无师自通

双色版

多媒体教学光盘

书中内容的课堂式讲解、疑难问题解答，以及大量实战技巧

黑客攻防实战

星光科技 编著

图书特色

本套书采用“左边是操作步骤，右边是图片”的写作方式，配合由浅入深的教学内容，从而达到轻松学习、快速上手，没有老师也可以自己学会的目的

售后服务

在“图书+光盘”互动教学基础上，提供“网站+答疑电话+QQ群”三位一体的售后服务

- 学习网站：http://www.coolpen.org
- 答疑电话：028-87655295
- QQ群：51542728

人民邮电出版社
POSTS & TELECOM PRESS

无师自通

黑客攻防实战

星光科技 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

无师自通．黑客攻防实战／星光科技编著．—北京：人民邮电出版社，2008.7

ISBN 978-7-115-18087-2

Ⅰ．无… Ⅱ．星… Ⅲ．计算机网络—安全技术 Ⅳ．TP3

中国版本图书馆 CIP 数据核字（2008）第 063348 号

内 容 提 要

本书是“无师自通”丛书之一，针对初学者的需求，从零开始、系统全面地讲解了有关黑客的基础知识、Windows 操作系统漏洞的攻击与防护、网站系统漏洞的攻击与防护，以及木马的植入与清除的方法与操作技巧。

全书共分为 10 章，主要内容包括：黑客基础知识入门、系统漏洞攻防、信息搜索和扫描与远程控制、木马的植入与清除，还介绍了网络安全防范、网站脚本攻击的安全防范、IIS 系统漏洞的安全防范，以及系统与文件加密、信息隐藏与后门清理和查杀病毒与网络防范的方法等。

本书内容翔实、通俗易懂，实例丰富、步骤详细，图文并茂、以图析文，情景教学、生动有趣，版式精美、阅读轻松，双色印刷、重点突出，配套光盘、互动学习。

本书及配套多媒体光盘非常适合初学黑客知识的人员选用，也可作为高职高专相关专业和电脑短训班的培训教材。

无师自通——黑客攻防实战

◆ 编　　著　星光科技

责任编辑　刘建章

◆ 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

北京精彩雅恒印刷有限公司印刷

新华书店总店北京发行所经销

◆ 开本：787×1092　1/16

印张：12

字数：305 千字　　2008 年 7 月第 1 版

印数：1－8 000 册　　2008 年 7 月北京第 1 次印刷

ISBN 978-7-115-18087-2/TP

定价：24.80 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

前言

“无师自通”丛书是人民邮电出版社精心打造的系列品牌图书，该丛书自出版以来，以其实用、易学的特点深受广大读者的喜爱。

全新出版的“无师自通”丛书采用“左边是操作步骤、右边是图片”的双色、双栏排版方式，配合由浅入深、循序渐进的教学内容和简练的文字提示，使读者能够按照书中所述实际演练，达到轻松学习、快速上手，没有老师也可以达到自己学会的目的。

随书配有交互式多媒体教学光盘，光盘内容包括：书中内容的课堂式讲解、扩充读者知识面的电子图书、与本书内容密切相关的问题解答和实战技巧。

本套丛书还开设了“无师自通”专题学习网站（http://www.coolpen.org）、专题讨论 QQ 群（51542728）和专线答疑电话（028-87655295），在“图书+光盘”互动教学的基础上，提供“网站+QQ 群+电话”三位一体的售后服务。

丛书主要特色

- 表格编排 版式新颖
- 文图对照 方便阅读
- 内容精选 实用够用
- 书盘配合 互动学习
- 边学边练 快速上手
- 电子图书 扩充内容
- 网站教学 答疑解惑
- 双色印刷 突出重点

丛书主要内容

作为一套面向初级电脑用户、全新出版的丛书，“无师自通”是一套覆盖面非常广的丛书，知识体系比较全面。

从计算机知识的大众化普及到入门读者的必备技能，从生活娱乐到工作学习，从软件操作到行业应用；无论是一般性了解与掌握，还是进一步深入学习，读者都能在“无师自通”丛书中找到适合自己学习的图书。“无师自通”丛书已出版书目如下表所示。

