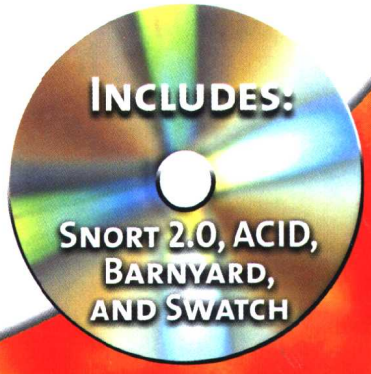
Snort 2.0 入侵检测

Snort 2.0 Intrusion Detection

〔美〕Brian Caswell，Jay Beale，James C.Foster，Jeffrey Posluns 著

宋劲松 等 译



国防工业出版社

http://www.ndip.cn

[美] Brian Caswell
Jay Beale
James C.Foster
Jeffrey Posluns 著
宋劲松 等译

Snort2.0 Intrusion Detection

Snort 2.0 入侵检测

国防工业出版社
·北京·

著作权合同登记　图字:军-2003-016号

图书在版编目(CIP)数据

Snort 2.0 入侵检测/(美)卡斯维尔(Caswell,B.)等著;宋劲松等译. —北京:国防工业出版社,2004.1
书名原文:Snort 2.0 Intrusion Detection
ISBN 7-118-03305-7

Ⅰ.S...　Ⅱ.①卡...②比...③宋...
Ⅲ.计算机网络-安全技术-应用软件,Snort 2.0　Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2003)第100302号

责　编　笪许燕
装帧设计　张丽华

出版发行　国防工业出版社出版发行
地　址　北京市海淀区紫竹院南路23号
邮　编　100044
经　售　新华书店
网　址　http://www.ndip.cn
印　刷　北京奥隆印刷厂
开　本　787×960　1/16
印　张　25¾
字　数　567千字
版　次　2004年1月第1版
印　次　2004年1月北京第1次印刷
印　数　1—3000册
定　价　56.00元(含光盘)

译者序

2003年5月6日，几乎在Snort2.0版本发布的同时，Snort的官方网站上隆重介绍了《Snort2.0入侵检测》这本书。本书具有权威性、及时性、新颖性三大特点，中译本的推出使国内的网络安全从业人员、网络管理员和网络安全爱好者能及时深入地剖析这款著名入侵检测软件的最新版本。

入侵检测系统是网络安全体系中的重要组成部分，随着防火墙的渐渐普及，人们不再满足于防火墙的网络控制功能，需要有一种安全产品能够智能发现网络入侵行为，和防火墙一起组成立体防御体系。智能发现网络入侵行为就是入侵检测系统的工作。Snort作为世界上应用最广泛的开放源码的入侵检测系统，在业内有着重要的地位，在国内的网络安全行业甚至成为入侵检测系统的代名词。

正因为大家对Snort如此关注，Snort2.0版本一直受到人们的期待，因为这是对1.x版本的一次大的变革。在Snort2.0版本中力图摆脱单包检测的弊病，在检测效率、准确率上有了很大的改进，而如何实现这些改进一直是人们关注的焦点。

本书的作者都是Snort核心开发组的成员，在Snort2.0开发的同时他们即着手本书的写作，凭着对Snort和入侵检测系统的深刻理解，完成了一本帮助读者了解入侵检测系统和Snort2.0体

系结构的读物，并且在第一时间出版，出版时间甚至稍早于 Snort2.0 的发布时间。这也是惟一一本 Snort 官方推荐的书籍。

本书的引进解决了国内没有介绍 Snort 的权威资料的现状，帮助读者直接、全面地了解 Snort 的最新版本，无论是对以前接触过 Snort 的人员还是对第一次接触 Snort 的人员都大有裨益。

全书由宋劲松、李俊、郑理、徐鹏、杨燚、曲亚东主持翻译，宋劲松完成了校对工作。由于译者和审校者水平有限，对译文中不妥之处敬请广大读者批评指正。

译 者

2003 年 7 月

前言

在现代社会互联网飞速发展的同时，入侵攻击，拒绝服务攻击，网络资源滥用等威胁也如影随形，为互联网带来很多负面的影响。面对这些挑战，很多公司都开发出阻止和检测网络攻击的软件。但是一套入侵检测软件价值不菲，少则数千，多则上万，因此它们在这个市场中面临着强劲的竞争对手：Snort。Snort 是高效的，稳定的，并拥有一个不断成长的用户群体。最重要的是，Snort 是免费的。

