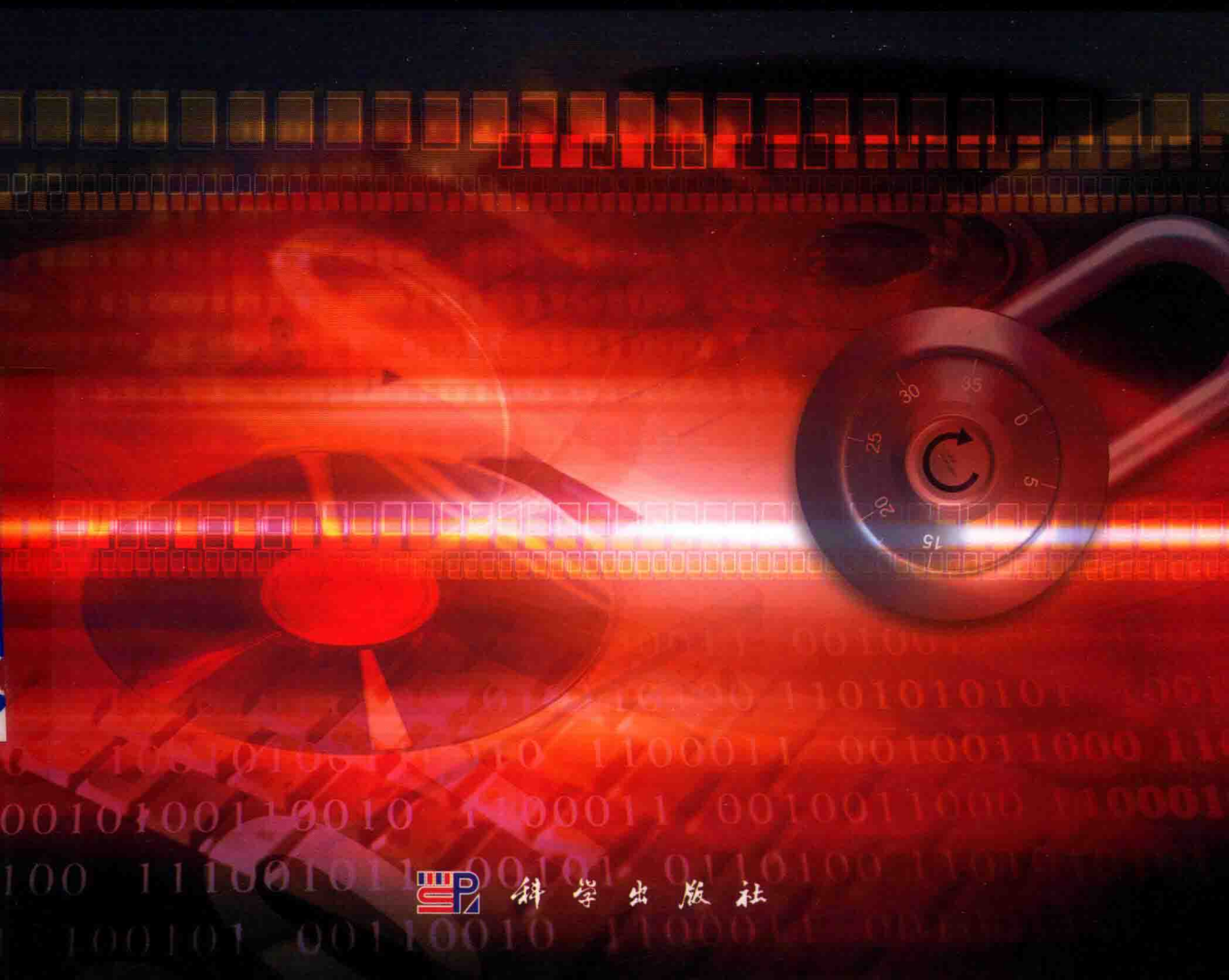
普通高等教育计算机创新系列规划教材·网络安全系列

网络安全攻防技术：移动安全篇

主编　苗刚中　罗永龙　陶　陶　陈付龙



科学出版社

普通高等教育计算机创新系列规划教材·网络安全系列

网络安全攻防技术：移动安全篇

主　编　苗刚中　罗永龙　陶　陶　陈付龙

副主编　石　雷　阚志刚　王涛春　殷梦蛟

科学出版社

北　京

内 容 简 介

本书从无线安全、移动安全以及移动物联网安全的基础理论、工作原理和实训实战等多个方面进行全面与系统的介绍，内容涵盖当前无线移动安全领域的核心技术，包括无线安全概述、无线加密技术、蓝牙安全技术、GPS 安全技术、移动终端系统安全攻防技术、Java 层和 Native 层的移动逆向技术、Android 程序的反破解技术、物联网关键技术、RFID 系统安全技术、无线传感器网络安全技术和智能终端网络安全攻防技术等。

