反黑
教学基地

VIP精品指南
特别奉献

反黑风暴

网站入侵与脚本技术快速防杀

DVD
超大容量 超值享受

- 理论+实战 图文+视频=让读者不会也会
- 任务驱动式讲解，揭秘多种黑客攻击手法
- 攻防互参，全面确保用户网络安全
- 挑战自我，享受黑客攻防的乐趣

武新华 孙世宁 等编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

反黑风暴

网站入侵与脚本技术快速防杀

武新华　孙世宁　等编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书由浅入深、图文并茂地再现了网站入侵与脚本技术快速防杀的全过程，内容涵盖：Windows 系统编程基础、黑客程序的配置和数据包嗅探、Web 脚本攻击与防御、基于 Web 的 DDoS 攻击与防御、流行的黑客编程技术、XSS 跨站脚本攻击技术与防范、Cookie 欺骗与防御技术剖析、数据库入侵与防范技术、SQL 注入攻击与防范、网络上传漏洞的攻击与防范、系统后门编程技术、编程攻击与防御实例等应用技巧，并通过一些综合应用案例，向读者讲解了黑客与反黑客工具多种应用的全面技术。

本书内容丰富全面，图文并茂，深入浅出，面向广大网络爱好者，同时可作为一本速查手册，也适用于网络安全从业人员及网络管理者。

图书在版编目（CIP）数据

网站入侵与脚本技术快速防杀/武新华等编著. —北京：电子工业出版社，2011.1
（反黑风暴）
ISBN 978-7-121-12574-4

Ⅰ. ①网… Ⅱ. ①武… 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(2010)第 247369 号

策划编辑：郭鹏飞
责任编辑：鄂卫华
印　　刷：中国电影出版社印刷厂
装　　订：中国电影出版社印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：26　字数：666 千字
印　　次：2011 年 1 月第 1 次印刷
定　　价：56.00 元（含光盘 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前 言 FREFACE

长期以来，可能是受影视剧的影响，人们在潜意识中已经对“黑客”这个字眼十分敏感，认为黑客是不应该存在的，他们是网络的破坏者。一提起“黑客”，便会不由自主地浮现出上述遐想。

其实，这是对“黑客”的一种极其片面的认识，因为从客观存在的事实来看，黑客这类群体往往存在着一些共同点：如驱动他们成长的是对技术的无限渴望，进而总是把获得技术提高当成自己的最终任务；强烈的责任感使他们不会走向歧途，告诉他们不要在任何媒体上公布成功入侵的服务器；不要对其入侵的服务器进行任何的破坏；在发现系统漏洞后要马上通知官方对该漏洞采取必要的修补措施，在官方补丁没有公布之前，绝对不要大范围地公开漏洞利用代码。

关于本书

目前国内书店中关于脚本方面的书籍特别多，但这些书更多地是偏重于理论性知识。更重要的是，这些书中所介绍的例子，在安全性上都是漏洞百出，导致新学脚本的朋友在阅读后写出来的程序也同样如此！典型的恶性循环！针对当前主要讲述脚本程序漏洞方面的书籍还非常少，我们本着精益求精的态度，力争对本书中的每个脚本程序进行调试通过，目的是用通俗的语言来讲述脚本环境下的各种安全问题，期间没有复杂的理论，非常适合不同水平的大众阅读。

在写作本书的过程中针对目前网友们关心的黑客技术进行了全新升级，本着让所有计算机使用者能够防患于未然的主旨，着重而详细地介绍了各种黑客入侵 PHP 网页的手法，虽然不能说是全部的入侵手段，但大致上已经能够概括绝大部分的攻击方式。

