

<<网络安全技术项目化教程>>

图书基本信息

书名：<<网络安全技术项目化教程>>

13位ISBN编号：9787302294474

10位ISBN编号：730229447X

出版时间：2012-8

出版时间：清华大学出版社

作者：黄林国 主编

页数：304

字数：477000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<网络安全技术项目化教程>>

### 内容概要

《网络安全技术项目化教程》基于“项目引导、任务驱动”的项目化教学方式编写而成，体现“基于工作过程”、“教、学、做”一体化的教学理念。

本书内容划分为11个工程项目，具体内容包括：认识计算机网络安全技术、Windows系统安全加固、网络协议与分析、计算机病毒及防治、密码技术、网络攻击与防范、防火墙技术、入侵检测技术、VPN技术、Web

安全、无线网络安全。

每个项目案例按照“提出问题”“分析问题”

“解决问题”“拓展提高”四部曲展开。

读者能够通过项目案例完成相关知识的学习和技能的训练，每个项目案例来自企业工程实践，具有典型性、实用性、趣味性和可操作性。

《网络安全技术项目化教程》可作为高等职业院校和高等专科院校“

网络安全技术”课程的教学用书，也可作为成人高等院校、各类培训、计算机从业人员和爱好者的参考用书。

本书由黄林国、章仪任主编。

## <<网络安全技术项目化教程>>

### 书籍目录

#### 项目1 认识计算机网络安全技术

- 1.1 项目提出
- 1.2 项目分析
- 1.3 相关知识点
  - 1.3.1 网络安全概述
  - 1.3.2 网络安全所涉及的内容
  - 1.3.3 网络安全防护
  - 1.3.4 网络安全标准
  - 1.3.5 虚拟机技术
- 1.4 项目实施
  - 1.4.1 任务1：系统安全“傻事清单”
  - 1.4.2 任务2：VMware虚拟机的安装与使用
- 1.5 拓展提高：基本物理安全
- 1.6 习题

#### 项目2 Windows系统安全加固

- 2.1 项目提出
- 2.2 项目分析
- 2.3 相关知识点
  - 2.3.1 操作系统安全的概念
  - 2.3.2 服务与端口
  - 2.3.3 组策略
  - 2.3.4 账户与密码安全
  - 2.3.5 漏洞与后门
- 2.4 项目实施
  - 2.4.1 任务1：账户安全配置
  - 2.4.2 任务2：密码安全配置
  - 2.4.3 任务3：系统安全配置
  - 2.4.4 任务4：服务安全配置
  - 2.4.5 任务5：禁用注册表编辑器
- 2.5 拓展提高：Windows系统的安全模板
- 2.6 习题

#### 项目3 网络协议与分析

- 3.1 项目提出
- 3.2 项目分析
- 3.3 相关知识点
  - 3.3.1 计算机网络体系结构
  - 3.3.2 以太网的帧格式
  - 3.3.3 网络层协议格式
  - 3.3.4 传输层协议格式
  - 3.3.5 三次握手机制
  - 3.3.6 ARP欺骗攻击
  - 3.3.7 网络监听
- 3.4 项目实施
  - 3.4.1 任务1：Sniffer软件的安装与使用
  - 3.4.2 任务2：ARP欺骗攻击与防范

