

基础入门 | 工具使用 | 攻防技巧 | 实战演练

黑客技术新手、爱好者一定要看的**最佳工具书**

最新案例实战版

玩转

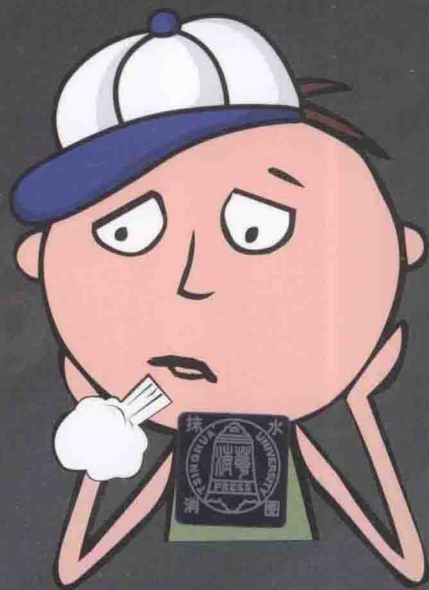
# 黑客攻防

## 从入门到精通

少侠 编著

PC、手机、Wi-Fi……

经典热门黑客攻防技术 **全搞定**



超值视频课程免费下载

清华大学出版社

介绍国内

玩转

# 黑客攻防 从入门到精通

少侠 编著

清华大学出版社  
北京

## 内 容 简 介

本书由易到难、循序渐进地介绍了黑客入侵攻击及防御黑客入侵攻击的基础知识及应用技巧,主要包括黑客入门基础知识、扫描和嗅探的实施与防范、防范与清除电脑病毒、防范与清除电脑木马、移动设备黑客攻击与防范、Wi-Fi 攻击与防范、文件加密与解密、Windows 系统漏洞入侵防范、局域网攻击与防范、账号盗取与安全防范、网站常见攻击方式、系统远程控制与反控制、网络代理与追踪、后门的创建与检测、黑客入侵检测、清理入侵痕迹、系统清理与间谍软件的清除、网络支付工具安全防范、系统和数据的备份与恢复共 19 章内容。本书重点在学习黑客入侵的基础上,掌握如何采取有效的防范措施,还介绍了移动设备与 Wi-Fi 等热点技术与应用。

本书适用于黑客技术初学者和爱好者,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和培训机构。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

### 图书在版编目(CIP)数据

玩转黑客攻防从入门到精通 / 少侠编著. —北京:清华大学出版社, 2015

ISBN 978-7-302-39867-7

I. ①玩… II. ①少… III. ①计算机网络—安全技术 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 080716 号

责任编辑:王金柱

封面设计:王翔

责任校对:闫秀华

责任印制:何羊

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, [c-service@tup.tsinghua.edu.cn](mailto:c-service@tup.tsinghua.edu.cn)

质量反馈:010-62772015, [zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

印刷者:北京富博印刷有限公司

装订者:北京市密云县京文制本装订厂

经 销:全国新华书店

开 本:190mm×260mm 印 张:27.5 字 数:704 千字

版 次:2015 年 6 月第 1 版 印 次:2015 年 6 月第 1 次印刷

印 数:1~3500

定 价:69.00 元

# 前言

如今网上购物、投资、理财等已经占据了很大的消费市场，财产的安全性也越来越重要，如果账户、密码被黑客截取，将会带来很大的损失。而计算机网络的普及、黑客工具的传播，使得只需简单的工具，就能够对一些疏于防范的电脑或终端进行攻击，并在受侵入的电脑或终端里为所欲为。当发现自己的密码被盗、资料被修改删除、硬盘变作一片空白之时，再想亡羊补牢，为时已晚。

