

宝典丛书

100万

网络安全

与黑客攻防

宝典

普及安全知识, 深入分析黑客入侵的全部过程, 剖析病毒和木马的来龙去脉

将基本理论与实践技巧融入到范例中, 全面覆盖网络安全与黑客攻防的各种知识及应对技巧

以基础知识为主, 同时吸纳大量如Metasploit、UTM、网络钓鱼和NetS-tumbler等新知识



电子工业出版社  
Publishing House of Electronics Industry  
<http://www.phei.com.cn>

张庆华 编著

宝典丛书

# 网络安全与黑客攻防宝典

张庆华 编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

## 内 容 简 介

本书由浅入深、循序渐进地介绍了计算机网络安全知识体系。全书共分 14 章，内容涵盖了网络的基础知识、黑客初步、操作系统漏洞与应用软件漏洞的攻防、BBS 与 Blog 的漏洞分析、信息收集、扫描目标、渗透测试、网络设备的攻击与防范、木马分析、病毒分析、防火墙技术、入侵检测技术、计算机取证、无线网络安全等内容。本书最大的特色在于知识全面、实例丰富，每一节的例子都是经过精挑细选，具有很强的针对性，读者可以通过亲手实践而掌握安全防护基本要领和技巧。

本书适合初、中级用户学习网络安全知识时使用，同时也可作为高级安全工程师的参考资料。

**未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。**

**版权所有，侵权必究。**

### 图书在版编目(CIP)数据

网络安全与黑客攻防宝典 / 张庆华编著. —北京: 电子工业出版社, 2007.4

(宝典丛书)

ISBN 978-7-121-04142-6

I. 网… II. 张… 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 (2007) 第 041212 号

责任编辑: 于 兰

印 刷: 北京市天竺颖华印刷厂

装 订: 三河金马印装有限公司

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: 787×1092 1/16 印张: 44 字数: 1253 千字

印 次: 2007 年 4 月第 1 次印刷

定 价: 78.00 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, 联系电话: (010) 68279077; 邮购电话: (010) 88254888。

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

服务热线: (010) 88258888。

# 前 言

在当今的网络时代，黑客、病毒让人们谈虎色变，那么到底什么是黑客，他们如何工作，病毒到底是什么，病毒的出现又会对人们的生活造成什么样的影响？本书将给出这些问题的答案。

计算机网络安全是现今网络的主旋律，关于网络安全的话题在媒体上随处可见。随着黑客工具的日益“傻瓜”化，黑客已经被剥离了神秘的外衣。但是计算机安全、网络安全知识的普及仍然是一个严峻的问题，为了解决这个问题，本书以普及安全知识为己任，帮助用户深入了解网络安全的方方面面，如将深入分析黑客入侵计算机的全部过程，模仿黑客入侵计算机并提升远程计算机的权限进而达到控制的目的，剖析病毒和木马的来龙去脉，预测入侵检测的技术发展及趋势，此外，神秘的计算机取证技术和热点的无线网络安全问题都将在本书中呈现。

本书依照读者的学习规律，首先从了解网络安全的基础知识讲起，介绍基本概念和基本观点，在读者掌握了这些基本知识的基础上，再介绍历史上著名的黑客人物及历史事件，以立体的角度、有趣故事情节为依托，严格遵循由浅入深、循序渐进的原则。本书以计算机网络安全知识的层次结构为主线将各种工具、命令和理论知识交织编排在一起，使读者可以深入学习任何一章的内容。

本书在内容编排和目录组织上都十分讲究，章节之间既可相互呼应也可各自成章。比如在第1章熟悉了网络的基础知识以后，立刻引入一些著名的黑客人物的经历，以一个实例告诉读者这些知识的重要性，让读者在茶余饭后的闲谈中即可快速入门。同时，每章之间又相互独立，如果读者希望直接了解病毒的相关知识，可快速查阅第9章和第10章。第9章对木马进行了深入的分析，第10章按照病毒的机制对病毒进行了深入的剖析。

和其他书籍相比，本书具有以下特点：

## ◆ 内容丰富，实例经典。

在学习计算机网络安全知识时，经常遇到两种情况，一是单纯地讲理论而对知识实践只字不提；另外就是纯粹讲解实战而对涉及的理论不予理会。本书则不同，本书追求理论与实践的结合，使用浅显的语言尽可能地通过精心设计的经典实例，将计算机网络安全的基本理论和实践技巧融入到范例当中，全面覆盖计算机网络安全各个角落。

