

<<黑客防范手册>>

图书基本信息

书名：<<黑客防范手册>>

13位ISBN编号：9787111175087

10位ISBN编号：7111175085

出版时间：2006-1

出版时间：机械工业出版社

作者：杨

页数：488

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>

## <<黑客防范手册>>

### 内容概要

虽然市面上已有不少介绍系统和网络安全的书籍，但本书从不同的视角来阐述安全问题，使本书在安全图书领域独具特色。

本书使用分析的观点来看待黑客行为和安全，将攻击和防御类比为国际象棋游戏中的对弈，攻与守之间存在着对立统一性。

本书适合有一定安全经验的系统管理员、网络管理员和安全管理员阅读，通过揭示黑客行为的技术内幕，让管理员们做到知己知彼，准确地将黑客行为“映射”到未来的防御系统中。

## <<黑客防范手册>>

### 作者简介

作者：(美)杨Susan Young过去七年一直在安全领域工作，其中四年致力于安全咨询工作，帮助客户设计和实现安全的网络，进行安全技术培训，并对客户的系统进行安全评估和穿透性测试，或者进行网络防御。

她目前是国际网络服务公司(INS)波士顿区安全培训部的高级安全咨询师。

## &lt;&lt;黑客防范手册&gt;&gt;

## 书籍目录

译者序致谢第1章 导论：国际象棋游戏第一部分 基础材料第2章 案例研究2.1 Dalmedica2.2 困境2.3 调查第3章 了解对手3.1 术语3.1.1 脚本小子3.1.2 骇客3.1.3 白帽子黑客3.1.4 黑帽子黑客3.1.5 黑客激进主义3.1.6 专业攻击者3.2 历史3.2.1 计算机产业和大学3.2.2 系统管理3.2.3 家用计算机3.2.4 家用计算机：商业软件3.2.5 家用计算机：BBS3.2.6 电话系统3.3 道德规范和完全公开3.4 内部对手3.4.1 内部攻击者3.4.2 企业策略小结第4章 攻击剖析4.1 概览4.2 探测4.3 社会工程和场所探测4.4 因特网探测4.4.1 因特网搜索引擎和Usenet工具4.4.2 财务搜索工具、目录、黄页和其他资源4.5 IP和网络探测4.5.1 域名注册商和whois搜索4.5.2 网络域名注册商搜索(ARIN)4.6 DNS探测4.7 映射目标4.8 网络映射(ICMP)4.8.1 ICMP查询4.8.2 TCP ping：ICMP的替代4.8.3 traceroute4.8.4 其他网络映射工具4.9 端口扫描4.9.1 TCP和UDP扫描4.9.2 标志获取4.9.3 包分片选项4.9.4 欺骗扫描能力4.9.5 标识扫描4.9.6 FTP反弹扫描4.9.7 源端口扫描4.9.8 栈指纹识别技术4.10 漏洞扫描(网络操作系统及应用问询)4.11 漏洞的研究和探测4.12 系统/网络穿透4.12.1 账号(口令)破解4.12.2 应用程序攻击4.12.3 缓存利用4.12.4 文件系统攻击4.12.5 恶意和自我复制代码4.12.6 编程策略4.12.7 进程操纵4.12.8 shell攻击4.12.9 会话劫持4.12.10 哄骗4.12.11 基于状态的攻击4.12.12 流量捕获(嗅探)4.12.13 可信关系滥用4.13 拒绝服务攻击4.14 巩固4.15 安全参考文献第5章 防御武器库5.1 防御武器库5.1.1 访问控制5.1.2 系统访问控制5.2 鉴别5.2.1 IP鉴别5.2.2 口令鉴别5.2.3 窃听攻击5.2.4 口令猜测攻击5.2.5 基于令牌的鉴别5.2.6 会话鉴别5.2.7 客户端会话/ID窃取5.2.8 密码(基于密钥的)鉴别5.2.9 密钥传输和密钥管理漏洞5.2.10 密钥绑定和假冒漏洞5.2.11 针对弱密钥的字典攻击和蛮力攻击5.2.12 集中式鉴别服务器5.2.13 人体特征鉴别(生物测定学)5.3 资源控制5.4 抗抵赖性5.5 私密性5.5.1 虚拟专用网5.5.2 会话和协议加密5.5.3 文件系统加密.....

## <<黑客防范手册>>

### 媒体关注与评论

书评本书通过剖析黑客攻击技术，介绍了网络攻击和防御中所采取的策略。

本书从黑客攻击/安全防御两个方面分析了不同的主题，详细给出了黑客攻击的动机和防御的方法。本书根据特定的技术领域和管理任务来组织章节，为网络防御者提供了理论知识，因为入侵者使用不断变化的、主动的工具和技术。

本书每个章节都提供了访问攻击或保护性Web站点和其他资源的“路径”，以便对已有内容进行补充。

参考这些补充的不断升级的资源可以确保本书的时效性和长期有效性。

通过告诉IT专业人员如何模拟黑客的思维，为打赢保护数字资产的“战争”提供了非常有价值的武器。

本书具有以下特点：集中于Unix和微软的Windows NT/2000平台。

根据合理的安全架构，利用图表方式对攻击和对抗两个方面进行了比较分析。

为下列内容提供技术基础：程序设计和代码利用的方法，协议及其基本脆弱性，数据库及其弱点和防御措施。

分析入侵者在深入网络内部过程中所使用的策略和工具。

揭示了调查取证的有关工作。

## <<黑客防范手册>>

### 编辑推荐

本书通过剖析黑客攻击技术，介绍了网络攻击和防御中所采取的策略。

全书分三个部分：第一部分给出了实施黑客攻击所必需具备的基础知识；第二部分从网络协议、服务、数据库入侵和恶意代码等方面，阐述了黑客是如何对系统和网络进行渗透的；最后一部分详细介绍了黑客在成功破解系统或网络后，通常会如何去扩大“战果”。

本书适合有一定安全经验的系统管理员、网络管理员和安全管理员阅读，通过揭示黑客行为的技术内幕，让管理员们做到知己知彼，准确地将黑客行为“映射”到未来的防御系统中。

#### 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>