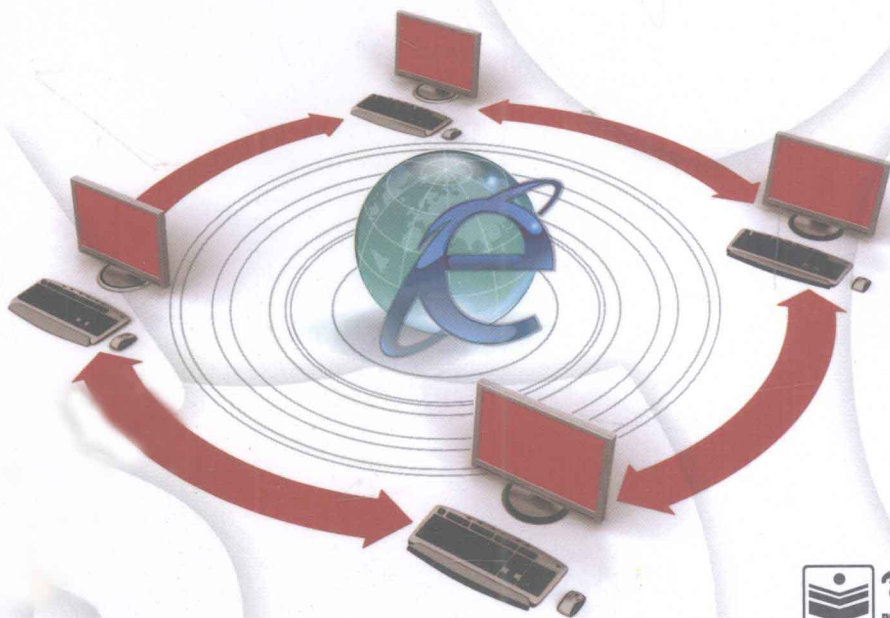


- 详解网络程序和网络性能监控
- 分析常见的6大通信协议
- 分析和排除常见网络故障
- 深入讲解Sniffer过滤器、触发器、报表高级应用
- 介绍常见木马和病毒的分析和防护



局域网安全与攻防解密： 基于Sniffer Pro实现

公芳亮 等编著



电子工业出版社
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。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究。

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 zltz@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昊燃、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 1 章 什么是 Sniffer	17
1.1 局域网安全概述	17
1.1.1 网络分段	17
1.1.2 交换式集线器代替共享式集线器	18
1.1.3 VLAN 的划分	18
1.2 Sniffer 的用途	19
1.2.1 网络数据传输原理	19
1.2.2 Sniffer 工作原理	20
1.2.3 Sniffer 应用	21
1.3 相关网络知识	21
1.3.1 OSI 参考模型	21
1.3.2 网络协议	24
1.3.4 交换机	28
1.3.5 桥接	30
1.3.6 网卡	32
1.3.7 网桥	34
1.3.8 网关	35
1.3.9 路由器	36
1.3.10 路由器和网桥的比较	39
1.4 Sniffer 的基本原理	41
1.5 Sniffer 常用的工具 Sniffer Pro 和 Sniffit	43
1.5.1 Sniffer Pro 的特点	43
1.5.2 Sniffit 的特点	43
1.6 小结	44

