

<<Snort轻量级入侵检测系统全攻略>>

图书基本信息

书名：<<Snort轻量级入侵检测系统全攻略>>

13位ISBN编号：9787563519668

10位ISBN编号：7563519661

出版时间：2009-7

出版时间：北京邮电大学出版社

作者：孙伟，周继军，许德武 编著

页数：314

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轻量级入侵检测系统全攻略>>

### 前言

随着互联网的飞速发展，攻击和入侵等安全问题与日俱增，给很多网络管理员带来了巨大的压力。考虑到网络数据的巨大价值，安全业务已持续成为各大公司和研究机构关注的重点。面对这些挑战，国内外很多公司近年来相继开发出了各种专用入侵检测系统（IDS，Intrusion Detection System），其价值动辄数万元甚至数十万元人民币。

厂商的宣传往往让用户眼花缭乱，在面对形形色色价格昂贵的商用产品时难以适从。大部分技术人员往往更关心如何判断产品的好坏，如何在网络中部署IDS，如何在使用中配置和调试IDS等问题，而这些从厂商的宣传材料中是得不到的。

其实，人们还有更好的选择，这就是著名的骨灰级开源IDS软件系统——Snort。

它在业内的重要地位可称“一直被模仿，从未被超越”，在国内的安全行业甚至成为IDS系统的代名词，其规则语法更成为了事实上的业界标准。

Snort设计简洁，功能强大，无论对小的家庭用户还是繁忙的公司网络，它都有能力实时分析和记录通信流，其基于规则的检测引擎能够检测多种变种攻击。

Snort几乎能兼容所有硬件平台和操作系统，并提供丰富的报警记录信息以供选择。

它还能帮助用户确定网络中一些莫名其妙的服务的作用，其可扩展的体系结构和开源模式更使得用户群不断增长。

上述优点来自Snort开发小组的紧密努力：构造一个卓越的IDS系统内核。

“量身订做”的特性是如此灵活，以至于新手们往往无所适从。

对此，全世界的程序员们围绕着Snort开发了大量适用于各种需求和各种应用环境的应用程序、工具和脚本，极大地降低了Snort配置使用所要求的技术门槛。

因此，管理员们所需做的不是强忍不适磕磕绊绊地使用Snort，而是发现Snort的奇妙之处，找到称手的Snort应用工具，将它们和Snort内核DIY成一款强大的IDS。

## <<Snort轻量级入侵检测系统全攻略>>

### 内容概要

全书共11章，主要内容包括四个方面，较为全面地介绍了Snort入侵检测系统的安装部署、配置、调整及使用，基本涵盖了Snort有关的方方面面。

本书的特点是实用性非常强，概念准确、实例丰富，能够培养读者建立一套实用IDS的实际动手能力。另外，本书深入到snort的具体技术细节中，是一本不可多得的全面掌握Snort的技术图书。

本书面向的对象为具有基本网络技术知识的读者，即使读者以前从未接触过IDS，书中穿插的实例也能帮助读者成为IDS高手。

对于资深网管，本书能提供一种性价比高的安全解决方案。

同时，对于已学习过网络课程的大中专在校生，本书也可作为入侵检测或信息安全课程的授课辅助材料。

## &lt;&lt;Snort轻量级入侵检测系统全攻略&gt;&gt;

## 书籍目录

第1章 入侵检测基础概念 1.1 入侵检测系统的作用 1.2 IDS的标准结构 1.3 如何检测入侵 1.4 IDS的分类 1.4.1 NIDS 1.4.2 HIDS 1.4.3 DIDS 1.5 攻击的来源 1.6 IDS的部署和使用 1.6.1 IDS的选择 1.6.2 IDS的部署第2章 Snort应用基础 2.1 Snort简介 2.2 Snort原理 2.2.1 整体结构 2.2.2 Snort在网络层次模型中的位置 2.3 代码流程 2.4 内部工作流程 2.4.1 捕获网络流量 2.4.2 包解码器 2.4.3 预处理器 2.4.4 规则解析和探测引擎 2.4.5 报警输出模块 2.5 Snort的部署 2.5.1 部署策略 2.5.2 操作系统平台的选择 2.5.3 三层体系结构 2.5.4 三位一体的集成式安装第3章 面向小型网络的集成式安装 3.1 安装Snort IDS所需软件 3.1.1 传感器层软件 3.1.2 服务器层软件 3.1.3 集成工具包 3.1.4 管理员控制台 3.1.5 Snort管理工具 3.1.6 各类库 3.1.7 Snort虚拟机 3.2 windows下的集成式安装 3.2.1 安装Snort和Winpcap包 3.2.2 AppServ 3.2.3 安装Adodb、jgraph和ACID 3.2.4 配置Snort 3.2.5 系统测试 3.3 Linux下的集成式安装 3.3.1 Linux平台下软件的一般安装方法 3.3.2 安装Snort 3.3.3 安装IDS配套软件 3.3.4 MySQL的安装和配置 3.3.5 Adodb、ACID的安装和配置 3.3.6 Linux下的安装测试第4章 Snort的分离式安装 4.1 分离式安装中的安全连接 4.1.1 openSSL 4.1.2 Stunnel 4.1.3 ODenSSH 4.1.4 其他SSH软件 4.2 建立服务器 4.2.1 安装指南 4.2.2 Linux平台下安装配置 4.2.3 Windows平台下安装配置 4.3 建立传感器 4.3.1 安装指南 4.3.2 安装传感器 4.4 建立管理员控制台 4.4.1 PuTTY的安装和使用 4.4.2 ScreenCRT的安装和使用第5章 Snort的使用 5.1 配置文件 5.1.1 定义和使用变量 .....第6章 规则语法及使用第7章 IDS攻击与Snort预处理器第8章 输出插件和数据分析工具第9章 Snort管理工具第10章 IDS测试评估第11章 Snort入侵检测实例分析参考文献

## <<Snort轻量级入侵检测系统全攻略>>

### 章节摘录

插图：HIDS和NIDS有两点不同：HIDS只能保护它所在的计算机，计算机网卡设置的是“非混杂模式”，不像NIDS需要将网卡设置为混杂模式，在HIDS中，网卡只在正常的“非混杂模式”下工作，因为不是所有的网卡都能设置成混杂模式的。

另外，对配置低的计算机来说，混杂模式对CPU的占用会很明显地体现出来。

HIDS的另一个好处是可以精确地根据自己的需要定制规则。

例如，如果运行HIDS的计算机上没有运行域名服务（DNS），就不需要加上那些检测DNS攻击的规则集。

减少了不相关的规则可以提高检测效率和降低处理器的负荷。

图1-3描述了一个在一些服务器和个人计算机上安装了HIDS的网络。

如前所述，安装在邮件服务器上的HIDS主要设置和邮件服务器相关的规则，使其免受入侵，而安装在Web服务器上的IDS主要设置和web服务相关的规则，检测对Web服务器的攻击。

在安装的时候，零散的计算机可以使用常用的规则集，当有新的漏洞公布后，规则要及时和定期地更新以检测新漏洞。

基于主机的传感器收集的信息准确，但是占用服务器资源，尤其在繁忙的服务器上会降低服务器性能。

而且，基于主机的传感器是与操作系统相关的，如果使用了IDS产品不支持的操作系统就不能安装HIDS。

## <<Snort轻量级入侵检测系统全攻略>>

### 编辑推荐

《Snort轻量级入侵检测系统全攻略》由北京邮电大学出版社出版。

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>