Hack Attacks Denied,
Second Edition

网络与信息安全技术丛书

黑客攻击
防范篇
（原书第2版）

附赠 CD-ROM

（美）John Chirillo 著

李宏平 王计艳 徐宇晖 周鹏 等译

机械工业出版社
China Machine Press

网络与信息安全技术丛书

黑客攻击防范篇

（原书第2版）

（美） John Chirillo 著

李宏平 王计艳 徐宇晖 周鹏 等译

机械工业出版社
China Machine Press

本书详细阐述了如何成功地保护网络和系统、防止安全威胁，全面覆盖了Windows、UNIX和Linux，是一本指导读者如何将黑客攻击拒之于网络之外的网络安全技术参考书。本书内容包括：保护计算机系统常见端口和服务、隐式端口和服务分析与保护、发现的应付对策、防范渗透攻击、保护周边设备和服务守护进程、最常用的75种黑客攻击方法、安全策略。本书的附录部分提供了有关安全件和安全计划模板的内容，还给出了随书光盘的内容介绍。

图书在版编目（CIP）数据

黑客攻击防范篇：第2版/（美）奇里罗尔（Chirillo, J.）著；李宏平等译. -北京：机械工业出版社，2003. 8

（网络与信息安全技术丛书）

书名原文：Hack Attacks Denied: A Complete Guide to Network Lockdown for UNIX, Windows, and Linux, 2E

ISBN 7-111-12307-7

Ⅰ. 黑… Ⅱ. ①奇… ②李… Ⅲ. 计算机网络-安全技术 Ⅳ. TP393. 08

中国版本图书馆CIP数据核字（2003）第043721号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：周睿 李冰 李炎

北京中加印刷有限公司印刷·新华书店北京发行所发行

2003年8月第1版第1次印刷

787mm × 1092mm 1/16 · 30 印张

印数：0 001 - 4 000 册

定价：56.00 元（附光盘）

译 者 序

本书作者John Chirillo是非常有名的超级黑客，他推出的《黑客攻击》三部曲是所有对计算机网络和系统安全关注的人无法不动心的三本书。

“《黑客攻击防范篇》在为读者提供防止黑客攻击的信息方面博大精深。”

HiTech Review

我们摘录了这句话不仅仅是为了表示对这本书的赞赏，同时也是提醒读者，要仔细掌握本书的内容，必须仔细咀嚼，反复体会，才能明白这句话的真正含义！

本书中的文本和程序文件都是那些地下黑客所实际应用的，因而本书清楚地揭示了过去和现在黑客技术的真实面貌。

全书由李宏平、王计艳、徐宇晖、周鹏、李家峻、郝丽杰、吴淑英、邓多多、李欣、成洁易、王政、桂黎明、方巍巍、孙淑芳、王胜利、章波、曾心洁、陈安然、李克雅、周木、张立明、赵云芳、黄凯等进行翻译，前导工作室全体工作人员共同完成了本书的翻译、录排、校对等工作。本书最后由宋涛统稿。由于时间仓促，且译者的水平有限，在翻译过程中难免会出现一些错误，请读者批评指正。

2003年3月

前　言

越来越多的专用网用户需要访问Internet的服务，例如www、email、telnet和FTP。企业想通过Internet为公共访问提供Internet主页和FTP服务器。随着在线世界的不断扩展，越来越多的内容涉及到安全问题。网络管理员和经理们担心数目不断增长的、各式各样的Internet黑客、解密高手、计算机朋客和电话飞客会暴露公司机密的和私有的数据以及他们的网络基础设施。简而言之，在线安全已成为一个组织将专用网络引入到Internet时所关心的主要问题。为了提供所需的保护级别，组织不仅需要一个健壮的安全策略来防止未授权的访问，同时为了抵制黑客攻击还必须建立坚固的防御工事，组织的管理者还需要对其中涉及的所有因素有一个全面的理解。即使是那些没有连接到Internet上的组织，如果他们想要成功地管理用户访问并且保护敏感和机密的信息，也需要建立企业内部网安全措施。

本书描述了以上所有内容，详细说明了成功地保护网络和系统、防止安全威胁所需要的过程。通过介绍阶段性解决方法（这个方法和我的另一本书《Hack Attacks Revealed，Second Edition》[⊖]互相关联），本书简略地描述了规划和实现一个有效的安全策略所采取的安全步骤。

