

<<网络安全实用技术>>

图书基本信息

书名：<<网络安全实用技术>>

13位ISBN编号：9787115241153

10位ISBN编号：7115241155

出版时间：2010-12

出版单位：人民邮电出版社

作者：张仕斌,曾派兴,黄南铨 编著

页数：273

字数：438000

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>

<<网络安全实用技术>>

内容概要

本书以网络安全实用技术为基础，全面介绍了网络安全应用技能。

全书共分9章，重点介绍了网络安全基础知识、病毒及恶意软件清除与防御技术、计算机日常安全配置及防范技术、系统漏洞修复与扫描技术、企业服务器安全配置技术、系统灾难恢复技术、虚拟网络应用技术、文件加密和数字签名技术、PKI技术等内容。

本书具有科学严谨的体系结构，系统性强，内容全面，突出实用。

本书可作为普通高等院校计算机、通信、网络工程、信息安全等相关专业的教材，也可供计算机、通信、信息等领域研究人员和专业技术人员学习参考。

书籍目录

- 第1章 网络安全概述 11.1 网络安全简介 11.1.1 网络安全的定义 11.1.2 网络安全的主要特征
 21.2 网络安全案例与分析 21.2.1 网络犯罪案例 31.2.2 网络犯罪活动分析 71.3 网络系统的安全威胁与漏洞 91.3.1 网络系统的安全威胁 91.3.2 网络信息系统的漏洞及弱点 101.4 网络系统安全目标及构成要素 111.4.1 网络系统安全目标 111.4.2 网络系统安全的构成要素 111.5 网络信息系统安全保护等级 131.5.1 用户自主保护级 131.5.2 系统审计保护级 141.5.3 安全标记保护级 151.5.4 结构化保护级 161.4.5 访问验证保护级 18习题1 20第2章 病毒及恶意软件清除与防御技术 212.1 概述 212.2 宏病毒的清除与防御 212.2.1 几种典型的宏病毒 222.2.2 宏病毒的清除与预防 222.3 网络蠕虫病毒的清除与防御 242.3.1 网络蠕虫概述 242.3.2 维金病毒的查找与清除 262.3.3 熊猫烧香蠕虫病毒的查找与清除 282.3.4 地址解析协议病毒的清除与防御 302.4 木马的清除与防御 312.4.1 木马的手动清除与防御 312.4.2 木马的查找、清除与防御 322.4.3 灰鸽子的清除与防御 332.5 恶意软件的清除与防御 352.5.1 恶意软件简介 352.5.2 恶意软件的清除与防御 372.6 恶意代码的清除与防御 372.6.1 恶意代码简介 372.6.2 恶意代码的清除与防御 412.6.3 恶意网页代码的清除与防御 43习题2 61第3章 计算机日常安全配置及防范技术 623.1 本地安全策略的配置 623.2 IP安全策略及设置 633.2.1 IP安全隐患 633.2.2 默认的IP安全策略 643.2.3 IP安全规则的创建 653.3 个人防火墙的配置 653.3.1 Windows个人防火墙的配置 653.3.2 Windows防火墙的高级配置 663.3.3 基于组策略的Windows防火墙配置 673.3.4 基于防病毒软件的防火墙配置 703.4 IE安全防范及配置 713.4.1 Internet安全选项及隐私配置 713.4.2 IE的恶意修改与恢复 723.4.3 其他浏览器的安全设置 743.4.4 浏览器的安全检测 753.5 网络浏览安全防范 783.5.1 网页炸弹的攻击与防御 783.5.2 “网络钓鱼”及防范 793.6 网络应用的安全防范及配置 823.6.1 电子邮件的安全防范 823.6.2 网络聊天的安全防范 883.6.3 桌面应用程序的安全配置 94习题3 94第4章 系统漏洞修复与扫描技术 964.1 系统漏洞概述 964.2 系统漏洞及防范 984.2.1 IPC\$默认共享漏洞 984.2.2 Unicode漏洞 994.2.3 IDQ溢出漏洞 1004.2.4 WebDAV溢出漏洞 1014.2.5 SQL空密码漏洞 1024.3 系统漏洞检测与补丁更新技术 1034.3.1 系统漏洞检测技术 1034.3.2 及时更新系统补丁 1044.3.3 扫描并修复系统漏洞工具软件简介 1054.4 基于MBSA的系统漏洞扫描与修复技术 1074.4.1 MBSA简介 1074.4.2 MBSA在系统漏洞扫描与修复中的应用 109习题4 110第5章 企业服务器安全配置技术 1115.1 企业服务器安全概述 1115.2 基于Windows系统的服务器安全配置 1125.2.1 系统安全加固 1125.2.2 基于Windows系统的Web服务器安全配置 1135.2.3 基于Windows系统的FTP服务器安全配置 1165.3 基于UNIX/Linux系统的服务器安全配置 1175.3.1 基于UNIX/Linux系统的Web服务器安全配置 1175.3.2 基于UNIX/Linux系统的FTP服务器安全配置 122习题5 125第6章 系统灾难恢复技术 1396.1 系统灾难恢复概述 1396.2 Active Directory数据库备份与恢复技术 1406.2.1 备份Active Directory数据库 1406.2.2 还原Active Directory数据库 1426.3 SQL Server 2000数据库备份与恢复技术 1446.3.1 数据库维护计划创建备份 1456.3.2 数据库的恢复 1486.4 操作系统灾难恢复技术 1506.4.1 Acronis True Image Server 1506.4.2 Veritas灾难恢复系统 156习题6 159第7章 虚拟网络应用技术 1607.1 虚拟专用网络技术 1607.1.1 VPN技术简介 1607.1.2 VPN的关键安全技术 1627.1.3 VPN的配置示例 1647.2 虚拟局域网技术 1717.2.1 VLAN技术简介 1717.2.2 VLAN配置示例 1737.3 专用虚拟局域网技术 1807.3.1 PVLAN技术简介 1807.3.2 PVLAN的配置 182习题7 185第8章 文件加密和数字签名技术 1878.1 文件加密与数字签名概述 1878.2 EFS文件加密技术 1888.2.1 EFS概述 1888.2.2 EFS加密技术的应用 1888.3 加密数据的恢复 1898.3.1 数据恢复的基本思路 1898.3.2 配置加密文件系统故障恢复代理模板 1908.3.3 申请加密文件系统故障恢复代理证书 1928.3.4 添加域的故障恢复代理 1938.3.5 创建默认的独立计算机上的数据恢复代理 1968.4 密钥的存档与恢复 1968.4.1 密钥存档与恢复概述 1978.4.2 创建密钥恢复代理账户 1978.4.3 获取密钥恢复代理证书 1988.4.4 配置密钥存档与恢复属性 1998.4.5 创建新的可以进行密钥存档的证书模板 2008.4.6 获取具有存档密钥的用户证书 2018.4.7 执行密钥恢复示例 2038.4.8 导入已恢复的私钥 2058.5 PGP动态文件加密和数字签名 2068.5.1 PGP密钥的生成