无师自通——电脑打字	无师自通——笔记本电脑综合应用
无师自通——五笔打字	无师自通——网上冲浪
无师自通——电脑入门（Windows 98 版）	无师自通——网上炒股
无师自通——电脑入门（Windows XP 版）	无师自通——电脑组装与维护
无师自通——电脑入门（Windows Vista 版）	无师自通——系统安装与重装
无师自通——电脑操作（Windows XP 版）	无师自通——Office 2003 电脑办公
无师自通——电脑操作（Windows Vista 版）	无师自通——Office 2007 电脑办公
无师自通——电脑入门（老年版）	无师自通——Excel 2007 电子表格制作
无师自通——家用电脑综合应用	无师自通——Excel 2007 函数、公式与图表应用

续 表

无师自通——黑客攻防实战	无师自通——Dreamweaver CS3 网页制作
无师自通——电脑常见故障诊断与排除	无师自通——Flash CS3 动画制作
无师自通——数码摄影与数码相片修饰	无师自通——AutoCAD 2008 辅助绘图
无师自通——Photoshop CS3 图像处理	无师自通——Dreamweaver、Fireworks、Flash 网页制作

本书主要内容

《无师自通——黑客攻防实战》一书主要针对初学者的需求，精心安排了 10 章内容，从零开始、系统全面地讲解黑客攻防等方面的基础知识，同时还在书中提出了各种疑难问题与操作技巧。

全书章目	主要内容
第 1 章 黑客基础知识入门	通过对黑客认识、端口知识、常用命令、常用入侵方式和常用工具的介绍，让读者对黑客有个感性的认识
第 2 章 系统漏洞攻防	介绍了 Windows 系统安全解析、本地提权类漏洞攻防、Windows 系统用户交互类漏洞、Windows 系统的远程溢出漏洞和电脑安全防护策略等内容
第 3 章 信息搜索、扫描与远程控制	讲解了搜索网络电脑信息、使用 MBSA 扫描端口及检测系统的方法，介绍了远程控制技术
第 4 章 木马的植入与清除	重点介绍有关木马的知识，包括木马知识快速入门、木马种植方法和木马的清除与防范
第 5 章 网络安全防范	介绍网络炸弹防范、IE 浏览器漏洞的安全防范、网络聊天软件安全防范以及电子邮件安全防范
第 6 章 网站脚本攻击的安全防范	介绍脚本攻击的类型特点、网站管理系统账号与安全防护、网络论坛与安全防护、跨站 Script 安全防护和常见脚本攻击安全防护
第 7 章 IIS 系统漏洞的安全防范	主要介绍 IIS 系统的漏洞攻防，包括：Unicode 漏洞与安全防范、缓冲区溢出漏洞与安全防范、IIS 错误解码漏洞与安全防范，以及 IIS 服务器与安全防范
第 8 章 系统与文件加密	介绍了 BIOS 加密、系统登录加密、常用电脑加密设置、驱动器加密、办公软件加密、文件夹与文件加密和常用加密软件
第 9 章 信息隐藏与后门清理	隐藏是黑客攻击的重要部分，主要介绍文件传输与文件隐藏技术、扫描技术、入侵隐藏技术、后门和清除痕迹
第 10 章 查杀病毒与网络防范	主要讲解常用防护软件的使用，包括：使用卡巴斯基 7 查杀病毒、使用 Norton AntiVirus 查杀病毒、使用天网防火墙和使用 360 安全卫士维护系统安全

本书学习方法

我们在编写本书时，非常注重初学者的认知规律和学习心态，每章都安排了“内容导航”、“学习要点”、“本章小结”、“巩固练习”等栏目和内容，让读者可以更加高效地学习。

- 内容导航——在每章的首页，简明扼要地介绍了本章将要学习的重要内容。
- 学习要点——本章主要知识点、重点和难点的学习提示。
- 本章小结——对本章所讲知识进行更准确、更全面的概括，完成对新概念、新知识、重点、难点、操作步骤和应用技巧的总结回顾。
- 巩固练习——通过相关练习题，温习并巩固本章所学的内容，力求达到举一反三的目的。

