A COURSE OF INFORMATION SECURITY AND APPLICATION PROGRAMMING EXPERIMENTS

信息安全与应用编程实验教程

主　编　姜　斌　吕秋云
副主编　朱　芳　唐向宏

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

信息安全与应用编程实验教程

主　编　姜　斌　吕秋云
副主编　朱　芳　唐向宏

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

内容简介

本书主要包括了四大部分实验：信息安全基础操作实验、编程基础训练实验、密码学编程实验和网络安全编程实验。

本书压缩了繁琐的理论指导，紧扣课程实验教学的目标，注重培养学生实际动手能力，发挥学生自我动手和创造能力。对实验案例的分析和讲解，力求做到简明、清晰和准确，通过有针对性的案例实践操作，使学生更高效地掌握相关理论依据和知识。

本书既可作为信息安全、通信和计算机专业信息安全方向的本科生和研究生的实验用书，也可供企业信息安全方面教学培训学习参考。

图书在版编目（CIP）数据

信息安全与应用编程实验教程 / 姜斌，吕秋云主编.
—杭州：浙江大学出版社，2014.2
ISBN 978-7-308-12841-4

Ⅰ.①信… Ⅱ.①姜… ②吕… Ⅲ.①信息安全—高等学校—教材 ②程序设计—高等学校—教材
Ⅳ.①TP309 ②TP311.1

中国版本图书馆 CIP 数据核字（2014）第 040[illegible] 号

信息安全与应用编程实验教程

姜 斌 吕秋云 主编

责任编辑 樊晓燕(fxy@zju.edu.cn)
封面设计 十木米
出版发行 浙江大学出版社
（杭州市天目山路 148 号 邮政编码 310007）
（网址：http://www.zjupress.com）
排 版 杭州中大图文设计有限公司
印 刷 杭州杭新印务有限公司
开 本 787mm×1092mm 1/16
印 张 20
字 数 487 千
版 印 次 2014 年 2 月第 1 版 2014 年 2 月第 1 次印刷
书 号 ISBN 978-7-308-12841-4
定 价 39.00 元

前　言

随着计算机科学技术的不断发展，计算机和网络已经成为人们学习和工作的重要组成部分，而随之产生的信息安全问题也日益受到人们的关注。实际上，信息安全已成为影响国家安全、经济发展、社会稳定、公民利益的重要问题。因此，国家和社会迫切需要高素质、有实战能力的信息安全类专业人才。

目前，国内高校各级、各类信息安全技术类课程的教学过程，在夯实理论知识的基础上，都大幅度提升了实验教学的比例，而且不同课程都在不同层面上引入实验内容，以期锻炼学生的理论联系实际的能力、实际动手能力以及创新能力。然而，每门课程的实验教学内容相对零散，往往不能构成一本实验教材。因此，本书力求为各类信息安全技术理论课程提供实验教学内容，方便教师指导，方便学生学习。

本书主要包括了四大部分：

第一部分是信息安全基础操作实验，包括网络数据信息抓包与安全分析实验、常见网络攻击实验、常见网络防御实验、操作系统安全配置、数据备份与恢复实验。这部分内容可以作为信息安全导论、信息安全技术等课程的实验素材，可以加深学生对信息安全、网络安全技术的感性认识和理解。

第二部分是编程基础训练实验，包括C和C++开发环境使用实验、信息安全编程基础实验。这部分内容的主要目的是训练学生的编程调试能力、可视化界面编程能力以及信息安全基本理论编程实现的能力。此部分内容适合非专业类的信息安全程序设计课程、信息安全专业低年级编程训练课程、信息安全数学基础课程使用。

第三部分是密码学编程实验，包括古典密码算法实验、对称密码算法实验、非对称密码算法实验。这部分内容主要服务于信息安全专业的核心基础课程——密码学课程，训练学生的各类加密算法实现能力。

第四部分是网络安全编程实验，包括网络通信编程实验、网络安全编程实验。这部分内容主要作为网络安全理论与技术相关课程的实验素材。

本书压缩了繁琐的理论指导，紧扣课程实验教学的目标，注重培养学生的实际动手能力，发挥学生自我动手和创造能力。本书对实验案例的分析和讲解，力求做到简明、清晰和准确，通过有针对性的案例实践操作，使学生更高效地掌握相关理论依据和知识。

本书适合信息安全、通信和计算机专业信息安全方向的本科生和研究生进行信息安全实验，也适合于企业进行信息安全方面的教学培训等。

本书由姜斌、吕秋云担任主编，负责制定全书大纲和审稿工作。由朱芳、唐向宏担任副主编。王秋华、王小军、吴震东等也参与了教材部分章节的编写。在此特别感谢卢毅、张程浩、缪金纬、周雷雷、常涛、潘腾蛟同学在教材编写中做的大量工作。

本教材在编写过程中得到了模拟实验训练系统软件厂商的大力支持，在此向他们表示衷心的感谢。

本教材在编写过程中，参考了一些国内外的教材和学术材料，在此向这些作者表示衷心的感谢。

浙江大学出版社大力支持了本书的出版，樊晓燕编审对本书的编写给予了很多有益的建议并认真负责地审阅了全书，在此表示衷心的感谢。

由于编者的水平有限，经验不足，时间仓促，教材中难免存在错误或不完善之处，恳请广大同行和读者予以批评指正，我们将在今后再版时改正。读者可以通过电子邮件(jiangbin@hdu.edu.cn、laqyzj@hdu.edu.cn)与编者联系。

