Information Security

PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI

普通高等学校信息安全"十一五"规划教材

网络安全技术实验教程

WANGLUO ANQUAN JISHU SHIYAN JIAOCHENG

谌黔燕　郑方伟　刘杰彦　编著
杨国纬　主审

电子科技大学出版社

PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI
普通高等学校信息安全"十一五"规划教材

网络安全技术实验教程

谌黔燕　郑方伟　刘杰彦　编著

杨国纬　主审

电子科技大学出版社

图书在版编目（CIP）数据

网络安全技术实验教程 / 谌黔燕等编著. —成都：电子科技大学出版社，2007.3

普通高等学校信息安全“十一五”规划教材

ISBN 978-7-81114-227-3

Ⅰ. 网… Ⅱ. 谌… Ⅲ. 计算机网络—安全技术—高等学校—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 024718 号

内 容 提 要

本书为普通高等学校信息安全“十一五”规划教材之一，内容丰富新颖，涵盖对当前网络安全领域内各主要攻防技术的实施和实现方法的详细分析和讨论。涉及的主要安全技术有：主机安全技术、认证技术、访问控制技术、密码与加解密技术、防火墙技术、入侵检测技术以及网站与数据库的综合安全技术等。

本书既可作为信息安全或计算机专业本科生、研究生的实验教材，也可作为相关领域专业技术人员的参考用书。

普通高等学校信息安全“十一五”规划教材

网络安全技术实验教程

谌黔燕 郑方伟 刘杰彦 编著

杨国纬 主审

出 版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦 邮编：610051）

策划编辑：曾 艺

责任编辑：曾 艺

主 页：www.uestcp com cn

电子邮箱：uestcp@uestcp com cn

发 行：新华书店经销

印 刷：成都蜀通印务有限责任公司

成品尺寸：185mm×260mm 印张 18 5 字数 445 千字

版 次：2007 年 3 月第一版

印 次：2007 年 3 月第一次印刷

书 号：ISBN 978-7-81114-227-3

定 价：30.00 元

编委会名单

编委会主任

郝玉洁

编委（按姓氏笔画为序）

刘乃琦　许春香　李毅超　佘　堃

周世杰　秦　科　谌黔燕　鲁　珂

学术顾问

秦志光　李建平　周明天

序言

随着社会信息化的快速发展，信息已成为社会发展的重要资源，围绕着这一资源所展开的全球性的竞争日趋激烈。信息的安全已不再是个人和涉及少数人利益的问题，而是事关部门、公司、企业甚至国家、地区等政治和经济利益的十分重要的问题。信息安全正在作为一种产业快速发展，而与此相悖的是，信息安全人才匮乏，远远不能满足商业、金融、公安、军事和政府等部门的需求。因此，培养信息安全领域的高技术人才已成为我国高等工程教育领域的重要任务。

信息安全是集计算机、通信工程、数学等学科知识为一体的交叉型新学科，对于这一新兴学科的培养模式和课程设置，各高等院校普遍缺乏经验，为此，电子科技大学计算机科学与工程学院信息安全专业的专家、学者和工作在教学一线的老师们，以我国本科高等工程教育人才培养目标为宗旨，组织了一系列信息安全的研讨活动，认真研讨了国内外高等院校信息安全专业的教学体系和课程设置，在进行了大量前瞻性研究的基础上，启动了普通高等院校信息安全“十一五”规划教材的编写工作。该系列教材由 8 本理论教材和 2 本实验教材组成，全方位、多角度地阐述了信息安全技术的原理，反映了当代信息安全研究发展的趋势，突出了实践在高等工程教育人才培养中的重要性，弥补了目前该类教材理论教学内容丰富，而实践教学不成体系的缺点，使其成为该系列教材的特点，也是其成功所在。

感谢电子科技大学信息安全专业的老师们为促进我国高等院校信息安全专业建设所付出的辛勤劳动，相信这套教材一定会成为我国高等院校信息安全人才培养的优秀教材。同时希望电子科技大学的教师们继续努力，为培养更多、更好的信息安全人才，为我国的信息安全事业作出更大的贡献。

