揭开黑客神秘的面纱，黑客就这几招！

讲述黑客惯用的伎俩，见招拆招！

重点提示　任务过程　范例图示

专家讲解　打破常规　层层递进

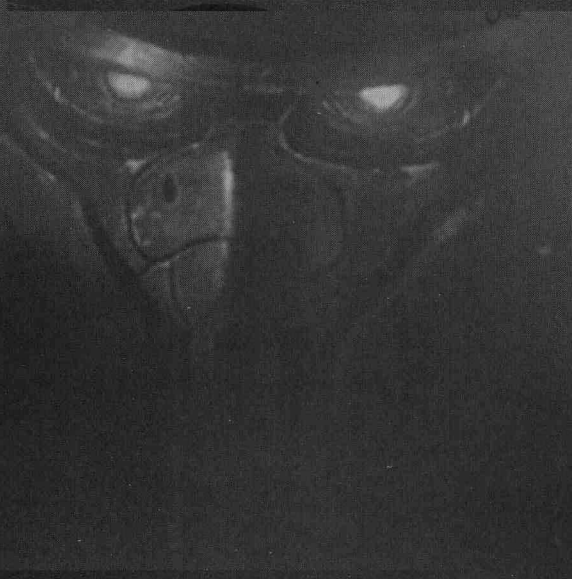
一书在手　边用边学　即查即用

矛与盾 黑客就这几招

108招多媒体视频讲解
让你快速从入门到精通

武新华 孙世宁 杨平 等编著

机械工业出版社
China Machine Press



矛与盾
黑客就这几招

武新华 孙世宁 杨平 等编著

机械工业出版社
China Machine Press

本书系统记述了黑客入侵与防御的关键技术与常用工具，全书共分为12章，主要包括：揭秘黑客攻击前的准备、扫描与反扫描技术、控制与反控制技术、欺骗与反欺骗、加密与解密工具、病毒与木马攻击防御、网络代理与追踪技术、注入工具与溢出攻击、账号盗取与安全防范、日志与后门清除技术、安全分析与入侵检测、流氓软件与间谍程序清除等内容。

本书力争把最流行，最实用的网络安全技术与工具介绍给迫切需要的读者；力争对每一种入侵手段进行最详细的剖析，对其防御方法进行最具体而有效的讲明，知其“矛与盾”，百战而不殆！

本书内容丰富全面，图文并茂，深入浅出，是广大网络爱好者和网络安全从业人员及网络管理者的必备工具书。

图书在版编目（CIP）数据

矛与盾——黑客就这几招 / 武新华等编著. —北京：机械工业出版社，2009.10

ISBN 978-7-111-28384-3

Ⅰ. 矛… Ⅱ. 武… 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（2009）第172871号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）

责任编辑：李东震

北京京师印务有限公司印刷

2010年1月第1版第1次印刷

184mm×260mm · 24.25印张

标准书号：ISBN 978-7-111-28384-3

ISBN 978-7-89451-228-4（光盘）

定价：49.80元（附光盘）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991；88361066

购书热线：（010）68326294；88379649；68995259

投稿热线：（010）88379604

读者信箱：hzjsj@hzbook.com

前 言

本书写作的目的主要是通过介绍黑客的攻击手段和提供相应的主动防御保护措施，使读者能够循序渐进地了解黑客入侵主动防御的关键技术与方法，提高安全防护意识，并将这些技术与方法应用于实际工作中。希望本书能成为网络信息安全专业技术人员、网络安全管理人员、网络使用者及信息时代的创业者的一本实用的网络安全工具书。

下面简要介绍本书的特点、学习方法以及提供的服务。

本书内容

本书以配图、图释、标注、指引线框等丰富的图解手段，再辅以浅显易懂的语言，通过对黑客攻击前的准备、扫描与反扫描技术、控制与反控制技术、欺骗与反欺骗、加密与解密工具、病毒与木马攻击防御、网络代理与追踪技术、注入工具与溢出攻击、账号盗取与安全防范、日志与后门清除技术、安全分析与入侵检测、流氓软件与间谍程序清除 12 大类，100 多个知识点的详细介绍，给出了相关代表性产品和工具的介绍及使用方法，使得读者可对网络安全主动防护及黑客入侵主动防御等具有代表性的技术有一个全面认识。

