<<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

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。

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。

<<Snort轻量级入侵检测系统全攻略>>

书籍目录

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Nil）S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（2PIJ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。

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