看出传统的计算机、网络教学层次是远远不够的。可能出于安全等其他角度的考虑，传统教学往往只注重表面上的应用，而避开一些敏感的技术。设想一下，如果一个网站的管理员只学会架构网站，却不关心如何入侵自己的网站，那么他如何对自己网站的缺陷了如指掌？如何能够及时地获知最新漏洞的描述而提前做好抵御？如果以上都做不到，那就更不要谈日常的系统更新、维护和打补丁了。然而，国内精通入侵的网管又有多少呢？长期以来，国内网管的潜意识里都认为“入侵”是个不光彩的勾当，甚至嗤之以鼻。随着信息化程度越来越高，信息技术与生活的联系越来越紧密，可以上网的电子设备逐年增加，电脑、PDA、手机，甚至家电。可以想像 10 年后，如果不了解入侵者的手段来采取必要的防御措施，将要被入侵的设备不会仅仅限于电脑，也许还包括你的手机、家电、汽车，等等。因此，在信息技术如此发达，沟通方式日益丰富和复杂的今天，我们不仅要学会如何正确使用网络，而且还需要学会如何防御自己的网络被他人入侵。

出于以上原因，本书作者通过多年的研究与实践，系统地总结了网络上广为使用的入侵、防御技术，并针对广大网管以及对网络感兴趣的在校学生编写了本书。希望大家能够从多个角度了解网络安全技术，从而更有效地保护网络安全。

本书主要内容

本书以深入剖析入侵过程为主线来展开全书内容，向读者介绍入侵者如何实现信息的搜集，如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马的入侵），如何实现入侵即远程连接，入侵后如何执行各种任务，如何留下后门以便再次进入系统，以及入侵者如何清除系统日志防止目标服务器发现入侵痕迹。此外，书中还详细地介绍了入侵者是如何实现从信息扫描到入侵过程中的隐身保护，如何逃避被他人发现。全书会对每一个入侵步骤作详细的分析，以推断入侵者在每一入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答，此外，还会对几种常见的入侵手段进行比较与分析。

关于本书作者

邓吉，原国内著名黑客组织成员，《黑客攻防实战入门》与《黑客攻防实战详解》的策划发起人，负责全书的统稿工作。2000 年～2004 年就读于大连理工大学电子系，2004 年放弃免试研究生资格，加盟世界 500 强之一的公司工作。2006 年 10 月创办大连启明科技有限公司，目前从事网络安全解决方案与嵌入式产品方面的开发工作。

曹轶，毕业于大连理工大学自动化系，现从事于金融行业机器的软件开发工作。从 DOS 时代开始接触计算机，熟悉 Windows 操作系统的底层应用。此外，对 SQL Server，MySQL，ASP，PHP，JSP 等都有很深入的理解。并对漏洞溢出程序的编写有着独到的研究和见解。在本书的修订工作中，主要负责书中所用软件版本升级更新工作。

罗诗尧（网名：流速），原 2.14 黑客组织站长，在网络安全方面已经取得了不凡的成绩。现任上海导航安全顾问（021dh.com），国安网络公司 CEO。安全经验相当丰富，对大、中型网络的安全环境拥有较多比较成熟的解决方案。在本书的修订工作中，主要负责第 3 章和第 4 章内容的修改。

此外，大连理工大学的柳靖也参与了本书的修订编写工作。

需要声明的是，**本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任；本书的目的在于最大限度地唤起大家的网络安全意识，正视我们的网络世界所面临的一场危机，并采取行动。**

邓　吉

目　录

CHAPTER

1

第 1 章　信息搜集

《孙子兵法》有云：“知己知彼、百战不殆”。入侵者在入侵之前都会想方设法搜集尽可能多的信息，甚至是网络管理员的私人邮箱和住宅电话。入侵者始终坚信这样一个信条：“无论目标网络的规模有多大、安全指数有多高，只要是人类参与设计的网络就必然存在着人为因素，而任何人为因素都有可能导致网络设计的缺陷。”入侵者很清楚，自己的任务就是去发掘这些被常人忽略的缺陷。事实也证明，如果让入侵者获得的信息越多，他们发现的缺陷也就越多，侵入网络的可能性也就越大。成熟的入侵者犹如经验丰富的猎豹，他们花费在信息搜集上的时间往往是最多的。信息搜集、筛选、分析，再收集、再筛选、再分析是入侵者最重要、最枯燥的工作。入侵者的哲学是：“没有无用信息”。

