普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇
网络侦查与电子物证系列丛书主编：秦玉海

网络安全基础

徐国天 主 编
段严兵 副主编
秦玉海 审

Information Security

http://www.tup.com.cn

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

网络安全基础

徐国天 主 编

段严兵 副主编

Information Security

http://www.tup.com.cn

清华大学出版社

北 京

内 容 简 介

本书共分为11章，按照TCP/IP协议族的层次结构，从下至上按照数据链路层、网络层、传输层、应用层的次序展开，重点研究各层主要协议的基本原理、相关协议存在的漏洞以及利用这些安全漏洞实施的网络攻击和攻击痕迹的提取分析方法。

本书主要的学习目标包括：掌握借助Sniffer Pro来分析各种网络协议的方法，学习利用协议漏洞实施的网络攻击，掌握网络设备的配置方法，掌握在网络设备中提取入侵痕迹的方法。

传统的计算机网络教材侧重讲解TCP/IP的基本原理，与之不同，本书重点讲解TCP/IP的相关安全漏洞，以及如何利用这些安全漏洞实施网络攻击。与普通的网络安全类教材重点讲解安全漏洞的防御措施不同，本书侧重研究网络攻击之后如何提取入侵痕迹。与普通的计算机网络教材直接讲解协议原理不同，本书借助协议分析仪Sniffer Pro来学习网络协议，这样能使学生对网络协议有一个清晰、直观的认识。

本书可用于国内公安院校的网络安全类专业本科生教学，也可作为地方大学的计算机类、信息类相关专业本科生参考用书。

图书在版编目(CIP)数据

网络安全基础/徐国天主编. --北京：清华大学出版社，2014
高等院校信息安全专业系列教材
ISBN 978-7-302-34859-7

Ⅰ. ①网… Ⅱ. ①徐… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2013)第310946号

责任编辑：张　民　薛　阳
封面设计：常雪影
责任校对：焦丽丽
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：19.25　　**字　　数**：447千字
版　　次：2014年5月第1版　　**印　　次**：2014年5月第1次印刷
印　　数：1～2000
定　　价：39.50元

产品编号：056302-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专

家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个信息安全专业指导性专业规范，于2012年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》（由清华大学出版社正式出版）。“高等院校信息安全专业系列教材”在教育部高等学校信息安全专业教学指导委员会的指导下，根据《高等学校信息安全专业指导性专业规范》组织编写和修订，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断完善。

我们的E-mail地址：zhangm@tup.tsinghua.edu.cn；联系人：张民。

“高等院校信息安全专业系列教材”编审委员会

前言

随着信息科学的快速发展，网络攻防技术的新旧更替速度也在加快，两年前的入侵技术，现在可能已经过时。与网络攻防技术的快速更新、换代相比，TCP/IP 的更新相对缓慢，多年前推出的 IPv6 协议至今仍未完全替代 IPv4 协议。这导致 TCP/IP 的漏洞利用技术成为相对稳定的网络攻击技术。目前国内高校普遍将研究重点放在 TCP/IP 本身及各类私有协议分析上，忽视了协议相关漏洞的深入研究。“网络安全基础”教材就是在这个背景下提出的，它在分析协议基本原理的基础之上，重点研究协议的相关漏洞，通过具体实例讲解如何利用这些漏洞，既有理论知识，又有实践操作，可以使学生对 TCP/IP 的相关漏洞有一个全面的了解。

传统的计算机网络教材侧重讲解 TCP/IP 的基本原理，与之不同，本书重点讲解 TCP/IP 的相关安全漏洞，以及不法分子是如何利用这些安全漏洞的。与普通的网络安全类教材重点讲解安全漏洞的防御措施不同，本书侧重研究网络攻击之后如何提取入侵痕迹。与普通的计算机网络教材直接讲解协议原理不同，本书借助协议分析仪 Sniffer Pro 来学习网络协议，这样能使学生对网络协议有一个清晰、直观的认识。

本书共分为 11 章，按照 TCP/IP 协议族的层次结构，从下至上按照数据链路层、网络层、传输层、应用层的次序展开，重点研究各层主要协议的基本原理、相关协议存在的漏洞、利用这些安全漏洞实施的网络攻击，以及攻击痕迹的提取分析方法。各章节具体安排如下：