此外，本书还从黑客入侵防护应用角度给出了相对独立的内容的论述，使读者可对如何构建一个实用的黑客入侵防范体系有一个基本概念和思路，并可为读者提供几种典型行业的安全防护系统建设方案，以供参考和借鉴。

增值服务

随书所附光盘提供了多种攻防实战的教学视频，汇集了众多高手的操作精华，通过增进读者对主流操作手法感性认识的方式，使读者实现高效学习。

此外，如发现本书中有不妥或需要改进之处，还可通过访问 http://www.newtop01.com 或 QQ: 274648972 与编者进行沟通，编者将衷心感谢提供建议的读者，并真心希望在和广大读者互动的过程中能得到提高。

组织方式

本书包含了 3 种学习方式，即简明教程、图解教程和范例教程。

- 简明教程：用最简单明了的语言来讲解，只介绍最重要的知识点及最常见的应用，与此无关的内容均不涉及。
- 图解教程：“理论+实战 图文+视频=让读者快速入门”，编者采用最为通俗易懂的图文解说，即使是电脑新手也能通读全书。
- 范例教程：用任务驱动、情景教学的方式来介绍，在学习案例过程中掌握知识点。最新黑客技术盘点，让读者实现“先下手为强”。学习目的性、指向性最强。

本书特色

本书以情景教学、案例驱动与任务进阶为鲜明特色，在书中可以看到一个个生动的情景案例。通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 从基础到实践，完全站在实用的角度，介绍黑客攻防技术，突出了实用性和案例分析，所举实例，来自于实际应用，学以致用，真正解决问题。
- 通俗易学，结合图解、标注和多媒体教学，使神秘、高深、难以掌握的黑客攻防技术学习起来省时、省力，易于上手，非常适合新手、大专院校学生，以及网络从业人员掌握快速掌握实用技术。
- 紧扣“理论+实战　图文+视频=全面提升学习效率!”的主导思想，详细分析每一个操作案例，以实现读者用更少时间尽快掌握加密解密技术的操作，并对实战过程中常见问题作必要的说明与解答。
- 当前最新技术、热点技术和常用相关工具软件都在本书有所涉及，有关黑客攻防技术、方法与思路，也做了重点讲解，并通过实例介绍综合技术的运用手段，最后能够达到举一反三。

读者对象

本书作为一本面向广大网络爱好者的速查手册，适合于如下读者学习使用：

- 电脑爱好者。
- 具备一定黑客知识基础和工具使用基础的读者。
- 网络管理人员。
- 喜欢研究黑客技术的网友。
- 大、中专院校相关学生。

本书作者

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验，可带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。参与本书编写工作的有：安向东负责第 1 章，田靖负责第 2 章，孙世宁、李防负责第 3、4、5 章，孙璐红负责第 6 章，王肖苗负责第 7 章，赵慧婷负责第 8 章，杨平负责第 9 章，段玲华负责第 10 章，李伟负责第 11 章，王英英负责第 12 章，最后由武新华通审全稿。我们虽满腔热情，但限于自己的水平，书中仍难免有疏漏之处。因此，还望大家本着共同探讨、共同进步的平和心态来阅读本书。作者心存谨敬，随时恭候您提出的宝贵意见。

最后，需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记!切记!

编　者

2009 年 8 月

目 录

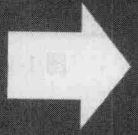
第 1 章　黑客攻击前的准备

重点提示

- 探测操作系统
- 探测网站信息
- 探测搜索引擎
- 网络监听与嗅探
- 创建安全测试环境
- Virtual PC 安全测试环境
- 虚拟机网站平台

本章精粹：

本章主要介绍了黑客攻击前应做的准备工作，主要包括：探测操作系统、探测网站信息、探测搜索引擎、网络监听与嗅探等多个方面，有助于读者了解黑客如何运用相关工具进行探测、分析出被攻击主机的详细信息，以便预防黑客入侵。



黑客在进行攻击前往往会花很多时间和精力去做准备工作，比如搜集对方使用什么类型的操作系统、管理账号是否为空口令或者弱口令、系统是否存在某些严重的漏洞……做足了这些准备工作，攻击就会又多了几分胜算，越熟练的黑客花费在准备工作上的时间往往越多。信息搜索、筛选、分析……这是最枯燥却也是最重要的准备工作。

