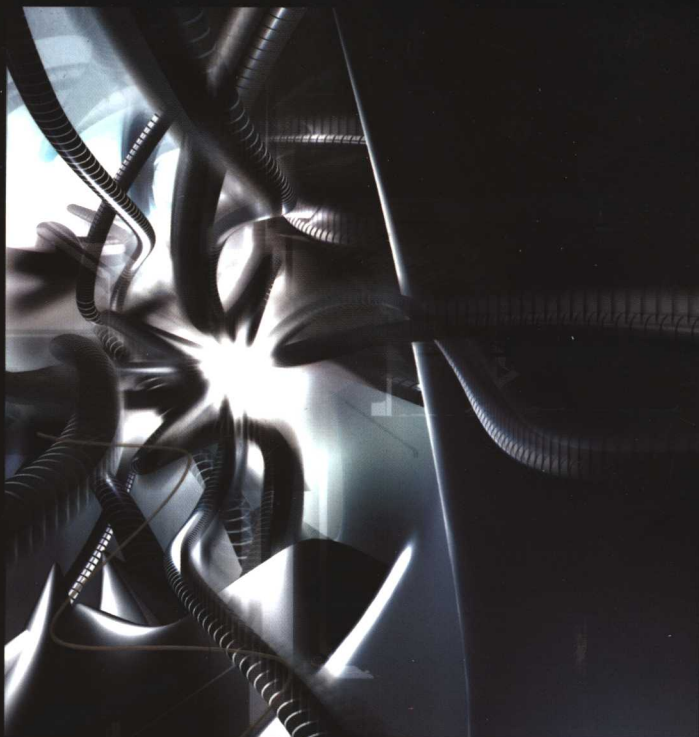


WANGLUO DE
GONGJI YU
FANGFAN
LILUN YU SHIJIAN

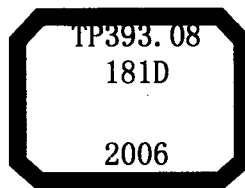


网络的攻击与防范 ——理论与实践

牛少彰 江为强 编著



北京邮电大学出版社
www.buptpress.com



网络的攻击与防范

——理论与实践

牛少彰 江为强 编著

北京邮电大学出版社

·北京·

内 容 简 介

本书系统论述了网络攻击与防范的原理与技术,并通过大量实践例程加深对内容的理解。本书主要针对 Windows 操作系统,从攻击者和防御者两个方面系统阐述了计算机和网络的入侵手段及相应防范措施。全书共分三篇,18 章,主要包括:网络攻击与防范概论、网络攻击篇和网络防范篇,每章都阐述了其原理、技术及实验,最后对网络安全防范的整体解决方案进行了详细分析。

全书理论与实践相结合,通过实践来理解攻防的具体过程。对所阐述的攻击手段都指出了其危害并提供了防范对策。本书可操作性强,介绍了大量典型的网络攻防工具及操作实例,让读者通过实际操作来掌握相应的原理及技术。

本书可以作为计算机、通信工程、信息安全及相关专业本科高年级学生、研究生的教材和实验或实训用书,也可供从事网络与网络安全工作的工程技术人员及对网络安全技术感兴趣的读者参考。

图书在版编目(CIP)数据

网络的攻击与防范:理论与实践/牛少彰,江为强编著. —北京:北京邮电大学出版社,2006

ISBN 7-5635-1342-6

I. 网... II. ①牛... ②江... 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(2006)第 129496 号

书 名:网络的攻击与防范——理论与实践

编 著:牛少彰 江为强

责任编辑:王晓丹

出版发行:北京邮电大学出版社

社 址:北京市海淀区西土城路 10 号(邮编:100876)

