普通高校本科计算机专业特色教材精选·网络与通信

计算机网络安全学习辅导与实验指南

沈鑫剡 叶寒锋 刘鹏 景丽 编著

清华大学出版社

普通高校本科计算机专业特色教材精选·网络与通信

计算机网络安全学习辅导与实验指南

沈鑫剡 叶寒锋 刘鹏 景丽 编著

清华大学出版社
北京

内 容 简 介

本书是《计算机网络安全》(沈鑫剡编著,清华大学出版社出版)的配套辅导教材,也是 CCNA 安全课程理想的学习辅导和实验指南。每一章由三部分组成:知识要点、例题解析和实验。知识要点部分给出了教材中对应章的知识脉络,重点、难点问题的理解和分析方法。例题解析部分分为自测题、简答题和综合题。自测题用于自我评判对教材内容的理解程度;简答题和综合题使读者进一步理解计算机网络安全的基本概念、方法和技术,掌握解题思路,培养分析、解决问题的能力。实验部分是本书的一大特色,以 Cisco Packet Tracer 软件为实验平台,针对每一章内容设计了大量帮助读者理解、掌握教材内容的实验,同时也设计了大量旨在帮助读者掌握 CCNA 安全课程内容的实验。

本书适合作为大专院校计算机专业学生"计算机网络安全"课程的参考书和实验指南,也可作为参加 CCNA 安全课程学习和用 Cisco 网络设备进行复杂安全网络设计的工程技术人员的参考书。

图书在版编目(CIP)数据

计算机网络安全学习辅导与实验指南/沈鑫剡,叶寒锋等编著. —北京:清华大学出版社,2012.5
(普通高校本科计算机专业特色教材精选·网络与通信)
ISBN 978-7-302-28165-8

Ⅰ. ①计… Ⅱ. ①沈… ②叶… Ⅲ. ①计算机网络—安全技术—高等学校—教学参考资料
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 034046 号

责任编辑:袁勤勇　顾　冰
封面设计:傅瑞学
责任校对:胡伟民
责任印制:何　芊

出版发行:清华大学出版社
网　　址:http://www.tup.com.cn, http://www.wqbook.com
地　　址:北京清华大学学研大厦 A 座　　邮　　编:100084
社 总 机:010-62770175　　邮　　购:010-62786544
投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn
印 刷 者:三河市君旺印装厂
装 订 者:三河市新茂装订有限公司
经　　销:全国新华书店
开　　本:185mm×260mm　　**印　　张**:23.5　　**字　　数**:590 千字
版　　次:2012 年 5 月第 1 版　　**印　　次**:2012 年 5 月第1 次印刷
印　　数:1～3000
定　　价:35.00 元

产品编号:043197-01

出版说明

INTRODUCTION

在我国高等教育逐步实现大众化后，越来越多的高等学校将会面向国民经济发展的第一线，为行业、企业培养各级各类高级应用型专门人才。为此，教育部已经启动了“高等学校教学质量和教学改革工程”，强调要以信息技术为手段，深化教学改革和人才培养模式改革。如何根据社会的实际需要，根据各行各业的具体人才需求，培养具有特色显著的人才，是我们共同面临的重大问题。具体地说，培养具有一定专业特色和特定能力强的计算机专业应用型人才是计算机教育要解决的问题。

为了适应21世纪人才培养的需要，培养具有特色的计算机人才，急需一批适合各种人才培养特点的计算机专业教材。目前，一些高校在计算机专业教学和教材改革方面已经做了大量工作，许多教师在计算机专业教学和科研方面已经积累了许多宝贵经验。将他们的教研成果转化为教材的形式，向全国其他学校推广，对于深化我国高等学校的教学改革是一件十分有意义的事情。

清华大学出版社在经过大量调查研究的基础上，决定组织出版一套“普通高校本科计算机专业特色教材精选”。本套教材是针对当前高等教育改革的新形势，以社会对人才的需求为导向，主要以培养应用型计算机人才为目标，立足课程改革和教材创新，广泛吸纳全国各地的高等院校计算机优秀教师参与编写，从中精选出版确实反映计算机专业教学方向的特色教材，供普通高等院校计算机专业学生使用。

