**熟悉Kali系统，并整理Kali2.0自带的所有无线攻击软件的功能和用法**

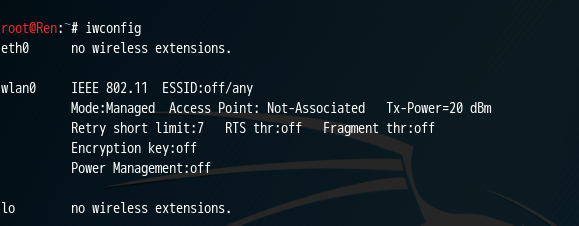
**1.在官网下载kali linux最新版，在VMware上安装配置。**



无线攻击相关软件



测试安装的无线网卡，成功被虚拟机中的kali系统识别（wlan0），并启动wlan0





**2.Aircrack-ng**

|  |  |  |
| --- | --- | --- |
| **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 |  |

Aircrack-ng是一款用于破解无线802.11WEP及WPA-PSK加密的工具，包含了多款工具的无线攻击审计套装， Aircrack-ng包含的组件具体列表如下。

**使用aircrack-ng工具集将无线网卡设置为混杂模式**

1. **启动混杂模式**

使用airmon-ng工具启动网卡的混杂模式，airmon-ng的语法格式如下：

airmon-ng <start|stop> <interface> [channel]

以上语法中个选项的含义：

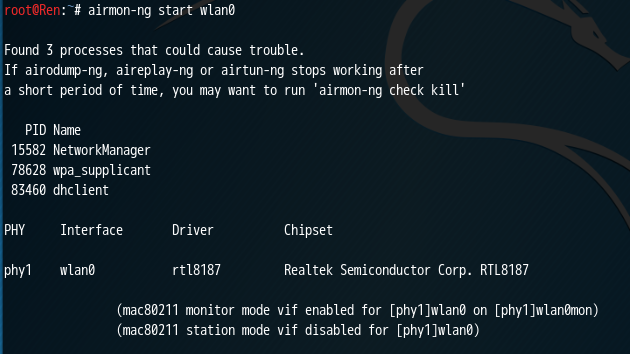
·start：表示将无线网卡设置为混杂模式

·stop：表示禁用无线网卡的混杂模式

·interface：指定无线网卡接口名称

·channel：在启动无线网卡为混杂模式时，指定一个信道

使用airmon-ng开启网卡的混杂模式



1. **扫描网络范围**

airodump-ng是用来捕获802.11数据报文的工具。通过查看捕获的报文，可以扫描附近AP的SSID（包括隐藏的）、BSSID、信道、客户端的MAC及数量等。

airodump-ng工具的语法格式如下：

airodump-ng [选项] <interface name>

其中几个常用的选项:

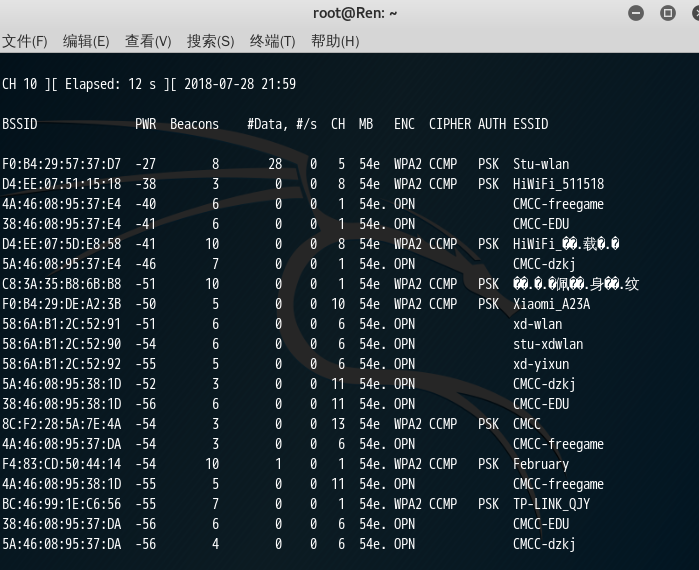
·-c：指定目标AP的工作信道

·-i,--ivs：用来设置过滤。指定该选项后，仅保存可用于破解的IVS数据报文，而不是保存所有无线数据报文，这样可以有效地减少保存的数据包大小

·-w：指定保存的IVS数据报文的文件名

·<interface name>：指定接口名称

使用命令airodum-ng wlan0mon查看扫描到的附近的wifi



1. **破解wifi密码**
2. 对**WEP**加密的网络进行破解：
3. 将无线网卡设置为混杂模式，并扫描附近的无线网络
4. 在扫描到的无线网络中，找到要攻击目标的BSSID，使用如下命令：

airodump-ng –ivs -w test –bssid aa:bb:cc:dd:ee:ff -c 6 wlan0mon

参数含义：

·--ivs：用于设置过滤，只保存可用于破解的IVS数据包

·-w：指定捕获数据包要保存的文件名（TEST）

·--bssid：用于指定攻击目标的BSSID（aa：bb：cc：dd：ee：ff）

·-c：指定攻击目标的信道（6）

注：这里指定捕获数据包的文件名为TEST，但实际上aircrack-ng为了后续方便调用这些文件，在每个文件名后加上了序号，这里假设TEST这组数据的文件名实际为TEST-01.ivs

