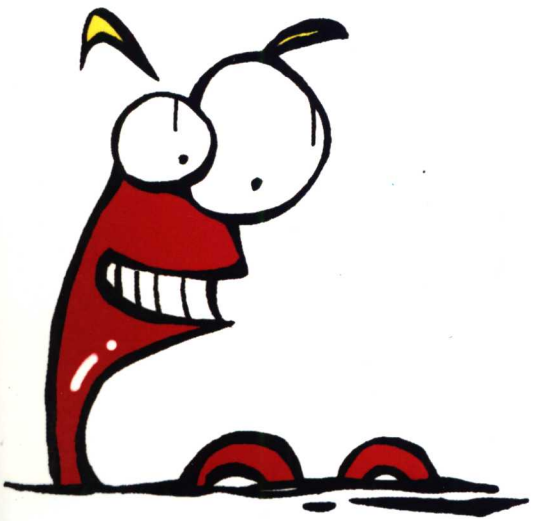
黑客营

黑客入门

所有黑客入侵伎俩逃不出我们手心！

吴自容　张聆玲　邓泽霞 编著

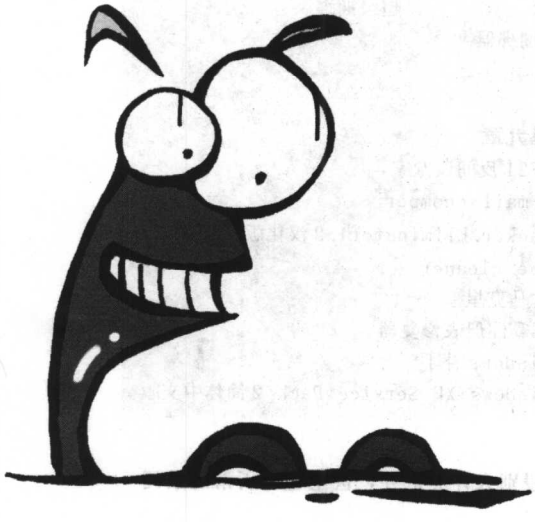


山东电子音像出版社出版

黑客营

黑客入门

吴自容　张聆玲　邓泽霞 编著



山东电子音像出版社出版

书　　名：黑客营——黑客入门

策　　划：张　洁
编　　著：吴自容　张聆玲　邓泽霞 编著
责任编辑：刁　戈
执行编辑：罗应中　彭　葵　王　莹　杨 震
封面设计：黄　丹
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
技术支持：(023) 63658888－13093

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：重庆诚凤印务有限公司
开本规格：787×1092毫米 16开 印张17.25 200千字

版本号：ISBN 7-89491-234-4
版　次：2005年5月第1版
定　价：28.00元（1CD+手册）

为什么购买本书

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！

本书不是要教你如何入侵，而是用众多鲜活的入侵案例全程剖析，让你了解黑客入侵的方法、原理，从而提高安全意识、掌握安全防御技术。正所谓：知己知彼，百战百胜！

本书特别为新手和稍微有一点基础的读者而制作，抛弃诸多艰深的原理，直接为大家提供黑客攻防的应用技术，从密码破解、系统入侵、网络攻击、扫描、安全漏洞、木马……都一一以图文详解！

光盘内容：

黑客入侵案例视频教学

黑客工具软件

光盘导读

黑客视频教学

第一章
制作字典文件演示
使用Superscan扫描漏洞演示
常用的黑客指令使用

第二章
流光破解邮箱演示
破解ZIP密码演示
远程破解Win2000登录密码演示

第三章
IPC$漏洞攻击过程演示
利用Netbios漏洞入侵过程演示

第四章
冰河木马攻击过程演示

第五章
QQ密码攻击过程演示
偷窥QQ用户聊天记录

第六章
利用邮件欺骗对方邮件密码
绕过Foxmail的密码封锁

第七章
窗口炸弹演示
打开网页时删除硬盘文件演示

第八章
制作代理跳板过程演示

第九章
Win2000系统如何防范恶意代码
防范终端服务攻击
使用RecoverNT恢复数据演示

黑客工具

第一章
Back Orifice 2000
iphacker1.2
KABOOM!3
SnadBoy's Revelation 2.0.1
superscan汉化版
X-Scan3.1
万能钥匙字典制作工具
广外女生1.53b
网络刺客II