第 1 章 网络安全基础概述。介绍基本概念和常用网络命令，重点讲解网络协议的层次结构、虚拟机技术和协议分析仪 Sniffer Pro 的使用。

第 2 章 数据链路层及其安全问题。重点讲解交换机的地址学习机制，以及针对交换机的 MAC-PORT、生成树和 MAC 地址攻击。

第 3 章 IP 协议及其安全问题。重点讲解网络地址转换（NAT）和网络层的安全协议 IPSec。

第 4 章 ARP 及 ARP 欺骗。重点讲解 ARP 欺骗、“中间人”攻击、“半中间人”攻击、DNS 欺骗，以及 ARP 欺骗的线索调查方法。

第 5 章 RIP 及其安全问题。重点讲解基于 RIP 欺骗的“中间人”攻击和“黑洞”攻击。

第 6 章 OSPF 协议及其安全问题。重点讲解基于 OSPF 路由欺骗的网

络监听和“黑洞”攻击。

第 7 章 ICMP 及其安全问题。重点讲解基于 ICMP 重定向的“半中间人”攻击、基于 DNS 协议和 ICMP 重定向的数据监听方法。

第 8 章 运输层协议及其安全问题。重点讲解 TCP 和 UDP 端口扫描。

第 9 章 SMTP/POP3 及 DNS 协议。重点讲解利用 Sniffer 学习发送邮件的通信过程，利用 Sniffer 追查盗号木马线索的方法。

第 10 章 HTTP 及其安全问题。重点介绍 HTTP 的三种提交参数方式，即 GET、POST 和 Cookie 方式，以及数据加密协议 SSL。

第 11 章 FTP 及其安全问题。重点讲解控制连接和数据连接的建立过程，以及利用 Sniffer 分析 FTP 的通信过程。

本书的主要学习内容包括：常用网络协议的漏洞及利用方法；常见网络服务器的搭建方法；网络设备的使用方法；网络入侵痕迹的提取方法。

本书主要的学习目标包括：掌握借助 Sniffer Pro 来分析各种协议的方法；学习利用协议漏洞实施的网络攻击；掌握网络设备的配置方法；掌握在网络设备中提取入侵痕迹的方法。

本书可用于公安院校的网络安全类专业本科生教学，也可作为地方大学的计算机类、信息类相关专业本科生参考用书。

本书第 1.2 节由武晓飞编写，第 2.1 节由肖萍编写，第 4.1 节由郭睿编写，第 8、9 章由段严兵编写，其他章节由徐国天编写。本书作者多年从事网络安全类课程的教学工作，有丰富的教学实践经验，但书中难免存在疏漏或不当之处，恳请各位读者批评指正。

编　者

2014 年 1 月

目 录

第 1 章　网络安全基础概述 …… 1

1.1　基本概念和常用网络命令 …… 1

1.1.1　基本概念 …… 1

1.1.2　常用网络命令的使用 …… 1

1.2　虚拟机技术 …… 4

1.3　网络协议的层次结构 …… 7

1.4　协议分析仪 Sniffer Pro 的使用 …… 9

思考题 …… 15

第 2 章　数据链路层及其安全问题 …… 16

2.1　以太网数据链路层帧格式 …… 16

2.2　交换机的地址学习机制 …… 17

2.2.1　交换机的地址学习过程 …… 17

2.2.2　测试交换机的 MAC 地址学习机制 …… 19

2.3　MAC-PORT 攻击 …… 21

2.3.1　MAC-PORT 攻击原理 …… 21

2.3.2　测试 MAC-PORT 地址攻击 …… 22

2.4　生成树机制 …… 25

2.4.1　冗余链路 …… 25

2.4.2　重复帧、循环问题和 MAC 地址表不稳定问题 …… 26

2.4.3　生成树 …… 29

2.4.4　测试生成树机制 …… 31

2.5　生成树攻击 …… 34

2.5.1　利用生成树攻击达到使网络拓扑不稳定和拒绝服务的攻击效果 …… 34

2.5.2　测试生成树攻击 …… 36

2.5.3　利用生成树攻击实施数据监听 …… 39

2.5.4　模拟利用生成树攻击实施的数据监听 …… 40

2.6　MAC 地址攻击 …… 44

思考题 …… 45

第 3 章　IP 协议及其安全问题 …… 46
3.1　IP 地址 …… 46
3.2　IP 协议 …… 46
3.2.1　IP 数据报格式 …… 47
3.2.2　IP 数据报的分片和重组 …… 48
3.3　泪滴攻击 …… 51
3.4　网络地址转换 …… 52
3.4.1　专用地址 …… 52
3.4.2　网络地址转换概述 …… 53
3.4.3　同时使用 IP 地址和端口号 …… 53
3.4.4　利用静态 NAT 实现因特网主机访问局域网服务器 …… 56
3.5　网络层的安全协议 IPSec …… 57
3.5.1　测试开通 IPSec 通道、采用 AH 协议、提供完整性校验 …… 58
3.5.2　测试开通 IPSec 通道、选择 ESP、提供完整性 …… 61
3.5.3　测试开通 IPSec 通道、选择 ESP、提供保密性和完整性 …… 62
思考题 …… 63

