

宝典丛书

200万

网络安全 与黑客攻防

(第3版)

宝典

作者根据实战经验精心改编的实例将帮助读者借鉴并开拓思路

涉及无线网络、Metasploit、Nessus、UTM、网络钓鱼、流氓软件等最新技术, 阅读价值大大提升

全面提供有针对性的防守方案

李俊民 等编著



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

宝典丛书

网络安全与黑客攻防宝典

(第3版)

李俊民 等编著

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 21 章，内容涵盖网络的基础知识、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、网络脚本攻防、SQL 注入攻防、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，每一节的例子都经过精挑细选，具有很强的针对性，读者可以通过亲手实践进而掌握安全防护的基本要领和技巧。

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 / 李俊民 等编著. —3 版. —北京: 电子工业出版社, 2011.5
(宝典丛书)

ISBN 978-7-121-13124-0

I. ①网… II. ①李… 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(2011)第 044830 号

责任编辑: 张月萍

印 刷: 北京东光印刷厂

装 订: 三河市皇庄路通装订厂

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: 49.25 字数: 1386千字

印 次: 2011年5月第1次印刷

印 数: 4000册

定 价: 89.00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 zlt@spei.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

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，如深入分析黑客入侵计算机的全过程，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系统的目的，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、有趣的情节为依托，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。

本书特色

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；二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，使思路变得更加开拓。

◆ **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。**

在本书中介绍了大量的新知识，如 Metasploit、Nessus、UTM、EnCase、网络钓鱼、流氓软件和 NetStumbler 等。这些新知识的介绍充实了本书的内容，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。

◆ **兼顾各种水平的读者。**

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，这些内容可为高级读者提供进一步参考。

本书内容

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 帮助读者了解高级黑客搜集信息的工具及方法，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 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 用户在使用网络资源时，需要了解针对各种计算机病毒和木马的防范方法。本章介绍了这些方法。

第 12 章 脚本攻击通常针对这些数据库来配合脚本对一些变量的过滤不严等问题，得到用户密码等敏感信息。本章就教会我们如何摆脱脚本攻击。

第 13 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 14 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 15 章 让用户学习通过对网络的封锁和代理突破，来实现维护计算机网络的安全性和可靠性。

第 16 章 讲解针对计算机操作系统的攻防技术，以及如何实现对软件和文件资料进行加密等相关的内容。

第 17 章 讲解 ASP 和 PHP 环境下的 SQL 注入技术，并了解 SQL 注入的防护。

第 18 章 讲解在计算机网络安全攻防中，使用欺骗攻击技术实施攻击的原理及其安全防范方面的相关知识。

第 19 章 讲解与后门技术相关的一些内容，使得读者对后门技术的攻击及防范知识有一定的了解。

第 20 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 21 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。

本书作者

本书主要由李俊民编写。其他参与编写的人员有张金霞、于锋、张伟、曾广平、刘海峰、刘涛、赵宝永、郑莲华、张涛、杨强、陈涛、罗渊文、李居英、郭永胜。在此对所有参与编写的人表示感谢！

由于笔者水平所限，书中可能还存在疏漏和错误，还望广大读者批评指正。

严正声明

严正声明：本书所讨论的技术仅用于研究学习，旨在最大限度地唤醒大家的信息安全意识，提高信息安全防护技能，严禁用于非法活动。任何个人、团体、组织不得将其用于非法目的，违法犯罪必将受到法律的严厉制裁。

