



学电脑从入门到精通

THE SECRETS OF BEING AN EXPERT
IN COMPUTER FROM A BEGINNER




黑客攻防

从入门到精通

恒盛杰资讯 编著

- 多媒体视频+技巧+案例的学习模式
- 赠送重点、难点及案例多媒体视频讲解
- 赠送《黑客攻防秘笈》电子书

 机械工业出版社
China Machine Press



013038401

TP393.08
678

学电脑从入门到精通

黑客攻防

从入门到精通

恒盛杰资讯 编著



TP393.08
678



北航 C1643939



机械工业出版社
China Machine Press

p

013038401

图书在版编目 (CIP) 数据

黑客攻防从入门到精通 / 恒盛杰资讯编著 . —北京 : 机械工业出版社 , 2013.3

(学电脑从入门到精通)

ISBN 978-7-111-41765-1

I. 黑… II. 恒… III. 计算机网络-安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字 (2013) 第 047279 号

版权所有 · 侵权必究

封底无防伪标均为盗版

本书法律顾问 北京市展达律师事务所

本书全面且详细地介绍了黑客攻防的基础知识, 主要包括黑客攻防前的准备工作、扫描与嗅探攻防、Windows 系统漏洞攻防、密码攻防、病毒攻防、木马攻防等内容。虽然书中介绍了黑客入侵攻击目标计算机的一些相关操作, 但是这不是本书的重点, 本书的重点在于介绍如何采取有效的防范措施来防御黑客入侵攻击自己的计算机。

本书按照由易到难、循序渐进的顺序安排知识点。本书图文并茂, 讲解深浅适宜, 叙述条理清楚, 通过阅读本书, 读者不仅能了解黑客入侵攻击的原理和使用工具, 而且还能掌握防御入侵攻击的相关操作。本书配有多媒体教学光盘, 光盘中提供了相关的视频教学演示。

本书适用于计算机初学者, 也适用于计算机维护人员、IT 从业人员以及对黑客攻防与网络安全维护感兴趣的计算机中级用户, 同时也可作为各种计算机培训班的辅导用书。

机械工业出版社 (北京市西城区百万庄大街 22 号 邮政编码 100037)

责任编辑: 陈佳媛

北京瑞德印刷有限公司印刷

2013 年 4 月第 1 版第 1 次印刷

185mm × 260mm · 22 印张

标准书号: ISBN 978-7-111-41765-1

ISBN 978-7-89433-831-0 (光盘)

定 价: 49.00 元 (附光盘)

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

客服热线: (010) 88378991 88361066

投稿热线: (010) 88379604

购书热线: (010) 68326294 88379649 68995259

读者信箱: hzsj@hzbook.com

前言

在 Internet 中，黑客通常都是一类拥有高超计算机技术的人，他们甚至不需要亲自接触用户的计算机，就可以偷窥其中的账户、密码等信息，甚至破坏其操作系统。随着越来越多的金融贸易要通过 Internet 来实现，防御黑客入侵已成为至关重要的工作。作者特为此编写了本书。

主要内容

本书包括 17 章，第 1 章介绍了黑客的基础知识，包括 IP 地址、端口、系统进程以及 DOS 命令等内容；第 2 章介绍了黑客攻防前的准备工作，包括安装 VMware 和虚拟操作系统，认识黑客常用的入侵工具、入侵方法以及防护策略等内容；第 3 章介绍了扫描与嗅探攻防的知识，包括搜索目标计算机的 IP 地址、扫描其端口以及嗅探网络中的数据包等内容；第 4 章介绍了 Windows 系统漏洞攻防的相关知识，包括认识、检测和修复 Windows 系统漏洞等内容；第 5 章介绍了密码攻防的相关知识，包括解除系统中的密码、破解文件密码以及防范密码被轻易破解等内容；第 6 ~ 7 章介绍了病毒、木马攻防相关知识，包括认识病毒木马、制作病毒木马以及防范病毒木马等内容；第 8 ~ 10 章介绍了后门技术、局域网和远程控制攻防的相关知识，包括认识后门、制作后门、清除日志信息、防御局域网中的攻击类型以及常见的远程入侵方式等内容；第 11 ~ 13 章介绍了 QQ、E-Mail 与 IE 浏览器和网站攻防的相关知识，包括盗取 QQ 密码和远程攻击 QQ、保护 QQ 密码和聊天记录、攻击 IE 浏览器和电子邮箱、DoS 攻击、DDoS 攻击等内容；第 14 ~ 16 章介绍了防范流氓与间谍软件、计算机安全防护以及系统与数据的备份与恢复的相关知识，包括清除流氓软件与间谍软件、系统\注册表\组策略的安全设置以及系统的备份与还原等内容；第 17 章

