

THE SECRETS OF BEING AN EXPERT
IN COMPUTER FROM A BEGINNER



黑客攻防

从入门到精通

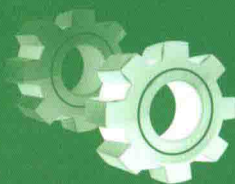
(命令版)

武新华 李书梅 编著

- 与时俱进，完备移动终端（安卓、苹果等）的黑客攻防命令。
- 从零起步，由浅入深地讲解，使初学者快速掌握黑客防范技巧与工具的使用方法。
- 注重实用性，理论和实例相结合，使读者能够融会贯通。大量的小技巧和小窍门，提高读者的学习效率。
- 通俗易懂的图文解说、任务驱动式的黑客软件讲解、攻防互参的防御方法剖析，使读者能够全面确保自己的网络安全。



机械工业出版社
China Machine Press



黑客攻防

从入门到精通

(命令版)

武新华 李书梅 编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

黑客攻防从入门到精通：命令版 / 武新华，李书梅编著 . —北京：机械工业出版社，2016.3
(学电脑从入门到精通)

ISBN 978-7-111-53279-8

I. 黑… II. ①武… ②李… 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（2016）第 053885 号

本书紧紧围绕黑客命令与实际应用展开，剖析在用户设备被黑客入侵时用户迫切需要用到或想要用到的命令，力求进行傻瓜式的讲解，使读者对网络入侵防御技术有系统了解，能够更好地防范黑客的攻击。全书共分为 15 章，包括：初识黑客、Windows 系统中的命令行、黑客常用的 Windows 网络命令行、Windows 系统命令行配置、基于 Windows 认证的入侵、远程管理 Windows 系统、局域网攻击与防范、DOS 命令的实际应用、制作启动盘、批处理 BAT 文件编程、病毒木马的主动防御和清除、流氓软件和间谍软件的清除、Android 操作系统的控制与安全、iOS 操作系统的常见应用及安全、移动 Wi-Fi 安全攻防等内容。

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。

黑客攻防从入门到精通（命令版）

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：张梦玲

责任校对：董纪丽

印 刷：北京瑞德印刷有限公司

版 次：2016 年 4 月第 1 版第 1 次印刷

开 本：185mm×260mm 1/16

印 张：24.75

书 号：ISBN 978-7-111-53279-8

定 价：69.00 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

投稿热线：（010）88379604

购书热线：（010）68326294 88379649 68995259

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

黑客使用得最多、最频繁的工具不是那些 Windows 系统中的工具软件，而是那些被 Microsoft（微软）刻意摒弃的 DOS 命令，或者更具体地说，就是那些需要手工在命令行状态下输入的网络命令。因此，就有人不断发出“DOS 不是万能的，但没有 DOS 是万万不能的”感慨。

在计算机技术日新月异的今天，称霸天下的 Windows 系统仍有很多做不了和做不好的事，学习和掌握 DOS 命令行技术仍然是成为计算机高手的必修课程。

本书涵盖了 DOS 和 Windows 各版本操作系统下几乎所有的网络操作命令，详细地讲解了各种命令的功能和参数，并针对具体应用列举了大量经典示例，能使广大 Windows 用户知其然，更知其所以然，真正做到学以致用，技高一筹。

为了节省用户宝贵的时间，提高用户的使用水平，本书在创作过程中尽量具备如下特色：

- 与时俱进，加入移动终端（Android、iOS 等）安全方面内容的介绍。
- 从零起步，步步深入，由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。
- 注重实用性，理论和实例相结合，并配以大量插图，生动易懂。
- 介绍大量小技巧和小窍门，提高读者的学习效率，节省他们的摸索时间。
- 重点突出、操作简单、内容丰富，同时附有大量的操作实例，读者可以一边学习，一边在计算机上操作，做到即学即用、即用即得。

本书内容全面、语言简练、深入浅出、通俗易懂，既可作为即查即用的工具手册，也可作为了解黑客的参考书目。本书不论在体例结构上，还是在技术实现及创作思想上，都做了精心的安排，力求将最新的技术、最好的学习方法奉献给读者。

作者采用通俗易懂的图文解说，即使你是计算机新手也能通读全书；用任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；新颖的黑客技术盘点，有助于你做好“先下手为强”的防护；攻防互参的防御方法，全面确保你的网络安全。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

