本手册随盘赠送

黑客入门全程图解

吴自容 武新华 孙献璞 编著

披露黑客“练功”全过程！

山东电子音像出版社出版

黑客入门

全程图解

吴自容 武新华 孙献璞 编著

山东电子音像出版社出版

书　　名：黑客入门全程图解
编　　著：吴自容 武新华 孙献璞
策　　划：张　洁
责任编辑：刁　戈
执行编辑：罗应中　彭　葵
封面设计：王妙婷
组版编辑：石　磊

出版单位：山东电子音像出版社
地　　址：济南市胜利大街39号
邮　　编：250001
电　　话：（0531）2060055－7616

发　　行：山东电子音像出版社
经　　销：各地新华书店、报刊亭
CD 生产：淄博永宝镭射音像有限公司
文本印刷：重庆市升光电力印务有限公司
开本规格：787×1092毫米 16开19印张 300千字

版本号：ISBN 7-900370-86-2
版　次：2004年3月第1版
定　价：28元（1CD+手册）

为什么购买此书

首先声明：全书从技术分析角度出发，对黑客的每个攻击入侵方法和所有实例都进行了测试，全部可以实现和做到，但，害人之心不可有，读者诸君切勿将本书内容用于任何违法行为，否则一切法律责任自负！

上网大家都会，但网络安全的观念和常识却相当缺乏，在遇到别有用心者的入侵后，结果会非常严重！针对这群电脑用户，本书特别披露黑客“练功”全过程，并将其入侵伎俩和招数大曝光，大家在一步步跟着学做后即可熟知那些所谓“神秘”的黑客手法，从而高度重视网络安全，并采取相关措施现场自救！

链接：

米尼克（Kevin Mitnick），第一个登上美国联邦调查局通缉犯名单的电脑黑客。他是“名留青史”的大盗，曾经入侵Digital公司电脑系统，偷走价值百万美元的程序代码；入侵通用电器公司网络，使全球通用人度过七十二小时公司无网络的黑暗时刻。米尼克最后入狱服刑四年半，在2000年出狱后，到2003年前都被禁止接触电脑。在这个大盗的诠释中，“人性”是最大的弱点；人最不安全的时候，就是自以为安全的时候。

光盘内容：本书重点黑客攻防实例的视频展示，任何人都没理由看不懂！

本书特色：不需要专业的网络知识，不需要任何编程基础。

适用读者：

1. 电脑初学者和稍微有点基础的电脑用户。
2. 对黑客和黑客技术感兴趣的所有电脑用户。

光盘导读

视频教学

黑客攻击的第一步	
常用黑客命令	\AutoPlay\Videos\ 常用的黑客命令 .avi
Superscan 扫描	\AutoPlay\Videos\ 使用 Superscan 扫描开放的端口 .avi

入侵 Windows	
IPC$ 漏洞攻击	\AutoPlay\Videos\IPC$ 漏洞攻击过程演示 .avi
关闭 IPC$ 漏洞	\AutoPlay\Videos\ 关闭 IPC$ 默认共享漏洞演示 .avi
Netbios 入侵	\AutoPlay\Videos\ 利用 Netbios 漏洞入侵过程演示 .avi
生成黑客字典	\AutoPlay\Videos\ 生成黑客字典过程演示 .avi
破解登录密码	\AutoPlay\Videos\ 远程破解 Win2000 登录密码 .avi

木马的植入与清除	
冰河攻击过程	\AutoPlay\Videos\ 冰河木马攻击过程演示 .avi

地毯式攻击 QQ	
QQ 密码攻击	\AutoPlay\Videos\QQ 密码攻击过程演示 .avi

邮件偷窥与信箱轰炸	
邮件欺骗	\AutoPlay\Videos\ 利用邮件欺骗对方邮件密码 .avi
破 Foxmail 密码	\AutoPlay\Videos\ 绕过 Foxmail 的密码封锁 .avi

恶意攻击浏览器	
防范恶意代码	\AutoPlay\Videos\Win2000 系统如何防范恶意代码 .avi

恶意攻击 IIS 服务器	
ida 溢出漏洞	\AutoPlay\Videos\ida 溢出漏洞攻击演示 .avi
WEB 服务器	\AutoPlay\Videos\ 配置一个安全的 WEB 服务器 .avi
制作代理跳板	\AutoPlay\Videos\ 制作代理跳板过程演示 .avi

