21世纪高职高专规划教材

高等职业教育规划教材编委会专家审定

JISUANJI WANGLUOANQUAN JISHU
SHIYAN JIAOCHENG

计算机网络安全技术实验教程

周绯菲 何 文 主 编
夏永恒 孙春兴 副主编

北京邮电大学出版社
www.buptpress.com

21世纪高职高专规划教材

计算机网络安全技术实验教程

周绯菲　何　文　主　编
夏永恒　孙春兴　副主编

北京邮电大学出版社
·北京·

内 容 简 介

本书是适应计算机网络安全教学而编写的一本实验教材。本书以突出网络安全的系统性为宗旨，以分析和解决具体安全问题为目的，与网络安全原理相结合，按照由浅入深、由局部至整体的思路，对网络安全课程中的实验进行了系统分类。本书将局域网及一般网站常见的安全配置与网络攻击技术相结合，强调攻防的对立与平衡。

本书通俗易懂，注重实用。作者在多年的教学实践中，找到了实用性与学生兴趣的结合点，设计的实验技巧性和趣味性较强。考虑到不同学校实验条件的不同，实验内容大部分是基于容易搭建的 Windows 操作系统的实验环境，降低了实验开设过程中的成本。本书的实验是按由易到难的顺序设计的，教师可以根据学生的不同情况灵活布置。本书中的每个实验由实验目的、实验设备、实验步骤、实验小结等几部分组成，实验的设计既突出了各实验的独立性又注意到了实验之间的连贯性。本书注意与其他计算机课程的结合，突出了计算机知识的系统性、综合性，每个实验都与相关的计算机知识相结合，使读者建立起计算机网络安全的基本概念与基本架构。

本书不仅可以作为高职高专的计算机专业、网络管理专业、信息安全专业、通信专业的教材，也可以作为计算机网络安全的培训、自学教材，同时还可以作为网络工程技术人员、网络管理人员、信息安全管理人员的技术参考书。本书全部讲授需要 64～72 课时（含理论部分的讲授）。作为教材，授课教师可根据具体的实验室条件、专业情况以及教学计划的安排进行取舍。

图书在版编目(CIP)数据

计算机网络安全技术实验教程/周绯菲，何文主编．—北京：北京邮电大学出版社，2009
ISBN 978-7-5635-1959-0

Ⅰ．计…　Ⅱ．①周…②何…　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(2009)第 085115 号

书　　名：计算机网络安全技术实验教程
作　　者：周绯菲　何 文　夏永恒　孙春兴
责任编辑：满志文
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京源海印刷有限责任公司
开　　本：787 mm×1 092 mm　1/16
印　　张：13.25
字　　数：326 千字
印　　数：1—3 000 册
版　　次：2009 年 8 第 1 版　2009 年 8 第 1 次印刷

ISBN 978-7-5635-1959-0　　定　价：24.00 元

· 如有印装质量问题，请与北京邮电大学出版社发行部联系 ·

前　言

随着通信技术和互联网技术的发展，人们在享受网络带来便利的同时，黑客攻击、泄密等网络安全问题也变得越来越突出。只要有网络的存在，网络的安全维护就是个极其重要的问题。网络安全是指为计算机系统建立所采取的技术和管理的安全保护措施，保护计算机系统中的硬件、软件及数据，防止其因偶然、恶意的原因使系统遭到破坏、更改或泄露。网络安全是基于通信、数学、计算机等多个学科的综合概念。同时，网络安全也是一门实践性很强的课程，主要研究的就是攻击与防御。本书是针对计算机网络安全课程的特点而编写的。只有将计算机硬件、操作系统、各种应用软件、服务等理论知识的教学与实践教学相结合，才能很好地培养学生分析问题、解决问题的能力和专业实践能力。加强实践教学是培养应用型人才的重要途径，这点对于高职高专学生尤为重要。