第 1 招　探测操作系统

由于系统本身往往会存在某些弱点与不足之处，黑客之所以能够入侵，就是利用了这些弱点与错误。现在网上流行的各种各样的入侵工具，都是黑客在分析了系统的弱点及存在的问题之后编写出来的。作为一般的黑客，并不需要去编写工具，只要善于使用现成的入侵工具，就可以实现入侵。

1. 使用 X-Scan 工具探测系统

X-Scan 扫描器不同于一些常见攻击工具，它能用来发现问题，而不能直接攻击目标机器，执行如下操作可完成对远程计算机的操作系统探测。

使用 X-Scan 探测远程计算机的方法极其简单，具体的操作步骤如下。

步骤 1：先从网上下载并解压“X-Scan”压缩包。双击“X-Scan_gui.exe”应用程序图标，即可进入“X-Scan_gui”扫描器的主窗口，在其中可以浏览此软件的功能简介、常见问题解答等信息，如图 1-1 所示。

步骤 2：选择【设置】→【扫描参数】菜单项，即可打开【扫描参数】对话框，在其中选择“检测范围”选项设置扫描 IP 地址的范围，如图 1-2 所示。在“指定 IP 范围”文本框中输入需要扫描的目标 IP 地址（如 192.168.0.10）、IP 地址段（如 192.168.0.10 ~ 192.168.0.255），还能增加子网掩码（如 192.168.0.10/24）等。若不知道输入的格式，则可以单击该文本框右侧的【示例】按钮，在【示例】对话框中查看输入的有效格式，如图 1-3 所示。

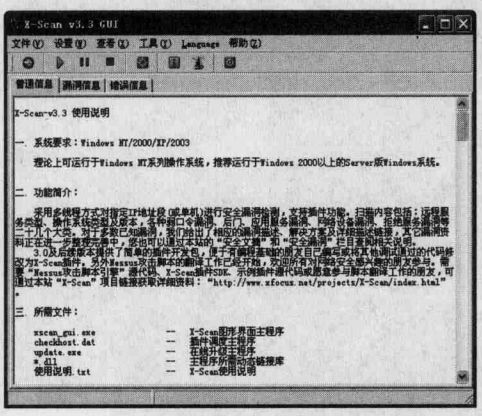


图 1-1　“X-Scan_gui”扫描器主窗口

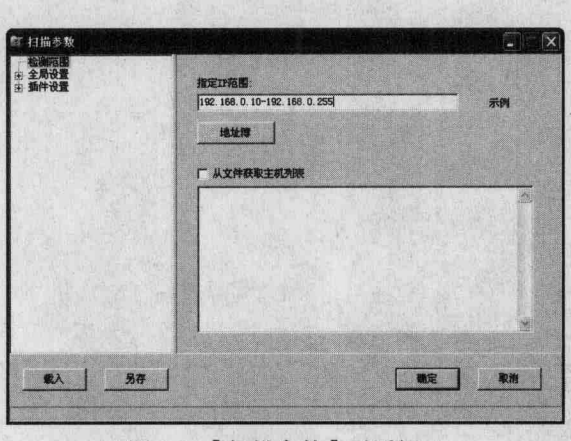


图 1-2　【扫描参数】对话框

步骤 3：展开“全局设置”选项之后，选取其中的“扫描模块”选项，则可选择扫描过程中需要扫描的模块（这里需要勾选“远程操作系统”选项），在选择扫描模块时，还可在其右侧窗格中查看远程计算机的操作系统，识别是否通过“SNMP（Simple Network Management Protocol，简单网络管理协议）、NETBIOS（Network Basic Input/Output System，网络基本输入/输出系统）协议主动识别远程操作系统类型及版本”插件来完成，如图 1-4 所示。