Snort 的创始人 Marty Roesch 把 Snort 定位为轻量级的入侵检测系统。其实，这个定位是不妥当的。无论对小的家庭用户还是繁忙的公司网络，Snort 都有能力实时分析和记录 IP 数据包，其基于规则的检测引擎能够检测多种变种攻击，包括 CGI 扫描，缓存区溢出攻击，SMB 探测等。还能为确定网络中一些莫名其妙的服务都是做什么的提供帮助。

Snort 能运行在众多的硬件平台和操作系统上。因为其可扩展的体系结构和开放源码的发布模式，Snort 成为入侵检测软件中非常流行的选择。经常有已经花费了数千美元购买入侵检测系统的管理员还使用 Snort 来填补网络中的一些缺口。

从本质上说，Snort 是网络数据包嗅探器。只要运行 Snort 时不加载规则，就可以把网络中的数据包显示出来。但是 Snort 的

真正价值在于把数据包经过规则处理的过程。Snort 灵活的和强大的语言能对网络中的所有数据包作充分的分析，决定如何处理任何特殊的数据包。Snort 可以选择的方式有忽略、记录或告警管理员。Snort 有很多种记录或告警的方法，例如，syslog、写入文件、写入 XML 格式文件、发送 WinPopup 消息等。当有了新的攻击手段时，只要简单加入新的规则就可以升级 Snort。

尽管 Snort 设计得很简洁，但它并不是一个能够即安即用的方案。要想把 Snort 用好，用户必须对 Snort 的原理非常熟悉。本书的作者将花很多篇幅教读者如何使用 Snort，从基础的安装到高级的规则配置，覆盖了使用 Snort 的方方面面，包括基本安装、预处理插件配置、系统优化等。在这些方面作者提供了珍贵的和有价值的经验，并用简单易懂的语言描述出来。这是目前惟一如此深入地描述如何安装、配置和使用 Snort 的文档。

Snort 没有打算做所有的事情，没有打算和商业入侵检测软件作全面竞争。但是在分析和定位恶意的网络流量时，Snort 会做得更好。秘诀就是 Snort 能让使用者完全定制自己的规则。定制规则的前提是使用者有关于 Snort 规则的相关知识。第五章剖析了 Snort 规则的构成，指导读者如何完成一个高效和精确的规则，并详细介绍了每个变量，选项和可能用到的动作。

第六章《预处理器》和第七章《Snort 输出插件的实现》描述了预处理器和输出选项的细节问题，可以使读者很轻松地为自己的网络环境定制 Snort。最后的几章解答了如何优化和使用 Snort 的问题，是 Snort 的高级进阶内容。

Snort 没有提供友好的图形化用户界面，华丽的报表和在线帮助。Snort 一直只在一点上深入发展，即如何做好入侵检测。有了强大的规则引擎和简洁的体系结构，它能毫无疑问地取代任何商业 IDS 的工作。Snort 是必备的网络安全工具软件，如果您想使用这个工具保护您的网络，本书是您必备的参考书。

——***Mark Burnett***

Brian Caswell

本书技术编辑，是Snort的团队中倍受尊敬的人物。他是snort.org站点的管理者，是Snort系统规则的首席维护人。无论在小企业或大企业的用户环境下，他对Snort的部署和配置都有非常丰富的经验，并在2002年和2003年的CanSecWest年会上就此问题做了多次专题演讲。Brian还是Sourcefire的成员，Sourcefire由Snort的开发团队创办，基于Snort IDS提供世界领先的和最灵活的入侵管理方案。2002年，Sourcefire被《信息安全杂志》(Information Security Magazine)评为IT安全市场最有影响的厂商之一。