确保自己的上网安全	
防范终端攻击	\AutoPlay\Videos\ 防范终端服务攻击 .avi

Contents 目录

第 3 章　木马的植入与清除

第 4 章　地毯式攻击 QQ

第一章 黑客攻击的第一步

- 黑客为什么要攻击
- 攻击的流程
- 黑客常用工具
- 黑客常用命令

在网上常常会听到网友说：“我被黑了！”。在很多人眼里，“黑客”就是网络破坏者的代名词，再加上美国大片《黑客帝国》的热播，似乎整个电脑世界都已经被“黑客”所统治。那些带着墨镜、运指如飞、坐在一台不断跳动着数据的屏幕前、一脸深沉的人就是“黑客”了，是这样的吗？

在许多人眼中，“黑客”是这样一些高深莫测的神秘人物，他们利用手中所掌握的技术肆意攻击网络、盗取商业机密。加上一些媒体对黑客和黑客事件不负责任的夸大报道，使得黑客以及黑客技术对大多数普通网民而言更多了一层神秘的面纱。其实，黑客以及黑客技术并不神秘，也不高深。一个普通的网民在具备了一定基础知识之后，就可以成为一名黑客，甚至无需任何知识，只要学会使用一些黑客软件，同样有能力对网络实施攻击。

本章将介绍一名黑客需要了解的一些初步知识：黑客为什么要攻击？攻击的流程怎样？黑客常用的工具和命令有哪些？……

1.1 黑客为什么要攻击，攻击的流程怎样？

1.1.1 黑客为什么要攻击

为什么会存在黑客？他们入侵的理由和目标又是什么？

其实许多时候，大多数的黑客进行攻击的理由都是很简单的，大体上有以下几种原因：

●想要在别人面前炫耀一下自己的技术，如进入别人的电脑去修改一个文件或目录名，算是打个招呼，也会让他对自己更加崇拜。

●看不惯同事（同学）的某些做法，又不便当面指责，于是攻击他的电脑，更改他的桌面，更有甚者获得他的隐私。

●好玩，恶作剧、练功，这是许多人或学生入侵或破坏的最主要原因，除了有练功的效果外还有些许网络探险的感觉。

●窃取数据，可能是偷取硬盘中的文件或各种上网密码，然后从事各种商业应用。

●抗议与宣示，如2001年5月1日中美黑客大战，两国的黑客互相攻击对方网站，双方均有数以千计的网站遭到攻击，轻者被篡改主页面，严重的则整个系统遭受毁灭性打击，如图1-1-1所示为一个被黑网站的主页。

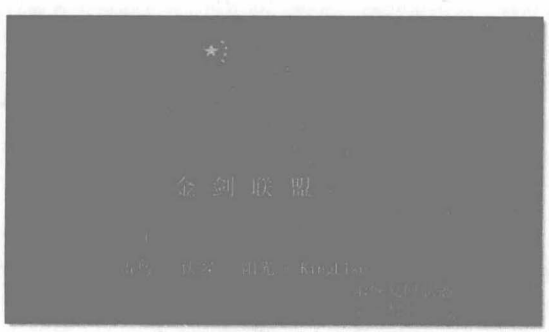

图1-1-1 一个被黑网站

提示

当然了，我们也不排除某些仅仅只是出于好奇，并不想实现什么目的，只是利用现在遍布网络的“傻瓜”式工具进行攻击的攻击者，因为从某种意义上来说，他们并不代表真正意义上的黑客，至多只能算是一个“骇客”而已。

1.1.2 了解黑客攻击的流程

通常，我们很多时候中了黑客的招还不知道自己是怎么中的，更有甚者，自己的电脑已经被人植了木马还不知道自己已经成了“板上的肉鸡”（任人宰割的机器），这才叫惨呢。

下面我们就来看看黑客是如何攻击用户电脑的，当然，偶然的一次攻击可能过程就没有这么烦琐，但是如果你本机的安全问题确实比较糟糕的话，就很有可能被黑客轻松掳为“肉鸡”。

一般来讲，黑客攻击的流程大致如下：

“确定目标的IP地址”→“扫描开放的端口”→“破解账号和密码”→“实现目的”。

为什么要首先进行IP扫描和端口扫描呢?