《中华人民共和国刑法》关于信息安全的条例

第二百五十三条之一 国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

第二百八十五条 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

第二百八十六条 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

第二百八十七条 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

目 录

第 1 部分 黑客基础篇	1	2.3 国内的黑客发展历史	24
第 1 章 网络基础知识	2	2.4 早期著名的黑客	25
1.1 OSI 模型	2	2.4.1 约翰·德拉浦	25
1.1.1 物理层	3	2.4.2 理查德·M·史托曼	25
1.1.2 数据链路层	3	2.4.3 罗伯特·莫里斯	25
1.1.3 网络层	4	2.4.4 凯文·米特尼克	26
1.1.4 传输层	4	2.5 著名的黑客组织	26
1.1.5 会话层	4	2.5.1 Blackhat	26
1.1.6 表示层	5	2.5.2 L0pht	26
1.1.7 应用层	5	2.5.3 中国绿色兵团	27
1.2 TCP/IP 基础	5	2.6 黑客常用攻击手法: 踩点	27
1.2.1 TCP/IP 协议参考模型	5	2.6.1 社交工程	27
1.2.2 主机与网络层	6	2.6.2 搜索引擎	27
1.2.3 互联网层	6	2.6.3 Whois 方法	28
1.2.4 传输层	6	2.6.4 DNS 查询	28
1.2.5 应用层	6	2.7 黑客常用攻击手法: 扫描	28
1.2.6 IP 协议	7	2.7.1 Ping 扫描	28
1.2.7 UDP 协议	8	2.7.2 ICMP 查询	28
1.2.8 TCP 协议	9	2.7.3 操作系统指纹识别	28
1.2.9 ARP 协议	10	2.7.4 端口扫描	29
1.2.10 ICMP 协议	11	2.7.5 拓扑自动发现	29
1.2.11 HTTP 协议	12	2.8 黑客常用攻击手法: 渗透	29
1.2.12 FTP 协议	12	2.8.1 弱口令	29
1.2.13 TCP/IP 协议的分析工具	13	2.8.2 开放端口	29
Ethereal	13	2.8.3 开放服务	30
1.2.14 入侵检测工具 Snort	14	2.8.4 操作系统版本信息	30
1.2.15 Windows 自带的 Netstat 工具	15	2.8.5 操作系统的漏洞信息	30
1.3 与互联网相关的一些知识	15	2.8.6 应用软件的漏洞信息	30
1.3.1 域名系统	15	2.9 黑客常用攻击手法: 权限提升	30
1.3.2 动态主机配置协议 DHCP	16	2.10 黑客常用攻击手法: 木马与远程	31
1.3.3 TCP/IP 上的 NetBIOS	16	控制	31
1.3.4 服务器消息块 SMB	18	2.10.1 木马的原理	31
1.4 网络相关知识	19	2.10.2 著名的木马	31
1.4.1 计算机端口基础知识	19	2.11 使用防火墙防护个人计算机	32
1.4.2 计算机的安全分析工具	20	2.11.1 防火墙的基本原理	32
1.5 小结	21	2.11.2 防火墙的功能	32
第 2 章 黑客基础	22	2.11.3 基于状态的防火墙	32
2.1 黑客文化简史	22	2.11.4 基于代理的防火墙	33
2.1.1 黑客文化的古文化时期	22	2.11.5 防火墙的不足	33
2.1.2 黑客的 UNIX 时代	23	2.12 使用杀毒软件防护个人计算机	33
2.1.3 今天的黑客	23	2.12.1 杀毒软件的原理	33
2.2 帽子问题	23	2.12.2 杀毒软件的特点	33
2.2.1 “黑色”的黑客精神	23	2.13 使用木马清除工具检查木马	34
2.2.2 帽子的划分	24	2.13.1 木马清除工具的原理	34
		2.13.2 反间谍软件	34
		2.13.3 木马清除工具的局限性	34



2.14	一些常见的安全事件	34	3.1.17	UPnP 缓冲区溢出漏洞的 实战	65
2.14.1	拒绝服务攻击	35	3.1.18	UPnP 缓冲区溢出漏洞的安全 解决方案	66
2.14.2	蠕虫引起的互联网瘫痪问题	36	3.1.19	Microsoft RPC 接口远程任意 代码可执行漏洞	66
2.14.3	僵尸网络	36	3.1.20	Microsoft RPC 接口远程任意 代码可执行漏洞的实战	68
2.14.4	网络“钓鱼”	37	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	69
2.15	黑客的道德与法律问题	38	3.1.22	Microsoft WINS 服务远程缓 冲区溢出漏洞	70
2.16	黑客软件开发工具	38	3.1.23	Microsoft WINS 服务远程缓 冲区溢出漏洞的实战	72
2.16.1	Visual Basic 编程语言介绍	38	3.1.24	Microsoft WINS 服务远程缓 冲区溢出漏洞的安全解决 方案	74
2.16.2	Delphi 编程语言介绍	41	3.2	IIS 漏洞	74
2.16.3	Visual C++编程语言介绍	44	3.2.1	IIS 的基础知识	74
2.17	小结	46	3.2.2	IIS 漏洞基础知识	76
第2部分 漏洞、木马与病毒篇			3.2.3	printer 漏洞	77
第3章 漏洞基础知识			3.2.4	.printer 漏洞的实战	78
3.1	Windows 操作系统漏洞	48	3.2.5	.printer 漏洞的安全解决方案	81
3.1.1	Microsoft Windows 内核消息 处理本地缓冲区溢出漏洞的 简介	48	3.2.6	Unicode 目录遍历漏洞	81
3.1.2	Microsoft Windows 内核消息 处理本地缓冲区溢出漏洞的 实战	49	3.2.7	Unicode 目录遍历的实战	83
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	50	3.2.8	Unicode 目录遍历的安全解决 方案	86
3.1.4	Microsoft Windows LPC 本地 堆溢出漏洞的简介	51	3.2.9	.asp 映射分块编码漏洞	86
3.1.5	Microsoft Windows LPC 本地 堆溢出漏洞的实战	51	3.2.10	.asp 映射分块编码漏洞的 实战	87
3.1.6	Microsoft Windows LPC 本地 堆溢出漏洞的安全解决方案	53	3.2.11	.asp 映射分块编码漏洞的安 全解决方案	89
3.1.7	Microsoft OLE 和 COM 远程 缓冲区溢出漏洞简介	54	3.2.12	WebDAV 远程缓冲区溢出 漏洞	89
3.1.8	Microsoft OLE 和 COM 远程 缓冲区溢出漏洞的实战	54	3.2.13	WebDAV 远程缓冲区溢出漏 洞实战	91
3.1.9	Microsoft OLE 和 COM 远程 缓冲区溢出漏洞的安全解决 方案	56	3.2.14	WebDAV 远程缓冲区溢出漏 洞的安全解决方案	92
3.1.10	Microsoft Windows GDI+ JPG 解析组件缓冲区溢出漏洞 简介	56	3.2.15	WebDAV 超长请求远程拒绝 服务攻击漏洞	92
3.1.11	Microsoft Windows GDI+ JPG 解析组件缓冲区溢出漏洞的 实战	57	3.2.16	WebDAV 超长请求远程拒绝 服务攻击漏洞实战	94
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	59	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	96
3.1.13	Microsoft Windows 图形渲染 引擎安全漏洞简介	61	3.2.18	WebDAV XML 消息处理远程 拒绝服务漏洞	96
3.1.14	Microsoft Windows 图形渲染 引擎安全漏洞的实战	61	3.2.19	WebDAV XML 消息处理远程 拒绝服务漏洞实战	97
3.1.15	Microsoft Windows 图形渲染 引擎安全漏洞的安全解决 方案	64	3.2.20	WebDAV XML 消息处理远程 拒绝服务漏洞的安全解决 方案	99
3.1.16	Microsoft UPnP 缓冲溢出漏洞 简介	65	3.2.21	Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞	100