## ◆ 实战众多，内容充实。

作者在讲解每一个知识点之后，都要安排尽可能多的实例。这些实例都是根据实战经验改编，充分考虑了读者的理解水平，并且实战的每一步都介绍得非常详细，读者能够根据自身的知识水平有针对性地学习，思路变得更加开拓。

## ◆ 讲解通俗，步骤详细。

每个实例的演练步骤都以通俗易懂的语言阐述，并穿插说明文字，还附加了详细的插图作为演练的参考。

## ◆ 知识面开阔，重点突出。

本书涉及的内容众多，有基础知识，也有深入的理论探讨。为了说明某一个知识点，



在前面使用了一些基础知识作为铺垫，这些知识既可作为了解的必要步骤，也可作为参考知识供读者查阅。

◆ **新知识多，讲解全面。**

在本书中使用了大量的新知识，如 Metasploit、Nessus、UTM、EnCase、网络钓鱼、流氓软件和 NetStumbler 等。这些新知识的使用充实了本书的内容，也使得本书与同类书中陈旧的技术内容形成了鲜明的差别。本书不仅介绍了新知识，而且针对这些知识进行实战演练，帮助读者快速了解新内容。

◆ **实例鲜活，应用软件可随时获得。**

虽然本书中使用了大量软件，但是这些软件基本上都是免费软件，读者可以从网络上随时下载进行练习，这就避免了读者只能阅读，不能实战的尴尬。

◆ **兼顾各个水平的读者。**

虽然本书面向基础读者，但是本书中也介绍了很多理论知识，这些内容可以为高级读者进一步参考。

本书包括以下内容：

**第 1 章** 首先介绍网络的基本体系构成、网络的工作原理、黑客的基本知识、常用的端口知识，以及一般性的安全防范知识。

**第 2 章** 切入正题，介绍黑客的一些情况，如历史上的著名黑客及其参与的事件、著名的黑客组织、黑客通常使用的入侵手法和这些手法的防范方法等。

**第 3 章** 以操作系统常见的漏洞为主题，介绍如何利用这些漏洞入侵远程计算机的过程，并给出了防范方法。另外，还介绍了服务器软件的一些漏洞及其解决方法。

**第 4 章** 继续第 3 章重点分析 BBS 系统和 Blog 系统的一些问题，如提升权限、Cookies 问题及数据库暴库的问题。

**第 5 章** 帮助读者了解高级的黑客搜集信息工具及方法，如使用 Google 搜集网站信息、DNS 查询和追踪路由等知识。

**第 6 章** 主要介绍各种扫描技术及技巧，如 SYN 扫描、圣诞树扫描、FIN 扫描、空扫描、UDP 扫描等，还介绍了操作系统协议栈指纹识别技术。这一章使用了各种著名的扫描器，并给出了实战分析。

**第 7 章** 介绍黑客入侵的高级知识及渗透测试。其中重点介绍了一些渗透测试的基础知识和测试过程中涉及的技术问题，如分析缓冲区溢出问题及各种溢出知识，还介绍了数据库及 Web 渗透的基本技术，并在最后演示了一种在国外非常流行的测试工具平台 Metasploit 的使用方法。

**第 8 章** 介绍网络设备的基本知识，如路由器和交换机的工作原理，以及一些常用的网络设备攻击方法，如使用 SNMP 对路由器入侵及 TFTP 的使用方法。

**第 9 章** 从各个角度对木马进行了深入剖析。其中涉及木马的基本概念、木马常用攻击手段、木马程序的隐藏技术、木马攻击的防范与清除；介绍一些典型木马，如灰鸽子、冰河、RAdmin 的基本知识；还介绍了使用冰刃检查木马进程及 Ethereal 防范木马的一些方法和技巧。