我们知道，黑客在发动一场攻击之前，一般都要先选定自己的攻击目标，也就是我们所说的要先确定自己想要攻击的目标电脑的IP地址。

对于这一步，我们可以假设，黑客可能是在一开始就确定了攻击目标，也可能是先大量地收集网上计算机的信息，然后根据各个主机安全性的强弱来确定自己最后的攻击目标。

仅仅是有目标的IP地址还不够，黑客还需要收集目标计算机的各种信息，例如操作系统版本、开放的服务端口、端口提供的服务类型及软件版本等。了解这些信息能够帮助攻击者发现目标机的某些内在弱点，也就是目标机开放的端口和漏洞之类的东西。

在对这些信息进行缜密、细致的分析之后，黑客就可以选择进攻途径开始发动攻击了。在后面的章节我们将会陆续进行介绍。

1.1.3 确定目标的IP地址

什么是IP地址?

IP是英语Internet Protocol的缩写，意即“互联网协议”，在Internet上，每台电脑节点都依靠唯一的IP地址互相区分和相互联系。形象地说，电脑的IP地址就像人的住址一样，是唯一的，数据的交换全靠它了。

IP地址构成了整个Internet的基础，它是如此重要，互联网上的每一台计算机无权自行设定IP地址，有一个统一的机构——IANA负责对申请的组织（如电信、网通等）分配一个网络IP段，而该组织可以对自己网络中的每一个主机分配一个唯一的主机IP（如果你是通过电信ADSL上网，你的IP地址就是由电信分配），正如一个单位无权决定自己在所属城市的街道名称和门牌号，但可以自主决定本单位内部的各个办公室编号一样。它是一个32位二进制数的地址，由4个8位字段组成，每个字段之间用点号隔开，用于标识TCP/IP宿主机，比如61.220.111.1。

IP地址到底有什么用?

简单地说，如果对方想访问你的电脑，就必须知道你电脑的IP地址；如果你想访问对方的电脑，也必须知道对方电脑的IP地址，当知道IP地址后，由网络服务器按照所输入的IP地址去查找相对应的电脑，将信息传送到对方的电脑里。更进一步，主叫方只要获得了被叫方的IP地址，就可以发出呼叫、建立连接、实现应用，

如利用网络电话NetMeeting直接通话或者发送文件。讲到这里，有朋友可能会问，那我访问网站输入的网址是，http://www.sina.com.cn/，没有用到IP地址呀，其实http://www.sina.com.cn/ 只是一个域名，要想访问这个网站，网络上的DNS服务器会把这个域名翻译成IP地址，再查找相对应的服务器，传送、交换数据。

所以说，一般情况下只要利用域名和IP地址都是可以顺利找到主机的，除非你的网络不通。

也就是说，如果想要攻击某台电脑，首先需要确定攻击目标，也就是说要知道这台被攻击主机的域名或者IP地址，例如：www.gongji.com或124.18.65.1等。

对使用Windows系列操作系统上网的用户来说，如果安全意识不强，没有给自己的系统打什么补丁的话，那么只要知道了他的IP地址，就可以使用一些现成的工具如IPhacker让他莫名其妙地蓝屏，另外，还可以使用一些扫描器（如Superscan）找出他主机上的很多漏洞，入侵主机，进而控制机器，获取机器上的任意文件，包括QQ目录的密码信息文件和聊天记录……当然，得到他IP地址后，利用一些黑客攻击软件让他的QQ下线，至于给他发送一大堆垃圾信息让他应接不暇，那就更是小菜一碟了。

小博士，我想问一个问题，就是我如何知道自己和对方电脑的IP地址呢？

有些黑客攻击软件需要输入自己本机的IP地址，那我们先来看看如何查看自己本机的IP地址。

1．查看本机的IP地址

对于Windows 98，我们可以采用以下方法来查看IP地址：

在“开始|运行”里输入：winipcfg。接着，Windows就会打开“IP 配置”对话框。其中，在“Ethernet适配器信息”中的“IP 地址”显示的xxx.xxx.xxx.xxx，如图1-1-2所示，就是你的IP地址。