考虑到高职高专教育的定位和学生的实际情况，本书涉及的43个实验基本覆盖了当前计算机网络安全的主要分支和主要理论。这些实验是按照由浅到深、由易到难的顺序排列的。教师可以有选择性地给学生布置，也可以在本书实验的基础上进行扩展。本书中的每个实验都由实验目的、实验设备、实验步骤、实验小结等几个部分组成。对于黑客攻击的实验，本书全部给出了防御措施。

本书由交通部管理干部学院计算机系网络教研室组织编写，本书分为网络基础及网络嗅探技术、黑客攻击技术、预防黑客攻击、攻击的检测与响应共4篇。第1篇网络基础及网络嗅探技术即第1章；第2篇黑客攻击技术由第2章漏洞扫描及网络隐身、第3章木马攻击、第4章主动攻击、第5章脚本攻击与后门账号的建立组成；第3篇预防黑客攻击由第6章Windows操作系统平台的安全设置、第7章网络通信安全组成；第4篇攻击的检测与响应即第8章。第1～8章均由周绯菲老师编写，其中第6章的Windows XP操作系统的安全设置部分以及部分截图由何文老师完成。此外，夏永恒、孙春兴、陈小全、鲁一力、汪洁、张传立等老师对本书的编写提供了大力支持，在此表示衷心感谢。

学习本书需要注意：

(1) 由于操作系统和应用软件的生产商会经常更新自己的版本，所以本书中的少数实验在讲授时可能无法看到书中展示的效果。有些实验只能在Windows 2000 Server主机上进行。有些实验使用Windows 2003 Server作为操作系统时，只能使用正版系统，否则实验不能成功。

(2) 实验中所有的计算机都有意设置了简单密码，这是为了便于实验使用，实验中也演示了简单密码的危险。

(3) 实验中所有的计算机都没有开启防火墙和杀毒软件，这是为了让大家更好地看到

实验效果。

(4) 为了保护网络实验环境，本书中没有涉及蠕虫病毒的实验，也没有涉及病毒免杀、木马免杀的实验。

(5) 为保护软件版权，本书没有涉及程序加壳与脱壳的实验。

需要声明的是，本书的编写目的是为了让读者全面了解信息安全方面的基本技术，建立起安全防范意识，不是给怀有不良动机的人提供支持，也不承担由此产生的连带责任。

本书在编写过程中参考了互联网上公布的一些相关资料，由于互联网上的资料较多，引用复杂，无法一一注明原出处，故在此声明，原文版权属于原作者。

网络安全是一门非常年轻的课程，它的内容与架构在不断地发展，其实验课程更是如此。由于作者水平有限，书中难免有不足之处，希望广大读者批评、指正，以期再版时进行修订。

作　者

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

第一篇　网络基础及网络嗅探技术

第 1 章　网络基础及网络嗅探技术

第二篇　黑客攻击技术

第 2 章　漏洞扫描与网络隐身

第 3 章　木马攻击

第 4 章　主动攻击

第 5 章　脚本攻击与后门账号的建立

第三篇　预防黑客攻击

第 6 章　Windows 操作系统平台的安全设置

第 7 章　网络安全通信

第四篇　攻击的检测与响应

第 8 章　攻击的检测与响应

第一篇　网络基础及网络嗅探技术

第1章 网络基础及网络嗅探技术

实验 1-1 Windows 网络通信分析(Ethereal)

Ethereal 是一个强大的协议嗅探器,网络专业人士可以用它来检修故障和分析网络通信量。对于管理员来说,它是一个用来识别黑客攻击战略方法的有价值的工具。它可以帮助观察各种不同的协议是如何工作的。

