

Broadview®
www.broadview.com.cn

“十一五”国家重点图书出版规划项目

SECURITY
ZeroOne



Advanced

Defensive Techniques

Wireless

无线网络安全 攻防实战进阶

Advanced Wireless Network Offensive & Defensive Techniques

 电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

• 杨哲 编著

“十一五”国家重点图书出版规划项目

SECURITY
ZeroOne

安全技术
大系

无线网络安全 攻防实战进阶

Advanced Wireless Network Offensive & Defensive Techniques

■ 杨哲 编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

面对当前国内企事业单位及 SOHO 无线网络的飞速发展、智能手机等便携式设备的广泛使用以及无线网络犯罪案例日益递增的发展现状,本书作为《无线网络安全攻防实战》一书的延续,依然以日趋严峻的无线网络安全为切入点,从当前不为多数人所知的无线网络欺骗攻击案例讲起,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 10 章,包括无线 RADIUS 认证体系搭建及攻防、蓝牙攻防实战、PDA/手机渗透及攻防实战、无线欺骗攻击深入实战、新技术高速破解、无线路由器攻防实战、无线网络犯罪取证、新型钓鱼等。

全书内容衔接《无线网络安全攻防实战》一书,不再重复基础内容环节,而是以全新深入内容及全新案例来提升读者的实际水平。本书可以作为军警政机构无线安全人员、专业网络安全公司安全人员、无线评估及规划人员、企业及电子商务无线网络管理员、警务人员计算机犯罪鉴定及现场分析的有力参考,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。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

无线网络安全攻防实战进阶 / 杨哲编著. —北京: 电子工业出版社, 2011.1
(安全技术大系)

ISBN 978-7-121-12096-1

I. ①无… II. ①杨… III. ①无线电通信—通信网—安全技术 IV. ①TN92

中国版本图书馆 CIP 数据核字(2010)第 207880 号

策划编辑: 毕 宁 bn@phei.com.cn

责任编辑: 许 艳

文字编辑: 张丹阳

印 刷: 北京市天竺颖华印刷厂

装 订: 三河市鑫金马印装有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本: 787×980 1/16 印张: 38 字数: 716 千字

印 次: 2011 年 1 月第 1 次印刷

印 数: 4000 册 定价: 69.00 元

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010) 88254888。

质量投诉请发邮件至 zllts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线: (010) 88258888。

**Have you ever seen a one trick pony in the field so happy and free?
If you've ever seen a one trick pony then you've seen me
Have you ever seen a one-legged dog making its way down the
street?**

**If you've ever seen a one-legged dog then you've seen me
Then you've seen me, I come and stand at every door
Then you've seen me, I always leave with less than I had before
Then you've seen me, bet I can make you smile when the blood, it
hits the floor**

**Tell me, friend, can you ask for anything more?
Tell me can you ask for anything more?**

**Have you ever seen a scarecrow filled with nothing but dust and
wheat?**

**If you've ever seen that scarecrow then you've seen me
Have you ever seen a one-armed man punching at nothing but the
breeze?**

**If you've ever seen a one-armed man then you've seen me
Then you've seen me, I come and stand at every door
Then you've seen me, I always leave with less than I had before
Then you've seen me, bet I can make you smile when the blood, it
hits the floor**

**Tell me, friend, can you ask for anything more?
Tell me can you ask for anything more?**

**These things that have comforted me, I drive away
This place that is my home I cannot stay
My only faith's in the broken bones and bruises I display
Have you ever seen a one-legged man trying to dance his way
free?**

