

<<无线网络安全攻防实战>>

图书基本信息

书名：<<无线网络安全攻防实战>>

13位ISBN编号：9787121075087

10位ISBN编号：7121075083

出版时间：2008-11

出版时间：电子工业

作者：杨哲

页数：408

字数：636000

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>

<<无线网络安全攻防实战>>

前言

当你坐在3楼熟悉的星巴克咖啡屋，在靠窗的角落里习惯性地打开笔记本，连上星巴克提供的无线接入点，翻看着当天网络上最新的资讯信息时，可曾想过就在街对面，一栋新建不久的饭店4楼，有人正试图通过无线网络，攻入你的电脑并窃取你保存在硬盘深处的新闻调查笔记？

当你坐在办公室里，在空调送来的凉爽微风下，整理刚参加完的公司会议记录时，可曾想过就在和你间隔3米的楼上，有人正试图通过公司的无线网络，窃取你计算机上备份的公司内部发展计划？

当你坐在机场环境优雅的VIP候机厅里，一边漫不经心地在笔记本上翻看着自己的个人Blog，一边听着MP3时，可曾想过离你500米远的一辆黑色SUV里，会有一台笔记本正一样通过机场提供的无线接入服务，在快速下载并记录着你笔记本里所有关于后天安全技术峰会的秘密资料？

当你和朋友们外出旅游，在休息的酒店里拿出新买的iPhone，迫不及待地连上酒店的无线网络收取当天的电子邮件时，可曾想过就在走廊尽头的的一个单间里，有人已经通过无线网络进入你的iPhone，正翻看着你那些不能见光的个人写真图集？

这不是什么好莱坞的科幻电影，更不是什么危言耸听的传言，而是就在我们的身边，就在我们的桌旁，每一个标识着WiFi的便携设备上，一个繁华技术背后的安全阴影——无线网络，是不是真的方便了自己也方便了别人？

无线网络带来的巨大便利和庞大的商业价值，已经无须证明。

作为政府及通信部门对无线网络技术的扶持，也使得无线技术开始成为发展最快的高新技术之一。但是人们在沉浸于享受无线网络带来便利的同时，很多人却并没有意识到，技术的两面性已经开始在一些不为大多数人所知的领域有所体现。

应对当前国内外无线网络发展的种种势头，本书从身边基础的无线网络环境讲起，由浅至深地探讨了无线网络涉及的各个方面，包括无线WEP加密破解、无线WPA/WPA2破解、内网渗透、无线DoS攻击与防护、无线VPN搭建与攻击防护、War-Driving战争驾驶及其他各种无线攻击可能的角度和解决方案。

和以往注重理论化的无线安全书籍不同的是，在本书中，笔者将带给大家关于无线网络的实际攻击技术及对应的防御技术。

需要说明的是，在所有涉及攻击技术的章节，对那些试图通过无线网络进行非法攻击、渗透及破坏等非法行为的家伙们，本书中都会称之为“恶意的攻击者”。

真正能被称之为无线“黑客”的，正是那些通过不断研究无线攻防技术，来促使无线安全技术整体提升，以达到完善无线网络，推动更高级无线网络规范实施的可敬的人们。

谨以此书向这些投入大量心血的幕后黑客们致以发自内心的敬意。

如果说公布或者研究无线黑客技术会引起别有用心的人注意，甚至让一些人觉得有些不可理解的话，那么，摆在我们面前的现实是：很多无线网络只是由一些“自负”的管理员们凭着传统有线网络的经验管理，有很大部分的人无视或根本不知自身的无线将面临何种风险。

为此，与其不知所措，不如正视这些可能的攻击行为和方式，这样，才能够真正强化巩固好现有的无线网络。

何况，古人亦云：师夷长技以制夷。

希望这样一本实际操作的教程可以帮助同样喜欢无线网络安全的朋友们少走弯路，也希望能吸引更多的人投入到无线网络安全领域来。

<<无线网络安全攻防实战>>

内容概要

面对当前国内外无线网络飞速发展、无线化城市纷纷涌立的发展现状，本书以日趋严峻的无线网络安全为切入，从基本的无线网络攻击测试环境搭建讲起，由浅至深地剖析了无线网络安全及黑客技术涉及的各个方面。