介绍了网络支付工具安全的相关知识，包括防御黑客入侵支付宝账户、网上银行以及财付通等内容。

本书特色

简单易懂——本书为了能适用于初次接触黑客攻防技术的用户，将黑客入侵攻击演示以及防御黑客入侵的操作以图文结合的形式进行介绍，使读者可以轻松地掌握有关黑客入侵目标计算机和防御黑客入侵计算机的基础知识。

内容丰富——本书中添加了“提示”版块，既包括为读者答疑解惑的纯文字内容，又包括帮助读者提高动手能力的图文解析内容，帮助读者答疑解惑。

读者对象

本书内容详细，讲解具体，充分融入了作者的实际使用经验和操作心得，可以作为个人学习和了解黑客攻防的参考书籍。

希望本书能对广大读者朋友有所帮助。由于作者水平有限，在编写本书的过程中难免会存在疏漏之处，恳请广大读者批评指正，可登录 www.epubhome.com 网站提出宝贵意见。

作者

2013年2月

目 录

前 言

第 1 章 从零开始认识黑客 / 1

- 1.1 认识黑客 / 2
 - 1.1.1 区别黑客与骇客 / 2
 - 1.1.2 成为黑客必须掌握的知识 / 2
- 1.2 黑客的定位目标——IP 地址 / 3
 - 1.2.1 认识 IP 地址 / 3
 - 1.2.2 IP 地址的分类 / 4
 - 1.2.3 查看计算机的 IP 地址 / 5
- 1.3 黑客的专用通道——端口 / 5
 - 1.3.1 端口的分类 / 5
 - 1.3.2 关闭端口 / 6
 - 1.3.3 限制使用指定的端口 / 8
- 1.4 黑客藏匿的首选地——系统进程 / 13
 - 1.4.1 认识系统进程 / 14
 - 1.4.2 关闭和新建系统进程 / 14
- 1.5 认识黑客常用术语和 DOS 命令 / 16
 - 1.5.1 常用术语 / 16
 - 1.5.2 DOS 基本命令 / 17
 - 1.5.3 NET 命令 / 23

第 2 章 黑客攻防前的准备工作 / 29

- 2.1 在计算机中搭建虚拟环境 / 30
 - 2.1.1 认识虚拟机 / 30
 - 2.1.2 在 VMware 中新建虚拟机 / 30
 - 2.1.3 在 VMware 中安装操作系统 / 32
 - 2.1.4 安装 VMwareTools / 34
- 2.2 认识黑客常用的入侵工具 / 36
 - 2.2.1 端口扫描工具 / 37
 - 2.2.2 数据嗅探工具 / 37
 - 2.2.3 木马制作工具 / 38
 - 2.2.4 远程控制工具 / 38

- 2.3 认识黑客常用的入侵方法 / 39
 - 2.3.1 数据驱动攻击 / 39
 - 2.3.2 伪造信息攻击 / 39
 - 2.3.3 针对信息协议弱点攻击 / 39
 - 2.3.4 远端操纵 / 39
 - 2.3.5 利用系统管理员失误攻击 / 39
 - 2.3.6 重新发送攻击 / 40
 - 2.3.7 ICMP 报文攻击 / 40
 - 2.3.8 针对源路径选择的弱点攻击 / 40
 - 2.3.9 以太网广播法 / 40
 - 2.3.10 跳跃式攻击 / 40
 - 2.3.11 窃取 TCP 协议连接 / 41
 - 2.3.12 夺取系统控制权 / 41
- 2.4 掌握个人计算机安全的防护策略 / 41
 - 2.4.1 安装并及时升级杀毒软件 / 41
 - 2.4.2 启用防火墙 / 42
 - 2.4.3 防止木马和病毒 / 42
 - 2.4.4 警惕“网络钓鱼” / 42
 - 2.4.5 切勿随意共享文件夹 / 42
 - 2.4.6 定期备份重要数据 / 42

