

ATTACK

在攻与防的对立统一中
寻求技术突破

黑客攻防 从入门到精通

命令实战篇 · 全新升级版

明月工作室 宗立波◎编著

黑客攻防全能视频+计算机硬件管理超级手册+Windows文件管理高级手册+Linux命令应用大全

以下人群请勿翻阅本书:

1. 自以为很牛，对黑客不屑一顾的人
2. 心存侥幸，认为黑客离自己很远的人
3. 习惯黑客攻击，总是折腾他人的人
4. 号太多，习惯被盗号的人
5. 不差钱，不怕被盗刷的人
6. 我不是Boss，对交易安全漠不关心的人

DEFENSE



北京大学出版社
PEKING UNIVERSITY PRESS

ATTACK

黑客攻防

从入门到精通

命令实战篇 · 全新升级版

明月工作室 宗立波◎编著



DEFFENSE

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 提 要

本书由浅入深、图文并茂地再现了在计算机安全方面相关命令的使用和操作知识。

全书共分15章，分别为计算机基础知识、Windows系统中的命令行基础、配置Windows系统的命令行、黑客基础知识、揭秘黑客常用的命令、批处理BAT文件编程、黑客攻防前的准备工作、揭露基于Windows认证的入侵方式、局域网攻防、远程管理Windows系统攻防、DOS命令攻防、后门技术攻防、流氓软件和间谍软件的清除与防御、制作启动盘进行防御、木马病毒的主动防御清除。

本书语言简洁、流畅，内容丰富全面，适用于计算机初中级用户、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人群，计算机培训班也可以将其作为辅导用书。

图书在版编目(CIP)数据

黑客攻防从入门到精通. 命令实战篇: 全新升级版 / 明月工作室, 宗立波编著. —北京: 北京大学出版社, 2016.12

ISBN 978-7-301-27777-5

I. ①黑… II. ①明… ②宗… III. ①黑客—网络防御 IV. ①TP393.081

中国版本图书馆CIP数据核字(2016)第280198号

书 名: 黑客攻防从入门到精通 (命令实战篇·全新升级版)

HEIKE GONGFANG CONG RUMEN DAO JINGTONG

著作责任者: 明月工作室 宗立波 编著

责任编辑: 尹 毅

标准书号: ISBN 978-7-301-27777-5

出版发行: 北京大学出版社

地 址: 北京市海淀区成府路205号 100871

网 址: <http://www.pup.cn> 新浪微博: @北京大学出版社

电子信箱: pup7@pup.cn

电 话: 邮购部62752015 发行部62750672 编辑部62580653

印 刷 者: 北京大学印刷厂

经 销 者: 新华书店

787毫米×1092毫米 16开本 30.5印张 663千字

2016年12月第1版 2016年12月第1次印刷

印 数: 1-3000册

定 价: 65.00元

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有，侵权必究

举报电话: 010-62752024 电子信箱: fd@pupku.edu.cn

图书如有印装质量问题，请与出版部联系，电话: 010-62756370

前言 · 全新升级版

INTRODUCTION

从2003年起，中国互联网逐渐找到了适合国情的商业模式和发展道路，互联网应用呈现多元化局面，电子商务、网络游戏、视频网站、社交娱乐等百花齐放。计算机技术及通信技术的进一步发展，持续推动中国互联网新一轮的高速增长，到2008年，中国互联网用户已经达到2.53亿人，首次超过美国，跃居世界首位。

2009年开始，移动互联网兴起；互联网与移动互联网共同营造了当前双网互联的盛世。网络已经成为个人生活与工作中获取信息的重要手段，网络购物也已经成为民众重要的消费渠道。当前，“互联网+”的战略布局与工业4.0的深度发展，使国家经济发展、民众工作生活，都与网络安全休戚相关，一个安全的网络环境是必不可少的。

当前最大的一个问题是广大用户对网络相关软硬件技术的掌握程度远远不够，这就为不法分子提供了大量的机会，借助于计算机网络滋生的各种网络病毒、木马、流氓软件、间谍软件，给广大网络用户的个人信息及财产带来了非常大的威胁。

为提升广大民众对于计算机网络安全知识的掌握程度，做好个人信息财产安全的防护；我们编写了这套“黑客攻防从入门到精通”丛书，本书为其中的《黑客攻防从入门到精通（命令实战篇·全新升级版）》分册。