本书理论联系实际，不仅可作为高等院校网络与信息安全、计算机科学与技术、软件工程和物联网等相关专业的教材，而且适合行业培训人员使用。与本书配套的实训平台是国内目前网络安全培训与学习课程中系统性较强的教学实训系统，且实训平台可用于读者自学。

图书在版编目（CIP）数据

网络安全攻防技术. 移动安全篇 / 苗刚中等主编. —北京：科学出版社，2018.12

普通高等教育计算机创新系列规划教材. 网络安全系列

ISBN 978-7-03-058327-7

Ⅰ. ①网… Ⅱ. ①苗… Ⅲ. ①计算机网络-网络安全-高等学校-教材 ②移动网-网络安全-高等学校-教材 Ⅳ. ①TP393.08 ②TN929.5

中国版本图书馆 CIP 数据核字（2018）第 271600 号

责任编辑：滕亚帆 王迎春 / 责任校对：桂伟利

责任印制：霍 兵 / 封面设计：华路天然工作室

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京市密东印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2018 年 12 月第 一 版 开本：787×1092 1/16

2018 年 12 月第一次印刷 印张：20 1/2

字数：490 000

定价：59.00 元

（如有印装质量问题，我社负责调换）

“普通高等教育计算机创新系列规划教材·网络安全系列”编委会

丛 书 序

当今时代大数据、云计算、物联网、移动网络技术等新技术已融入我们社会的方方面面。在造福国家和人民的同时，新技术也给我们提出了一系列新的课题，其中网络与信息安全是摆在我们面前亟需加强和解决的重要问题之一。2014 年 2 月 27 日，习近平总书记在主持召开的中央网络安全和信息化领导小组第一次会议上指出：没有网络安全就没有国家安全，没有信息化就没有现代化。

网络与信息安全是一个系统工程，其中网络安全人才的培养是其根本，这方面我国和西方发达国家相比还有不小的差距，存在诸多不足，具体体现在：开设网络安全专业的高水平院校不多，师资力量非常薄弱，缺乏高质量教材，教学系统性差以及学生实践环节欠缺等。面对我国的这一现状，习近平总书记曾指出：培养网信人才，要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建立一流的网络空间安全学院。这套“网络安全系列”教材从一定意义上讲也是贯彻习近平总书记这一指示的一个实践。

“网络安全系列”教材是在一套多年从事行业网络安全竞赛培训教材的基础上结合高校网络安全教育现状重新编写完成的，许多高校教师、网络安全专家、技术人员以及负责网络安全工作的领导，参加了这套系统的总体架构设计、选题及丛书的编写、校对、审稿和实训平台设备软硬件的设计、开发、测试等工作。梆梆安全公司、君立华域公司等国内从事信息安全实施和教育培训的龙头企业，以及网络与信息安全安徽省重点实验室、安徽省高等学校计算机教育研究会提供了大力支持。其体系架构、知识点、攻防技术曾多次被国家相关部委和部分省市工会、公安、通管局举行的网络与信息安全竞赛采纳和使用。

本套书包括三个部分和一套“高等学校网络安全实训平台”，各自自成体系，读者可以根据自己的需求和兴趣进行有选择性的学习：三个部分分别是系统安全篇、Web 安全篇、移动安全篇，从不同角度系统地介绍了网络安全体系架构中的安全基本概念、基础知识和攻防技术及手段，它既可以作为没有网络与信息安全技术基础人员的入门教材，也可以作为网络安全管理和工程技术人员的参考书，具有很强的实用性；高等学校网络安全实训平台作为本书的配套平台，供读者学习、实训使用，读者可以通过实际操作，有效提升自己的实战水平。

该书理论联系实际，且实训平台可用于读者自学，是国内目前网络安全培训与学习课程中系统性较强的教学实训系统，它不仅可以作为高等学校网络与信息安全专业的教材，也可作为行业培训的参考书。

2018 年 7 月 30 日

前　言

随着移动通信技术和移动应用的普及，无线网络、移动智能设备等正以前所未有的速度迅猛发展，已经渗透到了社会的各个方面，成为人们生产和生活不可或缺的工具和手段。此外，被誉为继计算机、互联网之后世界信息产业发展的第三次浪潮的物联网，亦得益于无线网络、无线感知技术的发展。与此同时，无线网络、移动智能设备所具有的开放性、结构复杂性等特点使其面临的安全威胁日益凸显。特别是如今移动电子商务和移动支付的广泛使用，使得移动智能设备成为各种恶意攻击的目标。因此，无线网络、移动智能设备的安全问题已成为当前世界范围内关注的焦点问题之一。