本套教材具有以下特点：

1. 编写目的明确

本套教材是在深入研究各地各学校办学特色的基础上，面向普通高校的计算机专业学生编写的。学生通过本套教材，主要学习计算机科学与技术专业的基本理论和基本知识，接受利用计算机解决实际问题的基本训练，培养研究和开发计算机系统，特别是应用系统的基本能力。

2. 理论知识与实践训练相结合

根据计算机学科的三个学科形态及其关系，本套教材力求突出学科的理论与实践紧密结合的特征，结合实例讲解理论，使理论来源于实践，又进一步指导实践。学生通过实践深化对理论的理解，更重要的是使学生学会理论方法的实际运用。在编写教材时突出实用性，并做到通俗易懂，易教易学，使学生不仅知其然，知其所以然，还要会其如何然。

3. 注意培养学生的动手能力

每种教材都增加了能力训练部分的内容，学生通过学习和练习，能比较熟练地应用计算机知识解决实际问题。既注重培养学生分析问题的能力，也注重培养学生解决问题的能力，以适应新经济时代对人才的需要，满足就业要求。

4. 注重教材的立体化配套

大多数教材都将陆续配套教师用课件、习题及其解答提示，学生上机实验指导等辅助教学资源，有些教材还提供能用于网上下载的文件，以方便教学。

由于各地区各学校的培养目标、教学要求和办学特色均有所不同，所以对特色教学的理解也不尽一致，我们恳切希望大家在使用教材的过程中，及时地给我们提出批评和改进意见，以便我们做好教材的修订改版工作，使其日趋完善。

我们相信经过大家的共同努力，这套教材一定能成为特色鲜明、质量上乘的优秀教材。同时，我们也希望通过本套教材的编写出版，为“高等学校教学质量和教学改革工程”作出贡献。

清华大学出版社

前言

PREFACE

本书是《计算机网络安全》（沈鑫剡编著，清华大学出版社出版）的配套辅导教材。每一章由三部分组成：知识要点、例题解析和实验。知识要点部分，一是对学生学习过程中碰到的难点进行更深入的讨论；二是理清教材内容的知识结构，给出完整理解教材内容的方法和思路；三是精确描述与网络安全相关的各种技术、概念的本质含义和相互之间区别。大量的例题解析，一是能够帮助学生更好地理解教材内容，掌握解题思路，培养分析、解决问题的能力；二是许多例题都是典型应用的案例，使学生能够将教材内容和实际安全网络设计有机结合，解决学生学以致用的问题；三是通过给出综合运用教材内容进行复杂安全网络分析、设计的详细步骤，为学生树立完整的网络安全知识结构，了解网络安全技术的本质，掌握各种类型安全网络的设计方法和思路。本书最大的特点是实验，基于 Cisco Packet Tracer 软件，一是针对教材的每一章内容设计了大量的实验，这些实验一部分是教材中的案例和实例的具体实现，用于验证教材内容，帮助学生更好地理解、掌握教材内容，另一部分是实际问题的解决方案，给出用 Cisco 网络设备设计各种类型安全网络的方法和步骤；二是针对 CCNA 安全课程内容设计了大量实验，用于帮助读者更好地理解、掌握 CCNA 安全课程内容。

Cisco Packet Tracer 软件的人机界面非常接近实际设备的配置过程，除了连接线缆等物理动作外，学生通过 Cisco Packet Tracer 软件完成实验与通过实际 Cisco 网络设备完成实验几乎没有差别，通过 Cisco Packet Tracer 软件，学生完全可以完成复杂的安全网络的设计、配置和验证过程。更为难得的是，Cisco Packet Tracer 软件可以模拟 IP 分组端到端传输过程中交换机、路由器等网络设备处理 IP 分组的每一个步骤，显示各个阶段应用层报文、传输层报文、IP 分组、封装 IP 分组的链路层帧的结构、内容和首部中每一个字段的值，使得学生可以直观了解 IP 分组的端到端传输过程及 IP 分组端到端传输过程中各层 PDU 的细节和变换过程。