第 3 章 扫描与嗅探攻防 / 43

- 3.1 搜集目标计算机的重要信息 / 44
 - 3.1.1 获取目标计算机的 IP 地址 / 44
 - 3.1.2 根据 IP 地址查看地理位置 / 45
 - 3.1.3 了解网站备案信息 / 46
- 3.2 扫描目标计算机的端口 / 47
 - 3.2.1 认识端口扫描的原理 / 47
 - 3.2.2 使用 SuperScan 扫描计算机端口 / 47
 - 3.2.3 使用 X-Scan 扫描计算机端口 / 51
- 3.3 嗅探网络中的数据包 / 54
 - 3.3.1 认识嗅探的原理 / 54
 - 3.3.2 使用 Sniffer Pro 捕获并分析网络数据 / 55
 - 3.3.3 使用“艾菲网页侦探”嗅探浏览过的网页 / 56
- 3.4 防范端口扫描与嗅探 / 58
 - 3.4.1 掌握防范端口扫描的常用措施 / 58
 - 3.4.2 利用瑞星防火墙防范扫描 / 58
 - 3.4.3 了解防范嗅探的常用措施 / 59

第 4 章 Windows 系统漏洞攻防 / 61

- 4.1 认识 Windows 系统漏洞 / 62
 - 4.1.1 认识系统产生漏洞的原因 / 62
 - 4.1.2 了解系统中存在的安全隐患 / 62
- 4.2 了解 Windows 系统中存在的漏洞 / 63
 - 4.2.1 认识 WindowsXP 中存在的漏洞 / 63

- 4.2.2 认识 Windows 7 中存在的漏洞 / 65
- 4.3 检测 Windows 系统中存在的漏洞 / 66
 - 4.3.1 使用 MBSA 检测系统安全性 / 66
 - 4.3.2 使用 360 安全卫士检测系统中的漏洞 / 68
- 4.4 学会手动修复 Windows 系统漏洞 / 68
 - 4.4.1 使用 WindowsUpdate 修复系统漏洞 / 68
 - 4.4.2 使用 360 安全卫士修复系统漏洞 / 71

第 5 章 密码攻防 / 72

- 5.1 加密与解密基础 / 73
 - 5.1.1 认识加密与解密 / 73
 - 5.1.2 破解密码的常用方法 / 73
- 5.2 解除系统中的密码 / 74
 - 5.2.1 解除 BIOS 密码 / 74
 - 5.2.2 解除系统登录密码 / 75
- 5.3 破解常见的文件密码 / 81
 - 5.3.1 破解 Office 文档密码 / 81
 - 5.3.2 破解压缩文件的打开密码 / 85
 - 5.3.3 查看星号密码 / 86
- 5.4 防范密码被轻易破解 / 88
 - 5.4.1 设置安全系数较高的密码 / 88
 - 5.4.2 使用隐身侠加密保护文件 / 88
 - 5.4.3 使用 Bitlocker 强化系统安全 / 91

第 6 章 病毒攻防 / 95

- 6.1 认识病毒 / 96
 - 6.1.1 认识病毒的分类 / 96
 - 6.1.2 认识病毒的特征 / 97
 - 6.1.3 认识病毒常见的传播途径 / 98
 - 6.1.4 认识计算机中毒后的常见症状 / 99
- 6.2 学会制作简单的病毒 / 100
 - 6.2.1 制作 Restart 病毒 / 100
 - 6.2.2 制作 U 盘病毒 / 104
- 6.3 预防和查杀计算机病毒 / 106
 - 6.3.1 掌握防范病毒的常用措施 / 106
 - 6.3.2 使用杀毒软件查杀病毒 / 109

第7章 木马攻防 / 114

- 7.1 认识木马 / 115
 - 7.1.1 认识木马的组成 / 115
 - 7.1.2 认识木马的分类 / 115
 - 7.1.3 认识木马的特征 / 116
 - 7.1.4 认识木马的入侵方式 / 117
 - 7.1.5 认识木马的伪装手段 / 118
- 7.2 认识制作木马的常用工具 / 119
 - 7.2.1 “冰河”木马 / 119
 - 7.2.2 CHM 木马 / 125
 - 7.2.3 捆绑木马 / 131
- 7.3 木马的加壳与脱壳 / 133
 - 7.3.1 为木马加壳 / 134
 - 7.3.2 检测加壳的木马 / 135
 - 7.3.2 为木马脱壳 / 136
- 7.4 使用第三方软件防范木马入侵计算机 / 138
 - 7.4.1 Windows 木马清道夫 / 138
 - 7.4.2 360 安全卫士 / 140