1. 当捕获到数据包后，执行如下命令

aircrack-ng TEST-01.ivs

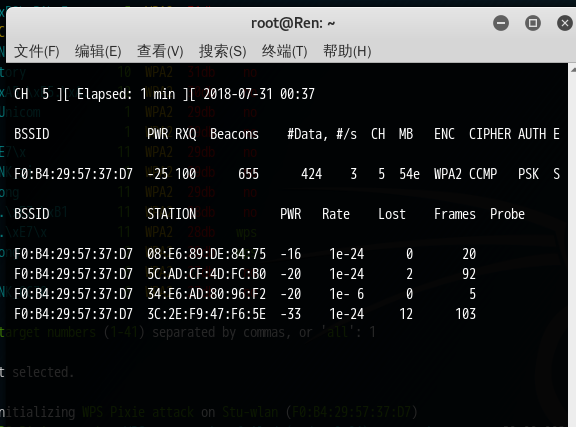
开始破解BSSID为aa：bb：cc：dd：ee：ff的无线网络密码。

1. 对**WPA**加密方式进行破解
2. 为了降低被发现的风险，可以更改无线网卡的MAC地址，在关闭混杂模式的前提下使用如下命令：

macchanger –mac 00:11:22:33:44:55 wlan0

1. 获取目标无线网络的数据包

airodump-ng –c 1 -w test –bssid aa:bb:cc:dd:ee:ff -c 6 wlan0mon



可看出有四个客户端连接了目标网络。在破解WPA加密的数据包中，必须捕获到握手包，即有新的客户端连接到网络时可以进行破解。

1. 如果没能捕获到握手信息，可使用aireplay-ng工具，语法格式如下：

aireplay-ng -0 1 -a AP’MAC -c client’s MAC wlan0mon

各参数含义如下：

·-0 1：0表示使用Deauth攻击模式，1表示攻击1次

·-a：指定AP的MAC地址

·-c：指定客户端的MAC地址

1. 攻击完成后将生成.cap文件，使用如下命令进行暴力破解：

aircrack-ng -w dic cap

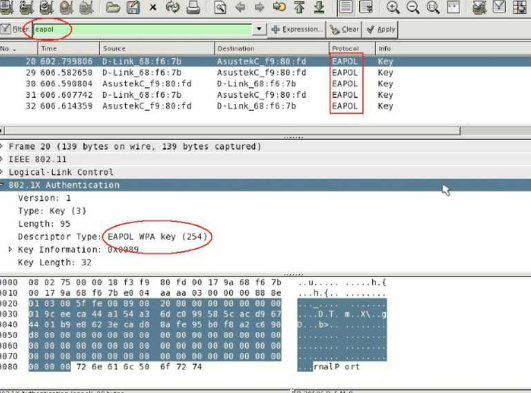
其中：

·-w：指定使用的密码字典

·cap即使用aireplay-ng捕获的数据包

1. **Cowpatty**

cowpatty是一款WPA-PSK字典攻击软件。具体使用步骤是首先使用Ethereal、wireshark等嗅探工具抓取包含WPA握手的cap文件，使用eapol进行过滤得到抓取的key数据



将抓到的数据包保存命名为wpa.cap，之后使用cowpatty进行破解，使用如下命令

Cowpatty -f passwd.txt -r wpa.cap -s AP’sSSID -v

其中：

-f是字典破解（暴力破解模式），passwd.txt为所用的字典文件；

-r 后面跟WPA验证的抓包文件

-s 后面跟检测到的AP的ESSID

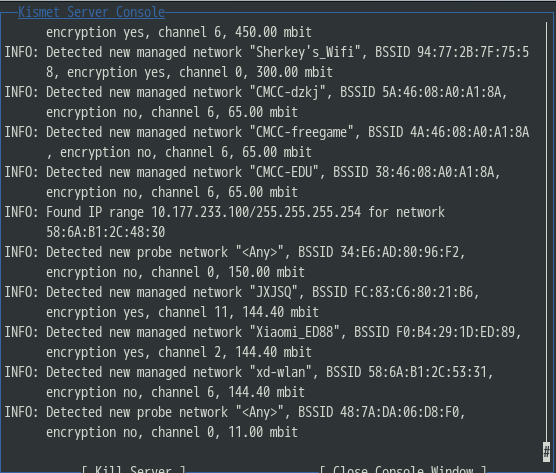
-v 显示详细过程

1. **使用kismet扫描**
2. **Kismet简介**

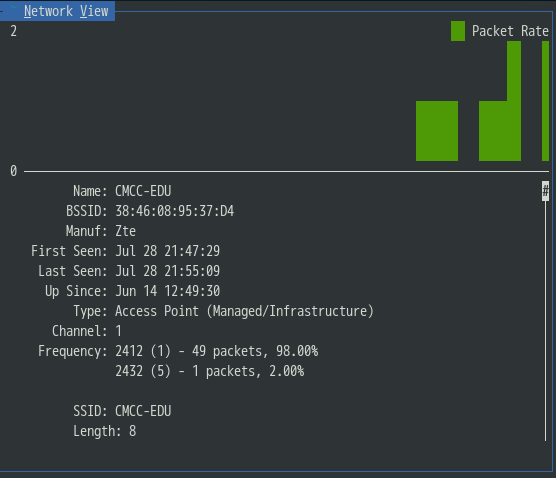
Kismet是一个图形化的无线网络扫描工具。该工具通过测量周围的无线信号，可以扫描到附近所有可用的AP及所使用的信道等。Kismet不仅可以对网络进行扫描，还可以捕获网络中的数据包到一个文件中，方便用户对数据包进行分析使用。

