

Reversing



[Reversing_下载链接1](#)

著者:艾拉姆 (Eilam,E.)

出版者:电子工业出版社

出版时间:2007-9

装帧:

isbn:9787121049958

本书描述的是在逆向与反逆向之间展开的一场旷日持久的拉锯战。作者Eldad Eilam以一个解说人的身份为我们详尽地评述了双方使用的每一招每一式的优点与不足。

书中包含的主要内容有：操作系统的逆向工程；.NET平台上的逆向工程；逆向未公开的文件格式和网络协议；逆向工程的合法性问题；拷贝保护和数字版权管理技术的逆向工程；防止别人对你的代码实施逆向工程的各种技术；恶意程序的逆向工程；反编译器的基本原理以及它对逆向过程的影响。

本书适合软件逆向工程的从业人员...

作者介绍:

Eldad

Eilam逆向工程领域顾问。他帮助客户解决处理操作系统和深入的软件逆向工程问题，并数年致力于开发高级逆向工程技术。

目录: 第1部分 逆向101

第1章 基础 3

1.1 什么是逆向工程 3

1.2 软件逆向工程：逆向 4

1.3 逆向应用 4

1.3.1 与安全相关的逆向 5

1.3.2 软件开发中的逆向 8

1.4 底层软件 9

1.4.1 汇编语言 10

1.4.2 编译器 11

1.4.3 虚拟机和字节码 12

1.4.4 操作系统 13

1.5 逆向过程 13

1.5.1 系统级逆向 14

1.5.2 代码级逆向 14

1.6 工具 14

1.6.1 系统监控工具 15

1.6.2 反汇编器 15

1.6.3 调试器 15

1.6.4 反编译器 16

1.7 逆向合法吗？ 17

1.7.1 互操作性 17

1.7.2 竞争 18

1.7.3 版权法 19

1.7.4 商业机密和专利权 20

1.7.5 美国数字千禧版权法 20

1.7.6 DMCA案例 22

1.7.7 许可证协议 23

1.8 代码范例与工具 23

1.9 结论 23

第2章 底层软件 25

2.1 高阶视角 26

2.1.1 程序结构 26

2.1.2 数据管理 29

2.1.3 控制流 32

2.1.4 高级语言 33

2.2 低阶视角 37

2.2.1 底层数据管理 37

2.2.2 控制流 43

2.3 汇编语言101 44

2.3.1 寄存器 44

2.3.2 标志位 46

2.3.3 指令格式 47

2.3.4 基本指令 48

2.3.5 范例	52
2.4 编译器和编译入门	53
2.4.1 定义编译器	54
2.4.2 编译器架构	55
2.4.3 列表文件	58
2.4.4 专用编译器	59
2.5 执行环境	60
2.5.1 软件执行环境（虚拟机）	60
2.5.2 现代处理器的硬件执行环境	63
2.6 结论	68
第3章 Windows基础知识	69
3.1 组件及基本架构	70
3.1.1 简要回顾	70
3.1.2 特征	70
3.1.3 支持的硬件	71
3.2 内存管理	71
3.2.1 虚拟内存和分页	72
3.2.2 工作集	74
3.2.3 内核内存和用户内存	74
3.2.4 内核内存空间	75
3.2.5 区段对象	77
3.2.6 VAD树	78
3.2.7 用户模式的内存分配	78
3.2.8 内存管理API	79
3.3 对象与句柄	80
命名对象	81
3.4 进程与线程	83
3.4.1 进程	84
3.4.2 线程	84
3.4.3 运行状态切换	85
3.4.4 同步对象	86
3.4.5 进程初始化顺序	87
3.5 应用程序编程接口	88
3.5.1 Win32 API	88
3.5.2 本地API	90
3.5.3 系统调用机制	91
3.6 可执行文件格式	93
3.6.1 基本概念	93
3.6.2 映像区段（Image Sections）	95
3.6.3 区段对齐（Section Alignment）	95
3.6.4 动态链接库	96
3.6.5 头部	97
3.6.6 导入与导出	99
3.6.7 目录	99
3.7 输入与输出	103
3.7.1 I/O系统	103
3.7.2 Win32子系统	104
3.8 结构化异常处理	105
3.9 结论	107
第4章 逆向工具	109
4.1 不同的逆向方法	110
4.1.1 离线代码分析	110
4.1.2 现场代码分析	110
4.2 反汇编器——ILDasm	110

