轻而易举

★**电脑学习轻松上手：** 创新的模块化学习结构，引领读者由浅入深、循序渐进地学习。

★**众多疑难迎刃而解：** 根据初学者的学习习惯和需求量身打造，帮你排忧解难。

★**快速提高易如反掌：** 只讲最需要掌握、最有实战价值的知识和技能，让你事半功倍。

★**学练结合举一反三：** 知识点巧妙融入众多实际案例中讲解，理论联系实际。

配套光盘包含数小时精彩视频教程，并附带超值赠品！

升级版

黑客攻防入门

吴玉梅　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

轻而易举

升级版

黑客攻防入门

吴玉梅 编著

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

内容简介

本书从黑客新手的需要和学习习惯出发，详细介绍了黑客基础知识、信息搜集与漏洞扫描、黑客常用命令与工具、Windows系统漏洞防范、密码攻防、远程控制攻防、木马攻防、网络攻防、QQ和E-mail攻防、防范计算机病毒、防范间谍软件与流氓软件等知识。

本书语言通俗易懂、版式清晰、图文并茂、脉络清晰且操作性强，采用“试一试+学一学+练一练+想一想”模式进行讲解，将知识介绍与实战练习相结合，使读者能够轻松上手。同时，本书还配有精彩实用的多媒体自学光盘，通过直观生动的视频演示帮助读者轻松掌握重点和难点。

本书既适合对电脑安全和电脑攻防感兴趣的用户自学，也适合网络管理人员参考学习。

图书在版编目（CIP）数据

黑客攻防入门：升级版 / 吴玉梅编著. — 北京 :电子工业出版社, 2013.2
（轻而易举）
ISBN 978-7-121-19273-9

Ⅰ. ①黑… Ⅱ. ①吴… 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（2012）第303973号

策划编辑：牛　勇
责任编辑：董　英
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
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：14.75　　字数：397千字
印　　次：2013年2月第1次印刷
定　　价：29.80元（含光盘1张）

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，联系及邮购电话：（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。

致 读 者

还在为不知如何学电脑而**发愁**吗？

面对电脑问题经常**不知所措**吗？

现在，**不用再烦恼了！**答案就在眼前。《轻而易举》丛书能帮助你轻松、快速地学会电脑的多方面应用。也许你从未接触过电脑，或者对电脑略知一二，这套书都可以帮助你**轻而易举地学会使用电脑**。

丛书特点

如果你想快速掌握电脑的使用，《轻而易举》丛书一定会带给你意想不到的收获。因为，这套书具有众多突出的优势。

专为电脑初学者量身打造

本套丛书面向电脑初学者，无论是对电脑一无所知的读者，还是有一定基础、想要了解更多知识的电脑用户，都可以从书中轻松获取需要的内容。

图书结构科学合理

凭借深入细致的市场调查和研究，以及丰富的相关教学和出版的成功经验，我们针对电脑初学者的特点和需求，精心安排了最优的学习结构，通过学练结合、巩固提高等方式帮助读者轻松快速地进行学习。

精选最实用、最新的知识点

图书中不讲空洞无用的知识，不讲深奥难懂的理论，不讲脱离实际的案例，只讲电脑初学者迫切需要掌握的，在实际生活、工作和学习中用得上的知识和技能。

学练结合，理论联系实际

本丛书以实用为宗旨，大量知识点都融入贴近实际应用的案例中讲解，并提供了众多精彩、颇具实用价值的综合实例，有助于读者轻而易举地理解重点和难点，并能有效提高动手能力。

版式精美，易于阅读

图书采用双色印刷，版式精美大方，内容含量大且不显拥挤，易于阅读和查询。

配有精彩、超值的多媒体自学光盘

各书配有多媒体自学光盘，包含数小时的精彩视频教程，学习知识更加轻松自如！光盘中还免费赠送电脑故障排除、电脑应用技巧和Office实用技巧等实用电子书，并部分光盘还附赠方便好用的应用软件。

阅读指南

《轻而易举》丛书采用了创新的学习结构，图书的各章设置了4个教学模块，引领读者由浅入深、循序渐进地学习电脑知识和技能。

试一试

学电脑是为了什么？当然是为了使用。可是，你知道所学的知识都是做什么用的吗？很多电脑用户都是在实际应用中学到了最有价值的知识。这个模块就是通过一个简单实例带你入门，让你了解本章要学习的知识在实际应用中的用途或效果，也起到了“引人入胜”的目的。