在终端中执行kismet：

附近的无线wifi信息



可以看到某个网络的详细信息



1. **使用wireshark捕获数据包**
2. **无线网络数据包简介**

包（packet）是TCP/IP协议通信传输中的数据单位，一般数据包可分为三类：握手包、加密包和非加密包。

握手包：WiFi中的握手包指的是使用WEP或WPA加密方式的无线AP与无线客户端进行连接前的认证信息包；

非加密包：在WiFi网络中无线AP没有开启无线安全时传输的包，捕获到后可直接进行分析；

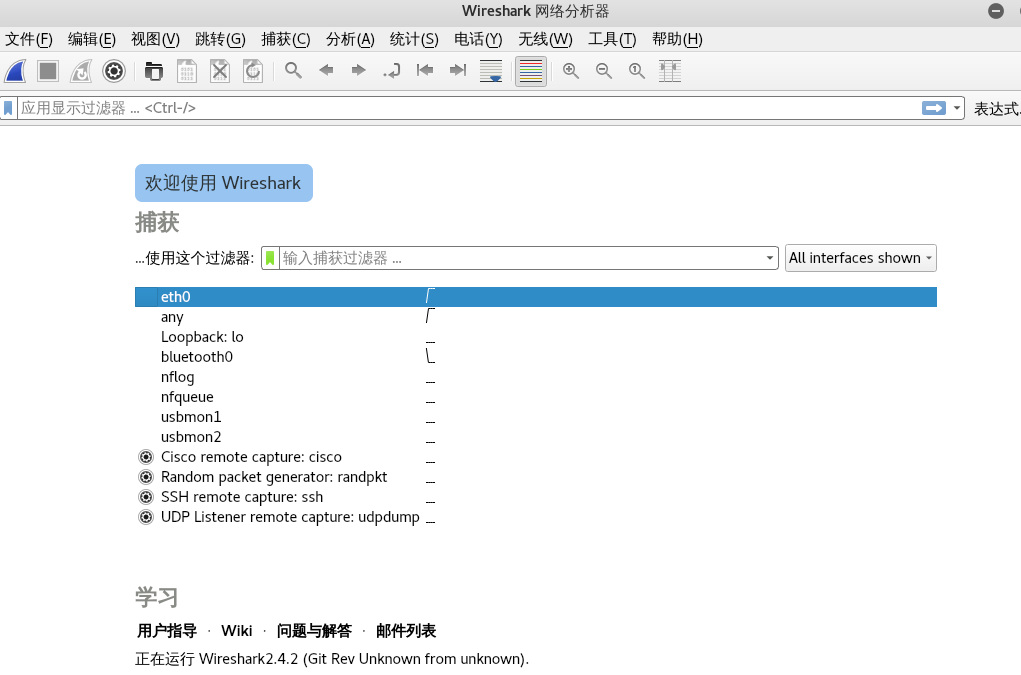
加密包：IEEE802.11提供了三种加密算法，分别是有线等效加密（WEP）、暂时密钥集成协议（TKIP）和AES-CCMP。当无线AP采用加密方式时，捕获的数据包都会被加密。

1. **使用wireshark捕获数据包**

Wireshark是常用的网络封包分析软件。

**捕获数据包的步骤：**

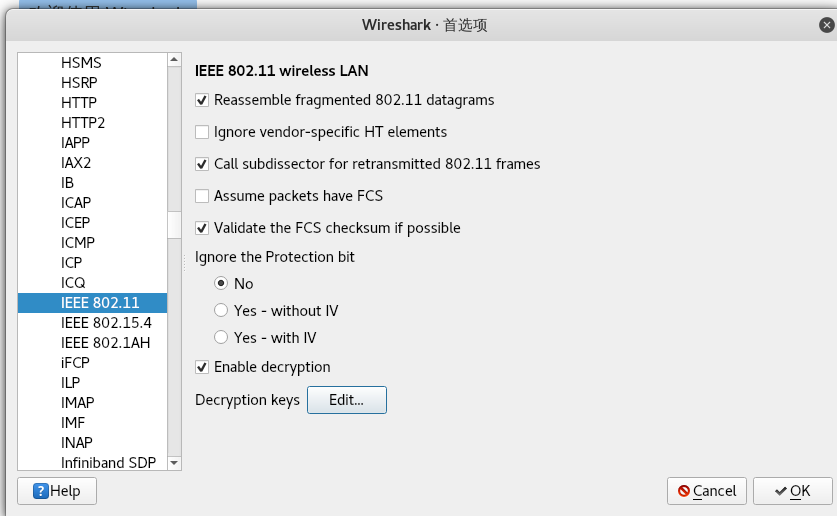
1. 使用airmon-ng工具启动混杂模式
2. 开启wireshark，选择无线网卡进行监听