无线网络、移动智能设备的安全有别于传统的网络安全，这就对新时期网络信息安全教育和攻防技术提出了新的挑战。本书正是在这种背景下开始编撰的，以应对无线网络、移动智能设备安全方面的新挑战，填补相关网络信息安全教育和攻防技术的空白。本书共7章，从以下几个方面进行介绍：无线局域网、无线广域网和无线安全研究工具；移动恶意软件的分类、传播方式及典型行为，当前主要移动智能设备的操作系统 Android 系统的构架以及环境的安装等；移动智能设备安全、通信接入安全和系统安全等；移动逆向技术 Java 层和 Native 层的阐述；当前主要移动安全攻防技术，包括 Android 软件的破解技术、Android 程序的反破解技术、Android 系统的攻击和防范；物联网的体系结构、物联网关键技术和物联网的安全威胁；智能移动终端常用操作系统和智能终端安全攻防技术，同时列举了一些常见漏洞案例和常用工具。通过对上述内容核心技术全面与系统的介绍，读者可以了解并掌握移动安全、移动智能设备和物联网安全的基本概念、基础知识、常用工具和攻防技术。

本书由苗刚中、罗永龙、陶陶、陈付龙任主编，负责全书的体系结构、内容范围以及统稿、编著等组织工作，石雷、阚志刚、王涛春、殷梦蛟任副主编，负责主审和校对。其中第1章由罗永龙编写，第2章由陶陶编写，第3章由陈付龙、殷梦蛟编写，第4章由石雷、王涛春编写，第5章由王涛春、石雷编写，第6章由苗刚中、阚志刚编写，第7章由阚志刚、苗刚中编写。本书的文稿整理、图表编辑还得到了金鑫、王咪、汪逸飞、刘盈、宁雪莉、刘晴晴等研究生的协助，在此对他们表示感谢。

本书在编写过程中，得到了多位专家和信息安全企业技术人员的大力支持和帮助，他们提出了许多宝贵的建设性意见，在此谨向他们表示衷心的感谢。

限于时间仓促，书中难免存在一些疏漏和不妥之处，欢迎读者批评指正，以期不断改进。

编　者

2018年11日

目　录

第1章 无线安全

随着通信技术以及互联网技术的发展，无线网络技术凭借自身的优势逐渐得到了广泛的认知与认可，甚至演变成为一种热潮，无论企业商务还是家庭生活娱乐都体现出了对无线网络技术的需求。也正因为如此，无线网络技术展示出了极大的应用价值和良好的发展前景。本章将对无线网络安全进行简单介绍。

1.1 无线局域网

1.1.1 无线网络基础

无线安全是信息安全体系下一门很广泛的学科，包括但并不仅限于近场(NFC)、蓝牙(bluetooth)、射频(radio frequency, RF)、无线局域网(WiFi)、手机蜂窝网络(cellular)、卫星定位(GPS)等。无线传输在传输、认证、加密等方面，在各种设备对无线网络技术依赖的加深下变得越来越重要；随着物联网(IoT)的持续蓬勃发展，现在手机、智能设备对各类无线模块、传感器的需求也越来越大，蓝牙、GPS、NFC 模块成为必备项。从安全角度对无线网络技术的研究是很有必要的。

RTL-SDR、USRP、HackRF 及 BladeRF 等外设的价格下降，软件环境社区的完善，使现在对无线网络的研究已经不再像以前只能利用 2.4GHz 的无线网卡进行狭义的“无线”攻防。无线电通信安全将成为信息安全体系重要的一环。

什么是无线网络？无线网络(wireless network)是采用无线通信技术实现的网络。无线网络既包括允许用户建立远距离无线连接的全球语音和数据网络，也包括为近距离无线连接进行优化的红外线技术及射频技术，与有线网络的用途十分类似，最大的不同在于传输媒介不同，利用无线电技术取代网线，可以和有线网络互为备份。

1.1.2 无线网络的加密方式及破解

1. WEP 加密及破解

1) WEP 加密方式

有线等效保密(wired equivalent privacy, WEP)协议使用 RC4(rivest cipher 4)串流加密技术保证机密性，并使用 CRC-32 校验和保证资料的正确性，包含开放式系统认证(open system authentication)和共有键认证(shared key authentication)。