If you've ever seen a one-legged man then you've seen me

你可曾见过一只在田野里欢快又自在小矮马？

如果你见过，那个就是我

你可曾见过一只在街上行走的独脚小犄？

如果你见过，那个就是我

如果你见过我，就知道我到过每扇门前

如果你见过我，就知道我拥有的东西已经日渐稀少

如果你见过我，当我的血滴在地上，我一定会让你笑出来。

告诉我，你就别无所求了吗？

你就别无所求了吗？

你曾见过一个身上只有生土和麦屑的稻草人吗？

如果你见过，那个就是我

你曾见过一个对着空气挥弄拳头的独臂男人吗？

如果你见过，那个就是我

如果你见过我，就知道我到过每扇门前

如果你见过我，就知道我拥有的东西已经日渐稀少

如果你见过我，当我的血滴在地上，我一定会让你笑出来。

告诉我，你就别无所求了么？

你就别无所求了么？

让我开怀的事情，已离我去

曾是我家的地方，已不能留

全身的伤痛和瘀青是我仅存的一切

你曾见过一个试着自由起舞的单腿男人么？

如果你见过，那个人就是我

——源自电影《摔跤手》(Wrestler) 主题曲《The wrestler》

前 言

随着国内各大运营商 3G 网络的普及，作为 3G 重要补充的 WLAN 无线网络，也已经被运营商广泛部署在各大中型城市。在面对当前国内运营商、企事业单位及 SOHO 无线网络的飞速发展、智能手机等便携式设备的广泛使用、无线网络犯罪案例日益递增的发展现状，本书作为《无线网络安全攻防实战》一书的延续，依然以日趋严峻的无线网络安全为切入点，从当前不为多数人所知的无线网络欺骗攻击案例讲起，由浅入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 10 章，包括无线 RADIUS 认证体系搭建及攻防、蓝牙攻防实战、PDA/手机渗透及攻防实战、无线欺骗攻击深入实战、新技术高速破解、无线路由器攻防实战、无线网络犯罪取证、新型钓鱼等。

全书内容衔接自由原作者撰写并于 2008 年 10 月出版的《无线网络安全攻防实战》一书，不过不再重复基础内容环节，而是以全新深入内容及全新案例来提升读者的实际水平。本书可以作为军警政机构无线安全人员、专业网络安全公司安全人员、无线评估及规划人员、企业及电子商务无线网络管理员、警务人员计算机犯罪鉴定及现场分析的有力参考，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。

和目前市面上一些注重理论化的无线安全书籍不同的是，本书作为“无线安全”系列书籍之一，笔者将一如既往地带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真正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的注意，甚至让一些人觉得有些不可理解的话，那么，摆在我们面前的事实是：在过去的数年期间，随着互联网中大量无线破解教程的普及，很多安全管理人员、网管员都已经对常见的无线加密破解手段比较了解，当然，这中间也有很多人认为所谓“无线黑客”也不过如此，所以又再次认为对无线设备进行基本的强化就可以避免无线网络的安全风险。为此，本书的目的就是再一次深入研究这些可能的攻击行为和方式，揭露其原理、工具、优缺点并给出防范方法，以便能够真正协助人们从认识到操作上逐步地理解无线安全，并逐步强化巩固好现有的无线网络。

希望这样一本重视实际操作的无线安全书籍可以帮助同样喜欢无线网络安全的朋友们少走弯路，也希望能为那些在无线网络安全领域进行安全研究的同行甚至专家提供一些支持和参考。

本书适合的读者

- 运营商通信部门安全人员、无线评估人员及规划人员、无线网络管理员；
- 军警政机构通信部门安全人员、无线评估人员、无线网络管理员；
- 企事业单位无线安全人员、无线网络管理员；
- 致力于无线网络安全技术的理论研究者；
- 无线产品开发人员；
- 高级黑客培训及国际网络安全认证课程讲师；
- 致力于学习高级网络安全技术的大中专院校学生；
- 所有无线黑客技术爱好者。

反馈与提问

读者在阅读本书时如遇到任何问题，可以到本书合作网站——中国无线门户网站 www.anywlan.com 论坛无线安全板块提问，同时读者可以从网站上找到本书中涉及的全部工具及其他一些有用的资料。

关于本书《无线网络安全攻防实战进阶》及其系列书籍之一的《无线网络安全攻防实战》的答疑修订、再版内容及更多深入无线安全技术信息，请关注我的个人博客 <http://bigpack.blogbus.com>。如有其他诸如研究、合作等事宜也可以通过博客与我联系，感谢大家的支持与关注。