唐远炎

二〇〇七年三月十日于香港

唐远炎　国际电子电气工程学会会士（IEEE Fellow）
国际模式识别学会会士（IAPR Fellow）
国际 IEEE SMC 机器学习委员会主席（Machine Learning Committee, IEEE SMC）
《中国高等学校学术期刊》计算机科学分册（Frontiers of Computer Science in China）副主编
国际 SCI 检索刊物《International Journal on Wavelet, Multiresolution, and Information Processing（IJWMIP）》（小波、多尺度分辨及信息处理国际期刊）创办人、主编
国际 SCI 检索刊物《International Journal of Pattern Recognition and Artificial Intelligence（IJPRAI）》（模式识别与人工智能国际期刊）副主编

前言

网络安全技术是一门囊括主机安全技术、认证技术、访问控制技术、密码与加解密技术、安全审计技术、防火墙技术、入侵检测技术和入侵者跟踪等学科内容的综合技术。从工程技术的角度来看，它涵盖了计算机系统、计算机网络、计算机通信和信息数据（库）安全等多学科工程技术知识，从而形成了知识点丰富、技术相互交错、工程实践性强的特点。作为实验教程，本书在实验原理的阐述、内容的设计和实验方案的实现等方面都充分考虑了网络安全技术的这一特点。

本书由一系列实验组成，每个实验由实验简介、实验环境、实验内容以及问题与讨论四部分构成，将技术原理与实现方法融合在一起，共同完成对某一特定技术的讨论。

全书共分 8 章，考虑到读者对象的不同以及网络安全技术本身的难易不同和复杂性，我们将实验分层，并以章节的形式集中体现。

第 1 章主要讨论了一些重要的 Windows 自带程序在网络安全中的功能和作用。第 2 章介绍了几种典型安全工具的使用方法。作为安全技术的基础知识这两章共同形成本书的初级实验。尽管我们把这些实验定位为初级实验，但这并不意味着它们不重要，实际上，无论是学习攻击技术还是防御技术，这两章的内容都很重要。

第 3 章和第 4 章的所有实验都是基于硬件的安全防御技术实验，突出强调了网络安全技术的工程性。主要讨论了防火墙和 VPN 技术的原理及具体实现方法。两章共同形成本书的中级实验。我们希望读者通过这两章的学习，不仅学会对相应硬件的配置方法，更重要的是学会网络安全规划和根据安全需求建立相应的安全策略，最终达到保护网络安全的目的。

第 5 章主要讨论了安全扫描技术。第 6 章主要讨论了目前常用的攻击技术以及结合各种技术形成的对网站、远程数据库和远程主机的攻击技术原理。第 7 章对身份认证技术进行了较为充分地讨论。第 8 章则着重讨论了安全控制技术，这一章的实验难度较大，是为那些希望获取更深层次技术知识的读者准备的。这几章的实验大都需要通过程序设计来完成，因此，要完成这些实验，除了要求读者具有较扎实的安全技术理论知识外，还要有一定的程序设计能力和综合运用能力。这几章共同组成本书的高级实验部分。

本书由谌黔燕老师、郑方伟老师和刘杰彦老师共同编写，并由谌黔燕老师统稿。在编写本书的过程中，我们力求把书中的实验设计得生动、翔实富有趣味，为教学双方所喜爱。

本书的大部分内容已经作为网络安全技术的实验内容在本科生和研究生中运用，在此我们真诚地把它们奉献给更加广大的读者。希望这本实验教材能给更多的读者带去学习网络安全技术知识的乐趣。

感谢所有对本书出版作出贡献的人，特别感谢李桂林、邱鹏、郑绍辉、苟瑞锋、张剑、

童永清同学，他们在本书的程序设计实验中付出了极大的劳动。感谢杨国纬教授，他不惜花费大量时间和精力，不辞辛劳地审阅本书，并对本书的一些关键问题提出了十分宝贵的意见。感谢刘乃琦教授、佘堃教授，他们给本书的内容规划提出过许多宝贵意见。感谢郝玉洁副教授，她是本书的主要策划人之一。是大家的共同努力使本书得以面世。

