

《网络安全原理与应用》

图书基本信息

书名：《网络安全原理与应用》

13位ISBN编号：9787517006077

10位ISBN编号：751700607X

出版时间：2013-2

出版社：水利水电出版社

页数：328

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

第二版前言 第一版前言 第1章 网络安全概述 学习目标 1.1 网络安全的基本概念 1.1.1 网络安全的定义及相关术语 1.1.2 主要的网络安全威胁 1.1.3 网络安全策略 1.1.4 网络安全模型 1.2 网络安全保障体系及相关立法 1.2.1 美国政府信息系统的安全防护体系 1.2.2 中国网络安全保障体系 1.3 网络安全现状 1.3.1 网络安全现状 1.3.2 研究网络安全的意义 习题1 第2章 网络体系结构及协议基础 学习目标 2.1 网络的体系结构 2.1.1 网络的层次结构 2.1.2 服务、接口和协议 2.2 OSI模型及其安全体系 2.2.1 OSI / RM 2.2.2 OSI模型的安全服务 2.2.3 OSI模型的安全机制 2.2.4 OSI安全服务与安全机制的关系 2.2.5 OSI各层中的安全服务配置 2.3 TCP / IP模型及其安全体系 2.3.1 TCP / IP参考模型 2.3.2 TCP / IP的安全体系 2.4 常用网络协议和服务 2.4.1 常用网络协议 2.4.2 常用网络服务 2.5 Windows常用的网络命令 2.5.1 ping命令 2.5.2 ipconfig命令 2.5.3 netstat命令 2.5.4 tracert命令 2.5.5 net命令 2.5.6 nbtstat命令 2.5.7 ftp命令 2.5.8 telnet命令 2.6 网络协议分析工具——Wireshark 2.6.1 Wireshark的安装 2.6.2 Wireshark主窗口 2.6.3 数据包捕获 习题2 第3章 密码学基础 学习目标 3.1 密码学概述 3.1.1 密码学的发展史 3.1.2 密码系统的概念 3.1.3 密码的分类 3.1.4 近代加密技术 3.1.5 密码的破译 3.2 古典密码学 3.2.1 代换密码 3.2.2 置换密码 3.3 对称密码学 3.3.1 分组密码概述 3.3.2 分组密码的基本设计思想——Feistel网络 3.3.3 DES算法 3.3.4 高级加密标准——AES 3.3.5 对称密码的工作模式 3.4 非对称密码算法 3.4.1.RSA算法 3.4.2.Diffie-Hellman算法 3.5 散列算法 3.5.1 单向散列函数 3.5.2 消息摘要算法MD5 3.5.3 安全散列算法SHA 习题3 第4章 密码学应用 学习目标 4.1 密钥管理 4.1.1 密钥产生及管理概述 4.1.2 对称密码体制的密钥管理 4.1.3 公开密钥体制的密钥管理 4.2 消息认证 4.2.1 数据完整性验证 4.2.2 数字签名 4.2.3 签名算法DSA 4.3 Kerberos认证交换协议 4.3.1 Kerberos模型的工作原理和步骤 4.3.2 Kerberos的优势与缺陷 4.4 公钥基础设施——PKI 4.4.1 PKI的定义、组成及功能 4.4.2 CA的功能 4.4.3 PKI的体系结构 4.4.4 PKI的相关问题 4.5 数字证书 4.5.1 数字证书的类型和格式 4.5.2 数字证书的管理 4.5.3 数字证书的验证 4.5.4 Windows 2000 Server的证书服务 习题4 第5章 防火墙技术 学习目标 5.1 防火墙概述 5.1.1 相关概念 5.1.2 防火墙的作用 5.1.3 防火墙的优、缺点 5.2 防火墙技术分类 5.2.1 包过滤技术 5.2.2 代理技术 5.2.3 防火墙技术的发展趋势 5.3 防火墙体系结构 5.3.1 双重宿主主机结构 5.3.2 屏蔽主机结构 5.3.3 屏蔽子网结构 