<<网络安全与软件系统修复>>

图书基本信息

书名：<<网络安全与软件系统修复>>

13位ISBN编号：9787302202295

10位ISBN编号：730220229X

出版时间：2009-10

出版时间：清华大学出版社

作者：《工作过程导向新理念丛书》编委会 编

页数：228

前言

互联网的发展，在带来了便利的同时，也给我们的生活增添了一份不安。
网络安全屡屡受到攻击威胁，回顾过去的网络安全事件，黑客事件的骇人听闻、计算机病毒的频繁变种、安全漏洞的层出不穷，形势的发展要求我们必须掌握一些基本的网络安全与软件系统修复知识。
网络安全技术的发展日新月异，本书主要从操作系统安全配置、网络常见攻击与防范、网络安全工具软件实例、计算机病毒防治、数据备份与恢复几个方面进行讲述。
本书以“课”的形式展开，全书共18课。
课前有情景式的“课堂任务”，包含了任务背景、任务目标和任务分析；课后有“课堂练习”，可分为任务背景、任务目标、任务要求和任务提示；“课堂练习”之后是“练习评价”。
为了拓展本课的知识，我们还准备了“本课小结”、“课外阅读”。
每课的最后还安排了“课后作业”。
本书的最后安排了两个“综合案例实践”，详细讲解了网络流量监控及内网入侵主机的过程。
全书共分6章18课：第1章（第1～3课）讲解了操作系统安全配置；第2章（第4～6课）讲解了几种常见的网络攻击与防范技术；第3章（第7～9课）讲解了几个网络安全工具软件实例：第4章（第10～12课）讲解了计算机病毒的基础知识；第5章（第13～16课）详细讲解了数据备份与恢复的相关技术；第6章（第17～18课）讲解了两个综合案例实践过程及演示。

内容概要

本书根据教育部教学大纲，按照新的“工作过程导向”教学模式编写。
为便于教师排课、备课、授课以及学生预习、上机练习、复习，本书将教学内容分解落实到每一课时，通过“课堂任务”、“课堂练习”、“本课小结”、“课外阅读”和“课后作业”五个环节实施教学。

本书共6章18课。
第1～5章介绍了网络安全与软件系统修复的相关基础知识；第6章为综合案例实践，介绍了网络流量监控和内网入侵主机的过程。
每课为两个标准学时，共90分钟内容。
建议学时为1学期，每周3课时，也可以分为两学期授课。

本书从实用的角度出发，通过实例循序渐进地讲解了网络安全与软件系统修复的基础知识。
书中详细地介绍了初学者必须掌握的网络安全基本知识和具体操作步骤，并对一些最新的网络安全技术也做了简单介绍，以适应形势发展的需要。

本书可作为中等职业学校网络安全相关专业的教材，也可作为各类技能型紧缺人才培训班的教材。

<<网络安全与软件系统修复>>

书籍目录

章节摘录

插图：步骤4 了解计算机病毒发展的最新趋势计算机病毒的发展近几年出现了一些新的趋势，概括来讲有以下几点。
（1）综合利用多种编程新技术的病毒将成为主流从Rootkit技术到映像劫持技术，磁盘过滤驱动到还原系统SSDTHOOK和还原其他内核HOOK技术，病毒为达到目的所采取的手段已经无所不用其极。
通过Rootkit技术和映像劫持技术隐藏自身的进程、注册表键值；通过插入进程、线程避免被杀毒软件查杀；通过实时监测对自身进程进行回写，避免被杀毒软件查杀；通过还原系统SSDTHOOK和还原其他内核HOOK技术破坏反病毒软件。
其中仅映像劫持技术就包括“进程映像劫持”、“磁盘映像劫持”、“域名映像劫持”、“系统DLL动态连接库映像劫持”等多种方式。
目前几乎所有的盗取网络游戏账号的木马病毒都具备了以上一种以上的技术特征，几乎所有最新的程序应用技术都被病毒一一应用。
计算机一旦感染病毒，普通用户根本无能力彻底清除，只能求助专业技术人员。
未来的计算机病毒将综合利用以上新技术，使得杀毒软件查杀难度更大。
（2）ARP病毒仍将成为局域网中的最大祸害ARP病毒已经成为近年来企业、网吧、校园网络等局域网的最大威胁。
此类病毒采用ARP挂马攻击技术，利用MAC地址欺骗，传播恶意广告或病毒程序，使得ARP病毒猖獗一时。
ARP病毒发作时，通常会造成网络掉线，但网络连接正常；内网的部分计算机不能上网，或者所有计算机均不能上网；无法打开网页或打开网页慢以及局域网连接时断时续并且网速较慢等现象。
更为严重的是，ARP病毒的新变种能够把自身伪装成网关，在所有用户请求访问的网页添加恶意代码，导致杀毒软件在用户访问任意网站时均发出病毒警报，用户下载的任何可执行文件均被替换为病毒，严重影响到企业网络、网吧、校园网络等局域网的正常运行。

编辑推荐

《网络安全与软件系统修复》：工作过程导向新理念丛书，中等职业学校教材·计算机专业。

<<网络安全与软件系统修复>>

版权说明