网络安全专家
Network security experts

# 暗战小强

# 黑客攻防入门全程图解

武新华 冯世雄 李防 等编著
飞思科技产品研发中心 监制

披露黑客练功全过程
识破黑客入侵小伎俩
轻松实现从菜鸟到大虾
练就黑客终极必杀技

DVD 小强 视频大讲堂

共6小时40课高品质语音教学视频
额外超值赠送2.5小时28课新视频

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络安全专家
Network security experts

# 暗战强人

# 黑客攻防

# 程图解

武新华 冯世雄 李防 等编著
飞思科技产品研发中心 监制

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

# 内容简介

本书以配图、图释、标注、指引线框等丰富的图解手段，辅以浅显易懂的语言，不但介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具，而且详细地讲述了防御黑客攻击的方法，并对入侵过程中常见问题进行必要的说明与解答。全书共分为15章，主要包括：如何成为一名黑客，黑客需要掌握的基本知识，网络安全技术基础，加密解密技术基础，软件破解技术基础，防不胜防的病毒攻击，揭秘木马技术，恶意网页代码技术，漏洞攻击技术，跳板、后门与日志的清除，系统清理与间谍软件清除，防火墙和入侵检测技术，网络通信工具的攻击与防范，系统账号入侵与防范，系统安全防御实战等内容。

随书所附的DVD光盘提供了多种网络安全及黑客工具的教学视频，汇集了众多黑客高手的操作精华。

本书内容丰富、图文并茂、深入浅出，不仅适用于广大网络爱好者，而且适用于网络安全从业人员及网络管理员。



**图书在版编目（CIP）数据**

暗战强人. 黑客攻防入门全程图解 / 武新华等编著.—北京：电子工业出版社，2009.9
（网络安全专家）
ISBN 978-7-121-09175-9

Ⅰ. 暗… Ⅱ.武… Ⅲ.计算机网络－安全技术－图解 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2009）第 107795 号

责任编辑：杨　鸽
印　　刷：北京东光印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×1092　1/16　印张：26　字数：665.6 千字
印　　次：2009 年 9 月第 1 次印刷
印　　数：4 000 册　　定价：49.80 元（含视频 DVD 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

# 前　言

随着网络攻击手段的日趋复杂，有组织、有预谋、有目的、有针对性、多样化的攻击和破坏活动频繁发生，攻击点也越来越趋于集中和精确，攻击破坏的影响面不断扩大并产生连环效应，就势必需要构筑一种主动的安全防御，才有可能最大限度地有效应对攻击方式的变化。本系列图书依托作者长期从事网络安全管理苦心积累的心得与一线拼杀的经验，以深入体验来揭示实战精要，带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。

下面，我们为大家简要介绍本套丛书的特点、学习方法及我们提供的服务。

## “暗战强人”系列的组成及特色

本套“暗战强人”系列共包含了3本图书，即《暗战强人：黑客攻防入门全程图解》、《暗战强人：黑客及反黑客工具快速精通》、《暗战强人：黑客攻防实战高级演练》。关于3本图书的说明如下。

| 图书组成 | 特　色 | 适合人群 | 增值服务 |
| --- | --- | --- | --- |
| 暗战强人：黑客攻防入门全程图解 | ● 内容合理：精选入门读者最迫切需要掌握的知识点，构成一个实用、完整的知识体系<br>● 举一反三：本书力求通过一个知识点的讲解让读者彻底理解和掌握类似场合的应对思路<br>● 高效模式：全程图解模式可彻底克服攻防操作的学习障碍 | 没有多少电脑操作基础的广大读者、需要获得数据保护的日常办公人员、广大网友等 | 随书所附的DVD光盘提供了多种攻防实战的教学视频，汇集了众多黑客高手的操作精华，通过增加读者对主流攻防手法感性认识的方式，使读者实现高效学习 |
| 暗战强人：黑客及反黑客工具快速精通 | ● 理论+实战、图文+视频=让读者不会也会！作者采用最为通俗易懂的图文解说，即使是电脑新手也能理解<br>● 任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法<br>● 最新的黑客技术盘点，让读者实现“先下手为强”<br>● 攻防互参的防御方法，全面确保用户的网络安全 | 喜欢钻研黑客技术但编程基础薄弱的读者、网络管理员、广大网友等 | |
| 暗战强人：黑客攻防实战高级演练 | ● 技术内容新颖：网络攻击手法日新月异，导致已有图书时效性降低，本书力求摒弃过时内容并考虑前瞻性<br>● 知识体系完整，注重攻防操作与原理、思路的印证，以培养读者举一反三、可灵活应对未来攻击的分析与实践能力<br>● 案例丰富，注重时效，克服其他图书因无法再现攻防现场而泛泛而谈的弊病 | 具备一定黑客知识基础和工具使用基础的读者、网络管理人员、喜欢研究黑客技术的网友等 | |