学一学

学习通常都是枯燥的，但是，《轻而易举》丛书打破了这个“魔咒”。通过完成一个个在使用电脑时经常会遇到的任务，使你在不知不觉中，已经掌握了很多必要的知识和技能。这个模块就是将实用的知识融入大大小小的案例，让读者在轻松的氛围中进行学习。

练一练

实践是最有效的学习方法，这个模块通过几个综合案例帮助读者融会贯通所学的重点知识，还会介绍一些提高性知识和小技巧。各案例讲解细致、效果典型、贴近实际应用，通常是用户使用电脑最经常用到的操作。

想一想

这个模块包括两部分内容：“疑难解答”就读者在学习过程中最常遇到的问题进行解答，所列举的问题大部分来源于广大网友的热门提问；“学习小结”帮助读者梳理所学的知识，了解这些知识的用途。

丛书作者

本套丛书的作者和编委会成员均是多年从事电脑应用教学和科研的专家或学者，有着丰富的教学经验和实践经验，这些作品都是他们多年科研成果和教学经验的结晶。本书由吴玉梅主编，参与本书编写的还有戴伟丽、陈瑜、张艺、黄元林、董路、唐波、龚平、叶德梅、潘远军、郭晓华、谭巧莲、梁礼燕、熊伟、彭敏等。由于作者水平有限，书中疏漏和不足之处在所难免，恳请广大读者及专家不吝赐教。

结束语

亲爱的读者，电脑没有你想象得那么神秘，不必望而生畏，赶快拿起这本书，投身于电脑学习的轻松之旅吧！

目　录

第1章　黑客基础知识

第2章　信息搜集与漏洞扫描

第11章 防范间谍软件与流氓软件

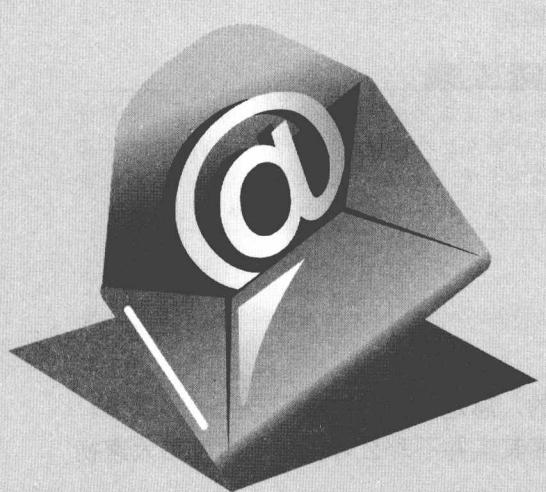
第1章

黑客基础知识

本章要点：

- 认识黑客
- IP地址与端口
- 了解系统服务
- 了解系统进程

Chapter 1



学生：老师，我的计算机经常被黑客攻击，你能教我怎么防范吗？

老师：当然可以呀，要想防御黑客攻击就需要了解一些黑客技术。

学生：老师，那你快给我讲解有关黑客的知识吧！

老师：好的，下面我就先给你讲解黑客的基础知识。

学生：太好了！

网络就像一把双刃剑，它在给我们带来便利的同时，也让我们的个人财产受到了病毒、木马以及恶意软件等的威胁。随着各种网络攻击的频繁出现，“黑客”这个名字已为广大计算机用户所熟知，然而很多人并不知道黑客的具体含义，以及其攻击的手段等，本章就为读者介绍黑客基础知识，带领大家走进黑客的世界。

试一试 1.1 查看计算机的端口 >>

案例描述 知识要点 素材文件 操作步骤

在Windows操作系统中，打开命令提示符窗口，然后通过执行netstat命令来查看系统中端口的开启和关闭状态。通过此例可以了解使用系统工具查看端口的方法。

案例描述 知识要点 素材文件 操作步骤

- 打开命令提示符窗口
- 执行命令，查看端口

案例描述 知识要点 素材文件 操作步骤

01 单击系统桌面左下角的“开始”按钮，在弹出的“开始”菜单的搜索框中输入“cmd”命令，然后按下“Enter”键，如图1.1所示。

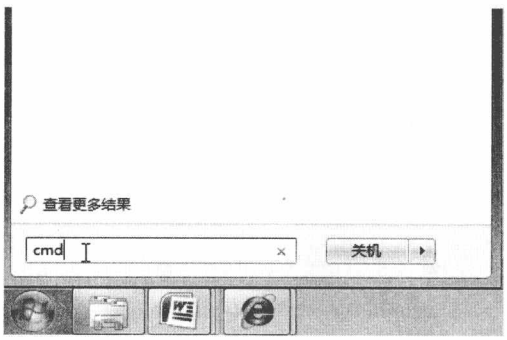


图1.1

02 在弹出的命令提示符窗口中输入“netstat -a -n”命令，按下“Enter”键，然后在接着出现的界面中即可查看当前计算机中端口的状态，如图1.2所示。