第8章 后门技术攻防 / 142

- 8.1 认识常见的后门 / 143
- 8.2 认识账号后门技术 / 143
 - 8.2.1 手动克隆账户 / 144
 - 8.2.2 使用软件克隆账号 / 147
- 8.3 认识系统服务后门技术 / 148
 - 8.3.1 使用 Instsrv 创建系统服务后门 / 148
 - 8.3.2 使用 Srvinstw 创建系统服务后门 / 150
- 8.4 清除日志信息 / 153
 - 8.4.1 手动清除日志信息 / 154
 - 8.4.2 使用批处理文件清除日志信息 / 155
 - 8.4.3 使用工具清除日志信息 / 157
- 8.5 检测系统中的后门程序 / 160

第9章 局域网攻防 / 161

- 9.1 局域网中常见的攻击类型 / 162
 - 9.1.1 广播风暴 / 162
 - 9.1.2 ARP 欺骗攻击 / 163
 - 9.1.3 IP 冲突攻击 / 164
- 9.2 防御广播风暴 / 164
 - 9.2.1 防御广播风暴的常用措施 / 165
 - 9.2.2 使用 VLAN 技术防御广播风暴 / 165

- 9.3 防御 ARP 欺骗攻击 / 166
 - 9.3.1 使用静态 ARP 列表防御 ARP 欺骗攻击 / 166
 - 9.3.2 使用 360 木马防火墙防御 ARP 欺骗攻击 / 168
- 9.4 绑定 MAC 防御 IP 冲突攻击 / 170
- 9.5 提高无线局域网的安全系数 / 173
 - 9.5.1 修改路由器登录口令 / 174
 - 9.5.2 隐藏或修改 SSID / 174
 - 9.5.3 设置 WPA2—PSK 密码 / 175

第10章 远程控制攻防 / 176

- 10.1 远程控制概述 / 177
 - 10.1.1 认识远程控制的原理 / 177
 - 10.1.2 常见远程控制的类别 / 177
- 10.2 基于认证入侵 / 178
 - 10.2.1 IPC\$ 入侵 / 178
 - 10.2.2 Telnet 入侵 / 179
- 10.3 基于注册表入侵 / 183
 - 10.3.1 修改注册表实现远程监控 / 183
 - 10.3.2 开启远程注册表服务 / 185
- 10.4 使用专业软件实现远程控制 / 187
 - 10.4.1 网络执法官 / 187
 - 10.4.2 远程控制任我行 / 190
- 10.5 有效防范远程入侵和远程监控 / 196
 - 10.5.1 防范 IPC\$ 远程入侵 / 196
 - 10.5.2 防范注册表和 Telnet 远程入侵 / 201
- 10.6 其他常见的远程控制方式 / 203
 - 10.6.1 QQ 远程协助 / 203
 - 10.6.2 Windows 远程协助 / 205

第11章 QQ 攻防 / 209

- 11.1 攻击 QQ 常用的方式 / 210
 - 11.1.1 向指定 QQ 发送炸弹 / 210
 - 11.1.2 盗取指定 QQ 的密码 / 210
- 11.2 黑客盗取 QQ 密码的常用工具 / 211
 - 11.2.1 QQ 简单盗 / 211
 - 11.2.2 QQ 眼睛 / 213
 - 11.2.3 阿拉 QQ 密码潜伏者 / 214
- 11.3 黑客远程攻击 QQ 的常用工具 / 216
 - 11.3.1 风云 QQ 尾巴生成器 / 216
 - 11.3.2 QQ 细胞发送器 / 217
- 11.4 保护 QQ 密码和聊天记录 / 217
 - 11.4.1 定期修改 QQ 密码 / 218
 - 11.4.2 加密聊天记录 / 218
 - 11.4.3 申请 QQ 密保 / 219
 - 11.4.4 利用 QQ 电脑管家保障 QQ 安全 / 221