“计算机网络安全”课程的宗旨是培养学生解决信息存储、传输和处

理过程中面临的安全问题的能力，是一门实验性很强的课程。但目前有的教材只是给学生罗列了大量有关网络安全的概念和术语，提供的实验仅仅是让学生掌握一些扫描和加密软件的使用方法，并不能实现培养学生具有各种类型安全网络的分析和设计能力的教学目标。究其原因，无法提供设计、配置和调试各种类型安全网络的实验环境是导致教学内容落后的重要因素。因此，实现“计算机网络安全”课程的教学目标需要从两个方面着手：一是需要一本提供完整、系统的网络安全理论，深入讨论当前主流网络安全技术，在具体网络环境下讨论运用网络安全技术设计安全网络的方法和过程的教材；二是需要提供一个能够完成各种类型安全网络设计、配置和调试过程的实验环境和一本给出运用教材提供的理论和技术设计、配置和调试各种类型的安全网络的步骤和方法的实验指导书。Cisco Packet Tracer软件实验平台就是一个能够完成各种类型安全网络设计、配置和调试过程的实验环境，本书提供了在Cisco Packet Tracer软件实验平台上运用教材提供的理论和技术设计、配置和调试各种规模的安全网络的步骤和方法。《计算机网络安全》和本书相得益彰，学生用教材提供的安全网络设计原理和技术指导实验，反过来又通过实验来加深理解教材内容，课堂教学和实验形成良性互动。

本书由解放军理工大学工程兵工程学院计算机应用教研室的沈鑫剡和吉林大学研究生叶寒锋共同编写，由沈鑫剡定稿。限于作者的水平，错误和不足之处在所难免，殷切希望使用本书的老师和学生批评指正，也殷切希望读者能够就本书内容和叙述方式提出宝贵建议和意见，以便进一步完善本书内容。作者E-mail地址为shenxinshan@163.com。

编者

2011年10月

目录

CONTENTS

第1章 概述 …… 1

1.1 知识要点 …… 1

1.1.1 黑客攻击对象和攻击手段 …… 1

1.1.2 信息安全与网络安全 …… 2

1.1.3 网络安全内容和体系结构 …… 4

1.2 例题解析 …… 5

1.2.1 自测题 …… 5

1.2.2 自测题答案 …… 9

1.2.3 简答题解析 …… 11

1.3 Cisco Packet Tracer 5.3 使用说明 …… 12

1.3.1 功能介绍 …… 12

1.3.2 用户界面 …… 13

1.3.3 工作区分类 …… 14

1.3.4 操作模式 …… 15

1.3.5 设备类型和配置方式 …… 16

1.4 实验 …… 18

1.4.1 信息嗅探攻击实验 …… 18

1.4.2 信息截获攻击实验 …… 22

1.4.3 拒绝服务攻击实验 …… 25

1.4.4 路由项欺骗攻击实验 …… 27

1.4.5 DHCP 欺骗攻击实验 …… 32

1.4.6 DNS 欺骗攻击实验 …… 34

1.4.7 非法接入实验 …… 39

第2章 恶意代码分析与防御 …… 43

2.1 知识要点 …… 43

2.1.1 病毒传播和感染方式 …… 43

2.1.2 恶意代码危害 …… 44

2.1.3 网络安全技术对阻止病毒和蠕虫传播的作用 …… 45
2.1.4 网络安全技术对减少恶意代码危害的作用 …… 52
2.2 例题解析 …… 54
2.2.1 自测题 …… 54
2.2.2 自测题答案 …… 57
2.2.3 简答题解析 …… 59
2.2.4 综合题解析 …… 59
2.3 实验 …… 61
2.3.1 NAT 隐藏内部网络实验 …… 61
2.3.2 有状态分组过滤器控制信息交换过程实验 …… 69
2.3.3 流量管制器抑制病毒传播实验 …… 74
第 3 章 黑客攻击机制 …… 77
3.1 知识要点 …… 77
3.1.1 黑客攻击对象 …… 77
3.1.2 黑客攻击手段 …… 77
3.1.3 黑客攻击防御机制 …… 78
3.2 例题解析 …… 81
3.2.1 自测题 …… 81
3.2.2 自测题答案 …… 85
3.2.3 简答题解析 …… 86
3.2.4 综合题解析 …… 88
3.3 实验 …… 89
3.3.1 交换式以太网远程设备配置实验 …… 89
3.3.2 简单互连网远程设备配置实验 …… 97
3.3.3 交换机端口配置实验 …… 103
3.3.4 访问控制和流量管制实验 …… 104
3.3.5 安全路由实验 …… 109
3.3.6 审计实验 …… 114
第 4 章 加密和报文摘要算法 …… 119
4.1 知识要点 …… 119
4.1.1 加密算法分类 …… 119
4.1.2 报文摘要算法的单向性和抗冲突性要求 …… 121
4.1.3 加密和报文摘要算法在网络安全中的作用 …… 122
4.2 例题解析 …… 124
4.2.1 自测题 …… 124
4.2.2 自测题答案 …… 128
4.2.3 简答题解析 …… 130