针对不同的读者群和不同的读者需求，上述3本书可使读者有选择、有针对性地根据自己的阅读喜好和操作水平进行选择。

## 关于本书

本书以配图、图释、标注、指引线框等丰富的图解手段，辅以浅显易懂的语言，不但介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具，而且详细地讲述了防御黑客攻击的方法，可使读者在了解基本网络安全知识的前提下，轻松而快速地掌握基本的反黑知识、工具和修复技巧，在遇到别有用心者的入侵时能够不再茫然无措。

## 本书特色

本书以情景教学、案例驱动与任务进阶为鲜明特色，在书中可以看到一个个生动的情景案例。通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 高效模式：全程图解模式可彻底克服攻防操作的学习障碍。
- 内容合理：精选入门读者最迫切需要掌握的知识点，构成一个实用、完整的知识体系。
- 举一反三：本书力求通过一个知识点的讲解，让读者彻底理解和掌握类似场合的应对思路。

## 本书适合人群

本书作为一本面向广大网络爱好者的速查手册，适合如下读者学习使用：

- 电脑爱好者、提高者；
- 具备一定黑客知识基础和工具使用基础的读者；
- 网络管理人员；
- 喜欢研究黑客技术的网友；
- 大、中专院校相关学生。

## 本书作者

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验。

本书编写情况：冯世雄负责第 1、2、3、4 章，李防负责第 5、6 章，王肖苗负责第 7 章，孙世宁负责第 8 章，杨平负责第 9 章，段玲华负责第 10 章，李伟负责第 11 章，王英英负责第 12 章，陈艳艳负责第 13 章，张晓新负责第 14 章，郑静负责第 15 章，最后由武新华通审全稿。我们虽满腔热情，但限于自己的水平，书中仍难免有失误、遗漏之处，因此，还望大家以宽容为本，慈悲为怀，本着共同探讨、共同进步的平和心态来阅读本书。作者随时恭候您提出的宝贵意见。

## 最后，需要提醒大家的是：

根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记，切记！

编 著 者

联系方式

咨询电话：（010）88254160　88254161-67

电子邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn　　http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

# 目　录


第 1 章　如何成为一名黑客 …… 1
1.1　黑客的前世今生 …… 2
1.1.1　黑客的由来 …… 2
1.1.2　黑客的现状 …… 2
1.2　成为黑客需要哪些知识 …… 3
1.2.1　学习编程 …… 3
1.2.2　使用操作系统 …… 4
1.2.3　掌握计算机网络 …… 5
1.2.4　培养学习的态度 …… 6
1.3　创建安全测试环境 …… 6
1.3.1　安全测试环境的概念 …… 6
1.3.2　虚拟机软件概述 …… 7
1.3.3　用 VMware 创建虚拟系统 …… 8
1.3.4　虚拟机工具安装 …… 16
1.3.5　在虚拟机上架设 IIS 服务器 …… 18
1.3.6　在虚拟机中安装网站 …… 20
1.4　专家点拨：常见问题与解答 …… 22
1.5　总结与经验积累 …… 22

