<<入侵检测理论与技术>>

图书基本信息

书名：<<入侵检测理论与技术>>

13位ISBN编号：9787040200164

10位ISBN编号：7040200163

出版时间：2006-9

出版时间：北京蓝色畅想图书发行有限公司（原高等教育出版社）

作者：杨义先,钮心忻

页数：321

前言

顾名思义，入侵检测就是检测入侵行为。
目前的入侵检测系统（IDS）大致可以分为两类：基于主机的IDS和基于网络的IDS。
前者是一种集中式的IDS，相当于直接针对敌方总部，一旦发现敌情马上报告，并采取相应的措施。
后者是一种分散式的IDS，它广泛收集敌方各军事点的情报，加以综合分析，一旦发现敌情，马上采取措施加以应对。
最近，基于网络的IDS又进一步发展成为分布式IDS和大规模分布式IDS。
形象地说，分布式IDS不但要对敌国的各军事点情报进行综合和分析，而且也不放过敌国其他领域的情报，比如，根据敌国大量屯集医药用品的事实来判断敌国可能发动战争等。
而大规模分布式IDS则将刺探敌情的范围扩大到敌国的伙伴国家，因为，这些国家的异常举动可能泄露某种攻击信息。
本书将对包括基于主机的IDS和基于网络的IDS进行研究，重点研究分布式IDS和大规模分布式IDS系统的理论和技术。
全书共分为7章，各章内容与安排如下。
第l章着重分析了当今主流网络攻击手段，并针对每一种攻击，尽量提出相应的检测、防御方法。
当前的入侵方法中，有的是寻找并利用操作系统的漏洞，有的是利用应用程序的实现上的漏洞，有的是针对网络协议漏洞而进行攻击，有的是寻找加密算法的弱点进行密码破解，有的是利用网络协议在特定的操作系统上的实现的漏洞进行入侵，等等。
本章重点分析了目前常见的拒绝服务攻击和分布式拒绝服务攻击的原理和手段，包括了CP标志位攻击、通用洪流攻击、反射式攻击等；介绍了常用的分布式拒绝服务攻击工具，包括Trinoo、TFN、TFN2K、Stachcldraht、shaft和stream等；总结了目前分布式攻击的类型和特点。
在对目前分布式攻击的类型和特点分析的基础上，提出了分布式攻击的发展趋势，主要包括体系结构及特点。
其中主要特点包括可控性强、隐蔽性强、可更新性、智能性和通信安全保密性等。
本章将目前针对分布式拒绝服务攻击的防御划分为三个层次并进行比较，然后提出了源端防御的概念；介绍了源端防御程序设计并给出其体系结构及各模块结构图。
本章在对分布式拒绝服务攻击的防御手段进行深入分析后，提出了未来分布式防御的发展趋势及智能型分布式防御模型，给出了模型的体系结构和特点，并分析了实现需要解决的一些关键问题。

<<入侵检测理论与技术>>

内容概要

本书从理论和技术两个方面对入侵检测相关知识进行了全面和系统的介绍。
全书共分7章，分别对常见入侵与防御、入侵检测基础、大规模分布式入侵检测系统（LDIDS）框架结构、LDIDS的互动协议与接口标准、LDIDS的任务分派机制、LDIDS的数据融合和入侵管理等进行了介绍，内容包括网络安全的主要威胁、常见网络攻击、DDoS攻击与防御、智能型分布式防御、IDS 系统模型等人侵检测理论与技术方面的知识。
另外，书中介绍的许多算法、协议、方案等都可直接应用于工程实践，书中提出的许多理论问题也有助于激发更多的后继研究。

本书可作为信息安全、密码学、信息与计算科学等专业的研究生和高年级大学生的教学参考书，也可作为上述领域相关科技工作者的实用工具书或技术培训教材。

作者简介

杨义先，北京邮电大学教授，博士生导师，首届长江学者特聘教授，首届政府特殊津贴获得者。
长期从事信息安全、信号与信息处理、密码学等专业的教学、科研和成果转化工作。
已发表论文300余篇、出版著作10余部。
本书相关研究成果获邮电部科技进步一等奖、国家教委科技进步二等奖、中国通信学会科学技术二等奖等多项奖励。

<<入侵检测理论与技术>>

书籍目录

章节摘录

插图：系统状态监控模块和网络数据包检测模块发现异常状态后，提交至事件处理模块，由该模块负责处理，处理时参照的规则是程序预先设定或者由用户通过配置模块设置的。
处理完毕后，由日志记录模块负责记录相应的处理结果。
同时，日志记录模块还负责对其他配置信息等进行记录。
源端防御的程序流程如图1.9所示。
程序启动时，用户可以对默认配置进行修改。
启动后，隐藏模块首先启动，与隐藏模块相关的所有进程、文件、注册表等内容均被隐藏，可以很好地保护源端程序。
然后，系统状态监控模块和网络数据包检测模块启动，针对系统状态和网络流量进行实时监测，一旦发现异常状态或流量，将其转人事件处理模块进行处理。
整个流程中的重要信息由日志记录模块进行记录。
源端防御各模块之间的交互如图1.10所示。
隐藏模块是所有模块的基石，为系统中所用到的程序、文件、注册表项等实现隐藏功能，保护防御程序自身。
配置模块与系统中其他模块均进行交互，可以配置监控选项，如进程、端口、特定目录和特定注册表等；也可以对网络数据包检测的规则进行修改、添加和删除等操作；还可以设置异常事件发生时处理的规则；同样也可以配置待隐藏的特征值。
需要注意的是，配置模块应该定期对以上各规则进行更新，以达到更好的保护效果。

编辑推荐

《入侵检测理论与技术》是由高等教育出版社出版的。

版权说明