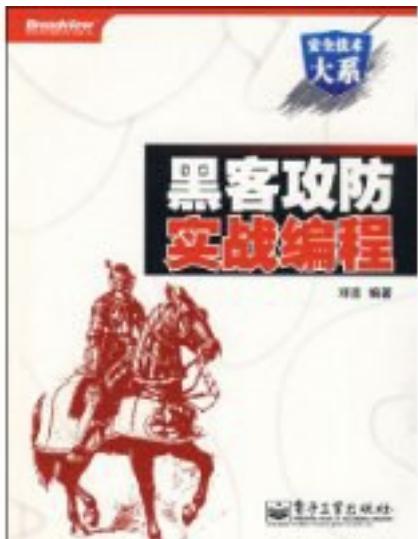


# 黑客攻防实战编程



[黑客攻防实战编程 下载链接1](#)

著者:邓吉

出版者:电子工业出版社

出版时间:2009-6

装帧:

isbn:9787121085376

《黑客攻防实战编程》一书作为《黑客攻防实战入门》、《黑客攻防实战详解》和《黑客攻防实战进阶》的提高篇，仍然以黑客“攻”、“防”的视角，针对目前国内外安全研究的热点和难点问题进行研究，内容涵盖了Web入侵脚本、病毒、木马、网马、加密解密、Shellcode、漏洞溢出渗透、以及漏洞挖掘等相关领域的程序开发研究。《黑客攻防实战编程》适合信息安全领域研究人员、机构、网管和那些对网络感兴趣的在校学生作为参考及教学之用，也适合杀毒软件、木马查杀软件等相关网络安全工具的开发人员作为参考之用。

作者介绍:

目录: 目录  
第1章 Web入侵脚本编程 1

1.1 SQL注入攻击研究 1
1.1.1 测试环境的搭建 1
1.1.2 一个简单的实例 5
1.1.3 用浏览器直接提交数据 10
1.1.4 注入型攻击原理 11
1.1.5 典型攻击过程及代码分析 15
1.1.6 Very-Zone SQL注入漏洞代码分析 20
1.1.7 动易商城2006 SQL注入漏洞代码分析 23
1.1.8 常见的SQL注入漏洞检测工具 28
1.1.9 如何防御SQL注入攻击 34
1.2 跨站脚本攻击 36
1.2.1 跨站攻击的来源 37
1.2.2 简单留言本的跨站漏洞 37
1.2.3 跨站漏洞脚本分析 39
1.2.4 预防和防御跨站漏洞 47
第2章 病毒原理及代码解析 49
2.1 计算机病毒基本知识 49
2.1.1 分类 50
2.1.2 传播途径 51
2.1.3 命名规则 52
2.2 病毒原理及程序分析 54
2.2.1 病毒原理与基础知识 54
2.2.2 重定位变量 62
2.2.3 获取API函数地址 63
2.2.4 文件搜索技术 69
2.2.5 病毒感染技术 69
2.2.6 实例分析 70
2.3 Auto病毒 78
2.4 小结 81
2.5 相关链接与参考资料 81
第3章 木马网马程序分析 82
3.1 木马综述 82
3.1.1 木马的起源 82
3.1.2 木马的种类 83
3.1.3 木马技术的发展 85
3.2 木马的工作原理及程序分析 87
3.2.1 木马的运行机制 87
3.2.2 木马的常见欺骗方式 88
3.2.3 木马的隐藏及其启动方式 89
3.2.4 木马关键技术及程序分析 93
3.3 网页木马 130
3.3.1 概述 130
3.3.2 网页木马与漏洞 132
3.3.3 网马程序分析 134
3.4 小结 136
3.5 相关链接 136
第4章 软件加密与解密 137
4.1 软件加密方法 137
4.1.1 序列号保护 137
4.1.2 软件狗 138
4.1.3 时间限制 139
4.1.4 Key文件保护 139
4.1.5 CD-Check 140
4.1.6 许可证管理方式 140

4.2 软件加密技术和注册机制	141
4.2.1 对称密钥密码体制	141
4.2.2 非对称密钥密码体制	142
4.2.3 单向散列算法	144
4.3 注册机程序分析	144
4.3.1 工作原理	144
4.3.2 生成注册码	146
4.3.3 用户注册	148
4.4 软件解密方法	150
4.4.1 使用OllyDbg	150
4.4.2 使用IDA	155
4.5 软件解密实例分析	159
4.6 反跟踪技术	166
4.6.1 反调试技术	166
4.6.2 断点检测技术	166
4.6.3 反静态分析技术	167
4.7 小结	167
4.8 相关链接与参考资料	167
第5章 ShellCode原理及其编写	168
5.1 缓冲区溢出	168
5.1.1 栈溢出	171
5.1.2 堆溢出	173
5.1.3 格式化字符串漏洞	175
5.1.4 整数溢出引发的缓冲区溢出	177
5.2 ShellCode	180
5.3 定位ShellCode	183
5.4 伪装ShellCode	188
5.5 最后的准备	191
5.5.1 PE文件分析	191
5.5.2 获取Kernel32.dll文件基址	196
5.6 生成ShellCode	201
5.7 ShellCode实例分析	211
5.7.1 漏洞简介	211
5.7.2 WinXP SP1下的ShellCode	212
5.8 小结	216
5.9 相关链接与参考资料	216
第6章 漏洞溢出程序分析与设计	217
6.1 缓冲区溢出漏洞产生的原理	217
6.1.1 栈溢出	218
6.1.2 堆溢出	219
6.2 类Unix下本地溢出研究	220
6.2.1 ret定位	220
6.2.2 构造ShellCode	221
6.2.3 类Unix本地利用方法及实例	224
6.2.4 类Unix下获得root权限的方法	227
6.3 Windows下本地溢出研究	229
6.3.1 ret定位	229
6.3.2 构造ShellCode	230
6.3.3 Windows下本地利用实例	233
6.4 Windows下远程溢出研究	235
6.4.1 Windows下缓冲区溢出	235
6.4.2 Windows下远程溢出实例分析	240
6.5 自动化溢出测试工具Metasploit	245
6.5.1 简介	245

6.5.2 msfweb模式	246
6.5.3 实例分析--ms03-026	254
6.5.4 msfconsole模式	256
6.6 防范溢出漏洞	262
6.6.1 编写安全的代码	262
6.6.2 堆栈不可执行	267
6.6.3 检查数组边界	268
6.6.4 数据段不可执行	268
6.6.5 硬件级别保护	268
6.7 小结	269
6.8 相关链接与参考资料	269
附表:Metasploit Payload列表	269
第7章 漏洞挖掘与Fuzzing程序设计	271
7.1 漏洞概述	271
7.2 Fuzzing技术简介	272
7.2.1 黑盒测试与Fuzzing技术	272
7.2.2 Fuzzing漏洞挖掘实例分析	273
7.3 Fuzzing工具	285
7.3.1 Fuzz	285
7.3.2 Ftpfuzz	292
7.3.3 FileFuzz	303
7.4 Fuzzing程序设计	310
7.4.1 Python脚本语言	310
7.4.2 Fuzzing工具的开发	339
7.4.3 Python攻击脚本编写	350
7.5 小结	359
7.6 相关链接与参考资料	360
• • • • • (收起)	

[黑客攻防实战编程\\_下载链接1](#)

标签

安全

黑客

编程

IT

计算机

hacker

Hack

信息安全

评论

比较原理的东西，讲得也蛮好懂得。就是代码例子太少，且知识有点老了。  
当然还是很有用的。。。

---

[黑客攻防实战编程 下载链接1](#)

书评

---

[黑客攻防实战编程 下载链接1](#)