2078.5.2 PGP密钥的发布 2098.5.3 用PGP加密文件 2108.5.4 用PGP进行邮件数字签名 2128.6
电子签章 2168.6.1 iSignature签章系统简介 2168.6.2 iSignature的主要功能 2178.6.3 个人数字
证书申请 2178.6.4 iSignature签章系统的使用 2198.6.5 天威诚信安证通简介 221习题8 223第9章
PKI技术 2299.1 PKI概述 2299.2 证书基? 2309.2.1 证书服务概述 2309.2.2 证书服务的安装
2319.3 证书的申请 2339.3.1 概述 2339.3.2 使用证书申请向导申请证书 2359.3.3 使
用Windows Server 2003证书服务网页申请证书 2399.4 证书的自动注册 2429.4.1 规划自动注册部署
2439.4.2 “用户”模板复制 2459.4.3 配置企业证书颁发机构 2469.4.4 建立自动注册域用户的
策略 2479.5 证书的导入/导出 2489.5.1 证书的导入/导出概述 2489.5.2 导入证书 2499.5.3 导
出证书 2499.5.4 导出带私钥的证书 2519.6 吊销证书和发布证书吊销列表 2529.6.1 吊销证书
2529.6.2 安排证书吊销列表的发布 2549.6.3 手动发布证书吊销列表 2559.7 PKI在文件传输加
密与数字签名方面的应用 2569.7.1 配置密钥用法 2569.7.2 文件传输加密 2579.7.3 数字签名
2599.7.4 加密密钥对的获取 2609.7.5 邮件中的文件加密和数字签名 262习题9 263参考文献
272

章节摘录

版权页：插图：2.3.4地址解析协议病毒的清除与防御当出现以下情况时，可能就是受到地址解析协议（ARP）攻击。

（1）网上银行、游戏及QQ账号频繁丢失。

一些人为了获取非法利益，利用ARP欺骗程序在网内进行非法活动，此类程序的主要目的在于破解账号登录时的加密解密算法，通过截取局域网中的数据包，以分析数据通信协议的方法截获用户的信息。

运行这类病毒，就可以获得整个局域网中上网用户账号的详细信息并盗取。

（2）网速时快时慢，极其不稳定，但单机进行光纤数据测试时一切正常。

当局域内的某台计算机被ARP的欺骗程序非法侵入后，它就会持续地向网内所有的计算机及网络设备发送大量的非法ARP欺骗数据包，阻塞网络通道，造成网络设备的承载过重，导致网络的通信质量不稳定。

（3）局域网内频繁性区域或整体掉线，重启计算机或网络设备后恢复正常。

当带有ARP欺骗程序的计算机在网内进行通信时，就会导致频繁掉线，出现此类问题后重启计算机或禁用网卡会暂时解决问题，但掉线情况还会发生。

出现这几种情况的主要原因是在局域网中有人使用了ARP欺骗木马程序，如一些盗号的软件。

例如，传奇外挂携带的ARP木马攻击，当局域网内使用外挂时，外挂携带的病毒会将该机器的MAC地址映射到网关的IP地址上，向局域网内大量发送ARP包，使同一网段地址内的其他机器误将其作为网关，掉线时内网是互通的，计算机却不能上网。

<<网络安全实用技术>>

编辑推荐

《网络安全实用技术》：结构严谨，系统性强，突出实用全面阐述最新网络安全实用技术满足高校培养应用型人才的需要

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>