不妨举个简单的例子来说明信息搜集对入侵者的重要性。前些天，偶然在论坛上看见一个网管询问“如何去掉某某服务器的默认密码”的帖子，从中可以知道该管理员所管辖网络的脆弱之处，甚至可以根据该网管的技术水平来推断该网络的总体安全指数。如果这个帖子被那些“感兴趣”的人发现，该服务器的命运就可想而知了。可见，仅仅是一个小小的帖子就极有可能导致该服务器，乃至整个网络的崩溃。

然而在如此浩渺的网络海洋中，如何在不可计量的信息中找到这张帖子也是一门技术。那么，入侵者在正式入侵之前都要搜集哪些信息，又是如何搜集的呢？

本章主要介绍如下内容：

- 网站信息搜集
- 地理位置信息搜集
- 共享资源搜集
- 端口扫描
- 综合扫描

1.1　网站信息搜集

网站是一个网络或集团的身份象征，它直接暴露在因特网上，为来访者提供服务，或

被集团、公司用来开展业务，因而网站的安全问题就显得尤为重要。不知从何时开始，“入侵网站”、“涂鸦网站”成了入侵者用来证明自己实力的“竞赛”。

1.1.1 相关知识

1. IP 地址

IP 地址是计算机在因特网上存在的标识，因特网上的每一台计算机必须有标识自己的 IP 地址，一台计算机可以有多个不同的 IP 地址，但是同一个 IP 地址不能分配给一台以上的计算机。无论这些地址是由 DHCP 服务自动分配的，还是由用户手动指定的固定 IP 地址，这些规则都是由 IP 协议规定的。此外，现在被广泛使用的 IP 地址规则属于 IPv4（IP 协议第 4 版）中规定的标准。IPv6 标准正在测试阶段，还没有大面积推广。

2. 关于网站的一些知识

这里提及的“网站”指的是 Web 服务器，也可以称之为 HTTP 服务器。它以超文本传输协议的方式提供服务，以超文本标记语言（HTML）作为基础来形成网页。超文本传输协议是一种按照人类习惯的思维方式来组织信息的一种格式，它使用“超链接”把不同的媒体，如图片、音乐、电影等组织在一起。网站提供的服务主要有网页浏览、软件下载、在线视频、搜索引擎，以及电子商务平台，如图 1-1 所示。

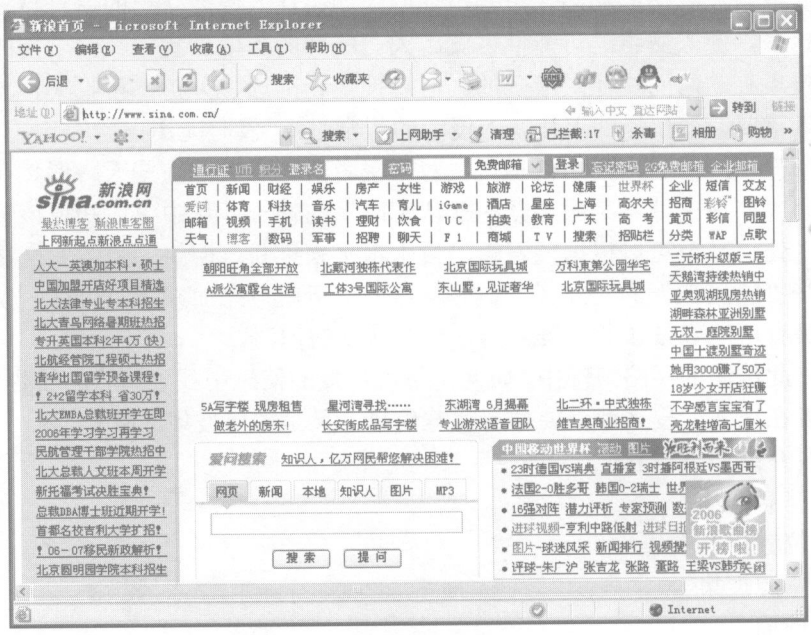

图 1-1

提示：网站的开发流程如下。

首先，由网站架构设计师根据需求设计网站的架构（前台界面，后台数据库）。接着，由网页设计师通过使用相关软件设计并编写网页，如使用 Dreamweaver，FrontPage 等网页设计软件；同时由数据库程序员设计并编写后台数

据库代码。然后，由网站架构师使用专门的 Web 服务器软件建立网站，如 IIS，Apache Server 等。一切准备工作就绪后，就可以由网站负责人向有关机构申请域名来发布网站了。