第12章 E-Mail与IE浏览器攻防 / 223

- 12.1 认识网页恶意代码 / 224
 - 12.1.1 网页恶意代码的特征 / 224
 - 12.1.2 认识网页恶意代码的传播方式 / 224
- 12.2 黑客攻击IE浏览器的常用方式 / 225
 - 12.2.1 使用IE炸弹攻击IE浏览器 / 225
 - 12.2.2 使用VBS脚本病毒攻击IE浏览器 / 226
- 12.3 黑客攻击电子邮箱的常用工具 / 228
 - 12.3.1 使用“流光”盗取邮箱密码 / 228
 - 12.3.2 使用E-Mail邮件群发大师发送邮箱炸弹 / 230
- 12.4 IE浏览器的防护 / 232
 - 12.4.1 限制访问危险网站 / 232
 - 12.4.2 提高IE安全防护等级 / 233
 - 12.4.3 清除临时文件和Cookie / 234
 - 12.4.4 清除网页恶意代码 / 235
- 12.5 电子邮箱的防护 / 238
 - 12.5.1 防范邮箱炸弹的攻击 / 238
 - 12.5.2 找回失窃的电子邮箱 / 240

第13章 网站攻防 / 241

- 13.1 认识网站攻击 / 242
 - 13.1.1 拒绝服务攻击 / 242
 - 13.1.2 SQL注入 / 242
 - 13.1.3 网络钓鱼 / 242
 - 13.1.4 社会工程学 / 243
- 13.2 DoS攻防 / 243
 - 13.2.1 认识DoS的攻击原理 / 243
 - 13.2.2 利用路由器防范DoS攻击 / 244
- 13.3 DDoS攻防 / 244
 - 13.3.1 利用“雪花DDoS攻击器”实现DDoS攻击 / 245
 - 13.3.2 防范DDoS攻击的常用措施 / 247
- 13.4 SQL注入攻击 / 248
 - 13.4.1 使用“啊D”实现SQL注入攻击 / 248
 - 13.4.2 使用NBSI实现SQL注入攻击 / 250

第14章 防范流氓与间谍软件 / 252

- 14.1 认识流氓软件与间谍软件 / 253
 - 14.1.1 认识流氓软件 / 253
 - 14.1.2 认识间谍软件 / 253
- 14.2 清除与防范流氓软件 / 253
 - 14.2.1 使用“瑞星安全助手”清理流氓软件 / 253
 - 14.2.2 使用“金山卫士”清理流氓软件 / 256
 - 14.2.3 使用“Windows 流氓软件清理大师”清理流氓软件 / 257
 - 14.2.4 防范流氓软件的常用措施 / 258
- 14.3 使用 Windows Defender 清除间谍软件 / 259

第15章 计算机安全防护设置 / 261

- 15.1 系统安全设置 / 262
 - 15.1.1 禁用来宾账户 / 262
 - 15.1.2 防范使用 Ping 命令探测计算机 / 263
 - 15.1.3 利用代理服务器隐藏 IP 地址 / 272
 - 15.1.4 设置离开时快速锁定桌面 / 274
 - 15.1.5 配置防火墙 / 275
- 15.2 注册表安全设置 / 278
 - 15.2.1 禁止远程修改注册表 / 278
 - 15.2.2 禁止程序在桌面上添加快捷方式 / 279
 - 15.2.3 禁止危险启动项 / 281
 - 15.2.4 关闭默认共享 / 282
 - 15.2.5 设置发生错误时不弹出警告对话框 / 283
- 15.3 组策略安全设置 / 284
 - 15.3.1 设置账户锁定策略 / 284
 - 15.3.2 设置用户权限 / 286
 - 15.3.3 阻止更改“任务栏和「开始」菜单”设置 / 288
 - 15.3.4 禁止访问控制面板 / 289

第16章

系统与数据的备份与恢复 / 290

- 16.1 备份与还原系统 / 291
 - 16.1.1 利用还原点备份与还原系统 / 291
 - 16.1.2 利用 GHOST 备份与还原系统 / 294
- 16.2 备份与还原数据 / 298
 - 16.2.1 备份与还原驱动程序 / 298
 - 16.2.2 备份与还原注册表信息 / 301
 - 16.2.3 备份与还原 IE 收藏夹信息 / 303
 - 16.2.4 备份与还原 QQ 聊天记录 / 307
 - 16.2.5 备份与还原 QQ 自定义表情 / 309
- 16.3 恢复被误删除的数据 / 311
 - 16.3.1 利用 FinalRecovery 恢复误删除的数据 / 311
 - 16.3.2 利用 FINALDATA 恢复误删除的数据 / 314

