<<计算机网络安全技术实验教程>>

图书基本信息

书名：<<计算机网络安全技术实验教程>>

13位ISBN编号：9787563519590

10位ISBN编号：7563519599

出版时间：2009-8

出版时间：北京邮电大学出版社

作者：周绯菲，何文 主编

页数：202

前言

随着通信技术和互联网技术的发展，人们在享受网络带来便利的同时，黑客攻击、泄密等网络安全问题也变得越来越突出。
只要有网络的存在，网络的安全维护就是个极其重要的问题。
网络安全是指为计算机系统建立所采取的技术和管理的安全保护措施，保护计算机系统中的硬件、软件及数据，防止其因偶然、恶意的原因使系统遭到破坏、更改或泄露。
网络安全是基于通信、数学、计算机等多个学科的综合概念。
同时，网络安全也是一门实践性很强的课程，主要研究的就是攻击与防御。
本书是针对计算机网络安全课程的特点而编写的。
只有将计算机硬件、操作系统、各种应用软件、服务等理论知识的教学与实践教学相结合，才能很好地培养学生分析问题、解决问题的能力和专业实践能力。
加强实践教学是培养应用型人才的重要途径，这点对于高职高专学生尤为重要。
考虑到高职高专教育的定位和学生的实际情况，本书涉及的43个实验基本覆盖了当前计算机网络安全的主要分支和主要理论。
这些实验是按照由浅到深、由易到难的顺序排列的。
教师可以有选择性地给学生布置，也可以在本书实验的基础上进行扩展。
本书中的每个实验都由实验目的、实验设备、实验步骤、实验小结等几个部分组成。
对于黑客攻击的实验，本书全部给出了防御措施。
本书由交通部管理干部学院计算机系网络教研室组织编写，本书分为网络基础及网络嗅探技术、黑客攻击技术、预防黑客攻击、攻击的检测与响应共4篇。
第1篇网络基础及网络嗅探技术即第1章；第2篇黑客攻击技术由第2章漏洞扫描及网络隐身、第3章木马攻击、第4章主动攻击、第5章脚本攻击与后门账号的建立组成；第3篇预防黑客攻击由第6章windows操作系统平台的安全设置、第7章网络通信安全组成；第4篇攻击的检测与响应即第8章。
第1～8章均由周绯菲老师编写，其中第6章的windows xP操作系统的安全设置部分以及部分截图由何文老师完成。
此外，夏永恒、孙春兴、陈小全、鲁一力、汪洁、张传立等老师对本书的编写提供了大力支持，在此表示衷心感谢。
学习本书需要注意：（1）由于操作系统和应用软件的生产商会经常更新自己的版本，所以本书中的少数实验在讲授时可能无法看到书中展示的效果。
有些实验只能在windows 2000 Servei。
主机上进行。
有些实验使用windows 2003 ServeI‘作为操作系统时，只能使用正版系统，否则实验不能成功。
（2）实验中所有的计算机都有意设置了简单密码，这是为了便于实验使用，实验中也演示了简单密码的危险。

<<计算机网络安全技术实验教程>>

内容概要

本书是适应计算机网络安全教学而编写的一本实验教材。
本书以突出网络安全的系统性为宗旨，以分析和解决具体安全问题为目的，与网络安全原理相结合，按照由浅人深、由局部至整体的思路，对网络安全课程中的实验进行了系统分类。
本书将局域网及一般网站常见的安全配置与网络攻击技术相结合，强调攻防的对立与平衡。
本书通俗易懂，注重实用。
作者在多年的教学实践中，找到了实用性与学生兴趣的结合点，设计的实验技巧性和趣味性较强。
考虑到不同学校实验条件的不同，实验内容大部分是基于容易搭建的Windows操作系统的实验环境，降低了实验开设过程中的成本。
本书的实验是按由易到难的顺序设计的，教师可以根据学生的不同情况灵活布置。
本书中的每个实验由实验目的、实验设备、实验步骤、实验小结等几部分组成，实验的设计既突出了各实验的独立性又注意到了实验之间的连贯性。
本书注意与其他计算机课程的结合，突出了计算机知识的系统性、综合性，每个实验都与相关的计算机知识相结合，使读者建立起计算机网络安全的基本概念与基本架构。
本书不仅可以作为高职高专的计算机专业、网络管理专业、信息安全专业、通信专业的教材，也可以作为计算机网络安全的培训、自学教材，同时还可以作为网络工程技术人员、网络管理人员、信息安全管理人员的技术参考书。
本书全部讲授需要64～72课时(含理论部分的讲授)。
作为教材，授课教师可根据具体的实验室条件、专业情况以及教学计划的安排进行取舍。

<<计算机网络安全技术实验教程>>

书籍目录

章节摘录

插图：默认情况下FTP、HTTP、Telnet等协议在客户端与服务器端进行身份验证时用明文传输数据包。

网络嗅探技术利用某些工具，通过将网卡的工作模式设置为“混杂模式”的方式，使网卡处于对网络进行“监听”的状态，可以监听到与“混杂模式”的网卡处于同一物理网络中传输的数据帧（无论数据帧的目标地址是广播地址、本机地址或者其他主机的地址）。

如果使用Hub等共享式设备将几台主机互联，A机与B机之间通信时产生的数据包可以被安装了网络嗅探工具的主机C嗅探到。

但是在交换的网络和ATM网络中，嗅探效果不理想。

使用嗅探工具时应该注意以下几点。

（1）嗅探工具应该和其他网络主机使用Hub等共享式设备互连，这样才能捕获到网络中所有的数据包。

（2）如果网络设备使用的是交换机，可以通过两种方法实现对网络的监控：①对交换机进行镜像端口配置。

将所有其他端口上的数据包复制并转发一份到“镜像”端口，并让该端口与安装了嗅探工具的主机相连。

否则，嗅探工具只能够捕获到嗅探主机所连接的交换机端口上的所有数据包。

②把交换机的“镜像”端口级联到集线器上，再把安装了嗅探工具的主机接到集线器上。

由于考虑到实验室环境的通用性问题（用交换机取代Hub作为网络互连设备，而且实验室的管理人员不允许对交换机进行端口镜像），所以本实验采用退而求其次的方法：即在A机、B机与C机上分别装上网络嗅探软件Ethereal，观察流入、流出A机、B机与C机的数据包中是否包含用户名和口令信息。

当然，可以根据实验室的具体情况来对本实验进行扩充。

编辑推荐

《计算机网络安全技术实验教程》由北京邮电大学出版社出版。

<<计算机网络安全技术实验教程>>

版权说明