

<<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>

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(Network 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)

## <<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。

## 书籍目录

第1章 网络安全基础1.1 网络安全的基本原理1.1.1 网络发展及需求1.1.2 攻击事件的来源1.1.3 网络安全的关键要素1.1.4 用户安全意识1.2 网络安全实例分析1.2.1 资产评估1.2.2 风险分析1.2.3 制定安全策略1.3 网络的漏洞与攻击1.3.1 常见网络弱点1.3.2 常见攻击方法1.3.3 攻击分类1.3.4 攻击评估1.4 本章小结第2章 网络安全解决方案概述2.1 网络安全框架2.1.1 安全基准测试2.1.2 安全日志分析2.2 网络安全产品及解决方案2.2.1 防火墙2.2.2 VPN接入2.2.3 入侵检测2.2.4 集成安全设备2.2.5 DDoS检测和防范2.2.6 CSA与NAC2.2.7 网络安全设备联动2.3 本章小结第3章 网络设备安全3.1 网络设备的物理安全3.2 网络设备冗余3.2.1 HSRP简介3.2.2 HSRP工作原理3.2.3 配置HSRP3.2.4 HSRP安全3.2.5 VRRP3.3 网络设备访问安全3.3.1 网络设备的安全登录3.3.2 保存网络设备日志3.3.3 SNMP安全配置3.3.4 禁用不必要的服务3.3.5 登录警告3.4 本章小结第4章 路由器及路由协议安全4.1 路由协议安全概述4.2 增强路由协议的安全4.2.1 路由协议的认证方法4.2.2 R1P协议安全4.2.3 OSPF协议安全4.3 定向组播控制4.3.1 Smurf攻击4.3.2 单播逆向路径转发4.4 路由黑洞过滤4.5 路径完整性检查4.5.1 IP源路由4.5.2 ICMP重定向4.6 本章小结第5章 交换机及交换网络安全5.1 vLAN隔离5.1.1 VLAN划分5.2.1 动态VLAN概述5.2.2 配置动态VLAN5.2 动态VLAN5.2.1 动态VLAN概述5.2.2 配置动态VLAN5.3 安全的VTP协议5.3.1 vTP概述5.3.2 配置vTP协议5.4 安全的STP协议5.4.1 STP协议概述5.4.2 配置STP协议5.5 PVLAN5.5.1 PVLAN概述5.5.2 配置PVLAN5.6 防范其他常见2层攻击5.6.1 防范MAC泛洪攻击5.6.2 防范DHCP攻击5.6.3 防范ARP攻击5.7 本章小结第6章 网络身份认证服务6.1 电子证书服务6.1.1 PKI公钥基础结构6.1.2 安装证书服务6.1.3 用户申请证书6.1.4 证书吊销6.1.5 证书导入、导出6.2 AAA体系结构6.2.1 AAA概述6.2.2 配置AAA身份认证6.2.3 配置AAA授权6.2.4 配置AAA记账6.3 配置RADIUS服务器6.3.1 RADIUS简介6.3.2 微软IAS6.3.3 Cisco Secure ACS6.3.4 Linux RADIUS6.4 本章小结第7章 网络安全接入7.1 802.1x协议7.1.1 802.1x协议概述7.1.2 配置802.1x协议7.2 Windows自动更新7.2.1 WS[JS]简介7.2.2 安装WS[JS]服务器7.2.3 配置WS[JS]服务器7.2.4 配置WS[JS]客户端自动更新7.3 NAC网络接入控制7.3.1 终端安全接入概述7.3.2 Cisco NAC概述7.3.3 配置Cisco NAC7.4 终端保护机制7.4.1 Cisco CSA概述7.4.2 Cisco cSA架构及工作原理7.4.3 安装Cisco CSA MC7.4.4 配置Cisco CSA MC7.4.5 配置Cisco CSA客户端7.4.6 临控Cisco CSA MC7.5 本章小结第8章 防火墙8.1 防火墙概述8.1.1 防火墙的硬件平台8.1.2 防火墙的体系结构8.1.3 防火墙的部署方式8.2 Cisco IOS防火墙8.2.1 基于访问控制列表过滤8.2.2 基于上下文的访问控制8.2.3 基于网络的应用识别8.3 Cisco PIX/ASA防火墙8.3.1 PIX/ASA防火墙基小配置8.3.2 利用ASDM配置PIX/ASA防火墙8.3.3 FWASM及虚拟防火墙8.4 微软ISA防火墙8.4.1 安装ISA Setver 20048.4.2 配置ISA访问控制8.4.3 发布服务器8.4.4 缓冲Web数据8.5 Linux防火墙8.5.1 Linux防火墙简介8.5.2 配置Linux防火墙8.5.3 透明Linux防火墙8.5.4 管理Linux防火墙8.6 本章小结第9章 入侵检测及防御9.1 IPS/IDS工作原理9.1.1 IDS工作原理9.1.2 部署IDS9.1.3 IPS与IDS的区别9.1.4 IPS简介9.1.5 常见IPS产品9.2 配置Cisco IPS/IDS9.2.1 配置基于Cisco IOS IPS/IDS9.2.2 配置Cisco NM—CIDS9.3 Snort9.4 DDoS检测与防御9.4.1 DDoS攻击原理9.4.2 传统的DDoS防御方式9.4.3 新型DDoS保护策略9.5 本章小结第10章 远程访问10.1 VPN概述10.1.1 VPN简介10.1.2 VPN分类10.1.3 IPSec VPN和SSLVPN的比较10.2 配置IPSec VPN10.2.1 IPSec VPN概述10.2.2 配置IPSec VPN10.3 拨号虚拟专网10.3.1 VPDN概述10.3.2 配置基于ISA Server 2004的VPN10.3.3 使用ASA配置VPN10.3.4 配置Linux VPN10.4 配置SSLVPN10.5 本章小结第11章 统一安全管理11.1 统一安全管理11.1.1 网络监控系统发展历程11.1.2 配置CS.MARS11.2 事件控制系统11.3 本章小结第12章 文件安全12.1 Windows RMS部署12.1.1 RMS概述12.1.2 安装与配置RMS服务器12.1.3 安装与配置RMS客户端12.2 EFS加密12.3 本章小结第13章 园区网络安全设计13.1 小型企业网络安全设计13.2 中型企业网络安全设计13.3 大型企业网络安全设计13.4 校园网络安全设计13.5 运营商网络安全设计13.6 本章小结参考文献

## 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%，暴力猜测比例为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1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11 828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SQL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是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。

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。

## <<网络安全大全>>

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。

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。

#### 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>