第一图书网, tushu007.com

# <<Snort 2.0入侵检测>>

## 图书基本信息

书名：<<Snort 2.0入侵检测>>

13位ISBN编号：9787118033052

10位ISBN编号：7118033057

出版时间：2004-1

出版时间：第1版 (2004年1月1日)

作者：卡斯韦尔 (CaswellBrian)

页数：395

字数：567000

译者：宋劲松

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

# <<Snort 2.0入侵检测>>

## 内容概要

《Snort2.0入侵检测》一书是第一本系统介绍Snod入侵检测系统的权威著作，snort．Org网站的BrianCas— wel，是本书作者之一。
通过本书对Snort的深入剖析，读者可洞悉Snon的技术内幕，全面掌握其复杂的安装、设置及所有技术难题。
Snort的三大主要功能：包嗅探、包日志和入侵检测。
详细说明如何在Linux或MicrosoftWindows上安装Snod。
确定五种选项中的哪一种最适合您：pass，log，alert，dynamic和activate。
如何根据所用网络中的关键协议、服务以及希望告警日志的多寡来取舍规则 使用stream4和frag2预处理器增强Snort原本的规则匹配模式。
使用unified日志提高Snort探测的效率，解放Snod引擎的负载。
管理输出插件。
通过安装、配置、使用Swatch、 ACID、SnodSaff、IDSCenter和其他插件来监视日志文件。
关注规则升级。
使用半自动工具oinkmaster下载和比较出新规则。
安装、配置Barnyard。
Barnyard主要工作在三种操作模式：单次模式、连续模式和连续检查点模式。

## 作者简介

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Source-fire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》评为IT安全市场最有影响的厂商之一。

## 书籍目录

第一章 入侵检测系统 1.1 什么是入侵检测 1.2 攻击三部曲 1.3 为什么IDS如此重要 1.4 IDS还能做什么 小结 本章快速回顾 FAQ第二章 Snort 2.0介绍 2.1 什么是Snort 2.2 Snort的特性 2.3 在网络中部署Snort 2.4 Snort的安全考虑 小结 本章快速回顾 FAQ第三章 安装Snort 3.1 关于Linux发布版本的简要介绍 3.2 安装PCAP 3.3 安装Snort 小结 本章快速回顾 FAQ第四章 Snort的内部工作 4.1 Snort的主要部件 4.2 包解码 4.3 数据包处理 4.4 规则解析和检测引擎 4.5 输出与日志 小结 本章快速回顾 FAQ第五章 规则的运行第六章 预处理器第七章 Snort输出插件的实现第八章 数据分析工具的使用第九章 Snort的升级第十章 Snort的优化第十一章 Barnyard插件第十二章 深入Snort附录

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com