

图文详解，轻松掌握
电脑\智能手机全适用

黑客攻防 极速入门

黑客知识、常用命令与工具实战
电脑与手机黑客攻防秘技全曝光

张阮阮 等编著

知彼知己，百战不殆。

——《孙子兵法·谋攻篇》



机械工业出版社
China Machine Press

黑客攻防 极速入门

张阮阮 等编著



机械工业出版社
China Machine Press

图书在版编目 (CIP) 数据

黑客攻防极速入门/张阮阮等编著. —北京: 机械工业出版社, 2016.5

ISBN 978-7-111-53812-7

I. ①黑… II. ①张… 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 (2016) 第110265号

本书全面详细地介绍了计算机及智能移动设备的黑客攻防常用技术, 并提供了大量实用工具和操作案例。本书分为四篇: 第一篇介绍黑客攻防基础, 包括黑客攻防入门、黑客攻击手段揭秘、黑客攻防命令揭秘、黑客攻防学习环境搭建等知识; 第二篇介绍计算机黑客攻防实战, 包括扫描与嗅探、病毒攻防、木马攻防、Windows 系统漏洞攻防、后门攻防、局域网攻防、流氓软件与间谍软件攻防、远程控制攻防、加密与解密、数据备份与还原等知识; 第三篇介绍无线与移动设备安全, 包括无线网络 WiFi 攻防、手机黑客攻防等知识; 第四篇介绍网游账号攻防、QQ 与 E-mail 账号攻防、网络支付工具安全等知识。

本书通俗易懂, 图文并茂, 适用于黑客及安全技术初学者、爱好者, 也适用于企事业单位从事网络安全与维护的各类读者。

黑客攻防极速入门

出版发行: 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: 夏非彼 迟振春

印 刷: 中国电影出版社印刷厂

开 本: 188mm×260mm 1/16

书 号: ISBN 978-7-111-53812-7

版 次: 2016 年 7 月第 1 版第 1 次印刷

印 张: 24.5

定 价: 59.00 元

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) 88379426 88361066

购书热线: (010) 68326294 88379649 68995259

投稿热线: (010) 88379604

读者信箱: hzit@hzbook.com

版权所有•侵权必究

封底无防伪标均为盗版

本书法律顾问: 北京大成律师事务所 韩光/邹晓东

前言

本书紧紧围绕“攻”与“防”两个不同的角度，图文并茂地介绍了网络入侵与防御的全过程，以帮助网络和计算机安全人员及爱好者了解黑客入侵的各种手段，找到防范方法，确保计算机与网络的安全。

本书内容

本书分为4篇：第一篇介绍黑客攻防基础，包括黑客攻防入门、黑客攻击手段揭秘、黑客攻防命令揭秘、黑客攻防学习环境搭建等知识；第二篇介绍计算机黑客攻防实战，包括扫描与嗅探、病毒攻防、木马攻防、Windows系统漏洞攻防、后门攻防、局域网攻防、流氓软件与间谍软件攻防、远程控制攻防、加密与解密、数据备份与还原等知识；第三篇介绍无线与移动设备安全，包括无线网络WiFi攻防、手机黑客攻防等知识；第四篇介绍网游账号攻防、QQ与E-Mail账号攻防、网络支付工具安全等知识。

本书特色

本书由浅入深地讲解了黑客入侵和防范的具体方法和技巧，通过具体形象的案例介绍向读者展示了入侵及防御方法和各种工具的使用。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。

