

信息安全系列教材

网络攻防技术教程

——从原理到实践

杜晔 张大伟 范艳芳 编著



WUHAN UNIVERSITY PRESS

武汉大学出版社

编：刘一、著：袁祥、张大为、张世、张英、张勇、张磊

信息安全系列教材

信息安全系列教材

网络攻防技术教程

——从原理到实践

杜晔 张大伟 范艳芳 编著



WUHAN UNIVERSITY PRESS

武汉大学出版社

图书在版编目(CIP)数据

网络攻防技术教程:从原理到实践/杜晔,张大伟,范艳芳编著. —武汉:武汉大学出版社,2008.6

信息安全系列教材

ISBN 978-7-307-06232-0

I. 网… II. ①杜… ②张… ③范… III. 计算机网络—安全技术—高等学校—教材 IV. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 063872 号

责任编辑:黄金文 夏炽元 责任校对:程小宜 版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.com.cn)

印刷:湖北金海印务公司

开本:787×1092 1/16 印张:23 字数:551千字

版次:2008年6月第1版 2008年6月第1次印刷

ISBN 978-7-307-06232-0/TP·294 定价:36.00元

版权所有,不得翻印;凡购买我社的图书,如有缺页、倒页、脱页等质量问题,请与当地图书销售部门联系调换。



内 容 简 介

本书详细地介绍了计算机及网络系统面临的威胁与黑客攻击方法，详尽、具体地披露了攻击技术的真相以及防范策略和技术实现措施。本书理论联系实际。在技术讨论之后，都会有一套详细的试验方案对相关技术进行验证。

全书共分4个部分，内容由浅入深，按照黑客攻击通常采用的步骤进行组织，分技术专题进行讨论。第一部分介绍了网络攻防基础知识，以使读者建立起网络攻防的基本概念。第二部分介绍信息收集技术，即攻击前的“踩点”，包括网络嗅探和漏洞扫描技术。第三部分是本书的核心内容，介绍了有代表性的网络攻击技术以及有针对性的防御技术。第四部分着重于防御技术，讨论了PKI网络安全协议和两种得到广泛应用的安全设备，即防火墙和入侵检测系统。

本书可作为信息安全、计算机、通信等专业本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相关技术人员参考和阅读。

前言

随着计算机和通信技术的飞速发展，网络应用已日益普及，成为人们生活中不可缺少的一部分。截止 2007 年 12 月，我国网民总人数已达 2 亿人。电子政务、电子商务得到了进一步推广，有大约 22.1% 的网民进行网络购物或者商业运作，人数规模达到 4 640 万人。但在网络服务为我们提供了极大便利的同时，对于信息系统的非法入侵和破坏活动正以惊人的速度在全世界蔓延，同时带来巨大的经济损失和安全威胁。据统计，每年全球因安全问题导致的损失已经可以用万亿美元的数量级来计算。在我国，“震荡波”系列蠕虫曾造成有超过 138 万个 IP 地址的主机被病毒感染的记录，而 2007 年也有约 4.5 万个 IP 地址的主机被植入木马程序。

面对如此不容乐观的网络环境和严峻的挑战，无论是网络管理人员还是个人都应掌握基本的网络攻防技术，做好自身防范，增强抵御黑客攻击的能力。

“知己知彼，百战不殆”。要想防范，首先要知道黑客如何攻击。书中总结了目前网络攻击的现状与发展趋势，详细地介绍了计算机及网络系统面临的威胁和黑客攻击方法，详尽、具体地披露了攻击技术的真相，以及防范策略和技术实现措施。作者采用尽可能简单的方式向读者讲解技术原理，希望读者在读完这本书后，能对网络攻防技术有进一步的了解。

本书的特点在于理论联系实际，在技术讨论之后，都会有一套详细的试验方案对相关技术进行验证。通过具体的试验操作，帮助读者实际掌握和理解各个知识点的精髓。考虑到不同单位千差万别的试验条件，我们的试验内容大部分基于很容易搭建的 Windows 和 Linux 操作系统，充分降低了试验开设过程的成本。

本书共分 4 个部分，内容由浅入深，按照黑客攻击通常采用的步骤进行组织，分技术专题进行讨论。

第一部分介绍了网络攻防基础知识，以使读者建立起网络攻防的基本概念。第二部分介绍信息收集技术，即黑客攻击前的“踩点”，包括网络嗅探和漏洞扫描技术。第三部分是本书的核心内容，介绍了有代表性的网络攻击技术以及有针对性的防御技术。第四部分着重于防御技术，讨论了 PKI 网络安全协议和两种得到广泛应用的安全设备，即防火墙和入侵检测系统。