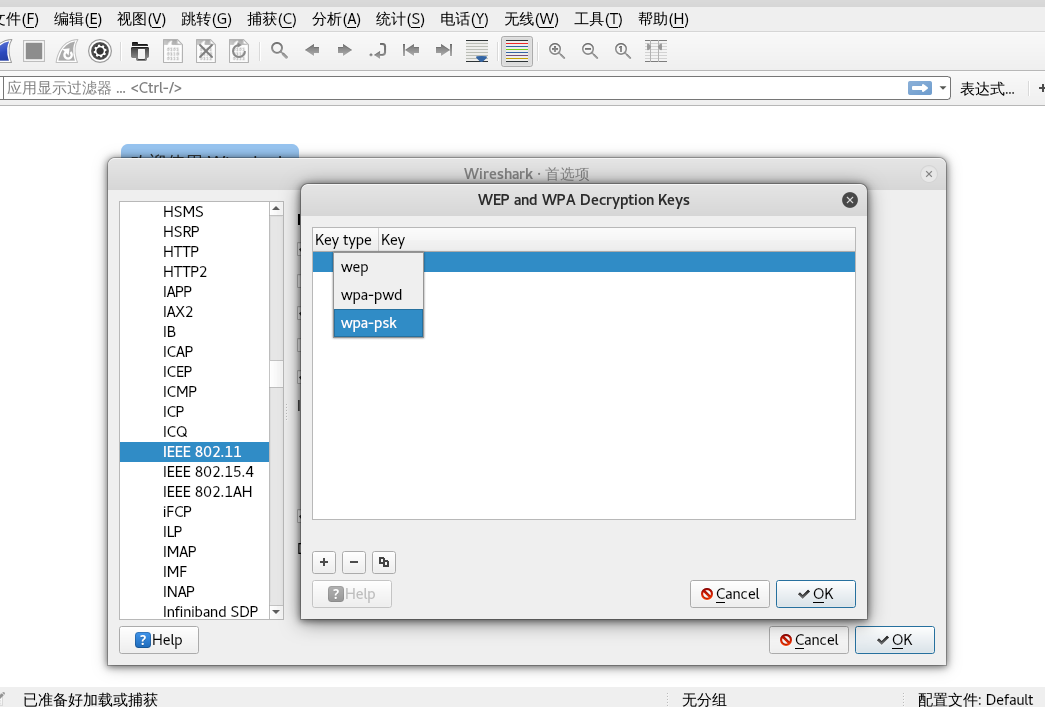
（wireshark启动后，暂无无线网卡端口，后续补上）

**捕获加密模式的数据包后的解密方法：**

1. 在wireshark的工具栏中选择编辑（Edit）🡪首选项（preference），展开protocols选项选择IEEE802.11。



勾选Enable decryption，并编辑密钥。

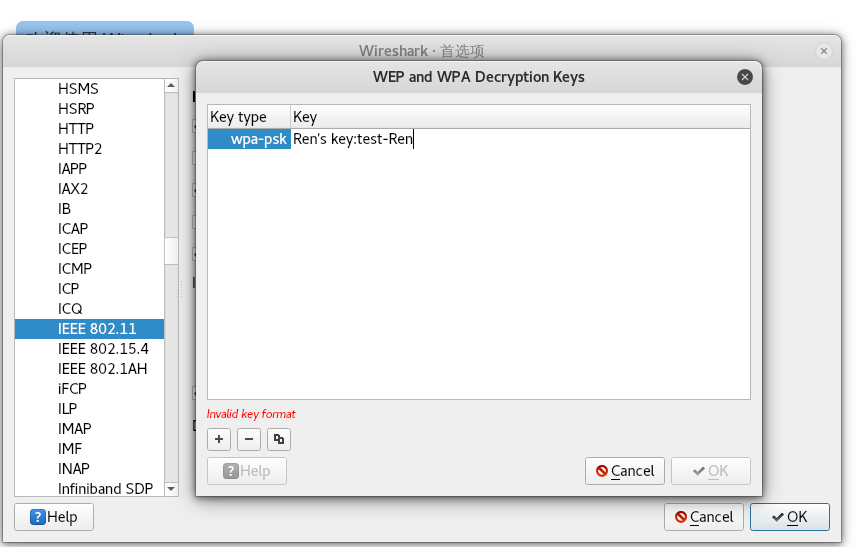


可看出有三种密钥类型wep、wpa-pwd和wpa-psk。以wep协议为例，依据WiFi密码输入密钥，注意输入的密钥格式为十六进制的ASCII值，如密码123456对应31:32:33:34:35。返回捕获数据包界面，可以发现加密的数据包被成功解密。

**捕获WPA-PSK/WPA2-PSK加密模式的数据包：**

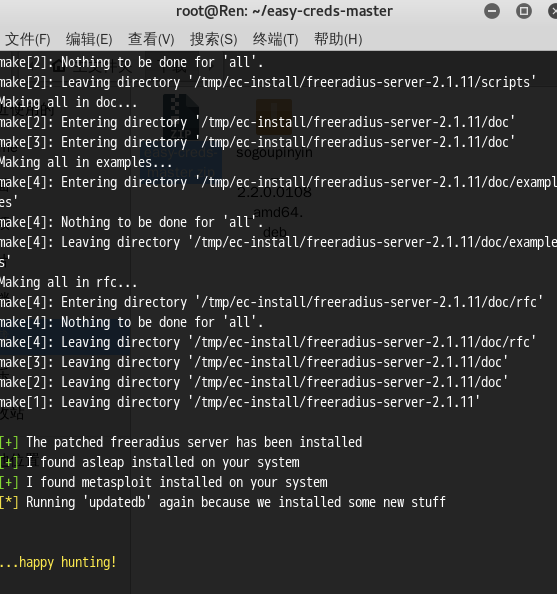
WPA-PSK/WPA2-PSK是WPA协议的简化版。WPA加密方式相较于WEP更安全，因为它改变了密钥的生成方式，更频繁地改变密钥以获得安全。另外增加了消息完整性检查防止数据包伪装。

因此在wireshark捕获的所有加密的包（协议为802.11的包）中解密以WPA加密的包，需要输入的密钥格式为：密码:BSSID。

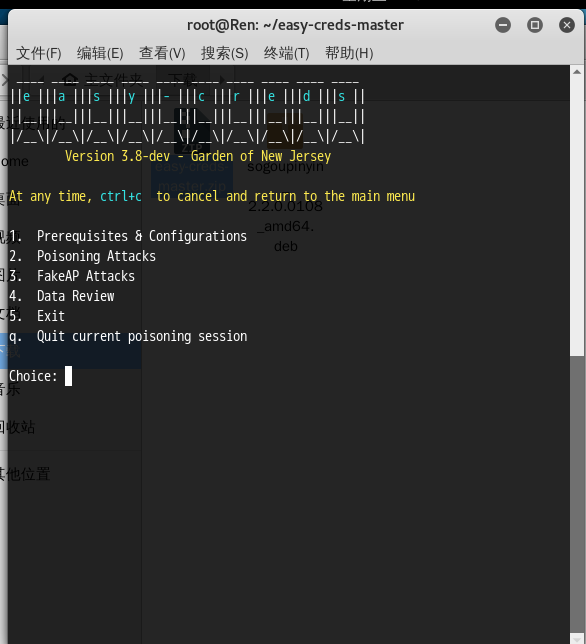


1. **开始创建伪AP**

我们使用的工具为Easy-Creds。通过URL：[https://github.com/brav0hax/easy-creds](https://github.com/brav0hax/easy-creds的) 安装该工具。