本书分为13章，包括无线WEP加密破解、无线WPA/WPA2破解、内网渗透、无线DoS攻击与防护、无线VPN搭建与攻击防护、War-Driving战争驾驶、无线钓鱼攻击及无线VoIP攻击、无线打印机攻击等特殊角度无线攻击和解决方案。

本书可以作为军警政机构无线安全人员、无线评估及规划人员、企业及电子商务无线网络管理员的有力参考，也可以作为高级黑客培训及网络安全认证机构的深入网络安全辅助教材，是安全技术爱好者、无线安全研究者、无线开发人员必备的参考宝典。

<<无线网络安全攻防实战>>

作者简介

杨哲，持有CIW国际网络安全分析师（CIW Security Analyst）、微软认证系统工程师（MCSE）及微软认证数据库专家（MCDBA）证书。

身为ZerOne安全团队负责人，中国无线门户网站AnyWlan无线安全版主。

目前工作为政府机构安全顾问、警务系统应急响应顾问、陕西零嘉壹信息科技有限公司技术总监及安全主管、多家国内知名培训中心金牌网络安全讲师及MCSE讲师、网络安全及黑客类杂志自由撰稿人等。

常担任户外领队及进行高山摄影，拥有7年户外经验，曾多次带队进行过太白山徒步穿越、自行车两省穿越、野外宿营、皮艇漂流、室内攀岩、悬崖速降等极限活动.....