第 2 章 Sniffer Pro 和 Sniffit 的安装	45
2.1 Sniffer Pro 的安装步骤	45
2.1.1 系统要求	45
2.1.2 安装 Sniffer Portable 4.9 MR2	46
2.2 定制自己的 Sniffer Pro	49
2.2.1 远程访问模式的使用	50
2.2.2 个人设置技巧	50
2.3 Sniffit 的安装	52
2.4 常见安装故障	53
2.5 小结	53
第 3 章 Sniffer Pro 和 Sniffit 的界面介绍	54
3.1 Sniffer Pro 和 Sniffit 概述	54
3.2 Sniffer Pro 的表盘	54
3.2.1 Sniffer Pro 表盘的基本信息	54
3.2.2 Sniffer Pro 表盘的设置	56
3.3 Sniffer Pro 的菜单	57
3.3.1 文件菜单 (File)	57
3.3.2 监控菜单 (Monitor)	58
3.3.3 捕获菜单 (Capture)	65
3.3.4 显示菜单 (Display)	66
3.3.5 工具菜单 (Tools)	66
3.3.6 数据库菜单 (Database)	67
3.3.7 窗口菜单 (Window)	68
3.4 Sniffer Pro 的工具栏	68
3.4.1 捕获过程工具栏	68
3.4.2 定义过滤器工具栏	69
3.4.3 打开捕获结果	69
3.5 Sniffer Pro 提供的基本工具	69
3.5.1 数据包产生器 (Packet Generator) 和环路模式	69
3.5.2 报告生成器 (Sniffer Reporters)	71
3.5.3 Ping 命令	72
3.5.4 路径检测 (Trace Route)	72

3.5.5	DNS 探测 (DNS Lookup)	74
3.5.6	Finger 工具	75
3.5.7	WhoIs	76
3.5.8	地址本 (Address Book)	76
3.6	Sniffer Pro 提供的高级工具	77
3.6.1	启动 / 关闭 Sniffer Pro 的高级工具	77
3.6.2	解码	77
3.6.3	矩阵	78
3.6.4	主机列表	79
3.6.5	协议分布统计	79
3.7	Sniffer Pro 的地址本	80
3.7.1	添加新地址	80
3.7.2	导出地址	82
3.8	Sniffit 的参数介绍	82
3.8.1	Sniffit 文本参数	82
3.8.2	Sniffit 的图形界面	83
3.9	小结	84

第 2 篇 Sniffer 应用

第 4 章	应用 Sniffer Pro 对网络程序的监测	86
4.1	网络程序监测概述	86
4.2	捕获数据	86
4.2.1	捕获过程	86
4.2.2	分析过程	92
4.2.3	时间标记	96
4.3	高级分析介绍	96
4.4	常见错误分析	101
4.5	设置高级分析	102
4.5.1	监控对象设置	102
4.5.2	警告的设置	103
4.5.3	监控协议的设置	103
4.5.4	子网掩码的设置	104

4.5.5	RIP 选项的设置	105
4.6	查看应用程序响应时间	105
4.7	小结	107
第 5 章	应用 Sniffer Pro 监控网络性能	108
5.1	网络性能监控概述	108
5.2	网络性能	108
5.2.1	什么是网络性能	108
5.2.2	影响网络性能的因素	109
5.3	监控方式	110
5.3.1	使用表盘	110
5.3.2	阈值	114
5.4	根据结果作出判断	115
5.4.1	实际网络情况说明	115
5.4.2	监控结果	116
5.4.3	根据监控结果判断并制定措施	119
5.5	使用网络性能监控发现网络病毒	120
5.5.1	网络情况说明	120
5.5.2	网络监控结果及分析	120
5.6	小结	121
第 6 章	分析捕获的数据	122
6.1	数据分析概述	122
6.2	捕获数据流	122
6.2.1	什么是数据包	122
6.2.2	开始捕获数据流	123
6.3	保存捕获的数据	126
6.3.1	保存一个 Sniffer Pro 捕获数据包的结果	126
6.3.2	载入文件并使用	127
6.4	分析地址解析协议 (ARP)	127
6.4.1	地址解析协议 (ARP)	128
6.4.2	ARP 的简单命令	129
6.4.3	运用 Sniffer Pro 捕获 ARP 数据包	130
6.4.4	分析 ARP 数据包	131