编者

2013 年 12 月于杭州电子科技大学

目　录

第 1 章　网络数据获取与安全分析实验 …… (1)

1.1　利用 Sniffer portable 软件进行数据包抓取 …… (1)
1.1.1　Sniffer portable 抓包工具使用实验 …… (1)
1.1.2　抓取一次完整的网络通信过程的数据包实验 …… (8)
1.2　利用 Sniffer portable 软件进行网络数据分析 …… (11)
1.2.1　基于协议的分析实验 …… (11)
1.2.2　基于关键字的安全分析实验 …… (13)
1.3　利用 Wireshark 软件进行数据包抓取 …… (18)
1.3.1　Wireshark 抓包工具使用实验 …… (18)
1.3.2　抓取一次完整的网络通信过程的数据包实验 …… (28)
1.4　利用 Wireshark 软件进行网络数据分析 …… (32)
1.4.1　TCP 协议的分析实验 …… (32)
1.4.2　HTTP 协议的分析实验 …… (39)

第 2 章　常见网络攻击实验 …… (46)

2.1　信息搜集实验 …… (46)
2.1.1　端口扫描实验 …… (46)
2.1.2　系统漏洞扫描实验 …… (50)
2.2　常见网络攻击实验 …… (57)
2.2.1　利用 IIS 缓冲区溢出漏洞实验 …… (57)
2.2.2　入侵网站管理系统实验 …… (62)
2.3　常见网络隐身实验 …… (65)
2.3.1　留后门实验 …… (65)
2.3.2　网络代理跳板使用实验 …… (69)

第 3 章　常见网络防御实验 …… (75)

3.1　防火墙实验 …… (75)
3.1.1　普通包过滤实验 …… (76)
3.1.2　状态检测实验 …… (80)
3.1.3　应用代理实验 …… (87)

3.2 入侵检测实验 …… (95)
3.3 病毒防护实验 …… (104)
3.3.1 网络炸弹脚本病毒 …… (104)
3.3.2 美丽莎宏病毒 …… (106)

第 4 章 操作系统安全配置 …… (110)

4.1 Windows 操作系统安全配置实验 …… (110)
4.1.1 系统安全配置实验 …… (110)
4.1.2 系统安全审核实验 …… (113)
4.1.3 NTFS 文件系统安全应用实验 …… (117)
4.2 Linux 操作系统安全设置实验 …… (119)

第 5 章 数据的备份与恢复实验 …… (126)

5.1 数据的备份与恢复 …… (126)
5.1.1 Acronis True Image 工具使用实验 …… (126)
5.1.2 数据的备份与恢复实验 …… (128)
5.2 系统的备份与恢复 …… (138)
5.2.1 系统的备份实验 …… (138)
5.2.2 误删除文件的恢复实验 …… (144)

第 6 章 C 和 C++开发环境使用实验 …… (147)

6.1 VC++6.0 开发工具使用实验 …… (147)
6.1.1 创建一个新的 C 语言的工程实验 …… (147)
6.1.2 添加一个文件到一个空的工程中实验 …… (152)
6.1.3 编写程序实验 …… (153)
6.1.4 运行程序实验 …… (156)
6.1.5 调试程序——设置断点实验 …… (158)
6.1.6 调试程序——动态察看变量的值 …… (159)
6.2 VC++6.0 下利用 MFC 实现友好界面编程实验 …… (161)
6.2.1 创建一个新 MFC 应用程序的工程实验 …… (161)
6.2.2 给对话框添加相关控件实验 …… (165)
6.2.3 编写 MFC 程序实验 …… (167)
6.3 Visual Studio 2012 开发工具使用实验 …… (169)
6.3.1 安装 Visual Studio 2012 实验 …… (170)
6.3.2 创建一个新的 C 语言的项目实验 …… (174)
6.3.3 添加一个文件到一个空的项目中实验 …… (178)
6.3.4 编写程序实验 …… (180)
6.3.5 运行程序实验 …… (182)
6.3.6 调试程序——设置断点实验 …… (183)

6.3.7　调试程序——动态察看变量的值 …… (185)
6.4　VS 2012 下利用 MFC 实现友好界面编程实验 …… (187)
6.4.1　创建一个基于对话框的 MFC 项目实验 …… (187)
6.4.2　编译运行生成的程序实验 …… (192)
6.4.3　给对话框添加相关控件实验 …… (194)
6.4.4　给控件添加消息处理函数实验 …… (196)

第 7 章　信息安全编程基础实验 …… (200)

7.1　大数的素性检测实验 …… (200)
7.2　大整数的加减法运算实验 …… (203)
7.3　利用矩阵变换实现加解密实验 …… (204)

第 8 章　古典密码算法编程实验 …… (207)

8.1　Caesar 密码 …… (207)
8.2　置换密码 …… (209)

第 9 章　对称密码算法编程实验 …… (212)

9.1　DES …… (212)
9.2　三重 DES …… (222)
9.3　AES …… (223)

第 10 章　非对称密码算法编程实验 …… (241)

