

《网络安全与防护》

图书基本信息

书名：《网络安全与防护》

13位ISBN编号：9787308101912

10位ISBN编号：7308101916

出版时间：2012-7

出版社：浙江大学出版社

作者：吴培飞

页数：358

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《网络安全与防护》

内容概要

《高职高专网络技术项目化系列教材:网络安全与防护》以神州数码网络设备为载体,通过项目化课程方式进行编排。从园区网安全维护、网络设备的访问控制、网络入侵检测与防御、网络流量过滤和整形、实施统一威胁管理系统这几个方面,介绍园区网络安全技术的攻击与防范。《高职高专网络技术项目化系列教材:网络安全与防护》共分为九个项目。

书籍目录

项目一初识网络安全

- 1.1 网络与信息安全发展史
 - 1.1.1 信息安全的由来
 - 1.1.2 信息安全的定义
 - 1.1.3 信息安全古今谈
- 1.2 网络及信息安全关键技术
 - 1.2.1 信息保密技术
 - 1.2.2 信息隐藏技术
 - 1.2.3 认证技术
 - 1.2.4 密钥管理技术
 - 1.2.5 数字签名技术
- 1.3 安全网络的搭建与管理
 - 1.3.1 常用网络信息安全命令介绍
 - 1.3.2 常用网络安全工具介绍
- 1.4 典型工作任务概述
 - 1.4.1 网络存在的典型安全问题
 - 1.4.2 办公室网络安全事件及解决
 - 1.4.3 园区网络安全事件及解决
 - 1.4.4 园区网络及信息安全解决方案设计与实施
- 1.5 思考与练习

项目二网络与攻防环境搭建及使用

- 2.1 项目描述
 - 2.1.1 项目背景
 - 2.1.2 项目需求描述
- 2.2 项目分析
 - 2.2.1 虚拟机技术
 - 2.2.2 服务器技术与网络服务
 - 2.2.3 “ IIS+ASP ” 技术介绍
 - 2.2.4 “ Apache+Tomcat ” 技术介绍
 - 2.2.5 信息安全教学系统介绍
- 2.3 项目实施
 - 2.3.1 网络环境搭建与安全维护
 - 2.3.2 堡垒主机环境搭建
 - 2.3.3 堡垒使用——网络病毒与恶意软件预防
 - 2.3.4 堡垒使用——网络服务与应用系统安全
 - 2.3.5 堡垒使用——加密与数字签名技术实践
- 2.4 项目延伸思考

项目三园区网安全维护

- 3.1 项目描述
 - 3.1.1 项目背景
 - 3.1.2 项目需求描述
- 3.2 项目分析
 - 3.2.1 识别并防御欺骗攻击——ARP。欺骗种类及防御方法
 - 3.2.2 识别并防御欺骗攻击——路由欺骗及防御
 - 3.2.3 识别并防御欺骗攻击——DHCP，欺骗及防御
 - 3.2.4 识别并防御欺骗攻击——生成树协议攻击及防御
 - 3.2.5 识别并防御欺骗攻击——ICMP协议攻击及防御

3.2.6 协议安全——基于无状态的协议安全保障方案

3.3 项目实施

3.3.1 ARP欺骗攻击及防御

3.3.2 RIP协议欺骗及防御

3.3.3 DHCP欺骗及防御

3.3.4 生成树协议攻击及防御

3.3.5 ICMP重定向问题及解决方案

3.3.6 基于UDP协议的攻击及防范

3.4 项目延伸思考

项目四利用网络设备加强园区访问控制

4.1 项目描述

4.1.1 项目背景

4.1.2 项目需求描述

4.2 项目分析

4.2.1 访问控制列表

4.2.2 防火墙对Web流量的控制

4.2.3 网内流量控制

4.3 项目实施

4.3.1 标准ACL列表的应用

4.3.2 扩展ACL的应用

4.3.3 交换机中的其他种类ACL

4.3.4 策略路由中的ACL应用

4.3.5 防火墙基础配置

4.3.6 防火墙策略应用

4.3.7 配置防火墙会话统计和会话控制

4.3.8 二层交换机基于MAC地址控制网络访问

4.4 项目延伸思考

项目五检测及防御网络入侵

5.1 项目描述

5.1.1 项目背景

5.1.2 项目需求描述

5.2 项目分析

5.2.1 常用网络攻击介绍

5.2.2 入侵检测系统概述

5.2.3 DCSM内网安全管理系统概述

5.2.4 WAF系统概述

5.3 项目实施

5.3.1 搭建IDS系统

5.3.2 拒绝服务攻击、发现、响应和处理

5.3.3 漏洞利用攻击、发现、响应和处理

5.3.4 网页攻击、发现、响应和处理

5.4 项目延伸思考

项目六信息安全风险评估

6.1 项目描述

6.1.1 项目背景

6.1.2 项目需求描述

6.2 项目分析

6.2.1 信息安全风险评估标准发展史

6.2.2 信息安全风险评估方法

- 6.2.3 评估参考依据
- 6.2.4 信息安全评估过程
- 6.2.5 操作系统的常用安全评估检查列表
- 6.2.6 数据库安全评估常见检查列表

6.3 项目实施

- 6.3.1 windows2003操作系统评估
- 6.3.2 Unix系统评估

6.4 项目延伸思考

项目七安全等级保护

7.1 项目描述

- 7.1.1 项目背景
- 7.1.2 项目需求描述

7.2 项目分析

- 7.2.1 等级保护标准
- 7.2.2 等级保护定级
- 7.2.3 信息系统等级保护基本要求
- 7.2.4 信息系统安全等级保护测评准则
- 7.2.5 术语和定义

7.3 项目实施

- 7.3.1 项目启动
- 7.3.2 项目实施

7.4 项目延伸思考

项目八综合案例——典型校园安全网络搭建与维护

8.1 项目描述

- 8.1.1 项目背景
- 8.1.2 项目需求描述

8.2 项目分析

- 8.2.1 校园网络现状分析
- 8.2.2 核心层设计分析
- 8.2.3 网络实名制设计分析
- 8.2.4 网络安全设计分析
- 8.2.5 流量整形网关设计分析

8.3 项目实施

- 8.3.1 设备分层设计
- 8.3.2 解决方案制定与建模

8.4 项目延伸思考

项目九理论建模——模型与体系架构

9.1 TCP/IP与OSI模型架构

- 9.1.1 OSI参考模型
- 9.1.2 TCP/IP模型

9.2 网络方案设计模型与架构

- 9.2.1 网络设计概述
- 9.2.2 层次型网络设计模型

9.3 信息安全道德规范

- 9.3.1 信息安全从业人员道德规范
- 9.3.2 国外一些信息安全相关职业道德规范

《网络安全与防护》

编辑推荐

《高职高专网络技术项目化系列教材：网络安全与防护》的特点：（1）注重实践操作，知识点围绕操作过程按需介绍。（2）攻防结合，重点在防。（3）由浅入深，由简入繁，循序渐进。（4）侧重应用，抛开复杂的理论说教，学以致用。

《网络安全与防护》

精彩短评

1、可惜没有配套PPT，得自己做了

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:www.tushu000.com