对于每个技术专题，都详细制定了实验方案，并对实验的每个步骤进行了演练，使读者学习后可以参照教程进行实际操作，通过实践深入理解技术原理。本书可作为信息安全、计算机、通信等专业本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相关技术人员参考和阅读。

本书编写的目的是帮助读者了解网络攻防技术与内幕，建立安全意识，增强对于黑客攻击的防范能力，绝不是为怀有不良动机的人提供支持，也不承担因为技术被滥用而产生的连带责任。

在本书编写的过程中，参考了互联网上公布的研究论文和相关资料，主要源于各大学、

科研机构、安全网站、安全公司以及一些研究网络安全问题的个人，在此向他们对于推动安全技术的发展表示感谢。由于资料较多，无法一一注明出处。写作过程中所参考的这些资料，其原文版权属于原作者，特此声明。

本书第1、第2章由范艳芳编写，第9章由张大伟编写，其余各章由杜晔编写并完成全书统稿。北京交通大学信息安全体系结构中心的李洁原、李程、刘博、李磊、何帆、李明、郝悦等参与了编写工作。本书的编写得到了北京交通大学何永忠、袁中兰、黎妹红，哈尔滨工程大学王桐、郭方方，北京理工大学冯远等多位老师的帮助，在此对他们表示衷心的感谢。

由于作者水平有限，书中难免会出现疏漏，加之网络攻防技术纵深宽广，在内容取舍与编排方面，难免有考虑不周之处，诚请广大读者批评指正。

杜 晔

2008年3月

目 录

第一部分 网络攻击基础知识

第 1 章 黑客与安全事件	3
1.1 网络安全事件	3
1.2 黑客与入侵者	5
1.2.1 黑客简史	5
1.2.2 黑客的定义	6
1.2.3 入侵者	7
1.3 黑客攻击的目标与步骤	7
1.3.1 黑客攻击的目标	7
1.3.2 黑客攻击的步骤	7
1.4 黑客攻击发展趋势	8
1.5 社会工程学	10
第 2 章 网络攻防相关概念	11
2.1 OSI 安全体系结构	11
2.1.1 五类安全服务	12
2.1.2 安全服务提供的安全机制	13
2.1.3 安全服务和特定安全机制的关系	14
2.1.4 OSI 安全体系的管理	16
2.2 网络脆弱性分析	17
2.2.1 网络安全威胁	17
2.2.2 网络安全风险	17
2.2.3 网络脆弱性	18
2.3 网络攻击的分类	19
2.4 主动攻击与被动攻击	20
2.4.1 主动攻击	20
2.4.2 被动攻击	20
2.5 网络安全模型	20
2.5.1 P ² DR 模型	20
2.5.2 PDR ² 模型	22

第二部分 信息收集技术

第3章 网络嗅探	27
3.1 嗅探器概述.....	27
3.1.1 嗅探器简介.....	27
3.1.2 嗅探器的工作原理.....	28
3.2 交换式网络上的嗅探.....	29
3.3 简易网络嗅探器的实现.....	31
3.4 嗅探器的检测与防范.....	32
3.5 常用嗅探工具.....	35
3.5.1 Tcpdump.....	35
3.5.2 Libpcap.....	35
3.5.3 Sniffer Pro.....	36
3.5.4 WireShark.....	36
实验部分.....	36
实验 3-1 WireShark 嗅探器的使用.....	36
实验 3-2 Sniffer Pro 嗅探器的使用.....	51
实验 3-3 Telnet 协议密码嗅探.....	53
第4章 漏洞扫描	57
4.1 系统漏洞.....	57
4.1.1 漏洞的概念.....	57
4.1.2 已知系统漏洞.....	57
4.2 漏洞扫描相关知识.....	58
4.2.1 漏洞扫描基本原理.....	58
4.2.2 漏洞扫描的分类.....	59
4.2.3 漏洞扫描器的组成.....	59
4.3 扫描策略与防范.....	60
4.3.1 端口扫描与防范.....	60
4.3.2 漏洞扫描与防范.....	66
4.4 常用扫描工具.....	70
实验部分.....	72
实验 4-1 Ping 命令的使用.....	72
实验 4-2 Superscan 工具的使用.....	75
实验 4-3 Nmap 工具的使用.....	79
实验 4-4 综合扫描工具——流光 Fluxay 的使用.....	83