编者

2016 年 1 月

目 录

前 言

第1章 初识黑客 / 1

- 1.1 认识黑客 / 2
 - 1.1.1 什么是黑客 / 2
 - 1.1.2 黑客的特点 / 2
 - 1.1.3 黑客常用术语 / 3
- 1.2 认识 IP 地址 / 5
 - 1.2.1 IP 地址概述 / 5
 - 1.2.2 IP 地址的分类 / 6
- 1.3 认识进程 / 7
 - 1.3.1 查看系统进程 / 7
 - 1.3.2 关闭和新建系统进程 / 8
- 1.4 认识端口 / 9
 - 1.4.1 端口的分类 / 10
 - 1.4.2 查看端口 / 11
- 1.5 在计算机中创建虚拟环境 / 12
 - 1.5.1 安装 VMware 虚拟机 / 13
 - 1.5.2 配置安装好的 VMware 虚拟机 / 16
 - 1.5.3 安装虚拟操作系统 / 18
 - 1.5.4 VMware Tools 安装 / 20

第2章 Windows系统中的命令行 / 22

- 2.1 Windows 系统中的命令行 / 23
 - 2.1.1 Windows 系统中的命令行概述 / 23
 - 2.1.2 Windows 系统中的命令行操作 / 27
 - 2.1.3 启动 Windows 系统中的命令行 / 27
- 2.2 在 Windows 系统中执行 DOS

命令 / 28

2.2.1 用菜单的形式进入 DOS

窗口 / 28

2.2.2 通过 IE 浏览器访问 DOS

窗口 / 28

2.2.3 复制、粘贴命令行 / 29

2.2.4 设置窗口风格 / 30

2.2.5 Windows 系统命令行 / 33

2.3 全面认识 DOS 系统 / 34

2.3.1 DOS 系统的功能 / 35

2.3.2 文件与目录 / 35

2.3.3 文件类型与属性 / 36

2.3.4 目录与磁盘 / 38

2.3.5 命令分类与命令格式 / 39

第3章

黑客常用的Windows网络命令行 / 41

3.1 必备的几个内部命令 / 42

3.1.1 命令行调用的 command

命令 / 42

3.1.2 复制命令 / 43

3.1.3 打开 / 关闭请求回显功能的

echo 命令 / 45

3.1.4 查看网络配置的 ipconfig

命令 / 46

3.1.5 命令行任务管理器的 at

命令 / 48

3.1.6 查看系统进程信息的 Tasklist

命令 / 50

3.2 黑客常用命令 / 51

3.2.1 测试物理网络的 ping 命令 / 51

3.2.2 查看网络连接的 netstat / 54

3.2.3 工作组和域的 net 命令 / 56

3.2.4 23 端口登录的 Telnet

命令 / 60

3.2.5 传输协议 FTP 命令 / 61

3.2.6 替换重要文件的 replace

命令 / 61

3.2.7 远程修改注册表的 reg

命令 / 62

3.3 其他的网络命令 / 65

3.3.1 tracert 命令 / 65

3.3.2 route 命令 / 66

3.3.3 netsh 命令 / 68

3.3.4 ARP 命令 / 70

第4章

Windows系统命令行配置 / 72

- 4.1 Config.sys 文件配置 / 73
 - 4.1.1 Config.sys 文件中的命令 / 73
 - 4.1.2 Config.sys 配置实例 / 74
 - 4.1.3 Config.sys 文件中常用的配置项目 / 75
- 4.2 批处理与管道 / 76
 - 4.2.1 批处理命令实例 / 77
 - 4.2.2 批处理中的常用命令 / 78
 - 4.2.3 常用的管道命令 / 81
 - 4.2.4 批处理的实例应用 / 83
- 4.3 对硬盘进行分区 / 86
 - 4.3.1 硬盘分区相关的知识 / 86
 - 4.3.2 利用 Diskpart 进行分区 / 87
- 4.4 可能出现的问题与解决方法 / 94
- 4.5 总结与经验积累 / 95