本书在编排体例上，注重初学者在学习过程中那种想抓住重点、举一反三的学习心态，每章的正文中还安排了“你知道吗？”、“看技巧呢！”、“注意点哦！”、“练一练啦！”、“光盘链接”、“网站链接”等栏目和内容，让读者可以更加轻松地学习。

- 你知道吗？—— 对相关内容的知识补充、解释或说明。
- 看技巧呢！—— 让读者快速掌握常见的简便方法或操作技巧。
- 注意点哦！—— 提醒初学者需要掌握的重要知识、操作要点及注意事项。对初学者在学习和使用电脑过程中遇到的问题进行专家级指导与经验传授。
- 练一练啦！—— 让读者通过自己动手练习来强化学习效果，相关练习在光盘中有比较详细的具体操作方法或步骤。
- 光盘链接 —— 针对部分重点、难点或图书中没有讲解到的知识点，提醒读者阅读光盘中的多媒体教学、互动练习或电子图书。
- 网站链接 —— 针对部分重点、难点或图书中没有讲解到的知识点，提醒读者学习网站上的相关内容。

配套光盘说明

本书配套交互式、多功能、超长播放的多媒体教学光盘，既是与图书内容互补的多媒体教学光盘，又是一套具备完整教学功能的电脑学习软件，既可以轻松自学，又可以互动学习。配套光盘具有以下特色。

- 功能强大、使用方便：具有情景对话、背景音乐更换、调节音量、光盘目录、安装光盘等众多功能模块，功能强大、界面美观、使用方便。
- 情景教学、生动有趣：配套光盘通过老师、学生和小精灵 3 个卡通人物真实再现学习过程，情景教学、生动有趣。
- 互动教学、直观实用：读者可跟随光盘的提示，在光盘演示中执行如单击、双击、输入、拖动等操作，实现现场互动教学的模拟形式，直观实用。
- 跟练教学、边学边练：可将光盘切换成一个文字演示窗口，读者可以根据文字说明和语音讲解的指导，在电脑中进行同步跟练操作，边学边练。

专题网站说明

“无师自通”丛书还开通了专题学习网站（http://www.coolpen.org）。“无师自通”专题学习网站以图书和光盘的教学内容为基础，更好地为读者提供完善的教学服务支持，提供一个很好的电脑学习平台。专题学习网站包括以下几个功能板块。

- 视频教学：通过视频教学内容、多媒体教学内容和交互式教学内容，为广大读者提供一个轻松、快速学习电脑知识的视频教学库。
- 网上教程：通过网上教程、问题解答、操作技巧和实践案例等内容，为广大读者提供一个轻松、快速学习电脑知识的网上教程库。
- 资料下载：这里提供丛书相关的素材、效果图、动画、案例、源代码和课后习题答案等给读者下载。
- 互动交流：这里提供一个交流心得、解答疑难的互动交流平台，通过答疑电话、在线论坛、E-mail 和 QQ 群等方式及时解答读者在学习过程中遇到的各种问题。
- 联系我们：这里有我们的详细联系方式，读者如有问题，可以随时获得帮助。

答疑电话与 QQ 群

现已开通“无师自通”丛书专线答疑电话：028-87655295，在周一到周五工作日内（节假日除外），读者有问题可以在 09:00～18:00 上班时间与我们取得联系，我们将及时给予解答。

现已开通“无师自通”丛书专题讨论 QQ 群：51542728，在周一到周五工作日内（节假日除外），读者有问题也可以在 09:00～18:00 上班时间与我们在线讨论、交流。

本书由星光科技集体创作，参与编写的人员有许明、刘贵洪、李林、曾全、叶俊、余兰平、邱凤尧、刘彬、张海波、周芳、代峥、王媛、张璇、王礼龙、许起琴、刘正红、吴晨超、沈兆龙、吴锦锦、李从英、赵鸿洲、李明、邓子军、韦晓亮等。

由于时间仓促和水平有限，书中难免有疏漏和不妥之处，敬请广大读者和专家批评指正，来函请发电子邮件至：liujianzhang@ptpress.com.cn（责任编辑）、mook@vip.sina.com（编者）。