第二章
007wasp
ADump
Web Cracker v4.0
dialupass
flashbios
fluxay5beta
netpass
passfoxmail
pqwak
XP星号密码破解器
溯雪
黑雨--POP3密码破解
scrsavpw
pwltool
pwdump3
Visual ZIP Password Recovery Processor
Advanced Office XP Password Recovery

第三章
NTSwitch
RPCscan
sc
Serv-U漏洞攻击程序
Shed

第四章
aspack加壳
beast202
bo2k中文版
exe2bmp
exeBinder
网络神偷
netspy30
winrar32
万能文件捆绑器
冰河
网络公牛
广外女生1.53b
超级捆绑

第五章
detourQQ
QQ万能登录1.2.8
QQ千夫指2005
QQ特工之密码破解秀
QQ细胞发送器2004
QQ骗子2.0
啊拉QQ大盗1.4
好友号好好盗2005

第七章
vbs脚本病毒生成器

第八章
CLEANIISLOG
CLEARLOGS
MultiProxy12
sockscap32

第九章
3721反间谍专家
e-mail chomper
Hacker.Eliminator1.2汉化版
the cleaner
木马克星
毒霸注册表修复器
Windows补丁
Windows XP Service Pack 2简体中文版

特别提醒：

一、本光盘中收录的黑客软件皆具有一定的杀伤力，除了可入侵别人计算机外，甚至也有所谓的杀硬盘程序，请千万小心使用。

二、这些软件仅供研究用，以帮助大家有效地抵御和防范黑客，切勿利用来破坏他人的计算机或数据，否则一切后果自负！

三、本光盘已经过严格杀毒，但因收录有黑客程序，所以在运行光盘时某些杀毒软件可能会报警。

目 录

第1章 黑客新手入门

黑客，一个充满神秘感的称谓，一个亦正亦邪的角色。有人说，有互联网就有黑客。电影《骇客帝国》里全黑装束、酷劲十足的基努·里维斯为我们塑造了经典的黑客形象。所以在很多人眼里，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”的标准形象，正是这些高深莫测的神秘人物，利用手中所掌握的技术肆意攻击网站、入侵军方系统、盗取个人隐私、商业机密、偷打免费电话等。

黑客真的个个都是“三头六臂”的么？

其实，黑客以及黑客技术并不神秘，也并不高深。一个普通的网民在具备了一定基础知识之后，也可以成为一名黑客，甚至无需任何知识，只要学会使用一些黑客软件，同样可以对网络实施攻击。黑客技术就像一把双刃剑，可以侵入他人主机，但也可以通过了解黑客入侵的手段，明白该如何防护自己的主机，以保护主机不受他人入侵。

1.1 黑客为什么能找到安全漏洞

系统漏洞是指某个程序（包括操作系统）在设计时未考虑周全，当程序遇到一个看似合理，但实际无法处理的问题时，引发的不可预见的错误。系统漏洞在某些情况下又称之为“安全缺陷”，如果当系统漏洞被恶意用户利用，就会造成信息泄漏、数据安全性受到威胁、用户权限被篡改等后果。而对普通用户来说，系统漏洞在特定条件下可能会造成不明原因的死机和丢失文件等现象。

漏洞的产生大致可分为以下三类：

① 在程序编写过程中人为遗留（留后门）

程序设计人员为了达到不可告人的目的，有意识地在程序的隐蔽处留下各种各样的后门，以供自己日后利用，有名的例子是C语言之父Ken Thompson，使用他写的C语言编译器来编译login程序，便造出后门，可让Thompson进入系统。不过，随着法律的完善，这类漏洞将越来越少（别有用心者除外）。

