

<<电脑报2013增刊>>

图书基本信息

书名：<<电脑报2013增刊>>

13位ISBN编号：9787894767189

10位ISBN编号：7894767182

出版时间：2012-9

出版时间：电脑报 电脑报电子音像出版社 (2012-09出版)

作者：电脑报

页数：304

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>

<<电脑报2013增刊>>

内容概要

《电脑报2013增刊：黑客攻防与电脑安全年度应用方案》关注最新黑客攻防技术，荟萃16大精彩专题，包含150套黑客攻防方案，累计1000余条操作技巧。

具体内容包括：密码安全、网络盗号、移动存储安全、图片病毒、IP地址追踪和隐藏、局域网嗅探与网吧攻防、网站挂马与钓鱼、无线网络破解实例、拒绝服务和网络炸弹攻防，以及系统账户与口令攻防、论坛与数据库攻防、服务器入侵与防范、入侵检测与日志管理等，让大家洞悉黑客攻防招式，轻松捍卫网络安全！

书籍目录

菜鸟黑客篇 密码安全你该如何hold住 强大否？

密码安全鉴定 一、中外弱密码PK 二、密码安全鉴定 三、创建强悍密码 密码管理工具 “喜”与“忧” 一、不用记？

KeePass密码管理工具 1.添加密码 2.密码管理 3.生成安全密码 二、福兮，祸兮？

密码软件的隐患 1.软件安装 2.密码一览无遗 3.消除隐患 另辟蹊径确保文件安全 一、“汉字+图片”组合密码 1.汉字也能做密码 2.SilentEye图片加密 3.文件解密 二、任意文件均可做密钥 三、巧借网站实现自动销毁 四、X—文件锁保护机密文件 五、FileMon监视发现“销毁真相” 六、破解“X—文件锁”加密的文件 常用密码防破解 一、密码轻松看 网易闪电邮之安全隐患 1.网易闪电邮的安全隐患 2.安装目录下轻松“获取”密码 3.防范之道 二、揭秘破解无线路由器密码 1.暴力破解无线路由器账号、密码 2.修改无线网络密码，免费蹭网 三、压缩文档加密与突破 1.用RARPasswordCracker恢复密码 2.WINZIP压缩文件的破解 3.WinRAR压缩文件的破解 新隐患 智能手机与微博安全 手机的安全隐患 一、手机安全七大问题 二、手机骷髅木马 善用工具保手机安全 一、常用手机安全软件 1.卡巴斯基手机安全软件 2.网秦手机安全卫士 二、拦截垃圾短信 1.来电通 2.当心“短信群发器”木马 三、监控失踪的手机流量 1.LBE安全大师 2.扣贾病毒伪装热门游戏 四、Android病毒不得不防 1.一键体检 2.病毒查杀 五、手机隐私保护 微博安全防范 一、中奖“钓鱼”陷阱 二、微博短链接挂马 三、短链接DDOS攻击 四、“微博卫士”保微博安全 1.金山微博卫士 2.360微博卫士 实战解析移动存储与图片病毒防范 Autorun病毒实战分析 一、初识U盘病毒 1.什么是U盘病毒 2.使用专杀工具剿杀U盘病毒 二、Autorun病毒解析 1.原理与分析 2.病毒查找 3.病毒清除 4.故障修复 U盘病毒防范之策 一、手工方式防U盘病毒 二、“防护盒”为U盘护航 三、内网当心U盘资料被窃取 1.当心黑手“闪盘窥探者” 2.防范“闪盘窥探者” USB访问权限设置 一、禁止安装USB设备的驱动程序 二、禁用USB存储设备 图片病毒的制作原理 一、什么是图片病毒 二、图片病毒的传播方式和原理 1.修改文件扩展名 2.寄生在压缩包中 3.利用漏洞传播 4.伪装成BMP图片 5.病毒程序使用图片文件图标 图片病毒实战解析 一、超强免杀图片病毒揭秘 二、图片网马实战解析 图片病毒防范方法 一、安装补丁 1.使用“自动更新” 2.使用第三程序修补漏洞 3.微软网站下载单个补丁 二、使用图片病毒专杀工具 寻找李鬼自己动手揪出“黑线”进程 进程攻防基础知识 一、进，线程是干什么的 二、怎样分析、关闭和重建进程 1.Windows任务管理器 2.DOS下管理进程 进程攻防实例解析 一、如何杀死黑客植入的隐藏进程 二、黑客如何查看远程进程 三、如何杀死病毒进程 四、怎样删除发起进程的恶意程序 五、如何查看木马进程对应的服务 六、进程的高级管理 进程攻防辅助工具 一、超级巡警为系统进程护航 1.全面查杀 2.实时防护 3.保险箱 4.系统安全增强工具 5.妙用SSDT工具清除流氓软件 二、XueTr：超强进程工具 1.从进程中发现可疑文件 2.查看网络端口与IE插件 3.强大的文件管理功能 4.服务与启动项管理 三、进程、服务藏污垢察言观色巧识别 1.不同颜色显示进程安全级别 2.进程比较找出可疑文件 3.系统服务也能对比分析 攻防实例篇 安全防范篇