3. IP 地址的分配

前面已经说过，网络中的每一台计算机，必须有自己的 IP 地址，那么怎样才能使自己的 IP 地址不和其他计算机“冲突”呢？这需要 IP 地址管理机构统一管理，然后把 IP 地址一层一层地分配。例如，假设全球 IP 地址管理机构给中国分配一个 IP 段 1.0.0.0，然后中国的 IP 地址管理机构可以把这个 IP 段再具体划分给下级 IP 地址管理机构，如 1.1.0.0。IP 地址就是这样被一层一层地划分，直到把 IP 分配给每个终端计算机。

需要补充说明的是，下列 IP 不需要向有关 IP 管理机构申请，只能供局域网内部使用，而且同一内网中不能将同一 IP 分配给不同的主机。

- 10.x.x.x
- 172.16.x.x~172.31.x.x
- 192.168.x.x

4. 常用 DOS 命令

（1）查询本机 IP 地址命令

步骤一：打开 MS-DOS。

对于 Windows 9x 系统，选择【开始】→【运行】，键入“command”命令，如图 1-2 所示。

对于 Windows 2000/XP/2003 系统，选择【开始】→【运行】，键入“cmd”命令，如图 1-3 所示。

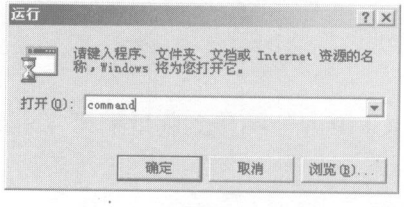

图 1-2

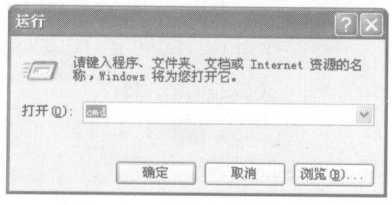

图 1-3

步骤二：查询本机 IP。

对于 Windows 9x 系统，键入“winipcfg”命令后打开的窗口如图 1-4 所示。

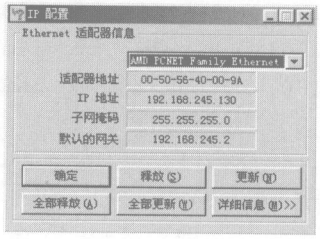

图 1-4

对于 Windows 2000/XP/2003 系统，使用 ipconfig 命令，如图 1-5 所示。

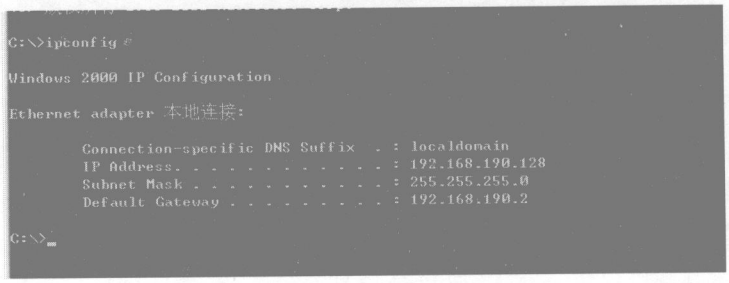

图 1-5

（2）ping 命令简介

ping 命令是入侵者经常使用的网络命令，该命令应用的是简单网络管理协议 ICMP 的一个管理方法，其目的就是通过发送特定形式的 ICMP 包来请求主机的回应，进而获得主机的一些属性。它的使用有些“投石问路”的味道。道理虽然简单，但是这个命令用途却非常广泛，通过这个命令，入侵者可以来试探目标主机是否活动，可以来查询目标主机的机器名，还可以配合 ARP 命令查询目标主机 MAC 地址，甚至可以用来推断目标主机操作系统类型，或者进行 DDoS（分布式拒绝服务）攻击等。

ping 命令的使用格式：

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] destination-list

常用参数说明：

-t　　一直 ping 下去，用 Ctrl+C 结束。

-a　　ping 的同时把 IP 地址转换成主机名。

-n count　　设定 ping 的次数。

-i TTL　　设置 ICMP 包的生存时间（指 ICMP 包能够传到临近的第几个节点）。

下面举两个例子进行说明。

试探目标主机是否活动。

命令使用格式：ping 目标主机 IP

```
C:\>ping 192.168.245.130
Pinging 192.168.245.130 with 32 bytes of data:
Reply from 192.168.245.130: bytes=32 time=10ms TTL=1
Reply from 192.168.245.130: bytes=32 time<10ms TTL=1
Reply from 192.168.245.130: bytes=32 time<10ms TTL=1
Reply from 192.168.245.130: bytes=32 time<10ms TTL=1
Ping statistics for 192.168.245.130:
      Packets: Sent = 4, Received = 4, Lost = 0 <0% lo ss>,
Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum =  10ms, Average =  2ms
```

