火龙果•整理
uml.org.cn

前　言

Kali Linux 是业内最知名的安全渗透测试专用操作系统。它的前身就是业界知名的 BackTrack 操作系统。BackTrack 在 2013 年停止更新，转为 Kali Linux。Kali Linux 集成了海量渗透测试、网络扫描、攻击等专用工具。通过系统更新，用户可以快速获取最新的各类工具。所以，Kali Linux 是专业人员的不二选择。

当今，由于无线网络使用方便，无线网络的应用非常广泛。并且无线网络的搭建也比较简单，仅需要一个无线路由器即可实现。由于无线网络环境中，数据是以广播的形式传输，因此引起了无线网络的安全问题。在无线路由器中，用户可以通过设置不同的加密方法来保证数据的安全。但是，由于某些加密算法存在的漏洞，使得专业人员可以将其密码破解出来。

本教程就针对无线网络存在的安全问题，介绍了对各种加密方式实施渗透的方法，如 PIN、WEP、WPA/WPA2、WPA+RADIUS。通过对无线网络实施渗透，可以获取到无线网络的各种信息。本教程还介绍了使用 Wireshark 捕获无线网络的数据包，并进行分析。

1.学习所需的系统和软件

- ❑ □安装 Kali Linux 操作系统
- ❑ □大功率的 USB 无线网卡

2.学习建议

大家学习之前，可以致信到 kali@daxueba.net，获取相关的资料和软件。如果大家在学习过程遇到问题，也可以将问题发送到该邮箱。我们尽可能给大家解决。

火龙果•整理
uml.org.cn

目　录

第 1 章　搭建渗透测试环境 .....
1.1　什么是渗透测试 .....
1.2　安装Kali Linux操作系统 .....
1.2.1　在物理机上安装Kali Linux .....
1.2.2　在VMware Workstation上安装Kali Linux .....
1.2.3　安装VMware tools .....
1.2.4　升级操作系统 .....
1.3　Kali Linux的基本配置 .....
1.3.1　配置软件源 .....
1.3.2　安装中文输入法 .....
1.3.3　虚拟机中使用USB设备 .....
第 2 章　WiFi网络的构成 .....
2.1　WiFi网络概述 .....
2.1.1　什么是WiFi网络 .....
2.1.2　WiFi网络结构 .....
2.1.3　WiFi工作原理 .....
2.1.4　AP常用术语概述 .....
2.2　802.11 协议概述 .....
2.2.1　频段 .....
2.2.2　使用WirelessMon规划频段 .....
2.2.3　带宽 .....
2.3　配置无线AP .....
2.3.1　在路由器上设置AP .....
2.3.2　在随身WiFi上设置AP .....
第 3 章　监听WiFi网络 5
3.1　网络监听原理 5
3.1.1　网卡的工作模式 5
3.1.2　工作原理 5
3.2　配置管理无线网卡 6
3.2.1　Linux支持的无线网卡 6
3.2.2　虚拟机使用无线网卡 8
3.2.3　设置无线网卡 8
3.3　设置监听模式 12
3.3.1　Aircrack-ng工具介绍 12
3.3.2　Aircrack-ng支持的网卡 13

火龙果•整理
uml.org.cn

3.3.3 启动监听模式 14
3.4 扫描网络范围 16
3.4.1 使用airodump-ng扫描 16
3.4.2 使用Kismet扫描 19
第 4 章 捕获数据包 .....
4.1 数据包简介 .....
4.1.1 握手包 .....
4.1.2 非加密包 .....
4.1.3 加密包 .....
4.2 使用Wireshark捕获数据包 .....
4.2.1 捕获非加密模式的数据包 .....
4.2.2 捕获WEP加密模式的数据包 .....
4.2.3 捕获WPA-PSK/WPA2-PSK加密模式的数据包 .....
4.3 使用伪AP .....
4.3.1 AP的工作模式 .....
4.3.2 创建伪AP .....
4.3.3 强制客户端下线 .....
4.3.4 捕获数据包 .....
第 5 章 分析数据包 .....
5.1 Wireshark简介 .....
5.1.1 捕获过滤器 .....
5.1.2 显示过滤器 .....
5.1.3 数据包导出 .....
5.1.4 在Packet List面板增加无线专用列 .....
5.2 使用Wireshark .....
5.2.1 802.11 数据包结构 .....
5.2.2 分析特定BSSID包 .....
5.2.3 分析特定的包类型 .....
5.2.4 分析特定频率的包 .....
5.3 分析无线AP认证包 .....
5.3.1 分析WEP认证包 .....
5.3.2 分析WPA认证包 .....
第 6 章 获取信息 .....
6.1 AP的信息 .....
6.1.1 AP的SSID名称 .....
6.1.2 AP的MAC地址 .....
6.1.3 AP工作的信道 .....
6.1.4 AP使用的加密方式 .....
6.2 客户端的信息 .....
6.2.1 客户端连接的AP .....
6.2.2 判断是否有客户端蹭网 .....

火龙果•整理
uml.org.cn

6.2.3 查看客户端使用的QQ号.....
6.2.4 查看手机客户端是否有流量产生.....
第 7 章 WPS加密模式.....
7.1 WPS简介.....
7.1.1 什么是WPS加密.....
7.1.2 WPS工作原理.....
7.1.3 WPS的漏洞.....
7.1.4 WPS的优点和缺点.....
7.2 设置WPS.....
7.2.1 开启WPS功能.....
7.2.1 在无线网卡上设置WPS加密.....
7.2.2 在移动客户端上设置WPS加密.....
7.3 破解WPS加密.....
7.3.1 使用Reaver工具.....
7.3.2 使用Wifite工具.....
7.3.3 使用Fern WiFi Cracker工具.....
第 8 章 WEP加密模式.....
8.1 WEP加密简介.....
8.1.1 什么是WEP加密.....
8.1.2 WEP工作原理.....
8.1.3 WEP漏洞分析.....
8.2 设置WEP加密.....
8.2.1 WEP加密认证类型.....
8.2.2 在AP中设置WEP加密模式.....
8.3 破解WEP加密.....
8.3.1 使用Aircrack-ng工具.....
8.3.2 使用Wifite工具破解WEP加密.....
8.3.3 使用Gerix WiFi Cracker工具破解WEP加密.....
8.4 应对措施.....
第 9 章 WPA加密模式.....
9.1 WPA加密简介.....
9.1.1 什么是WPA加密.....
9.1.2 WPA加密工作原理.....
9.1.3 WPA弥补了WEP的安全问题.....
9.2 设置WPA加密模式.....
9.2.1 WPA认证类型.....
9.2.2 加密算法.....
9.2.3 设置AP为WPA加密模式.....
9.3 创建密码字典.....
9.3.1 使用Crunch工具.....
9.3.2 使用pwgen工具.....

火龙果•整理
uml.org.cn

9.3.3 创建彩虹表 .....
9.4 破解WPA加密 .....
9.4.1 使用Aircrack-ng工具 .....
9.4.2 使用Wifite工具破解WPA加密 .....
9.4.3 不指定字典破解WPA加密 .....
9.5 WPA的安全措施 .....
第 10 章 WPA+RADIUS加密模式 .....
10.1 RADIUS简介 .....
10.1.1 什么是RADIUS协议 .....
10.1.2 RADIUS的工作原理 .....
10.2 搭建RADIUS服务 .....
10.2.1 安装RADIUS服务 .....
10.2.2 配置文件介绍 .....
10.3 设置WPA+RADIUS加密 .....
10.3.1 配置RADIUS服务 .....
10.3.2 配置MySQL数据库服务 .....
10.3.3 配置WiFi网络 .....
10.4 连接RADIUS加密的WiFi网络 .....
10.4.1 在Windows下连接RADIUS加密的WiFi网络 .....
10.4.2 在Linux下连接RADIUS加密的WiFi网络 .....
10.4.3 移动客户端连接RADIUS加密的WiFi网络 .....
10.5 破解RADIUS加密的WiFi网络 .....
10.5.1 使用hostapd-wpe创建伪AP .....
10.5.2 Kali Linux的问题处理 .....
10.5.3 使用asleap破解密码 .....
10.6 WPA+RADIUS的安全措施 .....