10.1　RSA …… (241)
10.2　Elgamal 加密算法 …… (252)

第 11 章　网络通信编程实验 …… (255)

11.1　VC++6.0 下 CSocket 的基于 TCP 协议通信编程实验 …… (255)
11.2　VC++6.0 下 CSocket 的基于 UDP 协议通信编程实验 …… (262)
11.3　VC++6.0 下 CAsyncSocket 的基于 TCP 协议通信编程实验 …… (268)
11.4　VC++6.0 下 Socket 基于 TCP 协议的通信编程实验 …… (276)
11.5　VS2012 下 CSocket 基于 TCP 协议的通信编程实验 …… (283)

第 12 章　网络安全编程实验 …… (290)

12.1　端口扫描器编程实验 …… (290)
12.2　注册表安全防护编程实验 …… (296)
12.3　恶意代码及防护编程实验 …… (301)

第 1 章

网络数据获取与安全分析实验

网络抓包也称网络嗅探(sniffer),在信息安全业内也叫“被动扫描”。嗅探的主要目的是截获通信报文,并对报文进行分析,从而获知网络上的通信内容。完整的嗅探具体分解为如下三步:

第一步,配置嗅探环境;

第二步,开始嗅探并保存数据;

第三步,分析第二步截取的数据并挖掘有用信息。

对于网络管理者来说,掌握目标网络的数据流的分布、数据内容、存在的安全问题是必要的;对于学习网络协议、网络安全以及网络管理的学生来说,通过动手实验,获取网络中流动的数据流,分析数据流的协议、网络数据内容和网络安全问题是一项十分有效的学习手段。本章借此介绍著名的网络抓包工具 Sniffer 以及 WireShark,进行网络数据获取和安全分析实验。

1.1 利用 Sniffer portable 软件进行数据包抓取

1.1.1 Sniffer portable 抓包工具使用实验

实验目的

通过本实验对抓包工具有较深的理解,能够完成正确安装 Sniffer 软件,并且能够熟练使用 Sniffer 的主要功能模块。

实验环境

操作系统 Windows XP 或者 Windows 2000 ,抓包工具 Sniffer Portable。

实验步骤

1. Sniffer 安装主要步骤

(1) 注册使用英文

本实验使用 Sniffer Portable 4.7.5 安装包。Sniffer 的安装比较简单,一般只要按照说

明进行即可。但是，对于初次使用该软件的初学者来说，有几步需要注意。第一步需要注意的是注册软件时建议使用英文，如图 1-1 所示。

图 1-1 Sniffer 安装注册

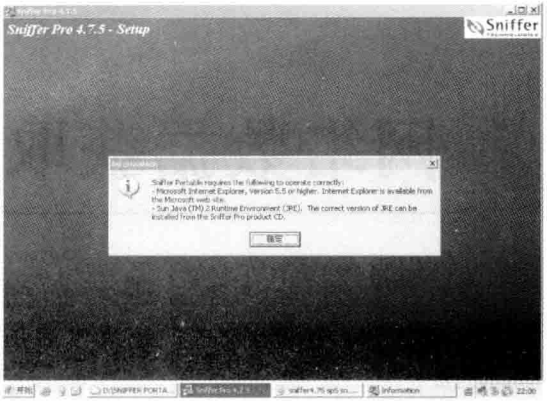


图 1-2 Sniffer 用户软件环境要求

(2) 确认用户软件环境

Sniffer Portable 对用户软件环境有要求，一般要求 IE 浏览器 5.0 以上，还要求有 Java 2 的虚拟机做支撑(主要是对 Dashboard 提供运行环境)。请用户确认，如果不能满足要求会导致 Sniffer 工作不正常(见图 1-2)。

(3) 勾选“卸载服务质量”

Sniffer Portable 为了保证抓包质量将要卸载“服务质量”，如果没有特殊要求请选择默认点击“Finish”(见图 1-3)。

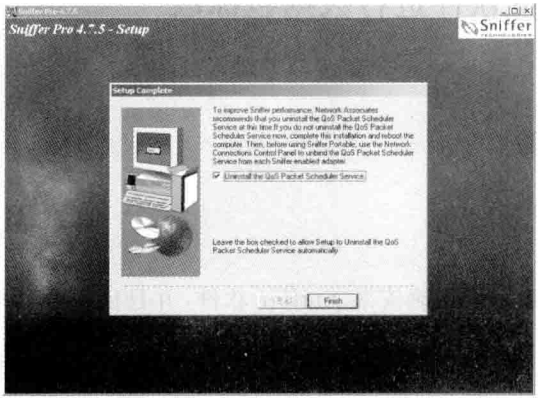


图 1-3 勾选“卸载服务质量”

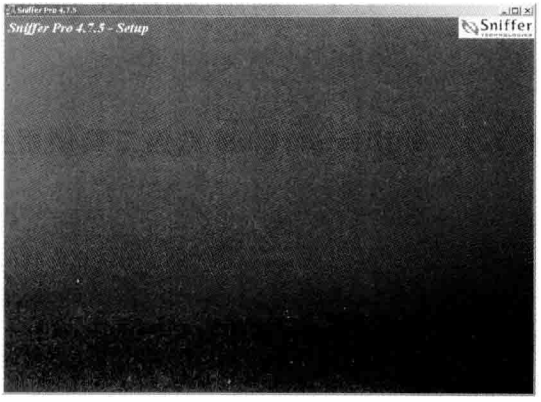


图 1-4 配置等待屏幕

(4) 等待配置窗口

在安装过程中有时屏幕会出现如图 1-4 显示画面，可能时间较长，请记住耐心等待，因为对 Sniffer Portable 的配置才刚刚开始。如果强制终止，会产生意外情况。