北方营销中心:电话:010-62282185 传真:010-62283578

南方营销中心:电话:010-62282902 传真:010-62282735

E-mail: publish@bupt.edu.cn

经 销:各地新华书店

印 刷:北京忠信诚胶印厂

开 本:787 mm × 960 mm 1/16

印 张:19

字 数:413 千字

印 数:1—3 000 册

版 次:2006 年 12 月第 1 版 2006 年 12 月第 1 次印刷

ISBN 7-5635-1342-6/TP · 259

定 价:35.00 元(附光盘)

· 如有印装质量问题,请与北京邮电大学出版社营销中心联系 ·

网络安全是一门综合学科,包括了技术、管理、人才、法律法规诸多方面。从技术的角度重点包含了对攻击手段的分析及其相应的防范措施,安全管理与法律法规是网络安全技术得以实现的有力保障,人才的培养是它的基石。在当前网络安全形势十分严峻的情况下,网络安全人才的缺口越来越大,许多高校都开设了信息安全专业或信息安全课程,相关教材也应运而生。编者深感在信息安全教育中,实践动手能力的培养对其掌握信息安全原理技术起着重要的作用,同时又能快速获得工作中的实际操作经验。目前,研究网络攻击与防范技术的著作很多,但同时对其实践操作进行详细分析的著作不多见。鉴于此,作者根据从事网络安全方面的实验室建设和实训教学的经验,编写了这部理论与实践操作紧密结合的著作,目的是让读者在掌握网络攻击与安全理论的同时,能够通过实际动手操作来加深对攻防原理以及网络攻击的危害和网络防御的重要性的理解。

本书内容全面,既有网络攻防的理论知识,又有其实用技术和实践,并包括网络信息安全方面的一些最新成果。全书共分三篇,18章。第一篇为网络攻击与防范概论,共3章,主要介绍了网络攻击与防范的历史、现状与发展趋势;网络攻击与防范的方法;网络攻击与防范模型;网络安全策略。第二篇为网络攻击篇,共7章,按照网络攻击的基本过程,详细介绍了网络攻击的各个阶段以及所使用的手段,并对网络攻击的实施及其原理进行了分析,对所讨论的攻击手段都指出了其危害并提供了防范对策。第三篇为网络防范篇,共8章,主要针对第二篇所阐述的攻击手段,介绍了相应的网络防御理论及其在实践中典型的安全技术和产品,包括一些新的安全技术(如蜜罐与蜜网技术等),最后对前述的相关网络安全技术进行归纳,给出了网络安全整体解决方案。在本书后2篇中,每章的后面都有实验或技术解决方案。为了帮助读者更好地理解网络攻击与防范的原理,书中每章后面列出了部分实践的主要步骤,随书所附的光盘中给出了实践的详细的资料及更多的操作实例。

本书最大的特点是理论与实践相结合,通过实践来理解攻防的具体过程。本书

可操作性强,介绍了大量典型的网络攻防工具及操作实例,让读者通过实际操作来掌握相应的原理及技术。

本书可以作为计算机、通信工程、信息安全及相关专业本科高年级学生、研究生的教材和实验用书,特别适合用于信息安全相关专业的实训教学,以及网络攻防的培训教材。本书也可供从事网络与网络安全工作的工程技术人员及对网络安全技术感兴趣的读者参考。

在本书的编写过程中,北京邮电大学的本科毕业生冯浩、冯成晶、张岳、钱进、韦成府、郑直、单艮俊、梁蒙奇、齐麟等为本书收集和整理了大量的材料。研究生丁昆写了部分实验并对所有的实验进行了整理。研究生张丽、化宇鹏、张玮、刘博、向楠、张同庆、卢娜等对书稿进行了大量的校对工作。北京电信教育培训中心的史凤婷老师在实验的组织中做了大量的工作。刘洋、梁凯、王子戈和唐志雄等提供了部分实验内容。本书在编写过程中得到了北京邮电大学信息安全中心和北京电信教育培训中心的大力支持和帮助。在此一并表示衷心感谢

