第一图书网, tushu007.com

<<Visual C++黑客编程揭秘与防范>>

图书基本信息

书名：<<Visual C++黑客编程揭秘与防范>>

13位ISBN编号：9787115206640

10位ISBN编号：7115206643

出版时间：2009-7

出版时间：人民邮电出版社

作者：梁洋洋

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

能编写出属于自己的防范黑客软件一直是很多网络安全爱好者梦寐以求的。
然而由于各种编程技术的门槛较高，加之很少能找到相关的学习资料和具体技术细节，很多安全爱好者只能叹息黑客编程技术遥不可及。
笔者在初学网络编程时也有同样的困惑，因此，非常能理解很多读者一直不得入门的心情。
为了让更多的网络安全爱好者能够迅速掌握防范黑客软件和安全工具的开发技术，也为了提高国内网络安全技术的整体水平，笔者精心编写了本书。
本书是根据自己多年的学习和工作经验，结合当前网络安全技术最新的发展趋势，循序渐进地为读者讲解了，如何在VisualC++（简称VC）环境下开发各种防范黑客工具和安全软件。
本书旨在技术上为读者提供一种学习的方法和参考，以便在实践中逐步提高防范黑客的技能。
本书的特点　　本书通过4篇（基础篇、提高篇、综合篇、拓展篇）内容，循序渐进地为读者讲解了当前流行的网络安全技术，以及黑客软件和安全工具的实现原理及编程实现方法。
本书涵盖的内容丰富，从WindowsSocket及API编程基础到最基本的网络扫描器编程，从基本防范黑客攻击程序到基于认证的网络程序破解，从下载者程序的编程实现到u盘防火墙等安全工具实现，从Windows底层的RootKit编程到远程控制软件开发，从网络准入控制技术到网络蜘蛛编程等。
本书都逐个讲解各类技术的实现原理，并通过代码编程实现，其中很多代码具有很高的实用价值。
本书的特点主要体现在以下几个方面。
· 本书的编排采用循序渐进的方式，适合于对VC程序开发有一定了解，并对黑客程序开发抱有兴趣的网络安全爱好者。
· 本书在介绍大量网络安全技术实现原理时，均提供了典型的案例和参考图例。
读者通过对原理的学习，能够掌握用VC开发黑客工具的具体技术，同时，也能更加深入地理解网络安全技术的具体细节。
· 本书除了介绍主流的安全技术及编程方法外，还涉及到RootKit、SSDT恢复等系统底层编程技术，对于希望提高黑客软件开发技术的读者无疑是一个很大的帮助。
· 本书虽然以剖析黑客软件开发为基本出发点，但是并不限于黑客技术，更多的是从技术角度探讨技术原理及实现方法，同时将网络安全思想时刻灌输其中。
如书中涉及的U盘防火墙、网络准入技术等都是对当前互联网黑客攻击泛滥的思考和防范方法的具体实现。

内容概要

《Visual C++黑客编程揭秘与防范》全面介绍了在VisualC++环境中，使用WindowsSocket及API开发各类防范黑客软件及安全防护工具的编程实现方法，深入剖析了目前热门的黑客编程技术。
《Visual C++黑客编程揭秘与防范》通过基础篇、提高篇、综合篇和拓展篇这种循序渐进地方式，向读者介绍了防范黑客攻击程序、安全防护工具、远程控制软件和网络安全管理软件的原理及具体编程实现方法。
《Visual C++黑客编程揭秘与防范》内容丰富，实用性和实战性强，不仅包括读者必备的防范黑客的编程知识，更深入阐述了网络编程方面的高级技术。
不仅适用于黑客程序开发，在读者掌握了《Visual C++黑客编程揭秘与防范》介绍的各种编程技术后，还能用于开发各类网络安全防护软件。
《Visual C++黑客编程揭秘与防范》适合初、中级网络安全爱好者学习网络安全知识时使用，同时也可作为程序员和网络高级安全工程师的参考用书。

作者简介

梁洋洋，历任程序员、测试工程师、技术支持工程师等职位，曾在国内著名的安全公司做研发工作，在远程控制、黑客攻防技术、网络编程、Windows编程、杀毒工具实现上有丰富的软件开发经验。