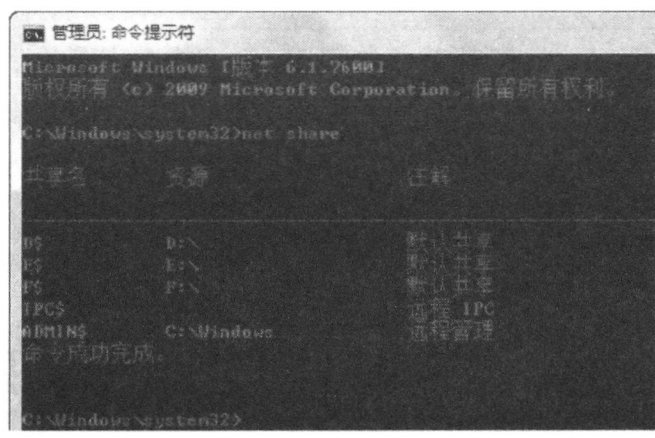
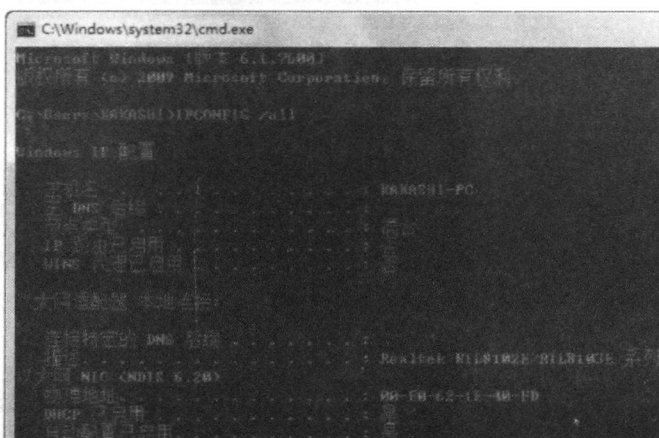
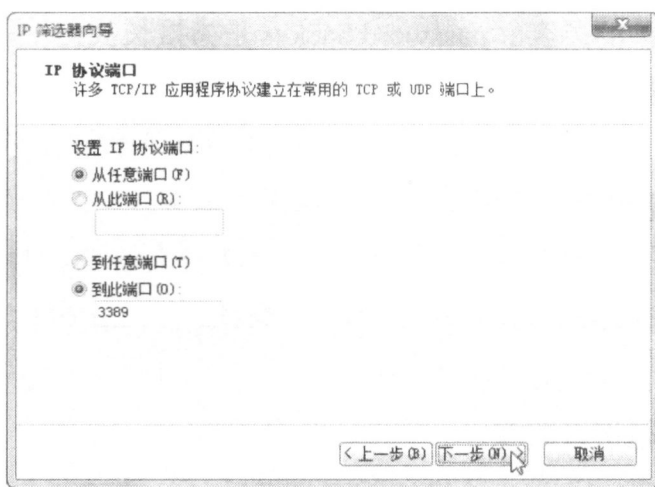
第17章

加强网络支付工具的安全 / 317

- 17.1 防御黑客入侵支付宝账户 / 318
 - 17.1.1 保障支付宝账户的安全 / 318
 - 17.1.2 保障支付宝内资金的安全 / 321
- 17.2 防御黑客入侵网上银行 / 325
 - 17.2.1 定期修改登录密码 / 325
 - 17.2.2 设置预留验证信息 / 326
 - 17.2.3 使用“小e安全检测”系统 / 327
 - 17.2.4 安装防钓鱼安全控件 / 329
 - 17.2.5 使用电子口令卡保障账户安全 / 331
 - 17.2.6 使用工行 U 盾保障账户安全 / 331
- 17.3 防御黑客入侵财付通 / 332
 - 17.3.1 保障财付通账户的安全 / 332
 - 17.3.2 保障财付通资金的安全 / 336

从零开始认识黑客

如今，Internet 在人们的生活、工作和学习中起着十分重要的作用。但是，随之而来的却是 Internet 的安全问题越来越突出。在 Internet 中，有一类人，他们掌握高超的计算机技术，可能他们会维护 Internet 的安全，可能他们会破坏 Internet 的安全，这类人就是黑客——一个让绝大部分网络用户敬畏的人群。