由于时间仓促和水平所限，书中难免出现这样那样的错误，希望读者批评指正。

（为了方便教学，本书附有所有程序源代码的光盘，如有需要，请与作者联系：sky_qy@163.com）

编　者

2007.1

目录

第 1 章　网络安全基础实验

第 2 章　典型的网络安全工具的使用

第 3 章　防火墙技术实验

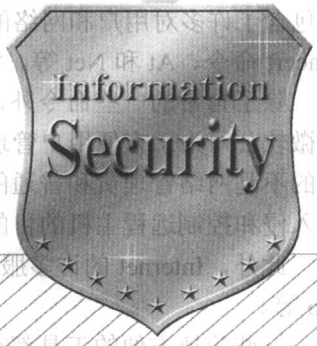
第 4 章　VPN 技术实验

第 5 章　安全扫描系统实验

第 6 章 常见攻击技术综合分析实验

第 7 章 身份认证实验

第 8 章 网络安全控制实验



第1章

网络安全基础实验

本章概要

作为一名网络或系统管理员，你一定希望采用一种操作简单、方便快捷的方法来开展工作。既不需要携带和安装专门的工具软件，也不需要做多余和重复的低效工作。有这样的方法吗？答案是肯定的。

Windows 系统本身自带了许多命令。它的命令行控制台不仅包含了各种常规 DOS 命令，还包含了许多对用户和网络的管理和控制命令。比如 Ping 命令、Nbtstat 命令、Netstat 命令、Tracert 命令、At 和 Net 等。它们的特点正是操作简便、功能强大。

除了自带的一些命令外，Windows 系统还具有一项特有的管理功能——IPC$。它本来是微软公司为了方便用户管理和使用远程计算机而特别设计的，但事实上，使用这个功能最多的不是网络管理员和普通的网络用户，而是网络入侵者。他们往往通过建立 IPC$连接达到入侵和控制远程主机的目的。

此外，Internet 的许多服务也可以成为我们使用和管理网络的便捷工具，比如 Telnet 、Ftp 等。

这些简捷方便的工具都有些什么功能，应该怎样使用，它们与网络安全之间又有着怎样的联系？这些正是本章将要讨论的重点。本章着重讨论了几个 Windows 自带的网络管理命令、IPC$功能以及 Internet 的 Telnet 服务在网络资源管理、信息搜集和远程控制等方面的功能、作用和具体使用方法。同时也讨论了如何防御入侵者利用这些工具进行入侵的防御方法。

实验 1.1 网络基本信息探测实验

实验简介

尽管 Windows 2000/XP 系统已经断然抛弃了 DOS，但它仍保留了对命令行命令的支持。在 Windows 2000/XP 系统里，Windows 2000/XP 所调用的命令行控制台主程序被放在系统文件 system32 目录下，文件名为 cmd.exe。同时该文件还在受保护的文件夹 system32\dllcache 中附有备份，以防原程序被破坏后进行恢复时使用。仅从这一点我们就可以看出 cmd.exe 文件的重要性。进入命令行控制台的方法很简单，单击桌面上的“开始”→“所有程序”→“附件”弹出如图 1-1-1 所示的对话框。在“打开”选项框中键入 cmd.exe，运行该程序便可以进入命令行提示符状态。