丛书书目

- 黑客攻防从入门到精通（全新升级版）
- 黑客攻防从入门到精通（Web技术实战篇）
- 黑客攻防从入门到精通（Web脚本编程篇·全新升级版）
- 黑客攻防从入门到精通（黑客与反黑工具篇·全新升级版）
- 黑客攻防从入门到精通（加密与解密篇）
- 黑客攻防从入门到精通（手机安全篇·全新升级版）
- 黑客攻防从入门到精通（应用大全篇·全新升级版）
- 黑客攻防从入门到精通（命令实战篇·全新升级版）
- 黑客攻防从入门到精通（社会工程学篇）

本书特点

(1) 内容全面: 涵盖了从计算机黑客攻防入门, 到专业级的Web技术安全知识, 适合各个层面、不同基础的读者阅读。

(2) 与时俱进: 本书主要适用于Windows 7及更新版本的操作系统用户阅读。尽管本书中的许多工具、案例等可以在Windows XP操作系统下运行或使用, 但为了能够顺利学习本书全部的内容, 强烈建议广大读者安装Windows 7及更高版本的操作系统。

(3) 任务驱动: 本书理论和实例相结合, 在介绍完相关知识点以后, 即以案例的形式对该知识点进行介绍, 加深读者对该知识点的理解和认知能力, 力争彻底掌握该知识点。

(4) 适合阅读: 本书摒弃了大量枯燥文字叙述的编写方式, 而是采用了图文并茂的方式进行编排, 以大量的插图进行讲解, 可以让读者的学习过程更加轻松。

(5) 深入浅出: 本书内容从零起步, 步步深入, 通俗易懂, 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。

读者对象

- (1) 计算机初、中级用户。
- (2) 网店店主、网店管理及开发人员。
- (3) 计算机爱好者、提高者。
- (4) 各行各业需要网络防护的人员、中小企业的网络管理员。
- (5) Web前、后端的开发及管理人员。
- (6) 无线网络相关行业的从业人员。
- (7) 计算机及网络相关的培训机构。
- (8) 大中专院校相关学生。

本书结构及内容

本书共15章。内容由浅入深, 循序渐进, 前后衔接紧密, 逻辑性较强。

第1章 计算机基础知识

第2章 Windows系统中的命令行基础

第3章 配置Windows系统的命令行

第4章 黑客基础知识

第5章 揭秘黑客常用的命令

第6章 批处理BAT文件编程

- 第7章 黑客攻防前的准备工作
- 第8章 揭露基于Windows认证的入侵方式
- 第9章 局域网攻防
- 第10章 远程管理Windows系统攻防
- 第11章 DOS命令攻防
- 第12章 后门技术攻防
- 第13章 流氓软件和间谍软件的清除与防御
- 第14章 制作启动盘进行防御
- 第15章 木马病毒的主动防御清除

超值赠送资源

1. 黑客攻防全能视频

为了读者能全面地了解黑客方面的知识从而有效地防御黑客的不法入侵行为，本书特赠送全能教学视频，视频内容包括社会工程学、黑客攻防入门、信息的扫描与嗅探、木马与病毒的防范、系统漏洞防范、远程控制术、加密与解密、数据备份与恢复、移动网络安全等内容。

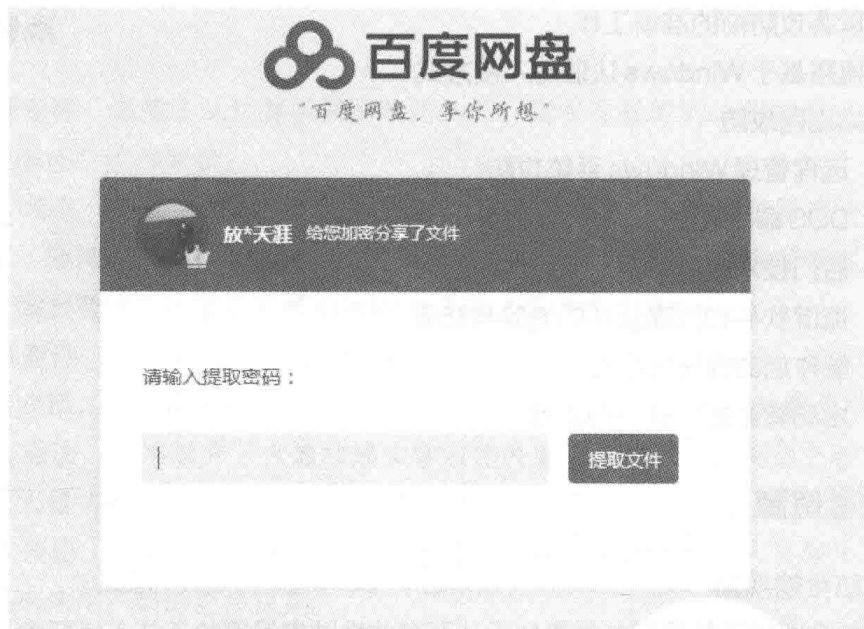
2. 其他赠送资源

- Windows系统安全与维护手册
- 计算机硬件管理超级手册
- Windows文件管理高级手册
- (140个) Windows系统常用快捷键大全
- (157个) Linux基础命令手册
- (136个) Linux系统管理与维护命令手册
- (58个) Linux网络与服务器命令手册
- 黑客攻防命令手册