从返回的结果“Reply from 192.168.245.130: bytes=32 time=10ms TTL=1”来看，目标主机有响应，说明 192.168.245.130 这台主机是活动的。下面的结果是相反的情况：

```
C:\>ping 192.168.245.130
Pinging 192.168.245.130 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.245.130:
      Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

从返回的结果“Request timed out.”来看，目标主机不是活动的，即目标主机不在线或安装有网络防火墙，这样的主机是不容易入侵的。

➘ 使用 ping 命令探测操作系统。

不同的操作系统对于 ping 的 TTL 返回值是不同的，参见表 1-1。

表 1-1　不同的操作系统对 ping 的 TTL 返回值

操 作 系 统	默认 TTL 返回值
UNIX 类	255
Windows 95	32
Windows NT/2000/XP/2003	128
Compaq Tru64 5.0	64

因此，入侵者便可以根据不同的 TTL 返回值来推测目标究竟属于何种操作系统。对于入侵者的这种信息收集手段，网管可以通过修改注册表来改变默认的 TTL 返回值。

1.1.2　基本信息搜集

1．由域名得到网站 IP 地址

为了记忆方便，出现了用域名来代替网站的 IP 地址的方法，那么，在已知域名的情况下入侵者是如何得到目标的 IP 地址的呢？可以通过下面几种方法来实现。

（1）方法一：ping 命令试探

使用命令：ping 域名。

例如，入侵者想知道 163 服务器的 IP 地址，可以在 MS-DOS 中键入“ping www.163.com”命令，如图 1-6 所示。

从图 1-6 可以看出，www.163.com 对应的 IP 地址为 202.108.36.153。

（2）方法二：nslookup 命令

仍然以 163 服务器为例，在 MS-DOS 中键入“nslookup”命令，如图 1-7 所示。

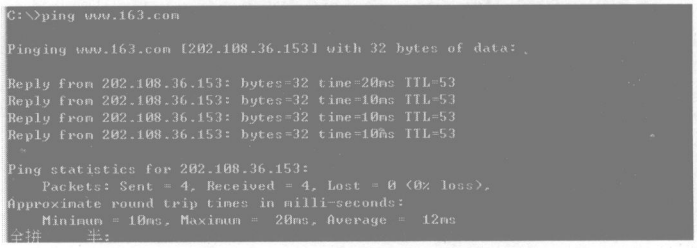

图 1-6

图 1-7

图 1-7 中的 202.□.□.6 是本机所在域的 DNS 服务器，在提示符“>”后键入“www.163.com”命令，回车后便可以得到域名查询结果，如图 1-8 所示。

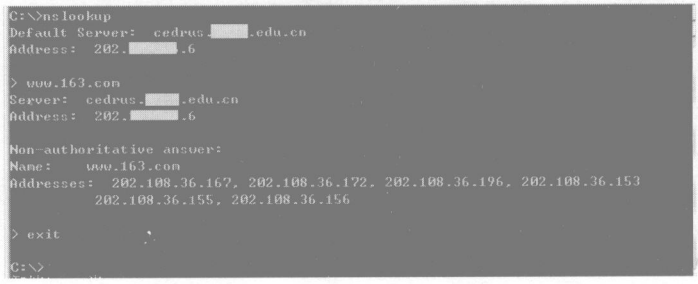

图 1-8

从图 1-8 返回的结果分析，Address 后面所列的就是 www.163.com 所使用的 Web 服务器群的 IP。

上面介绍的是入侵者经常使用的两种最基本方法。此外，还有一些软件附带域名、IP 相互转换的功能，实现起来更加简单，功能更加强大。从这两种方法中可以看出，ping 命令方便、快捷，nslookup 命令查询到的结果更为详细。

2. 由 IP 得到目标主机的地理位置

由于 IP 地址的分配是全球统一管理的，因此入侵者可以通过查询有关机构的 IP 地址数据库来得到该 IP 所对应的地理位置，由于 IP 管理机构多处于国外，而且分布比较零散，因此这里介绍两个能查询到 IP 数据库的国内个人网站。

网站一：http://www.intron.ac/service/index.html。如图 1-9 所示。

例如，要查询 202.108.36.153（163 的 IP）的物理地址，可在图 1-9 的“IP 地址”右面的文本框中输入“202.108.36.153”，然后单击“查询”按钮，就会得到如下查询结果。