第5章

基于Windows认证的入侵 / 96

- 5.1 IPC\$ 的空连接漏洞 / 97
 - 5.1.1 IPC\$ 概述 / 97
 - 5.1.2 IPC\$ 空连接漏洞 / 98
 - 5.1.3 IPC\$ 的安全解决方案 / 99
- 5.2 Telnet 高级入侵 / 103
 - 5.2.1 突破 Telnet 中的 NTLM 权限认证 / 103
 - 5.2.2 Telnet 典型入侵 / 105
 - 5.2.3 Telnet 杀手锏 / 108
 - 5.2.4 Telnet 高级入侵常用的工具 / 110
- 5.3 通过注册表入侵 / 111
 - 5.3.1 注册表的相关知识 / 111
 - 5.3.2 远程开启注册表服务功能 / 113
 - 5.3.3 连接远程主机的“远程注册表服务” / 115
 - 5.3.4 编辑注册表文件 / 115
 - 5.3.5 通过注册表开启终端服务 / 120
- 5.4 实现 MS SQL 入侵 / 121
 - 5.4.1 用 MS SQL 实现弱口令入侵 / 121
 - 5.4.2 入侵 MS SQL 主机 / 126
 - 5.4.3 MS SQL 注入攻击与防护 / 126
 - 5.4.4 用 NBSI 软件实现 MS SQL 注入攻击 / 128
 - 5.4.5 MS SQL 入侵安全解决方案 / 130
- 5.5 获取账号密码 / 132
 - 5.5.1 用 Sniffer 获取账号密码 / 132
 - 5.5.2 字典工具 / 137
 - 5.5.3 远程暴力破解 / 142
- 5.6 可能出现的问题与解决方法 / 144
- 5.7 总结与经验积累 / 145

第6章

远程管理Windows系统 / 146

- 6.1 远程计算机管理入侵 / 147
 - 6.1.1 计算机管理概述 / 147
 - 6.1.2 连接到远程计算机并开启服务 / 148
 - 6.1.3 查看远程计算机信息 / 149
 - 6.1.4 用远程控制软件实现远程管理 / 151
- 6.2 远程命令执行与进程查杀 / 152
 - 6.2.1 远程执行命令 / 153
 - 6.2.2 查杀系统进程 / 154
 - 6.2.3 远程执行命令方法汇总 / 156
- 6.3 FTP 远程入侵 / 156
 - 6.3.1 FTP 相关内容 / 156
 - 6.3.2 扫描 FTP 弱口令 / 159
 - 6.3.3 设置 FTP 服务器 / 160
- 6.4 可能出现的问题与解决方法 / 163
- 6.5 总结与经验积累 / 164

第7章

局域网攻击与防范 / 165

- 7.1 局域网安全介绍 / 166
 - 7.1.1 局域网基础知识 / 166
 - 7.1.2 局域网安全隐患 / 166
- 7.2 ARP 欺骗与防御 / 167
 - 7.2.1 ARP 欺骗概述 / 168
 - 7.2.2 WinArpAttacker ARP 欺骗攻击曝光 / 168
 - 7.2.3 网络监听与 ARP 欺骗 / 171
 - 7.2.4 金山贝壳 ARP 防火墙的使用 / 172
 - 7.2.5 AntiArp-DNS 防火墙 / 174
- 7.3 绑定 MAC 防御 IP 冲突攻击 / 175
 - 7.3.1 查看本机的 MAC 地址 / 175
 - 7.3.2 绑定 MAC 防御 IP 冲突攻击 / 176
- 7.4 局域网助手攻击与防御 / 177
- 7.5 利用网络守护神实现 DNS 欺骗 / 180
- 7.6 局域网监控工具 / 183
 - 7.6.1 网络特工 / 183
 - 7.6.2 LanSee 工具 / 188
 - 7.6.3 长角牛网络监控机 / 190