本书内容

本书紧紧围绕“攻”、“防”两个不同的角度，在讲解黑客攻击手段的同时，介绍了相应的防范方法，图文并茂地再现了网站入侵与防御的全过程。本书系统地介绍了入侵的全部过程，以及相应的防御措施和方法，以方便读者了解入侵者常用的方式、方法，保卫网络安全。其中包括：Windows 系统编程基础、黑客程序的配置和数据包嗅探、Web 脚本攻击与防御、基于 Web 的 DDoS 攻击与防御、流行的黑客编程技术、XSS 跨站脚本攻击技术与防范、Cookie 欺骗与防御技术剖析、SQL 注入攻击与防范、网络上传漏洞的攻击与防范、系统后门编程技术、编程攻击与防御实例等内容。

本书虽然详细解说了每个攻击手法的原理与实际操作，但毕竟如何防范这些入侵才是本书的重点。想要开发安全的 PHP 应用程序，就赶快拿起这本书仔细地阅读吧!只有使读者在了解黑客攻击知识的基础上，最大限度地做到“知己知彼”，才有可能在遭受黑客攻击时尽量减少自己的损失。

本书特色

本书以情景教学、案例驱动及任务进阶为鲜明特色，在书中可以看到一个个生动的情景案例。通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。结合图解、标注和多媒体教学，精选入门读者最迫切需要掌握的知识点，构建一个实用、够用、完整的知识体系。

- 理论+实战，图文+视频=让读者不会也会！作者采用最为通俗易懂的图文解说，即使是电脑新手也能通读全书
- 用任务驱动、情景教学的方式来介绍，在学习案例过程中掌握知识点
- 最新黑客技术盘点，让读者实现“先下手为强”
- 学习目的性、指向性最强

本书以网络安全技术中时下最火爆的 Web 脚本攻击为主要讲解方向，以实例分析加案例剖解为主要脉络，以图文并茂、按图索骥的方式详细讲解黑客的攻击手法和相应的网络安全管理防御技术，并采用案例驱动的写作方法，照顾初级读者，详细分析每一个操作案例，力求通过一个知识点的讲解，以实现读者用更少时间尽快掌握黑客编程技术，让读者彻底理解和掌握类似场合的应对思路。

本书适合人群

本书紧紧围绕“攻”、“防”两个不同的角度，在讲解黑客入侵手段的同时，介绍了相应的防范方法，图文并茂地再现了网络脚本入侵与防御的全过程。

本书作为一本面向广大网络爱好者的速查手册，适合于如下读者学习使用：

- 没有多少电脑操作基础的广大读者；
- 需要获得数据保护的日常办公人员；
- 喜欢看图学习的广大读者；
- 相关网络管理人员、网吧工作人员等；
- 明确学习目的的读者、喜欢钻研黑客技术但编程基础薄弱的读者；
- 网络管理员、广大网友等。

本书作者：

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验，可带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。本书的编写情况是：杨平负责第 1 章，王英英、李防负责第 2 章，孙世宁负责第 3、4、5 章，安向东负责第 6 章，李伟负责第 7 章，段玲华负责第 8 章，王肖苗负责第 9 章，吕志华负责第 10 章，张晓新负责第 11 章，陈艳艳负责第 12 章，最后由武新华统审全稿。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的行为都属于违法行为，希望读者在阅读本书后最好不要使用本书中介绍的黑客技术对别人进行攻击，否则后果自负，切记切记！

我们的联系方式：zhangbg@phei.com.cn

编著者

2010 年 10 月

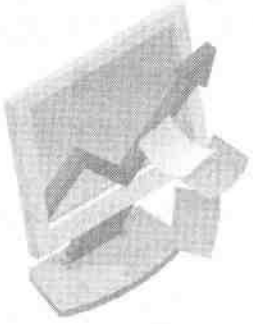
目 录 CONTENTS

第1章

Windows 系统编程基础

重点提示：

- 黑客编程概述
- Windows 系统编程概述



本章主要介绍了黑客常用的编程语言以及黑客编程技术；还介绍了 Windows 系统编程，其中包括网络通信编程、文件操作编程、注册表编程、进程和线程编程以及动态链接库编程等相关内容；有助于读者对黑客编程和各种 Web 攻击的了解，并采取相应的措施来防御网站的攻击，从而保护数据安全。

