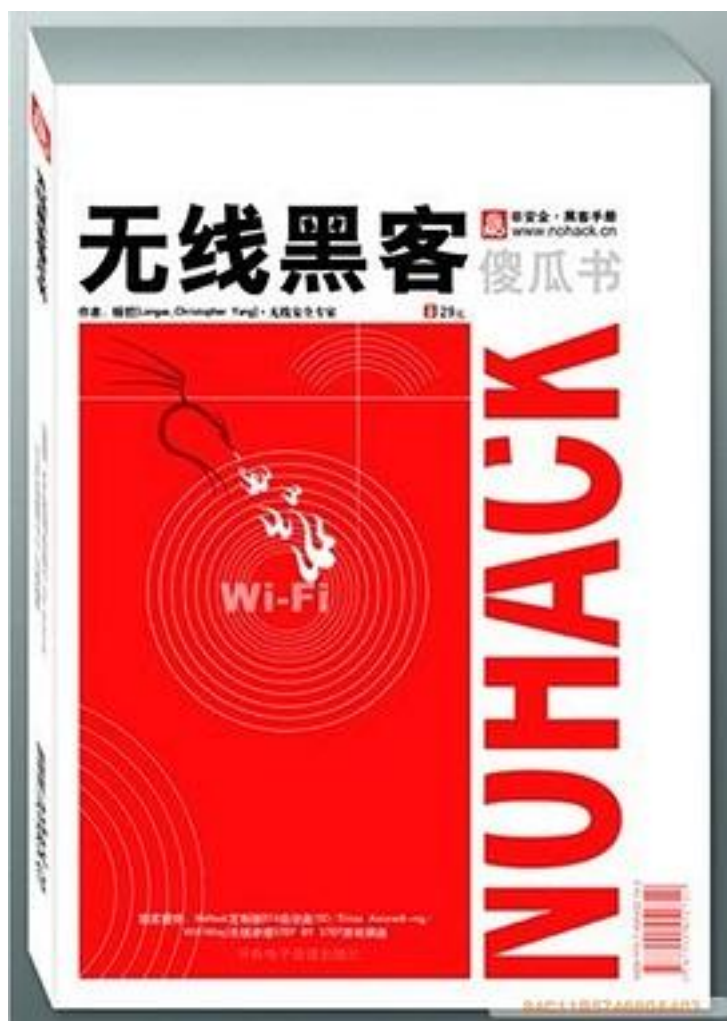


无线黑客傻瓜书



[无线黑客傻瓜书_下载链接1](#)

著者:杨哲

出版者:nohack

出版时间:2009

装帧:

isbn:9787900452740

Part0：幼稚园篇

卷1 无线基础知识扫盲.....	7
1.1 什么是无线网络.....	7
1.1.1 狭义无线网络.....	7
1.1.2 广义无线网络.....	9
1.2 蓬勃发展的无线城市.....	11
1.3 无线安全及Hacking技术的发展.....	12
卷2 常见无线网络设备.....	15
2.1 认识无线路由器.....	15
2.2 了解无线网卡.....	16
2.3 走近天线.....	17
2.4 其它.....	18
卷3 搭建自己的无线网络.....	19
3.1 WEP基础.....	19
3.1.1 关于WEP.....	19
3.1.2 WEP及其漏洞.....	20
3.1.3 WEP的改进.....	20
3.2 WEP加密设置和连接.....	21
3.2.1 配置无线路由器.....	21
3.2.2 Windows下客户端设置.....	22
3.2.3 Linux下客户端设置.....	23
3.3 WPA基础.....	26
3.3.1 WPA简介.....	26
3.3.2 WPA分类.....	26
3.3.3 WPA的改进.....	27
3.3.4 WPA 2简介.....	28
3.3.5 WPA面临日的安全问题.....	28
3.3.6 关于Windows下WPA2支持性.....	28

3.4 WPA-PSK加密设置和连接.....	28
3.4.1 配置无线路由器.....	29
3.4.2 Windows下客户端设置.....	30
3.4.3 Linux下客户端设置.....	30
卷4 无线黑客环境准备.....	32
4.1 适合的无线网卡.....	32
4.1.1 无线网卡的选择.....	32
4.1.2 无线网卡的芯片.....	33
4.1.3 总结整理.....	34
4.2 必备操作系统.....	35
4.2.1 BackTrack4 Linux.....	35
4.2.2 Slitaz Aircrack-ng Live CD.....	36
4.2.3 WiFiSlax.....	37
4.2.4 WiFiWay.....	37
4.2.5 其它Live CD.....	38
4.3 Vmware虚拟机下无线攻防测试环境搭建.....	39
4.3.1 建立全新的无线攻防测试用虚拟机.....	39
4.3.2 对无线攻防测试用虚拟机进行基本配置.....	41
4.3.3 了解你的无线攻防测试环境BT4.....	43
4.4 打造U盘版无线攻防环境.....	44