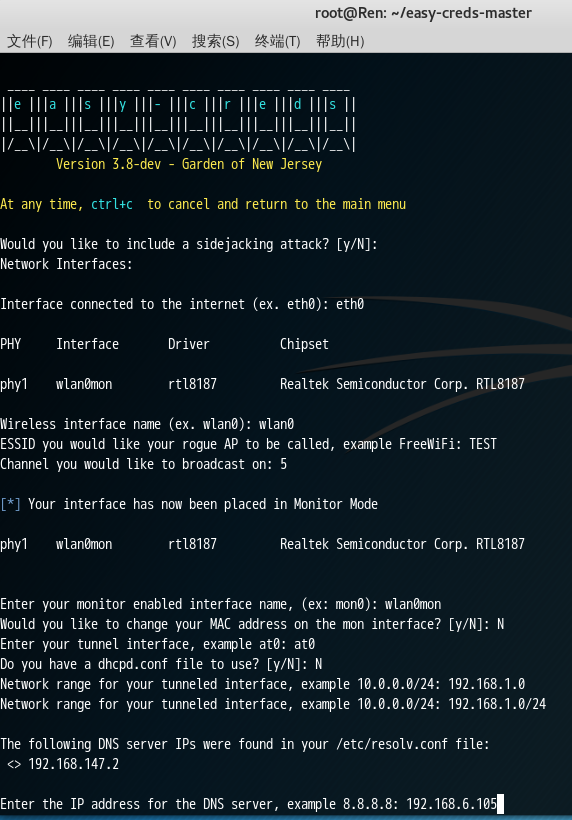


安装完成后执行easy-creds.sh，展示该工具的攻击菜单。



这里我们选择伪AP攻击，即编号3，然后选择子菜单中的静态伪AP攻击方法，如图

采用如下配置创建伪AP



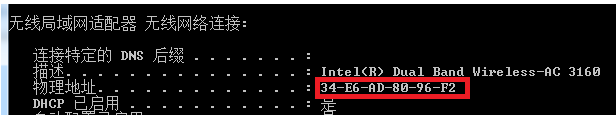
成功发现并连接该名为TEST的伪AP



在kali里可看到有设备连接到了我们的伪AP，在这里是我的主机win7



Win7无线网卡的MAC地址，可看出我的主机成功连接到我配置的伪AP



1. **强制客户端下线**

成功创建伪AP后可以通过强制用户在其连接的AP下线，以迫使其连接到我们创建的伪AP上。强制用户下线可用到MDK3工具，其语法格式为：

mdk3 <interface> <test\_mode> <test\_options>

各参数含义如下：

·intertface：指定网络接口；

·test\_mode：指定测试模式。该工具支持的模式有a（DOS模式），b（Beacon洪水模式）、d（解除验证/解除关联暴力模式）、f（MAC过滤暴力模式）、g（WPA降级测试）、m（关闭开发）、p（基本探测和ESSID暴力模式）、w（WIDS/WIPS混乱）以及x（802.1x测试）；

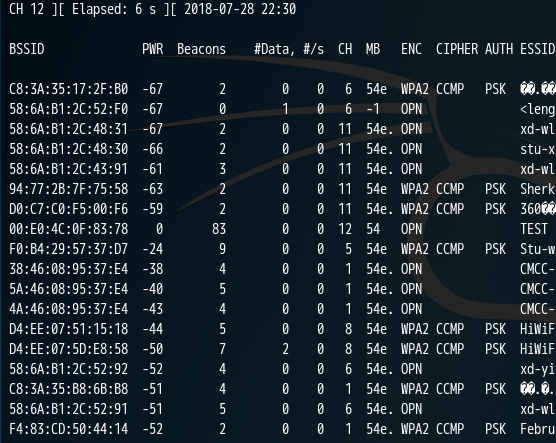
·test\_options：指定一些测试选项。

在将网卡设置为混杂模式（使用Aircrack-ng的Airmon-ng），然后利用工具Airodump-ng扫描附近的wifi信号，并确定攻击的目标（记录其MAC地址，如6C:E8:73:7A:35:A8）。完成上述工作后，开始进行攻击，执行如下命令：

mdk3 mon0 d a -a 6C:E8:73:7A:35:A8

其中mon0为无线网卡接口名称。

Airodump-ng扫描附近的wifi



我手机连接的AP的ESSID为“Stu-wlan”



