Broadview
www.broadview.com.cn

安全技术大系

黑客攻防实战编程

邓吉 编著

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

安全技术大系

黑客攻防实战编程

邓吉 编著

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

内 容 简 介

《黑客攻防实战编程》一书作为《黑客攻防实战入门》、《黑客攻防实战详解》和《黑客攻防实战进阶》的提高篇，仍然以黑客“攻”、“防”的视角，针对目前国内外安全研究的热点和难点问题进行研究，内容涵盖了 Web 入侵脚本、病毒、木马、网马、加密解密、Shellcode、漏洞溢出渗透、以及漏洞挖掘等相关领域的程序开发研究。本书适合信息安全领域研究人员、机构、网管和那些对网络感兴趣的在校学生作为参考及教学之用，也适合杀毒软件、木马查杀软件等相关网络安全工具的开发人员作为参考之用。

图书在版编目（CIP）数据

黑客攻防实战编程 / 邓吉编著.—北京：电子工业出版社，2009.6
ISBN 978-7-121-08537-6

Ⅰ. 黑… Ⅱ.邓… Ⅲ.计算机网络－安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2009）第 041651 号

策划编辑：毕宁　　bn@phei.com.cn
责任编辑：孙学瑛
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
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：787×980　1/16　印张：23.5　字数：436 千字
印　　次：2009 年 6 月第 1 次印刷
印　　数：4000 册　　定价：48.00 元

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。

Preface

前言

《黑客攻防实战入门》、《黑客攻防实战详解》和《黑客攻防实战进阶》这3本书自面世以来，得到了广大读者的肯定与好评。其销量一直排在同类书籍的前列，笔者在此深表感谢。与此同时，应广大读者的要求，笔者针对当前黑客编程领域的热点及难点问题，撰写了这本《黑客攻防实战编程》一书。本书一如既往地保持着前3本书的“授之以鱼，不如授之以渔”的风格，向读者介绍黑客入侵及防御相关编程技术的思考方法和思维方式，而不是单单介绍编程语法。本书是笔者通过多年的研究与实践，在把握国内外安全领域研究的热点及难点的基础之上，进行归纳总结所完成的一本黑客编程入门及提高书籍，这一点是本书区别于其他同类书籍的根本之处。

关于黑客

长期以来，由于诸多方面的因素，“黑客”这个字眼变得十分敏感。不同的人群对黑客也存在不同的理解，甚至没有人愿意承认自己是黑客。有些人认为，黑客是一群狂热的技术爱好者，他们无限度地追求技术的完美；有些人认为，黑客只是一群拥有技术，但思想简单的毛头小伙子；还有些人认为黑客是不应该存在的，他们是网络的破坏者。这里，我们没有必要对这个问题争论不休，也无须为黑客加上一个标准的定义，但从客观存在的事实来看，黑客这类群体往往存在以下共同点。

（1）强烈的技术渴望与完美主义：驱动他们成长的是对技术的无限渴望，获得技术的提高才是他们最终的任务。

（2）强烈的责任感：只有强烈的责任感才能使他们不会走向歧途，责任感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破坏；在发现系统漏洞后要立即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。一方面，黑客入侵可能造成网络的暂时瘫痪；另一方面，

黑客也是整个网络的建设者，他们不知疲倦地寻找网络大厦的缺陷，使得网络大厦的根基更加稳固。

为什么写作本书

不容乐观的事实是，一部分人歪曲了黑客的本质，被不良动机所驱使而进行入侵活动，威胁网络的健康发展。对于我国来说，形势尤为严峻。我国信息化建设迟于美国等发达国家，信息安全技术水平也相对落后。在几次黑客大战中，国内网站的弱口令及漏洞比比皆是。这种现状实在令人担忧，值得深思和反省，从中也可以看出传统的计算机网络教学层次是远远不够的。可能出于安全等其他角度的考虑，传统教学往往只注重表面上的应用，而避开一些敏感的技术。设想一下，如果一个网站的管理员只学会架构网站，却不关心如何入侵自己的网站，那么如何对自己网站的缺陷了如指掌？如何能够及时地获知最新漏洞的描述而提前做好抵御？如果以上都做不到，那就更不要谈日常的系统更新、维护和打补丁了。然而国内精通入侵的网管又有多少呢？长期以来，国内网管的潜意识里都认为“入侵”是个不光彩的勾当，甚至嗤之以鼻。随着信息化程度越来越高，信息技术与生活的联系越来越紧密，可以上网的电子设备逐年增加，电脑、PDA、手机，甚至家电。可以想像10年后，如果不了解入侵者的手段来采取必要的防御措施，将要被入侵的设备不会仅仅限于电脑，也许还包括手机、家电和汽车等。因此在信息技术如此发达，沟通方式日益丰富和复杂的今天，我们不仅要学会如何正确使用网络，而且还需要学会如何防御自己的网络被他人入侵，这也正是笔者写作本书的初衷。

