学以致用

黑客攻防

从零到运用自如

附情景·互动式
多媒体教学光盘

神龙工作室 孙连三 编著

实战入门

从零开始 一学就会 任务驱动

全书涵盖入门者必须通过的7关

黑客入门关： 1章，了解黑客攻防相关的基础知识。
远程监控关： 3章，教你如何实施远程监控。
密码防盗关： 2章，教你如何防范密码被盗。
文件加密关： 1章，教你如何给重要文件加密。
系统安全关： 6章，提升系统的安全系数。
病毒防范关： 1章，快速查杀流行木马和病毒。
清除记录关： 1章，清除系统中的记录，防止隐私外泄。

谁适合学习这本书？

如果你是一个对黑客**不了解**的人。
如果你是一个对黑客攻击**束手无策**的人。
如果你是一个**不想成为“肉鸡”**的人。
如果你是一个想掌握**网络安全实用技术**的人。
如果你是一个想让自己的电脑**更加安全**的人。

人民邮电出版社
POSTS & TELECOM PRESS

学以致用

黑客攻防

实战入门

◉ 神龙工作室 孙连三 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

黑客攻防实战入门 / 孙连三编著. -- 北京 : 人民邮电出版社, 2009.10
（学以致用）
ISBN 978-7-115-21309-9

Ⅰ. ①黑… Ⅱ. ①孙… Ⅲ. ①计算机网络－安全技术
Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2009)第166173号

内 容 提 要

本书是指导初学者快速掌握黑客攻防的入门书籍，该书打破了传统按部就班讲解知识的模式，以解决问题为出发点，通过大量来源于实际的精彩实例，全面涵盖了读者在防御黑客攻击过程中所遇到的问题及其解决方案。全书共分 15 章，分别介绍黑客基础、扫描工具应用实战、远程控制的攻击与防范、屏幕监控攻防策略、管理员账户攻防策略、QQ/邮箱账号攻防策略、密码与数据恢复、设置注册表、设置组策略、设置本地安全策略、计算机管理策略、系统漏洞防范、巧用防护软件保护系统安全、快速查杀木马和病毒，以及清除系统中的历史记录等内容。

本书附带一张专业级多媒体电脑教学光盘，提供长达 4 个小时的精彩实例的多媒体教学内容，通过全程语音讲解、情景式教学等方式对书中知识点进行深入的讲解，一步一步地引导读者掌握黑客攻防的方法和技巧。此外赠送包含 200 个黑客攻防实用技巧的电子图书，全面帮助读者解决在防御黑客攻击和捍卫网络安全的过程中所遇到的问题。

本书既适合电脑初学者阅读，同时对有经验的网络安全爱好者也有较高的参考价值。

学以致用——黑客攻防实战入门

◆ 编　　著　神龙工作室　孙连三
责任编辑　马雪伶

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京顺义振华印刷厂印刷

◆ 开本：787×1092　1/16
印张：18
字数：459 千字　　2009 年 10 月第 1 版
印数：1- 5 000 册　　2009 年 10 月北京第 1 次印刷

ISBN 978-7-115-21309-9

定价：34.00 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

如今，Internet 已经深入人们日常生活和工作的各个角落，人们在享受网络带来的便利的同时，多数网民都在面临着不同程度的网络安全的威胁。为了帮助初学者提高防御黑客攻击的能力，满足他们学习电脑安全防护知识的迫切需求，我们组织了一批网络安全方面的专家，以解决问题为出发点，特别为电脑初学者量身定制了本书。

本书特色一览

任务驱动、自主学习：本书采用任务驱动的形式，对读者在预防黑客攻击过程中需要做的准备工作以及可能使用到的软件知识给予了详尽的介绍，读者可以根据自己的实际需求有选择地阅读。

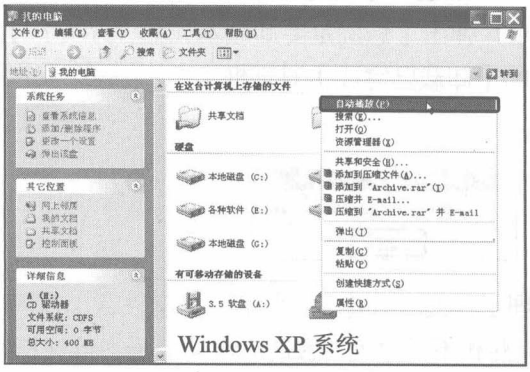
讲解全面、轻松入门：本书在挑选每个实例的过程中都兼顾了黑客攻防的各个方面，并且详细地介绍了黑客攻防常用软件的功能及特点，使读者在实际操作的过程中能够轻松地掌握黑客攻防技能及其相关软件的使用方法，读者可以将本书作为电脑安全防护的入门图书。