新内容

在本书第2版中，你可以发现最新的安全危险和老虎队处理程序，还有全面的例子和图解。这本书从逻辑上分为四个部分：

- 第一阶段涉及系统基础设施设计，说明保护易受攻击的端口和服务所需的处理。
- 第二阶段详述如何实施保护措施，防止在《黑客攻击揭密篇》中列举的种种秘密脆弱性渗透入侵。
- 第三阶段介绍在流行的网关、路由器、Internet服务器守护进程、操作系统、代理和防火墙上使用的必要的黑客攻击应付对策，以及应付排名前75位的黑客攻击的对策。
- 第四阶段通过制定一个有效的安全策略使这些安全措施汇总成一个安全观点。

除了上述改动，还将发现超过170个新对策、TigerSurf 2.0 Intrusion Defense Full Suite Edition（在本书附带光盘中），对*NIX和Windows系统中Top 75黑客攻击的修补程序，以及Myparty、Goner、Sircam、BadTrans、Nimda、Code Red Ⅰ/Ⅱ等的清除与防范。

谁应该读这本书

本书对每一个关心在线安全或对此感兴趣的人都会有启发作用，它将指导人们如何以最好的方式形成他们所需要的安全。

本书特别针对以下读者：

- SOHO Internet热衷者，他们的Web浏览包括安全在线购物、填写表格以及传送文件、数据和信息。
- 网络工程师，他们整天围绕着安全问题转。

⊖ 本书中文版已由机械工业出版社出版，中译名为《黑客攻击揭密篇》。——编辑注

- 安全工程师，他们的目的就是成为一个安全方面的奇才。
- 黑客、解密高手和电话飞客，他们为了学习和娱乐而使用本书。
- 非技术管理者，他们的工作也许需要这里的信息。
- 类似于电影《通天神偷》、《骇客帝国》、《入侵网络》和《剑鱼行动》中的黑客热衷者和崇拜者。
- 聪明、好奇的少年，读过这本书后，他们的命运如何将会变得非常清楚。

目　录

第三阶段 老虎队秘笈

第四阶段 整 理

第一阶段

保护端口和服务

在本书的姊妹篇《Hack Attacks Revealed，Second Edition》（黑客攻击揭密篇——已由机械工业出版社出版）中详细描述了计算机端口和服务并且说明了什么因素会使它们变成潜在的攻击对象。对于那些没有读过该书的人来说，需要做一下简单的回顾，计算机端口是信息进出计算机的重要途径，输入/输出端口是数据在输入输出设备和处理器之间流动的通道，对于IP来说就是上层处理从底层获得信息。端口常被扫描或者“监听”以便判断那些潜在地易受攻击端口是否正处于打开状态。安全分析工具例如端口扫描器能够在几分钟之内轻易地扫描一台计算机上65 000多个端口中的任何一个。然而，它们通常只仔细地检查前1024个端口，这些端口被称为常用端口（well-known port）（剩下的端口称为隐式端口（concealed port），这1024个常用端口为系统服务而预留，是作为响应请求的联系端口（contact port）。因特网号码分配管理局（IANA：Internet Assigned Numbers Authority）的定义表明，在大多数系统上，只有系统（或者root）或特权用户执行的程序才能使用常用端口。在TCP[RFC793]中的端口被用来命名承载长期会话的逻辑连接端点。为了给未知的调用程序提供服务，还定义了服务联系端口。联系端口有时候又叫“常用端口”。当一个端口扫描器扫描计算机端口时，在大多数情况下，它会一个接一个地询问端口是打开的还是关闭的。计算机只知道自动地发送应答，提供攻击者所需的信息，其他的它什么都不知道。如果执行恰当的话，这种扫描可以在没有任何人知道的情况下进行。

使用这本书可以建立牢固的安全基础。在本书的最后，为了与《黑客攻击揭密篇》一书中描述的老虎队（Tiger Team）解决方案联系起来，我将这本书分为所谓的“老虎队过程”系列步骤（阶段），按重要顺序依次描述了成功防止安全漏洞的措施。

第一阶段主要是介绍一些保护上述端口和服务的技术。首先探讨一下保护常用端口和增强隐式端口的一些方法。在此基础上深入研究应付发现（discovery）和扫描（scan）的对策。在《黑客攻击揭密篇》中，将发现解释为最初的“踩点”或信息收集，信息收集是一种攻击者所采取的能导致攻击成功的便捷计划。目标端口扫描一般是这种发现处理的第二个基本步骤。