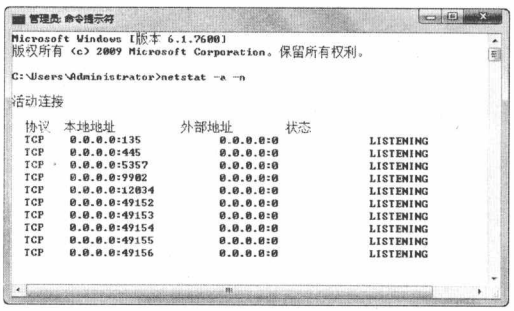


图1.2

提示

在Windows XP系统中可在“开始”菜单中单击“运行”命令，然后在弹出的“运行”对话框中进行上述操作。

提示

本地IP地址后列出的就是开放的端口号，如果计算机中的7626端口的状态显示为LISTENING（正在监听等待连接）状态，那么计算机极有可能是感染了冰河病毒，应马上断开网络，进行杀毒。

学一学 1.2 认识黑客 >>

黑客对于很多计算机用户来说是非常神秘的，总是由心底对他们产生一种畏惧。但是如果对黑客有一定的了解，我们会发现黑客其实并不那么可怕，下面就带大家初步认识黑客。

1.2.1 什么是黑客

黑客一词源于英文“Hacker”，原指热衷于计算机技术、水平高超的计算机专家，尤其是程序设计人员。这些人专注于研究系统漏洞和程序缺陷，他们不以入侵网络为乐趣，他们更多地致力于发现新的漏洞，并提出修补漏洞的方法，这类人被称为“白帽黑客”。

但到了今天，黑客一词已被用于泛指那些为了显示自己的本领和成就，以恶意入侵别人计算机进行破坏和信息窃取为目的的群体，这些人其实应该被称为“Cracker”，即“骇客”。这类人以利用自己掌握的技术入侵网络中的计算机为乐趣，网络上被骇客入侵的计算机被他们称为“肉鸡”。一旦他们入侵了某台计算机，他们就取得了这台计算机的绝对控制权，可以随意对系统进行破坏并窃取数据等。

1.2.2 黑客常用的攻击手段

黑客攻击手段可分为非破坏性攻击和破坏性攻击两大类。非破坏性攻击一般只是为了扰乱系统的运行，并不盗窃系统资料，通常采用拒绝服务攻击或信息炸弹等方式；破坏性攻击以入侵他人计算机系统、盗窃系统保密信息、破坏目标系统的数据为目的。下面介绍几种黑客常用的攻击手段。

网络嗅探与监听

网络嗅探其实最开始是应用于网络管理的，就像远程控制软件一样。但是，随着黑客技术的进步，这些强大的功能就开始被黑客们所利用。最普遍的安全威胁来自内部，同时这些威胁通常是致命的，且破坏性也非常大。很多黑客使用嗅探器进行网络入侵渗透。

提示

网络嗅探器对信息安全的威胁来自其被动性和被干扰性，使得网络嗅探具有很强的隐蔽性，这也让网络信息的泄密变得不容易被发现。

网络监听是一种监视网络状态、数据流以及网络上传输信息的管理工具，它可以将网络接口设置为监听模式，并且可以截获网上传输的信息。也就是说，当黑客登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听可以有效地截获网上的数据，这是黑客使用最多的方法，但是，网络监听只能应用于物理上连接于同一网段的主机，通常被用于获取用户口令。

应用基层攻击

应用基层攻击能够使用多种不同的方法来实现，最平常的方法是使用服务器上可找到的应用软件（例如SQL Server、Sendmail和FTP等）的缺陷。通过使用这些缺陷，攻击者能够获得计算机的访问权，以及在该计算机上运行相应程序所需的账户许可权等。