## 本书内容

本书从“攻”、“防”两个不同的角度讲解黑客攻击手段的同时，介绍了相应的防范方法，图文并茂地再现了网络入侵与防御的全过程。本书内容涵盖了黑客入门基础知识、扫描和嗅探的实施与防范、电脑安全防范、移动设备黑客攻击与防范、Wi-Fi 攻击与防范、文件加密与解密、Windows 系统漏洞入侵防范、局域网攻击与防范、账号盗取与安全防范、网站常见攻击方式、系统远程控制与反控制、网络代理与追踪、后门的创建与检测、黑客入侵检测、清理入侵痕迹、系统清理与间谍软件的清除、网络支付工具安全防范、系统和数据的备份与恢复等，让读者在了解黑客如何攻击的同时学习到如何拒敌于千里的方法。

本书还在各章安排了实战演练案例，读者可以边学边练，提高实战技能。

## 本书特色

本书由浅入深地讲解了黑客攻击和防范的具体方法和技巧，通过具体形象的案例向读者展示了多种攻击方法和攻击工具的使用。通过完成实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升防范黑客的实战技能。

- 任务驱动，自主学习，理论+实战+图文=让读者快速精通。
- 讲解全面，轻松入门，快速打通初学者学习的重要关卡。
- 实例为主，易于上手，模拟真实工作环境，解决各种疑难问题。

本书以实例分析加案例剖解为主要脉络，以图文并茂、按图索骥方式详细讲解黑客的攻击手法和相应的网络安全管理防御技术，并采用案例驱动的写作方法，照顾初级读者，详细分析每一个操作案例，力求通过一个知识点的讲解，实现读者用更少的时间快速掌握黑客技术，理解和掌握类似场合的应对思路。



## 提供教学视频下载

为方便初学者尽快上手，节省学习时间，本书还录制了部分章节的教学视频，提供共 64 段教学视频操作录像，读者可在电脑上直接播放观看。视频下载地址：<http://pan.baidu.com/s/1c0gy51Y>。

## 本书适合人群

本书适合如下读者学习使用：

- 使用电脑的广大读者；
- 需要获得数据保护的日常办公人员；
- 热衷黑客技术的初学者及安全技术的爱好者；
- 网络管理人员、网吧工作人员。

由于时间紧迫，水平有限，书中难免存在疏漏和不当之处，敬请读者批评指正，在您使用本书的过程中如遇到问题，请联系 QQ：3113088。

编者

2015 年 3 月

# 目 录

第 1 章 黑客入门基础知识.....	1
1.1 认识黑客.....	1
1.1.1 白帽、灰帽及黑帽黑客.....	1
1.1.2 黑客、红客、蓝客及骇客.....	2
1.1.3 成为黑客必须掌握的知识.....	2
1.1.4 黑客常用术语.....	3
1.2 认识进程.....	5
1.2.1 查看进程.....	5
1.2.2 关闭和新建系统进程.....	6
1.3 认识端口.....	8
1.3.1 端口的分类.....	8
1.3.2 查看端口.....	10
1.4 认识 IP 地址.....	11
1.4.1 IP 地址概述.....	11
1.4.2 IP 地址的分类.....	12
1.5 黑客常用命令.....	13
1.5.1 测试物理网络的 Ping 命令.....	13
1.5.2 查看网络连接的 Netstat 命令.....	15
1.5.3 工作组和域的 Net 命令.....	17
1.5.4 23 端口登录的 Telnet 命令.....	20
1.5.5 传输协议 FTP 命令.....	20
1.5.6 查看网络配置的 IPconfig 命令.....	21
1.6 实战演练：开启和关闭端口.....	22
第 2 章 扫描和嗅探的实施与防范.....	25
2.1 在计算机中创建虚拟测试环境.....	25
2.1.1 安装 VMware 虚拟机.....	25
2.1.2 配置安装好的 VMware 虚拟机.....	28
2.1.3 安装虚拟操作系统.....	29
2.1.4 VMware Tools 安装.....	31