本书主要内容

作为《黑客攻防实战入门》、《黑客攻防实战详解》和《黑客攻防实战进阶》的提高篇，本书以黑客“攻”、“防”的视角，针对目前国内外安全研究的热点和难点问题进行研究，涵盖了Web入侵脚本、病毒、木马、网马、加密解密、Shellcode、漏洞溢出渗透，以及漏洞挖掘等相关领域的程序开发研究。

本书分为内容独立的7章，读者可以根据实际需求有选择跳跃式阅读，各章的主要内容如下。

第1章“Web入侵脚本编程”从服务器搭建开始，介绍目前网络上最为猖獗的“SQL注入”和“跨站脚本攻击”入侵手段、原理与编程技术，以及防护手段。

第2章“病毒原理及代码解析”在总结计算机病毒发展历史、病毒种类及病毒命名方

式之后，详细地介绍计算机病毒原理，并对病毒源代码进行了全面的剖析。

第 3 章“木马网马程序分析”针对木马及网马的源代码进行解析、总结了其工作原理、启动方式、隐藏与防杀等相关技术。

第 4 章“软件加密与解密”介绍序列号保护、软件加密狗、时间限制及 Key 文件保护等目前常见软件的加密方法，并分析注册机等软件的解密原理，以及跟踪调试与反跟踪调试技术。

第 5 章“shellcode 原理与编写”介绍了栈溢出、堆溢出等程序溢出原理，分析了 PE 文件结构，以及如何针对已知漏洞编写 Shellcode。

第 6 章“漏洞溢出程序分析与设计”详细介绍了缓冲区溢出原理、类 Unix、Windows 及远程 Windows 程序溢出方法等渗透方法，并介绍一款自动化渗透测试工具 Metasploit 及其使用方法。

第 7 章“漏洞挖掘与 Fuzzing 程序设计”介绍一种行之有效的自动化漏洞挖掘技术“Fuzzing”，进而介绍如何挖掘已知系统中所存在的漏洞。

另外，本书中所使用的源代码及动画教程等相关资源下载，链接地址为 http://www.broadview.com.cn。

本书的姊妹书籍

本书的姊妹书籍有《黑客攻防实战入门(第 2 版)》、《黑客攻防实战详解》和《黑客攻防实战进阶》3 本，在本书推出之后，这 4 本书便形成了一个由浅入深完整的知识体系。几乎涵盖了黑客安全领域由入门到专家所必需掌握的所有的知识与技术，以供不同层次的读者学习。

（1）《黑客攻防实战入门》：踏入网络安全之门，初窥黑客攻防实战技巧。

（2）《黑客攻防实战详解》：透析网络安全内幕，详解黑客攻防体系。

（3）《黑客攻防实战进阶》：深入网络安全技术，进阶黑客攻防专家。

（4）《黑客攻防实战编程》：把握网络安全方向，实战黑客攻防编程。

致谢

感谢张毅编辑在我还是学生时代时就接受了我的《黑客攻防实战入门》样稿，才使得这么多年我都有机会和信心将自己的经验通过电子工业出版社分享给广大读者朋友。

感谢毕宁编辑长年来的指导与支持，并推荐给我大量的朋友与学习机会。才使得我能

够陆续撰写《黑客攻防实战入门（第 2 版）》、《黑客攻防实战详解》、《黑客攻防实战进阶》和《黑客攻防实战编程》这 4 本书。

感谢孙学瑛老师和黄爱萍助理的指导，以及为本书的出版所付出辛勤劳动的所有朋友。

感谢 qixu.liu 在技术方面给与我的支持。

感谢长期以来支持我的读者朋友和网友们。

需要声明的是，**本书的目的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。本书的目的在于最大限度地唤起大家的网络安全意识，正视我们的网络世界所面临的一场危机并采取相应的行动**。

邓 吉

CONTENTS

目录

CHAPTER

1

第 1 章　Web 入侵脚本编程

随着 Internet 的发展，网站服务器越来越多。黑客们也将攻击中心由个人计算机转向了网站服务器。在各种各样的攻击方法中，通过 Web 脚本漏洞入侵最为常见。在本章中，将介绍目前最热点的 SQL 注入，以及跨站脚本入侵及其防御方法。

通过本章的学习，我们能够了解到以下知识。

（1）SQL 注入。

（2）跨站脚本攻击及其防御方法。

1.1　SQL 注入攻击研究

“注入攻击”这个词在网络上已经是屡见不鲜了。当入侵者准备入侵一台主机时，通常情况下首先查看这台服务器上有无动态网页的 Web 服务，并且这些动态网页是否存在漏洞。如果存在漏洞，则可以通过一些手段来得到管理员的密码，甚至是整台服务器的控制权。在这些漏洞中比较常见且容易上手的一种攻击方式就是 SQL 注入攻击，这种技术并不需要太高深的理论基础和复杂的操作。目前掌握这门技术的人较多，也是当前对网站进行入侵的一种主流方式。