第8章

DOS命令的实际应用 / 197

- 8.1 DOS 命令的基础应用 / 198
 - 8.1.1 在 DOS 下正确显示中文信息 / 198
 - 8.1.2 恢复误删除文件 / 199
 - 8.1.3 让 DOS 窗口无处不在 / 200
 - 8.1.4 DOS 系统的维护 / 203
- 8.2 DOS 中的环境变量 / 204
 - 8.2.1 SET 命令的使用 / 205
 - 8.2.2 使用 Debug 命令 / 205
 - 8.2.3 认识不同的环境变量 / 207
 - 8.2.4 环境变量和批处理 / 210
- 8.3 在 DOS 中进行文件操作 / 210
 - 8.3.1 抓取 DOS 窗口中的文本 / 211
 - 8.3.2 在 DOS 中使用注册表 / 212
 - 8.3.3 在 DOS 中实现注册表编程 / 213
 - 8.3.4 在 DOS 中使用注册表扫描程序 / 214
- 8.4 网络中的 DOS 命令运用 / 215
 - 8.4.1 检测 DOS 程序执行的目录 / 215
 - 8.4.2 内存虚拟盘软件 XMS-DSK 的使用 / 216
 - 8.4.3 在 DOS 中恢复回收站中的文件 / 217
 - 8.4.4 在 DOS 中删除不必要的文件 / 217
- 8.5 可能出现的问题与解决方法 / 218
- 8.6 总结与经验积累 / 218

第9章

制作启动盘 / 219

- 9.1 制作启动盘简述 / 220
 - 9.1.1 认识启动盘 / 220
 - 9.1.2 应急启动盘的作用 / 220
 - 9.1.3 制作 Windows PE 启动盘 / 221
 - 9.1.4 制作 DOS 启动盘 / 223
- 9.2 U 盘启动盘的使用 / 226
 - 9.2.1 进入 U 盘系统 / 226
 - 9.2.2 用 U 盘启动盘安装系统 / 227
- 9.3 使用启动盘排除故障 / 229
 - 9.3.1 使用启动盘备份数据 / 229
 - 9.3.2 用启动盘替换损坏的系统文件 / 229
 - 9.3.3 用启动盘维修注册表故障 / 230
 - 9.3.4 用 Windows 诊断工具排除故障 / 230
- 9.4 可能出现的问题与解决方法 / 233
- 9.5 总结与经验积累 / 233

第10章

批处理BAT文件编程 / 234

- 10.1 在 Windows 中编辑批处理文件 / 235
- 10.2 在批处理文件中使用参数与组合命令 / 235
 - 10.2.1 在批处理文件中使用参数 / 236
 - 10.2.2 组合命令的实际应用 / 236
- 10.3 配置文件中常用的命令 / 238
 - 10.3.1 分配缓冲区数目的 Buffers 命令 / 238
 - 10.3.2 加载程序的 Device 命令 / 239
 - 10.3.3 扩展键检查的 Break 命令 / 239
 - 10.3.4 程序加载的 Devicehigh 命令 / 240
 - 10.3.5 设置可存取文件数 Files 命令 / 241
 - 10.3.6 安装内存驻留程序的 Install 命令 / 241
 - 10.3.7 中断处理的 Stacks 命令 / 242
 - 10.3.8 扩充内存管理程序 Himem.sys / 242
- 10.4 用 BAT 编程实现综合应用 / 244
 - 10.4.1 系统加固 / 244
 - 10.4.2 删除日志 / 244
 - 10.4.3 删除系统中的垃圾文件 / 245
- 10.5 可能出现的问题与解决方法 / 245
- 10.6 总结与经验积累 / 246

第11章

病毒木马的主动防御和清除 / 248

- 11.1 认识病毒和木马 / 249
 - 11.1.1 病毒知识入门 / 249
 - 11.1.2 木马的组成与分类 / 250
- 11.2 关闭危险端口 / 252
 - 11.2.1 通过安全策略关闭危险端口 / 252
 - 11.2.2 自动优化 IP 安全策略 / 255
 - 11.2.3 系统安全设置 / 261
- 11.3 用防火墙隔离系统与病毒 / 263
 - 11.3.1 使用 Windows 防火墙 / 263
 - 11.3.2 设置 Windows 防火墙的入站规则 / 265
- 11.4 杀毒软件的使用 / 268
 - 11.4.1 用 NOD32 查杀病毒 / 268
 - 11.4.2 瑞星杀毒软件 / 269
- 11.5 木马清除软件的使用 / 271
 - 11.5.1 用木马清除专家清除木马 / 271
 - 11.5.2 用木马清道夫清除木马 / 274
- 11.6 可能出现的问题与解决方法 / 275
- 11.7 总结与经验积累 / 276