后门程序

由于程序员设计一些功能复杂的程序时，一般采用模块化的程序设计思想，将整个项目分割为多个功能模块分别进行设计、调试，这时的后门就是一个模块的秘密入口。在程序开发阶段，后门便于测试、更改和增强模块功能。正常情况下，完成设计之后需要去掉各个模块的后门，不过有时由于疏忽或者其他原因（如将其留在程序中，便于日后访问、测试或维护）后门没有被去掉，一些别有用心的人会利用“穷举搜索法”发现并利用这些后门，然后进入系统并发动攻击。

拒绝服务

“拒绝服务”又叫分布式DOS攻击，它是使用超出被攻击目标处理能力的大量数据包消耗系统的可用内存、带宽资源，最后导致网络服务瘫痪的一种攻击手段。攻击者通过常规的黑客手段侵入并控制某个网站，然后在服务器上安装并启动一个可由攻击者发出的特殊指令来控制的进程，攻击者把攻击对象的IP地址作为指令下达给进程的时候，这些进程就开始对目标主机发起攻击。这种方式可以集中大量的网络服务器带宽，对某个特定目标实施攻击，因而威力巨大，顷刻之间就可以使被攻击目标带宽资源耗尽，导致服务器瘫痪。比如1999年美国明尼苏达大学遭到的黑客攻击就属于这种方式。

信息炸弹

信息炸弹是指使用一些特殊工具软件，短时间内向目标服务器发送大量超出系统负荷的信息，造成目标服务器超负荷、网络堵塞、系统崩溃的攻击手段。比如向没有安装补丁的Windows系统发送特定组合的UDP数据包，会导致目标系统死机或重启；向某型号的路由器发送特定数据包致使路由器死机；向某人的电子邮箱发送大量的垃圾邮件将此邮箱“撑爆”等。目前常见的信息炸弹有邮件炸弹、逻辑炸弹等。

IP地址欺骗

IP地址欺骗攻击是黑客们假冒受信主机对目标进行的攻击。在这种攻击中，受信主机指的是拥有管理控制权限的主机或明确做出“信任”决定允许其访问自己网络的主机。通常，这种IP地址欺骗攻击局限于把数据或命令注入到客户机/服务器应用之间，或对等网络连接传送中已存在的数据流。为了达到双向通信，攻击者必须改变指向被欺骗IP地址的所有路由表。

1.3 IP地址与端口

IP地址和端口是计算机中不可或缺的两个部分。IP地址是一台连接到Internet中的计算机的标识，通过它可以轻松地找到目标主机；端口是为计算机提供服务的大门，黑客通常会通过开启某些端口来提高权限。本节将为读者介绍IP地址和端口的基础知识。

1.3.1 IP和IP地址

IP是英文Internet Protocol（网络之间互连的协议）的缩写，中文简称为“网协”，也就是为计算机网络相互连接进行通信而设计的协议。在Internet中，它是能

使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在Internet上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只要遵守 IP协议就可以与Internet互连互通。

IP地址是按照网络协议给每个连接在Internet上的主机分配的一个32bit的标识符（IPv4是32bit，IPv6是128bit。本书后面提到的IP地址除非特别声明，否则均指IPv4）。按照TCP/IP协议规定，IP地址用二进制来表示，每个IP地址长32bit，比特（bit）换算成字节，就是4个字节。例如一个采用二进制形式的IP地址是“00001010000000000000000000000001”，这么长的地址，人们处理起来也太费劲了。为了方便人们的使用，IP地址经常被写成十进制的形式，中间使用符号“.”分隔不同的字节。于是，上面的IP地址可以表示为“10.0.0.1”。IP地址的这种表示法叫做“点分十进制表示法”，这显然比二进制的1和0的形式容易记忆得多。

提示

TCP/IP（Transmission Control Protocol/Internet Protocol）的简写，中文译名为传输控制协议/因特网互联协议，又叫网络通信协议，这个协议是Internet最基本的协议，是Internet国际互联网络的基础，简单地说，就是由网络层的IP协议和传输层的TCP协议组成的。

1.3.2 端口的分类 >>>

计算机中的“端口”是英文“port”的意译，可以认为是计算机与外界通信交流的出口。其中硬件领域的端口又称接口，如USB端口、串行端口等。软件领域的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端口，是一种抽象的软件结构，包括一些数据结构和I/O（基本输入/输出）缓冲区，这类端口也是黑客们入侵计算机的途径之一。