第1章 通用端口和服务

本章主要介绍保护常用端口列表中易受攻击的端口的技术，这些端口包括TCP和UDP服务。在RFC793和RFC768中分别阐述了TCP和UDP端口，并以此来命名在系统上和系统间进行委托服务会话的逻辑连接端。这些列表指定由服务守护进程作为其联系端口的端口，这些联系端口也可称为“常用端口”。IP有许多的弱点，其中之一就是不可靠的包传递——传输错误、路由失败和/或吞吐量下降都会导致包的丢失。传输控制协议（TCP，Transmission Control Protocol）可以提供可靠的、面向流的连接，这有助于缓解以上问题。事实上，TCP/IP主要依赖TCP的功能来组成TCP/IP包，而TCP又是基于IP的，这样就形成了TCP/IP协议簇。这些特点描述了在通信建立时面向连接的过程。

TCP的可靠服务传递取决于很多因素，下面列出主要的几点：

- 流　将数据组织成8位的字节，并以位流的形式来传送数据。当接收到这些位时，再用同样的方式将它们转发出去。
- 缓冲区流控　既然数据以流的形式传输，那么协议软件也可以把这些流分开，用来填充特定大小的缓冲区。TCP控制这些处理，从而保证缓冲区不会溢出。在这个处理过程中，为了与缓慢的接收站保持同步，会预先停止快速发送站的数据发送。
- 虚电路　当一个站需要与另一个站进行通信时，这两个站都会通知它们各自的应用程序，并且只有双方都同意时，才能进行此次通信。如果它们之间的连接或通信失败了，那么这两个站都会察觉到并通知它们各自的软件应用程序。出现这种情况时，双方会再次尝试连接。
- 全双工连接　双向流传送，以减少全网的流量堵塞。

TCP用32位序列数组织和计算数据流中的字节。每个TCP数据包包括一个开始序列号（第一个字节）和一个确认号（最后一个字节）。此处有一个概念叫滑动窗口，它可以更有效地实现流传输。在收到确认号之前，滑动窗口可以传输多个包，通过这种方式，可以更有效地利用带宽。

这里讲述一个TCP滑动窗口的例子，一个发送站用一个大小为4的窗口将一个字节序列（1到8）发送到一个接收站。发送站将前4个字节放在窗口中发送出去，然后等待一个确认（ACK=5）。这个确认表明前4个字节已经收到。接着，假定窗口大小仍然是4，接收站也在等下一个字节（字节5），发送站将滑动窗口向右移动4个字节，并且将5到8字节发送出去。接收站收到这些字节以后就会发一个确认（ACK=9），表明它在等字节9。继续以上的过程。在某个时刻，接收者可能会指出窗口大小为0，在这种情况下，发送者不能再发送字节，直到窗口的尺寸变大为止。造成这种情况的主要原因是缓冲区溢出。

TCP能够在一台机器上的不同应用程序之间同时进行通信，它用端口号区别每一个接收站的目的地址。一对端点标志着两个站之间的一个连接。也就是说，将这些端点定义为两站通信时各自应用程序之间的连接；TCP将它定义成一个整数对，形式为：（主机，端口）。主机是站的IP地址，端口是此站的TCP端口号。例如，一个站的端点为：

206.0.125.81: 1026

（主机）　（端口）

例如，下面是进行通信的两个站的端点：

站1	站2
206.0.125.81：1022	207.63.129.2：26
（主机）（端口）	（主机）（端口）

这是TCP的一个非常重要的技术，通过为每一个站的连接分配独立的端口，TCP可同时进行通信。

在一个TCP会话期间，在建立两个节点之间的连接时，为了使连接的两端同步，需要进行三次握手。在这个过程中，双方都采用数字序列方法来回地跟踪通信流中的字节。基本上，第一个节点通过发送一个含有序列号和SYN位的包来请求通信。第二个节点用一个含有序列号加1的确认信号进行应答，将它本身的序列号送回到第一个节点。此时，第一个节点会发出应答，于是两点之间的通信就开始了。当数据传送完之后，其中的一个TCP节点会发送一个FIN位，它表示关闭控制信号。此时，两个节点同时关闭。

