

<<计算机安全基础>>

图书基本信息

书名：<<计算机安全基础>>

13位ISBN编号：9787302176275

10位ISBN编号：7302176272

出版时间：2008-10

出版时间：伊斯特姆 (Chuck Easttom)、贺民 清华大学出版社 (2008-10出版)

作者：伊斯特姆

页数：261

译者：贺民

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>

<<计算机安全基础>>

前言

本书是一本入门书籍，从总体上介绍了信息安全领域的各个方面，描述了黑客如何定位系统、获取信息并用之攻击系统。

通过对本书的学习，读者可以了解如何利用密码工具以及网络扫描工具防护自身系统；同时，本书还介绍了安全侵入的细节，但要注意，本书不是一本入侵手册，不是写给黑客的。

本书通过解释说明、定义和各种例子，来深入讲解数据、计算机以及网络防护的重要性，而且还介绍了各种防护重要信息的安全措施所采取的操作步骤。

最后，本书主要以Windows系统环境为例来介绍安全知识，但其中的原理和概念是普遍适用的。

之所以选择Windows，是因为其应用范围广泛，受攻击的几率也比较大。

读者对象本书主要面向希望扎实了解计算机安全概念的读者。

本书虽然是一本基础丛书，但要求读者是熟练的计算机用户，能够使用计算机工作或学习，并熟练使用电子邮件和Web浏览器，了解基本的术语如RAM和USB等。

读者应该具备基本的计算机知识，但不需要系统学习计算机课程。

计算机科学、计算机信息系统专业之外的读者也会发现本书十分有用，特别是相关法律工作者和电子商务人员。

本书主要内容本书概要地介绍了网络犯罪和计算机安全。

第1章详细介绍了网络犯罪和计算机安全，并详细阐述了网络犯罪的严重性以及学习系统防护的必要性。

第1章还介绍了基本的计算机安全知识，包括威胁分类、常见攻击类型、一些术语和范例等，以及在法律许可范围内的安全框架。

在第1章最后描述了一些安全资源，并在后面的练习中实践了一些工具的用法。

第2章介绍的内容是网络安全最重要的几个方面之一：网络操作的实际工作经验。

计算机经验比较丰富的读者可以快速浏览本章，系统地复习一下这些知识。

初学者通过对本章的学习将能够了解到基本的网络模型及其工作机制，在后面的练习中可以动手使用IPconfig、tracert、ping等工具，以便加强对网络的理解，并学会如何防护网络安全。

计算机安全基础前言第3章介绍了一些评估系统脆弱性的工具（黑客经常使用这些工具），并讲述了网络安全管理者如何利用这些工具评估系统的安全性，以免受到攻击；还提供了一些实践内容以使读者了解最常用的端口扫描工具的用法，并在实践中加深学习。

第4~5章主要介绍各种黑客攻击类型。

第4章讲述拒绝服务，重点介绍了SYN泛洪、Smurf攻击和分布式拒绝服务攻击；同时还通过一些真实的拒绝服务攻击案例来说明此类攻击所造成后果的严重性，以及如何应对。

第5章介绍了恶意软件、病毒、特洛伊木马、缓冲区溢出攻击、间谍软件等，也通过一些真实例子来揭示这些威胁所在，并说明如何利用检测和清除工具，如Norton、McAfee来进行防护。