② 受水平、经验和当时安全加密方法局限

现在的操作系统和应用软件越来越庞大复杂，想让这些由几百万条代码组成的软件保证绝对没有安全漏洞是不可能的，由于受编程人员当时的水平、经验和安全技术加密方法局限，在程序中总会或多或少地出现些不足之处，这些地方有的影响程序的效率，有的会导致非授权用户的权利提升。所以不断爆出新的Windows漏洞，这是微软Windows补丁总也没有尽头的原因。

③由于硬件原因，使编程人员无法弥补硬件的漏洞，从而使硬件的问题通过软件表现。

提示

Windows漏洞层出不穷也有它的客观原因，任何事物都不能十全十美，作为应用于桌面的操作系统——Windows也是如此，且由于它在桌面操作系统的垄断地位，使其存在的问题很快暴露。

其实，我们大家都知道，安全与不安全从来都是相对的，就目前而言，还没有出现绝无漏洞的系统，我们只能够以其所存在漏洞的多少以及危害程度来判定该程序的安全性。俗语说得好：“道高一尺，魔高一丈”也就是说，正因为有了这些漏洞的存在，才会有我们的不懈追求和安全技术水平不断提高。

1.2 黑客攻击的一般步骤

黑客为什么要攻击？他们入侵的理由和目标又是什么？

1.2.1 黑客为什么要攻击

其实，许多时候，大多数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，如进入心仪的MM的机器上去修改一个文件或目录名，算是打个招呼，不但给MM一个惊喜，也会让她对自己更加崇拜。

●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，在适当的时机揭他的老底，让他难堪。

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

●窃取数据，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，恶意偷窃银行存款等等。

●抗议与宣示，这是敌对国、敌对势力之间最常出现的黑客行为，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1-2-1所示为美方白宫网站（www.whitehouse.net）被黑后的图片截图。

图1-2-1 美方白宫网站被黑后的图片截图

基于以上一些原因，黑客就产生了。

提示

当然了，我们也不排除某些仅仅只是出于好奇，并不想实现什么样的目的，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。

1.2.2 黑客攻击的流程

黑客经常光临我们爱机而且“来无踪，去无影”，让我们感觉太神秘了，有时自己的机器被植入木马，成了黑客的肉鸡还浑然不知，黑客究竟是如何进入我们的爱机的呢？

下面我们就来看看黑客是如何攻击你那可怜的机器的，当然，偶然的一次攻击过程可能就没有这么烦琐，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：

“确定目标机的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机的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。

仅仅是有目标机的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。通过这些信息能够帮助攻击者发现目标机的某些内在的弱点，也就是目标机开放的端口和漏洞之类的东东。

在对这些信息进行缜密、细致的分析之后，黑客们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。

1.2.3 确定目标机的IP地址

什么是IP地址?

所谓“IP地址”，就是“Internet Protocol Address”的缩写，意即“互联网协议地址”，在Internet上，每一个节点都依靠唯一的IP地址区分和相互联系。形象地说，IP地址就像人的住址一样，是唯一的，数据的交换全靠它了。

我们可以把互联网想象成一个地球村，当你拨号或是连接上网络的时候，就是想要加入到这个地球村，成为其中的一分子，既然要加入，当然就需要一个地址，让他人可以找到你，知道你的位置在哪里，这就是IP地址的基本概念。

一般我们使用的住址，通常是某某国家某某城市……而互联网上的IP地址，概念也是类似的，但是却是由四组数字组成，并且以“.”来分别，例如“61.128.128.199”。而这四组数字是由十进制所组成，必须介于0～255之间，所以255.255.255.255是互联网中最大的一组IP地址了。知道对方的IP是黑客攻击的第一步，不知道IP就什么都做不了。

IP地址到底有什么用呢?