一、实验目的

了解 Windows 网络中的 ARP 通信会话数据包的结构;
掌握使用 Ethereal 进行数据包捕获、过滤的方法。

二、实验设备

2 台 Windows 主机:1 台 Windows XP 主机,1 台 Windows 2000 Server 主机。

三、实验步骤

(1) 在 Windows XP Professional PC 上登录。

(2) 清除 ARP 缓存。

ARP 缓存是一个内存区域,计算机将所发现的信息存储在 ARP 表中。在启动捕获会话之前清除 ARP 缓存可以更好地控制所捕获的数据。

① 在"开始"任务条菜单上→运行→输入"cmd",并单击"确定"按钮。

② 在 DOS 命令行窗口中,输入"arp -a"并按 Enter 键。此处不应该出现任何条目,如果有的话,用 arp -d 命令清除它们。

(3) 启动 Ethereal 并捕获一个通信会话。

① 在 Windows XP 主机上安装并启动 Ethereal。

② 在 Ethereal 界面中→Capture 菜单→Options→选择网络接口卡类型,如图 1-1所示。

③ 回到命令提示符窗口,输入 ping 192.168.0.250(Windows 2000 Server 的 IP),只

此为试读,需要完整PDF请访问: www.ertongbook.com

要局域网保持正常通信状态就会收到 4 条回复。

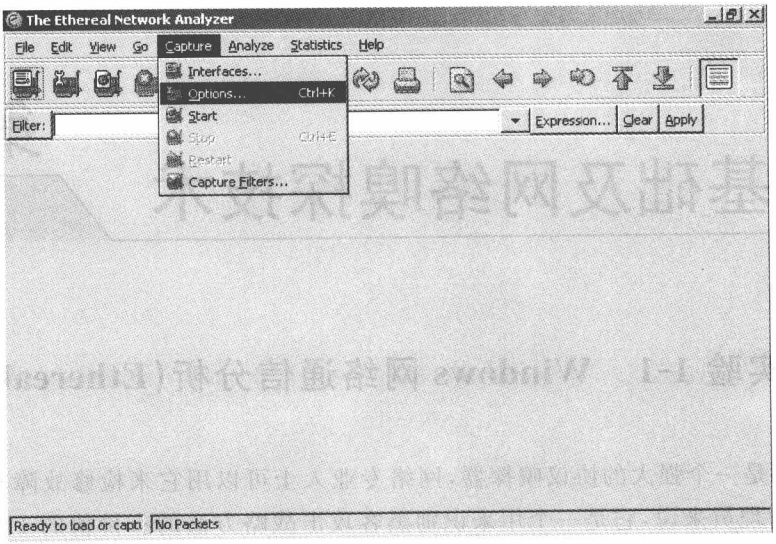

图 1-1　Windows 中的 Ethereal 程序

(4) 在 Ethereal 界面中单击“Capture”菜单→Stop，如图 1-2 所示，会发现捕获到的很多是 ICMP 数据包，如图 1-3 所示。

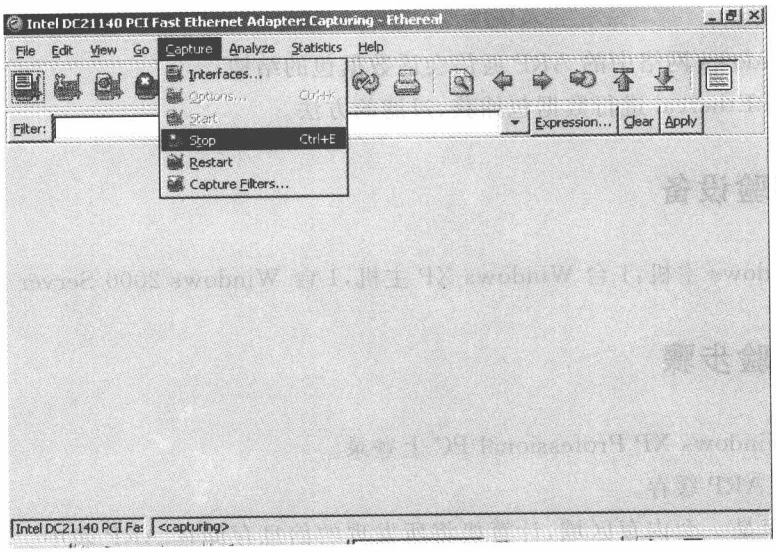

