异步图书
www.epubit.com

◎ 理论技术与实战操作相辅相成，凸显“道与术”
◎ 庖丁解牛式剖析 Windows 用户层和内核层黑客技术原理
◎ 代码兼容性高，支持 Windows 7 到 Windows 10 全平台系统

甘迪文 著

Windows 黑客编程技术详解

非外借

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

甘迪文 著

Windows 黑客编程技术详解

人民邮电出版社
北京

图书在版编目（CIP）数据

Windows黑客编程技术详解 / 甘迪文著. -- 北京 : 人民邮电出版社, 2018.12
ISBN 978-7-115-49924-0

Ⅰ. ①W… Ⅱ. ①甘… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2018)第244983号

内 容 提 要

本书介绍的是黑客编程的基础技术，涉及用户层下的 Windows 编程和内核层下的 Rootkit 编程。本书分为用户篇和内核篇两部分，用户篇包括 11 章，配套 49 个示例程序源码；内核篇包括 7 章，配套 28 个示例程序源码。本书介绍的每个技术都有详细的实现原理，以及对应的示例代码（配套代码均支持 32 位和 64 位 Windows 7、Windows 8.1 及 Windows 10 系统），旨在帮助初学者建立起黑客编程技术的基础。

本书面向对计算机系统安全开发感兴趣，或者希望提升安全开发水平的读者，以及从事恶意代码分析研究的安全人员。

◆ 著　　甘迪文
责任编辑　傅道坤
责任印制　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：29
字数：683 千字　　2018 年 12 月第 1 版
印数：1－2 400 册　　2018 年 12 月河北第 1 次印刷

定价：108.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

作者简介

甘迪文，北京邮电大学网络空间安全学院在读研究生，Write-Bug 技术共享平台（www.write-bug.com）创始人，2019 年秋季将步入清华大学攻读软件工程专业的博士学位。对信息安全领域兴趣颇深，常利用课余时间自学和钻研安全开发技术。擅长 Windows 系统安全程序开发，熟悉 Windows 内核编程，闲来无事之时喜欢开发功能各异的小软件。

致谢

本书能够出版发行，需要感谢的人很多，由于篇幅有限，不能一一列举。感谢人民邮电出版社傅道坤编辑对本书的认可与支持，没有他，本书只是我个人的一个想法而已。感谢北京邮电大学崔宝江老师在我研究生期间的传道、授业、解惑，他使我的技术水平得到历练和提升。感谢中国农业大学李婉婷、李思捷和夏琨三位好友，他们对本书的撰写提出许多关键建议，并对书稿文笔进行修改润色，让书稿更加通俗易懂。最后，感谢家人一直以来的支持与鼓励。

前言

信息安全行业是一个朝阳行业，国家、企业以及高校都予以高度重视。其中，Windows 系统的市场占有率高达 90%以上，因此 Windows 系统上的安全需求更多，安全攻防更激烈。

我从本科开始就对黑客技术感兴趣，通过自学，积累了许多这方面的开发技术，并逐渐有了自己的心得和感悟。到了研究生阶段，之前积累的知识帮助我快速而高效地完成了项目的安全开发工作，但是却发现周围仍有很多安全相关专业的同学仍陷于开发难的苦恼中，于是便萌生了写作本书的想法，希望通过分享自己积累的心得体会，让更多的初学者能少走些弯路。

古人云“知其然，知其所以然”。作为一个初学者，首先要做到的是“知其然”，即学会怎么去做；然后再去理解这样做的缘由，即“知其所以然”。本书着重于“知其然”阶段，编写一本能够让初学者看懂的技术科普书。所以，本书在详细介绍每一种黑客技术时，均是按照下述 7 个模块进行写作的。

- **背景**：介绍技术的应用场景。
- **函数介绍**：给出技术实现所需的前提知识。
- **实现原理（过程）**：讲解技术实现的原理。
- **编码实现**：给出技术实现的部分关键代码。
- **测试**：对程序进行测试，给出测试方法和测试结果。
- **小结**：对该技术点进行总结，指出难易点和注意事项。
- **安全小贴士**：针对一些有攻击性的技术，给出检测或防御方法。