火龙果•整理
uml.org.cn

第 3 章　监听 WiFi 网络

网络监听是指监视网络状态、数据流程以及网络上信息传输。通常需要将网络设备设定成监听模式，然后就可以截获网络上所传输的信息。这是渗透测试使用最好的方法。WiFi 网络有其特殊性，所以本章讲解如何监听 WiFi 网络。

3.1　网络监听原理

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到这些信息。但是，如果要截获到所有信号，则需要将无线网卡设置为监听模式。只有在这种模式下，无线网卡才能接收到所有流过网卡的信息。本节将介绍网络监听原理。

3.1.1　网卡的工作模式

无线网卡是采用无线信号进行数据传输的终端。无线网卡通常包括四种模式，分别是广播模式、多播模式、直接模式和混杂模式。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监听模式。监听模式就是指混杂模式，下面将对网卡的几种工作模式进行详细介绍。如下所示：

（1）广播模式（Broad Cast Model）：它的物理地址（MAC）地址是 0Xffffff 的帧为广播帧，工作在广播模式的网卡接收广播帧。

（2）多播传送（MultiCast Model）：多播传送地址作为目的物理地址的帧可以被组内的其它主机同时接收，而组外主机却接收不到。但是，如果将网卡设置为多播传送模式，它可以接收所有的多播传送帧，而不论它是不是组内成员。

（3）直接模式（Direct Model）：工作在直接模式下的网卡只接收目的地址是自己 Mac 地址的帧。

（4）混杂模式（Promiscuous Model）：工作在混杂模式下的网卡接收所有的流过网卡的帧，通信包捕获程序就是在这种模式下运行的。

网卡的缺省工作模式包含广播模式和直接模式，即它只接收广播帧和发给自己的帧。如果采用混杂模式，一个站点的网卡将接受同一网络内所有站点所发送的数据包。这样，就可以到达对于网络信息监视捕获的目的。

3.1.2　工作原理

由于在 WiFi 网络中，无线网卡是以广播模式发射信号的。当无线网卡将信息广播出去后，所有的设备都可以接收到该信息。但是，在发送的包中包括有应该接收数据包的正确地址，并且只有与数据包中目标地址一致的那台主机才接收该信息包。所以，如果要想接收整

火龙果•整理
uml.org.cn

个网络中所有的包时，需要将无线网卡设置为混杂模式。

WiFi 网络由无线网卡、无线接入点（AP）、计算机和有关设备组成，其拓扑结构如图 3.1 所示。

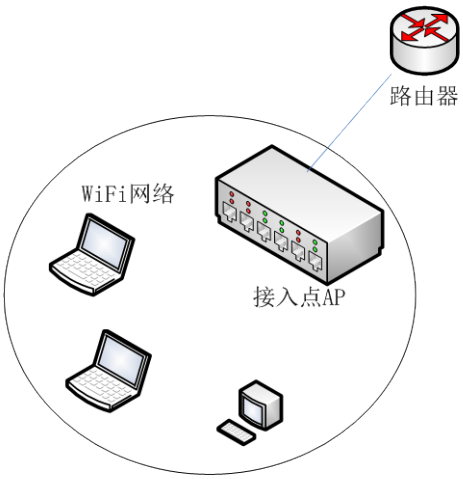


图 3.1　WiFi 网络拓扑结构

图 3.1 是一个 WiFi 网络拓扑结构。在该网络中，正常情况下每个客户端在接收数据包时，只能接收发给自己网卡的数据。如果要开启监听模式，将会收到所有主机发出去的信号。大部分的无线网卡都支持在 Linux 下设置为混杂模式，但是如果无线网卡的功率小的话，发射和接收信号都比较弱。如果用户捕获远距离的数据包，接收到的信号又强，则建议使用一个功率较大的无线网卡。如拓实 G618、拓实 N95 都是不错的大功率无线网卡。

3.2　配置管理无线网卡

无线网卡是终端无线网络的设备，是不通过有线连接，采用无线信号进行数据传输的终端。在计算机操作系统中，都会有一个网络管理器来管理网络设备的。本节将介绍在 Kali Linux 中如何管理无线网卡。

3.2.1　Linux 支持的无线网卡

在日常生活中，使用的无线网卡形形色色。但是，每个网卡支持的芯片和驱动不同。对于一些无线网卡，可能在 Linux 操作系统中不支持。为了帮助用户对无线网卡的选择，本节将介绍一下在 Linux 中支持的无线网卡。Linux 下支持的无线网卡，如表 3-1 所示。

表 3-1　Linux支持的无线网卡

驱动	制造商	AP	监听	PHY模式
adm8211	ADMtek/Infineon	no	?	B
airo	Aironet/Cisco	?	?	B
ar5523	Atheros	no	yes	A(2)/B/G
at76c50x-usb	Atmel	no	no	B

火龙果•整理
uml.org.cn

ath5k	Atheros	yes	yes	A/B/G
ath6kl	Atheros	no	no	A/B/G/N
ath9k	Atheros	yes	yes	A/B/G/N
ath9k_htc	Atheros	yes	yes	B/G/N
ath10k	Atheros	?	?	AC
atmel	Atmel	?	?	B
b43	Broadcom	yes	yes	A(2)/B/G
b43legacy	Broadcom	yes	yes	A(2)/B/G
brcmfmac	Broadcom	no	no	A(1)/B/G/N
brcmsmac	Broadcom	yes	yes	A(1)/B/G/N
carl9170	ZyDAS/Atheros	yes	yes	A(1)/B/G/N
cw1200	ST-Ericsson	?	?	A/B/G/N
hostap	Intersil/Conexant	?	?	B
ipw2100	Intel	no	no	B
ipw2200	Intel	no (3)	no	A/B/G
iwlegacy	Intel	no	no	A/B/G
iwlwifi	Intel	yes (6)	yes	A/B/G/N/AC
libertas	Marvell	no	no	B/G
libertas_tf	Marvell	yes	?	B/G
mac80211_hwsim	Jouni	yes	yes	A/B/G/N
mwifiex	Marvell	yes	?	A/B/G/N
mwl8k	Marvell	yes	yes	A/B/G/N
orinoco	Agere/Intersil/Symbol	no	yes	B
p54pci	Intersil/Conexant	yes	yes	A(1)/B/G
p54spi	Conexant/ST-NXP	yes	yes	A(1)/B/G
p54usb	Intersil/Conexant	yes	yes	A(1)/B/G
** prism2_usb	Intersil/Conexant	?	?	B
** r8192e_pci	Realtek	?	?	B/G/N
** r8192u_usb	Realtek	?	?	B/G/N
** r8712u	Realtek	?	?	B/G/N
ray_cs	Raytheon	?	?	pre802.11
rndis_wlan	Broadcom	no	no	B/G
rt61pci	Ralink	yes	yes	A(1)/B/G
rt73usb	Ralink	yes	yes	A(1)/B/G
rt2400pci	Ralink	yes	yes	B
rt2500pci	Ralink	yes	yes	A(1)/B/G
rt2500usb	Ralink	yes	yes	A(1)/B/G
rt2800pci	Ralink	yes	yes	A(1)/B/G/N
rt2800usb	Ralink	yes	yes	A(1)/B/G/N
rtl8180	Realtek	no	?	B/G
rtl8187	Realtek	no	yes	B/G
rtl8188ee	Realtek	?	?	B/G/N
rtl8192ce	Realtek	?	?	B/G/N
rtl8192cu	Realtek	?	?	B/G/N
rtl8192de	Realtek	?	?	B/G/N
rtl8192se	Realtek	?	?	B/G/N
rtl8723ae	Realtek	?	?	B/G/N
** vt6655	VIA	?	?	A/B/G
vt6656	VIA	yes	?	A/B/G
wil6210	Atheros	yes	yes	AD
** winbond	Winbond	?	?	B
wl1251	Texas Instruments	no	yes	B/G
wl12xx	Texas Instruments	yes	no	A(1)/B/G/N
wl18xx	Texas Instruments	?	?	?
wl3501_cs	Z-Com	?	?	pre802.11
** wlags49_h2	Lucent/Agere	?	?	B/G
zd1201	ZyDAS/Atheros	?	?	B
zd1211rw	ZyDAS/Atheros	yes	yes	A(2)/B/G

