电脑报 总策划

大师禅言 MASTERS QUOTATION

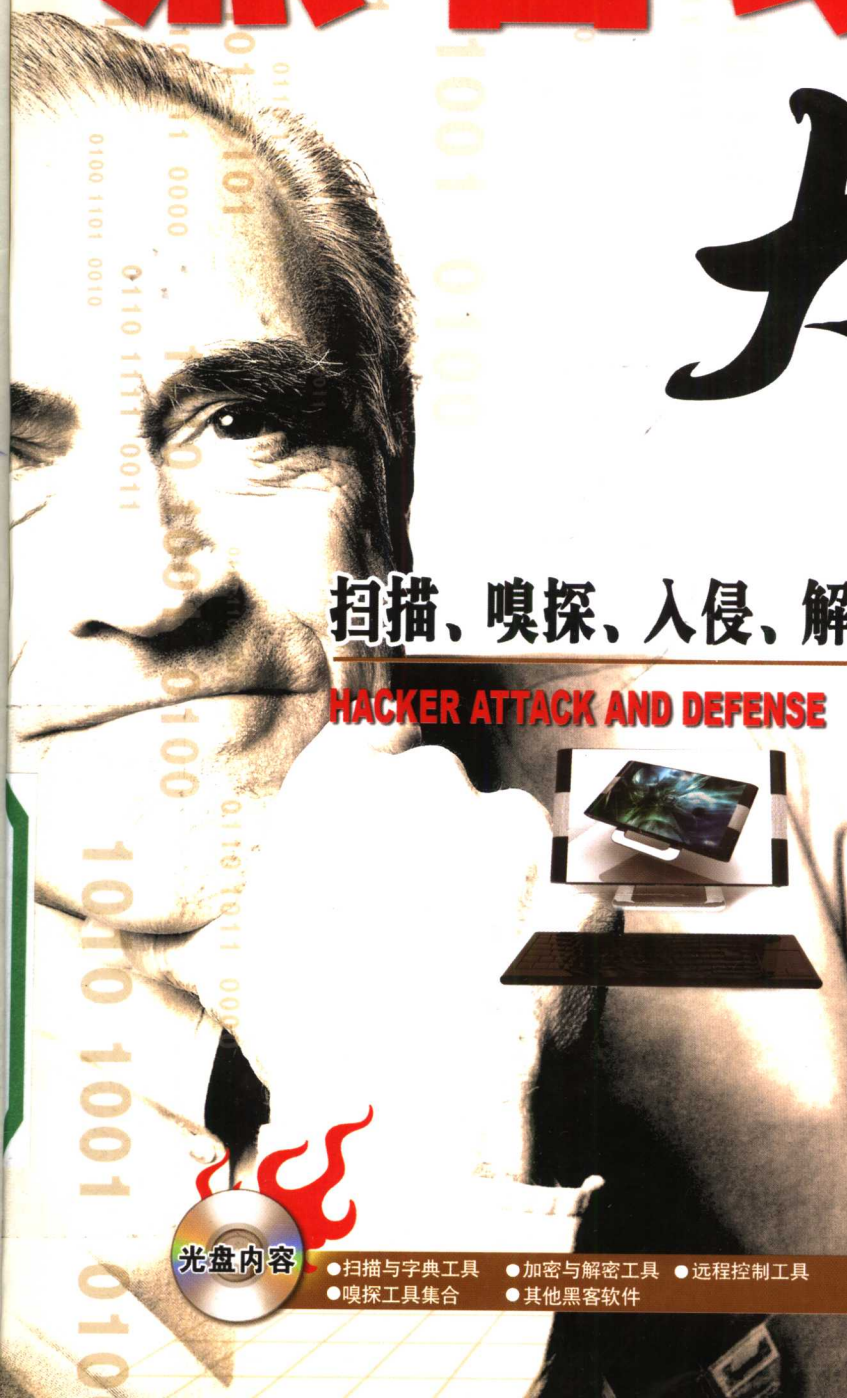
大师传道，授业解惑，引领你登堂入室，从入门到精通

黑客攻防大师

电脑报 编

扫描、嗅探、入侵、解密示例与防范要略

HACKER ATTACK AND DEFENSE



扫描与嗅探

攻击准备，锁定目标，扫描主机漏洞
监听局域网络信息，嗅探机密数据

远程入侵与木马控制

IPC$、Telnet等远程入侵系统与防范
木马制作、植入与特征码防杀技术

追踪黑客与黑客防身术

日志分析，让黑客无所遁形
无线、代理隐藏黑客IP地址

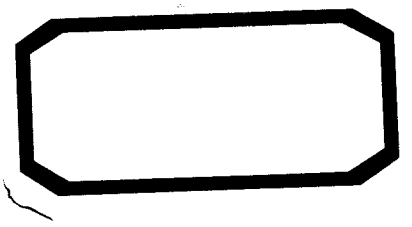
加密与解密

系统、文档口令密码解密技巧
数据加密解密攻防实战

光盘内容

- 扫描与字典工具
- 加密与解密工具
- 远程控制工具
- 嗅探工具集合
- 其他黑客软件

电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS



黑客攻防大师

电脑报　编

电脑报
电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

内容提要

黑客的出现可以说是当今信息社会中有目共睹、不容忽视的一个独特现象。一些黑客的网络袭击行为无意或者有意地对社会造成了不同程度的危害。为了捍卫信息社会的安全，本书以客观实例为基础，并结合作者长期实验的心得体会，从多个角度来分析了黑客“攻”与“防”的全过程。全书共分 3 篇 13 章，其中第 1 章到第 3 章为黑客入门基础篇，包括了 IP、端口、扫描等网络基础知识。第 4 章到第 11 章为黑客攻防实战篇，包括远程控制、木马植入、嗅探监听、QQ 盗号等内容，帮助读者真正了解黑客入侵的手法，这样才能做到切实有效的防范。第 12、13 章为密码策略应用篇，介绍了黑客破解密码的方法，并指出了信息安全保护的要点。

