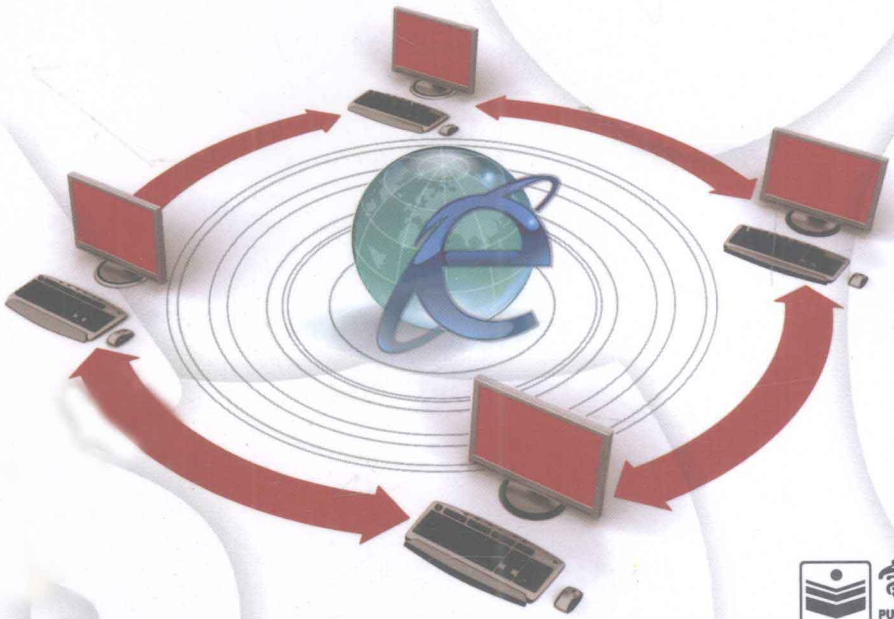
Broadview
www.broadview.com.cn

- 详解网络程序和网络性能监控
- 分析常见的6大通信协议
- 分析和排除常见网络故障
- 深入讲解Sniffer过滤器、触发器、报表高级应用
- 介绍常见木马和病毒的分析和防护

安全技术大系

局域网安全与攻防解密：基于Sniffer Pro实现

公芳亮 等编著

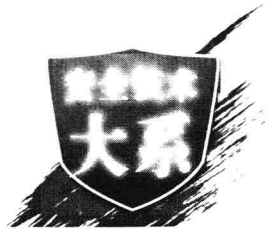


電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

作者介绍

公芳亮

从事网络工作近十年，具有大规模网络管理经验。长期致力于网络管理、监控领域研究。曾参与千橡集团网络集群管理工作。现就职于大型网络公司。



局域网安全与攻防解密：基于Sniffer Pro实现

公芳亮 等编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

Sniffer Pro 是美国 Network Associates 公司出品的一款网络分析软件。它可用于网络故障分析与性能管理，在网络界应用非常广泛。本书不仅详细地介绍了 Sniffer 的基本知识，还结合实际讲述了 Sniffer 在网络管理中的应用，内容包括 Sniffer Pro 和 Sniffit 的安装、应用 Sniffer Pro 对网络程序的监测、Sniffer 在 Linux 下的应用和网络安全问题等。为了便于读者理解掌握，笔者根据多年网络管理维护工作的经验，选取了经典案例进行讲解。每个实例都具有极强的代表性。

本书适于网络管理人员及其他相关领域的专业技术人员、管理人员阅读，也可作为高等院校相关课程的核心参考书。

图书在版编目（CIP）数据

局域网安全与攻防解密：基于 Sniffer Pro 实现/公芳亮等编著. —北京：电子工业出版社，2011.5
（安全技术大系）
ISBN 978-7-121-13166-0

Ⅰ. ①局… Ⅱ. ①公… Ⅲ. ①局域网－安全技术－应用软件，Sniffer Pro Ⅳ. ①TP393.108

中国版本图书馆 CIP 数据核字（2011）第 052918 号

责任编辑：胡辛征　刘娴庆
特约编辑：赵树刚
印　　刷：北京中新伟业印刷有限公司
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：25　字数：520 千字
印　　次：2011 年 5 月第 1 次印刷
印　　数：4000 册　　定价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

本书目的

网络是一个很广泛的概念，包括了很多的内容。其中最基础的内容就是构成网络的所有硬件设备和运行在这些设备上的协议和基础软件。没有这些作基础，任何使用网络的服务都无法进行。如何保证这些网络基础的正常运行就是每一个网络工程师的工作。随着网络的发展，网络互连的范围在不断扩大，每一个网络工程师的负担也越来越重，如何使用最简单、快捷的方式诊断网络中的故障成为每一个网络工程师必要的研究主题。使用相应的工具软件是一个很好的解决方式。本书介绍的 Sniffer 软件是广大网络工程师常用的一类软件。希望本书能够为有志于从事网络工程的读者打开一扇管理网络、分析网络的大门。