在以上表格中，列出了支持网卡的驱动、制造商、是否作为 AP、是否支持监听及支持

火龙果•整理
uml.org.cn

的协议模式。在表格中，“？”表示不确定，“yes”表示支持，“no”表示不支持。

3.2.2 虚拟机使用无线网卡

如果要管理无线网卡，则首先需要将该网卡插入到系统中。当用户在物理机中使用无线网卡时，可能直接会被识别出来。如果是在虚拟机中使用的话，可能无法直接连接到虚拟机的操作系统中。这时候用户需要断开该网卡与物理机的连接，然后选择连接到虚拟机。在虚拟机中只支持 USB 接口的无线网卡，下面以 Ralink RT2870/3070 芯片的无线网卡为例，介绍在虚拟机中使用无线网卡的方法。

【实例 3-1】在虚拟机中使用无线网卡，具体操作步骤如下所示：

（1）将 USB 无线网卡连接到虚拟机中，如图 3.2 所示。

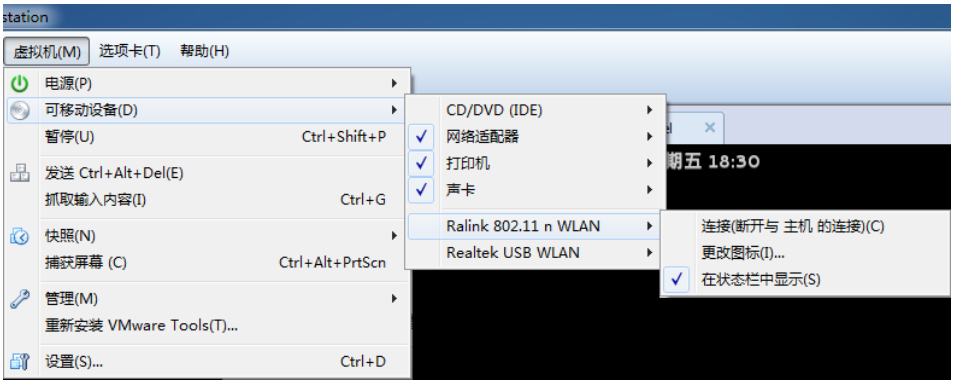


图 3.2 连接无线网卡

（2）在该界面依次选择“虚拟机”|“可移动设备”|Ralink 802.11 n WLAN|“连接(断开与主机的连接)(C)”命令后，将显示如图 3.3 所示的界面。

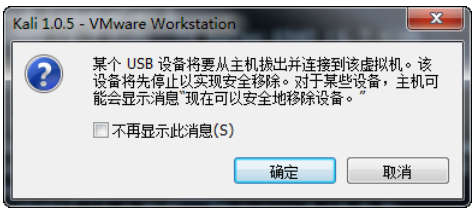


图 3.3 提示对话框

（3）该界面是一个提示对话框，这里单击“确定”按钮，该无线网卡将自动连接到虚拟机操作系统中。然后，用户就可以通过该无线网卡连接搜索到的无线网络。

3.2.3 设置无线网卡

下面介绍使用 Kali Linux 中的网络管理器来管理无线网卡。具体操作步骤如下所示：

（1）在图形界面依次选择“应用程序”|“系统工具”|“首选项”|“系统设置”命令，将打开如图 3.4 所示的界面。

火龙果•整理
uml.org.cn

图 3.4　系统设置

（2）在该界面单击“网络”图标，设置无线网络。单击“网络”图标后，将显示如图 3.5 所示的界面。

图 3.5　网络设置界面

（3）从该界面左侧框中，可以看到有线、无线和网络代理三个选项。这里选择“无线”选项，将显示如图 3.6 所示的界面。

火龙果•整理
uml.org.cn

图 3.6　设置无线

（4）从该界面可以看到，当前的无线处于断开状态。在该界面单击网络名称后面的图标选择，将要连接的无线网络。然后单击“选项(O)...”按钮，在弹出的界面选择“无线安全性”选项卡设置 WiFi 的安全性和密码，如图 3.7 所示。

图 3.7　设置安全性和密码

（5）在该界面输入 Test 无线网卡的加密方式和密码。这里默认密码是以加密形式显示的，如果想显示密码的话，将“显示密码”前面的复选框勾上。然后单击“保存”按钮，将开始连接 Test 无线网络。连接成功后，显示界面如图 3.8 所示。

火龙果•整理
uml.org.cn

图 3.8　连接成功

（6）从该界面可以看到，已成功连接到 Test 无线网络，并且显示了获取到的 IP 地址、默认路由、DNS 等显示。用户也可以使用 iwconfig 命令查看无线网络的详细信息。其中，iwconfig 命令的语法格式如下所示：

```
iwconfig [interface]
```

在该语法中，interface 表示网络接口名称。用户也可以不指定单个网络接口，查看所有接口的详细信息。如下所示：

```
root@localhost:~# iwconfig
wlan2     IEEE 802.11bgn  ESSID:"Test"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 14:E6:E4:AC:FB:20
          Bit Rate=28.9 Mb/s   Tx-Power=30 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=70/70  Signal level=-39 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:7   Missed beacon:0
lo        no wireless extensions.
eth0      no wireless extensions.
```

从输出的信息中，可以看到显示了本机中所有网络接口。其中，wlan2 是无线网卡的详细配置。由于 iwconfig 命令主要是用来查看无线接口的配置信息，所以在输出的信息中没有显示有线网络接口 eth0 的详细信息。如果用户想查看的话，可以使用 ifconfig 命令。该命令的语法格式如下所示：

```
ifconfig [interface]
```

在以上语法中，interface 选项表示指定的网络接口。使用 ifconfig 命令时，可以指定 interface 参数，也可以不指定。如果指定的话，只显示指定接口的配置信息；如果不指定的话，显示所有接口的配置信息。如下所示：

```
root@localhost:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:62:ea:43
          inet addr:192.168.6.105  Bcast:255.255.255.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe62:ea43/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47075 errors:0 dropped:0 overruns:0 frame:0
```