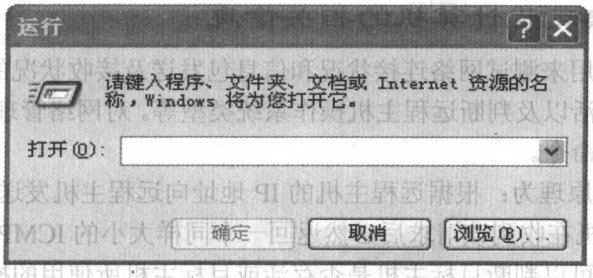


图 1-1-1 运行对话框

另一种进入命令行控制台的方法是：单击“开始”→“所有程序”→“附件”→“命令行提示符”直接进入命令行提示符状态。如图 1-1-2 所示。

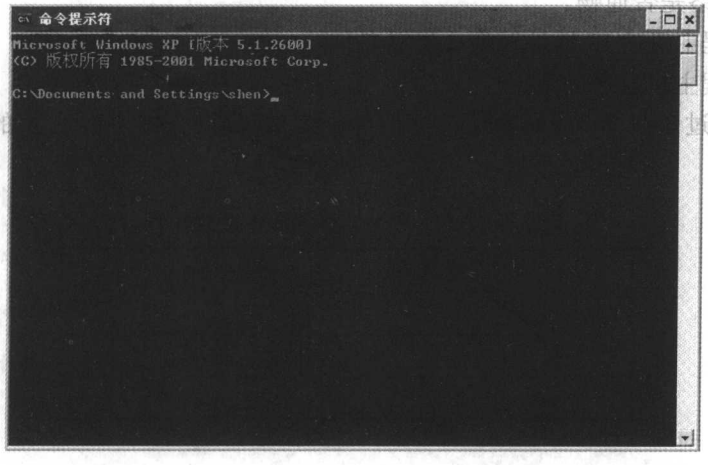


图 1-1-2 Windows 2000/XP 命令行提示符状态

实验 1.1 中的所有内容都在系统的命令行状态下完成。

Windows 2000/XP 系统命令行控制台提供了大约 71 个操作简单、功能强大的命令行命令。如果要查看这些命令的具体含义，只需在命令行控制台下直接键入“help”命令既可。这些命令中包括 Ping、Nbtstat、Netstat、Tracert、Nslooup、At、Net 等命令。这些命令看似简单，却有着极强的用户和网络管理功能。

在本实验中，我们将详细介绍这些工具的网络管理功能、运行环境和使用方法，以及它们在信息收集方面的功能和作用。

实验环境

由于实验中用到的命令都是 Windows 本身自带的命令，因此实验只需在一台连入网络并安装了 Windows 2000/98 操作系统的计算机上进行即可。

实验

用 ping 命令搜集远程计算机的相关信息

Ping 程序是一个用来测试网络连接状况和信息包发送及接收状况的常用工具。主要用来验证目标主机是否存活以及判断远程主机操作系统类型等。对网络管理员表说，Ping 命令是一个必须掌握的网络命令。

Ping 命令的探测原理为：根据远程主机的 IP 地址向远程主机发送一个 ICMP 数据包请求主机回应，目标主机在收到该请求后必然返回一个同样大小的 ICMP 数据包。从该数据包的返回值中，我们就可以判断目标主机是否存活或目标主机所使用的操作系统类型等信息。

Ping 命令的使用格式为：Ping 主机 IP

Ping 命令带有许多参数，常用的参数有：

-t 不间断地 Ping 目标主机，直到用户按 Ctrl+C 键强行终止。主要用于网络调试，从其结果可判断网络是否通畅。

–a 将远程主机的 IP 地址转换成机器名称。

–n 向远程主机发送的数据包的个数，默认为 4。

Ping 命令通过 TTL（time to love 生存时间）值来判断远程主机所使用的操作系统类型。如表 1-1-1 所示。

表 1-1-1 TTL 值所对应的操作系统类型

TTL 值	操作系统类型
64	Unix/Linux
128	Windows NT
255	Windows 98

当我们要迷惑入侵者的时候，可以通过修改 TTL 值来达到目的。方法是：打开注册表编辑器后找到如下键值：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Tcpip\Parameters, 单击右边的

Parameters 键选项，找到 DefaultTTL 键，然后修改其数据。修改后保存，退出注册表后重启主机即可。

TTL 值的范围为 0～256。

需要注意的是：Ping 命令使用的是 Internet 访问控制协议（ICMP），如果对方安装了防火墙并禁止了 ICMP 协议，Ping 命令就无法使用了。

动手做

已知目标主机 IP 地址的 Ping 命令探测方法

假设目标主机的 IP 地址为：192.168.1.2，在命令行提示符下键入：Ping 192.168.1.2，屏幕的返回信息如图 1-1-3 所示。

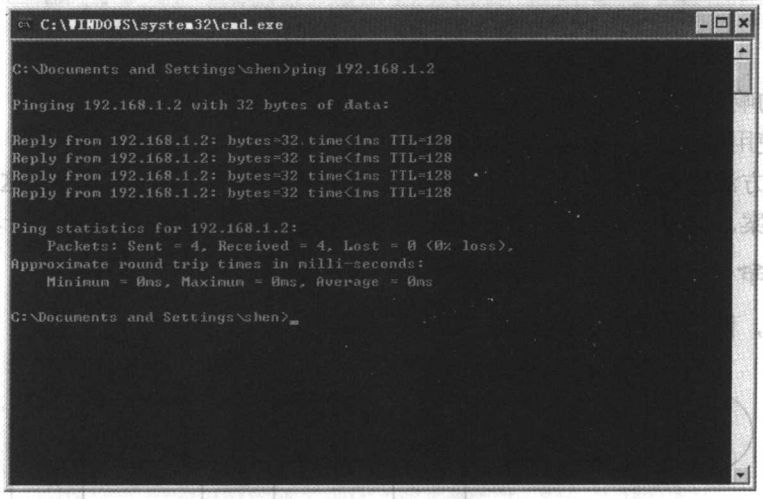


图 1-1-3　Ping 命令用法 1

从这个显示结果中我们可以看到，ping 命令向目标主机发送了 4 个 32 字节的数据包，同样也收到了 4 个返回包，中间没有数据丢失。由于目标主机在局域网内部，请求和应答时间都很短，数据包的返回平均值为 0 ms。从 TTL=128 来判断，被 Ping 主机使用的是 Windows NT 操作系统。综合一下，看看我们获得了目标主机的多少信息：

