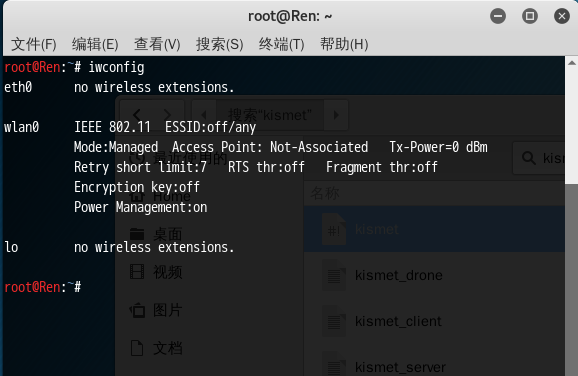
**第二章 无线WiFi网络状态监测与感知分析**

任旭杰 2018.8.2

1. **实验目的**
2. 掌握linux终端下的基本命令操作。
3. 掌握捕获wifi数据包的方法。
4. 掌握分析wifi数据包，提取相关信息的方法。
5. 掌握linux下python/java/c编程。
6. **实验需求**
7. 一台PC或笔记本（带无线网卡）、多个AP。
8. linux Kali系统、aircrack-ng无线嗅探软件、iw无线配置软件、处理数据的python/java/c程序。
9. **查看网卡状态**

实验使用的网卡型号为RTL8187L，实验环境为kali linux（在VMware下）。

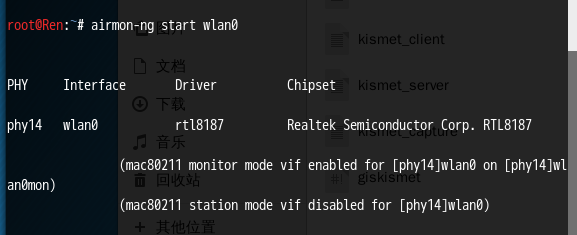
使用命令iwconfig查看网卡状态：



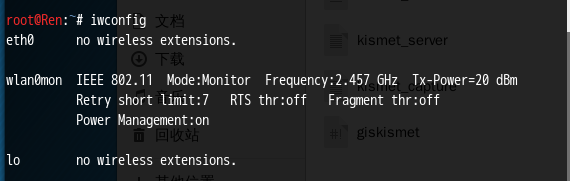
其中wlan0是我们的无线网卡，其工作模式为Managed，在此模式下可使用网卡连接无线AP实现访问Internet的功能。