本书所包含的知识点循序渐进，语言平实，每个技术点条理清晰，主要有 3 个突出的特点。

- **技术点讲解详细**。因为我是一边编著本书，一边重写程序，所以，能够在书中把实现步骤和注意事项一一指明。
- **知识点兼容性高**。本书的技术以及对应的示例代码（包括内核层下的 Rootkit 技术代码），均支持 32 位和 64 位的 Windows 7、Windows 8.1 和 Windows 10 操作系统。
- **注重实战**。本书所介绍的技术知识都贴近实战技术，可以让读者直接感受到实战的魅力。

由于本书是基于每一个技术点去撰写的，章节独立性较高。所以，读者可以按顺序阅读，也可以选择自己感兴趣的章节跳读。对于每一章的阅读，建议依次按照背景、函数介绍、实现原理、编码实现、测试和总结的顺序进行阅读，这样才能更好地提高自己的安全开发水平。

本书组织结构

本书分为“用户篇”（第 1~11 章）与“内核篇”（第 12~18 章）两篇，总计 18 章。为了帮

助读者更好地了解本书所讲的内容，下面列出了每章所讲的主要内容。

- **第 1 章，开发环境**，主要介绍 VS 2013 开发环境的安装、工程项目的设置，以及关于 Debug 模式和 Release 模式的相关注意事项。
- **第 2 章，基础技术**，介绍了运行单一实例、DLL 延迟加载和资源释放等内容。
- **第 3 章，注入技术**，介绍了全局钩子注入、远线程注入、突破 SESSON 0 隔离的远线程注入、APC 注入等内容。
- **第 4 章，启动技术**，介绍了创建进程 API、突破 SESSON 0 隔离创建用户进程、内存直接加载运行等知识。
- **第 5 章，自启动技术**，涵盖了注册表、快速启动目录、计划任务和系统服务等内容。
- **第 6 章，提权技术**，包含进程访问令牌权限提升、Bypass UAC 等内容。
- **第 7 章，隐藏技术**，讲解了进程伪装、傀儡进程、进程隐藏、DLL 劫持等知识。
- **第 8 章，压缩技术**，介绍了数据压缩 API、ZLIB 压缩库等知识。
- **第 9 章，加密技术**，介绍了 Windows 自带的加密库、Crypto++密码库等知识。
- **第 10 章，传输技术**，介绍了 Socket 通信、FTP 通信、HTTP 通信、HTTPS 通信等知识。
- **第 11 章，功能技术**，讲解了进程遍历、文件遍历、桌面截屏、按键记录、远程 CMD、U 盘监控、文件监控、自删除等知识。
- **第 12 章，开发环境**，介绍了内容开发环境的配置、驱动程序开发与测试、驱动无源码调试、32 位和 64 位驱动开发等知识。
- **第 13 章，文件管理技术**，介绍了文件管理中用到的内核 API、IRP、NTFS 解析等知识。
- **第 14 章，注册表管理技术**，讲解了注册表管理中用到的 API、HIVE 文件解析等知识。
- **第 15 章，HOOK 技术**，介绍了 SSDT HOOK、过滤驱动等知识。
- **第 16 章，监控技术**，讲解了进程创建监控、模块加载监控、注册表监控、对象监控、Minifilter 文件监控、WFP 网络监控等内容。
- **第 17 章，反监控技术**，与第 16 章相反，它介绍了反进程创建监控、反线程创建监控、反模块加载监控、反注册表监控、反对象监控、反 Minifilter 文件监控等内容。
- **第 18 章，功能技术**，介绍了过 PatchGuard 的驱动隐藏、过 PatchGuard 的进程隐藏、TDI 网络通信、强制结束进程、文件保护、文件强删等知识。
- **附录，函数一览表**，介绍了本书使用的函数以及相应的作用。

由于本书中的代码均使用 C/C++来编写，因此掌握 C/C++语言的概念可以更容易理解本书。如果不具备编程知识，也可继续学习并理解所有技术点的开发流程。对于书中的内核层开发部分，即使读者没有接触过内核开发，也可根据本书的内容一步步学习内核开发技术。