俗话说："万事开头难"，编程也不例外。初学者如何入门，关键要有一份正确的理论作为指导。从理论上讲，任何一门语言都可以在任何一个系统上编程，只要找到该系统所提供的"接口"和对系统内部机制有深入的了解就可以了。

实际上，编程是一项很繁杂的工作，除应用编程工具之外，了解系统本身内部工作原理也是编写稳定兼容的程序所必不可少的前提条件。其实黑客是通过各种工具来获得注册表、进程等信息，为其进行攻击作准备，高手们更是通过运用各种编程语言来编写出具有特定功能的入侵程序。

1.1 黑客编程概述

编程是每一个黑客所应该具备的最基本的技能，但黑客与程序员又有所不同。黑客往往掌握着许多种程序语言的精髓（或者可以说是弱点与漏洞），并且黑客们都是以独立于任何程序语言之上的概括性观念来思考程序设计上的问题。

1.1.1 黑客编程语言简介

要学习黑客编程至少要先学会一种编程语言。黑客们培养这种能力的方法，也与常人有所不同。他们也看种种书籍，但更多的是阅读别人的源代码。这些源代码大多数是前辈黑客们的作品，同时他们也不停地自己写程序。下面是黑客们常用的几种语言。

1. 脚本语言

脚本语言或扩建的语言，又叫动态语言，是一种编程语言控制软件应用程序。脚本语言有如下几个特点：

- 脚本语言（JavaScript、VBScript 等）介于 HTML 和 C、C++、Java、C#等编程语言之间。HTML 通常用于格式化和链接文本，而编程语言通常用于向机器发出一系列复杂指令。
- 脚本语言与编程语言也有很多相似地方，其函数与编程语言比较相似，也涉及变量。脚本语言与编程语言之间最大的区别是，编程语言的语法和规则更为严格和复杂。
- 脚本也是一种语言，同样由程序代码组成。脚本语言一般都有相应的脚本引擎来解释执行，一般需要解释器才能运行。例如，JavaScript、ASP、PHP 等都是脚本语言。
- 脚本语言是一种解释性的语言，如 VBScript、JavaScript、ActionScript 等，它不像 C\C++等可以编译成二进制代码，以可执行文件的形式存在。脚本语言不需要编译，可以直接由解释器来负责解释。
- 脚本语言一般都是以文本形式存在，类似于一种命令。

2. 解释性语言

解释性语言的程序不需要编译，解释性语言在运行程序的时候才翻译。解释性语言的特点是：效率比较低、依赖解释器、跨平台性好。典型代表语言有 BASIC 语言，专门有一个解释器能够直接执行 BASIC 程序，每个语句都是执行时才翻译。所以，解释性语言每执行一次就要翻译一次，效率比较低。

3. 编译性语言

使用编译性语言编写的程序在执行之前，需要一个专门的编译过程，把程序编译成为机器语言的文件，以后要运行的话就不用重复翻译了，直接使用编译的结果就可以。其特点是程序执行效率高、依赖编译器、跨平台性差。典型代码语言有 C、C++、Delphi 等。

4. 汇编语言

汇编语言（Assembly Language）是一种面向机器的程序设计语言，也是利用计算机所有硬件特性并能直接控制硬件的语言。汇编语言比机器语言易于读写、调试和修改，同时具有机器语言的全部优点。但在编写复杂程序时，相对高级语言代码量较大，而且汇编语言依赖于具体的处理器体系结构，不能通用，因此，不能直接在不同处理器体系结构之间移植。