致 谢

——仅以此书献给我辛劳宽容无以为报的母亲

一直以为本书作为“无线安全”系列的第二本书出版，会因为之前写作的经验变得简单，但自己还是高估了原以为能够支付的时间和精力。由于是第一本书的续篇，90%全新内容的撰写便超出了自己的预料，除去白天忙碌公司的各类安全项目外，常常会在实验到凌晨3、4点打着呵欠扑到床上睡几个小时，然后在公交车上一路睡到公司，亦或者在火车上、飞机上抱着笔记本敲着字睡着直到猛然惊醒，甚至坐在卫生间里我的脑海里都会不时浮现起书稿中一篇篇未完成的章节。前后花费了近一年的时间，中间由于负责项目几度中断，不过最终还是坚持完成了。回想起来，这本书的完稿除了自身的努力之外，真的离不开家人的包容和很多朋友们的鼓励与支持。

首先感谢我的家人，在我写书的日子，给予我最大程度的支持与鼓励。尤其是我的妻子，每当自己做实验到深夜看到她一个人陪着女儿静静地睡去，而平时在我写书时又默默地将家里琐事全部承担起来……回想起这一个个情景，我只想说：相信我，以后的日子一定会更美好。还有我的女儿丫丫，转眼间就要上幼儿园了，每当我抱着她坐在窗台上看着外面灯火辉煌的夜景时，我都会想，也许未来她终究不会如我所想般成为一流的女黑客，那也没有关系，只要她能过上自己喜欢的生活，开开心心的就好。

感谢挚友 Albert（徐枫），回想起过去几年一起努力、一起熬夜的点点滴滴，现在你终于步入婚姻的殿堂，谨以此书作为你幸福生活的真诚祝福。相信未来几年 ZerOne 无线安全团队在我们的共同努力下将会做得更好。

感谢小四（陈庆）哥的指点，能够和安全圈子里真正的高手交流是我的荣幸，你对技术一如既往的态度和对同伴真诚的笑容也使我不再迷茫，谢谢。

感谢 XCON 的组织者 Casper，能够在 xKungfoo2008 黑客大会上演讲给我带来了许多感触，见识到距离才知差距，接触到高手才会更加努力，谢谢你诚挚的邀请和交流。

感谢 PY（梁伟），这样的时刻怎能少了你光辉的身影。怀念在京城郊外小树林雨中观摩你练飞刀的日子，虽然有次弹回来差点扎了某人的腿。

还要感谢好友何国经，谢谢你的大力支持和鼓励，希望能和勤奋的你一起走得更远。

感谢中国无线门户网站 AnyWlan 的站长 Tange，谢谢你一直以来的信任和大力支持，同时也要对 AnyWlan 无线安全板块的各位朋友们一并表示感谢，谢谢你们的支持、鼓励和抨击，

和大家的探讨让我收益很多，希望你们继续支持和拍砖，同时也要感谢大家对无线 WPA 加密分布式破解测试的热情支持，也祝福各位能够在无线安全领域走得更远。

感谢 NSFocus 西北分公司的范挺、秋争超、王君、丁新荣等前辈的大力支持和鼓励，还有汤战勇、梁彪、张晟、刘炜，在 NSFocus 深受大家的照顾，和幽默的你们在一起总是让人感觉工作充满激情且轻松写意，谢谢大家。

感谢 NSFocus 西北区服务支撑组的许讯飞、陈伟同学，想起我们一起完成一个又一个安全项目、一起在无数个夜晚守在运营商机房通宵熬夜的日子，也真诚地祝愿你们能够攀上属于自己的高峰。

感谢 NSFocus 北京总部彼此相投的几位帅哥同事马志明、万慧星，以及初来绿盟对我照顾有加的几位美女同事吴梦珊、张昕、严娇雪，谢谢你们对我的支持与鼓励。还有“飞鹰队”的伙计们，宏宇、鹏飞……祝福你们。

感谢 Team509 的崔孝晨兄弟，还记得我们曾把酒言欢互诉衷肠，感谢老哥的鼓励与忠告，也祝愿你能够在技术和生活中找到期望的平衡点，兄弟可是对你的生活态度钦佩不已。