(5) 选择网卡

安装完成并重新启动计算机后，第一次运行时需要选择使用的网卡，如图 1-5 所示。

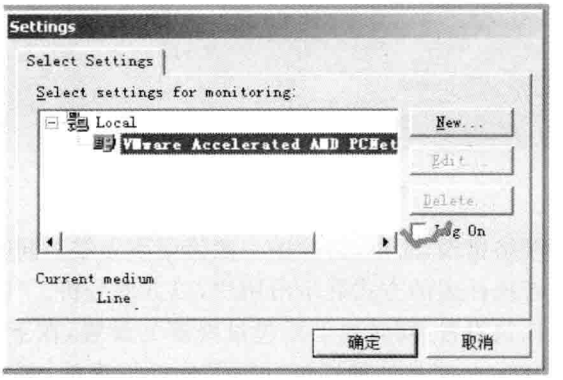


图 1-5　选择网卡

(6) 选择“总是授权”安装 Java 虚拟机

安装完成并重新启动计算机后，第一次开启 Dashboard 选项时，Sniffer Portable 将会自动安装自带的 Java 虚拟机，选择“总是授权”(见图 1-6)。由此，Sniffer Portable 已经很好地安装在计算机里了。

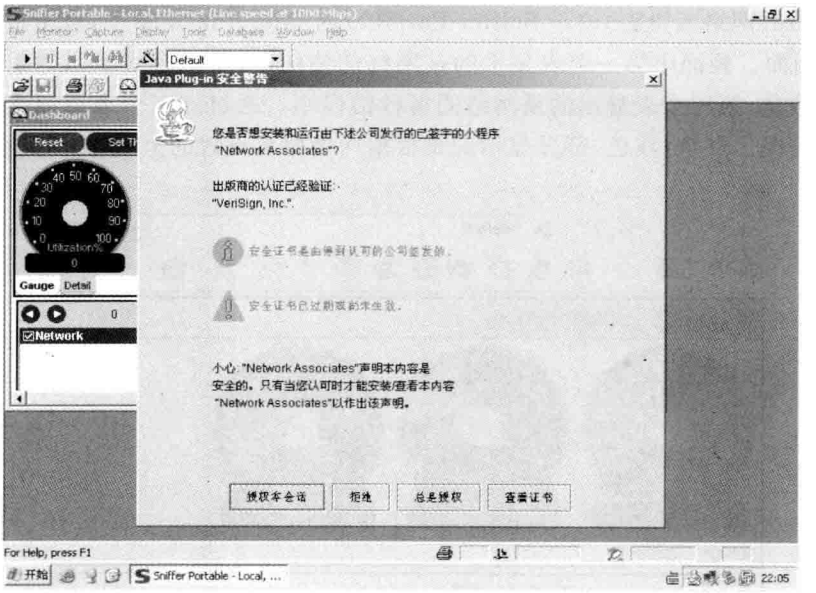


图 1-6　选择“总是授权”安装 Java 虚拟机

2. Sniffer 主要功能模块使用

(1)Sniffer Portable 菜单栏

Sniffer Portable 包含“File”、“Monitor”、“Capture”、“Display”、“Tools”、“DataBase”、“Window”、“Help”共 8 个菜单，如图 1-7 所示。

“File”菜单主要提供文件保存、打开等常用文件相关操作。“Monitor”下的菜单主要提供网络的实时情况，包括网络的使用率、网络的在线用户以及网络传输错误率。值得一提的

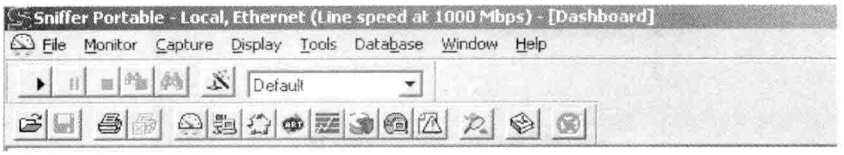


图 1-7 Sniffer 主要菜单

是普通的网卡无法抓取网络错误，所以，实验中一般错误率为零。同时，“Monitor”可以将网络实时情况以统计图或者统计表的方式展示给用户，以方便分析。“Capture”是一个简单的菜单，它提供启动、停止抓包设置，同时提供抓包过滤器的设置，在下面的实验中，我们将详细讲述此菜单的使用。“Display”是处理抓包后数据分析的菜单，它和 Word 等文字处理软件的“编辑”菜单很相近，有查找、选中等菜单，方便我们对数据的后期分析。“Tools”下是用户自定的软件，同时 Sniffer Portable 的设置项也在它的下面。“Database”只有和 Sniffer Reporter 结合起来才能看出效果，所以我们就不做介绍，有兴趣者可自己去看相关书籍。“Window”的作用和其他很多软件中的 Window 选项相同，就是以多种方式分别打开子窗口。“Help”，顾名思义，提供软件自带的使用手册。