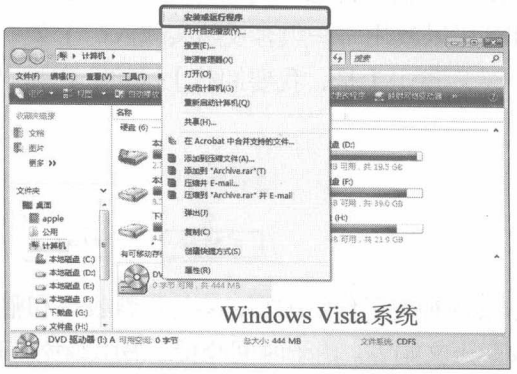
实例为主、易于上手：全面突破传统按部就班讲解知识的模式，模拟真实的工作环境，以实例为主导，将读者在黑客攻防过程中可能遇到的各种问题及其解决办法充分地融入到实际案例中，使读者能够轻松掌握黑客攻防的流程，解决各种疑难问题。

书盘结合、互动教学：本书附带一张多媒体电脑教学光盘。本光盘紧扣书中的内容，以实例的形式提供长达 4 个小时的视频讲解，使读者更易于理解和掌握各种知识。同时，光盘中还赠送包含 200 个黑客攻防的实用技巧的电子图书，帮助读者解决防御黑客攻击过程中所遇到的问题。

配套光盘运行方法

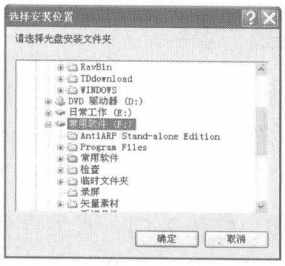
1. 将光盘印有文字的一面朝上放入光驱中，几秒钟后光盘就会自动运行。
2. 若光盘没有自动运行，在 Windows XP 操作系统下可以双击桌面上的【我的电脑】图标打开【我的电脑】窗口，然后双击光盘图标，或者在光盘图标上单击鼠标右键，从弹出的快捷菜单中选择【自动播放】菜单项，光盘就会运行；在 Windows Vista 操作系统下可以双击桌面上的【计算机】图标打开【计算机】窗口，然后双击光盘图标，或者在光盘图标上单击鼠标右键，从弹出的快捷菜单中选择【安装或运行程序】菜单项即可。





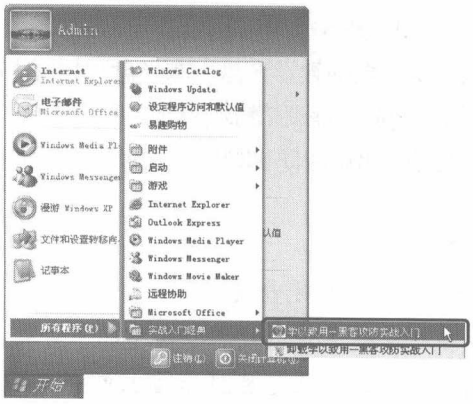
3. 由于光盘长期使用会损伤，旧光驱读盘的能力可能也比较差，因此最好将光盘内容安装到硬盘上观看，把配套光盘保存好作为备份。在光盘主界面中单击【安装光盘】按钮安装光盘，弹

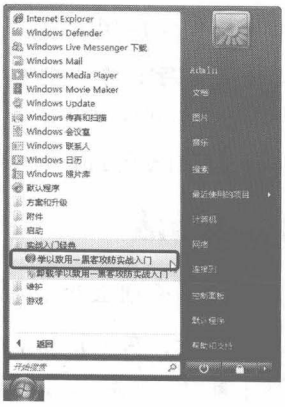
出【选择安装位置】对话框，从中选择合适的安装路径，然后单击 确定 按钮即可将光盘内容安装到硬盘中。