最后需要提醒大家的是：

根据国家有关法律规定，任何利用黑客技术攻击他人计算机的行为都属于违法行为。希望读者在阅读本书后一定不要使用本书介绍的技术对他人的计算机进行攻击，否则后果自负。

资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

配套资源

本书提供如下资源：

- 本书源代码。

要获得以上配套资源，请在异步社区本书页面中单击 配套资源，跳转到下载界面，按提示进行操作即可。注意：为保证购书读者的权益，该操作会给出相关提示，要求输入提取码进行验证。

如果您是教师，希望获得教学配套资源，请在社区本书页面中直接联系本书的责任编辑。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，单击“提交勘误”，输入勘误信息，单击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的 100 积分。积分可用于在异步社区兑换优惠券、样书或奖品。

扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。

与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问 www.epubit.com/selfpublish/submission 即可）。

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

“异步图书”是由异步社区编辑团队策划出版的精品 IT 专业图书的品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

异步社区

微信服务号

目录

第1篇 用户篇

第1篇　用户篇

平常计算机上使用的应用程序（例如截屏软件、音乐播放器、图片查看器等），都运行在用户层上，属于用户程序。在 Windows 系统上开发的用户程序，本质上是通过调用 WIN32 API 函数来实现程序功能的。WIN32 API 是一些预先定义的函数，目的是提升开发人员的开发效率，无需访问源码或理解内部工作机制的细节。

与普通的用户程序一样，病毒木马也是通过调用 WIN32 API 函数来实现窃取用户数据的。实质上，它也是一个应用程序，是一个隐蔽而特殊的软件。

本书根据病毒木马运行在用户层还是内核层，分成了用户篇和内核篇两部分。首先介绍用户篇，总计 11 章，主要内容有开发环境、基础技术、注入技术、启动技术、自启动技术、提权技术、隐藏技术、压缩技术、加密技术、传输技术和功能技术等。

01 第1章 开发环境

俗话说“工欲善其事，必先利其器”。选择一个好用的开发平台，会让程序开发事半功倍。对于 Windows 下的黑客来说，首选的开发平台自然是 VS“大礼包”——Microsoft Visual Studio。它在 Windows 程序开发路上是一块不错的“垫脚石”，可以使编程过程更加灵活、得心应手。

Microsoft Visual Studio 是流行的 Windows 平台应用程序的集成开发环境，目前最新版本为 Microsoft Visual Studio 2017 版本，基于.NET Framework 4.5.2。VS 是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具，如 UML 工具、代码管控工具、集成开发环境（IDE）等。所写的目标代码适用于微软支持的所有平台，包括 Microsoft Windows、Windows Mobile、Windows CE、.NET Framework、.NET Compact Framework 和 Microsoft Silverlight 及 Windows Phone。

本章将介绍 VS 2013 的安装过程、使用 VS 2013 开发项目过程中的编译设置以及 Debug 模式与 Release 模式的注意事项。

1.1 环境安装

本书所有的程序开发均是在 VS 2013 上完成的，在正式介绍 VS 2013 开发环境之前，需要到官网上下载安装文件镜像 VS 2013.5_ult_chs.iso 以及多字节 MFC 库安装文件 vc_mbcsmfc.exe。

上述两个安装文件下载完毕之后，就可以进行安装了，本书使用的操作系统是 64 位 Windows 10。安装步骤如下所示。

首先，直接双击运行 VS 2013.5_ult_chs.iso，虚拟镜像文件就会自动加载。打开加载文件的根目录，找到 vs_ultimate.exe 文件并双击运行。设置 VS 2013 安装目录，并勾选同意许可条款选项，如图 1-1 所示，然后单击下一步。

然后，选择要安装的功能模块。为了安装完整，本书安装了全部功能。选择完毕后，单击安装按钮进行安装，如图 1-2 所示。

图 1-1 设置安装路径

图 1-2 选择安装模块

之后要等待一段时间，根据计算机配置的不同等待时间也不同。快则 10 到 20 分钟，慢则要一个多小时，而且中途还需要重启安装，如图 1-3 所示。

在 VS 2013 安装完成之后，继续安装多字节 MFC 库，这个库在开发 MFC 工程项目时需要用到。单击 vc_mbcsmfc.exe 程序，选择安装目录以及勾选同意许可条款选项，并单击安装按钮进行安装，如图 1-4 所示。