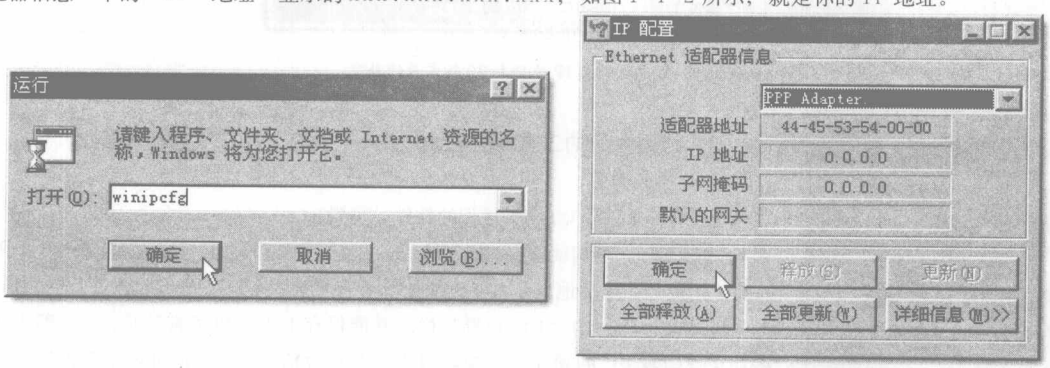

图1-1-2 在Windows 98中显示IP地址

对于Windows 2000，在“开始|运行”里输入：cmd。在命令行里输入：ipconfig，即可轻松查找到本机的IP地址（IP Address）。如图1-1-3所示。

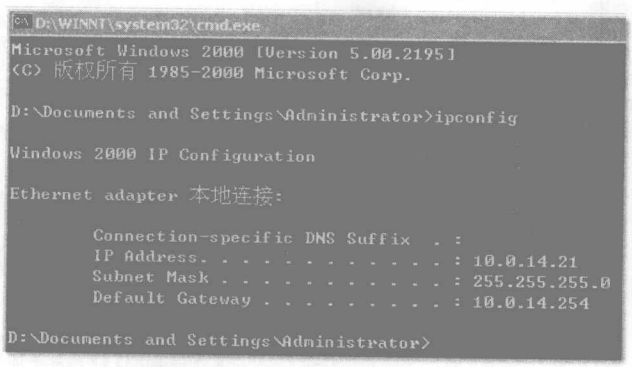

图1-1-3 在Windows 2000中显示本机IP地址

要攻击别人最重要的是要获得对方机器的IP地址，如何获得对方的IP地址呢？方法很多，下面我们就来详细看看如何得到对方的IP地址。

2．查看目标机的IP地址

（1）通过QQ软件查IP补丁查IP

每当QQ的一种新版本出来，隔不了几天补丁程序就出来了，即便是菜鸟查看IP地址和端口都异常容易，如木子工作室提供的QQ2003II的补丁在腾讯公司提供QQ2003II下载之后半个月就出来了，其下载地址为：http://www.muzi-studio.com，这种补丁只要对方在线就可以轻松查看对方的IP地址、所在地及QQ的版本号，如图1-1-4所示。