感谢无心呢喃（袁明坤）和 Kevin2600，很感谢在上海时无心呢喃的费心照顾，希望能再一起聚聚，交流一下，听听你自弹的吉他，也期待有机会能亲眼看看 Kevin2600 那深入人心的光头形象。

感谢宁夏省移动公司安全主管付雷和曲劲光先生，在安全项目里能遇到你们且得到你们的照顾是件很高兴的事情，谢谢你们为本书提供的支持和鼓励。

感谢韩国 IPTime 无线产品中国总代理广州三骏电脑的薛英凡大哥，在无线设备和其他设备上提供了许多便利，真的算是无线产品界前辈级人物，和你聊天总会有收获，希望以后的日子也不吝赐教。

感谢 SigLink 无线厂商提供的多款无线网卡支持，和廖先生的交流令人感慨，期待在未来的日子里能有更多的合作机会。

感谢昆山王峰通讯提供的多款无线网络设备支持，特别是赖先生的信任和支持，也祝新的无线设备能够在无线市场上大放异彩。

特别感谢电子工业出版社的毕宁，很感慨当初的相识，能遇见你这样的朋友是我的荣幸，也祝福果果，还有要对这本书的拖延说声对不起，谢谢你对我的容忍和包容，我知道我已多次挑战了你的极限，下次真的不会了。

感谢丹阳编辑，为这本书的顺利出版投入了很多心血，希望这本书能达到你预想的效果，另外，也怀念在 CNCERT2010 时与你、潘昕一起深夜加班的时光。感谢侯士卿美编的全身心投入，封面的设计麻烦你好多次才有了现在的效果，谢谢。

最后，再次感谢那些曾经鼓励我、安慰我、打击我、和我一起走过又离我而去的朋友们，真诚地感谢你们的陪伴。

杨 哲

于 2010 年 8 月 27 日晚

目 录

| | |
|---------------------------|----|
| 第 1 章 无线黑客的多项选择 | 1 |
| 1.1 开场：一些已经发生和正在发生的 | 1 |
| 1.1.1 国内运营商的无线部署现状 | 1 |
| 1.1.2 威胁来自何方 | 3 |
| 1.1.3 现实的面纱 | 8 |
| 1.1.4 看似遥远，实则可期 | 12 |
| 1.2 主流无线攻击技术回顾 | 12 |
| 1.2.1 攻击 WEP 加密无线网络 | 13 |
| 1.2.2 攻击 WPA 加密无线网络 | 21 |
| 1.2.3 小结 | 28 |
| 1.3 无线黑客的新选择 | 28 |
| 1.3.1 手机安全，新的战场 | 28 |
| 1.3.2 升级的无线攻击 | 31 |
| 1.3.3 全新的 GPU 技术 | 32 |
| 1.4 USB 移动攻防测试环境搭建 | 32 |
| 1.4.1 最简单的方法 | 33 |
| 1.4.2 关于 Unetbootin | 35 |
| 1.4.3 使用 Unetbootin | 37 |
| 第 2 章 推陈出新的攻击 | 41 |
| 2.1 关于 Aircrack-ng | 41 |
| 2.1.1 关于 Aircrack-ng 的版本 | 41 |
| 2.1.2 安装 Aircrack-ng | 42 |
| 2.1.3 Aircrack-ng 的其他相关工具 | 47 |
| 2.2 深入理解 Aircrack-ng 套装 | 47 |
| 2.2.1 关于 airdecap-ng | 47 |
| 2.2.2 关于 ivstools | 50 |
| 2.2.3 关于 airdriver-ng | 52 |
| 2.2.4 关于 airdecloak-ng | 55 |

