

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

加密与解密篇

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

加密与解密篇

明月工作室 宗立波◎编著

DEFENSE



北京大学出版社
PEKING UNIVERSITY PRESS

内 容 提 要

本书由浅入深、图文并茂地再现了计算机安全方面的知识。

本书主要内容有15章,分别为加密基础知识、软件加密技术、加密算法、解密基础知识、破解技术基础、静态反汇编工具、动态跟踪分析工具、补丁技术、解密壳技术、加密与解密的编程技术、常用软件加密解密技术应用、其他软件加密解密技术应用、光盘的加密解密技术、网络验证技术应用、自制加密工具。

本书语言简洁、流畅,内容丰富全面,适用于计算机中级用户、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计算机中级用户,各大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.加密与解密篇/明月工作室,宗立波编著. — 北京:
北京大学出版社, 2016.12
ISBN 978-7-301-27776-8

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280195号

书 名: 黑客攻防从入门到精通(加密与解密篇)
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 978-7-301-27776-8

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 33.5印张 729千字

2016年12月第1版 2016年12月第1次印刷

印 数: 1-3000册

定 价: 69.00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

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，持续推动着中国互联网新一轮的高速增长。到2008年，中国网民人数已经达到2.53亿人，首次大幅度超过美国，跃居世界首位。

从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，使得国家经济发展、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（加密与解密篇）》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

- 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。
- 与时俱进：本书主要适用于Windows 7及更高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等系统下运行或使用，但为了能够顺利学习本书的全部内容，强烈建议广大读者安装Windows 7及更高版本的操作系统。
- 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。
- 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。
- 深入浅出：本书内容从零起步，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

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

本书结构及内容

本书一共有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 加密基础知识

第2章 软件加密技术

第3章 加密算法

第4章 解密基础知识

第5章 破解技术基础

第6章 静态反汇编工具

第7章 动态跟踪分析工具

第8章 补丁技术

第9章 解密壳技术

第10章 加密与解密的编程技术

第11章 常用软件加密解密技术应用

第12章 其他软件加密解密技术应用

第13章 光盘的加密解密技术

第14章 网络验证技术应用

第15章 自制加密工具



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。

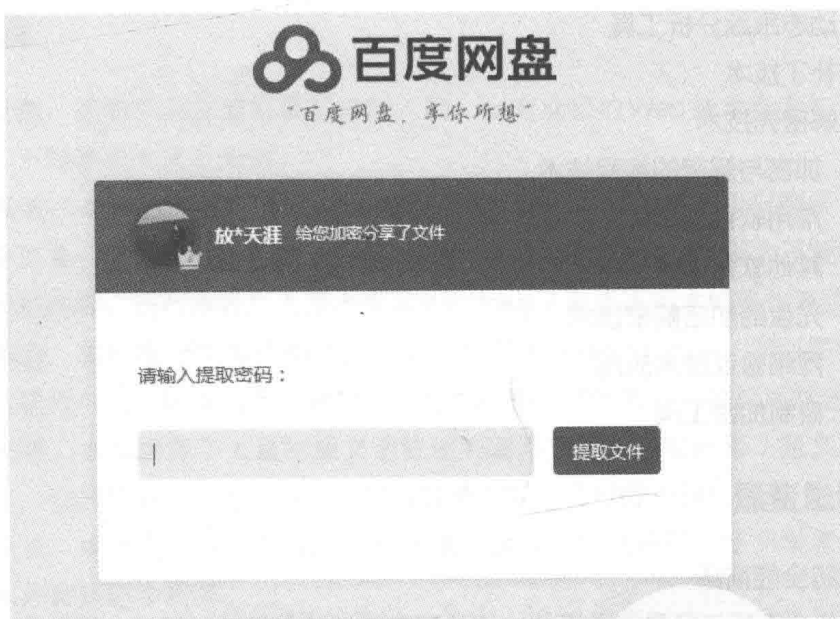
2. 其他赠送资源

- 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

本书由明月工作室宗立波编著，胡华、栾铭斌、王栋、高翔、马琳、赵玉萍、闫珊珊等老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，是为了让广大读者做好安全防范工作。