书籍目录

第一篇 基础篇第1章 开发网络安全程序基础 21.1 认识Windows API和Socket 21.1.1 Windows API编程的优点 21.1.2 Socket通信流程 31.2 服务器端Socket编程 41.2.1 使用Socket前的准备工作 41.2.2 建立Socket 41.2.3 绑定端口 51.2.4 监听端口 61.2.5 创建服务器端接受客户端请求 61.2.6 服务器端响应客户端连接请求 71.2.7 完成服务端与客户端Socket连接 81.3 客户端Socket编程 91.3.1 建立客户端的Socket 91.3.2 发起连接申请 91.4 用Socket实现数据的传送 91.4.1 认识TCP Socket与UDP Socket 101.4.2 发送和接收数据的函数 101.5 自定义Socket通信类 121.5.1 使用类的意义 121.5.2 VC中创建通信类 131.5.3 通信类的代码实现 161.6 小结 21第2章 网络扫描器程序的实现和代码分析 222.1 扫描器的产生及原理 222.1.1 扫描器的产生 222.1.2 各种扫描器的原理及性能简介 232.2 主机扫描技术 252.2.1 ICMP Echo扫描 252.2.2 ARP扫描 252.3 端口扫描技术 272.3.1 常用端口简介 272.3.2 TCP connect扫描 282.3.3 TCP SYN扫描 282.4 操作系统识别技术 292.4.1 根据ICMP协议的应用得到TTL值 292.4.2 获取应用程序标识 302.4.3 利用TCP/IP协议栈指纹鉴别 302.4.4 操作系统指纹识别依据 302.4.5 操作系统指纹识别代码实现 332.4.6 Web站点猜测 402.4.7 综合分析 412.5 扫描器程序实现 422.5.1 ICMP echo扫描原理 432.5.2 ICMP echo扫描的实现方法 442.5.3 ARP扫描的原理 482.5.4 ARP扫描的实现方法 482.5.5 TCP SYN扫描的原理 532.5.6 TCP SYN扫描的实现方法 542.5.7 综合应用实例-ARP欺骗程序 562.5.8 ARP欺骗的原理 562.5.9 环境初始化 572.5.10 欺骗主程序实现 612.6 资产信息扫描器开发 662.6.1 资产信息扫描器的应用范围 662.6.2 扫描器的原理(基于SNMP协议) 662.6.3 扫描器的实现方法(基于SNMP协议) 672.7 小结 69第3章 基于认证的扫描程序 703.1 通信认证的暴力破解剖析 703.1.1 FTP协议暴力破解原理 703.1.2 FTP协议暴力破解实现方法 703.1.3 IMAP协议破解原理 723.1.4 IMAP协议破解实现方法 733.1.5 POP3协议暴力破解原理 743.1.6 POP3协议暴力破解实现方法 753.1.7 Telnet协议暴力破解原理 773.1.8 Telnet协议暴力破解实现方法 773.2 防范恶意扫描及代码实现 793.2.1 防范恶意扫描的原理 803.2.2 防范恶意扫描的实现方法 803.3 小结 83第二篇 提高篇第4章 拒绝服务攻击剖析及防范 864.1 拒绝服务原理及概述 864.1.1 拒绝服务攻击技术类别 864.1.2 拒绝服务攻击形式 874.2 拒绝服务攻击原理及概述 884.2.1 DoS攻击剖析 884.2.2 DDoS攻击剖析 884.2.3 DRDoS攻击剖析 894.2.4 CC攻击剖析 904.3 拒绝服务攻击原理剖析 904.3.1 DoS实现的原理 904.3.2 DRDoS攻击实现剖析 1074.3.3 CC攻击实现剖析 1154.3.4 修改连接数限制 1174.4 拒绝服务攻击防范 1214.4.1 拒绝服务攻击现象及影响 1214.4.2 DoS攻击的防范 1214.4.3 DRDoS攻击的防范 1224.4.4 CC攻击的防范 1224.5 小结 124第5章 感染型下载者 1255.1 感染功能描述 1255.1.1 话说熊猫烧香病毒 1255.1.2 认识“ 下载者 ” 1265.1.3 感染功能描述 1275.2 感染型下载者工作流程剖析 1335.3 感染磁盘剖析 1355.3.1 感染所有磁盘原理 1355.3.2 感染所有磁盘的方法 1355.4 感染U盘和移动硬盘剖析 1355.4.1 U盘和移动硬盘感染的原理 1365.4.2 U盘和移动硬盘感染剖析 1365.5 关闭杀毒软件和文件下载的原理剖析 1395.5.1 关闭杀毒软件的原理 1395.5.2 关闭杀毒软件和文件下载的方法 1395.6 结束指定进程 1425.6.1 结束指定进程的原理 1435.6.2 结束指定进程的实现方法 1435.6.3 暴力结束进程 1445.7 局域网感染 1505.7.1 局域网感染原理 1505.7.2 局域网感染的方法 1505.8 隐藏进程 1535.8.1 隐藏进程的原理 1535.8.2 隐藏进程的实现方法 1545.9 感染可执行文件 1555.9.1 感染可执行文件的原理 1555.9.2 感染可执行文件的方法 1555.10 感染网页文件 1585.10.1 感染网页文件的原理 1585.10.2 感染网页文件的实现方法剖析 1585.11 多文件下载 1605.11.1 多文件下载的原理 1605.11.2 多文件下载的实现方法 1605.12 自删除功能 1625.12.1 自删除功能的原理 1625.12.2 自删除功能的实现方法 1625.13 下载者调用外部程序 1635.13.1 下载者调用外部程序的原理 1635.13.2 下载者调用外部程序的实现方法 1635.14 “ 机器狗 ” 程序 1665.14.1 “ 机器狗 ” 程序原理 1675.14.2 “ 机器狗 ” 实现剖析 1685.15 利用第三方程序漏洞剖析 1725.16 程序其他需要注意的地方 1745.16.1 窗口程序的创建 1745.16.2 应用程序互斥处理 1755.16.3 禁止关闭窗口 1765.17 小结 176第6章 下载者程序的防范 1776.1 下载者的防范措施 1776.1.1 U盘感染的防范 1776.1.2 驱动级病毒的防范 1796.1.3 阻止第三方程序引起的漏洞 1806.1.4 本地计算机防范ARP程序运行 1816.1.5 其他需要注意的地方 1826.2 U盘病毒防火墙的开发 1826.2.1 U盘病毒防火墙的功能及实现技术 1826.2.2 U盘病毒防火墙的代码实现 1836.3 小结 188第7章 浅谈RootKit 1897.1 RootKit与系统内核功能 1897.1.1 RootKit简介 1897.1.2 RootKit相关的系统功能 1897.1.3 Rootkit的分类及实现剖析 1907.2 RootKit对抗杀毒软件剖析 1937.2.1 增加空节来感染PE文件 1937.2.2 通过Rootkit来绕过网络监控 1987.2.3 绕过主动防御的方法 2007.2.4 关于进程PEB结构的修改实现 2027.2.5 RootKit程序实例