编者

2008 年 5 月

目 录

第 1 章 黑客基础知识入门

第 2 章 系统漏洞攻防

第 3 章 信息搜索、扫描与远程控制

第 4 章 木马的植入与清除

第 5 章 网络安全防范

第 6 章　网站脚本攻击的安全防范

第 7 章　IIS 系统漏洞的安全防范

第 8 章　系统与文件加密

第 9 章 信息隐藏与后门清理

第 10 章 查杀病毒与网络防范

黑客攻防实战

第 1 章 黑客基础知识入门

内容导航

在大多数人看来，黑客都是一个个神秘莫测的电脑高手，他们通过相关的电脑和网络强行侵入别人的电脑，并且肆意对电脑信息进行修改和窃取。同时，黑客和黑客技术对大多数网民而言也显得非常模糊。

本章将带领大家走入黑客世界，揭开黑客的神秘面纱，让大家了解有关黑客的一些基本知识。通过本章的学习，可使读者对黑客有初步的认识。

学习要点

- 浅谈黑客知识
- 黑客通道——端口
- 黑客常用的命令
- 黑客常用入侵方式
- 黑客常用工具

1.1 浅谈黑客知识

下面为大家介绍黑客的概念、黑客的具体行为、常用操作手段和攻击他人电脑的具体流程等知识。

1.1.1 认识黑客

黑客的英文名为“Hacker”，源于英语动词“Hack”，意为“劈、砍”，引申为“干了一件非常漂亮的工作”。现在提到的黑客一般泛指的是通过高级技术和巧妙手法侵入他人电脑系统的

人。黑客往往掌握了硬件和软件的高级知识，并有一定的能力通过创新的方法剖析系统，他们以保护网络为目的，而以不正当侵入为手段找出网络漏洞。

网络中还有一种利用网络漏洞破坏网络的入侵者，他们也具备广泛的电脑知识，但与黑客不同的是他们通常以破坏、窃取或恶作剧为目的进入他人的电脑，对电脑用户造成不同程度的损失，这些群体被称为“Cracker”，中文译音为“骇客”。

黑客与骇客在本质上虽然有很大的区别，但人们普遍认为黑客就是那些为了个人目的而擅自侵入和破坏别人电脑系统的人。本章就将为大家介绍这些入侵原理和途经，以及如何防范这类恶意攻击的方法。

1.1.2 黑客行为

黑客行为是指黑客进入他人电脑系统后进行的破坏行为，同时黑客往往也需要对这些黑客行为造成的损失承担相应的责任。黑客行为一般有以下几种。

1. 盗窃资料

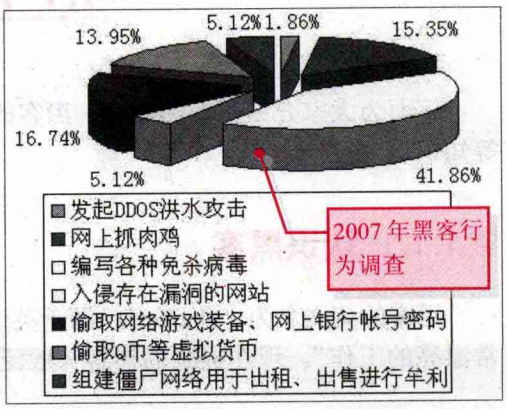
这里指的资料一般来说都是保密资料，因此根据资料的不同性质，黑客需承担的责任也不同。如果盗窃的是国家机密资料，那么就构成了犯罪，需要按国家法律承担相应的法律责任；如果通过黑客手段盗窃其他单位的技术或商业秘密，那么将有可能构成侵犯商业秘密罪；如果盗窃的是普通保密资料，也可能因为侵犯商业秘密而承担民事赔偿责任。

2. 攻击网站

黑客攻击他人的网站后，往往造成网络堵塞、其他人无法访问该网站的后果，这样就会对被攻击的网站造成损失。不管是出于竞争的目的或恶意攻击，还是出于恶作剧心理故意造成他人网站堵塞，黑客都将为对该网站造成的损失进行赔偿。如果是大型交易网站，网络堵塞造成的损失将是巨大的，因此黑客也将面临巨额的赔偿。

3. 进行恶作剧

这里的恶作剧是指黑客进入别人网站后，将其首页更换成其他图片，或将重要内容进行删除和修改等。黑客在制造这些恶作剧时虽然没有真正想攻击他人网站的意图，但同样也会对这些网站造成一定的损失，因此黑客需要承担相应的民事赔偿责任。