- 目标主机是活动的。
- 主机的响应速度很快，说明离本地机的距离很近。
- 目标主机使用的是 Windows NT 操作系统。

动手做

已知目标主机域名的 Ping 命令探测方法

在命令行状态下键入：Ping www.uestc.edu.cn，返回信息如图 1-1-4 所示。

从返回结果中我们可以得到电子科大网站www.uestc.edu.cn 的以下信息：

- 目标主机是活动的。
- 网站的 IP 地址为：202.112.15.104。

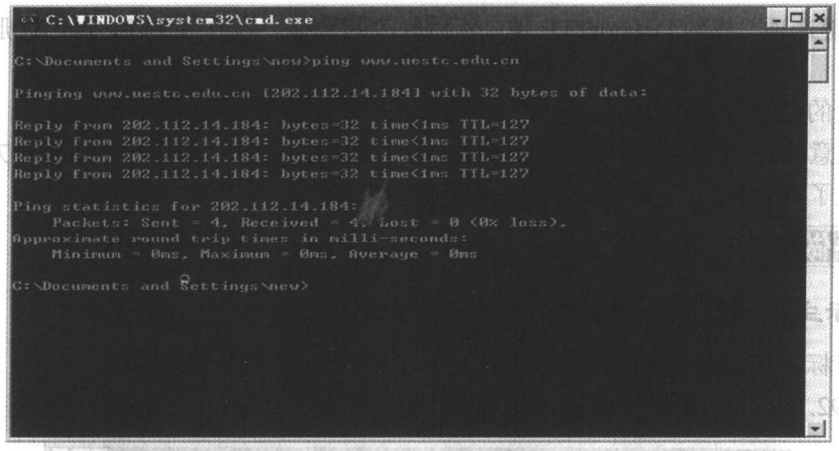


图 1-1-4　Ping 命令用法 2

- 网站的响应速度< 0 ms。
- 网站使用的是 Windows NT 操作系统。

上面两种方法探测到的信息对网络攻击者来说十分重要，他们可以根据这些信息制定进一步的入侵方案。此外，在 Ping 命令中加上- t 参数也是实施 DDoS 攻击的一种方法。

用 Tracert 命令进行简单的网络结构探测

一般说来，网络的基本结构如图 1-1-5 所示。

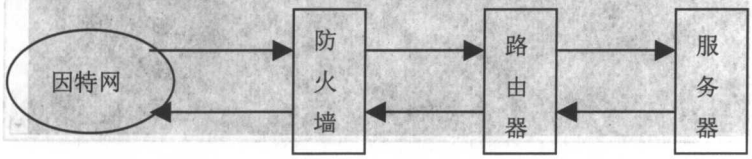


图 1-1-5　网络的基本结构

作为路由跟踪命令，执行 Tracert 命令可以获得本地到达目标主机所经过的路径、节点 IP 及到达每个节点所用的时间等信息。命令的基本格式为：

Tracert 目标主机 IP（或域名）。它有以下几个主要的参数：

-d 不解析目标主机的名字。

-h 指定搜索到目标地址的最大跳跃数。

-j 按主机列表中的地址释放源路由。

-w 指定超时时间的间隔，程序默认的时间单位是毫秒。

通过以上的学习我们知道，Ping 命令中有一个 TTL 参数，该参数是用来指定 ICMP 包存活时间的。Tracert 命令中也使用了这个参数，但这里的存活时间是指数据包所能经过的节点总数。例如，如果 ICMP 包的 TTL 值为 2，那么这个包只能传到网络上相邻的第二个节点。如果被设置成 1，就只能传到相邻的第一个节点了。Tracert 就是根据这一原理工作的。从本地向目标执行 Tracert 命令时，ICMP 数据包的 TTL 值为“1”，此后数据包每经过一个网络设备，TTL 值就自动加 1，然后显示每个设备的回应，从而探知网络路径中的每个节点。