2) WEP 漏洞及破解

(1) 802.2 头信息和简单的 RC4 流密码算法。导致攻击者在有客户端并有大量有效通信时，可以分析出 WEP 的密码。

(2) 重复使用。导致攻击者在有客户端少量通信或者没有通信时，可以使用 ARP 重放的方法获得大量有效数据。

(3) 无身份验证机制，使用线性函数 CRC-32 进行完整性校验。导致攻击者能使用虚连接和 AP 建立伪连接，进而获得 XOR 文件。使用线性函数 CRC-32 进行完整性校验，导致攻击者能用 XOR 文件伪造一个 ARP 包，然后依靠这个包去捕获大量有效数据。

破解 WEP 加密的无线信号依赖两个因素：①信号强度；②是否有在线客户端。通过抓包、注入，然后获取密码，只要有这类信号就是百分之百可以破解的。

2. WPA 加密

1) WPA 加密方式

WPA 全称为 WiFi protected access，即 WiFi 网络安全存取，有 WPA 和 WPA2 两个标准，是基于有线等效加密中几个严重的弱点而产生的。WPA 加密方式目前有四种认证方式：WPA、WPA-PSK、WPA2、WPA2-PSK。

WPA 加密流程如下。

(1) 无线 AP 定期发送 beacon 数据包，使无线终端更新自己的无线网络列表。

(2) 无线终端在每个信道(1～13)广播 Probe Request(非隐藏类型的 WiFi 含 ESSID，隐藏类型的 WiFi 不含 ESSID)。

(3) 每个信道的 AP 回应，Probe Response，包含 ESSID 及 RSN 信息。

(4) 无线终端给目标 AP 发送 AUTH 包。AUTH 认证类型有两种：0 为开放式，1 为共享式(WPA/WPA2 必须是开放式)。

(5) AP 回应网卡 AUTH 包。

(6) 无线终端向 AP 发送关联请求包 Association Request 数据包。

(7) AP 向无线终端发送关联响应包 Association Response 数据包。

(8) EAPOL 四次握手进行认证(握手包是破解的关键)。

(9) 完成认证可以上网。

大致流程如图 1-1 所示。

2) WPA 破解

WPA 的 WiFi 密码破解分两种方法：抓包和跑 Pin 码。

(1) 抓包破解。WiFi 信号是加密的，登录无线路由器，就要向路由器发送一个请求，请求和无线路由器建立连接，这个请求就是一个包，名叫握手包，这个包里面包含了发送过去的一个密码，但是这个密码是加密的。抓包破解成功与否取决于以下四个方面：信号强度、是否有客户端在线、跑包的机器是否足够强大、字典是否好用。

抓包流程如图 1-2 所示。

(2) 跑 Pin 码破解。WPS(QSS 或 AOSS)功能是 WiFi 保护设置的英文缩写。对于一般用户，WPS 提供了一种相当简便的加密方法。通过该功能，不仅可将具有 WPS 功能的 WiFi