Part1：小学篇

卷5 搞定WEP加密.....	50
5.1 破解须知.....	50
5.2 WEP破解利器——Aircrack-ng.....	50
5.2.1 什么是Aircrack-ng.....	50
5.2.2 轻松安装Aircrack-ng.....	51
5.3 BT4下破解WEP加密.....	53

5.3.1 破解WEP加密实战.....	53
5.3.2 WEP破解常见问题小结.....	59
5.4 全自动傻瓜工具SpoonWEP2.....	60
5.4.1 关于SpoonWEP的分类.....	60
5.4.2 SpoonWEP2实战.....	61
卷6 搞定WPA-PSK加密.....	63
6.1 第二个破解须知.....	63
6.2 WPA破解利器——Cowpatty.....	64
6.2.1 什么是Cowpatty.....	64
6.2.2 轻松安装Cowpatty.....	64
6.3 BT4下破解WPA-PSK加密.....	66
6.3.1 破解WPA-PSK加密实战.....	66
6.3.2 使用Cowpatty破解WPA-PSK加密.....	69
6.3.3 WPA-PSK破解常见问题小结.....	70
6.4 全自动傻瓜工具SpoonWPA.....	71
卷7 自己动手，制作破解专用字典.....	74
7.1 制作破解专用字典.....	74
7.2 BackTrack2/3/4下默认字典位置.....	75
7.3 将字典上传至Linux下的方法.....	76
卷8 升级进阶必学技能.....	81
8.1 突破MAC地址过滤.....	81
8.1.1 什么是MAC地址过滤.....	81
8.1.2 让我们来突破MAC地址过滤吧.....	82
8.1.3 如何防范？	87
8.2 破解关闭SSID的无线网络.....	87
8.3 不再依赖DHCP.....	92

卷9 我在悄悄地看你.....	95
9.1 截获及解码无线加密数据.....	95
9.1.1 截获无线加密数据.....	95
9.1.2 对截获的无线加密数据包解密.....	95
9.2 分析MSN\QQ\Yahoo聊天数据.....	98
9.3 分析Email\论坛账户名及密码.....	99
9.4 分析WEB交互数据.....	100
9.4.1 当前访问站点.....	100
9.4.2 当前杀毒软件版本判断.....	101
9.4.3 当前操作系统判断.....	101
9.4.4 当前网络设备识别.....	102
9.5 外一篇：我不在咖啡馆，就在去咖啡馆的路上.....	103
卷10 渗透的快感	
10.1 扫描为先.....	104
10.1.1 NMAP & Zenmap.....	104
10.1.2 AMAP.....	106
10.1.3 Nbtscan.....	107
10.1.4 DNS Walk.....	107
10.2 密码破解.....	108
10.2.1 Hydra.....	109
10.2.2 BruteSSH.....	111
10.3 缓冲区溢出（Metasploit3）	112
10.3.1 关于Metasploit3.....	112
10.3.2 Metasploit3的升级.....	113
10.3.3 Metasploit3操作实践.....	114
卷11 无线D.O.S，看不见就被踢下线.....	117
11.1 什么是无线D.O.S.....	117

11.2 安装无线D.O.S工具.....	117
11.2.1 浅谈MDK 3.....	117
11.2.2 图形界面无线D.O.S工具——Charon.....	120
11.2.3 D.O.S攻击工具的使用.....	121
11.3 无线D.O.S也疯狂.....	122
11.3.1 关于无线连接验证及客户端状态.....	122
11.3.2 Auth Flood攻击.....	122
11.3.3 Deauth Flood攻击.....	125
11.3.4 Association Flood攻击.....	127
11.3.5 Disassociation Flood攻击.....	129
11.3.6 RF Jamming攻击.....	130

Part3: 大学篇

卷12 速度，职业和业余的区别.....	134
12.1 什么是WPA-PSK的高速破解.....	134
12.2 提升WPA-PSK破解操作实战.....	139
12.2.1 回顾Cowpatty套装.....	139
12.2.2 使用genpmk制作WPA Hash.....	139
12.3 WPA PMK Hash初体验.....	140
12.3.1 使用Hash进行WPA破解	140
12.3.2 测试数据对比.....	141
12.4 更快的方法——GPU.....	141
12.4.1 关于GPU.....	141
12.4.2 GPU编程语言CUDA.....	142
12.4.3 GPU在安全领域的应用及发展.....	143
12.4.4 将GPU技术用于破解.....	144
12.5 不得不提的EWSA.....	145
12.5.1 EWSA的使用准备.....	145