5.3.4 防火墙的组合结构 5.4 内部防火墙 5.4.1 分布式防火墙 (Distributed Firewall) 5.4.2 嵌入式防火墙 (Embedded Firewall) 5.4.3 个人防火墙 5.5 防火墙产品介绍 5.5.1 FireWall-1 5.5.2 天网防火墙 5.5.3 WinRoute防火墙 习题5 第6章 网络攻击和防范 学习目标 6.1 网络攻击概述 6.1.1 关于黑客 6.1.2 黑客攻击的步骤 6.1.3 网络入侵的对象 6.1.4 主要的攻击方法 6.1.5 攻击的新趋势 6.2 口令攻击 6.2.1 获取口令的一些方法 6.2.2 设置安全的口令 6.2.3 一次性口令 6.3 扫描器 6.3.1 端口与服务 6.3.2 端口扫描 6.3.3 常用的扫描技术 6.3.4 一个简单的扫描程序分析 6.4 网络监听 6.4.1 网络监听的原理 6.4.2 网络监听工具及其作用 6.4.3 如何发现和防范Sniffer 6.5 IP欺骗 6.5.1 IP欺骗的工作原理 6.5.2 IP欺骗的防止 6.6 拒绝服务 6.6.1 什么是拒绝服务 6.6.2 分布式拒绝服务 6.6.3 DDoS的主要攻击方式及防范策略 6.7 缓冲区溢出 6.7.1 缓冲区溢出原理 6.7.2 对缓冲区溢出漏洞攻击的分析 6.7.3 缓冲区溢出的保护 6.8 特洛伊木马 6.8.1 特洛伊木马简介 6.8.2 木马的工作原理 6.8.3 木马的一般清除方法 习题6 第7章 入侵检测技术 学习目标 7.1 入侵检测概述 7.1.1 概念 7.1.2 IDS的任务和作用 7.1.3 入侵检测过程 7.2 入侵检测系统 7.2.1 入侵检测系统的分类 7.2.2 基于主机的入侵检测系统 7.2.3 基于网络的入侵检测系统 7.2.4 分布式入侵检测系统 7.3 入侵检测工具介绍 7.3.1 ISS BlackICE 7.3.2 ISS RealSecure 习题7 第8章 计算机病毒与反病毒技术 学习目标 8.1 计算机病毒 8.1.1 计算机病毒的历史 8.1.2 病毒的本质 8.1.3 病毒的发展阶段及其特征 8.1.4 病毒的分类 8.1.5 病毒的传播及危害 8.1.6 病毒的命名 8.2 几种典型病毒的分析 8.2.1 CIH病毒 8.2.2 宏病毒 8.2.3 蠕虫病毒 8.2.4 病毒的发展趋势 8.3 反病毒技术 8.3.1 反病毒技术的发展阶段 8.3.2 高级反病毒技术 8.4 病毒防范措施 8.4.1 防病毒措施 8.4.2 常用杀毒软件 8.4.3 在线杀毒 8.4.4 杀毒软件实例 习题8 第9章 WWW安全 学习目标 9.1 WWW安全概述 9.1.1 WWW服务 9.1.2 Web服务面临的安全威胁 9.2 WWW的安全问题 9.2.1 WWW服务器的安全漏洞 9.2.2 通用网关接口 (CGI) 的安全性 9.2.3 ASP与Access的安全性 9.2.4 Java与JavaScript的安全性 9.2.5 Cookies的安全性 9.3 Web服务器的安全配置 9.3.1 基本原则 9.3.2 Web服务器的安全配置方法 9.4 WWW客户的安全 9.4.1 防范恶意网页 9.4.2 隐私侵犯 9.5 SSL 技术 9.5.1 SSL 概述 9.5.2 SSL 体系结构 9.5.3 基于SSL 的Web安全访问配置 9.6 安全电子交易——SET 9.6.1 网上交易的安全需求 9.6.2 SET概述 9.6.3 SET的双重签名机制 习题9 第10章 电子邮件安全 学习目标 10.1 电子邮件系统的原理 10.1.1 电子邮件系统简介 10.1.2 邮件网关 10.1.3 SMTP与POP3协议 10.2 电子邮件系统的安全问题 10.2.1 匿名转发 10.2.2 电子邮件欺骗 10.2.3 E-mail炸弹 10.3 电子邮件安全协议 10.3.1 PGP 10.3.2 S / MIME