- 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。

本书适合人群

- 黑客及安全技术初学者、爱好者；
- 需要获得数据保护的日常办公人员；
- 企业网络管理人员、网吧工作人员；
- 家庭计算机用户及智能手机用户；
- 培训班。

本书主要由张阮阮编著，王鲁德、郑志华、王栋、宗立波、张辰、胡华、信传奇、李阳、王星凯等也参加了部分章节的编写。

由于编者水平所限，书中难免存在不足之处，敬请广大读者批评指正。

编者

2016年5月

目 录

前言

第一篇 黑客攻防基础

第 1 章 从零开始认识黑客	1
1.1 认识黑客	1
1.1.1 区别黑客、红客、蓝客、骇客及飞客	1
1.1.2 认识白帽、灰帽及黑帽黑客	2
1.1.3 黑客基础知识	2
1.1.4 黑客常用术语	3
1.2 网络协议	6
1.2.1 TCP/IP 协议	6
1.2.2 IP 协议	7
1.2.3 ARP 协议	9
1.2.4 ICMP 协议	10
1.3 系统进程	11
1.3.1 认识系统进程	11
1.3.2 关闭和新建系统进程	12
1.3.3 新建系统进程	13
1.4 端口	14
1.4.1 端口详解	14
1.4.2 查看端口	16
1.4.3 开启和关闭端口	17
1.4.4 端口的限制	19
第 2 章 黑客攻击手段大揭秘	25
2.1 了解黑客入侵的常见策略	25
2.1.1 数据驱动攻击	25
2.1.2 非法利用系统文件	25
2.1.3 伪造信息攻击	26
2.1.4 针对信息协议弱点攻击	26
2.1.5 远端操纵	26
2.1.6 利用系统管理员失误攻击	26
2.1.7 重新发送攻击	26
2.1.8 ICMP 报文攻击	26
2.1.9 针对源路径选择的弱点攻击	27

2.1.10	以太网广播攻击	27
2.1.11	跳跃式攻击	27
2.1.12	窃取 TCP 协议连接	27
2.1.13	夺取系统控制权	27
2.2	黑客入侵的常见手段	28
2.2.1	口令入侵	28
2.2.2	木马入侵	28
2.2.3	监听法入侵	28
2.2.4	E-mail 入侵	28
2.2.5	病毒入侵	28
2.3	认识黑客常用的入侵工具	29
2.3.1	端口扫描工具	29
2.3.2	数据嗅探工具	29
2.3.3	木马制作工具	30
2.3.4	远程控制工具	30
2.4	个人计算机安全的防护策略	30
2.4.1	安装并及时升级杀毒软件	31
2.4.2	启用防火墙	31
2.4.3	防止木马和病毒	31
2.4.4	警惕“网络钓鱼”	31
2.4.5	切勿随意共享文件夹	31
2.4.6	定期备份重要数据	32
第 3 章	黑客攻防命令大揭秘	33
3.1	常用命令行	33
3.1.1	进入 Windows 系统中的命令行界面	34
3.1.2	用菜单的形式进入 DOS 窗口	35
3.1.3	通过 IE 浏览器访问 DOS 窗口	35
3.1.4	复制、粘贴命令行	36
3.1.5	设置窗口风格	37
3.1.6	Windows 系统命令行	40
3.2	认识 DOS 系统	41
3.2.1	文件与目录	41
3.2.2	文件类型与属性	42
3.2.3	目录与磁盘	44
3.2.4	命令分类与命令格式	45
3.3	常用的网络命令	46
3.3.1	测试物理网络的 Ping 命令	46
3.3.2	查看网络连接的 Netstat	48
3.3.3	工作组和域的 Net 命令	51

3.3.4	23 端口登录的 Telnet 命令	56
3.3.5	传输协议 FTP 命令	56
3.3.6	查看网络配置的 IPConfig 命令	57
3.4	其他网络命令	57
3.4.1	Tracert 命令	58
3.4.2	Route 命令	59
3.4.3	Netsh 命令	60
3.4.4	Arp 命令	62
第 4 章	搭建黑客攻防学习环境	64
4.1	安装 VMware 虚拟机	64
4.2	配置安装完成的 VMware 虚拟机	67
4.3	安装虚拟操作系统	68
4.4	VMware Tools 安装	70
第二篇 计算机系统黑客攻防		
第 5 章	扫描与嗅探	72
5.1	扫描过程	72
5.1.1	确定目标计算机的 IP 地址	72
5.1.2	查看目标站点的备案信息	75
5.1.3	获取开放的端口和服务	76
5.2	扫描的实施与防范	78
5.2.1	扫描服务与端口	78
5.2.2	利用 X-scan 扫描本机隐患	80
5.2.3	FreePortScanner 与 ScanPort 等常见扫描工具	85
5.2.4	用 ProtectX 实现扫描的反击与追踪	87
5.3	嗅探的实施与防范	89
5.3.1	什么是嗅探器	89
5.3.2	经典嗅探器 Iris	90
5.3.3	使用影音神探嗅探在线视频地址	92
5.3.4	捕获网页内容的艾菲网页侦探	96
5.4	网络监控与安全防范	98
5.4.1	网络日常安全防范措施	98
5.4.2	运用网络执法官实现网络监控	99
第 6 章	病毒攻防	103
6.1	病毒知识入门	103
6.1.1	计算机病毒的特点	103