第 4 章　ARP 及 ARP 欺骗 …… 65
4.1　地址解析协议 ARP …… 65
4.2　ARP 数据报的格式 …… 66
4.3　ARP 缓存表 …… 69
4.4　ARP 欺骗 …… 70
4.5　基于 ARP 欺骗的“中间人”攻击 …… 75
4.5.1　“中间人”攻击简介 …… 75
4.5.2　测试“中间人”攻击 …… 75
4.6　利用网关实施的 ARP 欺骗 …… 81
4.7　针对网关实施 half ARP spoof 攻击 …… 85
4.7.1　针对网关实施 half ARP spoof 攻击的基本原理 …… 85
4.7.2　针对网关实施 half ARP spoof 攻击的危害 …… 86
4.7.3　half ARP spoof 攻击测试 …… 90
4.8　ARP 欺骗攻击者的调查方法 …… 95
4.9　基于 ARP 欺骗的网站挂马测试 …… 96
4.9.1　基于 ARP 欺骗的网站挂马简介 …… 96
4.9.2　测试环境和测试目的 …… 96
4.9.3　测试步骤 …… 97
4.10　基于 ARP 欺骗的 DNS 欺骗 …… 105
4.10.1　域名 …… 105
4.10.2　域名解析过程 …… 105

4.10.3 hosts 文件及其安全隐患 …… 106
4.10.4 配置 DNS 服务器 …… 107
4.10.5 DNS 缓存表 …… 110
4.10.6 DNS 报文分析 …… 110
4.10.7 基于 ARP 欺骗的 DNS 欺骗测试 …… 111
思考题 …… 120

第 5 章 RIP 及其安全问题 …… 121
5.1 路由器的工作原理 …… 121
5.1.1 路由表的组成 …… 121
5.1.2 路由器转发数据报的工作流程 …… 122
5.1.3 路由协议 …… 123
5.2 路由选择信息协议 …… 124
5.2.1 RIP 选择的是经过最少路由器的路由 …… 124
5.2.2 RIP 使用的路由表 …… 124
5.2.3 RIP 的三个特点 …… 125
5.3 Bellman-Ford 算法生成路由表 …… 125
5.4 RIP 形成路由表的过程 …… 127
5.5 当网络拓扑变化时 RIP 调整路由表的过程 …… 130
5.6 利用 RIP 组建网络 …… 132
5.7 RIP 数据报的格式 …… 135
5.8 RIP 路由欺骗 …… 136
5.8.1 基于 RIP 欺骗的“中间人”攻击 …… 136
5.8.2 “黑洞”攻击 …… 137
5.9 基于 RIP 路由欺骗的网络监听 …… 139
5.9.1 测试环境 …… 139
5.9.2 测试目的 …… 139
5.9.3 测试步骤 …… 139
5.10 RIP 的优缺点 …… 145
思考题 …… 145

第 6 章 OSPF 协议及其安全问题 …… 146
6.1 开放式最短路径优先 …… 146
6.1.1 Dijkstra 算法 …… 146
6.1.2 使用 OSPF 协议组建网络 …… 147
6.2 基于 OSPF 路由欺骗的网络监听 …… 152
6.2.1 OSPF 路由欺骗研究环境 …… 152
6.2.2 攻击者发布伪造的链路状态通告报文 …… 153

6.2.3 路由器应用 Dijkstra 算法更新自己的路由表 …… 154
6.3 基于 OSPF 路由欺骗的“黑洞攻击” …… 156
6.3.1 “黑洞攻击”的基本原理 …… 156
6.3.2 利用“黑洞攻击”截获敏感信息 …… 159
6.3.3 利用“黑洞攻击”进行木马植入 …… 160
6.3.4 通过实验验证“黑洞攻击” …… 161
6.4 基于数据链路状态数据库的网络拓扑绘制 …… 168
6.4.1 区域内网络拓扑主动发现方法 …… 168
6.4.2 数据链路类型 …… 168
6.4.3 根据链路数据库绘制网络拓扑 …… 169
6.4.4 通过实验验证主动的网络拓扑绘制方法 …… 170
思考题 …… 178