Jay Beale

是主机防护和安全审计方面的专家。他是Bastille项目的开发领导者，此项目用来加固Linux，HP-UX和Mac OS X。他还是Honeynet项目的开发成员，是互联网安全中心（Center for Internet Security）的核心参与者，各种会议的演讲者和培训师，例如黑帽子（Black Hat）和Linux世界等会议。Jay开发了互联网安全中心的UNIX安全工具，目前被广泛应用在各种组织机构中，从财富500强企业到国防部。他负责维护互联网安全中心的Linux安全基准文档，并且是中心UNIX小组的核心开发成员，该小组和其他私营企业一起开发美国工业界和政府的UNIX安全标准。在这些工作之外，Jay写了很多关于操作系统安全的文章和书籍。他是信息安全杂志的专栏作家，为SecurityPortal.com 和 SecurityFocus.com写了很多文章。

James C.Foster (CISSP, CCSE)

是Foundstone公司的研发部门经现，负责产品、咨询、开发等所有方面。在加入Foundstone公司之前，James是Guardent公司的高级顾问和研究员，并且是《信息安全杂志》的作者之一，后来又作为信息安全研究员在计算机科学协会工作。James精通WEB应用程序，加密和无线技术。James完成过对很多代码的评估，包括商业操作系统模块、Win32应用程序价值、WEB应用程序价值、无线和有线的渗透测试、商业加密算法等。Foster先生在很多方面取得过学位或认证，并在耶鲁商学院、哈佛大学、国会大厦学院、马里兰大学从事过研究工作。

Jeffrey Posluns (SSCP, CISSP, CISA, CCNP, CCDA, GSEC)

本书技术顾问，是SecuritySage的创始人。SecuritySage是信息安全和保密咨询顾问公司，Jeffrey领导一支队伍做专业服务，产品咨询和创新产品开发工作。Jeffrey有超过11年的信息安全方法，审计和控制方面的经验，他在分析黑客工具和技术，入侵检测，安全策略，紧急事件响应等方面有深厚的技术功底。在趋势判断、提供高品质的客户服务、教育研究和演讲等方面是业界公认的领导者。

目 录

第一章 入侵检测系统 …… 1
1.1 什么是入侵检测 …… 2
1.1.1 NIDS …… 3
1.1.2 HIDS …… 4
1.1.3 DIDS …… 5
1.2 攻击三部曲 …… 6
1.2.1 目录回溯漏洞 …… 6
1.2.2 红色代码蠕虫 …… 7
1.2.3 尼姆达蠕虫 …… 8
1.2.4 什么是入侵 …… 9
1.2.5 用 Snort 发现入侵 …… 10
1.3 为什么 IDS 如此重要 …… 12
1.3.1 为什么会受到攻击 …… 13
1.3.2 IDS 布置在什么位置合适 …… 13
1.3.3 防火墙能否替代 IDS …… 14
1.3.4 还有哪些常见的攻击类型 …… 14
1.4 IDS 还能做什么 …… 15
1.4.1 监视数据库应用 …… 16
1.4.2 监视 DNS 应用 …… 16
1.4.3 保护邮件服务器 …… 16
1.4.4 利用 IDS 监视公司的安全政策 …… 17
小结 …… 17
本章快速回顾 …… 18
FAQ …… 19

第二章 Snort2.0 介绍 …… 21
2.1 什么是 Snort …… 23
2.2 Snort 系统需求 …… 24
2.2.1 硬件 …… 25
2.3 Snort 的特性 …… 26
2.3.1 数据包嗅探器 …… 27
2.3.2 预处理器 …… 28
2.3.3 检测引擎模块 …… 29
2.3.4 报警/日志模块 …… 29
2.4 在网络中部署 Snort …… 32
2.4.1 Snort 的用途 …… 33
2.4.2 Snort 和网络体系结构 …… 38
2.4.3 运行 Snort 时的弱点 …… 41
2.5 Snort 的安全考虑 …… 42
2.5.1 Snort 易受攻击 …… 43
2.5.2 加固我们的 Snort 系统 …… 44
小结 …… 44
本章快速回顾 …… 44
FAQ …… 45
第三章 安装 Snort …… 47
3.1 关于 Linux 发布版本的简要介绍 …… 48
3.1.1 Debian …… 49
3.1.2 Slackware …… 49
3.1.3 Gentoo …… 49
3.2 安装 PCAP …… 50
3.2.1 使用源码包安装 libpcap …… 51
3.2.2 用 RPM 包安装 libpcap …… 57
3.3 安装 Snort …… 57
3.3.1 从源代码安装 Snort …… 57
3.3.2 定制安装:编辑 snort.conf 文件 …… 59
3.3.3 从 RPM 安装 Snort …… 62
3.3.4 在 MS Windows 平台上的安装 …… 63
3.3.5 安装 Bleeding-Edge 版本的 Snort …… 69
小结 …… 69
本章快速回顾 …… 70