本节将披露 SQL 注入攻击技术的原理和手法，并介绍针对注入攻击的防范措施，希望能够帮助更多的网络管理员远离这种攻击。

1.1.1　测试环境的搭建

本章中的许多内容需要通过实例讲解，考虑到不能随意攻击和破坏他人的网络，笔者在自己的电脑中搭建一台网站服务器，并构造一个存在漏洞的页面作为实例演示之用。

在 Windows 下有许多网站服务器软件，其中最为常见的是 IIS（Internet Information Server，Internet 信息服务）、PWS（Personal Web Server，个人网页服务器），以及 Apache

服务器等。其中 PWS 在 Windows 98 操作系统中比较常见，IIS 在 Windows 2000 以后的 Windows 操作系统中比较常见，Apache 经常在 Linux 中与 PHP 配合使用。考虑到大部分读者使用 Windows 操作系统平台，而且 IIS 也比较常见并且容易安装，所以以 IIS 为例讲解搭建如何网络服务器。

IIS 的安装过程如下。

（1）将 Windows XP 的安装光盘放入光驱中，然后单击“开始”|“设置”|“控制面板”选项，如图 1-1 所示。

（2）弹出“控制面板”窗口，单击“添加/删除 Windows 组件”按钮，如图 1-2 所示。

图 1-1 “控制面板”选项

图 1-2 “添加/删除 Windows 组件”按钮

（3）弹出如图 1-3 所示的“Windows 组件向导”对话框，选择“Internet 信息服务（IIS）”复选框。

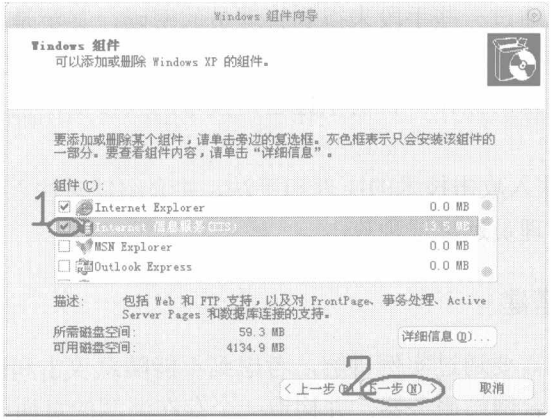

图 1-3 “Windows 组件向导”对话框

（4）单击“下一步”按钮，显示“正在配置组件”对话框，如图 1-4 所示。等待，直

到提示完成，如图 1-5 所示。

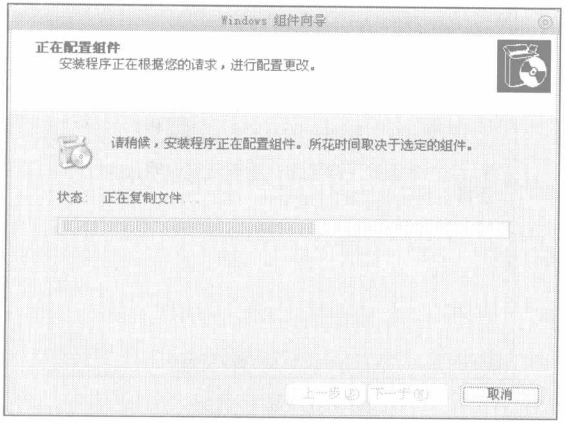

图 1-4　“正在配置组件”对话框

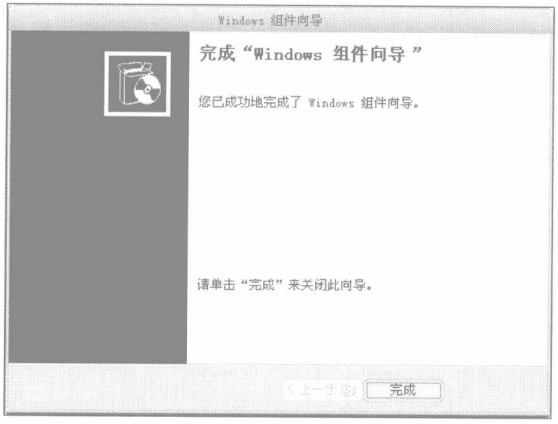

图 1-5　提示完成

安装 IIS 之后，IIS 会创建操作系统所在盘（下面以 C 盘为例）的\Inetpub\wwwroot 文件夹作为网站的根目录。将相关的网页文件放到这个目录中，即可在 IE 中浏览这个网页。