第 5 章 鉴别协议和数字签名 …… 131
5.1 知识要点 …… 131
5.1.1 Internet 接入控制 …… 131
5.1.2 鉴别方式和类型 …… 133
5.1.3 数字签名和身份鉴别 …… 135
5.2 例题解析 …… 137
5.2.1 自测题 …… 137
5.2.2 自测题答案 …… 142
5.2.3 简答题解析 …… 144
5.2.4 综合题解析 …… 145
5.3 实验 …… 147
5.3.1 终端接入本地鉴别实验 …… 147
5.3.2 局域网接入本地鉴别实验 …… 151
5.3.3 统一鉴别实验 …… 155
5.3.4 综合统一鉴别实验 …… 162
第 6 章 网络安全技术 …… 169
6.1 知识要点 …… 169
6.1.1 网络设备和安全设备 …… 169
6.1.2 以太网安全功能 …… 169
6.1.3 安全路由功能 …… 170
6.1.4 内部网络隐藏功能 …… 170
6.1.5 网络容错功能 …… 171
6.2 例题解析 …… 171
6.2.1 自测题 …… 171
6.2.2 自测题答案 …… 173
6.2.3 简答题解析 …… 175
6.3 实验 …… 175
6.3.1 安全校园网设计实验 …… 175
6.3.2 容错网络设计实验 …… 189
6.3.3 PAT 实验 …… 193
6.3.4 路由器身份鉴别实验 …… 204
第 7 章 无线局域网安全技术 …… 209
7.1 知识要点 …… 209
7.1.1 WEP …… 209
7.1.2 WPA …… 210
7.2 例题解析 …… 212
7.2.1 自测题 …… 212
7.2.2 自测题答案 …… 216

7.2.3 简答题解析 …… 218
7.3 实验 …… 219
7.3.1 WPA-PSK 配置实验 …… 219
7.3.2 WPA 配置实验 …… 222
第 8 章 虚拟专用网络 …… 231
8.1 知识要点 …… 231
8.1.1 点对点 IP 隧道 …… 231
8.1.2 IP Sec 和 VPN …… 234
8.1.3 Cisco Easy VPN …… 236
8.2 例题解析 …… 240
8.2.1 自测题 …… 240
8.2.2 自测题答案 …… 243
8.2.3 简答题解析 …… 244
8.3 实验 …… 245
8.3.1 点对点 IP 隧道配置实验 …… 245
8.3.2 IP Sec 配置实验 …… 254
8.3.3 Cisco Easy VPN 配置实验 …… 258
第 9 章 防火墙 …… 267
9.1 知识要点 …… 267
9.1.1 无状态分组过滤器 …… 267
9.1.2 有状态分组过滤器 …… 269
9.1.3 Cisco 区域策略防火墙 …… 274
9.2 例题解析 …… 278
9.2.1 自测题 …… 278
9.2.2 自测题答案 …… 281
9.2.3 简答题解析 …… 282
9.2.4 综合题解析 …… 283
9.3 实验 …… 285
9.3.1 标准分组过滤器配置实验 …… 285
9.3.2 扩展分组过滤器配置实验 …… 288
9.3.3 有状态分组过滤器配置实验 …… 291
9.3.4 区域策略防火墙配置实验 …… 298
第 10 章 入侵防御系统 …… 303
10.1 知识要点 …… 303
10.1.1 入侵防御系统定义和分类 …… 303
10.1.2 入侵检测机制 …… 304
10.1.3 反制动作 …… 304
10.1.4 元攻击特征实例 …… 305