| | | |
|---------------------|------------------------|------------|
| 2.3 | 破解 WEP 新工具 wesside-ng | 57 |
| 2.3.1 | 关于 wesside-ng | 57 |
| 2.3.2 | wesside-ng 的原理 | 57 |
| 2.3.3 | wesside-ng 操作实战 | 58 |
| 2.3.4 | 需要注意的问题 | 62 |
| 2.4 | 破解 WPA 新工具 Tkiptun-ng | 63 |
| 2.4.1 | 关于 Tkiptun-ng | 63 |
| 2.4.2 | Tkiptun-ng 原理 | 63 |
| 2.4.3 | 并不稳定的 Tkiptun-ng | 64 |
| 2.5 | WPS, 破解 WPA/WPA2 密钥的捷径 | 68 |
| 2.5.1 | 关于 WPS | 68 |
| 2.5.2 | 扫描开启 WPS 的无线设备 | 70 |
| 2.5.3 | 利用 WPS 破解 WPA/WPA2 密钥 | 74 |
| 2.5.4 | 延伸攻击 | 78 |
| 2.5.5 | 一些问题 | 80 |
| 2.6 | WPA 高速破解技术新趋势——显卡破解 | 81 |
| 2.6.1 | 关于 GPU | 81 |
| 2.6.2 | GPU 编程语言 CUDA | 83 |
| 2.6.3 | GPU 在安全领域的应用及发展 | 83 |
| 2.6.4 | 将 GPU 技术用于破解 | 86 |
| 2.6.5 | 关于 EWSA | 87 |
| 2.6.6 | EWSA 的使用准备 | 88 |
| 2.6.7 | 使用 EWSA 进行 WPA-PSK 破解 | 88 |
| 2.6.8 | 未注册 EWSA 的临时解决方法 | 92 |
| 2.7 | 其他的选择——分布式运算 | 95 |
| 2.7.1 | 无线加密 WPA 分布式破解项目 | 95 |
| 2.7.2 | 关于分布式架构 | 97 |
| 2.7.3 | 分布式的意义 | 98 |
| 第 3 章 无线欺骗攻击 | | 100 |
| 3.1 | 关于无线欺骗攻击 | 100 |
| 3.1.1 | 关于有线网络的中间人攻击 | 100 |
| 3.1.2 | 无线网络的中间人攻击原理 | 100 |
| 3.1.3 | 无线网络欺骗攻击 | 102 |
| 3.2 | 伪造 AP 攻击 | 102 |

| | | |
|--------------|---------------------|------------|
| 3.2.1 | 基于硬件的伪造 AP 攻击 | 102 |
| 3.2.2 | 基于软件的 FakeAP 攻击 | 102 |
| 3.2.3 | 深入的 MitmAP 攻击 | 106 |
| 3.3 | 无线欺骗利器——Airpwn | 110 |
| 3.3.1 | 关于 Airpwn 及攻击原理 | 111 |
| 3.3.2 | Airpwn 的安装 | 112 |
| 3.3.3 | 使用 Airpwn 进行无线中间人攻击 | 116 |
| 3.3.4 | Airpwn 的攻击效果 | 120 |
| 3.4 | 基于软件的无线跳板攻击 | 123 |
| 3.4.1 | 攻击原理 | 124 |
| 3.4.2 | 关于 aircserv-ng 工具 | 125 |
| 3.4.3 | 无线跳板实战 | 126 |
| 3.4.4 | 更高级的攻击方式 | 130 |
| 3.4.5 | 防范方法 | 131 |
| 3.5 | 基于硬件的无线跳板攻击 | 132 |
| 3.5.1 | 攻击原理 | 132 |
| 3.5.2 | 现场环境分析 | 133 |
| 3.5.3 | 跳板攻击实战 | 134 |
| 3.5.4 | 小结 | 140 |
| 3.6 | 新型钓鱼——WAPJack 攻击 | 140 |
| 3.6.1 | WAPJack 攻击原理 | 141 |
| 3.6.2 | WAPJack-DNS 欺骗攻击步骤 | 142 |
| 3.6.3 | WAPJack-DNS 欺骗攻击实战 | 142 |
| 3.6.4 | WAPJack-远程控制后门实战 | 148 |
| 3.6.5 | 防范方法 | 148 |
| 3.7 | 高复杂度的 WAPFunnel 攻击 | 150 |
| 3.7.1 | WAPFunnel 攻击原理 | 150 |
| 3.7.2 | WAPFunnel 攻击步骤 | 150 |
| 3.7.3 | WAPFunnel 攻击实战 | 151 |
| 3.7.4 | 如何防范 | 160 |
| 第 4 章 | 无线网络设备攻防 | 161 |
| 4.1 | 无线网络设备分类 | 161 |
| 4.1.1 | 胖 AP 与瘦 AP | 161 |
| 4.1.2 | 从功能上划分 | 162 |

