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

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

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

第二部分　信息收集技术

第三部分　网络攻击技术

第四部分 防 御 技 术

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26 476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。

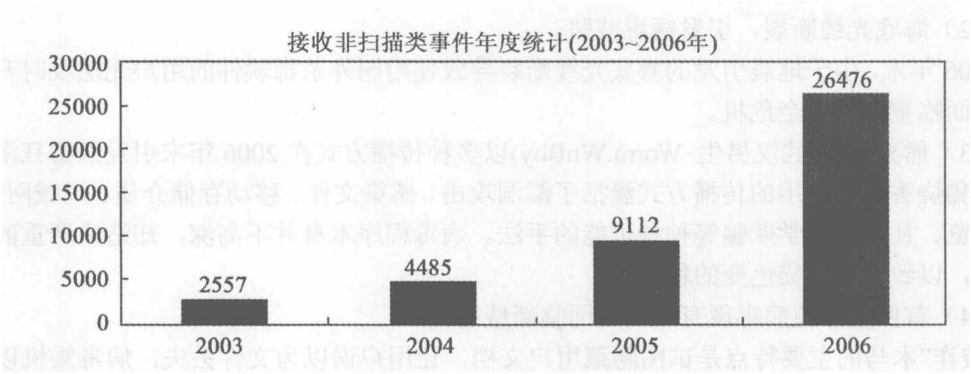

图1-1 CNCERT/CC接收非扫描类事件年度统计

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