4. 告知漏洞

还有一些黑客非法侵入他人网站，查看网站信息后不做任何更改，又退出该网站，然后向网站邮箱发送邮件，告知其网站安全有漏洞。

黑客行为有很多，造成的影响和损失也与行为的性质有关，不过，不管是哪种行为，黑客都应对其相应的行为承担责任。

1.1.3 黑客常用攻击手段

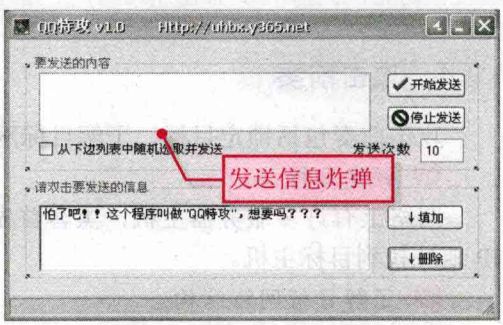
黑客攻击电脑系统的手段可分为非破坏性攻击和破坏性攻击两类。非破坏性攻击一般只是扰乱系统的正常运行，并不盗窃系统资料，通常采用拒绝服务攻击或信息炸弹手段实现；破坏性攻击往往是以侵入他人电脑系统、盗窃系统保密信息和破坏目标系统的数据为目的的攻击性黑客行为。下面为大家介绍几种常见的黑客攻击手段。

1. 后门程序

后门程序是指程序员在设计功能复杂的程序过程中，将整个项目分割为多个功能模块分别进行设计和调试时这些模块的秘密入口。采用模块化的程序设计思想进行程序开发阶段，通过后门程序可以有效地测试、更改和增强模块功能。在正常情况下，完成设计之后都会去掉各个模块的后门程序，不过有时由于疏忽或者其他原因后门程序没有去掉，因此一些别有用心的人就会采用各种穷举搜索法发现并利用这些后门程序，从而进入系统并发动攻击。

2. 信息炸弹

信息炸弹攻击手段是指使用一些特殊工具软件，在短时间内向目标服务器发送大量超出系统负荷的信息，从而造成目标服务器超负荷、网络堵塞或系统崩溃等结果的一种黑客攻击手段。向某型号的路由器发送特定数据包致使路由器死机，或向某人的电子邮件发送大量的垃圾邮件将此邮箱“撑爆”等都属于信息炸弹。



3. 拒绝服务

拒绝服务攻击，是指使用超出被攻击目标处理能力的大量数据包消耗系统可用系统和带宽资源，最后导致网络服务瘫痪的一种攻击手段。在此过程中攻击者首先需要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，当攻击者将攻击对象的 IP 地址作为指令下达给该进程的时候，这些进程就会开始对目标主机发起攻击。

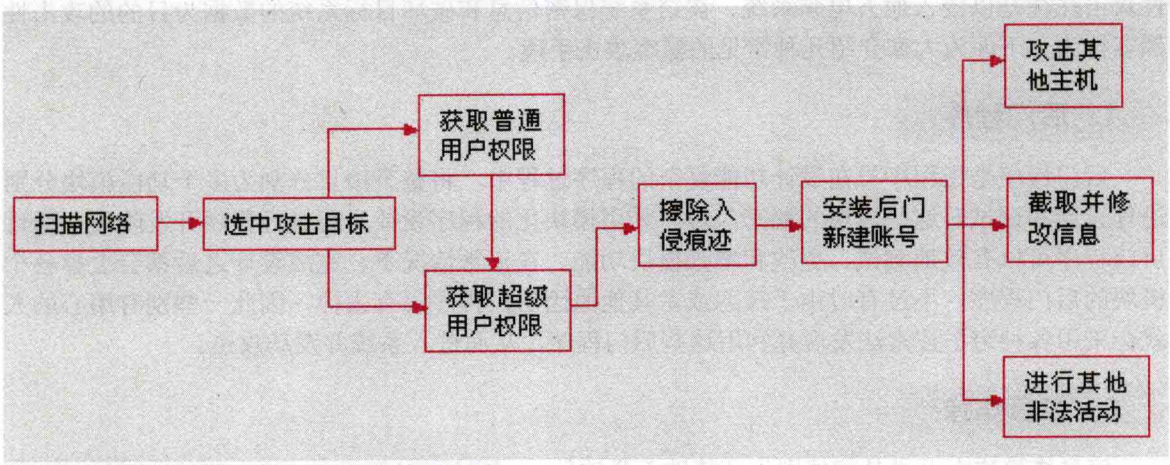
采用拒绝服务的攻击手段可以集中大量的网络服务器带宽，对某个特定目标实施攻击，因此在顷刻之间就可以将被攻击目标带宽资源耗尽，导致服务器瘫痪。