2057.3 小结 210第三篇 综合篇第8章 用VC开发远程控制软件 2128.1 远程控制软件简介 2128.1.1 远程控制软件的形式 2128.1.2 远程控制软件的特点 2138.2 远程控制软件的功能 2148.2.1 反向连接功能 2148.2.2 动态更新IP功能 2148.2.3 获取详细的计算机配置信息 2158.2.4 进程管理功能 2158.2.5 服务管理功能 2168.2.6 文件管理功能 2168.2.7 远程注册表管理 2168.2.8 键盘记录 2168.2.9 被控端的屏幕截取及控制 2178.2.10 视频截取 2178.2.11 语音监听 2178.2.12 远程卸载 2178.2.13 分组管理 2178.3 控制软件的技术指标 2178.3.1 隐蔽通信 2188.3.2 服务端加壳压缩 2188.3.3 程序自身保护技术 2228.3.4 感染系统功能 2238.4 小结 223第9章 远程控制软件的通信架构 2249.1 设计远程控制软件连接方式 2249.1.1 典型的木马连接方式 2249.1.2 反弹型木马连接 2259.2 基本传输结构的设计 2259.2.1 基本信息结构 2259.2.2 临时连接结构 2269.2.3 进程通信结构 2269.2.4 设计结构成员变量占用空间的大小 2279.3 命令调度过程的结构设计 2279.3.1 设计进程传递的结构 2289.3.2 优化结构成员变量占用空间的大小 2289.3.3 传输命令结构体定义 2299.3.4 传输命令结构的设计 2299.4 小结 236第10章 远程控制软件功能模块的实现——基础功能 23710.1 反弹端口和IP自动更新 23710.1.1 反弹端口原理 23710.1.2 更新IP模块代码实现 23910.2 基本信息的获得 24010.2.1 获得硬盘序列号 24010.2.2 获得服务端计算机的基本信息 25010.3 IP地址转换物理地址 25210.3.1 QQWry.Dat基本结构 25210.3.2 了解文件头 25310.3.3 了解记录区 25310.3.4 设计的理由 25410.3.5 IP地址库操作类 25610.4 小结 265第11章 远程控制软件功能模块的实现——标准功能 26611.1 进程管理 26611.1.1 Windows自带的任务管理器 26611.1.2 进程管理实现的原理 26711.1.3 进程管理相关API函数的介绍 26711.1.4 进程管理功能实现 26911.2 文件管理 27311.2.1 服务器端两个重要的函数 27411.2.2 客户端对应的两个函数 27511.3 服务管理 27711.3.1 客户端代码 27711.3.2 服务端代码 27811.4 服务端启动和网络更新 27911.4.1 服务启动工作函数 28011.4.2 网络下载器的选择和代码实现 28011.4.3 分析下载文件并反弹连接 30011.4.4 上线设置 30111.5 远程控制命令 30211.5.1 客户端代码 30211.5.2 服务端代码 30311.6 小结 304第12章 远程控制软件功能模块的实现——高级功能 30512.1 屏幕捕捉 30512.1.1 屏幕捕捉程序结构 30512.1.2 屏幕捕捉程序代码实现 30612.2 远程屏幕实现方式 31112.2.1 远程屏幕图像在网络上的传输过程 31212.2.2 屏幕抓取与传输实现 31212.2.3 屏幕图像数据流的压缩与解压缩 31412.3 键盘记录 32512.3.1 客户端执行代码 32512.3.2 服务端执行代码 32812.4 小结 329第13章 远程控制软件功能模块的实现——扩展功能 33013.1 客户端历史记录提取及系统日志删除 33013.2 压缩功能的实现 33213.3 DDoS功能模块 33313.3.1 基本DDoS功能模块 33313.3.2 UDP功能模块 33513.3.3 IGMP功能模块 33613.3.4 ICMP 功能模块 33813.3.5 HTTP功能函数 34013.4 SOCKS 5代理实现 34113.5 视频监控模块开发 35113.6 涉密文件关键字查询 35613.7 ADSL拨号连接密码获取的原理剖析 36013.8 小结 365第14章 控制软件后期设计完善 36614.1 版本控制 36614.1.1 SVN简介 36614.1.2 SVN使用 36614.2 界面美化 36814.2.1 概论 36814.2.2 具体操作步骤 36914.2.3 添加系统托盘 37014.3 小结 371第四篇 拓展篇第15章 网络安全编程技术延伸 37415.1 内网准入控制技术发展分析 37415.1.1 局域网接入控制技术发展分析 37415.1.2 可行的内网接入管理方案 37415.1.3 软件接入网关的原理 37515.1.4 软件接入网关的配置及实现 37515.1.5 硬件接入网关的原理 37615.1.6 硬件接入网关的认证程序流程 37715.1.7 联动802.1x接入认证的流程 37815.1.8 802.1x下的局域网准入控制方案 37915.2 网络蜘蛛在安全领域的应用 38115.2.1 网络蜘蛛的工作原理 38115.2.2 简单爬虫的代码实现 38215.3 SSDT及其恢复 38615.3.1 认识SSDT 38615.3.2 编程恢复SSDT 38715.4 小结 392