由于本书涉及的内容较多,参考了大量的论文、书籍和网络资源,书后列出了较为详尽的参考文献,但由于参加本书内容收集和整理的人员众多,难免挂一漏万,如有遗漏,敬请谅解。书中的实验部分参考和引用了网络资源,所附软件只是帮助读者学习和理解相应的理论与技术,其著作权属于原作者,请勿用于其他目的,如实际工作中需要使用,请向原作者购买。

限于编者水平有限,书中难免有疏漏和错误之处,恳请读者批评指正。

编者

2006年8月

第一篇 网络攻击与防范概论

第1章 网络攻击与防范的历史、现状与发展趋势	(3)
1.1 网络与黑客的历史	(3)
1.1.1 计算机网络的历史	(3)
1.1.2 黑客的历史	(5)
1.2 网络攻击技术的回顾与演变	(8)
1.3 网络安全技术的现状与发展	(10)
第2章 网络攻击与防范的方法	(13)
2.1 网络攻击的目的	(13)
2.2 网络攻击的方法分类	(15)
2.3 网络安全策略	(17)
2.4 网络防范的方法分类	(18)
2.5 网络攻击与防范的博弈	(19)
第3章 网络攻击与防范模型	(22)
3.1 网络攻击的整体模型描述	(22)
3.2 网络防范的原理及模型	(23)
3.3 网络攻防实训平台建设的总体方案	(26)

第二篇 网络攻击篇

第4章 获取目标系统信息	(31)
4.1 获取攻击目标主机的系统信息	(31)
4.2 获取网络信息的基本工具	(32)
4.2.1 通过常见的网络命令获取信息	(32)
4.2.2 通过专用的网络命令获取信息	(36)

4.3	信息踩点	(42)
4.3.1	踩点概述	(42)
4.3.2	踩点常用的工具和方法	(45)
4.3.3	图形界面的踩点工具	(47)
4.4	信息查点	(48)
4.4.1	Windows NT/2000 查点	(48)
4.4.2	Unix/Linux 查点	(54)
4.5	实验：端口扫描	(57)
第5章	目标主机的系统弱点挖掘技术	(58)
5.1	系统弱点可能造成的危害	(58)
5.2	系统弱点的分类	(59)
5.2.1	设计上的缺陷	(60)
5.2.2	操作系统的弱点	(60)
5.2.3	软件的错误、缺陷和漏洞	(60)
5.2.4	数据库的弱点	(61)
5.2.5	网络安全产品的弱点	(61)
5.2.6	用户的管理的疏忽	(62)
5.3	系统的主要漏洞分类	(63)
5.3.1	根据漏洞被攻击者利用的方式分类	(64)
5.3.2	根据漏洞所指的目标分类	(64)
5.3.3	根据漏洞导致的直接威胁分类	(64)
5.3.4	根据漏洞对系统安全性造成的损害分类	(65)
5.4	几种常见漏洞的分析	(65)
5.5	漏洞库及其使用	(67)
5.6	弱点挖掘的过程与方法	(68)
5.7	获取系统弱点的工具	(69)
5.8	实验：漏洞扫描	(71)
第6章	网络攻击身份欺骗	(73)
6.1	IP 欺骗攻击	(73)
6.1.1	IP 欺骗的原理	(74)
6.1.2	IP 欺骗过程	(76)
6.1.3	IP 地址盗用的常用方法	(77)
6.1.4	IP 欺骗的防范对策	(78)
6.2	与 IP 协议相关的欺骗手段	(79)