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，如利用网络电话如NetMeeting直接通话或者发送文件。黑客知道IP，就如小偷知道你家地址，你说严不严重呢?

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/ 只是一个方便我们记住地址的域名，要想访问这个网站，还需要网络上的DNS服务器把这个域名翻译成IP地址，再查找相对应的服务器，传送、交换数据。

所以说，我们一般情况下利用域名和IP地址都可以顺利找到主机，除非你的网络不通。

现在大多数人上网都喜欢用Windows系列操作系统，而且安全意识也不高，所以一般也就没有打什么补丁，只要知道了他的IP地址，也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，入侵他的主机，进而控制他的机器，获取他机器上的任意文件，包括你QQ目录的密码信息文件和聊天记录等，让他痛失心爱的QQ，还有MM给他的情书等重要文件也可以偷窥……当然，得到他IP地址后，利用一些黑客攻击软件让他QQ下线，或是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。

说了这么多，那么该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，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

不管你使用何种上网方式（宽带网络、拨号连接、固定IP网络），只要你能够连接到互联网上，就一定会存在一组IP地址，有了这组IP地址，你的计算机才能在互联网上与其他的计算机沟通。

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”就会显示xxx.xxx.xxx.xxx，如图1-2-2所示，这就是你的IP地址了。

对于Windows 2000/XP，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。如图1-2-3所示。

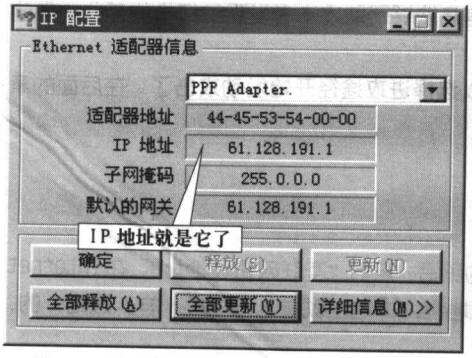


图1-2-2　在Windows 98中显示IP地址

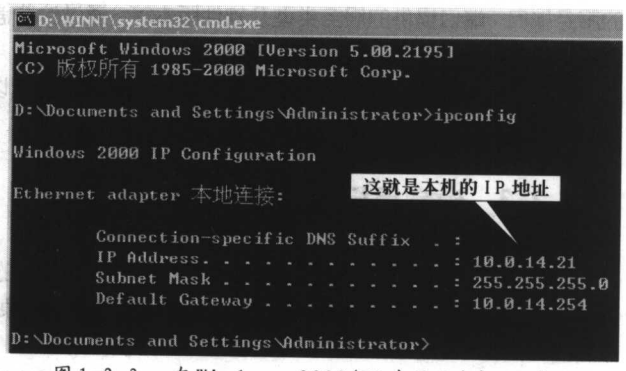


图1-2-3　在Windows 2000/XP中显示本机IP地址

作为一名黑客，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？获得对方电脑的IP地址的方法很多，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QQ2005珊瑚虫版就在腾讯公司提供QQ2005下载之后很短时间内就出来了，这种版本便是在QQ原有版本的基础上，增加了显示好友的IP地址以及地理位置的补丁，只要对方在线就可以轻松查看对方的IP地址、所在地等信息，如图1-2-4所示。