注意

硬件领域的端口不会被黑客利用，进而攻击计算机，所以本书后面提到的“端口”均指软件领域的端口。

在一台计算机中最多有65535个端口，我们可以按照端口号将它们划分为以下三类。

- **公认端口（Well Known Ports）：**从0到1023，它们紧密绑定（binding）于一些服务。通常这些端口的通信明确表明了某种服务的协议。例如，80端口实际上总是用于HTTP通信。
- **注册端口（Registered Ports）：**从1024到49151，它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他目的。例如，许多系统处理动态端口从1024左右开始。
- **动态和/或私有端口（Dynamic and/or Private Ports）：**从49152到65535。理论上，不应为服务分配这些端口。实际上，机器通常从1024起分配动态端口。但也有例外，SUN的RPC端口从32768开始。

1.3.3 扫描端口 >>>

在前面的学习中我们提到过使用netstat命令可以查看计算机系统中的端口状态，此外我们还可以使用第三方软件来对系统中的端口进行扫描，然后在扫描结果中查看端口的状态，例如TCPView端口查看器，其使用方法如下。

01 下载并启动TCPView端口查看器程序，在打开的主界面的网络连接显示框中，会显示所有进程的网络连接，包括病毒建立的由内到外的TCP连接，并且这些连接信息会实时进行动态变化，显示出详细的TCP连接参数信息，如图1.3所示。

提示

该对话框中显示的信息包括进程名、进程ID、本地地址和端口号、远程地址和端口号等信息。通过TCPView程序，我们可以很轻松地分析出每个TCP连接的情况。

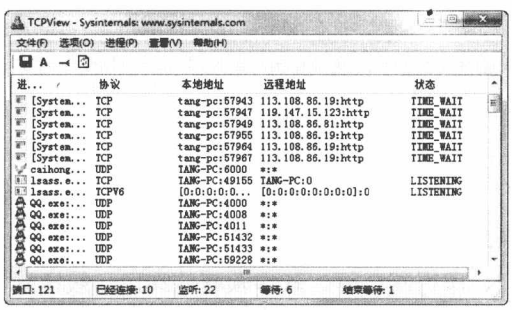


图1.3

02 在使用TCPView软件查看端口信息时，如果发现程序窗口中有熟悉的进程名，并且这个进程名的TCP连接数量非常多，变化频率也很快，这就说明这些TCP连接很可能是病毒建立的恶意TCP连接。为了防止病毒蔓延和传播，应记录下病毒进程使用的本地端口号。

03 使用鼠标右键单击不明进程，在弹出的菜单中单击“结束进程”命令，结束病毒由内到外的TCP连接，然后关闭前面记录下的端口（具体关闭方法将在后面的讲解中具体介绍）即可，如图1.4所示。

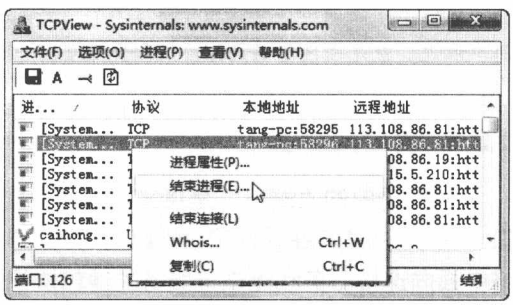


图1.4

1.3.4 限制端口

除了可以通过禁用服务来关闭端口外，还可以通过设置IP安全策略来限制相应的端口，以阻止他人访问该端口。下面以限制3389端口为例进行介绍，具体操作方法如下。

01 在“控制面板”窗口中单击“管理工具”链接，如图1.5所示。

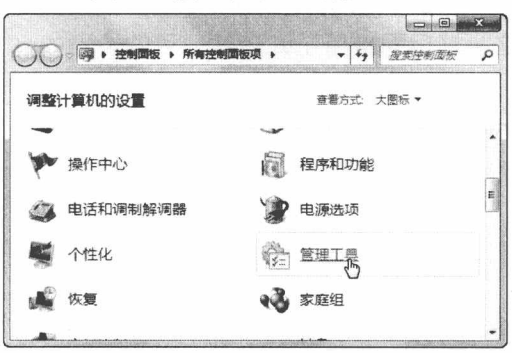


图1.5

02 在打开的“管理工具”窗口中双击“本地安全策略”选项，如图1.6所示。

图1.6