在 Windows 时代，大部分黑客软件都是基于 Windows 平台的。在 Windows 平台的编程语言有 JAVA、VC++、Delphi、VB 等。由于 VC++的代码执行效率高而且系统兼容好，对系统底层的操作比较强大，而且编写的程序体积小。因此，VC++是最适合编写黑客工具和木马后门的。而汇编语言作为一种低级的语言，可能已经不被很多用户采用，但是如果想成为真正的高手，在学完一门高级语言后，还需要学习汇编语言。

1.1.2 黑客与编程

“黑客”一词往往是指那些“软件骇客”（Software Cracker）。“黑客”一词，原指热心于计算机技术，水平高超的电脑专家，尤其是程序设计人员。“黑客”一词一般有如下 4 种意义：

- 一个对（某领域内）编程语言有足够了解，可不经长时间思考就创造出有用软件的人。
- 一个通过知识或猜测而对某段程序作出修改，并改变（或增强）该程序用途的人。
- 一个恶意（一般是非法地）试图破解或破坏某个程序、系统及网络安全的人。这个意义常常对那些符合条件的黑客造成严重困扰，建议媒体将这群人称为“骇客”（Cracker）。有时这群人也被称为“黑帽黑客”。
- 试图破解某系统或网络以提醒该系统所有者的系统安全漏洞。这群人往往被称为“白帽黑客”或“匿名客”（Sneaker）或红客。这些人多是电脑安全公司的雇员，并在完全合法的情况下攻击某系统。

其中有 3 条都提到编程或程序，可见编程和黑客是密不可分的。对一个黑客来说，学会入侵和破解是必要的，但最主要的还是编程，毕竟使用工具是体现别人的思路，而编程则是自己的想法。在从刚刚接触黑客技术到逐渐入门的过程中，很多人又会发现：其实不会编程也可以轻易得到一个服务器权限，再利用一些专门的工具来控制该目标主机，但有时很难让目标主机按照自己的意愿进行工作。初学者往往在这个过程浪费了大量精力在大多的入侵上，因为在这个过程中进步是非常慢的。在其中可以看出，编程在黑客技术中的重要性，所以早学编程可以少走很多弯路。

同时，黑客在入侵时使用的工具、控制服务器、木马等都是通过编程来实现的。黑客在入侵中通过编程来解决遇到的问题或编写需要实现特定的工具，而不是依靠别人的工具。在黑客技术中与编程相关的技术如图 1-1 所示。可见，要掌握高级黑客技术，编程是基础，也是关键。

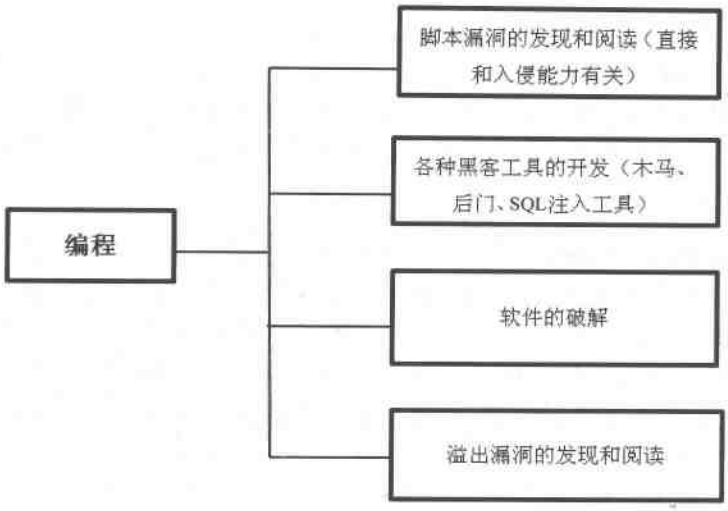


图 1-1 与编程相关的黑客技术

1.1.3 Visual C 编程基础

Visual C++（VC++）是一个功能强大的可视化软件开发工具。VC++ 6.0 不仅是一个 C++ 编译器，而且是一个基于 Windows 操作系统的可视化集成开发环境（Integrated Development Environment，IDE）。VC++ 6.0 由许多组件组成，包括编辑器、调试器以及程序向导 AppWizard、类向导 Class Wizard 等开发工具。这些组件通过一个名为 Developer Studio 的组件集成为和谐的开发环境。