| | | |
|-------|-----------------------|-----|
| 4.2 | 识别无线设备 | 163 |
| 4.2.1 | 无线网络设备指纹判断 | 163 |
| 4.2.2 | 基于 WPS 的判断 | 164 |
| 4.2.3 | 通过开启的端口判断 | 165 |
| 4.2.4 | 使用特定 ARP 报文探测 | 168 |
| 4.2.5 | 无线定位 | 169 |
| 4.2.6 | UPNP 探测 | 171 |
| 4.2.7 | SNMP 探测 | 172 |
| 4.3 | 内部无线网络设备的 MITM 攻击 | 173 |
| 4.3.1 | 针对内部无线网络设备的 MITM 攻击原理 | 173 |
| 4.3.2 | 确认无线网络设备 | 174 |
| 4.3.3 | MITM 中间人攻击实例 | 174 |
| 4.4 | DNS 缓存欺骗攻击 | 179 |
| 4.4.1 | 漏洞相关介绍 | 179 |
| 4.4.2 | 漏洞攻击代码 | 181 |
| 4.4.3 | 防范及建议 | 186 |
| 4.5 | 无线路由器认证会话劫持漏洞 | 186 |
| 4.5.1 | 漏洞相关介绍 | 186 |
| 4.5.2 | 漏洞利用与实现 | 187 |
| 4.6 | 登录验证绕过漏洞攻击 | 195 |
| 4.6.1 | 漏洞相关介绍 | 195 |
| 4.6.2 | 漏洞利用与实现 | 196 |
| 4.7 | 未经验证目录遍历漏洞 | 198 |
| 4.7.1 | 漏洞相关介绍 | 198 |
| 4.7.2 | 漏洞利用 | 199 |
| 4.7.3 | 防范方法 | 201 |
| 4.8 | UPnP Hacking | 201 |
| 4.8.1 | 关于 UPnP | 201 |
| 4.8.2 | 关于 UPnP 现状 | 202 |
| 4.8.3 | UPnP 管理工具 Miranda | 204 |
| 4.8.4 | UPnP Hacking 实战 | 205 |
| 4.9 | 来自 SNMP | 219 |
| 4.9.1 | 关于 SNMP | 219 |
| 4.9.2 | 攻击 SNMP | 220 |
| 4.9.3 | 改进与建议 | 222 |

| | | |
|--------|-----------------------|-----|
| 4.10 | XSS 跨站脚本攻击 | 223 |
| 4.10.1 | 漏洞相关介绍 | 223 |
| 4.10.2 | XSS 攻击实现 | 225 |
| 4.10.3 | 防范与建议 | 228 |
| 4.11 | config 文件泄露攻击 | 229 |
| 4.11.1 | config 文件未经验证泄露漏洞实战 | 229 |
| 4.11.2 | 分析并获取 config 文件泄露信息 | 231 |
| 4.11.3 | config 文件替换攻击 | 233 |
| 4.12 | 默认 WPA-PSK 连接密钥 | 236 |
| 4.13 | 恶意超长字符登录无响应漏洞 | 237 |
| 4.13.1 | 漏洞相关介绍 | 237 |
| 4.13.2 | 漏洞利用与实现 | 237 |
| 4.13.3 | 解决方法 | 239 |
| 4.14 | DHCP 服务洪水攻击 | 240 |
| 4.14.1 | 漏洞相关介绍 | 240 |
| 4.14.2 | DHCP Flood 攻击实现 | 241 |
| 4.14.3 | 防范方法 | 244 |
| 4.15 | 无线 D.O.S 攻击 | 244 |
| 4.15.1 | 关于无线连接状态 | 245 |
| 4.15.2 | 无线 D.O.S 工具 | 246 |
| 4.15.3 | 验证洪水攻击 | 251 |
| 4.15.4 | 取消验证洪水攻击 | 253 |
| 4.15.5 | 关联洪水攻击 | 256 |
| 4.15.6 | RF 干扰攻击 | 257 |
| 4.16 | 对某运营商无线节点设备渗透实战 | 259 |
| 4.16.1 | 渗透测试实战 | 260 |
| 4.16.2 | 小结 | 266 |
| 4.17 | 防范与加固 | 267 |
| 4.17.1 | 升级路由器的 Firmware 至最新版本 | 267 |
| 4.17.2 | 禁用 UPNP | 268 |
| 4.17.3 | 禁用 SNMP | 269 |
| 4.17.4 | 取消远程管理 | 269 |
| 4.17.5 | 修改 DHCP 默认设置 | 269 |
| 4.17.6 | 启用 MAC 地址过滤 | 270 |
| 4.17.7 | 关注最新安全漏洞及厂商补丁的发布 | 270 |