我们已将赠送内容上传百度网盘，在浏览器中输入下载链接，打开链接后，在如下图所示的文本框中输入提取码便可下载赠送资源。下载链接：<http://pan.baidu.com/s/1eSfvxDK>，提取码：ez6a。

提示

读者也可加入QQ群，在群文件中下载“资源下载地址列表”文档，直接复制链接和密码，下载多媒体视频。（注意：我们会在群文件中共享一些赠送资源，如百度网盘链接失效，请加入QQ群下载资源。）



后续服务

本书由宗立波编著，胡华、王栋、马琳、赵玉萍、闫珊珊、栾铭斌等教师也参加了本书部分内容的编写和统稿工作，在此一并表示感谢！在本书的编写过程中，我们竭尽所能地为您呈现最好、最全的实用功能，但仍难免有疏漏和不妥之处，敬请广大读者不吝指正。若您在学习过程中产生疑问或有任何建议，可以通过E-mail或QQ群与我们联系。

投稿邮箱：pup7@pup.cn

读者信箱：2751801073@qq.com

读者交流群：218192911（办公之家）、99839857

郑重声明

本丛书对大量计算机及移动端的攻击行为进行了曝光，是为广大读者做好安全防范工作。提醒广大读者注意：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是违法的！



第 1 章 计算机基础知识.....	1
1.1 端口的相关概念.....	2
1.1.1 端口的分类.....	2
1.1.2 如何查看端口.....	4
1.2 IP 地址的相关概念.....	5
1.2.1 IP 地址的构成.....	5
1.2.2 IP 地址的分类.....	6
1.3 进程的相关概念.....	7
1.3.1 如何查看系统进程.....	7
1.3.2 系统进程的操作.....	9
1.4 小结.....	10
技巧与问答.....	11
第 2 章 Windows 系统中的命令行基础.....	13
2.1 Windows 命令行基础.....	14
2.1.1 Windows 命令行概述.....	14
2.1.2 Windows 命令行的启动.....	18
2.1.3 Windows 命令行的操作.....	19
2.2 在 Windows 系统中执行 DOS 命令.....	20
2.2.1 通过 IE 浏览器访问 DOS 窗口.....	20
2.2.2 以菜单的形式进入 DOS 窗口.....	21
2.2.3 设置窗口风格.....	22

2.2.4	命令行的复制和粘贴.....	24
2.2.5	Windows 系统命令行介绍.....	25
2.3	全方位揭秘DOS系统.....	27
2.3.1	揭秘DOS系统的功能.....	27
2.3.2	DOS系统中的文件与目录.....	28
2.3.3	DOS系统中的文件类型和属性.....	29
2.3.4	DOS系统中的目录和磁盘.....	31
2.3.5	DOS系统中的命令分类与格式.....	32
2.4	小结.....	33
	技巧与问答.....	34

第3章 配置 Windows 系统的命令行..... 36

3.1	批处理与管道详解.....	37
3.1.1	批处理中常用的命令.....	37
3.1.2	批处理命令实例.....	42
3.1.3	常用的管道命令.....	45
3.1.4	批处理的应用.....	50
3.2	配置Config.sys文件.....	56
3.2.1	Config.sys 文件中的命令.....	56
3.2.2	常用的Config.sys配置项目.....	57
3.2.3	Config.sys配置实例.....	59
3.3	硬盘分区概述.....	61
3.3.1	硬盘分区的相关概念.....	61
3.3.2	命令行工具Diskpart的使用.....	63
3.4	小结.....	72
	技巧与问答.....	72