1. 建立第一个无窗口工程

木马、后门为了隐藏自己，总是没有窗口的，不会像应用程序那样会跳出一个很明显的窗口。下面介绍使用 VC++ 6.0 生成一个无窗口程序的过程。具体操作步骤如下：

步骤 01 双击桌面上创建的 VC++ 6.0 快捷方式图标，即可打开 VC++ 6.0 主窗口，如图 1-2 所示。

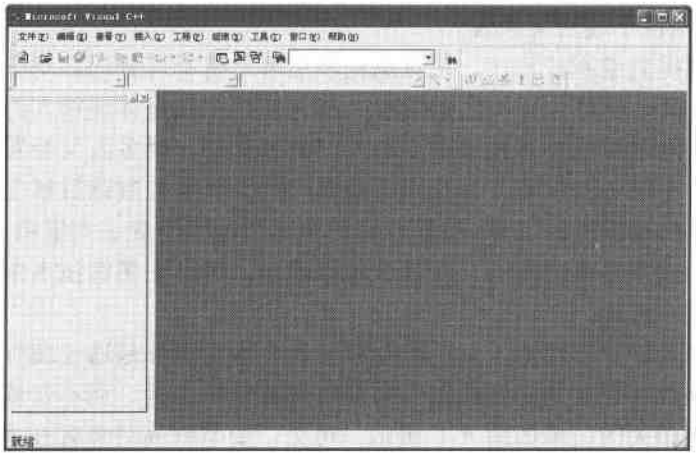


图 1-2 VC++ 6.0 主窗口

步骤 02 选择“文件”→“新建”菜单项，即可弹出“新建”对话框，切换到“工程”选项卡，选择列表中的“Win32 Console Application”工程项目，并填写好工程名称以及存储的位置，如图 1-3 所示。

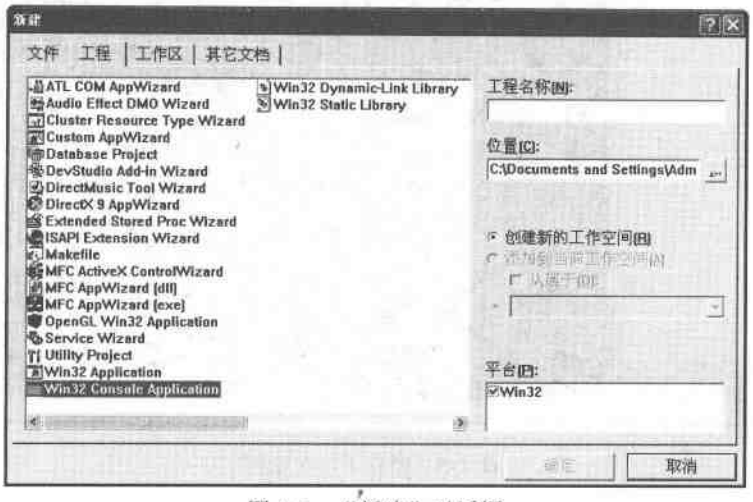


图 1-3 “新建”对话框

步骤 03 单击“确定”按钮，即可弹出“Win32 Console Application—步骤 1 共 1 步”对话框，在其中选择“一个简单的程序”选项，如图 1-4 所示。

图 1-4 “Win32 Console Application—步骤 1 共 1 步”对话框

步骤 04 待一切设置完毕后，单击“完成”按钮，这样就建立了一个工程了，但是编译运行后会发现有一个黑乎乎的控制台窗口，如图 1-5 所示。对于 NC 之类的程序当然无所谓了，但对于木马后门这样就不够隐蔽。此时用户只需在头文件中（默认情况下是 StdAfx.h）加入“#pragma comment(linker, "/subsystem:\" windows\" /entry:\" mainCRTStartup\" ")”代码，就不会有控制台窗口了。