火龙果•整理
uml.org.cn

```
          TX packets:37933 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:49785671 (47.4 MiB)  TX bytes:5499271 (5.2 MiB)
          Interrupt:19 Base address:0x2000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:10439 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10439 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1063248 (1.0 MiB)  TX bytes:1063248 (1.0 MiB)
wlan2     Link encap:Ethernet  HWaddr 00:c1:40:95:11:15
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

从以上输出信息中，可以看到显示了本机中四个接口的配置信息。其中，eth0 接口是指本地的第一个有线网卡信息；lo 接口表示本地回环地址接口信息。

3.3 设置监听模式

通过前面的详细介绍，用户可以知道如果要捕获所有包，则必须要将无线网卡设置为监听模式。本节将介绍如何设置监听模式。

3.3.1 Aircrack-ng 工具介绍

Aircrack-ng 是一个与 802.11 标准的无线网络分析有关的安全软件，主要功能包括网络侦测、数据包嗅探、WEP 和 WPA/WPA2-PSK 破解。Aircrack-ng 工具可以工作在任何支持监听模式的无线网卡上，并嗅探 802.11a、802.11b、802.11g 的数据。下面将对该工具进行详细介绍。

Aircrack-ng 是一个套件，在该套件中包括很多个小工具，如表 3-2 所示。

表 3-2 Aircrack-ng套件

包名称	描述
aircrack-ng	破解WEP以及WPA（字典攻击）密钥
airdecap-ng	通过已知密钥来解密WEP或WPA嗅探数据
airmon-ng	将网卡设定为监听模式
aireplay-ng	数据包注入工具（Linux和Windows使用CommView驱动程序）
airodump-ng	数据包嗅探，将无线网络数据输送到PCAP货IVS文件并显示网络信息
airtun-ng	创建虚拟管道
airolib-ng	保存、管理ESSID密码列表
packetforge-ng	创建数据包注入用的加密包
Tools	混合、转换工具
airbase-ng	软件模拟AP
airdecloak-ng	消除pcap文件中的WEP加密
airdriver-ng	无线设备驱动管理工具

火龙果•整理
uml.org.cn

airolib-ng	保存、管理ESSID密码列表，计算对应的密钥
airserv-ng	允许不同的进程访问无线网卡
buddy-ng	easside-ng的文件描述
easside-ng	和AP接入点通讯（无WEP）
tkiptun-ng	WPA/TKIP攻击
wesside-ng	自动破解WEP密钥

3.3.2 Aircrack-ng 支持的网卡

在上一节介绍了 Aircrack-ng 套件的功能，及包含的一些小工具。根据以上的介绍，可知 Aircrack-ng 套件中的 airmon-ng 工具可以将无线网卡设置为监听模式。由于 Aircrack-ng 套件对一些网卡的芯片不支持，为了使用户更好的使用该工具，下面介绍一下该工具支持的一些网卡芯片。Aircrack-ng 工具支持的网卡芯片如表 3-3 所示。

表 3-3 Aircrack-ng工具支持的网卡芯片

芯片	Windows驱动（监听模式）	Linux驱动
Atheros	v4.2、v3.0.1.12、AR5000	Madwifi、ath5k、ath9k、ath9k_htc、ar9170/carl9170
Atheros		ath6kl
Atmel		Atmel AT76c503a
Atmel		Atmel AT76 USB
Broadcom	Broadcom peek driver	bcm43xx
Broadcom with b43 driver		b43
Broadcom 802.11n		brcm80211
Centrino b		ipw2100
Centrino b/g		ipw2200
Centrino a/b/g		ipw2915、ipw3945、iwl3945
Centrino a/g/n		iwlwifi
Cisco/Aironet	Cisco PCX500/PCX504 peek driver	airo-linux
Hermes I	Agere peek driver	Orinoco、 Orinoco Monitor Mode Patch
Ndiswrapper	N/A	ndiswrapper
cx3110x (Nokia 770/800)		cx3110x
prism2/2.5	LinkFerret or aerosol	HostAP、wlan-ng
prismGT	PrismGT by 500brabus	prism54
prismGT (alternative)		p54
Ralink		rt2x00、 RaLink RT2570USB Enhanced Driver RaLink RT73 USB Enhanced Driver
Ralink RT2870/3070		rt2800usb
Realtek 8180	Realtek peek driver	rtl8180-sa2400
Realtek 8187L		r8187 rtl8187
Realtek 8187B		rtl8187 (2.6.27+) r8187b (beta)
TI		ACX100/ACX111/ACX100USB
ZyDAS 1201		zd1201
ZyDAS 1211		zd1211rw plus patch

火龙果•整理
uml.org.cn

3.3.3 启动监听模式

前面对网络监听及网卡的支持进行了详细介绍。如果用户将前面的一些工作准备好后，就可以启动监听模式。下面将介绍使用 airmon-ng 工具，启动无线网卡的监听模式。

在使用 airmon-ng 工具之前，首先介绍下该工具的语法格式。如下所示：

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

以上语法中各选项含义如下所示：

- start：表示将无线网卡启动为监听模式。
- stop：表示禁用无线网卡的监听模式。
- interface：指定无线网卡接口名称。
- channel：在启动无线网卡为监听模式时，指定一个信道。

使用 airmong-ng 工具时，如果没有指定任何参数的话，则显示当前系统无线网络接口状态。

【实例 3-2】使用 airmon-ng 工具将无线网卡设置为监听模式。具体操作步骤如下所示：

（1）将无线网卡插入到主机中。使用 ifconfig 命令查看活动的网络接口，如下所示：

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:62:ea:43
          inet addr:192.168.6.110  Bcast:255.255.255.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe62:ea43/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6602 (6.4 KiB)  TX bytes:3948 (3.8 KiB)
          Interrupt:19 Base address:0x2000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:820 (820.0 B)  TX bytes:820 (820.0 B)
wlan2     Link encap:Ethernet  HWaddr 00:c1:40:95:11:15
          inet6 addr: fe80::2c1:40ff:fe95:1115/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0

          collisions:0 txqueuelen:1000
          RX bytes:3737 (3.6 KiB)  TX bytes:2763 (2.6 KiB)
```

从以上输出的信息中，可以看到无线网卡已被激活，其网络接口名称为 wlan2。如果在输出的信息中，没有看到接口名称为 wlan 类似活动接口的话，说明该网卡没有被激活。此时，用户可以使用 ifconfig -a 命令查看所有的接口。当执行该命令后，查看到有 wlan 接口名称，则表示该网卡被成功识别。用户需要使用以下命令，将网卡激活。如下所示：

```
root@localhost:~# ifconfig wlan2 up
```

执行以上命令后，没有任何输出信息。为了证明该无线网卡是否被成功激活，用户可以再次使用 ifconfig 命令查看。

（2）通过以上步骤，确定该网卡成功被激活。此时就可以将该网卡设置为混杂模式，

火龙果•整理
uml.org.cn

执行命令如下所示：

```
root@localhost:~# airmon-ng start wlan2
Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID        Name
2573       dhclient
2743       NetworkManager
2985       wpa_supplicant
3795       dhclient
3930       dhclient
Process with PID 3930 (dhclient) is running on interface wlan2
Interface        Chipset                    Driver
wlan2            Ralink RT2870/3070         rt2800usb - [phy0]
                       (monitor mode enabled on mon0)
```

从输出的信息中，可以看到无线网络接口 wlan2 的监听模式在 mon0 接口上已经启用。在输出的信息中，还可以看到当前系统中无线网卡的芯片和驱动分别是 Ralink RT2870/3070 和 rt2800usb。

（3）为了确认当前网卡是否被成功设置为混杂模式，同样可以使用 ifconfig 命令查看。如下所示：

```
root@localhost:~# ifconfig
eth0        Link encap:Ethernet    HWaddr 00:0c:29:62:ea:43
            inet addr:192.168.6.110    Bcast:255.255.255.255    Mask:255.255.255.0
            inet6 addr: fe80::20c:29ff:fe62:ea43/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST    MTU:1500    Metric:1
            RX packets:49 errors:0 dropped:0 overruns:0 frame:0
            TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:7004 (6.8 KiB)    TX bytes:3948 (3.8 KiB)
            Interrupt:19 Base address:0x2000
lo          Link encap:Local Loopback
            inet addr:127.0.0.1    Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING    MTU:65536    Metric:1
            RX packets:14 errors:0 dropped:0 overruns:0 frame:0
            TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:820 (820.0 B)    TX bytes:820 (820.0 B)
mon0        Link encap:UNSPEC    HWaddr 00-C1-40-95-11-15-00-00-00-00-00-00-00-00-00-00
            UP BROADCAST RUNNING MULTICAST    MTU:1500    Metric:1
            RX packets:622 errors:0 dropped:637 overruns:0 frame:0
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:88619 (86.5 KiB)    TX bytes:0 (0.0 B)
wlan2       Link encap:Ethernet    HWaddr 00:c1:40:95:11:15
            inet addr:192.168.6.103    Bcast:192.168.6.255    Mask:255.255.255.0
            inet6 addr: fe80::2c1:40ff:fe95:1115/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST    MTU:1500    Metric:1
            RX packets:42 errors:0 dropped:0 overruns:0 frame:0
            TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
```

火龙果•整理
uml.org.cn

```
          RX bytes:4955 (4.8 KiB)   TX bytes:4233 (4.1 KiB)
```

从输出的信息中，可以看到有一个网络接口名称为 mon0。这表示当前系统中的无线网卡，已经为监听模式。如果用户只想查看无线网卡详细配置的话，可以使用 iwconfig 查看。如下所示：

```
root@Kali:~# iwconfig
mon0      IEEE 802.11bgn  Mode:Monitor  Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Power Management:off
wlan2     IEEE 802.11bgn  ESSID:"Test"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 14:E6:E4:AC:FB:20
          Bit Rate=150 Mb/s  Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-25 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:11  Missed beacon:0
eth0      no wireless extensions.
lo        no wireless extensions.
```

从以上输出信息中，可以看到有一个网络接口名称为 mon0，并且 Mode 值为 Monitor（监听模式）。

3.4 扫描网络范围

当用户将无线网卡设置为监听模式后，就可以捕获到该网卡接受范围的所有数据包。通过这些数据包，就可以分析出附近 WiFi 的网络范围。在 Kali Linux 中，提供了两个工具用于扫描网络范围。本节将介绍分别使用 airodump-ng 和 Kismet 工具实施扫描网络范围。

