

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 | |

版权所有 盗版必究
未经许可 不得以任何形式和手段复制和抄袭

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

C D 生产: 四川省崑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。

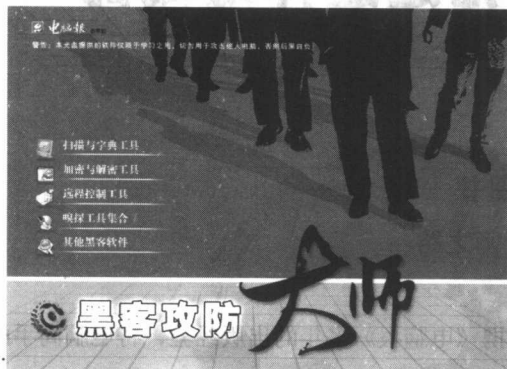
《大师禅言》系列图书致力于为广大读者提供最新、最热、最权威的电脑应用资讯和技巧，选取了广大电脑用户非常关心的电脑维护、网络管理维护和黑客攻防三大热门内容，按照由浅入深的思路进行编写：书中既有初级入门的内容，也有中级的提高应用，最后过渡到大师的独门秘笈。正文中还穿插着很多“技巧”和“大师点拨”，将电脑高手的经验和技巧毫无保留地奉献给大家，旨在帮助大家在成长为“大师”的道路上少走弯路。

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	

第一篇 黑客入门基础篇

第1章 黑客入侵与网络基础

1.1 网络中的黑客	1
1.1.1 什么是黑客	1
1.1.2 黑客攻击的过程	2
1.2 认识 IP 地址	3
1.2.1 什么是 IP 地址	3
1.2.2 公网 IP 与私有 IP	4
1.2.3 动态 IP 和固定 IP	5
1.2.4 私有 IP 地址分段	6
1.2.5 IP 的类别	6
1.2.6 子网掩码	8
1.2.7 特殊的回路 IP 段	9
1.2.8 NAT 网络地址转换	9
1.3 端口与协议	10
1.3.1 什么是端口	10
1.3.2 端口分类	11
1.3.3 常见的端口	12
1.3.4 查看端口	13
1.3.5 限制端口	14
1.4 识别操作系统的意义	16

第2章 虚拟机使用与训练

2.1 初识虚拟机	17
2.1.1 主流的虚拟机软件	18
2.1.2 虚拟机的名词概念	19
2.1.3 VMware 虚拟机模拟环境介绍	19
2.2 使用 VMware 虚拟机配置虚拟系统	20



2.2.1 安装虚拟系统前的初始配置	20
2.2.2 更改 VMware 配置	22
2.2.3 更改磁盘文件路径	25
2.2.4 安装虚拟系统	25
2.3 安装 VMware Tools 增强性能	25
2.3.1 什么是 VMware Tools	26
2.3.2 不同操作系统 VMware Tools 安装方法	26
2.3.3 访问主机资源	27
2.4 使用 VMware 快照与克隆恢复系统	29
2.4.1 使用快照恢复系统	29
2.4.2 使用克隆恢复系统	30
2.5 搭建虚拟网络	31
2.5.1 VMware 的 4 种网络模式	31
2.5.2 用 VMware 组建虚拟网络环境	34

第3章 信息扫描与目标锁定

3.1 搜索网络重要信息	36
3.1.1 获取目标主机 IP 地址	36
3.1.2 通过 IP 获取目标主机地理位置	38
3.1.3 网站注册信息查询	40
3.1.4 网站注册信息搜集	40
3.2 扫描目标主机的 IP 与端口	42
3.2.1 认识扫描器	42
3.2.2 IPScan 扫描活动主机	43
3.2.3 使用 NetSuper 扫描共享资源	44
3.2.4 局域网查看工具 LanSee	45
3.2.5 扫描目标主机开启的端口	46
3.2.6 功能丰富的 SuperScan 端口扫描器	47
3.2.7 综合扫描器 X-Scan	51
3.2.8 流光使用指南	57
3.3 防范黑客扫描	61

第二篇 黑客攻防实战篇

第4章 系统后门与漏洞入侵

4.1 IPC\$ 共享连接的入侵与防范	63
4.1.1 扫描 IPC\$ 漏洞主机	64
4.1.2 利用 IPC\$ 连接漏洞主机	65
4.1.3 建立后门账号	67
4.1.4 Windows XP 的 IPC\$ 连接	68
4.1.5 IPC\$ 连接失败的原因	73
4.1.6 IPC\$ 常见问题与解答	74
4.1.7 防范 IPC\$ 入侵	76
4.2 基于 Telnet 的入侵与防范	78
4.2.1 认识 Telnet	78
4.2.2 使用 Telnet 登录 Windows 2000	78
4.2.3 使用 Telnet 登录 Windows XP	81
4.2.4 防范 Telnet 入侵	86
4.3 典型系统漏洞入侵实例介绍	86
4.3.1 缓冲区溢出漏洞	86
4.3.2 拒绝服务攻击介绍	87
4.3.3 分布式拒绝服务攻击介绍	88