3.2.22	Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞实战	102	5.1.1	什么是踩点	169
3.2.23	Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞的安全解决方案	103	5.1.2	确定目标范围	170
3.3	Serv-U 漏洞	104	5.2	Google 搜索技术	170
3.3.1	Serv-U FTP 服务器 MDTM 命令缓冲区溢出漏洞	104	5.2.1	Google 的基本功能	170
3.3.2	Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞实战	106	5.2.2	site: 对搜索的网站进行限制	174
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	108	5.2.3	filetype: 在某一类文件中查找信息	174
3.3.4	Serv-U 本地权限提升漏洞	108	5.2.4	inurl: 搜索的关键词包含在 URL 链接中	175
3.3.5	Serv-U 本地权限提升漏洞实战	110	5.2.5	intitle: 搜索的关键词包含在网页标题中	176
3.3.6	Serv-U 本地权限提升漏洞的安全解决方案	113	5.2.6	inanchor: 搜索的关键词包含在网页的 anchor 链点内	176
3.4	小结	113	5.2.7	link: 搜索所有链接到某个 URL 地址的网页	177
			5.2.8	cache: 从 Google 服务器上的缓存页面中查询信息	178
			5.2.9	Google 相关工具	178
			5.2.10	Google 与黑客	181
第 4 章	BBS 与 Blog 的入侵实例	114	5.3	Whois: 注册信息查询工具	184
4.1	存在上传漏洞的 BBS 的入侵实例	114	5.3.1	ARIN: 国际域名注册机构	185
4.1.1	Google 可寻找的 BBS 系统	114	5.3.2	APNIC: 亚太域名注册机构	186
4.1.2	注册 BBS 资料	116	5.3.3	CNNIC: 中国域名注册机构	186
4.1.3	获取 Cookie	117	5.4	DNS 查询	188
4.1.4	生成网页木马	121	5.4.1	主机名和 IP 地址	188
4.1.5	上传网页木马	122	5.4.2	主机名的解析	189
4.1.6	漏洞的防护	125	5.4.3	主机名的分布	190
4.2	存在脚本漏洞的 BBS 的入侵实例	126	5.4.4	DNS 的工作方式	191
4.2.1	暴库漏洞的原理	127	5.4.5	主 DNS 服务器	193
4.2.2	Google 存在暴库漏洞的 BBS 论坛目标	127	5.4.6	辅 DNS 服务器	193
4.2.3	注册 BBS 资料	129	5.4.7	从主 DNS 服务器向辅 DNS 服务器传送数据	194
4.2.4	获取论坛管理员密码	131	5.4.8	客户机请求解析的过程	195
4.2.5	获取管理员账户	133	5.4.9	主机 IP 地址查询实例	196
4.2.6	获取管理员前台密码	136	5.4.10	使用 nslookup 命令查询 IP 地址	197
4.2.7	获取 Cookie	138	5.4.11	使用 nslookup 查询其他类型的域名	198
4.2.8	破解管理员后台密码	141	5.4.12	使用 nslookup 指定使用的名字服务器	199
4.2.9	安全解决方案	143	5.4.13	使用 nslookup 检查域名的缓存时间	200
4.3	与数据库相关的 Blog 的入侵实例	143	5.5	路由跟踪与 IP 追踪	205
4.3.1	漏洞的检测	143	5.5.1	TraceRoute: 路由跟踪	205
4.3.2	了解 Dlog 系统的结构	144	5.5.2	VisualRoute: IP 追踪	207
4.3.3	尝试入侵	146	5.6	小结	208
4.3.4	上传网页木马	153			
4.3.5	安全解决方案	158	第 6 章	扫描目标	209
4.4	基于 Cookie 欺骗的 Blog 入侵实例	159	6.1	漏洞扫描器的历史	209
4.4.1	漏洞的检测	159	6.2	确定正在运行的服务	209
4.4.2	了解 L-Blog 系统的结构	161	6.2.1	Ping 扫描	210
4.4.3	获取 Cookie 进行 Cookie 欺骗	162	6.2.2	ICMP 查询	211
4.4.4	安全解决方案	168	6.2.3	确定运行的 TCP 服务和 UDP 服务的旗标	212
4.5	小结	168	6.3	端口扫描原理	214
第 5 章	信息收集	169			
5.1	针对目标的信息搜集	169			