第 7 章 ICMP 及其安全问题 …… 179
7.1 ICMP 报文的类型 …… 179
7.2 计算机的路由表 …… 179
7.2.1 计算机路由表的作用 …… 179
7.2.2 计算机路由表测试实验 …… 179
7.3 ICMP 重定向 …… 182
7.3.1 ICMP 重定向过程 …… 182
7.3.2 ICMP 重定向报文结构 …… 183
7.3.3 ICMP 重定向测试实验 …… 184
7.4 基于 ICMP 重定向的“半中间人”攻击 …… 186
7.4.1 基于 ICMP 重定向的“半中间人”攻击过程 …… 186
7.4.2 伪造的 ICMP 重定向报文结构分析 …… 187
7.4.3 利用“ICMP 重定向攻击”实施数据监听实验 …… 188
7.5 基于 DNS 协议和 ICMP 重定向的数据监听方法 …… 192
7.5.1 基于 DNS 协议和 ICMP 重定向的数据监听流程 …… 193
7.5.2 通过 ICMP 重定向在受害者主机中添加到达 DNS 服务器的路由信息 …… 193
7.5.3 截获并转发 DNS 数据报 …… 194
7.5.4 监听通信数据、提取敏感信息 …… 196
7.6 基于 DNS 协议和 ICMP 重定向的数据监听实验 …… 197
7.6.1 测试环境 …… 197
7.6.2 测试目的 …… 197
7.6.3 测试步骤 …… 197
思考题 …… 205

第 8 章　运输层协议及其安全问题 …… 206
8.1　运输层协议概述 …… 206
8.2　用户数据报协议 …… 209
8.2.1　UDP 概述 …… 209
8.2.2　UDP 用户数据报的首部 …… 209
8.3　传输控制协议 …… 210
8.3.1　TCP 概述 …… 210
8.3.2　TCP 报文段的首部 …… 211
8.3.3　利用 Sniffer 分析三次握手建立 TCP 连接 …… 214
8.3.4　利用 Sniffer 分析四次挥手释放 TCP 连接 …… 216
8.4　端口扫描 …… 219
8.4.1　TCP 端口扫描 …… 220
8.4.2　UDP 端口扫描 …… 226
8.5　SYN Flood 攻击和 Land 攻击 …… 228
思考题 …… 228

第 9 章　SMTP/POP3 及 DNS 协议 …… 229
9.1　邮件协议概述 …… 229
9.2　搭建电子邮件服务器 …… 230
9.3　利用 Sniffer 学习发送邮件的通信过程 …… 233
9.4　利用 Sniffer 学习接收邮件的通信过程 …… 241
9.5　利用 Sniffer 追查盗号木马线索 …… 243
9.6　因特网的域名结构 …… 245
9.7　域名服务器进行域名解析 …… 246
9.8　DNS 欺骗 …… 249
思考题 …… 250

第 10 章　HTTP 及其安全问题 …… 251
10.1　HTTP 的工作流程 …… 251
10.2　HTTP 的报文格式 …… 253
10.3　HTTP 使用 GET、POST 和 Cookie 方式提交数据 …… 256
10.3.1　GET 方式提交参数 …… 256
10.3.2　POST 方式提交参数 …… 258
10.3.3　Cookie 方式提交参数 …… 258
10.4　HTTP 的缓存机制 …… 261
10.5　HTTP 数据加密协议 SSL …… 265
10.5.1　数字证书 …… 265
10.5.2　CA 认证中心颁发数字证书 …… 266

10.5.3 数字证书的真实性验证 …… 266
10.5.4 数字证书使用的 SSL 协议 …… 267
10.5.5 配置只使用服务器证书的 SSL 加密通道 …… 268
10.5.6 配置同时使用服务器证书和客户证书的 SSL 加密通道 …… 276
思考题 …… 280

第 11 章 FTP 及其安全问题 …… 281
11.1 FTP 服务器的搭建和使用 …… 281
11.2 FTP 使用两条逻辑连接 …… 283
11.3 控制连接和数据连接的建立过程 …… 284
11.3.1 控制连接的建立 …… 284
11.3.2 服务器主动方式建立数据连接(PORT 方式) …… 284
11.3.3 客户主动方式建立数据连接(PASV 方式) …… 285
11.4 FTP 的数据传送过程 …… 286
11.4.1 目录数据的传送过程 …… 286
11.4.2 文件数据的传送过程 …… 287
11.5 利用 Sniffer 分析 FTP 的通信过程 …… 288
11.6 测试防火墙对 FTP 数据通信的影响 …… 291
11.6.1 开启 FTP 服务器端的防火墙并允许 21 端口、测试 FTP 数据通信 …… 291
11.6.2 禁用 FTP 服务器的 PASV 功能,测试 FTP 通信能否进行 …… 293
思考题 …… 294