图 1-2　停止截获数据包

(5) 检查捕获的会话。

Ethereal 的主界面分为三部分。

数据包列表部分居于顶部。这部分展示了捕获的数据包的概要。单击这个部分中的任何一个数据包就可以在另外两个部分中显示更详细的信息。

树形视图部分居于中部。这一部分以树形格式展示所选数据包的详细信息。

数据视图部分位于底部。该部分以十六进制格式显示捕获的数据。任何在树形视图部分所选择的内容都将在那里高亮度显示。

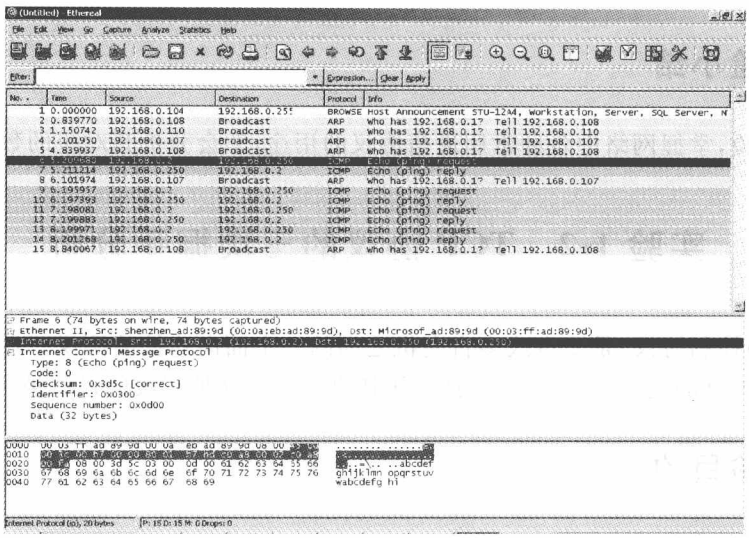

图 1-3　截获的 ICMP 数据包

在数据包列表部分有一些栏目，每一栏都提供了特定的信息。

① No.——数据包被接收的序号。

② Time——每一个数据包被捕获的时间，相对于捕获的起始时间计量。

③ Source——源地址。

④ Destination——目的地址。

⑤ Protocol——用于捕获数据包的协议。

⑥ Info——数据包概要。

(6) 过滤捕获的会话。

该软件可以获得成千上万的数据包。从头至尾进行查找数据包的工作非常麻烦。使用 Ethereal 中所含的过滤器可以帮助人们接近正在寻找的信息。

① 单击 Filter 工具条。

② 在 Filter 工具条中，输入 arp 并按 Enter 键，如图 1-4 所示。屏幕上只显示出了 ARP 数据包。

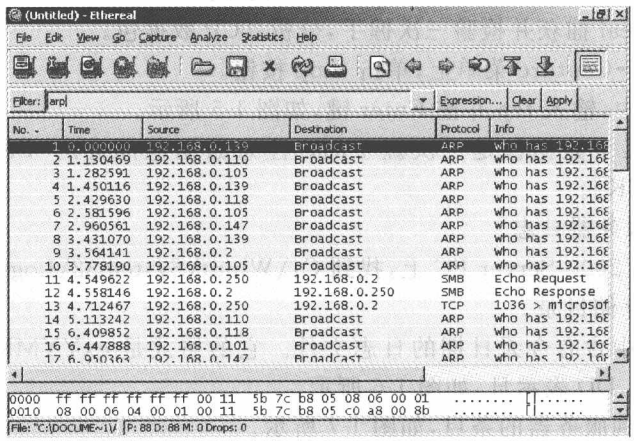

图 1-4　在 Ethereal 中使用过滤器

四、实验小结

通过本实验，掌握网络中各种常用通信协议的用途，学会分析其对应的数据包结构。

实验 1-2　TCP 协议的三次握手分析

TCP(传输控制协议)是 2 台或多台主机之间的一个面向连接的协议。在传输数据之前必须建立一条可靠的连接。2 台主机利用 TCP 协议建立这种连接的过程被称为三次握手。