6.3.1	标准端口与非标准端口的划分	214	7.4.3	图形界面的 Metasploit	274
6.3.2	标准端口和非标准端口的含义	216	7.5	小结	276
6.3.3	TCP/IP 的“三次握手”	216	第 8 章	网络设备的攻击	277
6.3.4	端口扫描应用	217	8.1	网络设备概述	277
6.3.5	Nessus 扫描器	218	8.1.1	交换机	277
6.3.6	X-Scan 扫描器	220	8.1.2	三层交换技术	278
6.4	扫描方法简介	223	8.1.3	局域网交换机的种类	278
6.4.1	TCP Connect 扫描	224	8.1.4	交换机应用中的问题	279
6.4.2	TCP SYN 扫描	225	8.1.5	路由器	279
6.4.3	TCP FIN 扫描	226	8.1.6	路由选择	281
6.4.4	圣诞树扫描	227	8.1.7	路由协议	281
6.4.5	TCP 空扫描	227	8.1.8	路由算法	282
6.4.6	TCP ACK 扫描	228	8.2	ASS 基础	283
6.4.7	TCP Windows 扫描	229	8.3	SNMP 原理	284
6.4.8	TCP RPC 扫描	229	8.3.1	SNMP 基础知识	284
6.4.9	UDP 扫描	229	8.3.2	SNMP v1	286
6.5	操作系统 (OS) 的识别	230	8.3.3	SNMP v2	286
6.5.1	主动协议栈指纹识别技术	231	8.4	TraceRoute 技术	287
6.5.2	被动协议栈指纹识别技术	232	8.4.1	TraceRoute 原理	287
6.5.3	其他的指纹识别技术	234	8.4.2	TraceRoute 工具	288
6.6	扫描过程中的攻击技术	239	8.5	攻击网络设备	289
6.6.1	IP 欺骗	239	8.5.1	SNMP 的安全性分析	289
6.6.2	DNS 欺骗	240	8.5.2	利用 TFTP	291
6.6.3	Sniffing 攻击	240	8.6	小结	292
6.6.4	缓冲区溢出	241	第 9 章	木马分析	293
6.7	扫描工具	241	9.1	木马的基本概念	293
6.7.1	Nmap: 扫描器之王	241	9.1.1	木马的定义	293
6.7.2	Nessus: 分布式的扫描器	243	9.1.2	木马的特征	293
6.7.3	X-Scan: 国内最好的扫描器	244	9.1.3	木马的基本功能: 远程监视、控制	294
6.8	小结	244	9.1.4	木马的基本功能: 远程视频监控	295
第 7 章	渗透测试	245	9.1.5	木马的基本功能: 远程管理	295
7.1	渗透的原理	245	9.1.6	木马的基本功能: 发送信息	296
7.1.1	渗透基础知识	245	9.1.7	木马的基本功能: 获得主机信息	296
7.1.2	缓冲区溢出攻击的基础知识	245	9.1.8	木马的基本功能: 修改系统注册表	297
7.1.3	缓冲区溢出漏洞的攻击方式	246	9.1.9	木马的基本功能: 远程命令	297
7.1.4	缓冲区溢出的防范	246	9.1.10	连接型木马	298
7.1.5	堆溢出	246	9.1.11	用途型木马	300
7.1.6	格式化串漏洞利用技术	248	9.1.12	木马的发展方向	300
7.1.7	内核溢出利用技术	249	9.1.13	灰鸽子木马	301
7.2	数据库的渗透	251	9.2	木马的行为分析	305
7.2.1	数据库的用户与权限	251	9.2.1	木马常用隐藏手段	305
7.2.2	SQL 注入技术	252	9.2.2	木马的自启动技术	307
7.2.3	使用 Nessus 进行数据库渗透测试	255	9.2.3	木马连接的隐藏技术	308
7.3	Web 应用的渗透	259	9.3	冰河远程控制	309
7.3.1	CGI 渗透测试技术	260	9.3.1	配置服务端	310
7.3.2	使用 Nessus 进行 Web 应用渗透测试	261	9.3.2	服务端的基本特征	311
7.3.3	使用 Wikto 进行 Web 应用渗透测试	265	9.3.3	冰河的使用	312
7.4	Metasploit: 渗透测试工具	269	9.3.4	冰河的手工卸载	313
7.4.1	Metasploit 基础	269			
7.4.2	命令行界面的 Metasploit	270			