根据扫描结果可知，该wifi使用的无线信道为5，使用MDK3命令将信道为5的wifi强制下线



查看手机发现wifi断开



当用户客户端重新连接AP时，创建的伪AP将会出现在所有信号的最前面（信号最强）。

1. **使用wireshark捕获数据包**

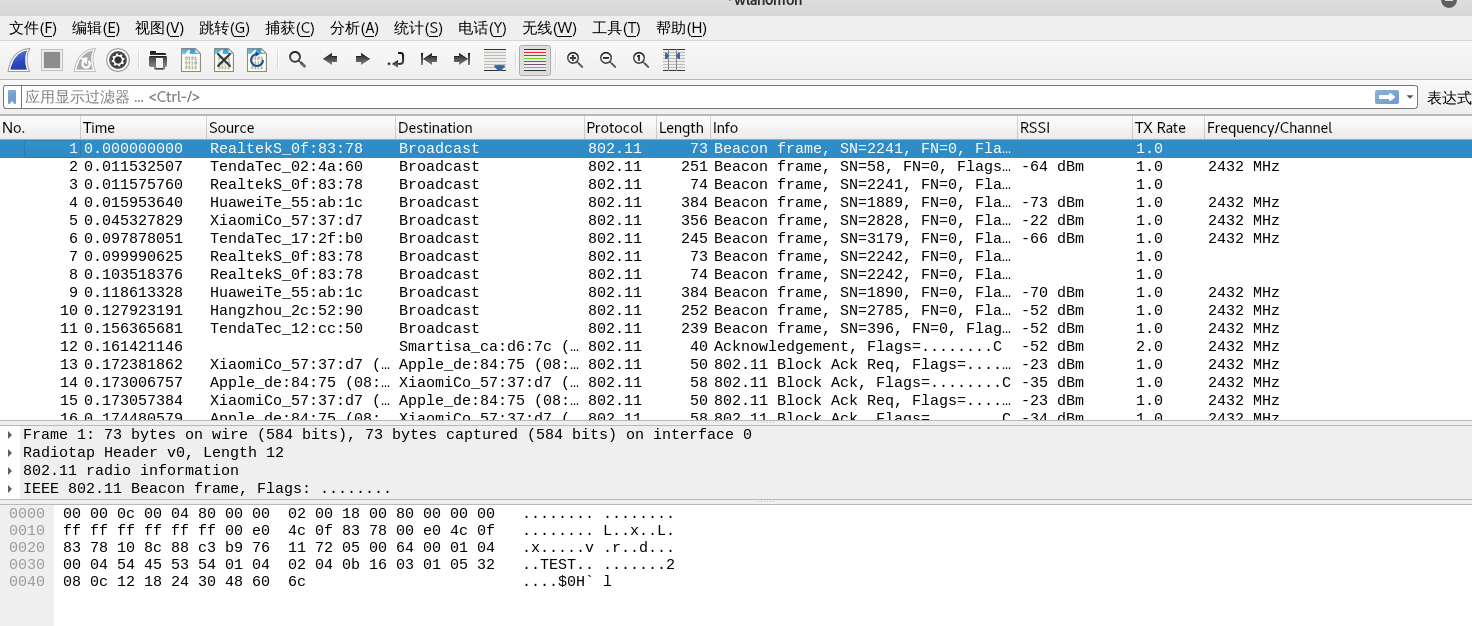
用户连接我们创建的伪AP后，我们可以使用wireshark开始抓包。

通过抓取的DHCP包我们可以得到用户的IP地址，然后设置过滤规则查看该IP（即该用户）传送的数据包。

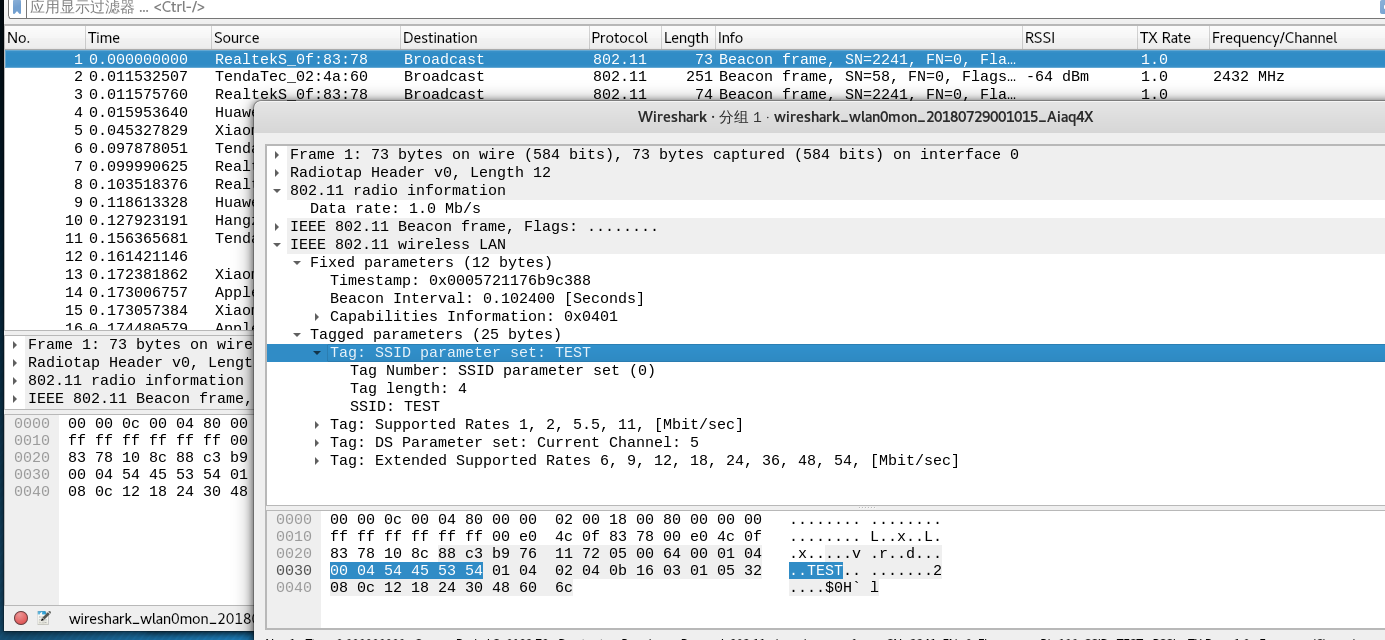
在首选项中添加三列：RSSI（显示捕获数据包的射频信号强度）、TX Rate（显示捕获数据包的数据率）、Frequency/Channel（显示捕获数据包的频率和信道）