**第 10 章** 介绍从病毒基本知识、病毒分析、病毒类型、新型病毒分析、各种操作系统病毒等方面介绍计算机病毒相关知识。

**第 11 章** 介绍防火墙的基本功能、工作原理、分类、体系结构、规则，随后介绍如何选择

合适的防火墙和部分防火墙产品，在此基础上详细介绍了在不同操作系统平台下的防火墙软件的使用方法。

**第 12 章** 首先概述 IDS 的功能与模型、基本原理等，随后介绍产品选型原则及部分产品，然后着重介绍开源入侵检测系统 Snort，最后还阐述了入侵防御系统与 UTM 等未来发展方向。

**第 13 章** 介绍计算机取证的相关知识。计算机取证将计算机系统视为犯罪现场，运用先进的技术工具，按照规程全面检查计算机系统，提取、保护并分析与计算机犯罪相关的证据，以期据此提起诉讼。这一章从证据的获取和证据的分析两个方面结合相应软件进行了介绍。

**第 14 章** 介绍无线网络安全的内容，其中对无线访问设备、AP、无线网络协议、WEP 安全协议、NetStumbler 检测无线网络、无线网络的攻击及防护无线网络等知识进行了浅显的阐述。

本书具有知识全面、实例精彩、指导性强的特点，力求以全面的知识性及丰富的实例来指导读者透彻学习计算机网络安全技术。本书可以作为对计算机网络安全感兴趣的读者的启蒙书，也可以帮助具有一定技术程度的中级读者提高技能，对高级读者也有一定的启发意义。

本书由张庆华主编，参加本书编写工作的人员还有杨光景、杨毅、李海涛、汪洋、谷文港、陈亮、李守军、江旭初、王坤、赵元、易福华、易阳华、孙江苏、姜海森、张明霞、王江、王斌、郭剑云、张大发、刘挺、尹海涛、戴隆忠、李善坡、张磊、唐友生、于兆海、刘洪燕、傅翠娇、王悠。在此向他们表示感谢。

作者

2007 年 1 月

# 反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010)88254396；(010)88258888

传 真：(010)88254397

E - mail: dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036

# 读者意见调查表

感谢您对电子工业出版社的支持！

为帮助我们进步，请将您的宝贵意见填于下表并寄回我们。

您购买的图书名称	
先进性和实用性	<input type="checkbox"/> 很好 <input type="checkbox"/> 好 <input type="checkbox"/> 一般 <input type="checkbox"/> 不太好 <input type="checkbox"/> 差
图书文字可读性	<input type="checkbox"/> 很好 <input type="checkbox"/> 好 <input type="checkbox"/> 一般 <input type="checkbox"/> 不太好 <input type="checkbox"/> 差
图书篇幅适宜度	<input type="checkbox"/> 很合适 <input type="checkbox"/> 合适 <input type="checkbox"/> 一般 <input type="checkbox"/> 不合适 <input type="checkbox"/> 差
出版物中差错	<input type="checkbox"/> 极少 <input type="checkbox"/> 较少 <input type="checkbox"/> 一般 <input type="checkbox"/> 较多 <input type="checkbox"/> 太多
图书封面设计水平	<input type="checkbox"/> 很好 <input type="checkbox"/> 好 <input type="checkbox"/> 一般 <input type="checkbox"/> 不太好 <input type="checkbox"/> 差
图书印刷装订质量	<input type="checkbox"/> 很好 <input type="checkbox"/> 好 <input type="checkbox"/> 一般 <input type="checkbox"/> 不太好 <input type="checkbox"/> 差
纸张质量	<input type="checkbox"/> 很好 <input type="checkbox"/> 好 <input type="checkbox"/> 一般 <input type="checkbox"/> 不太好 <input type="checkbox"/> 差
定价	<input type="checkbox"/> 很便宜 <input type="checkbox"/> 便宜 <input type="checkbox"/> 合理 <input type="checkbox"/> 贵 <input type="checkbox"/> 太贵
对宣传工作的感觉	<input type="checkbox"/> 很好 <input type="checkbox"/> 好 <input type="checkbox"/> 一般 <input type="checkbox"/> 不好 <input type="checkbox"/> 差
对服务质量的感覺	<input type="checkbox"/> 很好 <input type="checkbox"/> 好 <input type="checkbox"/> 一般 <input type="checkbox"/> 不好 <input type="checkbox"/> 差
从何处获取出版物信息	<input type="checkbox"/> 书目报 <input type="checkbox"/> 电子社宣传材料 <input type="checkbox"/> 书店 <input type="checkbox"/> 他人转告 <input type="checkbox"/> 网站 <input type="checkbox"/> 报刊
您认为电子工业出版社应改进的方面	<input type="checkbox"/> 先进性和实用性 <input type="checkbox"/> 文字可读性 <input type="checkbox"/> 篇幅适宜度 <input type="checkbox"/> 出版物中差错 <input type="checkbox"/> 设计水平 <input type="checkbox"/> 印刷装订质量 <input type="checkbox"/> 纸张质量（光盘材质） <input type="checkbox"/> 定价 <input type="checkbox"/> 宣传工作 <input type="checkbox"/> 服务质量
您的具体意见或建议	
读者姓名：	联系方式：
从事工作： <input type="checkbox"/> 技术研发 <input type="checkbox"/> 技术管理 <input type="checkbox"/> 经营管理 <input type="checkbox"/> 行政管理 <input type="checkbox"/> 教育培训 <input type="checkbox"/> 在校学习	