3.4.1 使用 airodump-ng 扫描

airodump-ng 是 Aircrack-ng 套件中的一个小工具，该工具主要用来捕获 802.11 数据报文。通过查看捕获的报文，可以扫描的附近 AP 的 SSID（包括隐藏的）、BSSID、信道、客户端的 MAC 及数量等。下面将介绍使用 airodump-ng 工具进行扫描。

在使用 airodump-ng 工具实施扫描之前，首先要将扫描的无线网卡开启监听模式。当网卡的监听模式开启后，就可以实施网络扫描。其中，airodump-ng 工具的语法格式如下所示：

```
airodump-ng [选项] <interface name>
```

airodump-ng 命令中可使用的选项有很多，用户可以使用--help 来查看。下面介绍几个常用的选项，其含义如下所示：

- -c：指定目标 AP 的工作信道。
- -i,--ivs：该选项是用来设置过滤的。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：指定一个自己希望保存的文件名，用来保存有效的 IVS 数据报文。
- <interface name>：指定接口名称。

【实例 3-3】使用 airodump-ng 工具扫描网络。执行命令如下所示：

```
root@Kali:~# airodump-ng mon0
```

火龙果•整理
uml.org.cn

执行以上命令后，将输出如下信息：

```
CH 11 ][ Elapsed: 3 mins ][ 2014-11-10 16:45
 BSSID              PWR   Beacons   #Data,  #/s   CH   MB        ENC   CIPHER
AUTH  ESSID
 EC:17:2F:46:70:BA  -26   47        16   0   6   54e.   WPA2   CCMP
      PSK  yzty
 8C:21:0A:44:09:F8  -35   16        0    0   1   54e.   WPA2   CCMP
      PSK  bob
 14:E6:E4:AC:FB:20  -42   68        3    0   1   54e.   WPA2   CCMP
      PSK  Test
 1C:FA:68:5A:3D:C0  -57   21        0    0   6   54e.   WPA2   CCMP
      PSK  QQ
 C8:64:C7:2F:A1:34  -60   12        0    0   1   54 .   OPN
       CMCC
 EA:64:C7:2F:A1:34  -60   10        0    0   1   54 .   WPA2   CCMP
      MGT CMCC-AUTO
 1C:FA:68:D7:11:8A  -59   23        0    0   6   54e.   WPA2   CCMP
      PSK TP-LINK_D7118A
 DA:64:C7:2F:A1:34  -63   8         0    0   1   54 .   OPN
CMCC-EDU
 4A:46:08:C3:99:D9  -68   4         0    0   11  54 .   OPN
CMCC-EDU
 5A:46:08:C3:99:D9  -69   6         0    0   11  54 .   WPA2   CCMP
      MGT CMCC-AUTO
 38:46:08:C3:99:D9  -70   3         0    0   11  54 .   OPN
      CMCC
 6C:E8:73:6B:DC:42  -1    0         0    0   1   -1
      <length:  0>
BSSID              STATION            PWR   Rate    Lost   Frames
Probe
 (not associated)  B0:79:94:BC:01:F0  -34   0 - 1   30     8
      wkbhui2000
 8C:21:0A:44:09:F8  14:F6:5A:CE:EE:2A  -24   0e- 0e  0      79
 EC:17:2F:46:70:BA  A0:EC:80:B2:D0:49  -58   0e- 1   0      8
 EC:17:2F:46:70:BA  14:F6:5A:CE:EE:2A  -22   0e- 1   0      146
      bob,Test,CMCC                   EC:17:2F:46:70:BA  D4:97:0B:44:32:C2
      -58   0e- 6   0   3
 14:E6:E4:AC:FB:20  00:C1:40:95:11:15  0   0e- 1   0      34
 6C:E8:73:6B:DC:42  EC:17:2F:46:70:BA  -58   0 - 1   0      8      yzty
 1C:FA:68:D7:11:8A  88:32:9B:B5:38:3B  -66   0 - 1   0      1
 1C:FA:68:D7:11:8A  88:32:9B:C6:E4:25  -68   0 - 1   0      6
```

输出的信息表示扫描到附近所有可用的无线 AP 及连接的客户端信息。执行 airodump-ng 命令后，需要用户手动按下 Ctrl+C 键停止扫描。从以上输出信息中，可以看到有很多参数。下面将对每个参数进行详细介绍。

- BSSID：表示无线 AP 的 MAC 地址。
- PWR：网卡报告的信号水平，它主要取决与驱动。当信号值越高时，说明离 AP 或计算机越近。如果一个 BSSID 的 PWR 是-1，说明网卡的驱动不支持报告信号水平。如果部分客户端的 PWR 为-1，那么说明该客户端不在当前网卡能监听到的范围内，但是能捕获到 AP 发往客户端的数据。如果所有的客户端 PWR 值都为-1，那么说明网卡驱动不支持信号水平报告。
- Beacons：无线 AP 发出的通告编号，每个接入点（AP）在最低速率（1M）时差不

火龙果•整理
uml.org.cn

多每秒会发送 10 个左右的 beacon，所以它们在很远的地方就被发现。。

- #Data：被捕获到的数据分组的数量（如果是 WEP，则代表唯一 IV 的数量），包括广播分组。
- #/s：过去 10 秒钟内每秒捕获数据分组的数量。
- CH：信道号（从 Beacons 中获取）。
- MB：无线 AP 所支持的最大速率。如果 MB=11，它是 802.11b；如果 MB=22，它是 802.11b+；如果更高就是 802.11g。后面的点（高于 54 之后）表明支持短前导码。‘e’表示网络中有 QoS（802.11 e）启用。
- ENC：使用的加密算法体系。OPN 表示无加密。WEP?表示 WEP 或者 WPA/WPA2，WEP（没有问号）表明静态或动态 WEP。如果出现 TKIP 或 CCMP，那么就是 WPA/WPA2。
- CIPHER：检测到的加密算法，CCMP、WRAAP、TKIP、WEP、WEP104 中的一个。典型的来说（不一定），TKIP 与 WPA 结合使用，CCMP 与 WPA2 结合使用。如果密钥索引值大于 0，显示为 WEP40。标准情况下，索引 0-3 是 40bit，104bit 应该是 0。
- AUTH：使用的认证协议。常用的有 MGT（WPA/WPA2 使用独立的认证服务器，平时我们常说的 802.1x，radius、eap 等），SKA（WEP 的共享密钥），PSK（WPA/WPA2 的预共享密钥）或者 OPN（WEP 开放式）。
- ESSID：也就是所谓的 SSID 号。如果启用隐藏的 SSID 的话，它可以为空，或者显示为 <length: 0>。这种情况下，airodump-ng 试图从 proberesponses 和 associationrequests 中获取 SSID。
- STATION：客户端的 MAC 地址，包括连上的和想要搜索无线来连接的客户端。如果客户端没有连接上，就在 BSSID 下显示“not associated”。
- Rate：表示传输率。
- Lost：在过去 10 秒钟内丢失的数据分组，基于序列号检测。它意味着从客户端来的数据丢包，每个非管理帧中都有一个序列号字段，把刚接收到的那个帧中的序列号和前一个帧中的序列号一减就可以知道丢了几个包。
- Frames：客户端发送的数据分组数量。
- Probe：被客户端查探的 ESSID。如果客户端正试图连接一个 AP，但是没有连接上，则将会显示在这里。

下面对以上扫描结果做一个简单分析，如表 3-4 所示。

表 3-4　扫描结果分析

AP的SSID名称	AP的MAC地址	AP的信道	信号强度	连接的客户端
yzty	EC:17:2F:46:70:BA	6	-26	A0:EC:80:B2:D0:49
				6C:E8:73:6B:DC:42
				14:F6:5A:CE:EE:2A
				D4:97:0B:44:32:C2
bob	8C:21:0A:44:09:F8	1	-35	14:F6:5A:CE:EE:2A
Test	14:E6:E4:AC:FB:20	1	-42	00:C1:40:95:11:15
QQ	1C:FA:68:5A:3D:C0	6	-57	
CMCC	C8:64:C7:2F:A1:34	1	-60	
CMCC-AUTO	EA:64:C7:2F:A1:34	1	-60	
TP-LINK_D7118A	1C:FA:68:D7:11:8A	6	-59	88:32:9B:B5:38:3B
				88:32:9B:C6:E4:25
CMCC-EDU	DA:64:C7:2F:A1:34	1	-63	
CMCC-EDU	4A:46:08:C3:99:D9	11	-68	
CMCC-AUTO	5A:46:08:C3:99:D9	11	-69	