④ 以后观看光盘内容时，只要单击【开始】按钮（Windows XP：开始，Windows Vista：），然后在弹出的菜单中选择【所有程序】➢【实战入门经典】➢【学以致用——黑客攻防实战入门】菜单项就可以了。

Windows XP 系统

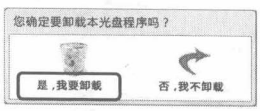


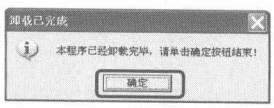


Windows Vista 系统

如果光盘演示画面不能正常显示，请双击光盘根目录下的 tscc.exe 文件，然后重新运行光盘即可。

如果以后想要卸载本光盘，则可在【开始】菜单中选择【所有程序】➢【实战入门经典】➢【卸载学以致用——黑客攻防实战入门】菜单项，弹出【您确定要卸载本光盘程序吗？】对话框，然后单击【是，我要卸载】链接，在弹出的【卸载已完成】对话框中单击 确定 按钮即可。



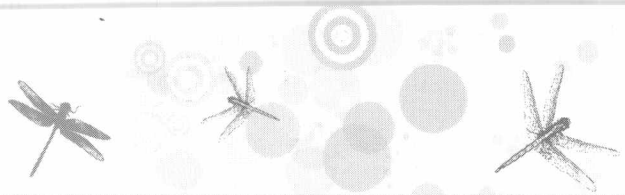


本书由神龙工作室编写，参与资料收集和整理工作的有孙连三、张彩霞、李轶君、郝凤玲、邓淑文、王文娟等。由于时间仓促，书中难免有疏漏和不妥之处，恳请广大读者不吝批评指正。

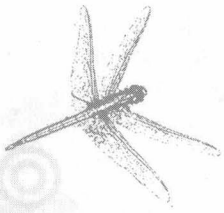
我们的联系信箱为 maxueling@ptpress.com.cn，欢迎读者来信交流。

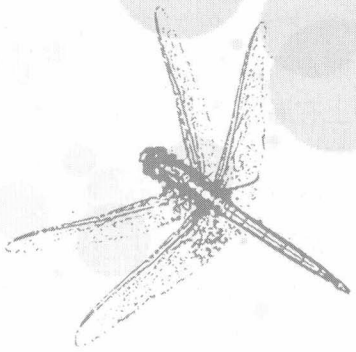
编 者

目 录



目 录



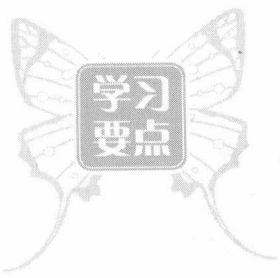


第 1 章 黑客基础

Chapter 1

随着网络技术的发展，如今人们的日常生活、工作和学习已经越来越离不开网络，互联网为计算机用户带来了极大的方便。但随之引发的网络安全问题也成了人们关注的焦点。

小王经常在一些计算机杂志上看到关于黑客的报道，黑客到底是一些什么样的人呢？



- 揭开黑客面纱
- 认识 IP 地址
- 设置端口
- 了解黑客常用命令

1.1 实例1——揭开黑客面纱

提起网络安全问题，人们便不由自主地联想到黑客，通常人们都会将他们和破坏网络安全、盗取网络账户等问题联系起来。在很多人眼里，黑客是神秘的，让人不可琢磨、难以接近的，下面就来揭开黑客的面纱，看看黑客到底是什么样的人。

黑客又被称为骇客，最早源自英文单词“hacker”，原指精通操作系统和网络技术，并善于利用专业知识编制新程序的人。

随着网络技术的发展和黑客工具的传播，一些人开始利用黑客工具对一些疏于防范的计算机进行攻击、破坏，例如监视他人计算机、偷窥他人隐私、盗取用户资料、入侵网络服务器等。这就不再属于黑客的范畴，而是属于犯罪活动了。在日常生活中，许多的网络安全故障也都出自黑客之手，例如某些网站无法访问、网上银行账户被盗等。

目前世界上有许多的黑客网站，这些网站都会介绍一些常用的攻击、防范技巧，并免费提供一些常用的攻击和防护软件供网友下载使用。现在，黑客技术已经被越来越多的人掌握，对于普通的计算机用户来说，了解了常用的黑客技术，就可以更好地保护自己的计算机免受恶意攻击。