12.5.2 使用EWSA进行WPA-PSK破解.....	146
12.5.3 未注册EWSA的解决方法.....	147
12.6 其它的选择：分布式破解.....	149
12.6.1 关于分布式.....	149
12.6.2 无线WPA加密分布式破解第一轮公测.....	150
12.6.3 加入分布式的意义.....	151
卷13 影分身是这样练成的.....	151
13.1 伪造AP并不难.....	152
13.1.1 伪装成合法的AP.....	152
13.1.2 恶意创建大量虚假AP信号.....	153
13.2 搜索及发现伪造AP.....	154
13.3 给伪造分身加个护盾.....	160
卷14 无客户端破解，敏感的捷径.....	163
14.1 什么是无客户端.....	163
14.1.1 关于无客户端的定义.....	163
14.1.2 关于无客户端的破解.....	164
14.2 无客户端破解第一弹：Chopchop攻击.....	164
14.3 无客户端破解第二弹：Fragment攻击.....	166
Part4：研究生篇	
卷15 War-Driving，战争驾驶.....	169
15.1 什么是War-Driving.....	169
15.1.1 War-Driving的概念.....	169
15.1.2 了解Hotspot热点地图.....	170
15.1.3 War-Driving所用工具及安装.....	171
15.2 在城市里War-Driving.....	172
15.2.1 关于WiFiForm.....	172
15.2.2 WiFiForm + GPS探测.....	173

15.3 绘制热点地图操作指南.....	175
15.3.1 绘制热点地图.....	175
15.3.2 某运营商内部无线热点地图.....	177
15.3.3 国内某机场无线热点地图.....	178
15.3.4 某省会城市繁华地段无线热点地图.....	179
15.4 一些案例.....	180
15.4.1 远程无线攻击的原理.....	181
15.4.2 真实案例.....	181
卷16 蓝牙，看不见才更危险.....	183
16.1 无处不在的Bluetooth.....	183
16.1.1 什么是蓝牙？	183
16.1.2 蓝牙体系及相关术语.....	184
16.1.3 蓝牙适配器的选择.....	186
16.1.4 蓝牙（驱动）工具安装.....	186
16.1.5 蓝牙设备配对操作.....	187
16.2 玩转蓝牙Hacking.....	189
16.2.1 识别及激活蓝牙设备.....	189
16.2.2 查看蓝牙设备相关内容.....	190
16.2.3 扫描蓝牙设备.....	191
16.2.4 蓝牙打印.....	192
16.2.5 蓝牙攻击.....	193
16.2.6 修改蓝牙设备地址.....	194
16.3 破坏，蓝牙D.O.S	195
16.3.1 蓝牙D.O.S实战.....	196
16.3.2 蓝牙D.O.S会遇到的问题.....	198
16.4 破解不可见的蓝牙设备.....	199
16.4.1 什么是不可见？	199

16.4.2 关于Redfang.....	199
16.4.3 使用Redfang进行破解.....	200
16.4.4 其它.....	201
卷17 再玩点有意思的.....	202
17.1 Wifizoo.....	202
17.1.1 关于Wifizoo.....	202
17.1.2 Wifizoo的安装.....	202
17.1.3 如何使用Wifizoo.....	202
17.2 无线攻击跳板.....	205
17.2.1 关于无线跳板.....	205
17.2.2 Aircrack-ng+Fpipe.....	205
17.2.3 无线跳板实战.....	207
尾声：关于“ceng”的一些感想.....	209
附录：	210
A、无线网卡芯片列表.....	210
B、中国计算机安全相关法律及规定.....	211
C、本书附赠的《黑客手册》专版Backtrack 4 Linux DVD光盘简介.....	213
光盘目录.....	214

作者介绍:

目录:

[无线黑客傻瓜书 下载链接1](#)

标签

无线黑客傻瓜书

黑客

无线

信息安全

安全

计算机

hack

无线网络安全

评论

bt入门不错

看不懂

深入浅出(・ゝ・)所展示的版本有点旧

[无线黑客傻瓜书_下载链接1](#)

书评

在这里怎么看

[无线黑客傻瓜书_下载链接1_](#)