第12章

流氓软件和间谍软件的清除 / 277

- 12.1 间谍软件防护实战 / 278
 - 12.1.1 间谍软件防护概述 / 278
 - 12.1.2 微软反间谍专家 Windows Defender / 278
 - 12.1.3 用 Spy Sweeper 清除间谍软件 / 282
 - 12.1.4 AD-Aware 让间谍程序消失无踪 / 284
- 12.2 流氓软件的清除 / 287
 - 12.2.1 清理浏览器插件 / 287
 - 12.2.2 金山清理专家清除恶意软件 / 289
 - 12.2.3 流氓软件的防范 / 290
- 12.3 常见的网络安全防护工具 / 293
 - 12.3.1 浏览器绑架克星 HijackThis / 293
 - 12.3.2 诺顿网络安全特警 / 297
 - 12.3.3 使用 360 安全卫士对计算机进行防护 / 302

第13章

Android操作系统的控制与安全 / 306

- 13.1 Android 手机数据备份功能 / 308
 - 13.1.1 recovery 模式 / 308
 - 13.1.2 recovery 的方法 / 308
- 13.2 Android root 权限 / 310
 - 13.2.1 root 的原理 / 310
 - 13.2.2 root 的好处以及风险 / 310
 - 13.2.3 如何获取 root 权限 / 311
- 13.3 Android 平台恶意软件及病毒 / 312
 - 13.3.1 ROM 内置恶意软件 / 312
 - 13.3.2 破坏类恶意软件 / 病毒 / 313
 - 13.3.3 吸费类恶意软件 / 病毒 / 314
 - 13.3.4 窃取隐私类恶意软件 / 病毒 / 314
 - 13.3.5 伪装类恶意软件 / 病毒 / 315
 - 13.3.6 云更新类恶意软件 / 病毒 / 316
 - 13.3.7 诱骗类恶意软件 / 病毒 / 317

第14章 iOS操作系统的常见应用及安全 / 318

- 14.1 针对 iOS 的攻击曝光 / 319
 - 14.1.1 iKee 攻击与防范 / 319
 - 14.1.2 中间人攻击与防范 / 320
 - 14.1.3 恶意应用程序 Handy Light 和 InstaStock 的曝光与防范 / 321
 - 14.1.4 具有漏洞的应用程序: iOS 应用程序和第三方应用程序 / 323
- 14.2 备份和恢复 iPhone/iPad/iPod 数据 / 324
 - 14.2.1 使用 iCloud 备份和恢复用户数据 / 324
 - 14.2.2 使用 iTunes 备份和还原用户数据 / 326
 - 14.2.3 使用 91 助手备份和还原用户数据 / 328

第15章 移动Wi-Fi安全攻防 / 332

- 15.1 认识 Wi-Fi / 333
 - 15.1.1 Wi-Fi 的技术原理 / 333
 - 15.1.2 Wi-Fi 的主要功能 / 333
 - 15.1.3 Wi-Fi 的优势 / 334
- 15.2 无线路由器的基本设置 / 334
 - 15.2.1 无线路由器外观 / 334
 - 15.2.2 无线路由器的参数设置 / 335
 - 15.2.3 设置完成后重启无线路由器 / 336
- 15.3 智能手机的 Wi-Fi 连接 / 337
 - 15.3.1 Android 手机 Wi-Fi 连接 / 337
 - 15.3.2 iPhone 手机 Wi-Fi 连接 / 339
- 15.4 无线路由器的安全设置 / 340
 - 15.4.1 修改 Wi-Fi 连接密码 / 340
 - 15.4.2 禁用 DHCP 功能 / 341
 - 15.4.3 无线加密 / 341
 - 15.4.4 关闭 SSID 广播 / 342
 - 15.4.5 设置 IP 过滤和 MAC 地址列表 / 342
 - 15.4.6 主动更新 / 342
- 15.5 Wi-Fi 密码破解及防范 / 343
 - 15.5.1 傻瓜式破解 Wi-Fi 密码曝光及防范 / 343
 - 15.5.2 Linux 下利用抓包破解 Wi-Fi 密码曝光 / 347
- 15.6 Wi-Fi 存在的安全风险 / 360
 - 15.6.1 Wi-Fi 钓鱼陷阱 / 361
 - 15.6.2 Wi-Fi 接入点被偷梁换柱 / 361
 - 15.6.3 攻击无线路由器 / 361
 - 15.6.4 内网监听攻击 / 362
 - 15.6.5 劫机风险 / 362
- 15.7 Wi-Fi 安全防范措施 / 363