本书绝不是为那些不良动机的人提供支持，而是最大限度地唤醒人们的网络安全意识，正视信息安全存在的危机，适合于网络技术爱好者、网络系统管理员以及信息安全人士阅读。

警告：使用网络技术攻击他人计算机属于违法行为，读者切勿用本书介绍的方法对他人计算机进行恶意攻击，否则后果自负！

光盘内容

1. 扫描与字典工具
2. 加密与解密工具
3. 远程控制工具
4. 嗅探工具集合
5. 其他黑客软件

书　　名：黑客攻防大师
编　　者：电脑报
技术编辑：何　磊
封面设计：程　晨
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路3号科协大厦
邮政编码：400013
对外合作：(023)63658933
发　　行：电脑报经营有限责任公司
经　　销：各地新华书店、报刊亭
CD生产：四川省鉴山数码科技有限公司
文本印刷：重庆升光电力印务有限公司
开本规格：787mm × 1092mm 1/16　20印张　400千字
版　　号：ISBN 978-7-900729-80-4
版　　次：2008年5月第1版　2008年5月第1次印刷
定　　价：32.00元(1CD+配套书)

大师是这样炼成的

- **“菜鸟”晋级首选品牌图书**
- **从零起步，轻松迈上大师之路**

《大师禅言》系列图书携《电脑报》多年的出版经验，将电脑高手的经验整理成册，孕育了一代又一代的电脑应用高手！系列图书自 1998 年推出以来，在策划、组稿、编辑等环节一直贯穿并秉承《电脑报》“权威、通俗、实用”的理念，想读者之所想，力求让大家从一位电脑新手快速成长为电脑应用大师！本套书一经推出，就得到了读者的好评，多次荣登全国图书畅销排行榜，并被《中华读书报》评为“书店经理眼中的好书”，图书历经多次改版、加印，累计销量达到 120 万余册。