- 4.3 调试器 116
 - 4.3.1 用户模式调试器 118
 - 4.3.2 内核模式调试器 122
- 4.4 反编译器 129
- 4.5 系统监控工具 129
- 4.6 修补工具 131
- Hex Workshop 131
- 4.7 其他类型的逆向工具 133
- 可执行程序转储工具 133
- 4.8 结论 138
- 第2部分 应用逆向
- 第5章 未公开的技术 141
 - 5.1 逆向和互操作性 142
 - 5.2 基本原则 142
 - 5.3 定位未公开的API函数 143
 - 我们要找什么? 144
 - 5.4 案例研究: NTDLL.DLL中的
 - 5.4 Generic Table API 145
 - 5.4.1 RtlInitializeGenericTable 146
 - 5.4.2 RtlNumberGenericTableElements 151
 - 5.4.3 RtlIsGenericTableEmpty 152
 - 5.4.4 RtlGetElementGenericTable 153
 - 5.4.5 RtlInsertElementGenericTable 168
 - 5.4.6 RtlLookupElementGenericTable 188
 - 5.4.7 RtlDeleteElementGenericTable 193
 - 5.4.8 思路整理 194
 - 5.5 结论 196
- 第6章 破译文件格式 199
 - 6.1 Cryptex 200
 - 6.2 使用Cryptex 201
 - 6.3 逆向Cryptex 202
 - 6.4 口令校验过程 207
 - 6.4.1 捕获“Bad Password”消息 207
 - 6.4.2 口令变换算法 210
 - 6.4.3 对口令作hash处理 213
 - 6.5 目录结构 218
 - 6.5.1 分析目录处理代码 218
 - 6.5.2 分析文件项 223
 - 6.6 转储目录结构 227
 - 6.7 文件提取过程 228
 - 6.7.1 扫描文件列表 234
 - 6.7.2 解密文件 235
 - 6.7.3 浮点运算代码 236
 - 6.7.4 解密循环 238
 - 6.7.5 验证Hash值 239
 - 6.8 要点总结 239
 - 6.9 进一步讨论 241
 - 6.10 结论 242
- 第7章 审查程序的二进制码 243
 - 7.1 定义问题 243
 - 7.2 漏洞 245
 - 7.2.1 堆栈溢出 245
 - 7.2.2 堆溢出 255
 - 7.2.3 字符串过滤程序 256

- 7.2.4 整数溢出 256
- 7.2.5 类型转换错误 260
- 7.3 案例研究：IIS索引服务漏洞 262
 - 7.3.1 CVariableSet::
 - 7.3.1 AddExtensionControlBlock 263
 - 7.3.2 DecodeURLEscapes 267
- 7.4 结论 271
- 第8章 逆向恶意软件 273
 - 8.1 恶意软件的分类 274
 - 8.1.1 病毒 274
 - 8.1.2 蠕虫 274
 - 8.1.3 特洛伊木马 275
 - 8.1.4 后门 276
 - 8.1.5 移动代码 276
 - 8.1.6 广告软件和间谍软件 276
 - 8.2 粘人的软件（Sticky Software） 277
 - 8.3 未来的恶意软件 278
 - 8.3.1 盗取信息的蠕虫 278
 - 8.3.2 BIOS/固件恶意软件 279
 - 8.4 恶意软件的使用 280
 - 8.5 恶意软件的弱点 281
 - 8.6 多态 282
 - 8.7 变形 283
 - 8.8 建立安全的环境 285
 - 8.9 Backdoor.Hacarmy.D 285
 - 8.9.1 脱壳可执行文件 286
 - 8.9.2 初次印象 290
 - 8.9.3 初次安装 291
 - 8.9.4 初始化通信设置 294
 - 8.9.5 连接到服务器 296
 - 8.9.6 连接信道 298
 - 8.9.7 与后门进行通信 299
 - 8.9.8 运行SOCK4服务器 303
 - 8.9.9 清理犯罪现场 303
 - 8.10 The Backdoor.Hacarmy.D:
 - 8.10 命令参考 304
 - 8.11 结论 306
- 第3部分 破解
- 第9章 盗版与拷贝保护 309
 - 9.1 世界中的版权 309
 - 9.2 社会方面 310
 - 9.3 软件盗版 310
 - 9.3.1 明确问题 311
 - 9.3.2 群破解 312
 - 9.3.3 需求 313
 - 9.3.4 理论上不可破解的模型 314
 - 9.4 各种类型的保护 314
 - 9.4.1 基于介质的保护 314
 - 9.4.2 序列号 315
 - 9.4.3 质询响应和在线激活 315
 - 9.4.4 基于硬件的保护 316
 - 9.4.5 软件即服务 317
 - 9.5 高级保护的概念 318