10.2 例题解析 …… 305
10.2.1 自测题 …… 305
10.2.2 自测题答案 …… 308
10.2.3 简答题解析 …… 309
10.3 实验 …… 311
10.3.1 网络入侵防御系统基本配置实验 …… 311
第 11 章 网络管理和监测 …… 315
11.1 知识要点 …… 315
11.1.1 网络设备配置方式 …… 315
11.1.2 SNMP 管理网络过程 …… 317
11.2 例题解析 …… 320
11.2.1 自测题 …… 320
11.2.2 自测题答案 …… 322
11.2.3 简答题解析 …… 323
11.3 实验 …… 323
11.3.1 控制台端口方式配置网络设备实验 …… 323
11.3.2 Telnet 方式配置网络设备实验 …… 325
11.3.3 SNMP 管理网络设备实验 …… 330
第 12 章 应用层安全协议 …… 335
12.1 知识要点 …… 335
12.1.1 内部资源和公共资源 …… 335
12.1.2 安全协议的适用性 …… 336
12.2 例题解析 …… 337
12.2.1 自测题 …… 337
12.2.2 自测题答案 …… 339
12.2.3 简答题解析 …… 340
第 13 章 试卷和答案 …… 343
13.1 试卷一 …… 343
13.1.1 试卷 …… 343
13.1.2 答案 …… 347
13.2 试卷二 …… 349
13.2.1 试卷 …… 349
13.2.2 答案 …… 353
13.3 试卷三 …… 356
13.3.1 试卷 …… 356
13.3.2 答案 …… 360
参考文献 …… 363

第1章 概 述

CHAPTER

1.1 知识要点

1.1.1 黑客攻击对象和攻击手段

黑客对网络的攻击可以分为对主机系统攻击和对通信系统的攻击。

1. 主机系统攻击手段

(1) 在主机系统运行恶意代码。

通过下属手段,在主机系统运行恶意代码。

- 手工植入恶意代码并激活。
- 在下载的网络资源中植入病毒。
- 利用主机系统漏洞上传并激活病毒。

(2) 利用主机系统漏洞非法登录。

通过下属手段,非法登录主机系统。

- 利用主机系统漏洞非法建立管理员账户,利用非法建立的管理员账户登录主机系统。
- 利用激活的木马程序非法访问主机系统资源。
- 利用主机系统错误开放的服务,如共享服务、远程调用服务非法访问主机系统资源。

(3) 穷举攻击。

- 猜测主机系统登录口令。
- 利用字典破解主机系统登录口令。

2. 通信系统攻击手段

(1) 信息嗅探攻击。

信息嗅探攻击是指非法窃取经过网络传输的信息,但不影响信息正常传输过程的攻击行为。

(2) 信息截获攻击。

信息截获攻击是指截获经过网络传输的信息,使信息无法继续正常传输的攻击行为。截获信息是篡改信息,实施重放攻击的前提。

(3) 重放攻击。

重放攻击是指黑客截获信息,延迟一段时间后,转发或反复转发截获的信息的攻击行为。重放攻击一般不对截获的信息进行处理。

(4) 拒绝服务攻击。

拒绝服务攻击是指通过消耗掉服务器处理资源、转发结点处理资源、物理链路带宽,使网络不能提供正常服务的攻击行为。

(5) 非法接入。

非法接入是指黑客将终端非法接入内部网络的行为,如未经授权建立和无线局域网接入点之间的关联,通过盗用的用户名和口令接入启动 802.1X 接入控制功能的交换机端口等。非法接入是对网络实施攻击的第一步。

(6) 诱骗攻击。

黑客通过接入伪造的 DHCP 服务器,使终端获取错误的网络配置信息,导致终端对网络资源的访问过程出现问题。更严重的是,黑客通过伪造的 DHCP 服务器和伪造的 DNS 服务器将一些著名网站的域名和黑客伪造的 Web 服务器的 IP 地址绑定在一起,使得用户对著名网站的访问变为对黑客伪造的 Web 服务器的访问。

(7) 路由项欺骗攻击。

通过向路由器发送伪造的路由项,使得路由器错误地将黑客终端作为通往某个网络的传输路径的下一跳,并将所有以该网络中的终端为目的终端的 IP 分组转发给该黑客终端。

3. 被动攻击和主动攻击

网络攻击可以分为被动攻击和主动攻击,被动攻击只是窃取信息,不会影响信息正常的存储、处理和传输过程,信息嗅探攻击是典型的被动攻击。主动攻击篡改已经存在的信息,影响信息正常的传输和处理过程,甚至伪造信息,信息截获攻击、重放攻击、各种欺骗攻击(包括源 IP 地址欺骗攻击、DHCP 欺骗攻击和 DNS 欺骗攻击等)和拒绝服务攻击是典型的主动攻击。主要通过预防,而不是检测来应对被动攻击。主动攻击是网络面临的主要安全问题,应对主动攻击需要各种安全机制(包括信息备份和恢复技术)的有机结合。