6.1.2	病毒的工作流程	104
6.2	计算机中毒后的常见症状	104
6.2.1	CPU 使用率始终保持在 95%以上	104
6.2.2	IE 浏览器窗口连续打开	105
6.2.3	杀毒软件被屏蔽	105
6.2.4	系统中的文件图标变成统一图标	105
6.2.5	系统时间被更改	105
6.3	简单病毒的生成与防范	106
6.3.1	U 盘病毒的生成与防范	106
6.3.2	Restart 病毒形成过程曝光	108
6.4	防范网络蠕虫	111
6.4.1	网络蠕虫病毒实例分析	111
6.4.2	网络蠕虫病毒的防范	112
6.5	杀毒软件的使用	114
6.5.1	360 杀毒软件	114
6.5.2	用 NOD32 查杀病毒	115
第 7 章	木马攻防	117
7.1	认识木马	117
7.1.1	木马的发展历程	117
7.1.2	木马的组成	118
7.1.3	木马的分类	119
7.1.4	木马的伪装手段	119
7.2	木马的捆绑技术	121
7.2.1	自解压捆绑木马曝光	121
7.2.2	案例分析: CHM 木马曝光	122
7.3	木马的加壳与脱壳	125
7.3.1	为木马加壳	125
7.3.2	检测木马是否加过壳	127
7.3.3	对木马进行脱壳	128
7.4	木马的清除与计算机防护	129
7.4.1	在“Windows 进程管理器”中管理进程	129
7.4.2	用木马清除专家清除木马	130
第 8 章	系统漏洞攻防	134
8.1	什么是系统漏洞	134
8.2	Windows 系统常见漏洞	135
8.2.1	Windows 早期版本的常见漏洞	135
8.2.2	Windows 7 系统常见漏洞	137
8.3	Windows 服务器系统入侵曝光	138

8.3.1	了解入侵流程	138
8.3.2	系统漏洞攻防	139
8.4	缓冲区溢出：实战 DcomRpc 漏洞	143
8.4.1	DcomRpc 漏洞描述	144
8.4.2	DcomRpc 入侵实战	145
8.4.3	DcomRpc 防范方法	146
8.5	使用 Windows Update 修复系统漏洞	147
第 9 章	后门技术攻防	150
9.1	什么是后门	150
9.2	后门的分类	151
9.2.1	网页后门	151
9.2.2	线程插入后门	151
9.2.3	扩展后门	151
9.2.4	C/S 后门	151
9.2.5	Rootkit	151
9.3	账号后门技术曝光	152
9.3.1	使用软件克隆账号曝光	152
9.3.2	手动克隆账号曝光	153
9.4	系统服务后门技术曝光	156
9.4.1	使用 Instsrv 创建系统服务后门曝光	157
9.4.2	使用 Srvinstw 创建系统服务后门曝光	158
9.5	手动检测系统中的后门程序	162
第 10 章	局域网攻防	163
10.1	局域网安全介绍	163
10.1.1	局域网的概念及特点	163
10.1.2	局域网安全隐患	164
10.2	ARP 欺骗	165
10.2.1	ARP 欺骗表现与分类	165
10.2.2	WinArpAttacker ARP 欺骗攻击曝光	166
10.2.3	网络监听	168
10.2.4	金山贝壳 ARP 防火墙的使用	169
10.3	绑定 MAC 防御 IP 冲突攻击	170
10.3.1	查看本机的 MAC 地址	170
10.3.2	绑定 MAC 防御 IP 冲突攻击	171
10.4	局域网助手 (LanHelper) 的使用	172
10.5	网络守护神的使用	174
10.6	局域网监控工具	177
10.6.1	网络特工	177