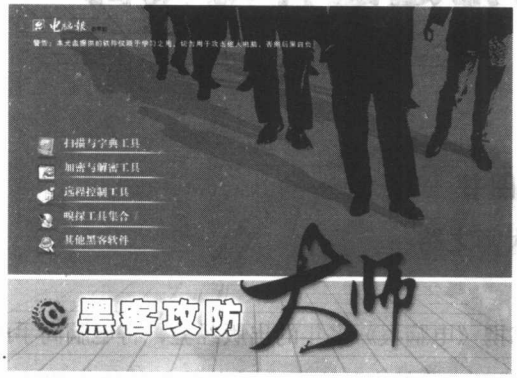
《大师禅言》系列图书致力于为广大读者提供最新、最热、最权威的电脑应用资讯和技巧，选取了广大电脑用户非常关心的电脑维护、网络管理维护和黑客攻防三大热门内容，按照由浅入深的思路进行编写：书中既有初级入门的内容，也有中级的提高应用，最后过渡到大师的独门秘笈。正文中还穿插着很多“技巧”和“大师点拨”，将电脑高手的经验和技巧毫无保留地奉献给大家，旨在帮助大家在成长为“大师”的道路上少走弯路。

在广大读者强烈要求下，我们结合电脑应用的最新动态，并采纳一些读者反馈提供的宝贵意见，再次对图书进行重新策划组稿，特别推出 2008 全新版《大师禅言》系列。

编 者

2008 年 5 月

光盘精彩内容导航



光盘最低配置要求：

CPU主频：850MHz
内　　存：128MB
分 辨 率：800 × 600
显　　存：32MB
光　　驱：52倍速CD光驱
声　　卡：SoundBlaster及兼容声卡
操作系统：Windows 98/Me/2000/XP/2003/Vista

警　　告：本光盘提供的软件仅供学习之用，切勿用于攻击他人电脑，否则后果自负！

光盘栏目	软件用途	精彩内容	
扫描与字典工具	本栏目收录图书中主要介绍的扫描工具及字典生产器，其中，扫描器的使用方法请读者参见图书第3章，字典工具的使用方法主要参见第10章。	NetSuper Protectx superscan 局域网查看工具	扫描端口 字典工具SDG 易优超级字典生成器 黑客字典
远程控制工具	本栏目收录了著名的远程控制工具，可以方便的帮助用户远程维护计算机，其具体的使用方法请参见图书第5章。	DameWare NT pcAnywhere v10.5.1 PsExec 1.82 版 PsTools WinVNC	
嗅探工具集合	本栏目收录了世界上著名的嗅探工具Sniffer Pro，它能帮助网管员维护网络，查找故障，同时也能帮助我们抵御局域网中的入侵。嗅探器的使用方法请读者参见图书第9章。	Sniffer Pro Iris 艾菲网页侦探 SpyNet Sniffer 屏幕间谍	
加密与解密工具	本栏目收录了世界上顶级的加密软件PGP，该软件的使用方法请读者参见图书第13章，此外本栏目中收录的其他文件密码清除器能让用户轻松找回丢失的密码。	PGP.Desktop Biospwds Office Password Remover	Advanced ZIP PasswordRecovery Word Password RecoveryMaster Advanced RAR PasswordRecovery 多功能密码破解软件
其他黑客软件	本栏目收录了其他未分类的软件，这些软件都在图书中有所介绍，其中VMware虚拟机出现在第2章，代理猎手出现在第8章，而花蝴蝶出现在第7章。	VMware 代理猎手 MultiProxy SocksCap32 socks2http C32asm OllyICE 花蝴蝶正式版	

目录

第一篇 黑客入门基础篇

第1章 黑客入侵与网络基础

第2章 虚拟机使用与训练

第3章 信息扫描与目标锁定

第二篇 黑客攻防实战篇

第4章 系统后门与漏洞入侵

第5章 远程控制过程演示

第6章 木马开启后门的入侵与防范

第7章 木马的植入与防范

第8章 行踪隐藏与痕迹清理

第9章 嗅探器截取数据与防范

第10章 QQ攻防实战

第11章 电子邮件攻防战

第三篇 密码策略应用篇

第12章 口令密码破解与防范

第13章 数据加密与解密

第1章 黑客入侵与网络基础

互联网的发展让人们的学习、工作和生活发生了巨大变化，不过网络安全问题也随之凸现而来，总有不法分子威胁着人们的信息安全。他们是如何在网络中兴风作浪的呢？我们将在本章做初步介绍。