1.1.2 信息安全与网络安全

1. 信息安全目标

信息安全目标是保障网络中信息资源的保密性、完整性、可用性、可控制性和不可抵赖性。网络中的信息资源包括存储在主机系统中的信息资源和经过网络传输的信息资源,因此,保障信息资源的完整性包括保障主机系统的完整性。可用性是综合指标,用于评估信息资源提供服务的能力,涉及通信系统、主机系统等多个方面。

2. 信息安全功能

(1) 消除主机系统漏洞。

主机系统漏洞包括操作系统漏洞和应用程序漏洞,它们是导致黑客入侵的主要原因。消除主机系统漏洞是避免黑客入侵的最有效方法,但完全消除主机系统漏洞是不现实的,因此,较长时间段内会是一个反复进行发现漏洞、利用漏洞入侵、修补漏洞的过程。

（2）避免主机系统植入恶意代码。

主机系统一旦植入恶意代码，将导致信息外泄，破坏信息的保密性；可能使主机系统崩溃，破坏信息的可用性；也可能篡改存储在主机系统中的信息，破坏信息的完整性。主机系统植入恶意代码是信息资源最大的安全隐患。网络是目前传播病毒的主要渠道，因此除了在主机系统安装查杀病毒软件外，必须有效隔断经过网络传播病毒的通道。

（3）确保经过网络传输的信息的保密性和完整性。

网络应用导致大量信息经过网络传输，必须保证这些经过网络传输的信息的保密性和完整性，因此必须采取有效手段杜绝信息嗅探、信息截获攻击的发生。

（4）隔断黑客和攻击目标之间的通道。

目前大量利用主机系统漏洞实施的攻击行为都是远程攻击行为，黑客必须经过网络实现和攻击目标之间的信息传输，必须能够鉴别出黑客实施攻击的信息流，并阻断黑客和攻击目标之间的信息流传输通道。

3. 信息安全技术

（1）加密、报文摘要和鉴别算法。

加密、报文摘要和鉴别算法是信息安全的基础，是保障信息保密性、完整性的有效手段。

（2）安全操作系统。

安装一个安全操作系统是防御黑客入侵的关键。安全操作系统是指没有漏洞；能够通过用户身份鉴别和授权对用户访问信息资源过程实施有效控制；能够通过制定用户行为规则发现病毒，并对病毒破坏信息资源行为实施反制；能够对主机系统资源实施有效保护的操作系统。

（3）安全应用程序。

运行安全应用程序也是防御黑客入侵的必要手段。安全应用程序是指没有漏洞；能够通过用户身份鉴别和授权对用户访问信息资源过程实施有效控制的应用程序。

（4）安全传输机制。

安全传输机制是指保障信息传输过程中的保密性和完整性的机制，包括有效防止黑客实施信息嗅探和信息截获攻击的机制、信息加密和完整性检测机制、信息源端鉴别机制等。

（5）接入控制机制。

接入控制机制是指保证只有授权终端接入网络，且使得网络只允许传输、接收端只允许接收授权终端发送的信息的机制，包括双向身份鉴别机制、安全参数协商机制和基于用户的接入控制机制等。

（6）访问控制机制。

访问控制机制保证授权用户只能访问到授权访问的信息，包括只在授权用户使用的终端和授权访问的信息资源所在主机系统之间建立传输通路的机制、只允许授权用户使用的终端和授权访问的信息资源所在主机系统之间传输与完成访问授权访问的信息有关的信息流的机制。

(7) 隔离病毒机制。

隔离病毒机制是指防止病毒传播,隔断病毒网络中传播途径的机制,包括检测出与病毒传播和因为病毒发作引发的攻击行为有关的信息流并予以丢弃的机制、禁止主机系统之间发生与病毒传播相似的信息流传输模式的机制。

4. 网络安全范畴

网络安全是信息安全的重要组成部分,网络安全可以定义为是所有用于保障传输过程中的信息的安全、阻断病毒传播和黑客非法访问途径、应对各种各样网络攻击手段的机制和技术的集合,它不包括信息安全技术中的安全操作系统和安全应用程序的内容。