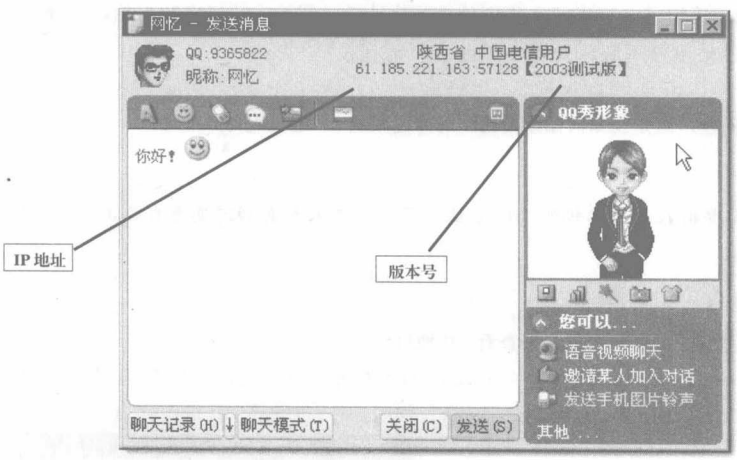

图1-1-4　查聊友IP地址和QQ版本号的补丁

图1-1-5　QQ聊天伴侣的主菜单

（2）利用专门的工具软件查IP

①QQ聊天伴侣

现在有一款称作QQ聊天伴侣的软件（可到http://www.jackysoft.com/cn/qqb1处下载），不但能查QQ好友的IP以及所在城市地址，而且还能查QQ上陌生人的IP和所在城市地址。其IP地址既可直接显示在QQ发送信息对话框的顶部，也可显示在该软件的“IP查看”栏，并能保存下来。更厉害的是，QQ聊天伴侣还具有查隐身IP的功能，只要隐身人一开口说话，其IP地址就暴露无遗，这样你就可以知道隐身好友到底是哪里的（别的查IP地址的软件不具备该功能）。

运行“QQ聊天伴侣”，会在系统托盘处出现一个黄色脸谱图标，点击此图标，会弹出一个菜单，如图1-1-5所示，该软件所有的功能都包含在此菜单中。

选择其中的“IP查看”命令，会弹出一个没有任何内容的窗口，此时可以给在线好友发一个消息。消息发过去后，他的QQ号码、IP地址、端口、所处的位置等信息会加入到前述的窗口中。以后，每得到一个新的好友IP地址信息，“QQ聊天伴侣”将自动将其相关信息加入“IP查看”窗口，这中间当然也包括隐身人和陌生人的IP地址，如图1-1-6所示。

图1-1-6　QQ聊天伴侣显示的IP地址等信息

有的时候，你所发送的消息不是直接发送给对方，而是通过腾讯服务器转发。对此，QQ 聊天伴侣无法得到对方的IP 地址。你可以从聊天记录中看到“通过服务器转发”的字样，此时，QQ 聊天伴侣是无法查到对方的IP 的，不过，这种情形并不多见。

② IPlocate

Iplocate (http://www.newhua.com/soft/13332.htm) 是一款专门用于查QQ 上好友、陌生人的IP 地址的软件，不管对方是否在线，只要你向他发信息或是他向你发信息，就可以查出他的IP 地址及所处地区；输入IP 便能查找出与之对应的国家或地区。