4. 网络监听

网络监听是指通过某种手段监视网络状态、数据流以及网络上传输信息的行为，通过网络监听可以将网络接口设置在监听模式，并且可以截获网络上传输的信息，通常被用来获取用户口令。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，那么使用网络监听就可以有效地截获网络上的数据。网络监听是黑客在攻击他人电脑系统时使用最多的方法，不过需注意的是，网络监听只能应用于物理上连接于同一网段的主机。

1.1.4 黑客攻击流程分析

黑客常用的攻击流程可以说是变幻莫测，不过其整个攻击过程还是有一定规律可循的，一般可以分攻击前奏、实施攻击、巩固控制和继续深入 4 个过程。下图为黑客攻击常见步骤。



1. 攻击前奏

攻击前奏包括锁定目标、了解目标网络结构和收集目标系统信息等。

- 锁定目标

网络上有许多服务器主机，黑客首先需寻找到要攻击的站点。一般黑客会通过网站域名和 IP 地址找到目标主机。

- 了解目标网络结构

确定要攻击的目标后，黑客就会设法了解其网络结构，包括网关、路由、防火墙及与要攻击的目标主机关系密切的其他主机信息等。黑客一般会通过使用 Tracert 命令追踪路由，或向目标主机发送一些数据包观察其是否能通过来分析其防火墙过滤设定。对于熟练的黑客来说，在进行以上操作时一般都会采用别人的电脑来间接探测目标主机，从而隐藏其真实的 IP 地址。

- 收集目标系统信息

了解到目标网络结构后，黑客会对网络上的每台主机进行全面的系统分析，以寻找该主机的安全漏洞或安全弱点。首先黑客需检测目标主机使用的操作系统及其版本，然后检查其开放端口并进行服务分析，看是否有可以被利用的服务。收集目标系统信息时黑客往往会利用一些安全扫描器来帮其发现系统的各种漏洞，包括各种系统服务漏洞、应用软件漏洞或弱口令用户等。

2. 实施攻击

黑客对目标系统的安全弱点有了足够的了解后就会对其发动攻击。黑客们会根据不同的网络结构和系统情况采用不同的攻击手段，由于并不是每次攻击都能够实现控制目标主机的目的，因此有时黑客也会发动拒绝服务攻击之类的干扰攻击，使系统不能正常工作，最后实现控制目标系统并窃取机密文件的目的。

3. 巩固控制

黑客进入目标主机系统并获得控制权之后，往往并不会马上进行删除数据或涂改网页等破坏活动。一般入侵成功后，黑客为了能长时间保留和巩固对系统的控制权而不被管理员发现，会进行清除记录和留下后门两个重要的操作。由于日志往往会记录下黑客攻击的一些蛛丝马迹，因此他们会将其删除或使用假日志将其覆盖，同时为了日后可以不被觉察地再次进入系统，黑客还会更改某些系统设置，在系统中植入特洛伊木马或其他一些远程操控程序。

4. 继续深入

当黑客确定隐藏好自己的踪迹之后，就会开始具体的入侵行动了，如窃取主机上的各种软件资料、客户名单、财务报表或信用卡卡号等。有时黑客攻陷某台主机只是为了将其系统作为存放黑客程序或资料的仓库，因此一般不会对目标主机中系统设置和文件做过多的修改，也可能利用这台已经攻陷的主机去继续入侵内部网络，或利用这台主机发动 DOS 攻击使网络瘫痪。