2.2	确定扫描目标	32
2.2.1	确定目标主机 IP 地址	32
2.2.2	了解网站备案信息	35
2.2.3	确定可能开放的端口和服务	36
2.3	扫描的实施与防范	39
2.3.1	扫描服务与端口	39
2.3.2	FreePortScanner 与 ScanPort 扫描工具	41
2.3.3	扫描器 X-Scan 查本机隐患	43
2.3.4	用 ProtectX 实现扫描的反击与追踪	49
2.4	嗅探的实施与防范	51
2.4.1	经典嗅探器 Iris	52
2.4.2	捕获网页内容的艾菲网页侦探	54
2.4.3	使用影音神探嗅探在线视频地址	55
2.5	运用工具实现网络监控	60
2.5.1	运用网络执法官实现网络监控	60
2.5.2	运用 Real Spy Monitor 监控网络	65
2.6	实战演练：用 SSS 扫描器扫描系统漏洞	70
<b>第 3 章 防范与清除电脑病毒</b>		<b>73</b>
3.1	病毒知识入门	73
3.1.1	计算机病毒的特点	73
3.1.2	病毒的三个基本结构	74
3.1.3	病毒的工作流程	75
3.2	制作简单的病毒	75
3.2.1	制作 Restart 病毒	75
3.2.2	制作 U 盘病毒	79
3.3	VBS 代码也可产生病毒	80
3.3.1	VBS 脚本病毒的特点	81
3.3.2	VBS 脚本病毒通过网络传播的几种方式	81
3.3.3	VBS 脚本病毒生成机	82
3.3.4	VBS 脚本病毒刷 QQ 聊天屏	84
3.3.5	如何防范 VBS 脚本病毒	85
3.4	宏病毒与邮件病毒的防范	86
3.4.1	宏病毒的判断方法	86
3.4.2	防范与清除宏病毒	87
3.4.3	全面防御邮件病毒	88
3.5	全面防范网络蠕虫	88



3.5.1	网络蠕虫病毒实例分析.....	88
3.5.2	网络蠕虫病毒的全面防范.....	89
3.6	用NOD32查杀病毒.....	91
3.7	实战演练：使用免费的专业防火墙 Zone Alarm.....	92
<b>第4章</b>	<b>防范与清除电脑木马.....</b>	<b>94</b>
4.1	认识木马.....	94
4.1.1	木马的发展历程.....	94
4.1.2	木马的组成.....	95
4.1.3	木马的分类.....	95
4.2	木马的伪装与生成.....	96
4.2.1	木马的伪装手段.....	96
4.2.2	使用文件捆绑器.....	98
4.2.3	制作自解压木马.....	101
4.2.4	制作CHM木马.....	102
4.3	木马的加壳与脱壳.....	105
4.3.1	使用ASPack进行加壳.....	106
4.3.2	使用“北斗压缩”对木马服务端进行多次加壳.....	107
4.3.3	使用PE-Scan检测木马是否加过壳.....	108
4.3.4	使用UnASPack进行脱壳.....	109
4.4	木马清除软件的使用.....	110
4.4.1	用木马清除专家清除木马.....	110
4.4.2	在“Windows进程管理器”中管理进程.....	113
4.5	实战演练：用木马清道夫清除木马.....	115
<b>第5章</b>	<b>移动设备黑客攻击与防范.....</b>	<b>117</b>
5.1	初识手机黑客.....	117
5.1.1	智能手机操作系统.....	117
5.1.2	常见的手机攻击类型.....	119
5.2	手机黑客基础知识.....	119
5.2.1	获取Android Root权限.....	119
5.2.2	Android手机备份功能.....	121
5.2.3	Android系统刷机.....	123
5.2.4	苹果手机越狱.....	124
5.3	手机蓝牙攻击曝光.....	126
5.3.1	蓝牙的工作原理.....	126
5.3.2	蓝劫攻击与防范.....	127



