<<网络攻击与防御技术>>

图书基本信息

书名：<<网络攻击与防御技术>>

13位ISBN编号：9787302234005

10位ISBN编号：7302234000

出版时间：2011-1

出版时间：清华大学

作者：张玉清

页数：322

前言

计算机和信息技术的飞速发展，网络的日益普及，深刻地改变着人们的生活方式、生产方式与管理方式，加快了国家现代化和社会文明的发展。
21世纪的竞争是经济全球化和信息化的竞争，“谁掌握信息，谁就掌握了世界”，信息安全不仅关系到公民个人、企业团体的日常生活，更是影响国家安全、社会稳定至关重要的因素之一。
近年来，我国网络安全事件发生比例呈上升趋势。
调查结果显示绝大多数网民的主机曾经感染病毒，超过一半的网民经历过账号／个人信息被盗窃、被篡改，部分网民曾被仿冒网站欺骗。
在经济利益的驱使下，制造、贩卖病毒木马、进行网络盗窃或诈骗、教授网络攻击技术等形式的网络犯罪活动明显增多，造成了巨大的经济损失和安全威胁，严重影响了我国互联网事业的健康发展。
面对如此严峻的挑战，国家明确提出要大力加强信息安全专门人才的培养，以满足社会对信息安全专门人才日益增长的需求，目前大多数高等院校都陆续开设了信息安全方面的课程，信息安全专门人才的培养逐渐步入正轨。
本书的目的是帮助安全人员掌握网络信息安全的基本知识，了解网络攻击方法和步骤，掌握基本的网络攻防技术，树立良好的网络安全防范意识。
书中总结了目前网络攻击的现状与发展趋势，详细介绍了计算机及网络系统面临的各种威胁和攻击手段。
作者以实例映衬原理，理论联系实际，采用尽可能简单和直观的方式向读者讲解技术原理，演绎攻击过程，希望能通过本书，向读者揭开“黑客”的神秘面纱，使读者对网络攻防技术有进一步的了解。
本书共分为13章，内容由浅入深。
第1章主要介绍了网络安全相关的基础知识和概念，阐述目前的网络安全形势，使读者对这一领域有一个初步的认识。
第2章介绍了网络攻击的一般步骤。
第3章至第11章则分门别类地阐述了目前黑客常用的一些攻击手段和技术，包括网络扫描技术、口令破解技术、欺骗攻击、拒绝服务攻击、缓冲区溢出、Web攻击、木马及计算机病毒等，对每种攻击手段既分析其技术原理、实现过程、性能、优缺点，又运用实际案例对知识要点进行阐释：并介绍了针对该种攻击手段可以采取的防范措施和策略。
第12章介绍了目前广泛应用的多种典型防御手段，包括常用的加密技术、身份认证技术、防火墙技术、入侵检测技术、虚拟专用网

<<网络攻击与防御技术>>

内容概要

本书从计算机网络安全基础知识人手，结合实际攻防案例，由浅入深地介绍网络攻与防御的技术原理和方法。

本书共分13章，主要讲述网络安全的基本概念和目前黑客常用的一些攻击手段和使技巧，包括网络扫描、口令破解技术、欺骗攻击、拒绝服务攻击、缓冲区溢出技术、Web攻击、特洛伊木马、计算机病毒等，并针对各种攻击方法介绍对应的检测或防御技术，此外，还简要阐述了目前应用较为广泛的多种典型防御手段，包括加密、身份认证、防火墙、入侵检测系统、虚拟专用网、蜜罐取证等。

本书内容全面，讲解细致，可作为高等院校信息安全等相关专业教学用书，也可供计算机网络的系统管理人员、安全技术人员和网络攻防技术爱好者学习参考之用。

作者简介

张玉清
　　国家计算机网络入侵防范中心副主任，信息安全国家重点实验室教授，博士生导师。
主要研究方向：网络攻防与系统安全。
在漏洞挖掘与利用、网络攻防渗透、密码协议分析等方面有深入研究。
先后主持国家高科技发展计划(863)项目、国家自然科学基金、国信安办项目、中国

<<网络攻击与防御技术>>

书籍目录

章节摘录

插图：1）源路由选项的使用IP包头中有一个源路由选项，用于该IP包的路由选择，一个IP包可按照预先指定的路由到达目的主机，如果目的主机使用该源路由的逆向路由与源主机通信，这样就给入侵者创造了良机，当一个入侵者预先知道某一主机有信任主机时，即可利用源路由选项伪装成信任主机，从而攻击系统。
2）伪装ARP包伪造ARP包的过程，是以受害者的IP地址和攻击者自身的MAC地址为源数据包发送ARP应答包，这样即造成另一种IP欺骗（即IP poof）。
这种攻击主要见于交换式以太网中，交换机在收到每一个ARP包时更新Cache，通过不停地发SpoofARP包可使本来要发往目的主机的包均送到入侵者处。
这个技术使得交换以太网也可以被监听。
3）RIP的攻击RIP是用于自治域内的一种路由协议，一个自治域的经典定义是指在一个管理机构控制之下的一组路由器。
这一协议主要用于内部交换路由信息，使用的算法是距离矢量算法，该算法的主要思想就是每个路由器向相邻路由器宣布可以通过它达到的路由器及其距离。
而接受到的主机并不检验这一信息，一个入侵者可能向目标主机以及沿途的各网关发出伪造的路由信息，入侵者可以冒充一条路由，使所有发往目的主机的数据包发往入侵者。
入侵者就可以冒充目的主机，也可以监听所有目的主机的数据包，甚至在数据流中插入任意包。
4）OSPF的攻击OSPF是用于自治域内的另一种路由协议，使用的算法是状态连接算法。
该算法中每个路由器向相邻的路由器发送的信息是一个完整的路由状态，包括可到达的路由器、连接类型和其他信息。
与RIP相比OSPF协议中已经实施认证过程，但是也存在着一些安全问题。
LSA（Link-State dvertisement）是OSPF协议路由器之间要交换的信息，其中的LS序列号为32位，用于指示该LSA的更新程度，LS序列号是一个有符号整数，大小介于Ox8000000l和0x7ffffiTff之间。

编辑推荐

《网络攻击与防御技术》：普通高等教育“十一五”国家级规划教材。
教育部高等学校信息安全类专业教学指导委员会、中国计算机学会教育专业委员会共同指导。

<<网络攻击与防御技术>>

版权说明