第三部分 网络攻击技术

第5章 拒绝服务攻击	95
5.1 拒绝服务攻击概述.....	95

5.1.1	什么是拒绝服务攻击	95
5.1.2	拒绝服务攻击原理	95
5.1.3	拒绝服务攻击时的现象	96
5.2	分布式拒绝服务攻击	96
5.2.1	分布式拒绝服务攻击背景	96
5.2.2	分布式拒绝服务攻击的步骤	97
5.2.3	分布式拒绝服务攻击分类	98
5.3	典型攻击与防范	100
5.4	DoS/DDoS 攻击工具分析	102
	实验部分	103
实验 5-1	Misoskian's Packet Builder 攻击工具使用	103
实验 5-2	阿拉丁 UDP 洪水攻击工具使用	105
实验 5-3	独裁者 Autocrat 攻击工具使用	107
第 6 章	缓冲区溢出攻击	114
6.1	缓冲区溢出攻击概述	114
6.1.1	什么是缓冲区溢出	114
6.1.2	缓冲区溢出攻击历史	114
6.1.3	缓冲区溢出原理	115
6.2	缓冲区溢出攻击分类	117
6.2.1	基于栈的缓冲区溢出	117
6.2.2	基于堆的缓冲区溢出	119
6.2.3	基于 BSS 段的缓冲区溢出	123
6.3	缓冲区溢出攻击的防范	124
6.3.1	编写正确的代码和代码审计	124
6.3.2	非执行的缓冲区	125
6.3.3	改进 C 语言函数库	126
6.3.4	数组边界检查	126
6.3.5	程序指针完整性检查	127
	实验部分	128
实验 6-1	利用 IEmail 溢出创建隐秘登录账号	128
实验 6-2	MS-06030 本地权限提升	136
实验 6-3	IIS5 溢出工具使用	139
实验 6-4	ida 漏洞入侵	144
第 7 章	Web 应用安全攻击	146
7.1	Web 应用安全概述	146
7.1.1	Web 应用安全简介	146
7.1.2	Web 应用相关技术	147
7.1.3	Web 应用十大安全漏洞	148

7.2	SQL 注入攻击	150
7.2.1	SQL 注入的定义	150
7.2.2	SQL 注入的原理	151
7.2.3	SQL 注入的实现过程	153
7.2.4	SQL 注入的检测与防范	154
7.2.5	SQL 注入提升权限攻击实例	154
7.3	跨站脚本攻击	158
7.3.1	跨站脚本攻击的定义	158
7.3.2	跨站脚本攻击的原理	159
7.3.3	跨站脚本攻击的实现过程	160
7.3.4	跨站脚本攻击的检测与防范	161
7.3.5	跨站脚本攻击实例分析	163
7.4	欺骗攻击	164
7.4.1	ARP 欺骗网页劫持	164
7.4.2	DNS 欺骗网站重定向	169
7.4.3	网络钓鱼	171
	实验部分	172
	实验 7-1 “啊 D”SQL 注入植入恶意程序	172
	实验 7-2 WIS 和 WED SQL 注入工具获取管理员权限	178
	实验 7-3 WinArpAttacker 工具的使用	182
	实验 7-4 IIS 中隐藏页面目录攻击	187
第 8 章	病毒、蠕虫与木马	191
8.1	计算机病毒	191
8.1.1	计算机病毒的概念	191
8.1.2	计算机病毒的分类	191
8.1.3	计算机病毒的特点	193
8.1.4	计算机病毒的生命周期	194
8.1.5	典型病毒及其解决方案	194
8.2	蠕虫	197
8.2.1	蠕虫的概念	197
8.2.2	蠕虫的传播过程	197
8.2.3	与计算机病毒的区别	198
8.2.4	典型蠕虫与解决方案	199
8.3	木马	201
8.3.1	木马的概念	201
8.3.2	木马的分类	201
8.3.3	与计算机病毒的区别	203
8.3.4	木马植入手段	204
8.3.5	木马攻击原理	204

8.3.6 木马的查杀	205
8.3.7 典型木马与解决方案	207
实验部分	209
实验 8-1 制作简单 word 宏病毒	209
实验 8-2 制作 CHM 木马	211
实验 8-3 利用 IPC 漏洞安装远程控制	214
实验 8-4 灰鸽子远程控制的配置	219