附录 / 364

想要学习黑客知识，就得了解进程、端口、IP 地址以及黑客常见的术语和命令。本章正是针对初学者对这方面了解不多，专门做出讲解，从而帮助读者为后面的学习打好基础。

主要内容：

- 认识黑客
- 认识 IP 地址
- 认识进程
- 认识端口
- 在计算机中创建虚拟环境

1.1 认识黑客

1994 年以来，互联网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且上网逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，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。随着计算机的普及和互联网技术的迅速发展，黑客也随之出现了。

1.1.1 什么是黑客

黑客的基本含义是一个拥有熟练计算机技术的人，但大部分媒体将计算机侵入者称为黑客，而实际上，黑客有如下几种：

白帽黑客是指有能力破坏计算机安全但不具恶意目的的黑客。白帽黑客一般遵守道德规范并常常试图同企业合作去改善所发现的计算机安全弱点。

灰帽黑客是指处于伦理和法律边缘的黑客。

黑帽黑客别称骇客，经常使用于区分黑帽黑客和一般（正面的）有理性的黑客。这个词流行于 1983 年，采用了“Safe Cracker”的相似发音，并且理论化为一个犯罪和黑客的混成语。

1.1.2 黑客的特点

黑客的一般特点是：有英文基础、知道常用的黑客术语和网络安全术语、能熟练使用常用的 DOS 命令和黑客工具，还会使用主流的编程语言及脚本。

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。除了掌握相关的黑客术语属于之外，黑客一般还掌握 TCP/IP 协议、ARP 协议等网络安全术语。

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，利用 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目标计算机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。

主流的编程语言以及脚本语言主要有 5 类，如下：

（1）网页脚本语言（web page script language）

网页脚本语言就是网页代码，比如 HTML、Javascript、CSS、ASP、PHP、XML 等。

（2）解释型语言（Interpreted Language）

解释型语言包括 Perl、Python、REBOL、Ruby 等，也常被称为脚本语言，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，因此不适合用来开发软件产品，一般用于网页服务器中。

(3) 混合型语言 (Hybrid Language)

混合型语言的代表是 Java 和 C#, 介于解释型和编译型之间。

(4) 编译型语言 (Compiling Language)

C/C++、Java 都是编译型语言。

(5) 汇编语言 (Assembly Language)

汇编语言是最接近于硬件的语言, 不过现在用的人很少。



提示

程序语言的学习顺序建议如下。

如果完全没有程序经验, 可照这个顺序学习: Javascript → 解释型语言 → 混合型语言 → 编译型语言 → 汇编。

1.1.3 黑客常用术语

1. 肉鸡

肉鸡比喻那些可以随意被黑客控制的计算机, 黑客可以像操作自己的计算机那样来操作它们, 而不被对方所发觉。

2. 木马

本马指表面上伪装成正常的程序, 但是当这些程序运行时, 入侵者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计算机, 比如灰鸽子、黑洞、PcShare 等。

3. 网页木马

网页本马指表面上伪装成普通的网页文件或是将恶意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木马的服务端下载到访问者的计算机上来自动执行。

4. 挂马

挂马指在别人的网站文件里放入网页木马或者是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

后门是一种形象的比喻, 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。这些改动从表面上很难被察觉, 但是黑客却可以使用相应的程序或者方法轻易地与这台计算机建立连接, 重新控制这台计算机, 这就好像黑客偷偷地配了一把主人房间的钥匙, 可以随时进出房间而不被主人发现一样。通常, 大多数的特洛伊木马程序都可以被入侵者用于制作后门。

6. IPC\$

IPC\$ 是共享“命名管道”的资源, 它是为了让进程之间通信而开放的命名管道, 可以通

过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

7. 弱口令

弱口令指那些强度不够，容易被猜解的口令，类似 123、abc 这样的口令（密码）。

8. Shell

Shell 指的是一种命令执行环境，比如，我们按下键盘上的“开始键+R”组合键时会出现“运行”对话框，在里面输入“cmd”会出现一个用于执行命令的黑窗口，这个就是 Windows 的 Shell 执行环境。

