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

- 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

杨哲 ZerOne无线安全团队 编著

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！

YZLI0890107196

DVD

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

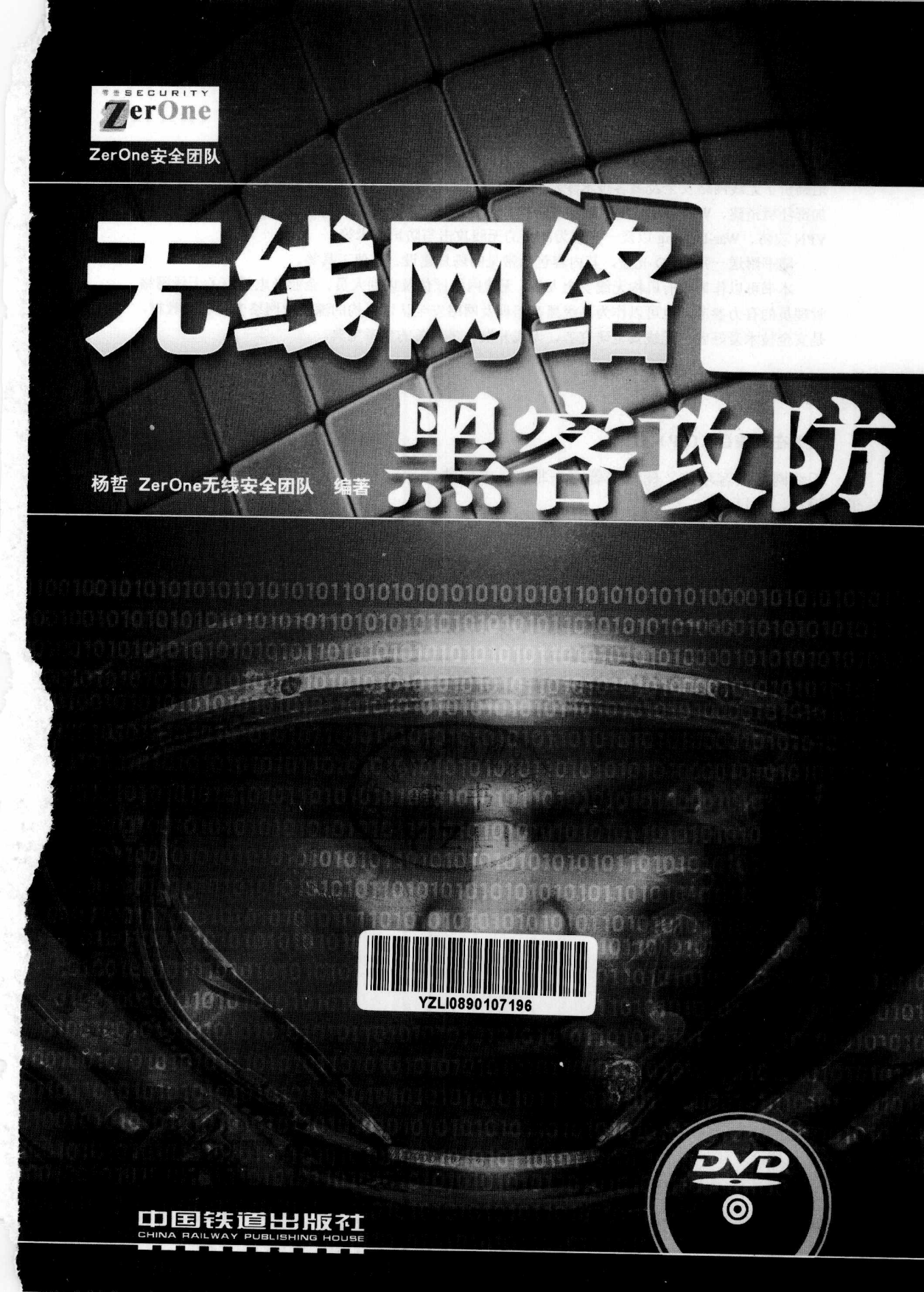
中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

SECURITY ZerOne

ZerOne安全团队

无线网络黑客攻防

杨哲 ZerOne无线安全团队 编著



DVD

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书以日趋严峻的无线网络安全为切入点，从常用的无线网络攻击环境搭建入手，循序渐进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，内容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。

随书附送一张 DVD 光盘，其内容包括常见的场景建设、超值工具等。

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

图书在版编目（CIP）数据

无线网络黑客攻防 / 杨哲编著. --北京：中国铁道出版社，2011.10

ISBN 978-7-113-13060-2

Ⅰ. ①无… Ⅱ. ①杨… Ⅲ. ①无线网－安全技术 Ⅳ. ①TN92

中国版本图书馆 CIP 数据核字（2011）第 155371 号

书　　名：无线网络黑客攻防
作　　者：杨哲　ZerOne 无线安全团队　编著

责任编辑：苏　茜　刘　伟　　**读者热线电话：010-63560056**
特邀编辑：赵树刚
封面设计：张　丽
责任印制：李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）
印　　刷：北京鑫正大印刷有限公司
版　　次：2011 年 10 月第 1 版　　2011 年 10 月第 1 次印刷
开　　本：787mm×1092mm　1/16　　印张：18　　字数：420 千
书　　号：ISBN 978-7-113-13060-2
定　　价：46.00 元（附赠光盘）

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本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