10.6.2	LanSee 工具	180
第 11 章 远程控制攻防		183
11.1	认识远程控制	183
11.1.1	远程控制技术的发展历程	183
11.1.2	远程控制的技术原理	184
11.1.3	远程控制的应用	184
11.2	远程桌面连接与协助	185
11.2.1	Windows 系统的远程桌面连接	185
11.2.2	Windows 系统远程关机	188
11.2.3	区别远程桌面与远程协助	189
11.3	基于认证入侵	189
11.3.1	IPC\$入侵	189
11.3.2	Telnet 入侵	191
11.4	基于注册表入侵	194
11.4.1	修改注册表实现远程监控	194
11.4.2	开启远程注册表服务	196
11.5	利用任我行软件进行远程控制	198
11.5.1	配置服务端	198
11.5.2	通过服务端程序进行远程控制	199
11.6	用 WinShell 实现远程控制	200
11.6.1	配置 WinShell	201
11.6.2	实现远程控制	203
11.7	用 QuickIP 进行多点控制	204
11.7.1	设置 QuickIP 服务器端	204
11.7.2	设置 QuickIP 客户端	205
11.7.3	实现远程控制	205
第 12 章 加密与解密技术		207
12.1	加密与解密基础知识	207
12.1.1	认识加密与解密	207
12.1.2	破解密码的常用方法	208
12.2	常见电脑文件的加密方法	209
12.2.1	RAR 压缩文件加解密	209
12.2.2	多媒体文件的加解密	210
12.2.3	光盘的加解密	213
12.2.4	Word 文件的加解密	215
12.2.5	Excel 文件的加解密	219
12.2.6	NTFS 文件系统加密数据	223
12.3	文件夹加密的方法	225

12.3.1	对文件夹进行加密	226
12.3.2	WinGuard 加密应用程序	230
12.4	破解常见的文件密码	232
12.4.1	破解 Office 文档密码	232
12.4.2	破解压缩文件的打开密码	235
12.4.3	查看星号密码	237
12.5	破解系统密码	238
12.5.1	利用 Windows 7 PE 破解系统登录密码	238
12.5.2	利用密码重设盘破解系统登录密码	242
12.5.3	使用 SecureIt Pro 给系统桌面加超级锁	245
12.5.4	系统加密大师 PC Security	247
第 13 章	间谍软件的清除和系统清理	252
13.1	流氓软件的清除	252
13.1.1	清理浏览器插件	252
13.1.2	流氓软件的防范	254
13.1.3	金山系统清理专家清除恶意软件	258
13.2	间谍软件防护实战	259
13.2.1	间谍软件防护概述	259
13.2.2	通过事件查看器抓住间谍	260
13.2.3	系统自带反间谍专家 Windows Defender 使用技巧	264
13.2.4	使用 360 安全卫士对电脑进行防护	266
第 14 章	系统与数据的备份与恢复	269
14.1	备份与还原操作系统	269
14.1.1	使用还原点备份与还原系统	269
14.1.2	使用 GHOST 备份与还原系统	272
14.2	备份与还原用户数据	276
14.2.1	使用驱动精灵备份与还原驱动程序	276
14.2.2	备份与还原 IE 浏览器的收藏夹	278
14.2.3	备份和还原 QQ 聊天记录	280
14.2.4	备份和还原 QQ 自定义表情	283
14.3	使用恢复工具来恢复误删除的数据	286
14.3.1	使用 Recuva 来恢复数据	286
14.3.2	使用 FinalData 来恢复数据	290
14.3.3	使用 FinalRecovery 来恢复数据	294