第5章 远程控制过程演示

5.1 DameWare 远程控制过程演示	90
5.1.1 扫描远程主机是否存在 NT 弱口令（获取管理员权限）	90
5.1.2 使用 DameWare 入侵漏洞主机	91
5.2 Radmin 入侵过程演示	97
5.2.1 使用 Radmin 远程控制	97
5.2.2 Radmin 服务端安装技巧	99

5.3 使用 pcAnywhere 的远程控制	100
5.3.1 pcAnywhere 的工作原理	101
5.3.2 被控端设置	101
5.3.3 主控端设置	103
5.3.4 网络连接的优化配置	103
5.3.5 远程控制的实现	104
5.4 WinVNC 远程控制详解	104
5.4.1 利用 WinVNC 的正向连接	104
5.4.2 利用 WinVNC 的逆向连接	106
5.5 Windows Vista 远程协助使用详解	107
5.5.1 改进的 Windows Vista 远程协助	107
5.5.2 远程桌面与远程协助	107
5.5.3 发送 Windows Vista 的远程协助请求	109
5.5.4 接受远程协助请求	111
5.5.5 远程协助其他设置	112
5.6 内网中的 Windows XP 远程协助设置	114
5.6.1 通过网关做端口映射	114
5.6.2 启用被控端远程控制	115
5.6.3 远程协助	117
5.6.4 远程桌面	117

第6章 木马开启后门的入侵与防范

6.1 木马取名的来历	118
6.1.1 木马的定义	119
6.1.2 木马的特征	119
6.1.3 木马的功能	120
6.1.4 木马的分类	120
6.2 典型木马“冰河”入侵实例	121
6.2.1 配置冰河木马的服务端	121
6.2.2 远程控制冰河服务端	123
6.2.3 冰河木马防范与反攻	124

6.3 “黑洞”木马探秘	125
6.3.1 配置“黑洞”服务端	125
6.3.2 揪出“黑洞”木马	127
6.3.3 防范摄像头木马	129
6.4 反弹式“灰鸽子”木马实战攻略	130
6.4.1 反弹式木马的特色	130
6.4.2 灰鸽子的特点	131
6.4.3 配置灰鸽子服务端	132
6.4.4 远程入侵服务端	135
6.4.5 利用动态域名为“灰鸽子”配置自动上线	137
6.4.6 “灰鸽子”客户端位于内网的配置方案	141
6.4.7 “灰鸽子”客户端位于内网中但不能设置网关	142
6.4.8 清除计算机中的灰鸽子	146
6.4.9 防止中灰鸽子病毒需要注意的事项	149

第7章 木马的植入与防范

7.1 木马是如何被植入的	150
7.1.1 修改图标	150
7.1.2 文件合并	150
7.1.3 文件夹木马	154
7.1.4 网页木马	156
7.2 修改特征码瞒骗杀毒软件	159
7.2.1 设置 MYCCL 复合特征码定位器	159
7.2.2 位特征码范围	159
7.2.3 特征码范围	160
7.2.4 修改特征码内容	161
7.2.5 特征码防杀总结	161
7.3 加壳木马防范查杀	161
7.3.1 壳是用来干什么的	161
7.3.2 单一加壳伪装木马	162
7.3.3 多重加壳伪装木马	162
7.3.4 加壳木马也能防	164



7.3.5 利用加壳伪装木马的总结	164
7.4 使用花指令防杀毒软件查杀	165
7.4.1 什么是花指令	165
7.4.2 垃圾代码是如何弄“晕”杀软件的	165
7.4.3 揭秘花指令免杀步骤	165

第8章 行踪隐藏与痕迹清理

8.1 IP 隐藏技巧	169
8.2 代理隐藏术	170
8.2.1 网上查找代理服务器	171
8.2.2 扫描工具查找	171
8.2.3 代理猎手使用要点	175
8.2.4 多代理切换保证安全	179
8.2.5 代理协议的转换	183
8.2.6 让黑客任务隐藏在代理服务下	185
8.2.7 使用代理的注意事项	188
8.3 黑客入侵与日志清除	188
8.3.1 认识系统日志	188
8.3.2 Windows 系列日志查看与分析	189
8.3.3 黑客如何清除系统日志	191

第9章 嗅探器截取数据与防范

9.1 局域网中的嗅探与监听	194
9.1.1 日记泄露的秘密	194
9.1.2 嗅探器应用范围	195
9.1.3 局域网内计算机通讯的概念和寻址	195
9.1.4 发生在共享式局域网内的窃听	197
9.1.5 发生在交换式局域网内的窃听	198
9.2 Sniffer 介绍	199