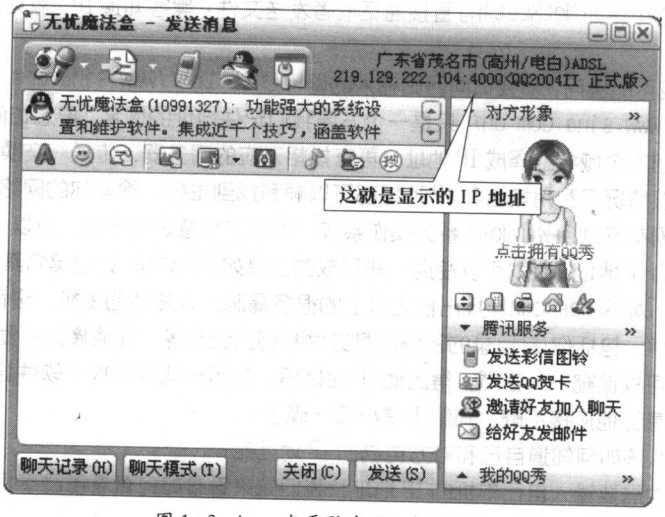


图1-2-4　查看聊友IP地址的补丁

(2) 用防火墙查看IP

由于QQ使用的是UDP协议来传送信息的，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，因此我们就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”那一栏把“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那个像磁盘一样的图标保存，如图1-2-5所示。

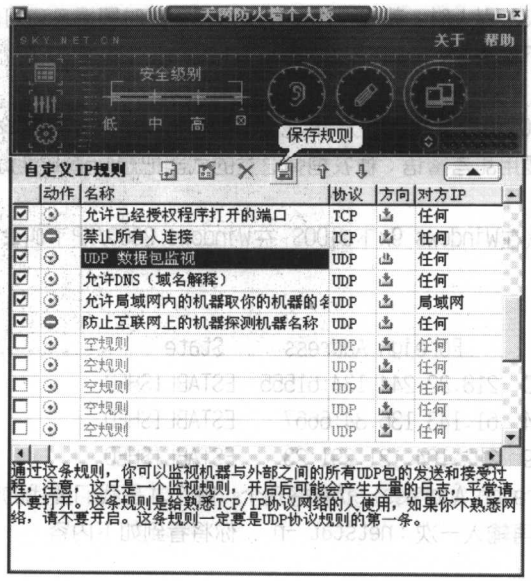


图1-2-5 在防火墙中选中UDP数据包监视规则

第二步：运行QQ，向想查询IP地址的对象发一信息；

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（点击主界面像铅笔一样的按钮即进入日志界面），如图1-2-6所示。

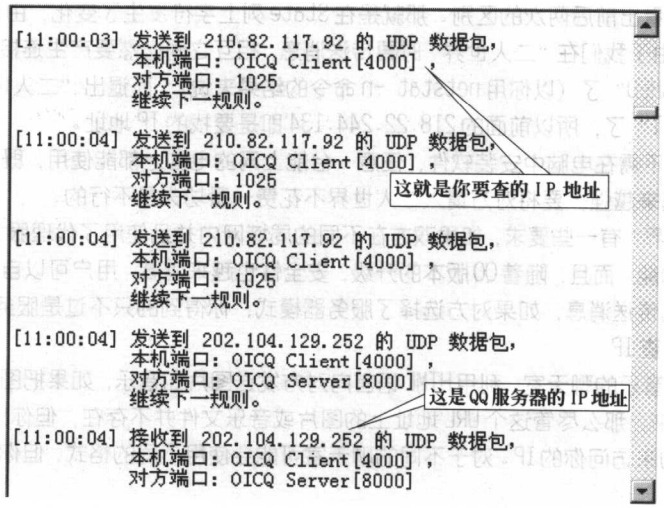


图1-2-6 天网防火墙的日志界面

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。

不过，随着QQ版本的升级，安全性也越来越高，用户可以自己设定是通过点对点模式还是服务器模式传送消息，如果对方选择了服务器模式，你也就得不到他的IP地址了。拥有了对方的IP地址，如果还想知道对方的地理位置，可以再配合“追捕”之类的工具软件，便可了解对方大概在哪里了。用这种方法来

查找IP地址，不会受QQ版本的限制，是一劳永逸的事！

另外，利用天网的日志功能也可以查到那些成天抱着一个扫描器到处扫描的人的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，时时警惕身边可能存在的黑客，以免弄得“出师未捷身先死”，那就得不偿失了。