第三篇 无线网络及智能手机黑客攻防

第 15 章 无线网络 WiFi 攻防	297
15.1 无线路由器基本设置	297
15.1.1 无线路由器各部分功能详解	297
15.1.2 无线路由器参数设置	298
15.1.3 设置完成重启无线路由器	300
15.1.4 搜索无线信号连接上网	301
15.2 傻瓜式破解 WiFi 密码曝光及防范	301
15.2.1 WiFi 万能钥匙手机破解 WiFi 密码曝光	301
15.2.2 WiFi 万能钥匙电脑破解 WiFi 密码曝光	303
15.2.3 防止 WiFi 万能钥匙破解密码	304
15.3 在 Linux 中利用抓包破解 WiFi 密码曝光	307
15.3.1 虚拟 Linux 系统	307
15.3.2 破解 PIN 码	309
15.3.3 破解 WPA 密码	311
15.3.4 破解 WPA2 密码	312
15.4 无线路由安全设置	313
15.4.1 修改 WiFi 连接密码	313
15.4.2 禁用 DHCP 功能	314
15.4.3 无线加密	314
15.4.4 关闭 SSID 广播	315
15.4.5 设置 IP 过滤和 MAC 地址列表	315
15.4.6 主动更新	316
第 16 章 智能手机黑客攻防	317
16.1 初识手机黑客	317
16.1.1 智能手机操作系统	317
16.1.2 手机 Root	319
16.1.3 Android 手机备份功能	321
16.2 手机病毒与木马攻防	323
16.2.1 手机病毒与木马带来的危害	323
16.2.2 手机病毒防范	325
16.3 手机蓝牙攻击曝光	326
16.3.1 蓝牙的工作原理	326
16.3.2 拦截攻击与防范	327
16.4 手机拒绝服务攻击曝光	327
16.4.1 常见的手机拒绝服务攻击曝光	328

16.4.2	手机拒绝服务攻击防范	328
16.5	手机电子邮件攻击曝光	329
16.5.1	认识邮件在网络上的传播方式	329
16.5.2	手机上常用的邮件系统	329
16.5.3	手机电子邮件攻击与防范	329
16.6	手机优化及安全性能的提升	330
16.6.1	360 手机卫士	330
16.6.2	腾讯手机管家	331
16.6.3	金山手机卫士	332

第四篇 网游、QQ、E-mail 及理财安全防范

第 17 章	网络游戏安全防范	333
17.1	网游账号失窃原因及应对方案	333
17.2	网游盗号木马曝光	334
17.2.1	捆绑木马盗号曝光	334
17.2.2	哪些网游账号容易被盗	336
17.3	解读网站充值欺骗术	337
17.3.1	欺骗原理	337
17.3.2	常见的欺骗方式	337
17.3.3	提高防范意识	338
17.4	防范游戏账号破解	340
17.4.1	勿用“自动记住密码”	340
17.4.2	防范方法	342
第 18 章	QQ 账号与 E-mail 防范	344
18.1	3 种常见 QQ 盗号软件大揭秘	344
18.1.1	“QQ 简单盗”盗取 QQ 密码曝光与防范	344
18.1.2	“好友号好好盗”盗取 QQ 号码曝光	346
18.1.3	“QQExplorer”在线破解 QQ 号码曝光与防范方法	347
18.2	用密码监听器揪出内鬼	348
18.2.1	“密码监听器”盗号披露	349
18.2.2	找出“卧底”拒绝监听	350
18.3	保护 QQ 密码和聊天记录	350
18.3.1	定期修改 QQ 密码	350
18.3.2	申请 QQ 密保	351
18.3.3	加密聊天记录	353
18.4	电子邮箱安全防范	353
18.4.1	使用“流光”盗取邮箱密码	353



18.4.2	使用 E-mail 邮件群发大师发送邮箱炸弹.....	355
18.4.3	防范邮箱炸弹的攻击.....	357
第 19 章 网络支付工具的安全防范.....		360
19.1	加强支付宝的安全防护.....	360
19.1.1	加强支付宝账户的安全防护	360
19.1.2	加强支付宝内资金的安全防护	364
19.2	加强财付通的安全防护.....	367
19.2.1	加强财付通账户的安全防护	367
19.2.2	加强财付通内资金的安全防护	370
19.3	加强网上银行安全防护.....	372
19.3.1	定期修改登录密码.....	372
19.3.2	设置预留验证信息.....	374
19.3.3	安装防钓鱼安全控件.....	375
19.3.4	使用小 e 安全检测系统.....	377
19.3.5	使用工行 U 盾.....	378
19.3.6	使用电子银行口令卡.....	378

第一篇 黑客攻防基础

»» 第 1 章 从零开始认识 黑客

黑客一词，源于英文 Hacker，原指热心于计算机技术，水平高超的电脑专家，尤其是程序设计人员。但到了今天，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家伙。想要打败黑客维护我们的信息安全，我们就要知己知彼，从真正意义上了解黑客，本章将会带你走进黑客的世界，带领你了解进程、端口、IP 地址以及黑客常见的术语和命令，从而帮助读者为后面的学习打好基础。



