<<网络防御与安全对策>>

图书基本信息

书名：<<网络防御与安全对策>>

13位ISBN编号：9787302177777

10位ISBN编号：7302177775

出版时间：2008-10

出版时间：伊斯特姆 (Easttom.C.)、 张长富 清华大学出版社 (2008-10出版)

作者：伊斯特姆

页数：324

译者：张长富

前言

安全系列丛书是为将要从事信息技术安全职业的学员准备的一套丛书。
这套丛书提供了来自业界专家的实践箴言，和对你手把手的培训。
该丛书中的每本书，都列举了现实生活中大量的例子。
这些例子能帮助你将所学到的知识应用到你的工作中去。
以下是本书的几个关键元素，这些元素的目的是帮助学员解决学习过程中的一些问题。
本章目标:这些扼要、可行的目标概括了该章将涵盖哪些内容。
本章导论: 每章开始先阐释一下每个主题的重要性，以及这些主题在整本书篇章结构中的地位。
实例:从书中提取出概念，而且展示这些概念是如何用在实际场所中的。
提示: 和主题相关、但是超出了本书讨论范围的额外信息。
注意:不可忽视的、关键的信息。
这些信息和上下文直接相关。
技能测试: 每章末都附有习题，这些习题呼应该章目标，巩固相关的知识点。
每章有四种题型：多项选择题: 测验读者对该章内容的理解程度。
练习题: 围绕章节中出现的个别概念设计的简要、引导性的课程项目。
项目题:综合一章内若干知识点的较长、引导性的课程项目。
案例研究:运用该章中的知识点来解决问题的实际场景。
本系列丛书包括：计算机安全基础信息安全：原理与实践防火墙与VPN：原理与实践安全策略与过程：原理与实践网络防御与安全对策：原理与实践

<<网络防御与安全对策>>

内容概要

《网络防御与安全对策：原理与实践》提供了理论基础与实际应用的结合。
每一章的末尾都给出了多项选择题、练习题、项目题和一个案例研究。
成功学完本教材，包括每章末尾的材料，读者应该能够深入地理解网络安全。
《网络防御与安全对策：原理与实践》向读者提供了额外的资源，它们扩充了相应章节提供的内容。
《网络防御与安全对策：原理与实践》适合于对网络运行（包括基本术语、协议和设备）有了基本了解的读者。
读者不需要拥有比初步计算机课程要求的更多的数学背景知识。
《网络防御与安全对策：原理与实践》概述　　《网络防御与安全对策：原理与实践》将带你穿越错综复杂的保护网络、避免攻击的迷宫。
第1章“网络安全引论”简要介绍网络安全领域，第2章“攻击类型”解释了对网络的威胁，包括拒绝服务攻击、缓冲区溢出攻击以及病毒。
第3章“防火墙基础”、第4章“防火墙实际应用”、第5章“入侵检测系统”和第7章“虚拟专用网”，详细叙述了各种安全技术，包括防火墙、入侵检测系统以及VPN。
这些项目是网络安全的核心，因此《网络防御与安全对策：原理与实践》的一个重要部分就是专注于确保读者全面理解隐藏在它们背后的概念以及实际的应用。
在每一案例中，都包括了给定网络下选择恰当技术的实际指导。
第6章“加密”提供了加密的坚实基础。
这个主题很关键，原因在于，计算机系统本质上就是一个用于存储、传输和操纵数据的设备。
无论网络如何安全，如果它传输的数据不安全的话，就存在相当大的危险。
第8章“操作系统加固”讲授操作系统的加固方法。
第9章“防御病毒攻击”和第10章“防御木马、间谍软件、广告软件的攻击”，为读者提供了特殊的防御策略和技术来抵御最常见的网络威胁。
第11章“安全策略”向读者提供了安全策略的概貌。

作者简介

作者：(美国)伊斯特姆 (Easttom.C.) 译者：张长富ChtJck Easttom，在IT行业具有多年的实践经验，随后有3年时间，在一家技术学院教授计算机科学．包括计算机安全课程。
后来，他又离开学术界，转向IT业，在美国得克萨斯州的达拉斯的一家公司担任IT经理。
除了日常事务之外，他还负责计算机安全。
他编写过7本有关程序设计、Web开发和Linux的图书。
Chuck拥有20多个不同的证书，包括CIW安全分析师（SecLJrity Arlalyst）、MCSE、MCSA、MCDBA、MCAD、Server+和其他证书。
在ComTIA（Computer Tectlrbology IndIJstryAssociation 计算机技术协会），他作为相关科目的专家，曾制定和修订4种认证考试，包括Security+认证的初始创建。
业余时间，ChtJck还是达拉斯地区学院的兼职教师，教授各种课程，包括计算机安全。
他时常还作计算机安全的咨询工作。
Chuck经常作为计算机团体的客座演讲人．主要讨论安全问题。

<<网络防御与安全对策>>

书籍目录

章节摘录

我们将考察的一种攻击类型是拒绝服务（Dos）。
回忆一下第1章，拒绝服务攻击是旨在阻止合法用户使用目标系统的任何攻击。
这类攻击并不实际侵入系统或获取敏感信息，它的目标简单说就是阻止合法用户访问给定的系统。
这种类型的攻击相当常见，事实上，这是最常见攻击类型之一。
许多专家认为这种攻击十分常见，原因在于绝大多数拒绝服务攻击都相当容易被实现。
这种易于实现的攻击特性意味着即使仅仅具备很低的技术素质也通常能够成功地完成拒绝服务攻击。
拒绝服务的本质概念基于这样的事实：任何设备都有可用性的限制。
这个事实适合于所有设备，而不仅仅适合于计算机系统。
例如，大桥的设计有一个承重限制；飞机有一个不重新加油时飞行距离的限制；汽车只能加速到一定的速度。
所有这些各式各样的设备都有一个共同的特征：它们对能够完成工作的能力都设置了限制。
计算机与这些设备或其他任何机器没有任何差别，它们也都有限制。
任何计算机系统、Web服务器或网络都仅仅能够处理有限的负载。
负载（及其限制）如何定义根据机器的不同而变化。
计算机系统的负载可以以数种不同的方式定义，包括按并发用户数量、文件的长度、数据传输速度或数据的存储量。
超过这些限制中的任何限制都将造成系统停止响应。
例如，如果你能够向web服务器发送大量超过其处理能力的请求，那么该服务器将过载，不再响应新的请求（Webopedia，2004）。
这一事实构成了DoS攻击的基础。
简单地使用请求使系统过载，它就不能够再对合法用户试图访问web服务器的请求做出响应。

编辑推荐

《网络防御与安全对策原理与实践》全面介绍了网络防御，网络安全威胁和保护网络的方法，内容包括拒绝服务攻击、缓冲区溢出攻击、以及病毒，防火墙和入侵检测系统，加密的基础知识，对网络的攻击、用于确保安全的设备和技术，安全策略的概貌如何评估网络安全，基于计算机的间谍和恐怖主义等。
每一章的末尾都给出了多项选择题、练习、项目和一个案例研究。
高等院校计算机及相关专业的本科生和教师，从事网络安全方面工作的人员。

<<网络防御与安全对策>>

版权说明