知识要点

- 认识黑客
- 黑客的定位目标——IP 地址
- 黑客的专用通道——端口
- 黑客藏匿的首选地——系统进程
- 认识黑客常用的 DOS 命令

1.1 认识黑客

黑客是一类掌握超高计算机技术的人群。凭借着掌握的知识，他们既可以从事保护计算机和网络安全的工作，又可以选择入侵他人的计算机或者破坏网络，对于黑客而言，他们所做的事情总是带有一定的目的，也许是为了炫耀，也许是为了报复。

1.1.1 区别黑客与骇客

黑客的原意是指那些精通操作系统和网络技术，并利用其专业编制新程序的人。黑客所做的不是恶意破坏，他们是一群纵横于网络上的技术人员，热衷于科技探索、计算机科学研究。在黑客圈中，Hack 一词带有正面的意义，例如 system hack 是指熟悉操作系统的设计与维护的黑客；password hacker 是指擅长找出使用者密码的黑客；computer hacker 则是指通晓计算机，可让计算机乖乖听话的黑客。

而骇客则不一样，骇客是指利用所掌握的计算机技术，从事恶意破解商业软件、恶意入侵别人的网站或计算机等事务的人。

总的来说，黑客是一类主要负责维护计算机和网络的安全的人员，而骇客则是入侵他人计算机或者网络的人员。其实黑客与骇客本质上都是相同的，即闯入计算机系统/软件者。黑客和骇客并没有一个十分明显的界限，但随着两者含义越来越模糊，因此造成了黑客一词越来越接近骇客。

提示：认识红客

红客是英文单词 Honker 的中文音译，它代表着一种精神，即热爱祖国、坚持正义和开拓进取的精神。因此只要具备这种精神并热衷于计算机技术的人都可以成为 Honker。Honker 是 Hacker 中的一部分人，这部分人以维护国家利益为己任，不利用掌握的计算机和网络技术入侵自己国家的计算机或服务器。他们维护正义，为国争光。

1.1.2 成为黑客必须掌握的知识

用户若想成为黑客，并不是一朝一夕的事情，需要掌握大量的计算机专业知识和技术，如果只是掌握了基础的 DOS 命令和一两款远程控制工具是算不上黑客的。成为黑客必须掌握的知识包括：一定的英文水平、理解常用的黑客术语和网络安全术语、熟练使用常用 DOS 命令和黑客工具，以及掌握主流的编程语言以及脚本语言。

1. 一定的英文水平

黑客学习的计算机知识虽然主要来源于国内，但是却经常需要参考国外的相关资料和教程，而国外的资料和教程大多数为英文版本，因此就需要具有一定的英文水平，以确保能够看

懂国外的一些参考资料。

2. 理解常用的黑客术语和网络安全术语

在常见的黑客论坛中，经常会看到肉鸡、挂马和后门等词语，这些词语可以统称为黑客术语，如果不理解这些词语，则在与其他黑客交流技术或经验时就会有障碍。除了掌握相关的黑客术语之外，作为黑客，还需要掌握 TCP / IP 协议、ARP 协议等网络安全术语。

3. 熟练使用常用DOS命令和黑客工具

常用 DOS 命令是指在 DOS 环境下使用的一些命令，主要包括 Ping、netstat 以及 net 命令等。利用这些命令可以实现对应不同的功能，如，利用使用 Ping 命令可以获取目标计算机的 IP 地址以及主机名。而黑客工具则是指用来远程入侵或者查看是否存在漏洞的工具，例如使用 X-Scan 可以查看目标计算机是否存在漏洞，利用 EXE 捆绑器可以制作带木马的其他应用程序。

4. 掌握主流的编程语言以及脚本语言

从 Internet 中获取的黑客工具通常是其他黑客利用指定类别的编程语言（C++、Java 等）制作的，如果想要成为一名黑客高手，仅仅使用别人制作的工具是不够的，需要具有创新精神，通过掌握主流的 C++、Java 等编程语言来编制属于自己的黑客工具。同时还需要掌握 JavaScript，VBScript 等脚本语言，用于自己编写脚本，实现脚本入侵。

提示：认识黑客攻击的目的

黑客攻击目标计算机或服务器的目的主要有 3 个，分别是盗取账户密码、恶作剧以及炫耀高超的计算机技术，其中盗取账户密码属于违法的行为，用户一定不要使用本书介绍的黑客工具去入侵他人的计算机。