章节摘录

第一篇　基础篇　　第1章　开发网络安全程序基础　　1.1　认识Windows API和Socket　　稍微有过Windows API编程经验的人员都知道，强大的Windows网络程序都是通过灵活的API编程实现的。这些Win32 API函数是网络编程中最基础的函数，在任何网络程序中都会用到。
下面各小节中，将介绍这些基础的Win32API函数，掌握此类函数，对后面的网络编程很有帮助。
1.1.1 Windows API编程的优点　　大多数Windows程序员已经熟悉MFC的编程开发。
实际上，如果要开发出更灵活、更实用、更有效率的应用程序，尤其是网络程序，必然要直接使用API函数进行编程。
与使用MFC编写出来的程序相比，使用Win32API编写出来的程序有很多优势：　　生成的可执行程序体积小：　　执行效率高；　　更适用于编写直接对系统进行底层操作的程序，其所生成的代码质量也更加高效简洁。
目前，大多数的黑客程序都依赖于网络，因此，开发黑客程序必然离不开网络通信，即在两台计算机间进行通信。
在网络编程中应用最广泛的是Winsock编程接口，即Windows SocketAPl。
所有在Win32平台上的Winsock编程都要经过下列步骤：定义变量-获得Winsock 版本-加载 Winsock库-初始化-创建套接字-设置套接字选项-关闭套接字-卸载Winsock库-释放所有资源，如图1.1所示。

编辑推荐

需要声明的是，《Visual C++黑客编程揭秘与防范》的目的在于普及网络安全知识，增强读者防范病毒及木马攻击的能力，并通过学习相应的防范技术来进一步保护信息、数据的安全。
绝不是为那些怀有不良动机的人提供支持。
也不承担因为技术被滥用所产生的连带责任，请读者自觉遵守国家相关法律。
5大编程案例： 网络扫描器编程、远程控制软件开发、基于认证的网络程序、U盘防火墙工具实现、Windows底层Rootkit编程； 20多个黑客编程关键技术：Socke、监听、绑定、后门、扫描、线程、注入、拒绝服务、杀毒工具、远程控制等； 从Socket、API基础到案例，全实例呈现黑客VC编程技术。
Windows Socket及API编程基础、网络扫描器编程.防范黑客攻击程序、基于认证的网络程序、下载者程序实现、U盘防火墙安全工具编程实现、Windows底层RootKit编程、远程控制软件开发、网络准入控制、网络蜘蛛编程

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