1.1 网络中的黑客

Internet（因特网）的普及使人们的工作生活发生了翻天覆地的变化，可是在 Internet 世界中却没有人来管理。如同武侠小说中的“江湖”一样，在这个没有王法的世界中滋生出了许多正派和邪派的力量，他们有秩序的建立者，也有潜在的破坏者，有人把他们称之为黑客。下面让我们走进黑客的世界，一同揭开黑客神秘的面纱。

1.1.1 什么是黑客

黑客，英文名为 Hacker，人们通常认为黑客是指在计算机技术上有一定特长，并凭借自己掌握的技术知识，采用非法的手段逃过计算机网络系统的存取控制，而获得进入计算机网络进行未授权的或非法的访问的人。

事实上黑客是指这样一群人：他们对计算机有着狂热的兴趣和执着的追求，不断地研究计算机和网络知识，发现计算机和网络中的漏洞，喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补方案。不过有的黑客却闯入他人计算机系统，其本意不在攻击对方和造成破坏，而是凭借自己的专业技能发现其中的漏洞，进入系统后留下一定的标记，以此来炫耀自己的能力。

黑客起源于 20 世纪 60 年代，当时在美国麻省理工学院的人工智能实验室里，有一群自称为黑客的学生们以编制复杂的程序为乐趣，当初他们并没有功利性目的。此后不久，连接多所大学计算机实验室的美国国防部实验性网络 APARNET 建成，黑客文化便通过网络传播到更多的大学乃至社会。后

来，有些人利用手中掌握的“绝技”，擅自闯入他人的计算机系统。随着 APARNET 逐步发展成为因特网，黑客们的活动天地越来越广阔，人数也越来越多，形成鱼龙混杂的局面。近年来，随着因特网在全球的飞速发展，各种恶性的非法闯入事件更是频频发生，对世界各国计算机系统的安全构成极大的威胁，我们称这些害群之马为“入侵者”。

图1-1 在互联网上黑客总是让人害怕

图1-2 病毒也是黑客入侵的利器

1.1.2 黑客攻击的过程

黑客在面对不同环境时所采取的攻击手段也会不同，但纵观其整个攻击过程，也有一定的规律可循，一般可以分：信息收集、实施攻击、巩固控制、继续深入几个过程。下面具体了解一下这几个过程。

1.攻击前的准备

黑客在发动攻击前必须了解目标的网络结构，搜集各种目标系统的信息等。

（1）锁定目标：网络上有许多主机，黑客首先要寻找他找的站点。当然能真正标识主机的是 IP 地址，黑客利用域名和 IP 地址就可以顺利地找到目标主机。

（2）了解目标的网络结构：确定要攻击的目标后，黑客就会设法了解其所在的网络结构，哪里是网关路由，哪里有防火墙、入侵检测系统 (IDS)，哪些主机与要攻击的目标主机关系密切等，最简单的就是用 Tracert 命令追踪路由，也可以发一些数据包看其是否能通过来猜测防火墙过滤规则的设定等。当然老练的黑客在干这些的时候都会利用别的计算机来间接地探测，从而隐藏他们真实的 IP 地址。

（3）搜集系统信息：在搜集到目标的第一批网络信息之后，黑客会对网络上的每台主机进行全面的系统分析，以寻求该主机的安全漏洞或安全弱点。搜集系统信息的方法有开放端口分析、利用信息服务、利用安全扫描器、以及社会工程学等。

接着黑客还会检查其开放端口进行服务分析，看是否有能被利用的服务。因特网上的主机大部分都提供 WWW、E-mail、FTP、Telnet 等日常网络服务，通常情况下 Telnet 服务的端口是 23 等，WWW 服务的端口是 80，FTP 服务的端口是 23。

（4）利用信息服务：像 SNMP 服务、Traceroute 程序、WHOIS 服务可用来查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节，Traceroute 程序能够用该程序获得到达目标主机所要经过的网络数和路由器数，WHOIS 协议服务能提供所有有关的 DNS 域和相关的管理参数，Finger 协议可以用 Finger 服务来获取一个指定主机上的所有用户的详细信息（如用户注册名、电话号码、最后注册时间以及他们有没有读邮件等）。所以如果没有特殊的需要，管理员应该关闭这些服务。