(3) 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来查看。不过用此方法有个前提条件，那就是一定要用甜言蜜语、糖衣炮弹之类的武器把想知道IP地址的好友请到QQ的“二人世界”里。

接着，我们在DOS窗口里（在Windows 9x下叫DOS，在Windows 2000/XP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，哪个才是我们要找的呢？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 ，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  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，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，任意一台能上网的电脑上都能使用，既简单又方便！只是现在人们的安全意识越来越强，要将对方请入二人世界不花费一番功夫是不行的。

使用QQ“二人世界”有一些要求，如果双方在不同的局域网内并且使用了代理服务器，情况比较复杂，有可能不能使用该功能。而且，随着QQ版本的升级，安全性也越来越高，用户可以自己设定是通过点对点模式还是服务器模式传送消息，如果对方选择了服务器模式，你得到的只不过是服务器的IP地址而已。

(4) 在聊天室中查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，但你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，但你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。

这样你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，lockdown，IP Hunter等就会显示出他（她）的IP。

只是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。对于使用代理服务器的，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。

(5) 查网站的IP地址

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

在MS-DOS命令行下输入ping www.xxx.com。如图1-2-7所示ping天极网的显示结果：

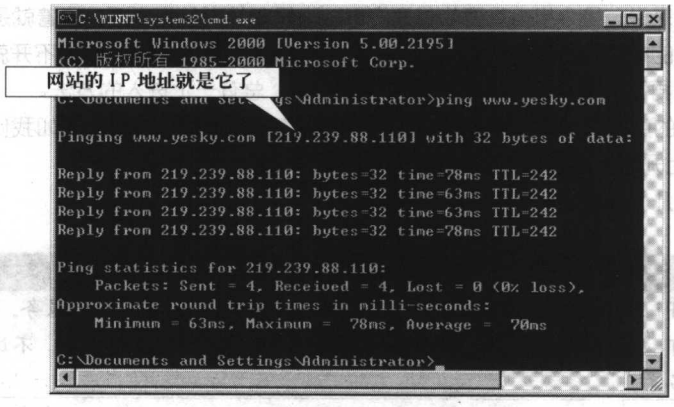


图1-2-7 用ping命令显示网站的IP地址

如果ping通了，将会从该IP地址返回byte,time和TTL的值，这样我们就具备进一步进攻的条件。其中time时间越短，表示响应时间越快。

如果ping不通，则会显示如图1-2-8所示，返回“Request timed out”，这就表明对方要么不在网络上（如未开机），或者是使用了防ping功能的防火墙。

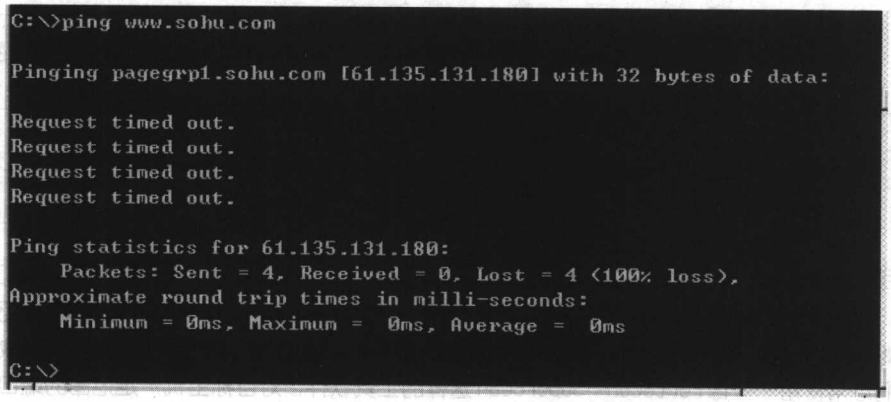


图1-2-8 用ping命令不通示意图

虽然上图返回了IP地址，但是ping不通，表明对方使用了防火墙以防止恶意乱ping的情况，要进行攻击就比较容易被发现，这种机器最好不好碰。

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

通过以上几种方法，我们可以获得对方的IP地址，如果没有固定的某台机器想要攻击，只是想找一些有漏洞的机器练练手艺，或是做个跳板什么的，可以利用后面章节介绍的扫描器来扫描有漏洞的IP地址，以免费力找到IP，却发现他并无漏洞可利用，岂不白辛苦一场。