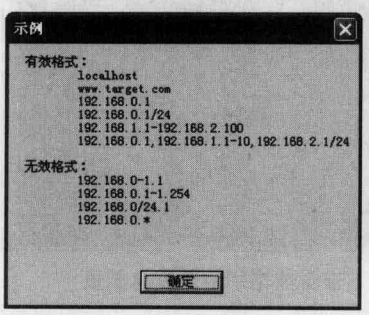


图 1-3 【示例】对话框

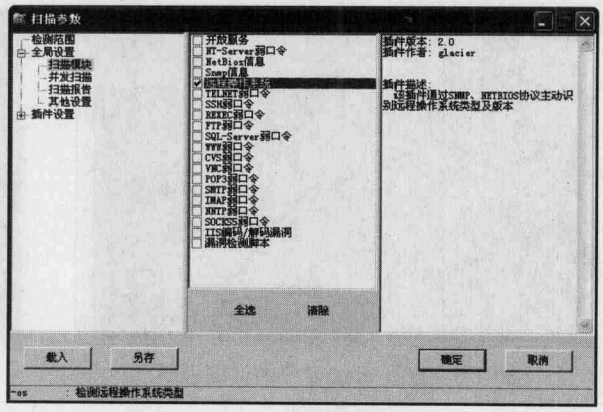


图 1-4 “扫描模块”选项

步骤 4：单击【确定】按钮返回到“X-Scan_gui”主窗口，单击 ▶ 按钮，耐心等待片刻就可以看到如图 1-5 所示的扫描结果了。在左侧的扫描目标右侧，即可看到“Windows XP”的标识，这就说明远程计算机使用的是 Windows XP 操作系统。

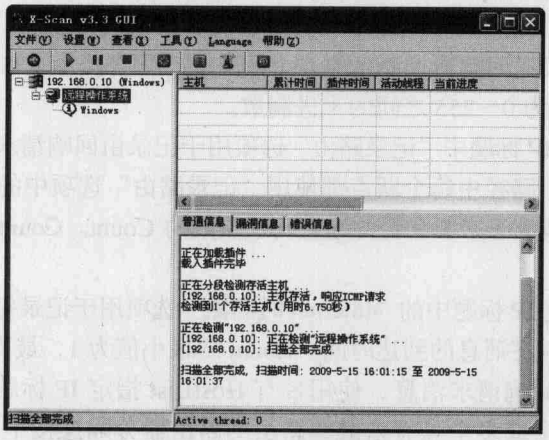


图 1-5 显示扫描结果

2. 使用 ping 命令探测系统

ping 命令是测试网络连接、信息发送和接收状况的实用型工具，是一个系统内置的探测工具。对于一个生活在网络上的管理员或黑客，ping 命令是第一个必须掌握的 DOS 命令，它所利用的原理是“网络上的机器都有唯一确定的 IP 地址，用户给目标 IP 地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包用户可以确定目标主机的存在，可以初步判断目标主机的操作系统等”。通过在命令提示符下输入“ping /?”命令，即可查看 ping 命令的详细说明，如图 1-6 所示。

- -a：指定对目的地 IP 地址进行反向名称解析。如解析成功，ping 将显示相应的主机名。
- -t：不断使用 ping 命令发送回响请求信息到目的地。要中断并退出 ping，只需要按下“Ctrl+C”组合键。初级黑客常常喜欢使用这个参数对目标计算机进行攻击。
- -n Count：指定发送回响请求消息的次数，默认值为 4。
- -I Size：指定发送的回响请求消息中“数据”字段的长度（以字节表示）。默认值为 32。如图 1-7 所示。Size 的最大值是 65527。

