

<<黑客防线2009>>

图书基本信息

书名：<<黑客防线2009>>

13位ISBN编号：9787115205544

10位ISBN编号：711520554X

出版时间：2009-6

出版时间：人民邮电

作者：《黑客防线》编辑部 编

页数：392

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

前言

当今时代的计算机功能十分强大，已经改变了太多传统的生活、工作方式，但是，没有程序的计算机就等于一堆废铁，不会理会我们对它下达的“命令”。

于是，我们要驯服它，只有通过一种方式编程，这也是我们目前和计算机沟通的唯一方式。

在种类纷繁复杂的高级编程语言中，随着技术的发展，经过时间的积淀，接近底层的高级语言VC脱颖而出，它不但易学易用，而且编程效率极高，这也是我们选择VC作为本书编程平台的根本原因。

现在的编程已经成为一种技能，很多人都会用一些基本的编程语言来实现自己需要的功能。

但是高级的编程却越来越重要，在现实社会中的价值也日渐提高，特别是基于各种系统核心函数的应用编程技术更是备受关注。

实际上，系统核心函数的编程运用，最高级的就是包含黑客攻击编程、网络安全防护编程在内的黑客编程！

时下，黑客编程已经成为衡量编程技术实力的标杆之一，但其本质却并没有那么神秘！

在各种编程思路、原理、框架类书籍众多的情况下，本书独辟蹊径，专精于黑客编程实例，用流行的VC为编程平台，以各种实用的网络安全、黑客工具编写为主题，包含木马后门类、扫描监控类、线程注入类、系统核心类、网络协议类和杀毒类程序编写，专注于它们的实例实现技术，并且书中所有代码都经过严格测试，所有代码均经过实际的编译测试，保证读者可以直接使用。

为了将高级黑客编程技术系统地呈现给读者，本书以功能主线为基础，涵盖7大类内容，共120余个黑客编程的具体实例，每一个实例均配合有详细的解说和源代码分析。

木马后门类内容全面介绍了端口复用木马、DLL木马、反弹穿墙木马、Activex启动和注入IE木马、Downloader下载器、3389后门、魔兽盗号木马、经典NameLess后门等实例，并深入讲解了最新的手机远程控制电脑和高级Rootkit开发，为读者呈献一本木马后门编程的实例宝典！

系统核心类内容包含SSDT挂钩、HOOKAPI、ROOtkit深入分析、API拦截、内核文件隐藏和内核键盘记录等内容，还包含最新的内核状态下拦截注册表操作防范木马、内核方法实现进程保护等防护技术，以达到攻防一体的效果。

本书将杀毒软件、杀毒程序的编写整理成集，让以往大家觉得无比神秘的杀毒类软件编程不再神秘。

本书杀毒类内容包含病毒专杀工具、流氓软件专杀工具、蠕虫专杀工具等常见流行安全工具的编写方法，同时还有完整的大型杀毒软件的整体编程规划，绝对物超所值！

除此以外，扫描监控类、线程注入类、网络协议类都包含有丰富的内容，具体的实例期待读者通过阅读本书自己发掘。

<<黑客防线2009>>

内容概要

《黑客防线2009黑客编程VC专辑》独辟蹊径，专精于黑客编程实例，用流行的VC为编程平台，以各种实用的网络安全、黑客工具编写为主题，以功能主线为基础，涵盖7大类内容，包含木马后门类、扫描监控类、线程注入类、系统核心类、网络协议类、杀毒类和其他类程序编写，专注于它们的具体实现技术。