请本丛书广大读者注意：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！



目录CONTENTS

第 1 章 加密基础知识 1

1.1 探究加密技术	2
1.1.1 理解加密技术	2
1.1.2 摘要算法的分类	3
1.1.3 加密技术的演化	4
1.1.4 加密技术的必要性	5
1.1.5 加密技术的发展前景	6
1.2 软件注册保护方式	7
1.3 加密技术中的相关概念	9
1.4 常用的汇编语言命令	11
1.5 小结	12
技巧与问答	12

第 2 章 软件加密技术 14

2.1 认识口令加密技术	15
2.1.1 口令加密技术的基本概念	15
2.1.2 口令加密软件的起始簇号	16
2.1.3 可执行文件的口令加密	16
2.2 软件狗加密技术概述	21
2.2.1 软件狗加密技术的基本概念	21
2.2.2 软件狗的功能和特点	22
2.2.3 软件狗加密的缺点	23

2.3 探究激光孔加密技术	25
2.4 伪随机数加密技术概述	27
2.5 软件自毁技术基础与实现	31
2.5.1 自毁软件的原理	31
2.5.2 自毁软件的实现	32
2.6 逆指令流技术实现加锁	36
2.7 小结	37
技巧与问答	37

第3章 加密算法..... 39

3.1 单向散列算法详解	40
3.1.1 单向散列算法	41
3.1.2 安全哈希算法	41
3.1.3 信息摘要算法的特点及应用	47
3.1.4 MD5的优势	67
3.2 对称密钥算法详解	68
3.2.1 对称密钥算法	68
3.2.2 对称密钥的加密模式	69
3.2.3 RC4流密码	71
3.2.4 TEA 算法	75
3.2.5 数据加密算法	76
3.2.6 高级加密标准算法概述	78
3.2.7 IDEA 加密算法	80
3.3 非对称密钥加密算法详解	81
3.3.1 非对称密钥算法	81
3.3.2 RSA 公钥加密算法	82
3.3.3 ElGamal 公钥算法	84
3.3.4 Diffie-Hellman 密钥交换系统	86
3.3.5 DSA 数字签名算法	88

3.4 邮件加密软件PGP详解.....	89
3.4.1 认识PGP.....	89
3.4.2 PGP邮件加密软件的原理.....	90
3.4.3 PGP的安全问题.....	92
3.5 小结.....	99
技巧与问答.....	100

第4章 解密基础知识 102

4.1 探究解密技术.....	103
4.1.1 解密技术的基本概念.....	103
4.1.2 解密技术的必要性.....	103
4.1.3 解密技术的发展前景.....	104
4.2 软件解密方式概述.....	104
4.3 解密技术中的相关问题.....	105
4.3.1 软件的破解方式.....	105
4.3.2 破解教程中程序代码地址问题.....	105
4.3.3 如何设置断点的问题.....	106
4.3.4 如何跟踪程序的问题.....	107
4.3.5 软件的反安装问题.....	107
4.4 小结.....	108
技巧与问答.....	108

第5章 破解技术基础 110

5.1 认识PE格式文件.....	111
5.2 掌握代码分析技术.....	113
5.2.1 文件偏移地址与虚拟地址.....	113
5.2.2 搜索程序的入口点.....	116
5.2.3 如何修复输入表.....	120

5.2.4	转储程序概述	121
5.3	了解静态分析技术及其工具	123
5.3.1	静态分析的概念	123
5.3.2	资源编辑器工具	123
5.3.4	掌握反汇编分析工具	128
5.4	动态分析技术及 OllyDbg 工具	130
5.5	流行注册表分析技术及工具	131
5.5.1	注册表监视工具 RegMonitor	131
5.5.2	注册表静态比较工具 Regshot	134
5.5.3	注册表编辑工具 Regedit	136
5.5.4	高级系统注册表编辑工具 Registry Workshop	141
5.5.5	注册表照相机 RegSnap	143
5.6	小结	145
	技巧与问答	146