FAQ …… 70
第四章 Snort 的内部工作 …… 73
4.1 Snort 的主要部件 …… 74
4.1.1 捕获网络流量 …… 75
4.1.2 抓包 …… 77
4.2 包解码 …… 80
4.3 数据包处理 …… 83
4.3.1 预处理器 …… 83
4.4 规则解析和检测引擎 …… 89
4.4.1 规则建立 …… 89
4.4.2 检测插件 …… 95
4.5 输出与日志 …… 96
4.5.1 将 Snort 用作快速嗅探器 …… 97
4.5.2 入侵检测模式 …… 100
4.5.3 将 Snort 用作 honeypot 捕获器和分析器 …… 102
4.5.4 记录至数据库 …… 102
4.5.5 使用 SNMP 方式报警 …… 105
4.5.6 以 Barnyard 和 Unified 格式输出 …… 104
小结 …… 105
本章快速回顾 …… 105
FAQ …… 106
第五章 规则的运行 …… 109
5.1 理解配置文件 …… 110
5.1.1 定义和使用变量 …… 110
5.1.2 配置项的灵活应用 …… 112
5.1.3 包含规则文件 …… 114
5.2 规则头 …… 115
5.2.1 规则动作选项 …… 115
5.2.2 可支持的协议 …… 117
5.2.3 指派源和目的 IP 地址 …… 118
5.2.4 指派源和目的端口 …… 119
5.2.5 理解方向操作符 …… 120
5.2.6 Activate 和 Dynamic 规则特性 …… 121
5.3 规则体 …… 122
5.3.1 规则 Content 选项 …… 123

5.3.2 IP 选项集合 …… 126
5.3.3 TCP 选项集合 …… 128
5.3.4 ICMP 选项集合 …… 129
5.3.5 规则识别选项集合 …… 129
5.3.6 其他规则选项 …… 132
5.4 “好”规则的构成 …… 134
5.4.1 规则动作 …… 134
5.4.2 定义恰当的 Content …… 134
5.4.3 合并子网掩码 …… 137
5.5 测试规则 …… 139
5.5.1 压力测试 …… 139
5.5.2 独立规则测试 …… 140
5.5.3 测试 BPF 规则 …… 140
5.6 调整规则 …… 140
5.6.1 配置规则变量 …… 140
5.6.2 取消规则 …… 141
5.6.3 BPF …… 142
小结 …… 143
本章快速回顾 …… 143
FAQ …… 144
第六章 预处理器 …… 147
6.1 什么是预处理器 …… 149
6.2 包重组的预处理器选项 …… 149
6.2.1 stream4 预处理器 …… 149
6.2.2 frag2——分片重组和攻击检测 …… 158
6.3 协议解码和规范化的预处理器选项 …… 159
6.3.1 Telnet 协商 …… 159
6.3.2 HTTP 规范化 …… 160
6.3.3 rpc_decode …… 162
6.4 非规则和异常检测预处理器选项 …… 164
6.4.1 端口扫描 …… 164
6.4.2 Back Orifice …… 166
6.4.3 非规则检测 …… 167
6.5 实验阶段的预处理器 …… 167
6.5.1 arpspoof …… 167