一、实验目的

了解 TCP 三次握手的原理；
掌握使用 Ethereal 捕获 TCP 数据包的方法。

二、实验设备

2 台主机：1 台 Windows XP 主机，1 台 Windows 2000 Server PC(IP 为 192.168.0.250)主机。

三、实验步骤

(1) 在 Windows 2000 Server PC 上登录，并开启一个 Web 默认站点。

(2) 在 Windows XP PC 上登录，启动 Ethereal 并捕获一个 HTTP 通信会话。

① 在 Windows XP 主机上，启动 Ethereal，单击“Capture”菜单→ Options 界面→选中网络接口卡并单击 OK 按钮。

② 在 Internet Explorer 的地址栏中，输入 http://192.168.0.250(即 Windows 2000 Server PC 的 IP)，访问 Windows 2000 Server PC 的站点。

(3) 停止 Ethereal 捕获并检验三次握手，分析 TCP 数据包。

① 在 Ethereal→Capture 菜单上，单击 Stop 按钮。

② 在 Filter 框中，输入 tcp 并按 Enter 键，如图 1-5 所示。

图 1-5 中的前三个数据包是三次握手的。注意数据包部分的“Info”栏中的[SYN]、[SYN,ACK]和[ACK]。

(4) 检查网络服务器日志。

① 在 Windows 2000 Server PC 上，找到 C:\Winnt\System32\Logfiles\W3svc1\目录，这就是日志文件的存储目录。