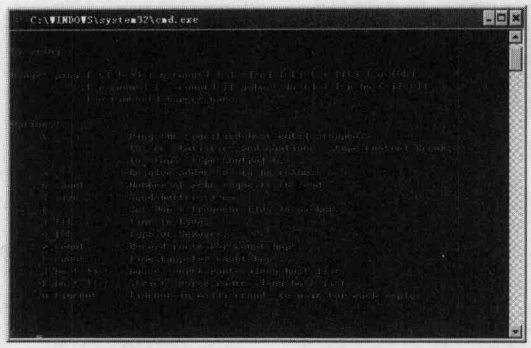


图 1-6　查看 ping 命令的详细说明

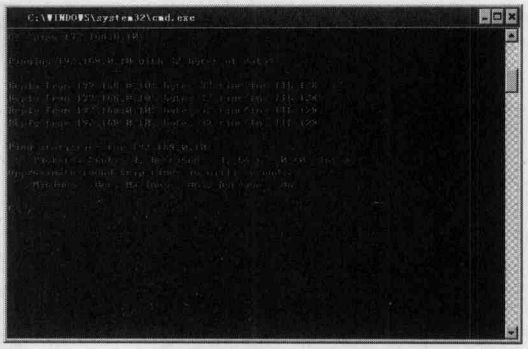


图 1-7　查看数据字节的默认长度

- -f：指定发送的回响请求消息带有“不要拆分”标志（所在的 IP 标题设为 1）。回响请求消息不能由目的地路径上的路由器进行拆分。该参数可用于检测并解决“路径最大传输单位（Path Maximum Transmission Unit，PMTU）”的故障。
- -I TTL：指定发送回响请求消息的 IP 标题中的 TTL（Time To Live，存活时间）字段值。其默认值是主机的默认 TTL 值。对于Windows XP 主机，该值一般是 128，TTL 的最大值是 255。
- -V TOS：指定发送回响请求消息的 IP 标题中的“服务类型（TOS）”字段值。默认值是 0。TOS 被指定为 0～255 之间的十进制数。
- -r Count：指定 IP 标题中“记录路由”选项用于记录由回响请求消息和相应的回响应答消息使用路径。路径中每个跃点都使用“记录路由”选项中的一个值。如果可能，可指定一个等于或大于来源和目的地之间跃点数的 Count。Count 最小值必须为 1，最大值为 9。
- -s Count：指定 IP 标题中的“Internet 时间戳”选项用于记录每个跃点的回响请求信息和相应的回响应答消息的到达时间。Count 的最小值为 1，最大值为 4。
- -j Path：指定回响请求消息，使用带有 HostList 指定 IP 标题中的“稀疏资源路由”选项。可由一个或多个具有松散源路由的路由器分隔连接中间目的地。主机列表中的地址或名称最大数为 9，主机列表是一系列由空格分开的 IP 地址（带点的十进制符号）。
- -k HostList：指定回响请求消息，使用带有 HostList 指定的中间目的地集的 IP 标题中的“严格来源路由”选项。使用严格来源路由，下一个中间目的地必须是直接可达的（必须是路由器接口上的邻居）。主机列表中的地址或名称的最大数为 9，主机列表是一系列由空格分开的 IP 地址（带点的十进制符号）。
- -w Timeout：指定等待回响应答消息响应的时间（以微秒计），该回响应答消息响应接收到的指定回响请求消息。如果在超时时间内未接收到回响应答消息，将会显示“请求超时”的错误消息。默认的超时时间为 4 000 000 微秒（4 秒）。
- Target Name：指定目的端，它既可以是 IP 地址，也可以是主机名。

典型示例：

（1）检测本机网卡驱动程序以及 TCP/IP 协议

若想检测本机的网卡驱动程序以及 TCP/IP 协议是否正常，只需要在命令提示符窗口中，输入“ping 192.168.0.7”命令，如图 1-8 所示。

（2）多参数合用检测

若要在命令提示符窗口中输入“ping -a -t 192.168.0.10”命令，即可对 192.168.0.10 的这台计算机进行探测。其探测结果如图 1-9 所示。通过反馈信息可得知上述命令中的参数“-a”检测出了该机器的 NetBios 名为 dns.sq.js.cn；参数“-t”在不断向该机发送数据包。

图 1-8 检测本机

图 1-9 多参数合用检测计算机

通常，ping 命令会反馈如下两种结果：

1）请求超时。表示没有收到网络设备返回的响应数据包，也就是说网络不通。出现这个结果原因很复杂，通常有对方装有防火墙并禁止 ICMP（Internet Control Message Protocol，网际控制信息协议）回显、对方已经关机、本机的 IP 设置不正确或网关设置错误、网线不通等几种可能。

2）来自 192.168.0.10 的回复：字节=32，时间<1ms，TTL=128。表示网络畅通，探测使用的数据包大小为 32 字节，响应时间小于 1ms。TTL 是指一个数据包在网络中的生存期，网管可通过它了解网络环境，辅助维护工作，通过 TTL 值可以粗略判断出对方计算机使用的操作系统类型，以及本机到达目标主机所经过的路由数。