9.4	上兴远程控制	314	10.3.7	“斯文”病毒	354
9.4.1	配置自动上线	315	10.3.8	SQL 蠕虫	355
9.4.2	配置服务端程序	315	10.3.9	一个简单的蠕虫实验	355
9.4.3	上兴远程控制的基本特征	315	10.4	网页脚本病毒	357
9.4.4	上兴远程控制的使用	316	10.4.1	网页脚本病毒的背景知识	357
9.4.5	手工删除上兴远程控制	320	10.4.2	“欢乐时光”病毒	358
9.5	RAdmin	321	10.4.3	一个简单的脚本及恶意网页实验	359
9.5.1	配置服务端	321	10.5	即时通信病毒分析	360
9.5.2	安装服务端	322	10.5.1	即时通信病毒背景介绍	360
9.5.3	RAdmin 的特征	322	10.5.2	MSN 性感鸡	361
9.5.4	RAdmin 的使用	324	10.6	操作系统漏洞攻击病毒分析	362
9.5.5	手工删除 RAdmin	325	10.6.1	漏洞攻击病毒背景介绍	362
9.6	木马的防范	325	10.6.2	红色代码	362
9.6.1	查: 检查系统进程与服务	326	10.6.3	冲击波病毒	363
9.6.2	堵: 控制木马的活动	327	10.6.4	震荡波病毒	364
9.6.3	杀: 消除木马的隐患	327	10.7	病毒发展的新阶段——移动通信病毒分析	365
9.7	netstat 命令	327	10.7.1	移动通信病毒背景介绍	365
9.7.1	netstat 命令用法	328	10.7.2	移动通信病毒的特点	366
9.7.2	用 netstat 命令来监测木马	329	10.7.3	手机病毒的传播途径	366
9.8	使用冰刃检查木马活动	329	10.7.4	手机病毒的攻击方式	367
9.8.1	利用冰刃查看进程	329	10.7.5	防范移动通信病毒的安全建议	368
9.8.2	利用冰刃查看端口	330	10.8	网络钓鱼概述	368
9.8.3	注册表	330	10.8.1	网络钓鱼背景介绍	368
9.8.4	用冰刃查看文件	331	10.8.2	网络钓鱼的手段和危害	369
9.8.5	用冰刃查看启动组	332	10.8.3	利用电子邮件“钓鱼”	369
9.8.6	用冰刃查看系统服务	332	10.8.4	防范网络钓鱼的安全建议	370
9.8.7	利用冰刃查找木马实战	332	10.9	流氓软件概述	370
9.9	Ethereal: 网络抓包工具	334	10.9.1	流氓软件分类及其危害	371
9.9.1	Ethereal 使用介绍	334	10.9.2	删除流氓软件的工具	371
9.9.2	对木马的监测	335	10.9.3	流氓软件的安全防范	374
9.10	小结	336	10.10	其他操作系统病毒	374
			10.10.1	Linux 与 UNIX 病毒	374
			10.10.2	MAC OS 病毒	375
			10.11	小结	376
第 10 章	病毒分析	337	第 3 部分	网络攻防篇	377
10.1	计算机病毒基础	337	第 11 章	网络安全防范	378
10.1.1	计算机病毒的定义	337	11.1	聊天工具安全防范	378
10.1.2	计算机病毒发展简史	338	11.1.1	QQ 聊天工具安全防范	378
10.1.3	计算机病毒的特征	338	11.1.2	WLM 与安全防范	383
10.1.4	计算机病毒的程序结构	340	11.2	IE 漏洞安全防范	385
10.1.5	计算机病毒的存储结构	340	11.2.1	MIME 漏洞的防范	385
10.1.6	计算机病毒的分类	342	11.2.2	IE 执行程序漏洞的防范	386
10.1.7	计算机病毒的入侵方式	344	11.2.3	IE 浏览器安全防范	387
10.1.8	计算机病毒的命名	345	11.3	网络炸弹安全防范	391
10.1.9	计算机病毒的生命周期	346	11.3.1	IE 窗口炸弹的防范	391
10.2	计算机病毒分析	347	11.3.2	QQ 信息炸弹的防范	391
10.2.1	早期的 DOS 病毒介绍	347	11.3.3	电子邮件炸弹的防范	393
10.2.2	宏病毒	347	11.4	电子邮件安全防范	394
10.2.3	文件型病毒	348	11.4.1	邮件客户端的防范	394
10.2.4	引导型病毒	350	11.4.2	网络邮箱的防范	396
10.3	蠕虫病毒	350	11.5	小结	397
10.3.1	蠕虫的基本结构和传播过程	351			
10.3.2	蠕虫传播的模式分析	351			
10.3.3	安全防御蠕虫的传播	351			
10.3.4	尼姆达 (Nimda) 病毒	352			
10.3.5	W32.Sircam 病毒	352			
10.3.6	SCO 炸弹	353			