为了检验 IIS 是否能正常工作，使用记事本编写如下代码：

```
<html>
<head>
<title>测试网页</title>
</head>
<body>测试 IIS 是否能正常工作，看到我就说明 IIS 能正常工作了！
</body>
</html>
```

将上述代码保存为 aaa.html 文件，并复制到上述目录中。打开 IE 浏览器，访问

http://127.0.0.1/aaa.html。如果显示如图 1-6 所示的测试结果，则说明 IIS 已正常运行。

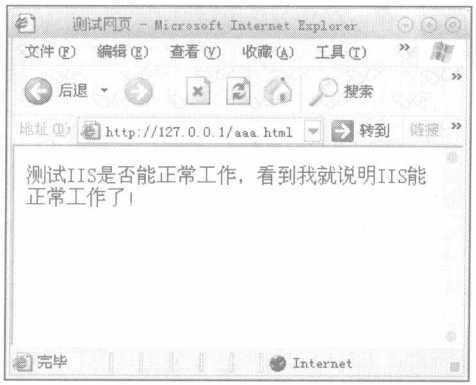

图 1-6　显示结果

下面测试 IIS 是否能正常地解析 ASP 动态脚本网页，在记事本中输入下述代码：

```
<html>
<head><title>测试 asp</title></head>
<body>
<%
Response.Write "Asp 正常执行"
%>
</body>
</html>
```

将上述代码保存为 aaa.asp 文件，并复制到上述目录中。然后打开 IE，访问 http://127.0.0.1/aaa.asp 或 http://localhost/aaa.asp。如果显示如图 1-7 所示的测试结果，说明 IIS 可以正常工作。

图 1-7　测试结果

1.1.2　一个简单的实例

大部分留言本的管理后台登录后才能进入。一般情况下，用户在输入密码并单击“登录”按钮后登录页面会把输入的密码提交给一个动态网页。这个网页查看该密码和数据库中的密码是否相同，如果相同，则登录成功；否则就会提示输入错误。

下面首先编写一个页面用来显示用户名和密码文本框，以及“登录”按钮网页文件，代码如下：

```
<html>
<head><title>登录页面</title></head>
<body>
    <div align="center">
        <form action="login.asp" method="post">
            请输入密码：
            <br><br>
            用　户：<input name="name" type="textbox">
            <br>

            密　码：<input name="pass" type="password">
            <br>
            <input type="submit" value="登录">
        </form>
    </div>
</body>
</html>
```

编写后保存为名为“login.html”的网页文件。

说明如下：

```
<form action="login.asp" method="post">
```

这行代码指定把数据提交给 login.asp 网页。

```
<input name="name" type="textbox">
    ……
<input name="pass" type="password">
```

这是一个典型的表单，这两行代码显示一个文本框和一个密码文本框。其名称“name”非常重要，login.asp 用其从提交的数据中获取用户名和密码数据。

login.asp 的代码如下：

```
<%
inname = Request("name")
inpass = Request("pass")
set conn=server.createobject("ADODB.CONNECTION")
```

```
conn.open "Provider=microsoft.jet.oledb.4.0; Data Source=C:\Inetpub\wwwroot\db.mdb;"
Set rs = conn.Execute("SELECT * FROM data WHERE uname='" & inname &"'")
truepass = rs("upass")
if inpass=truepass then
   response.write("登录成功！ ")
else
   response.write("登录失败！ ")
end if
%>
<p>用户编号：
<%response.write(rs("uid"))%>
</p>

<%
Set rs=Nothing
conn.close
%>
```

说明如下：

```
inname = Request("name")
inpass = Request("pass")
```

从提交的数据中查找名为“name”及“pass”的数据，并分别保存在 inname 和 inpass 两个变量中，后者用于比较 pass 是否正确。

```
set conn=server.createobject("ADODB.CONNECTION")
conn.open "Provider=microsoft.jet.oledb.4.0; Data Source=C:\Inetpub\wwwroot\db.mdb;"
```

使程序连接 C:\Inetpub\wwwroot 中的 db.mdb 数据库文件，以便查询数据。

```
Set rs = conn.Execute("SELECT * FROM data WHERE uname='" & inname &"'")
```

查询 db.mdb 数据库 data 表中，内容为 inname 的变量名“uname”，并将其保存在 rs 变量中。

```
truepass = rs("upass")
```

将查询记录中 upass 字段的内容保存到 truepass 变量中。

```
if inpass=truepass then
   response.write("登录成功！ ")
else
   response.write("登录失败！ ")
end if
```

这是经典的判断语句，用于判断 inpass 变量是否与 truepass 相同，即判断用户输入的密码是否与数据库中查询的密码相同。如果相同，则输出“登录成功”；否则输出“登录失败”。

```
<p>用户编号：<% respons.wirte(rs("uid"))%></p>
```