第 6 章 静态反汇编工具..... 148

6.1	认识常用的反汇编程序	149
6.1.1	程序的基本信息	149
6.1.2	程序的反汇编源代码	151
6.2	静态反汇编工具概述	153
6.2.1	静态反汇编工具 W32Dasm	153
6.2.2	静态反汇编工具 C32asm	169
6.2.3	静态分析软件 IDA Pro	176
6.3	静态分析解密详解	195
6.3.1	静态分析解密的过程概述	195
6.3.2	两种注册判断的修改方法	196
6.3.3	常见指令的机器码值	197
6.4	可执行文件编辑修改工具	198
6.4.1	WinHex 使用简介	198
6.4.2	Hiew 使用简介	199

6.4.3 Hex Workshop 使用简介	205
6.4.4 UltraEdit 使用简介	210
6.4.5 eXeScope 使用简介	217
6.5 小结	221
技巧与问答	222
第 7 章 动态跟踪分析工具	224
7.1 OllyDbg 动态跟踪分析工具	225
7.1.1 认识动态跟踪分析工具 OllyDbg 主窗口	226
7.1.2 配置动态跟踪分析工具 OllyDbg	228
7.1.3 动态跟踪分析工具 OllyDbg 的常用功能与操作	230
7.1.4 动态跟踪分析工具 OllyDbg 的常用插件	235
7.2 动态跟踪分析工具 OllyDbg 动态调试解密	235
7.2.1 动态调试解密过程	236
7.2.2 实例：动态调试解密	236
7.3 小结	242
技巧与问答	243
第 8 章 补丁技术	245
8.1 程序补丁概述	246
8.1.1 补丁的分类	246
8.1.2 如何构成补丁	247
8.2 DLL 劫持内存补丁工具	248
8.3 用 Keymake 制作补丁程序	257
8.3.1 文件补丁程序的制作	257
8.3.2 内存补丁程序的制作	259
8.4 小结	261
技巧与问答	261

第9章 解密壳技术..... 263

9.1 快速理解壳.....	264
9.1.1 认识壳.....	264
9.1.2 壳的作用和分类.....	264
9.2 常见查壳软件的使用方法.....	266
9.2.1 PEiDentifier的使用.....	266
9.2.2 Exeinfo PE的使用.....	268
9.3 几种常见的加壳软件.....	269
9.3.1 穿山甲加壳工具 Armadillo 的使用.....	269
9.3.2 压缩壳 UPX 的使用.....	273
9.3.3 EncryptPE 的使用.....	275
9.3.4 ASPack 的使用.....	278
9.4 几种常见的脱壳软件.....	279
9.4.1 探究脱壳工具 (WSUnpacker v0.20).....	280
9.4.2 万能脱壳工具详解.....	281
9.4.3 详解 RL!dePacker 软件.....	282
9.4.4 随机注册码保护实例.....	283
9.5 小结.....	287
技巧与问答.....	287

第10章 加密与解密的编程技术..... 289

10.1 编程资料基础.....	290
10.1.1 VXD、KMD、WDM 基本概念.....	290
10.1.2 程序自删除的实现.....	290
10.1.3 共享软件安全注册的实现.....	294
10.2 Win32 编程技术概述.....	296
10.2.1 Win32 编程基本概念.....	297
10.2.2 第一个 Win32 程序.....	299
10.2.3 应用程序编程接口.....	309
10.2.4 调试事件.....	313

10.2.5	在调试时创建并跟踪一个进程	315
10.2.6	调试循环体	316
10.2.7	调试事件的处理	317
10.2.8	在另一个进程中注入代码	319
10.3	调试API制作内存补丁	323
10.3.1	跨进程内存存取机制	324
10.3.2	Debug API机制	325
10.4	利用调试API编写脱壳机	333
10.4.1	tElock 脱壳概述	333
10.4.2	编写脱壳机	334
10.5	小结	340
	技巧与问答	341