本书优势

1．讲解力求通俗

网络数据传输一直以抽象著称。虽然网络应用相当普及，但是由于网络数据传输涉及较多底层知识，导致大多数读者对其望而却步。而作为网络探测利器，Sniffer 一直被认为是某些人士的专利。本书在内容讲解上突破常规，不去深究晦涩难懂的协议和报文构成，以多种形象生动的方式介绍如何使用 Sniffer。例如，以广大读者比较常见的自来水网络来解释网络的运作。

2．内容力求实用

多数网络书籍会大篇幅介绍网络设备、网络协议和网络构成。这些内容往往占大量篇幅，而与实际应用又有很大距离。为了不增加读者的阅读负担，本书只选取与实际应用相关的内容进行介绍。例如，本书中的协议相关内容都与 Sniffer 密切相关，是读者最需要的部分。

3．实例力求典型

作为大型服务器维护人员，笔者负责几百台服务器的维护。为了使读者学以致用，笔

者从工作日志中的几百个实例中精选出书中的实例。在选择时，力求实例具有最大的典型性和代表性。希望读者能仔细分析这些实例，便于日后工作中引为鉴戒。

本书组织结构

本书共分为 3 篇。

第 1 篇为基础篇，共包括 3 章。其中，第 1 章首先简单介绍了一下相关知识，讲述了一些和 Sniffer 相关的知识，尤其是为第一次接触网络管理的读者介绍了一些网络相关的知识和术语，为以后知识的展开做相应的铺垫；第 2 章按照标准的安装步骤搭建了 Windows 平台和 Linux 平台下的 Sniffer 软件，并针对其常见的问题给出了解决方案；第 3 章介绍了 Sniffer 软件的界面和参数，希望能够给读者一个直观的印象。

第 2 篇为 Sniffer 应用篇，共包括 9 章。第 4 章介绍了如何使用 Sniffer Pro 的基本功能——网络程序监控功能，作为 Sniffer Pro 的一个常用功能，希望读者熟悉 Sniffer Pro 操作及工作原理；第 5 章介绍了如何使用 Sniffer Pro 监控网络性能，读者可以将第 5 章看成是第 4 章的延续，继续通过本书的介绍熟悉操作；第 6 章讲解了如何分析捕获到的数据，这也是 Sniffer Pro 的难点之一，在后面的章节中要反复使用本章的内容；第 7 章是前面几章知识的实践，运用已学过的知识解决一些常见的简单网络故障；第 8 章和第 9 章在前面的基础上介绍了 Sniffer Pro 的扩展内容，将读者带入真正的数据捕获与监控的世界；第 10 章介绍了 Sniffer Pro 的报表功能；第 11 章介绍了 Sniffer 软件的防御措施，通过对这些措施的学习使用户对 Sniffer Pro 的工作原理有更进一步的了解，同时提高读者的网络安全防范意识；第 12 章则使用了一些例子介绍了另外一个主流网络平台——Linux 下的 Sniffer 软件的安装调试和工作方式。

第 3 篇为 Sniffer 实战篇。在前两部分的基础上，介绍了 Sniffer 在实际的网络工程中的一些实际应用。该部分包括 5 章。第 13 章讲解了 Sniffer 的一些攻击方式；第 14 章则针对网络操作平台的一些安全问题进行了讨论，并提出了一些常见的解决方案；第 15 章分析了网络中常见软件的监听和捕获方式；第 16 章和第 17 章有针对性地分析了病毒和木马这两种常见的网络软件。

作者的话

如何在迷宫一样的网络中更快捷地找到需要的资源与存在的错误，以及到达目的地的道路呢？在实际的迷宫中我们可以使用指南针，而在网络中我们则使用工具软件。我一直有这样一个想法，就是如何能够推开网络世界中的每一扇门，然后找到门后的真谛。但是

当我进入网络世界中以后，我发现每前进一步都会付出比上一步多十倍乃至百倍的努力。尽管这样，我还是在努力着。我希望能够完成我的梦想，同时也希望我身边能有一些和我有共同志向的朋友，和我一起努力。网络是广阔的，技术是无穷无尽的，而我的生命有限，希望能够在我有限的生命中推开更多扇网络知识的大门，为那些和我有着同样梦想的人开启通向梦想的道路。谨以这段文字与那些和我有着同样梦想的人共勉。

阅读本书的注意事项

任何一个网络检测和监控的软件都是以记录系统情况并发现系统漏洞为目的的。本书介绍了很多和网络漏洞相关的实例，希望读者在阅读本书时注意这些实例的使用方法和范围。尤其在做实验操作时，希望读者能够根据实验的内容构建自己的实验环境，对于大部分的实验，本书已经给出了相应的网络结构图，依照这些网络结构图搭建网络环境可以很好地做出相应的实验结果。

读者对象

- 计算机、信息安全、网络工程、信息工程等相关专业的在校学生
- 从事计算机网络安全设计、管理、维护的从业人员
- 网络爱好者

本书作者

本书由公芳亮主笔编写，其他参与编写的人员还有吴燃、张昆、方振宇、陈冠佐、傅奎、陈勤、梁洋洋、毕梦飞、陈庆、柴相花、陈非凡、陈华、陈嵩、承卓。在此表示感谢！

编著者

目　录

第 1 篇　Sniffer 基础

第 2 篇 Sniffer 应用

第 3 篇 Sniffer 实战