《黑客防线2009黑客编程VC专辑》完全以实例为引导，有代码都经过严格测试，并经过实际的编译测试，保证读者可以直接使用。

《黑客防线2009黑客编程VC专辑》适合网络安全爱好者、程序员、高级网络管理员阅读。

书籍目录

木马后门类VC实现端口复用木马2巧用WM_CREATE消息隐藏DLL木马6VC编写精小反弹穿墙木马8编程实现木马的ActiveX启动和注入IE的启动方式13利用C++让木马也能修改桌面背景16木马编程DIY之系统服务17木马编程DIY之单实例运行21木马编程DIY之注册表管理23木马编程DIY之线程守护27木马编程DIY之服务启动技术29编程实现手机远程控制电脑33为反弹远控服务端减肥37打造自己的VNC后门生成器40B/S模式远程控制简单实现43编写Downloader制造机47自己编程抓“肉鸡”48自己编程抓“肉鸡”——将捕获消息进行到底51基于反向连接的木马编写思路533389后门自己造54编程实现修改注册表完成程序自启动56Windows2003下的进程隐藏58服务级后门自己做61利用远程线程技术制造隐身程序65看我双兔傍地走——编程实现木马合并68用原始套接字创建穿墙木马72让木马藏得更深——线程注射技术新发展(上)76让木马藏得更深——线程注射技术新发展(下)81穿过防火墙的Shell后门83捆绑任意可执行文件做木马85魔兽盗号木马DIY88经典重现之NameLess后门技术全面分析93完整B/S后门开发实战96VC编写获取服务端系统信息的C/S型木马104扫描监控类构造自己的ARP扫描和欺骗工具108文件监控开发过程110利用WinPcap编写驱动Sniffer114直接访问键盘控制芯片获取键盘记录117小波变换+线性预测+LZ77算法实现极速屏幕监控120自己动手编写SQL注入漏洞扫描器126用原始套接字实现网络入侵检测系统129一个简易网络嗅探器的实现135编写调用门键盘记录程序137自己编写IP包监视工具141四种方法实现VC枚举系统当前进程144编写无驱动的Sniffer147键盘监视器原理及反窥探技术149如虎添翼——给嗅探器加上数据还原！154打造自己的程序行为监视器160线程注入类基于EPROCESS结构中双向链表的进程检测方法166卸载远程进程中的DLL168进程的冻结与解冻170植入执行文件穿越软件防火墙172一种基于PspCidTable的进程检测方法174进程隐藏技术解析——DLL远程线程插入主程序177编程实现远程Shell的获取182编程实现线程插入后门防范186SQL注入步步高——打造自己的扫描+注入综合工具189无进程式线程插入穿墙技术实现194搞定远程进程注入DLL——以ShellCode之名199系统核心类利用HookAPI实现进程守护204详解挂钩SSDT206浅窥导入函数及输出导入表的内容209Ring3下安全获取原始SSDT地址211Ring0中HookSSDT防止进程被结束213Ring0下恢复SSDTShadow216让一切输入都难逃法眼——驱动级键盘过滤钩子的实现220内核状态下拦截注册表操作防范木马224妙不可言——挂接ExitWindowsEx227NT操作系统下的Rootkit技术初探228内核级编程实践之进程检测232MessageHook攻与防234API拦截——实现Ring3全局HOOK238内核方法实现进程保护242感染PE文件加载DLL249在内核驱动中检测隐藏进程254主动防御之注册表保护255Ring3下终止江民KV2008259RootKit文件隐藏技术实现262编程打造自己的SSDT恢复工具265基于线程的隐藏进程检测271再谈内核及进程保护274用开源反汇编引擎检测inlinehook277Rootkit端口隐藏实现279Ring0中强行结束进程283直接调用NTFS文件驱动检测隐藏文件285用文件系统过滤驱动实现文件隐藏289InlinehookKeyboardClassServiceCallback实现键盘记录291恢复Ring0下的IAT与EAThook295网络协议类套接字编程实现网页内容的获取301编程实现DRDoS攻击302邮件群发器的分析与实现304DNS放大攻击原理、实现与防御306再谈邮件服务器的编写307基于SMTP/POP3协议的新型僵尸网络实现311IRCBOT，由协议分析到编程实现315Windows环境下实现原始UDP数据包发送319教你实现TFTP协议322基于Winpcap的原始数据包发送325NAT穿透之NAT类型检测327网络数据包捕获与发送的多重实现330ARPSpoof&DoS攻击编程实战334杀毒类病毒专杀工具编写DIY339编写自己的流氓软件专杀工具342菜鸟也会编写杀毒软件344浅谈蠕虫病毒的特性346自己编写ANI蠕虫专杀工具347仿制“熊猫烧香”，编程实现病毒特性349手把手教你编写威金病毒清除工具350打造专版的还原精灵密码读取工具353检测PE文件的有效性354枚举注册表搜索病毒痕迹的实现思路356简单打造蠕虫病毒专杀工具358其他类编写自己的搜索引擎查找用户QQ群362VC轻松打造Spy++364OfficeSpyDIY370盗号研究怎能缺少新浪UC372编程PK迅雷QQ暴力广告374也谈VC打造U盘防火墙376利用WinInet和多线程实现实时显示下载进度条378使用过滤驱动打造防火墙381图标大挪移——资源更新法更新程序图标383DES加密软件的实现385

章节摘录

木马后门类 VC实现端口复用木马 不知大家是否还记得《黑客防线》杂志上曾发表过的《编程打造cmdshell客户端》这篇文章7那篇文章主要是讲一个命令行下网络通信的模型。我起初是为编写自己的端口复用木马服务的，下面我就把这个不影响原服务的端口复用木马继续完成吧！

其实想实现端口复用很容易，在创建了一个SOCKET之后。用setsockopt设置SOCKET的SO_REUSEADDR属性就可以了。当然，要防止别人复用你的端口也很简单，用setsockopt指定SO_EXCLUSIVEADDRUSE就可以独占端口地址了。

我在开始编写前下载了一个wxhshell。它是加了端口复用功能的WinShell。我自己试了一下它的功能，发现在Windows XP+SP2+IIS5.1下可成功，在Windows 2003+1 1S6，0下没有成功。而在Windows XP下正常工作时，IIS就不能正常工作了，这要是放在“肉鸡”上，别人的网页都访问不了了，那管理员就会轻易发现问题。因此，这篇文章的重点就在这里——正确区分木马访问和正常的IIS访问，然后再分别加以处理。

编辑推荐

《黑客防线2009黑客编程VC专辑》编程平台的根本原因。

现在的编程已经成为一种技能，很多人都会用一些基本的编程语言来实现自己需要的功能。

但是高级的编程却越来越重要，在现实社会中的价值也日渐提高，特别是基于各种系统核心函数的应用编程技术更是备受关注。

以VC为编程平台，以各种实用的网络安全，黑客工具编写为主题。

内容涵盖木马后门类、扫描监控类、线程注入类、系统核心类、网络协议类和杀毒工具类程序编写。

120余篇编程实例解析，将黑客VC编程技术系统地呈现给读者。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>