

<<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

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>

## <<网络防御与安全对策>>

### 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在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

## &lt;&lt;网络防御与安全对策&gt;&gt;

## 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。

## <<网络防御与安全对策>>

### 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 Tectlrbiology IndlJstryAssociation 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。

## &lt;&lt;网络防御与安全对策&gt;&gt;

## 书籍目录

第1章 网络安全引论11.1 引言11.2 网络基础21.2.1 基本网络结构21.2.2 数据包21.2.3 对安全来说意味着什么31.3 评估针对网络的可能攻击31.3.1 威胁的分类61.3.2 可能攻击91.3.3 威胁评估101.4 理解安全术语111.4.1 有关黑客的术语111.4.2 有关安全的术语131.5 走近网络安全141.5.1 边界安全模式151.5.2 分层安全模式151.5.3 混合模式151.5.4 网络安全和法律161.6 使用安全资源171.7 本章小结171.8 自测题181.8.1 多项选择题181.8.2 练习题201.8.3 项目题221.8.4 案例研究22第2章 攻击类型252.1 引言252.2 防御拒绝服务攻击262.2.1 DoS在行动262.2.2 SYN洪流302.2.3 Smurf攻击312.2.4 Ping of Death332.2.5 分布式反射拒绝服务332.2.6 DoS工具342.2.7 现实世界的示例362.2.8 如何防御DoS攻击392.3 防御缓冲区溢出攻击402.4 防御IP欺骗422.5 防御会话攻击432.6 阻止病毒和木马攻击442.6.1 病毒442.6.2 木马482.7 本章小结502.8 自测题512.8.1 多项选择题512.8.2 练习题532.8.3 项目题542.8.4 案例研究54网络防御与安全对策——原理与实践第3章 防火墙基础553.1 引言553.2 什么是防火墙553.3 防火墙的类型573.3.1 包过滤防火墙573.3.2 应用网关583.3.3 电路层网关593.3.4 状态数据包检查603.3.5 混合防火墙613.4 实现防火墙613.4.1 基于网络主机623.4.2 双宿主主机633.4.3 基于路由器的防火墙643.4.4 屏蔽主机643.5 选择和使用防火墙663.6 使用代理服务673.6.1 WinGate代理服务器683.6.2 NAT683.7 本章小结693.8 自测题693.8.1 多项选择题693.8.2 练习题713.8.3 项目题733.8.4 案例研究73第4章 防火墙实际应用754.1 引言754.2 使用单机防火墙754.2.1 WindowsXP764.2.2 SymantecNorton防火墙784.2.3 McAfee个人防火墙794.2.4 Wolverine814.3 使用小型办公/家庭办公防火墙824.3.1 SonicWall824.3.2 D-LinkDFL-300Office防火墙834.4 使用中型规模网络防火墙844.4.1 CheckPointFirewall-1844.4.2 Cisco PIX 515E854.5 使用企业防火墙864.6 本章小结874.7 自测题874.7.1 多项选择题874.7.2 练习题894.7.3 项目题904.7.4 案例研究91第5章 入侵检测系统935.1 引言935.2 理解IDS概念945.2.1 抢先阻塞945.2.2 渗透945.2.3 入侵诱捕955.2.4 入侵威慑965.2.5 异常检测965.3 理解和实现IDS系统975.3.1 Snort985.3.2 Cisco入侵检测995.4 理解和实现蜜罐1005.4.1 Specter1015.4.2 Symantec Decoy Server1035.5 本章小结1035.6 自测题1045.6.1 多项选择题1045.6.2 练习题1055.6.3 项目题1065.6.4 案例研究107第6章 加密1096.1 引言1096.2 加密的历史1096.2.1 恺撒密码1106.2.2 多字母表置换1146.2.3 二进制操作1146.3 学习现代加密方法1166.3.1 PGP1166.3.2 公钥加密1176.3.3 数据加密标准1176.3.4 RSA1186.3.5 Blowfish1196.3.6 AES1196.3.7 IDEA加密1206.3.8 选择块密码1206.3.9 识别好的加密方法1216.4 理解数字签名和证书1216.5 理解和使用解密1226.5.1 Solarwinds1236.5.2 Brutus1236.5.3 John the Ripper1246.5.4 其他的口令破解器1256.6 加密的未来展望1256.7 本章小结1266.8 自测题1276.8.1 多项选择题1276.8.2 练习题1296.8.3 项目题1306.8.4 案例研究131第7章 虚拟专用网1337.1 引言1337.2 基本的VPN技术1347.3 使用用于VPN加密的VPN协议1357.3.1 PPTP1357.3.2 PPTP认证1377.3.3 L2TP1387.3.4 L2TP认证1387.3.5 L2TP与PPTP的比较1397.4 IPsec1407.5 实现VPN解决方案1417.5.1 Cisco解决方案1417.5.2 服务解决方案1427.5.3 FreeS/wan1427.5.4 其他解决方案1427.6 本章小结1447.7 自测题1447.7.1 多项选择题1447.7.2 练习题1467.6.3 项目题1487.6.4 案例研究148第8章 操作系统加固1498.1 引言1498.2 正确配置Windows1508.2.1 账户、用户、组和口令1508.2.2 设置安全策略1548.2.3 注册表设置1578.2.4 服务1618.2.5 加密文件系统1638.2.6 安全模板1658.3 正确配置Linux1668.4 给操作系统打补丁1688.5 配置浏览器1688.5.1 Microsoft Internet Explorer浏览器的安全设置1688.5.2 Netscape Navigator的安全设置1718.6 本章小结1738.7 自测题1738.7.1 多项选择题1738.7.2 练习题1758.7.3 项目题1778.7.4 案例研究177第9章 防范病毒攻击1799.1 引言1799.2 理解病毒攻击1809.2.1 什么是病毒1809.2.2 什么是蠕虫1809.2.3 病毒是怎样传播的1809.2.4 病毒愚弄1849.3 病毒扫描器1869.3.1 病毒扫描技巧1879.3.2 商业反病毒软件1889.4 反病毒策略和过程1969.5 防护系统的附加方法1979.6 如果系统感染了病毒怎么办1979.6.1 阻止病毒的传播1989.6.2 删除病毒1989.6.3 找出感染是怎样开始的1989.7 本章小结1999.8 自测题1999.8.1 多项选择题1999.8.2 练习题2019.8.3 项目题2029.8.4 案例研究203第10章 抵御特洛伊木马、间谍软件和广告软件20510.1 引言20510.2 特洛伊木马20610.2.1 识别特洛伊木马20610.2.2 特洛伊木马的征兆21010.2.3 阻止特洛伊木马21110.3 间谍软件和广告软件21210.3.1 识别间谍软件和广告软件21210.3.2 反间谍软件21410.3.3 反间谍软件策略21910.4 本章小结21910.5 自测题22010.5.1 多项选择题22010.5.2 练习题22210.5.3 项目题22310.5.4 案例研究223第11章 安全策略22511.1 引言22511.2 定义用户策略22611.2.1 口令22611.2.2 互联网使用22711.2.3 电子邮件附件22811.2.4 软件安装和删除22911.2.5 即时消息22911.2.6 桌面配置23011.2.7 有关