5.4	手机拒绝服务攻击曝光 .....	128
5.4.1	常见的手机拒绝服务攻击 .....	128
5.4.2	手机拒绝服务攻击防范 .....	129
5.5	手机电子邮件攻击曝光 .....	129
5.5.1	认识邮件在网络上的传播方式 .....	129
5.5.2	手机上常用的邮件系统 .....	130
5.5.3	手机电子邮件攻击与防范 .....	130
5.6	手机病毒与木马攻防 .....	131
5.6.1	手机病毒与木马带来的危害 .....	131
5.6.2	手机病毒防范 .....	132
5.7	手机加密技术 .....	133
5.7.1	手机开机密码设置与解密 .....	134
5.7.2	手机短信与照片加密 .....	137
5.8	手机支付安全防范 .....	143
5.8.1	手机支付的三种方式 .....	143
5.8.2	常用的 5 种手机支付 .....	144
5.8.3	手机支付安全问题 .....	145
5.9	手机优化及安全性能的提升 .....	146
5.9.1	“360 手机卫士”软件 .....	146
5.9.2	“腾讯手机管家”软件 .....	147
5.9.3	“金山手机卫士”软件 .....	147
5.10	实战演练：安卓手机刷机方法 .....	148
<b>第 6 章</b>	<b>Wi-Fi 攻击与防范 .....</b>	<b>150</b>
6.1	无线路由器基本设置 .....	150
6.1.1	无线路由器外观 .....	150
6.1.2	无线路由器参数设置 .....	151
6.1.3	设置完成重启无线路由器 .....	153
6.1.4	搜索无线信号连接上网 .....	154
6.2	傻瓜式破解 Wi-Fi 密码曝光及防范 .....	154
6.2.1	用“Wi-Fi 万能钥匙”软件破解 Wi-Fi 密码 .....	155
6.2.2	用“Wi-Fi 万能钥匙”在电脑上破解 Wi-Fi 密码 .....	156
6.2.3	防止“Wi-Fi 万能钥匙”破解密码 .....	157
6.3	Linux 下利用抓包破解 Wi-Fi 密码 .....	160
6.3.1	虚拟 Linux 系统 .....	160
6.3.2	破解 PIN 码 .....	162
6.3.3	破解 WPA 密码 .....	164

6.3.4 破解 WPA2 密码 .....	166
6.4 无线路由安全设置 .....	167
6.4.1 禁用 DHCP 功能 .....	167
6.4.2 无线加密 .....	168
6.4.3 关闭 SSID 广播 .....	168
6.4.4 设置 IP 过滤和 MAC 地址列表 .....	169
6.4.5 主动更新 .....	169
6.5 实战演练: 修改 Wi-Fi 连接密码 .....	170
<b>第 7 章 文件加密与解密 .....</b>	<b>171</b>
7.1 加密与解密基础知识 .....	171
7.1.1 认识加密与解密 .....	171
7.1.2 加密的通信模型 .....	171
7.2 7 种常见的加密解密类型 .....	172
7.2.1 RAR 压缩文件加密 .....	172
7.2.2 多媒体文件加密 .....	173
7.2.3 光盘加密 .....	177
7.2.4 Word 文件加密 .....	179
7.2.5 Excel 文件的加密与保护 .....	182
7.2.6 宏加密解密技术 .....	185
7.2.7 NTFS 文件系统加密数据 .....	188
7.3 系统密码攻防 .....	192
7.3.1 利用 Windows 7 PE 破解系统登录密码 .....	192
7.3.2 利用密码重置盘破解系统登录密码 .....	195
7.3.3 使用 SecureIt Pro 给系统桌面加把超级锁 .....	198
7.3.4 系统加密大师 PC Security .....	200
7.4 其他加密解密工具 .....	204
7.4.1 “加密精灵”加密工具 .....	204
7.4.2 MD 5 加密解密实例 .....	205
7.5 用“私人磁盘”隐藏大文件 .....	207
7.5.1 “私人磁盘”的创建 .....	208
7.5.2 “私人磁盘”的删除 .....	209
7.6 实战演练: 使用“常规选项”进行加密 .....	210
<b>第 8 章 Windows 系统漏洞入侵防范 .....</b>	<b>213</b>
8.1 系统漏洞基础知识 .....	213
8.1.1 系统漏洞概述 .....	213