运行Iplocate 程序，按下监听按钮，如图1-1-7 所示。

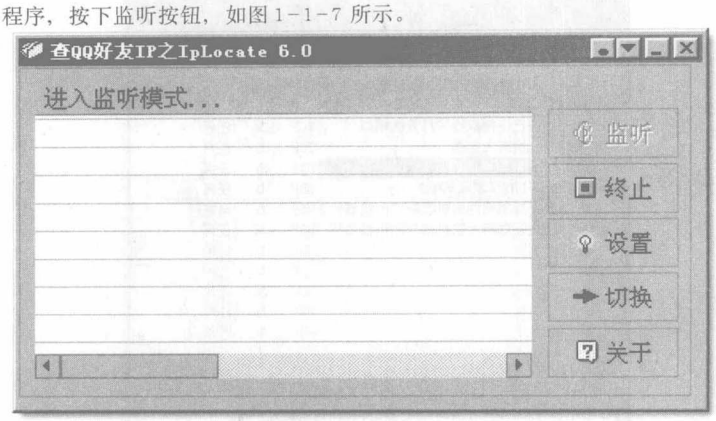

图1-1-7　Iplocate 的监听状态

然后向某人发一消息或等某人向你发消息，程序就会显示该人的QQ 号码、IP 地址，端口和所处区域，如图1-1-8 所示。

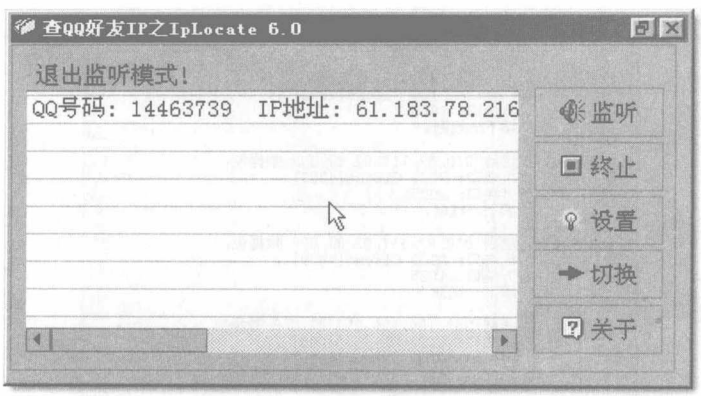

图1-1-8　Iplocate 的监听到IP 地址等信息

在监听过程中，若有好友发消息给你，程序将得到发消息的那个人的IP 地址，这样就中断了原来的监听，若需要继续监听，需要再按一次监听按钮。如果能返回IP 地址，且端口为4000，或4001，4002……，等则便是此人的IP 地址。如果端口为其他值，那此人可能是在网吧上网或在局域网内或使用代理服务器上QQ；如果网络不是很畅通的话，消息会经服务器转送，这样将得不到对方IP，可在网络畅通时，再试一次。

上面只是以两种较为典型的工具软件为例来介绍查看IP 地址的方法，其实还有很多查看IP 的工具，这里就不再多述。这些工具软件获得的好友IP 地址是准确无误的，但所示的地理位置不一定准确，可能是IP 地址库更新较慢的原因。如果想要精确知道对方的地理位置，可以采用一种叫“追捕”的软件进行辅助查看，由于追捕软件的IP 地址库非常大且很全，更新速度又快，因此得到的地理位置是比较准确的。

③用防火墙查看 IP

由于QQ 使用的是UDP 协议来传送信息，而UDP 是面向无连接的协议，QQ 为了保证信息到达对方，需要对方

发一个认证，告诉本机，对方已经收到消息，一般的防火墙（例如天网）都带有UDP监听的功能，因此可以利用这个功能来查看IP。

第一步：．运行防火墙程序，在“自定义IP规则”一栏把“UDP数据包监视”选项打上钩（QQ中的聊天功能使用的是UDP的4000端口作为数据发送和接收端口）。接着点一下工具按钮上的保存图标，如图1-1-9所示。