- 加密处理器 318
- 9.6 数字版权管理 319
- 数字版权管理模型 320
- 9.7 加水印 321
- 9.8 可信计算 322
- 9.9 破解拷贝保护技术 324
- 9.10 结论 324
- 第10章 反逆向技术 327
- 10.1 为什么要反逆向? 327
- 10.2 反逆向的基本方法 328
- 10.3 消除符号信息 329
- 10.4 代码加密 330
- 10.5 活跃的反调试器技术 331
- 10.5.1 调试器基础 331
- 10.5.2 API函数IsDebuggerPresent 332
- 10.5.3 SystemKernelDebugger Information 333
- 10.5.4 用单步中断检测SoftICE 334
- 10.5.5 陷阱标志 335
- 10.5.6 代码校验和 335
- 10.6 迷惑反汇编器 336
- 10.6.1 线性扫描反汇编器 337
- 10.6.2 递归遍历反汇编器 338
- 10.6.3 应用 343
- 10.7 代码混淆 344
- 10.8 控制流变换 346
- 10.8.1 暗晦谓词 346
- 10.8.2 迷惑反编译器 348
- 10.8.3 表译码 348
- 10.8.4 内联和外联 353
- 10.8.5 交叉代码 354
- 10.8.6 次序变换 355
- 10.9 数据变换 355
- 10.9.1 修改变量编码 355
- 10.9.2 重构数组 356
- 10.10 结论 356
- 第11章 突破保护 357
- 11.1 修补程序 (Patching) 358
- 11.2 生成密钥 364
- 11.3 取密钥生成算法 365
- 11.4 高级破解: Defender 370
- 11.4.1 逆向Defender的初始化程序 377
- 11.4.2 分析解密后的代码 387
- 11.4.3 SoftICE的消失 396
- 11.4.4 逆向分析第二个线程 396
- 11.4.5 击败“杀手 (Killer)”线程 399
- 11.4.6 加载KERNEL32.DLL 400
- 11.4.7 再加密函数 401
- 11.4.8 回到入口点 402
- 11.4.9 解析程序的参数 404
- 11.4.10 处理用户名 406
- 11.4.11 验证用户信息 407
- 11.4.12 解密代码 409
- 11.4.13 暴力破解Defender 409

- 11.5 Defender中的保护技术 415
 - 11.5.1 局部化的函数级加密 415
 - 11.5.2 混淆应用程序与操作系统之间的接口 416
 - 11.5.3 处理器时间戳验证线程 417
 - 11.5.4 在运行时生成解密密钥 418
 - 11.5.5 重度内联 419
- 11.6 结论 419
- 第4部分 反汇编之外
- 第12章 逆向.NET 423
 - 12.1 基本原则 424
 - 12.2 .NET基础 426
 - 12.2.1 托管代码 426
 - 12.2.2 .NET程序设计语言 428
 - 12.2.3 通用类型系统 428
 - 12.3 中间语言 429
 - 12.3.1 求值堆栈 430
 - 12.3.2 活动记录 430
 - 12.3.3 IL指令 430
 - 12.3.4 代码实例 433
 - 12.4 反编译器 443
 - 12.5 混淆器 444
 - 12.5.1 重命名符号 444
 - 12.5.2 控制流混淆 444
 - 12.5.3 中断反编译与中断反汇编 444
 - 12.6 逆向混淆代码 445
 - 12.6.1 XenoCode混淆器 446
 - 12.6.2 Dotfuscator by Preemptive Solutions 448
 - 12.6.3 Remotesoft 混淆器与连接器 451
 - 12.6.4 Remotesoft Protector 452
 - 12.6.5 预编译的汇编程序 453
 - 12.6.6 加密的汇编程序 453
 - 12.7 结论 455
- 第13章 反编译 457
 - 13.1 本地代码的反编译：是一个解决不了的问题吗？ 457
 - 13.2 典型的反编译器架构 459
 - 13.3 中间表示 459
 - 13.3.1 表达式和表达式树 461
 - 13.3.2 控制流图 462
 - 13.4 前端 463
 - 13.4.1 语义分析 463
 - 13.4.2 生成控制流图 464
 - 13.5 代码分析 466
 - 13.5.1 数据流分析 466
 - 13.5.2 类型分析 472
 - 13.5.3 控制流分析 475
 - 13.5.4 查找库函数 475
 - 13.6 反编译器后端 476
 - 13.7 Real-World IA-32反编译 477
 - 13.8 结论 477
- 附录A 解密代码结构 479
- 附录B 理解编译后的算术运算 519

附录C 破译程序数据 537
索引 561
· · · · · (收起)

[Reversing_ 下载链接1](#)

标签

逆向工程

反汇编

计算机

黑客

逆向

编程

计算机技术

安全

评论

这本书中文翻译的不错 感觉作者是真正懂这一块东西的

我的逆向第一本教程，10年读过，16年重读，受用一生。2016.2

内容老

多为基础的泛泛而谈，建议选择看雪入门

感谢大家对博文视点图书的关注

[Reversing_下载链接1](#)

书评

在好几年以前就看过这本书。普通书籍对于逆向工程，要么闭口不言，要么一瞥而过，从来没有这本书讲得这么详细。从工具的使用到分析的技巧，从标准的x86 assemble到.NET的CIL，再从reversing到anti-reversing，如此深入浅出的描述，都让我对作者的功力佩服得五体投地。记得...

书很好，但是amazon不厚道，居然在add this item to basket 下面加了一个buy this item with one click，手一抖就把它直接给买了。

[Reversing_下载链接1](#)