火龙果•整理
uml.org.cn

CMCC	38:46:08:C3:99:D9	11	-70	
<length: 0>（隐藏SSID）	6C:E8:73:6B:DC:42	1	-1	

3.4.2 使用 Kismet 扫描

Kismet 是一个图形界面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 工具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。这样，可以方便用户对数据包进行分析使用。下面将介绍使用 Kismet 工具实施网络扫描。

【实例 3-4】使用 Kismet 工具扫描网络范围。具体操作步骤如下所示：

（1）启动 Kismet 工具。执行命令如下所示：

```
root@kali:~# kismet
```

执行以上命令后，将显示如图 3.9 所示的界面。

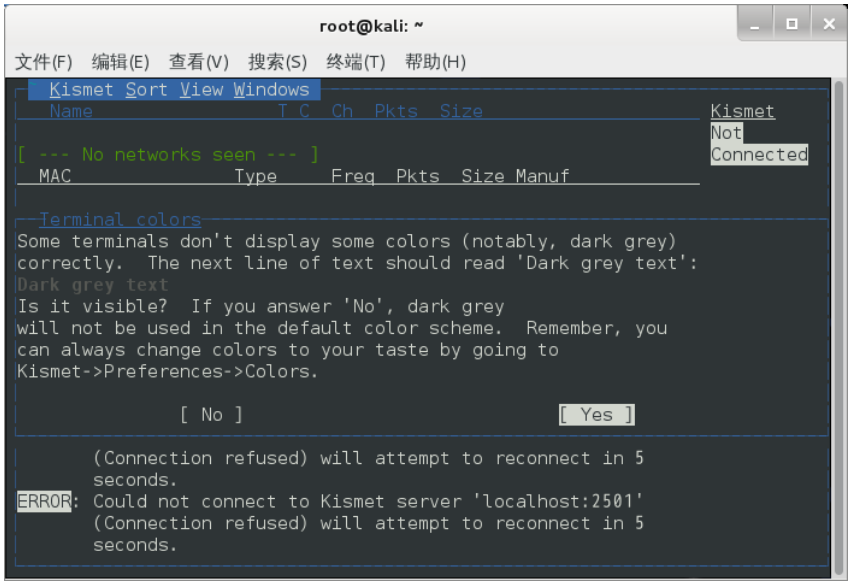


图 3.9 终端颜色

（2）该界面用来设置是否是用终端默认的颜色。因为 Kismet 默认颜色是灰色，可能一些终端不能显示。这里不使用默认的颜色，所以单击 No 按钮，将显示如图 3.10 所示的界面。

火龙果•整理
uml.org.cn

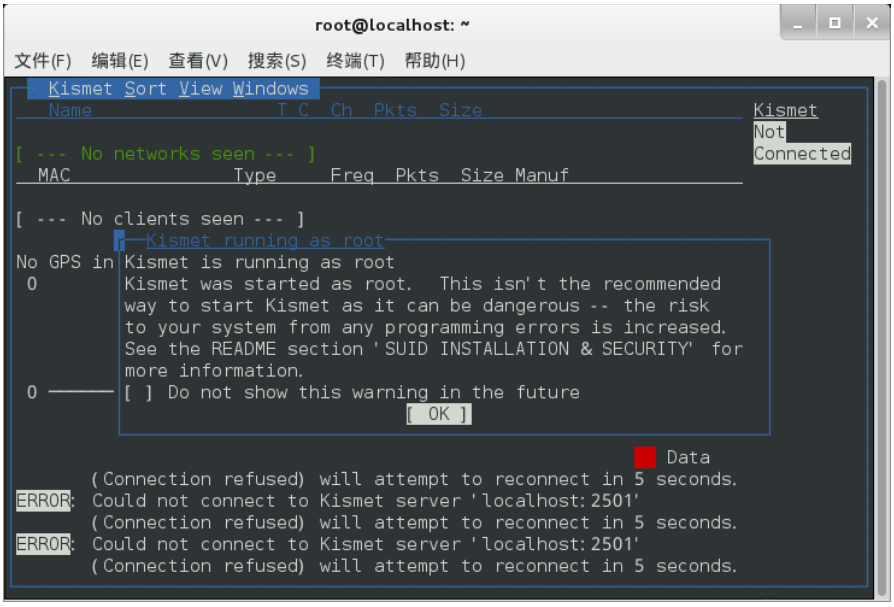


图 3.10　使用 root 用户运行 Kismet

（3）该界面提示正在使用 root 用户运行 Kismet 工具，并且该界面显示的字体颜色不是灰色，而是白色的。此时，单击 OK 按钮，将显示如图 3.11 所示的界面。

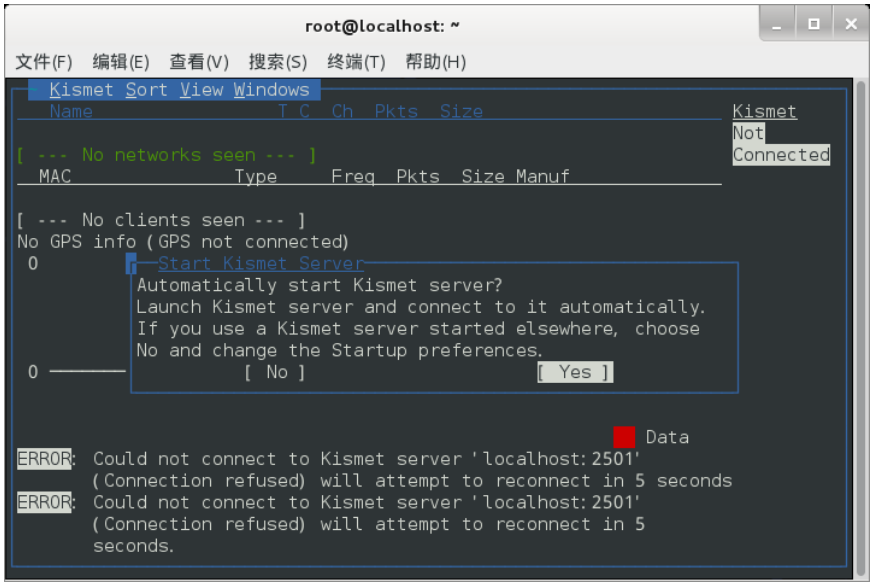
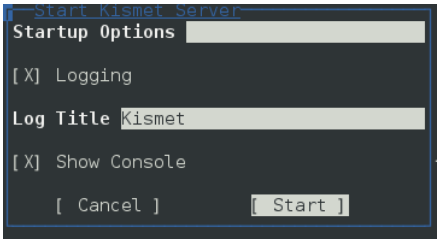


图 3.11　自动启动 Kismet 服务

（4）该界面提示是否要自动启动 Kismet 服务。这里选择 Yes，将显示如图 3.12 所示的界面。

（5）该界面显示设置 Kismet 服务的一些信息。这里使用默认设置，并选择 Start 按钮，将显示如图 3.13 所示的界面。

火龙果•整理
uml.org.cn



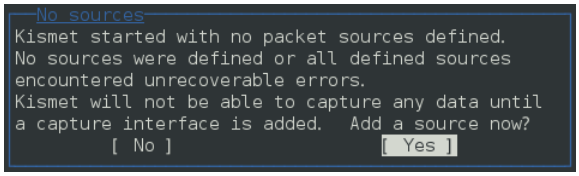
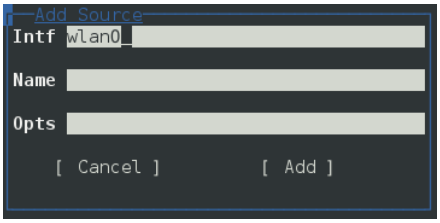