1.2 实例2——认识IP地址

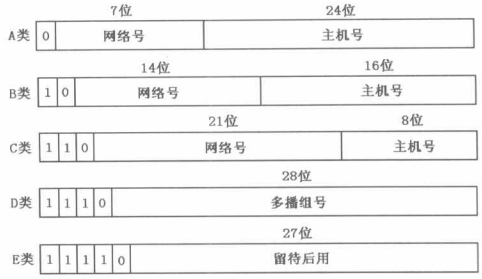
Internet 网络中的主机有很多，为了区分这些主机，人们为网络中的每台主机都分配了一个专门的地址，称为 IP 地址。

1. IP 地址的表示法

IP 地址由 4 个字节组成，每一个字节对应 8 位二进制位（即每部分数字不会超过 $2^8=256$），采用二进制形式记录的 IP 地址可以表示为“00010110001011001001000001010 1”。为了方便使用，IP 地址的每个字节通常被写成十进制的形式，中间用“.”分隔，这样就可以用 XXX.XXX.XXX.XXX 的形式来表示，其中每组“XXX”代表不大于 255 的十进制数，例如上面的 IP 地址就可以表示为 11.11.36.21。IP 的这种表示方法称为“点分十进制表示法”，这显然比二进制的 1 和 0 更容易记忆。

2. IP 地址的分类

一般情况下，可以将 IP 地址分为 5 大类。

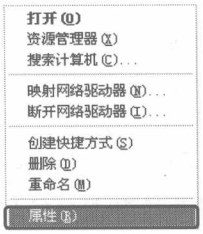


A 类地址以第 1 个字节为网络号，其范围为 1.0.0.1～126.255.255.254；B 类地址以前两个字节为网络号，其范围为 128.0.0.1～191.255.255.254；C 类地址以前 3 个字节为网络号，其范围为 192.0.0.1～223.255.255.254；D 类地址以前 4 个字节为网络号，其范围为 224.0.0.1～255.255.255.254；E 类地址保留为以后使用。而 127.0.0.1～127.255.255.254 这一地址段则保留作为本地软件环回测试本主机之用，

其中 127.0.0.1 就是指本机。

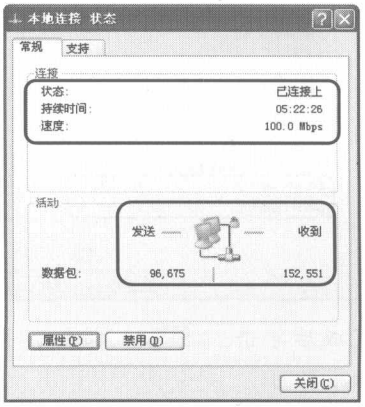
在局域网中查看/修改 IP 地址的具体步骤如下。

1 在桌面【网上邻居】图标上单击鼠标右键，从弹出的快捷菜单中选择【属性】菜单项。

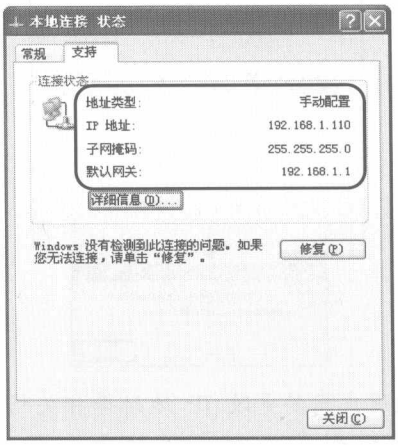


2 打开【网络连接】窗口，在【网络连接】窗口中双击【本地连接】图标，随即会打开【本地连接 状态】对话框。

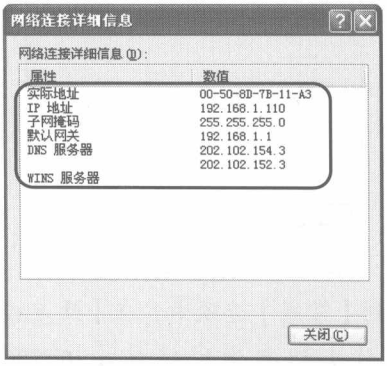
3 切换到【常规】选项卡，在【连接】组合框中显示了网络的连接状态、持续时间和速度。在【活动】组合框中可以看到数据包的发送和接收情况。