第 12 章 网站脚本的攻防	398	13.6.3 瑞星防火墙的主菜单	433
12.1 脚本攻击概述	398	13.7 基于 Linux 的防火墙 iptables	437
12.1.1 网站后台漏洞介绍	398	13.7.1 iptables 的发展历史	437
12.1.2 网页脚本攻击的分类	399	13.7.2 iptables 原理	437
12.2 常见脚本攻防	399	13.7.3 启动 iptables	438
12.2.1 常见的 ASP 脚本攻防	399	13.7.4 iptables 命令	439
12.2.2 JavaScript 语言与 HTML 脚本语言的防护	400	13.7.5 iptables 防火墙应用举例	441
12.3 跨站脚本的攻防	401	13.7.6 内核 Netfilter 框架的使用	443
12.3.1 HTML 输入概述	402	13.8 小结	446
12.3.2 跨站脚本攻击剖析	402	第 14 章 入侵检测技术	447
12.3.3 跨站脚本攻击的安全防护	403	14.1 入侵检测技术概述	447
12.4 网站管理账号的防护	403	14.1.1 入侵检测系统功能	447
12.4.1 DCP-Portal 系统安全防护	403	14.1.2 入侵检测系统的模型	448
12.4.2 动网文章管理系统账号破解与防护	404	14.1.3 IDS 的数据来源	449
12.5 论坛的防护	404	14.2 入侵检测方法	449
12.5.1 BBSXP 论坛安全防护	404	14.2.1 异常入侵检测技术	450
12.5.2 Leadbbs 论坛安全防护	405	14.2.2 误用入侵检测技术	450
12.6 小结	405	14.3 入侵检测系统的设计原理	451
第 13 章 防火墙技术	406	14.3.1 主机入侵检测系统 (HIDS)	451
13.1 防火墙概述	406	14.3.2 网络入侵检测系统 (NIDS)	452
13.1.1 防火墙的功能	406	14.3.3 分布式结构的入侵检测系统	454
13.1.2 防火墙的模型	407	14.4 入侵检测系统产品选型原则与产品介绍	455
13.1.3 防火墙发展史	408	14.4.1 入侵检测系统产品选型原则	455
13.1.4 防火墙的发展趋势	408	14.4.2 入侵检测系统产品介绍	455
13.1.5 防火墙的局限性	409	14.5 在 Windows 系统中安装 Snort	456
13.1.6 防火墙的脆弱性	410	14.5.1 软件准备工作	457
13.2 防火墙基础知识	411	14.5.2 安装 Web 服务器	457
13.2.1 防火墙的分类	411	14.5.3 为 Apache 安装 PHP 支持	459
13.2.2 包过滤防火墙	411	14.5.4 安装 MySQL 数据库	463
13.2.3 代理服务器防火墙	413	14.5.5 安装 ADODB、ACID 和 JpGraph	467
13.2.4 个人防火墙	414	14.5.6 安装包捕获库 WinPcap	469
13.2.5 分布式防火墙	414	14.5.7 安装 Snort IDS	470
13.3 防火墙体系结构	415	14.6 在 Linux 系统中安装 Snort	476
13.3.1 堡垒主机	415	14.6.1 软件准备工作	477
13.3.2 非军事区 (DMZ)	416	14.6.2 Linux 操作系统下安装源代码软件的基础知识	477
13.3.3 屏蔽路由器 (Screening Router)	416	14.6.3 安装 Apache、MySQL 和 PHP	480
13.3.4 体系结构	417	14.6.4 安装 LibPcap 库	482
13.3.5 防火墙的发展趋势	418	14.6.5 安装 pcre 软件包	482
13.3.6 防火墙的规则	418	14.6.6 安装 Snort 软件包	482
13.4 防火墙选型与产品简介	419	14.6.7 配置 ACID	485
13.4.1 防火墙选型原则	419	14.6.8 测试	485
13.4.2 防火墙产品介绍	420	14.7 Snort 配置文件 snort.conf	487
13.5 天网防火墙	421	14.7.1 定义变量	487
13.5.1 天网防火墙操作界面	422	14.7.2 配置动态装载库	489
13.5.2 天网防火墙开放端口应用	425	14.7.3 配置预处理器	489
13.5.3 应用自定义规则防止常见病毒	426	14.7.4 配置输出插件	489
13.5.4 打开 Web 和 FTP 服务	427	14.7.5 添加运行时配置指示符	490
13.5.5 在线升级功能	428	14.7.6 定制自己的规则集	490
13.6 瑞星防火墙	429		
13.6.1 安装瑞星防火墙	429		
13.6.2 瑞星防火墙操作界面	430		

