<<网络攻击与防御技术实验教程>>

图书基本信息

书名：<<网络攻击与防御技术实验教程>>

13位ISBN编号：9787302194354

10位ISBN编号：7302194351

出版时间：2010-7

出版时间：清华大学

作者：张玉清//陈深龙//杨彬

页数：122

前言

网络安全已成为人们在信息空间中生存与发展的重要保证条件，与国家的政治安全、经济安全、军事安全、社会稳定以及人们的日常生活密切相关。
由于兴趣爱好和经济利益的驱使，黑客攻击事件层出不穷。
公司和国家只有积极防御，才能在攻击环境下生存。
攻击与防御是一对相互制约和相互发展的网络安全技术。
本实验教程的目标是帮助安全人员理解黑客的攻击方法和步骤，事实一次又一次地证明，理解敌人的策略、技巧和工具对保护自己是多么的重要。
同时，本教程还让安全人员了解能采取哪些策略来防范各类攻击。
本书可作为《网络攻击与防御技术》的配套实验教程，同时又可自成体系，更注重攻防的实战性。
读者可以通过阅读该教程并动手实践达到提高网络安全技术的目的。
内容安排第1章：讲解安全技术的基本实验，包括windows账户和密码策略的设置、IIS和Apache安装与配置以及虚拟机软件VMware的使用。
第2章：讲解扫描技术，包括主机端口扫描和网络漏洞扫描。
第3章：讲解网络监听与防御技术，包括监听原理介绍、winPcap介绍和Sniffer工具的使用。
第4章：讲解口令攻击技术，包括UNIX和windows系统口令攻击技术的介绍、口令破解工具介绍。
第5章：讲解欺骗攻击及防御技术，欺骗攻击包括目前流行的IP欺骗和ARP欺骗。
第6章：讲解拒绝服务攻击与防范技术，包括DoS／DDoS攻击的原理、检测与防范，另外，还介绍了UDPFlood工具的使用方法。
第7章：讲解危害非常大的缓冲区溢出攻击，其中介绍了基本原理、攻击步骤、防范方法；同时还向读者介绍了一个非常典型的缓冲区溢出攻击实例。
第8章：讲解近几年网络攻击的热点——Web攻击及防范，该章用实例介绍了流行的SQL注入攻击和XSS攻击。
第9章：讲解了备受关注的木马攻击及防御，包括木马的自启动技术、隐藏技术，并用翔实的图文展示了冰河木马，最后介绍木马的防范。

<<网络攻击与防御技术实验教程>>

内容概要

网络攻击与防御技术是网络安全的核心和焦点，也是确保网络安全实际动手能力的综合体现。
全书共分11章，第1章介绍如何进行系统安全配置并搭建一个用于网络攻防实验的虚拟机，在接下来的各章中，在回顾理论知识的同时，结合动手实验介绍网络典型攻防技术，这些网络典型攻防技术包括扫描技术、网络监听及防御技术、口令攻击、欺骗攻击及防御、拒绝服务攻击与防范、缓冲区溢出攻击及防御、Web攻击及防范、木马攻击及防御、病毒与蠕虫攻击及防御和典型网络攻击防御技术。
通过这种理论与实践相结合的网络攻防技术的学习，读者会对网络攻击与防御技术有更直观和深刻的理解。

书中各章内容安排方式为：理论知识回顾、基本实验指导和巩固提高型实验。

本书可以作为信息安全、计算机、通信等相关专业研究生、本科生的教材，也可供从事网络安全研发的工程技术人员和热衷网络攻防技术的读者参考。

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、中国科学

<<网络攻击与防御技术实验教程>>

书籍目录

章节摘录

插图：当然，如果一个数据包没有到达发送的目标主机的网络接口，则目标主机无法监听到。
所以Sniffer‘所能监听到的信息仅限于在同一个物理网络内传送的数据包，也就是监听的目标中间不能有路由交换设备。
因此，当Sniffer工作在由集线器（Hub）构建的广播型局域网时，它可以监听到此物理网络内所有传送的数据；而对于由交换机（Switch）和路由器（Rotlte）构建的网络中，网络设备根据目标地址来分发和传送网络数据包，所以在这种网络中，Sniffei工具就只能监听到目标地址是本身的数据包和广播数据包。
虽然Sniffer能得到局域网中传送的大量数据，但如果不加选择地接收所有的数据包，并且长时间监听，那么获取的数据量将非常巨大，会耗费大量资源。
因此在使用Sniffer时要设置过滤器，把不想要的数据包过滤掉，这样Sniffer只监听想要的数据包，提高了监听效率，也为分析数据带来了方便。
使用Sniffer工具可以分析网络中的数据包协议和网络环境，同时也能够捕获口令，能够捕获专用的或者机密的信息，可以用来危害网上邻居的安全，或者用来获取更高级别的访问权限。

编辑推荐

《网络攻击与防御技术实验教程》：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。
根据教育部高等学校安全类专业教学指导委员会制订的《作息安全专业指导性专业规范》组织编写。

<<网络攻击与防御技术实验教程>>

版权说明