1.2 黑客的定位目标——IP 地址

IP 是 Internet Protocol 的简称，中文简称为“网协”，它是为计算机网络相互连接进行通信而设计的协议。无论任何操作系统，只要遵守 IP 协议就可以与 Internet 互联互通。而 IP 地址则是为了识别 Internet 或局域网中的电脑所产生的 32bit（bit 的中文名称是位，音译为比特）地址。下面就介绍什么是 IP 地址以及 IP 地址的分类。

1.2.1 认识 IP 地址

IP 地址其实就与现实生活中的住址一样，如果要将信件寄送给指定的好友，就必须知道该好友的住址，这样才能确保邮递员能够准确地将信件送到好友手中。在 Internet 中，计算机之间的通信就类似于现实生活中用户之间的通信，若想将信息发送给指定的计算机，就必须知

道目标计算机的 IP 地址。

IP 地址默认是利用二进制来表示的，目前的 IP 地址的长度为 32bit，例如采用二进制形式的 IP 地址是 11000000101010000000000100100101，这么长的 IP 地址处理起来会非常麻烦。因此为了方便使用，IP 地址经常被记为十进制形式的数字，分为 4 段，每段包括 8 位，并且在中间使用句点符号“.” 隔开，这样上面的 IP 地址可以写成 192.168.1.32。这种记法叫做“点分十进制表示法”，与一长串的 1 和 0 相比，利用点分十进制表示法表示的 IP 地址更容易被记住。

1.2.2 IP 地址的分类

在 Internet 中，每个 IP 地址都包括两个标识码（ID），它们分别是网络标识码和主机标识码。网络 ID 能够告诉用户计算机所处的特定网络，而主机 ID 则用来区分该网络中的多台计算机。

根据 IP 地址中网络 ID 与主机 ID 表示的不同数据段，可以将 IP 地址划分为 A、B、C、D 和 E 类。这 5 类 IP 地址的定义方式如表 1-1 所示。

表 1-1 IP 地址的分类及定义

地址类别	定义
A 类	第 1 段为网络地址，第 2 ~ 4 段为主机地址。网络 ID 的第 1 位必须是 0，因此该类 IP 地址中网络 ID 的长度为 8 位，主机 ID 的长度为 24 位，该类 IP 地址范围为 1.0.0.1 ~ 126.255.255.254，其子网掩码为 255.0.0.0
B 类	第 1 ~ 2 段为网络地址，第 3 ~ 4 段为主机地址。网络地址的前 2 位必须是 10，因此该类 IP 地址中网络 ID 的长度为 16 位，主机 ID 的长度为 16 位，该类 IP 地址范围为 128.1.0.1 ~ 191.254.255.254，其子网掩码为 255.255.0.0
C 类	第 1 ~ 3 段为网络地址，第 4 段为主机地址。网络地址的前 3 位必须是 110，因此该类 IP 地址中网络 ID 的长度为 24 位，主机 ID 的长度为 8 位，该类 IP 地址范围为 192.0.1.1 ~ 223.255.254.254，其子网掩码为 255.255.255.0
D 类	该类 IP 地址的第一个字节以 1110 开始，它是一个专门保留的地址，并不指向特定的网络。目前这类地址被用在多点广播（Multicast）中，其地址范围 224.0.0.1 ~ 239.255.255.254
E 类	该类 IP 地址以 11110 开始，为将来使用保留

除了以上介绍的 5 种 IP 地址以外，还有全 0 和全 1 的 IP 地址，其中全 0 的 IP 地址（0.0.0.0）是指当前网络，全 1 的 IP 地址（255.255.255.255）是广播地址（现在 CISCO 上可以使用全 0 地址）。

提示：认识 IPv4 地址与 IPv6 地址

IPv 是 Internet Protocol version 的简称，中文译为“网际协议版本”，目前 Internet 中常用的网际协议版本有 IPv4 和 IPv6 两个。随着 Internet 中电脑数量越来越多，IPv4 采用 32bit 地址长度，只能容纳大约 43 亿台电脑，而 IPv6 采用了 128bit 地址长度，几乎可以不受限制地提供 IP 地址。按保守方法估算，IPv6 可以在全球每平方米的面积上，除了能够提供现有的地址数量之外，还可以增加大约 1000 个地址。