第 2 章　黑客需要掌握的基础知识 …… 23
2.1　黑客知识基础 …… 24
2.1.1　进程、端口和服务概述 …… 24
2.1.2　Windows 命令行概述 …… 28
2.1.3　DOS 系统常用命令 …… 32
2.1.4　Windows 注册表 …… 40
2.1.5　Windows 常用服务配置 …… 41
2.2　网络应用技术 …… 45
2.2.1　TCP/IP 协议簇 …… 45
2.2.2　IP 协议 …… 46
2.2.3　ARP 协议 …… 47
2.2.4　ICMP 协议 …… 48
2.3　专家点拨：常见问题与解答 …… 50
2.4　总结与经验积累 …… 50

第 3 章　网络安全技术基础 …… 51
3.1　网络攻击和防御 …… 52
3.1.1　黑客攻击流程 …… 52
3.1.2　网络防御 …… 53
3.2　信息收集概述 …… 55
3.2.1　Google Hack …… 55
3.2.2　使用系统命令 …… 56
3.3　网络扫描技术 …… 57
3.3.1　ping 扫描技术 …… 57
3.3.2　端口扫描技术 …… 57
3.3.3　漏洞扫描技术 …… 58
3.4　黑客常用扫描嗅探软件 …… 59
3.4.1　Nmap 的使用 …… 59
3.4.2　X-Scan 的使用 …… 60
3.4.3　Sniffer 的使用 …… 63
3.4.4　IceSword 的使用 …… 65
3.5　专家点拨：常见问题与解答 …… 68
3.6　总结与经验积累 …… 68

第 4 章　加密和解密技术基础 …… 69
4.1　密码学概述 …… 70
4.1.1　密码体制分类 …… 70
4.1.2　分组密码 …… 71
4.1.3　密码算法 …… 72
4.2　加密和解密技术 …… 72
4.2.1　系统账户密码的安全 …… 73
4.2.2　使用 Windows 的 EFS 加密文件 …… 75
4.2.3　使用 LC5 破解密码 …… 77
4.3　使用第三方软件对文件加密 …… 79
4.3.1　Folder Vault 加密技术 …… 79
4.3.2　SecuKEEPER 加密技术 …… 80
4.4　破解 MD5 加密实例 …… 84
4.4.1　本地破解 MD5 …… 84
4.4.2　在线破解 MD5 …… 86
4.5　专家点拨：常见问题与解答 …… 87
4.6　总结与经验积累 …… 87

第 5 章　软件破解技术基础 …… 89
5.1　软件破解基础 …… 90

5.1.1 软件保护 …… 90
5.1.2 反汇编概述 …… 90
5.1.3 反汇编 Hello World 程序实例 …… 91
5.2 IDA Pro 反汇编工具 …… 93
5.2.1 IDA Pro 介绍 …… 93
5.2.2 IDA Pro 使用实例 …… 95
5.3 W32Dasm 静态分析工具 …… 96
5.3.1 W32Dasm 的介绍 …… 96
5.3.2 W32Dasm 的使用实例 …… 97
5.4 软件破解使用工具 …… 101
5.4.1 十六进制编辑器 UltraEdit …… 101
5.4.2 注册表监视器 Regshot …… 102
5.4.3 脱壳工具 ProcDump …… 104
5.5 专家点拨：常见问题与解答 …… 105
5.6 总结与经验积累 …… 105

第 6 章 防不胜防的病毒攻击 …… 107
6.1 病毒概述 …… 108
6.1.1 什么是病毒 …… 108
6.1.2 病毒的工作原理 …… 110
6.2 病毒分析与自制 …… 111
6.2.1 经典病毒分析 …… 111
6.2.2 自制脚本病毒 …… 114
6.3 手动查杀病毒 …… 115
6.3.1 查看系统进程 …… 115
6.3.2 搜索注册表 …… 116
6.3.3 删除病毒 …… 117
6.4 使用杀毒软件 …… 118
6.4.1 NOD32 杀毒软件 …… 119
6.4.2 江民杀毒软件 …… 122
6.4.3 金山毒霸杀毒软件 …… 126
6.5 专家点拨：常见问题与解答 …… 131
6.6 总结与经验积累 …… 131

第 7 章 揭秘木马技术 …… 133
7.1 木马概述 …… 134
7.1.1 什么是木马 …… 134
7.1.2 木马原理概述 …… 135
7.2 木马启动技术 …… 136