学完本书前面的内容，读者已经了解了各种系统面临的威胁以及防护、检测、清除这些威胁的措施。

第6章主要介绍系统评估与防护基础，第7章讲解加密，这两章的内容跳出各种攻击，从更为宽广的视角来审视计算机安全管理。

在第6章，读者将会了解到各种安全防护基础知识：脆弱性探测、设置策略、咨询顾问、防护个人工作站以及服务器、安全浏览网站。

第7章介绍了加密，包括加密的历史和现代密码学方法。

这两章拓展了读者在安全管理领域的视角，至少能够使读者有能力提出正确的问题，为深入学习打下基础。

第8~10章介绍了Internet上的各种犯罪形式。

第8章介绍了Internet欺骗和网络犯罪，讨论了身份盗用、网络侵犯。

第9章介绍了网络工业间谍，第10章介绍了网络恐怖袭击和信息战。

第11章讲解网络侦查，继续前3章的内容，描述了黑客如何利用Internet信息实施犯罪，并解释各种网络犯罪的原理，以便读者掌握如何应对各种犯罪并进行防护。

<<计算机安全基础>>

每一章都有一些真实的案例用以说明各种犯罪方法，以加强读者对网络安全重要性的认识。

第12章的内容涉及计算机安全软硬件，深入到计算机安全的技术层面，介绍了各种与安全相关的软硬件，其中一些在前面的章节里已提到过。

本章的目的就是使读者更为深入地理解病毒扫描器、防火墙、入侵检测系统和反间谍软件。

本章的内容对于即将从事计算机安全工作的读者来说是非常有用的。

附录中是一些附加内容，提供了各种有用的网站链接资源、安全清单模板、术语表和参考资料。

<<计算机安全基础>>

内容概要

《计算机安全基础》是一本入门书籍，从总体上介绍了信息安全领域的各个方面，描述了黑客如何定位系统、获取信息并用之攻击系统。

《计算机安全基础》介绍了如何利用密码工具以及网络扫描工具防护自身系统，以及安全侵入的细节。

《计算机安全基础》通过解释说明、定义和各种例子，来深入理解数据、计算机以及网络防护的重要性，而且还介绍了各种防护重要信息的安全措施所采取的操作步骤。

《计算机安全基础》不仅可以作为计算机科学、计算机信息系统专业学生关于计算机安全课程的教材，对其他专业人员，特别是相关法律工作者和电子商务人员也是一本很好的参考用书。

<<计算机安全基础>>

作者简介

作者：(美国)伊斯特姆 (Chuck Easttom) 译者：贺民Chuck Easttom，在IT行业具有多年的实践经验，随后有3年时间，在一家技术学院教授计算机科学，包括计算机安全课程。

后来，他又离开学术界，转向IT,在美国得克萨斯州的达拉斯的一家公司担任IT经理。

除了日常事务之外,他还负责计算机安全。

他编写过7本有关程序设计、Web开发和Linux的图书。

Chuck荣获20多个不同的证书，包括CIW安全分析师（Security Analyst）、MCSE、MCSA、MCDBA、MCAD、Server+和其他证书。

在ComTIA（Computer Technology Industry Association，计算机技术协会），他作为相关科目的专家，曾制定和修74种认证考试，包括Security+认证的初始创建。