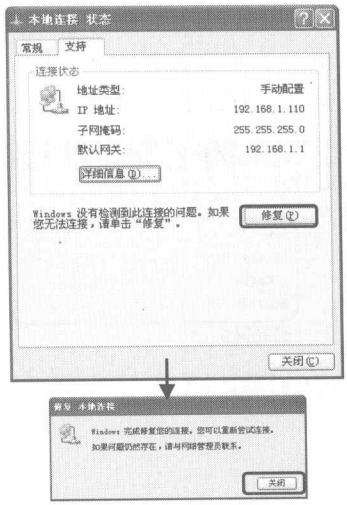
4 切换到【支持】选项卡，在【连接状态】组合框中显示了地址类型、IP 地址、子网掩码和默认网关的详细信息。



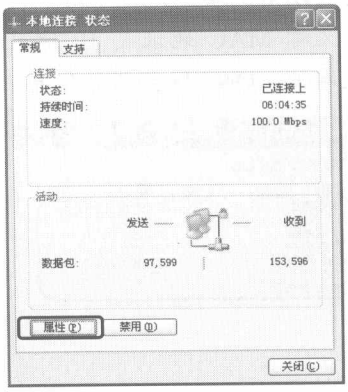
5 单击【连接状态】组合框中的 详细信息(D)... 按钮，打开【网络连接详细信息】对话框，在该对话框中可以看到实际地址（用户计算机的网卡地址，又称 MAC 地址）、IP 地址、子网掩码、默认网关、DNS 服务器等信息。



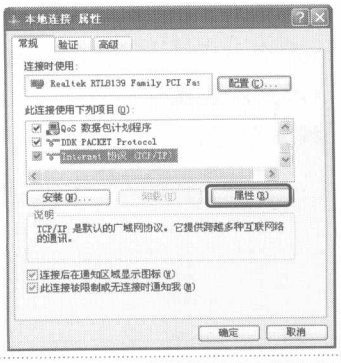
6 单击 关闭(C) 按钮返回【本地连接 状态】对话框，如果用户的网络出现无法连接的问题，可以先单击 修复(P) 按钮进行修复，修复完成后会打开【修复 本地连接】对话框，提示用户修复操作已经完成，此时单击 关闭 按钮即可。



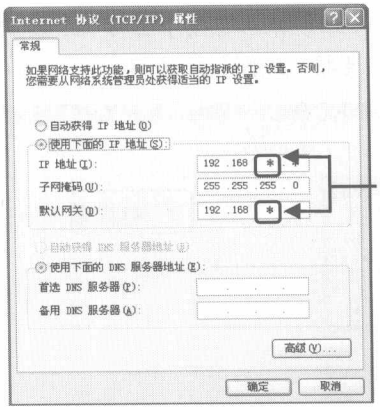
7 如果用户想要更改 IP 地址等相关信息，可以切换到【常规】选项卡，然后单击 属性(P) 按钮，随即会打开【本地连接 属性】对话框。



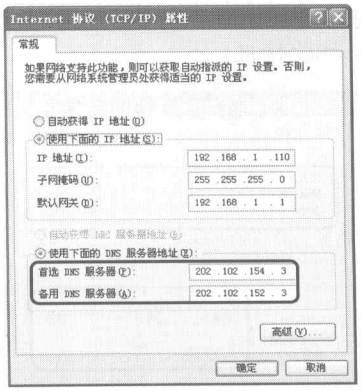
8 切换到【常规】选项卡，在【此连接使用下列项目】列表框中选择【Internet 协议（TCP/IP）】选项，然后单击 属性(R) 按钮。



9 随即打开【Internet 协议（TCP/IP） 属性】对话框中，在此即可设置 IP 地址和默认网关等信息。局域网中 IP 地址的格式一般为“192.168.*.*”，其中第 1 个“*”号代表用户的网段数，一个局域网中所有用户所处的网段是相同的，取值在 0～255 之间；第 2 个“*”号是该局域网用户的唯一标识，取值范围也是 0～255，用户可以使用此范围内的任何数字，但不能和局域网中的其他用户冲突，因为同一局域网中的每个 IP 地址是唯一的。默认网关的形式一般为“192.168.*.1”，其中“*”号和 IP 地址中的网段数是相同的。