第 11 章 常用软件加密解密技术应用 343

11.1	Excel 文件的加密解密	344
11.1.1	Excel 功能概述	344
11.1.2	Passware Kit Basic Demo 12.3 的使用	348
11.1.3	Advanced Office Password Recovery Trial 的使用	351
11.1.4	Excel Password Recovery 的使用	353
11.2	邮件加密软件 PGP 的使用	356
11.3	Word 文件的加密解密	365
11.3.1	Word 自身功能加密	365
11.3.2	Word 密码破解器 2016 的使用	369
11.3.3	风语者文件加密器的使用	370
11.3.4	AOPR 解密软件的使用	372
11.4	WinRAR 压缩文件的加密解密	375
11.4.1	WinRAR 加密文件	375
11.4.2	RAR 密码破解 (ARPR) 1.53 绿色版的使用	376
11.4.3	RAR 压缩包密码破解 (RAR Password Recovery) V1.80 特别版的使用	379

11.5	WinZip 压缩文件的加密解密	382
11.5.1	WinZip 加密文件	382
11.5.2	解密 Zip 密码软件 (ARCHPR) 的使用	384
11.5.3	利用 ZIP 密码暴力破解工具探测口令	386
11.6	EXE 文件的加密解密	389
11.6.1	EXE 文件添加运行密码	389
11.6.2	EXE 加壳保护工具下载汉化绿色版的使用	390
11.7	小结	392
	技巧与问答	392

第 12 章 其他软件加密解密技术应用 394

12.1	破解 MS SQL Server 密码	395
12.1.1	SA 口令清除工具的使用	395
12.1.2	实现本地用户的账户登录	397
12.1.3	文件复制的使用	398
12.2	宏加密解密技术的应用	401
12.2.1	宏加密文件	401
12.2.2	破解宏密码	408
12.3	多功能文件加密工具应用	409
12.3.1	“超级加密精灵”的使用	409
12.3.2	“易通文件夹锁”的使用	416
12.3.3	“文件密使”的使用	422
12.3.4	“隐身侠”文件夹加密软件的使用	427
12.4	FTP 密码的探测	433
12.4.1	使用网络刺客 II 探测 FTP 口令	433
12.4.2	“流光”探测 FTP 口令	436
12.4.3	实例：流光针对专门的账户进行穷举探测	438
12.5	多媒体文件加密工具的应用	440
12.5.1	CryptaPix 加密软件的使用	440
12.5.2	Private Pix 加密软件的使用	443

12.5.3 WinXFiles 加密软件的使用	447
12.6 小结.....	452
技巧与问答	452

第 13 章 光盘的加密解密技术..... 454

13.1 认识光盘的加密与解密技术.....	455
13.1.1 光盘加密技术	455
13.1.2 光盘加密流技术	456
13.2 光盘映像 ISO 文件编辑	458
13.2.1 使用光盘加密大师加密光盘	461
13.2.2 光盘加密软件（GiliSoft Secure Disc Creator）的使用	463
13.2.3 IsoBuster Pro 中文破解版的使用	465
13.2.4 加密 DVD 光盘的破解	467
13.2.5 隐藏文件夹、超大文件的制作	473
13.2.6 用光盘隐藏文件查看器对付隐藏文件夹的加密光盘	477
13.3 小结.....	479
技巧与问答	479

第 14 章 网络验证技术应用..... 481

14.1 本地服务器验证加密技术	482
14.1.1 服务器端加密实现.....	482
14.1.2 客户端加密实现	484
14.2 Web 服务器验证加密技术.....	486
14.2.1 本地计算机控制实现.....	486
14.2.2 客户端加密实现	490
14.3 在线升级验证加密技术.....	493
14.3.1 在线升级验证实现.....	493
14.3.2 实例：验证在线升级.....	494

14.4 网络身份认证技术的应用	499
14.4.1 身份认证的含义	500
14.4.2 用户身份认证的技术应用	500
14.4.3 常见的用户身份认证方式	501
14.5 小结	503
技巧与问答	504

第 15 章 自制加密工具 506

15.1 U 盘制作 Windows 开机加密狗	507
15.1.1 U 盘制作 Windows 开机加密狗的制作步骤	507
15.1.2 U 盘遗失情况下的解决办法	511
15.2 手机应用软件加密	512
15.2.1 手机设置应用软件加密	512
15.2.2 使用腾讯手机管家对应用软件加密	514
15.2.3 使用 360 卫士对手机软件进行加锁	516
15.3 小结	518
技巧与问答	519