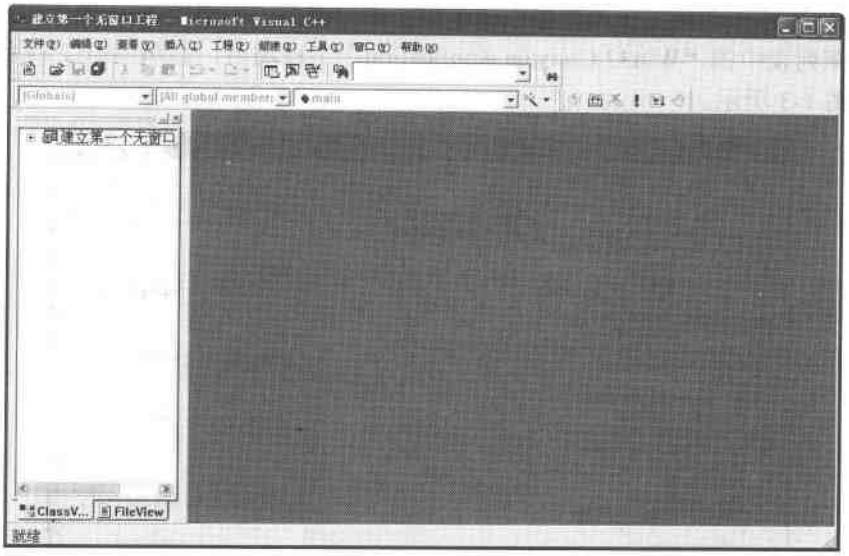


图 1-5 建立了一个工程

2. API 编程基础

所谓 API 就是 Application Programming Interface 的缩写，其实就是操作系统留给应用程序的一个调用接口，应用程序通过调用操作系统的 API 而使操作系统去执行应用程序的命令。

其实早在 DOS 时代就有 API 的概念，只不过那个时候的 API 是以中断调用的形式（INT21h）提供的，在 DOS 下运行的应用程序都直接或间接地通过中断调用，来使用操作系统功能。而在 Windows 中，系统 API 是以函数调用的方式提供的。API 函数都是包含在系统 DLL 中的导出函数，DLL 文件不能直接执行，通常由 exe 在执行时装入，其内含有一些资源以及可执行代码等。系统 DLL 中就含有 API 函数的执行代码。

直接调用 API 编程又称为 SDK 编程。SDK 即 Software Develop Kit（软件开发工具包）的缩写，包含了进行 Windows 软件开发的文档和 API 函数的输入库、头文件。早期 SDK 是一个单独发放的包，现在在 Visual C++和其他的一些开发环境中已经包含它了。如果用户已经安装了 VC++，那么就可以开始编写 Windows 程序了。

API 和 SDK 是开发 Windows 应用程序所必需的，所以其他编程框架和类库都是建立在它们之上的。像 MFC 类库就是对 API 的封装。所以 SDK 编程相对比较灵活，当然也是有一定难度的。SDK 还有一个优点就是其编写的程序体积比用类库的小得多。

在 SDK 中，API 函数的申明是包含在头文件和导入库中的，所以在程序中用户必须要有 API 函数的头文件（.H）和其导入库（.LIB），可以分别用“#include”和“#pragma Comment”语句加载到程序中。怎么才能调用 DLL 中的 API 函数呢？

具体操作步骤如下：

步骤 01 包含要调用函数的头文件，可以在文件开头使用“#include <windows.h>”，这里的 Windows.h 是指包含的头文件。

步骤 02 连接到指定的导入库文件（.LIB）。一般情况下，VC 默认已经连接了常用的导入库文件，在没有默认连接的情况下，可以在文件开头使用“#PragmaComment（lib，"Ws2_32")”，其中，Ws2_32 就是导入库的名称。