6.2.1	ARP 欺骗及防范	(79)
6.2.2	基于 ICMP 的路由欺骗	(79)
6.2.3	RIP 路由欺骗	(80)
6.2.4	DNS 欺骗	(81)
6.3	其他身份欺骗手段	(82)
6.4	实验: ARP 欺骗	(82)
第 7 章	网络攻击行为隐藏	(84)
7.1	文件隐藏	(84)
7.1.1	修改文件名称和属性	(84)
7.1.2	使用信息隐藏技术	(85)
7.2	进程活动隐藏	(86)
7.2.1	远程线程插入技术	(86)
7.2.2	动态链接库插入技术	(86)
7.2.3	挂钩 API	(87)
7.3	网络连接隐藏	(88)
7.4	网络隐藏通道	(88)
7.4.1	基于 TCP/IP 协议构建隐蔽通道	(89)
7.4.2	基于 HTTP 协议构建隐蔽通道	(91)
7.4.3	安全性考虑	(92)
7.5	实验: 文件隐藏	(93)
第 8 章	权限获取及提升	(94)
8.1	通过网络监听获取权限	(94)
8.1.1	网络监听的原理	(94)
8.1.2	网络监听获取权限	(95)
8.1.3	网络监听工具	(96)
8.2	通过网络漏洞获取权限	(97)
8.3	基于网络账号口令破解获取权限	(98)
8.3.1	操作系统的口令管理	(98)
8.3.2	破解口令方法	(98)
8.3.3	口令破解工具	(99)
8.4	通过网络欺骗获取权限	(100)
8.4.1	社会工程	(100)
8.4.2	网络钓鱼	(100)
8.5	基于 TCP/IP 会话劫持获取权限	(102)

8.5.1	TCP 运行机制	(102)
8.5.2	IP 劫持攻击原理	(104)
8.5.3	TCP 应答风暴	(105)
8.5.4	权限获取	(106)
8.5.5	进行会话劫持的工具	(106)
8.6	实验：口令破解	(106)
第9章	利用病毒和木马进行网络攻击	(108)
9.1	计算机病毒	(108)
9.1.1	计算机病毒的基本结构	(108)
9.1.2	计算机病毒的分类	(109)
9.1.3	计算机病毒的工作原理	(110)
9.1.4	计算机病毒的传播途径及危害	(111)
9.2	蠕虫病毒	(111)
9.2.1	蠕虫病毒的发展与现状	(111)
9.2.2	几个典型蠕虫病毒	(113)
9.2.3	网络蠕虫的扫描策略	(115)
9.3	木马的原理分析	(117)
9.3.1	木马的结构和原理	(118)
9.3.2	木马的分类	(120)
9.3.3	木马的功能	(121)
9.3.4	木马的攻击原理	(122)
9.3.5	木马与病毒的融合攻击机制	(123)
9.4	反病毒技术	(124)
9.4.1	检测计算机病毒的基本方法	(124)
9.4.2	反蠕虫病毒技术	(126)
9.4.3	木马的防治	(127)
9.5	实验：利用木马进行攻击	(128)
第10章	网络攻击实施和技术分析	(129)
10.1	网络嗅探技术	(129)
10.1.1	网络嗅探原理	(129)
10.1.2	嗅探造成的危害	(130)
10.1.3	常见的嗅探器	(131)
10.1.4	嗅探对策	(132)
10.2	缓冲区溢出攻击技术原理分析	(133)

10.2.1	堆栈的结构和组成	(133)
10.2.2	缓冲区溢出实例分析	(134)
10.2.3	缓冲区漏洞的利用	(135)
10.3	拒绝服务 (DoS) 攻击技术原理分析	(136)
10.3.1	DoS 的基本原理	(136)
10.3.2	攻击模式与种类	(136)
10.3.3	DDoS 攻击的最新发展	(139)
10.4	攻击后期行为归纳	(141)
10.5	实验: 网络攻击综合实施	(141)