8.1.2	Windows 系统常见漏洞.....	214
8.2	Windows 服务器系统入侵流程.....	217
8.2.1	入侵 Windows 服务器的流程.....	218
8.2.2	NetBIOS 漏洞攻防.....	219
8.3	DcomRpc 溢出工具.....	222
8.3.1	DcomRpc 漏洞描述.....	223
8.3.2	DcomRpc 入侵实战.....	224
8.3.3	DcomRpc 防范方法.....	225
8.4	用 MBSA 检测系统漏洞.....	227
8.4.1	检测单台计算机.....	227
8.4.2	检测多台计算机.....	228
8.5	实战演练：使用 Windows Update 修复系统漏洞.....	229
<b>第 9 章 局域网攻击与防范.....</b>		<b>231</b>
9.1	局域网安全介绍.....	231
9.1.1	局域网基础知识.....	231
9.1.2	局域网安全隐患.....	232
9.2	局域网攻击.....	233
9.2.1	网络剪刀手 Netcut.....	233
9.2.2	局域网 ARP 攻击工具 WinArpAttacker.....	235
9.2.3	网络特工.....	237
9.3	使用 LanSee 进行局域网监控.....	240
9.4	实战演练：长角牛网络监控机.....	242
<b>第 10 章 账号盗取与安全防范.....</b>		<b>248</b>
10.1	曝光“QQ 简单盗”盗取 QQ 密码.....	248
10.1.1	QQ 盗号曝光.....	248
10.1.2	防范“QQ 简单盗”.....	250
10.2	QQExplorer 在线破解 QQ 号码曝光.....	250
10.2.1	在线破解 QQ 号码.....	250
10.2.2	QQExplorer 在线破解及防范.....	251
10.3	用密码监听器揪出“内鬼”.....	251
10.3.1	“密码监听器”盗号披露.....	252
10.3.2	找出“卧底”拒绝监听.....	253
10.4	保护 QQ 密码和聊天记录.....	253
10.4.1	定期修改 QQ 密码.....	254
10.4.2	申请“QQ 密保”.....	255



10.4.3	加密聊天记录.....	256
10.5	实战演练：“好友号好好盗”盗取 QQ 号码.....	257
<b>第 11 章</b>	<b>网站常见攻击方式.....</b>	<b>259</b>
11.1	SQL 注入攻击.....	259
11.1.1	Domain（明小子）注入工具.....	259
11.1.2	“啊 D 注入”工具.....	264
11.1.3	对 SQL 注入漏洞的防御.....	267
11.2	Cookies 注入攻击.....	269
11.2.1	Cookies 欺骗简介.....	269
11.2.2	Cookies 注入工具.....	270
11.3	跨站脚本攻击.....	272
11.3.1	简单留言本的跨站漏洞.....	272
11.3.2	跨站漏洞的利用.....	275
11.3.3	对跨站漏洞的预防措施.....	279
11.4	实战演练：PHP 注入利器 ZBSI.....	281
<b>第 12 章</b>	<b>系统远程控制与反控制.....</b>	<b>283</b>
12.1	认识远程控制.....	283
12.1.1	远程控制的技术发展经历.....	283
12.1.2	远程控制的技术原理.....	283
12.1.3	远程控制的应用.....	284
12.2	远程桌面连接与协助.....	284
12.2.1	Windows 系统的远程桌面连接.....	285
12.2.2	Windows 系统远程关机.....	289
12.2.3	区别远程桌面与远程协助.....	290
12.3	用 WinShell 实现远程控制.....	290
12.3.1	配置 WinShell.....	291
12.3.2	实现远程控制.....	293
12.4	实战演练：用 QuickIP 进行多点控制.....	294
<b>第 13 章</b>	<b>网络代理与追踪.....</b>	<b>297</b>
13.1	代理服务器软件的使用.....	297
13.1.1	利用“代理猎手”找代理.....	297
13.1.2	防范远程跳板代理攻击.....	302
13.2	常见的黑客追踪工具.....	304
13.2.1	实战 IP 追踪技术.....	304
13.2.2	NeroTrace Pro 追踪工具的使用.....	305