1.1 认识黑客

1.1.1 区别黑客、红客、蓝客、骇客及飞客

黑客，最早源自英文 hacker，原指热心于计算机技术、水平高超的电脑专家，尤其是程序设计人员，但到了今天，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家伙。

红客可以说是中国黑客起的名字，英文“honker”是红客的译音。通常红客是一群为捍卫中国主权而战的黑客们。他们热爱自己的祖国，热爱民族，热爱和平，极力的维护国家安全与尊严。

“蓝客”一词由中国蓝客联盟在 2001 年 9 月提出，他们信仰自由，提倡爱国主义，用自己的力量来维护网络和平。

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

黑客和骇客根本的区别是：黑客们建设，而骇客们破坏。

飞客是电信网络的先行者，他们经常利用程控交换机的漏洞进入并研究电信网络。

1.1.2 认识白帽、灰帽及黑帽黑客

白帽黑客，是指那些专门研究或者从事网络、计算机技术防御的人，他们通常受雇于各大公司，是维护网络、计算机安全的主要力量。很多白帽还受雇于公司，对产品进行模拟黑客攻击，以检测产品的可靠性。

灰帽黑客是指那些懂得技术防御原理，并且有实力突破这些防御的黑客。尽管他们的技术实力往往要超过绝大部分白帽和黑帽，但灰帽通常并不受雇于大型企业，他们往往将黑客行为作为一种业余爱好或者是义务来做，希望通过他们的黑客行为来警告一些网络或者系统漏洞，以达到警示别人的目的，因此，他们的行为没有丝毫恶意。

黑帽黑客是指那些专门研究病毒木马、操作系统、寻找漏洞，并且以个人意志为出发点，攻击网络或者计算机的人，已被认为是一个犯罪和黑客的混成语。

1.1.3 黑客基础知识

想要成为黑客并不是一件简单的事情，不仅要熟练掌握英文，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. 熟练掌握英文

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，因此就需要掌握一定的英文语言技能，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 等命令，利用这些命令可以实现不同的功能，利用 Ping 命令可以获取目标计算机的 IP 地址及主机名。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等。

4. 掌握主流的编程语言及脚本语言

从互联网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，需要自己具有独立的思想，通过掌握主流的 C++ 和 JAVA 等编程语言来创建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。

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、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, 一般用于网页服务器。

(3) Hybrid Languages (混合型语言)

代表是 JAVA 和 C#, 介于解释型和编译型之间。

(4) COMPILING Languages (编译型语言)

C/C++ 和 JAVA 都是编译型语言。

(5) Assembly Languages (汇编语言)

汇编语言是最接近于硬件的语言, 不过现在很少有人使用。

1.1.4 黑客常用术语

1. 肉鸡

“肉鸡”是一种很形象的比喻, 比喻那些被黑客控制的电脑, 对方可以是 Windows 系统, 也可以是 UNIX/LINUX 系统, 可以是普通的个人电脑, 也可以是大型的服务器, 一旦你的电脑成为“肉鸡”, 就意味着别人可以随心所欲地操作你的电脑, 而不会被你发觉。

2. 木马

就是那些表面上伪装成正常的程序, 但是当这些程序运行时, 就会获取系统的整个控制权限。有很多黑客热衷于使用木马程序来控制别人的电脑, 比如灰鸽子、黑洞、PcShare 等。

3. 网页木马

表面上伪装成普通的网页文件或将自己的代码直接插入到正常的网页文件中, 当有人访问时, 网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马服务端下载到访问者的电脑上自动执行。

4. 挂马

就是在别人的网站文件里面放入网页木马或者将代码潜入到对方正常的网页文件里, 以使浏览者中马。

5. 后门

这是一种形象的比喻, 黑客在利用某些方法成功地控制了目标主机后, 可以在对方的系统中植入特定的程序, 或者是修改某些设置。这些改动表面上很难被察觉, 但是黑客却可以使用相应的程序或者方法来轻易地与这台电脑建立连接, 重新控制这台电脑, 就好像是客人偷偷地配了一把主人房间的钥匙, 可以随时进出主人的房间而不被主人发现一样。通常大多数的特洛伊木马 (Trojan Horse) 程序都可以被黑客用于制作后门 (BackDoor)。