第三篇 网络防范篇

第11章	安全扫描技术的原理与应用	(145)
11.1	安全扫描技术概述	(145)
11.1.1	发展历史	(146)
11.1.2	功能	(147)
11.1.3	分类	(147)
11.2	端口扫描和漏洞扫描	(148)
11.2.1	端口扫描技术及原理	(148)
11.2.2	漏洞扫描技术及原理	(150)
11.3	安全扫描器的原理、结构及设计	(151)
11.3.1	安全扫描器的原理	(151)
11.3.2	安全扫描器的结构	(151)
11.3.3	安全扫描器的设计	(152)
11.4	安全扫描技术的应用	(154)
11.4.1	安全扫描器产品	(154)
11.4.2	安全扫描器的选择	(155)
11.4.3	安全扫描技术的发展趋势	(156)
11.5	实验: 综合扫描及安全性评估	(156)
第12章	操作系统安全防范	(160)
12.1	操作系统的安全机制	(160)
12.1.1	安全模型	(161)
12.1.2	系统的认证	(162)
12.1.3	访问控制	(163)
12.1.4	远程访问	(166)

12.1.5 其他方面	(166)
12.2 Windows 2000/2003 的安全特性	(167)
12.2.1 Windows 2000 的安全特性	(167)
12.2.2 Windows 2003 的安全新特性	(168)
12.2.3 Windows 2003 系统的安全防范	(169)
12.3 实验: Unix/Linux 的安全性	(173)
第13章 密码及认证技术	(176)
13.1 加密技术原理及典型算法	(176)
13.1.1 对称密钥密码	(177)
13.1.2 公开密钥加密	(179)
13.1.3 电子信封技术	(180)
13.2 Hash 函数原理和典型算法	(181)
13.2.1 Hash 函数概述	(181)
13.2.2 Hash 算法的分类	(181)
13.3 数字签名	(182)
13.3.1 数字签名的实现方法	(182)
13.3.2 数字签名的特性和功能	(183)
13.3.3 常用数字签名体制	(183)
13.4 身份认证技术	(184)
13.4.1 身份认证系统的分类	(185)
13.4.2 基于口令的认证技术	(186)
13.4.3 双因子身份认证技术	(186)
13.4.4 生物特征认证技术	(187)
13.5 PKI 与 PMI 认证技术	(188)
13.5.1 PKI 原理	(188)
13.5.2 数字证书和证书撤销列表	(189)
13.5.3 PKI 系统的功能	(190)
13.5.4 PKI 系统的组成	(192)
13.5.5 PKI 相关标准	(193)
13.5.6 常用信任模型	(194)
13.5.7 基于 PKI 的服务	(195)
13.5.8 PKI 的应用	(196)
13.5.9 PKI 与 PMI 的关系	(196)
13.5.10 属性证书和结构模型	(197)

13.6 实验：电子邮件的加密和签名	(199)
第14章 防火墙的技术原理与应用	(202)
14.1 防火墙技术概论	(202)
14.1.1 防火墙的作用	(203)
14.1.2 防火墙的优缺点	(204)
14.2 防火墙的分类	(205)
14.2.1 按实现技术分类	(205)
14.2.2 按体系结构分类	(206)
14.3 防火墙技术	(206)
14.3.1 包过滤技术	(206)
14.3.2 代理技术	(207)
14.3.3 网络地址翻译技术	(209)
14.3.4 基于防火墙的 VPN 技术	(210)
14.3.5 其他防火墙技术	(212)
14.4 防火墙的体系结构	(213)
14.4.1 双宿/多宿主机模式	(213)
14.4.2 屏蔽主机模式	(214)
14.4.3 屏蔽子网模式	(215)
14.4.4 混合模式	(216)
14.5 防火墙的产品	(217)
14.5.1 国内主流防火墙	(218)
14.5.2 国外主流防火墙	(219)
14.6 实验：包过滤防火墙	(219)
第15章 入侵检测技术的原理与应用	(221)
15.1 入侵检测概述	(221)
15.1.1 IDS 的产生	(221)
15.1.2 IDS 功能与模型	(223)
15.2 IDS 的基本原理	(225)
15.2.1 信息源	(225)
15.2.2 IDS 类型	(229)
15.2.3 IDS 基本技术	(231)
15.3 实验：入侵检测系统 Snort	(235)
第16章 蜜罐与蜜网技术	(238)
16.1 概述	(238)