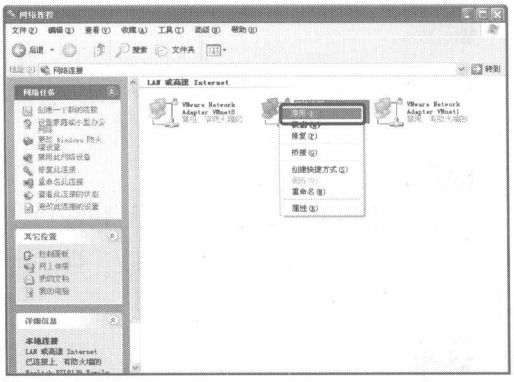


10 在【Internet 协议（TCP/IP） 属性】对话框中，首选 DNS 服务器和备选 DNS 服务器的地址信息是由当地的服务商提供的，不能随意填写。

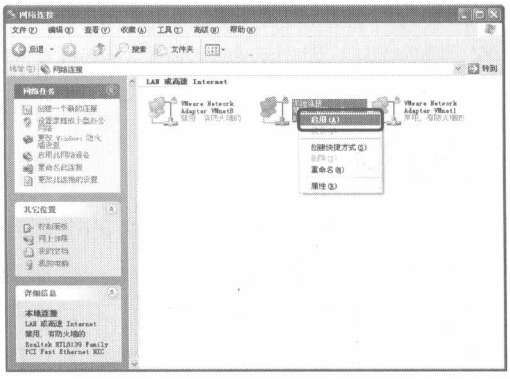


11 设置完成后单击 确定 按钮，关闭打开的对话框即可。

12 如果用户想要断开网络连接，在【网络连接】窗口中的【本地连接】图标上单击鼠标右键，从弹出的快捷菜单中选择【停用】菜单项即可。



13 开启网络连接的方法和停用网络连接的方法基本相同，只需在【网络连接】窗口中的【本地连接】图标上单击鼠标右键，从弹出的快捷菜单中选择【启用】菜单项即可。



1.3 实例3——设置端口

端口是计算机与外界进行通信交流的出口，主要分为硬件端口和软件端口两种。其中硬件端口又称为接口，分为串行接口和并行接口两种，其中串行接口主要有 USB、SATA 和 IDE 等，而平常使用的打印机接口就属于并行接口。软件端口一般指网络中面向连接服务和无连接服务的通信协议。

在网络技术中，端口大致有两种意思，一种是物理意义上的端口，例如 ADSL Modem、集线器、交换机、路由器等用于连接其他网络设备的接口；另一种是逻辑意义上的端口，一般是指 TCP/IP 中的端口，例如浏览网页服务采用的 80 号端口，FTP 服务采用的 21 号端口。下面介绍的是逻辑意义上的端口。

一般情况下，一台计算机最多有 65535 个端口，但实际上常用的端口只有十几个，可见未定义的端口相当多。黑客在入侵用户计算机之前通常会用扫描器对目标主机的端口进行扫描，以确定哪些端口是开放的，从开放的端口就可以知道目标主机大致提供了哪些服务，进而猜测可能存在的漏洞，然后利用技术手段侵入用户的计算机，从而对计算机进行控制。

1.3.1 了解端口的分类

计算机中的 65535 个端口按不同的分类标准可以分为很多类，其中最常用的分类标准有以下两种。

1. 按端口号分布划分

按端口号的分布可以将端口分为 3 类，分别是“公认端口”、“注册端口”和“动态和/或私有端口。

公认端口

公认端口（Well Known Ports）也称为“常用端口”，端口号从 0 到 1023，它们紧密地绑定于一些特定的服务。通常这些端口的通信明确地表明了某种服务的协议，这种端口不可再

重新定义它的作用对象。例如 21 号端口分配给了 FTP 服务，而 23 号端口是 Telnet 服务专用的，25 号端口分配给了 SMTP（简单邮件传输协议）服务，80 号端口是 HTTP 通信所使用的，135 端口分配给了 RPC（远程过程调用）服务，这些端口通常不会被如木马这样的黑客程序利用。

注册端口

注册端口（Registered Ports）的端口号从 1024 到 49151，它们松散地绑定于一些服务，大多数没有明确的定义服务对象，不同的程序可以根据实际需要自己定义，大多数的远程控制软件和木马程序都会有这些端口的定义，这些常见的程序端口在木马程序的防护和查杀上是非常有必要的。