表格寄回：邮寄地址：北京市万寿路 173 信箱

传真：(010) 88254300

电子信箱：xiaoping@hex.cn

邮政编码：100036

收件人：同收信人

收信人：肖萍



# 目 录

第 1 章 网络基础知识 .....	1
1.1 网络的历史 .....	1
1.1.1 ARPA 的诞生 .....	1
1.1.2 分组交换 .....	2
1.1.3 TCP/IP 协议的诞生 .....	2
1.1.4 国家高速信息公路 .....	3
1.1.5 Internet 诞生 .....	3
1.1.6 网络的战争 .....	3
1.1.7 互联网的现状 .....	4
1.2 网络的体系结构 .....	4
1.2.1 星型网络 .....	5
1.2.2 环型网络 .....	6
1.2.3 网络采取的结构方式 .....	6
1.3 OSI 模型 .....	7
1.3.1 物理层 .....	7
1.3.2 数据链路层 .....	8
1.3.3 网络层 .....	8
1.3.4 传输层 .....	9
1.3.5 会话层 .....	9
1.3.6 表示层 .....	10
1.3.7 应用层 .....	10
1.4 TCP/IP 基础 .....	10
1.4.1 TCP/IP 协议参考模型 .....	10
1.4.2 主机与网络层 .....	10
1.4.3 互联网层 .....	11
1.4.4 传输层 .....	11
1.4.5 应用层 .....	11
1.4.6 IP 协议 .....	11
1.4.7 UDP 协议 .....	14
1.4.8 TCP 协议 .....	15
1.4.9 ARP 协议 .....	17
1.4.10 ICMP 协议 .....	18
1.4.11 HTTP 协议 .....	18
1.4.12 FTP 协议 .....	20
1.4.13 TCP/IP 协议的分析工具: Ethereal .....	20
1.4.14 入侵检测工具 Snort .....	21
1.4.15 Windows 自带的 Netstat 工具 .....	22



1.5	互联网一些知识	23
1.5.1	域名系统	23
1.5.2	动态主机配置协议 DHCP	23
1.5.3	TCP/IP 上的 NetBIOS	24
1.5.4	服务器消息块 SMB	25
1.6	路由基础知识	26
1.6.1	RIP 协议	26
1.6.2	OSPF 协议	26
1.6.3	BGP 协议	27
1.7	网络相关知识	27
1.7.1	计算机端口基础知识	28
1.7.2	计算机的安全分析工具	29
1.8	小结	29
<b>第 2 章</b>	<b>黑客基础</b>	<b>30</b>
2.1	黑客文化简史	30
2.1.1	黑客文化的“古文化”时期	30
2.1.2	黑客的 UNIX 时代	31
2.1.3	今天的黑客	31
2.2	帽子问题	31
2.2.1	“黑色”的黑客精神	32
2.2.2	帽子的划分	32
2.3	国内的黑客发展历史	32
2.4	早期著名的黑客	33
2.4.1	约翰·德拉浦	33
2.4.2	理查德·M·史托曼	34
2.4.3	罗伯特·莫里斯	34
2.4.4	凯文·米特尼克	34
2.5	著名的黑客组织	35
2.5.1	Blackhat	35
2.5.2	L0pht	35
2.5.3	中国绿色兵团	36
2.6	黑客常用攻击手法：踩点	36
2.6.1	社交工程	36
2.6.2	搜索引擎	36
2.6.3	Whois 方法	37
2.6.4	DNS 查询	37
2.7	黑客常用攻击手法：扫描	37
2.7.1	Ping 扫描	37
2.7.2	ICMP 查询	37
2.7.3	操作系统指纹识别	38
2.7.4	端口扫描	38
2.7.5	拓扑发现	38
2.8	黑客常用攻击手法：渗透	38
2.8.1	弱口令	38