图 3.12　启动 Kismet 服务　　图 3.13　添加包资源

（6）该界面显示没有被定义的包资源，是否要现在添加。这里选择 Yes 按钮，将显示如图 3.14 所示的界面。

（7）在该界面指定无线网卡接口和描述信息。在 Intf 中，输入无线网卡接口。如果无线网卡已处于监听模式，可以输入 wlan0 或 mon0。其它配置信息可以不设置。然后单击 Add 按钮，将显示如图 3.15 所示的界面。



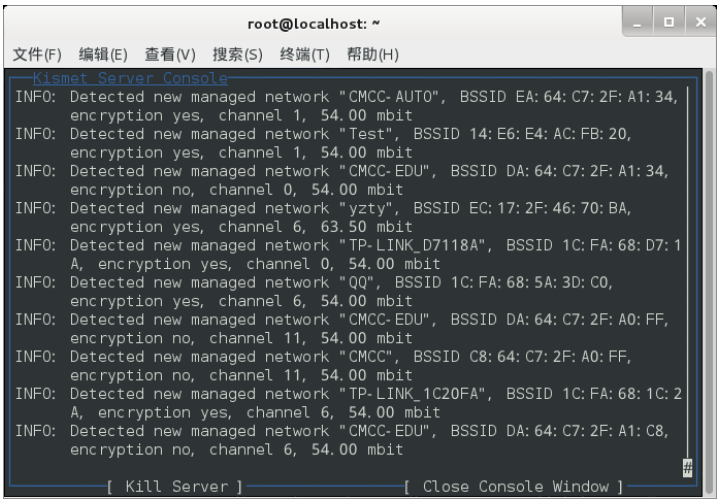


图 3.14　添加资源窗口　　图 3.15　关闭控制台窗口

（8）在该界面选择 Close Console Window 按钮，将显示如图 3.16 所示的界面。

火龙果•整理
uml.org.cn

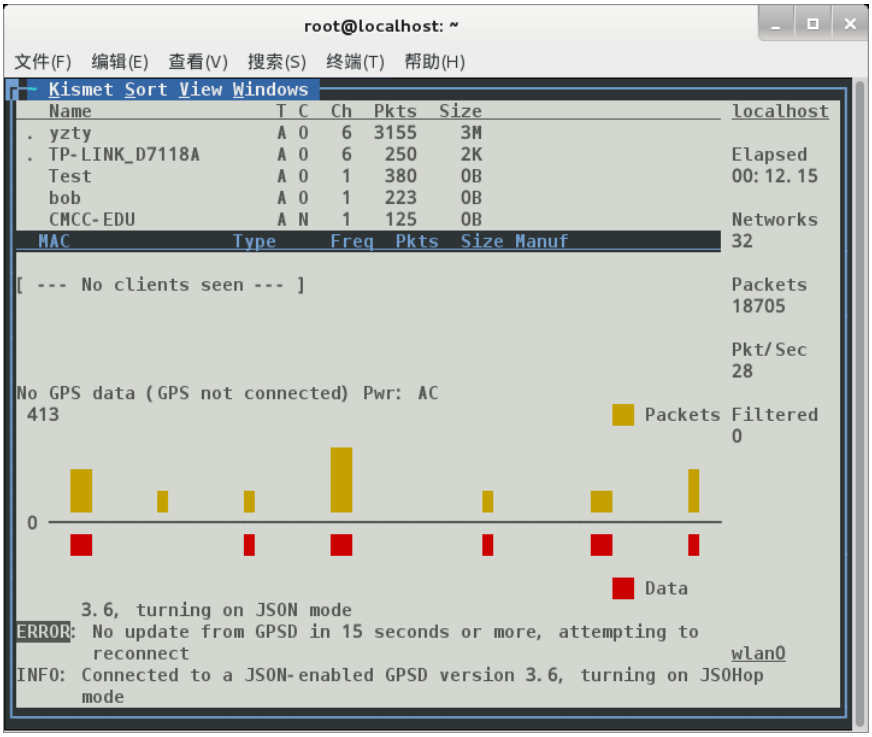


图 3.16　扫描的无线信息

（9）从该界面可以看到 Kismet 工具扫描到的所有无线 AP 信息。在该界面的左侧显示了，捕获包的时间，扫描到的网络数、包数等。用户可以发现，在该界面只看到搜索到的无线 AP、信道、包大小信息，但是没有看到这些 AP 的 MAC 地址及连接的客户端等信息。如果想查看到其它信息，还需要进行设置。如查看连接的客户端，在该界面的菜单栏中，依次选择 Sort|First Seen 命令，如图 3.17 所示。

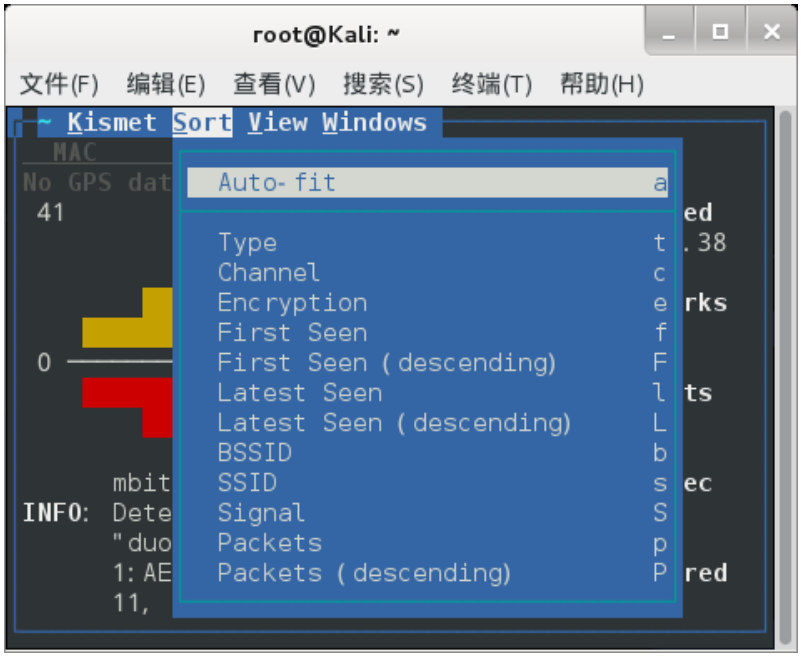


图 3.17　查看客户端信息

（10）在该界面单击 First Seen 命令后，将看到如图 3.18 所示的界面。

火龙果•整理
uml.org.cn

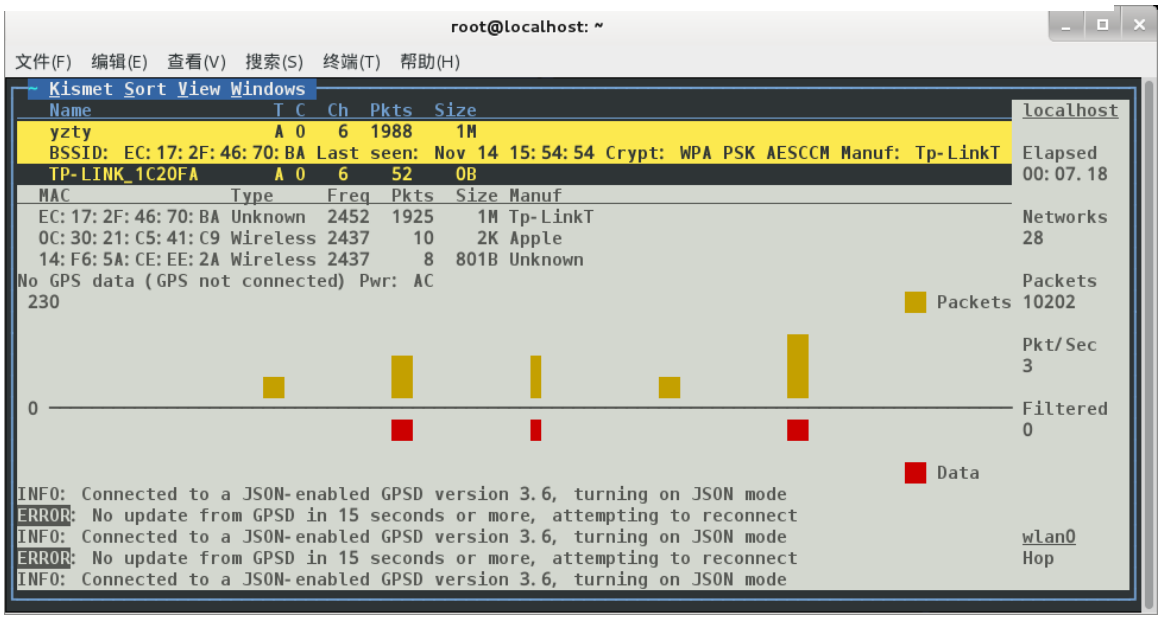


图 3.18　客户端的详细信息

（11）从该界面通过选择一个无线 AP，将会看到关于该 AP 的详细信息，如 AP 的 MAC 地址、加密方式等。如果希望查看到更详细的信息，选择上要查看的 AP，然后按下回车键，将查看到其详细信息。这里选择查看 ESSID 值为 yzty 的详细信息，如图 3.19 所示。