用户数据报（UDP，User Datagram Protocol）以一种无连接的方式进行传输；也就是说，它提供与IP相同的不可靠的数据报传送服务。不像TCP，UDP不发送SYN/ACK位信息，所以它不能保证传送和传输的可靠性。而且，UDP没有流控制和错误恢复功能。因此，UDP消息有可能丢失、重复或以错误的次序到达目的地。由于UDP包含较小的报头，所以它消耗的网络吞吐量比TCP要小，并且到达速度比接收站的处理速度要快。

UDP一般用于高层协议能够提供必要的错误恢复和流量控制的地方。几个常见的使用UDP的服务器守护进程包括：

- 网络文件系统（NFS，Network File System）
- 简单网络管理协议（SNMP，Simple Network Management Protocol）
- 小文件传输协议（TFTP，Trivial File Transfer Protocol）
- 域名系统（DNS，Domain Name System）

UDP消息通常被称为用户数据报，当通过因特网时，它被封装在IP中，包括UDP头和数据。UDP在要通过IP传送的用户数据前加一个报头，然后IP层在从UDP收到的数据之前再加一个报头，最后，在从一台机器发送到另一台之前，网络接口层把数据报插入到一个帧中。

UDP支持协议和应用软件之间的多路复用（一种将多个信号同时放在一个输入流中、通过一个物理通道发送的方法）和多路分解（指流的分解，即将那些被复用到一个流中的数据还原成多个输出流）。

当多路复用和多路分解用在UDP中时，它们总是通过端口散发出去。在发送一个UDP数据报之前，每一个站的应用程序都必须协商一个端口号。在数据报的接收端，UDP检查到来数据报的报头（目的端口字段）判断它和此站上正在使用的某个端口是否匹配。如果某个正在监听的应用程序正在使用这个端口，传输就继续下去；如果端口没在使用，就会产生一个ICMP错误消息，这个数据报就会被抛弃掉。

ICMP消息封装是一个双重处理过程。通过因特网时，它被封装在IP数据报中，IP数据报又被封装在帧中。作为数据报，ICMP同样使用的是不可靠的通信方式，这意味着ICMP错误消息也有可能丢失和重复。

ICMP的格式包括一个消息类型字段，表示消息的类型；一个编码字段，它含有有关类型的详细信息以及一个校验和字段，它与IP校验和的功能相同。当一个ICMP消息报告一个错误时，它含有报头和会引发特定问题的数据报的相关数据。这有助于接收站理解出错数据报是由哪些应用程序和协议发出的。

下面有许多有用的ICMP消息类型：

- Echo应答（类型0）（Echo Reply(Type 0)）/Echo请求（类型8）（Echo Request(Type 8)） 测试两节点间可能的通信的基本机制。当接收站可用时，发送站发出PING请求，由接收站应答，PING是Packet INternet Groper的缩写。PING是一个测试指定的计算机IP地址是否可用的协议；利用ICMP，可以发送

一个包到指定的IP地址，然后等待它的响应。有趣的是，PING起源于潜水艇发出的声纳，它传播一种称为ping的声音信号，然后通过周围物体对声音的反射来识别它们。可从很多地方执行PING，如路由器控制台或远程终端窗口，例如Microsoft Windows中的MS-DOS窗口，以及*NIX的终端控制台会话。