14.8	入侵检测技术发展趋势	492	16.6.1	EFS 加密	549
14.8.1	入侵防御系统 IPS	492	16.6.2	万能加密器	550
14.8.2	硬件 IDS	492	16.6.3	PGP 工具软件	551
14.9	统一威胁管理 (UTM)	494	16.7	小结	554
14.9.1	UTM 采用的技术	495	第 17 章	SQL 注入攻防技术	555
14.9.2	UTM 发展趋势	496	17.1	SQL 注入基础	555
14.10	小结	496	17.1.1	SQL 注入概述	555
第 4 部分	常见攻防技术篇	497	17.1.2	SQL 注入的原理	556
第 15 章	网络封锁与代理突破	498	17.1.3	SQL 注入的危害与风险	556
15.1	网络封锁概述	498	17.2	ASP 与 PHP 环境下的 SQL 注入	556
15.2	代理服务器软件	498	17.2.1	SQL 注入数据库的判断	557
15.2.1	代理服务器软件 CCProxy	499	17.2.2	ASP+Access 注入剖析	557
15.2.2	Socks 代理软件	502	17.2.3	破解 MD5 加密	560
15.2.3	花刺代理软件	503	17.2.4	ASP+SQL Server 注入剖析	562
15.2.4	代理猎手软件	506	17.2.5	PHP+MySQL 注入剖析	564
15.2.5	在线代理服务器	508	17.3	常见 Web 注入	566
15.3	网络工具代理	509	17.3.1	HTML 注入	566
15.3.1	MSN 代理工具设置	509	17.3.2	JSP 和 ASPX 注入	568
15.3.2	Foxmail 代理工具设置	511	17.3.3	Cookie 注入	568
15.4	SSH 隧道介绍	512	17.4	SQL 注入的防护	570
15.4.1	SSH 隧道概述	513	17.4.1	ASP 防注入系统介绍	570
15.4.2	建立 SSH 隧道	513	17.4.2	PHP 防注入系统介绍	572
15.5	共享网络的使用	514	17.5	小结	573
15.5.1	拨号共享网络的使用	514	第 18 章	欺骗攻击技术与安全防范	574
15.5.2	路由器共享网络的使用	519	18.1	URL 欺骗	574
15.6	小结	522	18.1.1	URL 介绍	574
第 16 章	操作系统与文件加密技术	523	18.1.2	URL 欺骗原理与防范	575
16.1	操作系统密码的破解	523	18.2	Cookie 欺骗	576
16.1.1	密码破解软件 SAMInside	523	18.2.1	Cookie 欺骗介绍	576
16.1.2	密码破解软件 LC5	525	18.2.2	Cookie 欺骗原理与防范	576
16.1.3	清空系统管理员密码	528	18.3	DNS 劫持技术	578
16.2	利用系统权限寻找漏洞	528	18.3.1	DNS 介绍	578
16.2.1	利用替换系统文件的方法进行攻击	528	18.3.2	DNS 劫持技术	578
16.2.2	利用本地溢出进行攻击	530	18.3.3	DNS 劫持技术的防范	578
16.3	操作系统中的加密设置	531	18.4	ARP 欺骗	580
16.3.1	设置电源管理密码	531	18.4.1	ARP 概述	580
16.3.2	设置屏幕保护密码	532	18.4.2	ARP 协议原理	580
16.3.3	计算机锁定加密设置	533	18.4.3	ARP 欺骗原理	580
16.3.4	驱动器隐藏与显示	534	18.4.4	ARP 欺骗攻击的防护	581
16.3.5	给硬盘加写保护	535	18.5	小结	581
16.3.6	给光盘加写保护	536	第 19 章	后门技术与痕迹清理	583
16.4	系统登录加密	538	19.1	常见后门介绍	583
16.4.1	防止 Windows 匿名登录	538	19.1.1	账号后门	583
16.4.2	设置 Windows XP 安全登录	539	19.1.2	系统服务后门	588
16.5	常用软件与文件加密	540	19.1.3	漏洞后门	594
16.5.1	Word 文档加密	541	19.1.4	木马程序后门	596
16.5.2	Excel 文档加密	542	19.1.5	Winshell 服务器后门	602
16.5.3	文本加密器	543	19.2	RootKit 技术	604
16.5.4	文件夹的隐藏与加密	545	19.2.1	RootKit 技术概述	604
16.5.5	禁止修改文件的属性	547	19.2.2	NTRootKit 后门	604
16.5.6	压缩软件加密	548	19.2.3	RootKit 专用检测工具介绍	606
16.6	常用加密软件介绍	549	19.3	黑客之门	608
			19.3.1	黑客之门介绍	608