7.2.1 用注册表启动木马 …… 136
7.2.2 系统服务启动木马 …… 137
7.2.3 系统配置文件启动木马 …… 137
7.3 常见的木马档案 …… 138
7.3.1 木马的伪装与隐藏 …… 138
7.3.2 Winsock 介绍 …… 140
7.4 常见的木马类型 …… 141
7.4.1 合并端口木马 …… 141
7.4.2 ICMP 木马 …… 142
7.4.3 反弹端口型木马 …… 142
7.4.4 原始套接字木马 …… 145
7.5 木马检测与清除 …… 145
7.5.1 手动检测木马 …… 145
7.5.2 木马的清除步骤 …… 146
7.5.3 木马的预防与清除 …… 147
7.6 木马攻击实例 …… 160
7.6.1 准备工作 …… 160
7.6.2 木马植入 …… 166
7.7 专家点拨：常见问题与解答 …… 168
7.8 总结与经验积累 …… 169

第 8 章 恶意网页代码技术 …… 171
8.1 网页恶意代码概述 …… 172
8.1.1 什么是网页恶意代码 …… 172
8.1.2 网页恶意代码的特点 …… 172
8.2 网页恶意代码攻击的形式 …… 173
8.2.1 网页恶意代码脚本 …… 174
8.2.2 网页恶意代码攻击 …… 176
8.3 恶意网页代码的修复与防范 …… 184
8.3.1 网页恶意代码的修复 …… 184
8.3.2 网页恶意代码的防范 …… 193
8.4 专家点拨：常见问题与解答 …… 196
8.5 总结与经验积累 …… 197

第 9 章 漏洞入侵技术 …… 199
9.1 系统漏洞基础 …… 200
9.1.1 系统漏洞概述 …… 200
9.1.2 常见系统漏洞 …… 200
9.2 利用 Unicode 漏洞实施入侵 …… 203

9.3 IIS 漏洞入侵 …… 209
9.4 SAM 数据库漏洞入侵 …… 212
9.5 IPC$漏洞 …… 214
9.5.1 IPC$漏洞概述 …… 214
9.5.2 IPC$漏洞入侵 …… 215
9.6 SQL 注入实例 …… 219
9.6.1 手工注入攻击 …… 219
9.6.2 NBSI 2.5 注入 …… 221
9.7 专家点拨：常见问题与解答 …… 224
9.8 总结与经验积累 …… 224

第 10 章 跳板、后门与日志的清除 …… 225
10.1 跳板与代理服务器 …… 226
10.1.1 代理服务器概述 …… 226
10.1.2 跳板概述 …… 227
10.1.3 轻松设置代理服务器 …… 227
10.1.4 自己动手制作一级跳板 …… 228
10.2 克隆账号和后门技术 …… 230
10.2.1 实现手工克隆账号 …… 231
10.2.2 命令行方式下制作后门账号 …… 234
10.2.3 克隆账号工具 …… 237
10.2.4 用 Wollf 留下木马后门 …… 238
10.2.5 简析 SQL 后门技术 …… 239
10.3 巧妙清除日志文件 …… 240
10.3.1 利用 elsave 清除日志 …… 240
10.3.2 手工清除服务器日志 …… 241
10.3.3 用清理工具清除日志 …… 243
10.4 恶意进程的追踪与清除 …… 244
10.4.1 区分进程和线程 …… 244
10.4.2 查看、关闭和重建进程 …… 245
10.4.3 隐藏进程和远程进程 …… 248
10.4.4 消灭潜藏在自己机器中的病毒进程 …… 251
10.5 专家点拨：常见问题与解答 …… 252
10.6 总结与经验积累 …… 253

第 11 章 系统清理与间谍软件清除 …… 255
11.1 间谍软件概述 …… 256
11.1.1 运用 Spybot 清除隐藏的间谍 …… 256
11.1.2 运用 Ad-Aware 拦截间谍广告 …… 259