第1章 网络安全基础概述

1.1 基本概念和常用网络命令

1.1.1 基本概念

(1) MAC 地址：由 6 个字节组成，用于在局域网内部实现主机到主机的通信。

(2) IP 地址：由 4 个字节组成，用于实现跨越不同网络的主机到主机的通信。

(3) 端口号：是一个整数，取值区间为 0～65 535，每个端口对应一个应用层协议，0～1023 保留给知名协议，实现进程到进程的通信。图 1-1 给出的是基于 TCP 的知名应用层协议的端口号。

端口	协议
7	Echo
20	FTP, data
21	FTP, control
23	Telnet
25	SMTP
53	DNS
80	HTTP
111	RPC

图 1-1 使用 TCP 的知名协议的端口号

1.1.2 常用网络命令的使用

1. 使用 ipconfig 命令查看本机的 IP 地址

使用 ipconfig 命令可以查看本机的 IP 地址、子网掩码、默认网关。使用方法为：单击“开始”→“运行”选项，输入“cmd”，单击“确定”按钮，在出现的 DOS 窗口中输入 ipconfig 后回车。图 1-2 为使用 ipconfig 命令查看到的本机的地址信息。

2. 使用 ipconfig /all 命令查看本机的全部地址信息

使用 ipconfig /all 命令查看本机的全部地址信息，包括 DNS 服务器的 IP 地址和本机的 MAC 地址。图 1-3 为使用 ipconfig /all 命令查看到的本机的全部地址信息。

3. 使用 netstat -an 命令查看本机的网络连接情况

使用 netstat -an 命令查看本机的网络连接情况，也可以了解本机端口开放情况。图 1-4 为 netstat -an 的执行结果。结果包括 4 个字段，依次为协议类型、本地地址、远程