13.3 实战演练：用 SocksCap32 设置动态代理 .....	308
<b>第 14 章 后门的创建与检测 .....</b>	<b>311</b>
14.1 认识后门 .....	311
14.1.1 后门的发展历史 .....	311
14.1.2 后门的分类 .....	312
14.2 账号后门技术 .....	313
14.2.1 使用软件克隆账号 .....	313
14.2.2 手动克隆账号 .....	314
14.3 系统服务后门技术 .....	317
14.3.1 使用 Instsrv 创建系统服务后门 .....	318
14.3.2 使用 Srvinstw 创建系统服务后门 .....	319
14.4 检测系统中的后门程序 .....	324
<b>第 15 章 黑客入侵检测 .....</b>	<b>325</b>
15.1 入侵检测概述 .....	325
15.2 基于网络的入侵检测系统 .....	325
15.2.1 包嗅探器和网络监视器 .....	326
15.2.2 包嗅探器和混杂模式 .....	326
15.2.3 基于网络的入侵检测：包嗅探器的发展 .....	327
15.3 基于主机的入侵检测系统 .....	327
15.4 基于漏洞的入侵检测系统 .....	329
15.4.1 运用“流光”软件进行批量主机扫描 .....	329
15.4.2 运用“流光”软件进行指定漏洞扫描 .....	331
15.5 Snort 入侵检测系统 .....	332
15.5.1 Snort 的系统组成 .....	333
15.5.2 Snort 命令介绍 .....	333
15.5.3 Snort 的工作模式 .....	334
15.6 实战演练：SaxII 入侵检测系统 .....	336
<b>第 16 章 清理入侵痕迹 .....</b>	<b>341</b>
16.1 黑客留下的脚印 .....	341
16.1.1 日志产生的原因 .....	341
16.1.2 为什么要清理日志 .....	344
16.2 清除服务器日志 .....	345
16.2.1 手工删除服务器日志 .....	345
16.2.2 使用批处理清除远程主机日志 .....	347

16.3	Windows 日志清理工具 .....	348
16.3.1	elsave 工具 .....	349
16.3.2	ClearLogs 工具 .....	350
16.4	清除历史痕迹 .....	351
16.4.1	清除网络历史记录 .....	352
16.4.2	使用 Windows 优化大师进行清理 .....	355
16.5	实战演练: 使用 CCleaner 清除系统垃圾 .....	356
<b>第 17 章</b>	<b>系统清理与间谍软件的清除 .....</b>	<b>360</b>
17.1	间谍软件防护实战 .....	360
17.1.1	间谍软件防护概述 .....	360
17.1.2	用 SpySweeper 清除间谍软件 .....	361
17.1.3	微软反间谍专家 Windows Defender 使用流程 .....	363
17.2	流氓软件的清除 .....	365
17.2.1	清理浏览器插件 .....	365
17.2.2	“金山系统清理专家”软件清除恶意软件 .....	367
17.2.3	流氓软件的防范 .....	368
17.3	常见的网络安全防护工具 .....	372
17.3.1	浏览器绑架克星 HijackThis .....	372
17.3.2	诺盾网络安全特警 .....	376
17.4	实战演练: 使用“360 安全卫士”软件对电脑进行防护 .....	379
<b>第 18 章</b>	<b>网络支付工具安全防范 .....</b>	<b>383</b>
18.1	加强支付宝的安全防护 .....	383
18.1.1	加强支付宝账户的安全防护 .....	383
18.1.2	加强“支付宝”内资金的安全防护 .....	387
18.2	加强“财付通”的安全防护 .....	390
18.2.1	加强“财付通”账户的安全防护 .....	390
18.2.2	加强“财付通”内资金的安全防护 .....	394
<b>第 19 章</b>	<b>系统和数据的备份与恢复 .....</b>	<b>397</b>
19.1	备份和还原操作系统 .....	397
19.1.1	使用“还原点”备份与还原系统 .....	397
19.1.2	使用 GHOST 备份与还原系统 .....	400
19.2	备份和还原用户数据 .....	404
19.2.1	使用驱动精灵备份与还原驱动程序 .....	404
19.2.2	备份与还原 IE 浏览器的收藏夹 .....	406
19.2.3	备份和还原 QQ 聊天记录 .....	409