19.3.2	黑客之门的配置与安装	608	21.2	无线网络协议	668
19.3.3	连接黑客之门	609	21.2.1	IEEE 802.11a 协议	668
19.4	后门的防范	610	21.2.2	IEEE 802.11b 协议	668
19.4.1	Windows XP 风险后门	610	21.2.3	IEEE 802.11g 协议	671
19.4.2	操作系统内置后门的防范	612	21.2.4	IEEE 802.11i 协议	672
19.5	日志信息的清理	614	21.2.5	IEEE 802.11n 协议	674
19.5.1	手动清理本地计算机日志	614	21.2.6	蓝牙技术	676
19.5.2	清理远程计算机日志	616	21.3	无线网络保护机制	678
19.5.3	清理 FTP 和 WWW 日志	616	21.3.1	WEP 协议	678
19.6	使用日志工具清理日志	617	21.3.2	WPA 协议	681
19.6.1	使用 elsave 工具清理日志	617	21.3.3	WEP 升级到 WPA	684
19.6.2	使用 CleanlISLog 工具清理日志	618	21.4	无线网络安全工具	685
19.7	小结	619	21.4.1	NetStumbler	686
第 20 章	计算机取证	620	21.4.2	Kismet	691
20.1	电子证据	620	21.4.3	AiroPeek NX	694
20.1.1	电子证据的概念	620	21.4.4	AirSnort	712
20.1.2	电子证据的特点	622	21.4.5	WEPCrack	715
20.1.3	常见的电子证据	623	21.5	无线网络攻击与防护	718
20.2	计算机取证原则	625	21.5.1	无线网络攻击	718
20.3	获取证物	626	21.5.2	无线网络防护	720
20.3.1	获取证物的原则	626	21.6	小结	720
20.3.2	收集信息的策略	627	附录 A	Windows 的“运行”命令	721
20.4	使用 FinalData 软件	627	附录 B	常见程序进程详解	724
20.4.1	安装 FinalData	627	附录 C	网络管理命令大全	741
20.4.2	使用 FinalData	629	附录 D	病毒特征码和木马进程	759
20.5	使用 EasyRecovery 软件	631	附录 E	术语表	764
20.5.1	EasyRecovery 的功能	631			
20.5.2	使用 EasyRecovery	632			
20.6	使用盘载操作系统	637			
20.6.1	ERD Commander 盘载操作系统	637			
20.6.2	Windows PE 盘载操作系统	645			
20.7	硬盘分析	649			
20.7.1	硬盘性能参数	649			
20.7.2	硬盘接口结构	650			
20.7.3	PQMagic 与硬盘结构	651			
20.8	加密与解密	653			
20.8.1	密码体制	653			
20.8.2	算法的分类	654			
20.8.3	PDF 破解密码实战	654			
20.8.4	WinRAR 破解密码实战	656			
20.9	计算机取证常用工具	659			
20.9.1	EnCase: 软件取证工具	659			
20.9.2	Quick View Plus: 文件浏览器	660			
20.10	小结	663			
第 21 章	无线网络安全	664			
21.1	无线硬件设备	664			
21.1.1	访问点	665			
21.1.2	天线	665			
21.1.3	无线网卡	665			
21.1.4	手持设备	666			
21.1.5	无线设备的选购原则	666			



Part

第 1 部分 黑客基础篇

第 1 章 网络基础知识

第 2 章 黑客基础



第 1 章 网络基础知识

本章包括

- ◆ ISO 提出的 OSI 模型
- ◆ 网络的 TCP/IP 协议基础
- ◆ 域名系统、DHCP、NetBIOS 及 SMB 的简单知识
- ◆ 计算机端口的基础知识
- ◆ 计算机安全分析工具的简单介绍

进入 21 世纪之后，网络已经成为人们生活中不可或缺的获取信息的重要手段。截至 2009 年 6 月 30 日，根据 CNNIC（中国互联网络信息中心）的《第 24 次中国互联网络发展状况统计报告》，中国网民人数已经突破 3.38 亿。人们对网络的使用越来越频繁，网民平均每周上网 30 小时，达到了新的历史高度。对于办公室人员来说，每天上班的第一件事就是打开浏览器在新浪、搜狐、网易等主要网络新闻媒体上浏览当天的新闻，网络的力量可见一斑。

21 世纪的网络发展最主要的特点是计算机与通信的结合，这种方式对计算机的普及产生了深远的影响。依赖网线将多台分散的计算机互连起来使之成为共享模式即被称为计算机网络，而将这些计算机网络连接起来就形成了国际网络的模式，即互联网。

1.1 OSI 模型

OSI 模型是由国际标准化组织（ISO）提出的，它作为将各层上使用的协议国际化的第一步发展起来，这一模型被称为 ISO OSI 开放系统互联参考模型，因为这是关于如何把开放式系统连接起来的模型，故被简化称为 OSI 模型，如图 1.1 所示。OSI 模型有 7 层，其分层原理如下：

- ◆ 根据不同层次的抽象分层。
- ◆ 每层应当实现一个定义明确的功能。
- ◆ 每层功能的选择应该有助于制定网络协议的国际标准。
- ◆ 各层边界的选择应尽量减少跨接口的通信量。
- ◆ 层数应该足够多，以避免不同的功能混杂在同一层中，但也不能太多，否则体系结构会过于庞大。

图 1.1 演示了一个使用 OSI 模型时如何传输数据的例子。发送进程中有些数据需要发送给接收方，该发送方首先将数据交给应用层，应用层在此基础上增加一个应用报文头，再将结果交给表示层。表示层如法炮制，在要传输的报文首部也增加一个报文头。但是需要注意的是，表示层并不知道在要传输的数据中哪些是原始数据，哪些是应用报文头。这个过程重复进行直到数据抵达物理层，然后被实际传输到接收方。在接收方机制中，当信息向上传递时，各种报文头被一层一层地剥去，最后数据到达目的地。

下面将从物理层开始，依次讨论 OSI 参考模型中各层的功能和作用。