16.2	蜜罐技术	(239)
16.2.1	蜜罐的发展历程	(239)
16.2.2	蜜罐的分类	(240)
16.2.3	蜜罐的优缺点	(240)
16.3	蜜网工程	(241)
16.3.1	蜜网项目组	(241)
16.3.2	第二代蜜网方案	(242)
16.4	常见的网络诱骗工具及产品	(244)
16.4.1	DTK 欺骗工具包	(244)
16.4.2	Honeyd	(245)
16.4.3	Honeynet	(246)
16.5	实验: Honeyd 的安装和配置	(247)
第17章	数据备份与灾难恢复技术	(250)
17.1	数据备份技术分析	(250)
17.1.1	数据备份的定义与作用	(250)
17.1.2	数据备份的类型	(251)
17.1.3	数据备份系统的基本构成	(252)
17.1.4	存储介质与硬件设备	(253)
17.1.5	备份管理软件和工具	(253)
17.1.6	数据备份策略及其规划	(254)
17.2	灾难恢复技术分析	(256)
17.2.1	灾难恢复的定义与作用	(256)
17.2.2	灾难恢复策略及规划	(257)
17.2.3	灾前准备工作	(259)
17.2.4	灾难恢复计划	(260)
17.2.5	灾难恢复计划的测试和维护	(260)
17.2.6	常用灾难恢复工具介绍	(261)
17.3	数据库系统的数据备份与灾难恢复	(262)
17.3.1	MS SQL Server 数据库	(262)
17.3.2	Oracle 数据库的备份与恢复	(262)
17.3.3	Informix 数据库	(263)
17.4	网络数据备份与灾难恢复	(263)
17.4.1	网络数据备份的意义与目标	(264)
17.4.2	网络数据备份的实现	(265)

17.4.3 远程数据备份	(266)
17.5 实验：备份与恢复	(269)
第18章 网络安全综合防范平台	(271)
18.1 统一认证、授权和审计平台	(271)
18.1.1 AAA 平台技术简介	(272)
18.1.2 AAA 平台的结构模型	(272)
18.1.3 AAA 平台的组成和功能	(274)
18.1.4 AAA 平台方案的特点和技术优势	(276)
18.2 网络安全防御系统解决方案	(277)
18.2.1 广泛安全产品的联动	(277)
18.2.2 网络安全的整体解决方案	(279)
18.3 内网安全	(282)
18.3.1 移动存储介质管理	(283)
18.3.2 网络行为监控	(283)
18.3.3 内网安全整体解决方案	(284)
附录 实验内容	(285)
参考文献	(287)

第一篇

网络攻击与防范概论

网络攻击与防范

第 1 章

网络攻击与防范的历史、现状与发展趋势

随着由通信与计算机相结合而诞生的计算机互联网络全面进入千家万户,使得信息共享应用日益广泛与深入。世界范围的信息革命激发了人类历史上最活跃的生产力,人类开始从主要依赖物质和能源的社会步入物质、能源和信息三位一体的社会,信息成为人类社会必须的重要资源。但同时网络的安全问题也日渐突出,而且情况也越来越复杂。从大的方面来说,网络信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域。从小的方面来说,网络信息安全是人们能否保护自己个人隐私的关键。网络信息安全是社会稳定安全的必要前提条件。人们的生活已经无法脱离对网络与计算机的依赖,但是网络是开放的、共享的,因此,网络与计算机系统安全就成为科学研究的一个重大课题。而对网络与计算机安全的研究不能仅限于防御手段,还要从非法获取目标主机的系统信息、非法挖掘系统弱点等技术进行研究。正所谓对症下药,只有了解了攻击者的手法,才能更好地采取措施,来保护网络与计算机系统的正常运行。

1.1 网络与黑客的历史

1.1.1 计算机网络的历史

计算机网络的发展历史不长,但发展速度很快。计算机网络是计算机技术和通信技术紧密结合的产物,它涉及到通信与计算机两个领域。