1. **开启网卡的监听模式**

使用工具集aircrack-ng中的airmon-ng工具，开启无线网卡的监听模式

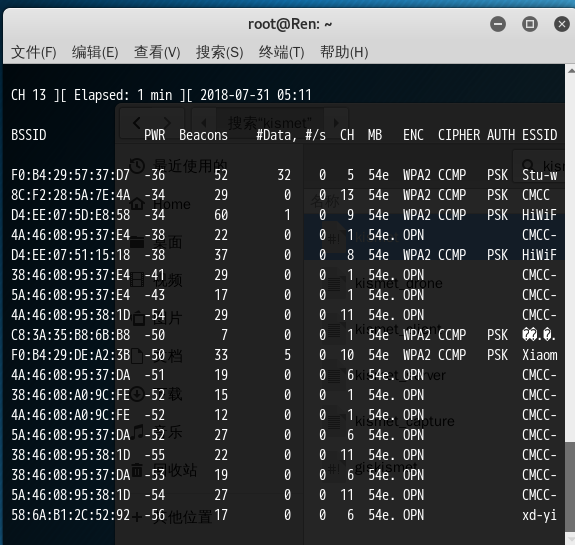


可看出将网卡wlan0设置为监听模式wlan0mon，执行iwconfig查看



1. **扫描附近的无线网络**

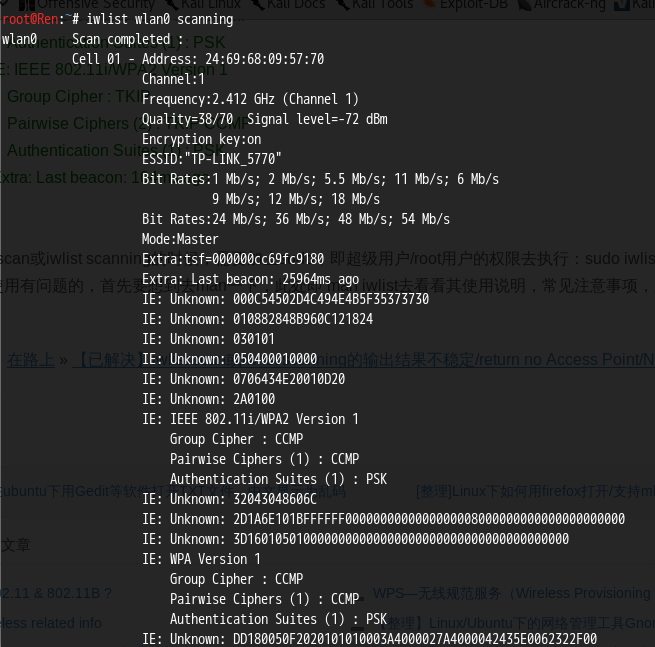
使用工具airodump-ng扫描附近的无线网络



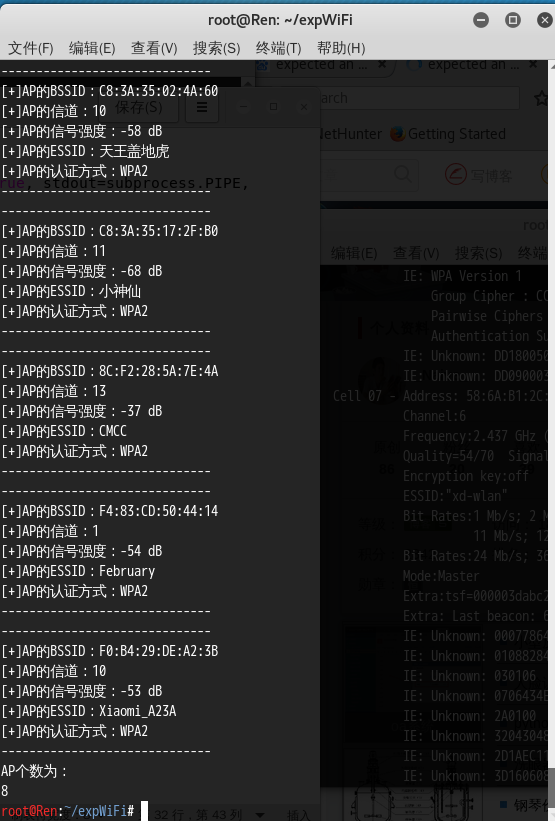
可以看到附近wifi的BSSID、ESSID、beacon广播次数、使用的信道、加密方式、最大传输速率等信息。

关闭监听模式，并用iwlist命令扫描附近wifi





1. **处理嗅探的结果**



Python代码如下：

#coding:utf-8

import os

import sys

import subprocess

from scapy.all import \*

AP = {'signal': [],'ESSID':[],'TYPE':[],'BSSID':[],'CHANNEL':[]}

def scan(num):

global j,i

j = 0

while num>0:

proc = subprocess.Popen("iwlist wlan0 scanning", shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE)

lines = proc.communicate()[0].split('\n')

for line in lines:

if 'Address' in line:

print '-'\*30

print '[+]AP的BSSID：'+line[29:]

AP['BSSID'].append(line[9:])

if 'Channel:' in line:

print '[+]AP的信道：'+line[28:]

AP['CHANNEL'].append(line[28:])

if 'Signal' in line:

print '[+]AP的信号强度：'+line[48:54]

AP['signal'].append(line[48:54])

if 'Encryption key:off' in line:

print '[+]AP的认证方式：'+'OPEN'

AP['TYPE'].append('OPEN')

if 'ESSID' in line:

line2 = line[27:]

line3 = line2.split('"',1)[0]

line4 = eval("'"+line3+"'")

print '[+]AP的ESSID：'+line4

AP['ESSID'].append(line4)

j+=1

if 'IEEE' in line:

print '[+]AP的认证方式：'+line[37:41]

AP['TYPE'].append(line[37:41])

print '-'\*30

num-=1

return j

def main():

scan(1)

print "AP个数为："

print j

if \_\_name\_\_ == '\_\_main\_\_':

main()