11.1.3 对潜藏的“间谍”学会说“不” …… 261
11.2 金山系统清理专家 …… 264
11.2.1 查杀恶意软件 …… 264
11.2.2 修复 IE 浏览器 …… 265
11.2.3 启动项管理 …… 266
11.2.4 进程管理 …… 266
11.2.5 清除历史记录 …… 267
11.2.6 其他特色功能的概述 …… 268
11.3 瑞星卡卡网络守护神 …… 271
11.3.1 查杀流行木马 …… 271
11.3.2 实现漏洞扫描与修复 …… 272
11.3.3 实现系统修复 …… 273
11.4 奇虎 360 保险箱 …… 274
11.4.1 修复系统漏洞 …… 274
11.4.2 查杀恶意插件 …… 275
11.4.3 对系统进行全面诊断与修复 …… 276
11.4.4 免费查杀病毒 …… 276
11.5 反黑精英 Anti Trojan Elite …… 277
11.5.1 系统设置 …… 277
11.5.2 实施监控 …… 279
11.5.3 实施扫描 …… 280
11.6 专家点拨：常见问题与解答 …… 282
11.7 总结与经验积累 …… 283

**第 12 章 防火墙和入侵检测技术** …… 285
12.1 防火墙技术基础 …… 286
12.1.1 防火墙概述 …… 286
12.1.2 防火墙的应用 …… 286
12.2 入侵检测 …… 300
12.2.1 入侵检测概述 …… 300
12.2.2 入侵检测原理 …… 301
12.2.3 入侵检测的分类 …… 303
12.2.4 RealSecure 系统介绍 …… 304
12.3 专家点拨：常见问题与解答 …… 305
12.4 总结与经验积累 …… 306

**第 13 章 网络通信工具的攻击与防范** …… 307
13.1 腾讯 QQ 的攻击 …… 308
13.1.1 腾讯 QQ 的攻击原理 …… 308

13.1.2 聊天记录的攻击 …… 309
13.2 腾讯 QQ 的密码攻击与防范 …… 310
13.2.1 盗取 QQ 的密码 …… 310
13.2.2 QQ 密码保护 …… 315
13.3 “QQ 信息炸弹”的攻击与防范 …… 329
13.4 MSN 的攻击与防范 …… 333
13.4.1 Msn Messenger Hack 盗号揭秘 …… 333
13.4.2 用 MessenPass 查看本地密码 …… 334
13.4.3 用 MSN Messenger Keylogger 查看密码 …… 335
13.4.4 MSN 密码的保护 …… 335
13.5 专家点拨：常见问题与解答 …… 339
13.6 总结与经验积累 …… 341

第 14 章 系统账号入侵与防范 …… 343
14.1 Windows 系统账号与口令 …… 344
14.1.1 破解 BIOS 开机口令 …… 344
14.1.2 更改与伪装 Administrator 账号 …… 346
14.1.3 破解 Windows 系统管理员口令 …… 350
14.1.4 识破混入管理员组的 Guest 账号 …… 350
14.1.5 Guest 账号权限管理 …… 352
14.1.6 伪装账户的破解与防范对策 …… 354
14.1.7 实现 SAM 跨系统攻防 …… 357
14.1.8 建立隐藏账号 …… 359
14.2 Windows 系统本地物理攻防 …… 364
14.2.1 绕过 Windows 系统的身份认证 …… 364
14.2.2 星号密码查看器 …… 368
14.2.3 设置 Windows 自动登录 …… 369
14.2.4 绕过防火墙 …… 369
14.3 专家点拨：常见问题与解答 …… 373
14.4 总结与经验积累 …… 374

第 15 章 系统安全防御实战 …… 375
15.1 建立系统漏洞防御体系 …… 376
15.1.1 扫描系统可疑漏洞 …… 376
15.1.2 修补系统漏洞 …… 378
15.1.3 设置 Web 服务安全 …… 383
15.1.4 监视系统操作进程 …… 385
15.1.5 实例：免费网络防火墙 ZoneAlarm …… 388
15.2 实战数据恢复 …… 391