2.8.2	开放端口	38
2.8.3	开放服务	39
2.8.4	操作系统版本信息	39
2.8.5	操作系统的漏洞信息与应用软件的漏洞信息	39
2.8.6	应用软件的漏洞信息	39
2.9	黑客常用攻击手法：权限提升	40
2.10	黑客常用攻击手法：木马与远程控制	40
2.10.1	木马的原理	40
2.10.2	著名的木马	40
2.11	使用防火墙防护个人计算机	41
2.11.1	防火墙的基本原理	41
2.11.2	防火墙的功能	41
2.11.3	基于状态的防火墙	42
2.11.4	基于代理的防火墙	42
2.11.5	防火墙的不足	42
2.12	使用杀毒软件防护个人计算机	42
2.12.1	杀毒软件的原理	42
2.12.2	杀毒软件的特点	43
2.13	使用木马清除工具检查木马	43
2.13.1	木马清除的原理	43
2.13.2	反间谍软件	43
2.13.3	木马清除工具的局限性	44
2.14	一些常见的安全事件	44
2.14.1	拒绝服务攻击	44
2.14.2	蠕虫引起的互联网瘫痪问题	45
2.14.3	僵尸网络	46
2.14.4	网络“钓鱼”	46
2.15	黑客的道德与法律问题	48
2.16	小结	48
<b>第3章</b>	<b>漏洞基础知识</b>	<b>50</b>
3.1	Windows 操作系统漏洞	50
3.1.1	Microsoft Windows 内核消息处理本地缓冲区溢出漏洞的简介	50
3.1.2	Microsoft Windows 内核消息处理本地缓冲区溢出漏洞的实战	51
3.1.3	Microsoft Windows 内核消息处理本地缓冲区溢出漏洞的安全解决方案	53
3.1.4	Microsoft Windows LPC 本地堆溢出漏洞的简介	55
3.1.5	Microsoft Windows LPC 本地堆溢出漏洞的实战	55
3.1.6	Microsoft Windows LPC 本地堆溢出漏洞的安全解决方案	57
3.1.7	Microsoft OLE 和 COM 远程缓冲区溢出漏洞简介	58
3.1.8	Microsoft OLE 和 COM 远程缓冲区溢出漏洞的实战	58
3.1.9	Microsoft OLE 和 COM 远程缓冲区溢出漏洞的安全解决方案	60
3.1.10	Microsoft Windows GDI+ JPG 解析组件缓冲区溢出漏洞简介	61
3.1.11	Microsoft Windows GDI+ JPG 解析组件缓冲区溢出漏洞的实战	61
3.1.12	Microsoft Windows GDI+ JPG 解析组件缓冲区溢出漏洞的安全解决方案	65
3.1.13	Microsoft Windows 图形渲染引擎安全漏洞简介	67

