

<<网络入侵检测>>

图书基本信息

书名：<<网络入侵检测>>

13位ISBN编号：9787118035377

10位ISBN编号：7118035378

出版时间：2004-9

出版时间：国防工业出版社

作者：宋劲松

页数：294

字数：436000

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>

<<网络入侵检测>>

内容概要

本书由浅入深，全面介绍了关于入侵检测产品和技术的方方面面。

全书共分16章，内容由四大部分组成。

第一部分为第1章至第3章，介绍入侵检测的概念、选购和使用等内容。

读者通过这一部分能了解入侵检测产品的现状，成为一个成熟的使用者。

第二部分为第4章至第8章，深入介绍一种开放源码的入侵检测系统(IDS)——Snort的配置、使用、维护等内容，帮助对IDS技术感兴趣的读者了解IDS的原理。

第三部分为第9章至第13章，分析了Snort的代码实现，从代码层面剖析IDS的技术，适合IDS的开发者和深入了解IDS技术的专业技术人员。

第四部分为第14章至第16章，分析了IDS的弱点，系统讨论了IDS的测试和发展趋势。

对IDS的欺骗、IDS的测试和IDS的前景是有一定IDS背景知识的人士所关心的热点问题，本书在这些问题上用专门的章节进行了深入的讨论。

本书可作为网络管理员、对网络安全产品和技术感兴趣的人士、网络安全开发人员和专家的参考资料，也可作为高等院校相关专业高年级本科生和研究生的教学参考书。

书籍目录

第1章 入侵检测概论 1.1 IDS是什么 1.2 如何检测入侵 1.3 IDS的分类 1.4 IDS的发展历史第2章 IDS产品介绍 2.1 NFR公司的NID 2.2 启明星辰天阜IDS 2.3 绿盟冰之眼IDS 2.4 Snort第3章 IDS的部署和使用 3.1 选择IDS的原则 3.2 IDS的部署 3.3 IDS的使用第4章 Snort介绍 4.1 Snort介绍 4.2 Snort安装第5章 Snort配置 5.1 命令行参数 5.2 Snort.conf文件 5.3 规则头 5.4 规则体 5.5 调整规则第6章 Snort预处理器 6.1 包重组的预处理 6.2 协议解码预处理器 6.3 异常检测处理器 6.4 实验阶段的预处理器第7章 Snort输出插件 7.1 关键组件介绍 7.2 输出插件选项第8章 Snort升级维护第9章 Snort代码构架第10章 Snort检测引擎第11章 Snort规则处理代码第12章 Snort预处理代码第13章 Snort日志模块代码第14章 IDS的弱点第15章 IDS的测试第16章 IDS产品的发展趋势

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>