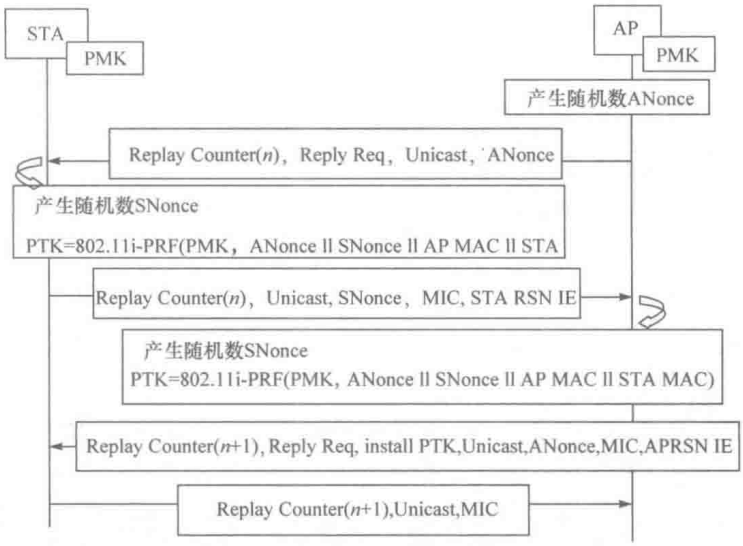


图 1-1 WAP 加密流程

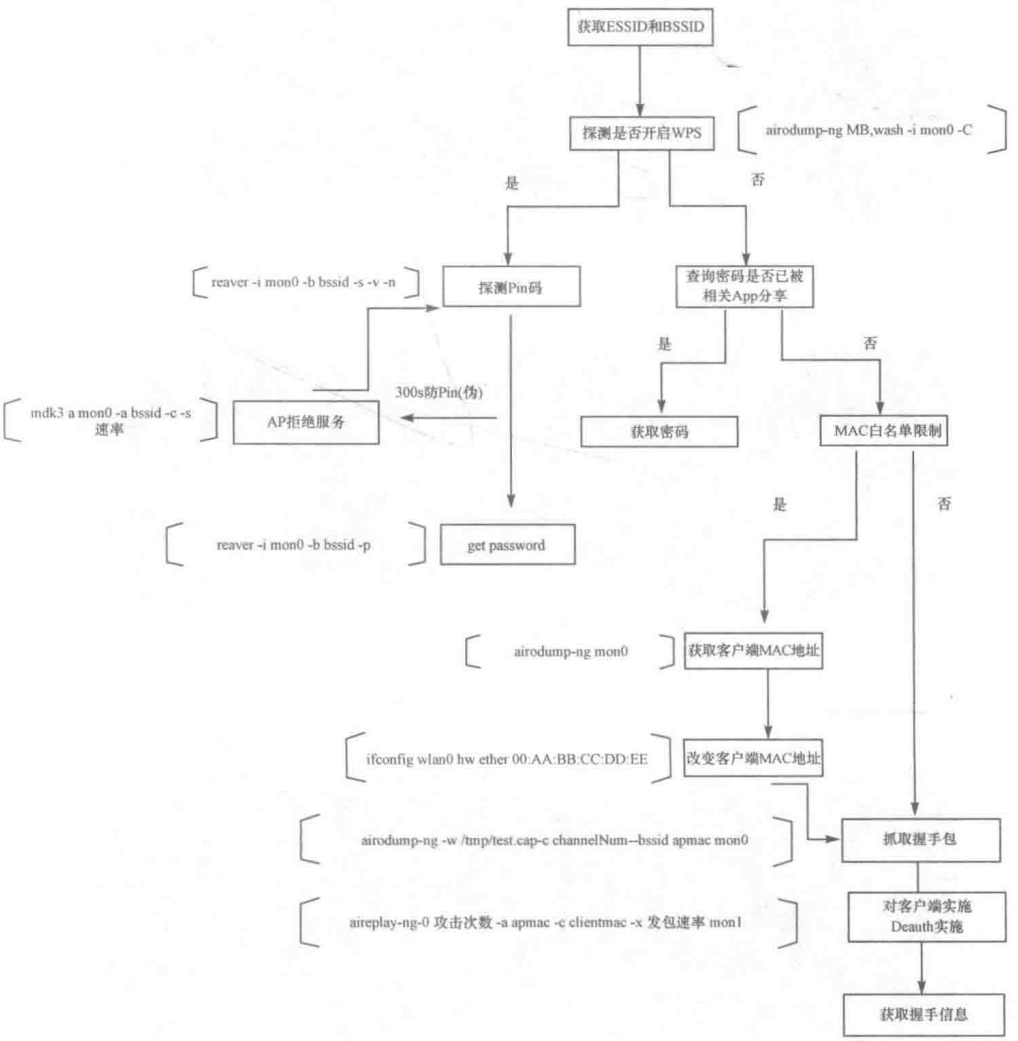


图 1-2 WAP 破解抓包流程

设备和无线路由器进行快速互连，还会随机产生一个八位数字的字符串作为个人识别号码(Pin)进行加密操作。省去了客户端需要连入无线网络时，必须手动添加网络名称(SSID)及输入冗长的无线加密密码的烦琐过程。

【例 1-1】　Kali 下 Aircrack-ng 套件破解 WiFi。

工具：wifite，minidwep，reaver。

实验环境描述如下。

基本信息：Kali Linux 2.0。

使用工具：Aircrack 套件。

实验过程如下。

第一步　插入破解网卡，并执行“虚拟机→可移动设备→连接主机”命令，输入 iwconfig 查看网卡列表，如图 1-3 所示。

```
root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0     IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.
```

图 1-3　网卡列表

第二步　输入 airmon-ng check kill 结束可能会影响结果的进程，如图 1-4 所示。

```
root@kali:~# airmon-ng check kill

Killing these processes:

  PID Name
 1060 dhclient
 1290 wpa_supplicant
```