1.2.4 扫描开放的端口

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。

一般家中会开启多个门以供进出，像前门（人走的）、后门（送红包的人走的）、窗户（小偷走的）、烟囱（圣诞老人走的）……前面说过IP就像我们家中的住址一样，而端口就是网络通道上的门，它是信息出入的必经通道。

前面我们已经知道了对方的IP地址，但仅仅是查到了IP地址还不够，我们还需要了解对方开放了哪些端口，端口对于黑客来说，是个相当重要的参考资料，当黑客锁定目标之后，接着就是针对这个目标进行端口扫描，找出开放的端口有哪些。接着就可以一一开启测试，反正大门锁着打不开就走后门，后门打不开就试着爬上窗户，再不然就从烟囱进入，如此一一测试，总有一个进入的方法。

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，计算机上开启的端口数值范围为1～65535。

下表列出常用的几个端口。

端口号	用途
21	FTP（Pile Transfer Protocol，文件传送协议），提供文件传输服务。这个端口开放的话我们可以从FTP服务器上下载或上传资料等，有的还是匿名登录的，不过这样的好事现在好像不多了。
23	Telnet（远程登录协议），提供主机连机服务，这个端口开放的话表明远程登录服务正在运行，在这里你可以远程登录到该主机。
25	SMTP（Simple Mail Transfer Protocol，邮件传输协议），提供主机发信服务。
53	DNS（Domain Name Serve，域名服务器），提供域名解析服务
79	finger（查看机器的运行情况），finger服务对入侵者来说是一个非常有用的信息，利用它入侵者可以获得目标用户信息，查看目标机器的运行情况等。
80	HTTP（Hyper Text Transfer Protocol，超文本传送协议），提供网页浏览服务，它表明WWW服务在该端口运行
110	POP（Post Office Protocol，邮局协议）
139	NetBIOS服务（即共享服务），这个端口开启可以查看该机开放的共享（包括默认共享）
3389	终端服务端口，这个端口开放表明可以远程登录该主机

就如我们按图索翼找到了对方的住址，走近一幢住宅里，可以清清楚楚地看到每一户人家装了哪些门，端口跟IP一样是开放性的，当我们知道IP地址之后，就可以轻松得知该IP所开的端口有哪些了。

但是如果我们一个IP一个IP查，那就太费时间和精力了，因此，为了查找目标主机都开放了哪些端口，黑客们经常使用一些像PortScan、SuperScan这样的工具软件，对目标主机一定范围的端口扫描，因为这样就可以完全掌握目标主机的端口开放情况。

提示

这里需要提醒大家注意的是，在扫描别人最好先扫描一下自己的机器看看是否开启了不必要的端口，若是自己的计算机上有被莫名其妙打开的端口，那可要小心了！首先解决自己的问题，再去准备攻击别人吧，否则，当你抱着个扫描器到处扫描的时候，被有经验的黑客捉住，来个以牙还牙，恐怕你的机器先成了别人的肉鸡，或者先被攻瘫了，那还怎么攻别人？

这里以SuperScan为例来进行说明，Superscan是一款功能非常强大的扫描软件。

如果检测的时候没有特定的目的，只是为了了解目标计算机的一些情况，可以对目标计算机的所有端口进行检测。点击“扫描”选项卡，在“IP地址”栏输入起始IP和结束IP，再点击右侧的按钮将扫描地