## &lt;&lt;网络防御与安全对策&gt;&gt;

用户策略的最后思考23011.3 定义系统管理员策略23111.3.1 新雇员23111.3.2 离开的雇员23111.3.3 变化要求23211.3.4 安全缺口23311.3.5 黑客入侵23411.4 定义访问控制23411.5 定义开发策略23511.6 本章小结23511.7 自测题23611.7.1 多项选择题23611.7.2 练习题23811.7.3 项目题24011.7.4 案例研究240第12章 评估系统24112.1 引言24112.2 评价安全风险24212.3 进行初期评估24412.3.1 补丁24412.3.2 端口24612.3.3 保护24612.3.4 物理24812.4 探查网络24912.4.1 NetCop24912.4.2 NetBrute25112.4.3 Cerberus25312.4.4 Unix上的端口扫描器：SATAN25612.4.5 SAINT25612.4.6 Nessus25712.4.7 NetStat Live25712.4.8 Active Ports25912.4.9 其他端口扫描器26012.5 安全文档26012.5.1 物理安全文档26112.5.2 策略和人员文档26112.5.3 探查文件26112.5.4 网络保护文件26112.6 本章小结26212.7 自测题26212.7.1 多项选择题26212.7.2 练习题26412.7.3 项目题26512.7.4 案例研究265第13章 安全标准26713.1 引言26713.2 运用Orange Book26713.2.1 D-最低保护26813.2.2 C-自主保护26813.2.3 B-强制的保护27113.2.4 A-可验证保护27513.3 运用彩虹系列27613.4 运用Common Criteria27913.5 使用安全模型28013.5.1 Bell-LaPadula模型28013.5.2 Biba Integrity模型28213.5.3 Clark-Wilson模型28213.5.4 Chinese Wall模型28213.5.5 State Machine模型28313.6 本章小结28313.7 自测题28413.7.1 多项选择题28413.7.2 练习题28513.7.3 项目题28613.7.4 案例研究287第14章 基于计算机的间谍活动和恐怖主义28914.1 引言28914.2 防范基于计算机的间谍活动29014.3 防范基于计算机的恐怖主义29514.3.1 经济攻击29614.3.2 威胁国防29714.3.3 一般攻击29814.4 选择防范策略30014.5 防范信息战30114.5.1 宣传30114.5.2 信息控制30214.5.3 实际案例30314.6 本章小结30414.7 自测题30414.7.1 多项选择题30414.7.2 练习题30614.7.3 项目题30714.7.4 案例研究308附录A 资源309A.1 Web站点309A.1.1 综合的网络安全309A.1.2 防火墙站点309A.1.3 反病毒站点309A.1.4 一般的计算机安全和计算机犯罪资源310A.1.5 加密310A.1.6 一般Hacking310A.1.7 端口扫描器和嗅探器310A.1.8 口令破解器311A.1.9 对策311A.1.10 间谍软件311A.1.11 反间谍软件网站311A.2 图书312A.3 机构312附录B 计算机安全教育和认证313B.1 理论培训和科目313B.2 行业认证314B.3 什么是理想的安全专业人员317词汇表319

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。

## <<网络防御与安全对策>>

### 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。

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>