第四部分 防御技术

第 9 章 PKI 网络安全协议	227
9.1 公钥基础设施 PKI 概述	227
9.1.1 PKI 简介	227
9.1.2 PKI 的组成	228
9.1.3 PKI 的功能	229
9.2 公钥基础设施 PKI 的应用	230
9.2.1 基于 PKI 的服务	230
9.2.2 SSL 协议	231
9.2.3 虚拟专用网 VPN	233
9.2.4 安全电子邮件	234
9.2.5 Web 安全	235
9.3 USB Key 在 PKI 中的应用	235
9.3.1 USB Key 简介	235
9.3.2 USB Key 的特点	236
9.3.3 Windows CSP 简介	237
实验部分	237
实验 9-1 Windows Server 中 CA 的配置	237
实验 9-2 配置 SSL 安全站点	251
实验 9-3 使用 USB Key 申请客户证书	264
实验 9-4 客户端使用 USB Key 登录 SSL 站点	271
实验 9-5 使用 USB Key 签名和加密电子邮件	271
第 10 章 防火墙	280
10.1 防火墙技术概述	280
10.1.1 防火墙的概念	280
10.1.2 防火墙的发展过程	281
10.1.3 防火墙基本安全策略	282
10.1.4 防火墙的优点	282
10.2 防火墙系统的分类	283
10.2.1 按结构分类	283
10.2.2 按技术分类	286

10.3	防火墙关键技术	288
10.3.1	数据包过滤	288
10.3.2	代理技术	289
10.3.3	网络地址转换	290
10.3.4	身份认证技术	290
10.3.5	安全审计和报警	290
10.3.6	流量统计和控制	291
10.4	防火墙的发展方向	291
实验部分		292
实验 10-1	天网防火墙的配置	292
实验 10-2	添加天网防火墙规则, 并验证效果	303
第 11 章	入侵检测系统	306
11.1	入侵检测技术概述	306
11.1.1	入侵检测的概念	306
11.1.2	入侵检测的发展史	306
11.1.3	通用入侵检测系统结构	308
11.1.4	入侵检测系统标准化	309
11.2	入侵检测系统分类	311
11.2.1	数据来源	311
11.2.2	分析方法	313
11.2.3	时效性	314
11.2.4	分布性	314
11.3	入侵检测系统的分析技术	314
11.3.1	异常入侵检测技术	314
11.3.2	误用入侵检测技术	318
11.3.3	异常检测与误用检测评价	320
11.4	典型入侵检测系统	320
11.4.1	Snort 系统	321
11.4.2	DIDS 系统	322
11.4.3	AAFID 系统	323
11.4.4	EMERALD 系统	323
11.4.5	NetSTAT 系统	324
11.5	入侵检测系统的发展方向	325
实验部分		326
实验 11-1	Snort 系统的安装与配置	326
实验 11-2	添加 Snort 规则, 并验证检测效果	333
附录一	Sniffer 程序源代码	345

附录二 常用跨站脚本攻击方法..... 347

参考文献..... 351

第一部分 | 网络攻击基础知识



第1章 黑客与安全事件

1.1 网络安全事件

随着信息技术的发展,网络已经渗入到我们生活的方方面面,成为社会结构的一个基本组成部分。目前,网络被应用于工商业的各个方面,包括电子银行、电子商务、现代化的企业管理、信息服务业等领域。可以毫不夸张地说,网络在当今世界无处不在。但是,任何事物都有两面性,网络同样是一把“双刃剑”。当人们尽情地在网络世界中遨游时,层出不穷的黑客攻击却使得安全性问题尤其突出,网络与信息系统的安全防护已经成为全社会关注的焦点。

国家计算机网络应急技术处理协调中心(CNCERT/CC)在《2006年网络安全工作报告》中指出,CNCERT/CC全年共接收26476件非扫描类网络安全事件报告,与2005年相比增长了两倍左右。从2003~2006年,CNCERT/CC接收非扫描类事件报告的数量比较如图1-1所示。

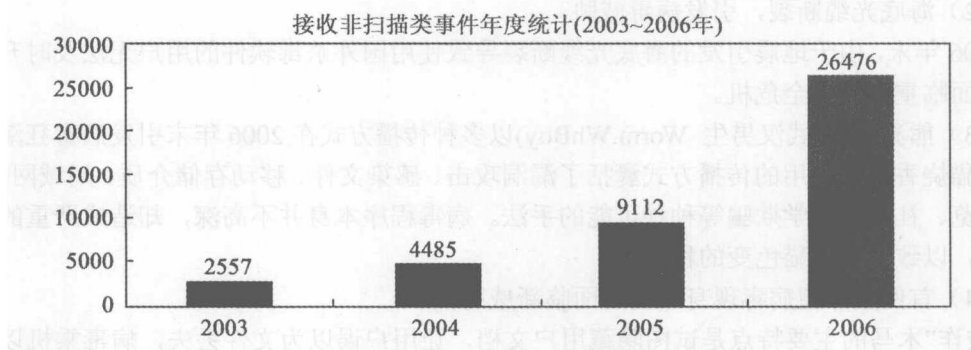


图 1-1 CNCERT/CC 接收非扫描类事件年度统计

从图中可以看到,近几年网络安全事件增长的速度是比较快的,而且呈现复杂化、协作化、分布式的特点。在此,我们通过回顾近年来影响比较大的安全事件,来揭示进行网络攻防技术研究的急迫性和必要性。