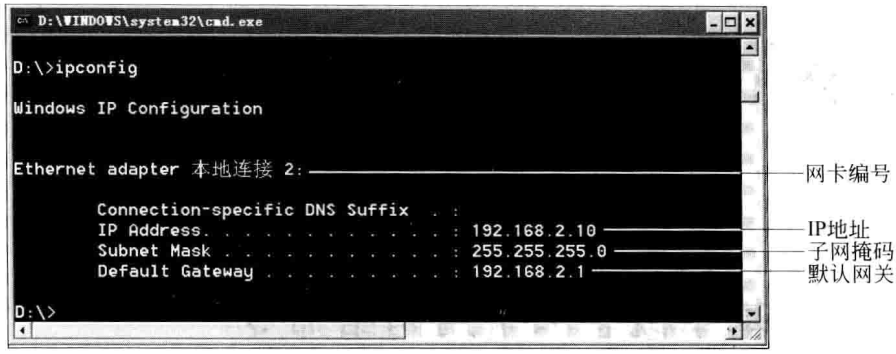

图 1-2　使用 ipconfig 命令查看到的本机的地址信息

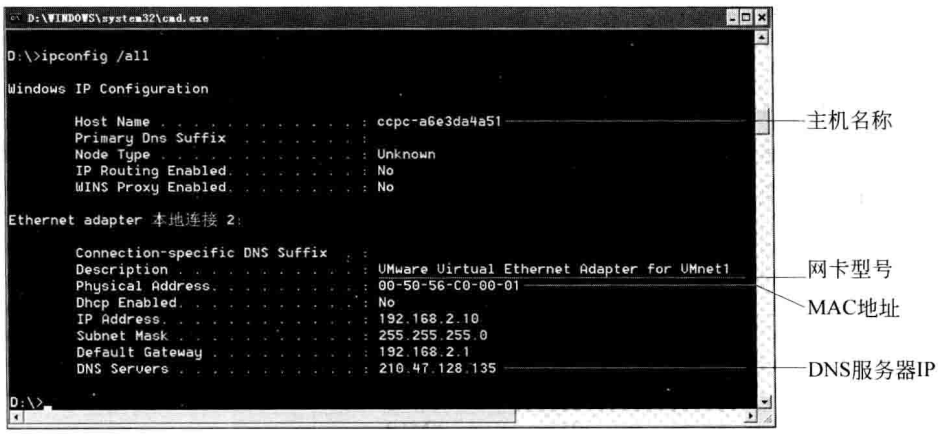

图 1-3　使用 ipconfig /all 命令查看到的本机的全部地址信息

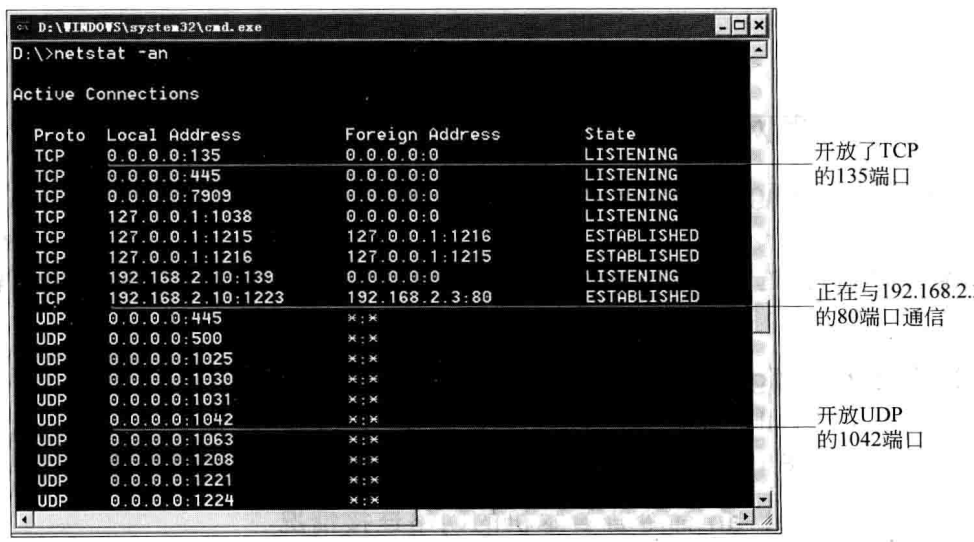

图 1-4　netstat -an 的执行结果

地址、状态。第 1 条记录中的 0.0.0.0 代表本机所有的 IP 地址(注：计算机可能安装多块网卡，因此可能存在多个 IP 地址)，它表明本机在所有 IP 地址上开放了 TCP135 端口。第 7 条记录表明本机在 IP 地址 192.168.2.10 上开放了 139 端口。第 8 条记录表明本机正在使用 IP 地址 192.168.2.10 和端口 1223 与远程主机 192.168.2.3 的 80 端口进行 TCP 通信，且连接状态为已建立。这条记录说明本机正在浏览 Web 服务器的主页。第 14 条记录说明本机在所有 IP 地址上开放了 UDP 的 1042 端口。

4. 使用 ping 命令测试网络通信状态

使用 ping 命令可以测试网络通信状态，执行该命令的主机将向目标主机发送 4 个 ICMP 请求报文，目标主机会返回 4 个 ICMP 应答报文，如果这些报文能够正常传输，说明通信线路正常。因此该命令通常用于测试通信线路是否正常工作。图 1-5 为在本机执行 ping 命令的结果。从统计结果可知，本机发送了 4 个 ICMP 请求报文，对方返回 4 个 ICMP 应答报文，这说明通信线路正常。

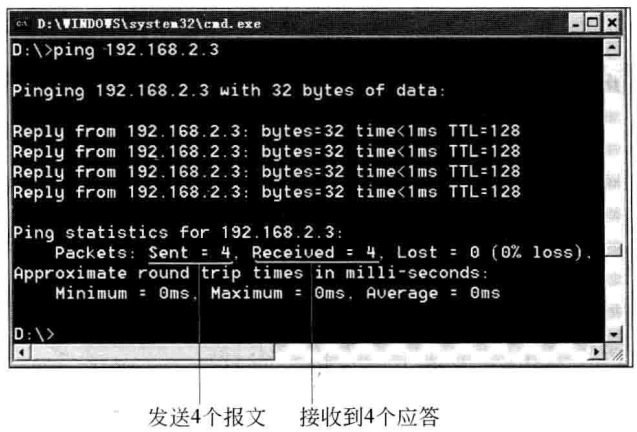

图 1-5　通信正常时 ping 命令的结果

图 1-6 为通信中断时 ping 命令的执行结果，从结果可知，本机向目标主机发送了 4 个 ICMP 请求报文，但是没有收到应答报文，因此可以判断通信中断。

图 1-6　通信中断时 ping 命令的执行结果