第一图书网, tushu007.com

<<网络安全大全>>

图书基本信息

书名：<<网络安全大全>>

13位ISBN编号：9787302186199

10位ISBN编号：7302186197

出版时间：2008-10

出版时间：清华大学出版社

作者：胡文启，徐军，张伍荣 编

页数：405

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

第一图书网, tushu007.com

<<网络安全大全>>

前言

他山之石，可以攻玉。
——《诗经》　　你应该了解真相，真相会使你自由。
——《圣经》　　我之所以成功，是因为站在巨人的肩膀上。
——牛顿　　策划初衷　　网管员fNetwork Administrator）是国家劳动和社会保障部近年颁布的第四批国家职业标准中明确规定的一个新兴职业。
网管员职业要求从业者具备一系列专业、高端的计算机及网络操作技能。
为了给广大网管员提供一套标准实用的高效实战教材，清华大学出版社在广泛调研与充分论证的基础上，聘请了国内著名院校资深学者和实战经验丰富的网管专家，历时18个月精心打造了这套《网管实战宝典》。
本丛书由网管员的职业应用切入，根据网管员的行业内容细划科目，以实际工作的项目案例为主线，解决实际应用中可能出现的问题，是目前市面上唯一从“网管员职业应用案例实战”角度切入的精品丛书。
本套丛书全面介绍网络管理、设计与维护的热点应用案例，剖析透彻，确保技术的先进性、实用性和深入性，是网络管理员必备的实践读物。
首推书目　　《网管实战宝典》系列首批推出10本，书目如下。
1.《中型局域网组建一本通》　　2.《网络规划、设计与配置》　　3.《Windows Server 2003配置与管理》　　4.《Windows Server 2003服务器架设与管理》　　5.《网络管理工具使用大全》　　6.《网络安全大全》　　7.《Linux服务器架设与管理》　　8.《网络故障排除与维护技巧》（Windows版）　　9.《网络故障排除与维护技巧》（Linux版）

第一图书网, tushu007.com

<<网络安全大全>>

内容概要

本书以“应用实例导航”为主线，由浅入深、系统全面地介绍了网络安全中所遇到的一些问题和常用的网络安全设备的使用方法。
《网络安全大全》以企业网络应用的安全需求作为出发点，以实例的形式陈述攻击行为，然后对攻击原理进行分析，并通过部署相应的设备防止攻击再次发生来介绍网络安全。
《网络安全大全》结构清晰，易教易学，实例丰富，可操作性强，注重能力的提高，既可作为大中专院校的教材，也可作为各类培训班的培训教材。
此外，《网络安全大全》也可作为各类企业网络管理员及各类网络爱好者、企业IT经理以及网络安全工程师的参考用书。

第一图书网, tushu007.com

<<网络安全大全>>

书籍目录

第一图书网, tushu007.com

章节摘录

第1章　网络安全基础　　1.1.2　攻击事件的来源　　除了少部分黑客基于研究目的带来的攻击外，大多数的网络攻击出于一些特定的目的。
根据《2006年度中国网络安全报告》的结论，截止到2006年12月25日，据不完全统计，中国网络发生的网络攻击事件中，脚本入侵比例为53%，拒绝服务攻击比例为260名，漏洞利用比例为13%，暴力猜解比例为8%，社会工程学比例为5%，其他方法为1%。
但与2005年同期相比，2006年度的网络攻击事件要多出l倍之多。
据不完全统计，自2006年1月1日起，截至2006年12月25日，中国网站被篡改的数量达25 820个。
其中政府类网站有3661个；企业类网站为1l 828个（其中博客运营类被攻击数量达1683个）；教育/培训类被攻击网站数量达2216个，其中：中、职专及中小学网站占73.5%（1628个），大学网站的二级网站占18.0%（398个），培训类机构为127个，大学一级域名站点为63个。
　　下面是2006年出现在我国几个著名的攻击的事件。
　　2006年5月27日，某市的区政府服务器被入侵并植入香港汇丰银行的假冒网站。
　　2006年4月，国外多家媒体以《中国的银行网站被利用作Phishing》为题，报道了中国某银行网站被植入假冒Paypal网站的事件。
　　2006年6月19日，D市某区政府网站邮件服务器被入侵并植入电子港湾（eBay）的假冒网站。
　　2006年9月12日，著名搜索引擎百度遭受有史以来最大规模的不明身份黑客攻击，导致百度搜索服务在全国各地出现了近30分钟的故障。
　　2006年9月21日，某域名服务商“新网”域名解析服务器发生故障，造成超过　　30%在其上注册的网站无法访问长达20小时。
“新网”官方确认此次断网事件是黑客所为。
此事件被称为中国互联网的“9?21事件”。
　　在具体的攻击手法上也有变化，猜测口令、物理入侵、安装键盘记录设备以及盗窃笔记本电脑等传统方式的攻击成功率逐渐下降，而SOL注入、钓鱼、拒绝服务攻击以及各类木马病毒等攻击频率急剧上升。
更值得关注的是，内部人员滥用网络、盗窃关键数据的事件也在上升。
随着无线网络的使用，无线网络入侵也成为一个非常值得关注的焦点。
　　1.1.3　网络安全的关键要素　　虽然Internet的成功带来了全球信息化的一次巨大飞跃，但是它必须以保护有价值数据和网络资源免受篡改和入侵为基石。
　　1.网络安全目标　　M.Fites、P.Kratz等在《Control and Security of Computer Information Systems》中提出了一个被广泛采用的网络安全性设计建议。
该建议包括以下内容。
　　◇　确定要保护什么。
　　◇　确定尽力保护它免于什么威胁。
　　◇　确定威胁的可能性。
　　◇　以一种相对廉价的方法来实现资产保护的目的。
　　不断地检查这些步骤，发现弱点就进行改进。
　　2．资产评估　　资产评估用于实现网络安全目标的第一步，需要确定保护什么。
通常的资产评估仅对网络设备（例如交换机、路由器、防火墙、电脑）等实物以及关键数据进行评估，而忽视了这些设备上的配置信息、用户访问权利，随着DDoS攻击的增加，可用带宽和访问速率也成为资产评估一个不可缺少的部分。
当然资产评估随着需要保护的资产数量增长还会出现变化，下面列举了一些重要的网络资产。
　　网络设备：路由器、交换机、防火墙、入侵检测设备。
　　网络数据：数据服务器、邮件服务器、Web服务器等。
　　网络带宽：链接网络的链路带宽和速度，以及冗余备份线路。
　　个人电脑：个人电脑是否携带关键数据以及个人电脑安全防护。

第一图书网, tushu007.com

任意时刻通过网络的消息是否安全。
网络身份识别是否有效。
3. 威胁评估　　根据网络安全目标，完成资产评估后需要对威胁进行评估。通常的攻击手段主要有3种类型。

第一图书网, tushu007.com

编辑推荐

实用性：　　以实战项目案例为主线，以案例带动知识点，边实践边学习，快速上手。
先进性：阐述最为主流的网络技术及应用，精选最优网络实施方案。
深入性：应用案例讲解细致入微，分析透彻，过程完整。

第一图书网, tushu007.com

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