## <<网络安全技术项目化教程>>

3.5 拓展提高：端口镜像

3.6 习题

项目4 计算机病毒及防治

4.1 项目提出

4.2 项目分析

4.3 相关知识点

4.3.1 计算机病毒的概念

4.3.2 计算机病毒的特征

4.3.3 计算机病毒的分类

4.3.4 宏病毒和蠕虫病毒

4.3.5 木马

4.3.6 反病毒技术

4.4 项目实施

4.4.1 任务1：360杀毒软件的使用

4.4.2 任务2：360安全卫士软件的使用

4.4.3 任务3：宏病毒和网页病毒的防范

4.4.4 任务4：利用自解压文件携带木马程序

4.4.5 任务5：反弹端口木马(灰鸽子)的演示

4.5 拓展提高：手机病毒

4.6 习题

项目5 密码技术

5.1 项目提出

5.2 项目分析

5.3 相关知识点

5.3.1 密码学的基础知识

5.3.2 古典密码技术

5.3.3 对称密码技术

5.3.4 非对称密码技术

5.3.5 单向散列算法

5.3.6 数字签名技术

5.3.7 数字证书

5.3.8 EFS加密文件系统

5.4 项目实施

5.4.1 任务1：DES、RSA和Hash算法的实现

5.4.2 任务2：PGP软件的使用

5.4.3 任务3：EFS的使用

5.5 拓展提高：密码分析

5.6 习题

项目6 网络攻击与防范

6.1 项目提出

6.2 项目分析

6.3 相关知识点

6.3.1 网络攻防概述

6.3.2 目标系统的探测

6.3.3 网络监听

6.3.4 口令破解

6.3.5 IPC\$入侵

## <<网络安全技术项目化教程>>

6.3.6 缓冲区溢出攻击

6.3.7 拒绝服务攻击

6.4 项目实施

6.4.1 任务1：黑客入侵的模拟演示

6.4.2 任务2：缓冲区溢出漏洞攻击的演示

6.4.3 任务3：拒绝服务攻击的演示

6.5 拓展提高：网络入侵证据的收集与分析

6.6 习题

项目7 防火墙技术

7.1 项目提出

7.2 项目分析

7.3 相关知识点

7.3.1 防火墙结构概述

7.3.2 防火墙技术原理

7.3.3 防火墙体系结构

7.3.4 Windows防火墙

7.3.5 天网防火墙

7.4 项目实施

7.4.1 任务1：Windows防火墙的应用

7.4.2 任务2：天网防火墙的配置

7.5 拓展提高：Cisco PIX防火墙配置

7.6 习题

项目8 入侵检测技术

8.1 项目提出

8.2 项目分析

8.3 相关知识点

8.3.1 入侵检测系统概述

8.3.2 入侵检测系统的基本结构

8.3.3 入侵检测系统的分类

8.3.4 基于网络和基于主机的入侵检测系统

8.4 项目实施

任务：SessionWall入侵检测软件的使用

8.5 拓展提高：入侵防护系统

8.6 习题

项目9 VPN技术

9.1 项目提出

9.2 项目分析

9.3 相关知识点

9.3.1 VPN概述

9.3.2 VPN的特点

9.3.3 VPN的处理过程

9.3.4 VPN的分类

9.3.5 VPN的关键技术

9.3.6 VPN隧道协议

9.4 项目实施

9.4.1 任务1：部署一台基本的VPN服务器

9.4.2 任务2：设置VPN客户端

## <<网络安全技术项目化教程>>

9.5 拓展提高：IPSec VPN与SSL VPN的比较

9.6 习题

### 项目10 Web安全

10.1 项目提出

10.2 项目分析

10.3 相关知识点

10.3.1 Web安全概述

10.3.2 IIS的安全

10.3.3 脚本语言的安全

10.3.4 Web浏览器的安全

10.4 项目实施

10.4.1 任务1：Web服务器的安全配置

10.4.2 任务2：通过SSL访问Web服务器

10.4.3 任务3：利用Unicode漏洞实现网页“涂鸦”的演示

10.4.4 任务4：利用SQL注入漏洞实现网站入侵的演示

10.5 拓展提高：防范网络钓鱼

10.6 习题

### 项目11 线网络安全

11.1 项目提出

11.2 项目分析

11.3 相关知识点

11.3.1 无线局域网基础

11.3.2 无线局域网标准

11.3.3 无线局域网设备

11.3.4 无线局域网的组网模式

11.3.5 服务集标识

11.3.6 无线加密标准

11.4 项目实施

任务：无线局域网安全配置

11.5 拓展提高：无线局域网的安全性

11.6 习题

参考文献

## 章节摘录

版权页：插图：2.3.4账户与密码安全 账户与密码的使用通常是许多系统预设的防护措施。事实上，有许多用户的密码是很容易被猜中的，或者使用系统预设的密码，甚至不设密码。用户应该避免使用不当的密码、系统预设密码或是使用空白密码，也可以配置本地安全策略要求密码符合安全性要求。