6.5	分析 ICMP 协议	132
6.5.1	ICMP 协议	133
6.5.2	ICMP 实验需要使用的命令	136
6.5.3	运用 Sniffer Pro 捕获 ICMP 数据包	137
6.5.4	分析 ICMP 数据包	138
6.6	分析 TCP 协议	141
6.6.1	TCP 协议	141
6.6.2	TCP 实验需要使用的命令	143
6.6.3	运用 Sniffer Pro 捕获 TCP 数据包	143
6.6.4	分析 TCP 数据包	144
6.7	分析 UDP 协议	146
6.7.1	UDP 协议	146
6.7.2	UDP 协议实验需要的简单命令	150
6.7.3	运用 Sniffer Pro 捕获 UDP 数据包	151
6.7.4	分析 UDP 数据包	152
6.8	分析 IPX 协议	154
6.8.1	IPX 协议	154
6.8.2	IPX 实验需要的实验环境	155
6.8.3	运用 Sniffer Pro 捕获 IPX 协议数据包	156
6.8.4	分析 IPX 协议数据包	157
6.9	分析 PPPoE 协议	158
6.9.1	PPPoE 协议	159
6.9.2	分析 PPPoE 数据包	160
6.10	小结	162
第 7 章	应用 Sniffer Pro	163
7.1	引言	163
7.2	网络传输速度下降	163
7.2.1	分析原因	163
7.2.2	简单案例分析	165
7.3	简单网络设备故障	176
7.3.1	BOOTP 协议	176
7.3.2	定义过滤器	177
7.3.3	分析捕获过程	178

7.3.4 典型故障分析.....	182
7.4 小结.....	184
第 8 章 Sniffer Pro 高级应用——过滤器.....	185
8.1 引言.....	185
8.2 过滤器的意义.....	185
8.3 预定义的过滤器.....	186
8.3.1 使用默认的过滤器.....	186
8.3.2 获得更多的过滤器.....	186
8.4 建立自己的过滤器.....	188
8.5 高级过滤功能使用.....	190
8.5.1 过滤节点间的过滤器.....	190
8.5.2 指定关键字的过滤器.....	192
8.5.3 使用逻辑关系建立过滤器.....	193
8.6 定制专用过滤器.....	195
8.7 小结.....	199
第 9 章 触发功能的应用.....	200
9.1 引言.....	200
9.2 触发的意义.....	200
9.3 触发功能的使用.....	200
9.3.1 触发介绍.....	201
9.3.2 开始触发.....	205
9.4 报警功能的使用.....	210
9.4.1 报警功能的处理.....	210
9.4.2 实际使用报警功能.....	211
9.5 定义警告的阈值.....	214
9.5.1 警告级别的设置.....	214
9.5.2 高级警告的阈值修改.....	215
9.5.3 监控警告的阈值修改.....	216
9.5.4 ART 监控警告的阈值修改.....	217
9.6 小结.....	218

第 10 章 详解 Sniffer Pro 的报表	219
10.1 引言	219
10.2 为什么要使用报表	219
10.3 输出数据	221
10.3.1 输出 HTML 格式的数据	221
10.3.2 输出 CSV 格式的数据	223
10.4 小结	226
第 11 章 防御 Sniffer 攻击	227
11.1 引言	227
11.2 Sniffer 攻击	227
11.2.1 Sniffer 攻击原理	227
11.2.2 攻击实例	228
11.3 防御 Sniffer Pro 攻击	230
11.3.1 发现 Sniffer Pro	230
11.3.2 使用 SSH 加密	232
11.3.3 改变网络拓扑结构	233
11.3.4 使用工具检查	234
11.4 小结	235
第 12 章 Sniffer Pro 在 Linux 下的应用	236
12.1 Sniffit 的应用举例	236
12.1.1 实验环境	236
12.1.2 使用 Sniffit Pro 捕获 Telnet 数据	237
12.2 TcpDump 的安装和应用	238
12.2.1 TcpDump 的安装	238
12.2.2 命令、参数和表达式	240
12.2.3 简单应用举例	242
12.2.4 TcpDump 的解码	242
12.2.5 TcpDump 输出结果的解释	243
12.3 Ethereal 的安装和应用	246
12.3.1 Ethereal 的安装	246
12.3.2 Ethereal 过滤规则的建立	248