- 目的地不可达（类型3）（Destination Unreachable(Type 3)） 产生这种类型的消息有好几种情况，例如，当一个路由器或网关不知道如何到达目的地时、当一个协议或应用程序没有激活时、当一个数据报指定了一个不稳定的路由时，或者当一个路由器必须分割数据报的大小，但却因为没有设置分段标志而不能分割时。
- 源抑制（Source Quench(Type 4)） 这是数据报传送流控制的基本形式。当需要处理的数据报到达接收站的速度太快时，这些数据报就会被丢弃。在这个过程中，每一个被丢弃的数据报都有一个相应的ICMP类型4被送回到发送站。源抑制消息实际上变成了减慢发送数据报速率的请求。但源抑制消息不会产生反作用从而使得发送站提高传输速率。
- 改变路由（Route Redirect(Type 5)） 为了适应网络的变化、保持路由表的更新，路由信息也在周期性地改变着。当路由器标识出一个没有可选路由的主机时，在向目的网络转发数据报的同时它会发出ICMP类型5消息。因此，路由器只能向直接连在其所在网络上的主机发送类型5消息。
- 数据报超时（Datagram Time Exceeded(Type 11)） 如果网关或路由器因为数据报的TTL（生存时间）字段为0而被迫丢弃这个数据报，那么网关或路由器就会发出类型11消息。如果路由器在截取数据报时发现它的TTL=0，那么它就会被迫丢弃这个数据报并发出一个ICMP类型11消息。
- 数据报参数问题（Datagram Parameter Problem(Type 12)） 用数据报头指出问题从而阻止进一步的处理。数据报会被丢弃，同时还会发出一个类型12的消息。
- 时间戳请求（Timestamp Request(Type 13)）/时间戳应答（Timestamp Reply(Type 14)） 这是提供网络延时表（delay tabulation）的一种途径。发送站插进一个发送时间戳（消息的发送时间），接收站将附加一个接收时间戳来计算估计的延时并且辅助内部时钟同步。
- 信息请求(Information Request(Type 15)/信息应答Information Reply(Type 16)) 作为反向地址解析协议（RARP，Reverse Address Resolution Protocol）的替代品。反向地址解析协议是指给出其MAC地址，一台计算机可以向RARP服务器请求它的IP地址。站点可利用类型15和类型16获得隶属网络的Internet地址。发送站发送此消息，其中含有Internet地址的网络部分，然后等待包含主机部分（它的IP地址）的应答。
- 地址掩码请求（Address Mask Request (Type 17)）/地址掩码应答（Address Mask Reply (Type 18)）类似于信息请求/应答，站点可发送类型17和类型18消息来获得隶属网络的子网掩码。站点向已知的节点提交请求，例如网关或路由器，或者向网络广播它的请求。

回忆一下TCP连接，当TCP窗口大小发生改变时，通过同步连接两端的序列号和确认号对它进行初始化。这称之为面向连接的可靠服务（connection-oriented, reliable service），而UDP提供的是无连接的数据报服务（connectionless datagram service），它支持不可靠的、尽力而为的数据传送，这意味着它不能够保证数据报的到达以及传送包的先后次序。

当两个系统进行通信时，TCP和UDP端口成为承载这些服务“会话”的逻辑连接端点。这些端点通过一个特定的服务守护进程指定某个端口作为它的联系端口，即“常见端口”。在这一章里，我们主要集中讲解《黑客攻击揭密篇》中作为潜在的易受攻击看待的那些端口。这些端口包括端口7：echo、端口11：systat、端口15：netstat、端口19：chargen、端口21：FTP、端口23：telnet、端口25：SMTP、端口53：domain、端

口67：bootp、端口69：TFTP、端口79：finger、端口80：http、端口109：pop2、端口110：pop3、端口111：portmap、端口135：loc-serv、端口137：nbname、端口138：nbdatagram、端口139：nbsession、端口161：SNMP、端口512：exec、端口513：login、端口514：shell、端口514：syslog、端口517：talk、端口518：ntalk、端口520：route和端口540：uucp。

1.1 保护常见端口

在开始研究特定端口之前，先对Windows注册表和*NIX Internet Servers Database（inetd）做一个简单的了解是非常合适的。inetd实际上是一个守护控制进程（daemon control process），它可以处理*NIX系统上运行的网络服务。用文件/etc/inetd.conf对这个守护进程进行配置，用它来控制服务的激活，包括ftp、telnet、login和其他的一些服务。虽然这本书只涉及到了Linux系统目录/etc/中实现的inetd.conf文件，但是还应该意识到每一种风格的*NIX都有一个不同的文件地址；例如，AIX使用目录/usr/sbin、Digital使用/usr/sbin、HP-UX9和10使用/etc和/usr/lbin、IRIX使用/usr/etc、Solaris使用/usr/sbin、SunOS使用/usr/etc等等。

在Windows系统中，系统注册表在某种程度上相当于*NIX inetd守护进程，它就像一个具有层次的数据库，里面的所有系统设置都进行了分类。它替代了管理老的Windows版本3.x的所有.ini文件。注册表中含有system.ini、win.ini和control.ini中的所有配置信息，Windows应用程序所有的初始化信息和配置数据也都存放在此处。