第二步：运行QQ，向想查询IP地址的对象发一信息；

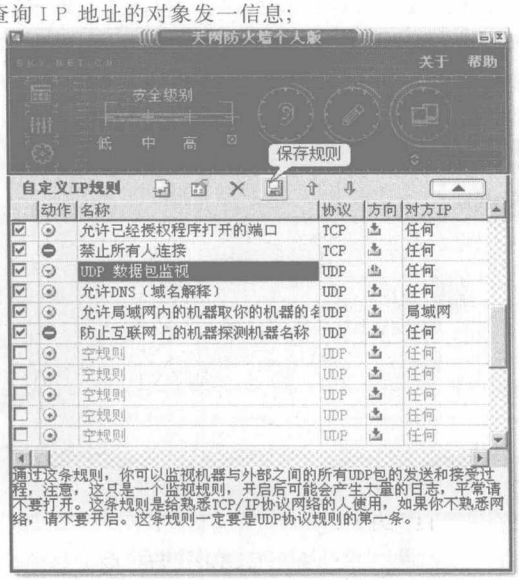

图1-1-9　在防火墙中选中UDP数据包监视规则

第三步：切换到防火墙程序所在窗口，看看当前由防火墙记录下来的日志（点击主界面中像铅笔一样的按钮■即进入日志界面），如图1-1-10所示。

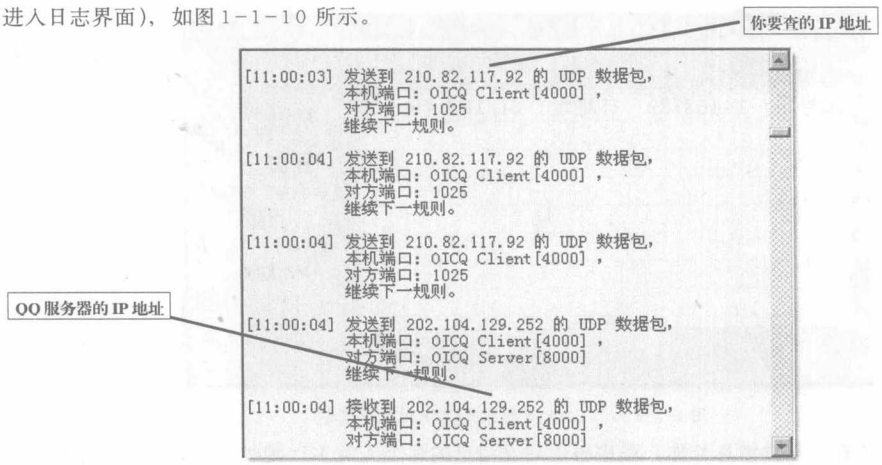

图1-1-10　天网防火墙的日志界面

在日志中，如果对方端口是OICQ Server[8000]，则表示该条日志上的IP地址是QQ服务器的。排除了本机的IP地址、发送到网关的IP地址以及QQ服务器的IP地址，剩下的就是对方的IP地址了，如图中为210.82.117.92。再配合“追捕”之类的工具软件，就可以知道对方的大概位置。用这种方法来查IP地址，不会受QQ版本的限制。

另外，还可利用天网的日志功能查到那些成天用扫描器软件到处扫描的人的IP地址。这是黑客需要具备的很重要的技能，在攻击别人时，首先要懂得保护自己。

④用DOS命令查看IP

我们还可以使用古老的DOS命令来查看对方IP地址，即借用网络命令Netstat。不过用此方法有个前提条

件，那就是一定要把想知道IP地址的好友请到QQ的“二人世界”里。

接着，在DOS窗口里（Windows 9x下叫DOS，Windows 2000下叫命令提示符）输入：netstat -n，你将看到如下内容：

```
Active Connections
Proto   Local Address        Foreign Address      State
TCP   61.109.34.78:1200   218.22.244.134:61555   ESTABLISHED
TCP   61.109.34.78:2694   61.143.136.34:6667     ESTABLISHED
TCP   61.109.34.78:4869   202.104.121.291:23     ESTABLISHED
```

从外部来的IP地址（Foreign Address）就有好几个，哪个才是要找的呢？现在找一个理由退出“二人世界”，在MS-DOS窗口再输入一次：netstat -n ，将看到如下内容：

```
Active Connections
Proto    Local Address      Foreign Address        State
TCP   61.109.34.78:1200    218.22.244.134:61555   TIME_WAIT
TCP   61.109.34.78:2694    202.109.72.40:6667     ESTABLISHED
TCP   61.109.34.78:4869    202.104.121.291:23     ESTABLISHED
```

仔细比较两次的结果，你会看出前后两次的区别。那就是在State列上字符发生了变化，由ESTABLISHED（建立）变为了TIME_WAIT。由于我们在“二人世界”时要传送消息，相互之间必然要产生连接（通过UDP协议），此时自然是“ESTABLISHED”了（以你用netstat -n命令的结果来说）；而退出“二人世界”连接就断开了，自然就是“TIME_WAIT”了，所以前面的218.22.244.134即是要找的IP地址。

使用这种方法，不需在电脑中安装软件，在任意一台能上网的电脑上都能使用。

另外，查QQ用户IP地址的方法和工具还有很多，如有人利用网络监听工具netxray 软件来进行查看，这有点像杀鸡用牛刀，其实上述方法已经足够你用了。

⑤聊天室中查IP

在允许贴图、放音乐的聊天室，利用HTML语言向对方发送图片和音乐，如果把图片或音乐文件的路径设定到自己的IP上来， 那么尽管这个URL地址上的图片或音乐文件并不存在，但只要向对方发送过去，对方的浏览器将自动来访问你的IP。对于不同的聊天室可能会使用不同的格式，但只需将路径设定到你的IP上就行了。

如：“XXX聊天室”发送格式如下：

发图像：img src="http:// 61.128.187.67/love.jpg"

发音乐：img bgsound="http:// 61.128.187.67/love.mid"