3.1.14	Microsoft Windows 图形渲染引擎安全漏洞的实战	67
3.1.15	Microsoft Windows 图形渲染引擎安全漏洞的安全解决方案	71
3.1.16	Microsoft UPnP 缓冲溢出漏洞简介	72
3.1.17	UPnP 缓冲区溢出漏洞的实战	73
3.1.18	UPnP 缓冲区溢出漏洞的安全解决方案	74
3.1.19	Microsoft RPC 接口远程任意代码可执行漏洞	74
3.1.20	Microsoft RPC 接口远程任意代码可执行漏洞的实战	75
3.1.21	Microsoft RPC 接口远程任意代码可执行漏洞的安全解决方案	77
3.1.22	Microsoft WINS 服务远程缓冲区溢出漏洞	78
3.1.23	WINS 服务远程缓冲区溢出漏洞的实战	81
3.1.24	WINS 服务远程缓冲区溢出漏洞的安全解决方案	82
3.2	IIS 漏洞	83
3.2.1	IIS 的基础知识	83
3.2.2	IIS 漏洞基础知识	85
3.2.3	.printer 漏洞	86
3.2.4	.printer 漏洞的实战	87
3.2.5	.printer 漏洞的安全解决方案	91
3.2.6	Unicode 目录遍历漏洞	91
3.2.7	Unicode 目录遍历的实战	93
3.2.8	Unicode 目录遍历的安全解决方案	96
3.2.9	.asp 映射分块编码漏洞	97
3.2.10	.asp 映射分块编码漏洞的实战	98
3.2.11	.asp 映射分块编码漏洞的安全解决方案	99
3.2.12	WebDAV 远程缓冲区溢出漏洞	100
3.2.13	WebDAV 远程缓冲区溢出漏洞实战	102
3.2.14	WebDAV 远程缓冲区溢出漏洞的安全解决方案	103
3.2.15	WebDAV 超长请求远程拒绝服务攻击漏洞	103
3.2.16	WebDAV 超长请求远程拒绝服务攻击漏洞实战	106
3.2.17	WebDAV 超长请求远程拒绝服务攻击漏洞的安全解决方案	107
3.2.18	WebDAV XML 消息处理远程拒绝服务漏洞	108
3.2.19	WebDAV XML 消息处理远程拒绝服务漏洞实战	110
3.2.20	WebDAV XML 消息处理远程拒绝服务漏洞的安全解决方案	113
3.2.21	Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞	113
3.2.22	Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞实战	115
3.2.23	Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞的安全解决方案	116
3.3	Serv-U 漏洞	117
3.3.1	Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞	117
3.3.2	Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞实战	119
3.3.3	Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞的安全解决方案	121
3.3.4	Serv-U 本地权限提升漏洞	121
3.3.5	Serv-U 本地权限提升漏洞实战	123
3.3.6	Serv-U 本地权限提升漏洞的安全解决方案	127
3.4	小结	127
<b>第 4 章 BBS 与 Blog 的入侵实例</b>		<b>128</b>
4.1	存在上传漏洞的 BBS 的入侵实例	128

4.1.1	Google 可寻找的 BBS 系统	128
4.1.2	注册 BBS 资料	130
4.1.3	获取 Cookie	132
4.1.4	生成网页木马	137
4.1.5	上传网页木马	138
4.1.6	漏洞的防护	143
4.2	存在脚本漏洞的 BBS 的入侵实例	144
4.2.1	暴库漏洞的原理	145
4.2.2	Google 存在暴库漏洞的 BBS 论坛目标	146
4.2.3	注册 BBS 资料	148
4.2.4	获取论坛管理员密码	149
4.2.5	获取管理员账户	153
4.2.6	获取管理员前台密码	156
4.2.7	获取 Cookie	159
4.2.8	破解管理员后台密码	162
4.2.9	安全解决方案	164
4.3	与数据库相关的 Blog 的入侵实例	164
4.3.1	漏洞的检测	165
4.3.2	了解 Dlog 系统的结构	166
4.3.3	尝试入侵	168
4.3.4	上传网页木马	176
4.3.5	安全解决方案	183
4.4	基于 Cookie 欺骗的 Blog 入侵实例	183
4.4.1	漏洞的检测	184
4.4.2	了解 L-Blog 系统的结构	186
4.4.3	获取 Cookie 进行 Cookie 欺骗	187
4.4.4	安全解决方案	194
4.5	小结	194
<b>第 5 章</b>	<b>信息收集</b>	<b>195</b>
5.1	针对目标的信息搜集	195
5.1.1	什么是踩点	195
5.1.2	确定目标范围	196
5.2	Google 搜索技术	196
5.2.1	Google 的基本功能	197
5.2.2	site: 对搜索的网站进行限制	200
5.2.3	filetype: 在某一类文件中查找信息	201
5.2.4	inurl: 搜索的关键字包含在 URL 链接中	202
5.2.5	intitle: 搜索的关键字包含在网页标题中	203
5.2.6	inanchor: 搜索的关键字包含在网页的 anchor 链点内	204
5.2.7	link: 搜索所有链接到某个 URL 地址的网页	204
5.2.8	cache: 从 Google 服务器上的缓存页面中查询信息	205
5.2.9	Google 相关工具	205
5.2.10	Google 与黑客	208
5.3	Whois: 注册信息查询工具	211