老虎提示：在进行任何改动之前都要记得对inetd.conf文件和Windows注册表进行备份。

需要注意的是注册表通常不能使用任何标准的编辑器打开和编辑；必须用一个Windows程序对此进行操作，在Windows 95、98和XP中将此程序称为regedit，在Windows 2000、NT4和NT5中称之为regedit32。这个程序没有列在Start Menu（开始菜单）中，实际上，它隐藏在Windows目录中。要运行此程序，先点击Start，然后点击Run，接着在输入框中敲入regedit（对于Win 9x）或regedit32（对于Win NT）。这样就可启动Registry Editor（注册表编辑器）。

老虎提示：在想实现本书此处所给出的方法或软件包之前，对系统注册表进行备份是一件非常重要的事情。注册表备份软件可到TuCows（www.tucows.com）和Download（www.download.com）上去下载。

注册表文件夹中的内容包括：

- HKEY_CLASSES_ROOT　包含有关拖放操作的软件设置；处理快捷信息和其他用户接口信息。此处定义的每一个文件链接都含有一个子键。
- HKEY_CURRENT_USER　含有当前登录用户的信息，包括：
  - AppEvents：包含为响应系统或应用程序声音事件所选定声音的配置。
  - Control Panel：包含类似于在Windows 3.xx的system.ini、win.ini和control.ini中定义的那些配置。
  - InstallLocationsMRU：含有到Startup文件夹中程序的路径。
  - Keyboard Layout：指定当前的键盘布局。
  - Network：给出网络连接信息。
  - RemoteAccess：如果使用的是拨号上网的话，则列出当前登录的位置信息。
  - Software：向当前的登录用户显示软件配置信息。
- HKEY_LOCAL_MACHINE　包含特定计算机上所有用户都会用到的软硬件设置信息，包括：

- Config：列出配置信息/设置。
- Enum：列出硬件设备信息/设置。
- Hardware：显示串行通信端口信息/设置。
- Network：给出用户当前所登录的网络的信息。
- Security：列举网络安全设置。
- Software：显示与软件相关的信息/设置。
- System：列举系统启动和设备驱动信息及操作系统设置。
- HKEY_USERS 包含每一个登录到同一个Windows 95系统的用户的桌面信息和用户设置。在这一栏中，每一个用户都有一个相应的子键。如果系统只有一个用户，子键就是.default。
- HKEY_CURRENT_CONFIG 包含当前的硬件配置信息，它指向HKEY_LOCAL_ MACHINE。
- HKEY_DYN_DATA 包含关于系统上安装的即插即用设备的动态信息，这些数据随着设备的增加和去掉而改变。

1.1.1 端口7：echo

echo服务与TCP和UDP的端口7有关系，对于TCP来说，此服务监听端口7的连接，然后送回它所收到的数据；对于UDP端口7数据报服务，服务器将以应答数据报的形式送回它收到的数据。这个服务一般用于创建拒绝服务（DoS）。当一个攻击者连接到端口7（echo）时，所传输的字符通常被送回（反射回）发送源，这是echo易受攻击的一个地方。在某些情况下可以滥用此服务，例如，在系统的echo服务和chargen服务（见端口19）之间形成一个环或者从另一个目标的chargen服务发送一个欺骗包给一个目标echo的服务。

如果只是简单地应答从TCP或UDP连接请求发送的数据，标准的通信策略不一定要使用echo服务。在这种情况下，建议禁用此服务，避免潜在的拒绝服务（DoS）攻击。但是，在禁用此服务前，应该先检查一下是否还有哪个专有软件还需要用它，比如系统监控包或客户故障诊断包。

- 禁用*NIX中的echo服务，只需简单地编辑/etc/inetd.conf文件，注释掉echo条目，如图1-1所示。然后重启整个系统或只是重启inetd进程。如果是Linux系统，只需简单地使用下面的命令重载inetd配置即可：killall—HUP inetd。

