**Airmon-ng** - This script can be used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode. Entering the airmon-ng command without parameters will show the interfaces status.

Specific uses:

1. Check status of wireless interfaces
2. Check for processes that could be interfering with your wireless interfaces
3. Stop or start monitor mode on wireless interfaces

**Airodump-ng** - used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng. If you have a GPS receiver connected to the computer, airodump-ng can log the coordinates of the found access points. Also, can write out details of access points.

Specific uses:

i) Provides user with list of access points being detected and connected clients

ii) The script provides the user with the

iii) BBSID (Mac Address of wireless access point)

iv) Packets (number of packets sent from client)

v) Station (Mac Address of the station(s) searching for access points)

vi) PWR (signal level reported the card, which usually means the higher the power level the closer to the access point you are)

vii) RXQ (% of packets successfully received of the last 10 seconds

   (a) Its measured overall management and data frames. The received frames contain a sequence number which is added by the sending access point. RXQ = 100 means that all packets were received from the access point in numerical sequence and none were missing. That's the clue, this allows you to read more things out of this value. Let's say you got 100 percent RXQ and all 10 (or whatever the rate) beacons per second coming in. Now suddenly, the RXQ drops below 90, but you still capture all sent beacons. Thus, you know that the AP is sending frames to a client, but you can't hear the client nor the AP sending to the client (need to get closer). Another thing would be, that you got a 11MB card to monitor and capture frames (say a prism 2.5) and you have a very good position to the AP. The AP is set to 54MBit and then again, the RXQ drops, so you know that there is at least one 54MBit client connected to the AP.

viii) Beacons (# of announcement packets sent by the AP)

ix) # Data (# of captured packets, includes broadcast packets)

x) #/s (# of data packets per second over the last 10 seconds)

xi) CH (channel number, taken from the beacon packets)

xii) MB (maximum supported speed for the access point)

xiii) ENC (encryption algorithm used)

- (a) OPN = no encryption used
- (b) WEP? = WEP or higher encryption used
- (c) WEP = static or dynamic WEP encryption used
- (d) TKIP or CCMP = WPA or WPA2

xiv) Cipher (cipher detected)

- (a) CCMP
- (b) WRAP
- (c) TKIP
- (d) WEP
- (e) WEP40
- (f) WEP104

xv) AUTH (authentication protocol used)

- (a) MGT = WPA/WPA2 using a separate authentication server
- (b) SKA = shared key for WEP
- (c) PSK = pre shared key for WPA/WPA2
- (d) OPN = open for WEP

xvi) Lost (number of data packets lost in the last 10 seconds)

xvii) Probes (ESSIDs probed by the client, which means the client is trying to connect the networks that it is not currently connected to)

a. Aireplay-ng - main use is to inject packets into a network. Primarily injects packets into the network so aircrack-ng can use the packets and info gathered later for cracking WEP and WPA2-PSK.

i) Attack 0: Deauthentication

- (a) This attack method is used in the cracking of WPA2 to allow airodump-ng to capture the WPA handshake from the access point.

i) Attack 1: Fake authentication
ii) Attack 2: Interactive packet replay
iii) Attack 3: ARP request replay attack
iv) Attack 4: KoreK chopchop attack
v) Attack 5: Fragmentation attack

vi) Attack 6: Cafe-latte attack
vii) Attack 7: Client-oriented fragmentation attack
viii) Attack 8: WPA Migration Mode
ix) Attack 9: Injection test

**Aircrack-ng** - Used to recover WEP key once enough encrypted packets have been captured using airodump-ng.

Methods used:

1) PTW(Pyshkin, Tews, Weinmann) approach:

   a) First phase uses ARP packets to find WEP key. Limited to 40 and 104-bit WEP keys.

      i) Advantage of this approach is you only need a small number of packets captured to crack the WEP key.

2) Default attack in Aircrack-ng

3) FMS/KoreK approach:

      i) Incorporates various statistical attacks to discover the WEP key along with a combination of brute forcing attacks.

4) Dictionary approach:

      i) Only used for cracking WPA/WPA2 pre shared keys

      ii) SSE2 support is included to speed up cracking

      iii) Requires a "four-way handshake"

Aircrack-ng can operate with just EAPOL packets (2 and 3) or packets (3 and 4)

Displayed on screen:

KB = Keybyte

Depth = depth of current key search

Byte = Byte the IVs leaked

Vote = votes indicating this is correct