<<无线局域网技术项目教程>>

图书基本信息

书名：<<无线局域网技术项目教程>>

13位ISBN编号：9787894360755

10位ISBN编号：7894360759

出版时间：2012-7

出版时间：东软电子出版社

作者：胡云 编

页数：248

字数：394000

<<无线局域网技术项目教程>>

内容概要

本教材以组建无线局域网的实例为主线，介绍了无线局域网的基本原理、协议标准、技术规范、通信传输、组网拓扑、设备功能、设备类型、工程安装、网络配置、监控优化、网络安全、网络规划、行业应用、故障排除等关键技术。
本教材注重分析无线网络与有线网络的关系，理解计算机网络架构的拓展，使读者更全面完整地认识计算机网络。
本教材广泛介绍了无线局域网技术的最新发展和前沿应用，内容全面丰富，叙述深入浅出，语言通俗易懂，不仅注重理论方法的引导，更注重工程实际的应用，着力提高读者设计和实现无线局域网的技能，具有很强的可操作性。
本教材可作为高等职业院校计算机网络技术及相关专业的教材，也可作为从事网络组建、网络管理等工程技术人员和无线网络爱好者的参考教材。

<<无线局域网技术项目教程>>

书籍目录

章节摘录

版权页： 插图： 4.8.1 WLAN IDS简介 802.11网络很容易受到各种网络威胁的影响，如未经授权的AP用户、Ad—hoc网络、拒绝服务型攻击等。
Rogue设备对于企业网络安全来说更是一个很严重的威胁。
无线入侵检测系统（Wireless Intrusion Detection System，WIDS）可以对有恶意的用户攻击行为和入侵行为进行早期检测，保护企业网络和用户不被无线网络上未经授权的设备访问。
WIDS可以在不影响网络性能的情况下对无线网络进行监测，从而提供对各种攻击的实时防范。
WLAN IDS涉及的常用术语：（1）Rogue AP：网络中未经授权或者有恶意的AP，它可以是私自接入到网络中的AP、未配置的AP、邻居AP或者攻击者操作的AP。
如果在这些AP上存在安全漏洞，黑客就有机会危害无线网络安全。
（2）Rogue Client：非法客户端，网络中未经授权或者有恶意的客户端，类似于Rogue AP。
（3）Rogue Wireless Bridge：非法无线网桥，网络中未经授权或者有恶意的网桥。
（4）Monitor AP：这种AP在无线网络中通过扫描或监听无线介质，检测无线网络中的Rogue设备。
一个AP可以同时作为接入AP和Monitor AP，也可以只作为Monitor AP。
（5）Ad-hoc mode：把无线客户端的工作模式设置为Ad-hoc模式，Ad-hoc终端可以不需要任何设备支持而直接进行通讯。
4.8.2无线入侵检测系统架构 无线入侵检测系统有集中式和分散式两种。
集中式无线入侵检测系统通常用于连接单独的Sensors（探测器，俗称探头），搜集数据并转发到存储和处理数据的中央系统中。
分散式无线入侵检测系统通常包括多种设备来完成IDS的处理和报告。
分散式无线入侵检测系统比较适合较小规模的无线局域网，因为它价格便宜且易于管理。
当过多的Sensors需要检测时，Sensors的数据处理将被禁用。
所以，多线程处理和报告的Sensors管理比集中式无线人侵检测系统花费更多的时间。
无线局域网通常被配置在一个相对大的场所。
为了更好的接收信号，需要配置多个无线基站（WAPS），在无线基站的位置上部署Sensors，会提高信号的覆盖范围。
这种物理架构能够检测到大多数的黑客行为，并且加强了同无线基站（WAPS）的距离，从而能更好地定位黑客的详细地理位置。
4.8.3 检测Rogue设备 一般可以把网络中的设备分为两种类型：非法设备（Rogue设备）和合法设备。
Rogue设备可能存在安全漏洞或被攻击者操纵，因此会对用户网络的安全造成严重威胁或危害。

版权说明