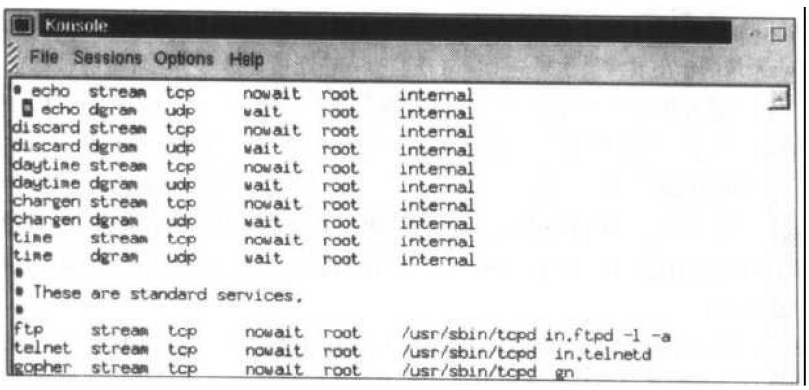

图1-1 在*NIX系统中禁用服务

- 禁用Windows系统中的echo服务（如果有的话），必须在Start/Run（开始/运行）命令提示符下运行regedit.exe来编辑系统注册表，从而搜索TCP/UDP的Echo条目，然后将它的值改为“false”或者空

（见图1-2）。完成后重启系统、验证所做的更改。

老虎提示：如果对Windows系统注册表中的修改不熟悉或者使用困难，参考附录A可以了解一些自定义安全软件或者安全件中的详细信息。在本例中，TigerWatch将使用户不必同注册表交互或者手动禁止某个服务即可执行预先监控或者锁住系统的端口和服务。在本书的后续内容中，将同其他程序一起继续描述TigerWatch，并给出其详细信息。

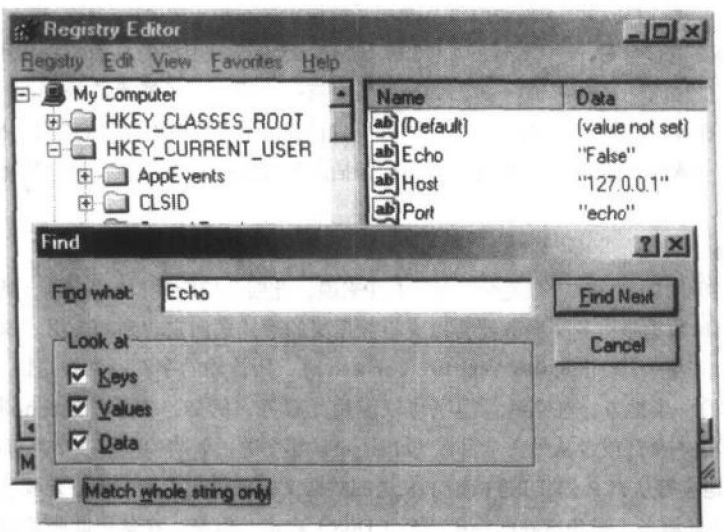

图1-2　编辑Windows系统注册表禁用Windows系统的服务

1.1.2　端口11：systat和端口15：netstat

systat用来显示机器当前的操作处理状态。systat通过远程启动来提供处理状态和用户信息。尤其是，与这个服务相联系的守护进程会给出当前正运行的软件类型，并且指出目标主机上的用户是谁。netstat服务用来显示机器的活跃网络连接和其他关于网络子系统的有用信息，例如协议、地址、连接的套接字和MTU尺寸。标准Windows系统的输出通常显示哪一个服务在监听入站连接，哪一个地址可能已建立了连接等等。

不像systat，攻击者可从netstat得到活跃网络连接和其他关于网络子系统的有用信息，例如协议、地址、连接的套接字和MTU尺寸（参考图1-3）。一旦攻击者进入了系统，这个服务还可以用一个后门程序取代。比较好的解决方法是用防火墙过滤掉这个信息或者使用一个类似于Tripwire（www.tripwire.com/products/servers/）的包。Tripwire监视文件的变化，验证完整性，并且通知用户网络服务器上任何静止的违规数据——不管发生在内部还是外部。Tripwire还能识别系统属性的改变，包括文件的大小、访问标志、写操作时间等等。

1.1.3　端口19：chargen

从这个服务充当的是字符流产生器的角色就可以很容易地推断出它的基本操作。不幸的是，这个服务可以无限循环地向另一个服务或者另一台机器发送数据。很明显，当因此导致的结果是消耗带宽和系统处理资源时，它会引起另一种形式的拒绝服务（DoS）攻击。

利用这个服务可向echo服务无限循环地传送和收回信息，这会引起严重的系统阻塞。作为字符流产生器，标准的通信策略未必需要此服务；因此，可以禁用它来避免遭受攻击。