15.2.1 什么是数据恢复 …… 391
15.2.2 造成数据丢失的原因 …… 392
15.2.3 EasyRecovery 数据恢复工具 …… 392
15.2.4 简洁易上手的恢复工具 FinalData …… 395
15.3 防病毒软件使用实战 …… 396
15.3.1 瑞星 2009 使用实战 …… 396
15.3.2 卡巴斯基使用实战 …… 398
15.4 专家点拨：常见问题与解答 …… 400
15.5 总结与经验积累 …… 401

# 第1章 如何成为一名黑客

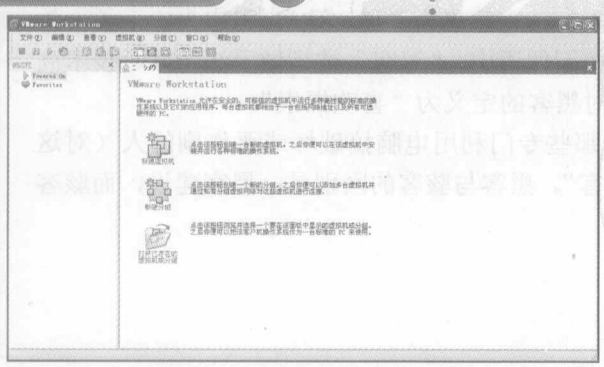
## 本章精粹

- 黑客的前世今生
- 成为黑客需要哪些知识
- 创建安全测试环境

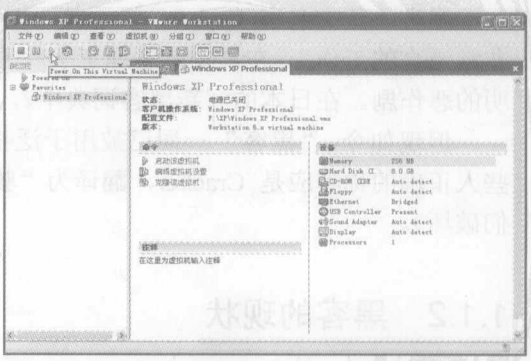
## 内容介绍

在本章中主要介绍了黑客的一些基本概念，让读者掌握黑客的由来、黑客的发展历史，以及黑客的现状，为读者今后学习黑客知识打下坚实的基础。

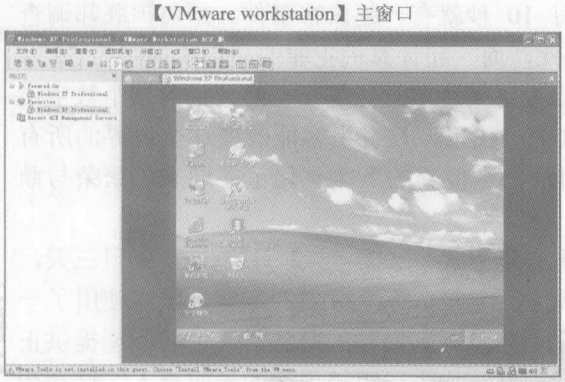
## 视频链接



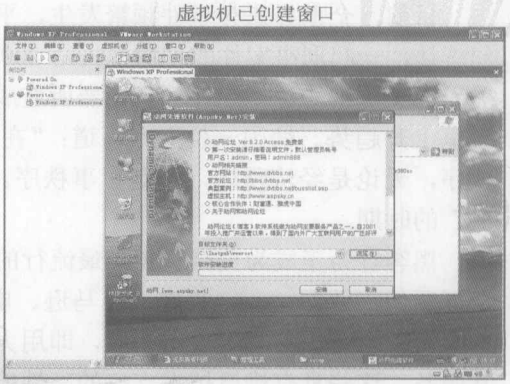
【VMware workstation】主窗口



虚拟机已创建窗口



虚拟机操作系统



【动网先锋软件（Aspsky.Net）安装】对话框

# 01 如何成为一名黑客

随着信息时代的发展和网络的普及，越来越多的人走近了网络，然而人们在享受网络带来便利的同时，也时刻面临着黑客残酷攻击的危险。下面我们就来了解黑客是如何成长，如何攻击计算机的，从而做到有力的防范，避免遭到损失。