(2) Dashboard(网络流量表)

Dashboard(网络流量表)位于 Sniffer Portable 的“Monitor”菜单下，点击进入后出现如图 1-8 所示画面。画面中第一个表显示的是网络的使用率，第二个表显示的是网络的每秒钟通过的包数量，第三个表显示的是网络的每秒错误率。通过这三个表可以直观地观察到网络的使用情况。红色(浅色)部分显示的是根据网络要求设置的上限(如果达到上限，软件

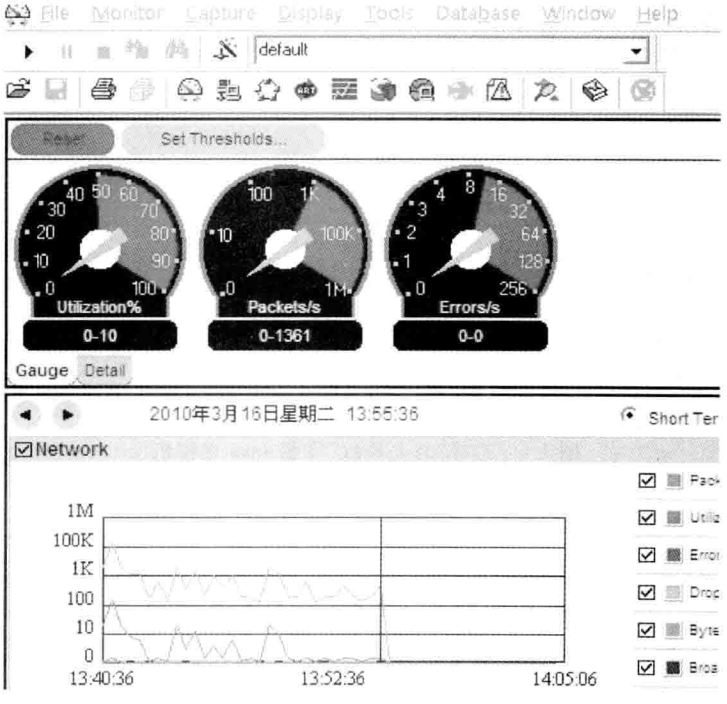
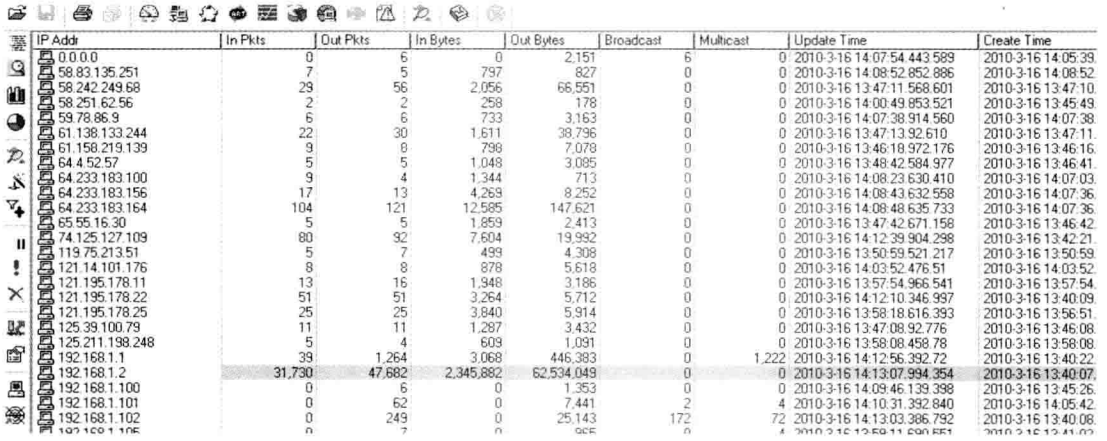


图 1-8 Dashboard

将根据配置做出反应和进行报警日志记录)。

(3) Host Table(主机列表)

Host Table(主机列表)位于 Sniffer Portable 的"Monitor"菜单下,点击进入后出现如图 1-9 所示的画面。此表单可以以列表、统计图、统计表的多种格式显示网络上的用户和用户使用的通信协议,并且对此做出了依据多种标准的划分,方便用户了解网络使用情况。