<<无线网络安全攻防实战>>

书籍目录

- 第1章 你所了解和不知道的无线世界 1.1 精彩的表面——无线网络现状 1.2 阴影下的世界——无线黑客技术的发展
- 第2章 准备工作——基础知识及工具 2.1 无线黑客的装备 2.1.1 无线网卡的选择 2.1.2 天线 2.1.3 基本知识 2.2 Windows及Linux攻击环境准备 2.2.1 Windows环境准备 2.2.2 Linux环境准备 2.2.3 Live CD 2.2.4 VMware 2.3 Windows下攻击准备——驱动程序安装 2.3.1 WildPackets 驱动程序安装指南 2.3.2 CommView驱动程序安装 2.4 Windows下无线探测工具 2.5 Linux下无线探测工具 2.6 基于PDA的无线探测工具
- 第3章 再见，WEP 3.1 WEP基础 3.1.1 WEP 3.1.2 WiFi安全的历史与演化 3.1.3 关于Aircrack-ng 3.1.4 安装Aircrack-ng 3.2 BackTrack 2 Linux下破解无线WEP 3.2.1 在Backtrack 2 Linux下进行WEP加密的破解 3.2.2 攻击中常见错误提示及解决方法 3.3 Windows下破解WEP 3.3.1 使用Aircrack-ng for Windows 3.3.2 使用Cain破解WPA-PSK 3.4 关于WEP加密破解的深度 3.4.1 关于WEP加密的深度 3.4.2 关于WEP加密的位数 3.5 推翻WEP强化的可笑观点
- 第4章 WEP破解的多米诺骨牌 4.1 无客户端Chopchop攻击 4.1.1 什么是无客户端 4.1.2 关于无客户端的破解 4.1.3 无客户端破解之Chopchop攻击实现 4.1.4 可能出现的出错提示 4.2 无客户端Fragment攻击 4.2.1 无客户端破解之Fragment攻击实现 4.2.2 注意事项 4.3 无客户端ARP+Deauth攻击 4.3.1 无客户端破解之ARP+Deauth攻击实现 4.3.2 整体攻击效果 4.4 共享密钥的WEP加密破解 4.4.1 配置共享密钥的WEP加密无线环境 4.4.2 破解共享密钥WEP加密的无线环境 4.4.3 整体攻击效果 4.5 关闭SSID广播的对策 4.6 突破MAC地址过滤 4.6.1 关于MAC地址过滤 4.6.2 突破MAC地址过滤步骤 4.6.3 防范方法 4.7 避开DHCP的正面限制 4.7.1 避开DHCP的正面限制步骤 4.7.2 深入细节 4.8 破解本地存储密码 4.9 自动化WEP破解工具 4.10 截获及分析无线WEP加密数据 4.10.1 截获无线数据 4.10.2 分析截获的无线数据包
- 第5章 击垮WPA家族 5.1 WPA/WPA2基础 5.1.1 关于WPA 5.1.2 关于Cowpatty 5.1.3 安装Cowpatty 5.2 BackTrack 2 Linux下破解无线WPA 5.2.1 Aircrack-ng攻击及破解 5.2.2 Cowpatty破解 5.2.3 WPA-PSK-TKIP和WPA-PSK-AES加密的区别 5.2.4 攻击中常见错误提示及解决方法 5.3 Windows下破解无线WPA-PSK加密 5.3.1 使用Aircrack-ng for Windows 5.3.2 使用Aircrack-ng for Windows 的细节 5.3.3 使用Cain破解WPA-PSK 5.4 Ubuntu下破解无线WPA2-PSK 5.4.1 关于Ubuntu (乌班图) 5.4.2 无线接入点WPA2-PSK加密破解步骤 5.4.3 攻击中的一些细节 5.4.4 攻击中常见错误提示及解决方法 5.4.5 WPA2-PSK-TKIP和WPA2-PSK-AES加密的区别 5.4.6 一些注意事项 5.5 PDA下破解WPA / WPA2 5.5.1 PDA进行无线破解的不足 5.5.2 PDA进行无线破解的方法 5.5.3 使用PDA进行无线破解的具体步骤 5.5.4 PDA进行无线破解的优势 5.6 WPA / WPA2连接配置 5.6.1 WPA连接设置 5.6.2 WPA2连接设置 5.6.3 Linux下连接设置总结 5.7 强化WPA-PSK / WPA2-PSK环境 5.7.1 在WPA / WPA2设置上采用复杂的密钥 5.7.2 检查密码是否强悍 5.8 WPA高速破解的真相 5.9 提升破解WPA实战 5.9.1 制作专用字典 5.9.2 使用Cowpatty实现高速破解 5.9.3 使用Aircrack-ng进行高速破解 5.9.4 破解速度对比 5.10 提高WPA安全系数的其他选择
- 第6章 渗透在内网——我悄悄地走正如我悄悄地来 6.1 端口扫描 6.1.1 扫描技术分类 6.1.2 常用的扫描工具 6.1.3 扫描实例 6.1.4 安全公司的选择 6.2 在线密码破解 6.2.1 内网在线密码破解工具 6.2.2 内网在线密码破解 6.2.3 小结 6.3 远程控制 6.4 缓冲区溢出 6.4.1 基础知识 6.4.2 相关工具及站点 6.4.3 使用Metasploit进行缓冲区溢出攻击 6.4.4 关于Metasploit的攻击代码库升级 6.4.5 防范及改进方法 6.5 MITM攻击 6.5.1 什么是MITM攻击 6.5.2 Linux下MITM攻击实现 6.5.3 Windows下MITM攻击实现 6.5.4 小结
- 第7章 耐心+伪装总是有效的 7.1 搭建伪造AP基站 7.1.1 伪造AP基站攻击及实现方法 7.1.2 搜索及发现伪造AP 7.2 无线MITM攻击 7.2.1 攻击原理 7.2.2 工具与实现 7.2.3 防御方法及建议 7.3 Wireless Phishing (无线钓鱼) 攻击及防御 7.3.1 关于钓鱼 7.3.2 Wireless AP Phishing (无线AP钓鱼) 7.3.3 伪造站点+DNS欺骗式钓鱼攻击 7.3.4 伪造电子邮件+伪造站点式钓鱼攻击 7.3.5 如何识别伪造邮件 7.3.6 如何防御
- 第8章 无线DoS及进阶攻击 8.1 DoS攻击 8.2 Access Point Overloaded攻击及对策 8.2.1 关于无线客户端状态 8.2.2 可能导致过载的原因及解决方法