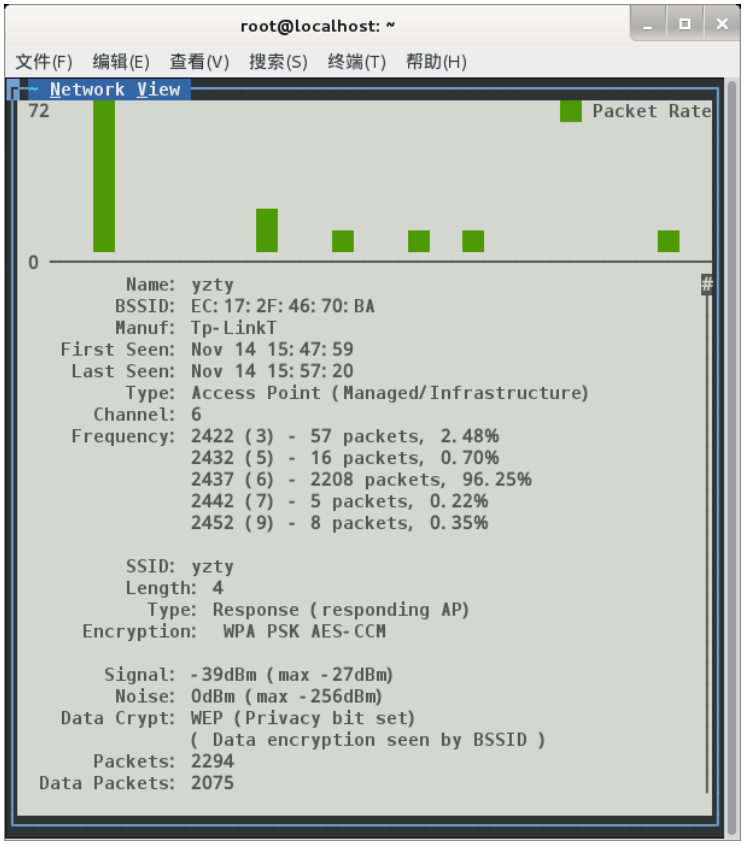


图 3.19　yzty 的详细信息

（12）从该界面可以看到无线 AP 的名称、MAC 地址、制造商、信道、运行速率等。当需要退出到 Kismet 主界面时，在该界面的菜单栏中依次选择 Network|Close window 命令，

火龙果•整理
uml.org.cn

如图 3.20 所示。

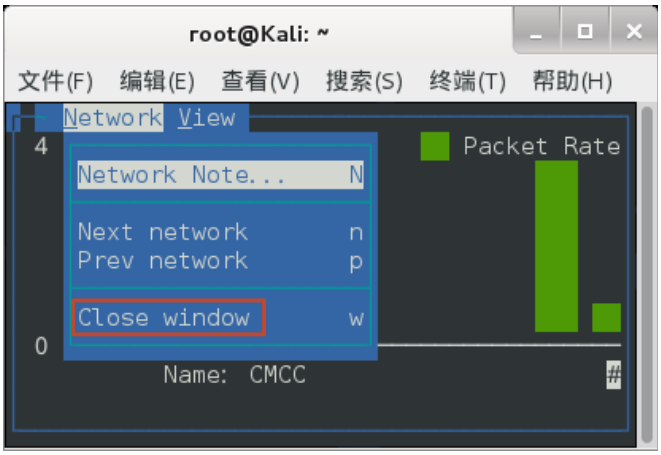


图 3.20　关闭当前窗口

（13）在该界面按下 Close windows 命令后，将返回到如图 3.18 所示的界面。当运行扫描到足够的信息时，停止扫描。此时，在图 3.18 界面依次选择 Kismet|Quit 命令退出 Kismet 程序，如图 3.21 所示的界面。

（13）按下 Quit 命令后，将显示如图 3.22 所示的界面。

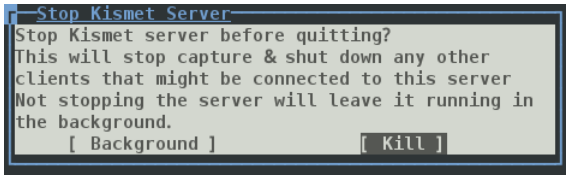


图 3.21　退出 Kismet　　图 3.22　停止 Kismet 服务

（14）在该界面单击 Kill 按钮，将停止 Kismet 服务并退出终端模式。此时，终端将会显示一些日志信息。如下所示：

```
*** KISMET CLIENT IS SHUTTING DOWN ***
[SERVER] INFO: Stopped source 'wlan0'
[SERVER] ERROR: TCP server client read() ended for 127.0.0.1
[SERVER]
[SERVER] *** KISMET IS SHUTTING DOWN ***
```

火龙果•整理
uml.org.cn

```
[SERVER] INFO: Closed pcapdump log file 'Kismet-20141113-15-32-40-1.pcapdump',
[SERVER]          155883 logged.
[SERVER] INFO: Closed netxml log file 'Kismet-20141113-15-32-40-1.netxml', 26
[SERVER]          logged.
[SERVER] INFO: Closed nettxt log file 'Kismet-20141113-15-32-40-1.nettxt', 26
[SERVER]          logged.
[SERVER] INFO: Closed gpsxml log file 'Kismet-20141113-15-32-40-1.gpsxml', 0 logged.
[SERVER] INFO: Closed alert log file 'Kismet-20141113-15-32-40-1.alert', 5 logged.
[SERVER] INFO: Shutting down plugins...
[SERVER] Shutting down log files...
[SERVER] WARNING: Kismet changes the configuration of network devices.
[SERVER]              In most cases you will need to restart networking for
[SERVER]              your interface (varies per distribution/OS, but
[SERVER]              usually:   /etc/init.d/networking restart
[SERVER]
[SERVER] Kismet exiting.
Spawned Kismet server has exited
*** KISMET CLIENT SHUTTING DOWN.   ***
Kismet client exiting.
```

从以上信息的 KISMET IS SHUTTING DOWN 部分中，将看到关闭了几个日志文件。这些日志文件，默认保存在/root/目录。在这些日志文件中，显示了生成日志的时间。当运行 Kismet 很多次或几天时，用户可以根据这些日志的时间快速的判断出那个日志文件是最近生成的。

接下来查看一下上面捕获到的数据包。切换到/root/目录，并使用 ls 命令查看以上生成的日志文件。执行命令如下所示：

```
root@kali:~# ls Kismet-20141113-15-32-40-1.*
Kismet-20141113-15-32-40-1.alert     Kismet-20141113-15-32-40-1.netxml
Kismet-20141113-15-32-40-1.gpsxml    Kismet-20141113-15-32-40-1.pcapdump
Kismet-20141113-15-32-40-1.nettxt
```

从输出的信息中，可以看到有五个日志文件，并且使用了不同的后缀名。Kismet 工具生成的所有信息，都保存在这些文件中。下面分别介绍下这几个文件格式中包括的信息：

- alert：该文件中包括所有的警告信息。
- gpsxml：如果使用了 GPS 源，则相关的 GPS 数据保存在该文件。
- nettxt：包括所有收集的文本输出信息。
- netxml：包括所有 XML 格式的数据。
- pcapdump：包括整个会话捕获的数据包。

注意：Kismet 工具中，用户可以在菜单栏中选择其它选项，查看一些其它信息。本例中，只简单的介绍了两个选项的详细信息。

火龙果•整理
uml.org.cn