IP Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast	Multicast	Update Time	Create Time
0.0.0.0	0	6	0	2,151	6	0	2010-3-16 14:07:54.443 589	2010-3-16 14:05:39.
58.83.135.251	7	5	797	827	0	0	2010-3-16 14:08:52.852 886	2010-3-16 14:08:52.
58.242.249.68	29	56	2,056	66,551	0	0	2010-3-16 13:47:11.568 601	2010-3-16 13:47:10.
58.251.62.56	2	2	258	178	0	0	2010-3-16 14:00:49.853 521	2010-3-16 13:45:49.
59.78.86.9	6	6	733	3,163	0	0	2010-3-16 14:07:38.914 560	2010-3-16 14:07:38.
61.138.133.244	22	30	1,611	38,796	0	0	2010-3-16 13:47:13.92.610	2010-3-16 13:47:11.
61.158.219.139	9	8	798	7,078	0	0	2010-3-16 13:46:18.972.176	2010-3-16 13:46:16.
64.4.52.57	5	5	1,048	3,085	0	0	2010-3-16 13:48:42.584.977	2010-3-16 13:46:41.
64.233.183.100	9	4	1,344	713	0	0	2010-3-16 14:08:23.630.410	2010-3-16 14:07:03.
64.233.183.156	17	13	4,269	8,252	0	0	2010-3-16 14:08:43.632.558	2010-3-16 14:07:36.
64.233.183.164	104	121	12,585	147,621	0	0	2010-3-16 14:08:48.635.733	2010-3-16 14:07:36.
65.55.16.30	5	5	1,859	2,413	0	0	2010-3-16 13:47:42.671.158	2010-3-16 13:46:42.
74.125.127.109	80	92	7,604	19,992	0	0	2010-3-16 14:12:39.904.298	2010-3-16 13:42:21.
119.75.213.51	5	7	499	4,308	0	0	2010-3-16 13:50:59.521.217	2010-3-16 13:50:59.
121.14.101.176	8	8	878	5,618	0	0	2010-3-16 14:03:52.476.51	2010-3-16 14:03:52.
121.195.178.11	13	16	1,948	3,186	0	0	2010-3-16 13:57:54.966.541	2010-3-16 13:57:54.
121.195.178.22	51	51	3,264	5,712	0	0	2010-3-16 14:12:10.346.997	2010-3-16 13:40:09.
121.195.178.25	25	25	3,840	5,914	0	0	2010-3-16 13:58:18.616.393	2010-3-16 13:56:51.
125.39.100.79	11	11	1,287	3,432	0	0	2010-3-16 13:47:08.92.776	2010-3-16 13:46:08.
125.211.198.248	5	4	609	1,091	0	0	2010-3-16 13:58:08.458.78	2010-3-16 13:58:08.
192.168.1.1	39	1,264	3,068	446,383	0	1,222	2010-3-16 14:12:56.392.72	2010-3-16 13:40:22.
192.168.1.2	31,730	47,682	2,345,882	62,534,049	0	0	2010-3-16 14:13:07.994.354	2010-3-16 13:40:07.
192.168.1.100	0	6	0	1,353	0	0	2010-3-16 14:09:46.139.398	2010-3-16 13:45:26.
192.168.1.101	0	62	0	7,441	2	4	2010-3-16 14:10:31.392.840	2010-3-16 14:05:42.
192.168.1.102	0	249	0	25,143	172	72	2010-3-16 14:13:03.386.792	2010-3-16 13:40:08.

图 1-9　Host Table(主机列表)

(4) Matrix(网络矩阵)

Matrix 提供的网络通信实时情况拓扑图 Matrix Map 如图 1-10 所示。Matrix Map 图展示了网络中互相通信的主机,其中,绿色的连线表示两个网络节点正在通信,灰色的连线表示刚才有过连接。

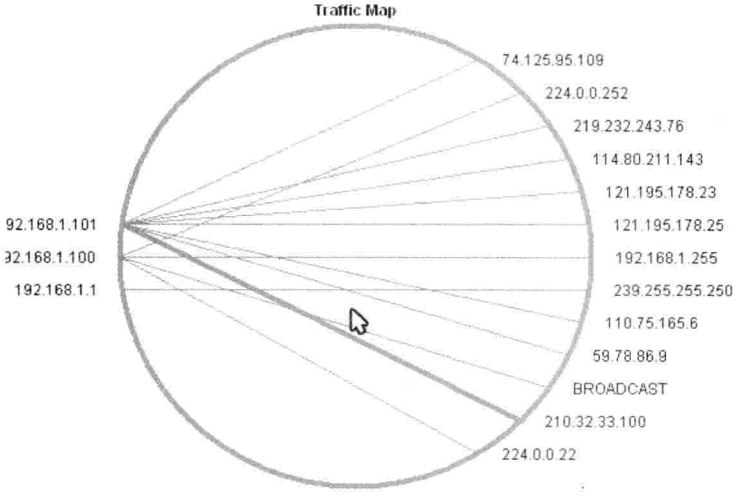


图 1-10　Matrix Map

Matrix 还提供饼图,如图 1-11 所示,显示每两台主机间的通信量在整个网络中所占的比例。当网络拥塞时可以发现瓶颈所在。

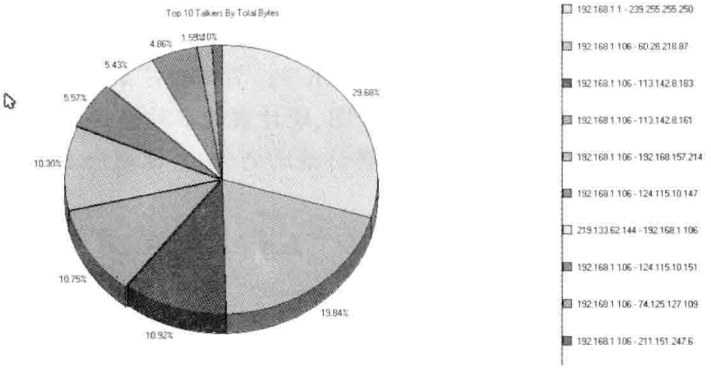


图 1-11 Matrix 饼图

(5) Protocol Distribution(协议分布)