## 1.1 黑客的前世今生

受影视剧的影响，黑客往往被渲染成了一个恐怖而又神秘的群体，能随心所欲地进入别人的计算机系统，盗取宝贵的资料，并且还可以使别人在不知不觉的情况下中招。这样，就促使很多电脑新手对黑客技术产生了崇拜心理，千方百计地想学习有关黑客的知识，甚至会断章取义做出一些无法想象的事情，导致很可怕的后果。

### 1.1.1 黑客的由来

黑客，英文名字 hacker，源于英语动词 hack，意思为“劈、砍”，引申为“干了一件非常漂亮的工作”。在早期麻省理工学院的校园俚语中，“黑客”被指做手法巧妙、技术高明的恶作剧。在日本的《新黑客词典中》，对黑客的定义为“喜欢探索”。

但现如今，“黑客”一词已被用于泛指那些专门利用电脑搞破坏或恶作剧的人（对这些人正确的称呼应是 Cracker，翻译为“骇客”。黑客与骇客的区别是：黑客建设，而骇客们破坏）。

### 1.1.2 黑客的现状

目前，全世界黑客事件频繁发生，平均每 10 秒就有一起黑客事件。据美国联邦调查局统计，一起刑事案件的平均损失是 2000 美元，而一起计算机犯罪的平均损失则为 50 万美元；美国平均每年因计算机犯罪所造成的损失可高达 75 亿美元。而且目前这个数字还在呈上升趋势。德国一位专家写道：“在未来的时代里，只有黑客能改变这个世界的所有秩序，无论是经济秩序，还是军事秩序。”目前，全世界的黑客文化正在迎来“繁荣与鼎盛”的时期。

黑客行为正成为美国青少年最流行的休闲娱乐方式。2000 年 2 月 7、8、9 日三天，全球顶级商业网站——雅虎、亚马逊、电子港湾、CNN 等纷纷陷入瘫痪，黑客使用了一种叫做“拒绝服务式”攻击手段，即用大量无用信息阻塞网站的服务器，使其不能提供正常服务。这些具有雄厚技术支持的高性能商业网站，均未能阻挡黑客的长驱直入。这次袭

击所造成的直接或间接的经济损失高达数十亿美元。随之而来的调查结果令全世界为之震惊，制造这起轰动世界的超级“黑客袭击事件”的竟然是一个貌不惊人、身材瘦小的“邻家男孩”——绰号为“黑手党男孩”（Mafiaboy）的 14 岁少年。男孩的邻居和朋友们几乎无法相信，这个平时沉默寡言、喜欢打篮球和玩计算机的小男孩竟然通过计算机造成了几百万甚至上亿美元的损失。而他只是通过卧室的一台普通电脑就制造了这一切。“黑手党男孩”的事件让人们第一次开始关注少年黑客的问题。同年 5 月，菲律宾学生奥内尔·古兹曼炮制出“爱虫”病毒，因这一病毒导致的电脑瘫痪所造成的损失高达 100 亿美元。

一家国际著名的网络安全研究机构的报告指出，“黑客行为正在全世界范围内流行，少年黑客越来越多，犯罪人员低龄化已成为计算机犯罪的突出特点。黑客行为已经变成了一种可供那些超级网虫们娱乐休闲的新方式。这一方面可以炫耀他们的技能，另一方面他们也从破坏中获得巨大的快感。仅从这两点来看，这和别的休闲方式并无本质区别。”美国一些青少年行为专家认为，黑客行为中所表现出的技术魔力、创造性、投入与奉献感，以及青少年对社会的不满、反叛及与社会的疏离，都是黑客行为在青少年中流行的原因。

对于很多青少年来说，黑客文化中那种“自由、反叛，以及侠客精神”具有很大的吸引力。这被一些美国心理学专家称做“罗宾逊心理综合症”。在美国，一个著名的黑客人物成为很多青少年崇拜的偶像。他五短身材、过肩的长发及连鬓胡子，不修边幅的打扮，看起来就像现代都市里的隐居人。他是颇具理想主义色彩的理查德·斯托曼。在很多黑客眼中，斯托曼被认为是有史以来最伟大的黑客。而他的目标就是打破束缚人们自由的数字鸿沟，建立“虚拟社会的乌托邦”。全世界反黑客、反病毒的斗争呈现出越来越激烈的趋势。