```
您要查询的是"202.108.36.153"，它被理解为"202.108.36.153"
准确性排序：域名反向解析 > 本站补充数据 > 官方数据 > 非官方数据
```

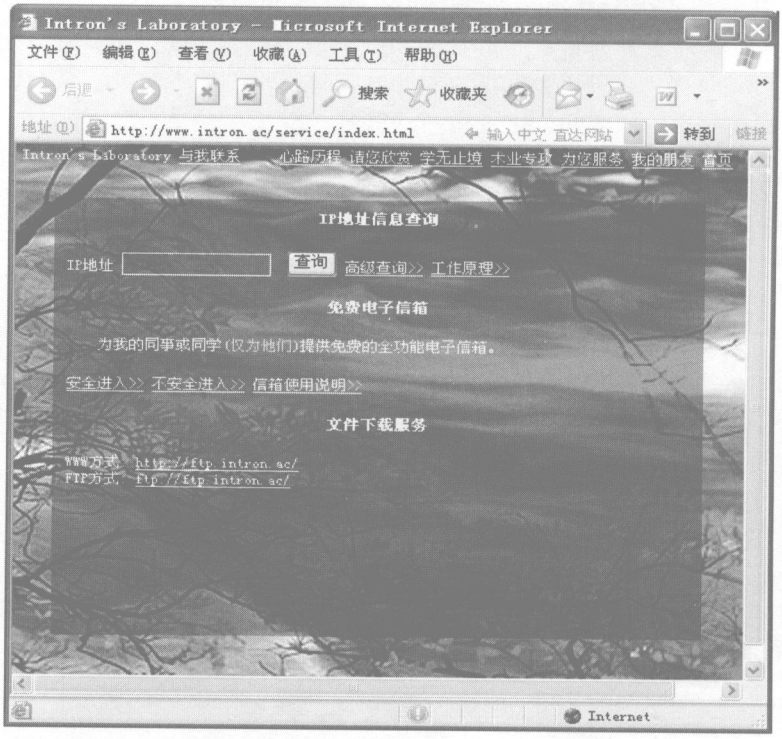

图 1-9

域名反向解析：
本站补充数据：
官方数据：
在亚洲与太平洋网络信息中心(APNIC)找到：

```
% [whois.apnic.net node-2]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html
网络地址范围:          202.108.0.0 - 202.108.255.255
网络名:                CNCGROUP-BJ
单位全名和地址:        CNCGROUP Beijing province network
单位全名和地址:        China Network Communications Group Corporation
单位全名和地址:        No.156,Fu-Xing-Men-Nei Street,
单位全名和地址:        Beijing 100031
国家或地区:            中国
管理员代码:            CH455-AP
技术员代码:            SY21-AP
维护者:                APNIC-HM
基层维护者:            MAINT-CNCGROUP-BJ
mnt-routes:            MAINT-CNCGROUP-RR
变更记录:              hm-changed@apnic.net 20031017
状况:                  ALLOCATED PORTABLE
```

```
变更记录：          hm-changed@apnic.net 20060124
信息来源：          APNIC
办事机构：          CNCGroup Hostmaster
电子信箱：          abuse@cnc-noc.net
地址：              No.156,Fu-Xing-Men-Nei Street,
地址：              Beijing,100031,P.R.China
代码：              CH455-AP
电话：              +86-10-82993155
传真：              +86-10-82993102
国家或地区：        中国
管理员代码：        CH444-AP
技术员代码：        CH444-AP
变更记录：          abuse@cnc-noc.net 20041119
维护者：            MAINT-CNCGROUP
信息来源：          APNIC
……
```

网站二：http://ip.loveroot.com。如图 1-10 所示，在“IP 地址”中填入欲查的 IP，单击“查询”按钮后，便会得到查询结果。但是该网站只能给出大致的地理位置。

图 1-10

网站三：http://map.sogou.com/如图 1-11 所示，如果已经获得了地理位置信息，那么可以通过该网站来获取实际的地理位置。该网站提供了全国各大城市的详细地图搜索，同时还可查到公交路线等信息。图 1-12 为北京海淀区的查询结果，在实际操作中，可以对查询结果进行多级放大和缩小，以得到更精确的指示。