Protocol Distribution 展示网络通信中各种协议所占的字节数(见图 1-12)。

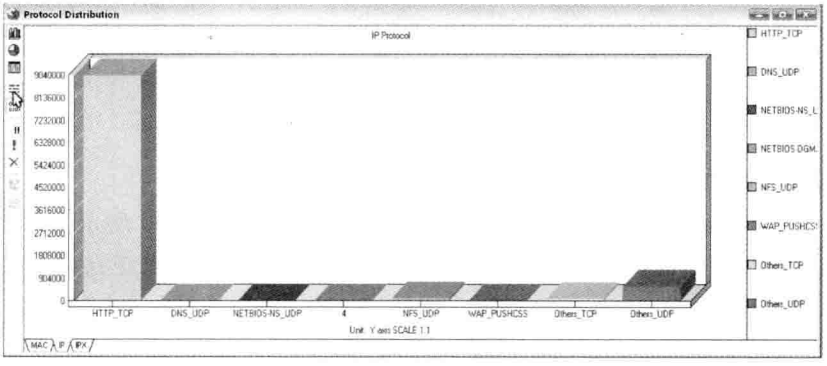


图 1-12 协议分布

(6) 抓包过滤设置

过滤设置位于 Sniffer Portable 的“Capture”菜单下,如图 1-13 所示。该菜单提供”Start”、“Stop”、“Display”、“Define Filter” 等几个功能,其中“Define Filter”是定义过滤规则。

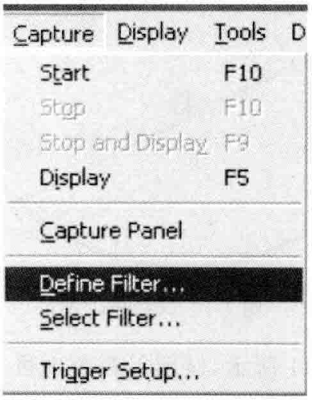


图 1-13 “Capture”菜单

值得注意的是在定义过滤规则前，首先要选择规则适用的网卡。第一步，选择“File”中 Select Settings 选项，如图 1-14 所示。点击进入后，这时 Sniffer Portable 的标题栏上会显示网卡情况，选择相应的网卡完成设置，如图 1-15 所示。

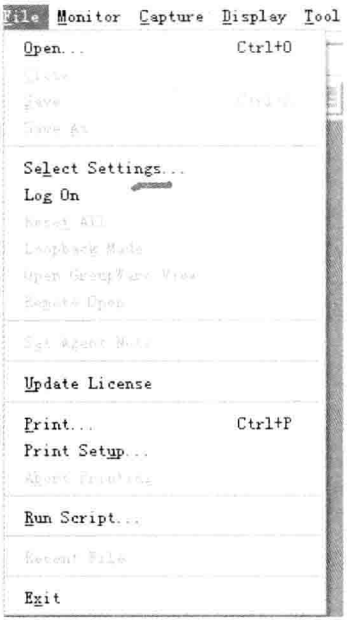


图 1-14　Select Setting 选项

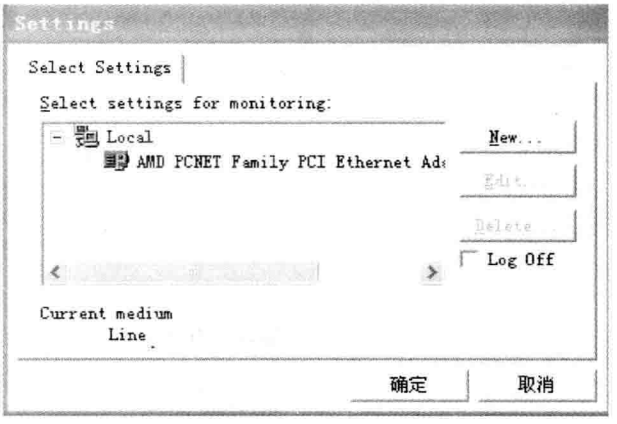


图 1-15　网卡选择

完成了要进行抓包的网卡的选择，接下来是进一步配置。如果我们明确要抓数据包的类型，在抓包时就可以做出选择。Sniffer Portable 可以提供这样的功能。“Define Filter”菜单可以提供较为高级的过滤设置，如图 1-16 所示。抓包过滤配置结束后，可以开始抓包——只要点击“Start”，Sniffer Portable 就自动开始抓包了。