《网络安全原理与应用》

协议 10.3.3 MOSS协议 10.3.4 PEM协议 10.4 通过Outlook Express发送安全电子邮件 10.4.1 OutlookExpress 中的安全措施 10.4.2 拒绝垃圾邮件 10.5 PGP 10.5.1 PGP简介 10.5.2 PGP的密钥管理 10.5.3 PGP应用 习题10
第11章 无线网络安全 学习目标 11.1 无线网络及安全问题 11.1.1 无线网络概述 11.1.2 影响无线网络稳定性 的因素 11.1.3 无线网络的安全威胁 11.1.4 无线网络安全业务 11.2 无线局域网安全 11.2.1 IEEE 802.11协 议 11.2.2 无线局域网体系结构及服务 11.2.3 WEP协议 11.2.4 IEEE 802.11i安全服务 11.2.5 IEEE 802.11i RSN 的具体操作过程 11.3 移动通信安全 11.3.1 移动通信发展过程 11.3.2 移动通信面临的安全威胁 11.3.3 2G (GSM) 安全机制 11.3.4 3G系统的安全机制 11.3.5 WAP安全机制 11.4 无线传感器网络安全 11.4.1 无线 传感器网络简介 11.4.2 无线传感器网络面临的安全威胁 11.4.3 WSN常用的安全防御机制 习题11 参考文 献

版权页：插图：防火墙并不能确保内部用户之间的安全访问。内部网络中每一个用户的安全要求是不一样的，一些机密信息（如财务、人事档案等）就要求较高的安全等级，否则一旦遭到攻击就会造成巨大损失。这种攻击可能来自外网，也可能来自内网，据统计，80%的攻击来自内部。对于来自内部的攻击，边界防火墙是无能为力的。为了机密信息的安全，还需要对内网的部分主机再加以保护，使之免受内部用户的侵袭。可以将内部网络的一部分与其余部分隔离，在内部网络的两个部分之间再建立防火墙，称之为内部防火墙。建立内部防火墙，可以使用分布式防火墙、嵌入式防火墙等新的产品。

5.4.1 分布式防火墙（Distributed Firewall）

1. 分布式防火墙简介

分布式防火墙是一种全新的防火墙概念，是比较完善的一种防火墙技术，它是在边界防火墙的基础上开发的，目前主要以软件形式出现。分布式防火墙是一种主机驻留式的安全系统，用以保护内部网络免受非法入侵的破坏。分布式防火墙把Internet和内部网络均视为“不友好的”，对所有的信息流进行过滤与限制，无论是来自Internet，还是来自内部网络。它们对个人计算机进行保护的方式如同边界防火墙对整个网络进行保护一样。分布式防火墙克服了操作系统具有的安全漏洞，如DoS（拒绝服务），从而使操作系统得到强化。分布式防火墙对每个主机都能进行专门的保护。

2. 分布式防火墙的体系结构

分布式防火墙包含以下三个部分：

- （1）网络防火墙（Network Firewall）：这一部分有的公司采用的是纯软件方式，有的公司可以提供相应的硬件支持。它用于内部网与外部网之间，以及内部网络各子网之间。与边界防火墙相比，它多了一种用于内部子网之间的安全防护层，这样整个网络的安全防护体系就显得更加全面，更加可靠。其功能与传统的边界式防火墙类似。
- （2）主机防火墙（Host Firewall）：同样也有纯软件和硬件两种产品，用于对网络中的服务器和工作站进行防护。这是边界防火墙所不具有的功能，是对边界防火墙在安全体系方面的一个完善。它作用在同一内部子网之间的各工作站与服务器之间，以确保内部网络的安全。
- （3）中心管理（Central Management）：这是一种服务器软件，负责总体安全策略的策划、管理、分发及日志的汇总。这样防火墙就可以进行智能管理，提高了防火墙的安全防护灵活性，具备可管理性。

3. 分布式防火墙的主要特点

综合起来这种新的防火墙技术具有以下几个主要特点：

- （1）主机驻留。分布式防火墙最主要的特点就是采用主机驻留方式，所以称之为“主机防火墙”。它驻留在被保护的主机上，该主机以外的网络不管是处在网络内部还是网络外部都认为是不可信任的，因此可以针对该主机设定针对性很强的安全策略。主机防火墙使安全策略不仅停留在内网与外网之间，而是把安全策略延伸到网络中的每台主机。

《网络安全原理与应用》

编辑推荐

戚文静、刘学主编《21世纪高等院校规划教材:网络安全原理与应用(第2版)》的目的是帮助读者了解网络所面临的各种安全威胁，掌握网络安全的基本原理，掌握保障网络安全的主要技术和方法，学会在开放的网络环境中保护信息和数据。《21世纪高等院校规划教材:网络安全原理与应用(第2版)》注重理论与实践相结合，每章都配有应用实例，一方面有助于读者对理论知识的理解和掌握；另一方面，学以致用可以提高读者的学习兴趣、增加学习动力，也有助于提高读者的实践能力。

《网络安全原理与应用》

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:www.tushu000.com