② 双击文件名中含有今天日期的日志文件。它的格式是 exYYMMDD.log，其中 YY 表示年，MM 表示月，DD 表示日，如图 1-6 所示。

③ 定位至连接到服务器的条目，如图 1-7 所示。

④ 分析图 1-7 中各行表示的含义。

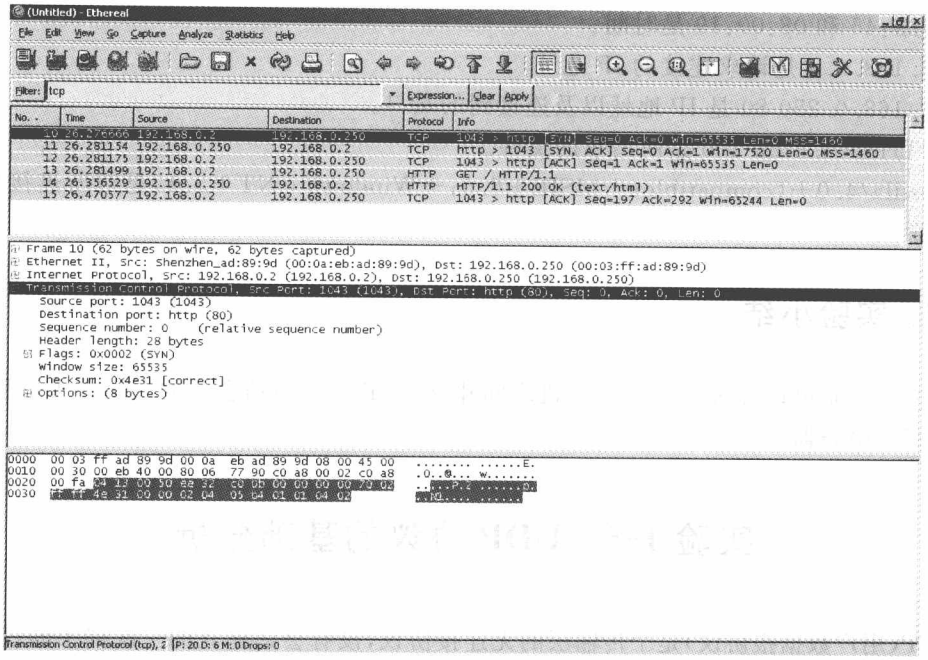

图 1-5　用 Ethereal 捕获的 Windows 中的三次握手

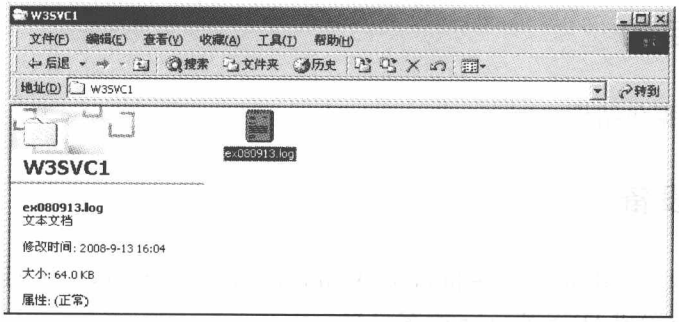

图 1-6　日志文件

2008-09-13 是以格林尼治标准时间表示的日期。

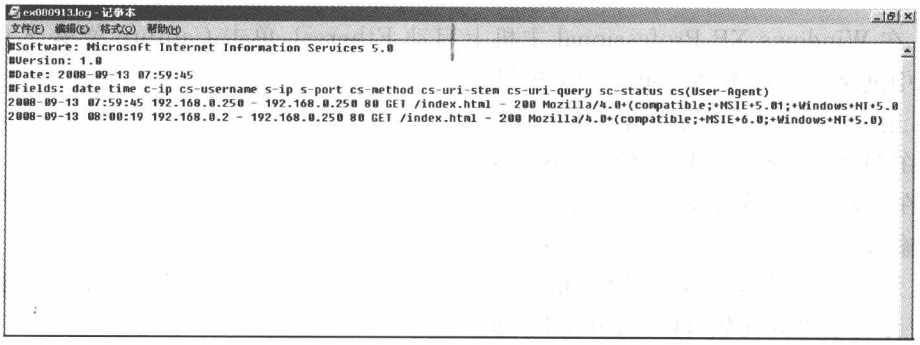

图 1-7　日志文件内容

07:59:45 和 08:00:19 是时间。

192.168.0.2 是请求连接的 IP 地址。

192.168.0.250 80 是 IP 地址以及连接到的端口。

GET/index.html-200 是所请求的文件。

Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)是对所连接的浏览器的推测。

四、实验小结

通过本实验可以详细了解 2 台主机之间建立 TCP 协议通信会话的三次握手过程，并学会分析网络服务器日志。

实验 1-3　UDP 协议的基础分析

UDP(用户数据报协议)是个传输层的无连接协议，没有会话建立的三次握手的过程。它没有任何错误恢复功能，也不担保数据包准确交付。但是，UDP 显著地减少了协议管理开销。

一、实验目的

了解 UDP 数据包结构。

二、实验设备

2 台主机：1 台 Windows XP 主机，1 台 Windows 2000 Server，局域网环境中设置 DNS Server 并把自己设置成 DNS Server 的客户端。

三、实验步骤

(1) 在 Windows XP Professional 主机上启动 Ethereal，单击 Capture 菜单→ Options 界面，选中网络接口卡类型并单击 OK 按钮。