2.3.5漏洞与后门 1.漏洞 漏洞即某个程序（包括操作系统）在设计时未考虑周全，当程序遇到一个看似合理，但实际无法处理的问题时，引发的不可预见的错误。

系统漏洞又称安全缺陷，对用户造成的不良后果有：如漏洞被恶意用户利用，会造成信息泄露。例如，黑客攻击网站即利用网络服务器操作系统的漏洞。

对用户操作造成不便。

例如，不明原因的死机和丢失文件等。

可见，仅有堵住系统漏洞，用户才会有一个安全和稳定的工作环境。

漏洞的产生大致有以下3个原因。

编程人员的人为因素。

在程序编写过程中，为实现不可告人的目的，在程序代码的隐蔽处留有后门。

受编程人员的能力、经验和当时安全技术所限，在程序中难免会有不足之处，轻则影响程序效率，重则导致非授权用户的权限提升。

由于硬件原因，使编程人员无法弥补硬件的漏洞，从而使硬件的问题通过软件表现出来。

可以说，几乎所有的操作系统都不是十全十美的，总是存在各种安全漏洞。

例如在Windows NT中，安全账户管理（SAM）数据库可以被以下用户所复制：Administrator账户、Administrators组中的所有成员、备份操作员、服务器操作员以及所有具有备份特权的人员。

SAM数据库的一个备份能够被某些工具所利用来破解口令。

又如，Windows NT对较大的ICMP数据包是很脆弱的，如果发一条ping命令，指定数据包的大小为64KB，Windows NT的TCP / IP栈将不会正常工作，可使系统离线乃至重新启动，结果造成某些服务的拒绝访问。

任何软件都难免存在漏洞，但作为系统最核心的软件，操作系统存在的漏洞会使黑客有机可乘。

例如，64位Windows 7图形显示组件中的一个漏洞有可能导致系统崩溃，或者被黑客利用并执行远程代码，用户可以通过关闭Windows Aero的方式或打上安全补丁来防止这一漏洞被他人利用。

实际上，根据目前的软件设计水平和开发工具，要想绝对避免软件漏洞几乎是不可能的。

操作系统作为一种系统软件，在设计和开发过程中造成这样或那样的缺陷，埋下一些安全隐患，使黑客有机可乘，也可以理解。

可以说，软件质量决定了软件的安全性。

2.后门 后门又称为Back Door，是绕过安全性控制而获取对程序或系统访问权的方法。

在软件的开发阶段，程序员常会在软件内创建后门以便可以修改程序中的缺陷。

如果后门被其他人知道，或是在发布软件之前没有删除后门，那么它就成了安全风险。

后门产生的必要条件如下。

必须以某种方式与其他终端节点相连。

因为都是从其他节点访问后门，因此必须使用双绞线、光纤、串 / 并口、蓝牙、红外等设备与目标主机连接才可以对端口进行访问。

只有访问成功，双方才可以进行信息交流，攻击方可有机会进行入侵。

目标主机默认开放的可供外界访问的端口必须在一个以上。

因为一台默认无任何端口开放的机器是无法进行通信的，而如果开放的端口无法被外界访问，则目标主机同样不可能遭到入侵。

## <<网络安全技术项目化教程>>

### 编辑推荐

《高职高专计算机任务驱动模式教材:网络安全技术项目化教程》可作为高等职业院校和高等专科院校“网络安全技术”课程的教学用书,也可作为成人高等院校、各类培训、计算机从业人员和爱好者的参考用书。

《高职高专计算机任务驱动模式教材:网络安全技术项目化教程》由黄林国、章仪任主编。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>