业余时间，Chuck还在达拉斯地区学院任兼职教师，教授各种课程,包括计算机安全。

他时常还从事计算机安全的咨询工作。

Chuck经常作为计算机团体的客座演讲人，主要讨论安全问题。

<<计算机安全基础>>

书籍目录

第1章 网络犯罪和网络安全概述1.1 简介1.2 网络安全隐患的严重性1.3 威胁分类1.3.1 恶意软件1.3.2 侵入系统安全防线1.3.3 拒绝服务式攻击1.4 常见的网络攻击1.5 基本的安全术语1.5.1 人1.5.2 安全设备1.5.3 行为1.6 网络安全模型1.6.1 边界安全1.6.2 分层安全1.6.3 主动性和响应速度1.6.4 混合安全方法1.7 网络安全相关法律1.8 计算机安全相关在线资源1.8.1 CERT1.8.2 微软安全建议1.8.3 F-Secure1.8.4 SANS学院1.9 本章小结1.10 课后练习1.10.1 多项选择题1.10.2 练习题1.10.3 项目题1.10.4 案例研究第2章 网络和Internet2.1 简介2.2 OSI模型2.3 网络基础2.3.1 介质访问控制 (MAC) 地址2.3.2 DNS服务器2.3.3 物理连接: 本地网络2.3.4 物理连接: Internet2.3.5 数据传输2.4 Internet的工作方式2.4.1 IP地址2.4.2 统一资源定位符2.5 基本的网络实用工具2.5.1 ipconfig2.5.2 ping2.5.3 tracert2.6 其他网络设备2.7 本章小结2.8 课后练习2.8.1 多项选择题2.8.2 练习题2.8.3 项目题2.8.4 案例研究40第3章 系统评估3.1 简介3.2 基本的排查3.2.1 Netcraft3.2.2 跟踪IP地址3.2.3 利用IP地址注册信息3.2.4 社会工程3.3 扫描3.3.1 端口扫描3.3.2 脆弱性扫描3.4 端口监控和管理3.4.1 NetStat Live3.4.2 Active Ports3.4.3 Fport3.4.4 TCPView3.5 深入研究3.6 本章小结3.7 课后练习3.7.1 多项选择题3.7.2 练习题3.7.3 项目题3.7.4 案例研究67第4章 拒绝服务攻击4.1 简介4.2 概述4.2.1 常用于DOS攻击的工具4.2.2 DoS的弱点4.3 DoS攻击4.3.1 TCP SYN泛洪攻击4.3.2 Smurf IP攻击4.3.3 UDP泛洪攻击4.3.4 ICMP泛洪攻击4.3.5 死亡之ping4.3.6 泪珠攻击4.3.7 着陆攻击4.3.8 Echo/Chargen攻击4.4 分布式拒绝服务攻击4.5 真实的例子4.5.1 MyDoom4.5.2 Slammer4.6 防御DoS攻击的方式4.7 本章小结4.8 课后练习4.8.1 多项选择题4.8.2 练习题4.8.3 项目题4.8.4 案例研究83第5章 恶意软件5.1 简介5.2 病毒5.2.1 病毒是如何传播的5.2.2 最新的病毒例子5.2.3 防御病毒的原则5.3 特洛伊木马5.4 缓冲区溢出攻击5.5 Sasser病毒/缓冲区溢出5.6 间谍软件5.6.1 正当利用间谍软件5.6.2 间谍软件“种”到目标系统的方式5.6.3 获取间谍软件5.7 其他形式的恶意软件5.7.1 Rootkit5.7.2 基于网页的恶意代码5.8 检测并清除病毒5.8.1 防病毒软件5.8.2 反间谍软件5.9 本章小结5.10 课后练习5.10.1 多项选择题5.10.2 练习题5.10.3 项目题5.10.4 案例研究102第6章 系统评估与防护基础6.1 简介6.2 系统评估基础6.2.1 补丁6.2.2 端口6.2.3 保护6.2.4 策略6.2.5 探测6.2.6 物理安全6.3 防护计算机系统6.3.1 防护个人工作站6.3.2 防护服务器6.3.3 防护网络6.4 安全网上冲浪6.5 向专家寻求帮助6.6 本章小结6.7 课后练习6.7.1 多项选择题6.7.2 练习题6.7.3 项目题6.7.4 案例研究125第7章 加密7.1 简介7.2 密码学基础7.3 加密的历史7.3.1 凯撒密码7.3.2 多字符替换7.3.3 二进制操作7.4 现代加密算法7.4.1 单密钥加密7.4.2 公钥加密算法7.4.3 正规的和假冒的加密算法7.5 虚拟专用网络7.5.1 PPTP7.5.2 L2TP7.5.3 IPsec7.6 本章小结7.7 课后练习7.7.1 多项选择题7.7.2 练习题7.7.3 项目题7.7.4 案例研究144第8章 Internet欺骗与网络犯罪8.1 简介8.2 网络欺骗8.2.1 投资邀请骗术8.2.2 投资建议骗术8.2.3 拍卖欺骗8.2.4 身份盗用8.3 网络侵犯8.4 有关网络犯罪的法律8.5 防御网络犯罪8.5.1 防止投资欺骗8.5.2 防止拍卖欺骗8.5.3 防止身份盗用8.5.4 防止网络侵犯8.6 本章小结8.7 课后练习8.7.1 多项选择题8.7.2 练习题8.7.3 项目题8.7.4 案例研究166第9章 网络世界的工业间谍9.1 简介9.2 什么是工业间谍9.3 把信息当作资产9.4 如何从事间谍活动9.4.1 低级工业间谍9.4.2 利用间谍软件9.5 防止工业间谍9.6 真实世界的工业间谍案例9.6.1 例1: VIA Technology公司9.6.2 例2: 通用汽车公司9.6.3 例3: 互动电视科技公司9.6.4 例4: Bloomberg公司9.6.5 例5: Avant软件公司9.6.6 身边的工业间谍9.7 本章小结9.8 课后练习9.8.1 多项选择题9.8.2 练习题9.8.3 项目题9.8.4 案例研究181第10章 网络恐怖主义和信息战10.1 简介10.2 经济攻击10.3 军事攻击10.4 通常的攻击10.5 信息战10.5.1 宣传10.5.2 信息控制10.5.3 假情报10.6 真实案例10.7 未来趋势10.7.1 积极的方面10.7.2 消极的方面10.8 防御网络恐怖主义10.9 本章小结10.10 课后练习10.10.1 多项选择题10.10.2 练习题10.10.3 项目题10.10.4 案例研究198第11章 网络侦查11.1 简介11.2 通常的搜索11.3 庭审记录和犯罪记录检查11.3.1 性侵犯记录11.3.2 国内庭审记录11.3.3 其他资源11.4 Usenet11.5 本章小结11.6 课后练习11.6.1 多项选择题11.6.2 练习题11.6.3 项目题11.6.4 案例研究211第12章 计算机软硬件安全12.1 简介12.2 病毒扫描器12.2.1 病毒扫描器的工作方式12.2.2 病毒扫描技术12.2.3 商业反病毒软件12.3 防火墙12.3.1 防火墙类型和组件12.3.2 防火墙检查数据包的方式12.3.3 防火墙配置12.3.4 商业防火墙和免费防火墙12.3.5 防火墙日志12.4 反间谍软件12.5 入侵检测软件12.5.1 IDS的分类12.5.2 IDS的工作方式12.5.3 商业IDS12.6 本章小结12.7 课后练习12.7.1 多项选择题12.7.2 练习题12.7.3 项目题12.7.4 案例研究附录A 计算机安全专家: 教育和认证考试A.1 学校教育和课程A.2 业界认证考试A.2.1 Security+A.2.2 CIW 安全分析师A.2.3 MCSE安全专家A.2.4 CISSPA.2.5 SANS学院认证A.2.6 高科技犯罪网络认证附录B 资源B.1 计算机