12.3.3 用 Ethereal 分析数据包	251
12.4 EtherApe 的安装和应用	252
12.4.1 EtherApe 的安装	252
12.4.2 设置 EtherApe 的过滤规则	253
12.5 小结	256

第 3 篇 Sniffer 实战

第 13 章 Sniffer 常见攻击	258
13.1 捕获 E-mail 密码	258
13.1.1 了解密码传输方式	258
13.1.2 定制过滤器	259
13.1.3 捕获数据包	261
13.1.4 获取密码	266
13.2 域名服务的攻击	267
13.2.1 DNS 工作方式	267
13.2.2 定制过滤器	268
13.2.3 捕获数据	270
13.2.4 处理 DNS 缓存数据	272
13.2.5 在 Windows 2003 中防止 DNS 污染	272
13.3 Telnet 密码捕获	273
13.3.1 Telnet 的工作原理	273
13.3.2 定制过滤器	274
13.3.3 数据捕获	275
13.4 小结	280
第 14 章 网络安全问题	282
14.1 网络安全技术措施	282
14.1.1 网络安全的概念	282
14.1.2 Internet 上存在的主要安全隐患	282
14.1.3 网络安全防范的内容	283
14.1.4 确保网络安全的主要技术	283
14.1.5 常见安全措施	284

14.2	网络漏洞介绍	284
14.2.1	常见网络漏洞	285
14.2.2	过滤器的定制	287
14.3	网络漏洞的扫描和监听	290
14.3.1	网络扫描	290
14.3.2	网络扫描和监听的实例	293
14.4	端口的禁止	296
14.4.1	Windows 服务器平台的端口禁止	296
14.4.2	Linux 平台的端口管理	299
14.5	访问的控制	300
14.6	操作系统安全漏洞的处理	303
14.6.1	Windows 平台的安全漏洞的处理	303
14.6.2	Linux 平台的安全漏洞的处理	306
14.7	小结	307
第 15 章	常用网络软件	308
15.1	FTP 类软件——CuteFTP	308
15.1.1	FTP 软件工作方式	308
15.1.2	定制 CuteFTP 专用过滤器	310
15.1.3	捕获及分析数据包	311
15.1.4	数据信息防护	315
15.2	邮件收发软件——Outlook Express	318
15.2.1	邮件收发软件的工作方式	319
15.2.2	定制专用过滤器	319
15.2.3	捕获数据包	321
15.2.4	数据信息防护	322
15.3	即时聊天工具——MSN Messenger	324
15.3.1	MSN Messenger 通信工作方式	324
15.3.2	定制 MSN 专用过滤器	325
15.3.3	捕获数据包	327
15.3.4	分析聊天信息	330
15.3.5	保护 MSN 通信安全	332
15.4	小结	336

第 16 章 病毒防护	337
16.1 病毒概述	337
16.1.1 病毒的定义	337
16.1.2 病毒发展趋势	337
16.2 Sniffer Pro 病毒防护	340
16.2.1 防护原理	340
16.2.2 定制过滤器	340
16.3 常见病毒分析	343
16.3.1 尼姆达病毒过滤	343
16.3.2 CodeRed 病毒过滤	345
16.3.3 病毒的发现与分析	348
16.3.4 制定病毒捕获措施	350
16.4 小结	351
第 17 章 木马防护	352
17.1 木马概述	352
17.1.1 木马类型	352
17.1.2 木马特性	354
17.1.3 中木马病毒后出现的状况	355
17.2 发现木马	356
17.2.1 木马常用端口	356
17.2.2 定制过滤器	360
17.2.3 定制触发器	363
17.3 常见木马的检查方案	365
17.3.1 木马隐身方法	365
17.3.2 手动检查木马	366
17.3.3 自动检查木马	370
17.4 小结	375
附录 A 网络操作	376
附录 B 病毒特征码和木马进程	395