<<无线网络安全攻防实战>>

8.3 Authentication Flood攻击及对策 8.3.1 关于连接验证 8.3.2 身份验证攻击原理 8.3.3 身份验证攻击实现及效果 8.3.4 管理员如何应对 8.4 Authentication Failure 攻击及对策 8.4.1 身份验证失败攻击定义 8.4.2 相关攻击工具及具体表现 8.4.3 管理员如何应对 8.5 Deauthentication Flood攻击及对策 8.5.1 攻击原理及步骤 8.5.2 攻击表现形式及效果 8.5.3 管理员应对方法 8.6 Association Flood攻击及对策 8.6.1 关联洪水攻击定义 8.6.2 攻击工具及表现 8.6.3 无线网络管理员应该如何应对 8.7 Disassociation Flood攻击及对策 8.7.1 攻击原理及步骤 8.7.2 攻击表现形式 8.7.3 管理员如何应对 8.8 Duration Attack 8.8.1 攻击原理及实现 8.8.2 应对方法 8.9 Wireless Adapter Driver Buffer OverFlow攻击及对策 8.9.1 无线网卡驱动溢出攻击定义 8.9.2 攻击涉及工具及资源 8.9.3 防御方法 8.10 RF Jamming攻击及对策 8.10.1 什么是RF Jamming攻击 8.10.2 可能面临的RF Jamming攻击 8.10.3 攻击者如何实现RF Jamming 攻击 8.10.4 如何检测RF冲突 8.10.5 管理员如何应对 8.11 Other Wireless Attack 类型第9章 绝对无敌与相对薄弱的矛盾体——VPN 9.1 VPN原理 9.1.1 虚拟专用网的组件 9.1.2 隧道协议 9.1.3 无线VPN 9.2 Wireless VPN 服务器搭建 9.2.1 在Windows Server 2003 下搭建无线VPN服务器 9.2.2 查看VPN服务器状态 9.3 无线接入点设置 9.4 Wireless VPN 客户端设置 9.5 攻击Wireless VPN 9.5.1 攻击PPTP VPN 9.5.2 攻击启用IPSec加密的VPN 9.5.3 本地破解VPN登录账户名及密码 9.6 强化VPN环境第10章 优雅地入侵：流动的War-Driving 10.1 永不消逝的电波 10.2 War-Xing概念 10.2.1 War-Driving 10.2.2 War-Biking 10.2.3 War-Walking 10.2.4 War-Chalking 10.2.5 War-Flying 10.2.6 War-Viewing 10.2.7 国内的War-Driving 10.3 War-Driving的准备工作 10.3.1 基本装备 10.3.2 NetStumbler & Kismet 安装 10.3.3 WiFiFoFum 安装 10.3.4 网卡改装 10.3.5 天线DIY 10.3.6 车辆改装 10.4 在城市里War-Driving 10.4.1 NetStumbler + GPS探测 10.4.2 WiFiFoFum + GPS探测 10.4.3 关于War-Walking 10.5 Hotspot (无线热点) 地图 10.6 使用Google + GPS绘制热点地图 10.6.1 主流探测工具及其输出文件格式 10.6.2 绘制热点地图操作指南 10.6.3 绘制自己的无线热点地图 10.7 结合热点地图进行远程攻击 10.7.1 远程无线攻击原理 10.7.2 远程无线攻击准备 10.7.3 实施无线远程攻击 10.7.4 防御方法 10.7.5 小结 10.8 War-Driving审计路线勘测 10.8.1 软件准备 10.8.2 PDA+GPS+GPS Tuner +Google Earth 10.8.3 其他注意事项 10.8.4 后记第11章 饭后甜点：也许有人同样会喜欢这些 11.1 已经出现的阴影 11.2 Wireless Camera/monitor 攻击 11.2.1 Wireless Camera 产品及介绍 11.2.2 Wireless Camera应用举例 11.2.3 攻击无线摄像设备 11.2.4 强化网络边界 11.3 PDA——WiFi 攻击 11.3.1 PDA的无线功能 11.3.2 攻击PDA等手持设备 11.3.3 结论 11.4 无线VoIP安全 11.4.1 发展的潜流——VoIP 11.4.2 无线VoIP攻击分类 11.4.3 改进现状 11.5 Wireless Spam (无线垃圾邮件) 11.5.1 关于垃圾邮件 11.5.2 国内垃圾邮件现状 11.5.3 基于无线网络的垃圾邮件 11.5.4 抵御来自无线网络的垃圾邮件 11.6 攻击无线打印机 11.6.1 什么是无线打印机 11.6.2 无线打印机和无线打印服务器 11.6.3 攻击打印机/打印服务器 11.6.4 保护内部打印设备第12章 抵御入侵者的可选方案 12.1 改进你的WLAN 12.1.1 WLAN 的基本安全配置 12.1.2 企业WLAN安全 12.1.3 不同用户按需选择 12.2 Wireless IDS & HoneyPot 12.2.1 关于IDS 12.2.2 Wireless IDS/IPS分类 12.2.3 无线IDS软件及方案 12.2.4 基于802.11的HoneyPot 12.3 无线安全防御汇总 12.3.1 常见无线网络安全隐患汇总 12.3.2 无线安全改进建议汇总 12.3.3 涉密补充第13章 向无线hackers致敬 13.1 各行业及领域无线网络部署现状 13.1.1 体育场馆无线接入方案 13.1.2 大学校园无线覆盖方案 13.1.3 运营商级无线接入方案 13.1.4 工厂无线网络摄像视频方案 13.1.5 无线社区实用方案 13.1.6 小结 13.2 无线安全技术前景展望 13.2.1 IEEE 802.11i——新一代WLAN安全标准 13.2.2 WAPI——中国提出的WLAN安全标准 13.2.3 无线安全的前景 13.3 Wireless Hack Timeline (无线黑客简史) 附录A BackTrack 2 Linux的硬盘安装附录B 部分无线网卡芯片及测试列表附录C 本书涉及的无线安全攻击及防护工具汇总附录D 中国计算机安全相关法律及规定