章节摘录

版权页：插图：一、认识VPN虚拟网 VPN之所以称为虚拟网，主要是因为整个VPN网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台（如Internet，ATM，Frame Relay等）之上的逻辑网络，用户数据在逻辑链路中传输。

由于通过公用IP网络来建立VPN，不再需要铺设专门的线路进行通信，这样就可以节省大量通信费用，可称得上物美价廉。

现在教育系统大力推行的城域网，实际上就是为了实现内部网络的安全性访问而组建的。

对于无法投入巨大资金铺设线路的一般性企业来说，大多都是采用租用电信运营商的线路，如光纤、SDH和DDN等实现专用网络。

这样做虽然已经节省了很多费用，但仍然没有自行使用VPN技术好，因为VPN的安全性、可靠性和可管理性更好。

概括起来，VPN就是通过公用网络在两台计算机或两个网络之间建立的专用连接。

换而言之，VPN就是把因特网变成了模拟的专用WAN。

根据VPN所起的作用，可以将VPN分为3类，且FIVPDN、Intranet VPN和Extranet VPN。

其中，Intranet VPN技术最为常用——在本书中讲解的也是这种技术。

Intranet VPN主要指的是在分支机构的LAN和总部LAN之间的VPN。

通过Internet这一公共网络将各地分支机构的LAN连到总部的LAN，以便内部的资源共享、文件传递等，可节省DDN等专线所带来的高额费用。

很明显，VPN技术不仅仅可以在学校网络中使用，因为越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司和研究所等，各个公司之间传统的网络连接方式一般是租用专线。

利用VPN特性可以在Internet上组建世界范围内的Intranet VPN。

利用Internet的线路可以保证网络的互联性，而利用隧道、加密技术等VPN特性可以保证信息进行安全传输。

VPN代理，是在VPN（Virtual Private Network）虚拟专用网络的基础上衍生出来的提高网络访问速度和安全的技術，它利用VPN的特殊加密通讯协议，在互联网两个不同地方节点之间临时建立一条安全、稳定的专用隧道，如图所示。

当用户计算机与VPN代理服务器之间通过登录凭据完成点对点连接后，就可以建立一个虚拟专用隧道，用户计算机原本要发送给目标服务器的请求，会自动通过隧道发送给VPN代理服务器，然后再由VPN代理服务器将请求转发给目标服务器。

VPN代理服务器在将通讯请求发送给目标服务器的过程中，会对请求数据包进行加密压缩处理。

VPN代理服务器接收到目标服务器的响应后，也原样转发给前端计算机。

我们使用可以多种方法实现VPN代理服务器的使用，即通过Windows内置的拨号组件和VPN拨号工具

。下面，分别予以介绍。

编辑推荐

《电脑报2013增刊:黑客攻防与电脑安全年度应用方案》每一个专题都是经过电脑报编辑精心提炼的热点应用方案：每一个方案都可以从头到尾帮你完成一项完整的应用任务；每一条秘技都会让你有茅塞顿开的感觉。

专题方案详尽、实用性强、汇集各种电脑热门应用，适合初、中级电脑用户以及广大的电脑爱好者阅读与收藏。

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>