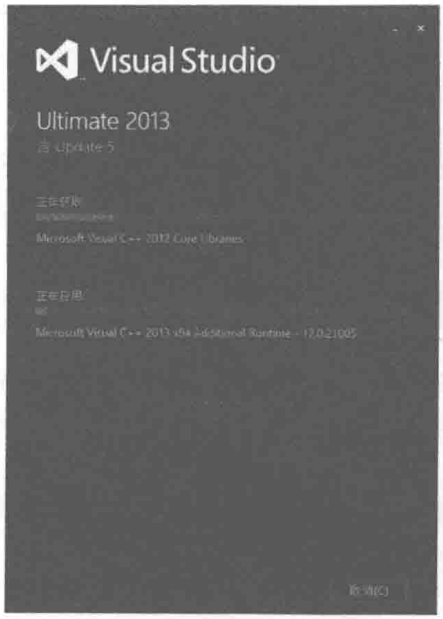

图 1-3 等待安装

图 1-4 安装多字节 MFC 库

上述都安装完成后，即可使用 VS 2013 来创建 MFC 项目、控制台项目或是 DLL 项目了。

1.2 工程项目设置

初学编程时，大多数教程使用的开发环境是 VC 6.0。VC 6.0 编译的是控制台程序或者 DLL，直接编译出来就可以在其他平台上运行或者调用，不需要额外加载运行库 DLL 等。若想使用 VC 6.0 编译出来的 MFC 程序，编译的时候设置在静态库中使用 MFC，即将 MFC 所需的 DLL 组件静态编译到程序里，这样程序在任意平台上运行时都不需要额外附加 MFC 所需的 DLL 文件。

随着技术提升，高效而稳定的开发环境成为大家追求的目标。因此，VC 6.0 慢慢淡出了视线，转而使用 VS 2010、VS 2012、VS 2013、VS 2015，甚至现在的 VS 2017。尽管 VS 系统开发环境的功能确实比较全面，能够提升开发效率，但是，在 VC 6.0 中一些习以为常的习惯（例如编译的设置等），都悄无声息地透露着区别。所以，本书的目的就是教你在使用 VS 系列开发环境的时候，如何设置编译选项，使得生成出来的程序可以直接在其他计算机上运行，就像 VC 6.0 一样，不需要额外加载 DLL 文件。

1.2.1 控制台程序和 DLL 程序的编译设置

之所以把控制台程序和 DLL 程序的编译设置放在一起，是因为它们的设置是一样的。本书以 VS 2013 开发环境为例，演示具体的操作步骤。

打开项目工程之后，右击项目工程，选中并单击“属性”，打开属性页。属性页界面如图 1-5 所示。

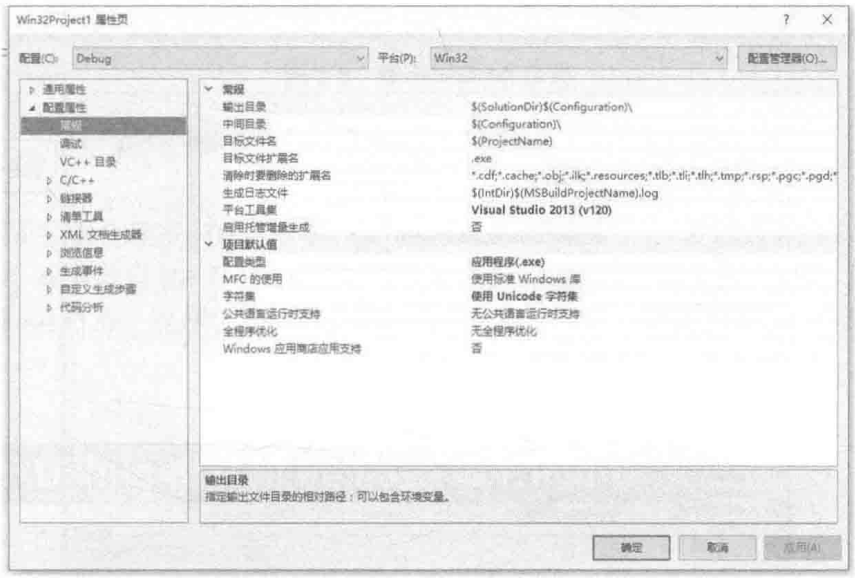

图 1-5 属性页界面