1.1.3 网络安全内容和体系结构

1. 网络安全内容

(1) 基础理论。

加密算法、报文摘要算法和鉴别算法等。

(2) 接入控制和访问控制机制。

802.11X、802.11i、PPP 和 PPPoE、VPN、防火墙和入侵防御系统等。

(3) 防御远程攻击和阻断病毒传播路径机制。

阻止端口扫描和漏洞探测机制、阻断病毒传播路径机制、端到端安全传输机制和流量管制机制等。

(4) 防御信息嗅探和信息截获攻击机制。

以太网安全机制、安全路由机制、虚拟网络技术、IP Sec 和 TLS 等。

(5) 防御诱骗攻击机制。

信任端口、DNS Sec、HTTPS 和 SET 等。

(6) 网络管理和监测机制。

基于 SNMPv3 的网络管理系统和网络综合监测系统等。

2. 网络安全体系结构

网络安全体系结构如图 1.1 所示,它由两部分组成:一部分是网络安全基础,它所包含的加密、报文摘要算法、数字签名技术、身份鉴别机制和各种安全协议是所有网络安全技术的基础。另一部分是作用于网络每一层的安全技术。

<table>
<tr><td colspan="6">HTTPS、SET、SSL VPN、PGP等</td><td colspan="2">应用层</td></tr>
<tr><td colspan="6">有状态检测、信息流管制等</td><td colspan="2">传输层</td></tr>
<tr><td colspan="6">安全路由协议、IPSec、分组过滤、NAT等</td><td colspan="2">网际层</td></tr>
<tr><td rowspan="2">以太网</td><td>安全端口，接入控制</td><td rowspan="2">无线局域网</td><td>802.11i</td><td rowspan="2">接入网络</td><td>接入控制、VPN、L2TP</td><td>链路层</td><td rowspan="2">网络接口层</td></tr>
<tr><td>电缆、光缆保护，电磁屏蔽</td><td>信号能量控制</td><td>电缆、光缆保护，电磁屏蔽</td><td>物理层</td></tr>
<tr><td colspan="6">加密、报文摘要和数字签名技术
TLS、RADIUS等</td><td colspan="2">网络
安全基础</td></tr>
</table>

图 1.1 网络安全体系结构

1.2　例题解析

1.2.1　自测题

1. 选择题

(1) 下述_____不属于网络面临的安全问题。

A. 病毒　　B. 拒绝服务攻击

C. 非法访问　　D. 网络设备快速更新

(2) 下述_____不属于引发网络安全问题的原因。

A. 网络原旨是方便通信

B. 大量商务活动在网上展开

C. 网络信息资源已经成为重要的战略资源

D. 网络安全设备发展迅速

(3) 下述_____无法破坏网络的可用性。

A. 病毒　　B. 拒绝服务攻击　　C. 非法访问　　D. 线缆遭受破坏

(4) 下述_____和信息保密性无关。

A. 加密解密算法　　B. 终端接入控制　　C. 病毒　　D. 拒绝服务攻击

(5) 下述_____和信息完整性无关。

A. 加密解密算法　　B. 报文摘要算法　　C. 信息嗅探攻击　　D. 信息截获攻击

(6) 下述_____和黑客远程入侵主机系统无关。

A. 操作系统漏洞　　B. 应用程序漏洞

C. 黑客和主机系统之间信息传输路径　　D. 主机系统的物理安保措施

(7) 下述_____和病毒植入主机系统无关。

A. 操作系统漏洞　　B. 配置主机系统网络信息方式

C. 黑客和主机系统之间信息传输路径　　D. 主机系统的物理安保措施

(8) 下述_____和信息嗅探攻击有关。

A. 操作系统漏洞　　B. 应用程序漏洞

C. 信息传输路径　　D. 主机系统的物理安保措施

(9) 下述_____和信息截获攻击有关。

A. 操作系统漏洞　　B. 应用程序漏洞

C. 配置主机系统网络信息方式　　D. 主机系统的物理安保措施

(10) 下述_____和诱骗用户登录伪造的著名网站无关。

A. 篡改 DNS 服务器的资源记录　　B. 伪造 DNS 服务器

C. 配置主机系统网络信息方式　　D. 著名网站的物理安保措施

(11) 下述_____和阻止信息截获攻击无关。

A. 禁止伪造的 DHCP 服务器接入网络　　B. 鉴别 DNS 资源记录

C. 鉴别路由消息　　D. 用交换机取代集线器