章节摘录

第1章 你所了解和不了解的无线世界 1.1 精彩的表面——无线网络现状 回想起并不遥远的以前，也就是4、5年前，在很多人为了给办公环境、酒店大厅及家庭SOHO的网络搭建、布线受到问题困扰时，无线网络作为一种新兴技术就已经开始崭露头角了。但由于当时无线设备过于昂贵，光是一张普通的802.11b无线网卡就能卖到1000元上下，更不用提其他的设备。

其高额的价格不但制约了人们接受无线网络的速度，还严重影响到了其自身的发展。

幸好，很多对无线网络报以极大期望的厂商和研究人员都注意到这一点，在经过不断尝试和改进后，随着技术的愈加成熟和成本的下降，无线网络终于开始走进大众视野。

在2007年，全球WiFi设备数量已超过7500万个，并且据估计在2008年，无线设备将再增加一倍。

现在，如图1.1所示的WiFi联盟认证，这个原本陌生的标识作为无线技术支持的象征，正开始频繁地出现在手机、PDA、笔记本和各种便携式设备上。

WiFi联盟（WiFi Alliance）是一家全球及非营利性的行业协会，拥有300多家成员企业，共同致力于推动无线局域网（WLAN）产业的发展。

以增强移动无线、便携、移动和家用设备的用户体验为目标，WiFi联盟一直致力于通过其测试和认证方案确保基于IEEE 802.11标准的无线局域网产品的可互操作性。

自2000年3月WiFi联盟开展此项认证以来，已经有超过4000种产品获得了WiFi CERTIFIEDTM指定认证标志，有力地推动了WiFi产品和服务在消费者市场和企业市场两方面的全面开展。

而无线局域网（Wireless Local Area Network，WLAN）具有可移动性、安装简单、高灵活性和扩展能力，作为对传统有线网络的延伸，在许多特殊环境中得到了广泛的应用。

随着无线数据网络解决方案的不断推出，“不论您在任何时间、任何地点都可以轻松上网”这一目标已经被轻松实现。

回顾国内无线网络的发展，可以直接从无线接入点数量的迅猛发展看出来，其完全可以用“与时俱进”来形容。

无论是在繁华的商业大街上、高新技术产业开发区，还是在大学校园、科研单位，亦或是政府、警务及部队所属机构，甚至是在普通家庭，无线网络经历了从无到有，直到现在星罗遍布的局面。除此之外，在一些行业性的无线项目中也已得到广泛应用，如：石油、矿山、集装箱码头等。

<<无线网络安全攻防实战>>

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>