图 1-4　输入 airmon-ng check kill

第三步　输入 ifconfig wlan0 up 激活无线网卡，输入 airmon-ng start wlan0 启动网卡到监听模式，如图 1-5 所示。

```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           rtl8187         NetGear, Inc. WG111v3 54 Mbps Wireless [realtek
RTL8187B]

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

图 1-5　启动监听模式

第四步 得到新的 monitor mode 下的网络接口 wlan0mon，开始监听周围无线网络：airodump-ng wlan0mon，如图 1-6 所示。

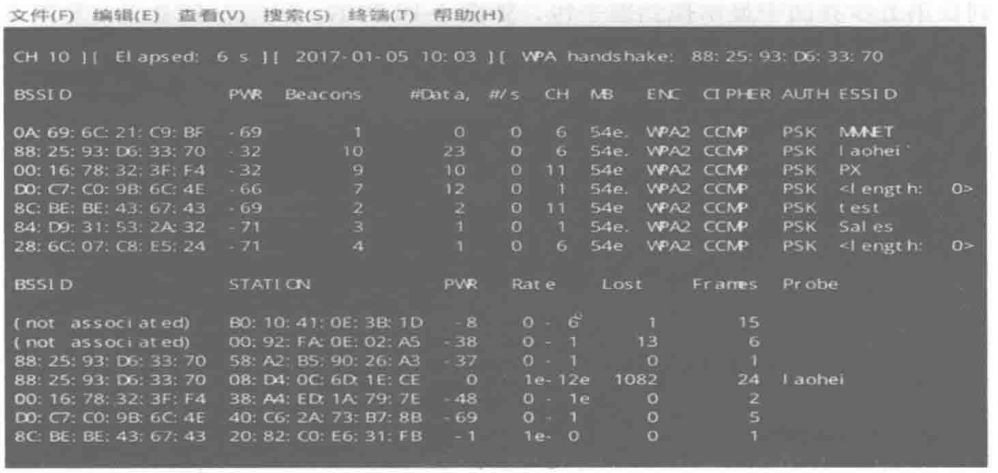


图 1-6 监听

第五步 按 Ctrl+C 键结束监听，下面的命令用于监听特定无线网(图 1-7、图 1-8)。

airodump-ng --bssid BSSID 下 MAC -c CH 行下的数字 -w 要保存的文件名 接口名

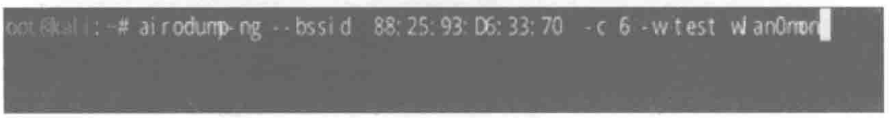


图 1-7 输入命令界面

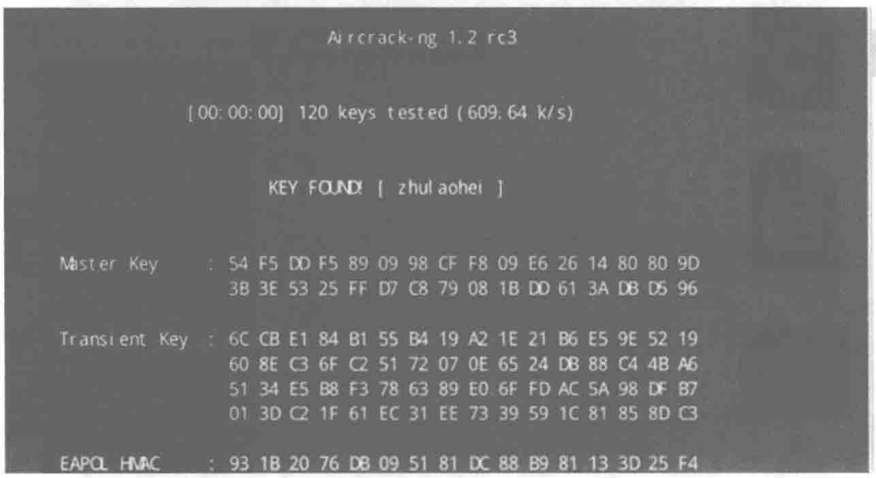


图 1-8 抓到的握手包

第六步 不关闭以上界面，另打开一个终端，开始 Deauth 攻击抓取 WPA 握手包(图 1-9)。

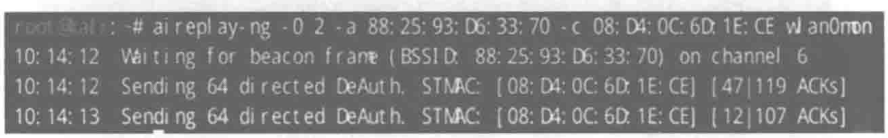


图 1-9 另开终端输入