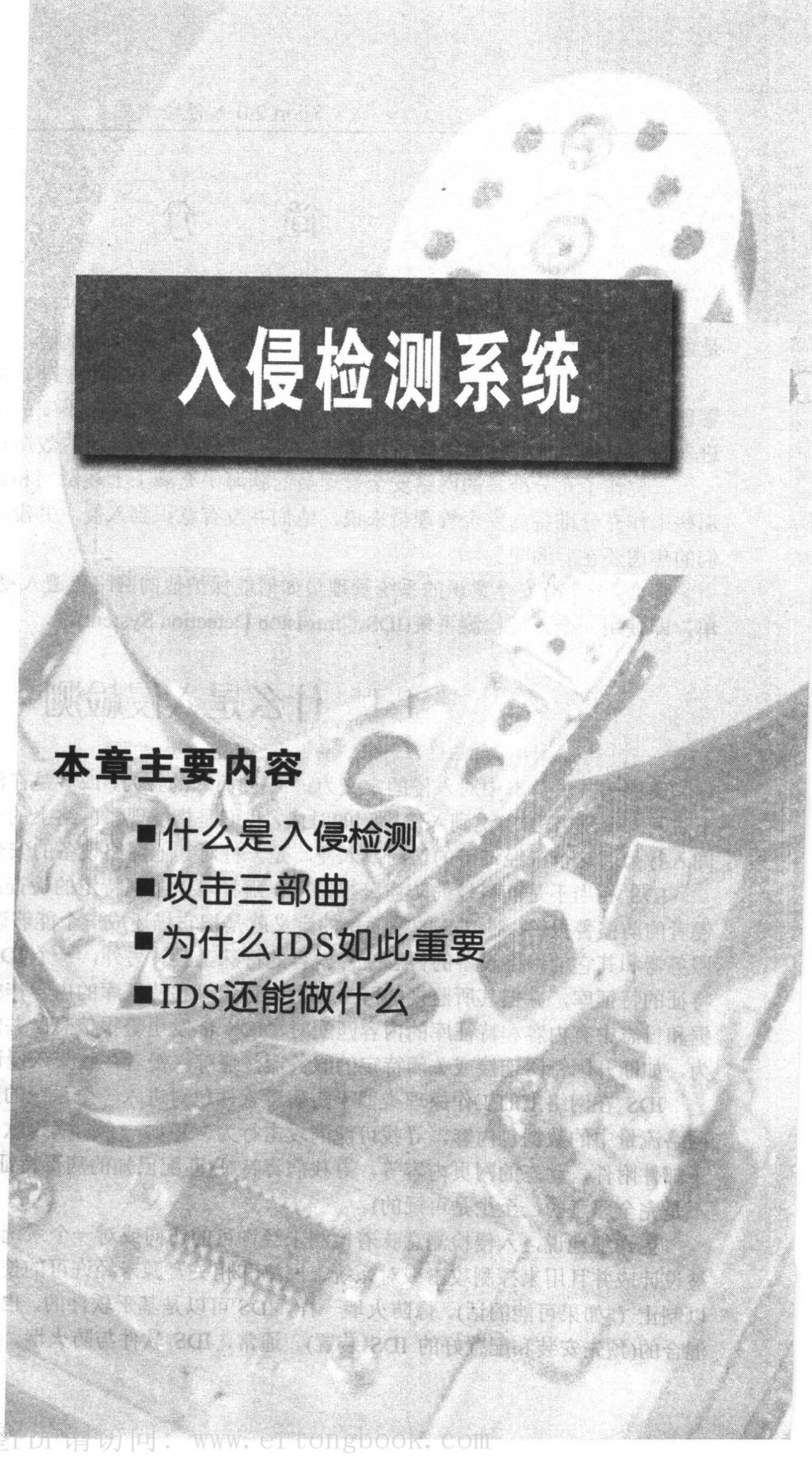
6.5.2 asn1 _ decode …… 168
6.5.3 fnord …… 168
6.5.4 portscan2 和 conversation 预处理器 …… 169
6.5.5 perfmonitor …… 171
6.6 书写自己的预处理器 …… 171
6.6.1 包重组 …… 171
6.6.2 解码协议 …… 171
6.6.3 非规则的或基于异常的检测 …… 172
6.6.4 建立自己的预处理器 …… 172
6.6.5 Snort 给了我什么 …… 174
6.6.6 在 Snort 内加入预处理器 …… 191
小结 …… 193
本章快速回顾 …… 194
FAQ …… 195
第七章 Snort 输出插件的实现 …… 197
7.1 什么是输出插件 …… 198
7.2 输出插件选项 …… 200
7.2.1 缺省的日志方式 …… 200
7.2.2 Syslog …… 204
7.2.3 PCAP 日志 …… 205
7.2.4 Snortdb …… 206
7.2.5 unified 日志 …… 211
7.3 编写输出插件 …… 214
7.3.1 为什么编写输出插件 …… 214
7.3.2 建立定制的输出插件 …… 215
7.3.3 Snort 的输出处理 …… 218
小结 …… 220
本章快速回顾 …… 221
FAQ …… 222
第八章 数据分析工具的使用 …… 225
8.1 使用 Swatch …… 226
8.1.1 安装 Swatch …… 226
8.1.2 配置 Swatch …… 228
8.1.3 使用 Swatch …… 229
8.2 使用 ACID …… 232