当检查本机的网络连通情况时，通常会使用 ping 命令给某个目标主机（如本机）发送 ICMP 数据包。在本机中生成 ICMP 数据包时，系统就会给这个 ICMP 数据包初始化一个 TTL 值，如 Windows XP 就会生成“128”，将这个 ICMP 数据包发送出去，遇到网络路由设备转发时，TTL 值就会被减去“1”，最后到达目标主机，如果在转发过程上 TTL 值变成“0”，路由设备就会丢弃这个 ICMP 数据包。

TTL 值在网络应用中很有用处，可以根据返回信息中的 TTL 值来推断发送的数据包到达目标主机所经过的路由数。路由发生在 OSI（Open System Interconnection，开放系统互联模型）网络参考模型中的第三层即为网络层。

提示 不同的操作系统，它的 TTL 值也是不相同的。默认情况下，Linux 系统的 TTL 值是 64 或 255，Windows NT/2000/XP 系统的 TTL 值为 128，Windows 98 系统的值为 32，UNIX 主机的 TTL 值为 255。

3. 通过网站判断系统

有时，黑客会通过网站来获得目标的操作系统信息。例如：若某黑客与某台计算机用户通过 QQ 聊天，黑客说：“我的网站不错，欢迎你来访问”，并给出了一个网页地址。很多个人计算机用户不会提防这个要求，于是立即访问了这个网页。

在访问这个网页的同时，此个人计算机用户的操作系统信息实际上已经被写入到数据库中

了。这样，黑客不费吹灰之力就得到了想要的信息。这样，获取指定信息的代码很简单，实现的方法有很多。比如，下面的代码就可以在网页上显示客户端的操作系统等信息。

```
<%
Response.write?Request.ServerVariables("HTTP_ACCEPT_LANGUAGE")&"<br>"Response.write?Request.ServerVariables("HTTP_USER_AGENT")&"<br>"
%>
```

在访问含有上述代码的网页时，就会看到相应的信息。通过这些信息，可以知道个人计算机用户的 IE 版本、操作系统版本等。并且这些信息都可以用于黑客任务。

提示 上述方法是使用了服务器变量集合保存了随 HTTP（Hyper Text Transfer Protocol，超文本传输协议）头请求一起传送的 HTTP 头的信息，HTTP 头中包含有很多来访者（客户端）的信息，可以通过它获得有关来访者的操作系统版本、浏览器版本等信息。

第 2 招　探测网站信息

网站是黑客入侵或攻击的主要对象之一，由于网站是人人都可以访问的一个内容载体，它只要有一点风吹草动，可能就会产生较大的影响，这很容易让黑客产生“成就感”。黑客在对网站展开任务之前，通常会执行相应的探测操作。

1．探测域名和 IP

对于购买了域名的网站，既可以直接使用 IP 地址作为网址，也可以使用域名作为网址，在如图 1-10 所示窗口中输入相应的内容，即可看到相应的绑定信息。这就是为什么有的网站只能用 IP 地址进行入侵，有的却可以使用 IP 地址或域名进行入侵的缘故。通常，用户把采用域名系统命名的网址称之为“域名”或“网址”（网站 IP 地址也可称为“网址”）。

域名地址以层次化表示：

1）后缀。最右边的后缀用于标识域名的性质，如 cn 表示中国，edu 表示教育机构。实际上，由于域名申请的开放性，用户可根据自己的喜好来注册.net 或.com。这就好比用户可随意到某个城市（随便使用.com 或.net）居住，但城市名称（.com 这样的后缀）却不能由用户来定义一样。