```
aireplay-ng-0 2-a(BSSID下)-c(STATION下)wlan0mon
```

其中，-0 指 Deauth 攻击方式，2 指攻击次数。

直到在第五步界面中显示抓到握手包，如图 1-10 所示。

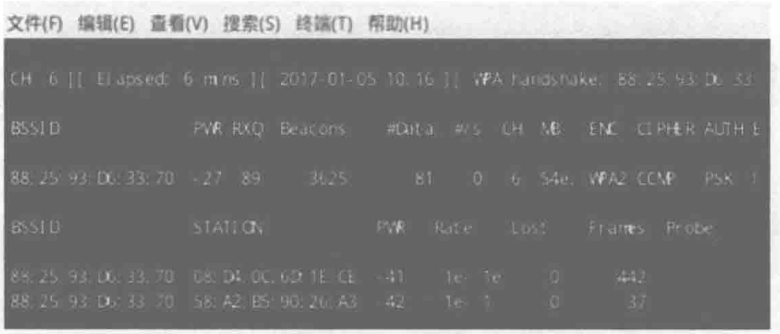


图 1-10　抓到握手包

发现在根目录/root 下出现三个数据包文件，这里需要的是 test-01.cap 文件，并创建自己的字典文件 passwd.txt，如图 1-11 所示。

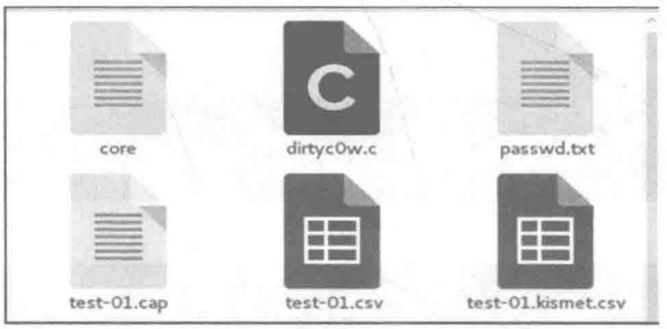


图 1-11　根目录

开始载入字典破解(图 1-12)：