<<计算机安全基础>>

犯罪与网络恐怖主义B.2 黑客行为B.3 网络侵犯B.4 身份盗用B.5 端口扫描和嗅探B.6 密码破译B.7 防护措施B.8 间谍软件B.9 反间谍软件B.10 网络调查工具B.11 一般工具B.12 病毒研究附录C 安全策略文档及清单C.1 家庭PC安全基础C.1.1 总体注意事项C.1.2 对Windows用户的特别提示C.2 PC基本安全保障清单C.2.1 基本安全措施C.2.2 强化安全措施C.3 基础网络安全保障清单C.3.1 基本安全要求C.3.2 强化安全措施C.4 网上欺骗防范清单C.4.1 投资邀请C.4.2 在线拍卖C.5 可用策略样本C.5.1 概述C.5.2 策略C.5.3 策略的执行C.6 密码策略C.6.1 概述C.6.2 目的C.6.3 适用对象C.6.4 策略内容C.7 雇用安全工程师C.7.1 经验C.7.2 教育/培训C.7.3 认证证书C.7.4 背景C.7.5 文档C.7.6 知名认证链接参考资料249术语表

<<计算机安全基础>>

章节摘录

插图：第1章 网络犯罪和网络安全概述本章目标在学习了本章内容并完成所有练习之后，读者将能够掌握如下内容。

了解最厉害的计算机网络攻击：入侵、拒绝服务和恶意软件。

学习如何对个人电脑和网络的脆弱性进行评估。

了解一些关键术语，如破译者、潜伏者、防火墙和认证等。

比较并对边界网络安全架构和分层网络安全架构的不同。

利用在线资源保护网络。

1.1 简介从某种程度上来说，现代生活的方方面面都要涉及计算机系统。

以下几个例子可以说明这一点。

金融交易——包括在线银行、ATM柜员机、信用卡，这些在现代商业中十分流行。

一些零售商用计算机自动结账。

你可能在网上进行了注册，或者在线上某一门课，也可以在网上买书。

目前大家广泛讨论的网络在线选举。

由于在商业上有这么多在线交易，所以，大量的个人信息被存储在计算机上，如医疗记录、纳税记录、教育记录等，所有这些都存储在计算机数据库中。

对日常生活而言，某些科技进步是否有利超出了本书讨论的范围。

事实上，人们的生活已经与计算机系统密不可分，这也导致了以下一些严重的问题。

怎样保障信息安全？

这些计算机系统都有哪些脆弱点？

要采取哪些措施来保障计算机系统以及数据的安全？

提示：网上银行最近的一项研究表明，28%的美国消费者每周至少3次通过电话、Internet或者分支机构办理银行业务（OnlineBankingReport，网上银行报道）。

这些消费者通过网上银行查看账单、在线支付、检查收支和在线转账。

<<计算机安全基础>>

编辑推荐

《计算机安全基础》主要以Windows系统环境为例来介绍安全知识，但其中的原理和概念是普遍适用的。之所以选择Windows，是因为其应用范围广泛，受攻击的几率也比较大。

<<计算机安全基础>>

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>