1.2 黑客通道——端口

电脑通过端口实现与外部通信的连接，同时黑客攻击电脑时也正是将系统和网络设置中的各种端口作为入侵的通道。在网络技术中，端口是指连接其他网络设备的接口，而这里所指的黑客通道并不是指物理意义上的端口，而是网络协议中的端口，是逻辑意义上的端口。

1.2.1 端口的分类

逻辑意义上的端口有多种分类标准。下面分别介绍两种常见的分类方法。

1. 按端口号分布划分

如果将 IP 地址比作一间房子，那么端口就是出入这间房子的门，不过真正的房子只有几个门，而一个 IP 地址的端口可以有 65536（256×256）个之多。IP 地址的端口是通过端口号来标记的，端口号依次为 0～65535 的整数。

- 公认端口（Well Known Ports）

公认端口从 0 到 1023。这些端口紧密地绑定于一些服务，这些端口的通信也明确表明了某种服务的协议，如 80 端口实际上总是 HTTP 通信。

- 注册端口（Registered Ports）

注册端口从 1024 到 49151。这些端口松散地绑定一些服务，即许多服务绑定于这些端口，因此这些端口同样可以用于许多其他目的，如许多系统处理动态端口从 1024 左右开始。

- 动态或私有端口（Dynamic and/or Private Ports）

动态或私有端口从 49152 到 65535。从理论上讲，不应为服务器分配这些端口，而在实际上，电脑通常从 1024 起分配动态端口，但也有例外，如 SUN 的 RPC 端口从 32768 开始。

2. 按协议类型划分

按协议类型可以将端口划分为 TCP、UDP、IP 和 ICMP 等端口。下面主要介绍 TCP 和 UDP 端口。

- TCP 端口

TCP 端口是指传输控制协议端口，它需要在客户端和服务器之间建立连接，从而提供可靠的数据传输。常见的 TCP 端口包括 FTP 服务的 21 端口、Telnet 服务的 23 端口、SMTP 服务的 25 端口和 HTTP 服务的 80 端口等。

- UDP 端口

UDP 端口是指用户数据包协议端口，它无需在客户端和服务器之间建立连接。常见的 UDP 端口有 DNS 服务的 53 端口、SNMP（简单网络管理协议）服务的 161 端口、QQ 使用的 8000 和 4000 端口等。

1.2.2 查看端口

在 Windows 2000/XP/Server 2003 操作系统下，使用 Netstat 命令可以查看电脑端口。Netstat 的命令格式为：

```
Netstat -a -e -n -o -s -an
```

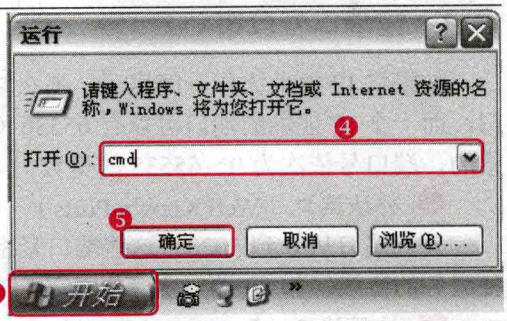
Netsta 命令后的-a、-e、-n、-o、-s 和-an 参数分别表示以下意义。

- -a: 显示所有活动的 TCP 连接以及电脑监听的 TCP 和 UDP 端口。
- -e: 显示以太网发送和接收的字节数、数据包数等。
- -n: 只以数字形式显示所有活动的 TCP 连接的地址和端口号。
- -o: 显示活动的 TCP 连接并包括每个连接的进程 ID（PID）。
- -s: 按协议显示各种连接的统计信息，包括端口号。
- -an: 显示所有开放的端口。

如要以数字形式显示 TCP 和 UDP 连接的端口号及状态，具体操作步骤如下。

第 1 步：打开命令提示符窗口

1. 单击 开始 按钮。
2. 选择 运行(R)... 命令。
3. 打开“运行”对话框。
4. 在 打开(O): 文本框中输入 cmd 命令。
5. 单击 确定 按钮。



老师，我输入 Netstat 命令怎么没有反应呢？

Netstat命令的作用是显示协议统计和当前的 TCP/IP 网络连接，只有在安装了 TCP/IP（协议）后该命令才能使用。