动态和/或私有端口

动态和/或私有端口（Dynamic and/or Private Ports）的端口号从 49152 到 65535。理论上讲，不应为服务分配这些端口。但一些较为特殊的程序，特别是木马程序就非常喜欢使用这些端口，因为这些端口通常不被人们注意，容易隐蔽。

2. 按协议类型划分

端口的另一种分类标准是按协议类型划分，网络上常用的通信协议有两种，分别是面向连接的 TCP（传输控制协议）和面向无连接的 UDP（用户数据报协议），对应使用以上两种通信协议的服务所提供的端口，可以将计算机端口分为 TCP 端口和 UDP 端口。由于 TCP 和 UDP 是相互独立的，因此它们各自的端口号也相互独立，例如 TCP 有 235 号端口，UDP 也可以有 235 号端口，这两者是不冲突的。

使用 TCP 的常见端口主要有以下几种。

FTP

文件传输协议，使用 21 号端口，主要用于文件传输服务，例如上传和下载文件。

Telnet

远程登录协议，使用 23 号端口，用户可以以自己的身份连接到远程计算机上。

SMTP

简单邮件传输协议，使用 25 号端口，大多数的邮件服务器都采用这个协议，用于发送邮件。

POP3

它和 SMTP 相对应，用于接收邮件，通常情况下使用的是 110 号端口。

使用 UDP 协议的常见端口主要有以下几种。

HTTP

这是用户使用最多的协议，也就是人们常说的“超文本传输协议”。上网浏览网页时就是使用这个协议，提供 HTTP 服务需要开启 80 号端口。

DNS

用于域名解析服务。由于 IP 地址是纯数字形式的，不方便记忆，于是就出现了便于记忆的域名，但是计算机只能通过 IP 地址寻找要访问的主机，此时就需要将域名解析成 IP 地址，将域名解析成 IP 地址的工作就是由 DNS 服务器来完成的，该服务使用 53 号端口。

SNMP

简单网络管理协议，使用 161 号端口，主要用来管理网络设备。

QQ

QQ 客户端既可以发送信息又可以接收信息，其采用的是 UDP。它使用 8000 号端口侦听是否有数据到来，使用 4000 号端口向外发送数据。

在计算机的 6 万多个端口中，通常将端口号在 1024 以内的称为常用端口，这些常用端口所对应的服务通常都是固定的。

1.3.2　查看系统的开放端口

为了查找目标主机都开放了哪些端口，黑客会使用一些扫描工具对目标主机一定范围内的端口进行扫描，只有掌握了目标主机的端口情况，黑客才能进一步对目标主机展开攻击。通过了解系统开放端口的状态变化，可以帮助用户更好地保护系统，防范入侵。在 Windows XP 系统中，可以使用下面两种方法来查看端口状态。

1.　用 netstat 命令查看

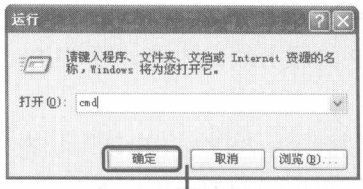
使用netstat命令查看端口状态的具体步骤如下。

❶选择【开始】➢【运行】菜单项，打开【运行】对话框。

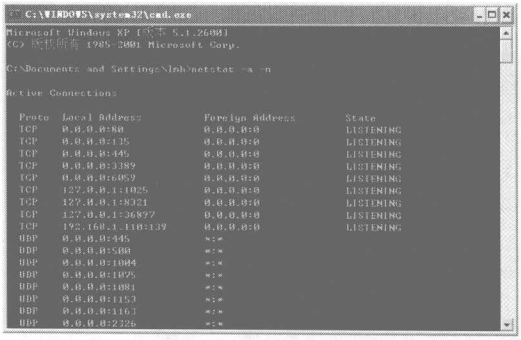
技　巧

按下键盘上的【Win】+【R】组合键，可以快速打开【运行】对话框。

❷在【打开】下拉列表文本框中输入“cmd”命令，然后单击 确定 按钮，随即打开【命令提示符】窗口。



❸在【命令提示符】窗口中输入“netstat –a –n”命令，然后按下【Enter】键即可看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态。