| | |
|---|-----|
| 第 5 章 无线数据解码与 IDS | 272 |
| 5.1 截获及解码无线加密数据 | 272 |
| 5.1.1 截获无线加密数据 | 272 |
| 5.1.2 对截获的无线加密数据包解密 | 273 |
| 5.2 分析无线数据——攻击者角度 | 278 |
| 5.2.1 关于分析工具 | 278 |
| 5.2.2 分析 MSN/QQ/Yahoo 聊天数据 | 279 |
| 5.2.3 分析 E-mail/论坛账户名及密码 | 280 |
| 5.2.4 分析 Web 交互数据 | 282 |
| 5.2.5 分析下载数据 | 287 |
| 5.3 分析无线数据——安全人员角度 | 288 |
| 5.3.1 识别 FTP 在线破解报文 | 289 |
| 5.3.2 识别 Web 在线攻击报文 | 290 |
| 5.3.3 识别扫描/溢出攻击报文 | 290 |
| 5.3.4 识别路由器非法登录报文 | 291 |
| 5.4 无线 IPS 替身——Airdrop-ng | 292 |
| 5.4.1 关于 Airdrop-ng | 293 |
| 5.4.2 Airdrop-ng 的安装 | 293 |
| 5.4.3 Airdrop-ng 的使用 | 297 |
| 5.4.4 Airdrop-ng 的规则编写 | 300 |
| 5.4.5 Airdrop-ng 的深入应用 | 303 |
| 第 6 章 高效低成本企业部署的主流：802.1X | 305 |
| 6.1 关于 802.1X | 305 |
| 6.1.1 关于 802.1X | 305 |
| 6.1.2 802.1X 认证过程步骤 | 306 |
| 6.1.3 802.1X 支持的认证类型 | 307 |
| 6.1.4 802.1X 和 IAS | 308 |
| 6.1.5 关于 AAA 与 RADIUS | 309 |
| 6.1.6 无线网络的 802.1X 安全和部署考虑事项 | 309 |
| 6.2 RADIUS 安装与注册 | 310 |
| 6.2.1 安装 IAS 服务器 | 310 |
| 6.2.2 让 IAS 服务器读取 Active Directory 内的用户账户 | 311 |
| 6.3 RADIUS 服务器设置 | 313 |
| 6.3.1 指定 RADIUS 客户端 | 313 |