```
aircrack-ng 数据包文件 -w 字典文件路径
```

图 1-12　输入界面

破解得到 WiFi 密码，如图 1-13 所示。

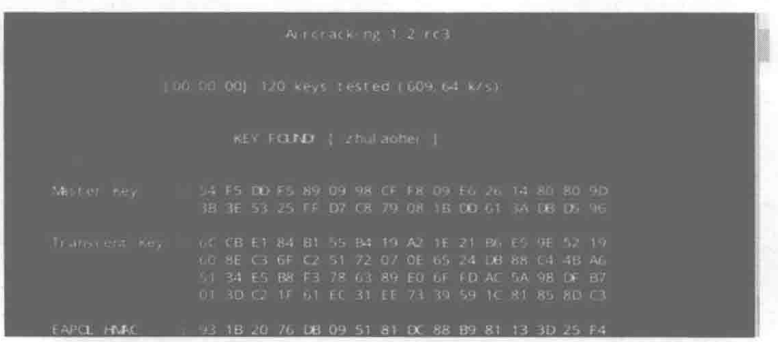


图 1-13　破解 WiFi 密码

【例 1-2】 利用 Fluxion 社工破解 WiFi 密码。

实验环境描述如下。

基本信息：Kali Linux。

使用工具：Fluxion。

实验过程描述如下。

第一步 以 Git 方式获得 Fluxion，并启动(图 1-14)，安装缺少的插件。

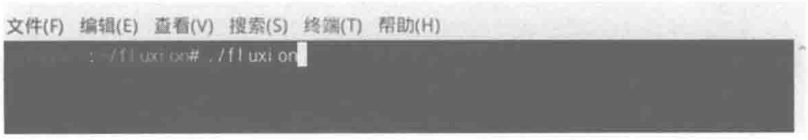


图 1-14 启动 Fluxion

第二步 选择语言，如图 1-15 所示。

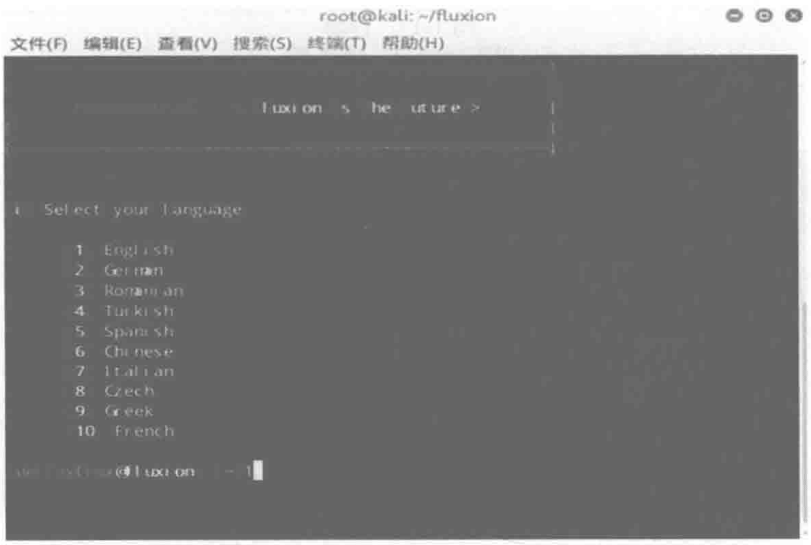


图 1-15 选择语言

第三步 选择网口及信道，如图 1-16 所示。

图 1-16 选择网口及信道

第四步　对网卡周围无线信号进行扫描，弹窗显示(图 1-17)，按 Ctrl+C 键结束。

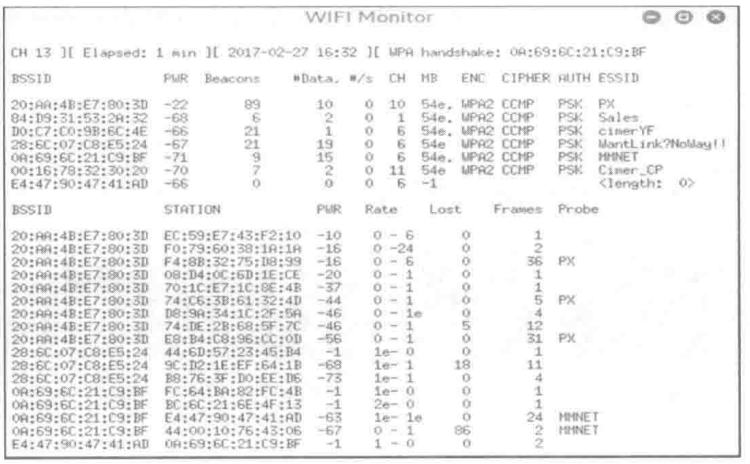


图 1-17　弹窗

第五步　选择网络，如图 1-18 所示。

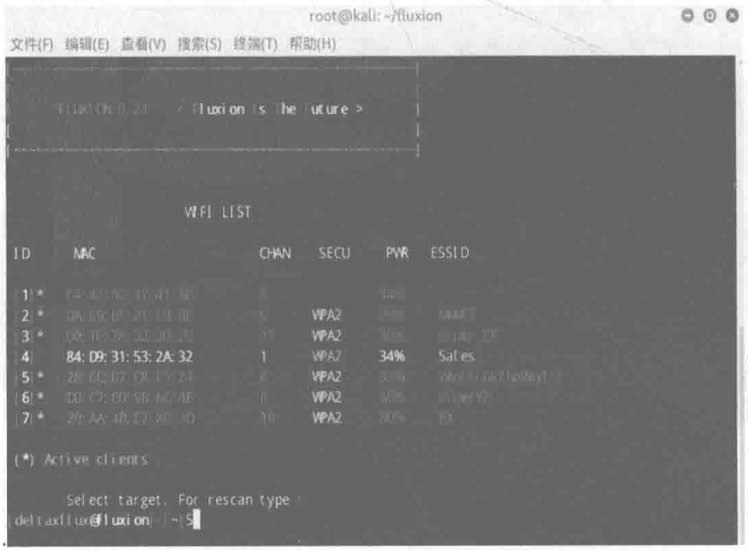


图 1-18　选择网络

第六步　选择抓取握手包，如图 1-19 所示。

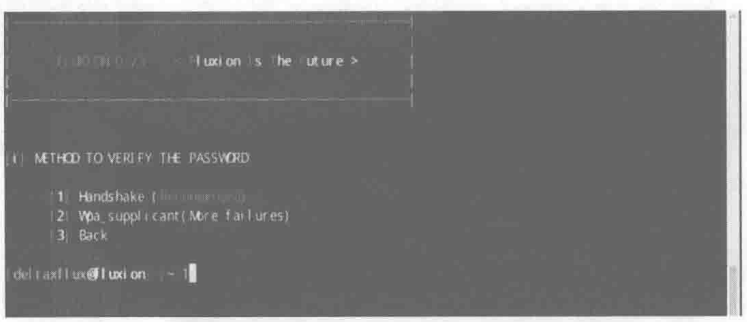


图 1-19　选择抓取握手包

第七步 选择数据包存放位置，按 Enter 键选择默认选项，如图 1-20 所示。

图 1-20 数据包存放

第八步 Aircrack-ng 套件破解，如图 1-21 所示。

图 1-21 Aircrack-ng 套件破解

第九步 握手包选项如图 1-22 所示，使目标 WiFi 的用户进行统一分配。

图 1-22 握手包选项

第十步 直到抓取到握手包，如图 1-23 所示。