## 1.2 成为黑客需要哪些知识

要想成为一个技术高超的黑客，技术固然是最为重要的。但如何才能使自己从一只菜鸟转变为黑客呢？这其中又需要学些什么，做些什么？这些都是必须要了解的。

### 1.2.1 学习编程

首先，程序语言就是成为黑客的基础技能。不过，你只掌握一种语言的话，还不能算是一个黑客，充其量也只能算是一个程序员。黑客的进攻最重要是寻找和发现漏洞，因此你必须学会以独立于任何语言之上的概念性观念来思考每一件程序设计上的问题。也就是说，你必须要掌握多种不同的计算机语言。而 C 语言也是所有计算机语言中的最基础的语言了。

当然，除了 C 语言之外，你至少还要熟悉 C++或 Perl 等。而且除这些重要的常用语言之外，还需要能够灵活地运用语言的共性，以便遇到不同的情况时能更快地掌握新的语言。

程序设计语言是一种相当复杂的技术，在这里就不再提供完整的学习步骤了。但可以告诉大家一个很实用的学习方法，这也是几乎所有黑客自学的主要方法，希望大家通过这种方法能够更快地找到学习程序语言的方法和乐趣。

其实方法很简单：一是多读别人的程序代码，二是多写程序。学习程序就像临摹书法一样，刚开始只能去临摹书法家们的书法风格，久而久之就会练习出属于自己的风格了。学习程序也是如此，刚入门时我们需要去看一些专家们写的东西，并尝试着写一些自己的东西，然后继续读更多的，再写更多的，一直持续，直到能拥有属于自己的风格和特色。

对于菜鸟黑客而言，想要找到好代码是一件很困难的事情，因为适用于他们阅读和学习的大型程序代码少之又少。不过，现在免费提供的软件、程序设计工具和操作系统大都公开提供代码，这为菜鸟学习提供了很好资源。

## 1.2.2 使用操作系统

### 1. 操作系统概念

操作系统（Operating System，简称 OS）是一个管理电脑硬件和软件资源的程序，主要负责管理与配置内存、为系统资源供需优先次序、控制输入与输出设备、操作网络与管理文件系统等基本事务。操作系统是管理着计算机系统的全部硬件资源（包括软件资源及数据资源）；它控制程序的运行，改善人机界面；为其他应用软件提供支持，使计算机系统所有资源最大限度地发挥作用，为用户提供方便的、有效的、友善的服务界面。操作系统是一个庞大的管理控制程序，可从以下 5 个方面进行管理：进程与处理机管理、作业管理、存储管理、设备管理、文件管理。所有操作系统都具有并发性、共享性、虚拟性和不确定性这 4 个基本特征。

### 2. 常见操作系统

下面介绍一下经常接触到的操作系统。

1）嵌入式系统

嵌入式系统适用于某些功能简单版的 Linux 或其他操作系统。在一些情况下，操作系统会被看做是一个内置了固定应用的巨大泛用程序。在许多简单的嵌入系统中，所有操作系统就是指唯一的应用程序。

2）Linux 系统

Linux 操作系统的稳定性及网络的功能，是其他商业操作系统无法比拟的。另外，Linux 最大的特色在于源代码完全公开，在符合 GUN GPL（General Public License）的原则下，任何人都可自由取得、散布甚至修改源代码。

从 Linux 的本质上来讲，它主要负责控制硬件、管理文件系统、程序进程等，只是作为操作系统的核心。其内核并不负责提供用户强大的应用程序，如系统管理工具、网络工具、Office、多媒体等，这样的系统也无法发挥其强大功能。因此，很多用户无法利用这个系统更好地工作，于是便提出了以 Linux Kernel 为核心，再集成搭配各式各样的系统程序或应用工具程序组成一个完整操作系统，经过如此的组合，便推