| | | |
|--------------|------------------------------------|------------|
| 6.3.2 | Active Directory 用户的无线网络访问配置 | 315 |
| 6.3.3 | 为 IAS 服务器申请 RADIUS 证书 | 316 |
| 6.3.4 | 建立 RADIUS 无线访问策略 | 321 |
| 6.3.5 | 更改 RADIUS 无线访问加密类型 | 326 |
| 6.3.6 | Windows 2008 下 RADIUS 的安装及设置 | 327 |
| 6.4 | 无线接入点设置 | 328 |
| 6.4.1 | 配置内容 | 328 |
| 6.4.2 | 配置步骤 | 328 |
| 6.5 | RADIUS 客户端设置 | 330 |
| 6.5.1 | 客户端向 CA 申请用户证书 | 330 |
| 6.5.2 | 无线客户端证书的导出及导入 | 336 |
| 6.5.3 | 在无线客户端上进行无线连接设置 | 340 |
| 6.6 | IAS 服务器日志及排错 | 344 |
| 6.6.1 | 在 IAS 中启用日志功能 | 344 |
| 6.6.2 | 查看 IAS 日志 | 344 |
| 6.6.3 | IAS 常见问题排错 | 346 |
| 6.7 | 无线探测及攻击 | 348 |
| 6.7.1 | RADIUS 环境安全分析 | 348 |
| 6.7.2 | 针对 RADIUS 的其他攻击思路 | 352 |
| 6.7.3 | 第三方 RADIUS 服务器安全 | 355 |
| 6.8 | 依然存在的 D.O.S 威胁 | 357 |
| 6.8.1 | 攻击 RADIUS 认证的 EAP 环境 | 357 |
| 6.8.2 | 攻击 CISCO 的 LEAP 认证 | 360 |
| 第 7 章 | 蓝牙攻击，闪动蓝色微光的魅影 | 362 |
| 7.1 | 关于蓝牙 | 362 |
| 7.1.1 | 什么是蓝牙 | 362 |
| 7.1.2 | 蓝牙体系及相关术语 | 364 |
| 7.1.3 | 蓝牙适配器与蓝牙芯片 | 368 |
| 7.2 | 蓝牙配置实例 | 371 |
| 7.2.1 | 蓝牙（驱动）工具安装 | 371 |
| 7.2.2 | Windows 下蓝牙设备配对操作 | 373 |
| 7.2.3 | Ubuntu 下蓝牙设备配对操作 | 377 |
| 7.2.4 | 蓝牙的优势 | 380 |
| 7.3 | 扫描蓝牙设备 | 381 |

| | | |
|-------|-------------------------|-----|
| 7.3.1 | 识别及激活蓝牙设备 | 381 |
| 7.3.2 | 查看蓝牙设备相关内容 | 382 |
| 7.3.3 | 扫描蓝牙设备 | 383 |
| 7.3.4 | 蓝牙打印 | 388 |
| 7.4 | BlueBug 攻击 | 389 |
| 7.4.1 | 基本概念 | 389 |
| 7.4.2 | 工具准备 | 390 |
| 7.4.3 | 攻击实战步骤 | 391 |
| 7.4.4 | Linux 下自动攻击工具 | 398 |
| 7.4.5 | 防范方法 | 398 |
| 7.5 | BlueJack 与 BlueSnarf 攻击 | 399 |
| 7.5.1 | 原理与工具 | 400 |
| 7.5.2 | BlueJack 攻击实现 | 402 |
| 7.5.3 | BlueSnarf 攻击实现 | 403 |
| 7.5.4 | 修改蓝牙设备地址 | 405 |
| 7.6 | 未经验证泄露服务漏洞 | 406 |
| 7.6.1 | 漏洞描述 | 406 |
| 7.6.2 | 涉及设备 | 406 |
| 7.6.3 | 漏洞利用步骤 | 406 |
| 7.6.4 | PDA 及智能手机下攻击工具 | 414 |
| 7.6.5 | 无此漏洞的移动设备表现 | 416 |
| 7.7 | OBEXFTP 目录遍历漏洞 | 416 |
| 7.7.1 | 漏洞相关介绍 | 416 |
| 7.7.2 | 漏洞利用与实现 | 419 |
| 7.7.3 | 一些说明 | 425 |
| 7.7.4 | 防范方法 | 426 |
| 7.8 | 远程 OBEX 拒绝服务攻击 | 427 |
| 7.8.1 | 漏洞描述 | 427 |
| 7.8.2 | 漏洞实现 | 427 |
| 7.8.3 | 解决方法 | 430 |
| 7.9 | 破解不可见的蓝牙设备 | 430 |
| 7.9.1 | 什么是不可见 | 430 |
| 7.9.2 | 关于 Redfang | 431 |
| 7.9.3 | 使用 Redfang 进行破解 | 431 |
| 7.9.4 | 其他 | 434 |
| 7.10 | 远距离蓝牙攻击设备改装 | 435 |