1. 中美黑客大战

2001年4月1日,美国一架海军EP-3侦察机在我国海南岛东南海域上空活动,我国两架军用飞机对其进行跟踪监视。北京时间上午9时7分,当我国飞机在海南岛东南104公里处正常飞行时,美机突然向我国飞机转向,其机头和左翼与我国一架飞机相撞,致使我国飞机坠毁,飞行员失踪。

中美撞机事件发生后,中美黑客之间展开了网络大战。自4月4日以来,美国黑客组织

不断袭击中国网站。对此,我国的网络安全人员积极防备美国黑客的攻击,一些黑客组织在“五一”期间打响了“黑客反击战”。在两天内已有超过 700 家中美政府及民间网站相继被“攻陷”。在此次攻击中,有很多国家的黑客加入到中美网战中,中美黑客大战战况惨烈,包括欧洲、中南美洲、亚洲及阿拉伯国家的黑客都加入了,各为自己所支持的一方出力,俨然是一场网络界的世界大战。

由于我国国内的很多网站的技术人员安全意识不足,不能针对具体攻击的特点制定有效的防护措施,导致系统被攻击后持续处于被破坏状态而造成不良影响。

2. 伊拉克打印机事件

据美国杂志披露,2003 年伊拉克战争爆发前不久,美国获悉伊拉克从法国购买了一种用于防空系统的新型电脑打印机,准备从安曼运往巴格达。美军派特工将安曼机场守卫人员买通,用一套固化有计算机病毒的同类芯片替换了打印机中的芯片。伊拉克战争爆发后,美军用指令激活了伊拉克防空系统电脑打印机芯片内的计算机病毒,病毒通过打印机侵入防空系统电脑中,使整个防空系统电脑瘫痪。这是世界上首次将计算机病毒用于实战,并取得效果的案例。

3. 知名安全公司金山毒霸评出的 2006 年度十大安全事件

(1) 维金蠕虫泛滥,引发企业用户网络瘫痪。

据金山毒霸反病毒监测中心最新数据显示,“维金(Worm.Viking.m,又名威金)”恶性蠕虫病毒自 2006 年 6 月 2 日被截获以来,截至 6 月 8 日 16 时,受攻击个人用户已由 3 000 多人迅速上升到 13 647 人,数 10 家企业用户网络瘫痪。这是继“狙击波”病毒爆发后,互联网受到的最严重的一次病毒袭击。

(2) 海底光缆断裂,引发病毒威胁。

2006 年末,由于地震引发的海底光缆断裂导致使用国外杀毒软件的用户无法及时升级病毒库,面临重大的安全危机。

(3) 熊猫烧香(武汉男生 Worm.WhBoy)以多种传播方式在 2006 年末引发病毒狂潮。

熊猫烧香病毒利用的传播方式囊括了漏洞攻击、感染文件、移动存储介质、局域网传播、网页浏览、社会工程学欺骗等种种可能的手法。病毒程序本身并不高深,却造成严重的大面积感染,以致达到谈猫色变的程度。

(4) 首例敲诈型病毒现身,用户面临新威胁。

“敲诈”木马的主要特点是试图隐藏用户文档,让用户误以为文件丢失,病毒乘机以帮用户恢复数据的名义要求用户向指定的银行账户内汇入定额款项。这也是国内首次出现此类对用户进行“敲诈勒索”的病毒,此后短时间内该木马已经相继出现了多个变种。

(5) 魔鬼波肆虐互联网,导致用户系统崩溃。

2006 年 8 月 14 日,金山毒霸反病毒监测中心及时截获了利用系统高危漏洞进行传播的恶性蠕虫病毒——魔鬼波(Worm.IRC.WargBot.a)。作为 IRCBot 系列病毒的新变种,该病毒主要利用 MS06-040 漏洞进行主动传播,强势攻击互联网,造成系统崩溃,网络瘫痪,并通过 IRC 聊天频道接受黑客的控制。

(6) 微软发布 Vista 操作系统,安全性遭受质疑。

虽然微软声称 Windows Vista 是历史上最安全的 Windows 系统,但有关公司进行的测试却表明实际情况并不容乐观。目前已经在 Windows Vista 中发现了包括存在于其语音识别过程中的数个安全漏洞,微软用大量新代码和新功能来取代以往的 Windows 架构,出现 Bug