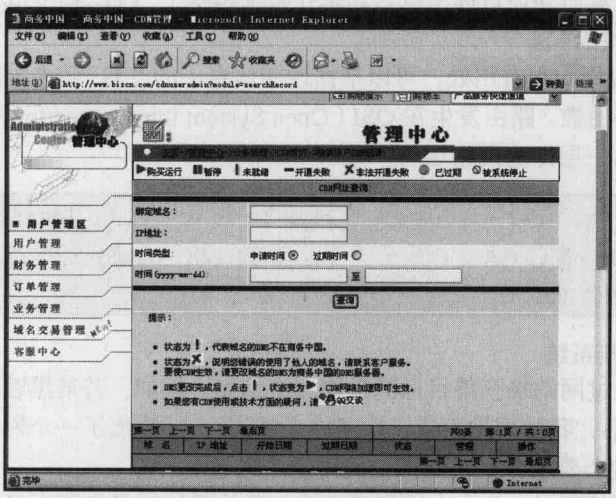


图 1-10　绑定 IP 地址

2）名称。名称即域名中间的网站名称，如 www.xinghuaye924.cn 这个域名中的网站名称就是 xinghuaye924。这是在注册域名时用户需要自定义的部分，它在同一种域名后缀中是唯一的。也就是说，可以有 xinghuaye924.net 和 xinghuaye924.cn。

3）前缀。最左侧的前缀用于标识网站类别，如 www 表示 Web 服务。由于申请的域名是 xinghuaye924.net，所以 www 和 ftp 这样的前缀可自由设置（不设置前缀也可以），如 360sight.cn 等。其中，要注意 www 和 ftp 这样的前缀名，已约定俗成供 Web 服务和 FTP 服务使用了。

通常，用户可以根据前缀看出网址所对应的具体内容。

- www：Web 服务，如 www.xinghuaye924.net。
- ftp：数据上传下载服务，如 ftp.xinghuaye924.net。
- bbs：论坛服务，如 bbs.xinghuaye924.net。
- mail：邮局服务，如 mail.xinghuaye924.net。
- down：下载服务，如 down.xinghuaye924.net。
- news：新闻服务，如 news.xinghuaye924.net。
- movie：电影服务，如 movie.xinghuaye924.net。
- music：音乐服务，如 music.xinghuaye924.net。

除这些约定俗成的名称外，通常用户会以常用英文单词或拼音等来作为前缀，如百度图片搜索就是 http://image.baidu.com/。通常，黑客在访问一个网址前，可凭经验判断出其提供什么服务。对于一名黑客来说，要入侵的网站有哪些域名，以及这些域名解析到哪些 IP 地址，都应该做到心中有数。检测的方法很简单，以检测 bbs.newtop01.com 网站解析到的 IP 地址为例，需要执行如下操作。具体的操作步骤如下。

步骤 1：在【运行】对话框的运行栏中输入“cmd”命令，即可进入命令提示符窗口。如图 1-11 所示。在当前命令提示符下输入“ping bbs.newtop01.com”命令，即可显示该论坛的反馈信息，如图 1-12 所示。

步骤 2：通过上述显示信息，可以看出 bbs.newtop01.com 这个网站解析到的 IP 地址是 203.171.239.143。也即 bbs.newtop01.com 网站内容存储在 203.171.239.143 这台服务器中。要查询域名对应的 IP 地址，可使用 ping 命令。

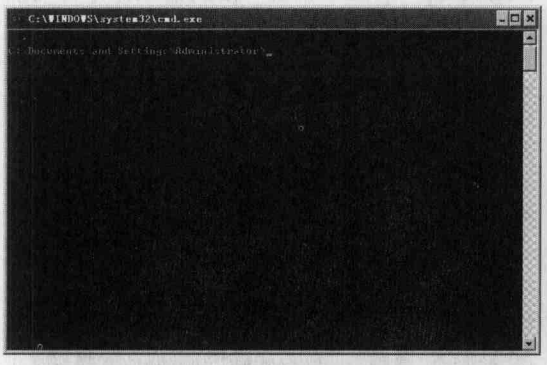


图 1-11 命令提示符窗口

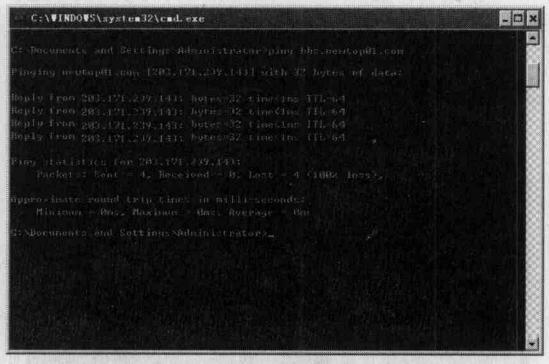


图 1-12 显示论坛的反馈信息

如果希望知道有多少不同的域名指向到某个 IP 地址，可以通过执行如下操作来完成查询，具体的操作步骤如下。

步骤 1：先在 IE 浏览器地址栏中输入“http://www.myipneighbors.com/”网址，即可进入“myipneighbors”的主页，如图 1-13 所示。