5.3.1	ARIN: 国际域名注册机构	212
5.3.2	APNIC: 亚太域名注册机构	213
5.3.3	CNNIC: 中国域名注册机构	214
5.4	DNS 查询	216
5.4.1	主机名和 IP 地址	216
5.4.2	主机名的解析	217
5.4.3	主机名的分布	218
5.4.4	DNS 的工作方式	219
5.4.5	主 DNS 服务器	221
5.4.6	辅 DNS 服务器	221
5.4.7	从主 DNS 服务器向辅 DNS 服务器传送数据	221
5.4.8	客户机请求解析的过程	222
5.4.9	主机-IP 地址查询实例	223
5.4.10	使用 nslookup 命令查询 IP 地址	225
5.4.11	使用 nslookup 查询其他类型的域名	226
5.4.12	使用 nslookup 指定使用的名字服务器	227
5.4.13	使用 nslookup 检查域名的缓存时间	228
5.5	路由跟踪与 IP 追踪	232
5.5.1	TraceRoute: 路由跟踪	233
5.5.2	VisualRoute: IP 追踪	235
5.6	小结	236
<b>第 6 章</b>	<b>扫描目标</b>	<b>237</b>
6.1	漏洞扫描器的历史	237
6.2	确定正在运行的服务	237
6.2.1	Ping 扫描	238
6.2.2	ICMP 查询	239
6.2.3	确定运行的 TCP 服务和 UDP 服务的旗标	240
6.3	端口扫描原理	242
6.3.1	标准端口与非标准端口的划分	242
6.3.2	标准端口和非标准端口的含义	244
6.3.3	TCP/IP 的“三次握手”	245
6.3.4	端口扫描应用	246
6.3.5	Nessus 扫描器	246
6.3.6	X-Scan 扫描器	248
6.4	扫描方法简介	252
6.4.1	TCP Connect 扫描	252
6.4.2	SYN 扫描	254
6.4.3	FIN 扫描	255
6.4.4	圣诞树扫描	256
6.4.5	TCP 空扫描	256
6.4.6	TCPACK 扫描	257
6.4.7	TCP Windows 扫描	258
6.4.8	TCP RPC 扫描	258
6.4.9	UDP 扫描	259



6.5	操作系统 (OS) 的识别	260
6.5.1	主动协议栈指纹识别技术	260
6.5.2	被动协议栈指纹识别技术	262
6.5.3	其他的指纹识别技术	263
6.6	扫描过程中的攻击技术	268
6.6.1	IP 欺骗	268
6.6.2	DNS 欺骗	269
6.6.3	Sniffing 攻击	269
6.6.4	缓冲区溢出	270
6.7	扫描工具	270
6.7.1	Nmap: 扫描器之王	270
6.7.2	Nessus: 分布式的扫描器	272
6.7.3	X-Scan: 国内最好的扫描器	273
6.8	小结	274
<b>第 7 章</b>	<b>渗透测试</b>	<b>275</b>
7.1	渗透的原理	275
7.1.1	渗透基础知识	275
7.1.2	缓冲区溢出攻击的基础知识	275
7.1.3	缓冲区溢出漏洞的攻击方式	276
7.1.4	缓冲区溢出的防范	276
7.1.5	堆溢出	277
7.1.6	格式化串漏洞利用技术	279
7.1.7	内核溢出利用技术	280
7.2	数据库的渗透	281
7.2.1	数据库的用户与权限	282
7.2.2	SQL 注入技术	282
7.2.3	使用 Nessus 进行数据库渗透测试	286
7.3	Web 应用的渗透	290
7.3.1	CGI 渗透测试技术	290
7.3.2	使用 Nessus 进行 Web 应用渗透测试	291
7.3.3	使用 Wikto 进行 Web 应用渗透测试	296
7.4	Metasploit: 渗透测试工具	299
7.4.1	Metasploit 基础	299
7.4.2	命令行界面的 Metasploit	300
7.4.3	图形界面的 Metasploit	304
7.5	小结	306
<b>第 8 章</b>	<b>网络设备的攻击</b>	<b>307</b>
8.1	网络设备概述	307
8.1.1	交换机	307
8.1.2	三层交换技术	308
8.1.3	局域网交换机的种类	308
8.1.4	交换机应用中的问题	309
8.1.5	路由器	309
8.1.6	路由选择	311