需要注意的是：这两个语句里的61.128.187.67需要替换成你自己的IP地址。

这样黑客用监视软件就可以看到连接到你机器的IP地址，这种软件很多，有lockdown，IP Hunter等。

如果对方在浏览器中将图像、声音全部禁止了，此方法就无能为力。对方使用代理服务器的，此方法也只能查到他所用代理的IP地址，无法查到其真实IP地址。

⑥查网站的IP地址

黑客要攻击某个网站，也需要首先获得该网站的IP地址，获取网站最简单的办法是使用Windows自带的一个小程序ping.exe。

在MS-DOS命令行下输入ping www.xxx.com。这时候就会出现：

```
C:\>ping www.xxx.com
Pinging www.xxx.com [xxx.xxx.xxx.xxx] with 32 bytes of data:
Reply from xxx.xxx.xxx.xxx: bytes=32 time=630ms TTL=116
Reply from xxx.xxx.xxx.xxx: bytes=32 time=630ms TTL=116
Reply from xxx.xxx.xxx.xxx: bytes=32 time=120ms TTL=116

Ping statistics for xxx.xxx.xxx.xxx:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum =120ms, Maximum =630ms, Average =187ms
```

其中：黑体字显示的xxx.xxx.xxx.xxx 就是 http://www.xxx.com 的网站服务器的IP地址。

如图1-1-11所示就是我们ping华军网站的一个实例：

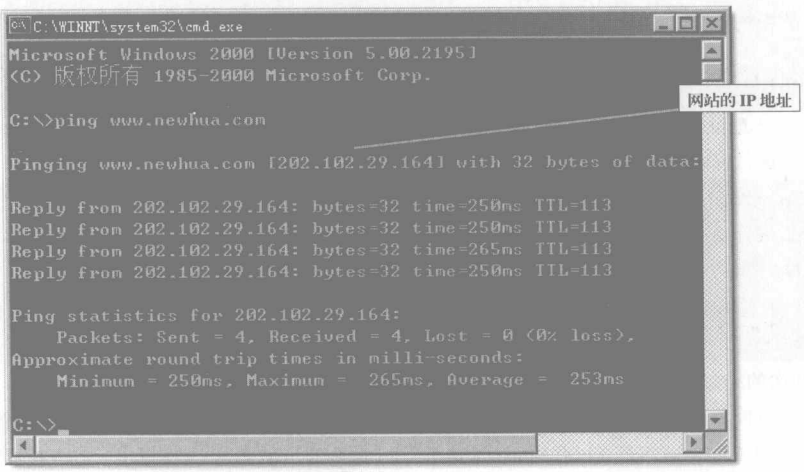

图1-1-11 用ping命令显示网站的IP地址

如果ping通了，将会从该IP地址返回byte,time和TTL的值，这样黑客就具备进一步进攻的条件。如果ping不通，就会返回“Request timed out”，表明对方要么不在网络上（如未开机），或者是使用了防火墙。如果使用了防火墙，要进行攻击就比较容易被发现。

提示

当然，对于个人计算机或是其它机器都可以使用ping命令看对方是否在线，只有对方在线，才能再进行下一步攻击。

通过以上几种方法，都可以获得对方的IP地址，为下一步的进攻打下了基础。

1.1.4 扫描开放的端口

前面已经知道了对方的IP地址，但是仅仅查到IP地址还不够，还需要了解对方开放了哪些端口，只有这样，才能真正找到进入对方机器的入口。正如即使找到对方所在地的门牌号，但还需要了解他家开了哪些门、窗、烟囱等入口。

什么是端口呢?

简单地说，端口就是计算机和外界连接的通道。

为了解释清楚端口，我们用房子来打个比方，端口就好比房子的门窗，它是信息出入的必经通道。另外，就如不同的门窗有不同的用处一样，不同的端口也有不同的功能，例如我们看网页用的实际上是80端口，而计算机上可开启的端口数值范围为1~65535。

以下是常用的几个端口：

① 21号端口：FTP（Pile Transfer Protocol，文件传送协议）

FTP服务和TELNET服务一样，它使得我们可以从FTP服务器上下载或上传资料等，有的还可以匿名登录，不过这样的情形现在好像不多了。