目 录

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）。

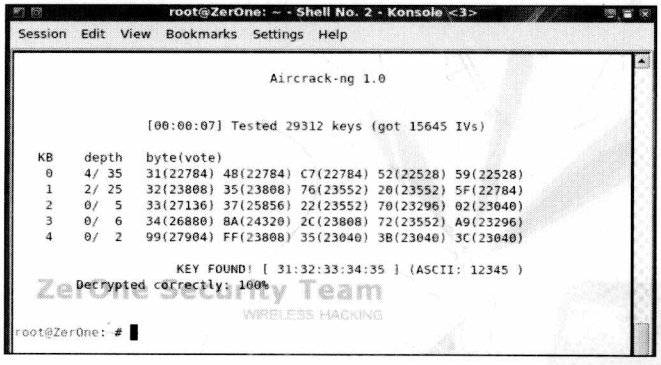


图 0-1

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）。

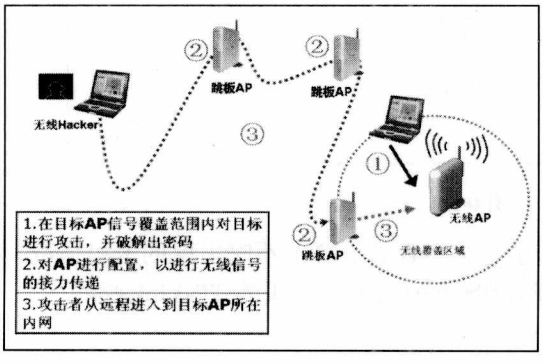


图 0-2

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。

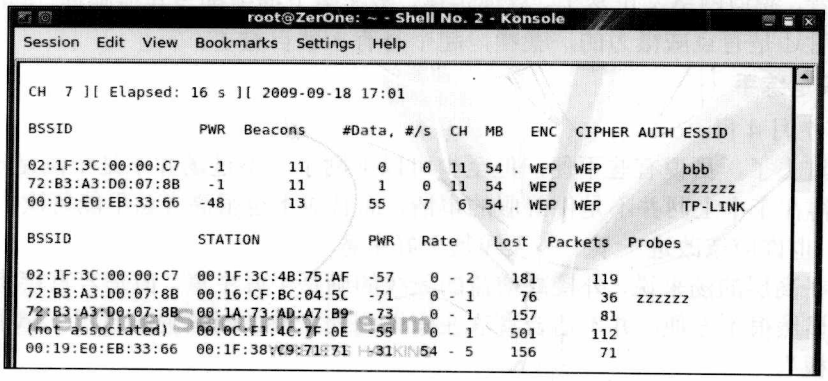


图 0-4

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。

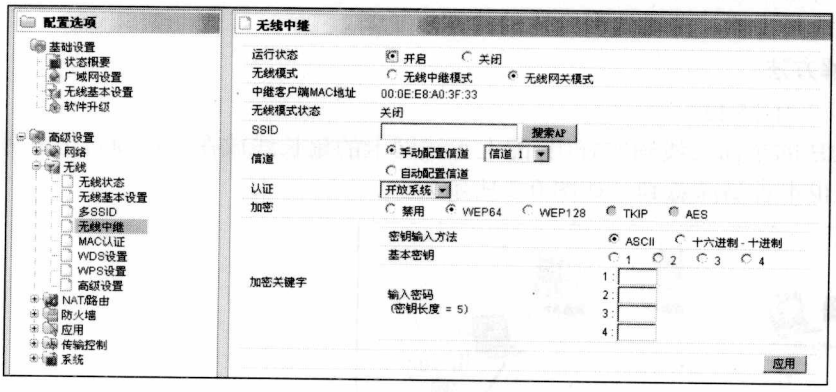


图 0-5

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。

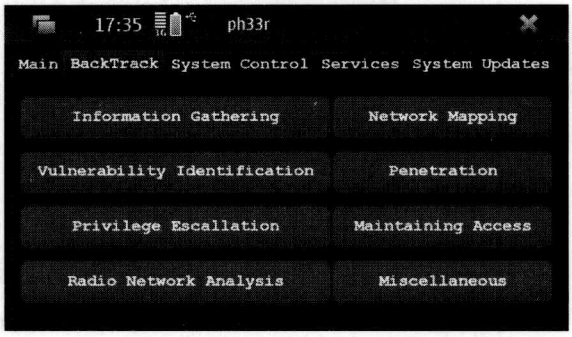


图 0-6

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”。

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）。

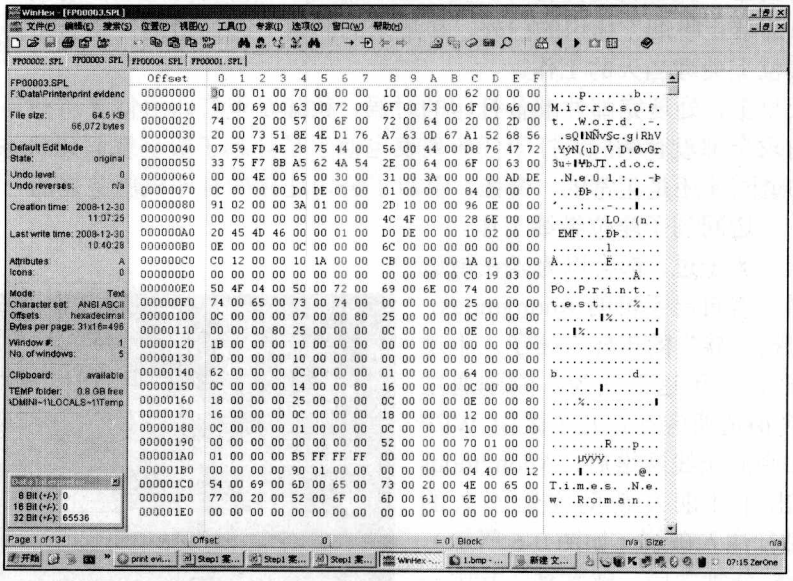


图 0-7

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@l0pht.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现场上用 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