选择wlan0mon（伪AP使用的接口）捕获数据，可以看到捕获到的包

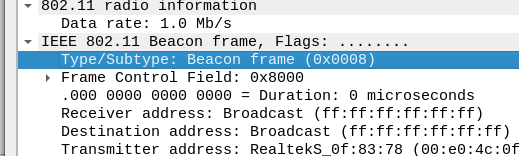


选择第一帧beacon包。这个包通过广播的方式发送，用于通知所有无线客户端存在这个可用的AP

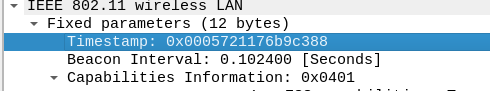


从包的内容中我们可以看到如下信息：

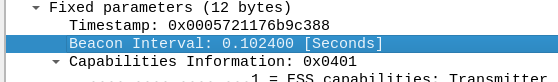
* 这个包在802.11头部的Type/Subtype域被定义为beacon



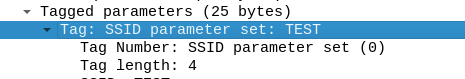
·Timestamp：发送数据包的时间戳



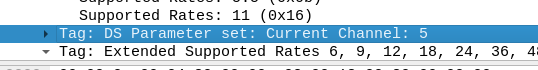
·Beacon Interval：beacon包的重传间隔



·SSID Parameter Set：WAP广播的SSID



·DS Parameter Set：WAP广播使用的信道



与之前我们使用easy-creds创建伪AP时的设置一致。

1. **使用Reaver工具暴力破解WPS加密**

Reaver是一个暴力破解WPS加密的工具，它通过一系列AP的PIN码暴力破解。

Reaver的语法格式如下：

Reaver -i <interface> -b <target bssid> -vv

以上参数的含义：

·-i：指定监听模式接口

·-b：指定目标AP的BSSID

·-vv：显示更多的详细信息

此外还有其他一些常用的选项：

·-c：指定接口工作的信道

·-e：指定目标AP的ESSID

·-p：指定WPS使用的PIN码

·-q：仅显示至关重要的信息

1. **使用Wifite工具**

Wifite是一款自动化WEP和WPA破解工具（仅支持Linux平台）。Wifite的特点是可以同时攻击多个采用WEP和WPA加密的网络。

1. 使用wifite破解WPS加密的语法格式：

wifite [options]