(2) 用 nslookup 命令来产生 UDP 通信。

① 在 DOS 命令行方式下，输入“nslookup”。

② 在提示符下，输入 www.jqm.com。

③ 输入 exit，并按 Enter 键退出 nslookup。

(3) 用 http 命令来产生 TCP 通信。输入“http://192.168.0.250”并按 Enter 键。

(4) 分析结果并比较 TCP 头和 UDP 头：

① 在 Ethereal 中，单击 Capture 菜单→ 单击 Stop 按钮。

② 分析 UDP 数据包。

在数据包部分，选中在协议栏中列出了 DNS 的第一个数据包项，如图 1-8 所示。观察显示的信息：源端口是什么，目的端口是什么，校验值是什么？

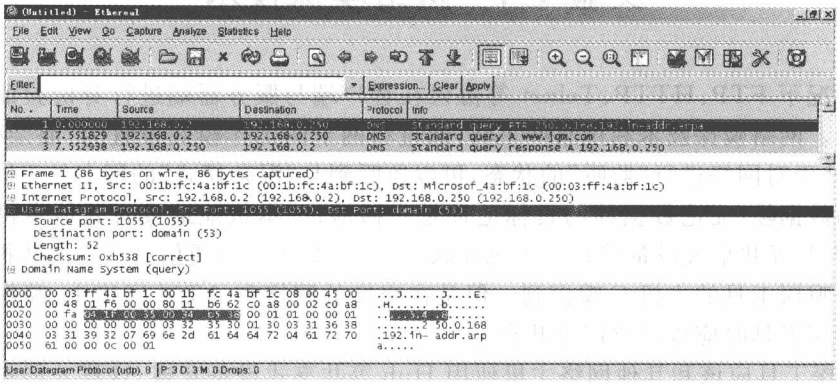

图 1-8　UDP 头截图

③ 分析 TCP 数据包：

在数据包部分，选中在协议栏中列出了 TCP 的第一个数据包项，如图 1-9 所示。在树形视图部分，展开 Transmission Control Protocol 项。观察显示的信息、源端口、目的端口、校验值，注意 TCP 头和 UDP 头之间有什么不同？

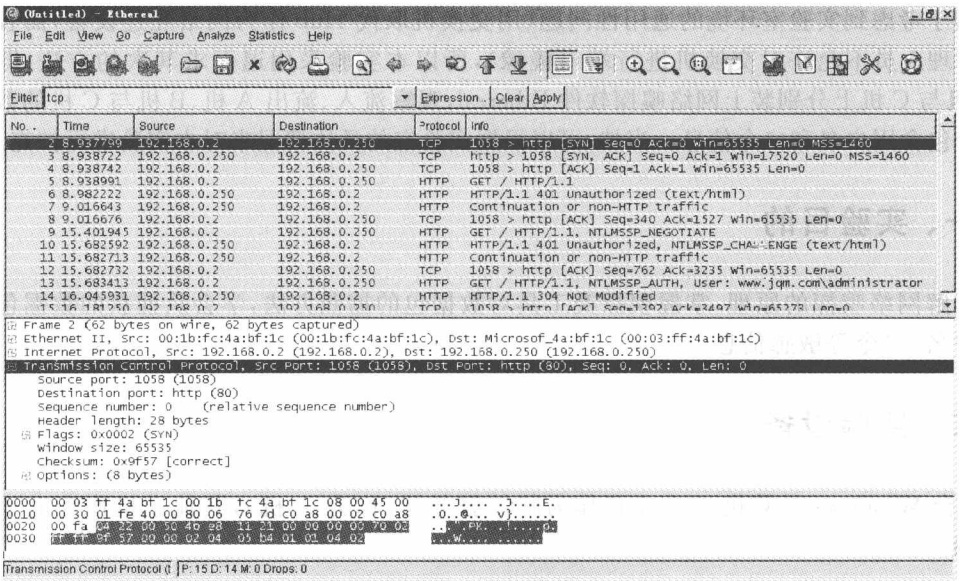

图 1-9　TCP 头截图

四、实验小结

通过本次实验可以获得 UDP 协议数据包的结构信息，并可比较出 UDP 协议与 TCP 协议数据包的不同。

此为试读，需要完整PDF请访问：www.ertongbook.com