19.2.4	备份和还原 QQ 自定义表情 .....	411
19.3	使用恢复工具来恢复误删除的数据 .....	414
19.3.1	使用 Recuva 来恢复数据 .....	414
19.3.2	使用 FinalData 来恢复数据 .....	419
19.4	实战演练：使用 FinalRecovery 恢复数据 .....	423

# 第 1 章

## 黑客入门基础知识

小呆：我的电脑最近老出问题，专家说中病毒了，所以想要学习一些黑客知识做预防，可是找了一些书籍，都不怎么能看懂，怎么办？

少侠：别担心，你了解过黑客常见的一些术语与命令吗？比如术语有肉鸡、木马，还有后门等等；命令有 ping 命令、netstat 命令、Net 命令等。

小呆：木马我知道，但是肉鸡和后门就不知道了。至于命令，我都不太了解。难道我要先了解这些吗？

少侠：是这样。学习黑客知识前，首先要了解黑客常见的术语与命令，不止这些，进程、端口、IP 地址等基础知识也是很必要的。

小呆：多谢少侠，那么我就先从这些基础知识开始学起吧。



### 1.1 认识黑客

信息已成为物质和能量以外维持人类社会的第三资源，它是未来生活中的重要介质。随着电脑的普及和因特网技术的迅速发展，黑客也随之出现了。

#### 1.1.1 白帽、灰帽及黑帽黑客

黑客的基本涵义是指拥有熟练电脑技术的人，但大部分人将“黑客”用于电脑侵入者。

白帽黑客是指有能力破坏电脑安全但不具恶意目的的黑客。白帽黑客一般有清楚的道德规范，并常常试图同企业合作去改善被发现的安全弱点。

灰帽黑客是指对于伦理和法律暧昧不清的黑客。

黑帽黑客和黑帽怪客经常用来区分黑帽黑客和一般（正面的）有理性的黑客。这个词自 1983 年开始流行，大概是由于采用了相似发音和对 safe cracker 的解释，并且理论化为一个犯罪和黑客的混成语。





## 1.1.2 黑客、红客、蓝客及骇客

黑客，最早源自英文 hacker，是指水平高超的电脑专家，尤其是程序设计人员，算是一个统称。

红客，是维护国家利益，不去利用网络技术入侵自己国家电脑，而是维护正义，为自己国家争光的黑客。

蓝客，是提倡爱国主义的黑客们，经常用自己的力量来维护网络的和平。

骇客，是 Cracker 的音译，就是“破解者”的意思。经常从事恶意破解商业软件、恶意入侵别人的网站等事务。

## 1.1.3 成为黑客必须掌握的知识

成为黑客，并不是一件简单的事情，不仅要熟练掌握一定的英文、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，而且要掌握主流的编程语言以及脚本。

### 1. 熟练掌握一定的英文

学习英文对于黑客来说非常重要，因为现在很多资料和教程都是英文版本，一个漏洞从发现到出现中文介绍，需要大约一个星期的时间，在这段时间内网络管理员就已经有足够的时间修补漏洞了，所以当看到中文介绍时，这个漏洞可能早就已经不存在了。因此学习黑客从一开始就要尽量阅读英文资料、使用英文软件，并且及时关注国外著名的网络安全网站。

### 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、后门和免杀等词语，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显得很吃力。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不同的功能，使用 Ping 命令可以获取目标计算机的 IP 地址以及主机名。而黑客工具则是指黑客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

程序语言可分为 5 类。

#### (1) Web Page Script Languages

就是网页代码，比如 HTML、JavaScript、CSS、ASP、PHP、XML 等。

#### (2) Interpreted Languages (解释型语言)

包括 Perl、Python、REBOL、Ruby 等，也常被称作 Script 语言，通常被用于和底层的操作系统沟通。这类语言的缺点是效率差、源代码外露，所以不适合用来开发软件产品，一般用于网页服