Broadview
www.broadview.com.cn

“十一五”国家重点图书出版规划项目

SECURITY ZerOne

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

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

“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

電子工業出版社
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。

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 zlts@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鸡？

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尘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舞拳头的独臂男人吗？

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

全身的伤痛和疲倦是我仅存的一切

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真正黑客们致以发自心底的敬意。

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，在我写书的日子里，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很多感触，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