第4章 黑客基础知识..... 74

4.1	认识黑客.....	75
-----	-----------	----

4.2 黑客的秘诀.....	75
4.3 黑客的常用术语.....	76
4.4 小结.....	78
技巧与问答	79

第5章 揭秘黑客常用的命令..... 81

5.1 必备的CMD命令.....	82
5.1.1 复制命令——Copy命令	82
5.1.2 更改文件扩展名——Assoc命令.....	85
5.1.3 命令行调用——Command命令.....	87
5.1.4 命令行任务管理器——At命令.....	88
5.1.5 查看网络配置的IPConfig命令	92
5.1.6 打开/关闭请求回显功能——Echo命令.....	95
5.1.7 查看系统进程信息——TaskList命令.....	96
5.2 网络命令应用.....	98
5.2.1 查看网络连接——Netstat命令	98
5.2.2 管理工作组和域——Net命令	101
5.2.3 测试物理网络连通——Ping命令	107
5.2.4 文件传输协议——FTP命令	110
5.2.5 远程登录——Telnet命令.....	110
5.2.6 远程修改注册表——Reg命令.....	111
5.2.7 替换文件——Replace命令	115
5.3 其他网络命令应用.....	116
5.3.1 手动配置路由表——Route命令	116
5.3.2 高速缓存——Arp命令	119
5.3.3 路由追踪——Tracert命令.....	120
5.3.4 脚本实用程序——Netsh命令.....	122
5.4 小结.....	124
技巧与问答	124

第 6 章 批处理 BAT 文件编程	127
6.1 批处理文件的编辑	128
6.2 组合命令与参数的使用	129
6.2.1 组合命令的使用	129
6.2.2 参数的使用	132
6.3 配置文件中常用的命令	134
6.3.1 加载程序——Device 命令	134
6.3.2 可存取文件数设置——Files 命令	135
6.3.3 缓冲区数目的分配——Buffers 命令	135
6.3.4 扩展键检查——Break 命令	136
6.3.5 程序加载——Devicehigh 命令	137
6.3.6 扩充内存管理程序——Himem.sys	138
6.3.7 安装内存驻留程序——Install 命令	139
6.3.8 中断处理——Stacks 命令	140
6.4 用 BAT 编程实现综合应用实例	141
6.4.1 删除日志	141
6.4.2 系统加固	142
6.4.3 删除系统中的垃圾文件	144
6.4.4 Windows 7 系统服务优化	147
6.5 小结	150
技巧与问答	150
第 7 章 黑客攻防前的准备工作	153
7.1 在计算机中搭建虚拟环境	154
7.1.1 VMware 虚拟机的安装	154
7.1.2 VMware 虚拟机的配置	158
7.1.3 在 VMware 虚拟机中安装操作系统	161
7.1.4 VMware Tools 安装	165

7.2 小结.....	167
技巧与问答	167
第8章 揭露基于 Windows 认证的入侵方式.....	169
8.1 揭秘IPC\$入侵方式	170
8.1.1 IPC\$的基本概念	170
8.1.2 IPC\$的空连接漏洞.....	171
8.1.3 IPC\$入侵的防范	172
8.2 揭秘注册表入侵方式	180
8.2.1 注册表概述	180
8.2.2 远程开启注册表服务.....	182
8.2.3 连接远程主机的“远程注册表服务”	184
8.2.4 注册表 (Reg) 文件的编辑	186
8.3.5 通过注册表开启终端服务	190
8.3 揭秘Telnet入侵方式.....	191
8.3.1 突破Telnet的NTLM权限认证.....	192
8.3.2 Telnet典型入侵	195
8.3.3 Telnet撒手铜	200
8.3.4 使用工具实现Telnet入侵	202
8.4 揭秘Windows账号和密码获取的入侵方式.....	204
8.4.1 使用Sniffer获取账号和密码.....	205
8.4.2 字典工具的使用	215
8.5 揭秘MS SQL入侵方式.....	222
8.5.1 弱口令入侵的实现.....	222
8.5.2 MS SQL主机的入侵	232
8.5.3 MS SQL入侵的防范.....	233
8.6 小结.....	237
技巧与问答	238

第9章 局域网攻防	240
9.1 局域网安全概述.....	241
9.1.1 局域网的相关概念.....	241
9.1.2 局域网的漏洞.....	241
9.2 MAC地址的绑定和IP冲突攻击的防御.....	242
9.2.1 如何查看MAC地址.....	243
9.2.2 IP冲突攻击的防御.....	243
9.3 ARP欺骗与防御.....	245
9.3.1 ARP欺骗的概念.....	245
9.3.2 网络监听与ARP欺骗.....	246
9.3.3 WinArpAttacker ARP欺骗攻击.....	248
9.3.4 AntiArp-DNS防火墙的使用.....	252
9.3.5 超级巡警ARP防火墙的使用.....	254
9.4 几种局域网监控工具.....	256
9.4.1 长角牛网络监控机的使用.....	256
9.4.2 网络特工的使用.....	266
9.4.3 LanSee工具的使用.....	272
9.5 局域网助手(LanHelper)攻击与防御.....	275
9.6 小结.....	279
技巧与问答.....	280
第10章 远程管理 Windows 系统攻防	282
10.1 曝光FTP远程入侵的实现.....	283
10.1.1 FTP的相关概念.....	283
10.1.2 FTP弱口令的扫描.....	286
10.2 曝光远程计算机管理入侵的实现.....	288
10.2.1 计算机管理概述.....	288
10.2.2 连接到远程计算机.....	290
10.2.3 远程计算机信息的查看.....	292