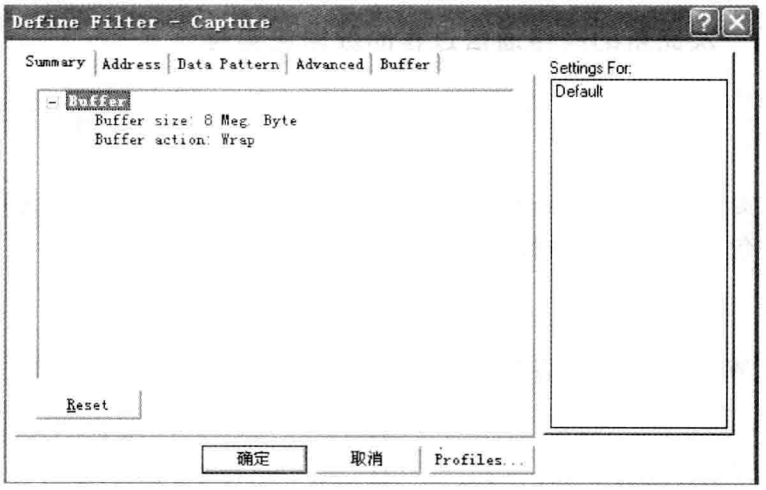


图 1-16　抓包规则设置

(7) 数据分析

"Display"菜单提供众多数据分析需要用的功能，如图 1-17 所示。这些菜单在没有数据时是不可用的。具体的操作在接下来的实验中讲述。

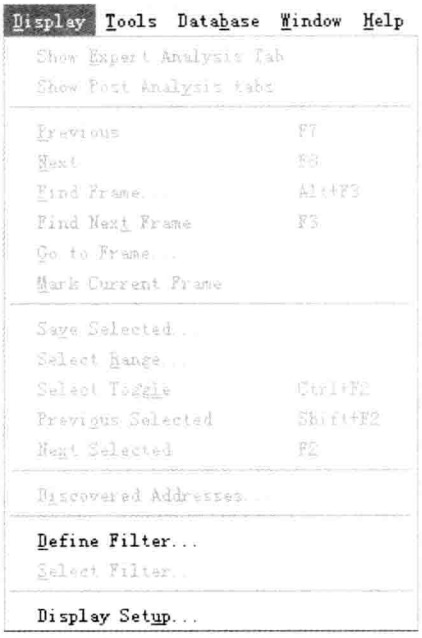


图 1-17 "Display"菜单

实验要求

本次实验要求按照步骤进行 Sniffer 的安装，并且熟练地掌握 Sniffer 各主要模块的使用，从整体上把握 Sniffer 抓包软件的精髓。

1.1.2 抓取一次完整的网络通信过程的数据包实验

实验目的

通过本次实验，掌握使用 Sniffer 抓取 ping 命令的完整通信过程的数据包的技能，熟悉 Sniffer 软件的包过滤设置和数据显示功能的使用。

实验环境

操作系统 Windows XP 或者 Windows 2000，抓包工具 Sniffer Portable。

实验原理

ping 是用来测试网络连通性的命令。一旦发出 ping 命令，主机会发出连续的测试数据包到网络中。在通常情况下，主机会收到回应数据包。值得一提的是，ping 采用的 ICMP

协议，通信过程相对简单。

实验步骤

1. 确定目标地址

这时我们应该选择比较大的网站或者自己的网关作为 ping 的对象，这是由于一般的计算机因为防火墙的缘故可能并不响应 ping，我们选择 www. baidu. com 作为目标。

2. 配置过滤器

这次我们只针对协议进行过滤器设置，ping 使用的是 ICMP 协议，过滤设置如图 1-18 所示。

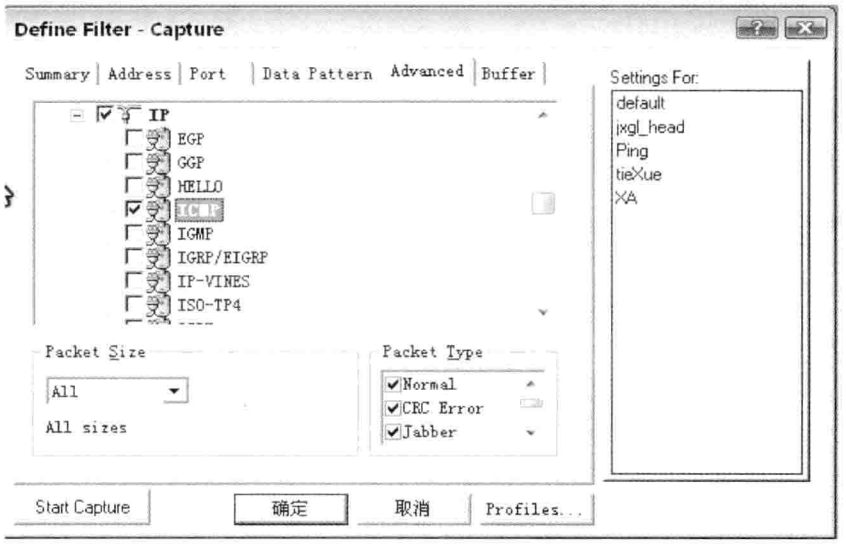


图 1-18　选择“ICMP”协议进行过滤设置

3. 启动抓包

选定过滤器后，点击“Start”，开始抓包。图 1-19 所示为 ping www. baidu. com。

```
C:\Documents and Settings\Administrator>ping www.baidu.com

Pinging www.a.shifen.com [119.75.213.50] with 32 bytes of data:

Reply from 119.75.213.50: bytes=32 time=826ms TTL=47
Reply from 119.75.213.50: bytes=32 time=73ms TTL=47
Reply from 119.75.213.50: bytes=32 time=77ms TTL=47
Reply from 119.75.213.50: bytes=32 time=73ms TTL=47

Ping statistics for 119.75.213.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 73ms, Maximum = 826ms, Average = 262ms
```

图 1-19　ping 百度网站命令

停止抓包后，所截取的数据如图 1-20 所示，共有 8 个数据包。