常用选项的含义：

·-i：指定捕获的无线接口

·-c：指定目标AP使用的信道

·-dict<file>：指定一个用于破解密码的字典

·-e：指定目标AP的SSID名称

·-b：指定目标AP的BSSIS名称

·-wpa：仅扫描WPA加密的网络

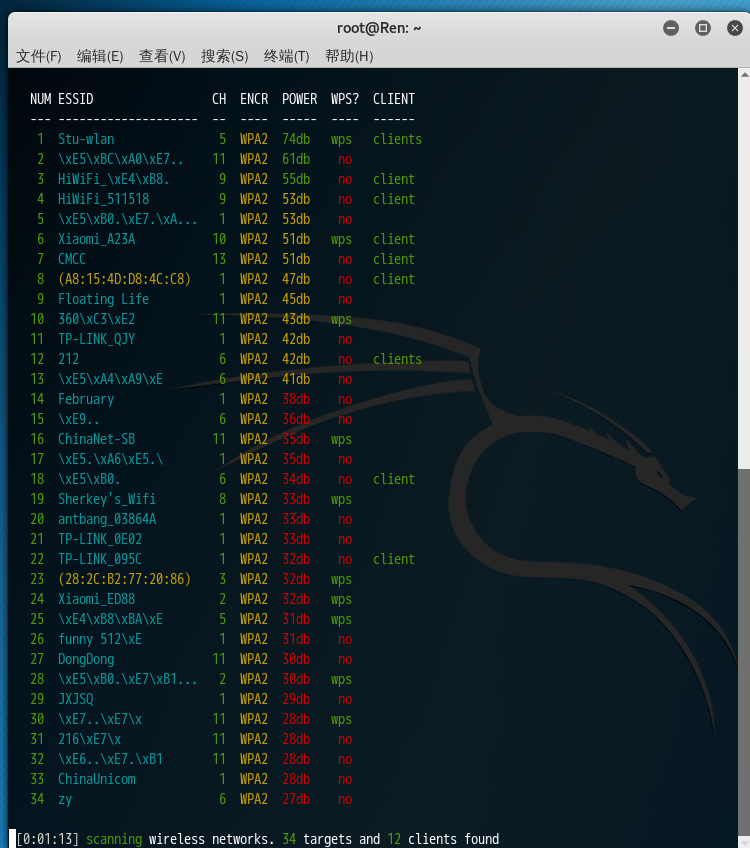
·-wep：仅扫描WEP加密的网络

·-pps：指定每秒注入的包数

·-wps：仅扫描WPS加密的网络

1. 使用wifite破解WEP加密

wifite



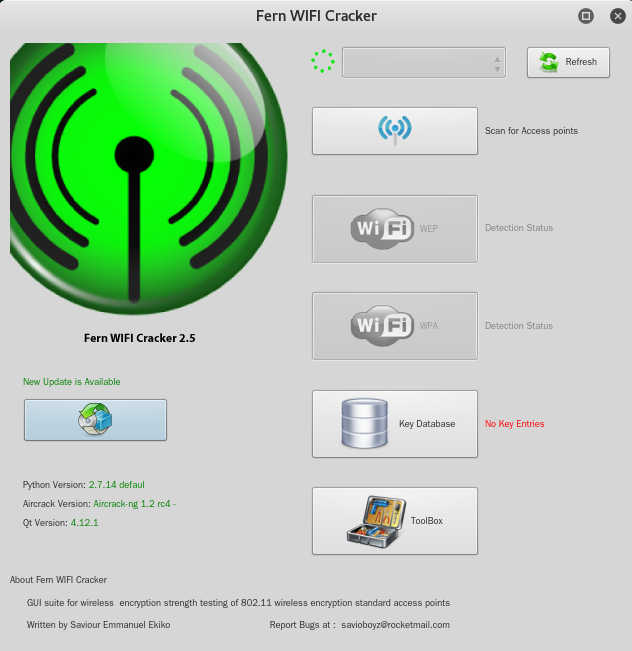
在扫描的的无线网络列表中选择要攻击的目标，即可开始进行破解

1. **Fern WiFi Cracker工具**

Fern WiFi Cracker是一种无线安全审计和攻击软件编写的程序，用于破解并恢复出WEP、WPA和WPS方式加密的无线网络密码。

使用步骤：

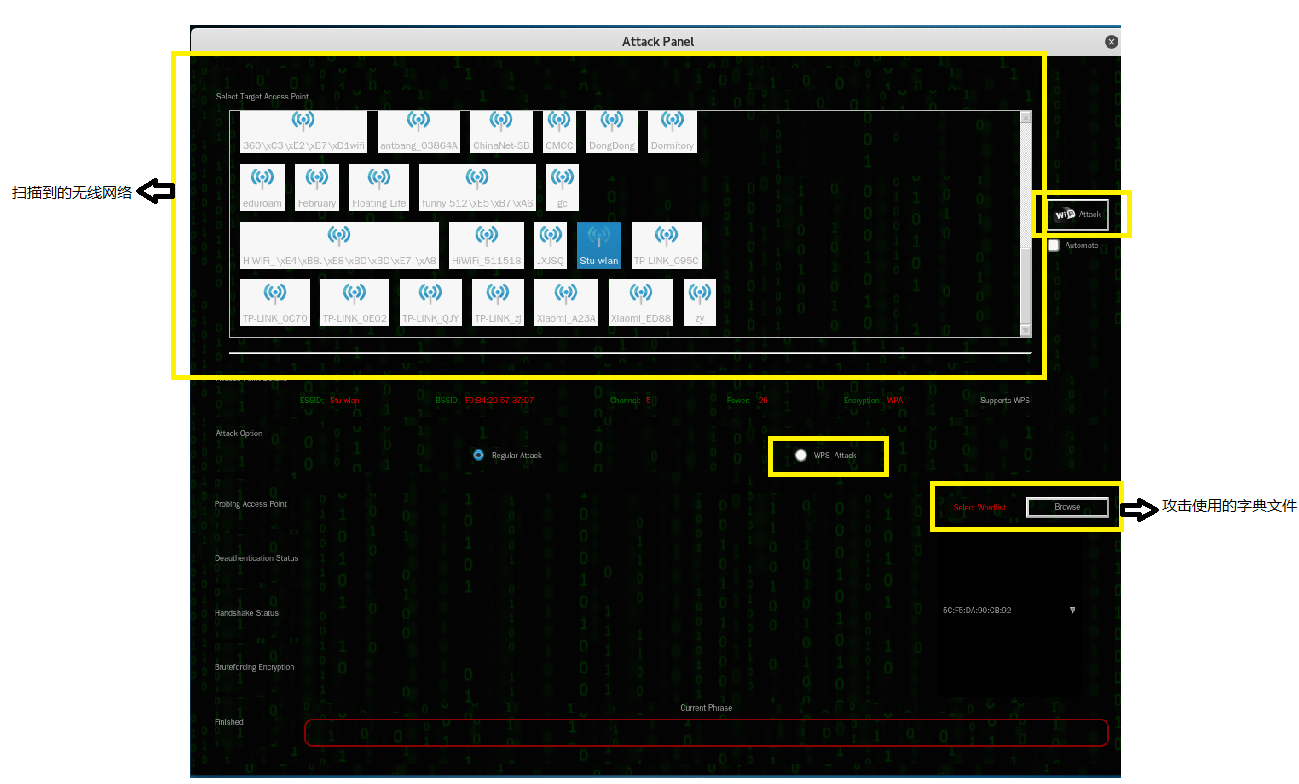
1. 打开Fern WiFi Cracker工具



1. 选择用于攻击的无线网卡，开始扫描附近的无线网络



1. 选择网络的加密类型（如这里的WPA，扫描到48个网络）



1. 使用crunch工具创建密码字典

Crunch工具常用语创建暴力破解密码时使用的密码字典。

语法格式如下：

crunch [minimum length] [maximum length] [character set] [options]

其参数含义如下：

·minimum length：指定生成密码的最小长度

·maximum length：指定生成密码的最大长度

·character set：指定一个用于生成密码字典的字符集

·-c：指定密码个数（行数）

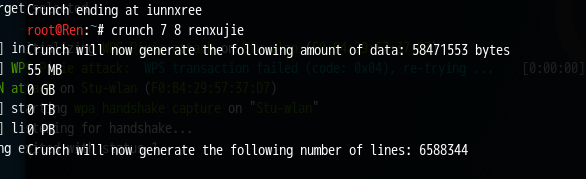
-d：限制相同元素出现的个数。如“-d 3”就不会出现如aaa、bbbb这样超过了三个相同的元素

·-e：定义停止生成的密码字符串

·-s：指定第一个密码

·-z：打包压缩格式（gzip、bzip2、lzma和7z等）

使用crunch创建一个7到8位的字典，使用的字符串为renxujie



将创建55MB（6588344个）密码



1. **使用****RainbowCrack创建彩虹表**

彩虹表是一个庞大的、针对各种可能的字母组合预先计算好的哈希值的集合，可以用于快速藕节各类密码。

RainbowCrack工具包含三个程序：rtgen、rtsort、rcrack。

它们分别用于：

·rtgen：彩虹表生成工具，生成口令、哈希值对照表

·rtsort：排序彩虹表，为rcrack提供输入

·rcrack：使用排好序的彩虹表进行口令破解

1. 使用rtgen创建彩虹表的语法格式：

rtgen hash\_algorihm charset plaintext\_len\_min plaintext\_len\_max table\_index chain\_len chain\_num part\_index

或

rtgen hash\_algorihm charset plaintext\_len\_min plaintext\_len\_max table\_index -bench

各部分含义如下：

·hash\_algorihm：指定密码的加密算法（包括lm、md5、sha1、mysqlsha1）

·charset：指定密码的字符集

·plaintext\_len\_min：指定密码的最小长度

·plaintext\_len\_max：指定密码的最大长度

·table\_index：指定彩虹表的索引

·chain\_len：指定彩虹链的长度

·chain\_num：指定彩虹链的个数

·part\_index：判断每一个彩虹链的起点是怎样产生的