8.1.7	路由协议 .....	311
8.1.8	路由算法 .....	312
8.2	ASS 基础 .....	313
8.3	SNMP 原理 .....	314
8.3.1	SNMP 基础知识 .....	314
8.3.2	SNMP v1 .....	316
8.3.3	SNMP v2 .....	317
8.4	TraceRoute 技术 .....	317
8.4.1	TraceRoute 原理 .....	317
8.4.2	TraceRoute 工具 .....	319
8.5	攻击网络设备 .....	320
8.5.1	SNMP 的安全性分析 .....	320
8.5.2	利用 TFTP .....	322
8.6	小结 .....	323
<b>第 9 章</b>	<b>木马分析 .....</b>	<b>324</b>
9.1	木马的基本概念 .....	324
9.1.1	木马的定义 .....	324
9.1.2	木马的特征 .....	324
9.1.3	木马的基本功能: 远程监视、控制 .....	325
9.1.4	木马的基本功能: 远程视频监控 .....	326
9.1.5	木马的基本功能: 远程管理 .....	326
9.1.6	木马的基本功能: 发送信息 .....	326
9.1.7	木马的基本功能: 获得主机信息 .....	327
9.1.8	木马的基本功能: 修改系统注册表 .....	327
9.1.9	木马的基本功能: 远程命令 .....	328
9.1.10	连接型木马 .....	328
9.1.11	用途型木马 .....	331
9.1.12	木马的发展方向 .....	331
9.1.13	灰鸽子木马 .....	332
9.2	木马的行为分析 .....	337
9.2.1	木马常用隐藏手段 .....	337
9.2.2	木马的自启动技术 .....	339
9.2.3	木马连接的隐藏技术 .....	340
9.3	冰河远程控制 .....	340
9.3.1	配置服务端 .....	341
9.3.2	服务端的基本特征 .....	342
9.3.3	冰河的使用 .....	343
9.3.4	冰河的手工卸载 .....	346
9.4	上兴远程控制 .....	346
9.4.1	配置自动上线 .....	346
9.4.2	配置服务端程序 .....	346
9.4.3	上兴远程控制的基本特征 .....	347
9.4.4	上兴远程控制的使用 .....	347
9.4.5	手工删除上兴远程控制 .....	353





9.5 RAdmin .....	354
9.5.1 配置服务端 .....	354
9.5.2 安装服务端 .....	354
9.5.3 RAdmin 的特征 .....	354
9.5.4 RAdmin 的使用 .....	356
9.5.5 手工删除 RAdmin .....	358
9.6 木马的防范 .....	358
9.6.1 查：检查系统进程与服务 .....	358
9.6.2 堵：控制木马的活动 .....	359
9.6.3 杀：消除木马的隐患 .....	359
9.7 netstat 命令 .....	360
9.7.1 netstat 命令用法 .....	360
9.7.2 用 netstat 命令来监测木马 .....	361
9.8 使用冰刃检查木马活动 .....	362
9.8.1 利用冰刃查看进程 .....	362
9.8.2 利用冰刃查看端口 .....	362
9.8.3 注册表 .....	363
9.8.4 用冰刃查看文件 .....	364
9.8.5 用冰刃查看启动组 .....	364
9.8.6 用冰刃查看系统服务 .....	365
9.8.7 利用冰刃查找木马实战 .....	365
9.9 Ethereal：网络抓包工具 .....	366
9.9.1 Ethereal 使用介绍 .....	366
9.9.2 对木马的监测 .....	368
9.10 小结 .....	369
<b>第 10 章 病毒分析</b> .....	<b>370</b>
10.1 计算机病毒基础 .....	370
10.1.1 计算机病毒的定义 .....	370
10.1.2 计算机病毒发展简史 .....	371
10.1.3 计算机病毒的特征 .....	372
10.1.4 计算机病毒的程序结构 .....	373
10.1.5 计算机病毒的存储结构 .....	374
10.1.6 计算机病毒的分类 .....	376
10.1.7 计算机病毒的入侵方式 .....	378
10.1.8 计算机病毒的命名 .....	379
10.1.9 计算机病毒的生命周期 .....	380
10.2 计算机病毒分析 .....	381
10.2.1 早期的 DOS 病毒介绍 .....	381
10.2.2 宏病毒 .....	381
10.2.3 文件型病毒 .....	382
10.2.4 引导型病毒 .....	384
10.3 蠕虫病毒 .....	385
10.3.1 蠕虫的基本结构和传播过程 .....	385
10.3.2 蠕虫传播的模式分析 .....	385