下面分析介绍【命令提示符】窗口中各项的具体代表含义。

“Proto”代表协议类型，从图中可以看出主要有 TCP 和 UDP 两种协议。

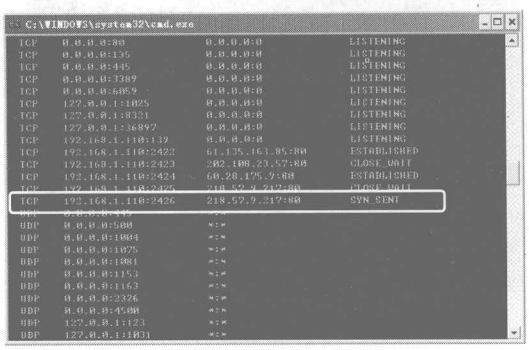
“Local Address”代表本地计算机的 IP 地址和连接正在使用的端口号。

“Foreign Address”代表连接本地端口的远程计算机的 IP 地址和端口号，如果正在和其他计算机进行通信，显示的就是对方计算机的地址。

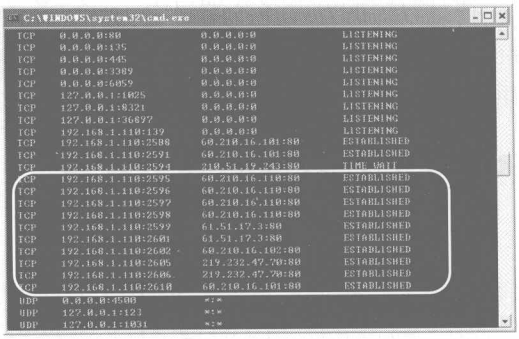
“State”代表运行状态，显示“LISTENING”表示处于监听状态，就是说该端口是开放的，

正等待连接，但还没有被连接，需要注意的是只有 TCP 的服务端口才能处于“LISTENING”状态。

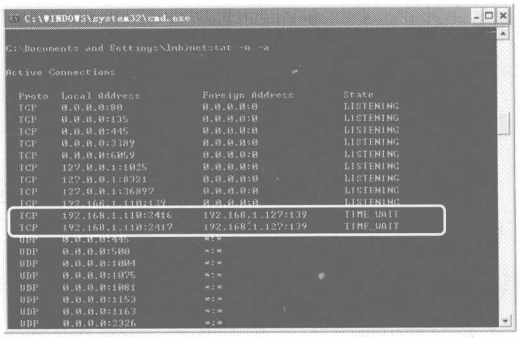
如果显示为“SYN_SENT”状态，表示本机正在向其他计算机发出连接请求，一般这个状态存在的时间很短。当用户要访问其他计算机的服务时首先要发送一个同步信号给该计算机的服务端口，此时就为“SYN_SENT”状态，如果连接成功就变为“ESTABLISHED”状态，因此“SYN_SENT”状态非常短暂。但是如果发现“SYN_SENT”状态非常多且在向多个不同的地址发送信号，那么用户的计算机很可能中了冲击波或者震荡波之类的病毒。这类病毒为了感染别的计算机，就会不停地进行扫描，在扫描的过程中对每个要扫描的计算机都会发出同步请求，这就是同时出现很多“SYN_SENT”状态的原因。



如果显示为“ESTABLISHED”状态，表示两个地址已经建立了连接，正在进行通信。如果用户访问的网站中有许多内容，就会发现一个地址会对应很多个“ESTABLISHED”状态，这是正常的，因为网站中的每个内容，比如图片、Flash 影片等都要单独建立一个连接。如果用户关闭了所有访问的网页及程序连接，然后多次在命令提示符窗口中运行“netstat –a –n”命令，始终有访问同一个网络 IP 地址的连接处于“ESTABLISHED”状态，则用户的计算机有可能已经中了木马。



如果显示为“TIME_WAIT”状态，表示结束本次连接，说明端口曾经有过访问。如果显示为“CLOSE_WAIT”状态，表示结束等待。



2. 使用 TCPView 软件查看

TCPView 是一款专门用来查看用户计算机端口开放状态的工具软件，其功能类似命令提示符下的“netstat –a –n”命令功能，但该软件小巧实用，其最大的特点是能够自动地实时刷新，当有新的端口被打开时会显示为绿色，当有端口被关闭时则显示为红色。