步骤 2：在窗口右上角“Search”栏中输入要查询的 IP 地址，单击右边的【search】按钮，即可查看相应的结果。如图 1-14 所示。

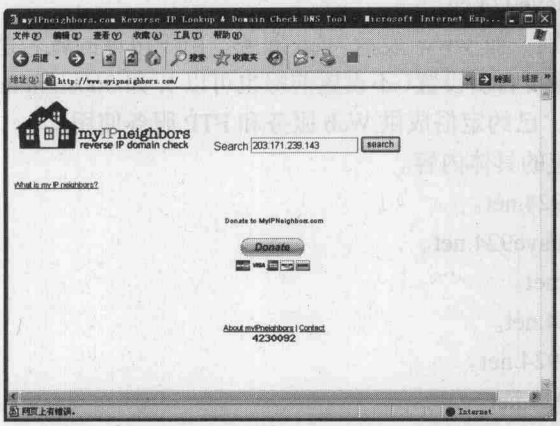


图 1-13 “myipneighbors”的主页

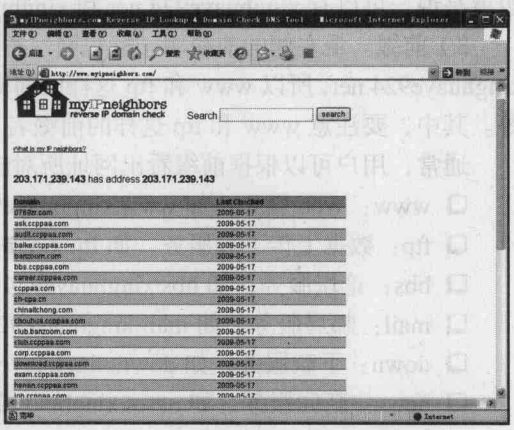


图 1-14 查看该站点的指向信息

步骤 3：在查询完毕后，该站点会将结果信息，以列表的形式反馈出来。最后任意选中一个域名并将其复制，粘贴到 IE 地址栏中，单击【转到】按钮，即可访问这个域名。

有时，一个网站的安全配置很好，并不代表其所在服务器上其他网站的安全配置也好。因此，先透过其他有漏洞的网站来完成服务器的入侵，最后再完成目标网站的破解，也是常见的网站入侵方法。

2. NsLookup 的使用

NsLookup 命令经常会被黑客用于查询域名对应的 IP 地址、A（Address，地址）记录、MX（Mail Exchanger，邮件交换）记录、NS（Name Server，域名服务器）记录、CNAME（Canonical Name，别名）记录等信息。使用 NsLookup 可以从如下几个示例来说明。

示例 1：若要查询 A 记录，则只需按“NsLookup 域名”格式输入命令，如“NsLookup newtop01.com”命令，如图 1-15 所示。

示例 2：若要查询 MX 记录，则只需要按“NsLookup -q=mx 域名”格式输入命令即可。如“nslookup -q=mx bbs.newtop01.com”命令。显示结果如图 1-16 所示。

图 1-15 查询 A 记录

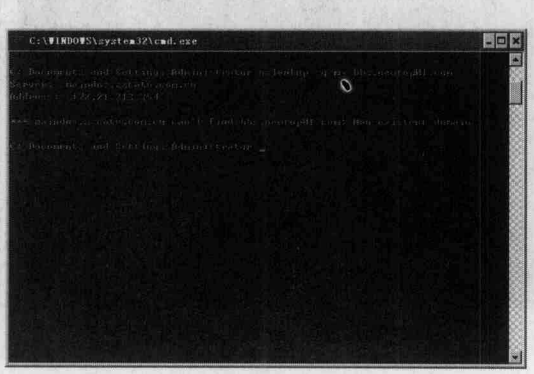


图 1-16 查询 MX 记录

示例 3：若查询 NS 记录，只需按“NsLookup -q=ns 域名”格式输入命令，如“nslookup -q=ns web.newtop01.com”命令，如图 1-17 所示。