8.2.1 安装 ACID …… 232
8.2.2 配置 ACID …… 238
8.2.3 ACID 的使用 …… 241
8.3 使用 SnortSnarf …… 250
8.3.1 安装 SnortSnarf …… 250
8.3.2 配置 Snort 使其和 SnortSnarf 一起工作 …… 251
8.3.3 SnortSnarf 的基本用途 …… 252
8.4 使用 IDScenter …… 254
8.4.1 安装 IDScenter …… 255
8.4.2 配置 IDScenter …… 256
8.4.3 IDScenter 基本用法 …… 258
小结 …… 264
本章快速回顾 …… 265
FAQ …… 265
第九章 Snort 的升级 …… 267
9.1 打补丁 …… 268
9.2 升级规则 …… 269
9.2.1 规则如何维护 …… 269
9.2.2 如何获得规则的更新 …… 271
9.2.3 如何合并规则 …… 274
9.3 测试规则更新 …… 276
9.4 关注规则更新 …… 281
小结 …… 281
本章快速回顾 …… 282
FAQ …… 283
第十章 Snort 的优化 …… 285
10.1 如何选择硬件 …… 286
10.1.1 什么构成了“好”硬件 …… 287
10.1.2 如何测试硬件 …… 289
10.2 如何选择操作系统 …… 290
10.2.1 对于 NIDS 来说什么是“好”操作系统 …… 290
10.2.2 应该使用何种操作系统 …… 294
10.2.3 如何测试所选择的操作系统 …… 295
10.3 加速 Snort 安装 …… 296
10.3.1 决定使用哪些规则 …… 296

10.3.2 配置预处理器以提高速度 …… 298
10.3.3 使用通用变量 …… 299
10.3.4 选择输出插件 …… 299
10.4 配置的基准测试 …… 300
10.4.1 基准测试的特征 …… 300
10.4.2 哪些工具可用于基准测试 …… 301
小结 …… 309
本章快速回顾 …… 310
FAQ …… 310
第十一章 Barnyard 插件 …… 313
11.1 Barnyard 是什么 …… 314
11.2 Barnyard 的准备与安装 …… 315
11.3 Barnyard 的工作方式 …… 318
11.3.1 使用 Barnyard 配置文件 …… 319
11.3.2 深入 Barnyard …… 320
11.3.3 创建并显示二进制日志输出文件 …… 322
11.4 Barnyard 输出选项 …… 326
11.5 如何设置个性化输出 …… 327
11.5.1 输出插件的例子 …… 328
小结 …… 350
本章快速回顾 …… 351
FAQ …… 352
第十二章 深入 Snort …… 353
12.1 基于策略的 IDS …… 354
12.1.1 定义 IDS 的网络策略 …… 355
12.1.2 基于策略 IDS 的例子 …… 358
12.1.3 制作基于策略的 IDS …… 364
12.2 内嵌式 IDS …… 367
12.2.1 基于 Snort 的内嵌式 IDS …… 368
12.2.2 安装 Snort 为内嵌模式 …… 368
12.2.3 使用内嵌式 IDS 保护网络 …… 383
小结 …… 386
本章快速回顾 …… 386
FAQ …… 387
附录 …… 388

第一章

入侵检测系统



本章主要内容

- 什么是入侵检测
- 攻击三部曲
- 为什么IDS如此重要
- IDS还能做什么