9.3 实用嗅探器 Sniffer Portable	201
9.3.1 Sniffer Portable 功能简介	201
9.3.2 查看捕获的报文	202
9.3.3 捕获数据包后的分析工作	203
9.3.4 设置捕获条件	204
9.3.5 报文发送	205
9.4 其他实用嗅探器	206
9.4.1 Iris 网络嗅探器	206
9.4.2 网络间谍 SpyNet Sniffer	211
9.4.3 艾菲网页侦探	212
9.5 防御 Sniffer 攻击	214
9.5.1 怎样发现 Sniffer	214
9.5.2 抵御 Sniffer	214
9.6 使用屏幕间谍监视本地计算机	215
9.6.1 软件功能面板	215
9.6.2 记录浏览	217

第10章 QQ攻防实战

10.1 扫描 QQ 信箱盗取密码	219
10.2 QQ 木马盗号的阴谋与反阴谋	221
10.2.1 揭秘 QQ 盗号木马	221
10.2.2 捕杀 QQ 盗号木马	222
10.2.3 揪出幕后元凶	223
10.3 揭开 QQ 币 /Q 点被盗之谜	225
10.3.1 制作盗 QQ 木马	225
10.3.2 批量登录被盗 QQ	226
10.3.3 Q 币 /Q 点被盗实录	227
10.4 流行 QQ 木马盗号实例演示	228
10.4.1 “QQ 简单盗”实例	228
10.4.2 “QQ 流感大盗”实例	230

10.4.3 “QQ 盗号王”实例	231
10.5 QQ 本地被破解	232
10.6 使用 QQ 申诉取回被盗的 QQ	234
10.7 QQ 炸弹式攻击	236
10.7.1 QQ 炸弹攻击	236
10.7.2 反击 QQ 炸弹	237
10.8 查看 QQ 聊天记录	238
10.8.1 利用“QQ 聊天记录查看器”查看聊天记录	238
10.8.2 防范聊天记录被偷窥	239
10.9 QQ 远程攻击测试	239
10.10 网吧内嗅探出 QQ 密码的阴谋	240
10.11 QQ 避开攻击保护密码的七个小技巧	242

第11章 电子邮件攻防战

11.1 黑客是如何破解邮箱的	244
11.1.1 利用邮件服务器操作系统漏洞	244
11.1.2 利用邮件服务器软件本身的漏洞	245
11.1.3 在邮件的传输过程中窃听	245
11.2 黑客破解邮箱示例	245
11.2.1 使用“流光”探测 POP3 邮箱密码	245
11.2.2 黑雨 POP3 邮件密码破解器	248
11.2.3 使用“流影”探测 POP3 邮箱	248
11.3 欺骗手段获取邮件信息	252
11.3.1 了解电子邮件欺骗的手法	252
11.3.2 利用 Foxmail 欺骗实例	253
11.3.3 Outlook Express 欺骗实例	256
11.3.4 绕过 SMTP 服务器的身份验证	260

11.4 电子邮件攻击与防范	261
11.4.1 电子邮箱信息攻击原理	261
11.4.2 随心邮箱炸弹	262
11.4.3 邮箱炸弹的防范	262
11.4.4 垃圾邮件的过滤	263

第三篇 密码策略应用篇

第12章 口令密码破解与防范

12.1 常见系统口令入侵法	265
12.1.1 解除 CMOS 口令	265
12.1.2 解除 Windows 账户登录密码	266
12.2 巧除 Word 与 Excel 文档密码	270
12.2.1 清除 Word 密码	270
12.2.2 清除 Excel 密码	271
12.3 清除压缩文件密码	271
12.3.1 压缩文件破解技巧	271
12.3.2 巧设压缩文件提升文件安全	274
12.4 黑客破解口令密码的心理学	275

第13章 数据加密与解密

13.1 走进密码生活	277
13.1.1 民用密码的应用和安全性	277
13.1.2 从官方到民间的密码术	278
13.1.3 区别口令加锁与文件加密	279
13.2 密码学的常识	279
13.2.1 明文与密文	280



13.2.2 算法和密钥	280
13.2.3 对称算法	281
13.2.4 非对称密钥算法	282
13.2.5 密码破译原理	284
13.3 顶级加密软件——PGP	284
13.3.1 大名鼎鼎的数据加密软件 PGP	284
13.3.2 PGP 密钥管理	286
13.3.3 应用 PGP 加密文件	289
13.4 其他加密软件介绍	290
13.4.1 加密金刚锁	290
13.4.2 iProtect Portable	293
13.4.3 文件加密利器 Fedt	294
13.5 Windows 中 EFS 加密及解密	295
13.5.1 EFS 特点简介	295
13.5.2 导出导入 EFS 密钥	296
13.5.3 EFS 应用实例	299
13.5.4 EFS 加密的破解	302



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。