9. WebShell

WebShell 就是以 ASP、PHP、JSP 或者 CGI 等网页文件形式存在的一种命令执行环境，也可以将其称为一种网页后门。

10. 溢出

确切地讲，应该是“缓冲区溢出”。简单地解释就是程序对接收的输入数据没有执行有效的检测而导致错误，后果可能是程序崩溃或者是执行攻击者的命令。其大致可以分为两类：①堆溢出；②栈溢出。

11. 注入

由于程序员的水平参差不齐，相当大一部分应用程序存在安全隐患，用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些想要的数据库，这个就是 SQL 注入。

12. 注入点

注入点是可以实行注入的地方，通常是一个访问数据库的连接。根据注入点数据库运行账号的不同权限，你所得到的权限也不同。

13. 内网

内网通俗地讲就是局域网，比如网吧、校园网、公司内部网等。IP 地址如果是在以下三个范围之内，就说明我们是处于内网之中的：10.0.0.0 ~ 10.255.255.255、172.16.0.0 ~ 172.31.255.255、192.168.0.0 ~ 192.168.255.255。

14. 外网

外网直接连入互联网，可以与互联网上的任意一台计算机互相访问。

15. 免杀

免杀通过加壳、加密、修改特征码、加花指令等技术来修改程序，使其逃过杀毒软件的查杀。

16. 加壳

利用特殊的算法，改变 EXE 可执行程序或者 DLL 动态链接库文件的编码（比如实现压缩、加密），以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的壳有 UPX、ASPack、PePack、PECompact、UPack 等。

17. 花指令

花指令是几句汇编指令，可让汇编语句进行一些跳转，使得杀毒软件不能正常地判断病

毒文件的构造。通俗地讲，就是杀毒软件是从头到脚按顺序来查找病毒的，如果我们把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了。

1.2 认识 IP 地址

在互联网中，只要利用 IP 地址，都可以找到目标主机，因此，如果想要攻击某个互联网主机，就要先确定该目标主机的域名或 IP 地址。

1.2.1 IP 地址概述

所谓 IP 地址就是一种主机编址方式，给每个连接在互联网中的主机分配一个 32 bit（比特）地址，也称为网际协议地址。

按照传输控制协议 /Internet 协议（Transport Control Protocol/Internet Protocol, TCP/IP）协议的规定，IP 地址用二进制来表示，每个 IP 地址长 32 bit，1 bit 换算成字节就是 4 个字节。例如一个采用二进制形式的 IP 地址是“00001010000000000000000000000001”，这么长的地址人们处理起来就会很费劲，为了方便使用，IP 地址经常被写成十进制的形式，中间使用符号“.”分为不同的字节，即用 XXX.XXX.XXX.XXX 的形式来表现，每组 XXX 代表小于等于 255 的 10 进制数，例如 192.168.38.6。IP 地址的这种表示方法称为“点分十进制表示法（Dotted decimal notation）”，这显然比二进制的 1 或 0 容易记忆。

一个完整的 IP 地址信息通常应包括 IP 地址、子网掩码、默认网关和 DNS 等 4 部分内容。它们 4 个只有协同工作时，用户才可以访问互联网并被互联网中的计算机所访问（采用静态 IP 地址接入互联网时，ISP 应当为用户提供全部的 IP 地址信息）。

1. IP 地址

企业网络使用的合法 IP 地址，由提供互联网接入的服务商（ISP）分配，私有 IP 地址则可以由网络管理员自由分配。但网络内部所有计算机的 IP 地址都不能相同，否则，会发生 IP 地址冲突，导致网络连接失败。

2. 子网掩码

子网掩码是与 IP 地址结合使用的一种技术，其主要作用有两个，一是用于确定地址中的网络号和主机号，二是用于将一个大 IP 网络划分为若干个子网络。

3. 默认网关

默认网关是指一台主机如果找不到可用的网关，就把数据包发送给默认指定的网关，由这个网关来处理数据包。从一个网络向另一个网络发送信息时，也必须经过一道“关口”，这道关口就是网关。

4. DNS

DNS 服务用于将用户的域名请求转换为 IP 地址。如果企业网络没有提供 DNS 服务，则