10.2.4 远程控制软件的使用.....	295
10.3 远程命令执行与进程查杀	296
10.3.1 远程执行命令	297
10.3.2 远程执行命令方法汇总.....	298
10.3.3 查杀系统进程	299
10.4 小结.....	302
技巧与问答	303

第 11 章 DOS 命令攻防..... 305

11.1 DOS 命令的基础应用	306
11.1.1 误删除文件的恢复.....	306
11.1.2 DOS 系统的维护.....	308
11.1.3 在DOS下显示中文信息.....	309
11.2 DOS 中环境变量概述	310
11.2.1 Debug 命令的使用	311
11.2.2 Set 命令的使用	313
11.2.3 识别不同的环境变量.....	314
11.2.4 环境变量和批处理知识.....	317
11.3 在DOS中实现文件操作	318
11.3.1 DOS窗口中文本的抓取	318
11.3.2 DOS中使用注册表.....	321
11.3.3 DOS中注册表编程的实现	321
11.3.4 DOS中注册表扫描程序的使用	323
11.4 网络中DOS命令的使用	323
11.4.1 DOS程序执行目录的检测	324
11.4.2 DOS中恢复回收站的文件	324
11.4.3 内存虚拟盘软件XMS-DSK的使用.....	325
11.4.4 在DOS中删除文件的实现.....	326
11.5 小结.....	327

技巧与问答 327

第 12 章 后门技术攻防 329

12.1 后门技术概述	330
12.1.1 后门的成长史	330
12.1.2 后门的分类	331
12.2 账号后门技术——手动制作克隆账号	332
12.3 系统服务后门技术	342
12.3.1 使用 Instsrv 创建系统服务后门	342
12.3.2 使用 Srvinstw 创建系统服务后门	345
12.4 检测软件中的后门程序	350
12.5 检测系统中的后门程序	351
12.6 小结	352
技巧与问答	353

第 13 章 流氓软件和间谍软件的清除与防御 355

13.1 流氓软件的清除	356
13.1.1 金山系统清理专家清除流氓软件	356
13.1.2 浏览器插件的清理	359
13.1.3 流氓软件的防范	361
13.2 网络安全防护工具的使用	366
13.2.1 诺盾网络安全特警的使用	366
13.2.2 浏览器绑架克星 HijackThis 的使用	381
13.2.3 360 安全卫士的使用	388
13.3 间谍软件的防护与清除	392
13.3.1 间谍软件防护概述	393
13.3.2 Spy Sweeper 消灭间谍软件	394
13.3.3 微软反间谍专家 Windows Defender 的使用	398

13.4 小结.....	404
技巧与问答	404
第 14 章 制作启动盘进行防御.....	407
14.1 启动盘的制作	408
14.1.1 启动盘概述	408
14.1.2 应急启动盘的作用.....	409
14.1.3 DOS 启动盘的制作.....	409
14.1.4 Windows PE 启动盘的制作	412
14.2 使用启动盘排除故障	415
14.2.1 使用启动盘维修注册表故障	416
14.2.2 使用启动盘备份数据.....	417
14.2.3 使用启动盘替换损坏的系统文件	417
14.2.4 用 Windows 诊断工具排除故障.....	418
14.3 U 盘启动盘的使用	422
14.3.1 进入 U 盘系统	422
14.3.2 使用 U 盘启动盘安装系统.....	423
14.4 小结.....	428
技巧与问答	428
第 15 章 木马病毒的主动防御清除	431
15.1 认识木马和病毒.....	432
15.1.1 计算机木马概述	432
15.1.2 计算机病毒概述	435
15.2 使用防火墙隔离系统和病毒.....	437
15.2.1 Windows 防火墙的使用	437
15.2.2 Windows 防火墙入站规则的设置	440
15.3 危险端口的关闭.....	443
15.3.1 通过安全策略关闭危险端口	443

15.3.2	系统安全的设置	449
15.3.3	IP安全策略的自动优化.....	452
15.4	木马清除软件的使用	460
15.4.1	木马清道夫的使用.....	461
15.4.2	木马清除专家的使用.....	462
15.5	杀毒软件的使用.....	466
15.5.1	瑞星杀毒软件的使用.....	466
15.5.2	查杀病毒软件NOD32的使用.....	468
15.6	小结.....	470
	技巧与问答	471